jamk.fi

SDN-verkon implementointi testiympäristöön

Tomi Auvinen

Opinnäytetyö
Toukokuu 2018
Tekniikan ja liikenteen ala
Insinööri (AMK), Tietotekniikan koulutusohjelma
Tietoverkkotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Auvinen, Tomi	Opinnäytetyö, AMK	31.05.2018
	Sivumäärä 55	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
SDN-verkon implementointi testiympäristöön

Tutkinto-ohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Karo Saharinen, Sampo Kotikoski

Toimeksiantaja(t)
Inmics Oy

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Inmics Oy, joka suunnittelee, rakentaa ja ylläpitää IT-ympäristöjä. Työn tavoitteina oli rakentaa SDN-testiympäristö, jossa voidaan testata nykyisin LAN-verkoissa olevia palveluita, etsiä ja testata näitä korvaavia ohjelmistoja sekä pohtia, onko SDN:stä hyötyä tavallisessa LAN-verkossa. Työssä SDN-testiympäristöön implementoitiin mahdollisuus tietoliikenteen seurantaan, 802.1x-protokolla ja RADIUS.

Opinnäytetyö toteutettiin käyttäen virtuaalisia ja fyysisiä komponentteja. SDN-kontrolleri (Aruba VAN SDN), Ubuntu ja Windows Server 2012 R2 virtualisoitiin VMwaressa oleviin palvelimiin. SDN-kontrollerin tehtävä on hallita kytkimiä OpenFlow-protokollalla sekä monitoroida verkkoa sovelluksen avulla. Tietoliikenteen seurantaa varten asennettiin myös Ubuntu, jossa pyörii sFlowTrend. Päätelaitteiden todentajana toimi Windows Server, jota käytettiin Active Directory- ja NPS-palvelimena. Fyysisinä laitteina verkossa oli HP:n ProCurve 3500yl- ja ProCurve 5406zl-kytkimet, joissa otettiin käyttöön OpenFlow.

Ympäristö toimii, mutta perinteisten palveluiden korvaavat ohjelmistot olivat ongelmallisia. sFlowTrendin korvaava ohjelmisto ei onnistunut kaappaamaan tietoliikennepaketteja, koska tämä ei pystynyt autentikoimaan 5406zl-kytkintä. Sama ohjelmisto kaatuili avatessa tiettyjä valikoita. Pääsynhallintaa korvaavaa ohjelmistoa ei löytynyt kyseiselle kontrollerille. sFlowTrend, 802.1x ja RADIUS saatiin toteutettua perinteisillä menetelmillä.

Kontrolleri on toteutettu Javalla, joten yhteensopivuutta muiden suosittujen kontrollerien ohjelmistojen kanssa ei ole. Ohjelmistotarjonta Aruban omassa sovelluskaupassa on erittäin rajallinen ja uusimmatkin sovellukset ovat vuoden vanhoja. Perinteisen LAN-verkon korvaaminen SDN:llä toteutetulla verkolla on erittäin riskialtista, sillä mukaan tulevat ohjelmistopohjaiset ongelmat.

Avainsanat (asiasanat)

SDN, OpenFlow, Aruba, HP, VAN, sFlowTrend, RADIUS, 802.1x

Muut tiedot (salassa pidettävät liitteet)

jamk.fi

Description

Author(s) Auvinen, Tomi	Bachelor's thesis	31.05.2018
		Language of publication: Finnish
	Number of pages 55	Permission for web publication: x

Title of publication

Implementation of SDN to test environment

Degree programme

Information Technology

Supervisor(s)

Karo Saharinen, Sampo Kotikoski

Assigned by

Inmics Oy

Abstract

The thesis was assigned by Inmics Oy, which designs, builds and maintains IT environments. The aim was to build an SDN test environment to test services currently in use in LAN networks, to find and test replacement software of these services and to consider if traditional LAN network can benefit from SDN. In this thesis, telecommunications monitoring, 802.1x protocol and RADIUS are implemented to the SDN test environment.

The thesis was carried out using virtual and physical components. Aruba VAN SDN, Ubuntu, and Windows Server 2012 R2 were virtualized on VMware servers. The task of the SDN controller was to manage switches with the OpenFlow protocol and to perform network monitoring with the application. Ubuntu was also installed for monitoring telecommunications, with sFlowTrend running. Verifier of the end hosts was Windows Server, which was used as an Active Directory and NPS server. The physical devices included the HP ProCurve 3500yl and ProCurve 5406zl switches, which introduced OpenFlow to the network.

The environment works, however, the software replacing traditional services was problematic. The replacement software for sFlowTrend failed to capture communication packets because it was unable to authenticate 5406zl switch. The same software crashed when trying to open certain menus. A software replacing access control was not found for that controller. sFlowTrend, 802.1x and RADIUS were implemented using traditional methods.

The controller is coded in Java; hence, there is no compatibility with other popular controllers' software. The software supply in Aruba's own application store is very limited and the latest applications are one year old. Replacing a traditional LAN network with an SDN is very risky because it also introduces software-based problems.

Keywords/tags (subjects)

SDN, OpenFlow, Aruba, HP, VAN, sFlowTrend, RADIUS, 802.1x

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
EAPOL	Extensible Authentication Protocol over Local Area Network
GUI	Graphical User Interface
HP	Hewlett Packard
HPE	Hewlett Packard Enterprise
L2	Layer2
L3	Layer3
LAN	Local Area Network
NPS	Network Policy Server
NTP	Network Time Protocol
OF	OpenFlow
ONF	Open Networking Foundation
OSGi	Open Service Gateway initiative
OU	Organizational Unit
OVA	Open Virtual Appliance
OVSDB	Open Virtual Switch Database
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Services
REST	Representational State Transfer
SDN	Software-Defined Networking
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VAN	Virtual Application Network
VLAN	Virtual Local Area Network

1 Lähtökohdat

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Jyväskylästä lähtöisin Inmics Oy. Yritys suunnittelee, rakentaa sekä ylläpitää edistyksellisiä IT-ympäristöjä. Inmics tarjoaa laajan valikoiman ICT-ratkaisuja ja-tuotteita, kuten tietoturvaratkaisut, järjestelmäkonsultoinnit ja projektit, tietoverkkojen toteutukset, laitteiden elinkaaren hallinta sekä pääsynhallintaratkaisut. Toimipaikkoja on kahdeksan, joista päätoimipaikka on Jyväskylässä. Muut toimipaikat ovat Helsinki, Lahti, Tampere, Kuopio, Joensuu, Vaasa ja Oulu. Yritysksen palveluksessa on tällä hetkellä n. 200 työntekijää. Kesäkuussa 2017 päättyneen tilikauden liikevaihto oli n. 42,7 miljoonaa euroa. (Liikevaihto ja henkilöstö & Sertifioitua osaamista)

1.2 Toimeksianto ja tavoitteet

Opinnäytetyön tavoitteena oli rakentaa SDN-testiympäristö. Ympäristössä oli tarkoitus testata normaaleissa verkkoympäristöissä käytössä olevia palveluita ja ratkaisuja, käyttäen Aruban SDN-kontrolleria ja OpenFlow-kytkimiä. Ympäristöön toteutettiin IEEE 802.1X-standardi käyttäen porttikohtaista- ja MAC-autentikointia sekä tietoliikenteen seurantaa. Tarkoituksena oli myös seurata, onko SDN-verkosta hyötyä käytettäessä kyseisiä palveluita perinteisessä LAN-verkossa sekä löytyykö työssä käytettäville palveluille valmiiksi korvaajia SDN-sovellusten muodossa. Ympäristön tarkoituksena oli myös toimia apuna SDN sertifikaattien läpäisyssä, sillä yrityksen pyrkimyksenä on pysyä kehityksen kärjessä sertifioimalla henkilöstöä uusimpien teknologioiden huippuosaajiksi.

Käytännön osuudessa suunniteltiin SDN-testiympäristö. Ympäristön tarkoituksena on toimia suljettuna ympäristönä, johon on helppoa lisätä uusia palveluita, joita mahdollisesti halutaan tutkia ja testata. Ympäristöstä mahdollistetaan haluttaessa yhteys ulkoverkkoon. Työssä oli käytössä kaksi HP:n kytkintä, jotka hyödyntävät OpenFlow-protokollaa sekä VMwareen virtuaalisoituja palvelimia, joissa pyörii SDN-kontrolleri, Active Directory (AD)- ja sFlow-palvelin.

2 Käytetyt tekniikat

2.1 Software-Defined Networking

2.1.1 Yleistä

Open Networking Foundation (ONF) on voittoa tavoittelematon konsortio, joka johtaa Software-Defined Networking (SDN) kehitystä sekä arkkitehtuuriin liittyvien kriittisten elementtien standardointia, kuten OpenFlow (OF)-protokolla. Organisaatio keskittyy edistämään ohjelmistopohjaisen verkon käyttöä avoimen standardin kehittämisen kautta. ONF:n perustivat Deutsche Telekom, Facebook, Google, Microsoft, Verizon ja Yahoo! vuonna 2011. Tällä hetkellä ONF:ään kuuluu yli 125 yritystä. (Who is the Open Networking Foundation?)

Nykypäivänä tietoverkkojen täytyy olla nopeampia ja joustavampia kuin koskaan aikaisemmi, mutta niistä on tullut vain monimutkaisempia ja vaikeampia hallita. Verkkojen provisiointi uusille sovelluksille ja käyttäjille vaatii huomattavan paljon aikaa, jolloin myös liikekulut kasvavat. (HP, Creating HP Software-defined Networks 2014, 1-6)

Software-Defined Networking (SDN) on lähestymistapa verkon virtualisointiin, joka pyrkii optimoimaan verkon resursseja sekä nopeasti sopeutumaan muuttuviin liiketoiminnan tarpeisiin, sovelluksiin ja tietoverkon liikenteeseen. SDN-verkko toimii erottamalla ohjaus- ja välitystaso toisistaan ja luomalla ohjelmoitavan infrastruktuurin joka on erillään fyysisistä laitteista. (What is SDN?)

SDN-verkoissa tietoverkon organisointia, hallintaa, analysointia ja automatisointia hoitaa SDN-kontrolleri. SDN-kontrollerit eivät ole verkkolaitteita, joten ne voivat myös hyödyntää nykyaikaisten pilvipalveluiden skaalautuvuutta, suorituskykyä, saatavuutta ja tallennustilan resursseja. Suuri osa SDN-kontrollereista on rakennettu avoimelle alustalle käyttäen avoimia standardeja ja avoimia ohjelmointirajapintoja, jolloin verkko voi toimia laitevalmistajasta riippumatta. (What is SDN?)

2.1.2 Arkkitehtuuri

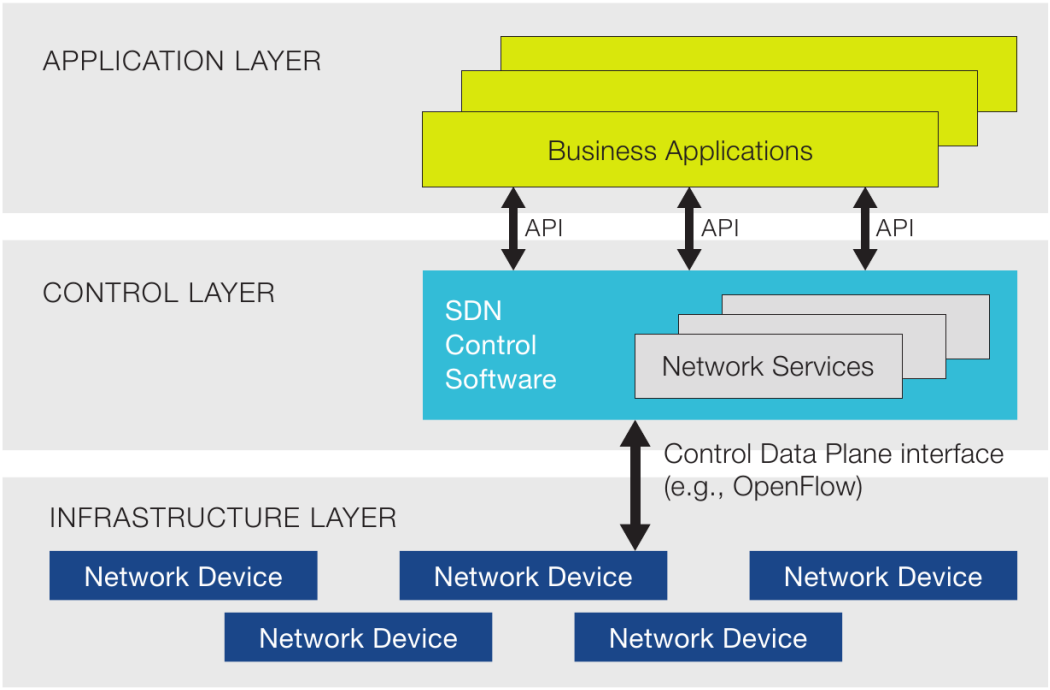
SDN arkkitehtuuri määrittelee, kuinka verkko- ja tietojärjestelmät voidaan rakentaa käyttäen avoimia ohjelmistopohjaisia tekniikoita yhdessä perinteisten verkkolaitteiden kanssa, jotka erottavat ohjaus- ja välitystason toisistaan. (Understanding the SDN Architecture)

Perinteisessä verkkoarkkitehtuurissa ohjaus- ja välitystasot on pakattu valmistajien yksinoikeudelliseen integroituun koodiin, jonka on jakanut yksi tai useampi verkkolaite valmistaja. Vuonna 2008 julkaistu OpenFlow-standardi tunnistettiin ensimmäisenä SDN-arkkitehtuurina, joka määritteli, kuinka ohjaus- ja välitystason elementit tulisi eritellä toisistaan ja kuinka näiden välillä kommunikoidaan käyttäen OpenFlow-protokollaa. (Understanding the SDN Architecture)

SDN-arkkitehtuurissa ohjaus- ja välitystason jakamista kutsutaan ”hajautukseksi”, koska nämä voidaan sijoitella erikseen, eikä sijoitettuna yhtenä integroituna järjestelmänä. Tämä arkkitehtuuri antaa sovelluksille enemmän lisätietoa koko verkon tilasta verkon kontrollerilta. (Understanding the SDN Architecture)

Kuvio 1 esittelee SDN-arkkitehtuurin kolme yleistä komponenttia. (The New Norm for Network 2012)

1. SDN-sovellukset ovat ohjelmia jotka viestivät SDN-kontrollerin kanssa käyttäytymistä ja tarvittavia resursseja Application Programming Interface (API) avulla. Lisäksi sovellukset voivat rakentaa abstraktin kuvan verkosta keräämällä informaatiota kontrollerilta tehdäkseen päätöksiä. Näihin sovelluksiin voi sisältyä verkonhallintaa, analyysia tai yrityssovelluksia, joita käytetään suurten datakeskusten käyttämiseen. Esimerkiksi analyysisovellus voidaan rakentaa tunnistamaan epäilyttävää verkkoaktiviteettiä turvallisuustarkoituksin.
2. SDN-kontrolleri on looginen kokonaisuus, joka vastaanottaa käskyt tai vaatimukset SDN-sovelluskerrokselta ja välittää ne verkkolaitteille. Kontrolleri myös kerää tietoja verkosta verkkolaitteilta ja kommunikoi tämän takaisin SDN-sovelluksille abstraktilla verkon näkymällä, mukaan lukien tilastot ja tapahtumat.
3. SDN-verkkolaitteet kontrolloivat verkon edelleenlähetys- ja tietojenkäsittely-ominaisuuksia. Tähän sisältyy polun edelleenlähetys ja käsittely.



Kuvio 1. SDN-arkkitehtuuri

2.2 OpenFlow

2.2.1 Yleistä

OpenFlow on ensimmäinen standardi, joka määrittelee kommunikaatiorajapinnan ohjaus- ja välityskerrokselle SDN-arkkitehtuurissa. OpenFlow-protokolla esiteltiin ensimmäisen kerran vuonna 2008 tarjotakseen vaihtoehdon valmistajien omille ratkaisuille, jotka rajoittavat joustavuutta ja lukitsevat käyttämään tietyn valmistajan laitteita. Määritelmä oli suunniteltu siten, että tutkijat voivat tehdä kokeiluja heterogeenisiä kytkimiä ja reitittimiä yhdenmukaisella tavalla ilman, että toimittajat joutuvat altistamaan tuotteidensa sisäistä toimintaa tai vaatimaan tutkijoita koodaamaan valmistajakohtaista hallinnointiohjelmia. (Software-Defined Networking 2012, 8.)

