Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

EANTC
EUROPEAN ADVANCED NETWORKING TEST CENTER

Praxistransferbericht II (IT2311)

Implementierung eines Wireless Local Area Networks

vorgelegt zum 22.08.2023

Name:	Oskar Mansfeld
Matrikelnummer:	77220696293
Fachbereich:	FB2: Duales Studium - Technik
Studiengang:	Informatik
Studienjahrgang:	2022
Semester:	SoSe 2023
Ausbildungsbetrieb:	EANTC AG
Betreuerin Hochschule:	Lara Maria Stricker
Betreuerin Unternehmen:	Gabriele Schrenk
Wortzahl:	2173

Von der betrieblichen Betreuung zur Kenntnis genommen:

Gabriele Schrenk

Oskar Mansfeld

Zusammenfassung

Diese Arbeit beschäftigt sich mit der Implementierung eines neuen Wireless Local Area Networks (WLAN) für die Büroräumlichkeiten des European Advanced Networking Test Centers (EANTC). Über das WLAN soll für die mobilen Endgeräte und Laptops der Mitarbeitenden und Gäst:innen eine Verbindung zum Internet und zu verschiedenen internen Diensten bereitgestellt werden.

Dazu wurde zuerst eine Anforderungsanalyse durchgeführt und das vorhandene Netzwerk analysiert. Anschließend wurde ein Entwurf erstellt, wie das WLAN im Netzwerk des EANTC eingebunden werden kann und dieser dann abschließend umgesetzt.

Das WLAN konnte erfolgreich implementiert werden. Zusätzlich wurde eine interne Dokumentation erstellt, anhand der die Implementation nachvollzogen und gewartet werden kann. Die Aufgabe wurde damit erfolgreich abgeschlossen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Akronyme

AP Access Point

DHCP Dynamic Host Configuration Protocol

EANTC European Advanced Networking Test Center

PoE Power over Ethernet

RADIUS Remote Authentification Dial-In User Service

VLAN Virtual Local Area Network

VM Virtuelle Maschine

WLAN Wireless Local Area Network

1 Einleitung

Für die Arbeit im EANTC ist es unerlässlich, dass sich alle Mitarbeitenden mit dem Internet, internen Diensten wie der Projektplanung, geteilten Laufwerken und dem internen Wiki, als auch dem eigenen Labor, in dem die Testprojekte durchgeführt werden, verbinden können. Da alle Mitarbeitenden mit Laptops arbeiten, werden diese Verbindungen über ein WLAN hergestellt.

Zusätzlich findet im EANTC jedes Jahr ein größeres Event statt, bei welchem viele externe Akteur:innen und Ingenieur:innen vor Ort kollaborieren. Auch hier ist es von höchster Wichtigkeit, dass die Verbindung zum WLAN unter hoher Auslastung zuverlässig funktioniert.

Nachdem es im EANTC in der Vergangenheit Ausfälle des WLANs – vor allem während der hohen Auslastung des Events – gab, soll nun ein neues WLAN zur Verbindung der Arbeitslaptops mit dem Internet und den internen Diensten eingerichtet werden.

Um das neue WLAN sinnvoll planen zu können, werden in Kapitel 2 Vorgaben diskutiert, eine Anforderungsanalyse durchgeführt und das Ziel der Arbeit formuliert. Danach soll in Kapitel 3 die vorhandene Netzwerktopologie untersucht und verstanden werden und anschließend in Kapitel 4 ein Entwurf für den Aufbau des neuen WLANs erstellt werden. Im Anschluss wird es in Kapitel 5 um die Umsetzung des Entwurfs gehen, deren Ergebnis dann in Kapitel 6 vorgestellt wird.

2 Anforderungsanalyse

Bevor die Arbeit an dem neuen WLAN aufgenommen werden kann, muss zuerst sichergestellt werden, dass alle Anforderungen definiert sind. Dazu wird zunächst in Kapitel 2.1 die grundlegende Frage beantwortet, was ein WLAN überhaupt ist. Im Anschluss werden in Kapitel 2.2 die Anforderungen ausgewertet, die an das neue WLAN gestellt werden und in Kapitel 2.3 festgelegt, was das konkrete Ziel der Aufgabe und dieser Arbeit ist.

