Analysis Report

The AAA Project

Name: Andres Vivas Rodriguez
Student number: 345155
Institution: Hanzehogeschool Groningen
Education: HBO-ICT, Network & Security Engineering

Internship Supervisor: Thies Keulen
Internship Lecturer: Jos Bos

Company: Axians ICS Groningen
Company Supervisor: Peter Eek

Table of Contents

1. Introduction

This report will be known as the analysis report. The purpose of the report is to provide information on the internship project proposed by Axians ICS Groningen.

This report is basically the first phase of the project, the analysis phase. The analysis phase is the gathering of information about the current environment and also the current problem which the internship project is based on. The main task for this phase is to gather every possible information on the current situation to be able to further plan out the possible solutions and how they can be implemented later on in which Axians may benefit from.

The next chapter will be about introducing the organization that proposed the internship project. After that, chapter 3 will be about introducing the project itself, the internship assignment and the problem surrounding it. Chapter 4 will be going over the current environment of Axians and any relevant information deemed necessary to mention. Chapter 5 will list possible solutions in which a choice could be made that may help solve the current problem(s) Axian is facing and lastly, the conclusion.

2. The Organization

This chapter will give an introduction to the company that offered the internship assignment, followed by the stakeholders for the internship project.

2.1 VINCI Energies

VINCI Energies is an international company operating in 53 countries worldwide, their 1,800 business units intervene in infrastructure, industry, service sector and information and communications technology (ICT). They are organized around five international brands – Omexom, Citeos, Actemium, VINCI Facilities and Axians – in addition to brands with a more regional identity.

In an ever-changing world, VINCI Energies focuses on networking and integration, performance optimization, energy efficiency and data. We do this to accelerate the roll-out of new technologies and to support two important changes: the digital transformation and the energy transition.

VINCI Energies delivers a customized solution for each individual project, from the smallest to the most complex, in order to meet their customers' challenges in terms of performance, reliability and safety in our four main areas of expertise: electricity, HVAC(Heating, Ventilation, and Air Conditioning), mechanical engineering and information and communications technologies (ICT).

2.2 Axians

VINCI Energies business units operate at the heart of the digital transformation to help businesses and organizations meet the challenges of transformation and to deliver customized, open, innovative, scalable and sustainable solutions to support their customers. From installing infrastructure to managing data, VINCI Energies technology teams deliver a broad range of expertise covering the entire data life cycle: collection, transmission, storage, processing, analysis, sharing and protection.

Axians is the VINCI Energies brand dedicated to information and communication technology (ICT). Axians specializes in various areas of expertise to support organizations and get the most out of the digital transformation together. Over the years Axians continues to expand their portfolio; from software development to automated data centers and from data analytics to the most advanced telecom solutions.

They advise, design, build and manage from their support, managed and "as-a-service" services. "Always based on trust and transparency and with a good dose of dedication, that is our human touch" (Axians' slogan).

2.3 Company Hierarchy

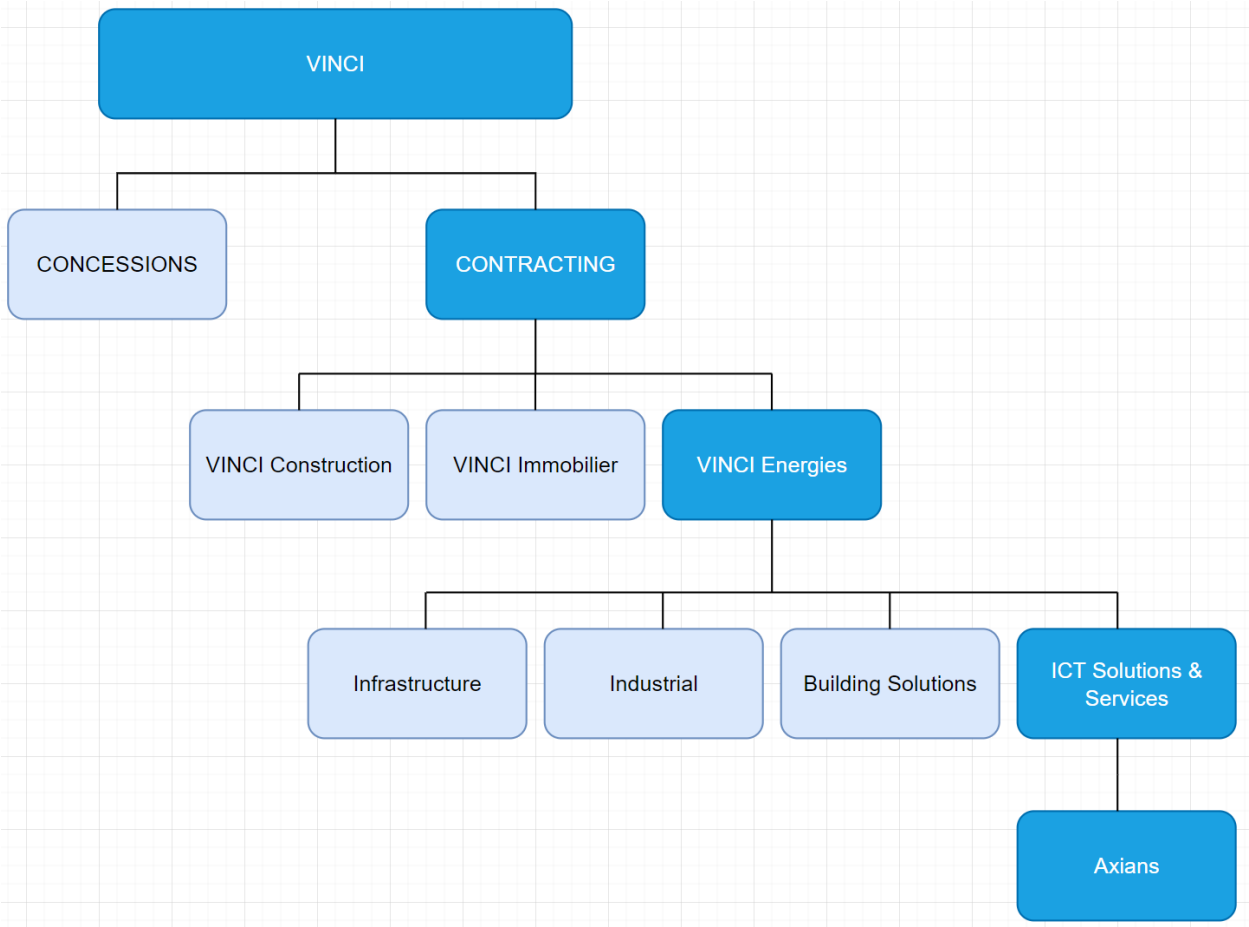

Figure 1: VINCI Organizational Structure

The image above shows the organizational structure of Axians. As there are multiple “Axians” around The Netherlands and the world, for simplicity’s sake the Axians shown above is to be seen as the company which provided the internship assignment (also known as **Axians ICS Groningen)**.

More information on the VINCI Energies brand can be seen in Appendix I: Vinci Energies Brands.

2.4 The Stakeholders

For the duration of the internship project there will be specific key employees that will be known as the stakeholders for the internship project. Throughout the report these stakeholders will be known by their company or project role. Please use the table below as a reference to the stakeholders and their roles.

Name	Company Role	Project Role	Comments
Peter Eek	Project Leader	Company Supervisor	- Report sick days/working remotely - Hardware device(s) requests
Timon Faber	Human Resources (HR) Business Partner	Human Resources (HR)	- Answers any questions regarding company policies - Extensive company knowledge
Novak Ciric	Network Engineer/ Security Officer	Project Supervisor	- Answers any questions related to project - Provides any advice or assist necessary for the project
Martijn Haarman	Senior Network Engineer	Senior Network Engineer	- Provides assistance with knowledge regarding the wishes and requirements of Axians

Aside from the company stakeholders above, there are also stakeholders from the *Hanzehogeschool Groningen.* The stakeholders from the Hanze make sure that the internship project that will be performed is of the appropriate level and also provide help with the documentation process.

Name	Project Role	Comments
Thies Keulen	Internship Supervisor	- Main contact person for documentation-related questions - Provides feedback of the structure of the internship report
Jos Bos	Internship Lecturer	- Second contact person for documentation-related questions - Provides feedback of the structure of the internship report

3. The Project

This chapter will go over the internship assignment project proposed by Axians and any problem(s) that may surround it.

