Schule	Höhere Fachschule Uster
Studiengang	HF Telekommunikation
Klasse	14T
Student	
Abschlussjahr	2019
Betreuer	Ruedi Kubli

DA

NETZWERK / TELEFONIE INFRASTRUKTUR FÜR UNTERNEHMEN MIT 3 STANDORTEN

Dokumentation der Diplomarbeit

1. Inhaltsverzeichnis

2 Management Summary

Durch die Digitalisierung wird der zuverlässige Austausch von Geschäftsdaten immer wichtiger. Mittels Standortvernetzung wird ein Datenaustausch innerhalb eines Firmennetzwerks, zwischen mehreren Standorten, gewährleistet. Dabei werden nicht nur Informationen übertragen, sondern zugleich auch die Telefonie.

Immer wichtiger wird der Gebrauch von privaten Geräten bei der Arbeit, hier spricht man von BYOD (Bring Your Own Device). Um den Gebrauch dieser Geräte zu gewährleisten wird ein Firmen WLAN implementiert, welches in der Cloud verwaltet wird. Ebenfalls wird ein WLAN Netz für Gäste angelegt, welches durch Kunden oder Geschäftspartner verwendet werden kann und getrennt von den Firmensystemen läuft.

Im Rahmen der Diplomarbeit werden folgende Systeme und Technologien umgesetzt:

- DNS Server
- DHCP Server
- Routing
- Switching
- Firewall Grundschutz
- Cloud-Managed WLAN
- IP Telefonie

Aus Kostengründen wird auf Redundanz verzichtet und es werden möglichst Geräte verwendet, welche bereits in meinem Besitz oder ausgeliehen werden können. Weiter werden, wo möglich, die Dienste mittels Testlizenzen ausgeführt.

3 Einleitung

3.1 Student

Detaillierte Angaben zu meiner Person:

Persönliche Angaben	
Privat	
Klasse	14T
Name	
Vorname	
Adresse (Privat)	
PLZ / Ort	
Telefon (Privat)	
E-Mail	
Geschäft	
Arbeitgeber	
Telefon	
E-Mail	

Tabelle 1 Persönliche Angaben

3.2 Motivation

Schon immer wollte ich mal eine gesamte Infrastruktur vom Server bis hin zum Client umsetzte, dies werde ich nun im Rahmen dieser Arbeit versuchen bestmöglich umzusetzen. Hinzu kommt noch das mit der Umsetzung vieles neues erlernt werden kann was man aus den Lehrbüchern nicht erfahren kann, da man nicht vor diverse Probleme gestellt wird.

Ich werde versuchen das erlernte aus der Praxis zu vertiefen um mich in verschiedenen Bereichen zu Zertifizieren. Vor allem im Bereich Netzwerktechnik und Telefonie bin ich bis zum Start dieser Arbeit nur theoretisch erfahren und konnte noch kein Projekt in diesem Umfang umsetzen.

3.3 Aufgabenstellung

Von der HFU, welche zudem als Auftraggeber auftritt, habe ich die Aufgabenstellung zur DA erhalten.

Die definitive Aufgabenstellung, wurde mir durch Frau Stefanie Gründler, zugestellt.

Hier die wichtigsten Punkte der Aufgabenstellung:

- Projektplanung
- Einarbeitung in das Thema Standortvernetzung, Netzwerk-Segmentierung (VLAN), IT-Sicherheit (Firewall) und WLAN-Infrastruktur mit Cloud-Management.
- Erstellung eines Pflichtenheftes mit Prioritäten
- Evaluation geeigneter Komponenten und Dienste
- Aufbau einer KMU-Umgebung mit 3 Standorten
- Folgende Netzwerk-Dienste, sind minimal zu implementieren: - DNS, DHCP, Internet, Telefonie und WLAN mit Cloud-Management, für alle 3 Standorte verfügbar
- Definition und Umsetzung eines IT-Sicherheits-Grundschutz (Firewall)
- Durchführung entsprechender Funktionstest und Gegenüberstellung Pflichtenheft
- Erstellung der technischen Dokumentation für Administratoren
- Dokumentation aller Arbeitsschritte

3.4 Technologie

In diesem Kapitel wird auf die Technologien eingegangen, welche im Rahmen dieser Arbeit verwendet werden. Es werden nur grobe Angaben gemacht, um die Funktion der jeweiligen Technologie zu erläutern.

3.4.1 Router

Router sind elektronische Geräte, die mehrere Computernetzwerke über drahtgebundene oder drahtlose Verbindungen miteinander verbinden. Technisch gesehen ist ein Router ein Layer-3-Netzwerk-Gateway-Gerät, d.h. er verbindet zwei oder mehr Netzwerke. Router enthalten einen Prozessor, verschiedene Speicher und -Schnittstellen. Im Speicher des Routers liegt ein Betriebssystem. Beispiele für Router-Betriebssysteme ist Cisco Internetwork Operating System (IOS). Diese Betriebssysteme werden in ein binäres Firmware-Image umgewandelt und werden allgemein als Router-Firmware bezeichnet. Durch die Pflege von Konfigurationsinformationen in einem Teil des Speichers, der als Routingtabelle bezeichnet wird, können Router auch eingehenden oder ausgehenden Datenverkehr basierend auf den Adressen von Sendern und Empfängern filtern. Router verfügen über verschiedene Routingprotokolle, wobei die statische Route, die mit den niedrigsten Kosten ist.

Der Router arbeitet auf der Netzwerkebene (Layer 3) des OSI-Modells.

3.4.2 Switch

Anders als beim Router kann ein Switch nicht zwischen verschiedenen Netzen kommunizieren. Er ist eine Weiterentwicklung des Hubs, die es jedoch ermöglicht den Datenverkehr durch erlernen der angeschlossenen MAC Adresse zu minimieren, die Nachrichten werden somit zielgerichtet an den Empfänger weitergeleitet. Der Switch ermöglicht es auch die Ports logisch zu trennen, diese Funktion nennt man VLAN und sie ermöglicht es mehrere Netze auf demselben Gerät zu verwalten.

Der Switch ist arbeitet auf der Data-Link-Ebene (Layer 2) des OSI-Models

3.5.4 Firewall

Eine Firewall ist ein Netzwerksicherheitssystem, um unbefugten Zugriff auf oder von einem privaten Netzwerk zu verhindern. Firewalls können sowohl als Hardware als auch als Software oder als Kombination aus beidem implementiert werden. Netzwerk-Firewalls werden häufig verwendet, um zu verhindern, dass unbefugte Internetnutzer auf private Netze, zugreifen können. Alle Nachrichten, die in das Intranet gelangen oder es verlassen, durchlaufen die Firewall, die jede Nachricht überprüft und diejenigen blockiert, die nicht den angegebenen Sicherheitskriterien entsprechen.

Hier ein paar Beispiele für Filtermethoden:

Paketfilter: Betrachtet jedes Paket, das in das Netzwerk eintritt oder es verlässt, und akzeptiert oder verwirft es auf der Grundlage benutzerdefinierter Regeln. Die Paketfilterung ist ziemlich effektiv und für den Benutzer transparent, aber es ist schwierig zu konfigurieren.

Applikation-Gateway: Wendet Sicherheitsmechanismen auf bestimmte Anwendungen an, wie z.B. FTP- und Telnet-Server. Dies ist sehr effektiv, kann aber zu einer Leistungsverschlechterung führen.

Proxy-Server: Fangen alle Nachrichten ab, die in das Netzwerk eindringen und es verlassen. Der Proxy-Server versteckt effektiv die wahren Netzwerkadressen.

Bei einer Firewall handelt es sich somit um ein Gerät, welches bis in den Applikations-Layer des OSI-Models den Verkehr Filtern kann.

3.5.5 IP PBX

Eine IP-PBX ist eine Telefonanlage, die Anrufe zwischen VoIP-Nutzern auf lokalen Leitungen umleitet und es allen Nutzern ermöglicht, eine bestimmte Anzahl von externen Telefonleitungen gemeinsam zu nutzen. bei einer herkömmlichen Telefonanlage sind separate Netzwerke für die Sprach- und Datenkommunikation erforderlich. Einer der Hauptvorteile einer IP-Telefonanlage ist die Tatsache, dass sie dasselbe Daten- und Sprachnetze nutzt. Dies bedeutet, dass sowohl der Internetzugang als auch die VoIP-Kommunikation und die traditionelle Telefonkommunikation über eine einzige Leitung für jeden Benutzer möglich sind. Dies bietet Flexibilität beim Wachstum eines Unternehmens und kann auch die langfristigen Betriebs- und Wartungskosten senken.

3.5.6 Session Border Controller

Ein Session Border Controller ist ein Security Gerät welches folgenden Features zur Verfügung stellt:

- NAT Traversal
- Transcoding
- Topology Hiding
- VoIP Firewall
- SIP Routing
- SIP Normalization
- Survivability

Es wird oft zwischen Netzwerksegmenten installiert, auf der einen Seite die „Trustet“ und auf der anderen die „Un-Trustet“ Seite. Er verwaltet die VoIP Sessions indem er die Sitzung Auf-, Abbaut sowie die Gesprächsführung übernimmt. Ein SBC dient vor allem auch der Normalisierung des SIP Protokolls, da jeder Provider oder PBX heutzutage ihre eigenen Standards hat. Auf die einzelnen verwendeten Features wird während der Umsetzung genauer eingegangen.

3.5.7 Cloud-Managed WLAN

Bei einem Cloud-Managed WLAN handelt es sich um eine WLAN Infrastruktur, bei der der WLAN Controller in der Cloud ausgelagert wird. Es ist vor allem dann zu empfehlen, wenn man keine zusätzliche Hardware warten will. Die Cloud Variante birgt jedoch meistens hohe Lizenzkosten.

3.5.8 Dynamic DNS

DynDNS ist ein Verfahren zur automatischen Anpassung der Domaininformationen im Domain Name System (DNS). DynDNS wird angewandt, wenn zum Beispiel im Heimnetz, bei ständig wechselnder IP Adresse, ein Webservice über den Browser erreicht werden soll. Dabei wird beim Router die fest vergebene IP Adresse des Servers angegeben und mittels DynDNS Diensten im Netz können diese dann erreicht werden. Die Synchronisation zwischen Router und DynDNS Dienst ist dabei wichtig, um die jeweils neu vergebene IP Adresse des Heimnetzes mitzuteilen. Somit kann via URL des Dienstes im privaten Netzwerk auch bei ständig ändernder IP Adresse erreicht werden.

Die Infrastruktur ist bereits vorhanden und wird nur erwähnt, weil sie bei der Präsentation verwendet wird um auf das System zuzugreifen.

3.5 Vorgehen

3.5.1 Allgemeines zum Vorgehen

Bei der Erstellung der Arbeit sollen die Projektmanagement Skills angewendet werden, um die Arbeit zeitgemäß umzusetzen.

Die Fortschritte werden mit mehreren Betreuersitzungen kontrolliert und protokolliert.

3.5.2 Projektphasen

Die Arbeit wird in logische Phasen unterteilt, welche jeweils an der Betreuersitzung besprochen werden.

Die Arbeit beinhaltet folgende Phasen:

Projektphasen	
Phase	Kapitel
Vorstudie	5
Hauptstudie	6
Detailstudie	7
Realisierung	8
Abschluss	9

Tabelle 2 Projektphasen

3.5.3 Arbeitspakete

Die Projektphasen werden in kleinere Arbeitspakte gegliedert um eine genauere Aufwandschätzung machen zu können. Ebenfalls werden die Pakete anhand eines Zeitdiagramm dargestellt.

Siehe: Kapital 5.3.2 Aufwandschätzung Arbeitspaket / 5.4.3 Zeitdiagramm

3.5.4 Meilensteine

Die Meilensteine dienen dazu sich den Weg für eine erfolgreiche Arbeit zu stecken. Dabei werden Abschlüsse von Studien oder Arbeitspaketen verwendet.

Die Meilensteine habe ich in einer Liste zusammengetragen und können auch aus dem Zeitdiagramm entnommen werden.

Siehe: Kapitel 5.4.3 Zeitdiagramm / 5.4.2 Meilensteine

4 Themenvorschlag

4.1 Themenvorschlag

4.1.1 Beschreibung

Durch die Digitalisierung wird der zuverlässige Austausch von Geschäftsdaten immer wichtiger. Mittels Standortvernetzung wird ein Datenaustausch innerhalb eines Firmennetzwerks, zwischen mehreren Standorten, gewährleistet. Dabei werden nicht nur Informationen übertragen, sondern zugleich auch die Telefonie.

4.1.2 Aufgabenstellung

Die Aufgabenstellung besteht darin, eine Umgebung eines KMU nachzubauen, welches über 3 Standorte verfügt. Die Standorte sind über eine WAN-Infrastruktur miteinander vernetzt. An einem der Standorte befindet sich der Hauptsitz, an welchem die zentrale Firewall und die Telefonie Lösung installiert sind. Der Internet-Zugang erfolgt für alle Standorte über den Hauptsitz und wird über die zentrale Firewall gesteuert. Zusätzlich wird, an allen Standorten, eine WLAN Infrastruktur aufgebaut, welche über ein Cloud-Management verfügt.

Gliedern Sie ihre Arbeit in folgende Teilaufgaben:

- Projektplanung
- Einarbeitung in das Thema Standortvernetzung, Netzwerk-Segmentierung (VLAN), IT-Sicherheit (Firewall) und WLAN-Infrastruktur mit Cloud-Management.
- Erstellung eines Pflichtenheftes mit Prioritäten
- Evaluation geeigneter Komponenten und Dienste
- Aufbau einer KMU-Umgebung mit 3 Standorten
- Folgende Netzwerk-Dienste, sind minimal zu implementieren: - DNS, DHCP, Internet, Telefonie und WLAN mit Cloud-Management, für alle 3 Standorte verfügbar
- Definition und Umsetzung eines IT-Sicherheits-Grundschutz (Firewall)
- Durchführung entsprechender Funktionstest und Gegenüberstellung Pflichtenheft
- Erstellung der technischen Dokumentation für Administratoren
- Dokumentation aller Arbeitsschritte

5 Vorstudie

5.1 Zweck und Umfang

Im Rahmen der Vorstudie werden verbindliche Aussagen zu Machbarkeit, Risiken und Nutzen erarbeitet. Die Grundlage dazu bietet Analyse der aktuellen Situation sowie klar vereinbarte Ziele. Die vereinbarten Ziele sind die Grundlage für die Hauptstudie und können nicht mehr verändert werden.

5.2 Pflichtenheft

5.2.1 Zweck und Umfang

Im Pflichtenheft wird beschrieben, wie und womit ich die Arbeit erstelle. Sie beinhaltet den Umfang der Arbeit und wird vom Auftraggeber (Betreuer) freigegeben oder beanstandet.

5.2.2 Kriterien

Unter diesem Kapitel zeige ich auf welche Kriterien erfüllt werden müssen und welche noch zusätzlich ausgeführt werden könnten, wenn es zeitlich reicht. Ebenfalls wird konkreter auf die einzelnen Punkte eingegangen und Richtlinien für die Umsetzung zu schaffen.

5.2.3 Muss-/Wunsch-Kriterien

Pflichtenheft			
Tätigkeit	Muss Ziele	Wunsch Ziele	Gewichtung
1. Planung			
1.1 Netzwerkkonzept erstellen	x		1
1.2 Sicherheitskonzept erstellen	x		1
1.3 Telefonie Konzept erstellen	x		1
1.4 WLAN-Konzept erstellen	x		1
2. Server und Dienste			
2.1 Server für Dienste aufsetzen	x		2
2.2 DHCP Server konfigurieren	x		2
2.3 DNS konfigurieren	x		2
2.4 TFTP/ConfigFile Server		x	3
3. Komponenten			
3.1 Routing / Switching			
3.1.1 Routing konfigurieren	x		2
3.1.2 Switching konfigurieren	x		2
3.1.3 WLAN-Konfiguration	x		2
3.1.4 Anbindung an Heimnetz / Internet	x		2
3.1.5 NAT-Konfiguration	x		2
3.2 Telefonie			
3.2.1 PBX aufsetzen und konfigurieren	x		2
3.2.2 Telefone konfigurieren	x		2
3.2.3 SIP Trunk anbinden	x		2
3.2.4 SBC		x	3
3.3 Firewall			
3.3.1 Firewall konfigurieren	x		2
3.3.2 ACL konfigurieren		x	3
3.3.3 VPN einrichten		x	3
3.4 Operation			
3.4.1 Monitoring		x	3
3.4.2 Syslog		x	3

Tabelle 3 Pflichtenheft

5.2.4 Details zu den Kriterien

5.2.4.1 Planung

Es soll zu jedem System ein möglichst genauer Netzwerkplan erstellt werden, um die Funktion und Umsetzung aufzuzeigen.

Folgende Zeichnungen sollen erstellt werden:

- Verkabelung
- VLAN
- Routing
- DNS
- DHCP
- WLAN
- VoIP
- Firewall

5.2.4.2 Server

Um die Serverdienste zur Verfügung zu stellen, muss ein geeignetes Server Betriebssystem evaluiert werden. Grundsätzlich sollen folgende Dienste bereitgestellt werden:

- DNS
- DHCP

5.2.4.2.1 DHCP

Durch die Unterteilung der Netze entsteht die Herausforderung einen DHCP Server zentral zu Verwalten. Dieses Problem entsteht, da die DHCP Discovery Nachrichten nur im eigenen Netz versendet wird und somit nicht geroutet wird. Durch die Funktion des DHCP Relay Agents oder unter Cisco IP-Helper genannt, soll eine zentrale Verwaltung umgesetzt werden, somit kann der administrative Aufwand minimiert werden.

5.2.4.2.2 DNS

Es soll mittels rekursivem DNS Server soll ein zentraler Punkt für die Namenauflösung umgesetzt werden. Somit gehen alle Anfragen aus den verschiedenen Netzen zum DNS Server und dieser löst die Namen nach Adresse auf oder dieser löst die Anfrage über einen externen DNS-Server auf. Somit kann der DNS Verkehr in das Internet mittels Firewall auf den DNS Server reduziert werden, was auch zur Sicherheit beiträgt.

5.2.4.3 VoIP

Die VoIP Umgebung soll folgende Komponenten enthalten:

- PBX
- Session Border Controller
- SIP Trunk

5.2.4.3.1 PBX

Die VoIP Umgebung wird mittels Alcatel-Lucent Omni PCX Enterprise PBX umgesetzt. Hierbei handelt es sich um eine Applikation, welche auf einem Linux Betriebssystem läuft. Diese soll virtuell auf einem ESX laufen. Sie dient als Registrar für lokale VoIP Telefone und übernimmt die Signalisierung für Verbindungen. Es werden nur einfache Telefone angelegt sowie ein SIP Trunk angemeldet um extern telefonieren zu können.

5.2.4.3.2 Session Border Controller

Um die PBX mit dem externen Netz zu verbinden wir ein SBC verwendet. Dieser soll für die Sicherheit sorgen und stellt z.B. mit Transcoding verschiedene Codecs für den Medienwechsel zur Verfügung. Hier wird ein Produkt der Firma AudioCodes verwendet, der ebenfalls virtuell auf einem ESX installiert werden soll. Der SBC soll als sogenannter „two-leg-SBC“ umgesetzt werden, wobei ein Bein auf den Call Server geht und das zweite auf die Firewall Richtung SIP Provider.

5.2.4.3.3 SIP Provider

Als SIP Provider habe ich von der Firma Peoplefone einen SIP Trunk zu Testzwecken zur Verfügung gestellt bekommen. Dieser enthält einen Nummernblock von 5 Nummern und einem Prepaid Guthaben von 20.- CHF, welcher für die Umsetzung und Tests ausreicht.

5.3 Aufwandschätzung

5.3.1 Aufwandschätzung der Projektphasen

Aufwandschätzung Projektphasen		
Phase	Aufwand (h)	Bemerkung
Vorstudie	40	
Hauptstudie	40	
Detailstudie	60	
Realisierung	60	
Abschluss	70	inkl. Doku
	Total 270h	

Tabelle 4 Aufwandschätzung Projektphasen

5.3.2 Aufwandschätzung Arbeitspakete

Aufwandschätzung Projektphasen im Detail		
Phase	Arbeitspaket	Aufwand (h)
Vorstudie	Aufwandschätzung, Terminplanung	5
	Einarbeitung, Einführung	15
	Pflichtenheft	20
Hauptstudie	Evaluation HW, Planung	20
	Evaluation SW, Planung	20
Detailstudie	Auswahl HW, Detailplanung	30
	Auswahl SW, Detailplanung	30
Realisierung	HW Umgebung	20
	SW Installation	30
	Tests	10
Abschluss	Doku	60
	Rückblick / Ausblick	5
	Präsentation	5
		Total 270.-

Tabelle 5 Aufwandschätzung Projektphasen im Detail

5.3.3 Kostenschätzung

Die Kostenschätzung wird nur für Geräte oder Software berechnet, welche auch zusätzlich besorgt wird. Da weitgehendst alles zur Verfügung steht oder ein Open Source Programm verwendet wird, muss somit nur die WLAN Lösung geschätzt werden.

Kostenschätzung	
Komponente / Dienst / Lizenz	Preis
Access Point	ca. 500.- CHF
AP Lizenz	ca.100.- / Jahr

Tabelle 6 Kostenschätzung

5.4 Terminplanung

Anhand der folgenden Zeitplanung kann kontrolliert werden, ob der Ist-Fortschritt dem Soll-Fortschritt entspricht.