2.1 Was ist ein Wireless Local Area Network?

Ein WLAN ist, wie der Name suggeriert, ein Lokales Netzwerk, das mittels Funkübertragung, also ohne Kabel, funktioniert. Dies lässt sich durch verschiedene Technologien erreichen, meist kommen aber die Übertragungstechniken aus der IEEE-802.11 Standardreihe zum Einsatz. In dieser wird die physische Übertragungsschicht in Funknetzen definiert. Im Laufe der Zeit wurde der 802.11 Standard kontinuierlich weiterentwickelt, wobei sich meistens die Übertragungsgeschwindigkeiten steigerten. Heute sind vor allem die Standards 802.11n (Wi-Fi 4) und 802.11ac (Wi-Fi 5) relevant, die jeweils in einem Frequenzbereich von 2,4 GHz beziehungsweise 5 GHz arbeiten. [ION22]

Die Datenübertragung im WLAN funktioniert über einen Access Point (AP) der ein Funksignal ausstrahlt, mit dem sich Endgeräte verbinden können. Dieser AP ist dann der Zugangspunkt zu dem dahinterliegenden kabelgebundenen Netzwerk. [Sch22]

2.2 Funktionale Anforderungen an das WLAN

Die zu benutzende Hardware und damit verbundene Software wurde in Form von APs der Firma UniFi vor Übergabe der Aufgabe bereits gekauft. Eine technische Anforderungsanalyse zur Auswahl der Hardware ist somit nicht Bestandteil dieser Arbeit. Der Fokus soll stattdessen vor allem auf der Installation und Konfiguration der verschiedenen Komponenten liegen.

Zu betrachten sind dabei die funktionalen Anforderungen an das WLAN, die von der Geschäftsleitung vorgegeben wurden:

1. Realisierung eines Mitarbeitenden- und eines Gäst:innen-WLANs mit verschiedenen Zugriffsbeschränkungen auf interne Dienste der Firma.

2. Sicherstellung der Betriebssicherheit des WLANs, unter anderem durch Einschränkung der Bandbreite für Gäst:innen.

3. Wartbarkeit und Dokumentation des Netzwerkes, um bei Fehlerauftritten Handlungsfähigkeit sicherzustellen.

2.3 Zielvorgabe

Das Ziel der praktischen Aufgabe ist es, das neue WLAN in Betrieb zu nehmen und alle Komponenten so zu implementieren beziehungsweise zu konfigurieren, dass die oben genannten funktionalen Anforderungen erfüllt sind. Außerdem soll eine umfassende interne Dokumentation erstellt werden, mit deren Hilfe das IT-Team des EANTC den Aufbau nachvollziehen und Fehler beheben oder Änderungen implementieren kann, falls dies notwendig wird.

Das Ziel dieser Arbeit ist es, den Prozess der Aufgabenbearbeitung zu beschreiben, mit theoretischen Hintergründen zu ergänzen und die Ergebnisse der Aufgabe auszuwerten.

3 Vorhandener Netzaufbau

Bevor der Entwurf zur Implementierung des WLANs erstellt werden kann, muss das vorhandene Netzwerk untersucht und verstanden werden. Dies ist nötig, um die Anforderungen an das WLAN besser zu verstehen und einordnen zu können. Vor allem für die Anforderung, verschiedene Zugangsberechtigungen für verschiedene Nutzer:innengruppen einzurichten, ist es unerlässlich, die internen Dienste zu kennen und zu wissen, welche Mittel zur Verfügung stehen, die Zugänge zu kontrollieren.

Das Netz des EANTC lässt sich grob in drei verschiedene logische Zonen einteilen, in denen Geräte und Dienste angesiedelt sind. Die erste Zone wird als *„Testing“* bezeichnet und in ihr befindet sich das Equipment im Testlabor, auf das auch externe Projektpartner:innen und Kund:innen Zugriff haben müssen, um zum Beispiel ihre vom EANTC zu testende Hardware zu konfigurieren. In der Zone *„Production“* befinden sich die verschiedenen Server und Dienste, mit denen die Mitarbeitenden von EANTC täglich arbeiten. Auch verschiedene IT-Dienste zur Verwaltung des Netzwerks sind hier zu verordnen, so wird beispielsweise auch der Controller für die UniFi-APs hier implementiert werden. Auf diesen wird in Kapitel 4.1 im Detail eingegangen. Die letzte Zone *„Management“* ist am stärksten isoliert. Hier sind verschiedene Management-Interfaces der wichtigsten Infrastrukturkomponenten des Netzwerks zu finden.