3.1 The Internship Assignment

Axians ICS Groningen are looking for a solution with which they can implement Authentication, Authorization and Accounting (AAA) on their network equipment within their data center. The data center of Axians ICS Groningen is a complex environment, in which there are strict requirements in place that impact both the security and performance of the network. It is therefore the idea that a proposal is made between different possible solutions, in which they would like to receive advice about the best-fitting solution for their data center.

3.2 Problem Definition

At the moment there is insufficient central AAA used to manage the network equipment within Axians' network. The insufficient AAA in Axians' case is the lack of accounting (logging). Aside from that, Axians currently has certain employees using a shared account in order to access certain resources within their data center. These issues can present many dangers for the company.

A potential danger that needs to be addressed when discussing the problem of shared accounts is nonrepudiation. When using a shared account, one cannot prove which particular user took a specific action. Let's say, for example, that someone using a shared IT administrator account logged into the VPN at 3 AM and did something malicious or fraudulent. Because 8 people have access to that password, you cannot prove which of those 8 users performed that action. This prevents you from taking action against the individual who performed the malicious activity, plus having a lack of accounting makes it increasingly difficult in taking any action at all, as there isn't enough information.

So, Axians want someone (an internship student) to advise them of the best possible AAA solution or some other alternative(s) where these problems can be resolved. An AAA will not only bring a solution to the current problem but also introduce scalability and central management. There is also a very strict requirement that must be kept in mind when introducing an AAA solution and that is that It must not impact the performance of the current network and be a financially attractive option.

After mentioning it numerous times, the question now is: what is AAA?

3.3 The AAA protocol

AAA stands for authentication, authorization, and accounting. **Authentication** involves verifying the authenticity of users' or machines' identities, **Authorization** involves granting permissions to read, update configuration files or execute programs and **Accounting** involves logging session statistics and usage information. See the image below.

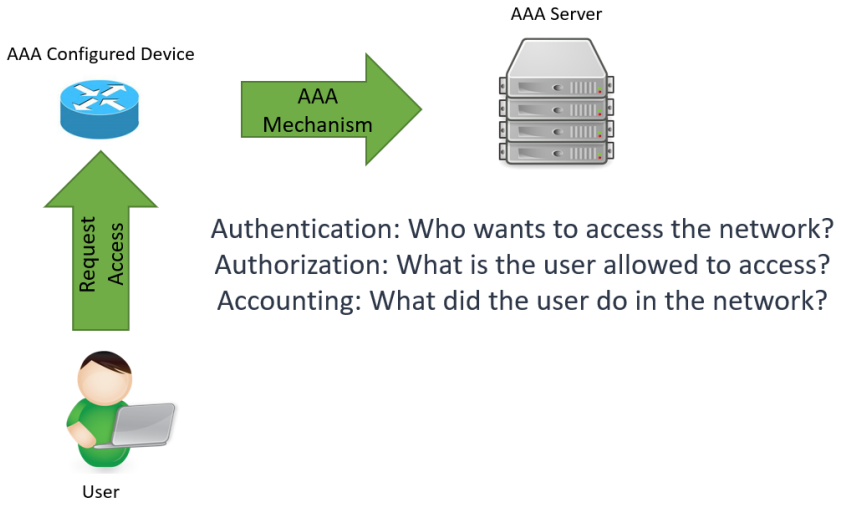

Figure 2: An AAA Example

AAA services are often provided by a dedicated AAA server. AAA protocols are primarily used for network access control (LAN, WAN resources) and network device administration (firewall, routers, switches). AAA protocols were designed as a centralized way to implement access control covering authentication, authorization, and accounting capabilities.

The benefits of implementing AAA include scalability, increased flexibility and control, standardized protocols and methods, and redundancy.

Now that the basics are down in knowing what AAA is and what it's for, the next step is to find out whether Axians have an AAA implemented, which one it is and any issues surrounding it. The reason for this is to better understand what is currently lacking in order to lead to a better AAA solution that Axians may benefit from. To do that there is more information needed on the current environment of Axians.

4. The Current Environment

This chapter will provide information about the current environment of Axians ICS Groningen.

At the start of the internship the first thing to do was to establish a list of questions (Questionnaire) that can be used to ask specific employees (representatives) within Axians in order to gather more information on the current environment to identify any issues that may or may not be present. The question and answers of the interviews can be found at Appendix II: Interview - Martijn Haarman and Appendix III: Interview - Novak Ciric.

Thanks to the interviews done, the following information was confirmed:

- Axians currently uses LDAP as an AAA protocol
- Axians does not have a Single Sign-on service, but they would like to see this implemented with the future solution
- Axians uses various different switches but mainly revolve around HP Switches

4.1 LDAP Authentication

Lightweight Directory Access Protocol, or LDAP, is a software protocol that stores and arranges data to make it easily searchable. The data can be any information about organizations, devices, or users stored in directories. LDAP is the protocol used by servers to speak with on-premise directories.The directory is essentially where all the credentials of the users are saved.

The main purpose of LDAP is to serve as a central hub for authentication and authorization. LDAP helps organizations store user credentials (username/password) and then access them later, like when a user is attempting to access an LDAP-enabled application. That user's credentials stored in LDAP authenticate the user. See the image below.

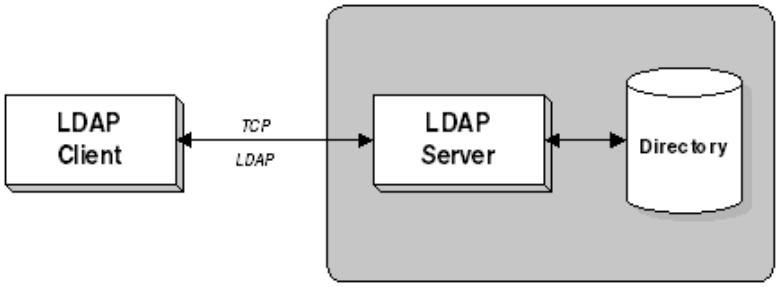

Figure 3: LDAP Overview

LDAP is based on a client-server interaction, as seen on the image above. The client begins a session with the server, called a "binding". The client presents their user credentials which the server can compare against the directory and authorize access based on that user's attributes.

The problem that Axians is currently experiencing is that, while LDAP does provide authentication and authorization, it does not do accounting (logging) which makes it hard for network management. If an incident occurs regarding a password leak, how does Axians figure out who was on the account and what was done on said account? This also confirms what was discussed at *3.2 Problem Definition* about the insufficient central AAA currently in use.

4.2 Single Sign-On

Another thing that was discovered is that Axians does not currently have a Single Sign-On service. This was found out during an interview with some of the network employees and would be something they would like to see when implementing the new AAA solution.

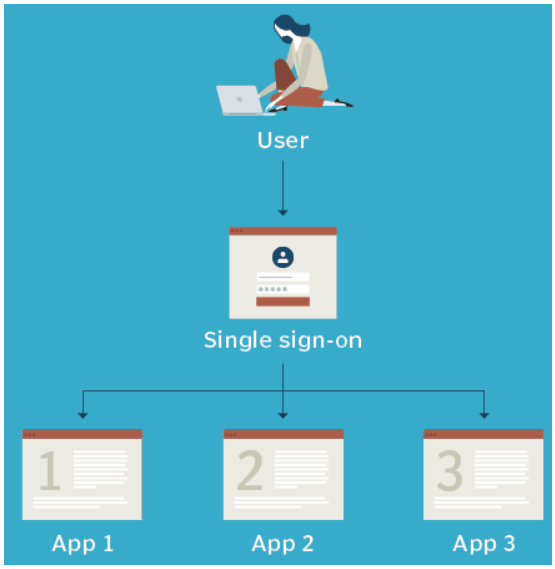

Figure 4: Single Sign-On Overview

Single Sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (see image above). Basically, SSO allows users to access all their applications by signing in with 1 account, this eliminates the need for multiple passwords and increases usability, access and productivity.

The problem with not having SSO is that this makes it difficult for network administrators to keep track of the multiple accounts/passwords needed to access certain devices/ applications. For example, because Axians does not have SSO, the network administrators use a local admin account in order to access their network devices. This makes it difficult for centralized user management, making it difficult to see which particular network employee accessed which specific device. This also correlates with the “shared accounts" issue which was discussed at *3.2 Problem Definition*.