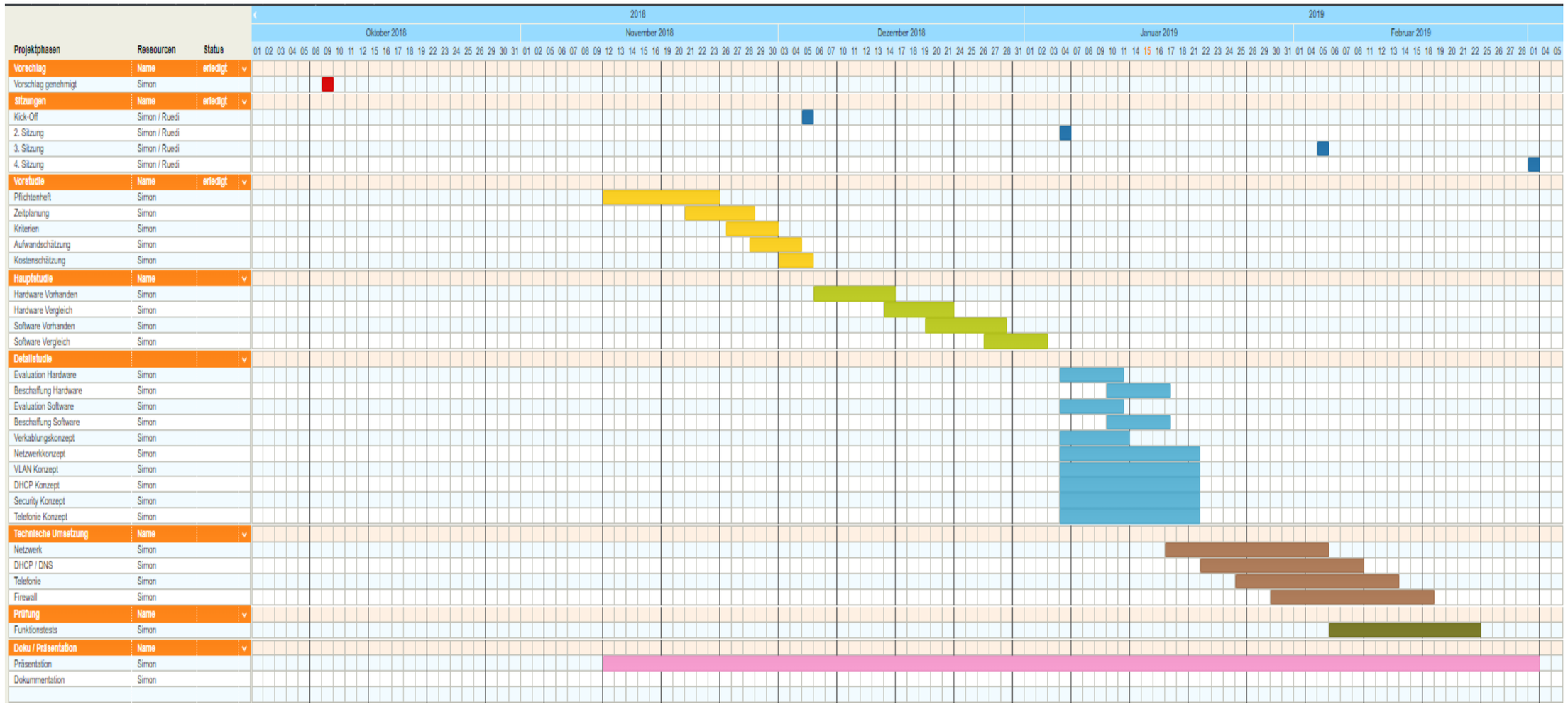


Abbildung 1 Terminplanung

5.4.1 Umfang und Zweck Terminplanung

Die Terminplanung bestimmt die Reihenfolge der Vorgänge meiner Arbeit, ebenfalls werden die Zusammenhänge zwischen den verschiedenen Arbeitspaketen aufgezeigt. Die Terminplanung dient ebenfalls zur Bestimmung der Start- sowie Endtermine.

5.4.2 Meilensteine

Die folgende Tabelle zeigt alle Meilensteine der Vordiplomarbeit auf. Sie teilen meine Arbeit in überschaubare Etappen, welche für ein gelingen der Arbeit erforderlich sind.

Meilensteine		
Datum	Meilenstein	Bemerkung
8.2018	Vorschlag erstellen	Durch Studierenden erstellt
8.2018	Vorschlag einreichen	An Sekretariat eingereicht
10.2018	Aufgabenstellung	Durch Sekretariat erhalten
11.2018	Pflichtenheft	Durch Studierenden erstellt
11.2018	Kick-Off	Student / Betreuer
11.2018	Vorstudie	Durch Studierenden erstellt
12.2018	Sitzung 1	Student / Betreuer
12.2018	Hauptstudie	Durch Studierenden erstellt
1.2019	Detailstudie	Durch Studierenden erstellt
2.2019	Sitzung 2	Student / Betreuer
2.2019	Realisierung	Durch Studierenden erstellt
3.2019	Sitzung 3	Student / Betreuer
3.2019	Abschluss	Durch Studierenden erstellt
3.2019	Doku	Durch Studierenden erstellt
4.2019	Präsentation	Durch Studierenden erstellt
4.2019	Ausstellung	Durch Studierenden erstellt

Tabelle 7 Meilensteine

5.4.3 Termine

Termin	Arbeit	Verantwortung
bis 30. Juni 18	Information über Bestimmungen und Einreichung von Vorschlägen	Bereichsleiter
bis 20. Aug. 18	Studierende reichen Vorschläge ein	Studierende
bis 10. 9. 18	Bereinigung der Themenvorschläge mit Studierenden	Betreuer
bis 12.09.2018	Auftrag zum Schreiben der Aufgabenstellungen an die Betreuerpersonen	Bereichsleiter
bis 18. Sept. 18	Aufgabenstellung zur Validierung an Bereichsleiter	Betreuer
bis 29. 9. 18	Aufgabenstellung validieren; in Dropbox speichern Mitteilung an Sekretariat	Bereichsleiter
bis 9. Okt. 18	Aufgabenstellungen an Studierende mailen	Sekretariat
Nov/Dez 18	Zuteilung der Experten und Expertinnen anhand der Aufgabenstellungen	Sekretariat
bis 4. März 19	Abgabe oder Einsenden der 2 Dokumentationen an das Sekretariat	Studierende
bis 6./7. März 19	Verschicken der Dokumentationen an Betreuer und Experten	Sekretariat
bis 22.03.2019	Versand Präsentationsplan an Studierende	Sekretariat
Sa 30. März 19	Präsentation der Diplomarbeiten	Studierende
Sa 30. März 19	öffentliche Ausstellung aller Diplomarbeiten	Studierende
Fr 12. April 19	Diplomfeier	Alle

Tabelle 8 Termine

6 Hauptstudie

6.1 Zweck und Umfang

In der Hauptstudie wird die Vorstudie genauer bearbeitet und konkretisiert. Ebenfalls werden die verschiedenen Hardware Komponenten sowie Software evaluiert.

Die Auswahl der Varianten wird danach in der Detailstudie bewertet und für die Realisierungsphase ausgewählt.

6.2 Hardware

6.2.1 Vorhandene Hardware

Da ich mir bereits ein kleines Labor zum rumtüfteln bei mir Zuhause angelegt habe, zähle ich hier die verwendeten Komponenten auf und erläutere deren Funktion.

Ausführliche Datasheets zu den Geräten sind auf dem angehängten USB Stick hinterlegt.

6.2.1.1 Intel NUC

Intel NUC Hades Canyon NUC8I7HNK2 (Intel Core i7-8705G, HDMI)

Intel NUC	
Prozessor	
Prozessortyp	Intel Core i7-8705G
Prozessor Taktfrequenz	3.10 GHz
Anzahl Prozessoren	1 x
Anzahl Prozessorkerne	4 (Quad Core)
Speicher	
Arbeitsspeichertyp	DDR4-RAM
Arbeitsspeicher (RAM)	32 GB
Speichermedium	SSD
Speichergrösse	500 GB
Netzwerk	
Ethernet-Ports	2 x
Port Geschwindigkeit	1 Gbit/s

Tabelle 9 Intel NUC

6.2.1.2 Cisco Catalyst 3560 (Switch)

Es stehen 3 Cisco Catalyst 3560 Switches zur Verfügung, wobei pro Standort ein Gerät verbaut wird. Die Switches sind im heutigen Gebrauch nicht mehr Zeitgemäss, da die Bandbreite auf 100 Mbit/s begrenzt ist. Für meine Laborumgebung sind sie bestens geeignet, da die Konfiguration und das CLI gleich wie neue Systeme konfiguriert wird. Bei den Switches handelt es sich um reine Layer 2 Switches somit muss das Inter-VLAN Routing von einem Router übernommen werden.

Switch	
Ports	24 x 10/100 Mbit/s
SFP	2
POE	Ja
HE	1
Management	CLI

Tabelle 10 Switch

6.2.1.3 Cisco 1841 (Router)

Wie beim Switch stehen mir 3 Geräte zur Verfügung, die ebenfalls etwas älter sind und sind mit seriellen WAN Slots ausgestattet. Somit kann zwischen den Standorten ein Border Gateway Protokoll verwendet werden. Sie werden im Netz primär für das Routing zwischen den VLAN verwendet.

Router	
Ports	2 x 10/100 Mbit/s
Serial Slots	2 (1 Einschub verwendet)
POE	Nein
HE	1
Management	CLI

Tabelle 11 Router

6.2.1.4 FortiGate 61^{E} (Firewall)

Firewall	
Ethernet	10 x GE
Serial	1
USB	1
UTM	ja
Durchsatz	3 Gbit/s

Tabelle 12 Firewall

6.2.2 WLAN

Alle Standorte sollen mit WLAN für Gäste sowie für BYOD aufgerüstet werden, um ein Enterprise Produkt zu evaluieren habe ich diverse führende Hersteller miteinander verglichen, um in der Evaluation das richtige Produkt zu wählen.

Tabelle 13 WLAN Gegenüberstellung

Hersteller	Produkt	Typ	Management	AP	Anzahl Client	Beschaffung	Preis AP	Preis Lizenez	Preis Appliance
Hewlett Packard	Aerohive Hive Manager NG	On-Premises / Cloud-Managed	Virtual oder Cloud	Physisch	Unlimitiert	HP Reseller	ab 220.-	ca. 140.- / Jahr und AP	ca. 1800.-
Aruba	Mobility Controller	On-Premises	Physisch oder Cloud	Physisch	<32'768 p. Appliance	Aruba Reseller	ab 260.-	keine	ca. 3000.-
Aruba	Central	Cloud-Managed	Cloud	Physisch	Unlimitiert	Aruba Reseller	ab 310.-	140.- / Jahr und AP	-
Cisco	Aironet	On-Premisis	Physisch	Physisch	<64'000 p. Appliance	Cisco Reseller	ab 350.-	keine	ca. 1000.-
Cisco	Meraki MR	Cloud-Managed	Cloud	Physisch	Unlimitiert	Cisco Reseller	ab 400.-	150.- /Jahr pro Cloud Controller	-
Extreme Networks	WiNG	On-Premises	Physisch und Virtual	Physisch	<200'000 p. Appliance	Extreme Network Reseller	ab 350.-	keine	ca. 4500.-
Extreme Networks	ExtremeCloud	Cloud-Managed	Cloud	Physisch	Unlimitiert	Extreme Network Reseller	ab 350.-	140.- / Jahr und AP	-
Ruckus Wireless	SmartZone	On-Premisis	Physisch oder Virtual	Physisch	100'000 p. Appliance	Ruckus Wireless Reseller	ab 370.-	keine	ca. 1300.-
Ruckus Wireless	Cloud Wi-Fi	Cloud-Managed	Cloud	Physisch	Unlimitiert	Ruckus Wireless Reseller	ab 370.-	120.- / Jahr und AP bei mehr als 1 AP	-

6.3 Software

6.3.1 Vorhandene Software

Wie bereits im Abschnitt 6.2.1 Hardware erwähnt, erläutere ich hier noch die vorhandene Software und deren Funktion.

6.3.1.1 VMWare vSphere ESXi 6.7

VMware ESX ist ein von VMware Inc. entwickeltes Produkt, das für die Server Virtualisierung eingesetzt wird. Es läuft ohne ein vorhandenes Betriebssystem auf der physischen Maschine. Dadurch können Hardwarekosten minimiert werden und alle Server über dasselbe Verwaltungsinstrument gewartet werden.

6.3.1.2 OpenVPN Server

Für die Präsentation meiner Arbeit muss der Zugriff auf das System gewährleistet werden, hierfür verwende ich meinen OpenVPN Server. Dieser erlaubt es mir einen VPN Tunnel auf mein System herzustellen und interne Adressen aufzurufen oder mittels Putty auf Systeme zuzugreifen.

6.3.1.3 Audiocodes Mediant Virtual Edition 7.20 (SBC)

Von Audiocodes steht mir der Mediant VE zu Verfügung, welcher ohne Lizenzen zwei gleichzeitige Sessions zulässt. Der Vorteil dabei ist, dass er mit allen Features konfiguriert werden kann und die virtuelle Version keine zusätzliche Hardware benötigt.

6.3.1.4 Alcatel Omni PCX Enterprise Virtual Edition R12.2(PBX)

Bei der Alcatel Omni PCX Enterprise handelt es sich um einen Call Server, welcher für grössere Unternehmen konzipiert ist. Er kann jedoch auch für kleinere Installationen verwendet werden. Hier setze ich ebenfalls auf eine virtuelle Version, diese kann bei höheren Ansprüchen auch um ISDN oder analog Gateway erweitert werden.

6.3.1.5 Alcatel IP Desktop Softphone 11.1.13

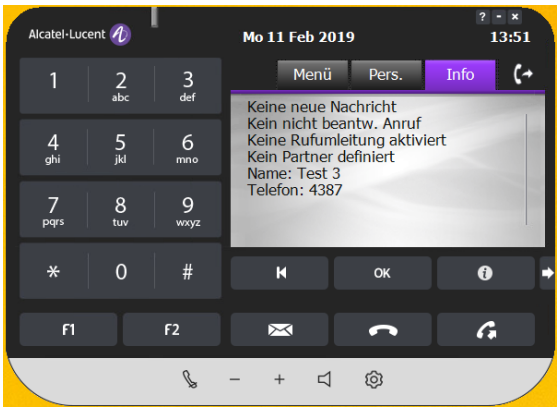


Abbildung 2 Softphone

Bei dem Alcatel IP Desktop Softphone, handelt es sich um eine Emulation des IP Touch 8068. Die Vorteile des Softphone sind Kosten Ersparnisse, ohne auf Leistungsmerkmale der Alcatel PBX zu verzichten. Für den Gebrauch wird lediglich ein Headset benötigt, welches über den PC angeschlossen werden kann.

6.3.2 Server

Um die Netze mit DHCP sowie DNS Funktion zu versorgen wird ein Server für den Betrieb gesucht. Hier werde ich ein Linux Server und Windows Server gegenüberstellen.

Server Gegenüberstellung		
	Windows	Linux
Kosten	Lizenzkosten	Supportkosten
Bedienung	GUI	CLI
Remote-Zugriff	Terminal	Terminal
Software / Features	Microsoft Anwendungen und gängige Programme	Eigene Programme, häufig nicht die gängigen
Hardware Unterstützung	neue Hardware wird nach Windows System ausgerichtet	Hardwaretreiber meist verzögert verfügbar
Sicherheit	Hohes Nutzerfehlerpotential bei Zugriff auf GUI	Durch CLI kann auch bei zufälligem Zugriff nichts ohne Grundkenntnisse geändert werden
Support	Langzeit Support	Support-Angebot variiert
Dokumentation	System und Anwendungen sind ausgezeichnet dokumentiert in verschiedenen Sprachen	System und Anwendungen sind dokumentiert, meist nur auf Englisch

Tabelle 14 Server Gegenüberstellung

7 Detailstudie

7.1 Zweck und Umfang

In der Detailstudie werden die evaluierten Komponenten, die Software sowie die Hardware, verglichen und die Auswahl für die Realisierung zusammengestellt.

Dabei liegt das Augenmerk auf möglichst Kostengünstige sowie an der besten realisierbaren Lösung. Die Auswahl wird mittels Wertung der verschiedenen Eigenschaften getroffen.

7.2 Auswahl der Hardware

7.2.1 WLAN

Hier werde ich das WLAN Produkt evaluieren, dabei habe ich oben die Kriterien und im Raster die Wertungen. Dabei werden Wertungen von 1 – 5 vergeben, wobei 1 „trifft nicht zu“ und 5 „trifft vollkommen zu“ bedeuten.

Name des Produktes	Homogenes Netz	Typ	Cloud Managed	Anzahl Client	Beschaffung	Preis	Jährliche Kosten	Preis Anschaffung	Ergebnis
Aerohive Hive Manager NG	1	5	5	5	3	4	3	1	27
Mobility Controller	1	1	5	2	5	4	5	1	24
Central	1	5	5	5	5	3	3	5	31
Aironet	5	0	1	3	5	3	5	1	24
Meraki MR	5	5	5	5	5	2	3	5	35
WiNG	1	0	1	4	3	3	5	1	18
ExtremeCloud	1	5	5	5	3	3	3	5	30
SmartZone	1	0	1	4	3	3	5	1	18
Cloud Wi-Fi	1	5	5	5	3	3	3	5	30

Tabelle 15 Auswahl WLAN

Somit werde ich für die Managed-Cloud WLAN Lösung das Produkt Meraki von Cisco verwenden. Es hat am besten abgeschnitten, da die bestehende Umgebung bereits auf Cisco basiert und Cisco proprietäre Funktionen unterstützt werden.

7.2.1.1 WLAN Access Point

Ich habe mich für das günstigste Model der Meraki Access Point entschieden, da die Installation für den Umfang der Arbeit ausreicht. Folgendes Model wurde gekauft:

Abbildung 3 Access Point

Hersteller	Cisco Meraki
Modell	MR30H
Senderfrequenz	2.4 / 5 GHz Dualband
Interface	1 x 10/100/1000 Base-T Input
Interface	1 x Gbit Ethernet mit PoE
Interface	3 x Gbit Ethernet Output
Management	GUI in Cloud

Tabelle 16 Access Point

7.2.1.2 WLAN Cloud-Managed Lizenz

Um den Access Point via Cloud zu managen wird eine Lizenz benötigt, diese kann bei Cisco Partner bezogen werden und ist mit verschiedenen Laufzeiten erhältlich. Für die Arbeit wird die Lizenz mit einem Jahr Laufzeit erworben.

Hersteller	Cisco Meraki
Modell	Meraki LIC-ENT-1YR
Beschreibung	Meraki Lizenz zu Access Point
Lizenzdauer	1 Jahr
Preis	147.- CHF
Management	GUI in Cloud

Tabelle 17 Cloud Lizenz

7.3 Auswahl der Software / Dienste

7.3.1 DHCP/DNS Server

Folgend werde ich ein Server System für meinen DNS/DHCP Server evaluieren. Da es nur eine Gegenüberstellung von 2 Produkten ist wird eine Wertung von 1 – 3 vorgenommen. Hier gilt wieder 1 „trifft nicht zu“ und 3 „trifft vollkommen zu“

Wertung Windows	Windows	Linux	Wertung Linux
1	Lizenzkosten	Supportkosten	1
3	GUI	CLI	1
3	Terminal	Terminal	3
3	Microsoft Anwendungen und gängige Programme	Eigene Programme, häufig nicht die gängigen	2
3	neue Hardware wird meist nach Windows System ausgerichtet	Hardwaretreiber meist verzögert verfügbar	2
1	Hohes Nutzerfehlerpotential bei Zugriff auf GUI	Durch CLI kann auch bei zufälligem Zugriff nichts ohne Grundkenntnisse geändert werden	3
3	Langzeit Support	Support-Angebot variiert	2
3	System und Anwendungen sind ausgezeichnet dokumentiert in verschiedenen Sprachen	System und Anwendungen sind dokumentiert, meist nur auf Englisch	2
20	Windows Server	Linux Server	16

Tabelle 18 Server Auswahl

Das Serverbetriebssystem für meine Dienste, wird mit dem Windows Server 2016 umgesetzt. Es sticht besonders durch seine Komptabilität und Dokumentation hervor. Ich persönlich bevorzuge auch das GUI von Windows, da es übersichtlicher ist und ich nicht alle Befehle auswendig kennen muss.

