Jarno Sippo

HUS LAN 802.1X POC

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

IoT & Cloud Computing

Insinöörityö

13.5.2024

Tiivistelmä

Tekijä:	Jarno Sippo
Otsikko:	HUS LAN 802.1X POC
Sivumäärä:	38 sivua
Aika:	13.5.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	IoT & Cloud Computing
Ohjaajat:	Kehittämispäällikkö Jan Tamlander
	Osaamisaluejohtaja Janne Salonen

Tämän insinöörityön tarkoituksena oli tarkastella konseptitasolla lankaverkon porttikohtaisen todennuksen toteuttamista haasteineen ja hidasteineen HUS-yhtymän 802.1X POC kohteen suunnitteluvaiheessa. Työn edellytyksinä oli tutustua tarkemmin käytettyihin teknologioihin ja konseptin eri osa-alueisiin. Kokonaiskuvan hahmotuttua pohdittiin konseptin olemassa olevia ja tulevia, todennettuja ja teoreettisia haasteita sekä hidasteita.

Insinöörityön käytännön osuuden alussa tunnistettiin konseptissa käytetyt protokollat ja teknologiat. Työn ympäristön muu tuntemus tulee omasta kymmenen vuoden mittaisesta työurasta HUS-lähituessa ja Tietohallinnossa. Kokonaiskuvan tarkennuttua voitiin ryhtyä luomaan lista hidasteista ja haasteista.

Tunnistettujen käytännön haasteiden ja hidasteiden pohdinnoissa syvennyin aiheisiin omien kokemuksieni ja teorian avuin. Pohdintojen tuloksena saavutettiin kirjallinen koonti todennetuista ja oletetuista haasteista ja hidasteista.

Työ vei aikaa ja ilman aikaisempaa uraa HUSin ympäristössä työn toteuttaminen ei olisi ollut mahdollista nykyisessä muodossaan ja laajuudessaan.

Avainsanat: HUS, 802.1X, POC, Cisco ISE

Abstract

Author:	Jarno Sippo
Title:	HUS LAN 802.1X POC
Number of Pages:	38 pages
Date:	13 May 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	IoT & Cloud Computing
Supervisors:	Jan Tamlander, Development Manager Janne Salonen, Director of school

---

The purpose of this thesis was to examine at the concept level the implementation of wired networks port-based authentication with its challenges and obstacles in HUS Group – The Joint Authority of the Helsinki and Uusimaa Hospital Districts 802.1X proof of concept location within planning. The prerequisites for the work included gaining a more detailed understanding of the technologies used and the various aspects of the concept. Once the overall picture became clear, existing, and future, confirmed and theoretical challenges and obstacles of the concept were reflected.

In the practical part of the thesis work, the protocols and technologies used in the concept were identified. The additional knowledge of the work environment comes from my own, ten-year career at HUS Onsite Support and IT management. Once the overall picture became clearer, a list of challenges and obstacles could be created.

In reflecting on the identified practical challenges and obstacles, i delved into the subjects with the help of my own experiences and learner theory. As a result of the reflections, a written summary of the verified and assumed challenges and obstacles was achieved.

Work took time and without previous experience in the HUS environment, the implementation of the work would not have been possible in its current form and extent.

Keywords: HUS, 802.1X, POC, Cisco ISE

Sisällys

Lyhenteet

802.1X: IEEE:n (Institute of Electrical and Electronics Engineers) ylläpitämä ja kehittämä porttikohtaisen todennuksen standardi.

AAA: Authentication, Authorization, Accounting. Protokolla tunnistamiseen, valtuuttamiseen ja tilastointiin.

AD: Active Directory. AD on hierarkkinen resurssienjakelu ja - tallennusjärjestelmä, jonne tallennetaan muun muassa käyttäjätietoa ja yrityksen dataa.

AD DC: Active Directory Domain Controller. AD DC on palvelin, jossa on Windows Server käyttöjärjestelmä ja AD-järjestelmää hallinnoivia ohjelmia.

API: Application Programming Interface. API on rajapinta, jossa kaksi tai useampi ohjelma keskustelee toisilleen.

CA: Certificate Authority. CA on järjestelmä, joka jakaa ja tallentaa digitaalisia sertifikaatteja PKI ympäristössä.

DHCP: Dynamic Host Configuration Protocol. IP osoitteiden jakamisessa käytetty verkkoprotokolla.

EAP: Extensible Authentication Protocol. Käyttäjien tunnistamisessa käytettävä protokolla.

EAPoL: Extensible Authentication Protocol over Local area network. Protokolla autentikoitavan käyttäjän ja verkon liityntäpisteen väliseen liikennöintiin.

HP: Hewlett-Packard. Maailmanlaajuinen vuonna 1939 perustettu tietotekniikka-alan yritys. Jakautui 2014 kuluttaja (HP) ja yritys (HPE) segmentteihin.

HPE: Hewlett-Packard Enterprice. 2014 perustettu maailmanlaajuisen tietotekniikka-alan yritys.

HTTP: HyperText Transfer Protocol. Internetselainten käyttämä tiedonsiirtoprotokolla.

HTTPS: HyperText Transfer Protocol Secure. Suojattu versio HTTP-protokollasta.

HUS: Helsingin ja Uudenmaan sairaanhoitopiiri.

HUSnet: HUSnet on yleisnimitys Tietohallinnon hallitsemille langalliseille ja langattomille verkoille.

IEEE: Institute of Electrical and Electrics Engineers. Kansainvälinen tekniikan alan järjestö.

IEC: International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio.

IETF: Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava organisaatio, kuten W3C, ISO ja IEC.

IKE: Internet Key Exchange. Protokolla salausavaimien vaihtamiseen IP-verkon yli.

IoT: Internet of Things. Esineiden internet.

IP: Internet Protocol. Yleisesti käytetty tietoliikenneprotokolla.

IPAM: IP Address Management. Järjestelmä IP osoitteiden hallintaan.

ISO: International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.

IT: Information Technology. IT on termi, joka kattaa yleisesti laitteita, jotka käyttävät tietotekniikkaa tiedonkäsittelyyn ja prosessointiin.

KRB5: Kerberos. Todennusprotokolla käyttäjien tunnistamiseen verkossa.

LAN: Local Area Network. Lähiverkko.

LDAP: Lightweight Directory Access Protocol. Hakemistopalveluiden käyttöön tarkoitettu protokolla.

OSI: Open Systems Interconnection Reference Model. Kuvaa tiedonsiirtoprotokollien yhteistoiminnot seitsemän kerroksen mallina.

NAC: Network access control. Verkkoonpääsyä kontrolloiva laite.

MAB: Mac Address Bypass. Porttikohtainen autentikointi MAC-osoitteen perusteella.

MAC: Media Access Control. OSI-mallin siirtoyhteyskerroksen toinen alikerros.

MnT: Monitoring node. MnT on Ciscon ISE-verkonhallintajärjestelmän lyhennys laitteiden monitorointinoodista.

PAN: Primary Administration Node. PAN on Ciscon ISE-verkonhallintajärjestelmän lyhennys hallintanoodista.

PEAP: Protected Extensible Authentication Protocol. Ciscon ja Microsoftin kehittämä suojattu EAP protokolla.

PKCS: Public Key Cryptography Standard. Salausmenetelmä, joka käyttää RSA-algoritmia.

PKI: Public Key Infrastructure. PKI on NAC-ympäristössä digitaalinen kokonaisuus, jossa luodaan ja välitetään sertifikaatteja tarvittaville päätelaitteille, jotta NAC-järjestelmä voi luottaa laitteisiin.

POC: Proof of concept.

PoE: Power-over-Ethernet. Tekniikka, jossa Ethernet-kaapelin välityksellä kulkee virransyöttö.

PSN: Policy Service node. Ciscon ISE-verkonhallintajärjestelmän lyhennys käytäntöjä hallitsevasta ja prosessoivasta noodista.

PxGrid: Platform eXchange Grid. PxGrid on Ciscon ISE-verkonhallintajärjestelmän lyhennys tietoturvajärjestelmiä yhdistävästä noodista.

RADIUS: Remote Authentication Dial In User Service. Verkon liityntäpisteen ja autentikointipalvelimen väliseen liikennöintiin käytetty protokolla.

REST: REpresentational State Transfer. REST on API, jossa tieto jaetaan HTTP-protokollan avulla.

RFC: Request For Comments. Kokoelma Internetiä koskevia standardeja.

RSA: Rivest, Shamir, Adleman algorith. Kehittäjien sukunimien alkukirjainten mukaan nimetty salausalgoritmi.

SFP: Small Form-factor Pluggable. Pienikokoinen ja helposti vaihdettava verkkoporttimoduuli, jota käytetään verkko- ja tietoliikennelaitteissa, kuten kytkimissä, reitittimissä ja palomuureissa.

SQL: Structured Query Language. Standardoitu kyselykieli relaatiotietokannan hallintaan.

TLS: Transport Layer Security. Salausprotokolla, jolla salataan liikenne IP-verkkojen yli.

VLAN: Virtual Local Area Network. Virtuaalinen lähiverkko.

VoIP: Voice Over Internet Protocol. Äänen siirtäminen reaaliaikaisesti internetin yli.

W3C: World Wide Web Consortium. Kansainvälinen organisaatio, joka ylläpitää ja arkistoi internetin standardeja.

WLAN: Wireless Local Area Network. Langaton lähiverkko.

X.509: Kryptografian standardi julkisen avaimen salauksessa käytettäville varmenteille.

1 Johdanto

Tietoturvan ja erityisesti fyysisen tietoturvan merkitys tietoliikenneverkkojen toteutuksessa on merkittävissä määrin kriittisessä asemassa nykyaikaisissa tietoyhteiskunnan instituutioissa. Verrattain suuren tietoturvariskin mahdollisuus luvattoman tai tavoitteellisesti vihamielisen osapuolen liittäessä päätelaitteensa avoimeen, kytkimelle ristikytkettyyn verkkorasiaan on estettävissä tehokkaasti porttikohtaisella todennuksella.

Tämän insinöörityön tarkoituksena oli perehtyä selvittämään porttikohtaisen autentikoinnin toteutusta konseptitasolla HUS-yhtymän POC toimipisteessä.

Insinöörityö alustetaan esittelemällä HUS-yhtymä ja Tietohallinto, yleisesti käytetyt protokollat ja teknologiat. Insinöörityössä keskitytään vain fyysisten porttien porttikohtaiseen autentikointiin sekä siihen liittyviin tavoitteisiin, haasteisiin ja hidasteisiin. HUS-yhtymän toimipisteiden langaton verkko on toteutettu jo 802.1X muodossa.

2 HUS-yhtymä ja Tietohallinto

Helsingin ja Uudenmaan sairaanhoitopiiri oli vuosina 2000–2022 Suomen suurin sairaanhoitopiiri ja toiseksi suurin työnantaja. 2023 alusta toiminta siirtyi soteuudistuksen kautta HUS-yhtymän (viittaa pidempään nimeen Helsingin kaupungin ja muun Uudenmaan hyvinvointialueiden sosiaali- ja terveydenhuollon yhtymä), lyh. HUS alaisuuteen. [1.]

Kuva 1. HUS yleisesti numeroina

Tietohallinto vastaa HUSin tietojärjestelmien ylläpidosta. Keskeisiä järjestelmiä ovat potilastietojärjestelmät, talous- ja henkilöstöhallinnon järjestelmät sekä tukipalveluyksiköiden järjestelmät. Tietohallinnon asiakkaita ovat HUS-yhtymä, yhtymän yhteistyökumppanit, tytär- ja osakkuusyhtiöt, hyvinvointialueet sekä yksityiset terveydenhuollon toimijat ja viranomaiset.

Kuva 2. Tietohallinto numeroina

3 Autentikointiprotokollat

Autentikointiprotokollien tehtävänä on varmistaa käyttäjän, laitteen tai palvelun henkilöllisyys ja oikeellisuus tietojärjestelmään tai verkkoon kirjautuessa. Protokollien avulla varmistetaan, että vain oikeutetut käyttäjät pääsevät käyttämään suojattuja resursseja ja ettei tietoja pääse vääristämään tai varastamaan. Autentikointiprotokollat sisältävät yleensä käyttäjätunnistuksen, salasanan tai muun tunnistautumistiedon tarkistuksen ja varmistuksen ennen kuin pääsy sallitaan. Tämä auttaa suojaamaan tietoja ja estämään luvattoman pääsyn tietojärjestelmiin.

