Expertise
and insight
for the future

Topias Kumpulainen

Network Access Control

Metropolia University of Applied Sciences

Bachelor of Engineering

Information technology

Bachelor's Thesis

4 September 2020

Author	Topias Kumpulainen
Title	Network Access Control
Number of Pages	31 pages
Date	4 September 2020
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	IoT and Cloud Computing
Instructors	Marko Uusitalo, Senior Lecturer

The goal of this thesis was to study Network Access Control and its importance in the modern world and how Network Access Control can be implemented using many different protocols, platforms and other means. The study also deals with IEEE standards of which a few are popular Network Access Control choices, and some are just useful major standards. The second goal of the thesis was to produce a simple guide for the initial configuration of the Cisco Identity Services Engine and some basic configuration of the policies used for Network Access Control.

This study was commissioned by a local Finnish company and partly made for them, which is the major reason the subject was chosen. The thesis is based on online material for the most part. For example, Cisco documentation offers a considerable amount of information. As part of the project, hands on learning with Cisco Identity Services Engine 2.6 was used.

Based on the study of Network Access Control, it can be concluded that there is no right or wrong here. Every type of Network Access Control protocol or platform serves a purpose and has its own use somewhere in the world. This depends on the size of the company, devices and many other factors. Based on the study, a small guide was compiled for the basic configuration of the Cisco Identity Services Engine and how the policy management system works in the platform.

Keywords	Cisco, ISE, IBNS, IEEE, 802.1X, NAC, MAB, TrustSec

Tekijä Otsikko Sivumäärä Aika	Topias Kumpulainen Network Access Control 31 sivua 4.9.2020
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	IoT and Cloud Computing
Ohjaajat	Lehtori Marko Uusitalo

Insinöörityön tavoitteena oli oppia lisää verkon pääsynhallinnasta sekä sen tärkeydestä modernissa maailmassa. Tavoite oli myös oppia, miten pääsynhallintaa voi luoda käyttämällä monia eri protokollia tai alustoja. Työssä myös tutkittiin IEEE-standardeja, joista muutamat ovat suosittuja vaihtoehtoja toteuttaa verkon pääsynhallintaa. Osa sandardeista on taas käytettyjä ja suosittuja yleisellä tasolla. Insinöörityön toinen tavoite oli luoda yksinkertainen asennusohje Ciscon tuottamalle Identity Services Engine -alustalle, sekä tuottaa sen avulla konfiguraatioohjeet, joiden avulla luodaan perustason verkon pääsynhallintaa.

Tämä insinöörityö on tehty yhteistyössä paikallisen suomalaisen yrityksen kanssa. Tämä oli yksi pääsyistä aiheen valintaan. Suurin osa materiaalista on verkkomateriaalia, joka pääasiassa keskittyy Ciscon itse tuottamaan dokumentaatioon sekä heidän webinaareihin. Osana työtä käytettiin Ciscon Identity Services Engine 2.6 -versiota. Tämän avulla saatiin hyvää materiaalia itse alustasta.

Työn lopputuloksena on se, että verkon pääsynhallintaan ei ole oikeita ratkaisuja. Eri protokollilla ja alustoilla on omat tarkoituksena, ne palvelevat eri tarkoituksia eri ympäristöissä. Suurimmat tekijät tällaisissä tilanteissa ovat yrityksen koko ja laitteisto, joita yritys käyttää. Työn lopputuloksena saatiin tuotettua ohjeet, miten konfiguroidaan Ciscon Identity Services Engine perustasolla sekä miten kyseisen alustan policy management toimii.

Avainsanat	Cisco, ISE, IBNS, IEEE, 802.1X, NAC, MAB, TrustSec

Contents

List of Abbreviations

IEEE	Institute of Electrical and Electronics Engineers
TAG	Technical Advisory Group
ISE	Identity Services Engine
IBNS	Identity-based Networking Services
VLAN	Virtual Local Area Network
OTP	One Time Password
MAC	Media Access Control
USB	Universal Serial Bus
BYOD	Bring your own device
NAC	Network Access Control
AIEE	American Institute of Electrical Engineers
PoE	Power Over Ethernet
ACL	Access Control List
ARP	Address Resolution Protocol

1 Introduction

The thesis deals with Network Access Control (NAC) and network security. The goal of this thesis is to research and learn more about different NAC Implementations and their importance in the modern world. As the world is becoming more connected and digitalized, the importance of securing a network from unwanted users is now more important than ever before. The easiest way to cause data leaks is giving a hacker an easy access to the network. That is why cyber security and network access control need to improve with time. This thesis was commissioned by a local Finnish company.

The thesis studies the possibilities, advantages and disadvantages of different methods for authentication of users, devices or anything in between / for authenticating users, devices or anything in between. The thesis covers some basic IEEE 802 standards and their usage in modern technology and how they affect NAC. Other than authentication methods, the thesis covers the Cisco Identity Services Engine (ISE) platform and Cisco IBNS tools, as they are great tools for easily making a company's network more secure. In addition, this thesis also deals with basic configuration and the setup of the Cisco ISE server, going into more detail about how the authentication and authorization policy works in the environment.

2 What Is Network Access Control?

A central question is what Network Access Control (NAC) is. To put it simply, it is controlling users who have access to a certain network and determining to which parts of the network they can have access. The most simple example of this would most likely be any home network. Wi-Fi access with a password for it is a good example. This is a simple way to control the users who have access to the network. Other places where network access control could be implemented is school or workplace Wi-Fi, for example.

When it comes to organizations or companies, simply having a password for network access is not enough as a company has most likely more to lose and simply cannot afford to lose its data, or have it leak. Therefore, extra steps are needed for securing the network. NAC has many different goals. Authorization, authentication and accounting of networks is one of the key goals. Other goals include encrypting the traffic, mitigation of zero-day attacks, and enforcing policies to the users. Guest networking access is also one of the most important features [1]. When a company has a guest over, an administrator needs to make sure the guest only gains access to specified parts of the network so that the guest simply cannot steal any important company data. The administrator should also make sure it is the guest user using the network and not a random person near the office. The job of NAC is simply to limit the network access of devices in the network and make sure only trusted users are accepted to the network. For example, someone from the HR or Accounting department may not need full access to the network or network files. This also helps in the case of a security breach done using phishing or social engineering.

Multiple companies have produced their own platform for managing network access control. Cisco has Identity Services Engine (ISE), Aruba has ClearPass and Fortinet has FortiNAC. All of these differ from each other but serve the same purpose. They provide easier management of the network with the usage of policies and Radius-server features. All of these have their advantages and disadvantages and should be researched thoroughly before starting to implement them to a company’s network.

2.1 Certificate Based Authentication

When it comes to wireless networks, network access control configurations are somewhat different from what they normally are like as no switch configuration is needed and Access points are used as authenticators. A clever way to overcome this issue is to use certificate-based authentication. This can be reached by using, for example, Cisco Meraki which allows easy deployment of certificate-based (EAP-TLS) Authentication to iOS, OS X, Android and Windows 10 clients.

Digital Certificates are a part of electronic credentials binding the identity of the owner to a pair of encryption keys. These keys are called Public and Private keys, which can be used to encrypt and sign information digitally. This maintains integrity of the certificate.

2.2 One Time Password

Like the name suggests, One Time Password is a password that can only be used once. Mostly OTPs are used when signing into servers or network devices for administrator work. However, it is indeed possible to configure a radius server so that the Wi-Fi password is used as an OTP. It is probably not the best way to secure a network. Usually OTPs are used on top of an existing username and password combination [2].

For example, an administrator is using Remote desktop connection to log into a Windows server and it first asks for the administrator's username and password. After this it asks the user to enter an OTP. The OTP can be given to the user via an SMS, generated by a physical token or an authenticator software in a smartphone. After entering the OTP, the administrator is granted access to the server. Depending on how it is implemented, it is also possible to use a pin and an OTP as the OTP. This means that first the administrator enters in a 3-4 digit pin and then enters the OTP. This is slightly more secure and more personalized. If someone gains access to someone else's phone or OTP token generator, the purpose of the OTP is negated. The pin brings more security by bringing in a fourth factor on top of the existing ones (username, password, and OTP). Image below illustrates a generic OTP token generator.

Figure 1. OTP token generator. Copied from [3].

OTP token generator [3]

Notable OTPs that are used are SMSs, physical tokens, Google Authenticator tokens and USB tokens [2]. USB tokens are notably the most different from the other options. The user needs to simply just plug in a USB drive to a USB port.

3 IEEE 802

IEEE 802 is a group of standards for local area and metropolitan area networks developed by the Institute of Electrical and Electronics Engineers. Its roots go back to 1884 New York, the USA, where a group of electrical professionals met. They formed an organization to support the professionals in the field. The name of the organization was American Institute of Electrical Engineers (AIEE). [3.] They focused on electrical power and it its ability to change people's lives. Through their meetings and publications, they led the growth of electrical engineering as professions. In late 1890, a new industry rose which was known as wireless telegraphy, in other words the radio industry. In 1912 a new organization was born, The Institute of Radio Engineers. Both organizations led the development of new innovations and industry and on January 1st, 1963 they merged and since then they have been known as the Institute of Electrical and Electronic Engineers (IEEE). [4.]