7.4 Konzepte

7.4.1 Netzwerk Übersicht

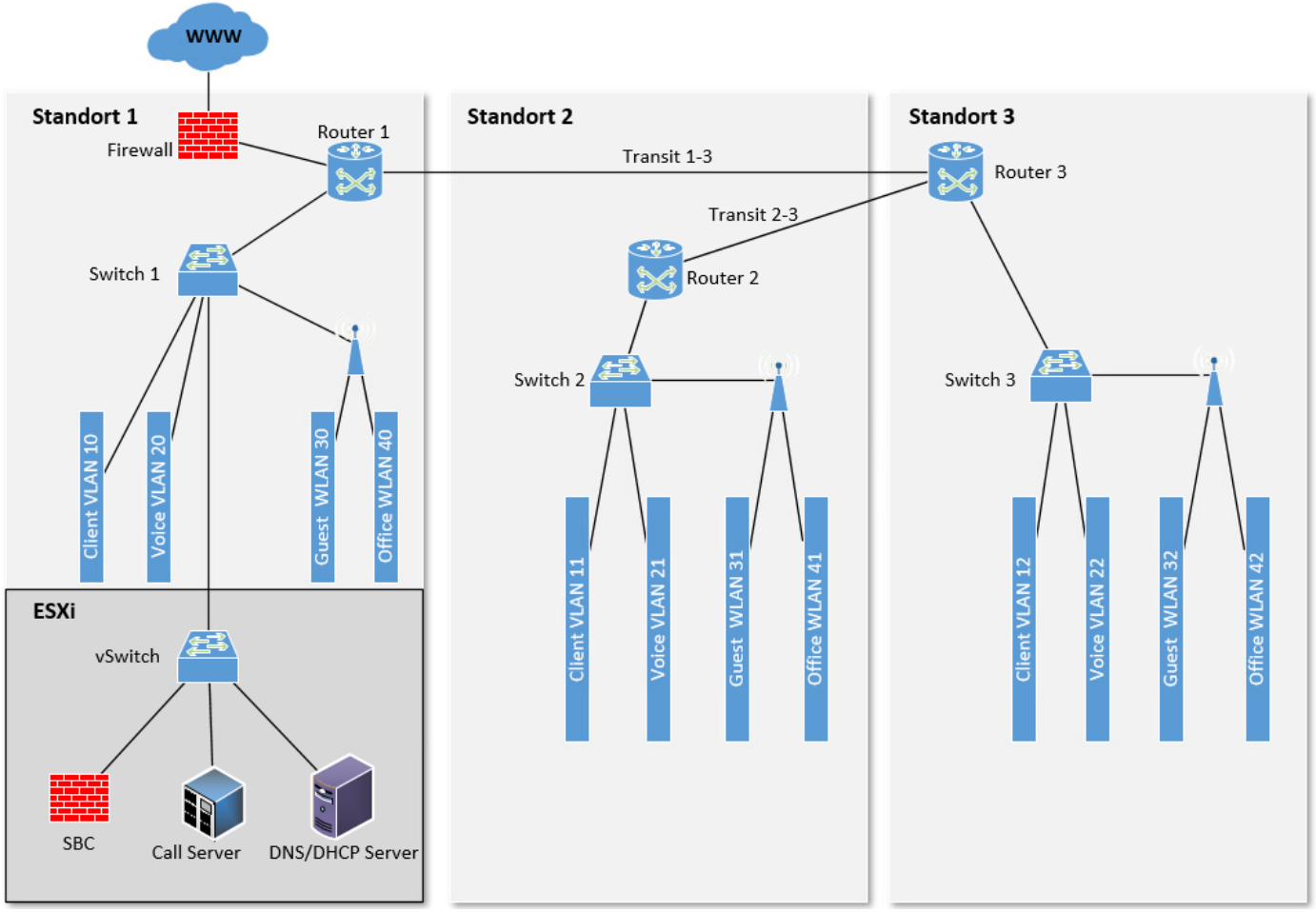


Abbildung 6 Netzwerk Übersicht

7.4.1.1 IP-Vergabe

Lokation	Name	VLAN-ID	Netz	Beschreibung	Geräte	Gateway
Standort 1	Standort 1					
	Client1	10	10.10.0.0/24	Client Standort1 DHCP	PC DHCP	10.10.0.254/24
	Voice1	20	10.10.64.0/24	Voice Standort1 DHCP	Telefon DHCP	10.10.64.254/24
	WLAN_Guest1	30	10.10.128.0/24	WLAN Guest Standort1 DHCP	WLAN Client Guest DHCP	10.10.128.254/24
	WLAN_Office1	40	10.10.192.0/24	WLAN Office Standort1 DHCP	WLAN Client Office DHCP	10.10.192.254/24
Standort 2	Standort 2					
	Client2	11	10.20.0.0/24	Client Standort2 DHCP	PC DHCP	10.20.0.254/24
	Voice2	21	10.20.64.0/24	Voice Standort2 DHCP	Telefon DHCP	10.20.64.254/24
	WLAN_Guest2	31	10.20.128.0/24	WLAN Guest Standort2 DHCP	WLAN Client Guest DHCP	10.20.128.254/24
	WLAN_Office2	41	10.20.192.0/24	WLAN Office Standort2 DHCP	WLAN Client Office DHCP	10.20.192.254/24
Standort 3	Standort 3					
	Client3	12	10.30.0.0/24	Client Standort3 DHCP	PC DHCP	10.30.0.254/24
	Voice3	22	10.30.64.0/24	Voice Standort3 DHCP	Telefon DHCP	10.30.64.254/24
	WLAN_Guest3	32	10.30.128.0/24	WLAN Guest Standort3 DHCP	WLAN Client Guest DHCP	10.30.128.254/24
	WLAN_Voice3	42	10.30.192.0/24	WLAN Voice Standort3 DHCP	WLAN Client Office DHCP	10.30.192.254/24
Systeme	Systeme					
	Voice FW-SBC	29	10.40.0.0/29	Voice Outbound Static	SBC 10.40.0.2/29, FW 10.40.0.1/29	10.40.0.6/29
	Voice SBC-CS	28	10.40.0.8/29	Voice Inbound Static	SBC 10.40.0.10/29, CS 10.40.0.13/29	10.40.0.14/29
	Server	50	10.40.128.0/24	Server Static	DNS DHCP 10.40.128.10/24	10.40.128.254/24
	Ausgehend		10.255.255.254	Ausgehend Internet	FW 10.255.255.254/24	10.255.255.254/24
Transfer	Transfer					
	S1 - S3	-	10.50.0.4/30	Standort 1 nach Standort 3	Router1 10.50.0.5/30, Router3 10.50.0.6/30	-
	S2 - S3	-	10.50.0.8/30	Standort 2 nach Standort 3	Router2 10.50.0.9/30, Router3 10.50.0.10/30	-

Tabelle 19 IP-Vergabe

7.4.2 Verkabelung

Da den verwendeten Switch nur über 10/100 Mbit/s Ports verfügen, muss für die maximale Datenübertragung mindesten es Kat. 5 Kabel verwendet werden. In meinem Fall werde ich Kat. 5e Kabel verwenden, da ich diese bereits vorhanden habe und nach einer Aufrüstung ebenfalls mit Gigabit Ethernet ausreichen würden.

Für die Transit-Strecken zwischen den Router werden serielle Kabel mit DTE und DCE Kabel verwendet.

Kabel	
Typ	Anzahl
Kat 5e Kupfer	9
seriellen Kabel mit DTE und DTE Stecker	3

Tabelle 20 Kabel

7.4.3 VLAN

Übersicht der Portverteilung, Port 1 wird in der Umsetzung jedoch als VLAN 0 belassen und fungiert als Managementzugang. Weitere Angaben zu den verwendeten VLAN sieht man unten in der Tabelle.

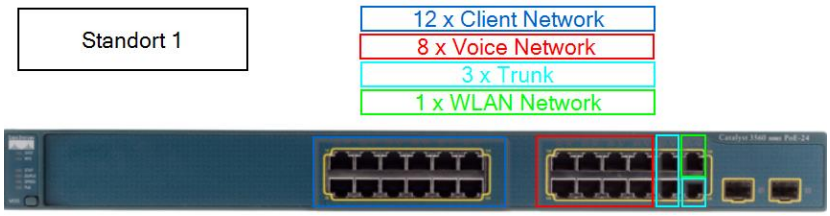


Abbildung 7 Switch Standort 1

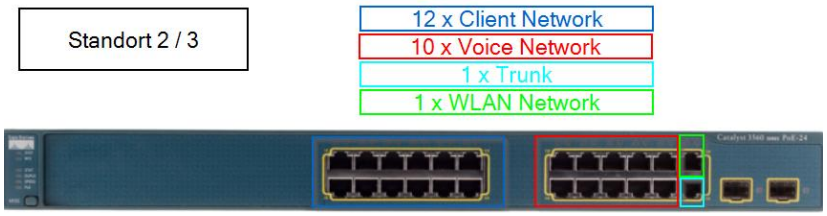


Abbildung 8 Switch Standort 2/3

Name	IP	VLAN-ID
	Standort 1	
Client1	10.10.0.20/24	10
Voice1	10.10.64.20/2	20
WLAN_Guest1	10.10.128.20/24	30
WLAN_Office1	10.10.192.10/24	40
	Standort 2	
Client2	10.20.0.20/24	11
Voice2	10.20.64.20/24	21
WLAN_Guest2	10.20.128.20/24	31
WLAN_Office2	10.20.192.20/24	41
	Standort 3	
Client3	10.30.0.20/24	12
Voice3	10.30.64.20/24	22
WLAN_Guest3	10.30.128.20/24	32
WLAN_Voice3	10.30.192.20/24	42
	Systeme	
Voice FW-SBC	10.40.0.6/29	29
Voice SBC-CS	10.40.0.12/29	28
Server	10.40.128.20/24	50

Tabelle 21 Switch Port / VLAN

7.4.4 DHCP / DHCP Relay Agent

Da DHCP Anfragen nicht über das eigene Netz hinweg übertragen werden, muss für die zentrale Verwaltung in jedem Netz ein Relay Agent konfiguriert werden, welcher die Anfragen an den DHCP Server weiterleitet. Hierfür habe ich die Umsetzung wie gefolgt geplant:

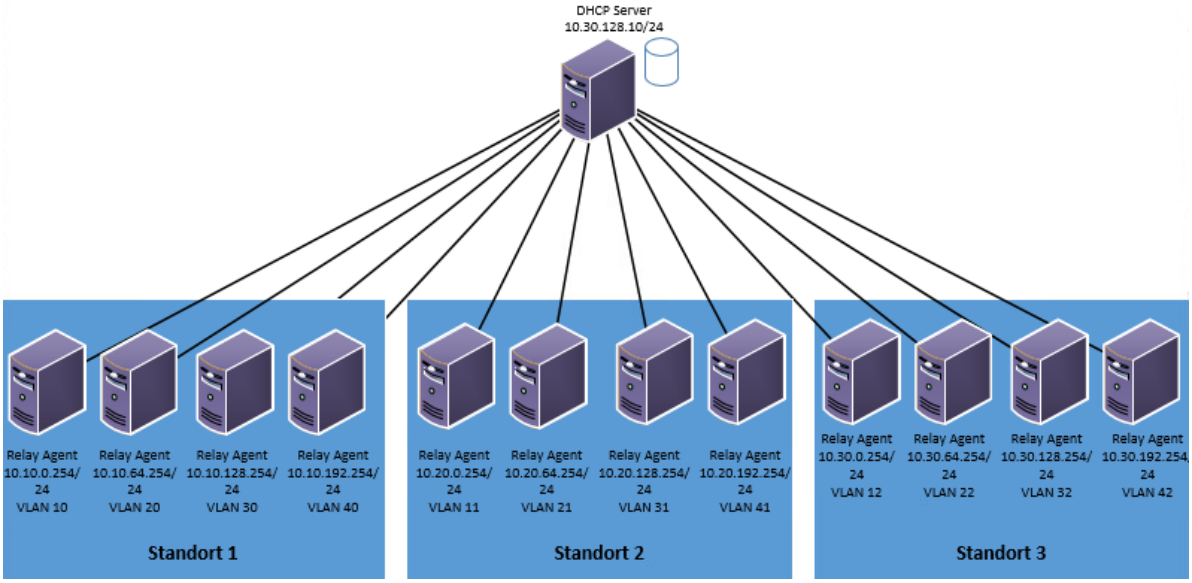


Abbildung 9 DHCP Server / Relay Agent

DHCP Server	Relay Agent	Scope	Option	VLAN-ID
	Standort 1			
10.40.128.10/24	10.10.0.254/24	10.10.0.100 -150		10
10.40.128.10/24	10.10.64.254/24	10.10.64.100 -150	43, 66, 67	20
10.40.128.10/24	10.10.128.254/24	10.10.128.100 -150		30
10.40.128.10/24	10.10.192.254/24	10.10.192.100 -150		40
	Standort 2			
10.40.128.10/24	10.20.0.254/24	10.20.0.100 -150		11
10.40.128.10/24	10.20.64.254/24	10.20.64.100 -150	43, 66, 67	21
10.40.128.10/24	10.20.128.254/24	10.20.128.100 -150		31
10.40.128.10/24	10.20.192.254/24	10.20.192.100 -150		41
	Standort 3			
10.40.128.10/24	10.30.0.254/24	10.30.0.100 -150		12
10.40.128.10/24	10.30.64.254/24	10.30.64.100 -150	43, 66, 67	22
10.40.128.10/24	10.30.128.254/24	10.30.128.100 -150		32
10.40.128.10/24	10.30.192.254/24	10.30.192.100 -150		42

Tabelle 22 DHCP

7.4.5 Routing

Da das Routing in dieser Umgebung ziemlich übersichtlich ist, werden die Routen ohne Routingprotokoll gemacht, sondern manuell gepflegt. Um die Routen zu bündeln wurden bei der IP-Vergabe darauf geachtet das komplette Standorte in einer Route zusammengefasst werden können.

Routingtabelle		
Bereich	Interface	Nach
	Router 1	
default Route	Fa0/1	Firewall 10.255.255.254
10.10.0.0/24	Fa0.0.10	Switch Trunk VLAN 10
10.10.64.0/24	Fa0/0.20	Switch Trunk VLAN 20
10.10.128.0/24	Fa0/0.30	Switch Trunk VLAN 30
10.10.192.0/24	Fa0/0.40	Switch Trunk VLAN 40
10.40.0.0/30	Fa0/0.28	Switch Trunk VLAN 28
10.40.0.8/29	Fa0/0.28	Switch Trunk VLAN 29
10.40.128.0/24	Fa0/0.50	Switch Trunk VLAN 50
10.20.0.0/16		Router 2
10.30.0.0/16		Router 3
	Router 2	
default Route		Router 1
10.20.0.0/24	Fa0.0.11	Switch Trunk VLAN 11
10.20.64.0/24	Fa0/0.21	Switch Trunk VLAN 21
10.20.128.0/24	Fa0/0.31	Switch Trunk VLAN 31
10.20.192.0/24	Fa0/0.41	Switch Trunk VLAN 41
10.10.0.0/16		Router 1
10.30.0.0/16		Router 3
10.40.0.0/16		Router 1
	Router 3	
default Route		Router 1
10.30.0.0/24	Fa0.0.12	Switch Trunk VLAN 12
10.30.64.0/24	Fa0/0.22	Switch Trunk VLAN 22
10.30.128.0/24	Fa0/0.32	Switch Trunk VLAN 32
10.30.192.0/24	Fa0/0.42	Switch Trunk VLAN 42
10.10.0.0/16		Router 1
10.20.0.0/16		Router 2
10.40.0.0/16		Router 1

Tabelle 23 Routing Tabelle

Da die Router nur über eine begrenzte Anzahl physische Interface besitz wird ein Trunk an den Router angebunden, dass Router Interface wird dann in Subinterfaces aufgetrennt, jeweils eines pro VLAN. Dadurch wird bereits im Router das VLAN eingesetzt und die DHCP-Relay Agent können auf diesen Subinterfaces konfiguriert werden.

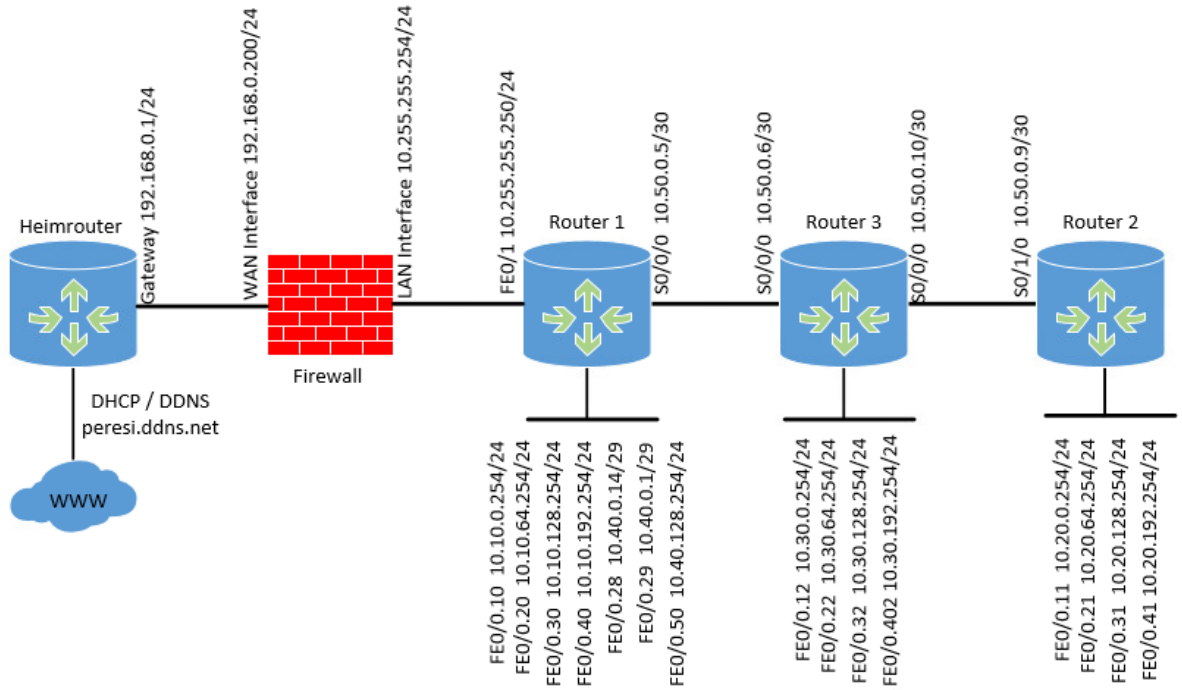


Abbildung 10 Routing

Auf den Transfer Routen zwischen den Routern, werden auf Grund mangelnder Ethernet Interfaces, die seriellen Schnittstellen verwendet. Diese werden mittels HDLC verkapselt und mit einem seriellen Kabel mit DTE und DTE Stecker verbunden. Hier muss beachtet werden das auf der DCE Seite eine Clock Rate konfiguriert werden muss, da diese Verbindung getaktet wird.

7.4.6 Firewall

Die Firewall über den WAN Port an mein Heimnetz angeschlossen, somit simuliere ich mit meinem Heimnetz den ISP. Hierfür vergebe ich auf dem WAN Port eine IP aus meinem Heimnetz und Route eingehenden Verkehr, welcher für meine Arbeit vorgesehen ist in diese Richtung. Dieses Vorgehen nennt sich Portforwarding, dabei wird der Ziel-Port des eingehenden Packets mit der Portforwardingliste verglichen und gemäss Liste weitergeleitet. Für meine Arbeit müssen zwei Portforwarding-Regeln auf dem Router und eine Regel auf der Firewall konfiguriert werden. Dies ergibt folgende eingehende Regeln:

Portforwarding			
Gerät	Port	Ziel	Ziel IP
Firewall	5060	SBC	10.40.0.2 (Outbound Port)
Heim Router	5060	Firewall	192.168.0.200
Heim Router	1193	VPN Server	192.168.0.60

Tabelle 24 Portforwarding

Da ich auf der WAN Seite nur ein IP habe, werden ich ein dynamisches NAT ohne PAT konfigurieren. Wobei ich eine externe IP Adresse und mehrere interne Hosts habe, welche nach extern kommunizieren. Um den Verkehr zwischen Firewall und SBC zu kanalisieren, wird bereits ab der Firewall, anhand des oben erwähnten Portforwardings, der Voice Verkehr in ein VLAN geroutet.

7.4.6.2 Whitelist

Um den Verkehr in das Internet zu Regeln wird eine Whitelist implementiert, diese verhindert das ungewünschte Protokolle oder Ziele nicht erreichbar sind oder nicht zur Verfügung stellen. Interne Regeln werden im nächsten Kapitel mittels ACL geregelt. Um den Verkehr möglichst knapp zu halten, werden nur benötigte Protokolle zugelassen.

Firewall - Whitelist		
Protokoll	Source IP	Destination
DNS 53	DNS Server	Swisscom DNS
HTTPS 443	any	any
SIP 5060 TCP	SBC	sips.peoplefone.ch
SIP 5060 TCP	sips.peoplefone.ch	SBC
RTP UDP	any	Telefon Subnetze
RTP UDP	Telefon Subnetze	any
ICMP	intern	extern
NTP	Intern	extern

Tabelle 25 Firewall Whitelist

7.4.6.3 Webfilter

Um den Mitarbeitern der Firma den Zugriff auf anstössige Seiten oder Social Media zu blockieren, wird ein Webfilter implementiert. Leider kann dieser nur geplant werden und nicht realisiert, da die Lizenz auf meiner Firewall fehlt.

Webfilter		
Schlagwort	URL	Action
facebook	https://facebook*	Block
instagram	https://instagram*	Block
anstössig	https://diverse	Block

Tabelle 26 Webfilter

7.4.6.4 ACL

Mit ACL werden auf Router Interfaces Regeln implementiert um den Datenverkehr zu regeln. Für meine Realisierung werde ich Regeln für das Gäste WLAN sowie für den Zugriff auf das Server Netz implementieren.

7.4.6.5 ACL Guest WLAN

Um das Gäste WLAN vom Firmennetz zu trennen, werden auf dem Router Regeln konfiguriert, die den Zugriff einschränken. Generell soll vom Gäste WLAN nur das Internet zu Verfügung stehen. Deshalb wird am Router auf der Installationsseite eine ACL Regel implementiert, welche den Datenverkehr in das Firmennetz untersagt. Diese soll möglichst nahe am Access Point konfiguriert werden, um unnötig die Bandbreite zu belasten.

ACL Guest_WLAN			
From	To	Protokol	Klassifizierung
Guest_WLAN	DNS Server 10.40.128.10/32	DNS 53	permit
Guest_WLAN	DHCP Server 10.40.128.10/32	DHCP 67/68	permit
Guest_WLAN	10.0.0.0/8	any	deny
Guest_WLAN	Any (Internet)	www	permit

Tabelle 27 ACL Guest WLAN

Diese Regel wird als „in“ definiert, somit wirkt diese auf eingehende Nachrichten auf den Router.

7.4.6.6 ACL Server

Die Serverumgebung wird ebenfalls mit einer ACL Liste geschützt, hier sollen nur diese Protokolle erlaubt werden, welche für die Serverdienste notwendig sind.

ACL Guest_WLAN			
From	To	Protokol	Klassifizierung
10.0.0.0/8	DNS Server 10.40.128.10/32	DNS 53	permit
10.0.0.0/8	DHCP Server 10.40.128.10/32	DHCP 67/68	permit
SBC	Syslog Server 10.40.128.10/32	514	permit
any	10.40.128.0/24	any	deny

Tabelle 28 ACL Server

Diese Regel wird als „out“ auf dem Gateway Interfaces des Servers gelegt und wirkt somit nach der Bearbeitung durch den Router.