OpenFlow-protokolla rakentaa kommunikaation ohjaus- ja välitystason välille tuetuilla verkkolaitteilla. OpenFlow sallii suoran pääsyn ja manipuloinnin fyysisten ja virtuaalisten verkkolaiteiden välitystasolle. Avoimen rajapinnan puute välitystasolla on johtanut siihen, että nykyiset verkkolaitteet ovat monoliittisia ja suljettuja. (Software-Defined Networking 2012, 8.)

2.2.2 Höydyt

OpenFlow-pohjaiset SDN-teknologiat mahdollistavat dynaamisemman verkon, adaptoitumalla jatkuvasti verkon muuttuviin tarpeisiin sekä vähentämällä verkon operaatioita ja helpottamalla laitteiden hallintaa. SDN-kontrolleri voi hallita mitä tahansa verkkolaitteita, joissa on OpenFlow käytössä. Tällöin verkkoon saadaan tehtyä helposti ja nopeasti muutoksia yhden laitteen kautta. (Software-Defined Networking 2012, 10.)

OpenFlow-pohjainen SDN tarjoaa joustavan verkon automaation ja hallintakehyksen. Tämä mahdollistaa työkalujen kehityksen, jotka automatisoivat monia hallintaan liittyviä tehtäviä. Nämä automaatiotyökalut vähentävät yleiskustannuksia, verkon epävakautta operaatiovirheiden kautta. (Software-Defined Networking 2012, 11.)

Tietoturvan kannalta OpenFlow-pohjainen SDN-verkko poistaa tarpeen konfiguroida jokainen verkonlaite erikseen aina, kun päätepiste, palvelu tai sovellus lisätään tai siirretään tai jos käytännöt muuttuvat. Koska SDN-kontrolleri tarjoaa täydellisen näkyvyyden ja hallinnan verkosta, tällä voidaan varmistaa, että pääsynhallinta, palvelunlaatu, turvallisuus ja muut käytännöt ovat käytössä langallisessa ja langattomassa verkossa, mukaan lukien muiden toimipisteiden konttorit, kampukset ja konesalit. Yritykset ja operaattorit hyötyvät vähenevistä operaatiokustannuksista, dynaamisemmasta konfiguraatioista ja johdonmukaisesta käytäntöjen täytäntöönpanosta. (Software-Defined Networking 2012, 11.)

2.3 OpenFlow-kytkin

2.3.1 Yleistä

Perinteiset kytkimet jakavat tehtävät hallinta-, ohjaus- ja välitystasoille. Välitystaso sisältää kanavat, jotka vastaanottavat ja siirtävät liikennettä. Tämä taso sisältää myös ohjaukseen liittyviä elementtejä, kuten pakettien prosessointi ja järjestely.

Ohjaustaso ohjelmoi välitystason tauluja niin paljon kuin mahdollista laitteistotasolla. Suurimmaksi osaksi ohjaustaso toimii ohjelmistolla, joka rakentaa kehykset perustuen Layer2 (L2) ja Layer3 (L3)-protokolliin. Ohjaustaso suorittaa reititysprotokollat ja

rakentaa reititystaulun. Se myös suorittaa L2-protokollat kuten Spanning Tree Protocol (STP). Osana sen tehtäviä, tämä taso generoi liikenteen joka on lähtöisin kytkimeltä, kuten reititysprotokolla päivitykset ja Bridge Protocol Data Unit (BPDU).

Jokaisella kytkimellä on oma keskitetty hallintataso. Yhdistäessä kytkimeen konsolin, Telnet:n, Secure Shell:in (SSH) tai muun istunnon kautta, liikennöinti tapahtuu hallintatason kautta. (Creating HP Software-defined Networks 2014, 3-4.)

2.3.2 OpenFlow-kanava

OpenFlow-kanava on rajapinta joka yhdistää jokaisen loogisen OpenFlow-kytkimen OpenFlow-kontrolleriin. Tämän rajapinnan kautta kontrolleri konfiguroi ja hallitsee kytkintä sekä vastaanottaa tapahtumia kytkimiltä ja lähettää paketit kytkimestä. OpenFlow-kytkin tukee yhtä tai useampaa OpenFlow-kanavaa, mahdollistaen useamman kontrollerin jakaa kytkimen hallinta. Yleensä OpenFlow-kanava salataan käyttäen TLS:ää, mutta sitä on myös mahdollista käyttää suoraan TCP:n yli. (OpenFlow Switch Specification 2015, 38.)

2.3.3 OpenFlow Switch Protocol

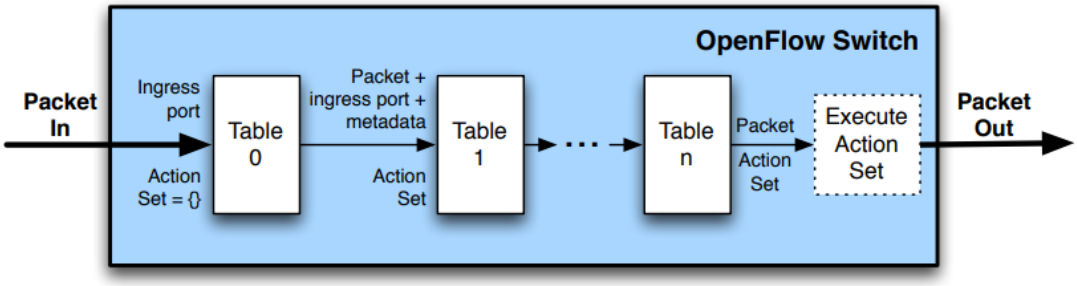
OpenFlow-kytkin koostuu yhdestä tai useammasta vuotaulusta, ryhmätaulusta ja OpenFlow-kanavasta ulkoiselle kontrollerille. OpenFlow Switch-protokolla tukee kolmea erilaista viestityyppiä, *controller-to-switch*, *asynchronous* ja *symmetric*, joista kullakin on useita eri alatyyppejä. *Controller-to-switch*-viestit lähtevät kontrollerilta ja niitä käytetään suoraan kytkimien tilan tarkistukseen ja hallintaan. *Asynchronous*-viestit lähtevät kytkimeltä. Näitä käytetään päivittämään kontrollerille tietoja verkon tapahtumista ja muutoksista kytkimen tilassa. *Symmetric*-viestejä voi lähettää kytkin ja kontrolleri ilman ilmoitusta. (OpenFlow Switch Specification 2015, 38.)

2.3.4 OpenFlow-only & OpenFlow-hybrid

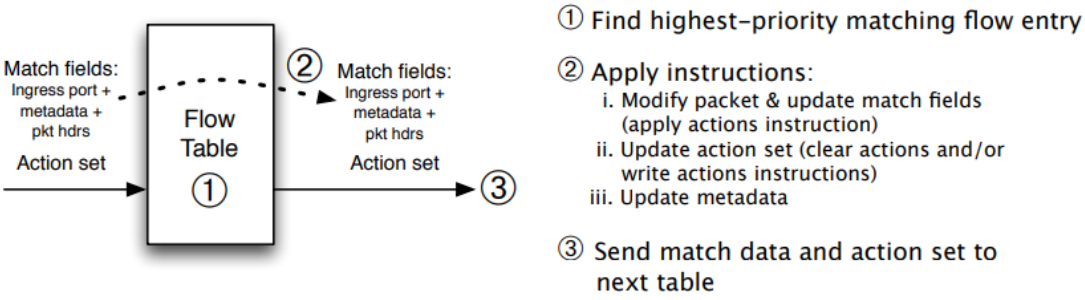
OpenFlow-sopivia kytkimiä on kahden tyyppisiä: OpenFlow-only ja OpenFlow-hybrid. OpenFlow-only-kytkimet tukevat vain OpenFlow operaatioita. Näissä kytkimissä kaikki paketit prosessoidaan OpenFlow-pipelinen mukaan, eikä niitä voida prosessoida muulla tavalla.

OpenFlow-hybrid-kytkimet tukevat OpenFlow operaatioita ja perinteisiä L2-kytkentöjä, L3-reitityksiä sekä prosesseja kuten Access Control List (ACL) ja Quality of Service (QoS). Näiden kytkimien täytyy tarjota OpenFlow'n ulkopuolella tapa, jolla liikenne ohjataan, joko OpenFlow- tai normaaliin pipelineen. Esimerkiksi kytkin voi käyttää Virtual LAN (VLAN) tunnistetta tai tuloporttia päättääkseen, mitä pipelineen ohjataan tai se voi ohjata kaikki paketit suoraan OpenFlow-pipelineen.

Jokainen OpenFlow-pipeline voi sisältää useita vuotauluja, joista jokainen sisältää useita vuomerkintöjä. OpenFlow-pipeline määrityksen määrittävät, kuinka paketit käyttäytyvät vuotaulujen kanssa. Kuviossa 2 on esitetty OpenFlow-pipeline toimintaa. (OpenFlow Switch Specification 2015, 19.)



(a) Packets are matched against multiple tables in the pipeline



(b) Per-table packet processing

Kuvio 2. OpenFlow-pipelinen toiminta

2.4 SDN-kontrolleri

2.4.1 Yleistä

SDN-kontrolleri on SDN-verkon ”aivot”. Sovellus toimii strategisena ohjauspisteenä SDN-verkossa, joka hallitsee datan välitystä kytkimille ja reitittimille Southbound APIn ja sovelluksille Northbound APIn kautta saadakseen verkkoon älykkyyttä. Organisaa-

tioiden ottaessa käyttöön lisää SDN-verkkoja, kontrollien täytyy yhdistyä samaan toimialueeseen käyttäen yleisiä sovellusrajapintoja, kuten OpenFlow ja Open Virtual Switch Databasea (OVSDB). (What are SDN Controllers?)

Tyypillisesti SDN-kontrollerialusta koostuu kokoelmasta ”liitettäviä” moduuleja, jotka suorittavat erilaisia verkkoon liittyviä tehtäviä, kuten mitä laitteita verkossa on ja näiden ominaisuuksien sekä verkkotilastojen kerääminen. Kontrollerille voidaan lisätä moduuleja jotka parantavat toimintoja ja tukevat kehittyneempiä ominaisuuksia, kuten algoritmeja jotka suorittavat analytiikkaa ja uusien sääntöjen luontia verkossa. (What are SDN Controllers?)

2.4.2 Northbound-rajapinta

Northbound APIa käytetään SDN-kontrollerin kommunikointiin palveluiden ja sovellusten kanssa. Tätä voidaan käyttää helpottamaan innovaatiota ja mahdollistamaan verkon tehokasta organisointia ja automatisointia, mukautuakseen eri sovellusten vaatimuksiin. (What are SDN Northbound APIs?)

Northbound API on epäilemättä kriittisin API-rajapinta SDN-ympäristössä, koska SDN:n arvo on sidoksissa innovatiivisiin sovelluksiin joita se voi tukea ja mahdollistaa. Koska sovellukset ovat kriittinen osa SDN-verkkoa, Norhtbound APIn täytyy tukea paljon erilaisia sovelluksia ja ei ole olemassa yhtä joka sopii kaikille. Tästä johtuen Northbound API on tällä hetkellä kaikista epämääräisin komponentti SDN-ympäristössä. Kontrollerille on olemassa useita erilaisia mahdollisia rajapintoja eri paikoissa, joilla hallita eri sovelluksia. Northbound API-rajapinnan kautta voidaan optimoida monia erilaisia verkkosovelluksia, kuten kuormanvakaajia, palomuureja ja muita ohjelmistopohjaisia tietoturvapalveluita sekä sovellusten orkestrointia pilviresursseille. (What are SDN Northbound APIs?)

Kyseistä rajapintaa käytetään myös integroitaessa SDN-kontrolleria automaatiopinojen kanssa, kuten Puppet ja CFEngine sekä orkestrointialustojen kuten OpenStack, VMware:n vCloudDirector sekä CloudStack. Tavoitteena on tiivistää verkon sisäiset toiminnot siten, että sovelluskehittäjät voivat ”kytkeytyä” verkkoon ja tehdä muutoksia sovelluksen tarpeiden mukaan ilman, että heidän on ymmärrettävä tarkasti mitä tämä tarkoittaa verkolle. (What are SDN Northbound APIs?)

Hiljattain ONF käänsi keskittymisensä Northbound API-rajapintaan ja perusti ’Northbound Working Group’ nimisen työryhmän. Ryhmän tehtävänä on koodata, kehittää prototyyppejä ja tarkastella, tehdäänkö rajapinnalle oma standardia selkeyttääkseen mitä se on ja mitä sillä tehdään. (What are SDN Northbound APIs?)

2.4.3 Southbound-rajapinta

Southbound API-rajapintaa käytetään SDN-kontrollerin ja verkkolaitteiden väliseen kommunikointiin. Tämän tehtävänä on helpottaa tehokasta verkon hallintaa ja mahdollistaa kontrollerin tehdä dynaamisesti muutoksia perustuen reaaliaikaisiin vaatimuksiin ja tarpeisiin. (What are SDN Southbound APIs?)

OpenFlow on tunnetuin Southbound API-rajapinta, mutta ei ainoa saatavilla tai kehityksessä. OpenFlow:sta on tullut alan standardi, jota tukee useat isot verkkolaite valmistajat, kuten Cisco, Juniper, Big Switch, Brodace, Extreme Networks, IBM, Dell ja HP monien muiden lisäksi. Korvaavia vaihtoehtoja OpenFlow:lle on mm. POX, Beavcon, Floodlight ja OpenDaylight, joka on Linux Foundationin kanssa yhteystyössä tehty projekti, jota myös tukee moni iso valmistaja kuten Cisco ja Big Switch. (What are SDN Southbound APIs?)

2.5 sFlow

SFlow on usean laitevalmistajan näytteenottotekniikka, joka sulautettu kytkimiin ja reitittimiin. Se tarjoaa kyvyn seurata sovellustason liikennevirtoja kaikissa rajapinnoissa samanaikaisesti. SFlow-agentti on laitteessa oleva ohjelmistoprosessi, joka toimii osana verkon hallintaohjelmistoa. Se yhdistää rajapinnan laskurit ja virtausnäytteen sFlow-datagrammeiksi, joka lähetetään verkon yli sFlow-kerääjälle. Yleisimmin pakettien näytteenoton suorittaa reitittimien ja kytkimien Application Specific Integrated Circuit (ASIC), joka on suunniteltu suorittamaan tiettyjä tehtäviä erittäin tehokkaasti. Jokaisen paketin mukana tallennetaan myös reititystauluun tehdyt merkinnät. (Traffic Monitoring using sFlow)

SFlow-agentti tekee erittäin vähän prosessointia, se vain paketoi datan sFlow-datagrammeiksi, jotka välittömästi lähetetään verkkoon. Datan välittäminen välittömästi

vähentää sFlow-agentin tarvitseman muistin ja prosessorin vaatimukset. SFlow-agentit ympäri verkon lähettävät jatkuvasti sFlow-datagrammeja keskitetylle sFlow-kerääjälle, jossa ne analysoidaan tuottaakseen reaaliaikaisia verkonlaajuista kuvaa liikennevirroista. (Traffic Monitoring using sFlow)

2.6 TShark

TShark on verkkoprotokolla analysaattori, jonka avulla voidaan kaapata paketteja dataa suoraan verkosta tai lukea paketit aikaisemmin tallennetusta tiedostosta. TSharkin natiivi talteenotto tiedostomuoto on pcap-formaatti, joka on myös tcpdumpin ja erilaisten muiden työkalujen käyttämä muoto. Se pystyy tunnistamaan, lukemaan ja kirjoittamaan samoja kaappaustiedostoja joita muun muassa suosittu Wireshark tukee. (TShark)

2.7 Active Directory Domain Services

Active Directory Domain Services (AD DS) on palvelu, jonka tehtävänä on varastoida yrityksen henkilökunnan perustietoja sekä turvallisuuspolitiikkaan liittyvä asetuksia kuten käyttäjän oikeuksia. AD DS huolehtii esimerkiksi käyttäjätunnusten, että muiden perustietojen kuten nimen, syntymäajan ja sähköpostiosoitteen varastoimisesta sekä näiden tietojen tarjoamisesta niitä kysyttäessä. Henkilökunnan kirjautuessa sisään yrityksen järjestelmään, yrityksen tietojärjestelmä ottaa yhteyttä AD-hakemistoon ja vertaa kirjautumisessa kysyttyjä tietoja hakemistossa oleviin tietoihin. Tämän perusteella joko annetaan käyttäjälle lupa kirjautua sisään tai evätään kirjautumisyritys ja estetään käyttäjän pääsy verkon resursseihin. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko, 2017.)

