Bernburg
Dessau
Köthen

Hochschule Anhalt (FH)
Anhalt University of Applied Sciences

emw
Fachbereich
Elektrotechnik, Maschinenbau
und Wirtschaftsingenieurwesen

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor of Engineering (B. Eng.)

Vorname Name

Bowen Li

Elektro- und Informationstechnik, 2011, 4057385

Studiengang, Matrikel, Matrikelnummer

Thema:

Aufbau des unternehmensweiten Wireless LAN

Prof. Dr. Igor Merfert

Vorsitzende(r) der Bachelorprüfungskommission

Prof. Dr. Igor Merfert

1. Prüfer(in)

Prof. Dr. Michael Brutscheck

2. Prüfer(in)

16. 04. 2015

Abgabe am

Eidesstattliche Erklärung

Hiermit erkläre ich, dass die Arbeit selbstständig verfasst, in gleicher oder ähnlicher Fassung noch nicht in einem anderen Studiengang als Prüfungsleistung vorgelegt wurde und keine anderen als die angegebenen Hilfsmittel und Quellen, einschließlich der angegebenen oder beschriebenen Software, verwendet wurden.

Köthen, 14.04.2015

Ort, Datum | Unterschrift des Studierenden

Sperrvermerk

Sperrvermerk: ja [ ] nein [X]

wenn ja: Der Inhalt der Arbeit darf Dritten ohne Genehmigung der/des (Bezeichnung des Unternehmens) nicht zugänglich gemacht werden. Dieser Sperrvermerk gilt für die Dauer von X Jahren.

Köthen, 14.04.2015

Ort, Datum | Unterschrift des Studierenden

Angaben zum Unternehmen

Logo des Unternehmens	
Name des Unternehmens	HUAWEI Technologies Düsseldorf GmbH
Abteilung	Regional SBG IT Department European Research Center
Name des Betreuers	Ing. Xiaoyi Bai
Kontaktdaten	Bai.xiaoyi@huawei.com
Anschrift des Standortes, an dem die Arbeit verfasst wurde	HUAWEI TECHNOLOGIES DÜSSELDORF GmbH Riesstraße 25, D-80992 München

Inhaltsverzeichnis

1 Motivation und Zielsetzung

1.1 Einleitung

Informationsaustausch ist ein wichtiger Bestandteil in der heutigen Gesellschaft. Während des früheren Anfangs des Ethernets war der Informationsaustausch auf drahtgebundene Netzwerklösungen angewiesen. Aber die Vernetzung war von Raum und Stoffen ziemlich eingeschränkt. Der dringende Bedarf wurde nach der Verabschiedung des IEEE-802.11-Standards erleichtert. Die Arbeitsgruppe 802.11 definierte ein neues Schlagwort der modernen Kommunikationsmethode, das sogenannte Wireless LAN, kurz WLAN. Wireless LAN ist eine revolutionierte Methode für den Datenaustausch und bahnt einen Trend der Datentransportierung an. Daten werden heute nicht nur ausschließlich über den Draht transportiert, sondern auch zunehmend über die Luft. Die Vorteile von Wireless LAN liegen klar auf den Hand: Der feste Kabelanschluss für die Netzwerkverbindung wird nicht mehr benötigt. Dabei erfreut sich der Benutzer der Flexibilität und Mobilität des Surfens. Wegen des großen Erfolges des Wireless LAN hat sich das drahtlose Netzwerk sowohl im gewerblichen als auch im privaten Bereich mehr und mehr etabliert.

Um eine bessere Arbeitsumgebung für die Mitarbeiter anbieten zu können, stellte die IT-Branche ein auf drahtgebunden basierendes Ethernet, das Wireless Netzwerk bereit. Die Netzwerkstruktur besteht aus drei Teilen: dem WLAN Controller (Access Controller), dem Access Point und dem Client. Eine drahtgebundene Anbindung zwischen dem WLAN Controller, dem Access Point und dem oberstromigen Netzwerk bildet in diesem Fall ein sogenanntes Distribution System. Das Distribution System spielt die Rolle als eine Art Backbone, über den die Benutzer auf die Ressourcen des oberstromigen Netzwerks zugreifen können. Der WLAN Controller funktioniert hier nicht bloß wie ein Bridge, er kann auch unterschiedliche Basic Service - Sets eintragen. Aber ein BSS kann für sich nur eine geringe Fläche abdecken. Die Kombination aus mehreren BSS dagegen erlaubt den Aufbau eines WLAN mit Ausdehnung und Komplexität. In diesem wird Extended Service Set, kurz ESS, verwendet. Normalerweise besteht ESS aus dem Access Point. Der Access Point ist eine spezielle Form der Station und dient einem Zugang zu BSS. Die Clients kommunizieren mit dem AP inner-

halb einer Funkzelle und die Daten werden über den AP an den Wireless - Controller weitergeleitet.

1.2 Zielsetzung der Arbeit

In der Arbeitszone stehen hier insgesamt 30 Büros und in jedem Büro stehen im Durchschnitt fünf Arbeitsplätze für die Mitarbeiter zur Verfügung. Das Arbeitsziel ist es, dass alle Mitarbeiter des Unternehmens zusätzlich ein drahtloses Netzwerk verwenden können. Die Datenrate des drahtlosen Netzwerks kann außerdem zumindest die Ausführung der Audio- und Videokonferenz garantieren.

Aufgrund der Unterschiede der von den Mitarbeitern genutzten Terminalgeräte werden die WLAN-Benutzer in zwei Gruppen, nämlich die Rechnerbenutzer und Mobilgerätebenutzer, aufgeteilt. Die Mitarbeiter, welche einen Desktop oder ein Laptop benutzen, werden als Rechnerbenutzer bezeichnet. Umgekehrt, die Mitarbeiter, die Smartphone oder Tablet verwenden, werden Mobilgerätebenutzer genannt. Der Hauptunterschied zwischen den beiden Benutzergruppen liegt darin, dass der Authentifizierungsprozess für die Mobilgerätbenutzer mittels eines zusätzlichen Authentifizierungsapplikation ausgeführt werden muss. Allerdings können die Rechnerbenutzer den Authentifizierungsprozess an ihren Rechnern direkt aufrufen und sich über die Eingabe des Benutzerkontos mit dem drahtlosen Netzwerk verbinden.

Außerdem, um die Verwaltung des drahtlosen Netzwerks zu vereinfachen, muss eine ferne Verwaltung der Netzwerkkomponenten, wie ein WLAN-Controller, vorhanden sein. Danach können alle Operationen der Netzwerkkomponenten in dem Büro der IT-Abteilung ausgeführt werden.

1.3 Arbeitsschwerpunkte

Die Konfiguration des Aufbaus des Funknetzwerks hat folgende zwei Kernpunkte:

- Die Konfiguration für die Netzwerk-Interconnection.
- Die Konfiguration für die WLAN-Dienste.

1.3.1 Arbeitsschwerpunkt für Netzwerk-Interconnection

Der Datenaustausch zwischen allen Komponenten wird mit der Hilfe der IP-Adresse über das Layer-3-Netz transportiert. Um die Kommunikation zu gewährleisten, muss jedem genutzten Terminalgerät eine ausschließliche IP-Adresse zugeordnet werden. Somit muss man eine Planung über die Einteilung von IP-Segmenten machen. Das gesamte IP-Segment wird durch die Subnetzmaske im Subnetz aufgeteilt. Danach wird jedes IP-Subnetz von einer Hülle verschaltet, die auch als VLAN bezeichnet wird. Das bedeutet, jedes VLAN hat sein eigenes IP-Segment, welches voneinander isoliert ist. Jede VLAN beschäftigt sich mit seiner eigenen Aufgabe. Beispielsweise werden einige VLANs als Quellschnittstellen festgelegt und andere verantworten die Transportierung der von den Benutzern gesendeten Dataframes. Daher ist eine berechtige Planung für das Subnetting sowie VLAN ziemlich wichtig und notwendig für die Netzwerkstruktur.

1.3.2 Arbeitsschwerpunkt für WLAN-Dienste

Der zweite Schritt ist die spezifische Konfiguration des WLAN Controllers. Für diesen Schritt kann man zwei weitere Schwerpunkte benennen:

1. Die Funkfrequenz konfigurieren;
2. Ein auf die Benutzerdomäne basierten Authentifizierungsmechanismus konfigurieren;

Beim ersten Punkt muss man nicht nur die optimale Kanalauswahl und Sendeleistung des Frequenzbands auswählen, sondern auch einen Kalibrierungsmechanismus für die praktische Umsetzung überlegen. Weil die Sendeleistung und optimale Kanalauswahl eine direkte Auswirkung an der Datenrate zur Folge haben, stehen die beiden Faktoren im Mittelpunkt der Arbeit.

Beim zweiten Punkt stehen die Domänenpartitionen und ein auf der Benutzerdomäne basierter Authentifizierungsmechanismus im Fokus. Um die verschiedenen Benutzergruppen unterscheiden zu können, bietet der WLAN Controller mehrere Möglichkeiten für die Authentifizierung an. Wenn die Benutzer eine Verbindung mit einem WLAN einrichten, sind sie gleichzeitig in eine mit diesem WLAN entsprechende Benutzerdomäne eingetreten. In den unterschiedlichen Benutzerdomänen werden unterschiedliche Authentifizierungsprozesse aufgerufen. Nach einer erfolgreichen Authentifizierung wird das WLAN freigeschaltet und

die Benutzer können die begrenzten Netzwerkressourcen verwenden. Die Einteilung der Nutzerdomäne vereinfacht nicht nur die Netzwerkverwaltung, sondern erhöht auch die Sicherheit des Netzwerks.

Der letzte Schritt ist der, dass sich die Access Points an dem WLAN Controller anmelden. Nach der Installierung müssen sich alle APs an dem WLAN Controller anmelden. Dieser Prozess geschieht durch Hinzufügen der MAC-Adresse an den WLAN Controller. Danach werden die Funktionen des Controllers auf den angemeldeten Access Points teilweise überlagert.

Bisher sind die Erklärungen über die hauptsächlichen Arbeitsaufgaben abgeschlossen. Aber es ist noch nicht sicher, dass alles auch fehlerlos erledigt wurde. In der praktischen Umsetzung gibt es unbedingt noch etwas zu verbessern. In Zukunft wird das Wireless Netzwerk nach der Rückmeldung der Benutzer von der IT-Branche weiter optimiert.

2 Grundlagen

Um eine Struktur eines WLANs planen und umsetzen zu können, sollte man zuerst die WLAN-Produkte kennen. Deshalb wird in diesem Schritt die zugrunde liegende Funktionsumgebung der verwendeten WLAN-Komponenten angezeigt. Die hauptsächliche Netzwerkstruktur wird mithilfe von drei Komponenten aufgebaut. Diese sind der WLAN Controller (Access Controller), der 3-Layer-PoE Switch und der Access Point. Obwohl es heutzutage eine Vielzahl von WLAN-Komponenten gibt, werden alle Produkte nach Berücksichtigung der Kompatibilität durch die innere Versorgung angeboten. Weil der Hersteller sich an die Vorgaben des IEEE-802.11-Standards und dessen Erweiterung hält, kann davon ausgegangen werden, dass alle Produkte dem 802.11-standard entsprechen. Deshalb wird der Datenaustausch zwischen diesen Komponenten abgesichert.

2.1 WLAN-Controller

Die WLAN-Infrastruktur basiert auf dem WLAN-Controller. Mit der Hilfe des WLAN-Controllers wird ein zentralisiertes WLAN ermöglicht, über welches die Arbeiten der Administration wesentlich vereinfacht werden. Die Verwaltung von unternehmensweitem WLAN basiert auf einer Kombination von WLAN-Controller und Lightweight Access Point. Es besteht keine lokale Konfiguration an dem Access Point und alle Funktionen werden von dem WLAN-Controller überlagert.

Die Kontrolle und Bereitstellung von Access Point wird durch ein interoperables Protokoll durchgeführt, das als Control and Provisioning of Wireless Access Points, kurz als CAPWAP, bezeichnet wird. Das CAPWAP- Protokoll stellt zwei Kanäle bereit, ein Kontrollband und einen Datenkanal. Die CAPWAP- Verwaltungsinformationen werden über den Kontrollkanal ausgetauscht. Außerdem bietet der Datenkanal einen auf CAPWAP basierenden Tunnel für den Datenaustausch zwischen WLAN-Controller und Access Point an. Die beiden Kanäle können via Datagram Transport Layer Security (DTLS) gesichert werden. In der Nomenklatur des CAPWAP- Protokolls werden die Access Points als Wireless Termination Points (WTP) bezeichnet und die zentralen WLAN-Controller als Access Controller (AC). Deswegen wird das Gerät, das in der zentralisierten WLAN-Lösung verwendet wird, als Access Point 6605, kurz AC6605, bezeichnet.

Abbildung 1: WLAN-Controller AC6605

(Quelle. HUAWEI)

2.2 Layer-3-Switch

Das verwendete HUAWEI S5700 Layer-3-Switch wird als ein Verkehrsknoten zwischen AC und AP beschrieben. Der Layer-3-Switch ist eine Kombination aus Router und Switch. Normalerweise arbeitet ein Switch auf der Schicht 2 des OSI-Schichtenmodells und ein Router arbeitet auf der Schicht 3. Es gibt unterschiedliche Datentransportierungen, die sich nach der verwendeten Adresse unterscheiden. Die Layer-2-Transportierung basiert auf einer MAC-Adresse, hingegen wird die Layer-3-Transportierung auf einer IP-Adresse aufgebaut. Um ein Multifunktionsgerät konstruieren zu können, muss der Layer-3-Switch, also Router und Switch, logisch miteinander kombiniert werden. Der Layer-3-Switch hat ähnliche Funktionen wie der Router und Switch - sie empfangen, speichern und leiten Datenpakete weiter. An einen Layer-3-Switch können verschiedene Subnetze auf einzelnen Ports zugeordnet werden und innerhalb dieser Subnetze arbeitet der Layer-3-Switch als Switch. Außerdem beherrscht er die Kommunikation zwischen diesen Subnetzen wie ein Router. Im Vergleich zu einem reinen Router hat der Layer-3-Switch eine höhere Geschwindigkeit und Datendurchsatz.

Abbildung 2: Layer-3-Switch S5700-28C-PWR-EI

(Quelle: HUAWEI)

Er funktioniert nicht nur wie ein „Bridge“ für die Datentransportierung, sondern auch der Switch S5700 bietet mehrere Anschlüsse für den Access Point an. Im vorhergehenden Abschnitt wurde erwähnt, dass das Distribution System durch das drahtgebundene Übertragungsmedium aufgebaut wird. Aber der Access Controller kann nur 24 Anschlüsse anbieten. Diese sind bei Weitem nicht genug. Dazu braucht man das Extended Interface, um mehrere Access Points anschließen zu können. Die Verwendung des Layer-3-Switch realisiert die Möglichkeit, dass hundert APs an einen AC indirekt angeschlossen werden können. Des Weiteren gibt es eine Funktion, bei der wird eine Spannung über das Netzwerkkabel angeboten. Die PoE-Technik (Power over Ethernet) vereinfacht zusätzlich die Installation von APs. Und dadurch können durch die Access Points enorme Kosten eingespart werden, weil die Hardware und Firmware von den benutzten APs gegenüber den herkömmlichen APs vereinfacht wurden.

2.3 802.11n-Access-Point

Ein Standard Access Point bietet ein WLAN-Interface an, über das eine Funkzelle für die Benutzer bereitgestellt werden kann. Außerdem steht auch eine Ethernet-Schnittstelle zur Verfügung, mit der der Access Point an ein Distribution System über ein drahtgebundenes Übertragungsmedium angeschlossen wird. In der Regel, wenn der Access Point direkt mit dem Switch angeschlossen wird, wird der angeschlossene Access Point von dem Access Controller automatisch erkannt. Darüber hinaus erfolgt die Spannungs- und Stromversorgung über das Netzwerkkabel, weil bei dem Access Point eine Power over Ethernet Funktion vorgesehen ist. Dadurch wird die Installation des Access Point wesentlich vereinfacht.

Das verwendete Modell des Access Point ist AP 6010-AGN. Wie die meisten der heutigen hergestellten Access Points entspricht der AP6010-AGN dem 802.11n-Standard. Dieser Access Point hat mehrere Sende- und Empfängerzüge zur Verfügung und unterstützt zwei Frequenzbände von 2,4 GHz und 5 GHz. Die maximale erzielbare Datenrate ist von der Kanalbandbreite und den Sende- und Empfängerzügen abhängig. Wenn der Access Point unter einem reinen 802.11n-Arbeitsmodi arbeitet, kann die maximale theoretische Datenrate von 300 Mbit/s bis 450 Mbit/s erreicht werden. Aber normalerweise arbeitet der Access Point unter einem abwärts kompatiblen Modus, um die Einrichtungen, die nur den Standards

802.11 a/b/g entsprechen, anzupassen. Aufgrund der Rückwärtskompatibilität sinkt die Datenrate.

Abbildung 3: Access Point AP 6010-AGN

(Quelle: HUAWEI)

3 Netzwerk Interconnection

Zu Beginn der Netzwerksabwicklung wurden die meisten lokalen Netzwerke (LANs) mit Layer-2-Switch eingerichtet und die Kommunikation zwischen den LANs wurde vom Router abgeschlossen. Noch vor einigen Jahren war der Datenverkehr innerhalb eines einzigen LAN ganz normal und zwischen den LANs war der Datenverkehr noch sehr gering im Vergleich zu heute. Deshalb reichten innerhalb eines Netzwerks einige Router aus, um die Datenübertragung zwischen den LANs aufrechtzuerhalten. Heutzutage entstehen wegen der Erweiterung des Datenkommunikationsnetzwerks mehr Dienstleistungen und diese erfordern mehr Datenverkehr zwischen den LANs. Die Router können aufgrund ihrer hohen Kosten und wenigen Ethernet-Anschlüssen nicht an den Entwicklungstrend angepasst werden. Deswegen werden von der Gesellschaft neue Geräte benötigt, die die Datenweiterleitung in der Vermittlungsschicht mit hohen Geschwindigkeiten verwirklichen können. Dazu wurde Layer-3-Switch eingewickelt.

3.1 Überblick über die Interconnection-Konfiguration

Normalerweise wird ein Layer-2-Netzwerk mit Hilfe des Layer-3-Switch in mehrere VLANs unterteilt. Die Switches führen ein „Switching“ an der Schicht 2 innerhalb eines VLANs durch. Gleichzeitig wird die Layer-3-Konnektivität zwischen VLANs mittels IP-Adressen aufgebaut. Die Interconnection enthält Layer-2-Switching und Layer-3-Switching. Deswegen sind die Zuweisung des VLANs und Zuordnung der IP-Adressen die Schwerpunkte dieses Kapitels.

Die Interconnection-Konfiguration besteht aus folgenden drei Punkten:

Schwerpunkt	Beschreibung
Konfiguration des VLAN	■ Zuordnung der VLANs ■ Errichtung der VLANIF-Schnittstelle
Konfiguration des IP-Dienstes	■ Zuordnung des Subnetzes ■ Konfiguration des DHCP-Dienstes
Konfiguration der Ethernet-Ports	■ Konfiguration des Weiterleitungsmodus der Datenpakete ■ Einstellung der Port-Typen ■ Verbindung der Ports mit VLAN

Tabelle 1: Überblick über die Interconnection-Konfiguration

3.2 VLAN

Die Virtual Local Area Network (VLAN) Technologie ermöglicht es, dass ein physikalisches LAN in eine Vielzahl von Broadcast - Domänen unterteilt wird. Jede einzige Broadcast - Domäne wird als VLAN bezeichnet. Die Hosts, die innerhalb eines VLANs bleiben, können direkt miteinander kommunizieren, während die Hosts in verschiedenen VLANs nicht direkt kommunizieren können. Daher werden die Broadcast - Pakete in einem VLAN eingeschränkt. Diese Technologie erspart die Bandbreite und verbessert die Netzwerkverarbeitungskapazität.

3.2.1 VLAN - Kommunikation

Innerhalb eines Switches trägt jedes Netzwerkpaket eine VLAN-Markierung, die auch als VLAN-Tag [6] bezeichnet wird, um eine effektive Verarbeitung der Frames zu erzielen. Wenn ein Frame auf dem Ethernet-Port des Switches angekommen ist, wird seine Markierung von dem Port kontrolliert. Falls das Frame keinen VLAN-Tag trägt und der Port hat eine PVID (Port Default VLAN-ID), wird die standardmäßige VLAN-ID dem Frame hinzugefügt. Wenn das Frame einen VLAN-Tag trägt, wird der VLAN-Tag des Frames nicht mehr von dem Ethernet Port verändert. Außerdem entsprechen unterschiedliche Behandlungen für die taggten oder nicht taggten Frames den unterschiedlichen Ethernet-Ports. Im Folgenden werden die Verarbeitungen der Frames mit entsprechenden Ethernet-Ports angezeigt [5].

Typ des Ports	Verarbeitung der nicht taggten Frames	Verarbeitung der taggten Frames	Übertragung der Frames
Access-Port	Die nicht taggten Frames werden übernommen und mit PVID markiert	Die taggten Frames werden übernommen, wenn die markierte ID-Nummer gleich wie die PVID ist, umgekehrt werden sie verworfen	Die Frames können gesendet werden, nachdem der Tag abgezogen worden ist.
Trunk-Port	Ein VLAN-Tag mit der PVID wird den nicht taggten Frames hinzugefügt. Die Pakete werden nur übernommen, wenn die PVID von dem geschlossenen Port erlaubt ist. Umgekehrt werden die Frames verworfen.	Die taggten Frames werden übernommen, wenn ihre VLAN-ID vom Port erlaubt ist. Umgekehrt werden die Frames verworfen.	Wenn die VLAN-ID gleich ist wie die vorgestellte PVID und vom angeschlossenen Port erlaubt ist, wird der Tag vor der Absendung entfernt. Wenn die VLAN-ID sich von der PVID unterscheidet, aber vom Port erlaubt ist, werden die Frames ohne Veränderung transportiert.
Hybrid-Port	Ein VLAN-Tag mit der PVID wird an den nicht taggten Frames hinzugefügt. Die Pakete werden nur übernommen, wenn die PVID vom geschlossenen Port erlaubt ist. Umgekehrt werden die Frames verworfen.	Die taggten Frames werden übernommen, wenn ihre VLAN-ID vom Port erlaubt ist. Umgekehrt werden die Frames verworfen.	Wenn die VLAN-ID der Frames vom Port zulässig ist, werden die Frames abgesendet. Allerdings im Vergleich mit dem Trunk-Port kann der Hybrid-Port so konfiguriert werden, als ob der VLAN-Tag abgezogen werden soll.

Tabelle 2: Behandlungsweise der Frames von unterschiedlichen Ethernet-Ports

Das „VLAN-Tagging“ Verfahren realisiert eine Intra-VLAN-Kommunikation. Manchmal erstreckt sich ein VLAN auf mehrere Geräte, allerdings befinden sich diese Geräte in verschieden Positionen. Mit der Hilfe der Trunk-Link-Technologie können die markierten Frames ohne Begrenzung zu ihren entsprechenden VLANs transportiert werden.