7.4.7 Telefonie

Durch den Einsatz eines Session Border Controllers, kann auf das SIP ALG der Firewall verzichtet werden. Um zu gewährleisten das alle eingehende Anrufe entgegengenommen werden können, werde ich mit dem SBC das SDP so anpassen, dass alle Codecs bei welchen keine Lizenzgebühren anfallen zulassen werden. Intern wird jedoch nur der Codec G711 A-Law verwendet. Ebenfalls wird über den SBC die SIP Signalisierung normalisiert um die Kommunikation zu gewährleisten.

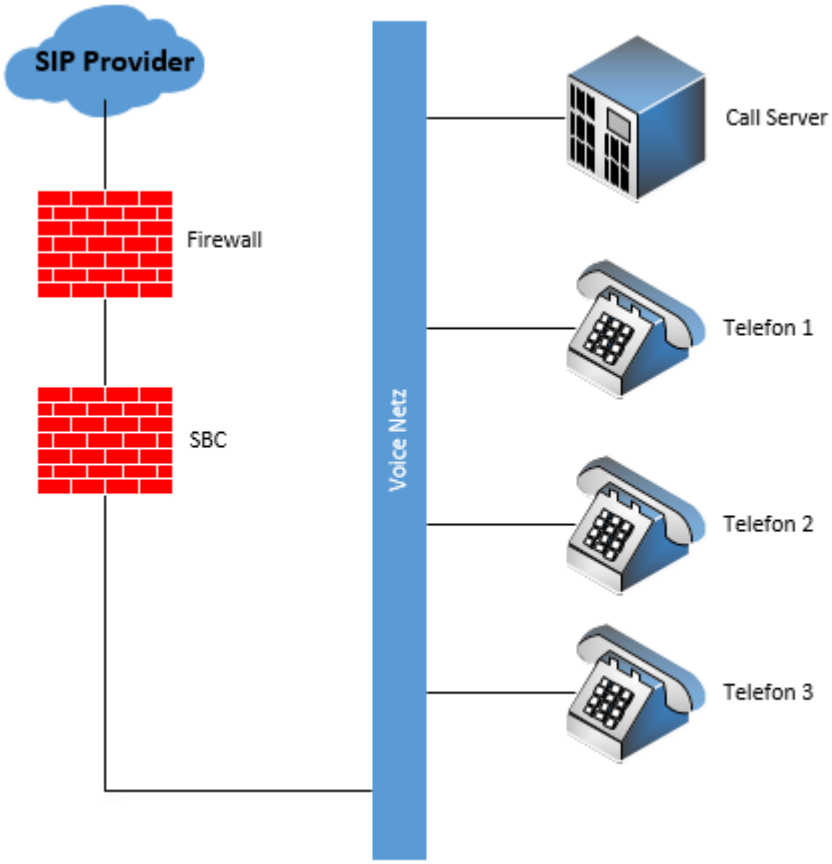


Abbildung 11 Telefonie Übersicht

Die Telefonie an sich, wird nicht mit vielen Features umgesetzt. Wichtig ist das die externe Telefonie funktioniert und die Rufnummernanzeige stimmt. Die Konfiguration besteht aus folgenden Punkten:

- CPU Loading
- Grundkonfiguration
- Trunk Anbindung
- User einrichten

7.4.7.1 SIP Trunk

Der SIP Trunk wurde von der Firma Peoplefone zur Verfügung gestellt, anbei die Trunk Informationen:

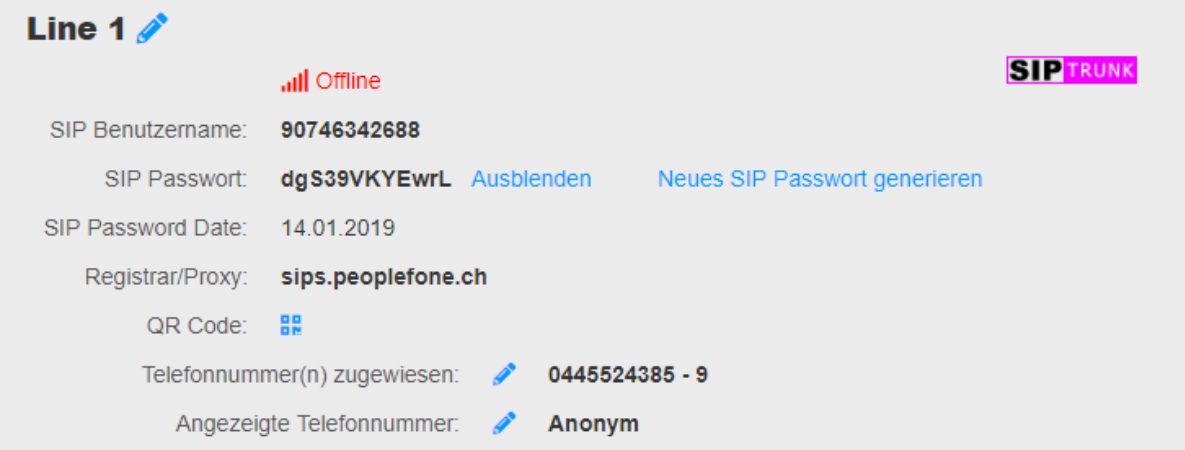


Abbildung 12 Provider Trunk

SIP Trunk	
Name	Wert
SIP Benutzername	90746342688
SIP Passwort	dgS39VKYEwrL
Registrar	sips.peoplefone.ch
Telefonnummer	044'552'43'85
Blockgrösse	5

Tabelle 29 SIP Trunk

7.4.7.2 User

Folgende Test User werden auf der Anlage konfiguriert, dabei steht ein Alcatel IP Touch 8068 zur Verfügung. Weitere Test User werden auf Softphones konfiguriert.

Userübersicht		
Name	interne Nummer	Externe Nummer
Test 1	4385	044 552 43 85
Test 2	4386	044 552 43 86
Test 3	4387	044 552 43 87
Test 4	4388	044 552 43 88
Test 5	4389	044 552 43 89

Tabelle 30 Nummernplan

7.4.7.3 Aufbau eines Telefonats

Wie bei den meisten Telefonanlagen wird bei Alcatel ein spezielles Verfahren angewendet, um ein externes Telefonat aufzubauen. Hier wird auf die einzelnen Schritte eingegangen und erklärt was diese machen.

Was bei einten Anlagen Amtskennziffer heisst, nennt man bei Alcatel ARS Wie der Name bereits sagt, besetzt man hier nicht einfach eine Linie, sondern durchgeht ein komplexes Verfahren um eine von mehreren Routen zu bestimmen. So kann zum Beispiel eine Vorwahl so konfiguriert werden, dass sie über einen zweiten Provider nach extern geht.

Da ich nicht über mehrere SIP Trunks, Provider oder Tarife besitze, wird meine Routen Konfiguration minimal ausfallen und somit immer über den gleichen Weg gehen.

Um Ihnen ein genaueres Bild des Ablaufs zu verschaffen, folgende Skizze:

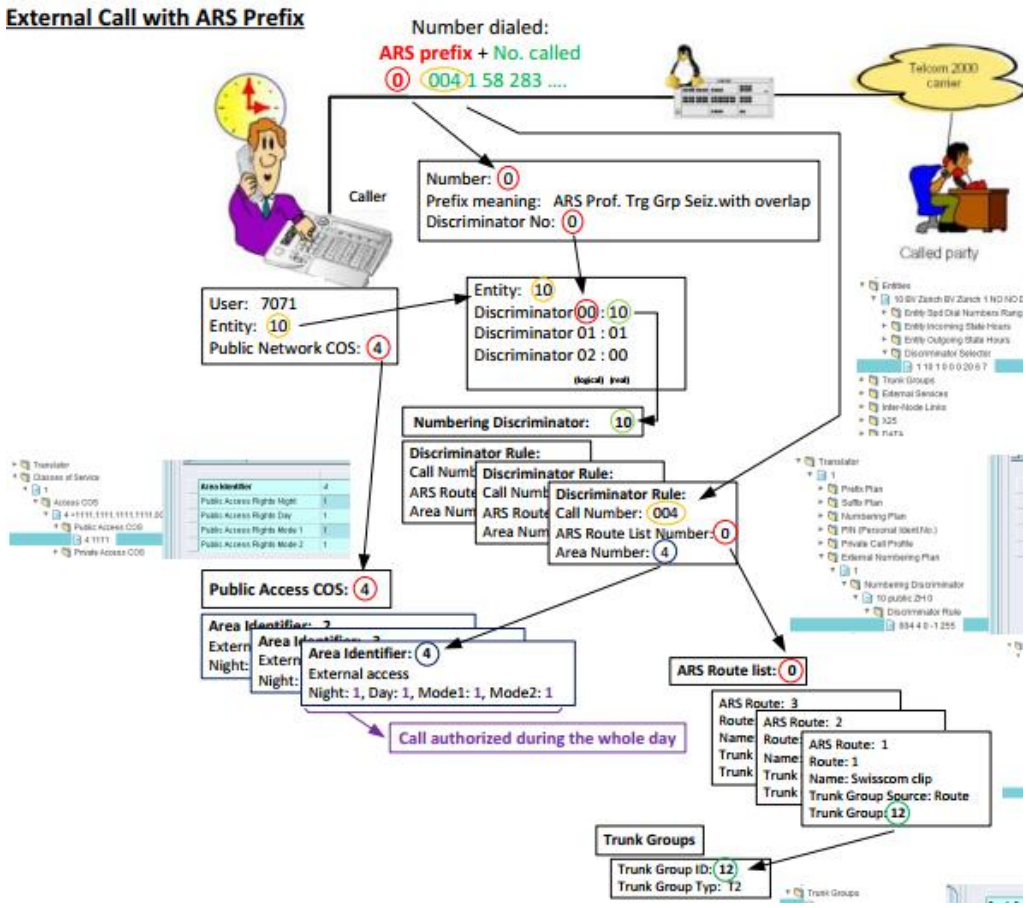


Abbildung 13 ARS

Die Konfiguration, kann aus der Realisierung entnommen werden.

7.4.8 WLAN

Um das WLAN wie gewünscht umzusetzen werden 2 SSID benötigt. Die eine SSID ist für Mitarbeiter gedacht, welche über WLAN auf Firmensystem zugreifen, das andere für Gäste, welche keinen Zugriff auf das Firmennetz haben sollen. Da es für eine Diplomarbeit zu teuer ist jeden Standort mit einem Access Point auszurüsten, wird nur an einem Standort ein Gerät verbaut und konfiguriert. Jedoch wird das ganze Netz auf einen Einbau vorbereitet.

Um die Netze voneinander zu trennen werden 2 SSID implementiert die jeweils mit eigenen VLAN vernetzt werden. Somit wird ein Trunk auf mit VLAN 3x und 4x auf die Access Points geführt.

WLAN / SSID		
SSID	VLAN	Netz
Guest1-3	3x	10.x.128.1/24
Office1-3	4x	10.x.192.1/24

Tabelle 31 WLAN SSID

Die Konfiguration findet auf der Cisco Meraki Plattform statt, hierfür muss ein Profil angelegt werden und die Cloud Lizenz eingespielt werden.

8 Realisierung

8.1 Zweck und Umfang

Nach der gesamten Planung und all deren Phasen wird das Projekt umgesetzt. Die entscheidenden Abklärungen wurden durch die Studien in den vorherigen Kapiteln gemacht.

8.2 Detaillierte Umsetzung

In der Umsetzung wird die Konfiguration ausführlich erklärt. Auf die Hardware wird nicht mehr eingegangen, da nichts beschafft werden musste was weitere Erklärungspunkte beinhaltet.

Die Realisierung wird in folgende vier Kapitel aufgeteilt:

- Netzwerk
- Telefonie
- Firewall
- DHCP / DNS Server

8.2.1 Netzwerk

8.2.1.1 Switch

8.2.1.1.1 Grundkonfiguration Switch

Die Konfiguration der verschiedenen Switches ist im Grunde dieselbe, deshalb werde ich hier nur die Dokumentation eines Switches aufzeigen. Einzug die VLAN Nummern und Adressen werden anders sein.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Switch3
Switch3(config)#line con 0
Switch3(config-line)#password cisco
Switch3(config-line)#login
Switch3(config-line)#end
Switch3#
```

hostname Switchx = Switchname Switchx setzen

line con 0 = Auf das Konsoleninterface wechseln

password cisco = Konsolenzugengspasswort auf „cisco“ setzen

login = Login für serielles Interface aktivieren

end = zurück ind den „priviledge mode „wechseln

Mit dem Konsolenkabel kann der Switch konfiguriert werden. Danach kann mittels „enable“-Befehl in den „priviledge mode“ gewechselt werden von hier aus sind keine Konfigurationen möglich, jedoch können „show“-Kommandos abgesetzt werden oder die Konfiguration gespeichert.

Um in den Konfigurationsmodus zu wechseln führt man den Befehl „configure terminal“ aus.

Nun kann die Konfiguration vorgenommen werden.

`Switch3#clock set 12:36:00 18 january 2019` clock set xxxx = setzen des Datums und Uhrzeit (wird vor allem bei Verschlüsselung wichtig)	Nun kann das Datum und Uhrzeit hinterlegt werden, es kann auch ein NTP Server hinterlegt werden.
`Switch3(config)#enable secret cisco` Enable secret cisco = Setzen eines Passworts für den „configuration mode“	Nun kann für noch mehr Sicherheit ein Passwort für die Konfiguration des Switches eingestellt werden.
`Switch3(config)#servic password-encryption` Service password-encryption = Passwörter in der Konfiguration verschlüsseln	Da die Passwörter in der start-up Konfiguration ersichtlich sind, sollten diese noch verschlüsselt werden.
`Switch3(config)#interface vlan1` `Switch3(config-if)#ip address 10.40.192.100 255.255.25` `Switch3(config-if)#no shutdown` `Switch3(config-if)#ip default-gateway 10.40.192.254` interface vlan1 = Auf das vlan1 wechseln ip adress xxxx = IP Adresse setzen no shutdown = VLAN aktivieren	Um über das Netz auf den Switch zuzugreifen muss es mit einer IP Adresse versehen werden. Somit kann die mit Ethernet Kabel vorgenommen werden und muss nicht mehr mit dem seriellen Kabel gemacht werden.
`Switch3(config)#line vty 0 4` `Switch3(config-line)#password cisco` line vty 0 4 = wählen der virtuellen Interfaces 0-4 password cisco = setzen des Passworts „cisco“ für die virtuellen Interfaces	Hier setze ich das Passwort für die virtuellen Interfaces 0 – 4, diese sind für den Zugriff über das Netz. Somit können 5 gleichzeitige Sitzungen stattfinden.
`Switch3(config)#ip name-server 10.40.128.10` ip name-server xxx = setzen des DNS Servers	Damit der Switch Namen auflösen kann, muss ein DNS-Server hinterlegt werden.

8.2.1.1.2 Konfiguration VLAN

Wie beim Switch, werde ich hier nur auf die Konfiguration eines VLAN eingehen und nicht jeden einzelnen aufzeigen.

<table>
<tr>
<td>

```
Switch3(config)#interface fa 0/2
Switch3(config-if)#switchport access vlan 12
```

interface fa 0/2 = In die Interface Konfiguration für den Port FastEthernet 0/2 wechseln

switchport access vlan 12 = Port als access port im VLAN12 setzen

</td>
<td>Als nächstes werden die VLAN erstellt und den Ports zugewiesen.</td>
</tr>
<tr>
<td>

```
12   Client3                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12
22   Voice3                           active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22
32   WLAN_Guest3                      active
42   WLAN_Office3                     active
```

show vlan brief = Anzeigen der VLAN mit dazugehörigen Ports

</td>
<td>Um das Ganze zu kontrollieren, kann man in den „priviledge mode“ wechseln und mit dem „show vlan brief“-Befehl die VLAN Übersicht aufrufen.</td>
</tr>
</table>

8.2.1.1.3 Konfiguration Trunk

<table>
<tr>
<td>