Die verschiedenen Zonen werden durch Subnetze und Virtual Local Area Networks (VLANs) logisch voneinander getrennt. Die IP-Adressen für die verschiedenen Subnetze werden von einem Dynamic Host Configuration Protocol (DHCP) Server vergeben. Im Detail wird hierauf in Kapitel 4.3 und Kapitel 4.4 eingegangen.

Um Datenverkehr zwischen den Zonen zu ermöglichen, wird mittels einer PfSense-Firewall kontrolliert, welche Quellgeräte aus welchem Subnetz, mit welchen Protokollen und mit welchen Zielgeräten kommunizieren dürfen. Die Firewall filtert außerdem auch den Datenverkehr aus dem Internet und routet zwischen den verschiedenen Subnetzen und VLANs.

4 Entwurf

Nun soll mit dem Wissen über das vorhandene Netz aus dem vorherigen Kapitel 3 ein Entwurf zur Implementierung des WLANs erstellt werden. Dazu wird in den verschiedenen Unterkapiteln auf die wichtigsten Komponenten eingegangen und erläutert, wie diese miteinander zusammenhängen.

4.1 UniFi Hard- und Software

Es sollen drei APs des Modells UniFi-AC-HD benutzt werden. Zusätzlich sollen zu einem späteren Zeitpunkt noch zwei UniFi-AC-Pro APs eingebunden werden, die im Moment noch im alten WLAN in Betrieb sind. UniFi APs benötigen zum Betrieb die UniFi-Network-Application als Controller, mit deren Hilfe Konfigurationen vorgenommen und die APs in das WLAN eingebunden werden können. Die UniFi-Network-Application kann entweder mit einer zusätzlichen UniFi-Console betrieben, oder auf einem eigenen Server installiert werden. [Ubi23e]

UniFi-Consoles sind als ganzheitliche Lösung zur Verwaltung eines Netzwerkes gedacht, welches vor allem aus UniFi-Hardware besteht. [Ubi23a] Da nur das WLAN mit UniFi-Geräten betrieben werden soll und die zusätzlichen Funktionen einer UniFi-Console nicht genutzt werden würden, scheint der Kauf eines solchen zusätzlichen Geräts nicht sinnvoll. Die Serverinfrastruktur zur Installation der Network-Application ist im EANTC bereits vorhanden, daher wurde sich dazu entschieden, diese selbst zu hosten.

4.2 Physische Verteilung der Geräte

Ihre Anbindung an das Netzwerk und ihre Stromversorgung bekommen die APs von verschiedenen Power over Ethernet (PoE) Switches, die wiederum mit dem Rest des Netzwerks verbunden sind. Von den PoE-Switches aus werden die Signale über Patchpanäle an Buchsen nahe den jeweiligen APs verteilt. In Abbildung 1 sind die geplanten Standorte der fünf APs zu sehen, wobei darauf zu achten ist, dass jeder Büroraum von mindestens zwei APs abgedeckt ist.