In February 2020, there were seven different IEEE standards that were in active development [4]. IEEE also has 16 different standards the development of which has ended or the development of which is on a pause. The seven standards which are in active development are show in the image below.

802.1	Higher Layer LAN Protocols
802.3	Ethernet
802.11	Wireless LAN
802.15	Wireless Personal Area Network (WPAN)
802.18	Radio Regulatory TAG
802.19	Wireless Coexistence
802.24	Vertical Applications TAG

Figure 2. IEEE 802 Standards in active development. Based on [5].

However, even if the development is on a pause or has ended, it does not necessarily mean that the standard is not in use. For example, one of the biggest standards in use is 802.15.1 which is commonly known as Bluetooth. IEEE 802.15.1 is based on Bluetooth 1.1 specifications. Nowadays the Bluetooth Special Interest Group is responsible for managing and developing a new version of Bluetooth. This is standard has been use since January 14th 2002. [6.]

One major part of IEEE 802 standards is its openness and open source type of approach. All meeting notes / All notes of meetings and their agenda are public information on their website. In addition, the minutes of the meetings list the people who were part of the meetings and their affiliation with companies. There are some notes which are only for the members of the working group, i.e. the working group's participants. Membership of IEEE is not a requirement for membership in a working group, but those who are not members of IEEE, IEEE Standards Association (SA) and the IEEE computer Society, are highly encouraged to join IEEE. To become a member of a working group, an individual must participate in two out of the four last plenary sessions. [7] These sessions are usually held four to five times a year. The membership starts the the third plenary session attended by the individual. The chair of the working group may also declare membership. The full list of requirements to fulfil to retain the membership is declared in a document on the IEEE website. [7]. Working groups consist of those who create and write the IEEE standards.

3.1 802.3

IEEE 802.3 is a standard which determines the Physical layer and Data Link layer's MAC in wired Ethernet. The standard for wireless Ethernet is determined by IEEE 802.11. The first version of 802.3 was released in 1983 which allowed up to 10 MB/s data rates. At that time, a coaxial cable was used. The now commonly used twisted pair cable came in to use with the version 802.3i in 1990. The first fiber optic standard was 802.3j which was published a few years later in 1992 [8.]

The Data link layer is divided into two different sublayers: Logical Link Control (LLC) and Media Access Control (MAC). From these, MAC forms an identification for all devices in the Ethernet network. The MAC address consists of 12-digit hexadecimal numbers for

the total of 48 bits. The first 24 bits are known as Organizational Unique Identifier (OUI), which determines the manufacturer. These bits can be used to determine the device and its manufacturer just from the MAC address. IEEE manages these OUIs. The last 24 bits represent a serial number given by the manufacturer. [9]

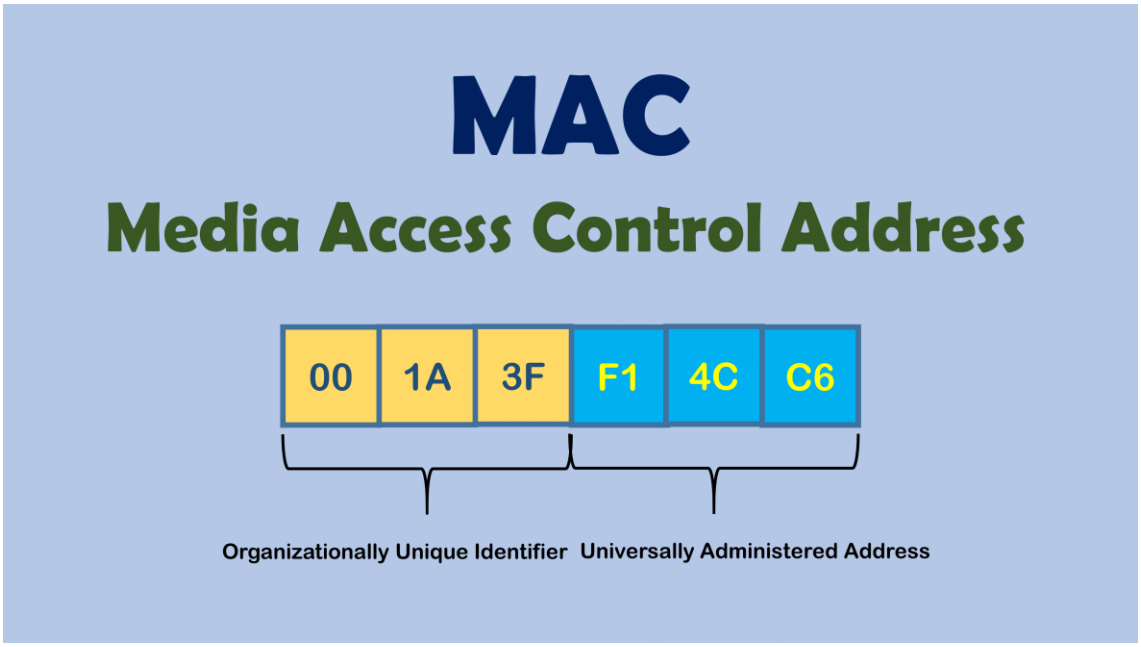

Figure 3. MAC address structure. Copied from [10].

As mentioned before, one way to secure a network is to use IEEE 802.1X, but not all devices support it, such as network printers or Ethernet based cameras or sensors. To overcome this issue, an administrator can configure the devices for MAC-Address bypass (MAB). When using MAB, the switch port drops all frames sent to the switch except for the first frame to learn the MAC address of the device. This works with any frame except for DTP, STP, CDP or LLDP traffic. [11] Once the switch has learned the mac address of the device, it will then check it with an authentication server, such as RADIUS to confirm if it can allow the other traffic from that MAC address and open that port. The checking of the MAC address works similarly to an EAP Request It is possible to configure MAB as a fallback, meaning that if 802.1X authentication fails the network device will switch to MAB. An example case would be a device that does not support 802.1X.

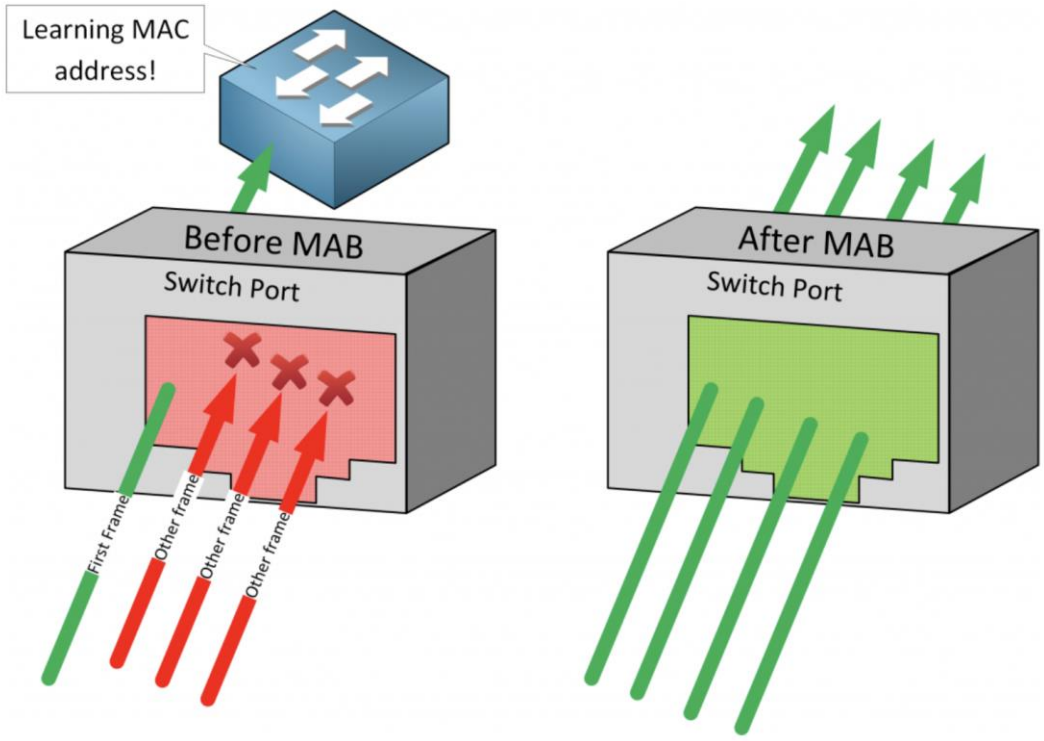

Figure 4. Demonstration of how MAB works. Copied from [11].

With its default configuration, MAB only supports a single device per switchport [8]. When more than one source MAC address appears in the network switch, it causes a security violation and shuts down the port. This is called Single-host Mode. To overcome this issue, there are multiple different modes which an admin can set them to. The multi-domain authentication host mode allows two source MAC addresses, for example, for different VLAN networks if there was a PC behind an IP phone. The Multi-Authentication host mode allows for multiple source MAC addresses. Example usage of this is connecting a switch to a switch. Each MAC address is separately authenticated. The multi-host mode allows multiple source MAC addresses, but only the first MAC address is authenticated. The rest of the MAC addresses are automatically permitted to the network. [11.]