3.1 AAA

AAA-protokollan toiminta perustuu kolmeen pääperiaatteeseen: Todentaminen (Authentication), Valtuutus (Authorization) ja Tilastointi (Accounting).

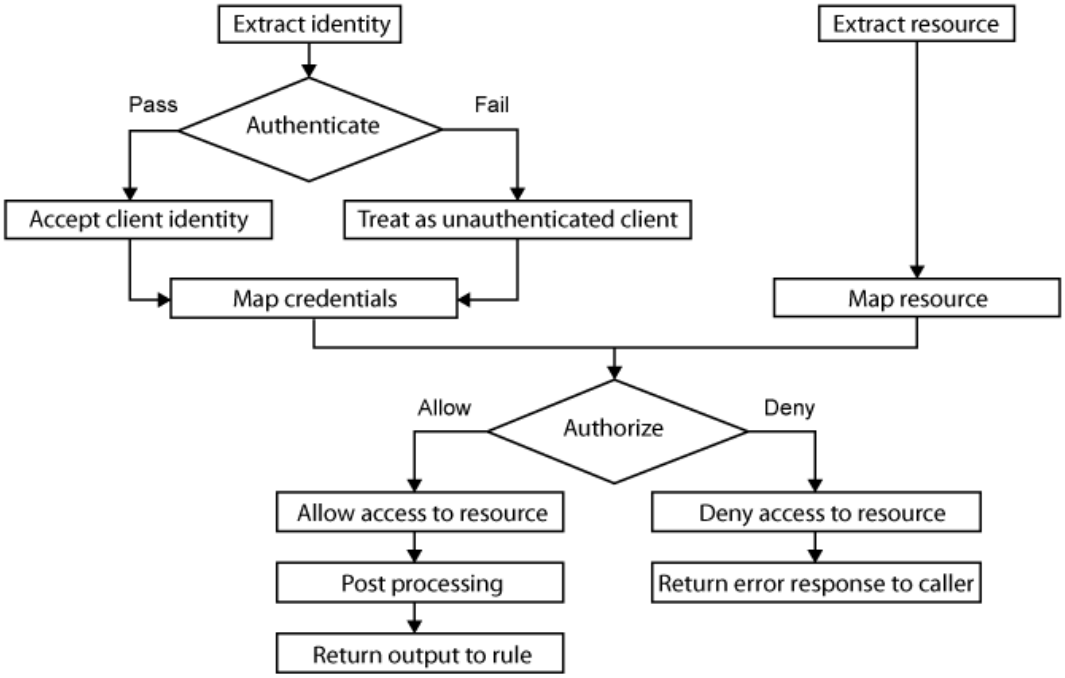
Todentaminen tarkoittaa käyttäjän tunnistamista ja varmennusta. Käyttäjän täytyy todistaa oma identiteettinsä esimerkiksi käyttäjätunnuksen ja salasanan avulla ennen kuin hänelle myönnetään pääsy palveluun.

Valtuutus määrittelee, mitä resursseja tai palveluita käyttäjä saa käyttää sen jälkeen, kun hän on tunnistautunut. Valtuutus perustuu yleensä käyttäjäryhmiin tai rooleihin, joita on määritelty etukäteen.

Tilastointi tallentaa kaikki käyttäjän tekemät toimenpiteet ja pääsyt resursseihin. Tilastointia käytetään jälkikäteen valvontaan ja tarkasteluun esimerkiksi mahdollisten tietoturvaloukkausten selvittämisessä.

AAA-protokolla on keskeinen osa monia verkkopalveluita, kuten yritysverkkoja, palvelinjärjestelmiä ja mobiilisovelluksia. Sen avulla varmistetaan tietoturvan ja hallinnan tasainen toteutus kaikissa käyttöympäristöissä.

Yleisimpiä käytettyjä AAA-protokollia ovat RADIUS, DIAMETER ja TACACS+. [2.]



Kuva 3. AAA-protokollan prosessikaavio [3.]

3.1.1 Todentaminen

Authentication [2.], eli todentaminen tarkoittaa palvelua, jolla tunnistetaan verkkoon kirjautuvan käyttäjän tai laitteen identiteetti. Tunnistamisessa voidaan käyttää esimerkiksi käyttäjätunnus-salasana yhdistelmää, sertifikaattia tai laitteen MAC-osoitetta. Todentamisprosessi suoritetaan ennen käyttäjän pääsyä verkkoon. (Kuva 3)

Käyttäjän todentamisessa yleisin käytetty menetelmä on salasanan ja käyttäjätunnukseen perustuva yhdistelmä. Tämän todentamisen muoto on kuitenkin verrattain haavoittuvaisempi muihin tapoihin verrattuna. Esimerkkeinä:

Heikot salasanat

Käyttäjät saattavat valita helposti arvattavia tai yleisesti käytettyjä salasanoja, jotka ovat helposti murrettavissa esimerkiksi julkisesti saatavilla olevien salasanalistojen avulla. Tämä voi johtua siitä, että käyttäjät eivät ymmärrä salasanan tärkeyttä tai eivät jaksa luoda vahvaa salasanaa.

Salasanojen jakaminen

Käyttäjät saattavat jakaa salasanansa muiden kanssa tai käyttää samaa salasanaa useissa eri palveluissa. Tämä lisää tietoturvariskiä, sillä jos yksi salasana vuotaa, kaikki käyttäjän tilit ovat vaarassa. Lisäksi vahvimmatkaan salasanat eivät kuitenkaan suojaa järjestelmää, jos ne päätyvät muiden kuin käyttäjän itsensä tietoon.

Salasanojen varastaminen

Huijaajat käyttävät erilaisia menetelmiä, kuten tietojenkalastelua (phishing), näppäimitölukijaa (keylogger) ja brute force -hyökkäystä. Käyttäjien salasanoja saadaan selvitettyä valitettavan menestyksekkäästi. [4.]

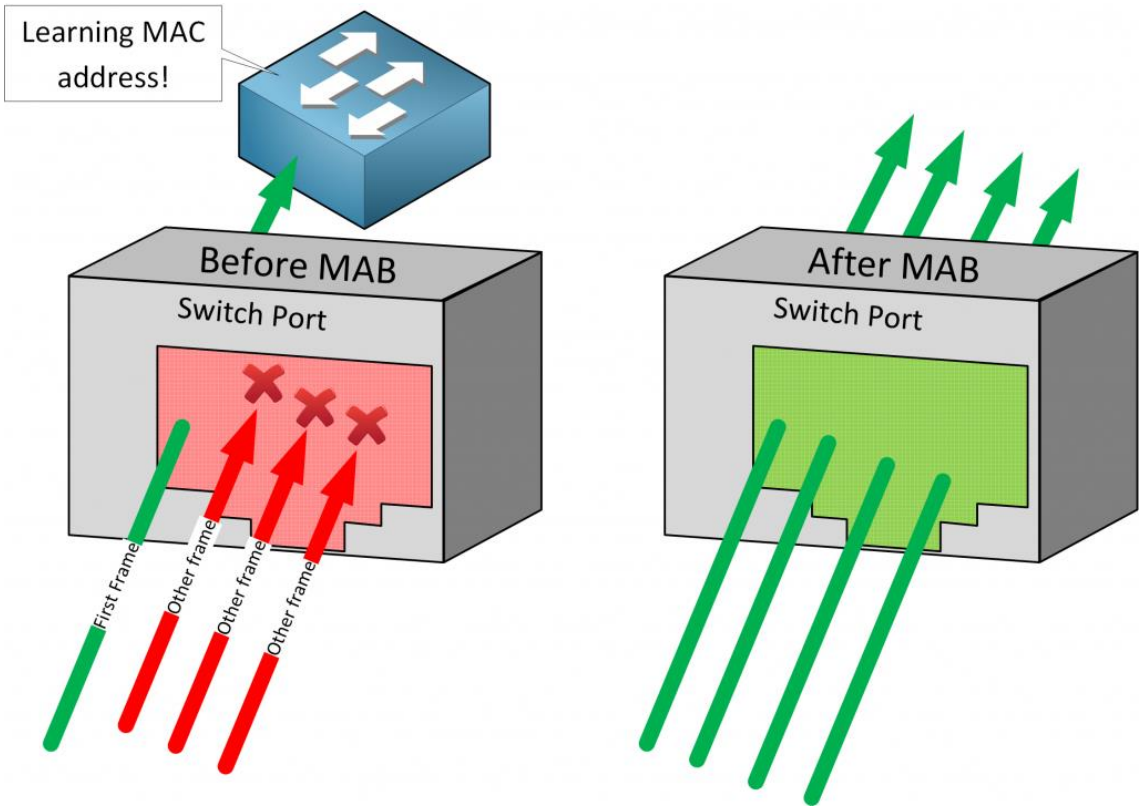
Salasanaan ja käyttäjätunnukseen perustuvan tunnistautumisen vahvistamiseksi on otettu laajalti käyttöön monivaiheinen tunnistautuminen. Siinä käyttäjä kirjautuu järjestelmään käyttäen omaa käyttäjätunnustaan, salasanaansa sekä esimerkiksi vaihtuvaa numerokoodia, jonka käyttäjä saa haltuunsa tekstiviestistä tai sovelluksesta, jonka hän syöttää vielä tunnistautuakseen. [5.]

Laitepohjainen sertifikaatti on tapa todentaa laitteen identiteetti ja varmistaa sen turvallisuus erilaisissa verkko- ja tietoliikenneympäristöissä. Sertifikaatti perustuu laitteen ainutlaatuiseen tunnistetietoon, kuten sen valmistajan antamaan laiteavaruuskohtaiseen salakirjoitusavaimen.

Todentaminen tapahtuu yleensä yhdistettäessä laitetta esimerkiksi verkkoon tai toiseen laitteeseen. Laitepohjainen sertifikaatti voi auttaa estämään haitallisia toimintoja, kuten tietomurtoja tai luvattomia pääsyjä laitteeseen. [6.]

MAB (MAC-based authentication) on menetelmä, jossa verkkolaitteiden käyttäjätunnistus perustuu laitteen MAC-osoitteeseen. MAC-osoite on verkkolaitteen ainutlaatuinen tunniste, joka voidaan käyttää laitteen tunnistamiseen verkon hallintaa varten. MAB-todentaminen edellyttää, että verkon hallintajärjestelmä tunnistaa laitteen MAC-osoitteen ja sallii tai estää verkkoyhteyden sen perusteella

osana laajempaa verkon turvallisuusstrategiaa. On tärkeää huomioida, että pelkkä MAC-osoitepohjainen todentaminen ei välttämättä tarjoa riittävää turvatasoa, ja siksi sitä kannattaa käyttää yhdessä muiden turvallisuustoimenpiteiden kanssa. [7.]



Kuva 4. MAB todennuksen havainnollistaminen [7.]

3.1.2 Valtuutus

Authorization [2.], eli valtuutuksen tarkoituksena on varmistaa, että käyttäjä on oikeutettu käyttämään tiettyjä verkkopalveluita tai resursseja. Valtuutus määrittelee käyttäjän tunnistamisen ja todennuksen sekä käyttöoikeuksien hallinnan.

Valtuutus suoritetaan todennuksen jälkeen, kun käyttäjä on onnistuneesti kirjautunut verkkoon. Valtuutus perustuu ennalta määrättyyn protokollaan, eli tietyille käyttäjille on tietyt oikeudet tehdä toimintoja verkossa.

Tietyiltä käyttäjiltä voidaan esimerkiksi estää pääsy julkisen verkon palveluihin kuten internettiin, ja sallia pääsy vain yrityksen sisäverkon testipalvelimelle. Toisena esimerkkinä sallitaan käyttäjälle pääsy vain julkisen verkon palveluihin yrityksen WLAN-verkossa, joissa vierailijat saavat internet-yhteyden käyttöönsä, mutta eivät voi käyttää yrityksen sisäverkon palveluita.