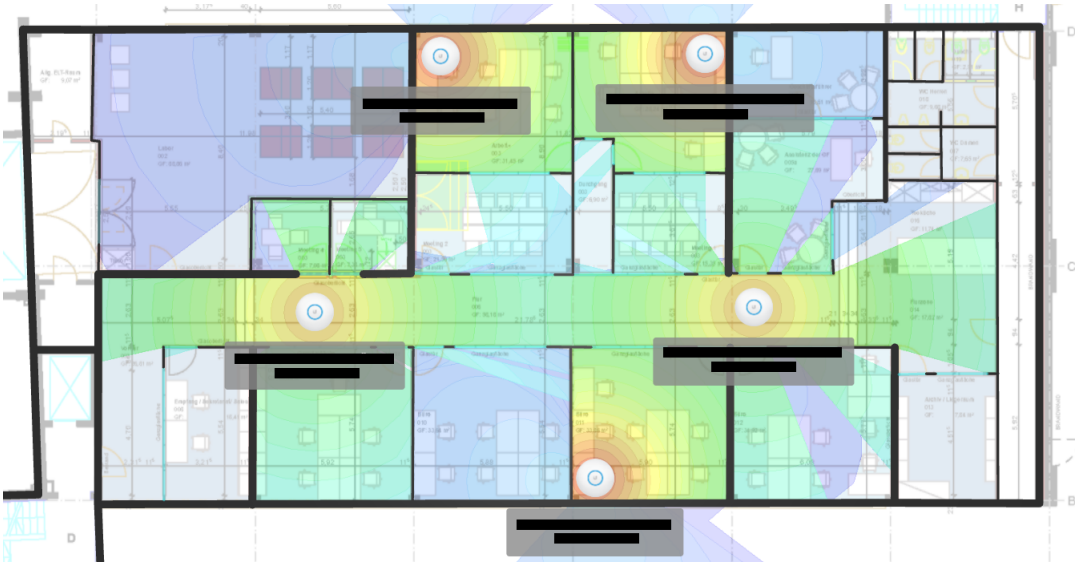

Abbildung 1: Physische Verteilung der Access Points (Screenshot aus der UniFi-Network-Application)

4.3 Routing und Switching

Die Datenpakete aus dem Gäst:innen- und dem Mitarbeitenden-WLAN müssen, damit die gewünschte Funktionalität erreicht werden kann, voneinander getrennt und unterscheidbar gemacht werden. Dies geschieht mit Hilfe von VLANs, die an den Switchports und im UniFi-Network-Controller konfiguriert werden. Dirk Srocke erklärt: „Mit VLANs lassen sich physische LANs in voneinander isolierte, logische Teilnetze aufteilen.“ [Sro18]

Mittels VLAN-Tagging können dann über einen Switchport mehrere VLANs übertragen werden. Je nachdem, aus welchem WLAN ein Paket kommt, bekommt oder behält dieses am Switch seinen VLAN-Tag und kann dann von der Firewall, wie in Abbildung 2 zu sehen ist, entsprechend in die verschiedenen Zonen geroutet werden. Wenn ein Laptop aus dem Gäst:innen-Netzwerk beispielsweise auf die UniFi-Network-Application zugreifen will, wird die Firewall diese Pakete nicht weiterleiten. Auch andersherum kann der AP anhand des VLAN-Tags erkennen, aus welchem VLAN ein Paket kommt, und dieses entsprechend dem Gäst:innen- oder Mitarbeitenden-WLAN zuordnen. [Hew15]