Im vorhergehenden Abschnitt wurde bereits erwähnt, dass die Hosts, die sich in unterschiedlichen VLANs befinden, nicht direkt kommunizieren können. Um eine Inter-Kommunikation zwischen VLANs aufbauen zu können, muss ein auf eine VLANIF-Schnittstelle basierendes Layer-3-Switching verwendet werden: Die VLANIF-Schnittstelle ist eine logische Stelle, die entweder auf einem 3-Layer-Switch oder einem Router konfiguriert werden kann. Jede VLANIF-Schnittstelle muss mit einer IP-Adresse verknüpft werden und diese IP-Adresse wird mit der eindeutigen MAC-Adresse des VLAN verknüpft. Wenn eine Interconnection zwischen unterschiedlichen VLANs zum ersten Mal aufgebaut werden soll, muss ein „Routing" Prozess mittels der IP-Adressen durchgeführt werden. Danach werden die IP-Adressen und die zugeordnete MAC-Adresse von beiden Seiten richtig in der Routing-Tabelle eingetragen. Wenn der Datenfluss zwischen den gleichen VLANs wieder transportiert wird, sendet das Switch den Datenfluss an die Schicht 2, statt an die Schicht 3. Im Allgemeinen garantiert die VLANIF-Schnittstelle einen erfolgreichen „Routing" Prozess während der ersten Kommunikation zwischen unterschiedlichen VLANs und der folgende „Switching" Prozess erhöht die Geschwindigkeit der Datenweiterleitung.

3.2.2 Zuordnung und Konfiguration der VLANs

In diesem Abschnitt wird eine Planung für die VLAN-Zuordnung nach den Anforderungen des Unternehmens bereitgestellt.

Zuordnung der VLANs

Es wurde in den Grundlagen bereits erwähnt, dass die WLAN-Infrastruktur für ein mittelgroßes Netzwerk aus einer Kombination aus WLAN-Controller und Fit AP besteht. Die Infrastruktur wird in der nachfolgenden Abbildung dargestellt.

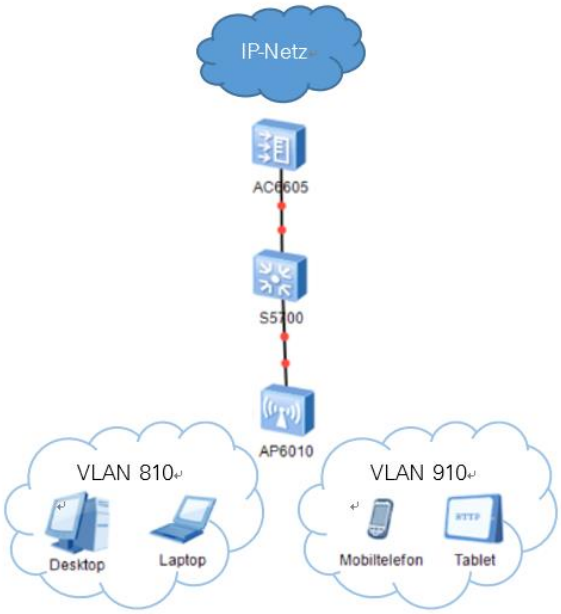

Abbildung 4: Zuordnung des VLAN

Das Unternehmen erfordert es, dass die Benutzer in zwei Gruppen unterteilt werden. Dazu muss man zwei Zugänge für diese Gruppen einstellen. Ein Zugang wird für die Benutzer, die Laptop oder Desktop verwenden, bereitgestellt. Ein weiterer Zugang wird für die Benutzer, die mit Mobiltelefon oder Tablet auf das WLAN zugreifen möchten, zur Verfügung gestellt. Weil ein Unterschied des Authentifizierungsprozesses zwischen den beiden Gruppen besteht, müssen die Datenflüsse der beiden Gruppen voneinander isoliert werden. Um auf die unterschiedlichen Endgeräte mit dem entsprechenden WLAN Service-Set zugreifen zu können, stellt man zwei VLANs für den Datenverkehr zur Verfügung.

Die zum Rechner zugehörigen WLAN-Frames werden im VLAN 810 transportiert und VLAN 910 trägt die von den Mobilgeräten gesendeten WLAN-Frames ein. Außerdem müssen die normalen WLAN-Frames und die Management-Frames getrennt werden. Deshalb ist ein spezieller VLAN für die Management-Frames notwendig. Aus diesem Grund wird VLAN 805 für den Austausch der Management-Frames generiert. Die andere Aufgabe von VLAN 805 ist es, dass das VLAN 805 als Management - VLAN für die Geräteverwaltung dient, zum Beispiel eine ferne Steuerung von Switch und Access Points. Daher werden die zum VLAN 805 zugehörigen statischen IP-Adressen diesen Geräten zugewiesen. In ähnlicher Weise muss ein zusätzlicher VLAN für den Datenaustausch zwischen dem WLAN-Controller und der Up-

link-Verbindung generiert werden und man vergibt eine statische IP-Adresse an den WLAN-Controller für die ferne Steuerung. Dazu wird VLAN 800 generiert. Bisher stehen hier insgesamt vier VLANs in der Netzwerkstruktur. VLAN 810 und VLAN 910 verantworten den Datenaustausch der WLAN-Frames und VLAN 805 transportiert die Management-Frames. Außerdem ermöglicht VLAN 800 die Kommunikation zwischen dem WLAN-Controller und dem oberstromigen Netzwerkgerät. Im nächsten Schritt werden diese VLANs mit den Switch-Befehlen generiert.

Konfiguration der VLANs

Mit folgenden Befehlen werden die zuvor beschriebenen VLANs konfiguriert:

```
<AC6605> system-view
[AC6605] vlan batch 800 805 810 910
```

Dieser Befehl „vlan batch" kann verwendet werden, um mehrere VLANs in einigen Betätigungen zu erstellen.

Nachdem die VLANs generiert wurden, können die Benutzer im selben VLAN miteinander kommunizieren. Um eine Inter - Kommunikation zwischen VLANs realisieren zu können, muss eine logische Layer-3-Schnittstelle beziehungsweise die VLANIF-Schnittstelle an jeden VLAN hinzugefügt werden. Beispielsweise kann man eine VLANIF-Schnittstelle für den VLAN 800 mit dem Befehl „interface vlanif 800" erstellen:

```
<AC6605> system-view
[AC6605] interface vlanif 800
[AC6605-Vlanif800]
```

Normalerweise muss eine WLANIF-Schnittstelle mit einer IP-Adresse oder einem Segment zugeordnet werden. Allerdings muss die Zuordnung der IP-Adressen an der VLANIF-Schnittstelle mit der Unterteilung des Subnetzes kombiniert werden. Die Unterteilung des Subnetzes wird im nächsten Abschnitt vorgestellt.

3.3 IP-Dienst

Der Hauptschwerpunkt in diesem Abschnitt ist die Planung der Subnetzunterteilung. Daran schließt sich die Konfigurierung des DHCP-Dienstes für die Clients an.

3.3.1 Subnetting

Ein physikalisches Netzwerk kann in mehrere Teilnetze unterteilt werden, um IP-Adressraum zu sparen. Normalerweise besteht eine IPV4-Adresse aus dem Netzwerkteil (Net-ID) und dem Geräteteil (Host-ID). Wenn viele Hosts in einem Netzwerk bestehen, kann ein Teil eines Geräteteils in ein Netzwerkteil umgewandelt werden. Das umgewandelte Teil wird als Subnetzidentifikation (Subnetz-ID) bezeichnet. Deswegen enthält das gesamte Netzwerk nur eine Netzwerkidentifikation für das externe Netzwerk. Wenn Frames von dem externen Netzwerk an das interne Subnetz übertragen werden, wählt das Gerät eine Route für die Frames zu den Bits vom Netzteil und Subnetzteil. Anschließend werden die Frames zu dem bestimmten Ziel-Host zu den Bits des Geräteteils von der IP-Adresse transportiert.

Die Abtrennung des vom Subnetz erfassten Netzwerkbereichs erfolgt mittels der Bit - weisen Maskierung eines bestimmten Teils der IP-Adresse durch die Subnetzmaske. Die Subnetzmaske ist auf binäre 1 gesetzt, dagegen sind alle Bits des Geräteteils auf binäre 0 gesetzt. Dann wird durch eine bitweise logische AND-Verknüpfung mit der Subnetzmaske das Netzwerkteil einer IPV4-Adresse hergestellt. Beispielsweise verbleiben bei einer 24-stelligen Subnetzmaske nur 8 Bits und damit 2^8=256 Adressen für das Geräteteil. Allerdings stehen in der Praxis nur 254 Adressen für die Hosts zur Verfügung. Das bedeutet, dass beliebige Hosts innerhalb dieses Subnetzes eine von diesen Netzadressen behalten kann.

Zuordnung des Subnetzes

Für eine ausführliche Planung muss man die gesamte Anzahl der Mitarbeiter kennen. Wenn man die genaue Anzahl der Mitarbeiter weiß, kann man die Größe des einzigen Subnetzes abschätzen.

Nach einer groben Statistik gibt es 30 Büros im Obergeschoss und in jedem Büro sitzen im Durchschnitt fünf Mitarbeiter. Damit arbeiten insgesamt mehr als 150 Mitarbeiter auf dieser Ebene. Nach dem Antrag steht ein Netzwerksegment mit der 24-Bit-Maske für jedes VLAN

zur Verfügung, nämlich 10.221.96.0/24, 10.221.97.0/24, 10.221.98.0/24 und 10.221.99.0/24. Dieses zugewiesene Segment ist jedoch in diesem praktischen Fall nicht geeignet, weil die Zuordnung keine Berücksichtigung an die praktischen Anforderungen an die IP-Adresse von jedem VLAN darstellt. Beispielsweise benötigt das VLAN 805 etwa nur 50 statische IP-Adressen für die Geräte. Wenn man ein ganzes Segment an VLAN 805 zuordnet, werden mehr als 200 IP-Adressen vergeudet. Im Gegensatz zum VLAN 805 benötigt das VLAN 910 mindestens mehr als 300 Netzwerkadressen, weil manche Mitarbeiter aufgrund ihrer Arbeit mehrere Mobilgeräte besitzen. Für diese hohen Anforderungen an die IP-Adressen ist ein Segment mit nur einer 24-Bit-Maske nicht geeignet. Dazu muss man eine geeignete Planung für die Subnetzunterteilung ausarbeiten.

Wie oben bereits erwähnt, wird das VLAN als Management-VLAN verwendet und bietet eine ferne Steuerung des WLAN-Controllers. Aus diesem Grund ist nur eine statische IPV4-Adresse für den WLAN-Controller erforderlich. Ähnlich wie beim VLAN 800 werden die statischen Adressen von Switch und Access Point von VLAN 805 zugewiesen. Die gesamte Anzahl solcher Geräte beträgt weniger als 50 und sie sind ausreichend, dass man über 100 IP-Adressen für VLAN 805 vorbereitet. Nach der Berechnung können sich VLAN 800 und VLAN 805 nur ein 24-Bit-Netz teilen. Die vordere Hälfte des Segments wird von VLAN 800 besetzt und das VLAN 805 verwendet die andere Hälfte des Segments. Um das 24-Bit-Net in weitere zwei Subnetze unterteilen zu können, benutzt man eine 25-Bit-Maske, die eine andere Schreibweise wie 255.255.255.128 oder einfach /25 hat. Dadurch umfasst das erste Subnetz die verfügbaren IP-Adressen von 10.221.96.1 bis 10.221.96.126, während das zweite Subnetz den Bereich zwischen 10.221.96.129 bis 10.221.96.254 umfasst. In der Regel wird die erste anwendbare IP-Adresse eines Segments als die Geräteadresse sowie Gateway-Adresse konfiguriert. Deswegen wird das Segment 10.221.96.1/25 dem VLAN 800 zugewiesen und die statische IPV4-Adresse 10.221.96.1 ist auch die Geräteadresse für den WLAN-Controller. Mittels dieser statischen Adresse kann man sich in den WLAN-Controller via Telnet einloggen. In ähnlicher Weise wird das Segment 10.221.96.129/25 dem VLAN 805 zugeordnet. Nach der Konfiguration wird dem VLAN 805 zugehöriges Gerät eine IPV4-Adresse aus dem Bereich 10.221.96.129 bis 10.221.96.254 zugewiesen.

Im Gegensatz zum Management-VLAN ist die Segmentunterteilung für VLAN 810 viel einfacher. Aus Sicherheitsgründen behält jeder Mitarbeiter in den meisten Fällen nur einen Laptop für die täglichen Arbeiten. Nur wenige Forscher besitzen zusätzlich noch einen Laptop für die Erforschung. Daraus ergibt sich die Konsequenz, dass ein 24-Bit-Netz das Bedürfnis der IP-Adressen vom VLAN 810 erfüllen kann. Endlich wird das Segment 10.221.97.1/24 dem VLAN 810 zugeordnet.

Es ist bereits in dem obigen Abschnitt erwähnt worden, dass mehr als 300 Mobilgeräte von den Mitarbeitern verwendet werden. Das bedeutet, dass nur ein 24-Bit-Netz die gesamte Nachfrage an die IP-Adressen nicht erfüllen kann. Deshalb wird eine 23-Bit-Maske verwendet, um die Größe des Subnetzes zu verdoppeln. Durch die Vereinigung der verbleibenden zwei Netzsegmente, nämlich 10.221.98.0/24 und 10.221.99.0/24, können hier 510 IP-Adressen im neuen Subnetz für die Mobilgeräte zur Verfügung gestellt werden. Das neue IP-Netz kann man als 10.221.98.0/23 beschreiben. Die erste verwendbare Adresse des Subnetzes, nämlich die Adresse 10.221.98.1/23, wird als die Gateway-Adresse an VLAN 910 hinzugefügt. Kurzum, die gesamte Netzwerkinfrastruktur besteht aus vier Subnetzen. Diese sind:

- VLAN 800 mit dem Segment 10.221.96.1/25
- VLAN 805 mit dem Segment 10.221.96.129/25
- VLAN 810 mit dem Segment 10.221.97.1/24
- VLAN 910 mit dem Segment 10.221.98.1/23

Konfiguration der IP-Adressen an der VLANIF- Schnittstelle

Die Kommunikation zwischen unterschiedlichen VLANs erfolgt mittels der VLANIF- Schnittstelle. Mit dem folgenden dargestellten Befehl werden die IP-Adressen sowie ihre entsprechenden Segmente an den VLANIF- Schnittstellen zugeordnet.

Beispielsweise für VLAN 810 soll die Gateway-Adresse 10.221.97.1/24 an seiner entsprechenden Schnittstelle VLANIF 810 zugeordnet werden:

```
<AC6605> system-view
[AC6605] interface vlanif 810
[AC6605-Vlanif810] ip address 10.221.97.1 255.255.255.0
```

Mit denselben Befehlen kann man die andere IP-Adresse und das Segment an ihrer entsprechenden VLANIF-Schnittstelle zuordnen.

3.3.2 DHCP-Dienst

Die Zuweisung der IP-Adresse an die Clients hat zwei Behandlungsweisen. Eine davon ist die statische Adressierung. Diese Vorgehensweise gilt nur für die Geräte, die in der Regel feste IP-Adressen brauchen. Durch die feste IP-Adresse kann eine ferne Verwaltung an dem Gerät realisiert werden. Deswegen wird jedem Netzwerkgerät, zum Beispiel dem WLAN-Controller, Switch und Access Point, eine feste IP-Adresse zugewiesen.

Jedoch für die Einrichtungen, die täglich von Mitarbeitern verwendet werden, ist die statische Adressierung nicht geeignet, weil für die statische Adressierung eine feste IP-Adresse einer jeden Einrichtung hinzufügt werden muss. Diese Arbeit ist ziemlich schwer zu realisieren. Deswegen wird für die normalen elektrischen Einrichtungen, zum Beispiel Rechner oder Mobilgeräte, eine dynamische Adressierung bereitgestellt.

Von einer dynamischen Adressierung spricht man, wenn einem Host bei einer neuen Verbindung mit einem Netz eine neue IP-Adresse zugewiesen wird. Im LAN Bereich wird die dynamische Adressierung durch DHCP verarbeitet:

DHCP ist die Abkürzung von Dynamic Host Configuration Protocol. Dieses Protokoll ermöglicht eine automatische Zuweisung der Netzwerkkonfiguration an Hosts durch den Server, statt einer manuellen Einstellung. Wo ohne DHCP-Einstellung, wie die IP-Adresse, die Netzmaske, die Gateway-Adresse oder die DNS-Serveradresse manuell konfiguriert werden müssen, verteilt der DHCP-Dienst die Einstellungen an die am Netzwerk angeschlossenen Hosts. In der Regel wird ein Client/Server-Modell verwendet. Ein DHCP-Client sendet einen

Antrag an den DHCP-Server, um die Konfigurationsdatei wie beispielsweise die IP-Adresse, Subnetzmaske anzufordern. Der DHCP-Server antwortet dem Client mit einem Paket, in dem die gewünschte Datei enthalten ist. Deswegen umfasst eine DHCP-Struktur mindestens zwei Aufgaben, nämlich den DHCP-Client und den DHCP-Server. In manchen Fällen gibt es noch ein DHCP.-Relay-Agent, um die vom Client gesendeten Anträge an den DHCP-Server weiterzuleiten. In der praktischen Umsetzung dient die VLANIF- Schnittstelle als DHCP-Server und darauf wird ein Adresspool eingerichtet.

Konfiguration eines auf eine VLANIF-Schnittstelle basierenden DHCP-Servers

Im vorhergehenden Abschnitt wurde bereits erwähnt, dass alle Hosts auf die WIFI-Dienste über VLAN 810 und VLAN 910 zugreifen können. Das bedeutet, dass alle Hosts in den VLAN 810 oder in den VLAN 910 eintreten. In diesem Fall werden die VLANIF- Schnittstellen von den beiden VLAN als DHCP-Server konfiguriert und der vom jeweiligen VLAN behaltene IP-Bereich wird gleichzeitig als Adresspool konfiguriert, um die IP-Adressen an DHCP zu den DHCP-Clients zu verteilen. Die IP-Adressen werden automatisch an den Hosts zugewiesen, die an VLAN 810 oder VLAN 910 angeschlossen sind. Außerdem hat nach der Zuweisung der IP-Adresse an einen Host der DHCP-Server in seiner Konfigurationsdatei eine Angabe, wie lange ein Host die zugewiesene IP-Adresse besitzen darf, bevor der Host sich erneut beim DHCP-Server melden und eine „Verlängerung" beantragen muss. Wenn der Host sich nicht meldet, wird die Adresse frei und kann an einen anderen Host neu zugewiesen werden. Man bezeichnet diese Zeit als „Lease-Time" und sie kann vom Administrator eingestellt werden. Um die Kommunikation zwischen den angeschlossenen Hosts und dem externen Netzwerk zu sichern, muss die Schnittstelle auch die Adresse des Nameservers während der dynamischen Adressierung an den Hosts abschicken. Ein Nameserver ist ein Server, der Namenauflösung anbietet. Normalerweise kennt der Benutzer nur die Domain im Internet und er sendet den Namen der Domäne als eine Anfrage zum Internet. Ein Nameserver ermöglicht es, den vom Benutzer gesendeten Domänenamen in die zugehörige IP-Adresse umzuwandeln. Durch die umgewandelte IP-Adresse wird der Benutzer zum richtigen Dienst oder Rechner geführt. Daher muss die Adresse des NS-Servers angegeben werden, bevor der DHCP-Server eine IP-Adresse an den DHCP-Client verteilt.

Zusammenfassend kann gesagt werden, dass ein auf einer Schnittstelle basierender DHCP-Server durch folgende drei Schritte konstruiert wird:

- Konfiguration eines IP- Adresspools auf der VLANIF- Schnittstelle
- Konfiguration der Leihdauer für die dynamische Adressierung
- Konfiguration der Adresse des DNS-Servers auf der VLANIF- Schnittstelle

Mit dem Befehl „dhcp select interface“ ist die Schnittstelle so konfiguriert, dass sie ihren lokalen IP-Adresspool verwendet. Jedem an dieser Schnittstelle angeschlossenen DHCP-Client wird eine IP-Adresse aus dem IP-Adresspool zugeordnet. Beispielsweise wenn man die Schnittstelle VLANIF 810 als DHCP-Server konfiguriert, werden die folgenden dargestellten Befehle ausgeführt:

```
<AC6605> system-view
[AC6605] dhcp enable
[AC6605] interface vlanif 810
[AC6605-Vlanif810] ip address 10.221.97.1 255.255.255.0
[AC6605-Vlanif810] dhcp select interface
```

Nach dem Konfigurieren der DHCP-Clients innerhalb des VLANs werden beliebige IP-Adressen aus dem Bereich 10.221.97.2 bis 10.221.97.254 zugeordnet. Die Leihdauer einer dynamischen IP-Adresse kann mit dem Befehl „dhcp server lease“ unter der Schnittstelle konfiguriert werden. Weil eine unbegrenzte Leihdauer zu einem langfristigen Besitz von begrenzten IP-Adressen führt, wird sie für drei Tage eingestellt. Das heißt, dass der DHCP-Client sich erneut beim DHCP-Server innerhalb von drei Tagen melden muss, sonst wird die Adresse frei und an einem anderen Host neu zugewiesen. Der Befehl lautet:

```
[AC6605-Vlanif810] dhcp server lease day 3 hour 0 minute 0
```

Anschließend sollen die Nameserveradressen auf den VLANIF- Schnittstellen konfiguriert werden. Mit dem Befehl „dhcp server dns-list“ werden die Nameserveradressen an der Schnittstelle hinzugefügt. Beispielsweise die Nameserver mit den Adressen 10.125.30.25, 10.127.4.25 und 10.72.255.100 werden an der Schnittstelle VLANIF 810 hinzugefügt.

```
[AC6605] interface vlanif 810
[AC6605-Vlanif810] ip address 10.221.97.1 255.255.255.0
[AC6605-Vlanif810] dhcp select interface
[AC6605-Vlanif810] dhcp server dns-list 10.125.30.25 10.127.4.25 10.72.255.100
```

Bisher wurden alle Konfigurationen der VLANs durchgeführt. Allerdings können die VLANs in der Praxis nur wirken, wenn sie mit den physikalischen Ethernet-Ports verbunden sind. Die Beziehungen zwischen den VLANs und den physikalischen Ethernet-Ports werden im nächsten Schritt dargestellt.

3.4 Verknüpfung des Ethernet-Ports mit VLAN

Um den physikalischen Ethernet-Port mit dem richtigen VLAN verknüpfen zu können, müssen zuerst die Weiterleitungsmodi der Frames des WLAN-Controllers näher erläutern.