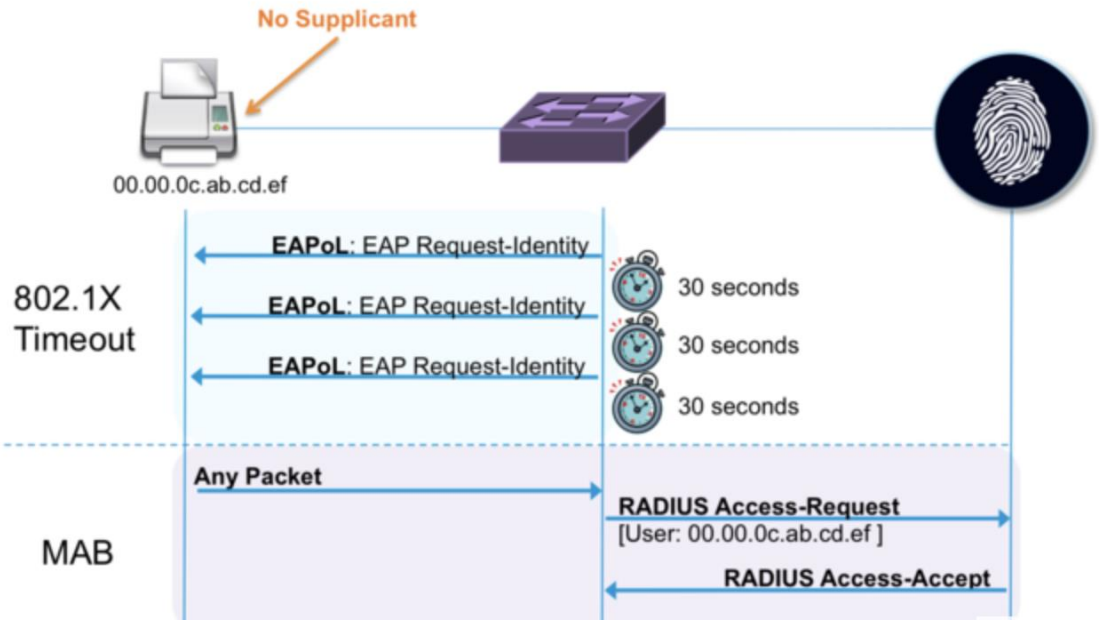

Figure 5. Example of EAPoL transaction 802.1X failing and switching to MAB. Copied from [11].

Another notable IEEE 802.3 Standard is IEEE 802.3af which is Power over Ethernet (PoE). This allows powering devices such as IP phones, switches, routers and other devices through an Ethernet cable. The standard was released in 2003 [12]. IEEE then released 802.3at which is just an upgraded version of PoE. This allows for more power output. This was released in 2009 [10]. 802.3bt-2018 is the newest version of PoE which was released in 2018 [13].

Type	Standard	PSE Minimum Output Power	PD Minimum Input Power	Cable Category	Cable Length	Power Over
Type 1	IEEE® 802.3af	15.4W	12.95W	Cat5e	100m	2 pairs
Type 2	IEEE® 802.3at	30W	25.5W	Cat5e	100m	2 pairs
Type 3	IEEE® 802.3bt	60W	51W-60W [1]	Cat5e	100m	2 or 4 pairs class 0-4 4 pairs class 5-6
Type 4	IEEE® 802.3bt	90W	71W-90W [1]	Cat5e	100m	4 pairs class 7-8

Figure 6. Differences between the three PoE versions. Copied from [13].

Type 3 and 4 both follow IEEE 802.3bt standard, but have a few minor differences as shown above, the most noticeable difference being the minimum output power.

3.2 802.1

IEEE 802.1 is a working group that is concerned with High Layer LAN protocols. It handles mostly network management and monitoring capabilities in IEEE 802 networks. The working group works on the two main tasks of IEEE 802.1 which are LAN/MAN management, network traffic management, data encryption and decoding and MAC bridging, for example. The second task is to implement and design standards which regulate network management practices. [14] These include standards such as 802.1X which will be discussed in more detail below.

IEEE 802.1X is a Port-based Network Access Control standard which can be used in wired or wireless IEEE 802 LAN networks. This protocol standard opens a network device port after the organization has authenticated the user and authorized the user to the network. The user's credentials are usually authenticated by a RADIUS server which can be, for example, connected to an organizations Active Directory server. IEEE 802.1X determines the capsulation of EAPs in IEEE 802 LAN networks.Extensive Authentication Protocol (EAP) is an authentication framework. It supports multiple different authentication methods such as OTPs, certificates and token cards [15]. EAPOL is EAP over LAN which is the encapsulation defined by the IEEE 802.1X.

In 802.1X authentication, the Supplicant (the user's device) sends a request to access the network to an authenticator such as a network switch, for example, which responds by sending an EAP Request to the Supplicant. The Supplicant responds by sending an EAP-Response. This usually contains an identity such as a username. The authenticator forwards the identity information that it received from the Supplicant to the authentication server. This Authentication Server is usually a RADIUS server. RADIUS servers can be configured to use the organizations Active Directory service. The authenticator uses a RADIUS Access-Request message for forwarding the message. When the Authentication Server receives the RADIUS Access-Request message the server will send a RADIUS Access-Challenge message back to the Authenticator. It contains a challenge and the authentication method. The Supplicant can reject this Authentication method and request a new one if it does not support it. The authenticator receives the Access-Challenge message from the authentication server and will prepare an EAP-Request message for the Supplicant and send it. The Supplicant has not received the Authentication method suggested by the Authentication server. If it does not support it, it will reject it

and request a new one. In the message the Supplicant sends back to server, it also specifies the authentication method which the Supplicant prefers to use. When the Supplicant and the Authentication Servers have decided which authentication method to use, the Supplicant will send the credentials to the server which confirms them or rejects them. If the credentials are valid, it will send a RADIUS Access-Accepts message indicating that they are valid. A RADIUS Access-Reject message is used when the credentials are invalid. The message will go through the Authenticator which will open the network port and send an EAP Success message to the Supplicant indicating that the credentials were/are valid and that the authentication has worked. [16]

4 Cisco ISE

Cisco ISE (Identity Services Engine) is a platform for identity and access control policy, which allows companies/organizations to enforce compliance, streamline their service

operations and to enhance the security of their infrastructure. ISE allows the gathering of real-time information from users, devices and networks. A network administrator can configure ISE to make proactive decisions by tying identity to network elements such as WLAN controllers, VPN gateways, data center switches or access switches [17]. ISE combines many different features into a single appliance such features as authentication, authorization, and accounting (AAA). It also includes guest access management applications for the administrator, monitoring of endpoint device and many other features. Cisco ISE is available in two different formats: as a virtual machine or a Cisco SNS appliance. The virtual machine is self-explanatory with any basic knowledge about VMs. SNS, on the other hand, is a rack server preconfigured to be an ISE server which is sold by Cisco. An administrator can acquire a server and mount it to their server rack and use it for, for example authorization and authentication requests. The product information and product specifications for Cisco secure network server can be found on their website. The price of Cisco ISE cannot be found on Cisco's website. In order to get the price, a person must ask for an invoice from Cisco, but estimates are in thousands for the VM licenses and for SNS appliances around €10,000.

Cisco ISE has three different distributed deployments for different sized networks. These architectures are called Small, Medium and Large. Small ISE consists of two Cisco ISE nodes in which one of the ISE nodes functions as a primary appliance and the secondary node functions as a backup one [18]. The main ISE node synchronizes or replicates all its content to the secondary node. This keeps them both up to date with the information in case the primary ISE node loses its power or connectivity and the secondary node must take over. It is also possible to have split deployment where the AAA load is split between the two Cisco ISE nodes to optimize the AAA workflow. Both nodes need to handle the full load of AAA requests in case of a connectivity or power loss in either one A small ISE virtual machine requires 16 cores [19.]