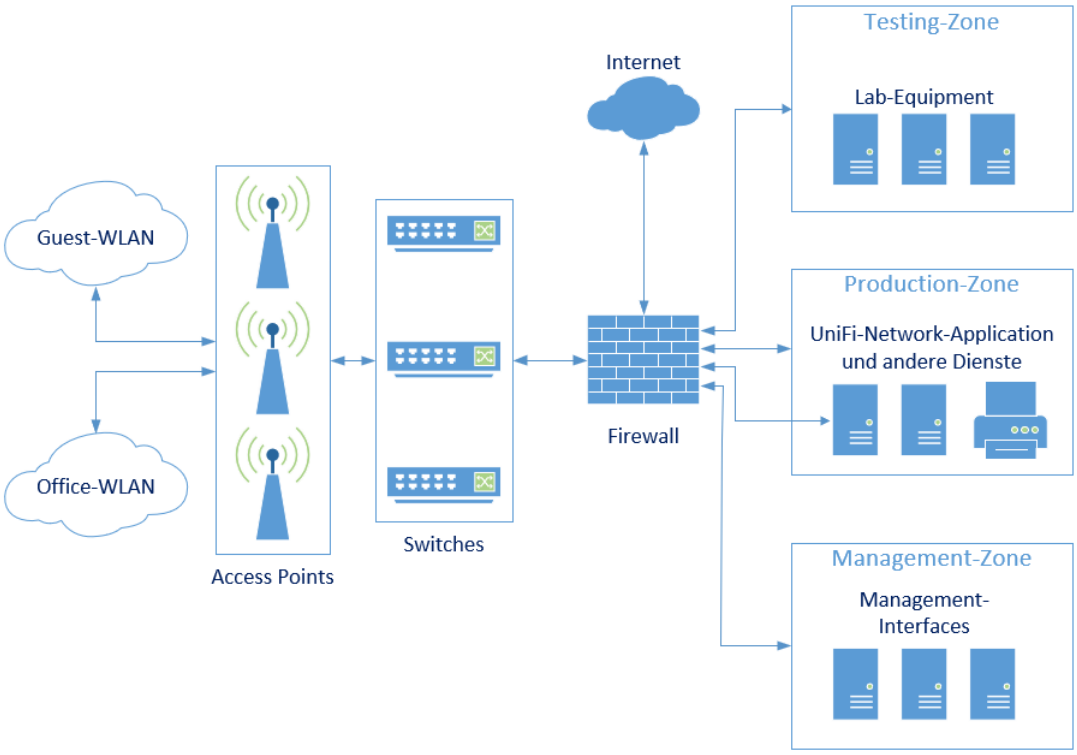

Abbildung 2: Entwurf für das WLAN (eigene Zeichnung)

4.4 IP-Adressverteilung

Eine weitere Trennung der verschiedenen Netzwerke wird durch die Vergabe von IP-Adressen erreicht. Dabei erhält jedes Gerät eine eindeutige, aus vier Byte bestehende IPv4-Adresse. Diese Adresse wird durch eine Subnetzmaske in einen Hostanteil und einen Netzanteil zerlegt. Bei der IP-Adresse 10.0.1.101 mit der Subnetzmaske 255.255.255.0 ist 10.0.1.x beispielsweise der Netzanteil und x.x.x.101 der Hostanteil. Durch das Subnetting können nur Geräte direkt miteinander kommunizieren, die den gleichen Netzanteil haben – also dem gleichen Subnetz angehören. [Man18, S. 41, 48ff.]

IP-Adressen für die Geräte, die sich mit den APs verbinden, sollen automatisch vergeben werden. Dazu soll der vorhandene DHCP-Server so konfiguriert werden, dass er, je nachdem aus welchem VLAN die Anfrage kommt, eine Adresse aus einem vorher definierten Adresspool zuweist. Zusätzlich soll es auch feste Adressreservierungen geben, zum Beispiel für die APs selbst.

5 Umsetzung

Nachdem in Kapitel 3 das Netzwerk des EANTC analysiert und in Kapitel 4 ein Entwurf für die Implementierung des WLANs nach den Anforderungen aus Kapitel 2 erstellt wurde, soll dieser nun umgesetzt werden.

5.1 Installation und Konfiguration der UniFi-Network-Application

Um die UniFi-Network-Application zu hosten, wurde eine Debian 10 Virtuelle Maschine (VM) zur Verfügung gestellt. Während der Installation stellte sich heraus, dass die UniFi-Network-Application ältere Versionen der von ihr verwendeten Datenbank MongoDB und der Programmiersprache Java benötigt, wodurch die Installation mit einer Fehlermeldung abbrach. Da UniFi während der Installation automatisch die zur Verfügung stehende Version von MongoDB installiert, mussten die Verweise auf das neuere MongoDB-Repository manuell gelöscht werden, um dann anschließend die ältere, von UniFi benötigte Version 3.4 als Repository hinzuzufügen. Außerdem musste Java 8 manuell installiert werden, da UniFi sonst automatisch eine inkompatible Version installierte. Nach diesen Vorbereitungen konnte die UniFi-Network-Application schließlich erfolgreich installiert werden. [Ubi23e]

Nun konnte über das Webinterface auf die Network-Application zugegriffen werden, wo einige Einstellungen vorgenommen werden mussten. Es wurden zwei Netzwerke angelegt, eines für das Gäst:innen-WLAN und eines für das Mitarbeitenden-WLAN. Das Gäst:innen-Netzwerk wurde als *„VLAN-only Network“* eingerichtet, das heißt, es ist mit dem entsprechenden VLAN-Tag versehen. Das Mitarbeitenden-Netzwerk wurde als normales Netzwerk angelegt, ohne VLAN-Tag. Die Switches mit denen die APs verbunden sind, wurden an den jeweiligen Ports analog dazu konfiguriert.