3.4.1 CAPWAP-Tunneling-Verfahren

Die Frames, die in einer WLAN-Struktur übertragen werden, teilt man in zwei Kategorien auf, nämlich in die Management-Frames und in die normalen WLAN-Frames. Für die Transportierung der Management-Frames gibt es nur eine Möglichkeit, nämlich durch den CAPWAP Tunnel. Wenn ein neue Wireless Termination Point sich an den WLAN-Controller anmeldet, wird der sogenannte CAPWAP-Tunnel zwischen dem Wireless Termination Point und dem WLAN-Controller aufgebaut. Dadurch werden zwei Kanäle bereitgestellt, ein Kontrollkanal und ein Datenkanal. Damit werden alle Managementframes über den Kontrollkanal ausgetauscht. Im Gegensatz zu den Managementframes gibt es zwei Möglichkeiten für die Transportierung der WLAN-Frames. Die WLAN-Frames können ohne Kapselung via VLAN direkt weitergeleitet werden, und dieses Weiterleitungsverfahren wird als lokale Weiterleitung

bezeichnet. Die andere Möglichkeit ist die, dass sie vor dem Austausch über das CAPWAP Protokoll gekapselt werden. Die gekapselten WLAN-Frames werden über den von CAPWAP angebotenen Datenkanal transportiert. Das CAPWAP-Tunneling-Verfahren ermöglicht es, dass ein WLAN mittels des Verfahrens zum IP-Subnetz verschaltet werden kann. Dazu werden die Layer-2-Frames über CAPWAP gekapselt und über das Layer-3-Netz übertragen [1]. Der Unterschied zwischen den beiden Weiterleitungsmodi wird in den folgenden zwei Darstellungen angezeigt:

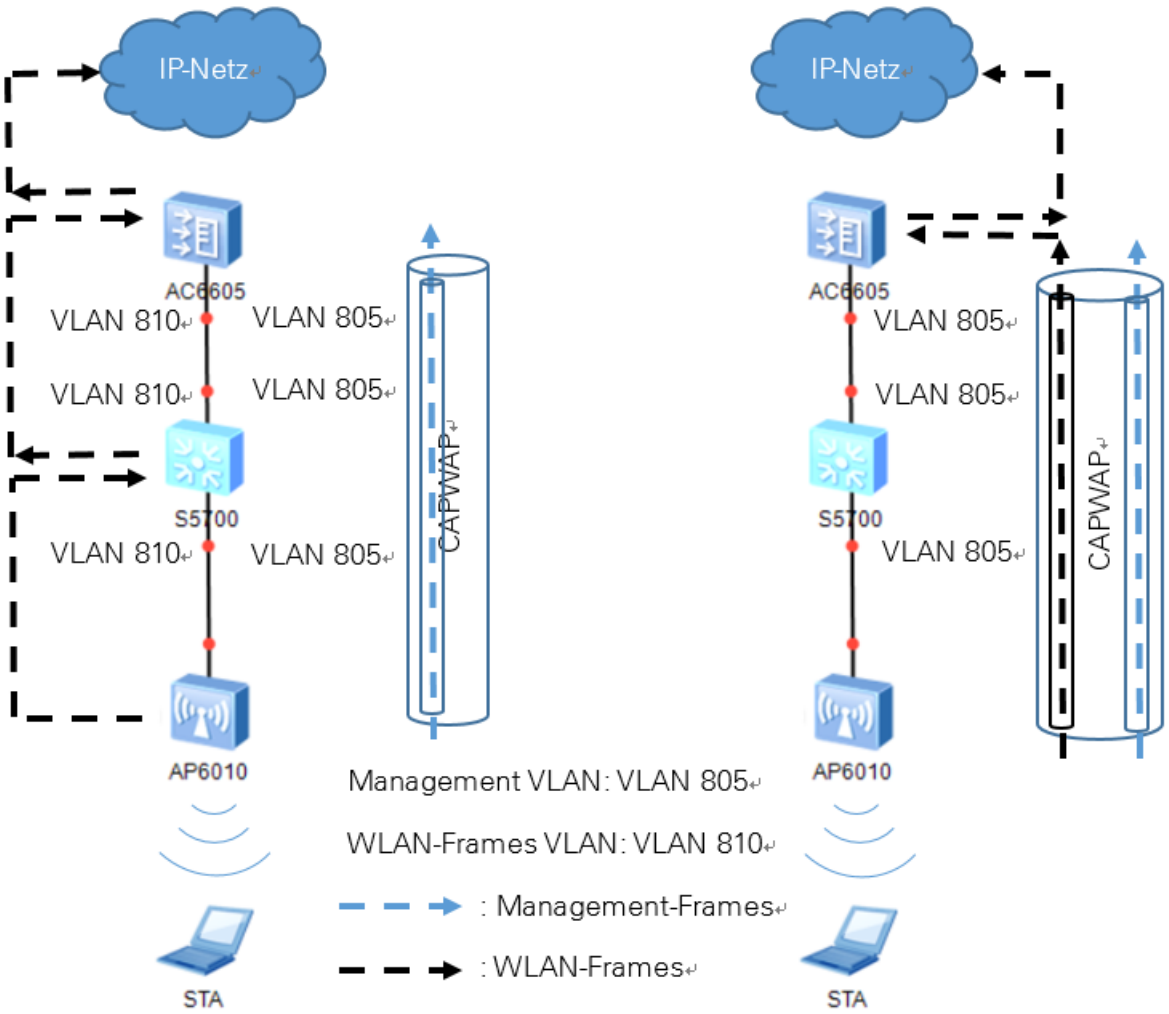

Abbildung 5: Unterschied zwischen beiden Weiterleitungsverfahren

Anhand der Darstellung wird deutlich, dass mit dem lokalen Weiterleitungsverfahren die Transportierung von WLAN-Frames und Managementframes in zwei getrennten VLANs durchgeführt wird. Außerdem muss das VLAN 810 mit dem Switch konfigurieren, um einen

Übergang für die WLAN-Frames anbieten zu können. Aber bei dem CAPWAP-Tunneling Verfahren werden hingegen die WLAN-Frames und Managementframes mittels des Tunnels über einen Management-VLAN transportiert.

Zuallererst muss eine VLANIF-Schnittstelle als Quellschnittstelle konfiguriert werden. Ein CAPWAP-Tunnel wird zwischen Wireless Termination Point und WLAN-Controller via der Quellschnittstelle aufgebaut, wenn sich der neue Wireless Termination Point an dem WLAN-Controller anmeldet. Anschließend werden die Managementframes wie die Konfigurationsdatei durch den auf der VLANIF-Schnittstelle basierenden Tunnel an den Wireless Termination Point vergeben. In dem obigen Inhalt wurde bereits erwähnt, dass VLAN 805 für den Transport der Managementframes verantwortlich ist. Deswegen wird seine entsprechende logische VLANIF-Schnittstelle als Quellschnittstelle konfiguriert. Die normalen WLAN-Frames können auch via den Tunnel transportiert werden, wenn die gekapselten WLAN-Frames mit dem VLAN- Tag „VLAN 805“ markiert werden. Nach der Markierung werden die WLAN-Frames ebenso wie die Managementframes von dem Switch behandelt. Obwohl die WLAN-Frames und Managementframes sich nur einen Tunnel teilen, verwenden sie unterschiedliche Kanäle.

Über den Tunnel werden die WLAN-Frames, ohne die Verarbeitung der Übergangsgeräte, direkt an den WLAN-Controller transportiert. Wenn die WLAN-Frames an den WLAN-Controller transportiert wurden, zieht der WLAN-Controller die Frames vom Kapseln aus und sendet sie zum oberstromigen Netzwerk.

Das Tunneling-Verfahren vereinfacht die WLAN-Struktur, damit werden die VLAN- Konfigurationen an den Übergangsgeräten auch vereinfacht. Dazu konfiguriert man nur das benötigte Management-VLAN an den Switch, nämlich das VLAN 805. Das VLAN 805 stellt einen Übergang für den Tunnel zur Verfügung.

Im Allgemeinen realisiert das CAPWAP-Tunneling-Verfahren, dass alle Frames innerhalb eines VLANs über zwei getrennte Datenkanäle direkt an den WLAN-Controller transportiert werden. Deswegen steht an dem Übergangsgerät keine komplizierte VLAN-Zuordnung, sondern ein einziges Management-VLAN.

3.4.2 Konfiguration des Ethernet-Ports

Nach dem zuvor beschriebenen Weiterleitungsverfahren wird die Konfiguration des Ethernet-Port in folgenden drei Schritten durchgeführt:

- Einstellen der VLANIF- Schnittstelle als Quellschnittstelle
- Festlegen des Typs des Ethernet-Ports
- Verknüpfen des Ethernet-Port mit dem richtigen VLAN

Für den ersten Schritt wird die Konfiguration einfach mit dem Befehl „wlan ac source interface vlanif 805“ durchgeführt.

```
<AC6605> system-view
[AC6605] wlan
[AC6605-wlan-view] wlan ac source interface vlanif 805
```

Nachdem der erste Schritt erledigt wurde, wird der zweite Schritt durchgeführt.
Im Abschnitt 3.2.1 „VLAN-Kommunikation“ wurde bereits erwähnt, dass der Ethernet-Port in drei Kataloge, nämlich den Access Port, den Trunk Port und den Hybrid Port, unterteilt ist. Die unterschiedlichen Ethernet-Ports entsprechen unterschiedlichen Behandlungsverfahren zur den Frames. In der Regel werden die mit Switch oder WLAN-Controller angeschlossenen Ethernet-Ports als Trunk Port eingestellt, um die taggten Frames zu ihrem entsprechenden VLAN weiterzuleiten. Weil die Terminalgeräte, wie Rechner oder Wireless Termination Point, nicht die Fähigkeit haben, VLAN-Tags zuerkennen, müssen die mit dem Terminalgerät angeschlossenen Ethernet-Ports als Access Point konfiguriert werden, um die VLAN-Tags vor der Dateitransportierung abzuziehen. Außerdem wird der letzte Ethernet-Port eines jeden Gerätes mit anderen oberstromigen Geräten verbunden, und die anderen Ethernet-Ports werden mit den unterstromigen Geräten verbunden, um eine leichtere Verwaltung zu erzielen. Wie im vorhergehenden Abschnitt geplant, soll das VLAN 805 sich wie ein Übergang durch die ganze Struktur hindurchziehen. Aus diesem Grund wird der letzte Ethernet-Port des Switches als Trunk Port eingestellt und mit VLAN 805 verknüpft. Gleichzeitig werden die

anderen Ethernet-Ports des Switches mit VLAN 805 verknüpft, aber umgekehrt als Access Port konfiguriert, um die VLAN-Tags von den empfangenen WLAN-Frames vor der Dateitransportierung auszuziehen. Beim WLAN-Controller wird der mit dem unterstromigen Switch verbundene Ethernet-Port als Trunk Port eingestellt und mit VLAN 805 verknüpft, um die von Switch abgesendeten Frames über VLAN 805 zu transportieren. Der ausführliche Verlauf des Weiterleitungsprozesses ist in der folgenden Abbildung dargestellt:

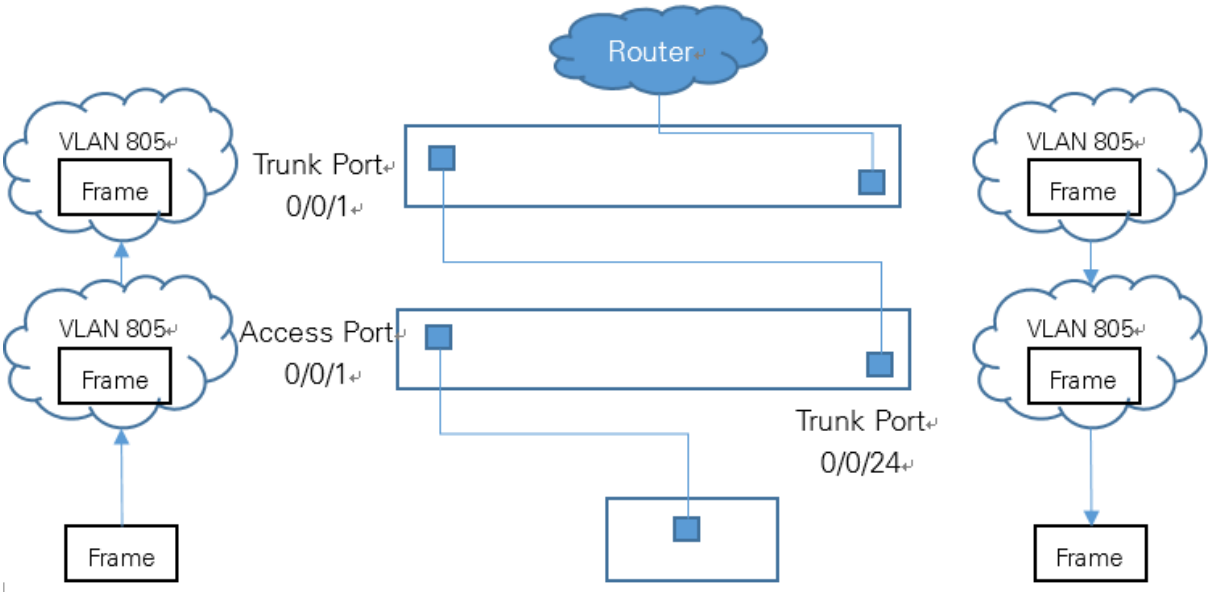

Abbildung 6: Überblick über den Weiterleitungsverlauf

Wenn die gekapselten WLAN-Frames beim WLAN-Controller angekommen sind, werden die WLAN-Frames von dem Controller entsiegelt. Die Managementframes werden von WLAN-Controller behandelt während der Dataframes an dem oberstromigen Netzwerk weiterhin weitergeleitet. Wenn die entsiegelte Dataframes über die ESS-Schnittstellen durchgehen, wird die VLAN-ID Nummern der jeweiligen ESS-Schnittstelle auf die Frames geprägt. Die WLAN-Frames mit den ID-Nummern 810 oder 910 werden anschießend an ihren entsprechenden VLAN zugestellt und der WLAN-Controller transportiert diese WLAN-Frames an das oberstromige Netzwerk. Der Verlauf wird in folgender dargestellten Abbildung angezeigt:

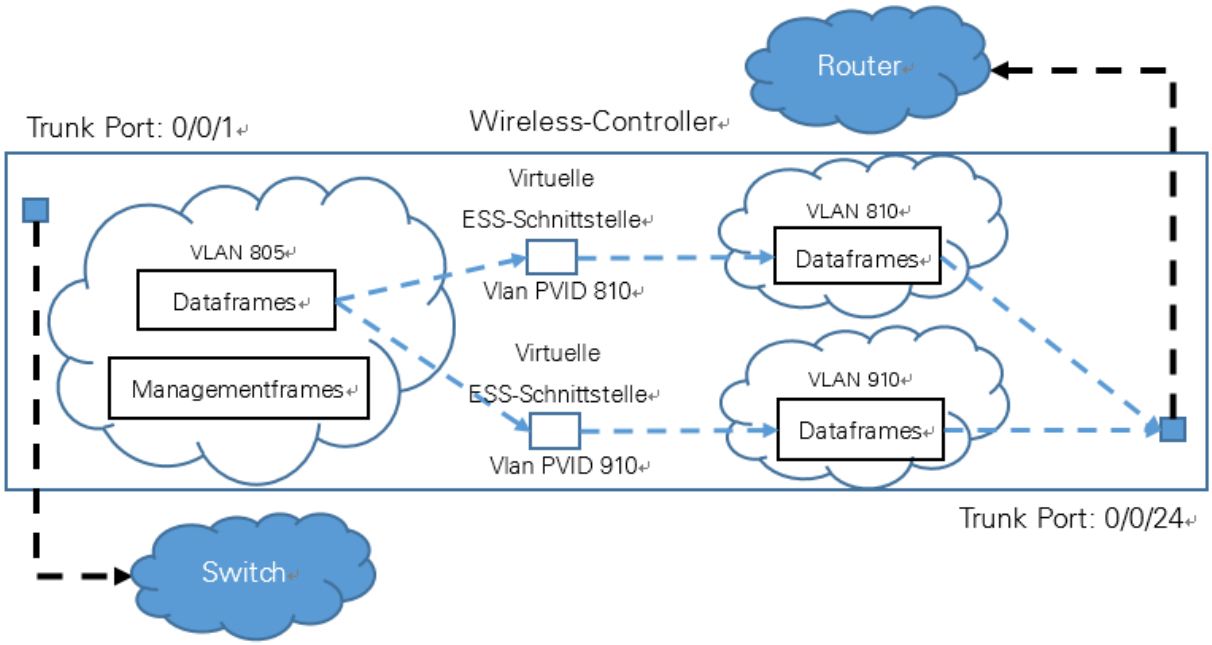

Abbildung 7: Weiterleitungsverlauf innerhalb des WLAN-Controllers

Anhand der Abbildung kann man deutlich ansehen, dass der letzte Ethernet-Port des WLAN-Controllers als Trunk Port eingestellt werden soll und mit VLAN 810 und VLAN 910 verknüpft wird. Nach der Einstellung können die enthüllten Dataframes über entsprechende VLANs an das oberstromige Gerät transportiert werden.

Konfiguration des Ethernet-Port an den Switch

Nach obigem Inhalt soll der letzte Ethernet-Port des Switches als Trunk Port eingestellt und mit VLAN 805 verknüpft werden. Mit dem Befehl „port link-type trunk“ kann der Port als Trunk Port eingestellt werden und man führt den Befehl „port trunk allow pass vlan 805“ aus, um den Ethernet-Port mit VLAN 805 zu verknüpfen.

```
<S5700> system-view
[S5700] interface gigabitethernet 0/0/24
[S5700-GigabitEthernet0/0/24] port link-type trunk
[S5700-GigabitEthernet0/0/24] port trunk allow-pass vlan 805
```

Wie der Ethernet-Port 0/0/24 sollen die anderen Ports des Switches mit VLAN 805 verknüpft, aber als Access Port eingestellt werden, um die VLAN-Tags abzuziehen. Mit dem Befehl „port default vlan 805“ werden die Ports mit VLAN 805 verknüpft. Beispielsweise für den Ethernet-Pool:

```
[S5700] interface gigabitethernet 0/0/1
[S5700-GigabitEthernet0/0/1] port link-type access
[S5700-GigabitEthernet0/0/1] port default vlan 805
```

Wenn alle Konfigurationen an dem Switch erledigt wurden, kann man die Konfigurationen an dem WLAN-Controller durchführen.

Konfiguration des Ethernet-Port an den WLAN-Controller

Zuerst wird der letzte Ethernet-Port des WLAN-Controllers, der mit dem Switch verbunden ist, als Trunk Port eingestellt und im VLAN 805 hinzugefügt.

```
[AC6605] interface gigabitethernet 0/0/1
[AC6605-GigabitEthernet0/0/1] port link-type trunk
[AC6605-GigabitEthernet0/0/1] port trunk allow-pass 805
```

Danach wird der mit dem oberstromigen Gerät verbundene Ethernet-Port 0/0/24 im VLAN 810 und VLAN 910 hinzugefügt und gleichzeitig als Trunk Port konfiguriert. Die Konfigurationen können durch folgende Befehle erfolgen:

```
[AC6605] interface gigabitethernet 0/0/4
[AC6605-GigabitEthernet0/0/24] port link-type trunk
[AC6605-GigabitEthernet0/0/24] port trunk allow-pass 810 910
```

Bisher wurden alle Konfigurationen über die Interconnection beschafft. Im folgenden Inhalt werden die Konfigurationen über unterschiedliche WLAN-Dienste vorgestellt.

4 Überblick über die Konfiguration der differenzierten WLAN-Dienste

Wenn die Konfiguration der Interconnection erledigt wurde, kann der WLAN-Controller die Konfigurationsdatei an den Wireless Termination Point, nämlich den Access Point, vergeben. Allerdings soll für die unterschiedliche Benutzergruppe das Wireless Netzwerk differenzierte WLAN-Dienste zur Verfügung stellen. Jeder Dienst hat seine eigene Eigenschaft wie beispielsweise das Service-Set Identifikation (SSID), das Authentifizierungsverfahren oder die Funkfrequenz. Die Virtual Access Point (VAP) Technologie ermöglicht es, dass VAP das Wireless LAN in mehrere Broadcast-Domänen aufteilt, das Äquivalent von Ethernet VLANs. Die VAPs simulieren mehrere Access Points auf einen physikalischen Access Point und jeder VAP hat eine eindeutige SSID. Das heißt, ein VAP ist eine Funktionseinheit an einem physikalischen Access Point und die mit entsprechendem VAP verbundene SSID bietet einen Zugang für unterschiedliche Benutzergruppen. Darüber können die unterschiedlichen Benutzergruppen verschiedene Netzwerkressourcen genießen. Wenn die Benutzer eine SSID entdecken und stellen eine Verbindung mit der entdeckten SSID her, verbindet der Benutzer sich zu dem entsprechenden VAP. Man kann es so konfigurieren, dass ein VAP mit nur einem einzigen VLAN verbunden ist, oder mehrere VAPs teilen sich nur einen VLAN. Ebenso wie bei der VLAN-Kommunikation wird der Datenverkehr zwischen dem Access Point und dem WLAN-Client über VLAN-Tagging erzielt. Dieser Prozess wird im nachfolgenden Kapitel ausführlich vorgestellt. Zuerst muss man wissen, wie ein VAP aufgebaut wird [5].

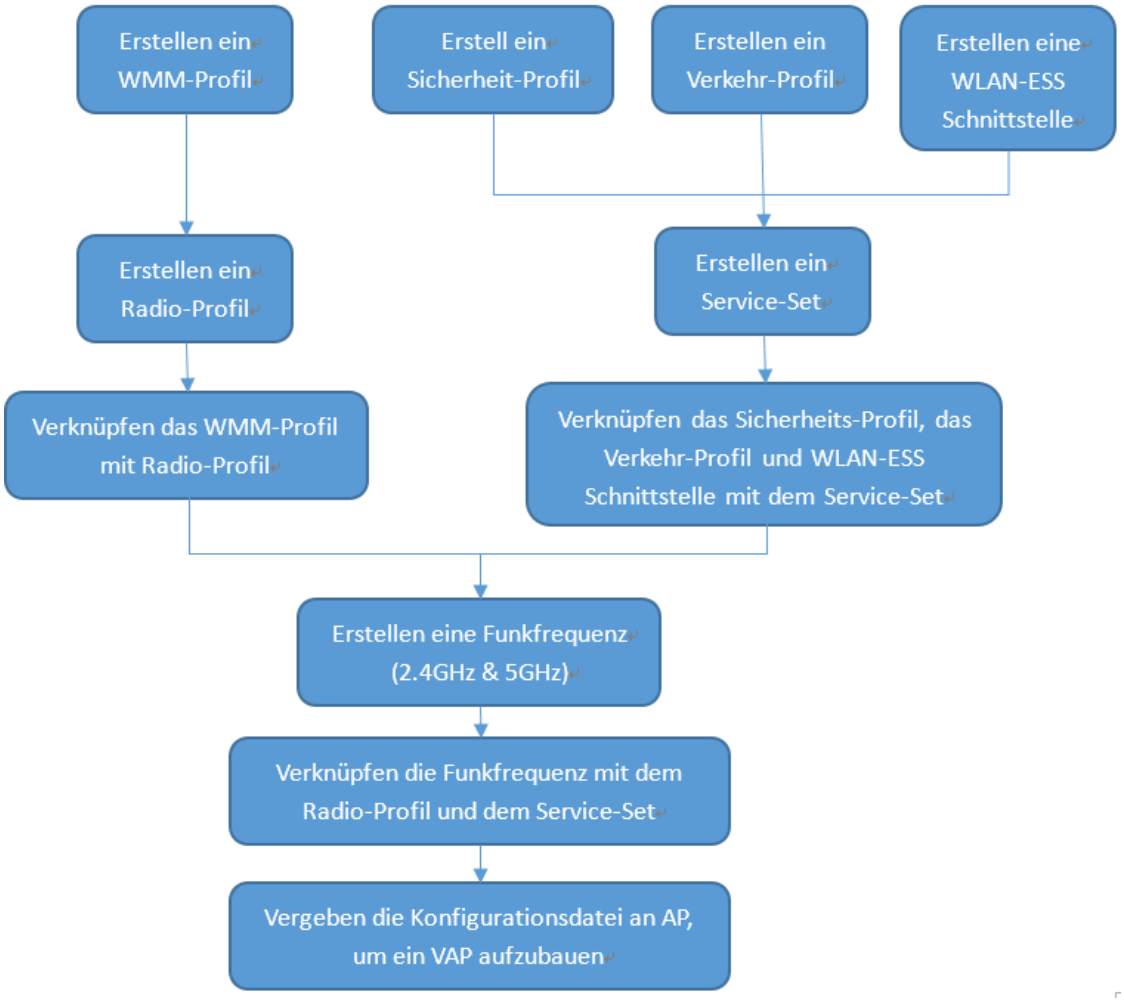

Abbildung 8: Konfigurationsablauf eines VAP

Nach der Unternehmensanforderung soll das Wireless-Netzwerk drei VAPs für die Benutzer zur Verfügung stellen. Ein VAP bietet einen Zugang für die Rechner und besitzt einige VLAN 810. Wenn die Benutzer mit den Mobilgeräten, wie Mobiltelefone oder Tablet, auf das drahtlose Netzwerk zugreifen möchten, müssen sie ihre Identifikation über eine spezielle Anwendung authentifizieren, erst dann können sie eine Verbindung herstellen. Man muss zwei VAPs für diese Benutzergruppen bereitstellen. Einer dieser VAPs ist ohne Authentifizierungsprozess, jedoch werden die Benutzer an eine Authentifizierungswebsite zwangsweise umgeleitet, um den Authentifizierungsclient herunterzuladen. Wenn die Identifikation von dem Benutzer erfolgreich war, kann er auf den andren VAP zugreifen. Über den neuen verbundenen VAP können die Benutzer ein normales drahtloses Netzwerk verwenden. Die zuvor beschriebenen zwei VAPs teilen sich nur einen VLAN, nämlich den geplanten VLAN 910.