Palvelimiin, jotka hallinnoivat Active Directoryä viitataan nimellä Domain Controller tai lyhenteellä DC. DC-palvelimilla voi olla erilaisia rooleja. AD DS määrittelee viisi Primary Master roolia; skeema master, domain naming master, relative identifier master (RID), primary domain controller (PDC) sekä infrastructure master. Näin voidaan määrittää palvelimelle oma tehtävä domainissa. Tämä voi myös epäjohdonmukaisuuksiin AD- tietokannassa, koska useat eri DC- palvelimet voivat tehdä ristiriitaisia merkintöjä tietokantaan. (Auvinen ym. 2017)

2.8 Network Policy Server

2.8.1 NPS periaate

Network Policy Server (NPS) on Microsoftin toteutustapa RADIUS palvelimesta. RADIUS palvelimena NPS suorittaa keskitettyä yhteyden todennusta, valtuutusta ja tilastointi erityyppisille verkkoonliittymismenetelmille. NPS-palvelimen ollessa osana toimialuetta NPS käyttää directory servicea käyttäjätilien tietokantana ja on osa kertakirjautumismenetelmää. RADIUS palvelimella on valtuudet päästä käsiksi käyttäjien tilitietoihin ja todentaa verkkoon yrittävän tunnuksen käyttäjätiedot. Jos käyttäjätiedot ovat autenttisia ja yhteysyritys hyväksytään, RADIUS-palvelin valtuuttaa käyttäjän pääsyä verkkoon määritettyjen olosuhteiden mukaan ja kirjaa tapahtuman lokiin. RADIUS palvelimen käyttö mahdollistaa todennus, valtuutusj a tilastointidatan keräämisen ja säilyttämisen keskitetyllä sijainnilla, eikä erikseen jokaisessa access-palvelimessa. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko, 2017.))

2.8.2 NAP

NAP auttaa suojaamaan pääsyä yksityisiin verkkoihin varmistamalla, että asiakaskoneet on konfiguroitu organisaation terveyskäytänteiden mukaisesti, ennen kuin niille annetaan pääsy verkon resursseihin. Terveyskäytänteitä voidaan määrittää Network Policy serverillä. Terveyskäytänteet voivat sisältää mm. ohjelmistovaatimuksia, tietoturvavaatimuksia ja vaadittuja konfiguraatioasetuksia. NAP estää koneiden pääsyn verkkoon, jos ne eivät toteuta näitä vaatimuksia. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko, 2017.)

2.9 RADIUS

2.9.1 RADIUS toiminta

Remote Authentication Dial-In User Services (RADIUS) on protokolla, jonka avulla hallitaan käyttäjien pääsyä palveluun. RADIUS-palvelin vastaanottaa käyttäjän yhteyspyynnöt, tunnistaa käyttäjän ja palauttaa vaaditut konfiguraation tiedot asiakkaalle,

jotta käyttäjä voi yhdistyä AD:hen. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko, 2017.)

2.10 AAA

AAA-malli mahdollistaa keskitetyn hallinnan ja tietoturvan verkossa. Se muodostuu nimensä mukaisesti kolmesta A:sta. Authentication eli todennus, Authorization eli valtuutus ja Accounting eli tilastointi. Näistä Authentication tarkistaa kuka olet, Authorization tarkistaa mitä saat tehdä ja Accounting kirjaa ylös mitä teit ollessasi palvelussa. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko, 2017.)

Autentikointi perustuu verkkomaailmassa useimmiten ”mitä tietoa sinulla on?” kysymykseen. Perinteinen tapa on ollut käyttäjätunnus ja salasana, mutta autentikointi voi myös perustua ”mitä sinulla on?” kysymykseen. Tällöin palvelu voi käyttää tunnistamiseen esimerkiksi käyttäjätunnusta ja jaettua salausavainta. (Auvinen ym. 2017.)

Valtuuttaminen mahdollistaa keskitetyssä käyttäjänhallinnassa eri käyttäjien oikeuksien rajoittamisen erilaisille tasoille. Näin voidaan esimerkiksi hallita, onko käyttäjällä oikeuksia muokata konfiguraatioita tai katsoa tietoja laitteista ja ohjelmista. Hyvin skaalautuvan hallittavuuden kannalta paras keino oikeuksien hallintaan on luoda erilaisia ryhmiä ja määritellä niille oikeudet. Käyttäjiä voidaan tarvittaessa lisätä tai poistaa ryhmistä, tarjoten näin myös tarvittavat oikeudet verkon ja sen palveluiden käyttäjälle. (Auvinen ym. 2017.)

Tilastoinnin avulla voidaan seurata ja tallentaa tietoa esimerkiksi istunnoista. Tiedot on mahdollista tallentaa vaikkapa ulkoiselle palvelimelle, ennalta määriteltyjen parametrien täyttyessä. Usein seurattuja asioita ovat esimerkiksi aiemmin mainittu verkkoistuntojen seuranta, yhteyksien seuranta, jolla voidaan tarkastella mistä osoitteista yhteyksiä muodostettiin ja kauanko yhteys kesti sekä järjestelmäkirjanpito, joka tallentaa tietoa järjestelmätapahtumista, kuten sammutuksista ja virheistä. (Auvinen ym. 2017.)

AAA-palveluita tarjoamaan perustetaan usein dedikoitu AAA-palvelin. Nykyinen käytänne jolla NAS (Network Access Server) toimi yhteen AAA-palvelimen kanssa on Remote Authentication Dial-In User Service eli RADIUS. (Auvinen ym. 2017.)

2.11 IEEE 802.1X

2.11.1 Yleistä

IEEE 802.1X-standardi on porttikohtainen autentikointimenetelmä. Standardi määrittelee asiakas- ja palvelinpohjaisen pääsynvalvonnan ja todentamisprotokollan, joka rajoittaa luvattomia asiakkaita liittymästä lähiverkkoon yleisesti saatavilla olevien porttien kautta. Todennuspalvelin autentikoi jokaisen asiakkaan, joka on liittynyt kytkimen porttiin ja määrittää Virtual Local Area Network:in (VLAN) portille, ennen kuin kytkin tai Local Area Network (LAN) tarjoaa asiakkaalle palveluita. Ennen kuin asiakas on autentikoitu, 802.1X-pääsynhallinta sallii vain Extensible Authentication Protocol over LAN (EAPOL) liikenteen portista, johon asiakas on yhdistynyt. Autentikoinnin onnistuttua normaali liikenne sallitaan portista. (IEEE 802.1X Port-Based Authentication)

2.11.2 802.1X laitteiden roolit

802.1X autentikointia käytettäessä jokaisella verkon laitteella on tietty rooli. Näitä rooleja ovat asiakas, kytkin ja todennuspalvelin. Asiakas eli työasema pyytää pääsyä LAN-verkkoon sekä kytkimen palveluihin ja vastaa kytkimen pyyntöihin. Työaseman täytyy käyttää 802.1X yhteensopivaa ohjelmistoa. Todennuspalvelin, eli Remote Authentication Dial-In User Service (RADIUS)-palvelin suorittaa asiakkaiden autentikoinnin. Palvelin vahvistaa asiakkaan identiteetin ja ilmoittaa kytkimelle, onko asiakas valtuutettu pääsemään LAN-verkkoon ja kytkimen palveluihin. Kytkin kontrolloi asiakkaan fyysistä pääsyä verkkoon, perustuen tämän autentikoinnin tilaan. Kytkin toimii välityspalvelimena asiakkaan ja todennuspalvelimen välillä pyytäen identiteetti tietoja asiakkaalta ja varmistaakseen nämä tiedot todennuspalvelimella ja välittääkseen vastauksen asiakkaalle. Kytkin sisältää oman RADIUS-asiakasohjelmistonsa, joka vastaa EAP-kehyksen kapseloimisesta ja tämän purkamisesta sekä vuorovaikutuksesta todennuspalvelimen kanssa. (IEEE 802.1X Port-Based Authentication)

2.11.3 802.1X Host-tilat

802.1X-portin Host-tilat määrittävät, voidaanko useampi kuin yksi asiakas autentikoida samasta portista ja kuinka autentikointi pakotetaan. Single-Host-tilassa vain

yksi asiakas voi yhdistää 802.1X-portin kautta. Kytkin tunnistaa asiakkaan lähettämällä EAPOL-kehyksen, jolloin portin tila muuttuu ylhäällä olevaksi. Jos asiakas poistuu tai korvataan toisella, kytkin vaihtaa portin tilan takaisin alhaalla olevaksi ja portti palaa valtuuttamattomaan tilaan. Multiple-Hosts-tilassa yhteen 802.1X-porttiin voidaan kytkeä useita asiakkaita. Tässä tilassa vain yhden liitetyistä asiakkaista täytyy olla valtuutettu, jotta kaikilla asiakkailla on pääsy verkkoon. Jos portti muuttuu valtuuttamattomaan tilaan, kytkin estää pääsyn verkkoon kaikilta liitetyiltä asiakkailta. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko)

2.11.4 802.1X VLAN Assignment

Onnistuneen tunnistautumisen jälkeen RADIUS-palvelin lähettää VLAN-tiedot 802.1X-portin asetuksia varten. RADIUS-palvelimella on tietokanta, joka liittää käyttäjät heille määrättyihin VLAN:hin. Multiple-hosts –tilassa kaikki asiakkaat määrätään samaan VLAN:iin, jossa ensimmäinen kytkimen porttiin todennettu asiakas on RADIUS-tietokannassa. Multiauth-tilassa VLAN-määrittelyt jätetään huomiotta. Mikäli RADIUS-palvelimella ei ole asetettu VLAN-tageja, portin VLAN jää rajapinta-asetuksissa määriteltyyn tilaan. (Auvinen, Filtshev, Haavisto, Meisalmi, Mäki-Ullakko)

2.12 SNMP

Simple Network Management Procotol eli SNMP on sovelluskerroksen protokolla, jota käytetään verkkolaitteiden hallintaan sekä ominaisuuksien monitorointiin. SNMP tarjoaa yhtenäisen kielen verkkolaitteille välittääkseen hallintatietoja LAN tai WAN-verkoissa. Versio kolme on uusin iteraatio SNMP:stä, tämä sisältää tietoturva parannuksia, jotka tunnistavat ja salaavat SNMP-viestit sekä suojaavat niitä kuljetuksen aikana. (SNMP)

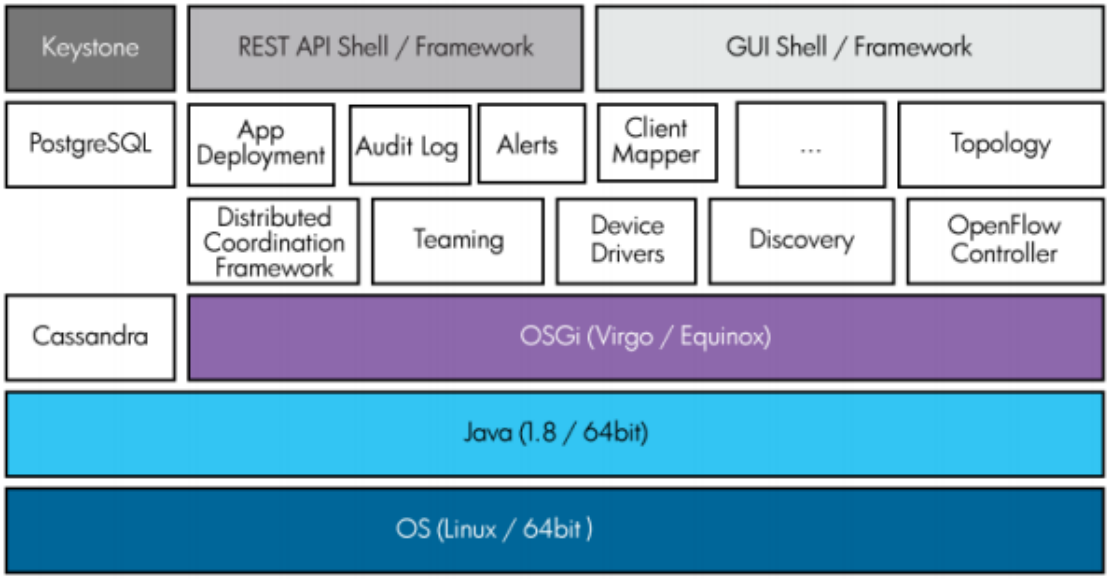
SNMP suorittaa lukuisia toimintoja verkkolaitteiden ja hallintajärjestelmien välillä *pusht and pull*-periaatteella. Se voi suorittaa luku ja kirjoitus komentoja, kuten salasanan resetointi tai tehdä konfiguraatioon muutoksia. Useimmissa tapauksissa SNMP toimii synkronisessa mallissa, jossa *SNMP manager* aloittaa kommunikaation ja *SNMP agent* vastaa tähän. Tyypillisesti nämä komennot ja viestit lähetetään käyttäen User Datagram Protocol (UDP) tai Transmission Control Protocol/Internet Protocol (TCP/IP), jolloin se tunnetaan nimellä Protocol Data Unit (PDU). (SNMP)

3 Laitteet ja ohjelmistot

3.1 Aruba VAN SDN-kontrolleri

Aruba Virtual Application Networks (VAN) SDN Controller-ohjelmisto perustuu Linuxiin, Java 1.8 ja Open Service Gateway initiativeeen (OSGi) sekä käyttää Apache Cassandraa hajauttaakseen 'post-relational' tietokannan. Lisäksi käytössä on keystone ulkoisena palveluna, joka tarjoaa autentikoinnin ja korkean tason valtuutuspalvelut. Se myös tukee 'token' pohjaista autentikointia. Lisäksi käytössä on muun muassa Representational State Transfer (REST) API ja Graphical User Interface (GUI) viitekehys, jota SDN sovelluskehittäjät voivat käyttää rakentaessa sovelluksia. Kuviossa 3 näytetään koko ohjelmistopino ja kuinka se rakentuu. (Aruba VAN SDN Controller 2.8)

Kontrolleri tarjoaa siis yhtenäisen ohjauspisteen SDN yhteensopivalle verkolle. Se liitetään verkkoinfrastruktuuriin käyttäen avoimia standardirajapintoja ja hallinta protokollia, kuten OpenFlow. Aruba VAN SDN Controller tarjoaa myös alustan SDN-sovelluksille. Sovellukset on rakennettu ja integroitu kontrolleriin tarjotakseen verkkopalveluita, kuten verkon virtualisointia, turvallisuutta ja liikenteen järjestelyä. Se tarjoaa myös ohjelmoitavan rajapinnan ohjaustasolle, sallien kolmansien osapuolien kehittää omia sovelluksia moduuleina kontrollerille tai integroida ulkoisia sovelluksia REST APIn kautta. (Creating HP Software-defined Networks 2014, 1-6)



Kuvio 3. Aruba SDN Controller-ohjelmistopino

3.2 SDN-sovellukset

Hewlett Packard Enterprise (HPE) Network Visualizer tarjoaa verkkoon näkyvyyttä ja joustavaa ratkaisua saada haltuun verkossa kulkevat paketit auditointia, varmistusta ja dynaamisia ongelmanselvitystilanteita varten. Paketit voidaan kopioida monista eri laitteista lähteenä ja toimittaa yhdelle laitteelle.

HPE Network Visualizer asentaa dynaamisesti OpenFlow-säännöt, joilla monitoroidaan verkon liikennettä käyttäen suodatuskriteerejä, jotka verkon hallitsijat ovat päättänee. Suodatuskriteerit määritellään SDN-käytäntöominaisuuksilla, jotka on rakennettu Access Control List (ACL)-verkon kanssa yhteensopivien attribuuttien kanssa. SDN käytäntö ominaisuuksia ovat käyttäjä, käyttäjän laite, sijainti, sovellus, verkon tila ja aika.

Network Visualizerilla voi monitoroida ja analysoida verkkoa kaventaakseen verkko-ongelmien lähdettä, tietääkseen verkon piikkien aiheuttajan ja varmistaakseen verkon toimivuuden. Visualizer käyttää TShark verkkoprotokolla analysaattoria tarjotakseen verkkoon näkyvyyttä kaappaamalla istuntojen aktiviteettiä, tilan ja yhteenvedon. Yhdistämällä nämä ominaisuudet verkkoon saadaan näkyvyyttä mm. tunnistamalla asiakaslaitteet, GUI pohjaisella reaaliaikaisella monitoroinnilla kaapatuille paketeille, dashboard-kaaviot, yksityiskohtainen kaappaussession näkymä, topologia monitori ja AD integraatio.