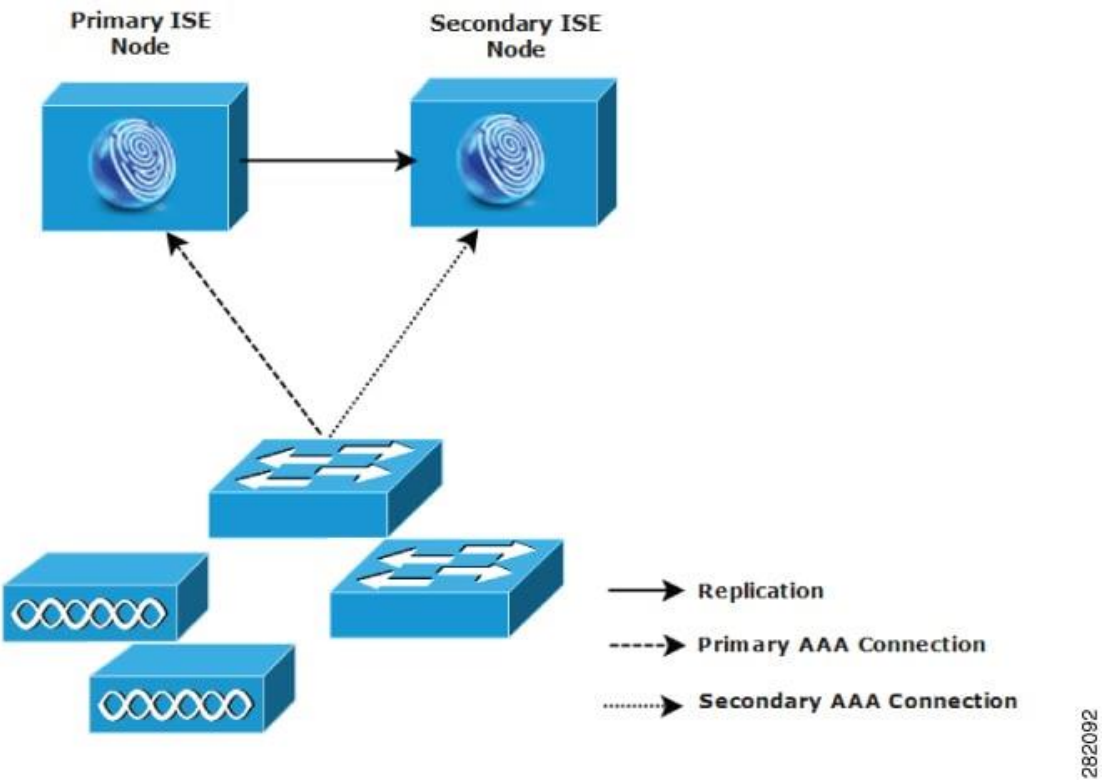

Figure 7. Small Network Deployment. Copied from [19].

In a medium-sized deployment it is possible to dedicate a few new nodes for AAA and keep using the old primary and secondary nodes for configuration and logging functions [19]. In a way, this is a split deployment as this divides the workload between different nodes, but a single node does not need to be capable of handling the whole workload in case loss of power or connectivity. A medium-sized deployment virtual machine requires 16 cores. [19]

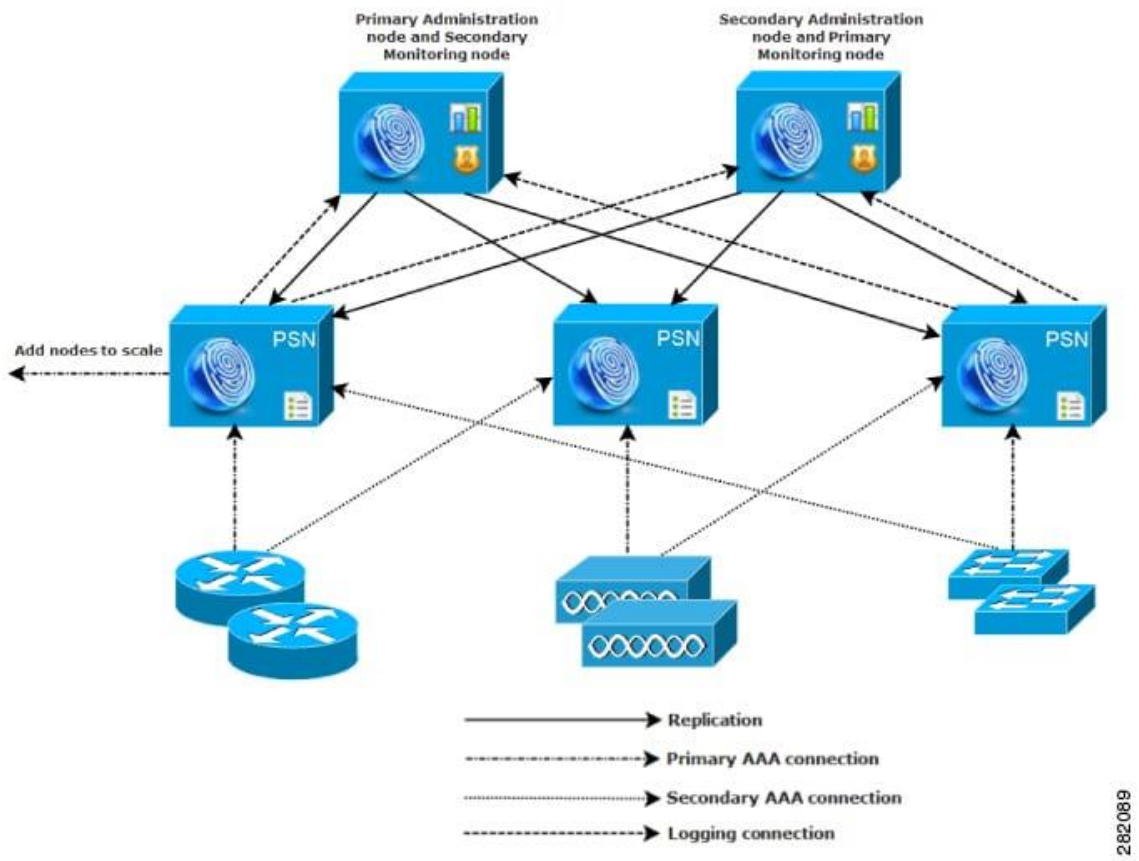

Figure 8. Medium-Sized Deployment. Copied from [19].

Large network deployments are not significantly more special than medium-sized ones. A load balancer is required, and it uses more ISE nodes for different purposes. A large Cisco ISE server requires 24 cores on a virtual machine. [19] When building a Cisco ISE system, the right license for the server is required. This could be a small one, a medium-sized or a large one.

Simply put, Cisco ISE allows an administrator to provide highly secure network access to users and other devices. It provides easy visibility to a network so monitoring becomes more efficient. Cisco ISE naturally works with Cisco devices but also supports other third-party devices. Some of the third-party devices only support wired or wireless mode.

5 IBNS 2.0

Cisco Identity-Based Networking Services (IBNS) is a set of tools used to configure network access control in a corporate network. As bring-your-own-device initiatives are on the rise alongside remote work, it is important to secure the network. Cisco IBNS allows the administrator to configure easily policies on the network devices, which manages the user's network access. This network access authorization can be done using IEEE 802.1X, MAC Authentication bypass (MAB) and web authentication. [20] A network administrator can create templates and assign these to existing network ports so that when a user connects to a wired Ethernet port, the network devices can automatically assign group policies or assign the user into a specific VLAN.

One of the key features of IBNS 2.0 is that it supports Cisco Common Classification Policy Language (C3PL). It is a structured feature-specific configuration language. To start using C3PL, the following command is needed to be issued on a network switch.

```
Authentication convert-to-new-style
```

To check which style the switch is currently using, the following command should be used.

```
Authentication display config-mode
```

Both commands need be run in the EXEC mode. It is important to note that converting the switch into the new style is permanent and cannot be reversed [21].

Policy maps are containers which are assigned into an interface. Inside these containers there are class maps which are short instructions which will be carried out on specified cases, for example, if a user connects to a network port and the user is authorized for that network. The network device can assign the user into a specific VLAN.

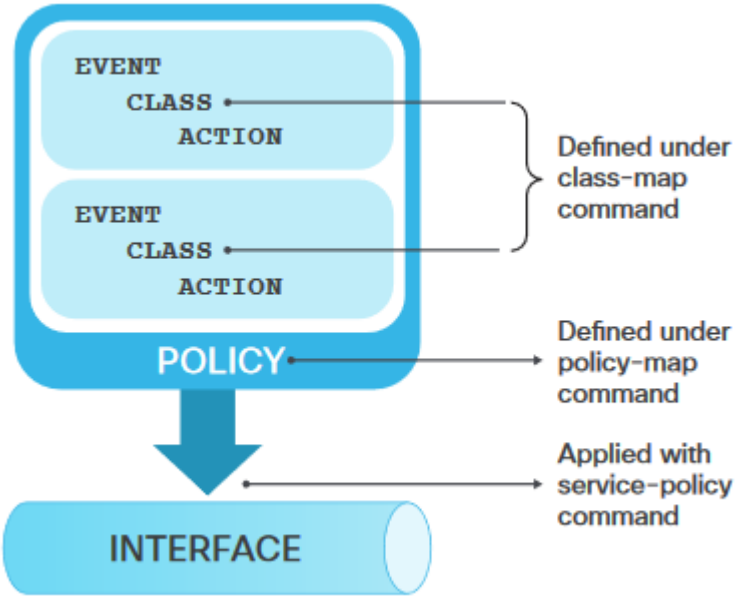

Figure 9. Example of a control policy configuration. Copied from [20].

Service templates can also be used to configure IBNS 2.0. These templates are a basic set of policies that have certain attributes or features which can be applied to a user's session through a control policy, RADIUS Change of Authorization (CoA) request, or a user profile. [22] These can authorize to user into a VLAN or access control lists. These can be defined locally in a switch or authorized by a centralized policy such Cisco ISE [22].