Aber unter jedem VAP gibt es noch eine logische Schnittstelle, um die unterschiedlichen VAPs abzutrennen. Diese logische Schnittstelle ist die sogenannte WLAN-ESS Schnittstelle. Ihre Funktionsweise wird im nachfolgenden Inhalt vorgestellt. Außerdem stellt der Access Point für die VAPs zwei Funkfrequenzen mit 2,4 GHz oder 5 GHz zur Verfügung, egal ob die VAP für die Rechner bereitgestellt werden oder für die Mobilgeräte. Die Funkfrequenz mit 5 GHz hat eine höhere Geschwindigkeit als 2,4 GHz, aber die meisten alten Geräte unterstützen die Funkfrequenz mit 5 GHz nicht. Daher muss man die beiden Funkfrequenzen anbieten, um die Kompatibilität des drahtlosen Netzwerks zu berücksichtigen.

Die gewünschte Planung des drahtlosen Netzwerks wird in folgender Abbildung angezeigt.

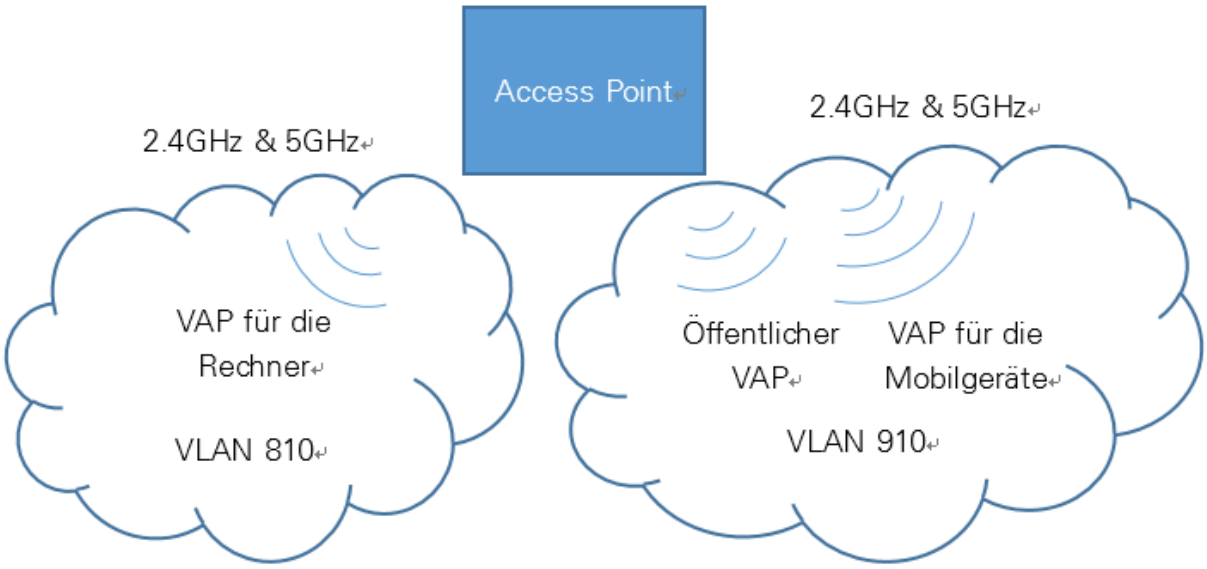

Abbildung 9: Gewünschte Planung des drahtlosen Netzwerks

In diesem Abschnitt werden Konfigurationsablauf des VAPs und eine gesamte Planung für die VAP-Struktur vorgestellt. Jetzt kann man mit dem WMM-Profil beginnen.

5 WLAN-Dienstgüte

Gemäß dem Standard 802.11 werden alle Datenpakete mit gleicher Priorität vom Gerät behandelt. Wegen der Netzwerkumgebung steht hier eine unterschiedliche Geschwindigkeit für die Datentransportierung zur Verfügung. Wenn die Bandbreite ausreichend bereit oder frei ist, geht die Transportierung glatt vonstatten und ohne Verzögerung. Aber wenn die Anzahl der Benutzer aufsteigend ist, führt es zur Verzögerung oder zum Verlust der Datenpakete. Der Datenverlust oder eine Datenverzögerung hat einen großen Einfluss auf die Benutzer, zum Beispiel, wenn die Benutzer eine Echtzeitanwendung, wie Videostreaming oder VoIP (Voice over IP) verwenden. Jedoch wenn die Datenverzögerung bei einem E-Mail-Dienst auftritt, dann hat das wenig Einfluss auf den Benutzer. Weil der Standard 802.11 kein differenziertes Datentransportierungsverfahren anbieten kann, verabschiedete das Wi-Fi Alliance einen neuen Standard, dass als Wi-Fi Multimedia (WMM) bezeichnet wird. WMM definiert ein differenziertes Datentransportierungsverfahren, das als „DiffServ" bezeichnet wird [5]. Damit wird jedes Paket mit dem Prioritätslabel markiert. Das bedeutet, Datenpakete mit höherer Priorität werden gegenüber einem Datenpaket mit einer niedrigeren Priorität bevorzugt behandelt. Um die „DiffServ" verstehen zu können, muss man zuerst den Kollisionsvermeidungsmechanismus bei Standard 802.11 verstehen. Die dargestellte Struktur ist der Entwicklungsprozess des Mechanismus.

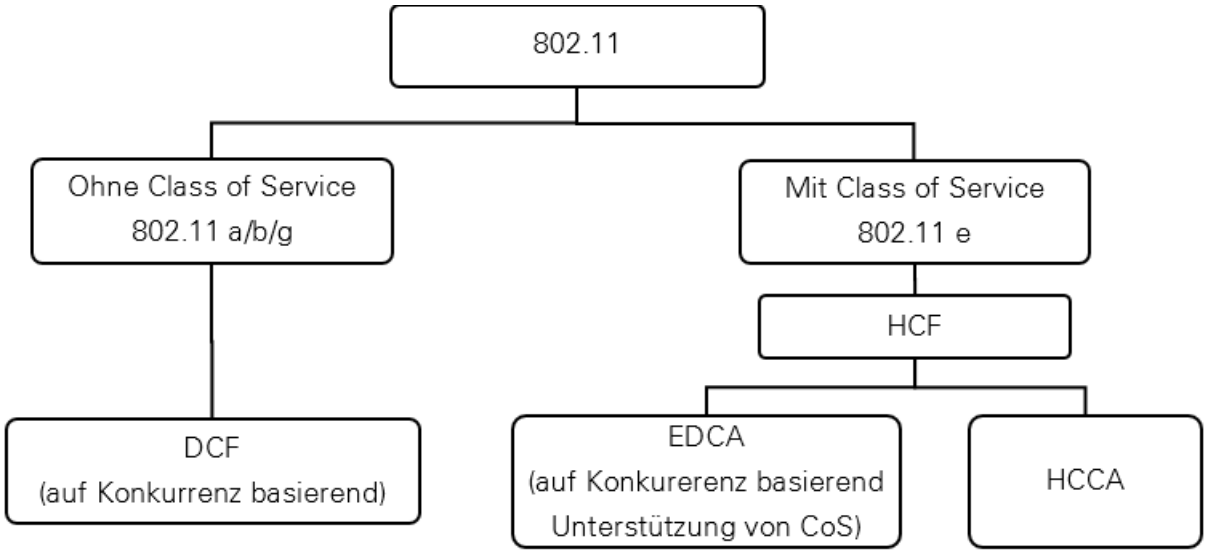

Abbildung 10: Entwicklungsprozess der Kollisionsvermeidungsmechanismen

5.1 Dienstgüte (QoS) gemäß 802.11

Distributed Coordination Function (DCF)

Aufgrund der Kollisionen in einer drahtlosen Umgebung ist es schwerer, ein Netzwerk zu erkennen, als in einem mit Kabel aufgebauten Netzwerk. Deshalb benutzt man eine auf Back-off basierte Kollisionsvermeidungstechnik (CSMA/CA) anstatt den normalen Kollisionserkennungsmechanismus (CSMA/CD). Dazu ist die Distributed Coordination Function (DCF) der Hauptbestandteil von CSMA/CA als ein unbedingter Mechanismus.

Zuerst muss jeder Wireless Benutzer das drahtlose Medium abhören. Wenn das Medium von anderen Benutzern besetzt wird, muss er warten, bis die laufende Übertragung zu Ende ist. Wenn kein Medienzugriff der anderen Station in einem Zeitraum DIFS (Distributed Inter Frame Space) vorkommt, beginnt die Station einen sogenannten Back-off Prozess. In einem Back-off Prozess wird eine zufällige Integralzahl aus einem CW ausgewählt. CW steht für Contention Window. Durch die Formel Back-off Time=Random (CW)*Slot Time wird die Wartezeit, nämlich die Back-off Wartezeit, ermittelt. Slot Time ist vom jeweiligen PHY-Typ abhängig und wird von diesem festgelegt. Nach der Bestimmung der Wartezeit beginnt ein Count-down Prozess für jeden freien Slot. Wenn im Verlauf des Back-off Prozesses ein Medienzugriff einer anderen Station erkannt wird, wartet der Count-down Prozess bis zum Ende der Übertragung. Nachdem das Medium für die Dauer eines weiteren DIFS nicht mehr belegt ist, setzt sich der Count-down Prozess fort. Sobald der Ablauf des Back-off ausgeführt wurde, beginnt die Station eine Übertragung. Die Größe von Contention Window wird von den zwei vorgegebenen Werten CW_{min} und CW_{max} ermittelt [4].

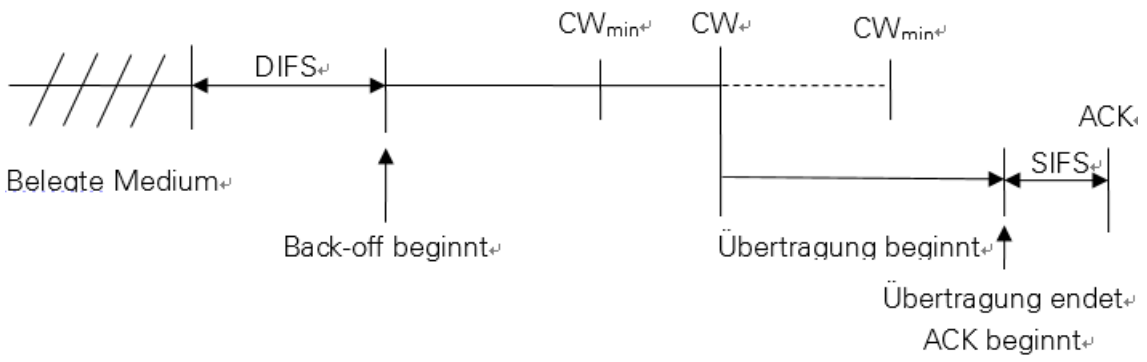

Abbildung 11: Funktionsweise der DCF

Nach der Übertragung der Daten wartet der Benutzer eine kurze Zeit, die als Short-Inter-Frame-Space (SIFS) genannt wird, um eine Bestimmung (ACK) für eine erfolgreiche Übertragung vom Empfänger abzuwarten. Wenn keine Bestimmung aus dem Empfänger zurückgemeldet wird, wiederholt der Sender die Übertragung nach einer weiteren Back-off- Wartezeit. Und die maximale Wiederholungsanzahl wird von einem vorgegebenen Wert beschränkt.

Die DCF-Technik definiert nur einen Kollisionsvermeidungsmechanismus für den Datenverkehr. Allerdings hat dieser Mechanismus keine Berücksichtigung auf die Prioritäten der Datenpakete. Bei der Entwicklung des drahtlosen Netzwerks wird die Implementierung von Sprachanwendungen von vielen Organisationen evaluiert. Dafür müssen aber zuerst technische Voraussetzungen erarbeitet werden. Deswegen wird die Arbeitsgruppe 802.11e, die Datenverkehrsklassen definiert, ausgegeben.

Im Vergleich mit dem früheren erarbeiteten Standard 802.11 hat Standard 802.11e eine Verbesserung an der Media Access Control (MAC) Teilschicht entwickelt, um eine QoS Funktion des Wi-Fi Netzwerk zu addieren. Diese Entwicklung hat die Einschränkung des Standards 802.11 über QoS Dienst gelöscht. Im IEEE 802.11e ist eine neue Technik, die als ,,Hybrid Coordination Function" bezeichnet wird. Diese wird an der MAC Teilschicht benutzt. HCF Technik ersetzt die DCF Zugriffstechnik, welche im Standard 802.11 a/b/g benutzt wird. Bei der HCF Zugriffstechnik kommen zwei folgende Zugriffsmethoden vor [4]:

- Enhanced Distributed Channel Access (EDCA) ist ein unbedingter Bestandteil von QoS, und dieser Mechanismus basiert auf Konkurrenz.
- Controlled Channel Access (HCCA) ist ein optionaler Bestandteil. Im Vergleich zum EDCA mit konkurrenzbasiertem Mechanismus benutzt HCCA einen Mechanismus, der auf dem Polling - Verfahren basiert. Und außerdem ist HCF ein optionales Modul für den Benutzer.

Eine herausragende Bedeutung kommt dem Begriff TXOP im Rahmen des HCFs zu. TXOP steht für die Zeitdauer, die eine Station zur Verfügung hat, um die Daten zu übertragen.

Enhanced Distributed Channel Access (EDCA)

EDCA ist ein auf Konkurrenz basierter Mechanismus vom HCF Rahmen. EDCA ist eine Erweiterung von DCF und definiert vier Stufen, die auch AC (Access Catalog) für Zugriffspriorität genannt werden. Das sind [5]:

- Data 0 (Best Effort, BE): Die meisten IP-Daten stehen in dieser Reihe. Dazu kommt ein mittlerer Durchsatz mit mittlerer Verzögerung.
- Data 1 (Background, BK): Die Daten, die nicht zeitkritisch sind, stehen in dieser Reihe.
- Data 2 (Video, VI): Zeitkritische Daten wie Video-Streaming gehören zu diesem Katalog. Wegen ihrer höheren Priorität ist keine Verzögerung vorhanden.
- Data 3 (Voice, VO): Echtzeitanwendungen wie VoIP stehen in dieser Reihe. Damit gibt es höchste Priorität und minimale Verzögerung.

Um die unterschiedlichen Zugriffsprioritäten des Datenverkehrs zu differenzieren, kommen hier vier Parameter vor. Es sind [4]:

- CW_{min}: Der minimale Wert von Content Window
- CW_{max}: Der maximale Wert von Content Window
- TXOP (Transmission Opportunity Limit). Da steht eine maximale Zeitdauer für eine Datenübertragung durch eine Station.
- AIFS (Arbitration Inter-Frame Spacing): Das hat eine gleiche Funktion wie DIFS im DCF Rahmen. Dadurch wird eine Wartezeit vor dem Back-off Prozess vorgestellt.

Im Allgemeinen besteht jede AC aus den vier Parametern mit jeweiligen einstellbaren Wert. Außer der Bedeutung TXOP existieren die anderen drei in dem DCF Rahmen bereits. Ein kleiner CW_{min}, CW_{max}, und AIFS führt zu einer höheren Priorität. Das bedeutet, dass die Wartezeit für die zeitkritische Anwendung, die zur Übertragung ansteht, verkürzt wird. Aus dem gleichen Grund bedeutet eine größere TXOP eine längere Laufzeit für die Echtzeitanwendungen mit hoher Priorität. Zusammengefasst kann man sagen, dass durch die Einstellung

der Parameter die Datenübertragung mit unterschiedlichen Zugriffsprioritäten und Dienstgüte realisiert wird.

5.2 Erstellen eines WMM-Profils

Die Konfiguration eines WMM-Profils kann durch folgende drei Schritte durchgeführt werden:

- Erstellung eines WMM-Profils
- Aktivierung des WMM-Profils
- EDCA Parametereinstellung für den Access Point

Damit wird der Arbeitsschwerpunkt auf den Schritt „EDCA Parametereinstellung für den Access Point“ gelegt.

Weil im nachfolgenden Schritt das WMM-Profil mit seinem entsprechenden Radio-Profil verknüpft werden soll, stellt man zwei WMM-Profile für die 2,4 GHz Funkfrequenz und 5 GHz Funkfrequenz zur Verfügung. Mit dem Befehl „wmm-profile {id *profile-id* | name *profile-name*}“ werden die beiden WMM-Profile generiert und mit dem Befehl „wmm enable“ werden sie aktiviert.

```
[AC6605] wlan
[AC6605-wlan-view] wmm-profile name 2.4G id 0
[AC6605-wlan-view-prof-2.4G] wmm enable
[AC6605-wlan-view] wmm-profile name 5G id 1
[AC6605-wlan-view-prof-5G] wmm enable
```

Normalerweise verwendet der EDCA Parameter einen standardmäßigen Wert gemäß der folgenden Tabelle [5].

Pakettypen	ECW_{max}	ECW_{min}	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

Tabelle 2: Standardmäßige EDCA Parameter

Allerdings wird in den Unternehmen das Videostreaming von den Mitarbeitern kaum benutzt, hingegen werden in den meisten Fällen viele Audiokonferenzen für die tägliche Arbeit bereitgestellt. Deswegen stellt man einen größeren TXOPLimit-Parameter für die Sprachanwendungen zur Verfügung, denen ein gleicher Wert wie beim Videostreaming vergeben wird. Beispielsweise wird die Parametereinstellung für das 2.4G WMM-Profil mit folgenden Befehlen durchgeführt:

```
[AC6605-wlan-view] wmm-profile name 2.4G id 0
[AC6605-wlan-wmm-prof-2.4G] wmm edca ap ac-vo aifsn 2 ecw ecwmin 2 ecwmax 3 txoplimit 94
[AC6605-wlan-wmm-prof-2.4G] wmm edca ap ac-vi aifsn 2 ecw ecwmin 3 ecwmax 4 txoplimit 94
[AC6605-wlan-wmm-prof-2.4G] wmm edca ap ac-be aifsn 3 ecw ecwmin 4 ecwmax 10 txoplimit 0
[AC6605-wlan-wmm-prof-2.4G] wmm edca ap ac-bk aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
```

Nach der Einstellung werden die Prioritäten der vier Datenpakete in einer Reihenfolge von AC_VO > AC_VI > AC_BE > AC_BK geordnet. Bisher wurden alle Konfigurationen für die WLAN-Dienstgütedurchgeführt.

6 WLAN-Funkfrequenzen

Für WLAN stehen hier zwei Frequenzbereiche zur Verfügung. Ein Frequenzbereich liegt bei 2,4 GHz und der andere bei 5 GHz. Beide Frequenzbereiche sind lizenzfrei zu verwenden. Das bedeutet, dass auf einem privaten Grund oder für eine öffentliche Benutzung die Gebühren nicht bezahlt werden müssen. Seit die Arbeitsgruppe 802.11a im Jahr 1991 verabschiedet wurde, wurde auch die Wi-Fi Technologie in den nachfolgenden Jahren immer weiterentwickelt. Danach wurden viele neue Arbeitsgruppen wie 802.11 b/g/n mit höheren Datenraten in der praktischen Umsetzung verarbeitet. Die nachfolgenden Inhalte fassen die wichtigsten Eigenschaften der Frequenzbereiche 2,4 GHz und 5 GHz zusammen. Anschließend wird über die Planung der optimalen Kanalauswahl, der Sendeleistung sowie das Kalibrierungsverfahren nach den Eigenschaften in diesem Kapitel diskutiert.

6.1 2,4 GHz-Frequenzband

Die untere Grenzfrequenz vom 2,4 GHz-Frequenzband ist 2403 MHz und die obere Grenzfrequenz ist 2482 MHz. Diese Frequenzbereiche werden von 13 verwendbaren Frequenzkanälen unterteilt [2]. Die Mittenfrequenzen der verwendbaren Frequenzkanäle sind in folgender Abbildung dargestellt:

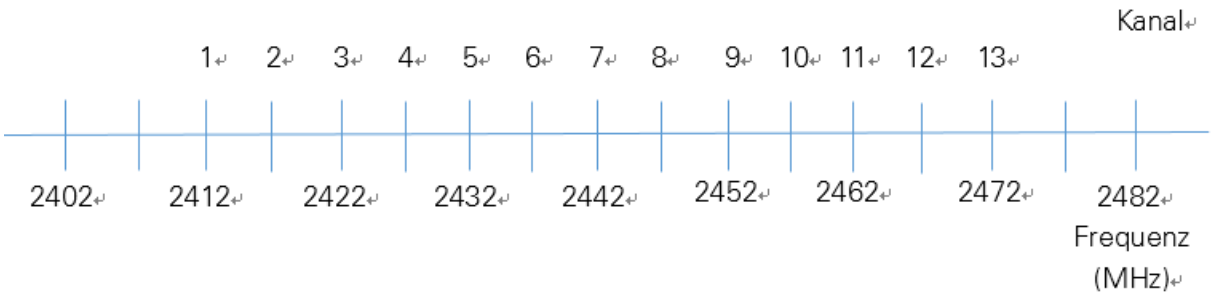

Abbildung 12: Frequenzspektrum der 2,4 GHz-Frequenzbereiche

Anhand der obigen Darstellung kann man deutlich sehen, dass die Mittenfrequenzen von einzelnen Frequenzkanälen nur einen Abstand von 5 MHz besitzen. Um die optimalen Frequenzkanäle auswählen zu können, die sich gegenseitig nicht beeinflussen, muss man über die von der jeweiligen 802.11-Arbeitsgruppe definierte Bandbreite nachdenken.