3.1.3 Tilastointi

Accounting [2.], eli tilastointi tarkoittaa tiedon keräämistä verkon käyttäjistä. Tilastointi on tarkoitettu keräämään tilastoja, raportteja ja lokitietoja, jotka liittyvät käyttäjän tunnistamiseen, valtuuttamiseen ja kirjautumiseen verkkopalveluihin. Tämä auttaa järjestelmänvalvojia seuraamaan ja analysoimaan verkon käyttöä ja tunnistautumista sekä havaitsemaan mahdollisia turvallisuusuhkia tai käyttöongelmia.

Tietoja tallennetaan muun muassa käyttäjien kirjautumisajoista, istunnoista, käyttöoikeuksista, käytetyistä palveluista sekä mahdollisista epäonnistuneista kirjautumisyrityksistä. Nämä tiedot voivat auttaa järjestelmänvalvojia havaitsemaan esimerkiksi luvattoman pääsyn yrityksen verkkoon tai tunnistamaan käyttäjiä, joilla on ongelmia kirjautumisessa.

Tilastojen avulla voidaan tarkastella verkon kuormitusta, käyttäjien käyttötottumuksia ja mahdollisia turvallisuusriskejä. Näiden tietojen avulla järjestelmänvalvojat voivat tehdä tarvittavia toimenpiteitä verkon suorituskyvyn optimoimiseksi ja turvallisuuden parantamiseksi.

Tilastointia voidaan käyttää myös raporttien luomiseen ja verkon käytön analysointiin. Raporttien avulla järjestelmänvalvojat voivat seurata verkon toimintaa, tunnistaa trendejä ja tehdä tulevaisuuden suunnitelmia verkon kehittämiseksi.

3.2 RADIUS

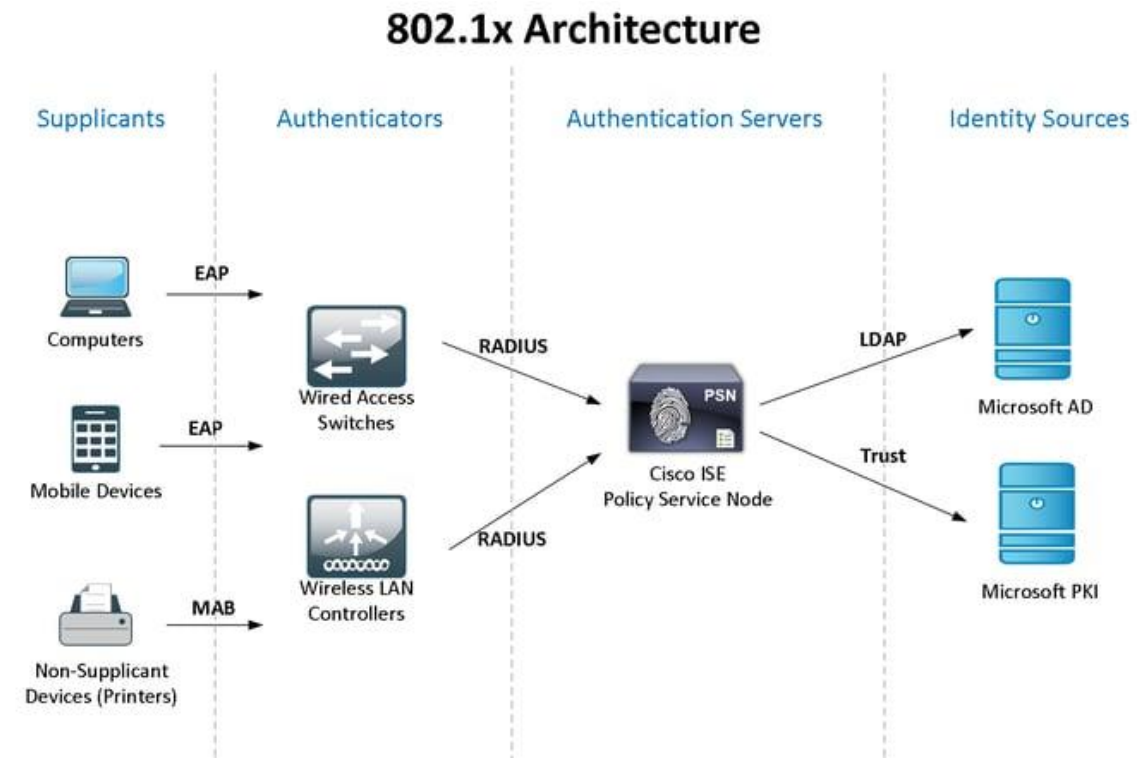
RADIUS (Remote Authentication Dial In User Service) on käyttäjien tunnistusta ja hallintaa tarjoava AAA-protokolla. RADIUS tarjoaa AAA-mallin mukaiset tunnistautumis-, valtuutus- ja tilastointipalvelut. RADIUS on de facto standardi etäkäyttäjien todentamisessa.

Nykymuodossaan RADIUS on määritelty IETF RFC 2865-dokumentissa. Määritykseen kuuluivat tunnistukseen ja valtuutukseen liittyvät toimenpiteet. Tilastointi on määritelty osaksi protokollaa myöhemmin RFC 2866-dokumentissa. Tilastoinnin tunnelointi on määriteltynä protokollaan RFC 2867-dokumentissa. Tunneloinnin attribuutit RFC 2868-dokumentissa ja RADIUS laajennokset RFC 2869-dokumentissa. [8.]

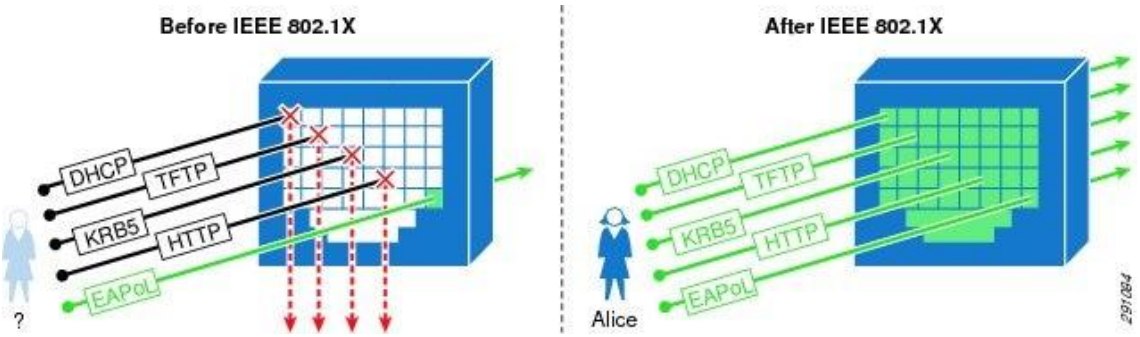
4 802.1X

802.1X on IEEE:n standardi, jota käytetään IEEE 802 -standardin määrittelemissä lähiverkoissa eli Ethernet-verkoissa ja WLAN-verkoissa. Yksinkertaistettuna standardi tarjoaa todentamismekanismin laitteille, jotka haluavat liittyä LAN- tai WLAN-verkkoon.

Estäen luvattoman päätelaitteen kommunikoinnin lähiverkon liityntäpisteessä. Ja salliessa luvallisten päätelaitteiden pääsyn verkkoon liityntäpisteestä riippumatta. [9.]



Kuva 5. 802.1X arkkitehtuuri ja erilliset identiteettilähteet [10.]



Kuva 6. Verkkoliikenne ennen ja jälkeen 802.1X todennukset [11.]

4.1 Protokollat

IEEE 802.1x -standardin mukaisessa porttikohtaisessa todennuksessa käytetään useita eri protokollia. Näitä käytetään niin tiedon siirtämiseen kuin salaamiseenkin. Protokollista oleellisimpia ovat erityisesti EAP, aiemmin kohdassa 3.2 esitelty RADIUS sekä kohdassa 4.1.5 esiteltävä EAPoL. RADIUSta käytetään liityntäpisteen ja todennuspalvelimen väliseen liikennöintiin, kun taas liikennöinti

asiakkaan ja liityntäpisteen välillä käydään EAPoL-protokollalla kuvion 6 mukaisesti tunnistautuessa. [9.]

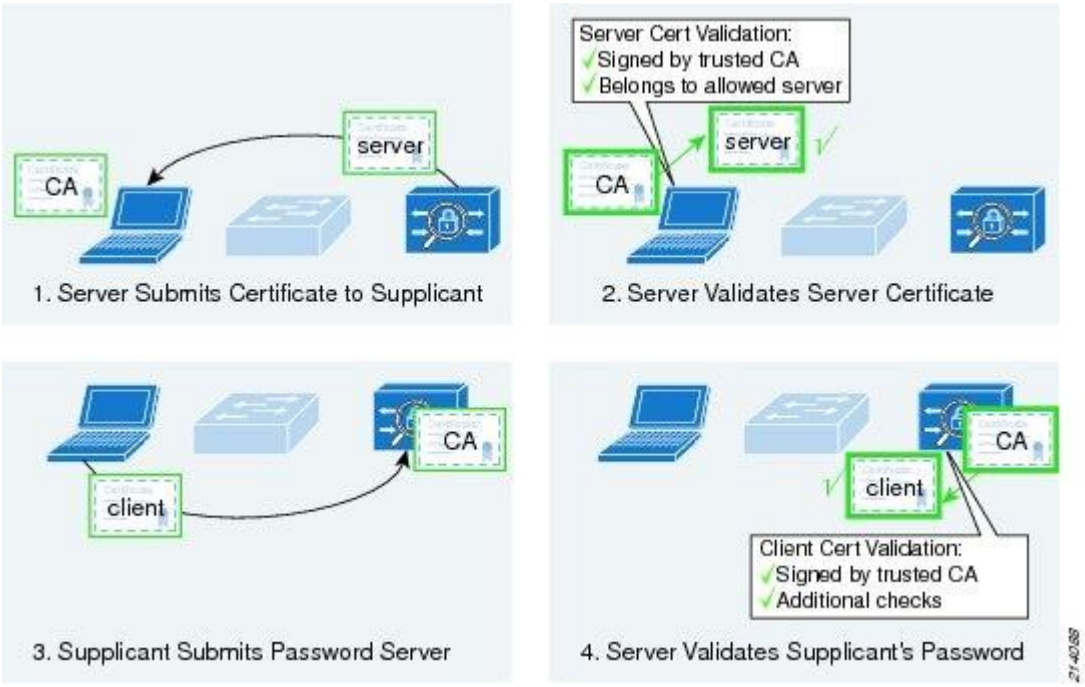
Kuva 7. 802.X komponentit [12.]

4.1.1 EAP

EAP (Extensible Authentication Protocol) on tietoturvaprotokollan viitekehys, jota käytetään laajasti porttikohtaisessa todentamisessa. EAP luo helposti omaan käyttöön sopivan arkkitehtuuripohjan. Se ei ole kuitenkaan todennusmenetelmä, vaan se tarjoaa kuljetusmetodin valitulle todennusmenetelmälle. EAP toimii OSI-mallin siirtoyhteyskerroksessa, eikä vaadi IP-yhteyttä toimiakseen. EAP soveltuu käytettäväksi kaikissa siirtoyhteyskerroksissa. [13.]

4.1.2 EAP-TLS

EAP-TLS (EAP with Transport Layer Security) käyttää todennusmenetelmänä varmenteita. Tämä vaatii asiakaslaitteelle asennetun asiakasvarmenteen ja todennuspalvelimelle asennetun palvelinvarmenteen. EAP-TLS on hyvin tuettu eri valmistajien keskuudessa, joten EAP-TLS tuki löytyy esimerkiksi Ciscon ja Microsoftin RADIUS-palvelimilta. [14.]



Kuva 8. EAP-TLS todennuksen askeleet [15.]