Im Anschluss wurden zwei WLANs eingerichtet und ihnen jeweils das richtige der beiden eben konfigurierten Netzwerke zugeordnet. Zusätzlich wurden hier noch Name und Passwort der beiden WLANs festgelegt und die Bandbreite des Gäst:innen-WLANs wurde den Anforderungen aus Kapitel 2.2 entsprechend beschränkt.

5.2 Firewall-Einstellungen

Zuerst musste sichergestellt werden, dass die APs und die UniFi-Network-Application reibungslos miteinander kommunizieren können. Dazu wurden nach Spezifikation verschiedene TCP- und UDP-Ports freigeschaltet. So wird beispielsweise UDP-Port 10001 benötigt, damit die Network-Application die APs finden kann. [Ubi23d]

Außerdem musste an dieser Stelle implementiert werden, dass Geräte aus dem Gäst:innen-WLAN nicht auf interne Ressourcen und Dienste zugreifen können und andersherum Geräte aus dem Mitarbeitenden-WLAN auf alle Dienste zugreifen können, die sie zum Arbeiten brauchen. Dazu wurden in Zusammenarbeit mit dem Firewall-Administrator verschiedene Regeln angelegt. Dabei wurde dem *least privilege*-Prinzip gefolgt, das besagt: „[...] a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function“ [Com15, S. 76]. Diesem Prinzip folgend wurde grundlegend aller Datenverkehr blockiert und dann explizit Regeln angelegt, die nur Verbindungen erlauben, die erwünscht sind. Dadurch wurde eine höhere Sicherheit erreicht, als wenn alle Verbindungen erlaubt wären und nur solche explizit blockiert werden würden, von denen bekannt ist, dass sie unerwünscht sind.

5.3 Einbindung der Access Points

Normalerweise sollten APs, die an das Netzwerk angeschlossen wurden, in dem Webinterface der UniFi-Network-Application auftauchen und durch Anklicken dem WLAN hinzugefügt werden können. Da sich APs und UniFi-Network-Application aber in verschiedenen Subnetzen befinden, funktionierte dies nicht auf Anhieb. [Ubi23b] Um das Problem zu lösen, wurde sich dazu entschieden, die DHCP-Option 43 zu benutzen, die dafür sorgt, dass der DHCP-Server den APs die IP-Adresse der UniFi-Network-Application mitteilt. [Ubi23c]

Mithilfe der offiziellen Dokumentation [GR23a, GR23b] des DHCP-Servers konnte folgender Code in dessen Konfigurationsdatei geschrieben werden, um die DHCP-Option 43 zu realisieren:

```
option space ubnt;
option ubnt.unifi-address code 1 = ip-address;

class "ubnt" {
    match if substring (option vendor-class-identifier, 0, 4) = "ubnt";
    option vendor-class-identifier "ubnt";
    vendor-option-space ubnt;
    }

option ubnt.unifi-address [controller.ip.address.here];
```

Nun waren die APs im Webinterface sichtbar und konnten eingebunden werden. Das neue WLAN war somit erstmalig benutzbar.

5.4 Inbetriebnahme und Dokumentation

Bevor das neue WLAN offiziell in Betrieb genommen werden konnte, wurde zuerst über eine Testphase beobachtet, ob dieses stabil ist und überprüft, dass es alle Anforderungen aus Kapitel 2.2 erfüllt. Während dieser Testphase wurden verschiedene Anpassungen an Firewall-Regeln vorgenommen, um die gewünschte Funktionalität herzustellen.

Nachdem die Testphase erfolgreich abgeschlossen war, wurde das alte WLAN abgeschaltet und das neue eingeschaltet. Die Mitarbeitenden des EANTC wurden darüber rechtzeitig informiert und anschließend neu eingeloggt. Schließlich konnten auch die zwei APs des alten WLANs zurückgesetzt und in das neue eingebunden werden.

Zuletzt wurde eine umfassende interne Dokumentation über den Aufbau und die Einrichtung des WLANs erstellt, mit dem dieses nachvollzogen und gewartet werden kann. Außerdem wurde ein weiterer Mitarbeiter in der Nutzung der UniFi-Network-Application geschult.