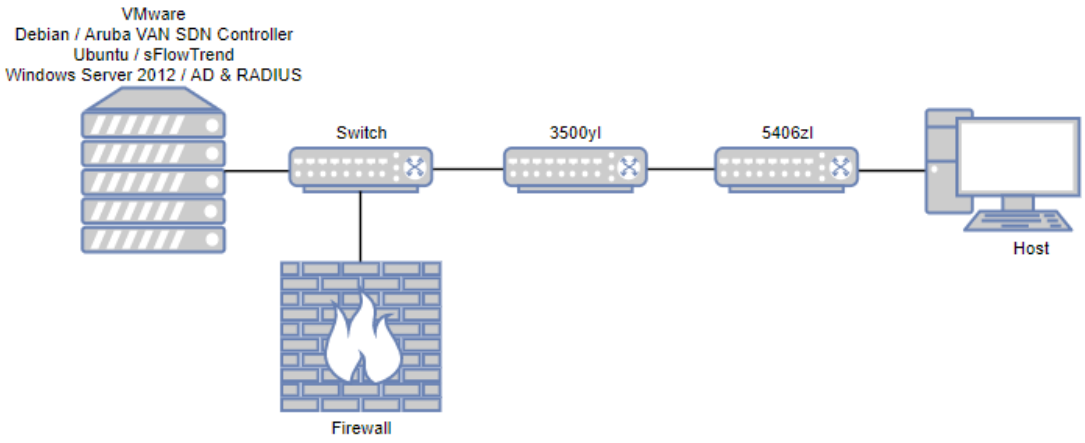
3.3 sFlowTrend

sFlowTrend on ilmainen graafinen verkko ja palvelin monitorointityökalu. Se käyttää suosittua sFlow-standardia tuottamaan reaaliaikaista kuvaa eniten verkkoa käyttävistä käyttäjistä ja sovelluksista. SFlowTrend käyttää sFlow-standardin laajennuksia fyysisen ja virtuaalisten palvelimien suorituskyvyn seurantaan. Tämän avulla voidaan yhdistääkseen verkon, palvelimen sekä sovellusten suorituskyvyt ja tarjota päästä päähän kuvan verkossa olevien laitteiden suorituskyvystä. Ilmainen versio SFlowTrend-ohjelmistosta hyväksyy sFlow dataa enintään viidestä kytkimestä tai päätelaitteesta sekä tallentaa dataa tunnin ajan. (inMon, sFlowTrend)

4 Ympäristön suunnitelma

4.1 Topologia

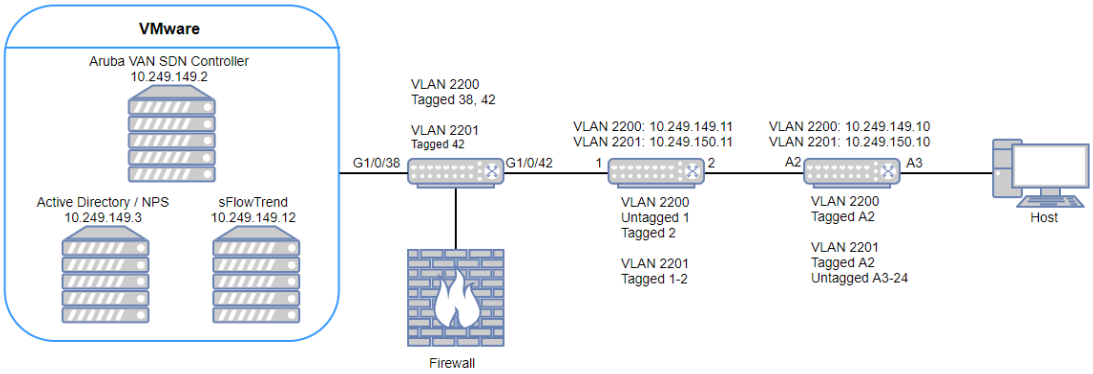
Verkon topologiasta oli tarkoitus tehdä mahdollisimman yksinkertainen, sillä työn tarkoituksena oli toteuttaa SDN-verkko, jossa voidaan testata nykyisin LAN-verkossa olevia palveluita. Topologia koostuu VMwaressa olevista kolmesta virtuaalipalvelimesta ja kahdesta OpenFlow-hybrid-kytkimestä sekä yhdestä tuotantokäytössä olevasta kytkimestä. Kuviossa 4 näkyy verkon topologia.



Kuvio 4. Fyysinen topologia

Tässä työssä toteutettiin palvelimien ja kytkimien 3500yl sekä 5406zl konfigurointi. Kuviossa 4 näkyvät ’Switch’ ja ’Firewall’ ovat tuotantokäytössä olevia laitteita, eikä niihin tehty muutoksia minun toimesta. Näiltä laitteilta on tuotu VLANit 2200 ja 2201

SDN-ympäristöä varten. Liikenne ulkoverkkoon voidaan halutessa reitittää ulkoverkkoon kuviossa näkyvän palomuurin kautta. Kaikki VMwaressa sijaitsevat palvelimet ovat VLANssa 2200. Kuviossa 5 on kuvattu verkon looginen topologia.



Kuvio 5. Looginen topologia

SDN-kontrollerina käytetään Aruban omaa VAN SDN-kontrolleria, joka virtualisoidaan VMwareen. Aruba tarjoaa omilla sivuillaan suoraan Open Virtual Appliance (OVA)-paketin, jossa tulee mukana Debia-käyttöjärjestelmä ja kaikki kontrolleriin vaadittavat ohjelmat. Tämän lisäksi Aruba tarjoaa SDN:lle oman sovelluskaupan, josta kontrollerille saa ladattua sovelluksia, kuten HPE Network Visualizer.

Näiden lisäksi Windows Server 2012 R2-palvelimelle asennetaan AD ja Network Policy Server (NPS)-palvelut. NPS konfiguroidaan toimimaan NAP- ja RADIUS-palvelimena. Ubuntulle puolestaan asennetaan sFlowTrend, jolle kytkimiltä syötetään tietoliikennevuoita, käyttäen sFlow protokollaa.

OpenFlow-kytkiminä toimii HP ProCurve 3500yl ja HP ProCurve 5406zl. Kummankin kytkimen firmware päivitetään K.16.02.0021 versioon. SDN-ympäristö käytetään OpenFlow-hybrid tilaa, jolloin kytkimet ymmärtävät OpenFlow operaatioita sekä perinteisiä L2-kytkentöjä ja L3-reitityksiä. Kytkimiin konfiguroidaan OpenFlow-kontrolleri yhdistymään VLANin 2200 kautta. Lisäksi määritellään OpenFlow Instance ja tähän määritellään VLANit jotka ovat osana OpenFlow:ta, kontrollerin ID ja käytettävä OpenFlow-versio.

Kytkimelle 3500yl konfiguroidaan VLAN 2200 IP-osoitteella 10.249.149.11/24 sekä VLAN 2201 IP-osoitteella 10.249.150.11/24. VLANille 2200 portti 1 pistetään untag-

ged tilaan ja portti 2 tagged. VLANissa 2201 portit 1 ja 2 pistetään tagged tilaan. Kytkimeen ei konfiguroida 802.1x autentikointia, koska kytkin esittää laitetta johon ei suoraan yhdistetä päätelaitteita.

Kytkimelle 5406zl puolestaan konfiguroidaan VLAN 2200 IP-osoitteella 10.249.149.10/24 ja VLAN 2201 IP-osoitteella 10.249.150.10/24. VLANille 2200 portti A2 pistetään tagged tilaan. VLANissa 2201 puolestaan portti A2 pistetään tagged ja portit A3-A24 pistetään untagged tilaan. Kytkimelle konfiguroidaan 802.1x autentikointi portteihin A3-A24. Tunnistetuilta laitteilta sallitaan pääsy VLANiin 2201 ja estetyt laitteet siirretään VLANiin 99, josta ei ole pääsyä mihinkään.

Tämän lisäksi kytkimelle konfiguroidaan RADIUS autentikointi kirjautumisille, sFlow kohde osoitteena 10.249.149.12, SNMPv3 ja Spanning-Tree. Oletus yhdyskäytäväksi määritellään IP-osoite 10.249.149.1.

5 Ympäristön toteutus

5.1 Kytkimet

5.1.1 RADIUS

Kytkimille päivitettiin K.16.02.0021 firmware, joka on yhteen sopiva OpenFlow:n kanssa ja konfiguroitiin suunnitelman mukaiset VLANit ja IP-osoitteet. Kytkimelle konfiguroitiin käytettäväksi RADIUS-palvelimeksi Windows Server 2012-palvelin, jonka osoite on 10.249.149.3. Lisäksi määriteltiin jaettu avain. Tämä onnistui alla olevemalla komennolla.

```
radius-server host 10.249.149.3 key "XXXX"
```

Käyttäjien autentikointi konfiguroitiin SSH ja Telnet yhteyksille. Lisäksi määriteltiin *aaa authentication login privilege-mode*, joka sallii tunnistettujen käyttäjien käyttää manager-tason oikeuksia ilman uudelleen tunnistautumista.

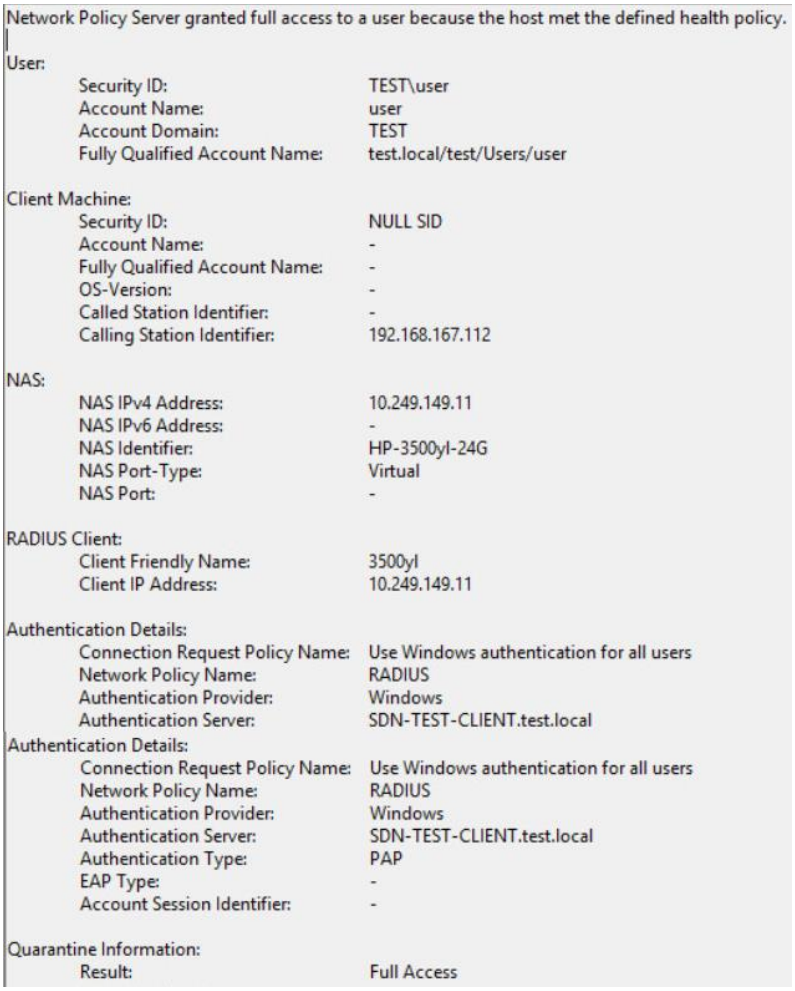
```
aaa accounting exec start-stop radius
aaa authentication login privilege-mode
aaa authentication telnet login radius
aaa authentication telnet enable radius
aaa authentication ssh login radius
aaa authentication ssh enable radius
aaa authentication port-access chap-radius
```

Kuviossa 6 nähdään käytettävä RADIUS-palvelin sekä käytettävät portit.

```
HP-3500yl-24G(config)# sh radius

 Status and Counters - General RADIUS Information

  Deadtime (minutes)             : 0
  Timeout (seconds)              : 5
  Retransmit Attempts            : 3
  Global Encryption Key          :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection            : Outgoing Interface
  Source IPv6 Selection          : Outgoing Interface
  Tracking                       : Disabled

                 Auth  Acct  DM/ Time   |
  Server IP Addr Port  Port  CoA Window | Encryption Key                   OOBM
  -------------- ----- ----- --- ------ + -------------------------------- ----
  10.249.149.3   1812  1813  No  300    | [redacted]                       No
```

Kuvio 6. HP 3500yl show radius

Kuviossa 7 nähdään onnistunut kirjautuminen käyttäen AD-käyttäjää “user”. Jokaisesta kirjautumisyrityksestä jaa jälki Windows Serverin tapahtumienvalvontaan, Network Policy and Access-välilehden alle.



Network Policy Server granted full access to a user because the host met the defined health policy.

User:
- Security ID: TEST\user
- Account Name: user
- Account Domain: TEST
- Fully Qualified Account Name: test.local/test/Users/user

Client Machine:
- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: -
- Calling Station Identifier: 192.168.167.112

NAS:
- NAS IPv4 Address: 10.249.149.11
- NAS IPv6 Address: -
- NAS Identifier: HP-3500yl-24G
- NAS Port-Type: Virtual
- NAS Port: -

RADIUS Client:
- Client Friendly Name: 3500yl
- Client IP Address: 10.249.149.11

Authentication Details:
- Connection Request Policy Name: Use Windows authentication for all users
- Network Policy Name: RADIUS
- Authentication Provider: Windows
- Authentication Server: SDN-TEST-CLIENT.test.local

Authentication Details:
- Connection Request Policy Name: Use Windows authentication for all users
- Network Policy Name: RADIUS
- Authentication Provider: Windows
- Authentication Server: SDN-TEST-CLIENT.test.local
- Authentication Type: PAP
- EAP Type: -
- Account Session Identifier: -

Quarantine Information:
- Result: Full Access

Kuvio 7. Onnistunut RADIUS autentikointi

5.1.2 OpenFlow

OpenFlow saadaan päälle kirjoittamalla *openflow*. Tämän jälkeen konfiguroidaan käytettävä kontrolleri komennolla *controller-id <x> ip <kontrollerin ip-osoite> controller-interface vlan <x>*. Alla käytetty komento.

```
openflow
controller-id 1 ip 10.249.149.2 controller-interface vlan 2200
```

Tämän jälkeen luodaan OpenFlow ”instance”. Instance:en määritellään mm. käytettävä OpenFlow-versio, VLANit jotka ovat osana OpenFlow-verkkoa ja kontrollerin aikaisemmin konfiguroitu ID. Alla käytätetyt komennot.

```
instance "1"
```

```
    member vlan 2201
    controller-id 1
    version 1.3
    enable
    exit
enable
exit
```

Kuviossa 8 nähdään konfiguroitu OpenFlow instance, laitteisto- ja ohjelmistopohjaisten vuoiden määrä sekä käytettävä OpenFlow versio.

```
HP-3500yl-24G(openflow)# show openflow

 OpenFlow                    : Enabled
 Egress Only Ports Mode      : Disabled

 Instance Information

                                          No. of     No. of     OpenFlow
  Instance Name                 Oper. Status H/W Flows  S/W Flows  Version
  ------------------------------ ------------ ---------- ---------- --------
  1                             Up           12         11         1.3
```

Kuvio 8. HP 3500yl show openflow

Kuviossa 9 nähdään konfiguroidun instance:n tiedot. Kuviosta huomatan, että osallistuja VLANina on VLAN 2201 sekä pipeline-mallina “Standard Match”.

```
HP-3500yl-24G(openflow)# show openflow instance 1

 Configured OF Version         : 1.3
 Negotiated OF Version         : 1.3
 Instance Name                 : 1
 Data-path Description         : 1
 Administrator Status          : Enabled
 Member List                   : VLAN 2201
 Pipeline Model                : Standard Match
 Listen Port                   : None
 Operational Status            : Up
 Operational Status Reason     : NA
 Datapath ID                   : 0899001635b5dbc0
 Mode                          : Active
 Flow Location                 : Hardware and Software
 No. of Hardware Flows         : 12
 No. of Software Flows         : 11
 Hardware Rate Limit           : 0 kbps
 Software Rate Limit           : 100 pps
 Conn. Interrupt Mode          : Fail-Secure
 Maximum Backoff Interval      : 60 seconds
 Probe Interval                : 10 seconds
 Hardware Table Miss Count     : NA
 No. of Software Flow Tables   : 1
 Egress Only Ports             : None
 Table Model                   : Policy Engine and Software
 Source MAC Group Table        : Disabled
 Destination MAC Group Table   : Disabled

 Controller Id Connection Status Connection State Secure Role
 ------------- ----------------- ---------------- ------ ------
 1             Connected         Active           No     Equal
```