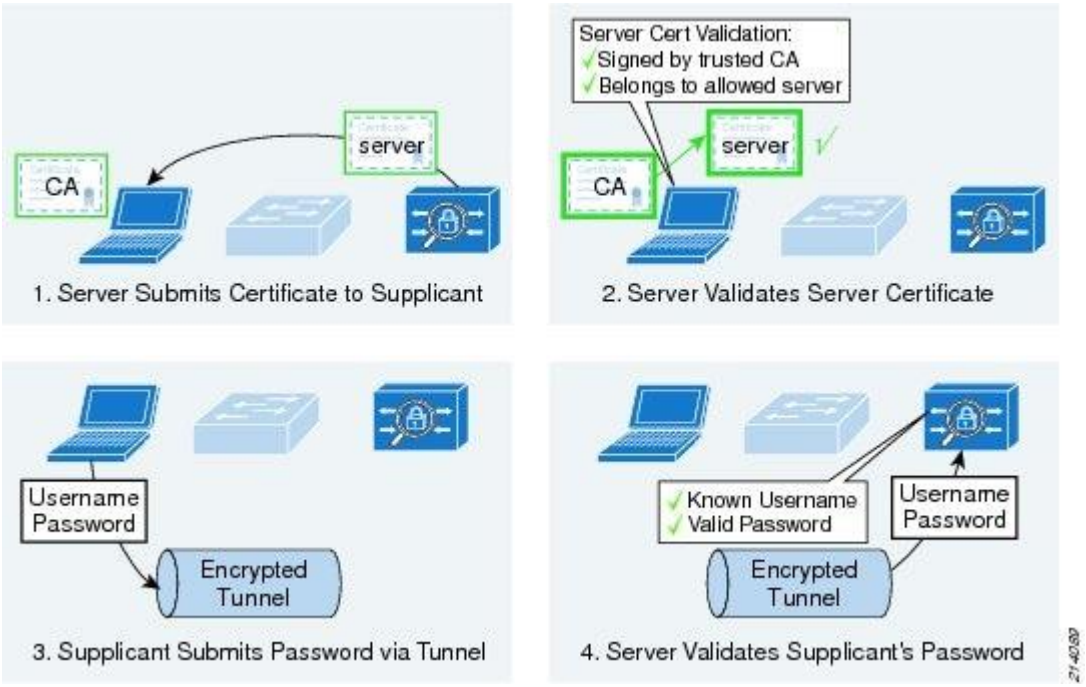
4.1.3 PEAP

PEAP (Protected Extensible Authentication Protocol) on Ciscon, Microsoftin ja RSA Securityn yhteistyössä kehittämä EAP-protokolla. PEAP ei ole todennusmenetelmä, vaan sen tarkoituksena on tarjota lisäturvaa muille EAP-protokollille. PEAP luo suojatun tunnelin tietoliikenteelle käyttäen TLS (Transport Layer Security) -protokollaa. Eroten EAP-protokollasta se lisää pakollisen molemminpuolisen todennuksen laitteiden välille. Näin pystytään estämään tehokkaasti liikenteen kaappaamista ja man-in-the-middle hyökkäyksiä. [16.]

4.1.4 MSCHAPv2

MS-CHAPv2 on Microsoftin toinen versio CHAP (Challenge-Handshake Authentication Protocol) -protokollasta. MS-CHAPv2-todennusta käytetään usein PEAP:n kanssa, jolloin asiakkaan ja todennuspalvelimen välinen liikenne on salattua. Ilman PEAP:n käyttöä MS-CHAPv2-todennus on alttiina niin kutsutuille sanakirjahyökkäyksille, joissa hyökkääjä yrittää arvata salasanan käymällä

kaikki sanakirjan sanat läpi komentosarjan avulla. MS-CHAPv2 on salasana-pohjainen todennusmenetelmä, joka tukee sekä asiakkaan että palvelimen todentamista. PEAP-MSCHAPv2-yhdistelmää käytetään pääosin Microsoftin Active Directory -ympäristöissä. [17.]



Kuva 9. PEAP-MSCHAPv2 todennuksen askeleet [18.]

4.1.5 EAPoL

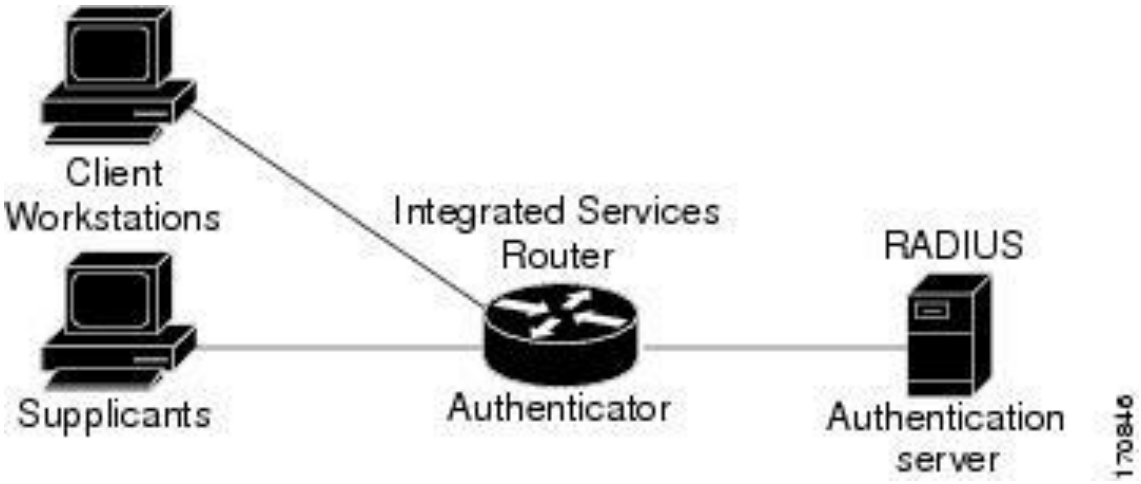
EAPoL (Extensible Authentication Protocol over LAN) on tietoliikenneprotokolla, jolla kapseloidaan 802.1x protokollan EAP-viestit ethernet kehykseen. Protokollaa käytetään välittämään asiakkaan ja todennuspalvelimen välistä EAP-liikennettä. [19.]

4.1.6 MAB

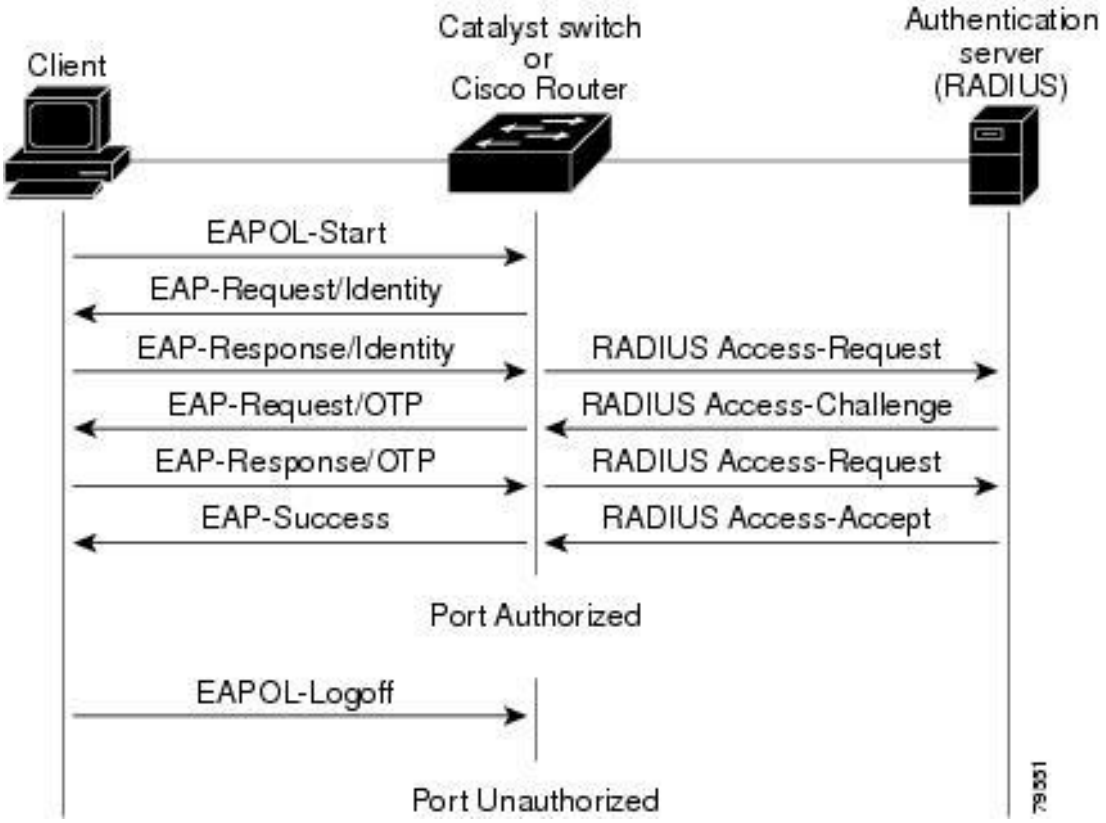
MAC Authentication Bypass on IEEE802.1x-standardin laajennus. Sitä käytetään, jos päätelaite ei tue EAP-todennusta. Näitä laitteita ovat yleensä verkkotulostimet, kamerat sekä muut sulautetut järjestelmät.

Kun MAB on konfiguroitu kytkimen porttiin, toimii se seuraavalla periaatteella. Kun laite kytketään verkkoon ja kytkin ei saa EAPoL-vastausta päätelaitteelta, lähettää kytkin RADIUS Access-Request-viestin todennuspalvelimelle. Tässä viestissä käyttäjätunnus ja salasanakentät täytetään todennettavan laitteen MAC-osoitteella. [20.]

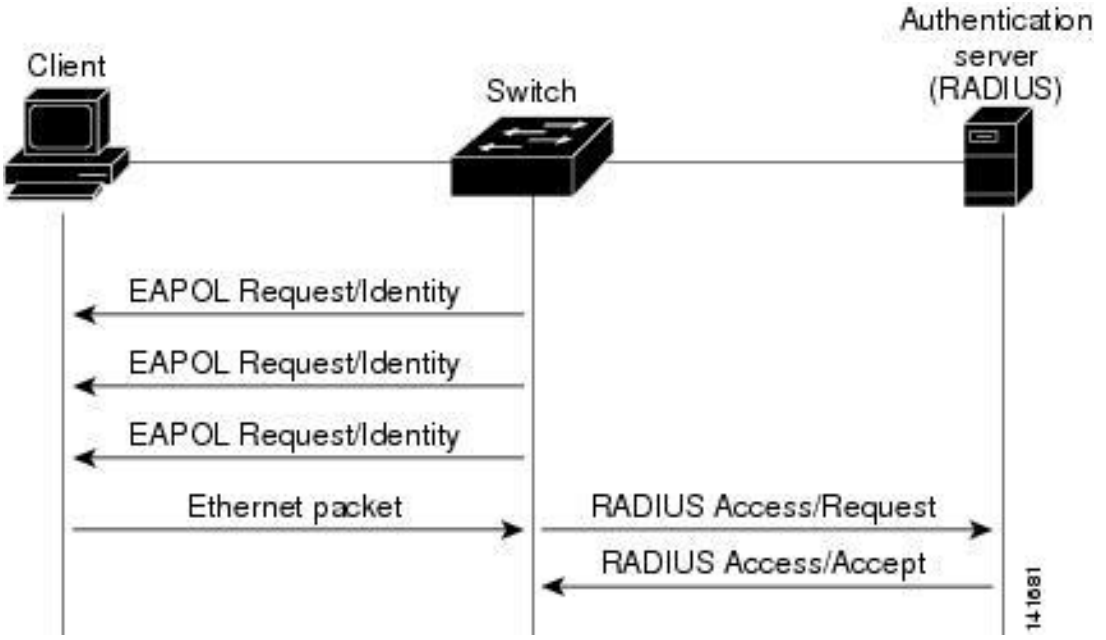
4.2 Porttikohtaisen todennuksen toiminta