```
Switch3(config-if)#interface FastEthernet0/24
Switch3(config-if)# switchport trunk encapsulation dot1q
Switch3(config-if)# switchport trunk allowed vlan 12,22,32,42
Switch3(config-if)# switchport mode trunk
Switch3(config-if)# switchport nonegotiate
Switch3(config-if)# spanning-tree portfast
```

interface FastEthernet0/24 = in den Konfigurationsmodus des Interface 0/24 wechseln

switchport trunk encapsulation dot1q = Trunking nach 802.1q aktivieren

switchport trunk allowed 12,22,32,42 = nur diese VLAN auf dem Trunk erlauben

switchport mode trunk = Switchport Modus von Access auf Trunk wechseln

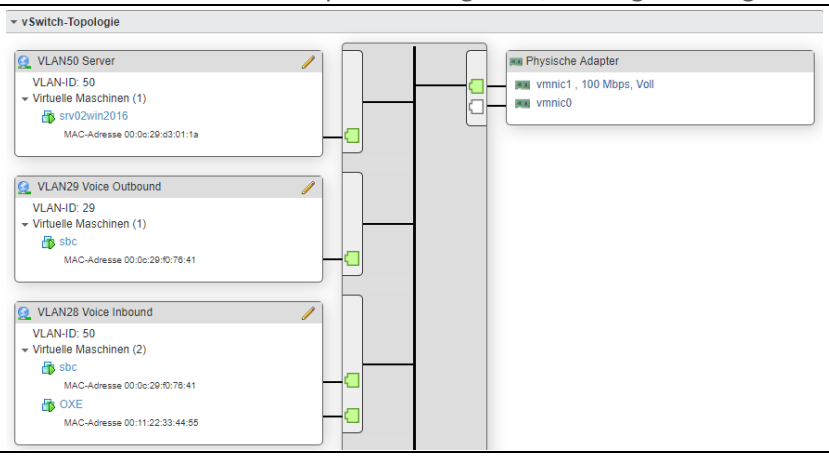
switchport nonegotiate = keine Aushandlung des Trunks, somit immer im Trunk Modus

spanning-tree portfast = berechnet die Schlaufen nicht mehr, ist somit erheblich schneller (Achtung bei Schlaufen)

</td>
<td>Da auf meinen Layer 2 Switches kein Routing möglich ist und die verschiedenen Netzt miteinander interagieren müssen, sollten Trunks erstellt werden. Dies ist bei meiner Anlage dringendst notwendig, da meine Router nur über sehr wenige Ethernet Interfaces verfügen.</td>
</tr>
</table>

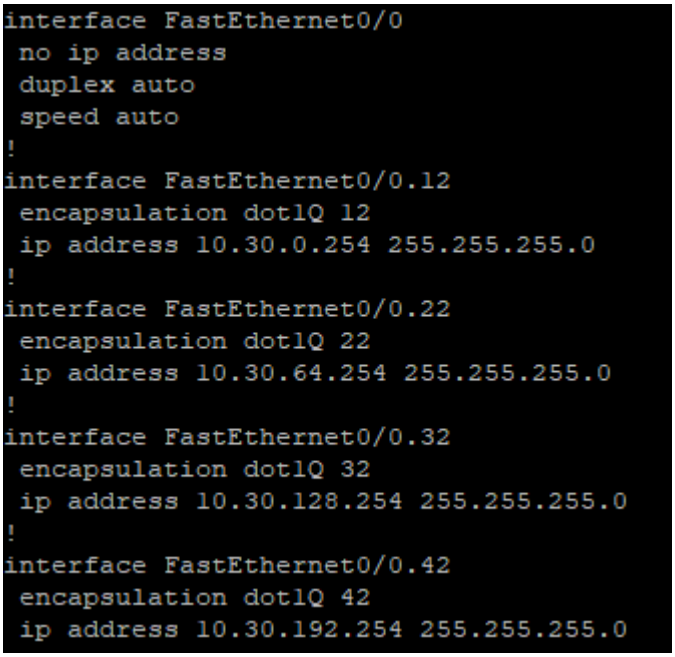
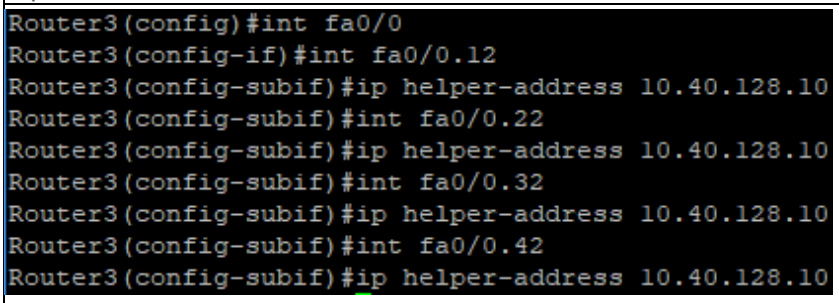
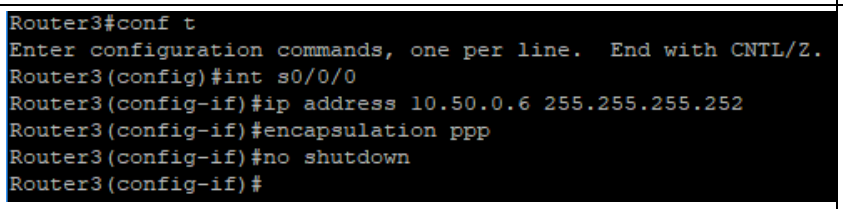
8.2.1.1.4 vSwitch

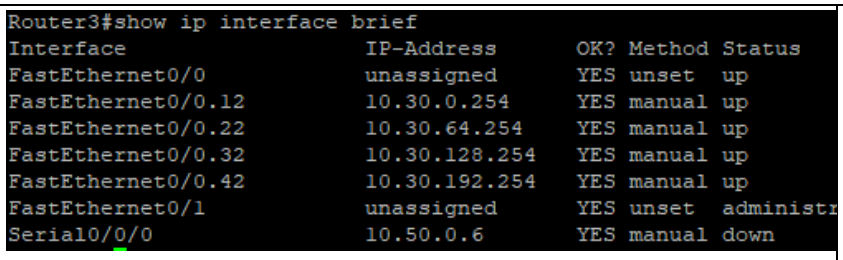
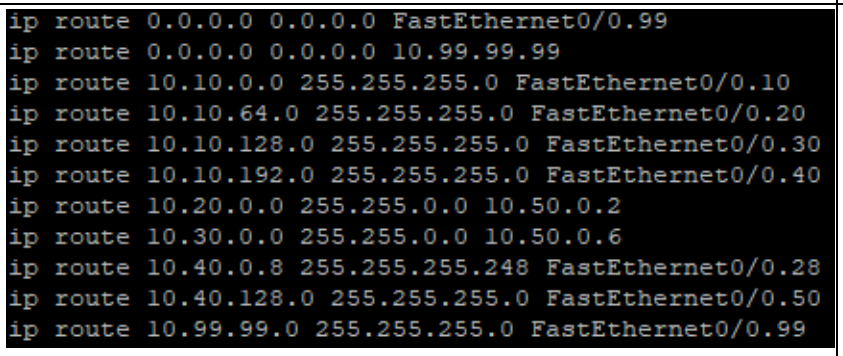
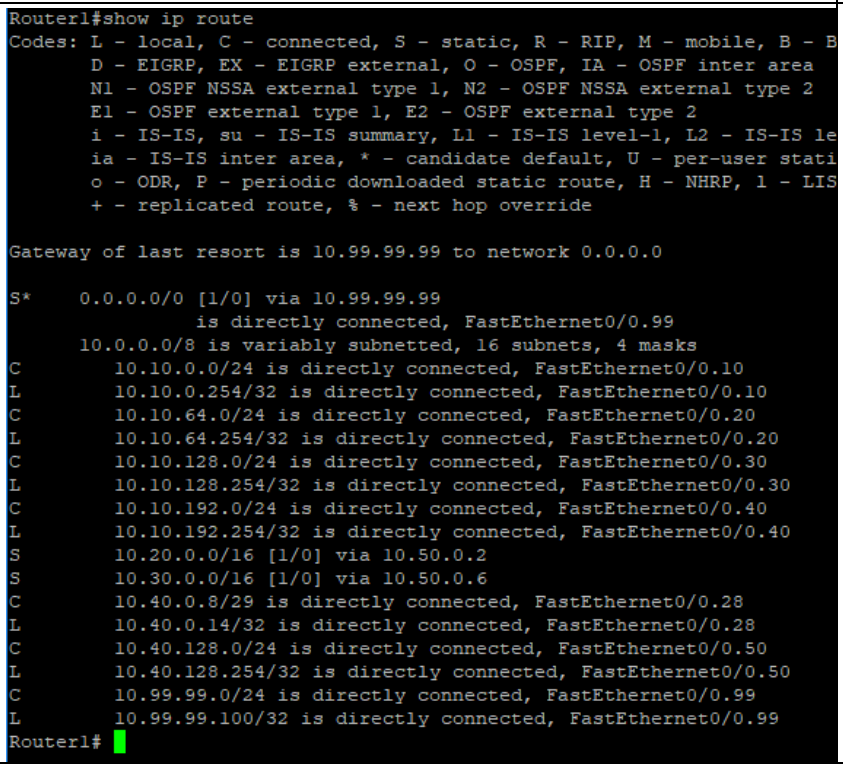
Der vSwitch wird auf dem vSphere konfiguriert, der Zugriff erfolgt über den Web Client.

	Auf dem vSwitch werden die VLAN konfiguriert und die jeweiligen Interfaces daran angeschlossen. Ein Trunk muss nicht explizit konfiguriert werden, der vSwitch generiert den 802.1q Trunk automatisch.

8.2.1.2 Router

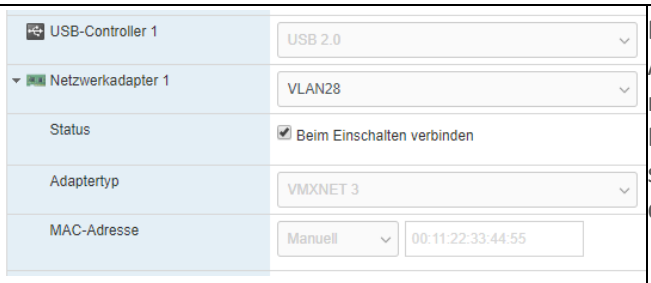
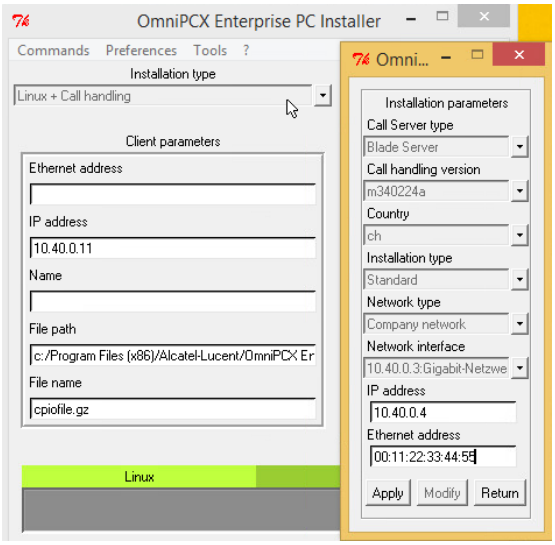
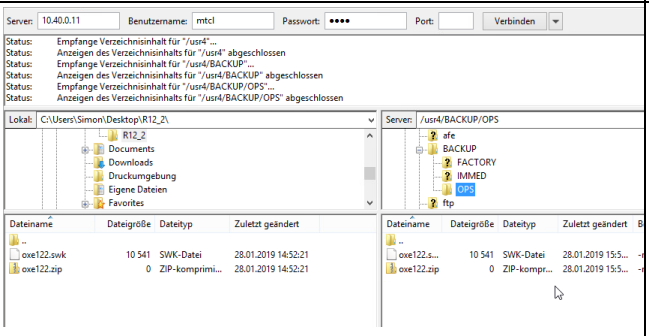
`` Router#conf t Enter configuration commands, one per line. End Router(config)#hostname Router3 ``` conf t = in den Konfigurationsmodus wechseln hostname xxx = Hostname setzen	Hier gilt wieder wie beim Switch, mit „enable“ kommt man in den „priviledge mode“ und mit configgure terminal“ in den Konfigurationsmodus
`` Router3(config)#line aux 0 Router3(config-line)#login ``` line aux 0 = in die Konfiguration für den Port aux 0 wechseln login = Zugriff nur mittels Logins erlauben	Beim Router gibt es neben dem Ethernet und seriellen Interface, auch noch einen Aux-Port, über den auf die Konfiguration zugegriffen werden kann. Deshalb wird dieser Port ebenfalls geschützt
`` Router3(config)#line con 0 Router3(config-line)#no login local Router3(config-line)#login % Login disabled on line 0, until 'password' is set Router3(config-line)#password cisco Router3(config-line)# Router3(config-line)#line vty 0 4 Router3(config-line)#no login local Router3(config-line)#login % Login disabled on line 194, until 'password' is set % Login disabled on line 195, until 'password' is set % Login disabled on line 196, until 'password' is set % Login disabled on line 197, until 'password' is set % Login disabled on line 198, until 'password' is set Router3(config-line)#password cisco ``` Die Bedeutung der Befehle kann bei der Switch Konfiguration entnommen werden.	Nun werden wie beim Switch die Zugänge gesichert. Dieser Vorgang ist derselbe wie beim Switch.

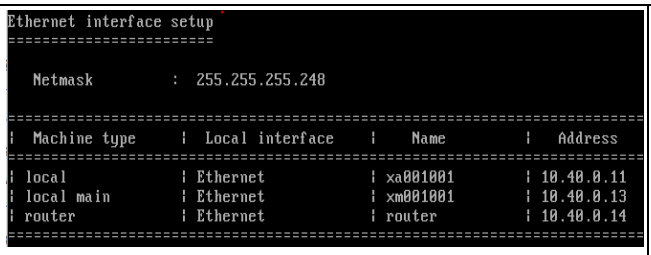
 int fa0/0.12 = Erstellen eines Subinterface auf dem Interface fa0/0 encapsulation dot1q 12 = Kappselung nach 802.1q mit VLAN ID 12 ip address xxx xxx = Setzen der IP und der Netzmaske	Da wir mit einem Trunk auf den Switch kommen müssen Subinterfaces gebildet werden, welche die Trunk Kapselung vornehmen können. Diese müssen so konfiguriert werden, dass das jeweilige Interface die richtige VLAN ID erhält.
 ip helper-address 10.40.128.10 = setzen der DHCP Server Adresse für den Relay Agent	Da die DHCP Discover Nachrichten nur im eigenen Netz gebroadcastet werden müssen die IP-Helper konfiguriert werden. Diese müssen pro Interface konfiguriert werden. Anhand der Absender Adresse weis der DHCP Server aus welchem Scope de Anfrage kommt.
 encapsulation ppp = Verkappselung mittels Point-to-Poit Protokoll	Nun kann noch die serielle Schnittstelle konfiguriert werden diese dient zur Transit Schnittstelle zu einem anderen Router. Hier muss zwingend auf die Stecker des Kabels geachtet werden, da die Taktseite vorgegeben ist.

 show ip interfaces brief = Übersicht der Interfaces aufrufen	Im „priviledge mode“ kann nun die übersicht der Interfaces überprüft werden. Hier kann ebenfalls der Status geprüft werden.
 ip route xxx xxx xxx = ip route [Ip Adresse] [Netzmaske] [Ziel IP oder Ausgangsport]	Nun werden die Routen konfiguriert diese können auch mittels VLSM zusammengefasst werden. So kann mit nur einem Routing Eintrag mehrere Netze geroutet werden.
	Mit dem Befehel „show ip route“ kann die Übersicht der Routen aufgerufen werden. Wie wir oben sehen wurde der „Gateway of last resort“ gesetzt, dieser ist der default Gateway und wird mit der Route 0.0.0.0 0.0.0.0 [Gateway] definiert.

8.2.2 Telefonie

8.2.2.1 Call Server Grundkonfiguration

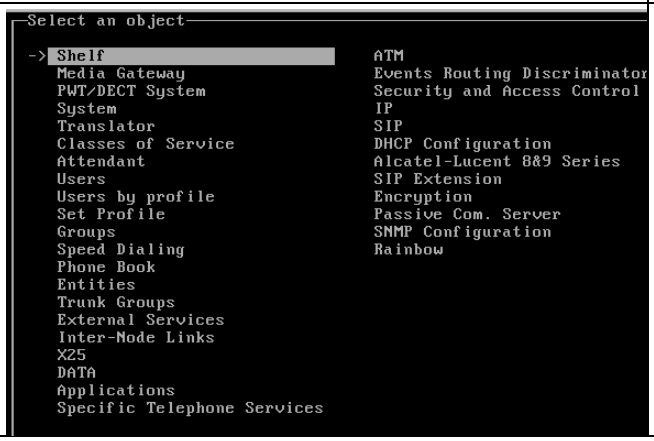
	Die VM des Call Servers wird anhand der MAC Adresse über das Netzwerk geladen. Diese muss mit der Adresse im PC Installer übereinstimmen. Ebenfalls muss die VM und der PC Installer im selben Netz sein, kann also nicht geroutet werden, da noch keine IP besteht.
	Nun kann der PC Installer installiert werden, dieser befindet sich im ISO des Call Servers und kann nach dem entpacken verwendet werden. Wichtig ist hier das für die Installation der Typ Blade Server verwendet wird und die MAC Adresse mit der oben angegebenen übereinstimmt. Nun wird das Linux OS und die Telefonapplikation geladen.
	Sobald die Installation beendet ist kann, kann das Lizenzfile geladen werden. Hierfür wird ein FTP Client verwendet. Lizenz Verzeichnis: /usr4/BACKUP/OPS
Ist das System geladen, kann mit der Konfiguration gestartet werden.	Auf der OXE gibt es folgende User: User : root Passwort: letacla User: mtcl Passwort: mtcl User: swinst Passwort SoftInst Die Funktion der User ist gemäss den Namen selbsterklärend.



NETADMIN

Mit dem Befehl «netadmin -m» kann die Netzwerkkonfiguration vorgenommen, sowie angezeigt werden.

Grundlegend wird immer eine Main Adresse konfiguriert, diese dient dazu redundante Call Server über dieselbe Adresse zu erreichen. Somit werden bei der Planung immer 3 Adressen reserviert, wobei zwei das Minimum in der Realisierung ist.

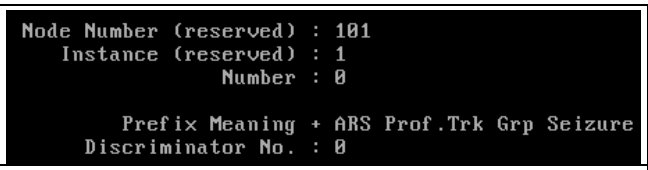


MANAGER

Um die Telefonapplikation zu konfigurieren wird mittels Befehles «mgr» der Manager aufgerufen.

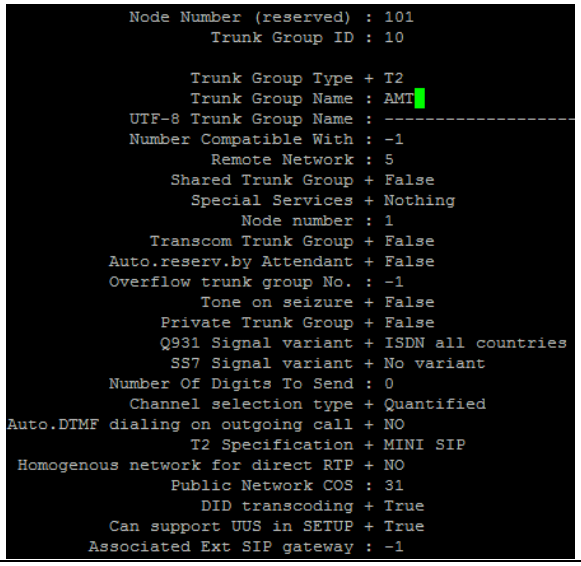
Dieses Menü erlaubt es, fast wie bei einem GUI, durch die Konfiguration zu navigieren. Hierfür werden die Pfeiltasten zu Navigieren, Ctrl+C für Rückgängig und Ctrl+V zum Bestätigen verwendet. Werte können wie gewohnt mit der Tastatur eingegeben werden.

8.2.2.2 ARS Konfiguration



ARS PRÄFIX

Erstellung des ARS Präfix für die externe Telefonie.

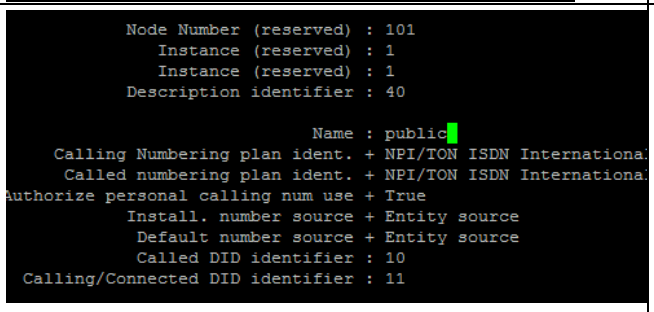


INTERNAL TRUNK

Erstellen von einem internen Trunk für die Routenbestimmung. Dieser wird ausschliesslich für externe Anrufe verwendet. Intern wird nicht das ISDN Protokoll, sondern das ABC F Protokoll verwendet. Dieser ist jedoch nur notwendig, wenn SIP Geräte verwendet werden, welche nicht von Alcatel sind.

Wichtige Punkte:

Trunk Group ID	10
Q931 Signal Variant	ISDN all countries
T2 Specification	Mini SIP



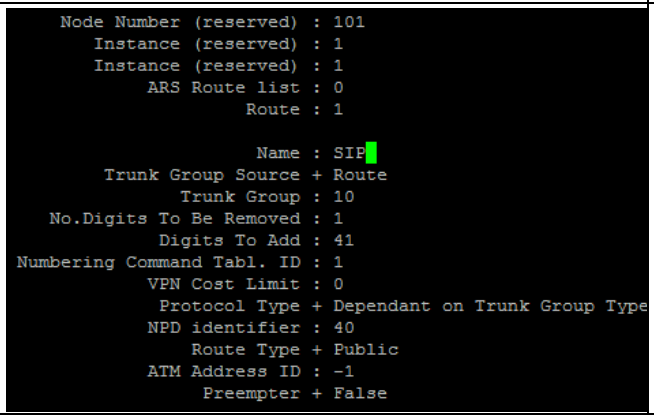
NUMBERING PLAN DESCRIPTION

Einrichten der «Numbering Plan Description», hier wird angegeben wie die Nummer extern/intern umgesetzt wird und welches Format sie haben soll.

Format: International (Fügt ein + ein)

Caller ID: 10 (Nummernübersetzung Eingehend)

Called ID: 11 (Nummernübersetzung Ausgehend)



ARS ROUTE

Hier werden weitere Angaben in der Route mitgegeben. Zum Beispiel kann der Nummer ein Country Code angefügt werden.

Trunk Group: 10 (

Digits to add: 41 (Country Code)

Digits to remove: 1 (erste Zahl entfernen)

NPD Identifier: 40

```
     Node Number (reserved) : 101
        Instance (reserved) : 1
        Instance (reserved) : 1
                   Table ID : 1

          Carrier Reference : 0
                    Command : I
Associated Ext SIP gateway : 1
```

NUMBERING COMMAND TABLE

Mit der «Numbering Comand Table» kann der externe SIP Gateway eîn die Route eingefügt werden.

Command: I (Insert/Einfügen)

Associated Ext SIP Gateway: 1

```
            Node Number (reserved) : 101
               Instance (reserved) : 1
          SIP External Gateway ID : 1

                     Gateway Name : SIP Peoplefone
                SIP Remote domain : 10.40.0.10
                   PCS IP Address : ----------
                  SIP Port Number : 5060
                   Transport type + TCP
                 Belonging Domain : 10.40.0.13
                  Registration ID : ----------
        Registration ID P_Asserted + False
                Registration timer : 0
                SIP Outbound Proxy : 10.40.0.10
                 Supervision timer : 10
                Trunk group number : 10
                       Pool Number : -1
                   Outgoing realm : ----------
                Outgoing username : ----------