Kuvio 9. HP 3500yl show openflow instance 1

5.1.3 802.1x

Porttikohtainen autentikointi konfiguroitiin kaikkiin paitsi A2 porttiin, komennolla *aaa port-access authneticator <x>*. Portti A2 on yhteydessä toiseen kytkimeen, joten tälle ei tarvita autentikointi. Jokaiselle portille määriteltiin VLANiksi onnistuneen todennuksen jälkeen VLAN 2201 ja epäonnistuneen VLAN 99 komennolla *aaa port-access authenticator <x> auth-vid <X>* ja *aaa port-access authenticator <x> unauth-vid <x>.* Lisäksi määritellään käytettävä algoritmi, jolla kommunikointi RADIUS-palvelimen kanssa tapahtuu komennolla *aaa authentication port-access <x>*. Autentikointi aktivoidaan vielä komennolla *aaa port-access authenticator active*. Alla käytetyt komennot.

```
aaa authentication port-access chap-radius
aaa port-access authenticator A1,A3-A24
aaa port-access authenticator A1,A3-A24 auth-vid 2201
aaa port-access authenticator A1,A3-A24 unauth-vid 99
```

aaa port-access authenticator active

Kuviossa 10 nähdään, että porttikohtainen tunnistautuminen tapahtuu ”ChapRadius”-menetelmällä.

```
HP-Switch-5406zl(config)# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Enabled
  Bypass Username For Operator and Manager Access : Disabled

                | Login       Login        Login
  Access Task   | Primary     Server Group Secondary
  ------------- + ----------- ------------ ----------
  Console       | Local                    None
  Telnet        | Radius      radius       None
  Port-Access   | ChapRadius  radius       None
  Webui         | Local                    None
  SSH           | Radius      radius       None
  Web-Auth      | ChapRadius  radius       None
  MAC-Auth      | ChapRadius  radius       None
  SNMP          | Local                    None
  Local-MAC-Auth| Local       radius       None

                | Enable      Enable       Enable
  Access Task   | Primary     Server Group Secondary
  ------------- + ----------- ------------ ----------
  Console       | Local                    None
  Telnet        | Radius      radius       None
  Webui         | Local                    None
  SSH           | Radius      radius       Local
```

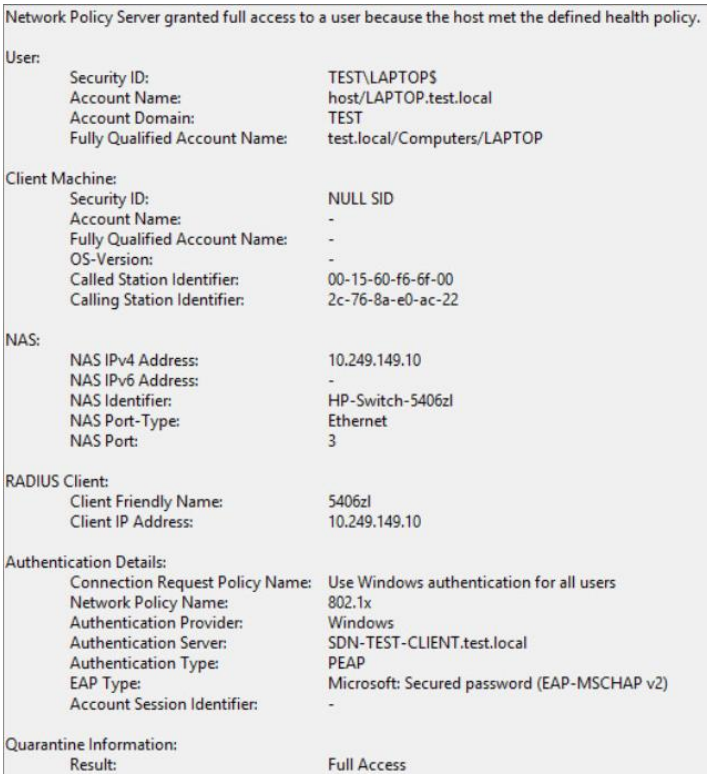
Kuvio 10. HP 5406zl show authentication

Kuviossa 11 nähdään porttien tilat. Portti A3 käyttää 802.1x autentikointia ja on tunnistautunut oikein, koska on VLANissa 2201.

```
HP-Switch-5406zl(config)# show vlan 2201

 Status and Counters - VLAN Information - VLAN 2201

  VLAN ID : 2201
  Name : OPENFLOW
  Status : Port-based
  Voice : No
  Jumbo : No
  Private VLAN : none
  Associated Primary VID : none
  Associated Secondary VIDs : none

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A1               Untagged Learn        Down
  A2               Tagged   Learn        Up
  A3               802.1x   Learn        Up
```

Kuvio 11. HP 5406zl show vlan 2201

Kuviossa 12 nähdään, että kyseessä on tietokone nimeltä LAPTOP, joka on onnistunut autentikoitumaan.



Network Policy Server granted full access to a user because the host met the defined health policy.

User:
- Security ID: TEST\LAPTOP$
- Account Name: host/LAPTOP.test.local
- Account Domain: TEST
- Fully Qualified Account Name: test.local/Computers/LAPTOP

Client Machine:
- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: 00-15-60-f6-6f-00
- Calling Station Identifier: 2c-76-8a-e0-ac-22

NAS:
- NAS IPv4 Address: 10.249.149.10
- NAS IPv6 Address: -
- NAS Identifier: HP-Switch-5406zl
- NAS Port-Type: Ethernet
- NAS Port: 3

RADIUS Client:
- Client Friendly Name: 5406zl
- Client IP Address: 10.249.149.10

Authentication Details:
- Connection Request Policy Name: Use Windows authentication for all users
- Network Policy Name: 802.1x
- Authentication Provider: Windows
- Authentication Server: SDN-TEST-CLIENT.test.local
- Authentication Type: PEAP
- EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
- Account Session Identifier: -

Quarantine Information:
- Result: Full Access

Kuvio 12. Onnistunut 802.1x autentikointi

Kuviossa 13 nähdää epäonnistunut autentikointi, kun koneen tili on poistettu AD-palvelimen 802.1x-ryhmästä.

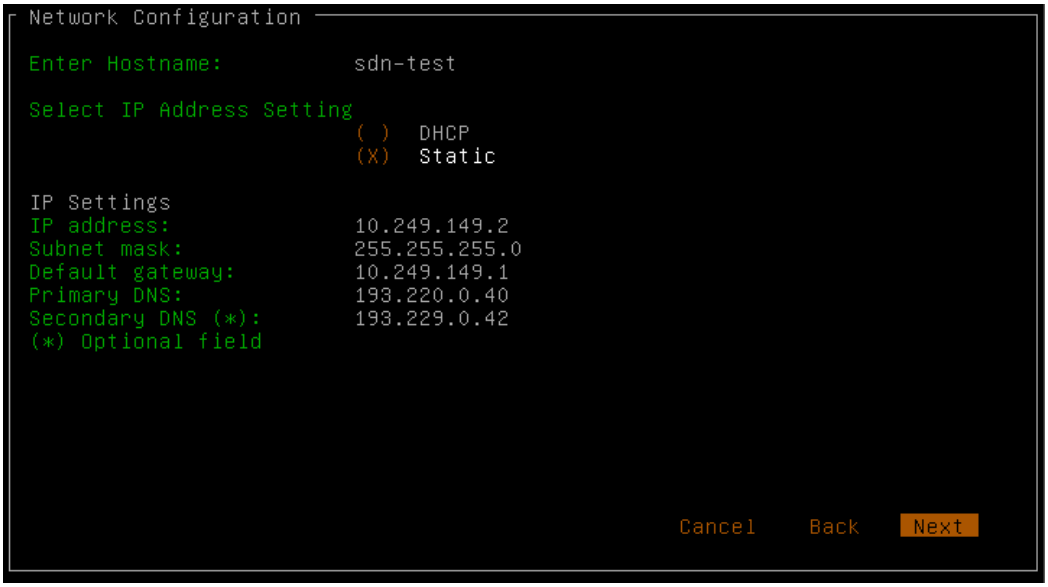
```
HP-Switch-5406zl(eth-A3)# show port-access authenticator clients a3

 Port Access Authenticator Client Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Use LLDP data to authenticate [No] : No

  Port  Client Name           MAC Address   IP Address      Client Status
  ----- --------------------- ------------- --------------- --------------------
  A3                          2c768a-e0ac22 n/a             Rejected,unauth-vlan
```

Kuvio 13. Epäonnistunut 802.1x autentikointi

5.2 SDN kontrolleri

Kontrolleri on tarjolla OVA-tiedostona, jolloin SDN-kontrolleri saadaan käyttöön tuomalla kyseinen paketti VMwareen ja käynnistämällä virtuaalikone. Oletuksena käyttäjä on *sdn* ja salasana *skyline*. Ensimmäisellä käynnistyskerralla kontrolleri tarjoaa Kuvio 14 mukaisen asennusvalikon, johon määritetään kontrollerin verkkoasetukset.

Kontrolleri konfiguroitiin 10.249.149.0/24-verkkoon staattisella IP-+osoitteella 10.249.149.2. Kuviossa 14 nähdään SDN-kontrollerin verkkoasetukset.

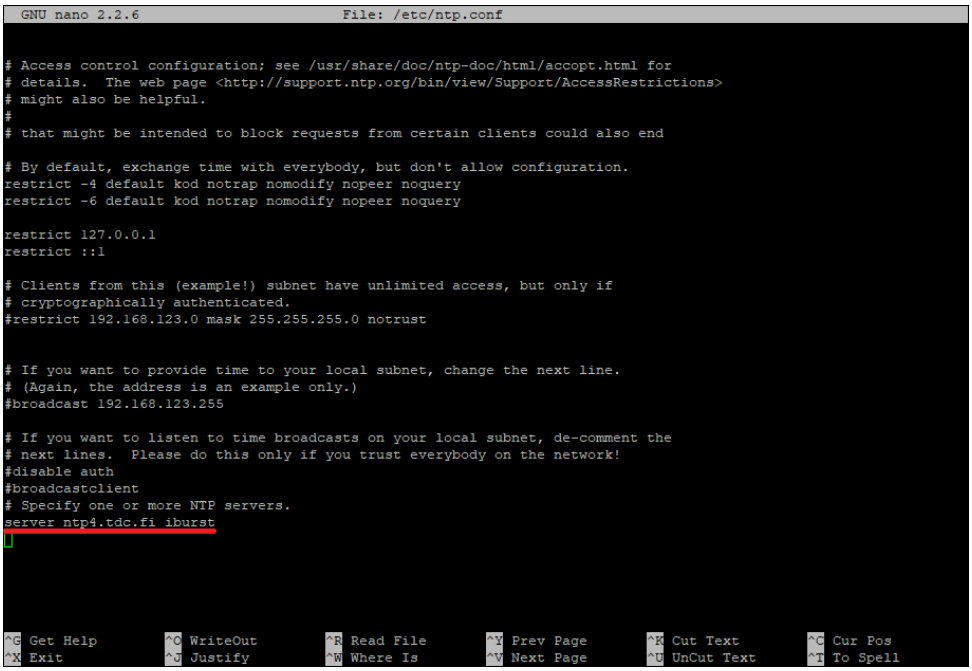


Kuvio 14. Kontrollerin verkkoasetukset

Jotta kontrollerilla toimii lokitus ja sovellusten asennukset helposti. Kontrollerille asetettiin aika ja ottaa pois jar/zip-signing validointi.

Kuviossa 15 määritettiin käytettävä Network Time Protocol (NTP)-palvelin. Käytettävä NTP-palvelin konfiguroidaan ntp.conf-tiedostoon. Tiedoston avattua alimmalle riville voidaan määritellä haluttu palvelin.

sudo nano /etc/ntp.conf
server ntp4.tdc.fi iburst



Kuvio 15. Käytettävä NTP-palvelin

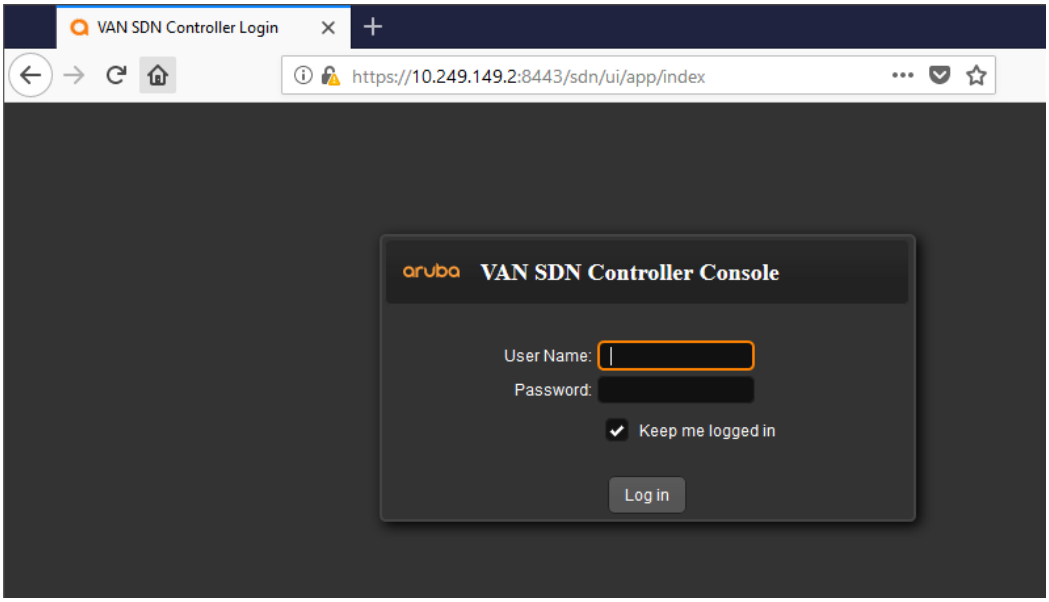
Kontrollerilta otettiin vielä pois jar/zip-signing validointi. Tällöin kontrollerille saatiin asennettua allekirjoittamattomia sovelluksia. Tällöin ei myöskään tarvitse lisätä jokaisen sovelluksen sertifikaattia kontrollerin truststore:en. Validointi saatiin pois muokkaamalla *dmk.sh*-skriptiä ja lisäämällä *$JMX_OPT* \ alle-*Dsdn.signedJar=none* \-rivi. Kuviossa 16 näkyy alleviivattuna lisätty rivi.

```
sudo service sdnc stop
sudo nano /opt/sdn/virgo/bin/dmk.sh
-Dsdn.signedJar=none \
sudo service sdnc start
```

```
 GNU nano 2.2.6                                File: /opt/sdn/virgo/bin/dmk.sh

        then
                TMP_DIR=$KERNEL_HOME/work/tmp
                # Ensure that the tmp directory exists
                mkdir -p $TMP_DIR

                cd $KERNEL_HOME; exec $JAVA_EXECUTABLE \
                        $JAVA_OPTS \
                        $DEBUG_OPTS \
                        $JMX_OPTS \
                        -XX:+HeapDumpOnOutOfMemoryError \
                        -XX:ErrorFile=$KERNEL_HOME/serviceability/error.log \
                        -XX:HeapDumpPath=$KERNEL_HOME/serviceability/heap_dump.hprof \
                        -Djava.security.auth.login.config=$AUTH_LOGIN \
                        -Dorg.eclipse.virgo.kernel.authentication.file=$AUTH_FILE \
                        -Dsdn.signedJar=none \
                        -Djava.io.tmpdir=$TMP_DIR \
                        -Dorg.eclipse.virgo.kernel.home=$KERNEL_HOME \
                        -Dorg.eclipse.virgo.kernel.config=$CONFIG_DIR \
                        -Dosgi.sharedConfiguration.area=$CONFIG_DIR \
                        -Dosgi.java.profile="file:$JAVA_PROFILE" \
            -Declipse.ignoreApp=true \
            -Dosgi.install.area=$KERNEL_HOME \
            -Dosgi.configuration.area=$CONFIG_AREA \
            -Dssh.server.keystore="$CONFIG_DIR/hostkey.ser" \
            -Dosgi.frameworkClassPath=$FWCLASSPATH \
            -Djava.endorsed.dirs="$KERNEL_HOME/lib/endorsed" \
            -classpath $CLASSPATH \
                        org.eclipse.equinox.launcher.Main \
            -noExit \
                        $LAUNCH_OPTS \
                        $ADDITIONAL_ARGS
        fi
elif [ "$COMMAND" = "stop" ]
then
```

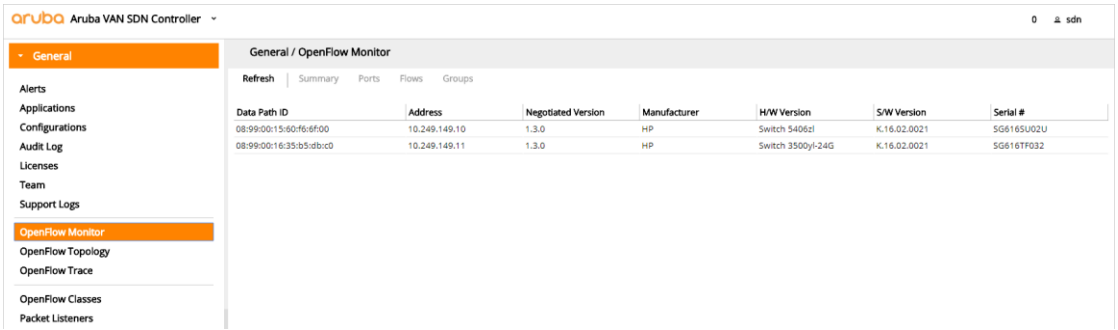
Kuvio 16. Jar/zip-signing validoinnin poisto

Asennuksen jälkeen kontrolleria voida käyttää web-käyttöliittymän kautta. Käyttöliittymään pääsee koneelta, joka on samassa verkossa kuin kontrolleri. Kuviossa 17 nähdään, että hallintasivulle pääsee osoitteella https://10.249.149.2:8443. Oletuksena web-käyttöliittymään käy samat tunnukset kuin muuhunkin hallintaan.