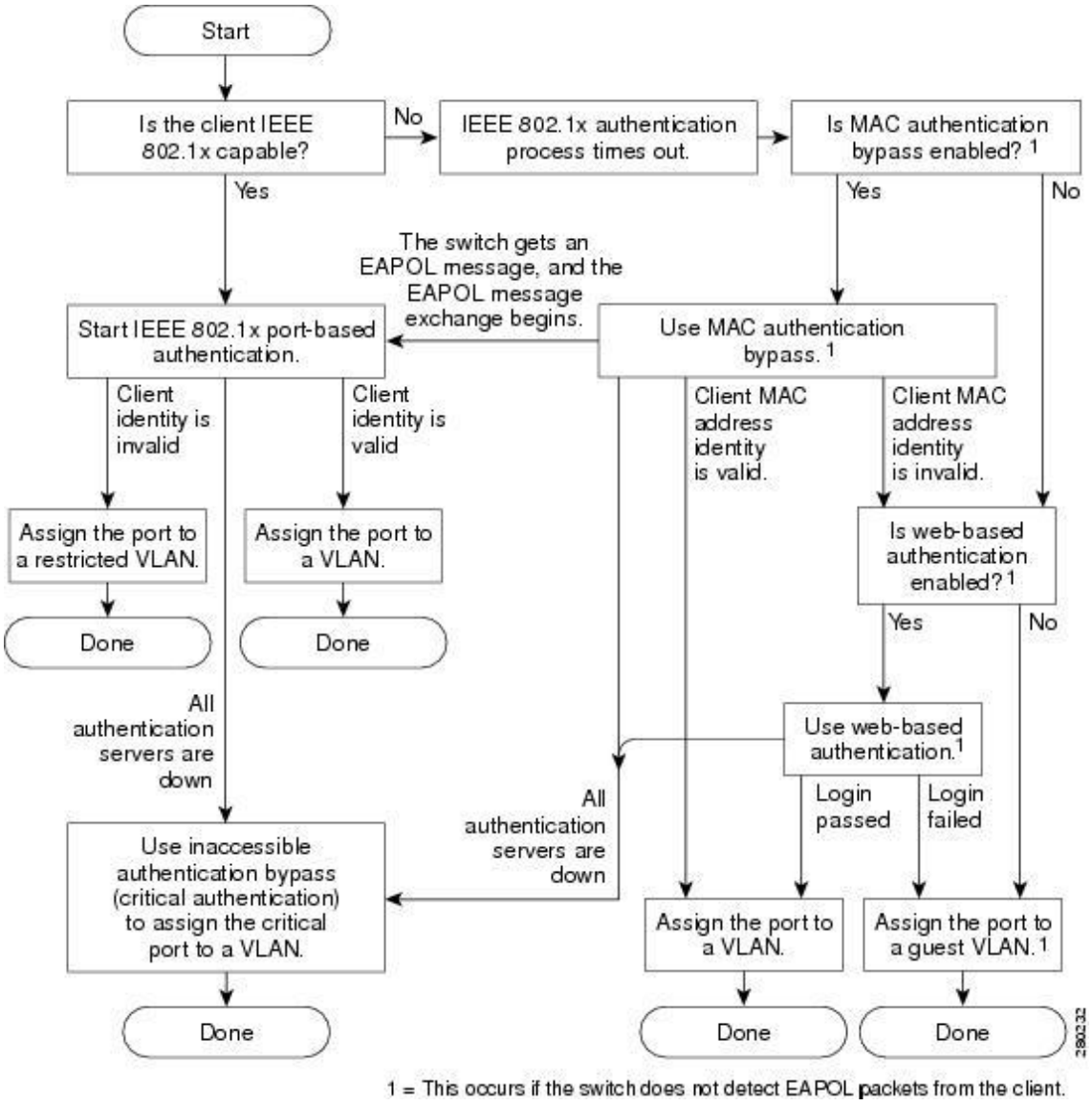
Kuva 10. Todennuksen laiteroolit [21.]



Kuva 11. EAP todennuksen viestien vaihto [22.]



Kuva 12. MAC pohjainen todennuksen viestin vaihto [23.]



Kuva 13. Todennuksen vuokaavio [24.]

Porttikohtaista todennusta käytettäessä kytkimen portti on aluksi unauthorized eli luvaton tilassa. Tässä tilassa vain EAPoL-liikenne on sallittu ja kaikki muu liikenne on estettynä. (kuva 6)

Kuvan 13 mukainen todennusprosessi alkaa kuvan 11 esittämällä mallilla, kun asiakas, eli päätelaite, kytketään porttiin ja päätelaite lähettää EAPoL-Start kehyksen kytkimelle. Kuvan 10 autentikaattori eli kytkin lähettää EAP-Request Identity-kehyksen. Asiakas avaa kuunteluyhteyden vastaanotettuaan EAP-Request Identity-kehyksen ja lähettää vastauksena EAP-Response Identity-

kehyksen autentikaattorille. Kehys sisältää asiakkaan tunnistustiedot, jotka autentikaattori kapseloi edelleen RADIUS Access-Request-paketiksi ja lähettää sen edelleen todennuspalvelimelle.

Neuvotteluvaihetta kutsutaan myös EAP-neuvotteluksi. Neuvotteluvaiheessa todennuspalvelin lähettää EAP Requestin sisältävän uudelleenlähetyksen autentikaattorille, jolla täsmennetään käytetty EAP-todennusmenetelmä. Autentikaattori kapseloi pyynnön EAPoL-kehykseen ja lähettää sen edelleen asiakkaalle.

Nyt asiakas voi käyttää todennuspalvelimen pyytämää EAP-todennusmenetelmää tai antaa Negative Acknowledgement vastauksen ja valita EAP-menetelmän, jolla haluaa tunnistuksen suorittaa.

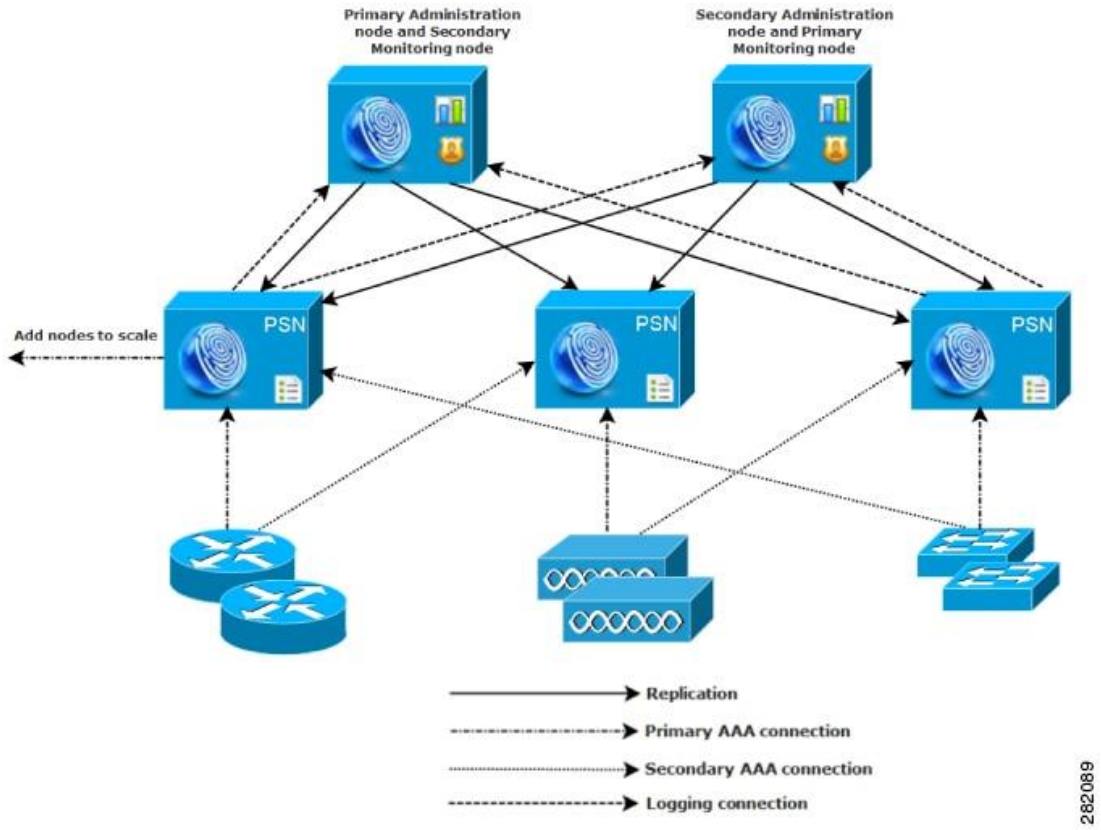
Todennus tapahtuu asiakkaan ja todennuspalvelimen sovittua käytetystä EAP-menetelmästä asiakkaan toimitettua RADIUS todennukseen vaadittavat tiedot valitulla EAP-menetelmällä.

Todennuspalvelin vastaa RADIUS Access Accept-paketin sisältävällä EAP Success-kehyksellä, tai todennuksen epäonnistuessa RADIUS Access Reject-paketin sisältävällä EAP Failure-kehyksellä. Todennuksen onnistuessa asettaa kytkin portin sallittu tilaan, jossa kaikki normaali verkkoliikenne sallitaan. Portti pysyy sallittu tilassa EAPoL-Logoff-kehyksen vastaanottamiseen asti. [25.]

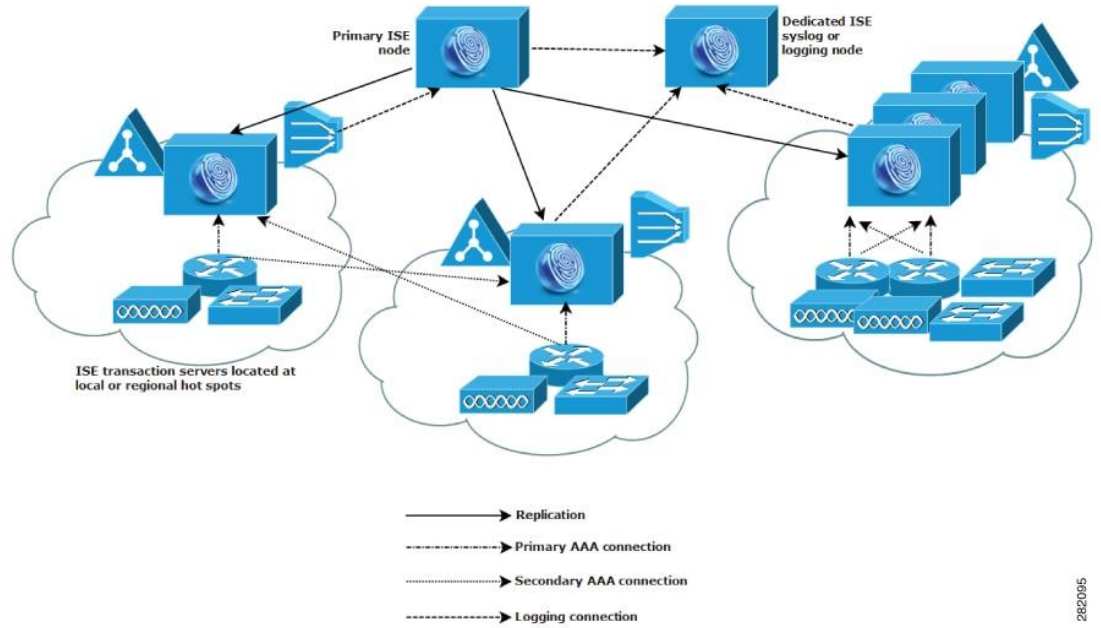
Vastaavasti jos EAPoL viestiä ei portille lähetetä, siirtyy portti määritellyn aikamääreen jälkeen yrittämään kuvan 12 MAB mukaista toteutusta.

4.3 Cisco ISE

ISE on Ciscon NAC-ratkaisu. Rakenteellisesti ISE on suunniteltu joko keskitetyksi tai hajautetuksi ratkaisuksi, koska todennus sekä valtaosa ominaisuuksista voidaan prosessoida yhdessä ISE:n laitenoodissa tai useammassa laitenoodissa antaen niille omat määritetyt roolitehtävät. [26.]



Kuva 14. Laajennettavan keskikokoisen ISE toteutuksen havainnekuva [27.]



Kuva 15. Hajautettu ISE havainnekuva [28.]

Noodien roolit ovat ISE:ssä kokonaisuuksia, joiden avulla määritellään ISE:ssä noodilaitteiden prosessointitehtävät.