Die zwei Standards 802.11b und 802.11g funktionieren bei dem 2,4 GHz-Frequenzband. Die maximale Datenrate von dem Standard 802.11b kann 11Mbit/s erreichen, jedoch können in der Praxis wegen der Dämpfung selten mehr als 5Mbit/s erreicht werden. Weil die einzelne Kanalbreite von 802.11b 22 MHz ist, gibt es drei überlappungsfreie Kanäle, nämlich die Kanäle 1, 7, 13, um die Frequenzbereiche auszunutzen. Ähnlich wie das Standard 802.11b wirkt das Standard 802.11g auch beim 2,4 GHz-Frequenzband, jedoch besitzt es nur eine einzelne Kanalbreite von 20 MHz. Deswegen empfiehlt es sich bei 802.11g, die Kanäle 1, 5, 9, 13 einzustellen. Die optimalen Kanalaufteilungen werden in der folgenden Abbildung angezeigt:

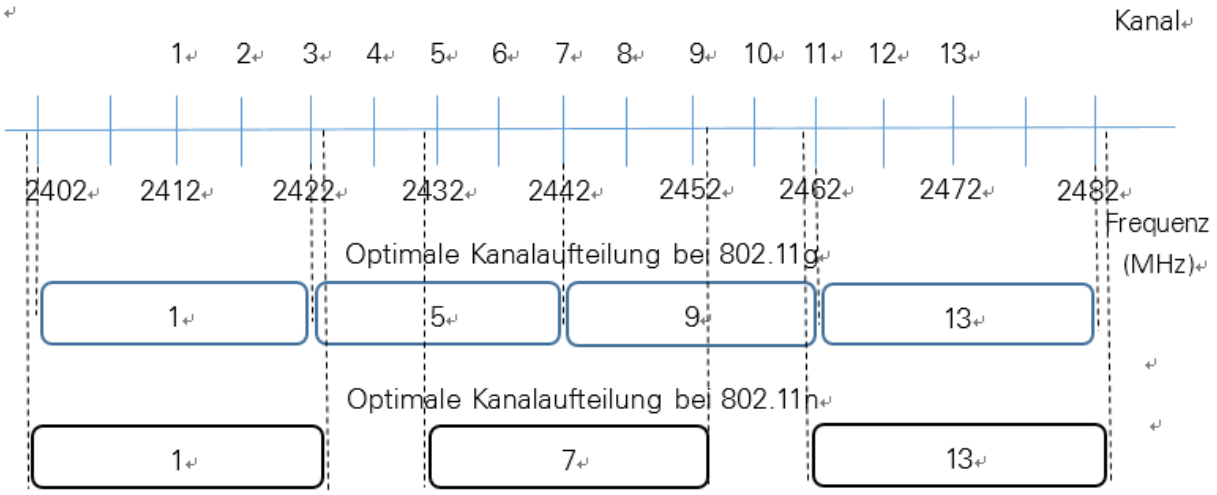

Abbildung 13: Optimale Kanalunterteilung beim 2,4 GHz-Frequenzband

Obwohl man bei Standard 802.11g mehrere Möglichkeiten für die Kanalwahl hat, wird das Standard 802.11g oft auf die Kanäle 1, 7 und 13 eingestellt. Der Hintergrund ist der, dass man die Kompatibilität zu dem Standard 802.11b berücksichtigen muss. Daher kann man so konfigurieren, dass die optimale Kanalwahl für das 2,4 GHz-Frequenzband die Kanäle 1, 7 und 13 sind.

6.2 5 GHz-Frequenzband

Im Gegensatz zu dem einzelnen Frequenzband von 2,4 GHz-Frequenzbereich werden die 5 GHz-Frequenzbänder in Deutschland in zwei Bereiche aufgeteilt, in 5,15 GHz bis 5,35 GHz

und 5,47 GHz bis 5,725 GHz [2]. Um die optimalen Kanäle auswählen zu können, muss man zuerst die Kanalbreiten von dem Standard 802.11n kennen.

Das Standard 802.11n sieht zwei Frequenzbereiche über 2,4 GHz sowie 5 GHz vor. Das bedeutet, es stehen zwei Frequenzbänder für 802.11n zur Verfügung. Aber die meisten billigen 11n-Geräte beherrschen nur die 2,4 GHz-Band mit einem verbesserten Modulationsverfahren. Dann bekommen die Geräte eine höhere Datenrate mit 72.2 Mbit/s in einem 20 MHz-Kanal und nicht nur 53 Mbit/s wie beim 802.11g [2]. Um eine höhere Datenrate zu erzielen, bietet 802.11n eine Kanalbandbreite von 40 MHz an. Die 40 MHz-Kanal wird von zwei nebeneinandergelegten 20 MHz-Kanälen verbunden, damit kann die maximale theoretische Datenrate in Höhe von 140 Mbit/s erreicht werden. Allerdings vermeidet man es in der praktischen Umsetzung, dass die Kanalbreite mit 40 MHz in 2,4 GHz-Frequenzbereiche eingerichtet wird. Weil man mit der 40 MHz-Kanalbreite die 2,4 GHz-Frequenzbereich nur zwei überlappungsfreie Kanäle aufteilen kann. Dazu wird die Kanalbreite von 40 MHz bei dem Standard 802.11n nur im 5 GHz-Frequenzspektrum eingerichtet. Hingegen kann die 20 MHz-Kanalbreite in beiden Frequenzbereichen, nämlich die 2,4 GHz-Frequenzbereich und 5 GHz-Frequenzbereich, eingerichtet werden.

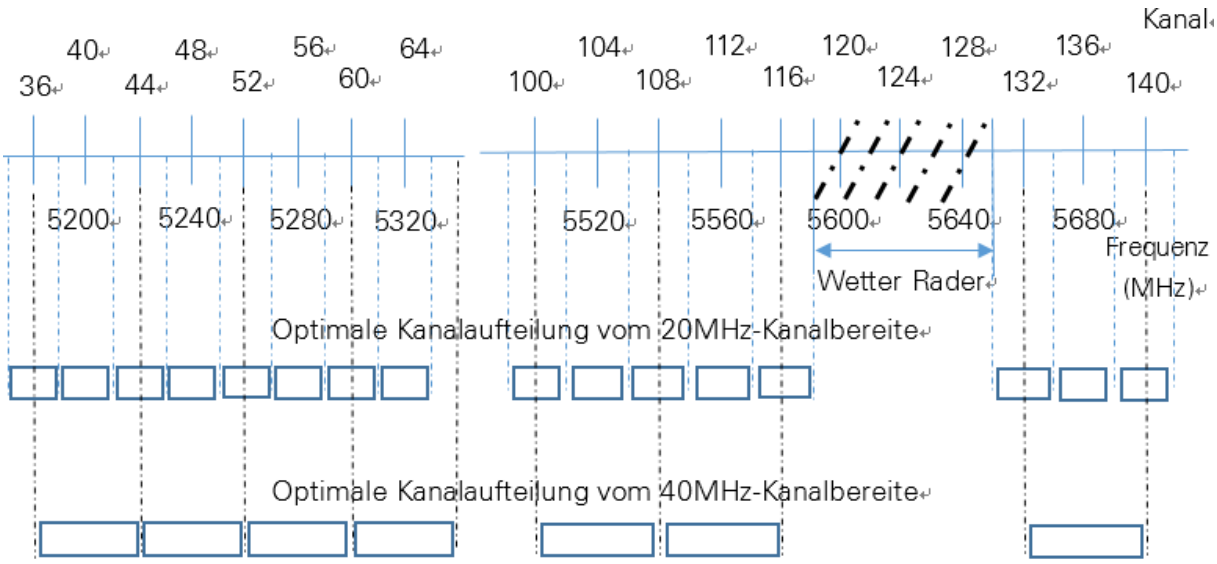

Abbildung 14: Optimale Kanalunterteilung beim 5 GHz-Frequenzband

Anhand dieser obigen Darstellung kann man deutlich sehen, dass die Mittenfrequenzen von einzelnen Frequenzkanälen einen Abstand von 20 MHz besitzen. Außerdem stellen die drei von Rader besetzten Kanäle 120, 124 und 128 [8] hier noch 16 Kanäle für die 20 MHz-Kanalbreite und sieben Kanäle für die 20MHz-Kanalbreite zur Verfügung. Für die tägliche Kalibrierung des Kanals muss man drei oder mehrere von den obigen beschriebenen Kanälen auswählen. Die ausgewählten Kanäle werden als standardmäßige Kanäle eingestellt. Dazu wird die tägliche Kalibrierung nach den ausgewählten Kanälen automatisch durchgeführt.

6.3 Reichweitenbetrachtungen

Die Reichweite der Funkzelle darf nicht zu groß oder zu klein sein. Wenn die Reichweite zu groß ist, führt es zu einer unerwünschten Überlappung mit einer anderen Funkzelle, die einen gleichen Kanal besitzt. Umgekehrt, wenn die Reichweite der einzigen Funkzelle zu klein ist, werden einige Orte von dem Funksignal bedeckt. Obwohl die Sendeleistung über die Funktion TPC (Transmit Power Control) nach der Wi-Fi-Umgebung automatisch eingestellt wird, muss man die Sendeleistung einer Funkzelle nach der praktischen Umsetzung manuell berechnen.

Um die Sendeleistung berechnen zu können, muss man die Freiraumdämpfung kennen. Nach einer groben Abmessung beträgt die Länge eines einzigen Büros acht Meter und die Breite beträgt drei Meter. Außerdem beträgt die Breite des Ganges noch etwa zwei Meter. Für jedes Büro wird der Access Point in der Mitte des Raumes angelegt. Der Entwurf wird durch folgende Abbildung angezeigt:

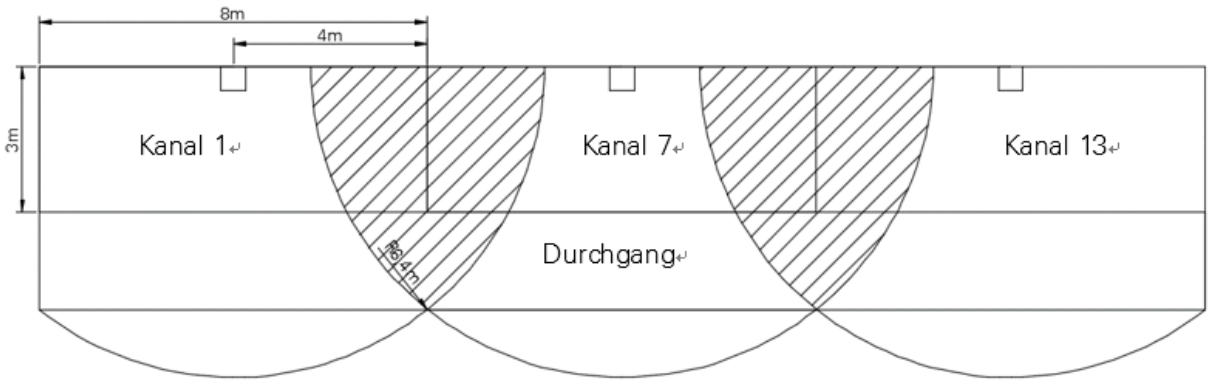

Abbildung 15: Reichweite einer einzigen Funkzelle

Nach einer groben Berechnung ergibt es sich, dass der maximale Abstand von dem Access Point 6,40 Meter beträgt. Durch den maximalen Abstand kann die maximale Freiraumdämpfung ausgerechnet werden. Die Freiraumdämpfung errechnet sich aus der Formel $A_{F.}$= 20 log (4 π d/λ) [dB] [1].

Symbol λ entspricht die Wellenlänge des Frequenzbandes und kann durch die Formel λ = c/f ausgerechnet werden. Hier entspricht c der Lichtgeschwindigkeit in Meter pro Sekunde und f der Frequenz in Hertz. Daher die Wellenlänge von 2,4 GHz-Frequenzband ergibt sich von λ = (3 × 10^8 m/s)/ 2,442GHz = 12,28 cm und für das 5 GHz-Frequenzband ergibt sich eine Wellenlänge von λ = (3 × 10^8 m/s)/ 5,4375 GHz = 5,51 cm. Danach kann die Freiraumdämpfung mit dem Abstand 6.4 Meter für die beiden Frequenzbänder ausgerechnet werden. Für das 2,4 GHz-Frequenzband ergibt sich die Freiraumdämpfung von $A_{F.}$= 20 log (4 π 6.5 m/12,28 cm) = 56.5 [dB] und für das 5 GHz-Frequenzband ergibt sich die Freiraumdämpfung von $A_{F.}$= 20 log (4 π 6.5 m/5,51 cm) = 63,4 [dB]. Außerdem führt die Wand auch zum Abfall der Sendeleistung. Wenn der Funk durch die Wand durchgeht, beträgt die Reduzierung der Signalstärke etwa 15dBi. Damit ergibt sich bei dem 2,4 GHz-Frequenzband hier eine maximale Dämpfung in einer Höhe von 71.6 dB und bei dem 5 GHz-Frequenzband ergibt sich eine Höhe von 78.4 dB.

Um eine gute Netzerfahrung anbieten zu können, liegt in der Regel die untere Begrenzung der Empfangsempfindlichkeit bei -60 dBm. Das heißt, wenn die Station die Stärke einer Funkzelle kleiner als 60dbm scannt, verbietet diese Funkzelle des zugehörigen Access Points, dass die Station in diese Funkzelle eintritt. Deswegen n muss die Sendeleistung bei dem 2,4 GHz-Frequenzband zu Mindesten 11.6 dBm (- 60 dBm – (-71.6 dB)) eingestellt werden, damit kann die fernste Station in die Funkzelle eintreten. Mit ähnlicher Weise muss die Sendeleistung bei dem 5 GHz-Frequenzband mindestens auf 18.4 dBm eingestellt werden. Zusätzlich sollen die beiden Werte einen standardmäßigen Wert des Antennengewinns von 4 dBi abziehen. Schließlich kann die Sendeleistung beim 2,4 GHz-Frequenzband von 7.6 dBm (11,6 dBm – 4 dBi) problemlos eingesetzt werden und beim 5 GHz-Frequenzband von 14.4 dBm (18.4 dBm – 4 dBi) eingestellt werden. Einfachheitshalber stellt man die beiden Sendeleistungen als 10 dBm und 15 dBm ein.

Manchmal hat die Station die Fähigkeit, sich innerhalb eines Netzwerks zu bewegen. Das wird als Roaming bezeichnet. Der in der Abbildung 15 mit einer schwarzen schrägen Linie markierte Bereich ist die sogenannte Wechselzone, und sie bietet die Möglichkeit, dass die Station sich innerhalb eines Netzwerks ohne Unterbrechung des Datenflusses bewegt. Ein Access Point-Wechsel wird automatisch an der Station durchgeführt, sobald sich die Station von einem Access Point entfernt und sich in die Reichweite eines anderen Access Point begibt. Der Prozess wird von dem Benutzer nicht wahrgenommen und hat keine Beeinflussung auf den Datenaustausch.

6.4 Erstellung eines Radioprofils

In diesem Abschnitt wird die Konfiguration von Frequenzband, Kanalwahl und Sendeleistung nach obigen vorgestellten Inhalten durchgeführt. Der Konfigurationsprozess wird durch die folgenden dargestellten drei Schritte durchgeführt:

- Erstellung eines Radioprofils
- Konfiguration der Sendeleistung für unterschiedliche Frequenzbänder
- Konfiguration der optimalen Kanäle für unterschiedliche Frequenzbänder
- Verknüpfung des Radioprofils mit dem WMM-Profil

Den ersten Schritt kann man direkt mit dem Befehl „radio-profile {profile-id | profile-name}“ durchführen. Beispielsweise ein Radio-Profil für das 2,4 GHz-Frequenzband kann so konfiguriert werden:

```
[AC6605] wlan
[AC6605-wlan-view] radio-profile name 2.4G id 0
```

Die Standards 802.11 b/g/n können bei dem 2,4 GHz-Frequenzband betrieben werden, deswegen werden die Funktypen des 2,4 GHz-Frequenzbandes als 802.11b/g/n konfiguriert. Für das 5 GHz-Frequenzband werden die Funktypen 802.11 a/n eingerichtet.

```
[AC6605-wlan-view] radio-profile name 2.4G id 0
[AC6605-wlan-radio-prof-2.4G] radio-type 80211bgn
[AC6605-wlan-radio-prof-2.4G] radio-profile name 5G id 1
[AC6605-wlan-radio-prof-2.4G] radio-type 80211an
```

Wenn die Radioprofile eingerichtet wurden, kann man jetzt die Sendeleistung der Funkzelle konfigurieren. Der Wert der Sendeleistung kann vom WLAN-Controller nach der drahtlosen Netzwerkumgebung automatisch eingestellt werden, oder man vergibt einen festen Wert für die Sendeleistung. Normalerweise verwendet man die automatische Einstellung vom WLAN-Controller statt einer manuellen Konfiguration. Der Grund dafür wird im nächsten Abschnitt „4.5 WLAN-Kalibierung“ vorgestellt. Der Betriebsmodus „Auto“ wird mit folgendem Befehl eingestellt:

```
[AC6605-wlan-radio-prof-2.4G] power-mode auto
```

Wenn man die Sendeleistung mit einem bestimmten Wert beim Administrator festlegt, muss man folgendermaßen konfigurieren:

```
[AC6605-wlan-radio-prof-2.4G] power-mode fixed
```

Dann wird die Konfiguration einer Sendeleistung durchgeführt.
Außerdem wurde im obigen Inhalt bereits erwähnt, dass eine Verbindung mit einer Signalstärke kleiner als -60 dBm verboten ist. Wenn die Station sich von einem verbundenen Access Point entfernt, muss die vorhandene Verbindung automatisch unterbrochen werden. Nach einer neuen Abfrage kann die Station eine neue Verbindung mit einem anderen Access Point aufbauen, dadurch wird ein verbesserter WLAN-Dienst angeboten. Daher sollte eine untere Begrenzung für die Signalstärke eingestellt werden. Mit den Befehlen:

```
[AC6605-wlan-radio-prof-2.4G] sta-forced-offline signal-strength switch enable
[AC6605-wlan-radio-prof-2.4G] sta-forced-offline signal-strength threshold -60
```

wird verhindert, dass die Anwender ihre vorhandene Verbindung, die mit einer Stärke schwächer als -60 dBm ist, weiterbenutzen. Dann wird die Verbindung automatisch gesperrt und die Station versucht eine neue Verbindung mit einem anderen Access Point aufzubauen. Ähnlich wie die Sendeleistung hat die Kanalwahl zwei Betriebsmodi. Man vermeidet es, für jeden Access Point einen bestimmten Kanal hinzuzufügen. Deswegen stellt man den Betriebsmodus der Kanalwahl auf „Auto". Dann muss man die standardmäßigen Kanäle für die automatische Einstellung auswählen. Beim 2,4 GHz-Frequenzband werden die drei optimalen Kanäle 1, 7, 13 ausgewählt. Das bedeutet, die automatische Kanalzuweisung für jeden Access Point wird auf die drei überlappungsfreien Kanäle übertragen. Dieser Prozess kann mit folgendem Befehl ausgeführt werden:

```
[AC6605-wlan-view] calibrate 2.4g 20mhz channel-set 1, 7, 13
```

Beim 5 GHz-Frequenzband mit einer Bandbreite von 20-MHz kann man drei oder mehrere von den 16 überlappungsfreien Kanälen auswählen. Hier stellt man die Kanälen 40, 44, 48, 52 als die standardmäßigen Kanäle ein.

```
[AC6605-wlan-view] calibrate 5g 20mhz channel-set 40, 44, 48, 52
```

Bisher wurden alle Konfigurationen über die Kanalwahl durchgeführt. Den letzten Schritt kann man mit dem folgenden Befehl ausführen:

```
[AC6605-wlan-radio-prof-2.4G] wmm-profile id 0
```

6.5 Kalibrierung der WLAN-Infrastruktur

Im Vergleich zum 5 GHz-Frequenzband hat das 2,4 GHz-Frequenzband weniger überlappungsfreie Kanäle. Die meisten Funkgeräte wie Bluetooth oder Mikrowelle senden auch auf dem 2,4 GHz-Frequenzband. Außerdem hat ein privat genutzter Access Point in manchen Fällen auch einen Einfluss auf die WLAN-Infrastruktur. Man bezeichnet solche Geräte als WLAN-Störenfriede und ordnet diese Funkgeräte in der Reihe der WLAN-Störer ein. Des-

wegen ist die tägliche Kalibrierung des Funknetzes notwendig, um Störungen von anderen Funkgeräten zu vermeiden. Die Störungsquelle wird in den zwei Katalogen eingeordnet, die Funkgeräte und die privat genutzten Access Points. Damit stehen hier unterschiedliche Kalibrierungsverfahrens zur Verfügung.

6.5.1 Störung von privat genutzten Access Points

Der Access Point, der sich nicht beim WLAN-Controller angemeldet hat, wird der Reihe der privat genutzten Access Points zugeordnet. Manchmal sendet solch ein Access Point über einen Kanal, der von einem angemeldeten Access Point bereits verwendet wird. Das heißt, die zwei Access Points teilen sich ein und denselben Kanal. Auf jeden Fall wird die Datenrate eingeschränkt, was zu einem langsamen WLAN führen kann. Deswegen muss der legale Access Point einen neuen Kanal auswählen, um den negativen Einfluss des illegalen Access Points zu vermeiden. Mit der Kalibrierungsverfahren „Rogue-AP“ [5] kann der beeinflusste legale Access Point auf einen anderen Kanal umgeschaltet werden. Der Kalibrierungsverlauf ist nachfolgend dargestellt:

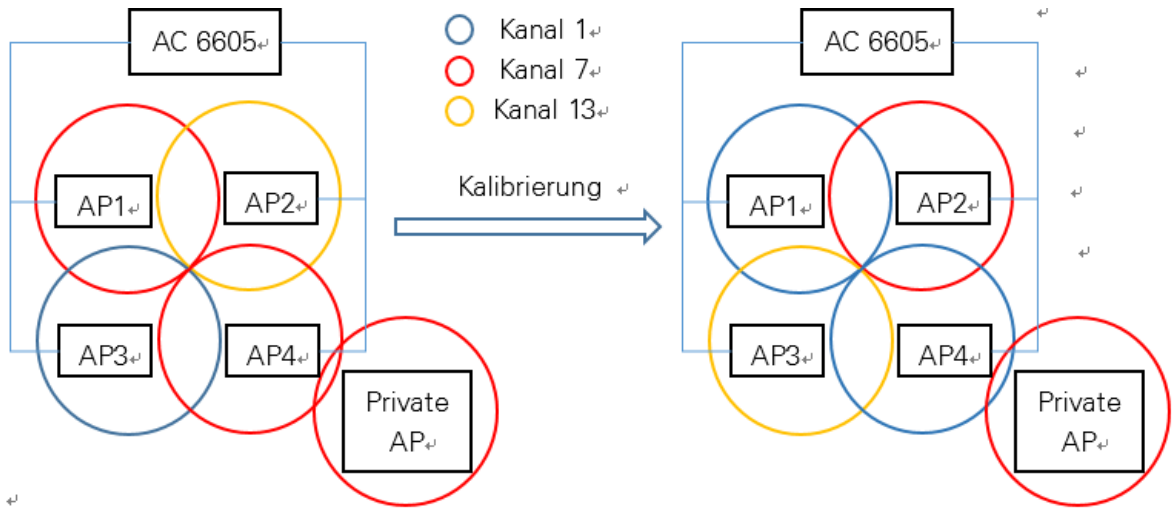

Abbildung 16: Kalibrierungsverfahren mit „Rogue-AP“

Um das Kalibrierungsverfahren „Rogue-AP“ zu aktivieren, muss man den Befehl „calibrate policy rogue-ap“ ausführen.

6.5.2 Störung durch andere Funkgeräte

Ähnlich wie der privat genutzte Access Point besitzen einige Funkgeräte auch das 2,4 GHz-Frequenzband. Zum Beispiel die vom Mikrowellenherd erzeugte Mikrowelle ist auch mit einer Frequenz von 2,4 GHz versehen. Deswegen muss der legale Access Point es vermeiden, denselben Kanal wie der Mikrowellenherd zu verwenden. Mit der Kalibrierungsverfahren „Non-WIFI“ [5] können die Störungen von solchen Geräten vermieden werden.