4.3 The Network Devices

As previously mentioned in *3.1 The Internship Assignment*, the network of Axians is quite complex. One of the reasons for the complexity is the fact that there are many different switches within the network, mainly HP-related switches.

4.3.1 HP(E) Switches

Axians is partnered with HP (Hewlett Packard) and is one of the reasons that most of the switches within the network in use are HP switches, more specifically they are HPE (HP Enterprise) Switches. HPe Switches are a very popular option within various companies, the reason for this is because the HPE switches are more financially attractive compared to other more expensive options (e.g. CISCO Switches).

In 2015 Hewlett Packard completed the acquisition of Aruba Networks, a networking company that manufactures network devices (network switches, access points, etc.).

4.3.2 Aruba Switches

The Aruba Switches were created by the Aruba Networks company (formerly known as Aruba Wireless Networks). Because of the partnership between Axians and HP, this gave Axians the availability to start using Aruba Switches. With the numerous functionalities and benefits that the Aruba Switches bring, this has not only made Axians happy but also the clients Axians work with.

Based on the interview done with the senior network engineer, the plan is to replace every switch they currently use to Aruba Switches in the future, this of course will take time in order to be fully realized. Nonetheless, this is something to keep in mind in order to have a better grasp on how the project will be implemented later on.

5. Requirements

This chapter will be discussing the necessary requirements for a successful project. After assessing the possible requirements and discussing this with the project stakeholders, a set amount of requirements have been established, however, now the next step would be how to prioritize these requirements. The prioritization will be done using an often used method when it comes to business projects, which is the MoSCoW method.

What will also be discussed is the necessary requirements that the potential AAA solution would need to comply with in order to become the best possible AAA solution choice.

5.1 MoSCoW method

Prioritization plays a crucial role in any business. The MoSCoW method is a task prioritization framework. It is most effective in situations where many tasks must be prioritized into an actionable to-do list, which makes it the perfect choice to use in this case.

The framework is based on four main categories that give it the name: **Must have** (Mo), **Should have** (S), **Could have** (Co) and **Won't have** (W). The o's in MoSCoW are added to make the acronym pronounceable and are often in lowercase to show they don't stand for anything.

- **Must Have -** As the name would suggest, the *Must have* category displays requirements that must be satisfied in the final implementation for the chosen AAA solution to be considered a success.

- **Should Have -** The *Should have* category represents high-priority item(s) that should be included in the solution, if at all possible.

- **Could Have -** The *Could have* category describes requirements which could be considered but not necessary for the completion of the project.

- **Won't Have -** Lastly, the *Won't have* category represents requirements that will not be implemented, but may be considered for the future

An important note to keep in mind is that the project will be launched in a test environment with the hopes of being used in the live production environment in the future.

With the MoSCoW method in mind, the project requirements can now be prioritized on what is most needed for the successful completion of the project. See image below.

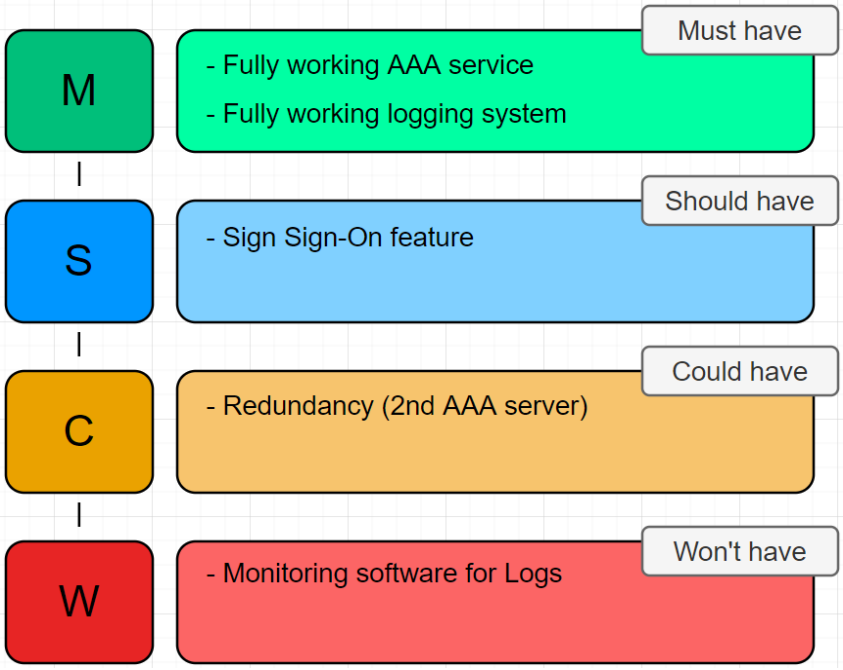

Figure 5: Project Requirements using MoSCoW

The image above provides an overview on the necessary project requirements using the MoSCoW method. The reasons why these particulair requirements have been chosen to be used within their respective MoSCoW categories can be found below.

MoSCoW	Description
Must have	The main purpose for this project is to realize a fully functional AAA solution. So, the absolute “Must have” requirements are: a fully working AAA server for authentications and a log server that will receive logging from said AAA server.
Should have	As mentioned before, Axians do not have a Single Sign-On (SSO) feature in place but after the conducted interviews around the workplace, it seems something that the employees really look forward to seeing happen with the future AAA solution.
Could have	The standard best practice when talking about implementing a AAA server is having a backup (redundancy) in case the first one goes under. While a 2nd AAA server is not critical for the successful project completion, if there is sufficient time left, this requirement will also be implemented.
Won’t have	Thanks to the interviews conducted with the network employees, It was found out that Axians already has a monitoring software in place. Therefore, it is not necessary to set up a new monitoring software as the future logging for the chosen AAA solution can be connected with their current monitoring software.

5.2 Requirements for a successful solution choice

In order to come to a successful decision (which will be done by Axians) on one of the potential AAA solutions, there needs to be a set amount of requirements established in which a specific potential AAA solution needs to comply with in order to become the best possible AAA solution choice.

After performing extensive research on what the potential AAA solutions needs to comply with and discussing this with network and sales employees within Axians, the requirements have been established. The discussions between the network and sales employees helped fill in knowledge that was potentially lacking and cover any basis that might have been missed. The overview of the requirements can be seen in the image below.

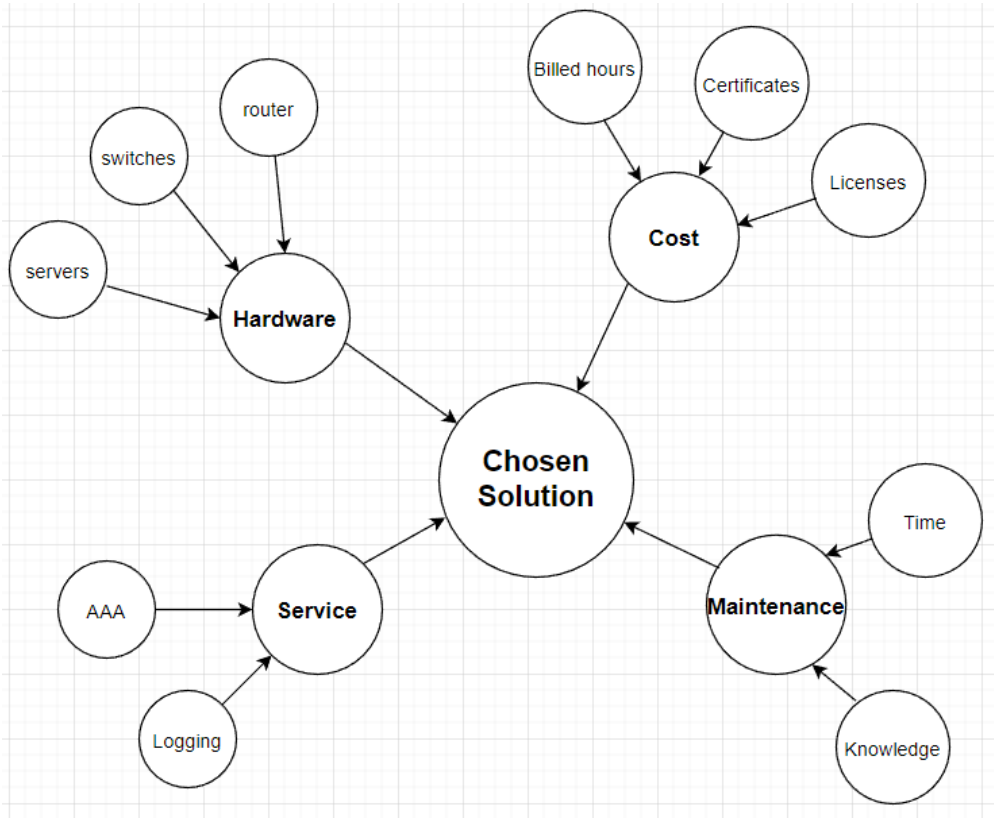

Figure 6: Requirements Overview

The requirements have been established with 4 main categories taken into account.