4.3.1 Primary Admin node (PAN)

Admin-noodit sisältävät kaikki admin-komennot ja ne konfiguroivat järjestelmään liittyviä kokonaisuuksia, johon kuuluvat esimerkiksi AAA-asetukset. Admin-noodeja voi olla korkeintaan kaksi yhdessä ISE-järjestelmässä eli primary ja secondary noodit. [29.]

4.3.2 Policy Service node (PSN)

Policy Service -noodit hallitsevat ja prosessoivat yritys- ja vieraskäyttäjien verkkopääsyä, tietoturva-asemaa, laitteen provisioita ja profilointia. Tässä roolissa noodi myös arvioi säännöt ja tekee kaikki päätökset niiden toteuttamisesta. Policy Service -noodeja voi olla useampi yhdessä ISE-järjestelmässä. [30.]

4.3.3 Monitoring node (MnT)

Monitoroivat noodit keräävät lokitietoa policy- ja admin-noodeista ja muodostavat niistä saadun tiedon perusteella raportteja. Monitoroivia noodeja voi olla korkeintaan kaksi yhdessä ISE-järjestelmässä primary ja secondary rooleissa. [31.]

4.3.4 Profilointi

ISE pystyy profiloimaan ja luokittelemaan laitteita automaattisesti, kun ne kytketään verkkoon. Laitteiden yhdistäessä verkkoon ISE kerää ominaisuuksista tietoa ja päättelee itse tai käyttäjän ohjeiden mukaisesti laitteen tyypin. Ominaisuus toimii käytännössä missä tahansa IP-verkolla toimivassa laitteessa. Se kattaa esimerkiksi tulostimet, tietokoneet ja IoT-laitteet. [32.]

Profilointia käytetään HUS toimipisteiden käyttöönottoa edeltäessä kartoittamaan toimipisteen laitekantaa. Näin saadaan kartoitettua ja ennakoivasti luotua

profiilittomille laitteille profiilit. HUS laitekannan ollessa heterogeenisesti huomattavan laaja. Tästä lisää osiossa 9.

4.3.5 pxGrid Node

PxGrid on REST-yhteyksiä ja PKI-rakennetta käyttävä järjestelmä, joka mahdollistaa ulkopuolisten tietoturvalaitteiden toiminnan ISE-verkoston sisällä ja hallitsee miten laitteet kommunikoivat, löytävät ja todentavat toisiaan.

PxGrid:ssä esimerkiksi kolmannen osapuolen tietoturvapalvelu pystyisi julkaisemaan tietoa verkkohaavoittuvuudesta muille verkon tietoturvalaitteille ja raportointijärjestelmät voisivat julkaista ja ladata toisiltaan tietoa luodakseen kattavampia raportteja.

PxGrid on ISE:ssä vaihtoehtoinen noodi, joka mahdollistaa pxGrid-palveluja, mutta sitä ei tarvita käyttäjien autentikointiin. [33.]

5 Active Directory

Active Directory (aktiivinen hakemisto) on Microsoftin kehittämä palvelinohjelmisto, joka toimii organisaation käyttäjien ja laitteiden hallintajärjestelmänä. Active Directoryn avulla voidaan hallita käyttäjätilejä, tietoturvaryhmiä, salasanoja, käyttöoikeuksia ja muita verkkoresursseja. [34.]

Active Directory on huomattavassa roolissa tunnistautumisprosessissa Certificate Services (AD CS).

5.1 Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) on palvelu, joka mahdollistaa digitaalisten sertifikaattien hallinnan ja jakamisen organisaation sisällä. AD CS on osa Windows Server -käyttöjärjestelmää ja sitä voidaan käyttää esimerkiksi verkon turvaamiseen, käyttäjien tunnistamiseen ja salauksen hallintaan.

AD CS:n avulla organisaatio pystyy luomaan, jakamaan ja hallitsemaan digitaalisia sertifikaatteja eri käyttötarkoituksiin, kuten HTTPS-sivustojen salaukseen, sähköpostiviestien allekirjoittamiseen ja salaamiseen sekä verkon suojaamiseen erilaisilta uhilta. Sertifikaatit voidaan myös automatisoida ja hallita keskitetysti, mikä helpottaa niiden käyttöä ja ylläpitoa organisaatiossa.

AD CS tukee erilaisia sertifikaattien varmentamisen ja luomisen standardeja, kuten X.509 ja PKCS. Palvelu sisältää myös Certificate Authority (CA) -roolin, joka vastaa sertifikaattien myöntämisestä ja hallinnasta organisaatiossa. [35.]

6 HUS POC konsepti

POC toteutus koskee HUSnet-verkkoon liitettäviä laitteita lankaverkossa. Langaton HUSnet-verkko on käyttöönotettu jo 802.1X määritelmien mukaisesti.

Konseptissa keskitytään tarkastelemaan toteutuksen yksinkertaistettua havainnollistamista, askeleita ja sen jalkauttamista. Sekä keskeisimpiä hidasteita ja haasteita omassa osiossaan. Konseptin tavoitteena on toteuttaa täydellinen porttikohtainen autentikointi POC kohteeseen. Toteutuksen yhteydessä saavutetaan verkon näkyvyyden osalta huomattava parannus nykyisiin ratkaisuihin verrattuna. Verkon näkyvyyden parantaminen lukeutuukin konseptin toiseksi kantavaksi tavoitteeksi tietoturvallisuuden parantamisen kanssa.

Porttikohtainen todennus toteutetaan tuotannossa olevalla Ciscon ISE NAC alustalla. Ciscon ISE lisensointi joudutaan kuitenkin päivittämään perustasoltaan advanced-tasolle porttikohtaisen todennuksen aktivoimiseksi. Cisco ISE käsiteltynä tarkemmin kohdassa 4.3.

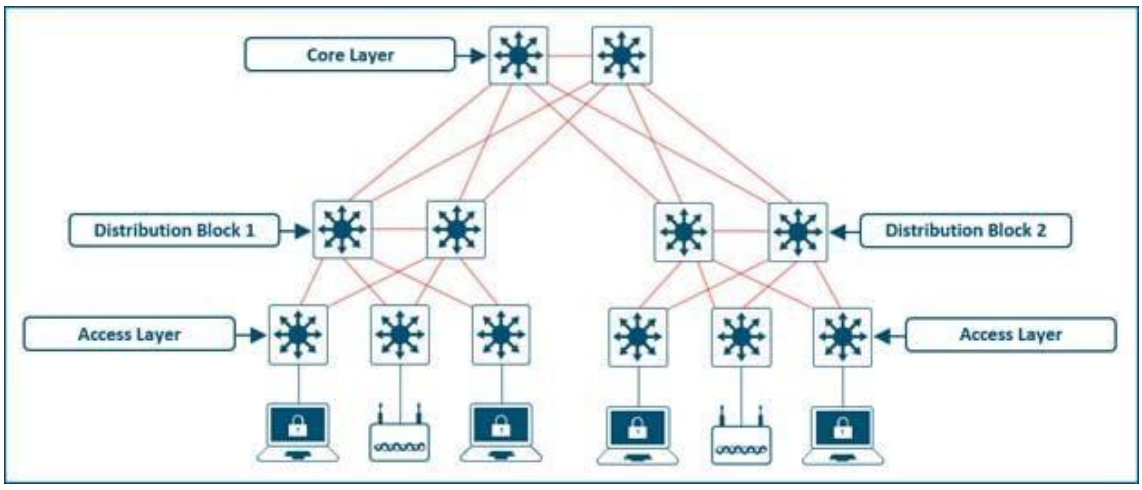
POC valmistuttua konsepti monistetaan muihin HUS toimipisteisiin omina pienoisprojekteinaan kattaen ajallaan kokonaisuudessaan kaikki HUSnet verkotetut toimipisteet.

6.1 POC kohde

POC toteutetaan Gradus-talossa, Tietohallinnon toimitiloissa, Meilahden kampussairaalan läheisyydessä. Siellä tunnistetaan ja luokitellaan paikallinen laitekanta ja niistä esille tulevat haasteet.

Kohteen valinnan kantavana voimana oli kohteen suppeampi erilaisten laitteiden määrä, laitekantojen ollessa volyymiltään kuitenkin HUSnet skaalassa suuria. Testaamisen osalta asiantuntijoiden ja sidosryhmien välitön läsnäolo POC kohteessa, sekä testilaitetilat, jotka mahdollistavat moninaisen ja samalla tehokkaan tavan testata erinäisiä laitteita ennen kriittisempiä sairaanhoidollisia toimipisteitä on huomattava etu.

6.2 Verkko ja topologia



Kuva 16. Havainnollistava yksinkertaistettu kolmitasoinen verkkotopologia [36.]

HUSnet-verkko on toteutettu yksinkertaistetun havainnekuvan 3 mukaisesti tähti mallilla konesalikytkimien (core) ympärille. Jokainen reunakytkin (Access) on yhteydeltään kahdennettu talokytkimelle (Distribution). Talokytkimet on kahdennettu vastaavasti konesalikytkimille. Havainnekuvan 3 kohteessa on kahdennettu talokytkin, kahdennus reunakytkimille tapahtuu jalkojen levittämisellä erillisille talokytkimille.

POC kohteesta voidaan käyttää esimerkkinä kuvan 15, Block 1 topologiaa. Topologian reunakytkimeen on liitetty kaksi kappaletta testikytkimiä:

- Cisco C9200L-48P-4X
- Aruba 6300M 24G CL4 PoE 4SFP56

HUSnet on toteutettu monitoimittajaverkkona, käsittäen Aruban, Ciscon, HP:n ja HPE:n kytkimiä ja reitittimiä. Näistä hidasteiden ja haasteiden muodossa pohdintaa paremmin kohdassa 7.9.

Testausvaiheen alkaessa testikytkimien kanssa luodaan referenssikonfiguraatiot perustasoisesti porttikohtaisen todennuksen toteuttamiseksi. Seuraavaksi aloitetaan testaus yleisimmillä päätelaitteilla, tässä tapauksessa perustyöasemilla ja tulostimilla. Laiteprofiileille luodaan säännöt käyttäen pohjana tuotannossa olevan langattoman verkon sääntöjä.

6.3 Monitorointi ja luokittelu

Tunnistaminen ja luokittelu saavutetaan monitoroimalla kohdetta ja profiloimalla Ciscon ISE:llä kohde kokonaisuutena laitekantansa osalta noin kahden viikon tarkkailulla. Tunnistettu laitekanta jakautuukin alkuun tunnistettuihin ja tunnistamattomiin laitetyyppeihin.

Tunnistettujen laitteiden kohdalla luodaan näille profiilit ja roolit valmiiksi. Tunnistamattomien laitteiden kohdalla aloitetaan tarkempi haasteiden ratkonta laitetyypeittäin. Laitetyyppien haasteista paremmin kohdassa 7.1.

6.4 Kohteen kokonaisvaltainen tunnistus

Haasteiden ratkettua tunnistuksen alustavien tapausten suhteen, kytketään porttikohtainen tunnistus päälle hallitusti ja aloitetaan uusien esille tulleiden haasteiden selvitys.

Hallitun päälle kytkennän osalta käydään vielä pohdintaa, aktivoidaanko tunnistus laajuudeltaan kerralla:

- kohdetasolla
- kerrostasolla
- jakamotasolla
- kytkintasolla
- porttikohtaisesti

Todennäköisimmin kohteen laajuinen tunnistuksen jalkauttaminen toteutetaan jakamo- ja kerroskohtaisesti, tai näiden tapauskohtaisella yhdistelmällä. Kohteen kattavan tunnistuksen päälle kytkemisen haasteista paremmin kohdassa 7.10.

6.5 POC yhteydessä luotavat ohjeistukset

POC vaiheiden matkassa opituilla testaus- ja dokumentointitiedoilla luodaan pohja ohjeistuksille. Ohjeistukset luodaan tahtotilallisesti alustavasti ainakin seuraavin aiheittain:

- ISE virhelokien tulkinta ja ongelmien ratkaisumallit
- Poikkeuskäytännöt tunnistautumispalvelun virhetilan tai kaatumisen aikana
- Porttitunnistus epäonnistuu päätelaitteella
- Vastuuyksiköiden ohjeistus
- Lähituen ohjeistus

- Henkilöstön ohjeistus
- Ulkopuolisen henkilöstön ohjeistus
- Tuotepäälliköiden ohjeistus uusien laitemallien dokumentointiin
- Laitevalmistajien ohjeistus uusien laitteiden osalta
- Laitemallikohtaiset ohjeet

Alustavien tiedostettujen ohjeistusten lisäksi projektin edetessä tulee varmasti uusia, vielä tunnistamattomia ohjeistuksen kohteita, nykyisten aiheiden kattaessa kuitenkin suhteellisen kattavasti oletetun tahtotilan.