                Outgoing Password : ----------
                          Confirm : ----------

                Incoming username : ----------

                Incoming Password : ----------
                          Confirm : ----------

RFC 3325 supported by the distant + True
                         DNS type + DNS A
               SIP DNS1 IP Address : ----------
               SIP DNS2 IP Address : ----------
                       SDP in 18x + False
     Minimal authentication method + SIP None
  INFO method for remote extension + False
                           To EMS + False
                             SRTP + RTP only
        Ignore inactive/black hole + False
           Contact with IP address + True
     Dynamic Payload type for DTMF : 101
           Outbound Calls 100 REL + Supported
           Incoming Calls 100 REL + Not Requested
                     Gateway type + Standard type
Re-Trans No. for REGISTER/OPTIONS : 2
   P-Asserted-ID in Calling Number + True
      Trusted P-Asserted-ID header + False
     Diversion Info to provide via + History Info
```

SIP EXTERNAL GATEWAY

Nun kann das letzte Bauteil der Route für die externe Kommunikation konfiguriert werden. Der «External SIP Gateway» ist das Bindeglied zwischen SBC und PBX, könnte jedoch auch direkt mit dem Provider verbunden werden.

SIP Remote Domain: 10.40.0.10 (SBC)

SIP Port: 5060 (Port für Signalisierung)

Transport Type: TCP

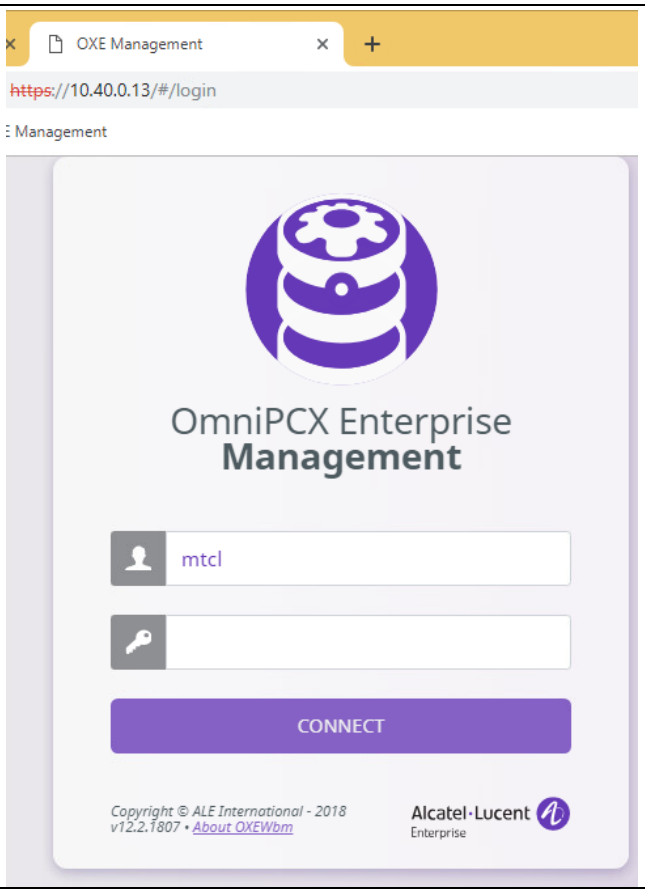
Belonging Domain: 10.40.0.13 (PBX)

SIP Outbound Proxy : 10.40.0.10 (SBC)

Supervision Timer: 10 (Keep Alive Options Timer)

Authentification: None (wird vom SBC gemacht)

8.2.2.2 User Verwaltung für Administratoren



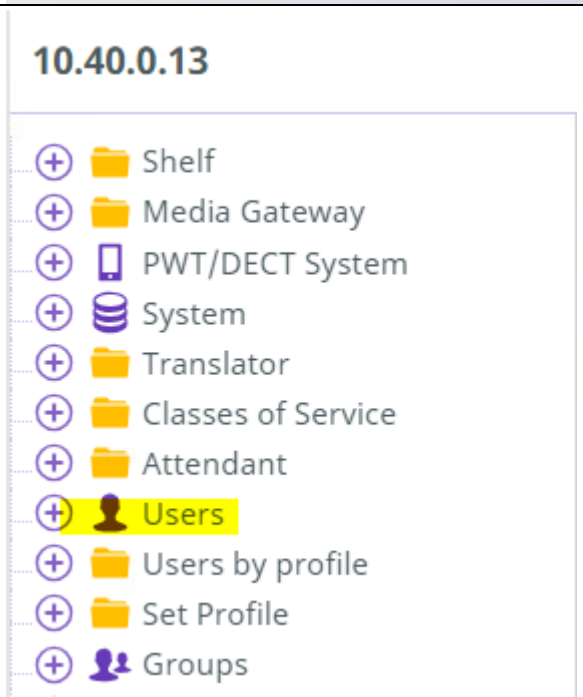
WEB BASED MANAGER WBM ZUGRIFF

Als alternative zum CLI steht auch ein GUI mittels Webzugriff zur Verfügung. Für die meisten Anwender ist das die priorisierte Variante, da sie übersichtlicher ist. Es sind keine Installationen dafür notwendig, sondern kann über die Main Adresse des Call Servers aufgerufen werden.

URL: https://10.40.0.13

User: mtcl

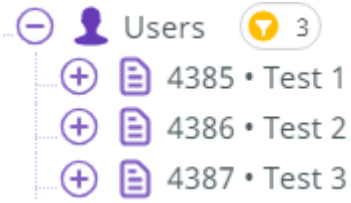
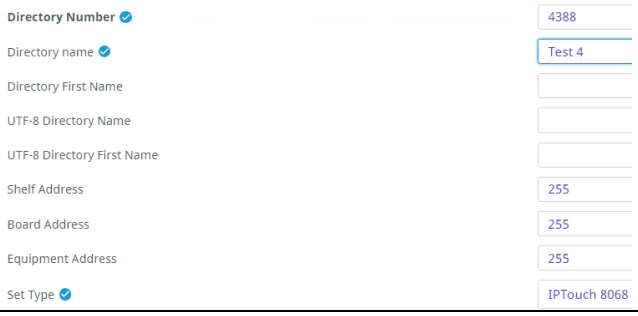
Passwort: mtcl



WBM ÜBERSICHT

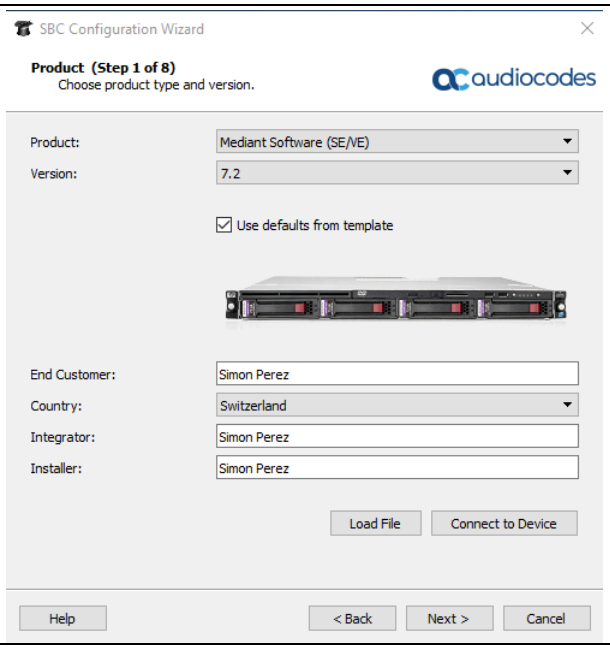
Wie auf den erstell Blick ersichtlich ist, ist der Aufbau des Web Manager derselbe wie der Manager über das CLI.

Unter User werden alle User auf dem System verwaltet. Wenn man nun das «+» drückt, klappt das User Feld auf und alle User werden ersichtlich.

	USER VERWALTUNG Die nun ersichtlichen Bentzer können hier Verwaltet werden.
	USER ERSTELLEN Mittels oben ersichtlichen «Create» kann ein neuer User angelegt werden
	USER DETAILS Nummer: Nur die letzten 4 Nummer der externen Rufnummer verwenden Set Type: Für Softphone sowie Hardphone muss der Typ IP Touch 8068 verwendet werden
Meldung auf Telefon: Please press a button **Nummer: xxxx** **Default PIN: 0000**	TELEFON ANMELDEN Der uSer muss zum Schluss noch auf dem gewünschten Gerät angemeldet werden. Hierfür wird die interne 4-stellige Nummer sowie der PIN 0000 verwendet.

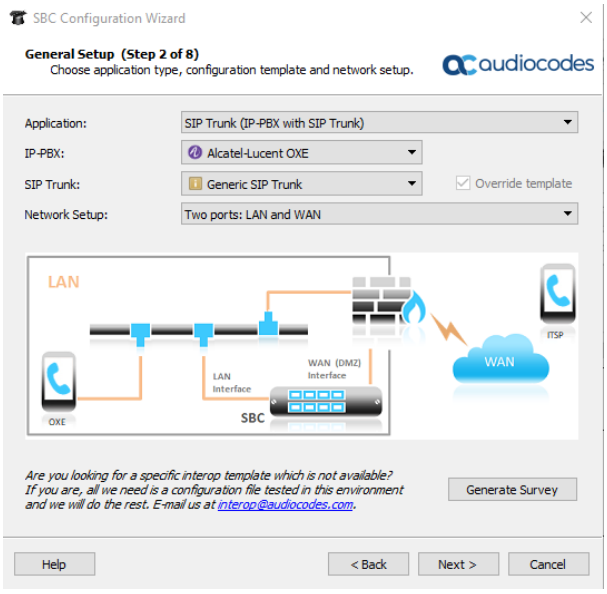
Die Installation des Session Boarder Controller kann mit dem Wizard vereinfacht konfiguriert werden. Er erzeugt eine Konfigurationsdatei, welche auf den SBC geladen werden kann.

8.2.2.2 Session Border Controller



START

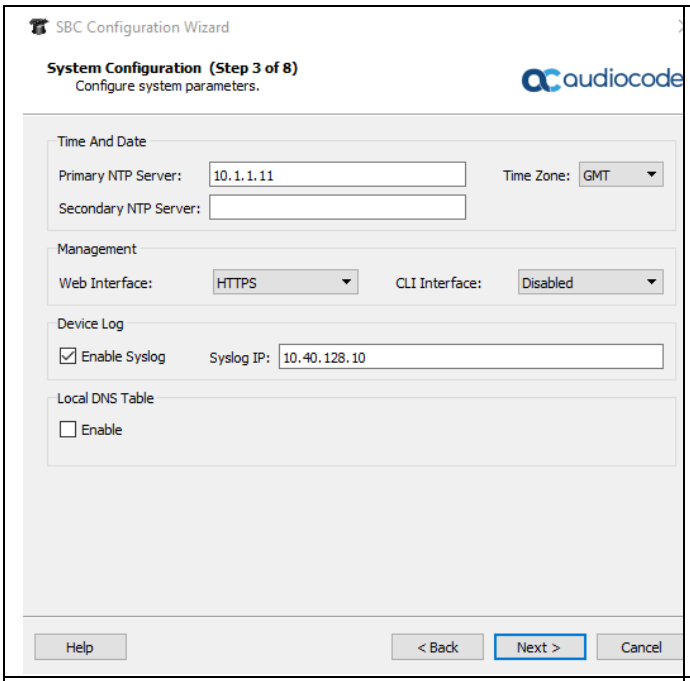
Die Installation des Session Border Controller kann mit dem Wizard vereinfacht konfiguriert werden. Er erzeugt eine Konfigurationsdatei, welche auf den SBC geladen werden kann.



ÜBERSICHT

Hier werden die PBX, Provider und der Aufbau des Netzes angegeben. Für die meisten Telefonanlagen und Provider gibt es eine Vorlage. In meinem Fall gibt es für den Provider keine. Da es sich um einen eher kleinen Provider handelt. Hier muss der «Generic SIP Trunk» ausgewählt werden und gegeben falls nach dem Laden manuell angepasst werden.

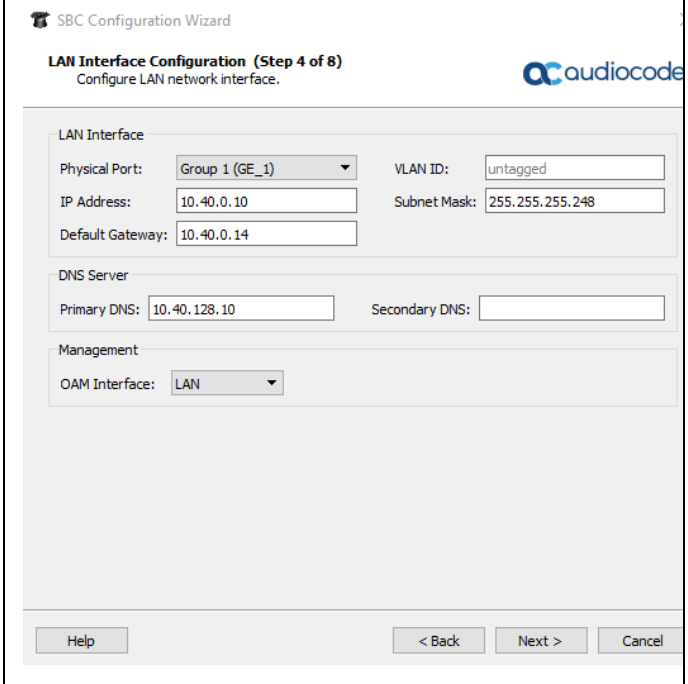
Der SBC wird mit zwei Ports und zwei IP Adressen konfiguriert.



GENARELL

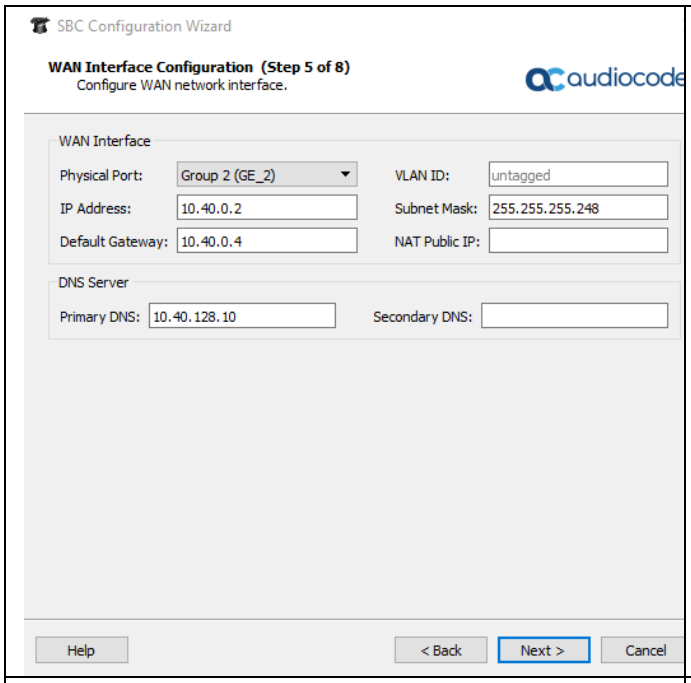
Um nach der Installation auf das Gerät zuzugreifen, wird das Protokoll HTTPS für Management Zugriff zugelassen.

Die Logs werden an den DNS/DHCP Server gesendet und auf dem Server wird der Syslog Viewer installiert, um den Signalisierungsverkehr zu analysieren.



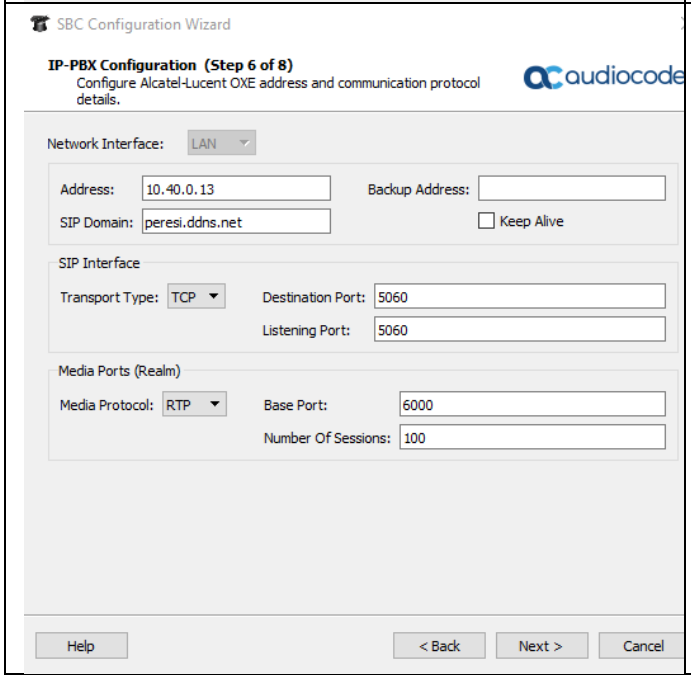
INTERNES INTERFACE (LAN)

Nun kann das interne Interface gemäss Planung konfiguriert werden. Neben den Standard Angaben für die Netzwerkkommunikation, wird noch das OAM Interface konfiguriert. Das OAM Interface sollte immer auf der internen Seite konfiguriert werden, um Zugriffe von Aussen zu vermeiden.



EXTERNES INTERFACE (WAN)

Wie beim LAN wird als nächstes noch das WAN Interface konfiguriert, hier sind die üblichen Netzwerkparameter bereits ausreichend. Die Parameter wurden während der Planung erarbeitet.

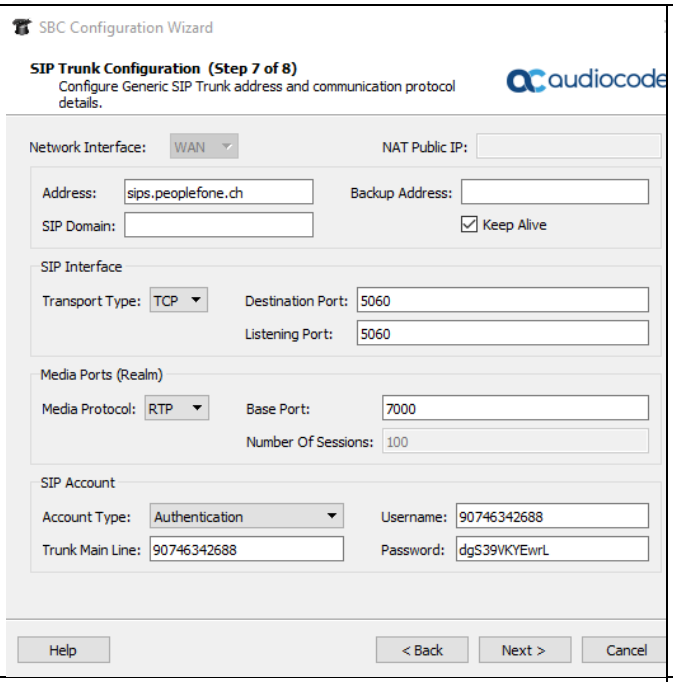


LAN PARAMETER

Unter diesem Konfigurationsschritt werden die Einstellungen für die interne Kommunikation festgelegt.

Um Verluste in der Signalisierung zu vermeiden setze ich auf TCP, den Port lasse ich auf 5060.

Im Media Realm werden die Ports für den RTP Stream angegeben, wobei es sich nur um die Ports handelt, welcher der SBC als eigenen angibt.



WAN / Provider Parameter

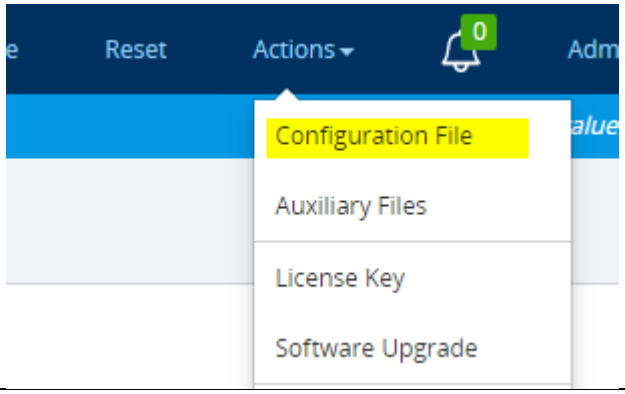
Um die Kommunikation zu Provider herzustellen, werden nun die Parameter dazu angegeben.

Die Adresse „sips.peoplefone.ch“ wird über den eigenen DNS Server aufgelöst und mit dem „Keep Alive“ werden ständig Optionen versendet um die Verbindung aufrecht zu erhalten.

Wie im LAN wird hier für die Signalisierung TCP mit dem Port 5060 verwendet.

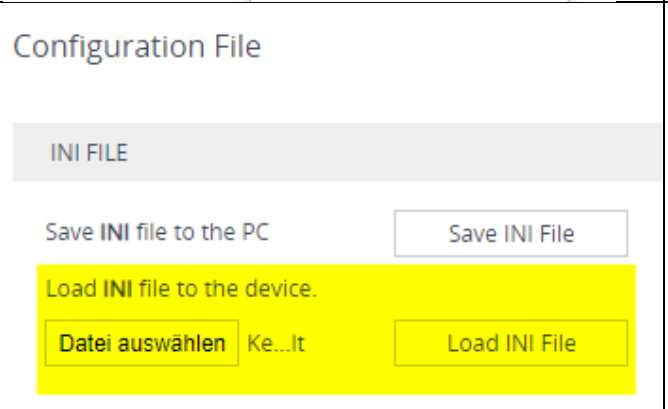
Der Media Realm für RTP muss in einem anderen Bereich liegen als der interne.

Und schlussendlich werden die Anmeldedaten für den SIP Trunk angegeben.



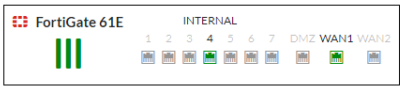
Nun kann über https://10.40.0.10 eine Verbindung auf den SBC hergestellt werden und über „Configuration Files“ gelangt man zur Verwaltung der Konfigurationsdatei.

Da die Konfiguration noch nicht geladen wurde, muss über das CLI und der seriellen Schnittstelle die IP Konfiguration vorgenommen werden.



Schlussendlich wird das Konfigurationsfile hochgeladen und der SBC kann neu gestartet werden.

8.2.3 Firewall



+ Create New ▾ | Edit | Delete

Status	Name	Members	IP/Netmask	Type
Hardware Switch (1)				
	internal	1 2 3 4 5 6 7	10.255.255.254 255.255.255.0	Hardware Switch (7)
Physical (3)				
	dmz		10.10.10.1 255.255.255.0	Physical Interface
	wan1		192.168.0.200 255.255.255.0	Physical Interface
	wan2		0.0.0.0 0.0.0.0	Physical Interface

INTERFACES

Als erstes werden auf der Firewall die Interfaces für LAN und WAN konfiguriert.

LAN: 10.255.255.254/24

WAN: 192.168.0.200/24

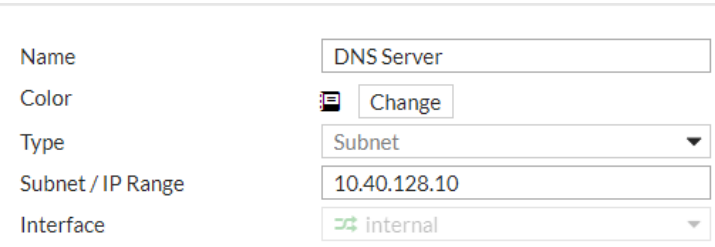
Destination	Interface	
0.0.0.0/0	wan1	192.168.0.1
10.0.0.0/8	internal	10.99.99.10

STATISCHE ROUTEN

Um den Datenverkehr zu gewährleisten müssen die Routen zu den Netzen hinterlegt werden.

0.0.0.0/0 -> WAN

10.0.0.0/8 -> LAN



ERFASSEN DER GERÄTE

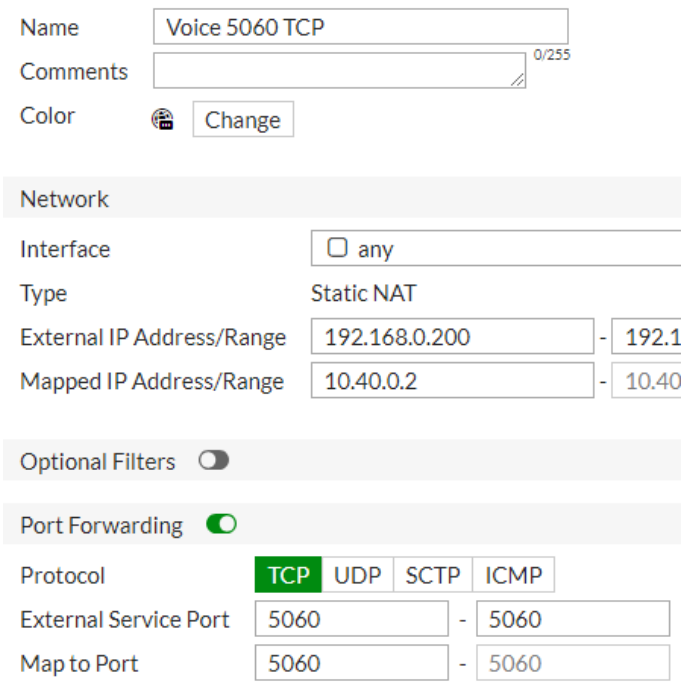
Nun werden alle Geräte erfasst, welche in einer Firewall Regel verwendet werden.

Diese können, wo nötig, auch zusammengefasst werden.

Telefon 1	Subnet	10.10.64.0/24
Telefon 2	Subnet	10.20.64.0/24
Telefon 3	Subnet	10.30.64.0/24

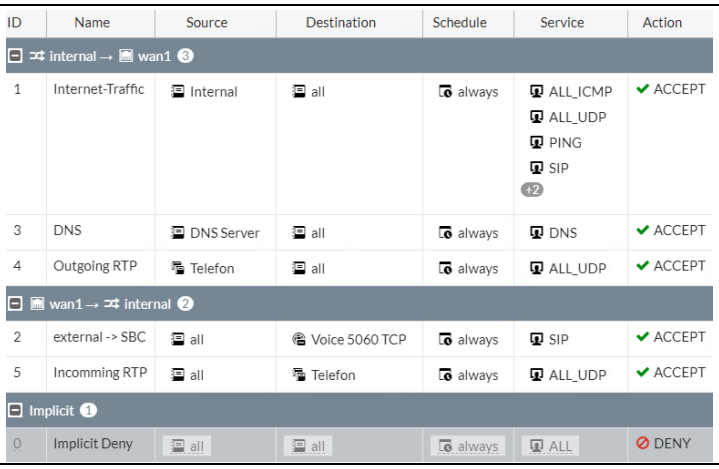
ERFASSEN NETZE

Wie beim Erfassen der Geräte, können auch Regeln für ganze Netze erstellt werden. Ich werde diese zum Beispiel für das Voice Netz anwenden und erstelle hierfür Netzwerk Adressen, die in der Regel verwendet werden.



VIRTUAL IP

Um die eingehende Kommunikation auf den Call Server zu sichern, muss ein Port Forwarding auf der Firewall konfiguriert werden. So wird sichergestellt das jede eingehende Nachricht, welche den Port 5060 anspricht direkt zum Session Border Controller weitergereicht wird.



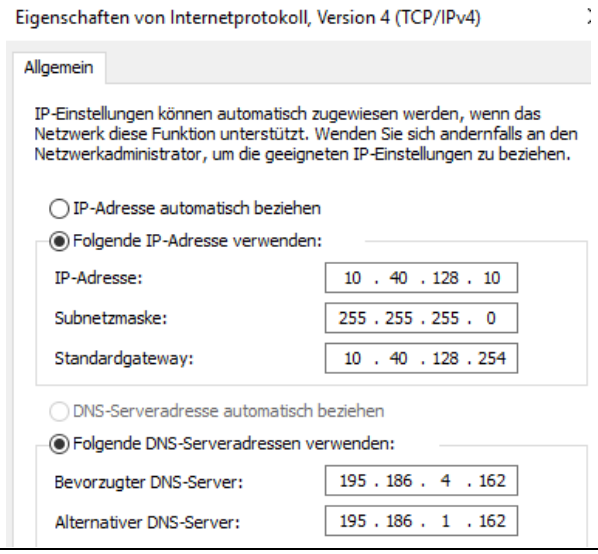
ID	Name	Source	Destination	Schedule	Service	Action
internal → wan1 3						