Requirement	Description
Hardware	There are compatible hardware devices needed in order to implement the chosen solution
Service	The chosen solution must perform authentication, authorization and provide logging (AAA) to a logging system (log server) and affect the network system's performance as less as possible
Cost	The cost of the potential solution must be financially attractive in order to be seen as a possible choice. This does not mean it has to be free but, even if the potential solution has a cost it should still be beneficial to the internship company (Axians)
Maintenance	The chosen solution must be able to be properly maintained in the event of a potential incident. This means that there has to be a designated employee with knowledge of the solution.

These requirements needed to be thorough in order to arrive at the best possible scenario with little to no surprises. The list of requirements can be found at Appendix IV: List of Requirements. The colors for the requirements were inspired by the Axians company colors.

The requirements were given a short abbreviation in order to easily refer to a specific requirement if necessary in the future. For example, when a specific requirement is called "R01", the R refers to *Requirement* and the 01 refers to *the number* of that specific requirement.

6. Potential AAA Solutions

This chapter will go over the potential AAA solutions in order to figure out which one would be the better choice in benefitting Axians, in order to solve the current problem. This is an important step in order to bring a specific potential solution over to the design-phase to further plan out how the project will be done. The reason these potential solutions were chosen is that they are proper AAA-specific solutions while also satisfying the established requirements in 5. Requirements.

6.1 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an open-standard AAA protocol that uses UDP port 1812 for authentication and UDP port 1813 for accounting. Essentially, RADIUS is a protocol that determines whether or not a user can access a local or remote network (authentication), establishes what sort of privileges they're allowed on that network (authorization) and then records the activity of the user (accounting) while they're connected to the network resource. The beauty of RADIUS is that it centralizes these AAA functions across networking infrastructure and locations.

RADIUS enables a company to maintain user profiles in a central database that all remote servers can share. Having a central database provides better security, enabling a company to set up a policy that can be applied at a single administered network point. A central database also makes it easier to track usage for billing for the network access or internet service provider and for keeping network statistics.

6.1.1 Basic Overview

When devices (clients) connect on a Network Access Server (NAS), the NAS device will send an *access-request* message to the AAA server in order to check the credentials. In response to the access request of the client, the AAA server will provide an *access-accept* message to the client if the credentials are valid and *access-reject* if the credentials do not match. In order to understand this in simpler terms, let's first talk about the components of RADIUS. RADIUS consist of 3 main components:

1. Client/Supplicant
The device/user seeking access to a network

2. Network Access Server (NAS)
The gateway between a user and a network (e.g. network switch or router)

3. RADIUS Server
The Authentication server that ensures the user is allowed to access the network with the proper permission levels. This server can also provide accounting functions for the purposes of billing, time tracking, and device/connection details.

6.1.2 The RADIUS process

Now, let's get a little deeper into those three primary components of the RADIUS protocol to understand exactly how it all works. See the image below.

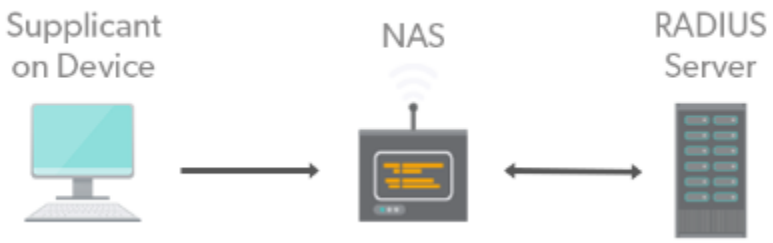

Figure 7: The RADIUS components

1. Supplicant: The supplicant is generally software built-in or installed ad hoc on a user's operating system that passes information about a user (username, password, etc.) to a second component, the network access server (NAS), along with an *access-request* query. An *access-request* query is just that, a request for access from a client to a server to utilize a resource like a network.

2. Network Access Server: In the client/server architecture, the NAS acts as the client. NAS devices can be network switches, routers, VPNs, or wireless access points (WAPs), among other things. The client/supplicant asks the server to determine if a user is allowed access to a particular resource — also called authentication.

3. RADIUS server: The RADIUS server waits for requests from NAS devices. The benefit of RADIUS is that no matter what type of NAS you're trying to connect to, the RADIUS server centralizes authentication and simplifies the process.

Once the server receives the access request, it either verifies the user's identity via an onboard user database or delegates the information to an identity provider.

If the match is made, then the server accepts the user by sending an *access-accept* message back to the NAS. If the match is not made, the user is rejected through an *access-reject* message. At the end of the transaction, the NAS issues accounting data to the RADIUS server which documents the transaction and allows for the storage or forwarding of transactional data.

For a more in depth view on the RADIUS protocol, you can check out the RFC 2138, which essentially outlines the standard. The "RFC" stands for Request for Comments, which covers many aspects of the computer networking world.

6.1.3 Pricing

The cost of the RADIUS protocol depends on the different types of RADIUS software applications that will be used. In order to talk about the costs, the different types of the RADIUS services must first be listed. After performing some research on this specific topic, it was found out that there are 3 potential choices for the RADIUS protocol. These RADIUS services can be seen in the image below.

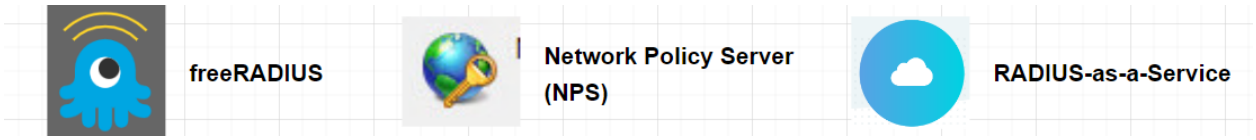

Figure 8: RADIUS services

freeRADIUS

freeRADIUS is an open-source implementation of the RADIUS protocol that runs on Linux-based operating systems (i.e. Ubuntu, CentOS, etc.).

Requirements for running this solution are:

- A server running a Linux-based operating system
- A good understand of the Linux-based operating systems
- A designated employee that needs to keep up with any changes made or needing to be made in the freeRADIUS server.

As the name suggests, there is **no cost** with freeRADIUS but there are other costs and considerations not included with this price, for example:

- The server cost
- The billable hours for the implementation (depending on the knowledge of the employee this can be high or low)
- Maintenance cost (since this an open-source, every update has a chance of changing how the service works, which makes this something needing to be constantly checked by a designated employee)

Network Policy Server (NPS)

NPS is a windows feature that can be configured within a Windows Server operating system. Since most companies already have Windows Servers, the NPS could be installed in one of those servers without the need of a completely separate server.

Requirements for running this solution are:

- A server running the Windows Server operating system
- A good understanding about Windows-based operating system

There is **no cost** for the NPS solution as it is a feature built into “Server Manager” a software application that runs on Windows Server. The only additional cost would be the billable hours on how long it would take a designated employee to set up. If the company desires the NPS to be

installed separately instead of on an existing server, then that server cost should also be taken into account in the total cost.

RADIUS-as-a-Service

Radius-as-a-Service is as the name suggests, a RADIUS service that is provided by an external company. The general idea is that the service provider will be the one that will handle all of the installation, configuration and maintenance. Most service providers also provide customer support which helps with potential troubleshooting needs.

Requirements for running this solution depends highly on the company (i.e Axians) needs and the specific company chosen to provide the RADIUS service. The general idea is that everything will be running on the servers of the provider, unless the desire is to have the servers locally and only let the provider have control on the AAA.

There are several prices offered at several different price points, both subscription based or upfront models. The prices vary from **$13 per month** to up to **$750+ per server**, plus additional servicing fees. These prices may also vary per region.