6 Installation and Configuration of Cisco ISE-Server

This installation of Cisco ISE 2.6 will use a virtual machine, VMware to be more specific. In this case, a medium-sized deployment is used for the Cisco ISE. In this case it is installed on an ESXi-server. In the ESXi client choosing New Virtual Machine will start the deployment. Choosing custom installation is needed for the installation, as ISE does not need much space. The recommended amount on data storage is enough. It is important to choose the right version from the drop-down list which is Linux and Red Hat Enterprise Linux 7 in this case. After this the client will ask for the number of virtual sockets and the number of cores. In this case medium-sized ISE is used which needs 16 cores. However, it is recommended to choose some more processing power to increase stability, as the 16 core is just the minimum requirement. E1000 is the recommended NIC driver to ensure the correct adapter order by default. Choosing VMXNET3 can cause some issues and maybe force to remap the ESXi adapter to synchronize it with the ISE adapter order. [19] For this installation, Paravirtual is required as the SCSI controller. When creating a virtual disk, Thick provision is recommended. ISE supports both thin and thick provisioning. On the next page, fault tolerance can be unchecked as it is not needed. The last page allows for a final check of the configuration. Pressing Finnish will complete the installation. Now the VMware system has been installed.

6.1 Initial Configuration of ISE

To start the initial configuration, booting up the newly installed Cisco ISE is required. Mapping the CD/DVD to an ISO image will continue the process and a screen will appear prompting the user to choose a boot option. In this case (Cisco ISE Installation (Keyboard/Monitor) is chosen. [18], after which the ISE will start to install some software which can take some time. After the software has been installed, it will now require the user to type ‘setup’ to configure ISE. Now the ISE will ask the user to submit the following parameters in order.

- Hostname
- IP address for Ethernet interface (eth0)
- Netmask
- Default gateway

- DNS domain name
- Add another name server (Optional)
- NTP server
- Add another NTP server (Optional)
- System Time Zone
- Username
- Password

After the setup program has been completed, the system will automatically reboot [19].

After the system has rebooted, it will ask the user for username and password in the login prompt. When successful, the ISE should be up and running. To verify this, enter the following command.

```
show application
```

It should now display that ISE is running. To check the status of ISE processes, enter the following command.

```
Show application status ise
```

It will now display the processes which are running. Now the ISE is up and working and it is accessible through the CLI or web GUI.

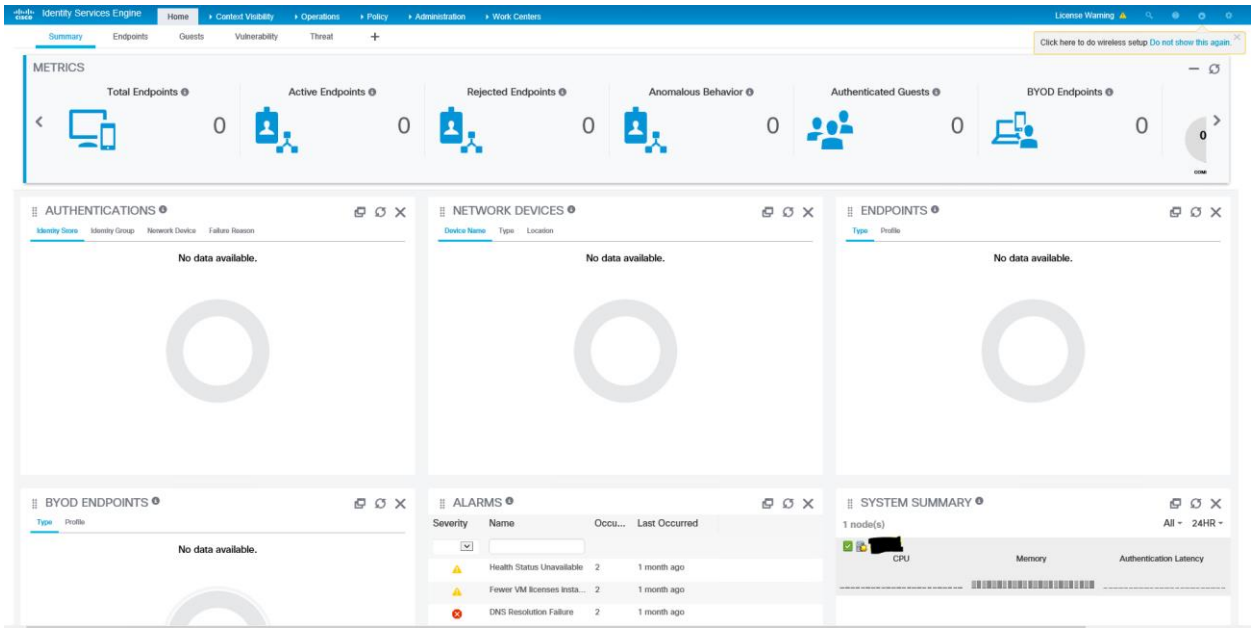

Figure 10. Reference picture of Cisco ISE 2.6 web GUI. Based on [Internal company document].

6.2 Policy Sets

Policy sets were introduced first in the version 2.3 [23]. The policy sets simplify authentication and authorization policies management. They allow the network admin to easily configure and view the policies. When a device tries to connect to a network, it will first check the Policy sets for the conditions that it matches, after which the device gets authorized to the network. There are two (2) levels of policy sets, i.e. the Parents and Child level. From the Parent level, it is possible to set the conditions for the devices to follow. The Parent level policy sets can be moved by simply dragging them around. From the Allowed Protocols box, access protocols or servers' sequences can be added for validation.

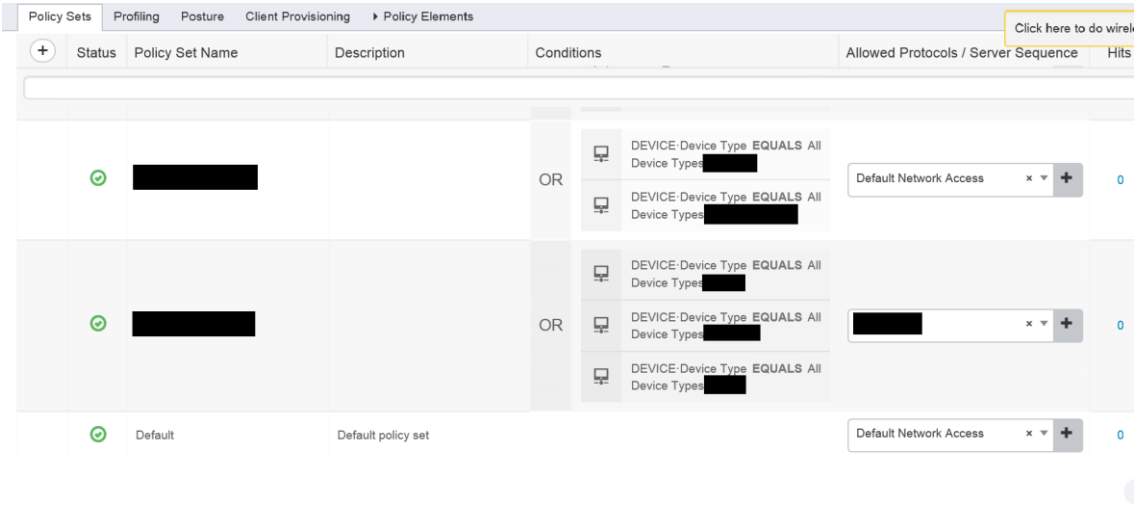

Figure 11. Policy sets parent level interface. Based on [Internal company document]

In this case if a laptop is connected to the network wirelessly it will go to the Default policy sets and get authorized to the network set by the rules inside the Policy set.

On the child level, it is possible to create rules for user authentication and set the specific rules for authorization [19]. For example, if the user is in a remote/secondary office, it is possible to automatically set the user into a specific VLAN, or if the user has a specific Active Directory group, the user is set to a specific VLAN. If the company has guests over and has a network just for them, it is possible to set it so that the users without a proper certificate on their computer must access the guest portal web UI first. Figure 12 below demonstrates how the Authorization policy works with any user and first checks if the user's devices have a certificate, then checking if it is wireless and then finally if it is part of the Active Directory group called "Laptop8200". If the devices do not match with all of these, it will skip this rule and go to the next one on the list.

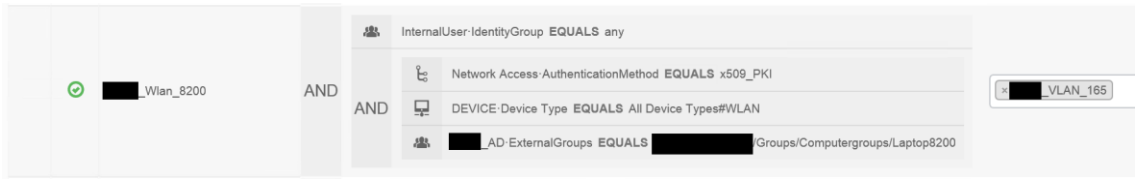

Figure 12. Example of a Child level policy. Based on [Internal company document].