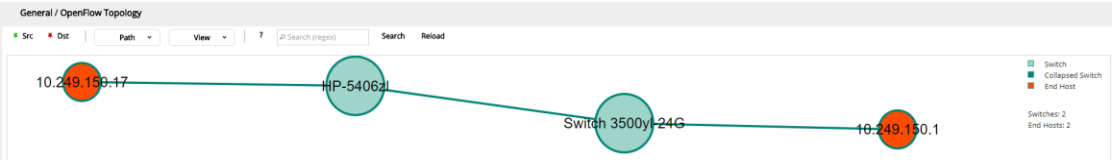
Kuvio 17. Web-käyttöliittymä

OpenFlow laitteet tunnistautuivat ja tulivat näkyviin OpenFlow Monitor-välilehden taakse. Kuviossa 18 nähdään kummatkin OpenFlow kytkimiksi tunnistaneet laitteet.



Kuvio 18. OpenFlow Monitor

OpenFlow Topology-välilehdeltä nähdään kaikki OpenFlow-laitteet sekä näissä kiinni olevat laitteet. Kuviossa 19 huomataan, että kytkimen 3500yl perässä näkyy end host. Tämä johtuu siitä, että kytkimelle jouduttiin konfiguroimaan VLAN 2201 myös porttiin yksi. Ilman tätä päätelaite ei pystynyt kommunikoimaan 3500yl-kytkimestä eteenpäin, sillä käytössä oli vain kontrollerin alkuperäiset vuotaulut. Tekemällä uuden vuotaulun, tämä voidaan reitittää 10.249.149.0/24 verkkoon.

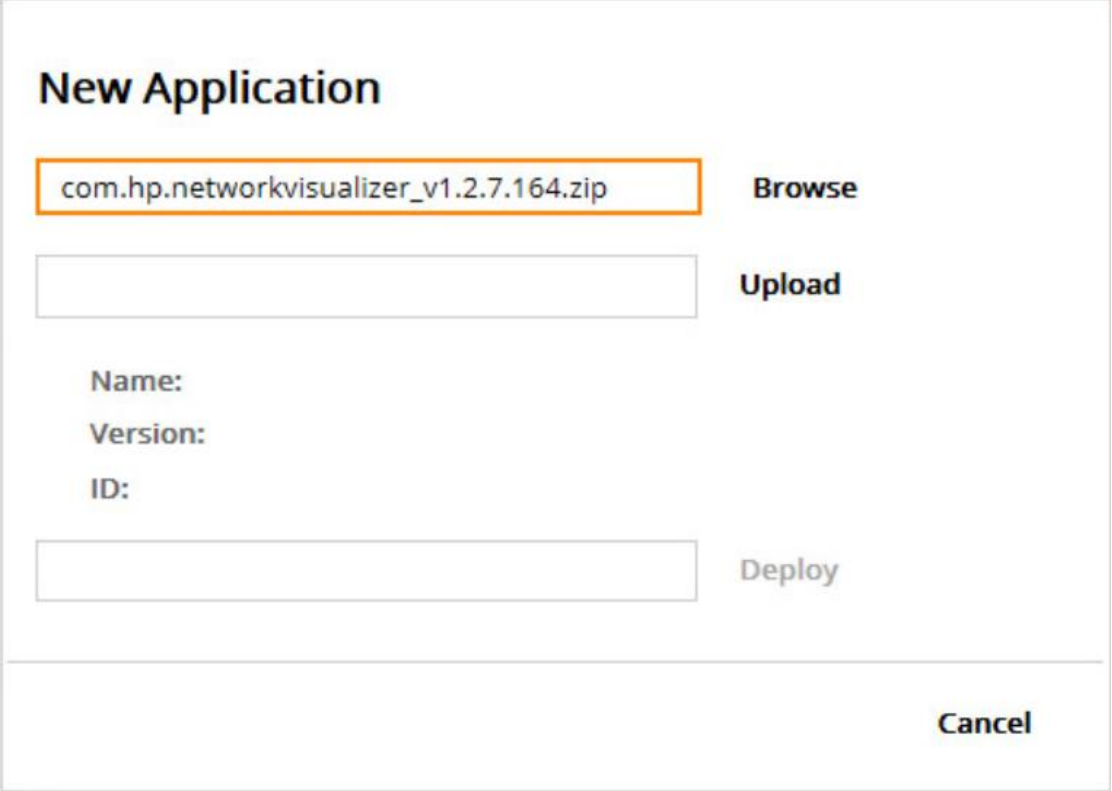


Kuvio 19. OpenFlow Topology

5.3 SDN-sovellukset

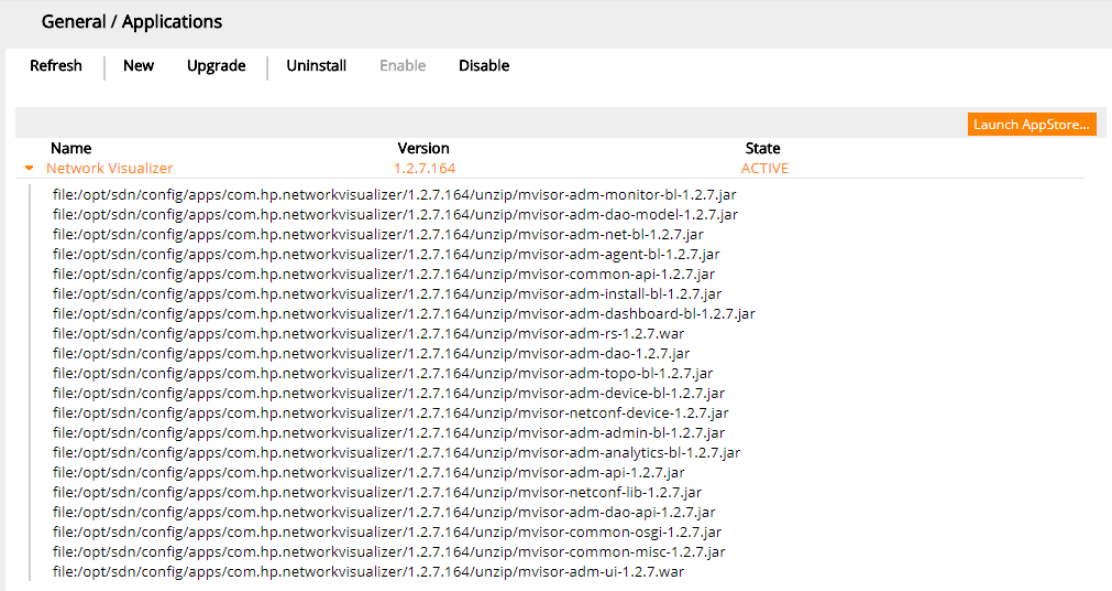
HPE Network Visualizer saatiin ladattua Aruban SDN sovelluskaupasta. Kauppaan pääsee kontrollerin web-käyttöliittymässä olevan Application välilehden kautta. Sivuston avauduttua Aruba Applications kohdan alta löytyy HPE Network Visualizer ja tätä klikkaamalla saa ladattua sovelluksen.

Sovelluksen asentaminen tapahtuu saman Application välilehden alta löytyvästä New valinnasta. Kuviossa 20 näkyy avautuva valikko, johon lisätään juuri ladattu paketti ja painetaan Upload.



Kuvio 20. SDN sovelluksen asentaminen

Asennuksen jälkeen, sovellus ilmestyy aikaisempaan Application välilehdelle. Samasta kohdasta voidaan disabloida ja enabloida haluttuja sovelluksia. Kuviossa 21 nähdään Network Visualizerin asentamat tiedostot.

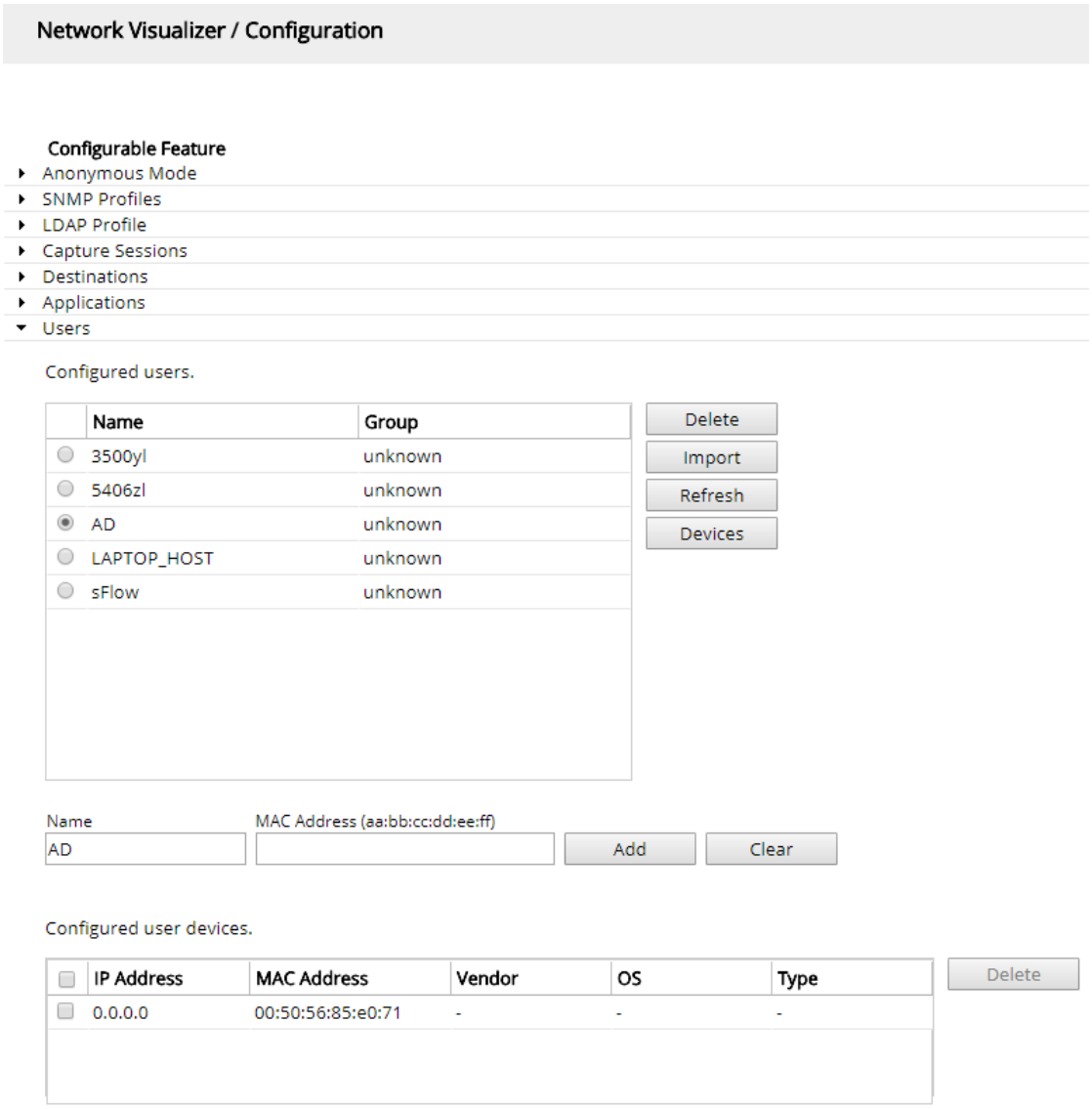


Kuvio 21. Network Visualizer asentamat tiedostot

Vasempaan laitaan tulee ”Network Visualizer” nappi, josta kyseinen sovellus saadaan auki. Kuviossa 22 nähdään ohjelman dashboard. Dashboardilla nähdään mm. konfiguroitujen pakettikaappauksien tilastoja, tunnistettujen laitteiden käyttöjärjestelmiä sekä näiden tyyppejä.

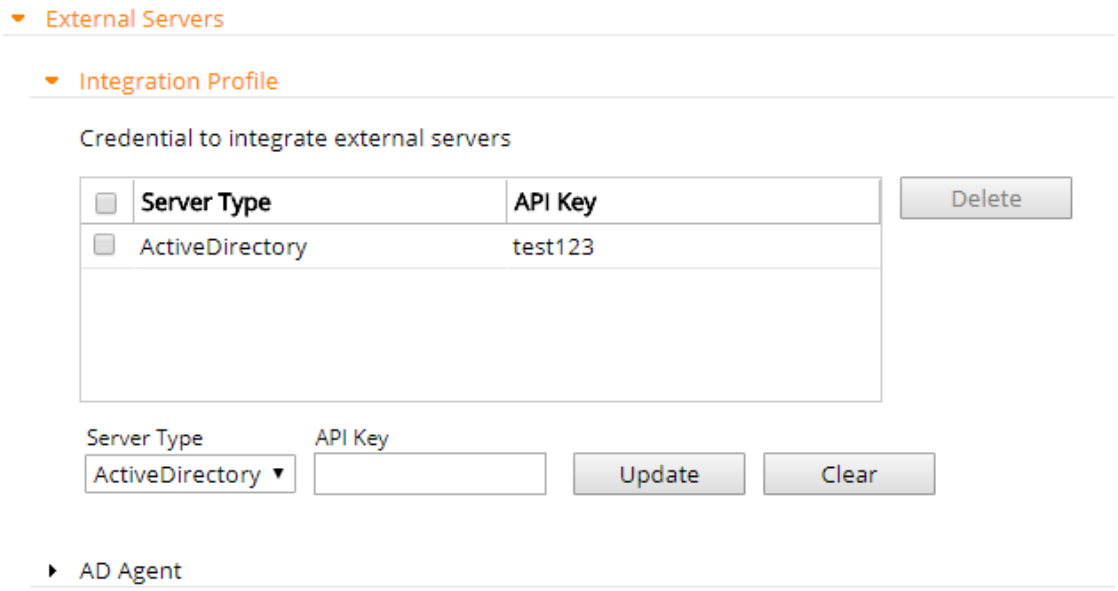
Kuvio 22. Network Visualizer dashboard

Network Visualizerin konfigurointi tapahtuu Configuration-välilehdeltä. Users-valikkoon lisättiin käytössä olleet palvelimet, kytkimet sekä tietokone. Kaikki tunnistautuvat MAC-osoitteella. Jos kytkimet tunnistaa MAC-osoitteita linkkien takaa, nämä voidaan lisätä suoraan ”Devices” napin takaa. Kuviossa 23 nähdään lisätyt laitteet.



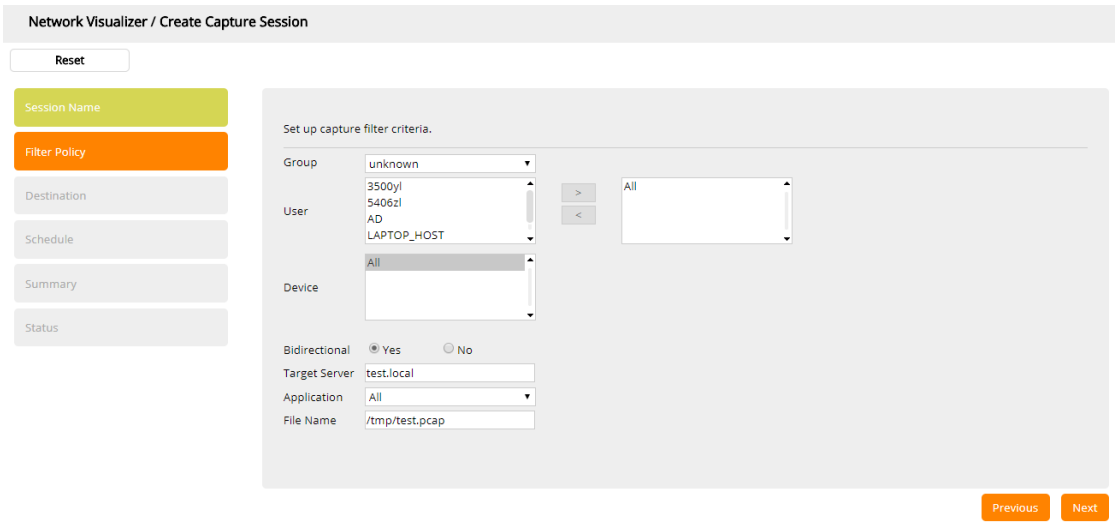
Kuvio 23. Network Visualizer users

Active Directory-palvelimelle asennettiin AD Agent. Tämä tarjoaa turvallisen mekanismin lähettääkseen tunnistettujen käyttäjien tietoja AD-palvelimelta Network Visualizerille. Network Visualizerille luotiin API Key, jonka avulla oikea palvelin tunnistautuu. Kuviossa 24 nähdään luotu API Key. Itse ohjelman saatiin ladattua samasta valikosta.