6.2 Diameter

Diameter is a protocol that was developed in 1998 as a direct response to overcome the limitations of RADIUS. The diameter of a circle is twice the radius, which is where the protocol derives its name. Diameter is also a protocol for Authentication, Authorization and Accounting. It is mostly used for IMS (IP Multimedia Subsystem) architectures.

Diameter includes numerous enhancements in all aspects, such as error handling and message delivery reliability. It extracts the essence of the AAA protocol from RADIUS and defines a set of messages that are general enough to be the core of the Diameter base protocol. The various applications that require AAA functions can define their own extensions on top of the Diameter base protocol, and can benefit from the general capabilities provided by the Diameter base protocol.

6.2.1 Basic Overview

Diameter is designed as a Peer-To-Peer architecture, and every host who implements the Diameter protocol can act as either a client or a server depending on network deployment. So the term “Diameter node” is used to refer to a Diameter client, a Diameter server, or a Diameter agent. The following image shows a simple overview between a Diameter client and server.

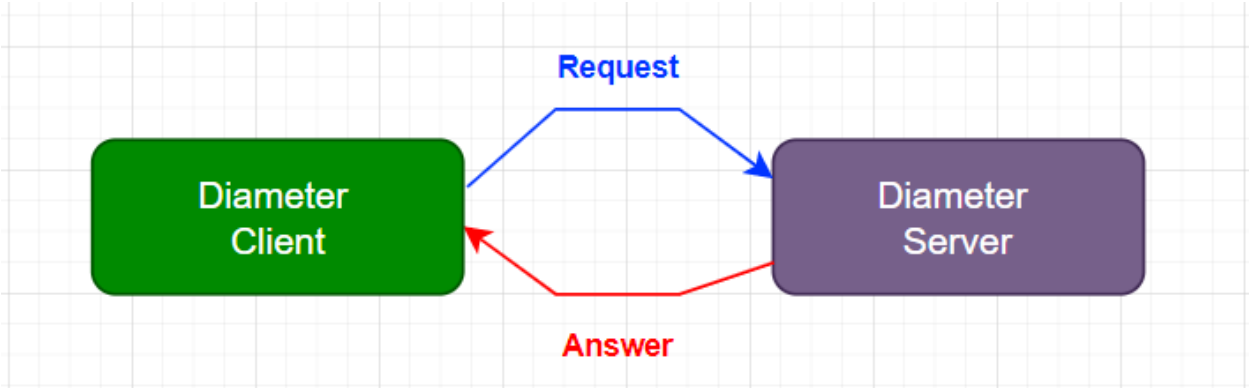

Figure 9: Basic Diameter Overview

The Diameter node that receives the user connection request will act as the Diameter client. After collecting user credentials, such as username and password, it will send an access request message to one Diameter node serving the request. For simplicity, we assume it is the Diameter server. The Diameter server then authenticates the user based on the information provided. If the authentication process succeeds, the user's access privileges are included in the response message and sent back to the corresponding Diameter client. Otherwise, an access reject message is sent.

6.2.2 Diameter Agents

Although the architecture just described looks like a traditional client-server architecture, a node acting as the Diameter server for some requests might actually act as a Diameter client in some other situations; the Diameter protocol is actually peer-to-peer-based architecture in a more generic sense. There is also a special Diameter node called Diameter agent which is defined in the Diameter protocol. Typically, there are three kinds of Diameter agents:

Relay Agent

A Relay Agent is used to forward a message to the appropriate destination, depending on the information contained in the message. The Relay Agent is advantageous because it can aggregate requests from different realms (or regions) to a specific realm, which eliminates the burdensome configurations of network access servers for every Diameter server change.

Figure 10: Relay Agent, Diameter

Proxy Agent

A Proxy Agent can also be used to forward messages, but unlike a Relay Agent, a Proxy Agent can modify the message content and, therefore, provide value-added services, enforce rules on different messages, or perform administrative tasks for a specific realm. Figure 8 shows how a Proxy Agent is used to forward a message to another domain. If the Proxy Agent will not modify the content of an original request, a Relay Agent in this scenario would be sufficient.

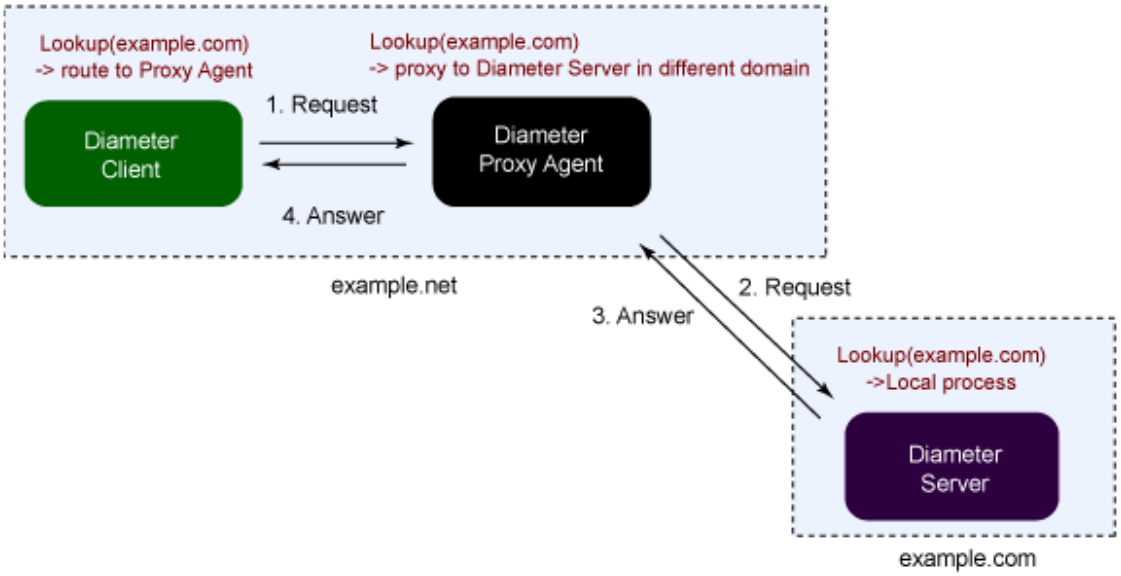

Figure 11: Proxy Agent, Diameter

Redirect Agent

A Redirect Agent acts as a centralized configuration repository for other Diameter nodes. When it receives a message, it checks its routing table, and returns a response message along with redirection information to its original sender. This would be very useful for other Diameter nodes because they won't need to keep a list routing entries locally and can look up a Redirect Agent when needed. Figure 9 illustrates how a Redirect Agent works. The scenario below is basically identical to the one in Figure 8, but this time the Proxy Agent is not aware of the address of the contacting Diameter node within example.com. Therefore, it looks up the information in the Redirect Agent of its own realm to get the address.