The possibilities are almost limitless. The authorization policies rules are set up with a conditions studio. The conditions studio works by allowing the user to drag and drop

different conditions which the devices need to have. It allows the usage of conditional statements such as And, Or and Is not. If the Active Directory has already been set up, it will be visible in the conditions studio when trying to use AD for something. It will automatically know existing groups which allows easy setup for the administrator.

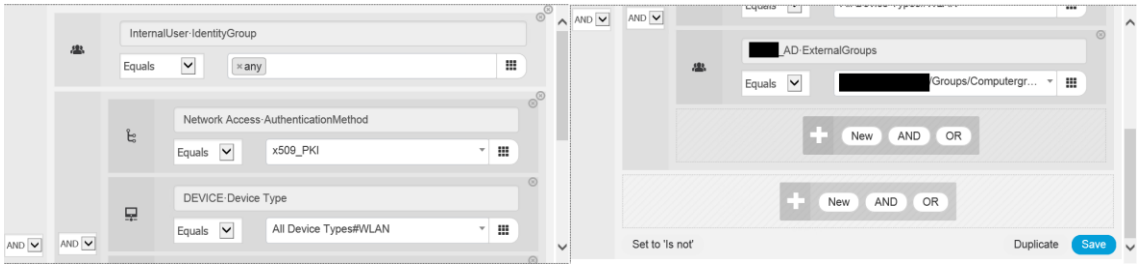

Figure 13. Reference picture of the conditions studio. Based on [Internal company document].

In the end, the core of ISE can be found in the Policy sets when it comes to network access control. The Policy sets did not exist before in versions older than 2.3, but they still had the same authentication and authorization rule setups. In addition, the conditions studio was also introduced in this version. That is one of the key reasons why version 2.3 or a newer version is highly recommended.

6.3 Setting up Cisco ISE Distributed Environment

As mentioned in section 4, Cisco ISE supports split deployment, distributed environment and clusters. They are all the same but with more sophisticated names. Basically, what this allows is that an administrator can configure one single ISE server, then copy it and then cluster the original and the copy together to be used as one. This is useful when the server needs to be available continuously. In case one of the server breaks or suffers a power loss, the secondary node will take over. The cluster can also be used to share the workload between the two ISE servers.

Clustering the two ISE servers is very simple. First, two ISE installations on different servers and IPs are needed. In the first ISE which is made into a primary node an administrator tab can be found and inside there is a select deployment button. On the left, there is a column. The Deployment tab should be opened next, after which the primary ISE is found. There is a section where the role is chosen for the ISE. If this part has not

been touched yet, it should say standalone [24]. Changing this to primary will it make it primary ISE.

Now a self-signed certificate is needed from the secondary ISE node. To retrieve the self-signed certificate from the secondary ISE node, the administrator tab should be clicked and System Certificates should be chosen. From there, the export button can be found. Now back in the Primary ISE Node's certificates tab, the import button can be found. On the frontpage, there is a register tab just under the Deployment Nodes. From there it is possible to register the secondary ISE node. Set a hostname, a username and a password for it. Now the Secondary ISE should automatically be setup to be the Secondary node and the Primary node as the other monitoring node. Save the settings and a pop up should appear telling it takes a couple of minutes to synchronize the two nodes [24]. Now a distributed environment using medium network deployment has been setup.

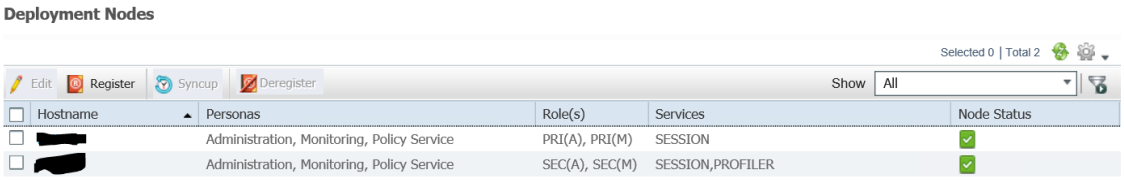

Figure 14. Two ISE nodes clustered together. The first one is primary and the second one is secondary. Based on [Internal company document].

7 TrustSec

TrustSec is software-defined segmentation technology made by Cisco. Instead of using an IP addresses, it uses endpoint roles for managing the network access control. This can be managed and configured by using Cisco ISE. [25] By using TrustSec, a network admin can implement network segmentation without changing the topology. Normally an admin would add more or remove VLANs but in this case it is not needed. With Cisco TrustSec, an admin can add Security Group Tags (SGT) to a network access endpoint such as router, switch or a firewall which is typically based on the user's location, device or the user itself [25]. SGTs are only supported by Cisco devices. However, SGT Exchange Protocol (SXP) can be used to propagate SGTs across the network for devices which do not have hardware support for Cisco TrustSec. [26]

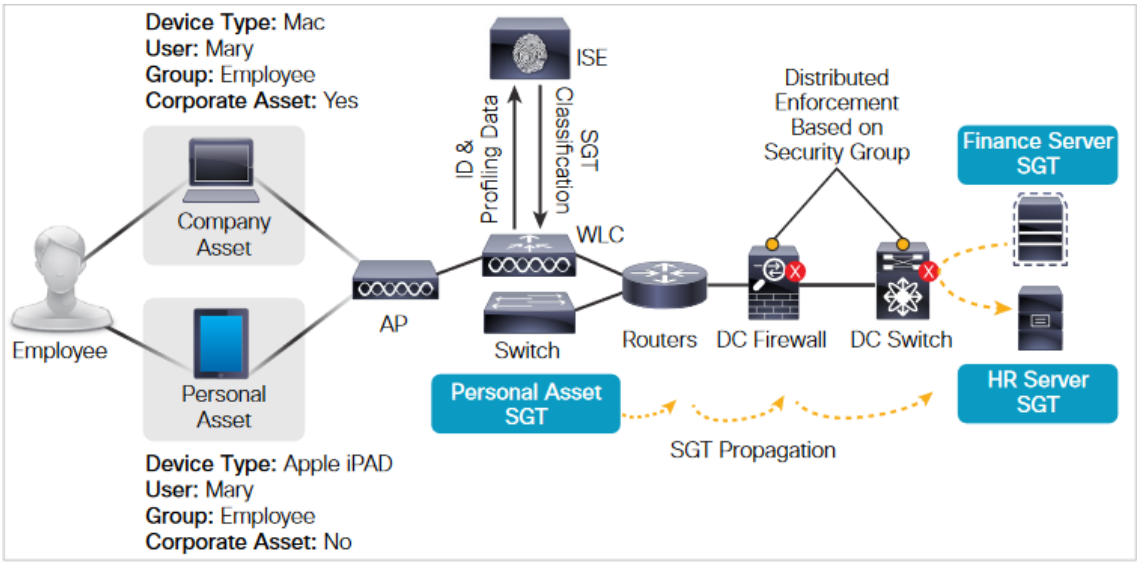

Figure 15. Example of SGT in use. Copied from [25].

As figure 15 shows, the Personal Asset has a SGT which does not allow access to the corporate assets. Cisco TrustSec can help the company to lower its costs by saving time, making BYOD easier and more accessible and making the whole network a bit more dynamic [25]. TrustSec also supports flexible authentication. What this mean that it combines 802.1X and MAB to a single authentication process. Commonly there are three modes which TrustSec is deployed in. These are Monitor Mode, Low-impact Mode and Closed mode which was previously known as High-Security Mode.

7.1 Monitor Mode

Monitor Mode uses logging data for validation. Administrators can use this mode to ensure all the devices are authenticating correctly and to discover devices in their network that do not belong there. Essentially this works like the audit mode [27]. To ensure the authentication goes smoothly, the monitor mode uses 802.1X or MAB. If a device is missing its 802.1X Supplicant or is misconfigured. The Open authentication mode in the monitor mode makes sure access will not be denied and it will collect data of the attempt.

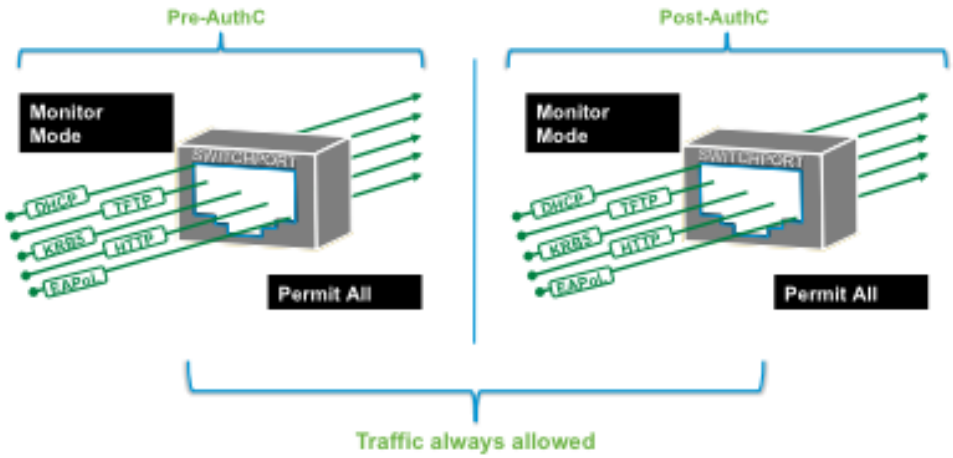

Figure 16. Monitor mode in use. Copied from [27].