7 Haasteet ja hidasteet

Haasteet ja hidasteet kattavat nykyisen 802.1X-projektin konseptivaiheen suurimman osuuden pohdinnallisella moninaisuudellaan. Haasteet ja hidasteet sisältävät todennettuja tiedossa olevia sekä teoreettisia mahdollisia tapauksia pohdittavaksi.

7.1 Laitekannan laajuus

Suurimpana hidasteena konseptin toteuttamiseksi on HUSnet-verkkoon liitetyn laitekannan huomattava laajuus, laitekannan kattaen toista tuhatta erilaista päätelaitetta. Vaikka POC ympäristö ei kata HUSnet koko laitekantaa, on laitekanta POC ympäristössä silti huomattavasi normaalia yritystoimintaympäristöä heterogeenisempi. Haasteelliseksi tämän tekee huomattava määrä laitetoimittajia, joille ei ole voimassa olevaa tukisopimusta, tai valmistajaa ei välttämättä enää ole olemassa. Tämä korostuu erityisesti POC vaiheen päätyttyä siirryttäessä tuotantokohteisiin.

7.2 Testaus

Laitekannan testaaminen ja dokumentointi on hidas ja huomattavasti aikaa vievä POC vaiheen osuus, vaatien laitevalmistajan edustajien asiantuntemusta laitemallikohtaisen porttitunnistuksen toimintaan saamisesta.

Suurimpana haasteena ovat laitevalmistajat, joita ei enää ole olemassa tai laitteita hallitsevia asiantuntijoita ja dokumentaatiota on niukasti, jos ollenkaan.

Laajempaa kokonaisuutta miettiessä vastaava ongelma on laitteissa, joita on olemassa kourallinen. Jokainen niistä on mahdollisesti vielä mukautettu yksilöllisesti asiakkaan tarpeisiin. Pahimmassa tapauksessa laite on uniikki koko maailmassa. Tämä korostuu erityisesti lääkintälaitteiden osalta.

7.3 Dokumentointi

Laitekannan dokumentointi asianmukaisesti ja eheästi loogiseen muotoon on tahtotila, josta ei olla taipumassa. Ongelmaksi tuleekin saadun dokumentoinnin yhtenevä muoto ja taso laitevalmistajien osalta haluttujen tietueiden täyttämisen suhteen.

Työn alla on luoda universaali pohja tietokantaan vietäväksi, mistä selviää:

- valmistaja
- laitteen malli
- laitteen revisio
- ohjelmistoversio
- valmistajan MAC-osoiteavaruus
- tuetut todennusmenetelmät

- laitekohtaiset erityispiirteet todennuksessa
- porttikohtaisen todennuksen ongelmavariaatiot ja niiden ratkaisut
- dokumentin täyttäneen yrityksen tai sen edustajan tiedot
- päivämäärä
- Tietohallinnon asiantuntijan tai tuotepäällikön hyväksyntä

7.4 Tulostimet

Tulostimien saaminen porttitunnistuksen osalta yhteensopiviksi vaatii laitevalmistajan tai valmistajan asiantuntijoita todennuksen käyttöönotossa ja kohdattujen ongelmien ratkaisemisessa.

7.4.1 Valmistaja A

Toteutus on verkkohallinnan kautta mallisen asetuspaketin takia helppo toteuttaa. Uudemmissa ja ominaisuuksiltaan kattavammissa laitteissa on tuki 802.1X autentikoinneille. MAB-todennus asetetaan laitteille, jotka eivät ohjelmistoiltaan tue kattavampia tunnistustapoja.

7.4.2 Valmistaja B

Laitekannalla on olemassa verkon etähallinta, jota ei ole kytkettynä kaikille tulostimille vakiona käyttöön. Etähallintatoteutus on rajoittunut ja vaatii fyysistä läsnä tapahtuvaa todennuksen asettamista tulostimille. Laitekanta tukee pääosiltaan EAP-TLS-protokollaa. Lopuissa käytetään PEAP-MSCHAPv2-protokollaa. Valmistajan tuki ja konsultointi ovat välttämättömiä nykytiedon puitteissa.

7.4.3 Valmistaja Muut

Lopuissa tulostimissa on käytettävä oletuksena MAB autentikointia, ellei laitevalmistaja tuo ilmi tiedusteltujen laitemallien 802.1X tukea.

7.5 Lääkintälaitteet

POC ympäristössä on testattavana, korjattavana ja demokäytössä aktiivisesti vaihtuva määrä erilaisia lääkintälaitteita, joita käytetään muissa HUSin kohteissa aktiivisesti. Lääkintälaitteet kattavat huomattavan osan HUSnetin laitekannan monimuotoisuudesta.

POC konseptin toteutuksen osalta lääkintälaitteet kuitenkin sivuutetaan, mutta laitekantaa testataan ja dokumentoidaan aktiivisesti taustalla konseptin siirtyessä toteutukseen muissa toimipisteissä tulevaisuudessa.

7.6 Älyttömät sensorit

Talotekniikka ja turvatekniikka omaa oman haasteensa vaatien laitetoimittajien ja valmistajien asiantuntijoita konsultoitavaksi. Todennus toteutetaan laitekannalle MAB autentikointia käyttäen, ellei laitevalmistaja toisin tuo ilmi 802.1X tukea.

7.7 Oikean verkon valinta usean roolin käyttäjälle

Haaste on tapauskohtainen ja tulee aiheuttamaan joillekin käyttäjille huomattavan määrän ongelmatilanteita ja odottamista ongelman korjaamiseksi.

Otetaan esimerkiksi käyttäjä, jolla on useampi rooli. Jokaisella roolilla on sallittuna erilaisin oikeuksin eri verkkojen resursseja.

Laitteen profiililla on oikeus useaan erilliseen virtuaaliverkkoon, mutta laite sijoitetaan lähtökohtaisesti virtuaaliverkkoon A.

Laitteen liitettäessä verkkoon laite siirtyy automaattisesti virtuaaliverkkoon A, mutta sijainnissa onkin käytettäviltä laitteiltaan virtuaaliverkossa B toimiva laiteympäristö, jotka eivät keskustele virtuaaliverkon A kanssa teknisen toteutuksensa tai laitevalmistajan määritysten takia. Käyttäjän profiililla virtuaaliverkko A on sallittuna ja järjestelmä ei haasta laitteen saamaa virtuaaliverkkoa.

Käyttäjä ei pääse käyttämään laitteella sijainnissaan tarvitsemiaan verkon resursseja ja joutuu odottamaan laitteen asettamista oikeaan verkkoon.

7.8 MAC-osoite pohjainen todentaminen

MAC-osoitteellisen todentamisen hidasteena tulee olemaan laitekannan perkaaminen oikeisiin verkkoihinsa.

Joissain yksittäisissä laitteissa on voitu verkkokortti vaihtaa toisen valmistajan tuotteeseen ja näin tunnistautuen mahdollisesti väärän verkon laitteeksi. Tämä koskeekin erityisesti itse hengissä pidettyjä tai luovempien sairaalainsinöörien verkkoon luomia ratkaisuja lääkintälaitteiden suhteen, joissa ei alkujaan ole ollut verkko-ominaisuuksia. Tällaisia olen kohdannut henkilökohtaisesti työurallani lähituessa.

Haasteena on myös MAC-osoitteiden väärentämisen helppous esimerkiksi kopioimalla vihamieliselle päätelaitteelle porttiin liitetyn laitteen MAC-osoite ja kytkemällä väärennetyn MAC-osoitteen vihamielinen päätelaite alkuperäisen tilalle.

7.9 Kytkimet

Kytkimien suhteen ensimmäisenä haasteena on tunnistaa kytkimet, jotka eivät tue mallinsa tai ohjelmistonsa puitteissa porttikohtaista tunnistusta. Kytkinmallien määrän ollessa huomattava ja näissä eriävien ohjelmistojen osalta vielä laajempi moninaisuus, on variaatioiden selvitystyö laajuudeltaan huomattava.

Hidasteena porttikohtaista tunnistusta tukemattomien laitemallien tunnistamisen jälkeen on selvittää porttikohtaisen tunnistuksen omaavien laitekantojen tila. Osaavatko nämä oikeellisen formaatin porttikohtaisen tunnistautumisen suhteen päätelaitteiden ja Ciscon ISE:n kanssa? Jos formaatti on virheellinen, onko mahdollista muuttaa sitä oikeaan formaatin ohjelmistopäivityksellä tai kytkimen asetuksista.

Kytkimet, jotka eivät tue porttikohtaista todennusta tai kykene oikeassa formaatissa viestimään porttikohtaisen todennuksen osalta, ovat lähtökohtaisesti jo elinkaarensa osalta odottamassa uusimista modernimpiin laitemalleihin.

7.10 Kytkennän laajuus

Kohteen tunnistuksen kytkennän osalta on arvioitavana, segmentoidaanko kohde vai kytketäänkö tunnistus kerralla koko kohteeseen.

Esimerkillisesti haasteena koko kohteen kerralla kytkiessä on esille nousevien ongelmien mahdollisen ruuhkautuminen ja käyttäjien päätelaitteiden verkon toimimattomuuden pitkittyminen ongelmien ratkonnan osalta. Vastaavasti kohteen porttitunnistus on heti täydellisesti kattava.

Vaihtoehtoisesti ääripäässä hidasteena jokainen portti aktivoidaan yksitellen ja käyttäjämäärät ongelmatilanteiden suhteen ovat minimaalisia, mutta kohteen täydellisen tunnistuksen saavuttaminen kestää huomattavan kauan jättäen verkon pidemmäksi ajaksi suojaamatta.

Vaikka POC kohteessa ei potilasturvallisuutta vaarannettaisikaan, niin tämä näkökulma on kuitenkin kantava lähestymismalli harkittaessa tunnistuksen käyttöönoton laajuutta siirryttäessä potilastyöskentelyä suorittaviin kohteisiin. Osassa kohteissa joudutaan joidenkin osastojen osalta etenemään porttikohtaisesti. Tästä esimerkkinä teho-osastot, leikkausosastot ja HUSLABin laboratoriot.

7.11 Karanteeniin joutuneet tuotannon laitteet

Haasteena ovat myös tuotannon laitteet, jotka syystä tai toisesta tunnistautuvat väärin ja joutuvat karanteeniin, joidenkin laitteiden kohdalla tämän toistuessa ja aiheuttaessa karanteenikierteen. Olipa syy itse päätelaitteessa, kytkimen virheellisessä todennusformaatissa tai jostain muusta, vielä tuntemattomassa syystä johtuvasta ongelmasta.

7.12 Todennuksen kattavuuden vajaaksi jääminen

Täydellisen porttikohtaisen todennuksen toteuttaminen on haastava prosessi aikaisemmin esille tuomieni haasteiden ja hidasteiden osalta. On mietittävä myös mahdollisuutta, missä täydellisen porttikohtaisen todennuksen toteuttaminen ei ole mahdollista. Vaikka nykyinen todennusmenettely tarjoaakin hyvin kattavan todentamisen erinäisen tekniikoin, on silti varauduttava tilanteeseen, missä jotkin laitteet tai laitekannat eivät sovellu vielä tuntemattomasta syystä todennuksen piiriin aiheuttaen esimerkiksi kohdassa 7.11 esille tuomaani karanteeniin joutumisen kierteen. Näiltä osin laitteiden siirtämisen tunnistuksen osalta poiskytkettyihin portteihin.

Haasteena on tässä skenaariossa porttien turvallisuus vihamielisen tai muutoin verkkoon kuulumattoman laitteen osalta. Täydellisessä maailmassa nämä tunnistamattomat portit olisivat erillisellä kytkimellä, joka on eristetty omaan verkkoonsa ja turvattu muilla tavoin esimerkiksi vahvaan seulontaan ennen pääsyä sisäverkkoon sekä laitteelle ominaiseen tai määriteltyyn käyttäytymismalliin perustuvaan toimintamallin seuraamiseen ja toimintamallin rikkoutuessa verkosta erottamiseen.