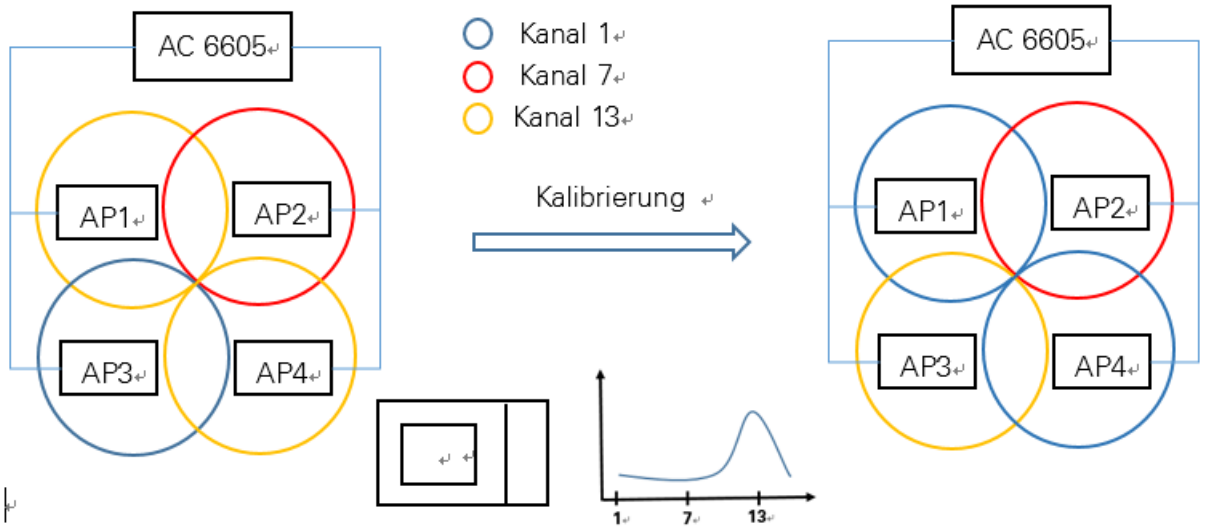

Abbildung 17: Kalibrierungsverfahren mit „Non-WIFI“

Anhand der obigen vorgestellten zwei Kalibrierungsverfahren kann man deutlich sehen, dass die Veränderung des Kanals beim WLAN-Controller automatisch durchgeführt wird. Deswegen stellt man den Betriebsmodus der Kanalwahl auf „Auto“ statt „Fixed“. Ähnlich wie die Kanalwahl sollte auch die Sendeleistung von jeder Funkzelle durch den WLAN-Controller automatisch eingestellt werden. Dazu gibt es folgende Fälle. Wenn ein neuer Access Point zur vorhandenen WLAN-Infrastruktur zusätzlich hinzufügt wird, sollten die Sendeleistungen von ihrem benachbarten Access Point nach der echten Funknetzumgebung verkleinert werden. Umgekehrt, wenn ein Access Point von der WLAN-Infrastruktur abgezogen wird, sollte sich die Sendeleistung von ihrem benachbarten Access Point automatisch vergrößern. Mit einem festen voreingestellten Wert kann sich die Sendeleistung nicht verändern. Daher ist eine automatische Regulierung der Sendeleistung beim WLAN-Controller geeignet für die WLAN-Infrastruktur.

Zuletzt sollte eine richtige Kalibrierungszeit für das Funknetzwerk eingestellt werden. Weil das Kalibrierungsverfahren für ein allgemeines Funknetz zu einer kurzen Unterbrechung des Datentransports führt. Die Kalibrierungszeit sollte in der Nacht eingestellt werden, somit steht hier kein negativer Einfluss an der täglichen Arbeit an. Deshalb stellt man die Kalibrierungszeit auf 23:00 Uhr mit folgendem Befehl ein:

```
[AC6605-wlan-view] calibrate enable schedule time 23:00:00
```

Bisher wurden alle Inhalte über die WLAN-Funkfrequenz vorgestellt. Im nächsten Abschnitt wird der Sicherheitsmechanismus des drahtlosen Netzwerkes beschrieben.

7 WLAN-Sicherheit

Funksignale können eine gewisse Reichweite erzielen. Das heißt, jeder kann diese Signale empfangen, sogar abhören und stören. Um die Störung oder das Abhören zu vermeiden, werden WLANs mit Verschlüsselung betrieben. Auch um die Qualität und Sicherheit des drahtlosen Netzwerkes zu garantieren, sollte die Zugriffsgenehmigung von einem Authentifizierungsverfahren eingeschränkt werden. Nur die Benutzer mit legalen Identifikationen dürfen auf das drahtlose Netzwerk zugreifen. Seit dem bei dem 802.11-Grundstandard vorgesehenen WEP-Verfahren werden bis heutige für die genutzte 802.11-Erweiterung vielfältige Sicherheitsmechanismen zur Verfügung gestellt. In diesem Abschnitt wird ein geeigneter Sicherheitsmechanismus für die WLAN-Infrastruktur ausgewählt. Zuerst wird ein Überblick über den Sicherheitsmechanismus gegeben.

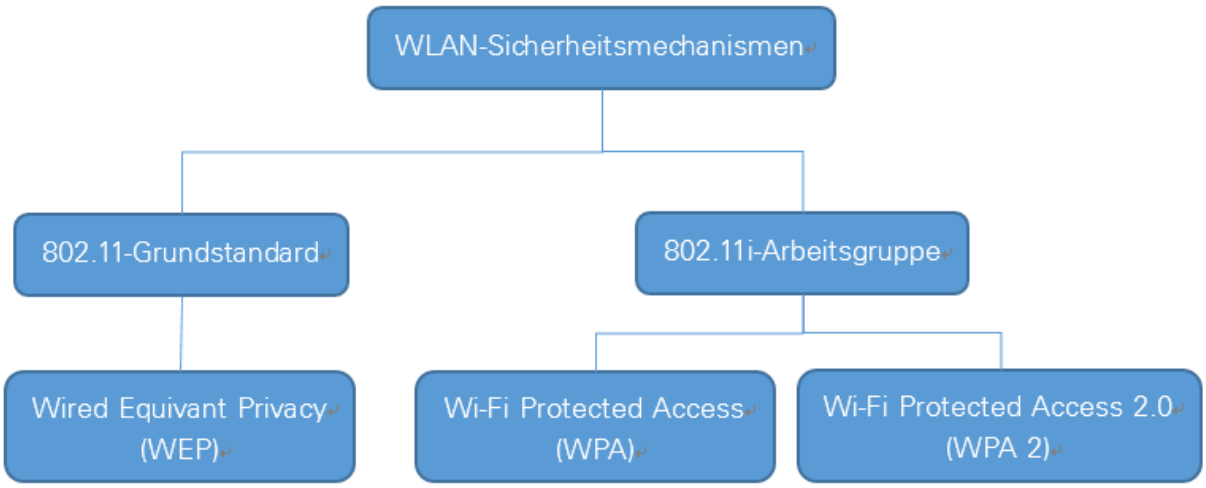

Abbildung 18: WLAN-Sicherheitsmechanismen

7.1 WEP-Verfahren

Beim 802.11-Grundstandard wird das WEP-Verfahren eingesetzt. WEP steht für Wired Equivalent Privacy und liefert eine gewisse Sicherheit für das drahtlose Netzwerk.

Für die Datenverschlüsselung benutzt das WEP-Verfahren eine Stromchiffre, die auf RC4-Algorithmus basiert. Ein pseudozufälliger Bitstrom wird durch eine Verkettung generiert, die aus einem 24-Bit-Länge-Initialisierungsvektor und einem Schlüssel besteht. Anschließend

wird das Klardatenpaket mit dem Bitstrom durch XOR-Verknüpfung kombiniert [3]. Zuletzt wird das verschlüsselte Datenpaket übertragen.

Beim Authentisierungsverfahren von WEP kann zwischen „Open" und „Shared Key" gewählt werden [3]. Bei ,,Open" steht keine Authentisierung, das bedeutet, jeder kann sich mit dem WLAN verbinden. Für den „Shared Key" Modus wird ein Challenge –Response Verfahren eingesetzt: Der Access Point stellt 128 zufällige Bytes her und sendet dieses Datenpaket ohne Verschlüsselung an einen Client. Der Client verschlüsselt das Datenpaket und sendet es dann zurück (Response). Wenn der AP die Response erfolgreich entschlüsselt hat, wird der Client authentisiert.

Allerdings, weil das Authentisierungsverfahren einfach geknackt werden kann und die 24-Bit-Länge für den Initialisierungsvektor viel zu kurz ist, wird das WEP-Verfahren heute nicht mehr als zuverlässige Sicherheit betrachtet. Deswegen ist das WEP-Verfahren nicht geeignet für die WLAN-Infrastruktur.

7.2 802.11i-Erweiterung

Aufgrund der Sicherheitsrisiken des WEP-Verfahrens arbeitet das IEEE die 802.11i-Erweiterung für den Sicherheitsmechanismus aus. Am Anfang definiert 802.11 ein optionales Verschlüsselungsverfahren als Übergangslösung, um die Sicherheitsrisiken des WEP-Verfahrens zu vermeiden. Die Übergangslösung wird als Temporary Key Integrity Protocol (TKIP) bezeichnet und dieses Verschlüsselungsverfahren basiert auch auf RC4-Algorithmus, somit lässt sich das Protokoll auf die meisten bestehenden WLAN-Produkte implantieren [1]. Das bedeutet, das TKIP - Verschlüsselungsverfahren hat eine gute Rückwärtskompatibilität zu den älteren WLAN-Produkten und bietet ein besseres Verschlüsselungsverfahren als das WEP-Verfahren.

Außerdem gibt es ein endgültiges Verschlüsselungsverfahren, das auf einen neuen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) basiert und in einem Modus Anwendung findet, der als Counter-Mode/CBC-MAC Protocol (kurz als AES-CCMP) bezeichnet wird. Im Gegensatz zum TKIP - Verschlüsselungsverfahren müssen alle 802.11-konformen WLAN-Produkte unterstützt werden. Deswegen wird das TKIP - Verschlüsse-

lungsverfahren von dem AES-CCMP- Verschlüsselungsverfahren als eine Übergangslösung ersetzt [1].

Für das Authentifizierungsverfahren unterstützt die 802.11-Erweiterung zwei Betriebsmodi. Einer ist der sogenannte Pre-Shared Key und der andere basiert auf dem Extensible Authentication Protocol (EAP). Der Unterschied zwischen den beiden Authentifizierungsverfahren ist, dass ersterer für kleine Netzwerke ohne Authentifizierungsserver geeignet sind, umgekehrt wird das auf EAP basierte Authentifizierungsverfahren von größeren WLAN benutzt, in denen ein zusätzlicher Authentifizierungsserver zur Verfügung steht.

7.3 Wi-Fi Protected Access

Der heutige generell bekannte WLAN-Sicherheitsmechanismus ist nicht der von IEEE verarbeitete 802.11i-Standard, sondern der sogenannte Wi-Fi Protected Access (WPA). WPA wurde als Quasisicherheitsstandard von der Wi-Fi Alliance verabschiedet und wird als Quasisicherheitsstandard betrachtet. Letztendlich wurde die 802.11i-Erweiterung als Teil des TKIP- Verschlüsselungsverfahrens weiter genutzt und nichts wurde verändert. Ein Jahr später wurde die neue WPA-Version von Wi-Fi Alliance verabschiedet und als WPA 2 bezeichnet. Dieses Mal ist WPA 2 auch an den 802.11i-Standard angelehnt. Im Vergleich zu der ersten Version benutzt WPA 2 ein Verschlüsselungsverfahren mit AES-CCMP, statt des TKIP- Verschlüsselungsverfahrens. Heutzutage wird WPA 2 mit dem Standard 802.11i gleichgesetzt.

Außerdem definieren WPA und WPA 2 zwei Begriffe für das Authentifizierungserfahren, nämlich das Personal-Mode und Enterprise-Mode. Die Personal-Mode ist ein sogenanntes PSK- Authentifizierungsverfahren, das sich für ein kleines drahtloses Netzwerk eignet. Umgekehrt setzt die Enterprise-Mode einen Authentifizierungsserver voraus, bei dem eine auf EAP basierte Client-Server-Authentifizierung durchgeführt wird. Deshalb eignet sich das auf EAP basierte Authentifizierungsverfahren für eine große WLAN-Infrastruktur [1]. Dieses Authentifizierungsverfahren ist im 802.1x-Standard spezifiziert und wird im nächsten Abschnitt ausführlich vorgestellt.

Letztendlich wird der WPA 2-Sicherheitmechanismus mit einem von Enterprise-Mode betriebenen Authentifizierungsverfahren für das unternehmensweite drahtlose Netzwerk ausgewählt.

7.4 Einstellung eines Sicherheitsprofils

Um den WPA 2- Sicherheitsmechanismus aktivieren zu können, sollte man zuerst ein Sicherheitsprofil erstellen. Zum Beispiel wird das Profil als „Huawei-Employee“ bezeichnet und hat folgenden Befehl:

```
[AC6605-wlan-view] security-profile name Huawei-Employee id 2
```

Danach wird die Sicherheitspolitik WPA 2 an dieses Profil durch folgenden Befehl hinzugefügt:

```
[AC6605-wlan-view-prof-Huawei-Employee] security-policy wp2
```

Allerdings steht beim Sicherheitsprofil keine ausführliche Konfiguration für das Authentifizierungsverfahren. Dieser Inhalt wird im nächsten Abschnitt vorgestellt.

7.5 802.1x-Authentifizierungsverfahren

Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN reicht die einfache Authentisierungsmethode mit PSK nicht aus. Wenn jeder den Schlüssel kennt, dann ist das WLAN praktisch offen. Der Sicherheitsstandard 802.1x stellt ein Rahmenwerk für Zugangskontrollen zur Verfügung, um die Geräte, die sich mit einem LAN oder WLAN verbinden möchten, zu authentisieren. Der Zugang zu den nicht angemeldeten Geräten wird so lange gesperrt, bis diese einen erfolgreichen Authentisierungsprozess passiert haben. Das vom 802.1x verwendete EAP-Protokoll beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentifizierungsdaten zwischen dem Benutzer und dem Authentifizierungsserver ausgetauscht werden. Deswegen wird das 802.1x-Standard häufig auch als EAP bezeichnet. Der Sicherheitsstandard 802.1x-Authentifizierungsstruktur besteht aus drei Instanzen, dem Supplicant, dem Authenticator und dem Authentifizierungsserver [1].

Der sogenannte Supplicant ist der Client, der eine Authentifizierungsabfrage aussendet. Der Access Point spielt die Rolle des Authenticators. Der Access Point bietet einen Netzwerkzugang für die Clients und leitet ihre Anfragen an den zentralen Authentifizierungsserver. Der

zentrale Authentifizierungsserver ist das Kernstück der Struktur und kommt in der Regel als RADIUS-Server zum Einsatz. Normalerweise spricht man bei der RADIUS-Authentifizierung von den drei großen „AAA“, diese stehen für Authentifizierung, Autorisierung und Accounting [1].

Die Authentifizierung kann man so verstehen. Im RADIUS-Server werden alle Kontodaten der Benutzer gespeichert. Wenn nur der vom Benutzer angegebene Benutzername und die Geheimzahl mit der im RADIUS-Server gespeicherten Kontoinformation gleich sind, wird der Netzwerkzugang über den Authenticator freigegeben. Bei der Autorisierung wird festgestellt, welchen Dienst der Anwender nutzen darf. Innerhalb einer WLAN-Infrastruktur werden mehrere Dienste angeboten, allerdings werden nicht alle pauschal hinter einer Authentisierung freigegeben. Dann macht es Sinn, die Berechtigung der Benutzer zu prüfen. Die Accounting-Funktion ermöglicht es, den Nutzungsrekorder des Benutzers zu dokumentieren. Danach kann die Nutzung abgerechnet werden.

Die Kommunikation zwischen Supplicant und Authenticator wird über das Extensible Authentication Protocol over LAN, kurz als EAPoL, durchgeführt und die Kommunikation zwischen Authenticator und Authentifizierungsserver erfolgt über in RADIUS-Paketen gekapselte EAP-Pakete, die auch als Extensible Authentication Protocol over RADIUS bezeichnet werden [3] [5].

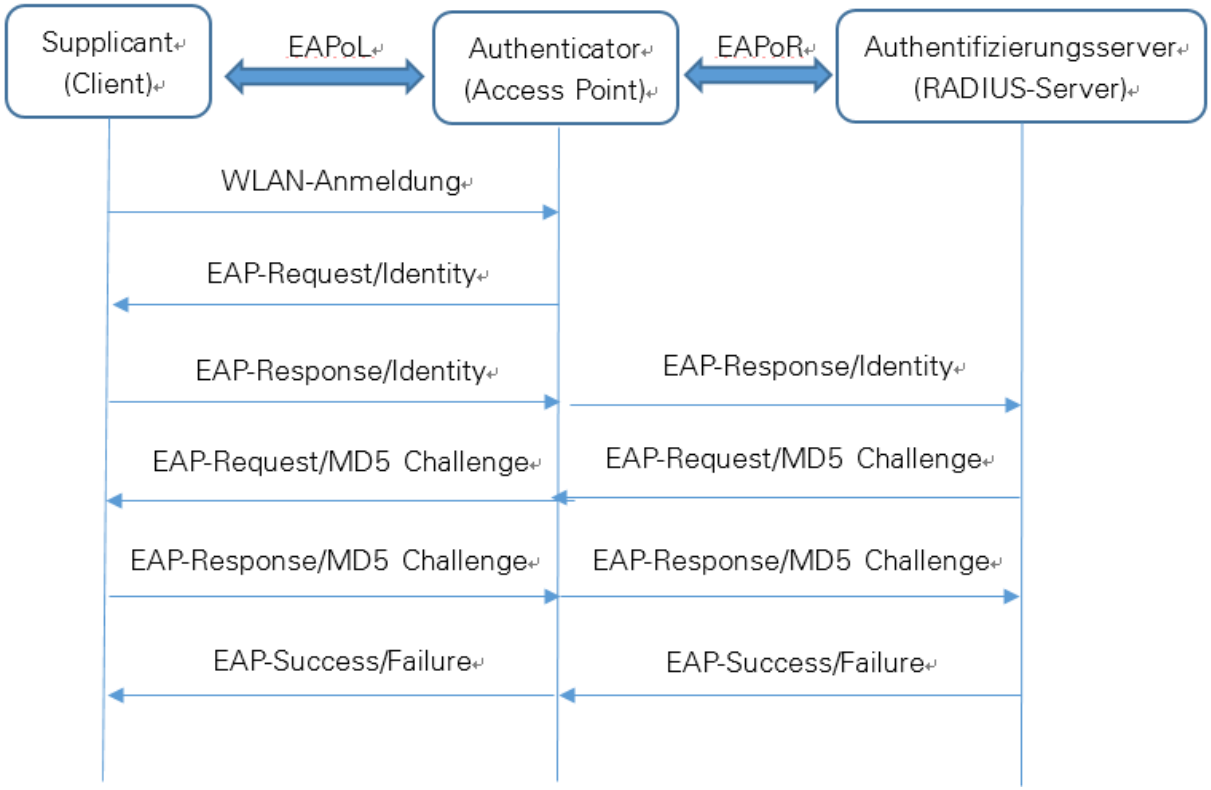

Abbildung 19: Authentifizierungsablauf

Der in der obigen Abbildung 19 angezeigte Authentifizierungsablauf ist EAP-Relay. Des Weiteren gibt es die EAP-Termination. EAP-Relay unterscheidet sich von der EAP-Termination nur im Verschlüsselungsverfahren-MD5, also, ob die Codierung und Decodierung der Benutzerdatei beim RADIUS-Server beschafft wurden. Dieses Verschlüsselungsverfahren ermöglicht es, den Benutzernamen und die Geheimzahl über den MD5-Hashing-Algorithmus zu codieren. Die Auswahl von EAP-Relay oder EAP-Termination ist abhängig von der Leistungsfähigkeit des RADIUS-Servers. Wenn in einer Infrastruktur ein einzelner RADIUS-Server zur Verfügung steht, kann man den EAP-Relay benutzen. Umgekehrt wird die EAP-Termination ausgewählt.

Normalerweise basiert die Zugriffsauthentifizierung der Benutzer auf der Benutzerdomäne. Im nächsten Abschnitt wird die Aufteilung der Benutzerdomäne ausführlich vorgestellt.

7.5.1 Auf Benutzerdomäne basiertes Authentifizierungsverfahren

Jedem Benutzer wird eine bestimmte Domäne zugeordnet. Wenn der Benutzer eine Verbindung herstellen möchte, muss der von ihm angegebene Benutzername in der Form wie „Benutzername @Domäne" sein. Anschließend wird ein mit der Benutzerdomäne entsprechendes Authentifizierungsverfahren aufgerufen. Wenn der vom Benutzer angegebene Benutzername ohne bestimmten Domäne – Name erscheint, wird er in der initialisierten Domäne zugeordnet. Beim System werden zwei initialisierte Domänen zur Verfügung gestellt. Eine wird als „Default" bezeichnet und wird für den Benutzer bereitgestellt, die andere, als „Defalt_Admin" bezeichnet, wird für den Administrator bereitgestellt.

Authentifizierungsverfahren für die Rechnerbenutzer

Um die von den Benutzern angegebenen Benutzernamen zu vereinfachen, werden die Rechnerbenutzer in der initialisierten Benutzerdomäne zugeordnet. Das heißt, die Rechnerbenutzer brauchen nur ihren Benutzernamen direkt eingeben, dann wird ein entsprechender Authentisierungsprozess aufgerufen. Um das Authentisierungsverfahren zu vervollkommnen, muss die Konfiguration durch folgende vier Schritte durchgeführt werden:

- Erzeugung einer Domäne
- Erzeugung eines Authentifizierungsschemas
- Konfiguration einer Vorlage für die RADIUS-Server
- Verknüpfung der Domäne mit Authentifizierungsschema und Vorlage

Weil die Rechnerbenutzer eine initialisierte Domäne verwenden, kann man den ersten Schritt direkt überspringen. Nach der Unternehmensanforderung wird die für Rechnerbenutzer bereitgestellte Domäne als „wlanaccess v2.0" bezeichnet und man erzeugt ein entsprechendes Authentifizierungsschema mit dem Namen „wlanaccess v2.0".