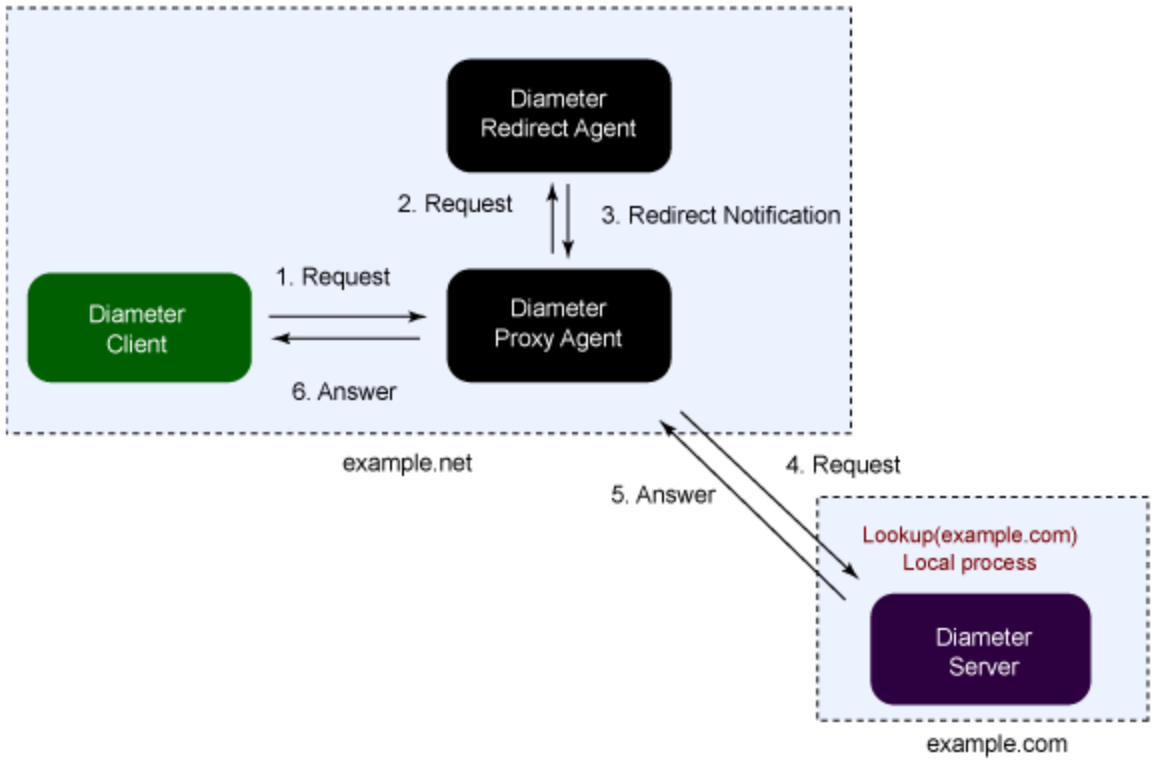

Figure 12: Redirect Agent, Diameter

For a more in depth view on the Diameter protocol, you can check out the RFC 6733.

6.2.3 Pricing

The cost of the DIAMETER protocol depends on the different types of DIAMETER software applications that will be used. After performing some research on this specific topic, it was found out that there is only one potential service choice for the DIAMETER protocol. This service can be seen in the image below.

Figure 13: DIAMETER service

freeDIAMETER

freeDIAMETER is an open source DIAMETER protocol implementation that runs on Linux-based operating systems (i.e. Ubuntu, CentOS, etc.).

Requirements for running this solution are:

- A server running a Linux-based operating system
- A good understand of the Linux-based operating systems

- A designated employee that needs to keep up with any changes made or needing to be made in the freeDIAMETER server.

As the name suggests, there is **no cost** with freeRADIUS but there are other costs and considerations not included with this price, for example:

- The server cost
- The billable hours for the implementation (depending on the knowledge of the employee this can be high or low)
- Maintenance cost (since this an open-source, every update has a chance of changing how the service works, which makes this something needing to be constantly checked by a designated employee)

6.3 TACACS+

Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for network access control through a centralized server. The original TACACS protocol, which dates back to 1984, was used for communicating with an authentication server, common in older UNIX networks.

Cisco created a new protocol called TACACS Plus (TACACS+) as a proprietary standard in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services. TACACS+ has largely replaced its predecessors.

In simpler terms, TACACS+ is a security protocol used in the AAA framework to provide centralized authentication for users who want to gain access to the network.

6.3.1 Basic Overview

Like RADIUS, TACACS+ is also a Client/Server protocol. Depending on the different AAA duties, different messages are used between the Server and Client. One side is the Client side and the other is the Server side. The client of a TACACS+ server is either called a Network Access Device (NAD) or a Network Access Server (NAS). TACACS+ has a very similar topology as RADIUS, however, works slightly differently. See image below.

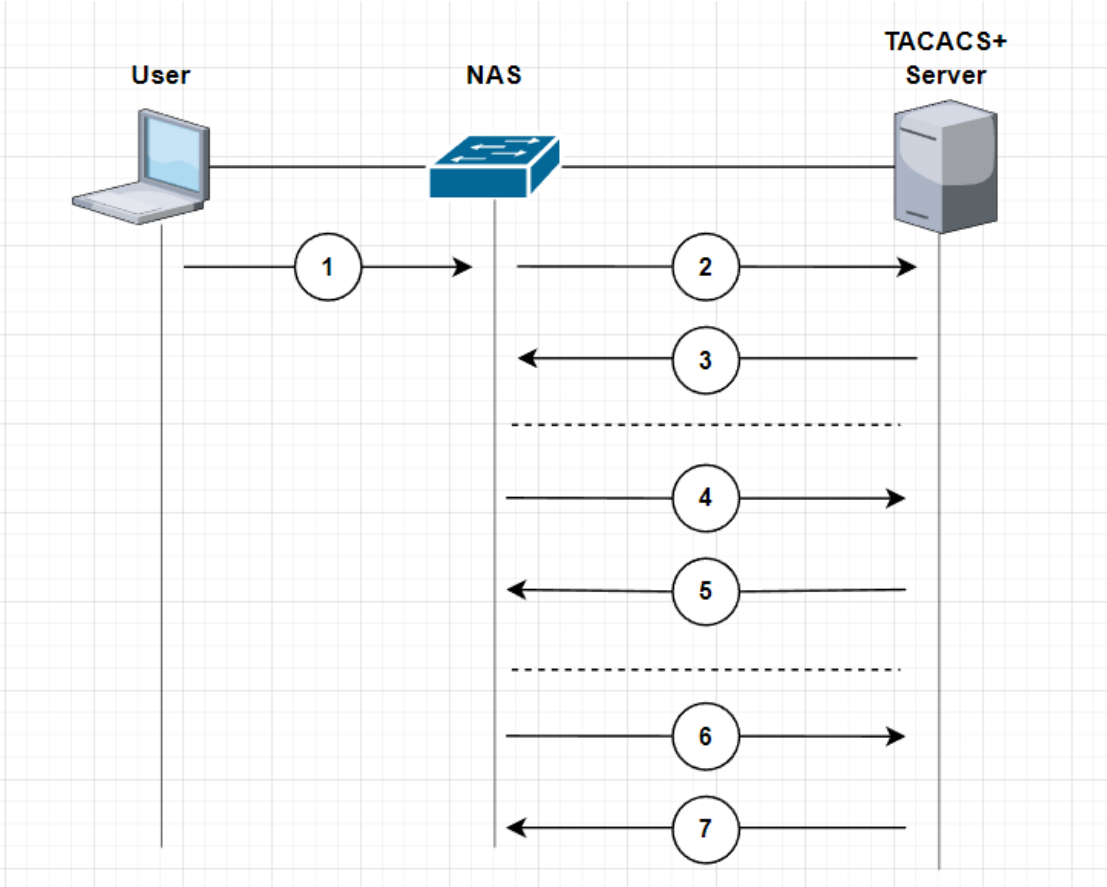

Figure 14: The TACACS+ process

1. The NAS receives the connection request from the user
2. The first packet type, **START,** is sent to the TACACS+ server
3. The TACACS+ server then sends the **REPLY** packet back to the AAA client to ask the client to get the username
4. The NAS sends a **CONTINUE** packet to the TACACS+ server with the username provided by the user
5. The TACACS+ server then sends the **REPLY** packet back to the NAS to ask the client to get the password
6. The NAS sends a **CONTINUE** packet to the TACACS+ server with the password provided by the user
7. The TACACS+ server then sends the **REPLY** packet back to the AAA client to indicate a pass or fail of authentication

For a more in depth view on the TACACS+ protocol, you can check out the RFC 8907,which essentially outlines the standard.

6.3.3 Pricing

The cost of the TACACS+ protocol depends on the different types of TACACS+ software applications that will be used.In order to talk about the costs, the different types of the TACACS+ services must first be listed. After performing some research on this specific topic, it was found out that there are 3 potential choices for the TACACS+ protocol. These services can be seen in the image below.

Figure 15: TACACS+ services

TACACS+ (.net)

TACACS.net is the name of the company that offers TACACS+ services for their clients/consumers. Depending on the payment plan of TACACS.net, the cost and services may vary.

The requirements for choosing TACACS.net as a provider is to have the server(s) available where the TACACS+ solution will be installed/configured. Any additional or specific requirements depend on the agreement made with the provider.

From the TACACS.net company website there are 2 choices of payment plans available. These payment plans can be seen below.

Basic Plan

This package provides:

- Basic installation, configuration and verification
- Q&A
- Configuration walkthrough
- Helpful Tips

The cost of this plan is **$1.795 per server** (may vary per region)

Premium Plan

This package provides:

- Remote installation and configuration + 1 Year Maintenance and Support Subscription
- Higher and unlimited Device & User thresholds to scale any network
- Telephone support hotline
- Email support with priority response
- Priority ticket system
- Security updates and patches
- 24/7/365 Support with priority response available

The cost of this plan is **$4.495 per server** (may vary per region)

TACACS+-as-a-Service

TACACS+-as-a-Service is as the name suggests, a TACACS+ service that is provided by an external company. The general idea is that the service provider will be the one that will handle all of the installation, configuration and maintenance. Most service providers also provide customer support which helps with potential troubleshooting needs.