The following picture show the flow of the Monitor Mode in use. First it will learn the MAC and then check if it is authenticated by Dot1X. If its not it will timeout and use MAB. If that fails it will still gain access to the network. If Dot1X or MAB is successful it will gain access to the network

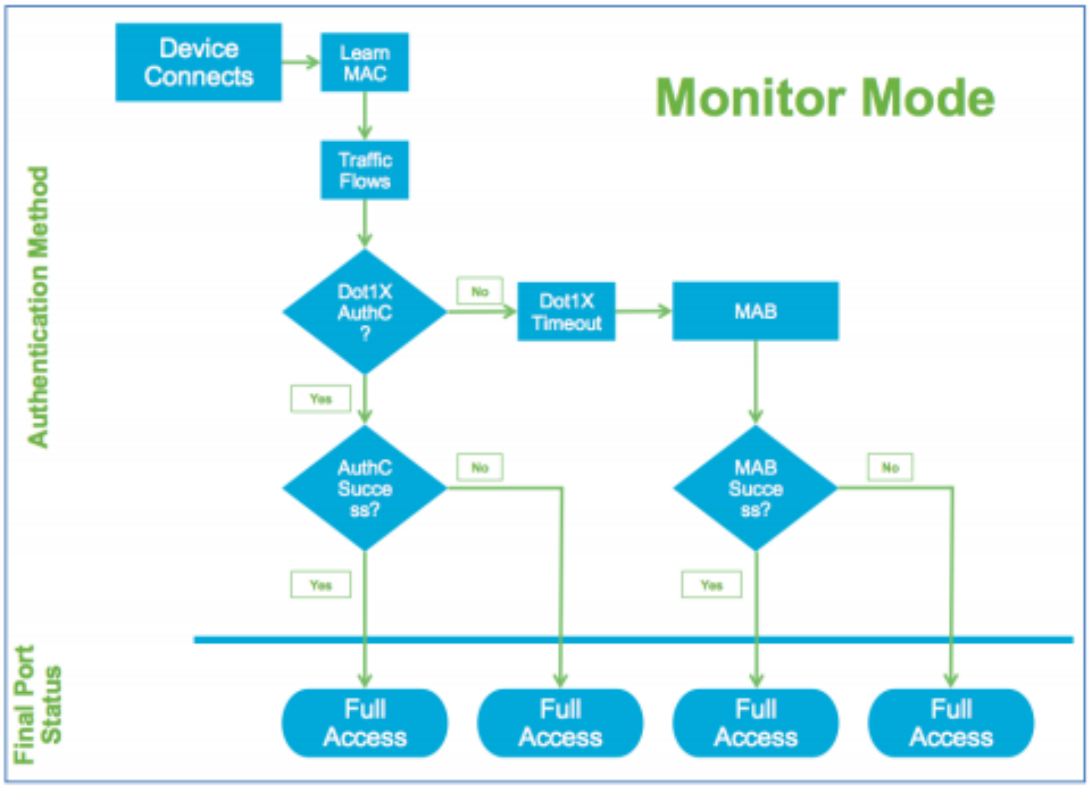

Figure 17. Flowchart of Monitor mode using Dot1x and MAB. Copied from [27].

7.2 Low-Impact Mode

The Low-Impact Mode can be used to allow connected devices to get an IP from DHCP using DNS or even access the internet. However, the mode blocks any access to internal network resources. This is achieved by deploying the Monitor Mode and then applying Access Control List (ACL) to the switchport. This ACL gives the port the restricted access. After the user has authenticated successfully, they will be granted better access to the network. These are just examples of what is achieved with the Low-Impact Mode and its purpose.

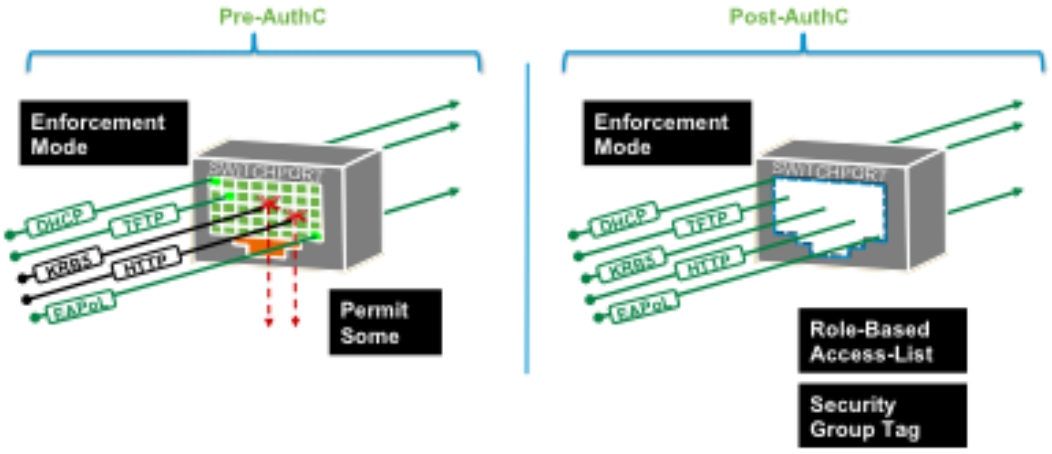

Figure 18. Example of Low-Impact Mode [27].

The Low-Impact Mode authentication process works similarly to the Monitor Mode, the only exception being the result and the status of the switchport. Essentially this allows the admin to increase the security of the network. The restricted access can be accommodated based on the results of the authentication and the authorization process by combining ACLs and (downloadable ACLs) with the Cisco TrustSec-enabled port.

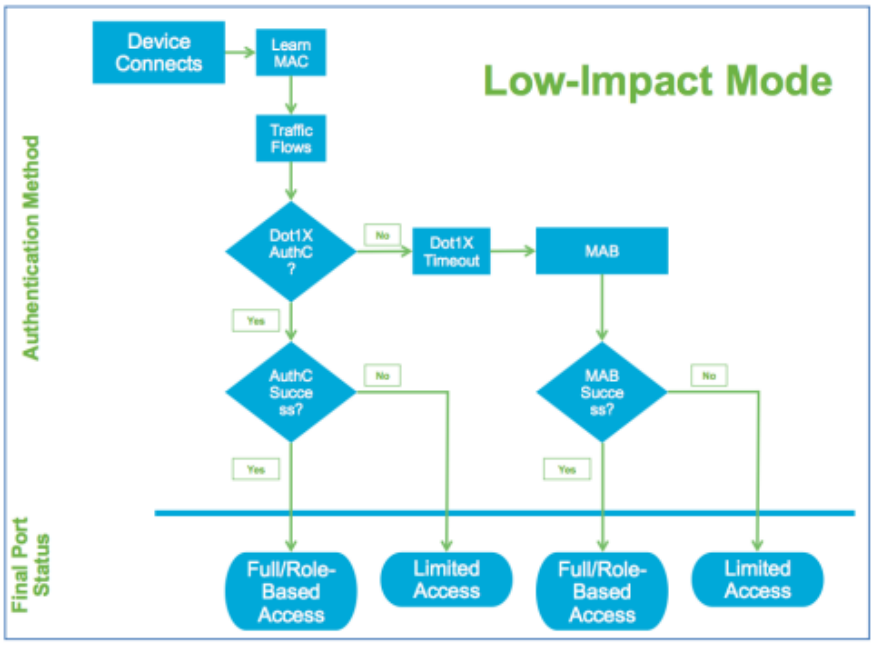

Figure 19. Flowchart of Low-Impact Mode. Copied from [27].

7.3 Closed Mode

The so-called default mode of 802.1X is Closed mode which was previously known as High-Security mode. It pretty much works like it was described earlier in this thesis in section 3.2.1. The Closed Mode is recommended for those who are experienced and ready to deal with the nuances that come with configuring something like this. The Closed Mode differs from the Monitor Mode and the Low-Impact Mode in that before the authentication is successful all upcoming traffic is dropped. This includes DHCP, DNS and ARP, for example.

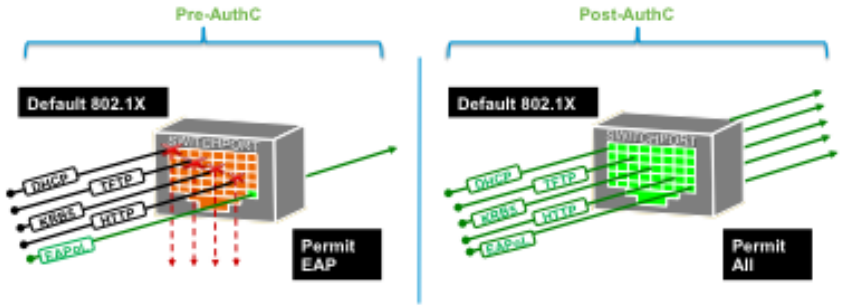

Figure 20. 802.1X authentication in closed mode. Copied from [27].