Die Authentifizierung erfolgt durch einen RADIUS-Server, daher wird der Betriebsmodus der Authentifizierung wie folgt konfiguriert:

```
[AC6605] aaa
[AC6605-aaa] authentication-scheme wlanaccessv2.0
[AC6605-aaa-authen-scheme-wlanaccessv2.0] authentication-mode radius
```

Ein weiteres Authentifizierungsverfahren ist die sogenannte lokale Authentifizierung. Dieses Verfahren wird im nachfolgenden Abschnitt vorgestellt.
Um das Benutzerkonto zu schützen, kann man die erlaubte maximale Versuchsanzahl für die Authentifizierung einstellen. Wenn die Ausfälle die Grenze überschreitet, wird das Benutzerkonto in einer voreingestellten Zeit gesperrt. Mit dem folgenden Befehl kann man das Authentifizierungswiederholungsintervall, die maximale Versuchsanzahl und die Sperrzeit einstellen.

```
[AC6605-aaa] remote-aaa-user authen-fail retry-interval 5 retry-time 3 block-time 5
```

Dieser Befehl bedeutet, dass das Authentifizierungswiederholungsintervall auf fünf Minuten eingestellt wurde und die maximale Versuchsanzahl lautet 3. Wenn die Authentifizierung immer noch nicht funktioniert, wird dieses Benutzerkonto in fünf Minuten gesperrt.
Danach folgen die Konfigurationen für die RADIUS-Server-Vorlage. In dieser Vorlage sollte die IP-Adresse des RADIUS-Servers und die IP-Adresse des Absenders vergeben werden, die die Authentifizierungsabfragen aussendet. In der WLAN-Infrastruktur werden die Authentifizierungsabfragen der Benutzer über WLAN-Controller weitergeleitet. Deswegen ist der WLAN-Controller der sogenannte Absender.

```
[AC6605] radius-server template wlanaccessv2.0
[AC6605-radius-wlanaccessv2.0] radius-server authentication 10.201.15.58 source ip-address 10.221.96.1
```

Außerdem verwendet der RADIUS-Server beim Austausch von Authentifizierungspaketen einen MD5-Hashing-Algorithmus, um wichtige Daten, wie die Geheimzahl oder den Benutzernamen, zu verschlüsseln. Um die Identität von beiden Seiten garantieren zu können,

muss der WLAN-Controller und der RADIUS-Server einen gleichen Schlüssel verwenden. Deswegen muss ein Schlüssel, der an dem RADIUS-Server bereits konfiguriert wurde, auch beim WLAN-Controller eingerichtet werden. Zum Beispiel verwenden die beiden Seiten „Hallo“ als „Shared-Key“:

```
[AC6605-radius-wlanaccessv2.0] radius-server shared-key cipher Hello
```

Zuletzt sollte die Domäne mit dem Authentifizierungsschema und der RADIUS-Server-Vorlage verknüpft werden:

```
[AC6605] aaa
[AC6605-aaa] domain default
[AC6605-aaa-domain-default] authentication-scheme wlanaccessv2.0
[AC6605-aaa-domain-default] radius-server template wlanaccessv2.0
```

Authentifizierungsverfahren für die Mobilgerätebenutzer

Nach der Unternehmensanforderung sollten die Benutzer vor der Authentifizierung einen speziellen Authentifizierungsclient herunterladen. Über diesen speziellen Authentifizierungsclient wird der Authentifizierungsprozess durchgeführt. In dem zweiten Abschnitt „Ein Überblick über Konfiguration der differenzierten WLAN-Dienste“ wurde bereits erwähnt, dass im VLAN 910 zwei VAPs zur Verfügung stehen. Der erst VAP wird für den Authentifizierungsclient bereitgestellt und dieser VAP ist für alle Leute geöffnet. Das bedeutet, man kann direkt eine Verbindung mit diesem VAP ohne Authentifizierungsprozess herstellen. Damit kann man den speziellen Authentifizierungsclient kostenlos herunterladen. Wenn der Client erfolgreich heruntergeladen wurde, sollten die Benutzer manuell zum anderen VAP umschalten. Im zweiten VAP müssen die Benutzer sich über den Authentifizierungsclient authentifizieren, um die Netzwerkressourcen verwenden zu können. Ähnlich wie die Rechnerbenutzer erfolgt die Authentifizierung auf dem RADIUS-Server.

Zuerst muss man eine Benutzerdomäne, die kein Authentifizierungsverfahren benötigt, erzeugen. Nach der Unternehmensanforderung wird die Domäne als „Huawei-Init“ bezeichnet,

und für diese Domäne steht kein Authentifizierungsverfahren zur Verfügung. Deshalb wird folgendermaßen konfiguriert:

```
[AC6605-aaa] domain Huawei-Init
[AC6605-aaa] authentication-scheme Huawei-Init
[AC6605-aaa-authen-scheme-Huawei-Init] authentication-mode none
```

Wenn die Benutzer auf diesen VAP zugreifen, werden sie zwangsweise an eine bestimmte Webseite weitergeleitet. Diese Website wird von einem Portal-Server angeboten. Dort kann man den Authentifizierungsclient kostenlos herunterladen. Deswegen sollte man die IP-Adresse und URL des Portal-Servers an den WLAN-Controller so konfigurieren:

```
[AC6605] web-auth-server Huawei-Init
[AC6605-web-auth-server-Huawei-Init] server-ip 1.1.1.1 port 50100
[AC6605-web-auth-server-Huawei-Init] URL
http://unibyod.huawei.com/custom/download.html
```

Zuletzt muss man den Portal-Server mit der von den Mobilgeräten genutzten VLANIF-Schnittstelle, nämlich dem VLANIF 910, verknüpfen. Dann wird die Konfiguration des Portal-Servers aktiviert.

Der Authentifizierungsclient bietet ein Portal für den Authentifizierungsprozess an. Wenn man diese Anwendung erfolgreich in den Mobilgeräten installiert hat, muss man an den anderen VAP umschalten. Im zweiten VAP wird eine Authentifizierung der Benutzeridentität über den Authentifizierungsclient via RADIUS durchgeführt. Ähnlich wie die Konfiguration der Domäne für die Rechnerbenutzer erzeugt man auch eine Domäne für die Mobilgerätebenutzer. Allerdings wird diese als „Huawei-Employee“ bezeichnet. Und bei der Konfiguration über das Authentifizierungsschema oder die RADIUS-Server-Vorlage sind alle anderen Teile gleich wie bei der Konfiguration für die Rechnerbenutzer, außer der Name. Letztendlich sieht die Huawei-Employee Domäne so aus:

```
[AC6605-aaa] domain Huawei-Employee
[AC6605-aaa-domain-Huawei-Employee] authentication-scheme Huawei-Employee
[AC6605-aaa-domain-Huawei-Employee] radius-server template Huawei-Employee
```

Zusammenfassend für die Mobilgerätebenutzer stehen hier zwei Domänen, nämlich die „Huawei-Init“ und die „Huawei-Employee“. Bei der Domäne „Huawei-Init“ braucht man keine Authentifizierung und darf den Authentifizierungsclient benutzen. Bei der Domäne „Huawei-Employee“ wird ein Authentifizierungsverfahren durchgeführt und man darf die Netzwerkressourcen nach einer erfolgreichen Authentifizierung benutzen.

Authentifizierungsverfahren für den Administrator

Beim Authentifizierungsverfahren des Administrators hat man zwei Möglichkeiten. Eine ist die lokale Authentifizierung und die andere ist die RADIUS-Authentifizierung. Bei der lokalen Authentifizierung werden alle Benutzerinformationen an dem WLAN-Controller statt an dem RADIUS-Server konfiguriert. Der Administrator kann sich mit dem lokalen gespeicherten Konto an dem WLAN-Controller über das Telnet-Protokoll anmelden, um eine ferne Steuerung zu realisieren. In der praktischen Umsetzung stellt man das lokale Authentifizierungsverfahren in der initialisierten Administrator-Domäne ein, nämlich die Domäne „default_admin“. Das heißt, wenn sich die Benutzer an dem Wireless–Controller mit dem Telnet-Protokoll einloggen und ein Benutzername ohne Domänename eingegeben wird, wird ein lokaler Authentisierungsprozess aufgerufen.

Um die lokale Authentifizierung zu realisieren, sollte man zuerst ein Authentisierungsschema für die lokale Authentifizierung erzeugen.

```
[AC6605-aaa] authentication-scheme local
[AC6605-aaa-authen-scheme-local] authentication-mode local
```

Als Nächstes muss man das lokale Benutzerkonto für die lokale Authentifizierung erzeugen. Beispielsweise wird ein Benutzerkonto mit Benutzername „admin“ und Geheimzahl „12345“ erzeugt

```
[AC6605] aaa
[AC6605-aaa] local-user user admin password cipher 12345
[AC6605-aaa] local-user user admin service-type telnet
```

Zuletzt muss die Domäne „default_admin“ mit dem Authentifizierungsschema „local“ verknüpft werden.
Wenn man sich mit dem Benutzernamen „admin“ und der Geheimzahl „12345“ über Telnet an den WLAN-Controller anmeldet, hat der Benutzer das Recht, den WLAN-Controller zu verwalten.

```
[AC6605-aaa] domain default_admin
[AC6605-aaa-domain-default_admin] authentication-scheme local
```

Die andere Möglichkeit für die Administratorauthentifizierung basiert auf dem RADIUS-Server. Ähnlich wie das Authentifizierungsverfahren der normalen Benutzer wird die Kontoinformation im RADIUS-Server gespeichert. Im Gegensatz zum normalen RADIUS-Server speichert der für den Administrator vorbereitete RADIUS-Server weniger Benutzerkonten, die in dem Bereich „Administrator“ zugeordnet sind. Zum Beispiel werden die individuellen Konten der IT-Abteilung als Administratorskonten betrachtet.
Zuerst muss man eine Domäne für die RADIUS-Authentifizierung erzeugen und diese nennt man „Admin“.

```
[AC6605-aaa] domain Admin
```

Dann wird das Authentifizierungsverfahren auf RADIUS eingestellt und zusätzlich muss man eine Vorlage für die Konfiguration des RADIUS-Servers erzeugen. Die Befehle unterscheiden sich von den anderen nur durch die IP-Adresse des RADIUS-Servers.

```
[AC6605-aaa] domain Admin
[AC6605-aaa-domain-Admin] authentication-scheme Admin
[AC6605-aaa-authen-scheme-Admin] authentication-mode radius
[AC6605-aaa-domain-Admin] radius-server template Admin
[AC6605-radius-Admin] radius-server authentication 10.72.133.120 source ip-address
10.221.96.1
```

Bisher wurden die auf der Benutzerdomäne basierten Authentifizierungsverfahren konstruiert. Zusammenfassend werden die Benutzer in den fünf Domänen aufgeteilt. Eine Domäne ist für die Rechnerbenutzer und mit dem Zeichen „wlanaccessv2.0“ versehen. Zwei Domänen werden für die Mobilgerätebenutzer bereitgestellt, nämlich die Domäne „Huawei-Init“ und die Domäne „Huawei-Employee“. Zuletzt stehen die Domänen „local“ und „Admin“ für den Administrator zur Verfügung.

Das oben beschriebene Authentifizierungsverfahren für die normalen Benutzer muss in ihren entsprechenden VPAs zugeordnet sein. Um die verschiedenen VAPs unterscheiden zu können, benötigt man die sogenannte ESS-Schnittstelle. Im nächsten Abschnitt wird die Konfiguration der ESS-Schnittstelle vorgestellt.

8 Erzeugung einer ESS-Schnittstelle

Wie oben bereits vorgestellt, ist jeder VAP eine Funktionseinheit am WLAN-Controller. Und an einem WLAN-Controller kann man vielfältige VAPs konfigurieren. Diese unterscheiden sich mittels der ESS-Schnittstelle. Diese ESS-Schnittstelle ist eine virtuelle logische Schnittstelle und ihre Funktionsweise ist ähnlich wie beim Hybrid-Port [5]. In der WLAN-Infrastruktur stehen hier insgesamt drei VAPs zur Verfügung und jeder VAP wird eine ESS-Schnittstelle zugeordnet. Um die Benennungsregel zu vereinheitlichen, wird der Domänenname auch als der Name der ESS-Schnittstelle betrachtet. Allerdings kann der ESS-Schnittstellenname nur mit der Ziffer bezeichnet werden. Deswegen fügt man zusätzlich eine Beschreibung an der ESS-Schnittstelle hinzu. Beispielsweise für die Domäne „wlanaccessv2.0“ stellt man eine ESS-Schnittstelle mit der Ziffer 0 zur Verfügung:

```
[AC6605] interface wlan-ess 0
[AC6605-Wlan-Ess0] description wlanaccessv2.0
```

Weil dieser VAP für die Rechnerbenutzer bereitgestellt wird, wird die der VAP zugehörige ESS-Schnittstelle in VLAN 810 zugeordnet. Außerdem bietet diese ESS-Schnittstelle einen Netzwerkzugang für die Benutzer an, das heißt, die virtuelle Schnittstelle ist mit den von dem Benutzer genutzten Terminals verknüpft. Nach der VLAN - Kommunikationsregel sollten alle von der ESS-Schnittstelle gesendeten Frames ohne VLAN-Tag sein. Um die VLAN-Tag abzuziehen, muss die ESS-Schnittstelle so konfiguriert werden:

```
[AC6605] interface wlan-ess 0
[AC6605-Wlan-Ess0] port hybrid pvid vlan 810
[AC6605-Wlan-Ess0] port hybrid untagged vlan 810
```

Zuletzt muss die von VAP zugehörige Benutzerdomäne „default“ mit der ESS-Schnittstelle verknüpft werden und das mit der Domäne entsprechende Authentifizierungsverfahren wird durch den Befehl „dot1x enable“ aktiviert.

```
[AC6605-Wlan-Ess0] force-domain name default
[AC6605-Wlan-Ess0] dot1x enable
[AC6605-Wlan-Ess0] dot1x authentication-methode eap
```

Auf die gleiche Weise werden die beiden VAPs, die zu den Mobilgerätebenutzern gehören, jeweils mit einer ESS-Schnittstelle zugeordnet. Die zwei Schnittstellen bezeichnet man mit den Ziffern 1 und 2. Der VAP, der öffentliche Netzwerkressourcen anbietet, wird mit der ESS-Schnittstelle 1 verknüpft und seine entsprechende Benutzerdomäne „Huawei-Init“ wird auch der ESS-Schnittstelle 1 zugeordnet. Der VAP, der normale Netzwerkressourcen anbietet, wird mit der ESS-Schnittstelle 2 verknüpft und seine entsprechende Benutzerdomäne „Huawei-Employee“ wird auch der ESS-Schnittstelle 2 zugeordnet. Weil sich die zwei VAPs nur einen VLAN 910 teilen, werden die zwei ESS-Schnittstellen im VLAN 910 zugewiesen. Ein kleiner Unterschied zwischen den zwei ESS-Schnittstellen ist, dass in der ESS-Schnittstelle 1 der Befehl über die Konfiguration des Authentifizierungsverfahrens fällt. Zum Beispiel für die ESS-Schnitte 1 sollte man so konfigurieren:

```
[AC6605] interface wlan-ess 1
[AC6605-Wlan-Ess1] port hybrid pvid vlan 910
[AC6605-Wlan-Ess1] port hybrid untagged vlan 910
[AC6605-Wlan-Ess1] force-domain name Huawei-Init
```

Bisher sind es alle Konfigurationen der ESS-Schnittstelle. Allerdings fehlen der obigen konfigurierten VAP noch ein Namen und ein Rahmen, der alle Konfigurationsanteile integrieren kann. Der Rahmen wird als „Service-Set“ bezeichnet und im nächsten Abschnitt vorgestellt.

9 WLAN-Service-Set

Der letzte Schritt ist, dass man die Konfigurationsparameter in das Service-Set integriert. Jedes Service-Set wird von einem Service-Set-Identifier, kurz als SSID bezeichnet, identifiziert. Der SSID wird als eindeutige Kennung für ein drahtloses LAN verwendet, da diese Kennung oft in Geräten manuell von dem Administrator eingegeben wird. Als eine lesbare Zeichenfolge wird der SSID von dem Benutzer verwendet, um die unterschiedlichen Wireless LAN erkennen zu können. Damit wird der SSID allgemein auch als „Netzwerkname" betrachtet.

Der Aufbau eines Service-Sets wird in folgenden Schritten durchgeführt:

- Erzeugung einer Vorlage für das Service-Set
- Verknüpfung der Konfigurationsparameter am entsprechenden Service-Set
- Verknüpfung des kompletten Service-Set mit Funkfrequenzen (2,4 GHz&5 GHz)

Beispielsweise wird ein für die Rechnerbenutzer verbreiteter VAP als „wlanaccessv2.0" bezeichnet. Dazu stellt man ein Service-Set „wlanaccessv2.0" mit folgenden Befehlen her:

```
[AC6605-wlan-view] service-set name wlanaccessv2.0 id 0
[AC6605-wlan-service-set-wlanaccessv2.0] ssid wlanaccessv2.0
```

Danach muss man das Sicherheitsprofil und die ESS-Schnittstelle mit dem Service-Set erstellen, so wie im Abschnitt 4. „Überblick über die Konfiguration der differenzierten WLAN-Dienste" vorgestellten Konfigurationsablauf:

```
[AC6605-wlan-service-set-wlanaccessv2.0] wlan-ess 0
[AC6605-wlan-service-set-wlanaccessv2.0] security-profile id 0
```

Zusätzlich muss der mit VAP entsprechende VLAN dem Service-Set zugeordnet werden.

Der VAP „wlanaccessv2.0“ besitzt den VLAN 810, deswegen wird VLAN 810 am Service-Set „wlanaccessv2.0“ folgendermaßen konfiguriert:

```
[AC6605-wlan-service-set-wlanaccessv2.0] service-vlan 810
```

Auf die gleiche Weise werden noch zwei Service-Sets für den VAP „Huawei-Init“ und den VAP „Huawei-Employee“ erzeugt. Hinterher stehen hier insgesamt drei drahtlose Netzwerke für die normalen Benutzer zur Verfügung, nämlich „wlanaccessv2.0“, „Huawei-Init“ und „Huawei-Employee“. Wenn die drei Service-Sets mit den Funkfrequenzen verknüpft werden, können sie durch Scannen entdeckt werden.

Die nächste Aufgabe ist es, die drei WLAN-Service-Sets mit den Funkfrequenzen, nämlich 2,4 GHz und 5 GHz, zu verknüpfen. Mit dem Befehl „radio 0/1“ kann man die Funkfrequenz herstellen. Hier entspricht die Ziffer 0 der Funkfrequenz von 2,4 GHz und die Ziffer 1 bedeutet die Funkfrequenz von 5 GHz. Die 2,4 GHz-Funkfrequenz entspricht dem im Abschnitt „6.4. Erstellung eines Radio-Profils“ bereits erstellten 2,4 GHz-Radio-Profile. Um die 2,4 GHz-Funkfrequenz aktivieren zu können, müssen die folgenden Befehle durchgeführt werden:

```
[AC6605-wlan-view] radio 0
[AC6605-wlan-view-radio-0] radio-profile id 0
[AC6605-wlan-view-radio-0] service-set name wlanaccessv2.0 id 0
[AC6605-wlan-view-radio-0] service-set name Huawei-Init id 1
[AC6605-wlan-view-radio-0] service-set name Huawei-Employee id 2
```

Ähnlich wie die 2,4 GHz-Funkfrequenz muss die Funkfrequenz von 5 GHz mit einem gleichen Konfigurationsablauf konfiguriert werden und das sieht so aus:

```
[AC6605-wlan-view] radio 1
[AC6605-wlan-view-radio-1] radio-profile id 1
[AC6605-wlan-view-radio-1] service-set name wlanaccessv2.0 id 0
[AC6605-wlan-view-radio-1] service-set name Huawei-Init id 1
[AC6605-wlan-view-radio-1] service-set name Huawei-Employee id 2
```

Das heißt, alle drei Service-Sets werden auf zwei Frequenzbändern ausgesendet. Und die Benutzer können nach dem Typ der genutzten Terminals an verschiedenen Service-Sets oder Frequenzbändern teilnehmen.

Zuletzt muss sich der einzelne Access Point an den WLAN-Controller anmelden. Der Anmeldungsprozess erfolgt durch die MAC-Adresse des Access Pointer. Man konfiguriert die MAC-Adresse des Access Points an den WLAN-Controller und mittels der MAC-Adresse kann der WLAN-Controller den bestimmten Access Point herausfinden und erkennen. Der folgende Befehl zeigt den Konfigurationsprozess, dass sich ein Access Point mittels der entsprechenden MAC-Adresse an dem WLAN-Controller anmeldet.

```
[AC6605] wlan
[AC6605-wlan-view] ap id 0 type-id 19 mac 0025-9e07-8270
```

Type-id entspricht einer Identifikationsnummer des Typs von dem genutzten Access Point. Die Nummer 19 ist die Produktnummer des Access Point 6010-AGN und die Ziffer 0 bedeutet, dass dieser Access Point der erste ist, der dem WLAN-Controller hinzugefügt wurde. Nach einer erfolgreichen Erkennung des Access Points beim WLAN-Controller kann man den Befehl „commit all“ ausführen, um alle Konfigurationsparameter über den CAPWAP-Tunnel an den Access Point zu vergeben.

Nach dem Scannen von einem Terminalgerät werden die folgenden dargestellten drei SSIDs verdeckt:

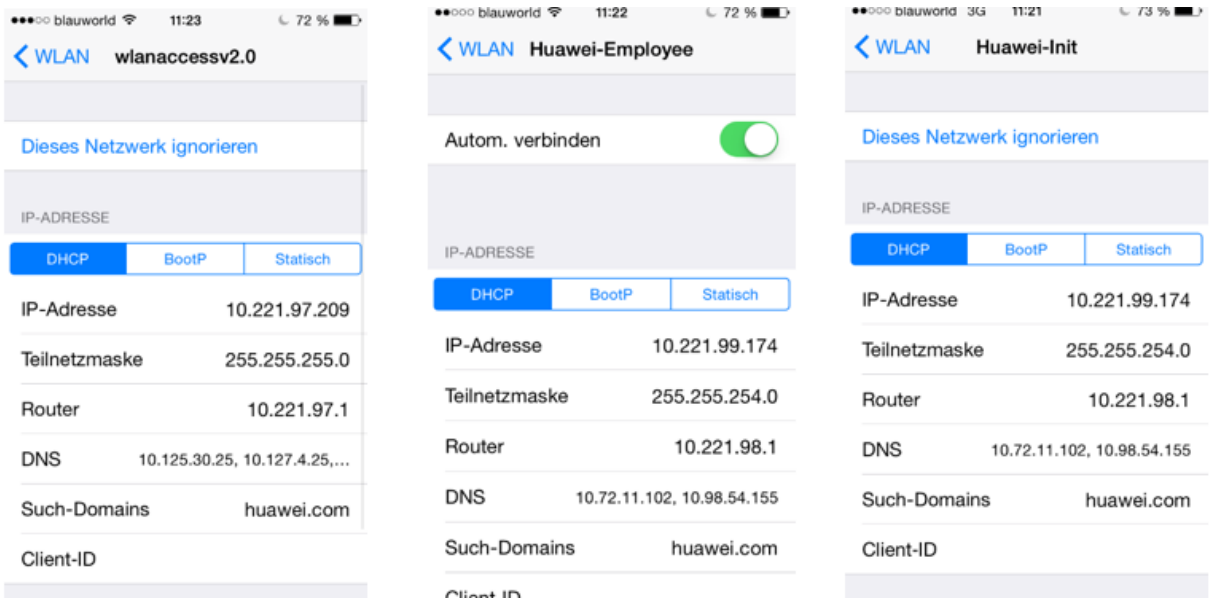

Abbildung 20: Praktische Überprüfung der Service-Sets

Anhand der Abbildung 20 kann man sehen, dass hier insgesamt drei drahtlose Netzwerke für die normalen Benutzer zu Verfügung stehen.

Im drahtlosen Netzwerk mit dem Namen „wlanaccessv2.0“ wird dem Benutzer eine IP-Adresse von „10.221.97.209“ zugewiesen. Das bedeutet, die Benutzer, die eine Verbindung mit „wlanaccessv2.0“ herstellen, werden im VLAN 810 zugeordnet und sie bekommen eine IP-Adresse aus dem Bereich von 10.221.97.2 bis 10.221.97.254. Ähnlich wie „wlanaccessv2.0“ basieren die drahtlosen Netzwerke „Huawei-Employee“ und „Huawei-Init“ auf dem VLAN 910. Deswegen wird den Benutzern eine IP-Adresse aus dem Bereich von 10.221.98.2 bis 80.221.9.254 zugeordnet, wenn sie sich mit den beiden SSIDs verbinden.