Requirements for running this solution depends highly on the company (i.e Axians) needs and the specific company chosen to provide the TACACS+ service. The general idea is that everything will be running on the servers of the provider, unless the desire is to have the servers locally and only let the provider have control on the AAA.

There are several prices offered at several different price points, both subscription based or upfront models. The price may differ depending on the chosen provider. In order to get a rough estimate on the cost, a specific company was chosen to serve as an example. This company is known as “Portnox” and the cost of the service starts at **€236 per month.**

CISCO Identity Services Engine (CISCO ISE)

CISCO ISE is a security policy management platform that provides secure network access to end users and devices. Administrators can use Cisco Identity Services Engine to control who has access to their network and ensure authorized policy-compliant devices are being used.

Requirements for running this solution are:

- A CISCO specific server (e.g. CISCO Secured Network Server (SNS) 3500/3600 series) or you can also run this as a virtual machine on VMware.
- A CISCO ISE license

Due to the fact that there are a lot of models each with a specific license type, it is difficult to have one static price. With the understanding of what the AAA project requires, a specific license was chosen as an example.

The Base License

This license provides:

- User visibility
- Enforcement features (AAA and 802.1x)
- Guest (Hotspot, Self-Reg)
- Easy connect (PassiveID)

The cost of this plan depends on the amount of devices needed. The more devices the higher the cost.

- **CISCO ISE 100 EndPoint Base License:** $500
- **CISCO ISE 250 EndPoint Base License:** $1.250
- **CISCO ISE 500 EndPoint Base License:** $2.500

As it is very dependent on what the company needs, the cost of the server and any extra services were not included in the above mentioned costs. The prices also may vary per region.

6.4 ClearPass

Aruba ClearPass is not like the other protocols, it is a *policy management platform* that when implemented helps to effortlessly onboard new devices, grant varying access levels, and keep the networks secure. As the name implies, Aruba ClearPass is a product made by Aruba Networks, It has a web-based interface that simplifies configuration and troubleshooting

While being specifically a policy focused management platform, ClearPass also provides authentication, authorization and accounting through its many different features/services. Besides AAA, ClearPass also provides specific built-in applications in order to make a network more secure. Some examples of these applications are the following:

- **ClearPass Guest** is basically a way to automate and securely bring guests on to the network while collecting information from them (accounting). The reason it collects information is of course for security purposes This application can work with any company, any device or network.

- **ClearPass Onboard** is meant for BYOD (Bring Your Own Device) and it is a way of automating bringing a device onto the network and giving it all the necessary configurations that the device would need. This is clearly a way better option than the old way of needing an IT admin to do this with every single device.

- **ClearPass OnGuard** ensures the health of the device before giving them network access. For example, when a device connects to the network OnGuard checks if the device is running on a predefined (configured) “level of health” which complies with ClearPass’s policies. If so then provides connection, if not then OnGuard blocks the device’s access to the network resources.

6.4.1 Basic Overview

How ClearPass works is through a relatively simple three-step plan:

1. Identify
2. Enforce
3. Protect

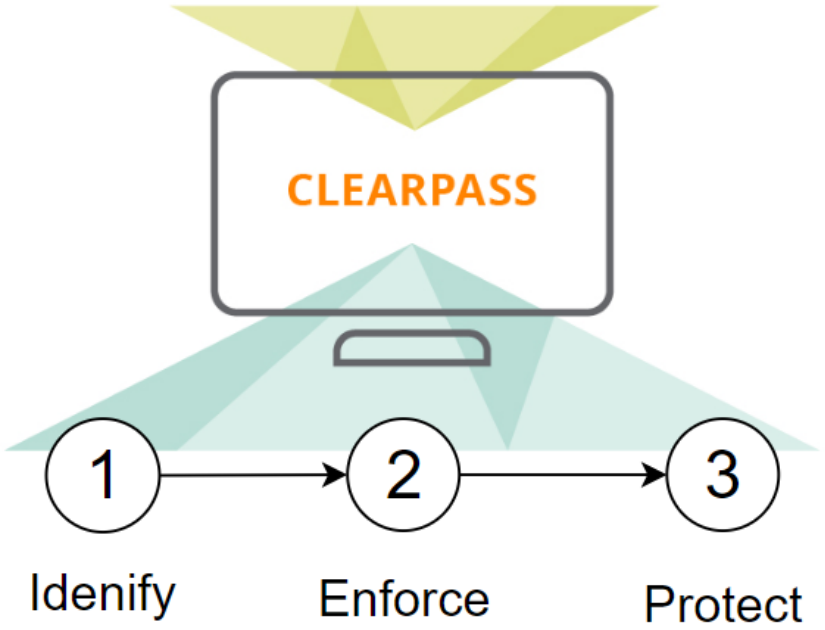

Figure 16: ClearPass 3-step plan

1. Identify

With this new demand for network access, the burden on anIT department has increased exponentially and it's not just laptops and smartphones that should be on the radar. IoT devices, printers, and even surveillance cameras are connecting to companies' wireless networks.

ClearPass helps identify which devices are being used, how many are connected to the network, where they're connecting from, and which operating systems are supported. It provides continuous visibility into changes on the network, including which devices are connecting and disconnecting.

When a device-specific information is needed, ClearPass can easily identify a device's:

- Type and model name
- MAC address
- IP address
- NIC vendor
- Operating System(OS) and version number
- VLAN

2. Enforce

Enforcing network policies can pose a huge challenge to IT departments. When an employee wants to add a new device to the network, they often have to go through extensive IT protocols. They may even need someone from IT to walk them through the process.

ClearPass enforces policies during the onboarding of new devices without any involvement from the IT department whether it's a laptop, smartphone, or security camera.

The IT admins will simply need to establish the foundation of security and write rules that define:

- Who can onboard a device
- The type of device users can onboard
- How many devices each user can onboard

These can then enforce access in a number of ways. By using the built-in portal, or by using the more secure and preferred method that uses encryption in the *authentication process*. After devices are granted access, ClearPass uses active and passive profiling methods to monitor your network and keep it safe.

3. Protect

The health of individual devices connected to a network is an essential component to network security. With *ClearPass OnGuard* (as mentioned previously) the IT admins can define the "level of health" a device must have in order to gain network access.

The ClearPass OnGuard automatically conducts critical endpoint health checks and "posture assessments" to ensure that all devices are compliant with the company's predefined requirements. It also works for both wired and wireless networks.

ClearPass also offers a variety of third-party integrations. These integrations empower one to implement dynamic policy controls and threat remediation (eliminates threats). They also provide a real-time insight into the activity on a network, equipping one to identify and address any threats that may present themselves.

6.4.2 Pricing

Like the previously mentioned CISCO ISE, the cost for ClearPass depends on the chosen license. As ClearPass is a policy management platform and not a specific protocol with different options, it will be the sole solution in this case. See the image below.

Figure 17: Aruba's ClearPass

Requirements for running this solution are:

- A HPE/Aruba specific server which are sold as Small (C1000), Medium (C2000) and Large (C3000) sizes hardware appliances
- An Aruba ClearPass license

Due to the fact that there are a lot of models each with a specific license type, it is difficult to have one static price. With the understanding of what the AAA project requires, a couple of licenses were chosen as an example.

Enterprise License for Aruba Clearpass Policy Manager (1-Year)
Total endpoints: 100
Price: **$3,1113.34** (may vary per region)

Enterprise License for Aruba Clearpass Policy Manager (1-Year)
Total endpoints: 500
Price: **$14,834.14** (may vary per region)

These mentioned prices do not include the server needed to operate ClearPass as this is dependent on the company's needs. ClearPass has always been known to be one of the most expensive AAA solutions, this is of course because of the extensive features it is able to perform and is usually considered among larger companies.

Conclusion

The analysis is now fully established with the help of the conducted research interviews. The information gathered here will help in building the next phase called the design-phase.

The information of the organization (Axians in this case) that provided the internship assignment is written down in order to give deeper insight into the company. The information also contains the company hierarchical structure while also identifying the relevant stakeholders for the project.