Todellisuudessa tämä ei kuitenkaan ole mahdollista, joten tämän toteutuksen osalta joudutaan tutkimaan erilaisia ratkaisumalleja.

7.13 Vastuuyksiköiden vastuut ja kompetenssit

Haasteellisena osuutena on tuotava esille myös vastuuyksiköiden rooli tunnistaa POC projektin mukana esille tulevia vastuualueidensa uusia lisävastuita ja tätä kautta ilmeneviä kompetenssitarpeita. Henkilöstön kouluttaminen uuden kompetenssin suhteen mahdollisimman ajoissa ja kattavasti ennen projektin siirtymistä seuraavan kohteen käyttöönottoon on valitettavan yleinen haaste.

Vastuuyksiköiden uusien lisävastuiden tunnistamisen puute lisää turhaa ajankäyttöä sopivan vastuuyksikön määrittelyn osalta. Varsinkin läpinäkyvämmissä vastuissa, jotka eivät ole yksiselitteisesti vain tämän yksikön vastuulla, vaan ovat läpinäkyvämpiä kokonaisuuksia, kuuluen useammalle yksikölle osuuksittain.

7.14 Jatkuvat palvelun vaikutukset

Tulevan POC toteutuksen käyttöönoton aikana tullaan arvioimaan ja tarkkailemaan, miten muutos vaikuttaa tuotannon jatkuvien palveluiden toimintaan.

Haasteen tai hidasteen sijaan kyseessä on huoli, joka painaa jokaista asiantuntijasta toimitusjohtajaan saakka. Onkin kriittistä tunnistaa mahdolliset vaikutukset erinäisine komplikaatioineen vastuuyksikkökohtaisesti. Haasteena on luoda näistä kattavat ja selkeät skenaariot, riskianalyysit ja valmiussuunnitelmat potilastuvallisuuden varmistamiseksi tilanteessa kuin tilanteessa.

8 Yhteenveto

Yhtenä nykyisen työni edellytyksenä oli saada tehdä työn ohella insinöörityö. Insinööritöiden aiheita oli useampia ennen nykyistä toteutunutta ratkaisua. Joidenkin toteutumattomien aiheiden kohdalla alustustyötä ja materiaalia kirjoitettiin huomattavastikin ennakkoon. Toteutuneen insinöörityön oli alustavasti tarkoitus kattaa POC kohteen projektin käyttöönoton toteutuksen aikaisista toimenpiteistä sisältäen kytkinten porttikohtaisen todennuksen konfiguroinnin,

todennuksen toteutumisen ja kytkimen lokien tarkemman tarkastelun oppimiseen todennuksen osalta. Cisco ISE:n monitorointi ja profilointi datan analysointi selvittäessä virhetilanteita, laitetestausta laitetoimittajien ja muiden asiantuntijoiden kanssa havaittujen ongelmien ratkaisemiseksi, ohjeistusten luomista sekä muita testaamiseen ja jalkauttamiseen kohdistuvia toimenpiteitä.

Insinöörityö oli kuitenkin aikataulullisesti järkevintä toteuttaa heti POC suunnitteluvaiheen alussa toteutuneella tavallaan, vaikka opinto-oikeutta olisikin ollut käytettäväksi kattavamman insinöörityön toteuttamiseksi. Valmistumisen viivyttelylle muiden opintojen ollessa suoritettuna ei ollut järjellistä perustetta.

Insinöörityön aloitus osoittautui kuitenkin haastavammaksi aihealueen oltua laajempi ja tiedon oltua turvaluokitukseltaan ja salassa pidettävyydeltään julkisesti esitettävään insinöörityöhön kelpaamatonta. Tästä syntyi sitten idea esittää POC projektin suunnitelmaa konseptitasolla.

Haasteet insinöörityön toteutuksessa eivät kuitenkaan päättyneet tähän. Konsepti oli kattava ja laaja. HUSnetin laitekanta on myös huomattavan laaja. Aikataulullisesti oli myös jo kiire toteuttaa insinöörityö muutaman viikon aikajänteellä.

Ilman aikaisempaa HUS työhistoriaa lähituessa ja mennyttä 18 kuukautta Tietohallinnon Tietoliikennepalveluiden palveluksessa, olisi insinöörityö jäänyt laajuudeltaan huomattavasti haasteellisemmaksi, ellei jopa mahdottomaksi toteutukseltaan nykyisessä toteutuneessa muodossaan. Insinöörityön päätyttyä jatkan projektissa työryhmän jäsenenä ja POC laitteiden testauksen koordinaattorina.

Insinöörityön teoriaan tutustuessani olin jo AAA-osuuden osalta konseptin tasolla tutulla alueella ja vanhan kertaaminen kävi joutuisasti. 802.1X suhteen astuin otsikkotasoa syvemmälle ensi kerran oikeasti. Active Directory oli aiheena tuttu jo koulun kurssien ja työn kautta. Eniten aikaa kuitenkin kului tutustuessa Ciscon ISE-palveluun ja sen dokumentointiin.

Kiinnostus Ciscon ISE-palvelua kohtaan työn aikana kasvoi huomattavasti ja

POC-projektin matkassa tavoitteena onkin oppia mahdollisimman kattavasti omavaraiseksi osaajaksi.

Suurella kiinnostuksella odotan POC-toteutuksen käyttöönotto vaiheen alkamista, sekä miten pohdintani haasteiden ja hidasteiden osalta heijastuu toteutuksen tulevassa suunnittelussa ja varautumisessa, sekä miten pohdinnoissani esittelemäni teoreettisemmat asiakohdat toteutuvat mahdollisesti ilmetessään toteutuksen edetessä ja miten ne ratkaistaan.

Lähteet

1 Omaisuusjärjestelyt Soteuudistus.fi. Valtioneuvosto. 2023. Verkkoaineisto. <https://web.archive.org/web/20230206023415/https://soteuudistus.fi/omaisuusjarjestelyt> Luettu 10.5.2024.

2 What is Authentication, Authorization, and Accounting (AAA) Security. Verkkoaineisto. <https://www.fortinet.com/resources/cyberglossary/aaa-security> Luettu 10.5.2024.

3 AAA policies. Figure 1. Processing of an AAA policy. Verkkoaineisto. <https://www.ibm.com/docs/en/datapower-gateway/10.5.0?topic=processing-aaa-policies> Päivitetty 1.3.2024. Luettu 10.5.2024.

4 Salasanat haltuun. Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf> Luettu 10.5.2024.

5 Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi> Päivitetty 7.5.2024. Luettu 10.5.2024.

6 Use certificates for authentication in Microsoft Intune. 2023. Verkkoaineisto. <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-configure> 21.8.2023. Luettu 10.5.2024.

7 MAC Authentication Bypass (MAB). Verkkoaineisto. <https://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab> Luettu 10.5.2024.

8 RADIUS Authentication, Authorization, and Accounting. 2020. Verkkoaineisto. <https://learn.microsoft.com/en-us/windows/win32/nps/ias-radius-authentication-and-accounting> 20.08.2020. Luettu 10.5.2024.

9 Wired 802.1X Deployment Guide. 2011. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386716> Päivitetty 6.9.2011. Luettu 10.5.2024.

10 Dominic, Zeni. Cisco ISE: Wired and Wireless 802.1X Network Authentication. Figure 1. Verkkoaineisto. <https://www.lookingpoint.com/blog/ise-series-802.1x> Luettu 10.5.2024.

11 Wired 802.1X Deployment Guide. Figure 1. 2011. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386725> Päivitetty 6.9.2011. Luettu 10.5.2024.

12 Wired 802.1X Deployment Guide. Figure 3. 2011. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386789> Päivitetty 6.9.2011. Luettu 10.5.2024.

13 802.1X Overview and EAP Types. Verkkoaineisto. 2023. <https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim> 19.6.2023 Luettu 10.5.2024.

14 The EAP-TLS Authentication Protocol. Verkkoaineisto. 2008. <https://datatracker.ietf.org/doc/html/rfc5216> Luettu 10.5.2024.

15 Wired 802.1X Deployment Guide. Figure 5. 2011. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386979> Päivitetty 6.9.2011. Luettu 10.5.2024.

16 Protected Extensible Authentication Protocol (PEAP). Verkkoaineisto. 2024 <https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-PEAP/%5bMS-PEAP%5d.pdf> 23.4.2024 Luettu 10.5.2024.

17 Microsoft PPP CHAP Extensions, Version 2. Verkkoaineisto. 2000 <https://www.ietf.org/rfc/rfc2759.txt> Luettu 10.5.2024.

18 Wired 802.1X Deployment Guide. Figure 6. 2011. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp387037> Päivitetty 6.9.2011. Luettu 10.5.2024.

19 Extensible Authentication Protocol (EAP). Link Layer. Verkkoaineisto. 2004 <https://datatracker.ietf.org/doc/html/rfc3748#section-7.12> Luettu 10.5.2024.

20 MAC authentication bypass (MAB). Verkkoaineisto. <https://docs.fortinet.com/document/fortiswitch/7.4.3/fortiswitchos-administration-guide/110307/mac-authentication-bypass-mab> Luettu 10.5.2024.

21 802.1X Authentication Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches). Figure 1. Verkkoaineisto. 2013. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html#GUID-C4AE2303-3ACC-482E-BDD1-73A61E6E4752> 29.1.2013 Luettu 10.5.2024.

22 Catalyst 6500 Release 12.2SX Software Configuration Guide. Figure 60–3. Verkkoaineisto. 2016. <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#68228> 7.7.2016. Luettu 10.5.2024.

23 Catalyst 6500 Release 12.2SX Software Configuration Guide. Figure 60–4. Verkkoaineisto. 2016. <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#706018> 7.7.2016. Luettu 10.5.2024.

24 Catalyst 6500 Release 12.2SX Software Configuration Guide. Figure 60–2. Verkkoaineisto. 2016. <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#67130> 7.7.2016. Luettu 10.5.2024.

25 Catalyst 6500 Release 12.2SX Software Configuration Guide. Verkkoaineisto. 2016. <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#35201> 7.7.2016. Luettu 10.5.2024.

26 Overview of Cisco ISE. Verkkoaineisto. <https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.pdf> Luettu 10.5.2024.

27 Cisco Identity Services Engine Installation Guide, Release 3.3. Figure 3. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#node-types-and-personas-in-distributed-deployments> 5.3.2024. Luettu 10.5.2024.

28 Cisco Identity Services Engine Installation Guide, Release 3.3. Figure 5. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#node-types-and-personas-in-distributed-deployments> 5.3.2024. Luettu 10.5.2024.

29 Cisco Identity Services Engine Installation Guide, Release 3.3. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#administration-node-cisco-ise> 5.3.2024. Luettu 10.5.2024.

30 Cisco Identity Services Engine Installation Guide, Release 3.3. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#policy-service-node-cisco-ise> 5.3.2024. Luettu 10.5.2024.

31 Cisco Identity Services Engine Installation Guide, Release 3.3. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#monitor-node-cisco-ise> 5.3.2024. Luettu 10.5.2024.

32 Craig, Hyps. ISE Profiling Design Guide. Verkkoaineisto. 2018 <https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456> Päivitetty 3.11.2023. Luettu 10.5.2024.

33 Cisco Identity Services Engine Installation Guide, Release 3.3. Verkkoaineisto. 2024. <https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/install_guide/b_ise_installationGuide33/b_ise_InstallationGuide33_chapter_1.html#pxgrid-node-cisco-ise> 5.3.2024. Luettu 10.5.2024.

34 Active Directory Domain Services Overview. Verkkoaineisto. 2022. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> 17.8.2022. Luettu 10.5.2024.

35 What is Active Directory Certificate Services? Verkkoaineisto. 2023. <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview> 21.3.2023. Luettu 10.5.2024.

36 Cisco SD-Access Solution Design Guide (CVD) Figure 16. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Layer3RoutedAccessandSDAccessNetworkDesign> Luettu 10.5.2024.