Wenn man im Netz „Huawei-Init“ teilnimmt und versucht, eine Webseite zu öffnen, wird man direkt zum dem Web-Link „uni-byod.huawei.com/-custom/download.html“ zugeleitet. Die Webseite wird angezeigt wie in der folgenden Abbildung 21 dargestellt:

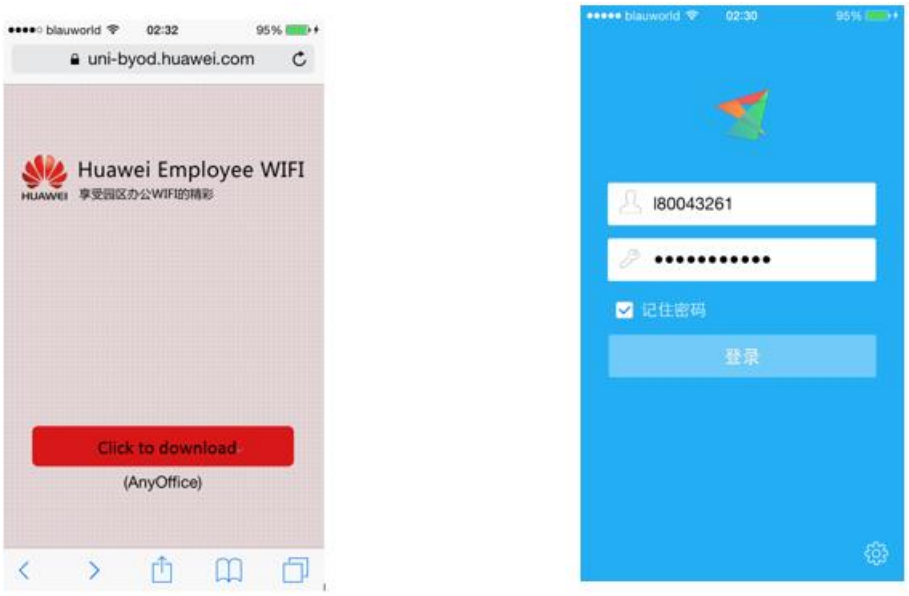

Abbildung 21: Authentifizierung mittels Authentifizierungsclient

10 Zusammenfassung und Ausblick

In diesem Abschnitt wird zuerst eine Zusammenfassung über die Arbeit gegeben. Danach werden die Benutzerseite und die Administratorseite näher erläutert. Anschließend erfolgt ein Ausblick über die Verbesserung des WLAN-Systems sowie zwei Aspekte hinsichtlich der Systemerweiterung und des sogenannten „Guest-WLAN".

10.1 Zusammenfassung

Allgemein werden die Mitarbeiter in zwei Gruppen eingeteilt, nämlich in die Gruppe der Administratoren und die Gruppe der normalen WLAN-Benutzer. Die nachfolgenden Inhalte beschreiben die beiden Gruppen.

10.1.1 Benutzerseite

Die normalen WLAN-Benutzer werden aufgrund der genutzten Terminalgeräte in die beiden Gruppen aufgeteilt und es stehen insgesamt drei WLANs für die WLAN-Benutzer zur Verfügung. Das WLAN mit dem SSID „wlanaccessv2.0" wird für die Rechnerbenutzer bereitgestellt. Um sich in das WLAN „wlanaccessv2.0" einzuwählen, müssen die Benutzer ihren Benutzernamen und ihr Password eingeben und nach einer erfolgreichen Authentifizierung wird das WLAN freigeschaltet.

Für die Mobilgerätebenutzer werden zwei WLANs zur Verfügung gestellt, nämlich „Huawei-Init" und „Huawei-Employee". Im Vergleich zu den Rechnerbenutzern werden die Mobilgerätebenutzer vor einer Authentifizierung direkt zu einer Webseite geleitet, wenn sie eines der oben genannten WLANs auswählen. Auf der Webseite können die Benutzer über das öffentliche WLAN „Huawei-Init" einen Authentifizierungsclient herunterladen. Nach einem erfolgreichen Download müssen sie zum WLAN „Huawei-Employee" umschalten. Mittels des Authentifizierungsclients werden die Authentifizierungsinformationen über „Huawei-Employee" zum Authentifizierungsserver gesendet und nach einer erfolgreichen Authentifizierung wird das WLAN „Huawei-Employee" freigeschaltet.

Um die Datenraten der WLANs zu garantieren, stellt man die untere Begrenzung für die Empfangsempfindlichkeit als -60dbm ein. Das Signal mit der Stärke -60 dBm entspricht normalerweise einer Datenrate von 54Mbit/s bei einem 2,4 GHz-Frequenzband. In der Praxis

kann die Übertragungsrate nicht mehr als 20Mbit/s erreichen und im Durchschnitt teilen sich je fünf Mitarbeiter einen Access Point. Dazu stehen für jeden Benutzer hier maximal 4 Mbit/s bei einem 2,4 GHz-Frequenzband zur Verfügung. Jeder Benutzer hat etwa zwei bis drei Geräte und im schlimmsten Fall benötigt jedes Gerät das WLAN. Dafür stehen hier noch 1.3 Mbit/s bis 2 Mbit/s für jedes Terminalgerät zur Verfügung. Nach einer Umrechnung kann die Übertragungsrate des einzelnen Terminalgeräts in diesem schlimmsten Fall zumindest 170 kB/s erreichen und in der Praxis beträgt die Datenrate unbedingt mehr als 170 kB/s. Diese Datenrate kann nicht nur die Audiokonferenz sondern auch die Videokonferenz garantieren.

10.1.2 Administratorseite

In der oben beschriebenen Konfiguration erfolgt eine ferne Verwaltung des WLAN-Controllers, nämlich das AC 6605. Über das Telnet Protokoll können die Administratoren eine ferne Verbindung mit der Zieladresse „10.221.96.1“ einrichten, um eine ferne Verwaltung durchführen zu können. Allerdings wird vor der Verwaltung ein Authentifizierungsprozess aufgerufen. Es gibt zwei Möglichkeiten für diesen Authentifizierungsprozess. Die Administratoren können ihr eigenes individuelles Benutzerkonto für die Authentifizierung verwenden. Wenn der Administrator sein individuelles Benutzerkonto vergessen hat, kann er auch ein an den WLAN-Controller voreingestelltes lokales Administratorkonto verwenden. Damit wird ein lokaler Authentifizierungsprozess statt des RADIUS - Authentifizierungsprozesses aufgerufen.

10.2 Ausblick

In diesem Teil erfolgt ein Ausblick über die Verbesserung des WLANs in der Zukunft. Der Inhalt ist in zwei Teile gegliedert. Ein Teil ist die Strukturvergrößerung für mehrere WLAN-Benutzer. Der andere Teil beschreibt die Öffnung eines neuen WLANs für Gäste.

10.2.1 Guest-WLAN

Aufgrund der Sicherheitsrichtlinien steht das Guest-WLAN derzeit nicht zur Verfügung. Sollte in Zukunft ein neues WLAN für Gäste bereitgestellt werden, kann man verfahren, wie nachfolgend erläutert wird.

Weil die Frames des Guest-WLANs sich von anderen WLANs isolieren müssen, konfiguriert man ein neues VLAN und ein Service-Set für das Guest-WLAN an den WLAN-Controller. Allerdings liegt der Arbeitsschwerpunkt darin, dass ein geeignetes Authentifizierungsverfahren für das Guest-WLAN auswählt wird. Das Guest-WLAN kann öffentlich sein oder ein Authentifizierungsverfahren mit PSK (Pre-Shared-Key) verwenden. Eine Netzwerkauthentifizierung mit PSK wird für das Guest-WLAN empfohlen, weil ein öffentliches WLAN viele Schwachstellen in der Netzwerksicherheit hat. Für das Authentifizierungsverfahren mit PSK braucht man nur ein Passwort für das Guest-WLAN voreinzustellen. Wenn die Gäste das Guest-WLAN benutzten möchten, müssen sie das voreingestellte Passwort eingeben. Das Guest-WLAN wird freigeschaltet, wenn die Gäste das richtige Passwort eingegeben haben.

10.2.2 Strukturvergrößerung

In Zukunft wird die Anzahl der Mitarbeiter dramatisch zunehmen. Das bedeutet, mehrere Büros werden für die neuen Mitarbeiter bereitgestellt. Dazu müssen mehrere Access Points in den neuen Büros montiert werden. Weil die Access Points mit dem Switch direkt durch physikalische Kabelverbindungen verbunden sind, muss man zusätzliche Switches an dem WLAN-Controller hinzufügen. Ein WLAN-Controller bietet maximal 23-Ethernetports für die Switches an und an jedem Switch stehen maximal auch 23-Ethernetports für die Access Points zur Verfügung. Daraus kann man ableiten, dass ein WLAN-Controller maximal mit 529 Access Points verbunden werden kann. Außerdem sollte man zusätzliche IP-Segmente für die neuen Mitarbeiter beantragen. Normalerweise stehen einem Segment mit einer 24-Bit-Maske maximal 254 IP-Adressen zur Verfügung.

Zum Schluss kann festgestellt werden, dass alle Aufgaben zum Thema „Aufbau des unternehmensweiten Wireless LAN“ erfolgreich gelöst wurden.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

Username:admin

Password:

User last login information:

Access Type: Telnet

IP-Address : 10.221.82.138

Time : 2015-02-12 18:46:17+00:00

<odemuccthw00>display current-configuration

#

sysname odemuccthw00

#

vlan batch 800 805 810 910

#

dot1x enable

mac-authen

#

wlan ac-global country-code DE

wlan ac-global carrier id other ac id 1

#

dhcp enable

#

dhcp relay detect enable

#

diffserv domain default

#

```
radius-server template wlanaccessv2.0
 radius-server shared-key cipher %@%@&4@S:w}>$S4bcrLI]Y)"xfvY%@%@
 radius-server authentication 10.201.15.58 1812 source ip-address 10.221.96.3 weight 80
 radius-server authentication 10.195.15.21 1812 source ip-address 10.221.96.3 weight 80
 radius-server testuser username test password cipher %@%@:"nJKW[u@;kr($*P-
%x8xfv.%@%@
```

// Generieren ein RADIUS-Server für die Domäne„default“

```
radius-server template Admin
 radius-server shared-key cipher %@%@k}sYBu~bu'nt^b<__~KUxfw+%@%@
 radius-server authentication 10.72.133.120 1812 weight 80
```

// Generieren ein RADIUS-Server für die Domäne “Admin”

```
radius-server template Huawei-Employee
 radius-server shared-key cipher %@%@%P67VX*.'-j}nK6!N_\<.J3%%@%@
 radius-server authentication 10.201.15.58 1812 source ip-address 10.221.96.3 weight 80
 radius-server authentication 10.195.15.21 1812 source ip-address 10.221.96.3 weight 80
```

// Generieren ein RADIUS-Server für die Domäne „Huawei-Employee“

```
web-auth-server Huawei-Init
 server-ip 1.1.1.1
 port 50100
 url https://uni-byod.huawei.com/-custom/download.html
```

// Generieren ein Portal-Server für die Domäne “Huawei-Init”

#

aaa

```
authentication-scheme default
 authentication-mode radius
```

// Generieren ein Authentifizierungsschema für die Domäne „default“

```
authentication-scheme Admin
 authentication-mode radius
```

// Generieren ein Authentifizierungsschema für die Domäne „Admin“

```
authentication-scheme local
authentication-scheme local
```

// Generieren ein Authentifizierungsschema für die Domäne „default_admin“

```
authentication-scheme Huawei-Employee
 authentication-mode radius
```

// Generieren ein Authentifizierungsschema für die Domäne „Huawei-Employee“

```
authentication-scheme Huawei-Init
 authentication-mode none
```

// Generieren ein Authentifizierungsschema für die Domäne „Huawei-Init“

```
domian default
 authentication-scheme default
 radius-server wlanaccessv2.0
```

// Konfiguration die Domäne “default” (Authentifizierung für den VAP „wlanaccessv2.0)

```
domain default_admin
 authentication-scheme local
```

// Konfiguration die Domäne “default_admin” (lokale Authentifizierung für Administrator)

```
domain Admin
 authentication-scheme Admin
 radius-server Admin
```

// Konfiguration die Domäne “Admin” (Authentifizierung mit RADIUS-Server für Administrator)

```
domain Huawei-Init
 authentication-scheme Init
```

// Konfiguration die Domäne "Huawei-Init" (Authentifizierung für den VAP „Huawei-Init")

```
domain Huawei-Employee
 authentication-scheme Huawei-Employee
 radius-server Huawei-Employee
```

// Konfiguration die Domäne „Huawei-Employee" (Authentifizierung für die VAP „Huawei-Employee"

```
local-user admin password cipher %@%@N1Ma~iQ)oJRwMXGK}2MC8^F-%@%@
local-user admin privilege level 3
local-user admin service-type telnet
```

// Erzeugen der lokalen Benutzer für die Domäne „default_admin"

#

```
interface Vlanif800
 description To_S6605-Logical
 ip address 10.221.96.1 255.255.255.128
```

// Konfiguration die VLANIF-Schnittstelle 800

#

```
interface Vlanif805
 ip address 10.221.96.129 255.255.255.128
```

// Konfiguration die VLANIF-Schnittstelle 805

#

```
interface Vlanif810
 ip address 10.221.97.1 255.255.255.0
 dhcp select interface
 dhcp server lease day 0 hour 3 minute 0
 dhcp server dns-list 10.125.30.25 10.127.4.25 10.72.255.100
```

// Konfigurieren ein Adresspool für die Rechnerbenutzer

// Konfiguration die VLANIF-Schnittstelle 810 für die Rechnerbenutzer

#

```
interface Vlanif910
 description BYOD-VLAN-00
 ip address 10.221.98.1 255.255.254.0
 web-auth-server Huawei-Init direct
 dhcp select interface
 dhcp server lease day 0 hour 3 minute 0
 dhcp server dns-list 10.72.11.102 10.98.54.155
```

// Konfigurieren ein Adresspool für die Mobilgerätebenutzer

// Konfiguration die VLANIF-Schnittstelle 910 für die Mobilgerätebenutzer

#

```
interface GigabitEthernet0/0/1
 description downlink_to_POE_10.221.96.132_GE0/0/24_groundfloor
 port link-type trunk
 port trunk allow-pass vlan 805
 //Dieser Port verbindet mit dem unterstromigen Switch und erlaubt VLAN805 durchzugehen.
 trust upstream default
 trust dscp
```

// Konfigurieren den Ethernet-Port 0/0/1

```
interface GigabitEthernet0/0/24
 description To_MA5200F_10.220.136.3_E20
 port link-type trunk
 port trunk allow-pass vlan 810 vlan 910
 // Dieser Port verbindet mit dem oberstromigen Router und erlaubt VLAN810 und VLAN910
durchzugehen
 trust upstream default
 trust dscp
```

// Konfigurieren den Ethernet-Port 0/0/24

```
#
interface Wlan-Ess0
 description wlanaccessv2.0
 port hybrid pvid vlan 810
 port hybrid untagged vlan 810
 trust upstream default
 trust dscp
 dot1x enable
 dot1x authentication-method eap
force-domain name default
```

// Generieren eine ESS-Schnittstelle für den VAP „wlanaccessv2.0“

```
#
interface Wlan-Ess1
 description Huawei-Init
 port hybrid pvid vlan 910
 port hybrid untagged vlan 910
 trust dscp
 force-domain name Huawei-Init
```

// Generieren eine ESS-Schnittstelle für den VAP „Huawei-Init“

```
#
interface Wlan-Ess2
 description Huawei-Employee
 port hybrid pvid vlan 910
 port hybrid untagged vlan 910
 trust dscp
 dot1x enable
 dot1x authentication-method eap
 force-domain name Huawei-Employee
```

// Generieren eine ESS-Schnittstelle für den VAP „Huawei-Employee“

```
#
```

```
wlan
 wlan ac source interface vlanif805
```

// Stellen eine Querschnittstelle ein

wlan ap username admin password cipher %@%@ATG6O>)L!$wB"'=#dm5-xJm%%@%@

```
ap id 1 type-id 19 mac ac85-3daf-1080 sn 2102354196W0E4002912
 ap-sysname odemudaphw11
ap id 2 type-id 19 mac ac85-3daf-11e0 sn 2102354196W0E4002923
 ap-sysname odemudaphw05
ap id 3 type-id 19 mac ac85-3daf-13a0 sn 2102354196W0E4002937
 ap-sysname odemudaphw02
```

// Melden den AP an WLAN-Controller mittels der MAC-Adresse

```
wmm-profile name 2.4G id 0
 wmm edca ap ac-vi aifsn 2 ecw ecwmin 3 ecwmax 4 txoplimit 94
 wmm edca ap ac-vo aifsn 2 ecw ecwmin 2 ecwmax 3 txoplimit 94
```

// Generieren eine Vorlage für die Dienstgüte (2,4 GHz)

```
wmm-profile name 5G id 1
 wmm edca ap ac-vi aifsn 2 ecw ecwmin 3 ecwmax 4 txoplimit 94
 wmm edca ap ac-vo aifsn 2 ecw ecwmin 2 ecwmax 3 txoplimit 94
```

// Generieren eine Vorlage für die Dienstgüte (5 GHz)

traffic-profile name hw-traffic id 0

```
security-profile name wlanaccessv2.0 id 0
 security-policy wpa2
```

// Generieren eine Sicherheitsvorlage für den VAP „wlanaccessv2.0“

```
security-profile name Huawei-Init id 1
 security-policy wpa2
```

// Generieren eine Sicherheitsvorlage für den VAP „Huawei-Init“

```
security-profile name Huawei-Employee id 2
 security-policy wpa2
```

// Generieren eine Sicherheitsvorlage für den VAP „Huawei-Employee“

```
service-set name wlanaccessv2.0 id 0
forward-mode tunnel
 wlan-ess 0
 ssid wlanaccessv2.0
 traffic-profile id 0
 security-profile id 0
 service-vlan 810
```

// Generieren einen Service-Set „wlanaccessv2.0“

```
service-set name Huawei-Init id 1
 forward-mode tunnel
 wlan-ess 1
 ssid Huawei-Init
 traffic-profile id 0
 security-profile id 1
 service-vlan 910
```

// Generieren einen Service-Set „Huawei-Init“

```
service-set name Huawei-Employee id 2
 forward-mode tunnel
 wlan-ess 2
 ssid Huawei-Employee
 traffic-profile id 0
 security-profile id 2
 service-vlan 910
```

// Generieren einen Service-Set „Huawei-Employee“

```
calibrate enable schedule time 16:00:00
calibrate policy rogue-ap
calibrate policy non-wifi
calibrate sensitivity high
calibrate 2.4g 20mhz channel-set 1,6,11
calibrate 5g 20mhz channel-set 40, 44, 48, 52
```

// Stellen das Kalibrierungsverfahren für Frequenzband 2,4 GHz&5 GHz

```
radio-profile name 2,4 GHz id 0
 radio-type 80211bgn
 power-mode auto
 channel-switch announcement enable
 sta-forced-offline signal-strength threshold -60
 sta-forced-offline signal-strength switch enable
 wmm-profile id 0
```

// Generieren eine Radioprofil für Frequenzband 2,4 GHz

```
radio-profile name 5G id 1
 radio-type 80211an
 power-mode auto
 channel-switch announcement enable
 sta-forced-offline signal-strength threshold -60
 sta-forced-offline signal-strength switch enable
 wmm-profile id 1
```

// Generieren eine Radioprofil für Frequenzband 5 GHz

```
radio 0
 radio-profile id 0
 service-set id 810 wlan 1
 service-set id 910 wlan 2
 service-set id 990 wlan 3
```

// Verknüfen den Service-Set mit 2,4 GHz-Funk

```
radio 1
 radio-profile id 1
 service-set id 810 wlan 1
 service-set id 910 wlan 2
 service-set id 990 wlan 3
```

// Verknüfen den Service-Set mit 5 GHz-Funk

#

Return

Abkürzungen

AAA	Authentication, Authorization and Accounting
AC	Access Controller
ACK	Acknowledgment
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AP	Access Point
BSS	Basic Service Set
CAPWAP	Control and Provisioning of Wireless Access Point
CBC-MAC	Cipher-Block Chaining with Message Authentication Code
CCMP	CTR with CBC-MAC Protocol
CoS	Class of Service
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CW	Contention Window
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LANs
EAPOR	Extensible Authentication Protocol over RADIUS
EDCA	Enhanced Distributed Channel Access
ESS	Extended Service Set
HCF	Hybrid Coordination Function
HCCA	Controlled Channel Access

ID	Identifier
IEEE	Institute of Electrical and Electronical Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
PVID	Port Default VLAN-ID
PoE	Power over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SIFS	Short-Inter-Frame Space
SSID	Service Set Identifier
STA	Station
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TXOP	Transmission Opportunity
VAP	Virtual Access Point
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multi Media
WPA	Wi-Fi Protected Access
WPA 2	Wi-Fi Protected Access 2
XOR	Exclusive or

Formel und Symbolverzeichnis

Formel

Wellenlänge: $\lambda = c / f$ [m]

Freiraumdämpfung: $A_{F.} = 20 \log (4 \pi d / \lambda)$ [dB]

Symbolverzeichnis

Symbol	Einheit	Bezeichnung
c	m/s	Ausbreitungsgeschwindigkeit
f	Hz	Frequenz der Welle
λ	m	Wellenlänge
d	m	Entfernung
π	-	Kreiszahl
A_F	dB	Freiraumdämpfung
log	-	Logarithmus
Mbit/s	-	Megabit pro Sekund
kB/s		Kilobyte per second

Quellenverzeichnis

[1] Jörg Rech; **Wireless LANs, 802.11-WLAN-Technologie und praktische Umsetzung im Detail, 4., aktualisierte und erweiterte Auflage**, Mai 2012.
ISBN 978-3-936931-75-4

[2] Patrick Schnabel; **Netzwerktechnik-Fibel**. Juni 2013, Ludwigsburg
ISBN 978-3833416811 (3-8334-1681-5)

[3] Gerhard Kafka; **WLAN, Technik, Standards, Planung und Sicherheit für Wireless LAN**, Herbst 2004, Egling
ISBN 3-446-22734-2

[4] Xiao Xipeng; **Technical, Commercial and Regulatory Challenges of QoS,** September 2008
ISBN 978-0-12-373693-2

Sonstige Veröffentlichungen

[5] Huawei Technologies Co.Ltd; **AC6605 Product Documentation, Product Version: V200R005,** Library Version: 04, 09/10/2014, Shenzhen, People Republic of China

[6] Huawei Technologies Co. Ltd; **VLAN and QinQ Technology White Paper**, Issue 01, 30/10/2012, Shenzhen, People Republic of China

[7] Huawei Technologies Co. Ltd; **Technical White Paper - Centralized authentication and local forwarding**, Issue 01, 31/10/2012, Shenzhen, People Republic of China

[8] Huawei Technologies Co. Ltd; **Country codes & Channels compliance status**, Issue 11, 15/11/2014, Shenzhen, People Republic of China

Quelle Bilder

Abbildung 22, WLAN-Controller AC6605,

http://enterprise.huawei.com/en/products/network/wlan/ac/hw-142054.htm,

Huawei Technologies Co. Ltd. 2014, Shenzhen, People Republic of China

Abbildung 23. Layer-3-Switch S5700-28C-PWR-EI

http://e.huawei.com/en/products/enterprise-networking/switches/campus-switches/s5700-ei-model,

Huawei Technologies Co. Ltd. 2014, Shenzhen, People Republic of China

Abbildung 24. Access Point AP 6010-AGN

http://enterprise.huawei.com/en/products/network/wlan/ap/hw-142050.htm,

Huawei Technologies Co. Ltd. 2014, Shenzhen, People Republic of China