Based on the conducted interviews and discussions held with the stakeholders, information on the current situation was gathered, listed and analyzed. Afterwards, a list of wishes/requirements was established. These requirements are necessary in order to come to a solution choice on the future potential solutions. Lastly, the potential solutions were researched and fully detailed listed in order to compare them later on in the design-phase.

Sources and Literature

Axians | “The best in digital transformation” | Retrieved 8 June 2022 from https://web.axians.nl/

F5 (2022) | “Diameter Protocol” | Retrieved 14 June from https://www.f5.com/services/resources/glossary/diameter-protocol#:~:text=The%20Diameter%20Protocol%20provides%20authentication,%2C%20and%20LTE%2F4G%20networks

Jeffrey Liu, Steven Jiang, and Hicks Lin (2006) | “Introduction to Diameter” | Retrieved 14 June from https://web.archive.org/web/20170705050231/https://www.ibm.com/developerworks/wireless/library/wi-diameter/

ProductPlan | ”MoSCoW Prioritization” | Retrieved 21 June 2022 from https://www.productplan.com/glossary/moscow-prioritization/

Sakshyam Shah (2022) | “What is AAA Security?” | Retrieved 8 June 2022 from https://goteleport.com/blog/aaa-security-protcols-for-network-access/

VINCI Energies | “”VINCI Energies In The Netherlands” | Retrieved 8 June 2022 from https://www.vinci-energies.nl/en/

Wikipedia (2022) | “RADIUS” | Retrieved 15 June 2022 from https://en.wikipedia.org/wiki/RADIUS

Wikipedia (2022) | “TACACS” | Retrieved 18 June 2022 from https://en.wikipedia.org/wiki/TACACS

Wikipedia (2022) | “Aruba Networks” | Retrieved 28 June 2022 from https://en.wikipedia.org/wiki/Aruba_Networks

Appendix

Appendix I: Vinci Energies Brands

Appendix II: Interview - Martijn Haarman

- Is the current problem for all branches? only Groningen?

As far as we know, this problem exists only on network infrastructure used and managed by this BU (Axians ICS Groningen). This excludes the office infrastructure managed centrally by Axians, customer infrastructure (we may want to apply the solution in the future), and infrastructure used and/or managed by other BU's (not visible to us)

- How many people/employees does the current problem affect?

In theory all employees could be affected, as they all use the network infrastructure in one way or another, and are thus affected by incidents resulting from credential exposure (security) or configuration errors (availability).

In more practical terms the problem mainly affects those who manage the network infrastructure (network administrators) and those responsible for security (security officer, security team) and operations (management). This limits the number to ~10

- Is there a AAA currently in use? Which?

Currently there is limited use of AAA for management access to (network-)devices that support direct LDAP(S) communication with our domain controllers. For the most part this will be limited to Fortinet devices (firewalls, mail appliances), but there may be a couple of other devices configured this way.

- How many/What type of devices does the potential AAA solution have to work with?

For now (we may want to extend the scope/functionality in the future) we are looking for a AAA management access solution for the following devices:

- *Switches for non-office use (provisioning, testing, development, etc.) at our Office location. For the most part these are access switches with a low change frequency and relatively low risk score (no customer equipment or central infrastructure connections).*
  Total number of switches approx. 15
- *Network infrastructure switches at our data center locations. This includes most switches at these locations, excluding out-of-band infrastructure and CPE's. These are core-, aggregation-, and access-switches with a high change frequency and high risk score (customer equipment and central infrastructure connected).*
  Total number of switches approx. 40

Both location types use a wide variety of switch brands and types:

- *ArubaOS (formerly HPE Procurve)*
- *HPE Flexnetwork (formerly H3C/Comware) versions 5 and 7*
- *ArubaOS-CX*

- Are there any specific wishes that you would like to see with the potential solution?

Must have:

- *Applicable to other network device types (mainly Fortinet) in the future*
- *Integration with existing AD domain (Windows Active Directory)*
- *Documentation*

Should have:

- *Clear and comprehensible management interface*
- *Troubleshooting tools*
- *Audit logging*
- *Single solution(SSO) for all switch types*

Nice to have:

- *Possibility to use for NAC*
- *Integration with central monitoring tool (Zabbix)*

- How does it work in the event of an incident? is there no logging?

Currently, all (most) network devices send basic logs to a central logcollector, however most device types do not log configuration changes. Also, since a single local admin account is used on most devices, we have no way of auditing changes, even if they are logged.

- What happens at a password leak? Is Activity tracking possible?

See previous answer

Appendix III: Interview - Novak Ciric

- Is the current problem for all branches? only Groningen?

The scope for this project is limited to the business unit "Axians ICS Groningen", which is located at the Zeewinde 5 in Groningen. Axians' business units are autonomous, which is why all other Axians establishments are not within the scope for this project.

- How many people/employees does the current problem affect?

The current problem affects the Network team (they will use the solution to log in), security employees (they will want the AAA features for security reasons and ISO27001 compliance) and management (since management is ultimately responsible for the business unit). An account manager or a Windows Engineer is not directly affected by the current problem.

At the time of writing that would be approximately 15 employees.

- Is there a AAA currently in use? Which?

There is currently no AAA solution being used in the production networking environment from Axians ICS Groningen.

- How many/What type of devices does the potential AAA solution have to work with?

The solution should work with all of the networking equipment in use by Axians ICS Groningen:

- *ArubaOS*
- *ArubaOS-CX*
- *Comware 5*
- *Comware 7*
- *ProCurve*
- *FortiGates*

- Are there any specific wishes that you would like to see with the potential solution?

Aside from the originally provided requirements that Axians is looking for, I personally would like to see that the new product comes with a Single Sign-On feature. This will make it essential for network administration and solve the "shared accounts" we are currently facing on the network devices.

- How does it work in the event of an incident? is there no logging?

All network devices send their logs to a log-server. When an incident occurs these logs will be consulted. However, there is no AAA-specific logs

- What happens at a password leak? Is Activity tracking possible?

The actions which will be taken depend on where the password has been leaked. If the password was leaked to an external party, the password will be changed ASAP and we will start a "root cause analysis" to inspect the incident.

Activity tracking is not possible on all devices, since some devices use shared accounts. We also have to rely on regular logging, so there is no direct way to link a user to certain executed commands on the devices.

Appendix IV: List of Requirements

Requirement	R01
Name	AAA Server
Type	Hardware Requirement
Description	There needs to be a server present that will act as the AAA Server, regardless of the Operating System(OS).

Requirement	R02
Name	Log Server
Type	Hardware Requirement
Description	There needs to be a server present that will act as the Log Server, this is where all the logs from the AAA server will be received. The Operating System (OS) must be Linux-based as specifically requested.

Requirement	R03
Name	Network Switches
Type	Hardware Requirement
Description	There needs to be network switches in place that will act as if they were the ones being used in the live production environment. These switches will be used to check if they are compatible with the chosen AAA. The specific amount of switches needed will be discussed in the design report.

Requirement	R04
Name	Router
Type	Hardware Requirement
Description	There needs to be a router in place that will act as the gateway between the AAA server and the network switches. The router also needs to be compatible with the potential solution choice.

Requirement	R05
Name	AAA - Authentication
Type	Service Requirement
Description	The AAA must be able authenticate the user by checking the credentials of the user and comparing this with the stored credentials. If the credentials pass then accept the request, if not, deny.

Requirement	R06
Name	AAA - Authorization
Type	Service Requirement
Description	The AAA must Authorize users by giving them their respective permissions/roles retrieved from the User Database (in the Active Directory)

Requirement	R07
Name	AAA - Accounting
Type	Service Requirement
Description	All the AAA events must be logged and sent to the Log Server. This is for the network employees to use for activity tracing in case of a security incident and is also a main requirement for the project

Requirement	R08
Name	Switch - AAA
Type	Service Requirement
Description	The network switches must be able to be configured with the chosen AAA protocol in order to authenticate/authorize the user connecting to the switch and then forwards all the logs (accounting) to the Log Server

Requirement	R09
Name	Switch - Single Sign-On
Type	Service Requirement
Description	In order to have an SSO service, the switches must be able to be accessed using employees' own accounts and not a local shared account (i.e local admin). This is mainly for network employees needing to manage the network switches.

Requirement	R10
Name	Router - AAA
Type	Service Requirement
Description	The router must be able to be configured with the chosen AAA protocol in order to authenticate/authorize users connecting to the possible WiFi network and then forwards all the logs (accounting) to the Log Server