1	Internet-Traffic	Internal	all	always	ALL_ICMP ALL_UDP PING SIP +2	ACCEPT
3	DNS	DNS Server	all	always	DNS	ACCEPT
4	Outgoing RTP	Telefon	all	always	ALL_UDP	ACCEPT
wan1 → internal 2						
2	external -> SBC	all	Voice 5060 TCP	always	SIP	ACCEPT
5	Incomming RTP	all	Telefon	always	ALL_UDP	ACCEPT
Implicit 1						
0	Implicit Deny	all	all	always	ALL	DENY

FIREWALL REGELN

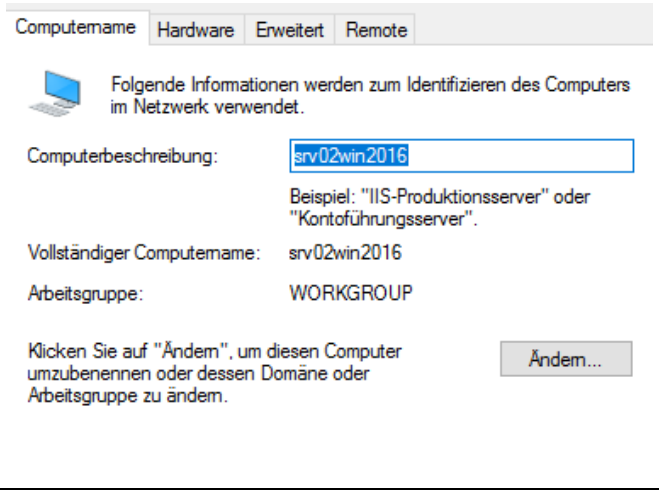
Zum Schluss können die erstellten Adressen, Netze und VIP in die Regeln eingebunden werden. Die Regeln werden so umgesetzt, dass nur die Dienste laufen, die geplant sind.

8.2.4 DHCP / DNS Server

8.2.4.1 Grundkonfiguration Server



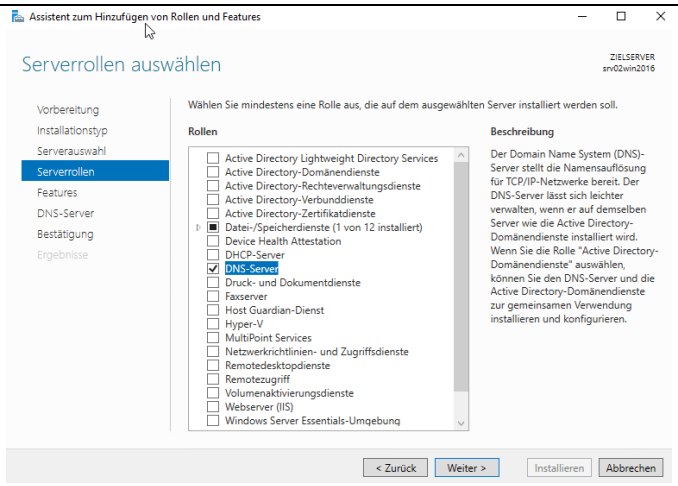
Nachdem der Server aufgesetzt wurde und alle Updates durchgeführt wurden, kann die IP Konfiguration vorgenommen werden.



Ist die Netzwerkkonfiguration fertig, kann man noch den Servernamen vergeben.

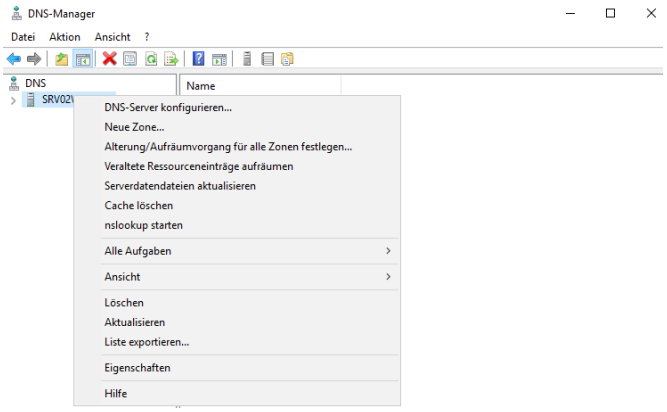
Ich habe mich für den Name **srv02win2016** entschieden, da in meiner Serverumgebung bereits ein Server mit der Nummer eins existiert.

8.2.4.2 DNS Konfiguration

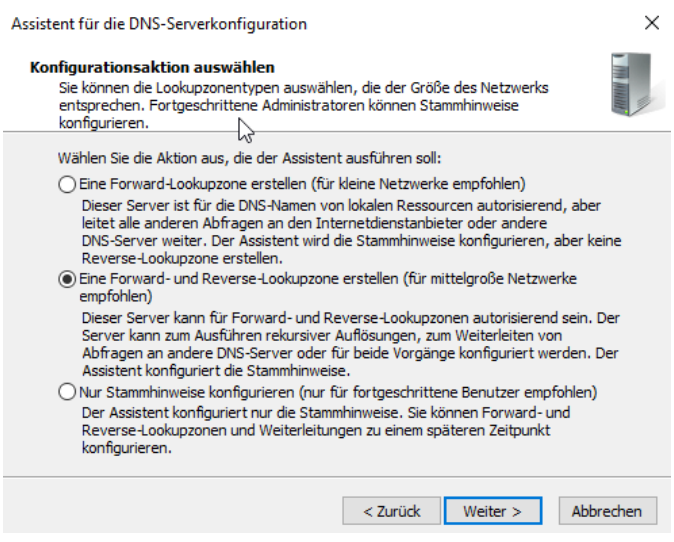


Um mit der DNS Konfiguration zu starten, muss auf dem Server die Serverrolle DNS-Server aktiviert werden.

Das ist bereits der wichtigste Punkt der Vorbereitung, die weiteren Einstellungen werden nach der Installation vorgenommen.



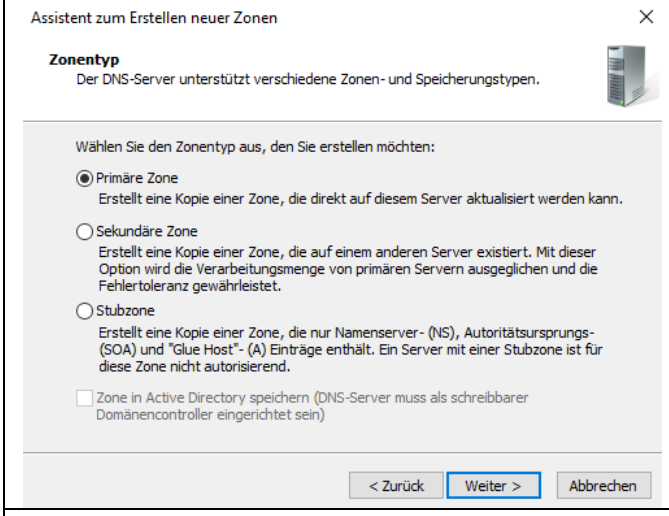
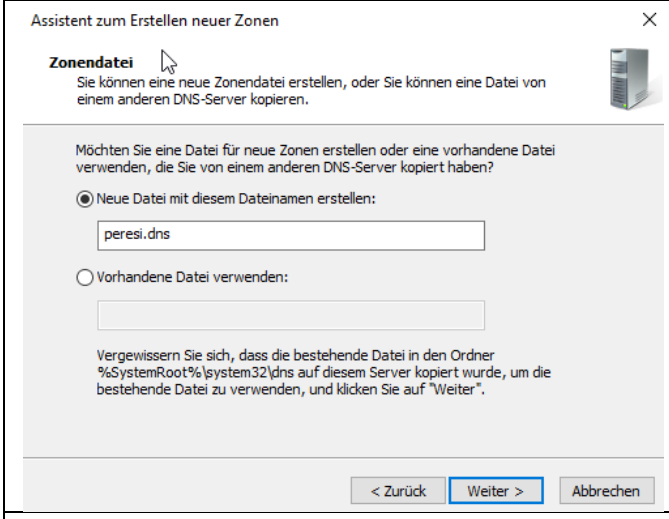
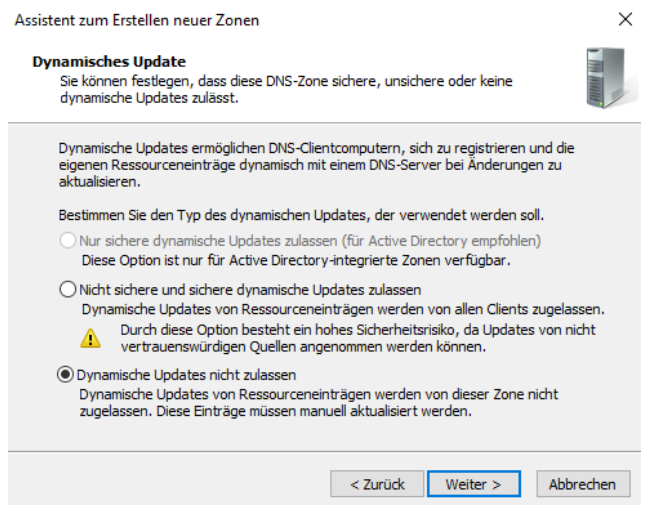
Nun kann unter «Tools» der DNS Manager geöffnet werden. Um mit der Konfiguration zu starten, kann man den Assistenten starten.

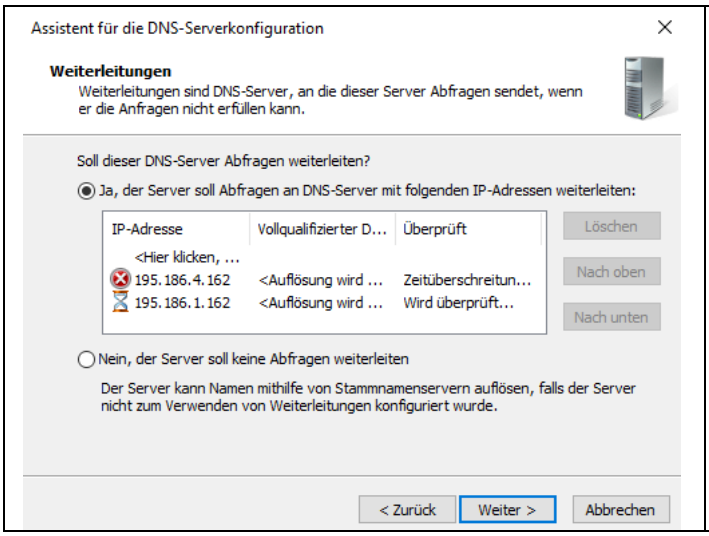


Nun wird die Variante des DNS Servers gewählt, wobei für meine rekursiven DNS, eine Forward und Reverse Lookupzone konfiguriert wird.

Forward Loookupzone: Auflösung von Namen in IP Adressen

Reverse Lookupzone: Auflösung von IP Adressen in Namen

	Im nächsten Schritt geht es an das Erstellen einer primären Zone, mit Speicher auf dem eigenen Server.
	Nun wird die Zonendatei erstellt, welche einen Namen braucht. Zonendateiname: peresi.dns
	Jetzt kann gewählt werden ob dynamisch Updates der Hosts zugelassen wird. Weil es in meiner Umgebung keinen Active Directory Dienst gibt, werde ich das aus Sicherheitsgründen nicht verwenden.

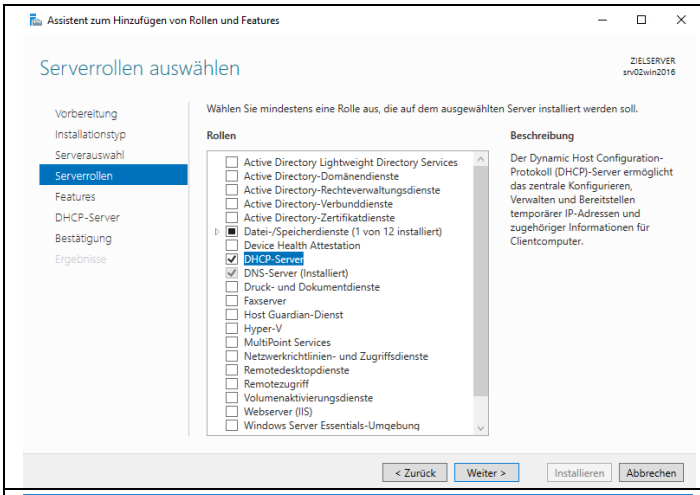


Angabe eines externen DNS Servers zur Auflösung nicht bekannter Namen.

Swisscom primär DNS:
195.186.4.162

Swisscom sekundär DNS:
195.186.1.162

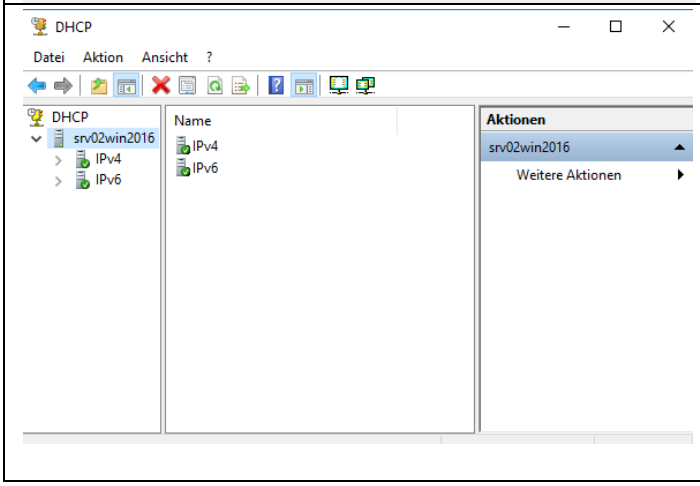
8.2.4.3 Konfiguration des DHCP Servers



SERVERROLLE

Als erstes wird der DHCP Server Dienst konfiguriert. Dieser ist wie der DNS Server unter den Serverrollen zu finden.

Ist die Installation beendet kann, kann der DHCP Manager geöffnet werden.

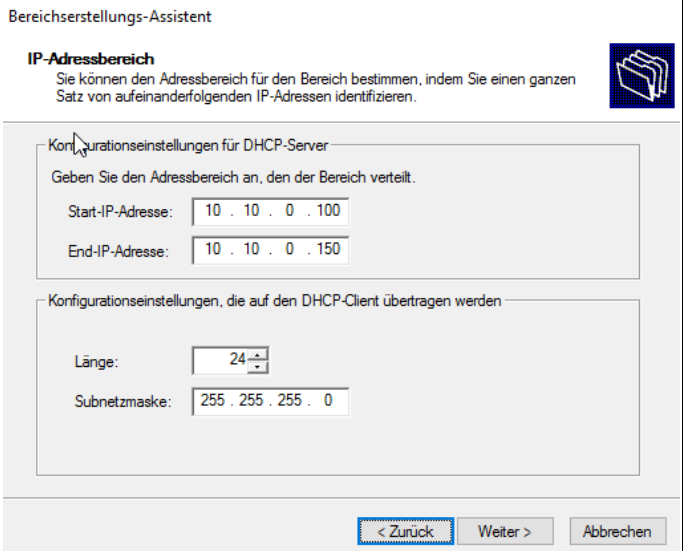


Nun kann der DHCP Manager geöffnet werden um den Server zu konfigurieren.

Ich werde hierfür den IPv4 DHCP Server nutzen.

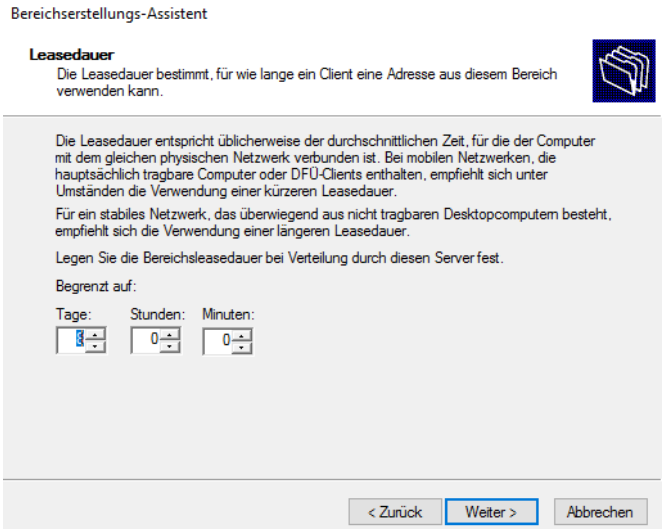
Als erstes wird der DHCP Server Dienst konfiguriert. Dieser ist wie der DNS Server unter den Serverrollen zu finden.

Ist die Installation beendet kann, kann der DHCP Manager geöffnet werden.



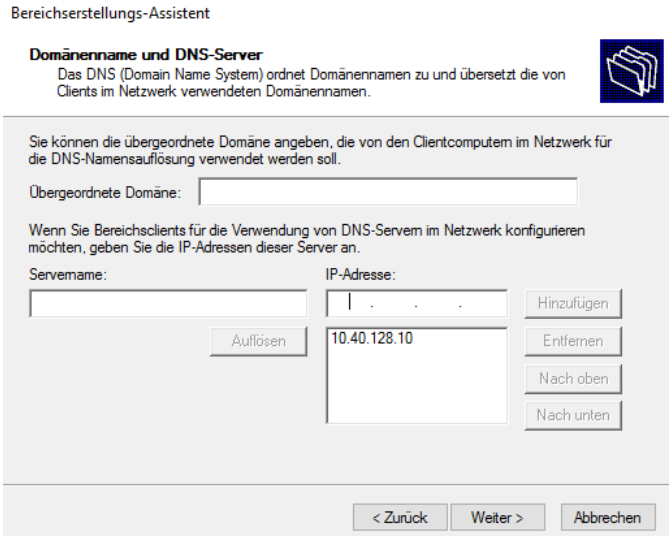
Als nächstes wird für jedes Netz ein Adressbereich angelegt, welcher dem Server zur Weitergabe der Adressen dient.

Zu Testzwecken werde ich jeweils den Hostbereich von 100 -150 verwenden.



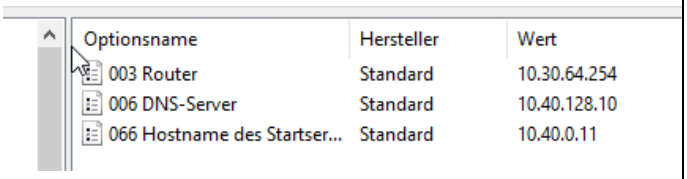
Über die Leasedauer kann den Clients die Dauer der Gültigkeit ihrer IP Adresse mitgegeben werden.

Ich lasse hier den Standard Wert von 8 Tagen stehen, werde diesen für die Tests jedoch noch ändern.



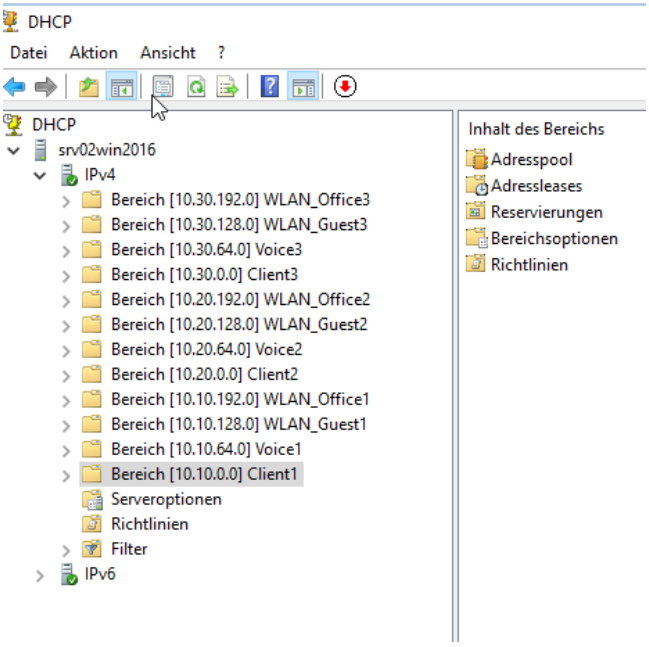
Mit dem DHCP Server können nicht nur IP Adressen verteilt werden, es können auch weitere Informationen an die Clients verteilt werden.

Im Assistenten wird Bereits die Option für DNS Server abgefragt, dieser kann also bereits definiert werden.



Da die Alcatel IP Telefone ihre Konfiguration vom Call Server beziehen müssen diese die Adresse ihres Startservers kennen.

Option 66 für den Startserver



Hier die Übersicht aller konfigurierten DHCP Scopes.

Vergeben wird für jedes Netz der Bereich von:
xxx.xxx.xxx.100 – xxx.xxx.xxx.150

8.2.5 WLAN

Leider wurde der Liefertermin für meinen AP immer weiter nach hinten verschoben und konnte somit nicht mehr termingerecht umgesetzt werden. Jedoch kann die Konfiguration auf der Demo Umgebung umgesetzt werden, das Handling ist dasselbe.

8.2.5.1 Konfiguration SSID

Unter den SSID kann der Schlüssel für die WPA2 Verbindung gesetzt werden, es sind auch andere Varianten möglich. Hinzu kommt noch die Methode der Client IP Vergabe, diese wird ja vom DHCP Server gemacht und muss somit in das 30 oder 40 VLAN gebridged werden. Hierfür werden die VLAN den zugehörigen SSID angehängt und das IP Client assignement auf Local LAN geschaltet.

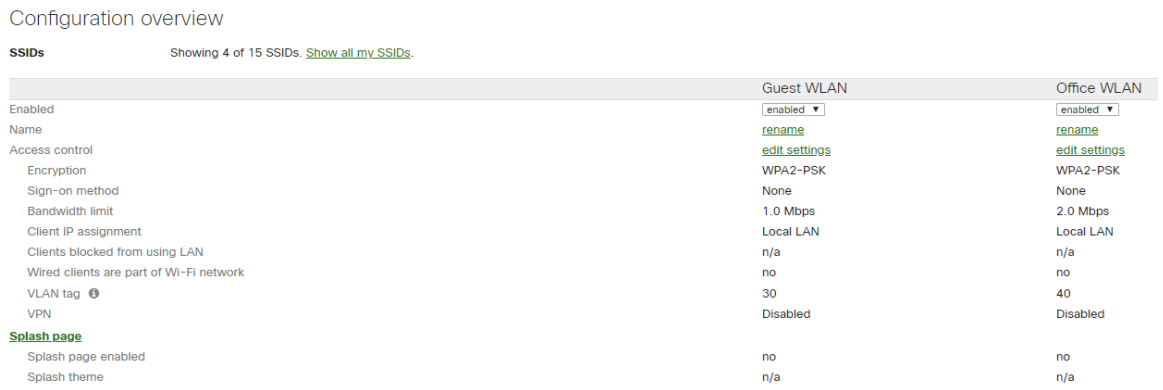


Abbildung 14 SSID

8.2.5.2 Registrierung Access Point

Die Access Points müssen auf dem Kundenportal registriert werden, dazu kann die Seriennummer, welche auf dem Gerät zu finden ist, registriert werden.

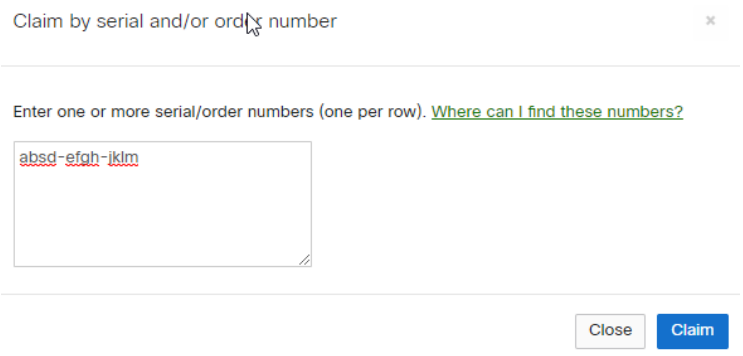


Abbildung 15 AP Registrierung

9 Tests

Um die Funktion der verschiedenen Bauteile zu gewährleisten, folgt ein Funktionstest über alle Teile der Arbeit.

9.1 Testkonzept

9.1.1 Testziele

Das Ziel der Tests ist die Funktionsprüfung des geplanten Projekts und der einzelnen Bausteine. Es ist der letzte Schritt vor der Übernahme des Projekts und prüft ob soll- und ist Zustand übereinstimmen. Die einzelne Testprotokolle dienen der Zustandsprüfung bei der Projektübergabe und versichern die einwandfreie Funktion der einzelnen Bausteine.

9.1.2 Testobjekte

Testobjekte	
Objekt	Beschreibung
Switch VLAN	Es wird die Kommunikation zwischen den VLAN getestet
Routing	Es wird das Routing zwischen den Netzen getestet
Firewall	Die Firewall regeln werden getestet
DHCP Server	Die Vergabe der DHCP Leases wird getestet
DNS Server	Die Namensauflösung auf dem lokalen DNS wird getestet
Call Server	Ein- und Ausgehende Anrufe werden getestet
SBC	Der Funktion und Sicherheitsaspekt des SBC werden getestet

Tabelle 32 Testobjekte

9.1.3 Testarten

Testarten	
Testart	Beschreibung
Funktionstest	Prüfung der Funktion anhand der erwarteten Ergebnisse
Logs	Prüfen der Logfiles

Tabelle 33 Testarten

9.1.4 Testvoraussetzungen

Testvoraussetzungen	
Voraussetzung	Beschreibung
Tester	Um die Tests durchzuführen muss ein Tester zur Verfügung stehen
Vorkenntnisse	Um die Ergebnisse zu analysieren müssen gewissen Kenntnisse erarbeitet werden

Tabelle 34 Testvoraussetzungen

9.1.5 Fehlerklassen

Fehlerklassen	
Klasse	Beschreibung
0	Fehlerfrei
1	Unwesentlicher Mangel
2	Leichter Mangel
3	Schwerer Mangel
4	Kritischer Mangel

Tabelle 35 Fehlerklassen

9.1.6 Testinfrastruktur

Die Testinfrastruktur besteht aus allen in der Realisation erwähnten Bestandteile. Zusätzlich werden Hilfsmittel verwendet, welche in der Testbeschreibung erwähnt werden.

Testinfrastruktur	
Objekt	Beschreibung
VLAN	Switch konfiguriert gemäss Planung und Realisierung
Router	Router konfiguriert gemäss Planung und Realisierung
Firewall	Firewall konfiguriert gemäss Planung und Realisierung
DHCP	DHCP Server konfiguriert gemäss Planung und Realisierung
DNS	DNS konfiguriert gemäss Planung und Realisierung
Call Server	Call Server konfiguriert gemäss Planung und Realisierung
SBC	SBC konfiguriert gemäss Planung und Realisierung
WLAN	nicht verfügbar
Telefon	internes Telefon
Notebook	Notebook für Tests
Mobile	Mobile für externe Anrufe
Syslog Server	Syslog für die Analyse der SIP Signalisierung

Tabelle 36 Testinfrastruktur

9.2 Switch VLAN

Die VLAN Konfiguration kann mittels «show vlan brief»-Befehl angezeigt werden. So ist ersichtlich auf welchen Ports, welches VLAN konfiguriert wurde. Um zu testen ob die VLAN mit einander verbunden sind, kann der Switch vom Router entfernt werden, nun sollte die Kommunikation nur noch zwischen den VLAN möglich sein. Dieser Test kann mit 2 Clients und dem Ping-Befehl durchgeführt werden, es ist jedoch darauf zu achten das beide Clients im selben Netz sind.