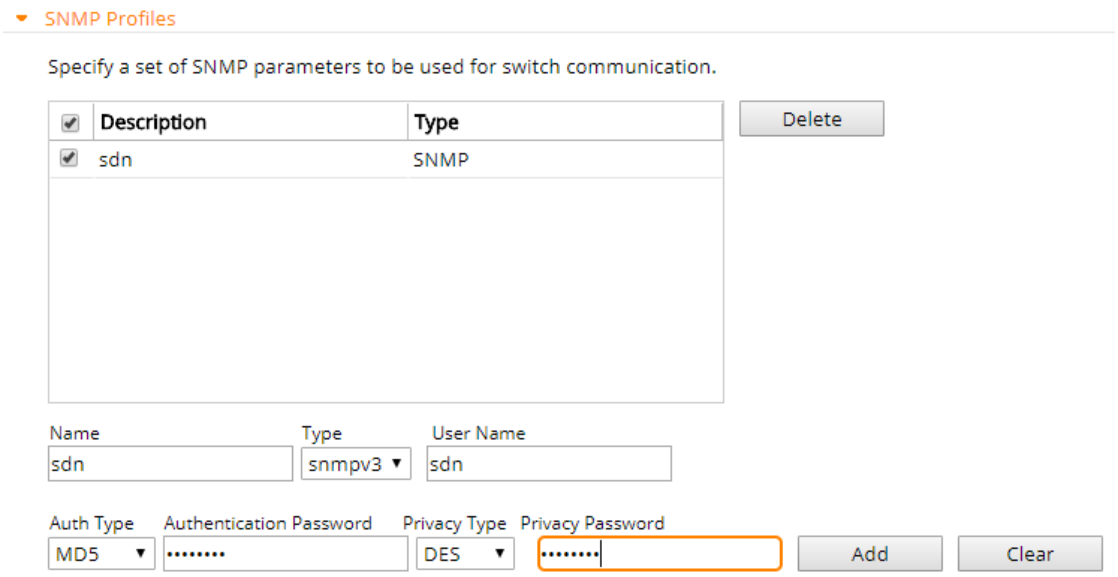
Kuvio 24. Network Visualizer AD agent

Pakettikaappauksia voidaan tehdä Create Capture Session välilehden takaa. Kaappauksia voidaan tehdä monilla eri kriteereillä. Jos Session Modeksi valitaan User, filtteröinti voidaan tehdä käyttäjän, käyttäjän ryhmän, laitteen ja protokollan avulla. Custom moodissa filtteröinti voidaan tehdä protokollan, lähde- ja kohdeportin sekä IP- ja MAC-osoitteen perusteella. Kuviossa 25 nähdään Filter Policy, kun Session Modeksi on valittu User. Kaappaus voidaan ajoitta halutuille ajankohdille tai aina päällä olevaksi.



Kuvio 25. Network Visualizer capture session

Configuration-välilehdeltä täytyy vielä konfiguroida SNMP, jotta kaappaus toimii oikein. Kuviossa 26 nähdään konfiguroitu SNMPv3 profiili.



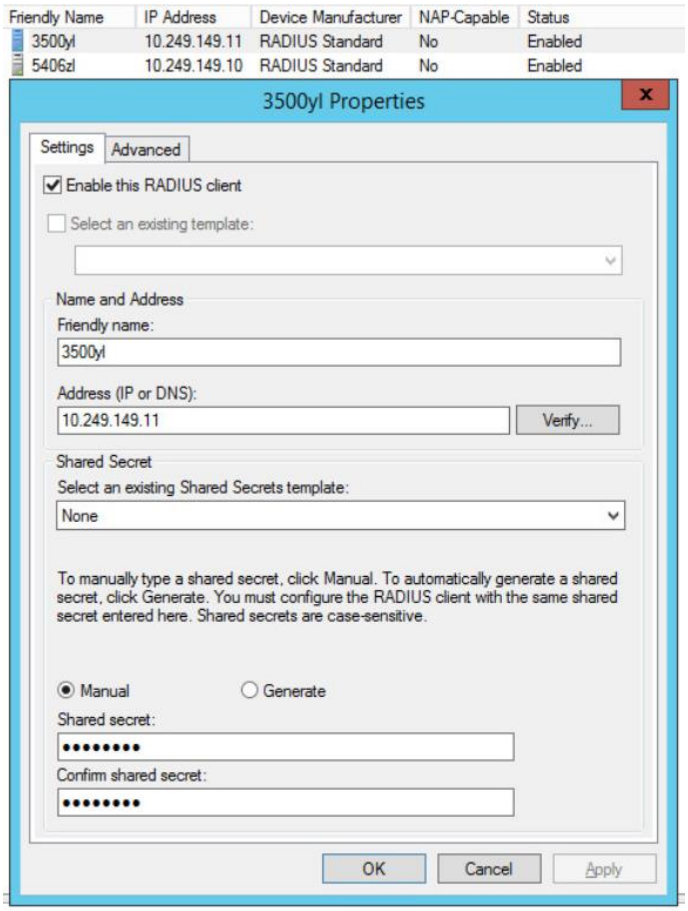
Kuvio 26. Network Visualizer SNMP

5.4 Active Directory & NPS

Windows Server 2012 R2-käyttöjärjestelmän asennuksen jälkeen, palvelimelle asennetaan roolit *Active Directory Domain Services*, *Network Policy and Access Services* ja *DNS Server*.

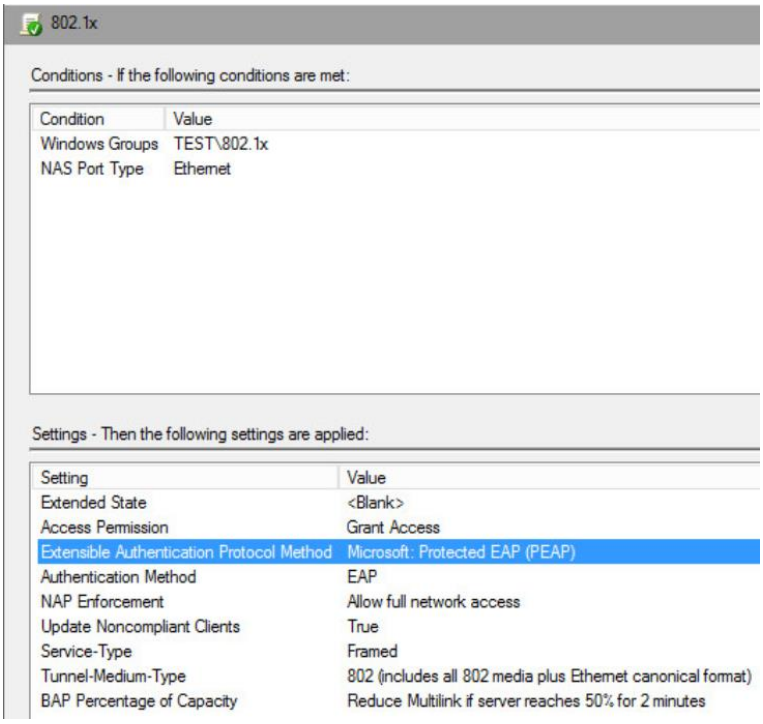
Näiden asennuksen jälkeen, avataan *Active Directory Users and Computer*, jonne luodaan *Organizational Unit* (OU) nimeltä test. Tämän alle luotiin vielä Groups ja Users OU:t. OU:n Users alle luotiin käyttäjät user ja manager. OU:n Groups alle luotiin ryhmät 802.1x ja RADIUS. Kummatkin käyttäjät pistettiin RADIUS-ryhmän jäseniksi. Toimialueen tietokoneet pistetään 802.1x-ryhmän jäseniksi.

Seuraavaksi määriteltiin NPS:n asetukset. *RADIUS Clients and Server/RADIUS Client*-välilehden alle lisättiin kummatkin kytkimet. Kuviossa 27 nähdään lisätyt kytkimet sekä valikko, josta kytkin lisätään.



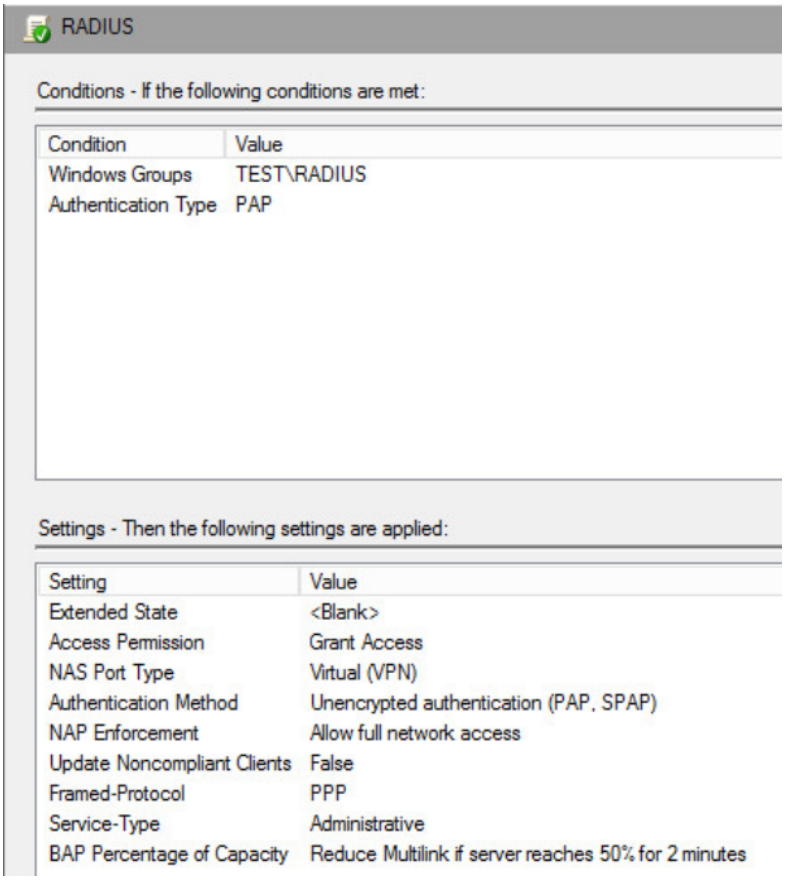
Kuvio 27. NPS RADIUS Clients

Kuviossa 28 nähdään 802.1x autentikoinnissa käytetyt määreet, kuten ryhmä johon täytyy kuulua sekä laitteen liittymis tapa verkkoon.



Kuvio 28. NPS Network Policies 802.1x

Kuviossa 29 puolestaan nähdään RADIUS autentikoinnissa käytetyt määreet, kuten ryhmä ja autentikointi metodi.

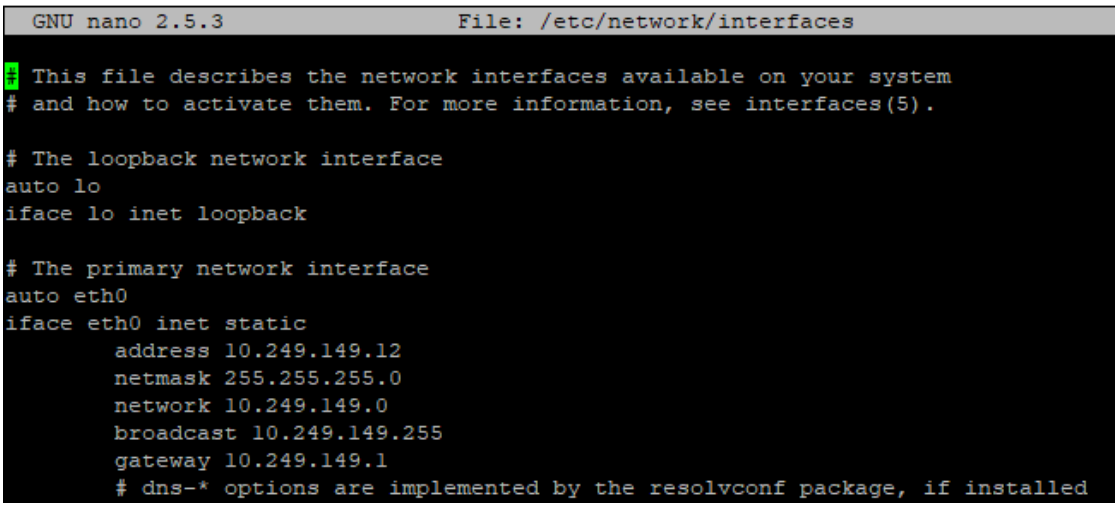


Kuvio 29. NPS Network Policies RADIUS

5.5 sFlowTrend

sFlowTrend asennettiin Ubuntu virtuaalikoneelle. Inmon tarjoaa sFlowTrendin asennuspaketin mm. Debian pohjaisille käyttöjärjestelmille, joten asentaminen on hyvin yksinkertaista. Ohjelma on Java pohjainen, joten tämä täytyy olla asennettuna ennen sFlowTrendin asennusta. Ubuntu asennuspaketissa tulee mukana Java. Ubuntun asennuksen jälkeen määritellään verkkoasetukset. Näitä voidaan muuttaa muokkaamalla *interfaces*-tiedostoa ja kirjoittamalla alla olevat komennot. Kuviossa 30 nähdään määritetyt verkkoasetukset.

```
sudo nano /etc/network/interfaces
iface eth0 inet static
address 10.249.149.12
netmask 255.255.255.0
network 10.249.149.0
broadcast 10.249.149.255
gateway 10.249.149.1
```



Kuvio 30. Ubuntun verkkoasetukset

DNS-asetukset konfiguroidaan muokkaamalla */etc/resolvconf/resolv.conf.d/base* ja */etc/resolvconf/resolv.conf.d/head*-tiedostoja. Kumpaankin tiedostoon määritellään käytettävät DNS-palvelimet alla olevien komentojen mukaan. Ensisijaiseksi DNS-palvelimeksi konfiguroidaan ympäristössä käytössä oleva AD-palvelin. Kuviossa 31 nähdään *base* ja *head*-tiedostoihin määritetyt nimipalvelimet.

```
sudo nano /etc/resolvconf/resolv.conf.d/base
nameserver 10.249.149.3
```

```
nameserver 193.229.0.40
nameserver 1.1.1.1
```

```
 GNU nano 2.5.3              File: /etc/resolvconf/resolv.conf.d/base

nameserver 10.249.149.3
nameserver 193.229.0.40
nameserver 1.1.1.1
```

Kuvio 31. Ubuntun DNS-palvelimet

Tiedostojen muokkaamisen jälkeen networking-palvelu täytyy käynnistää uudelleen komennolla *sudo service networking restart*. Kuviossa 32 nähdään */etc/resolv.conf*-tiedosto palvelun uudelleen käynnistyksen jälkeen.

```
 GNU nano 2.5.3                  File: /etc/resolv.conf

# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.249.149.3
nameserver 193.229.0.40
nameserver 1.1.1.1
```

Kuvio 32. Ubuntun resolv.conf

sFlowTrend-ohjelmisto saadaan ladattua suoraan Inmonin sivuilta ja asennettua alla olevilla komennoilla.

```
wget https://inmon.com/products/sFlowTrend/downloads/sFlowTrend-linux-6_7.deb
sudo dpkg-i sFlowTrend-linux-6_7.deb
```

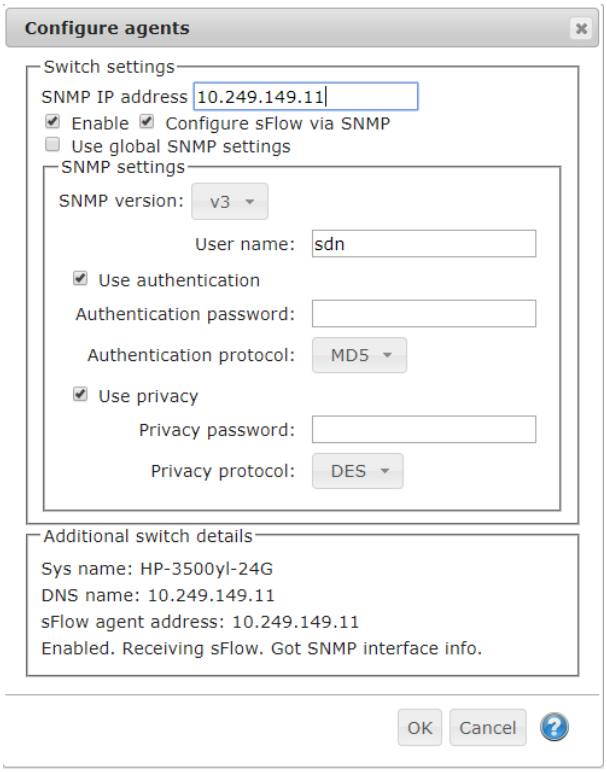
Asennuksen jälkeen sFlowTrendin hallintaan pääsee osoitteella http://10.249.149.12:8087.