Hence, the closed mode is the default type when using 802.1X to authenticate and authorize the network users. When the authentication is not successful via 802.1X or MAB, it generally closes the switchport or just grants limited access. Limited access can mean that it drops everything except for packets needed for authentication.

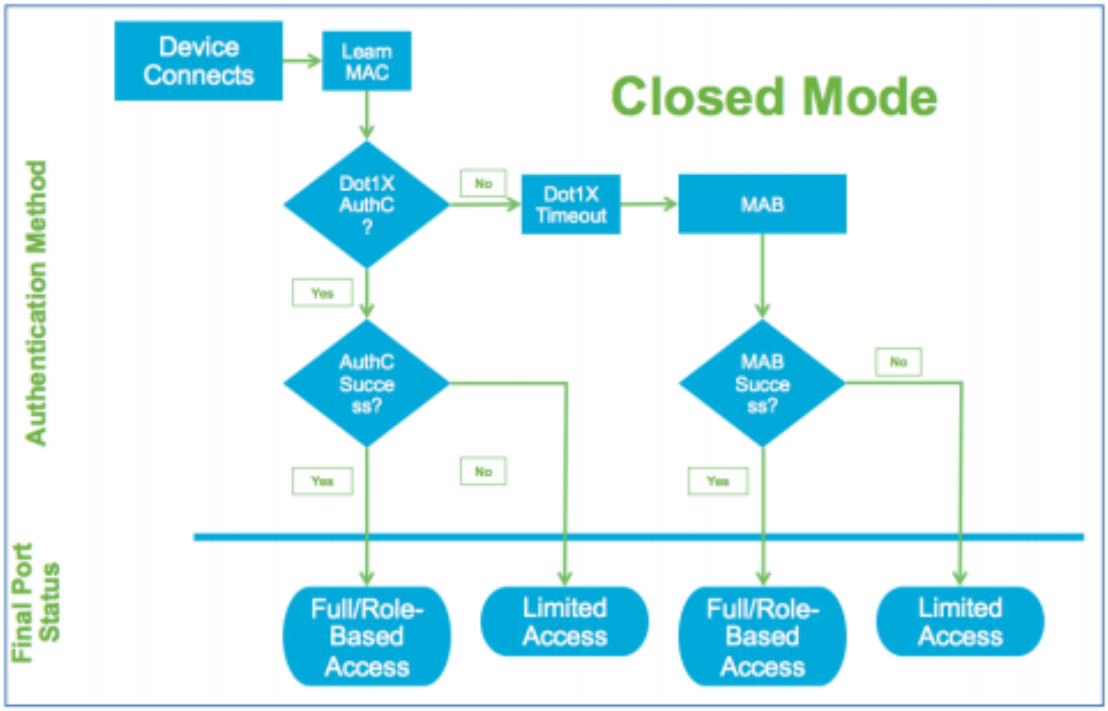

Figure 21. Closed mode flowchart. Copied from [27].

To summarize the three different modes, they have their differences and their own use cases. The Monitor mode can be used to discover devices while not disrupting the network and its users. The Low-impact mode can be used to give the right users and other users access, such as a guest's basic internet access, to network resources. The Closed mode can be used for high security in the network.

8 Conclusion

The goal of this thesis was to study the opportunities and technologies in terms of Network Access Control and to learn more about different platforms which can be used to manage the access of users in corporate network.

The goal was accomplished by studying Cisco documentation and through hands-on learning when migrating the Cisco Identity Services Engine from an older version to the newer 2.6 version for a Finnish company. The project was completed successfully. This thesis describes many ways to implement some level of network access control. In addition, the guidelines compiled in the final year project also cover how to implement basic level Network Access Control using the Cisco Identity Services Engine.

This bachelor's thesis is useful to anyone who does not have much knowledge of network access control or to someone who wishes to implement the Cisco Identity Services Engine to their network and is looking for basic instructions.

The world of network access control is large and complicated, which is good because every situation is different, and companies have different needs when it comes to security and network access control. Although the IEEE 802 standards are old, they are still in use and should be learned by future network administrators. Cisco, Aruba and Fortinet, for example, are constantly developing new platforms and features, which means that there is always more to learn about network access control.

References

1 What Is Network Access Control? 2018. Online. Comodo. <https://enterprise.comodo.com/blog/what-is-network-access-control/> Accessed August 25, 2020.

2 What Is a One-Time Password (OTP). 2020. Online. Okta. <https://www.okta.com/blog/2020/06/what-is-a-one-time-password-otp/> Accessed August 25, 2020

3 One-time Password (OTP) Tokens. Online. Microcosm. <https://www.microcosm.com/products/oath-otp-authentication-tokens> Accessed September 9, 2020

4 History of IEEE. 2020. Online. IEEE <https://www.ieee.org/about/ieee-history.html> accessed April 11, 2020.

5 IEEE 802 LAN/MAN Standards Commitee. 2020. Online. IEEE. <http://www.ieee802.org/> Accessed April 11, 2020.

6 IEEE 802.15 WPAN Task Group 1 (TG1). 2004. Online. IEEE. <http://www.ieee802.org/15/pub/TG1.html> Accessed April 12, 2020.

7 IEEE 802 LMSC Working Group Policies and Procedures, v19. 2016. Online. IEEE. <http://www.ieee802.org/PNP/approved/IEEE_802_WG_PandP_v19.pdf> Accessed May 26, 2020.

8 What Is Ethernet (IEEE 802.3)? 2018. Online. IONOS. <https://www.ionos.com/digitalguide/server/know-how/ethernet/> Accessed May 8, 2020.

9 MAC Address. Online. Richland Education. <https://people.richland.edu/dkirby/141macaddress.htm> Accessed May 26, 2020.

10 Mac Address. Online. Network Encyclopedia. <https://networkencyclopedia.com/mac-address/> Accessed September 9, 2020

11 MAC Authentication Bypass. 2019. Online. Kumari Priyanka. <https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari/> Accessed May 27, 2020.

12 PoE – IEE 802.3af and IEE 802.3at.Online. Dipol. <https://www.dipolnet.com/poe_-_iee_802_3af_and_iee_802_3at_bib746.html> Accessed September 9, 2020

13 Next-Generation PoE: IEEE 802.3bt White Paper. 2018. Online. Shahar Feldman. <https://www.microsemi.com/document-portal/doc_view/136209-next-generation-poe-ieee-802-3bt-white-paper> Accessed September 9,2020

14 IEEE 802.1 Working Group (IEEE 802.1).Online. Technopedia. <https://www.techopedia.com/definition/19936/ieee-8021-working-group-ieee-8021> Accessed April 17, 2020.

15 EAP – Extensible Authentication Protocol. Online. Webopedia. <https://www.webopedia.com/TERM/E/EAP.html> Accessed May 22, 2020.

16 How IEEE 802.1x (dot1x) Port Based Authentication Works. Online OmniSecu. <https://www.omnisecu.com/tcpip/how-ieee-802.1x-port-based-authentication-works.php> Accessed May 26, 2020.

17 Cisco Identity Services Engine Adminisrator Guide, Release 2.6. 2020. Online. Cisco. <https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_00.html#concept_C1FC4506C12A48519CF3131845464164> Accessed July 29, 2020.

18 Overview of Cisco ISE. Online. Cisco. <https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.pdf> Accessed July 13, 2020.

19 Cisco Identity Services Engine Installation Guide, Release 2.6. 2020. Online. Cisco. <https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26/b_ise_InstallationGuide_26_chapter_011.html#ID-1417-00000271> Accessed July 29, 2020

20 Cisco Identitity Based Networking Services 2.0 At-A-Glance. 2014. Online. Cisco. <https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/aag_c45-731544.pdf> Accessed May 26, 2020.

21 Identity-Based Networking Services Configuration Guide, Cisco IOS Release 15E. 2019. Online. Cisco. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-e/ibns-15-e-book/ibns-cntrl-pol.html> Accessed May 26, 2020.

22 Identity Based Networking Services. Online. Cisco. < <https://www.cisco.com/c/en/us/products/ios-nx-os-software/identity-based-networking-services/index.html> accessed May 26, 2020.

23 Cisco ISE: Introduction to Policy Sets 2019. Online. Cisco. <https://www.cisco.com/c/en/us/td/docs/security/ise/videos/policy_sets/v1/cisco-Introduction-to-Policy-Sets.html> Accessed August 13, 2020

24 Configuring Cisco ISE 2.1 For Distributed Deployment. 2016. Online. Tharakak. <https://www.youtube.com/watch?v=uSxk0zQm2go> Accessed September 1, 2020

25 Cisco TrustSec. 2013. Online. Cisco. <https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf> Accessed September 3, 2020

26 Chapter: SFT Exchange Protocol over TCP (SXP) 2019. Online. Cisco. <https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_config.html > Accessed September 9, 2020

27 Introduction to the Cisco TrustSec System. Online. Guides. <https://guides.co/g/cisco-trustsec-phased-deployment-overview/11101> Accessed September 2, 2020