6 Ergebnisse und Ausblick

Das WLAN konnte dem Entwurf aus Kapitel 4 folgend implementiert werden. Wünschenswert wäre es zusätzlich, wenn die Mitarbeitenden sich durch ihre Firmenaccounts im WLAN authentifizieren könnten. Dies umzusetzen war zum Zeitpunkt der Aufgabenbearbeitung nicht möglich, da der Remote Authentification Dial-In User Service (RADIUS) Server des EANTC überarbeitet wurde. In Zukunft könnte diese Funktionalität jedoch noch ergänzt werden.

Die Anforderungen aus Kapitel 2.2 werden durch das WLAN erfüllt. Die Zugriffsbeschränkungen für die zwei verschiedenen Netze funktionieren wie geplant und das WLAN ist seit Inbetriebnahme stabil. Einzelne aufgetretene Fehler konnten behoben und in der Dokumentation mit Lösungsschritten festgehalten werden. Durch das Fortführen dieser Praxis soll mit der Zeit eine Sammlung von Handlungsschritten zur Fehlerbehebung entstehen. Aufgrund der einheitlichen Konfiguration und Dokumentation ist das WLAN einfacher zu Warten als das vorherige und es können problemlos APs hinzugefügt werden, um das Netzwerk weiter zu skalieren. Die in Kapitel 2.3 gesetzte Zielvorgabe der Aufgabe wurde somit erfüllt.

Literaturverzeichnis

[Com15] Committee on National Security Systems (2015). CNSSI No. 4009 - Committee on National Security Systems Glossary. National Security Agency.

[GR23a] Goldlust, S. and Risk, V. (2023a). ISC DHCP 4.4 Manual Pages - dhcp-options. https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcp-options. Abgerufen: 31.07.23.

[GR23b] Goldlust, S. and Risk, V. (2023b). ISC DHCP 4.4 Manual Pages - dhcpd.conf. https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcpdconf. Abgerufen: 31.07.23.

[Hew15] Hewlett-Packard Development Company (2015). Static VLAN Operation. https://techhub.hpe.com/eginfolib/networking/docs/switches/YA-YB/15-18/5998-8157_yayb_2530_atmg/content/ch01s02.html. Abgerufen: 19.07.2023.

[ION22] IONOS (2022). Was ist 802.11? WLAN-Standards erklärt. https://www.ionos.de/digitalguide/server/knowhow/ieee-80211/. Abgerufen: 19.07.23.

[Man18] Mandl, P. (2018). Internet Internals - Vermittlungsschicht, Aufbau und Protokolle. Springer Vieweg Wiesbaden.

[Sch22] Schnabel, P. (2022). Netzwerktechnik-Fibel: Netzwerke, Ethernet, WLAN, TCP/IP, Anwendungen, Dienste und Sicherheit. Patrick Schnabel.

[Sro18] Srocke, D. (2018). Was ist VLAN? https://www.ip-insider.de/was-ist-vlan-a-598987/. Abgerufen: 19.07.23.

[Ubi23a] Ubiquiti (2023a). Introduction to UniFi. https://help.ui.com/hc/en-us/articles/360012192813. Abgerufen: 20.07.23.

[Ubi23b] Ubiquiti (2023b). UniFi - Device Adoption. https://help.ui.com/hc/en-us/articles/360012622613-UniFi-Device-Adoption. Abgerufen: 20.07.23.

[Ubi23c] Ubiquiti (2023c). UniFi Network - L3 Adoption Methods: DHCP Option 43. https://help.ui.com/hc/en-us/articles/204909754-UniFi-Layer-3-methods-for-UAP-adoption-and-management. Abgerufen: 31.07.23.

[Ubi23d] Ubiquiti (2023d). UniFi Network - Required Ports Reference. https://help.ui.com/hc/en-us/articles/218506997-UniFi-Network-Required-Ports-Reference. Abgerufen: 20.07.23.

[Ubi23e] Ubiquiti (2023e). Updating Self-Hosted UniFi Network Servers (Linux). https://help.ui.com/hc/en-us/articles/220066768. Abgerufen: 20.07.23.

Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich:

1. Dass ich meinen Praxistransferbericht ohne fremde Hilfe angefertigt habe.

2. Dass ich die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autor:innen an den entsprechenden Stellen innerhalb der Arbeit gekennzeichnet habe.

3. Dass ich meinen Praxistransferbericht bei keiner anderen Prüfung vorgelegt habe.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Berlin, 18.08.2023

Ort, Datum

Oskar Mansfeld