Kytkimet konfiguroidaan lähettämään sFlowTrend-ohjelmistolle dataa. Kummallekin HP ProCurve-kytkimelle konfiguroidaan vastaanotto osoitteeksi 10.249.149.12 ja sampling-määreeksi 50. Sampling kertoo suunnilleen, kuinka monesta paketista otetaan yksi näyte. Lisäksi määritellään polling-määreeksi 20. Tämä määrittää kuinka monen sekunnin välein laskureista otetaan dataa. Alla kytkimille määritetyt konfiguraatiot.

```
sflow 1 destination 10.249.149.12
sflow 1 polling A1-A4 20
sflow 1 sampling A1-A4 50
snmpv3 enable
```

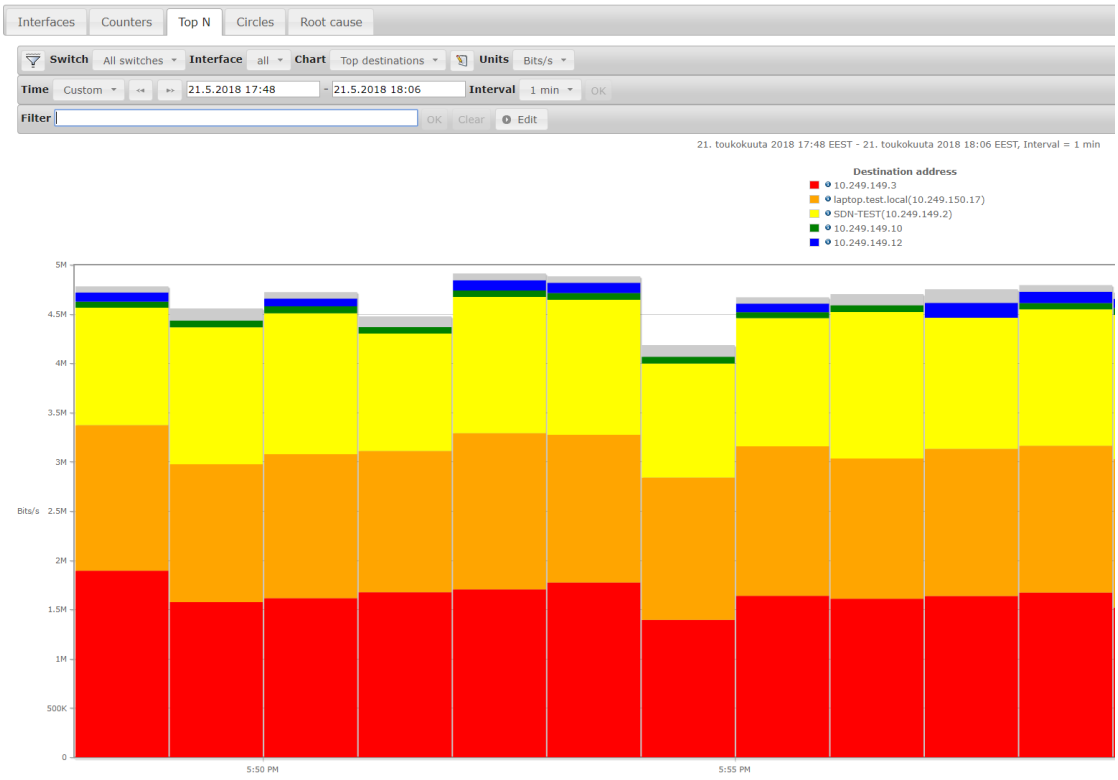
```
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "sdn"
```

sFlowTrendiin määritetään kummatkin kytkimet käyttämään sFlow via SNMP aikaisemmin määritetyllä SNMPv3 käyttäjällä. Kuviossa 33 nähdään HP 3500yl-kytkimelle määritelty agentti.



Kuvio 33. sFlowTrend agentin määrittely

Työasemalta pistettiin ping menemään AD-palvelimelle ja SDN kontrollerille, jotta sFlowTrend saa dataa. Kuviossa 34 nähdään jokaisen kytkimen jokaisesta rajapinnasta otettua dataa.



Kuvio 34. sFlowTrend Top N

6 Pohdinta ja yhteenveto

Opinnäytetyön tavoitteena oli rakentaa SDN-testiympäristö. Ympäristössä oli tarkoitus testata normaaleissa verkkoympäristöissä käytössä olevia palveluita ja ratkaisuja, etsiä ja testata SDN-sovelluksia joilla voitaisiin korvata perinteisiä versioita palveluista sekä pohtia onko perinteistä lähiverkkoa järkevää korvata SDN-verkolla.

Työssä käytettiin Aruba VAN SDN-kontrolleria. Itse kontrolleri toimi hyvin ilman ongelmia, mutta tähän asennetut ohjelmat tuottivat paljon ongelmia. Aruba VAN SDN-kontrolleri on uudelleen brändätty versio HPE VAN SDN-kontrollerista. Ohjelma jolla pyrittiin korvaamaan sFlowTrendia, oli HPE Network Visualizer. Vaikkakin kontrolleri ja ohjelma on tehty samassa yrityksessä, yhteensopivuusongelmia oli paljon. Aruba tarjoaa myös SDN-sovelluksille sovelluskauppaa, mutta uusinkin sovellus on jo vuoden ikäinen. Sovellusten tarjonta on myös erittäin vähäistä. Sovelluskaupasta ladatuista viidestä ohjelmasta vain kaksi asentui ongelmitta.

Kontrollerille ei myöskään löytynyt mitään ohjelmaa, joka pystyisi hoitamaan käyttäjien tai päätelaitteiden autentikointia. Vastaavia ohjelmia on saatavilla muille kontrollereille, jotka eivät ole Java-pohjaisia. Perinteisen lähiverkon korvaaminen SDN-pohjaisella verkolla vaikuttaa erittäin riskialttiilta. Jos verkossa ilmenee ongelmia, voi ongelma olla konfiguraatioissa kuten nykyään tai se voi olla puhtaasti ohjelmistopohjainen jossakin SDN-sovelluksessa.

Opinnäytetyön tavoitteissa onnistuttiin osittain. Testiympäristöön saatiin toteutettua kaikki nykyisin käytössä olevat palvelut ja nämä toimivat ongelmitta. Myöskin SDN-kontrolleri toimii hyvin OpenFlown-kytkimien kanssa. Perinteisen verkon palveluita ei kuitenkaan saatu korvattua SDN:n pohjaisilla sovelluksilla, joko niiden puutteen vuoksi tai yhteensopivuusongelmien takia.

Kytkimet eivät tukeneet *custom pipeline*-ominaisuutta. Tämän ominaisuuden myötä verkko olisi huomattavasti hyödyllisempi SDN:n kannalta, sillä ominaisuuden mukana tulee runsaasti lisää vuotauluja. Nykyisellään vuotaulut täytyy luoda erillisellä ohjelmalla. Kytkinten korvaaminen uudemmilla saattaisi myös korjata kytkimen ja HPE

Network Visualizerin välisen autentikointi ongelman. Jos SDN halutaan ottaa käyttöön tuotannossa, kannattaa tutkia vaihtoehtoisia kontrollereita tai varautua koodaamaan lähes kaikki ohjelmat itse

Lähteet

Aruba VAN SDN Controller 2.8 Administrator Guide, 2017. Viitattu 18.05.2018. http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00003662en_us-1.pdf

Auvinen, T., Filtshev, S., Haavisto, E., Meisalmi, A. & Mäki-Ullakko, J. 2017. IT-palveluiden hallinta ja tietoturvan toteutus. Jyväskylän ammattikorkeakoulu.

Chapter: IEEE 802.1X Port-Based Authentication. 2016. Viitattu 14.12.2017. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html

Creating HP Software-defined Networks, Rev 14.31. 2014. HP ExpertOne Learner Guide – Book 1 of 3.

HPE Network Visualizer SDN Application 1.1 Administration Guide. Viitattu 16.04.2018. https://support.hpe.com/hpsc/doc/public/display?docId=c05040369

Liikevaihto ja henkilöstö. N.d. Viitattu 11.05.2018. https://www.inmics.fi/yritys/liikevaihto-ja-henkilosto/

OpenFlow Switch Specification Version 1.5.1. 2015. https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

Sertifioitua osaamista. N.d. Viitattu 11.05.2018. https://www.inmics.fi/yritys/sertifioitua-osaamista/

sFlowTrend. N.d. Viitattu 15.04.2018. https://inmon.com/products/sFlowTrend.php

Software-Defined Networking: The New Norm for Networks. 2012. Viitattu 11.12.2017. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

sFlow, Traffic Monitoring using sFlow. 2013. Viitattu 12.12.2017. http://www.sflow.org/sFlowOverview.pdf

Simple Network Management Protocol. 2018. Viitattu 18.05.2018. https://searchnetworking.techtarget.com/definition/SNMP

TShark – Dump and analyze network traffic. N.d. Viitattu 16.04.2018. https://www.wireshark.org/docs/man-pages/tshark.html

Understanding the SDN Architecture – SDN Control Plane & SDN Data Plane. N.d. Viitattu 12.12.2017. https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture/

What are SDN Controller (or SDN Controllers Platforms)? N.d. Viitattu 12.12.2017. https://www.sdxcentral.com/sdn/definitions/sdn-controllers/

What are SDN Northbound APIs? N.d. Viitattu 12.12.2017. https://www.sdxcentral.com/sdn/definitions/north-bound-interfaces-api/

What are SDN Southbound APIs? N.d. Viitattu 12.12.2017. https://www.sdxcentral.com/sdn/definitions/southbound-interface-api/

What is SDN? N.d. Viitattu 11.12.2017.
https://www.juniper.net/us/en/solutions/sdn/what-is-sdn/

Who is the Open Networking Foundation? N.d. Viitattu 12.12.2017.
https://www.sdxcentral.com/sdn/definitions/who-is-open-networking-foundation-onf/

Liitteet

Liite 1. HP ProCurve 3500yl konfiguraatiot

```
hostname "HP-3500yl-24G"
module 1 type j86xxa
console idle-timeout 7200
console idle-timeout serial-usb 7200
radius-server host 10.249.149.3 key "XXX"
sflow 1 destination 10.249.149.12
sflow 1 polling 1-4 20
sflow 1 sampling 1-4 50
ip default-gateway 10.249.149.1
interface 1
   name "to VM"
   exit
interface 2
   name "to 5406"
   exit
snmp-server community "public" unrestricted
snmpv3 enable
snmpv3 only
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "sdn"
aaa accounting exec start-stop radius
aaa authentication login privilege-mode
aaa authentication telnet login radius
aaa authentication telnet enable radius
aaa authentication ssh login radius
aaa authentication ssh enable radius local
aaa authentication port-access chap-radius
openflow
   controller-id 1 ip 10.249.149.2 controller-interface vlan 2200
   instance "1"
      member vlan 2201
      controller-id 1
      version 1.3
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-2
   untagged 3-24
   no ip address
   exit
vlan 2200
   name "VLAN2200"
   untagged 1
   tagged 2
   ip address 10.249.149.11 255.255.255.0
   exit
vlan 2201
   name "OPENFLOW"
   tagged 1-2
   ip address 10.249.150.11 255.255.255.0
   exit
spanning-tree
spanning-tree mode rapid-pvst
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
device-profile name "default-ap-profile"
   cos 0
   exit
password manager
password operator
```

Liite 2. HP ProCurve 5406zl konfiguraatio

```
hostname "HP-Switch-5406zl"
module 1 type j8702a
console idle-timeout 7200
console idle-timeout serial-usb 7200
radius-server host 10.249.149.3 key "XXX"
sflow 1 destination 10.249.149.12
sflow 1 polling A2-A3 20
sflow 1 sampling A2-A3 50
ip default-gateway 10.249.149.1
interface A2
   name "to 3500"
   exit
interface A3
   name "LAPTOP"
   exit
snmp-server community "public" operator unrestricted
snmpv3 enable
snmpv3 only
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "sdn"
aaa accounting exec start-stop radius
aaa authentication login privilege-mode
aaa authentication telnet login radius
aaa authentication telnet enable radius
aaa authentication ssh login radius
aaa authentication ssh enable radius local
aaa authentication port-access chap-radius
aaa port-access authenticator A1,A3-A24
aaa port-access authenticator A1 auth-vid 2201
aaa port-access authenticator A1 unauth-vid 99
aaa port-access authenticator A3 auth-vid 2201
aaa port-access authenticator A3 unauth-vid 99
aaa port-access authenticator A4 auth-vid 2201
aaa port-access authenticator A4 unauth-vid 99
aaa port-access authenticator A5 auth-vid 2201
aaa port-access authenticator A5 unauth-vid 99
aaa port-access authenticator A6 auth-vid 2201
aaa port-access authenticator A6 unauth-vid 99
aaa port-access authenticator A7 auth-vid 2201
aaa port-access authenticator A7 unauth-vid 99
aaa port-access authenticator A8 auth-vid 2201
aaa port-access authenticator A8 unauth-vid 99
aaa port-access authenticator A9 auth-vid 2201
aaa port-access authenticator A9 unauth-vid 99
aaa port-access authenticator A10 auth-vid 2201
aaa port-access authenticator A10 unauth-vid 99
aaa port-access authenticator A11 auth-vid 2201
aaa port-access authenticator A11 unauth-vid 99
aaa port-access authenticator A12 auth-vid 2201
aaa port-access authenticator A12 unauth-vid 99
aaa port-access authenticator A13 auth-vid 2201
aaa port-access authenticator A13 unauth-vid 99
aaa port-access authenticator A14 auth-vid 2201
aaa port-access authenticator A14 unauth-vid 99
aaa port-access authenticator A15 auth-vid 2201
aaa port-access authenticator A15 unauth-vid 99
aaa port-access authenticator A16 auth-vid 2201
aaa port-access authenticator A16 unauth-vid 99
aaa port-access authenticator A17 auth-vid 2201
aaa port-access authenticator A17 unauth-vid 99
aaa port-access authenticator A18 auth-vid 2201
aaa port-access authenticator A18 unauth-vid 99
aaa port-access authenticator A19 auth-vid 2201
aaa port-access authenticator A19 unauth-vid 99
aaa port-access authenticator A20 auth-vid 2201
aaa port-access authenticator A20 unauth-vid 99
aaa port-access authenticator A21 auth-vid 2201
aaa port-access authenticator A21 unauth-vid 99
aaa port-access authenticator A22 auth-vid 2201
aaa port-access authenticator A22 unauth-vid 99
aaa port-access authenticator A23 auth-vid 2201
aaa port-access authenticator A23 unauth-vid 99
aaa port-access authenticator A24 auth-vid 2201
aaa port-access authenticator A24 unauth-vid 99
aaa port-access authenticator active
```

```
openflow
   controller-id 1 ip 10.249.149.2 controller-interface vlan 2200
   instance "1"
      member vlan 2201
      controller-id 1
      version 1.3
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged A1-A24
   no ip address
   exit
vlan 99
   name "BLOCKED"
   no ip address
   ip helper-address 10.249.149.3
   exit
vlan 2200
   name "VLAN2200"
   tagged A1-A2
   ip address 10.249.149.10 255.255.255.0
   exit
vlan 2201
   name "OPENFLOW"
   untagged A1,A3-A24
   tagged A2
   ip address 10.249.150.10 255.255.255.0
   ip helper-address 10.249.149.3
   exit
spanning-tree
no spanning-tree bpdu-throttle
spanning-tree mode rapid-pvst
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
device-profile name "default-ap-profile"
   cos 0
   exit
password manager
password operator
```