```
Switch3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/23, Gi0/1, Gi0/2
12   Client3                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
22   Voice3                           active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22
32   WLAN_Guest3                      active
42   WLAN_Office3                     active
```

Abbildung 16 VLAN Test

Testbeschreibung	
Beschreibung	Switch VLAN Test
Testvoraussetzungen	2 x IP Geräte welche Pingbar sind, Konfigurierter Switch
Testschritte	Konfiguration einer statischen IP auf beiden Testnotebooks Anschluss mittels Kat 5 Ethernet Kabel auf selben VLAN Trennung vom Router Ping zwischen beiden Notebooks im selben VLAN
Erwartetes Ergebnis	Pings wird erfolgreich beantwortet

Tabelle 37 Testbeschreibung VLAN

Testergebnis	
Tester	
Testergebnis	Ping im selben VLAN erfolgreich durchgeführt
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 38 Testergebnis VLAN

9.3 Router

Nun wird getestet ob die Vernetzung der Teilnetze funktioniert. Auch hier wird auf den einfachen PING-Befehl zurückgegriffen. Mit dem Befehl „show ip route“ kann auf dem Router kontrolliert werden auf welchem Gateway das Netz zu finden ist. Die Routen welche mit „S“ gekennzeichnet sind, sind statische Routen, die mit „C“ sind an dem jeweiligen Port angebunden und die mit „L“ sind lokale Gateway Adressen.

```
Router3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.50.0.5 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.50.0.5, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 11 subnets, 4 masks
S        10.10.0.0/16 [1/0] via 10.50.0.5, Serial0/0/0
C        10.30.0.0/24 is directly connected, FastEthernet0/0.12
L        10.30.0.254/32 is directly connected, FastEthernet0/0.12
C        10.30.64.0/24 is directly connected, FastEthernet0/0.22
L        10.30.64.254/32 is directly connected, FastEthernet0/0.22
C        10.30.128.0/24 is directly connected, FastEthernet0/0.32
L        10.30.128.254/32 is directly connected, FastEthernet0/0.32
C        10.30.192.0/24 is directly connected, FastEthernet0/0.42
L        10.30.192.254/32 is directly connected, FastEthernet0/0.42
C        10.50.0.4/30 is directly connected, Serial0/0/0
L        10.50.0.6/32 is directly connected, Serial0/0/0
```

Abbildung 17 Router Test 1

Nun kann mit « tracert » die Route zu einer bestimmten Adresse geprüft werden. Ich prüfe nun mit „tracert google.ch“ die Hops auf dem Weg zu google.ch.

```
C:\Users\SPSO0297>tracert google.ch

Routenverfolgung zu google.ch [172.217.168.35]
über maximal 30 Hops:

  1    <1 ms    <1 ms    <1 ms  10.30.0.254
  2     1 ms     1 ms     1 ms  10.50.0.5
  3     1 ms     1 ms     1 ms  10.255.255.254
  4     3 ms     3 ms     2 ms  192.168.0.1
  5    23 ms    35 ms    12 ms  217-162-240-1.dynamic.hispeed.ch [217.162.240.1]
  6    12 ms    16 ms    16 ms  217-168-63-61.static.cablecom.ch [217.168.63.61]
  7    26 ms    27 ms    25 ms  ch-zrh03a-rc1-ae51-0.aorta.net [84.116.200.237]
  8    11 ms    11 ms    12 ms  ch-zrh01b-ra1-ae1-0.aorta.net [84.116.134.142]
  9    18 ms    11 ms    10 ms  72.14.221.112
 10    18 ms    15 ms    15 ms  74.125.243.129
 11    12 ms    14 ms    15 ms  172.253.50.3
 12    16 ms    12 ms    10 ms  zrh04s14-in-f3.1e100.net [172.217.168.35]

Ablaufverfolgung beendet.
```

Abbildung 18 Router Test 2

Wie man erkennen kann konnte die Route von Netz Client3 bis zu google.ch bestimmt werden wobei die oberen drei Hops in meiner Umgebung sind und der vierte mein Heimrouter ist. Das Routing vom abgelegenen Standort, über den Hauptstandort in das Internet funktioniert somit.

Testbeschreibung	
Beschreibung	Router
Testvoraussetzungen	2 x IP Geräte welche Pingbar sind, Konfigurierter Switch und Router
Testschritte	Konfiguration einer statischen IP auf beiden Testnotebooks Anschluss mittels Kat 5 Ethernet Kabel auf selben VLAN Trennung vom Router Ping zwischen beiden Notebooks im selben VLAN
Erwartetes Ergebnis	Pings wird erfolgreich beantwortet

Tabelle 39 Testbeschreibung Router

Testergebnis	
Tester	
Testergebnis	Ping aus verschiedenen Netzen erfolgreich durchgeführt
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 40 Testergebnis Router

9.4 Firewall

Um die Firewall Regeln zu testen sind die lokalen Logs der Firewall hilfreich, diese können direkt unter den Regeln eingeschaltet werden und werden auf dem eigenen System gespeichert, ein Syslog Server ist für kleinere Umgebung somit nicht nötig.

Als Beispiel für einen Funktionierende Regel nehme ich das Internetprotokoll http und HTTPS. Wie aus der Planung und Realisierung entnommen werden konnte, ist HTTP für das interne Netz nicht zugelassen und HTTPS ist zugelassen. Nun wird mit einem Client im Browser die Seite 20min.ch aufgerufen, jeweils als https://20min.ch und http://20min.ch. Danach können die Logs geprüft werden.

https://20min.ch

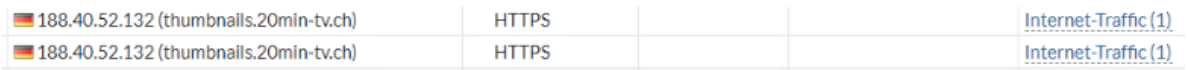


Abbildung 19 Firewall Test 1

http://20min.ch

Abbildung 20 Firewall Test 2

Wie wir feststellen wird die Kommunikation mit HTTP von der Firewall unterbunden und die mit HTTPS wird zugelassen. Somit konnte die Funktion der Firewall sichergestellt werden. Diese Methode konnte auch auf andere Regeln adaptiert werden.

Testbeschreibung	
Beschreibung	Firewall
Testvoraussetzungen	Notebook in Client Netz, Konfigurierte Firewall, Switch, Router und DHCP Server, Anschluss an Internet
Testschritte	Testnotebook mit DHCP Anschluss mittels Kat 5 Ethernet Kabel auf Client VLAN Internet Browser CMD für direkte DNS nach extern (siehe DNS Test) Intervention Logs auf Firewall prüfen
Erwartetes Ergebnis	Firewall blockt unerlaubte Protokolle

Tabelle 41Testbeschreibung Firewall

Testergebnis	
Tester	
Testergebnis	Test mit Client war erfolgreich Es konnte im Log erkannt werden das unerlaubte Protokolle oder Ziele gesperrt werden.
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 42 Testergebnis Firewall

9.5 DHCP Test

Die Funktion des DHCP-Servers, kann ganz einfach mittels DHCP-Clients und der Einsicht in die Lease vergabe des DHCP Mangers gemacht werden. In meinem Beispiel verwende ich ein Alcatel IP Touch 8068 welches auf DHCP geschalten ist. Ich verwende dieses Gerät, da es die komplexeste DHCP Konfiguration erfordert. Zum Schluss muss das Telefon mittels DHCP Informationen selbstständig seine Konfigurationsdatei vom Call Server beziehen.

Einstecken des Telefons in Netz Voice1:

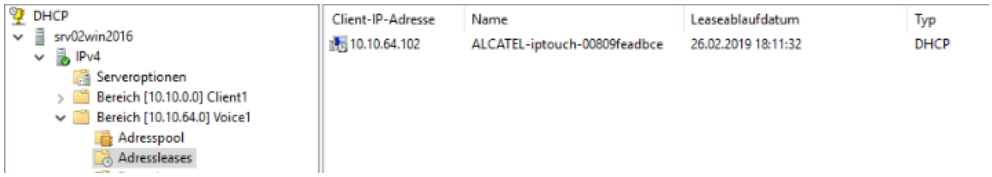


Abbildung 21 DHCP Test 1

Einstecken des Telefons in Netz Voice3:

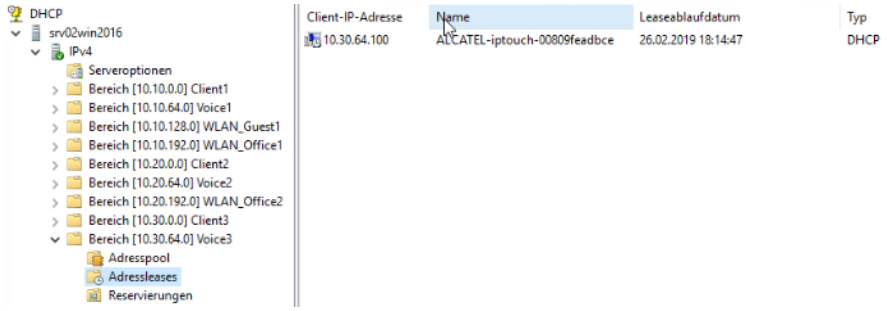


Abbildung 22 DHCP Test 2

Einstecken eines Clients im Netz Client3 mit ipconfig /all:

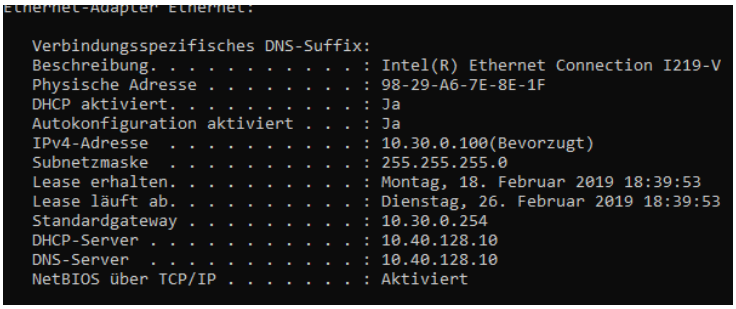


Abbildung 23 DHCP Test 3

Wie man erkennen kann, hat das Telefon in jedem Netz einen neuen Lease erhalten und konnte mit den erhaltenen Daten seine Konfiguration beim Call Server beziehen. Ebenfalls konnte geprüft werden welche Optionen dem PC übergeben wurden.

Testbeschreibung	
Beschreibung	DHCP Server
Testvoraussetzungen	Notebook, Telefon, Konfigurierter Switch, Router und DHCP Server
Testschritte	Telefon und Notebook mit DHCP Einstellen Anschluss mittels Kat 5 Ethernet Kabel an vorgesehenes VLAN Prüfen des bezogenen DHCP Leases DHCP-Manager auf Server prüfen Bezug des Konfiguration Files für Telefon prüfen
Erwartetes Ergebnis	Lease mit allen Optionen werden von den DHCP Relay Agents an Clients vergeben.

Tabelle 43 Testbeschreibung DHCP

Testergebnis	
Tester	
Testergebnis	DHCP Lease und Optionen wurden erfolgreich in alle vorgesehenen Netze vergeben.
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 44 Testergebnis DHCP

9.6 DNS Test

Der DNS Server kann mittels Syntax «nslookup domain» geprüft werden. Die Syntax kann am Ende noch die Adresse eines DNS Servers erweitert werden. Dies dient dazu, einen bestimmten DNS Server anzusprechen und kann gleich dafür genutzt werden um die Einstellung der Firewall nochmals zu prüfen.

nslookup google.ch

```
C:\Users\SPSO0297>nslookup google.ch
Server:  UnKnown
Address:  10.40.128.10

Nicht autorisierende Antwort:
Name:    google.ch
Addresses:  2a00:1450:400a:802::2003
          172.217.168.35
```

Abbildung 24 DNS Test 1

Gibt man den Befehl ohne weitere Adresse an, wird die bekannte Adresse aus der DHCP Option verwendet. Diese lautet 10.40.128.10 und konnte google.ch in 172.217.168.35 auflösen.

nslookup google.ch 8.8.8.8

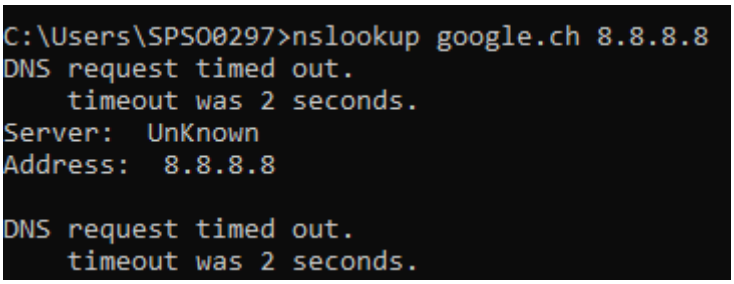


Abbildung 25 DNS Test 2

Hier wird nun versucht direkt auf dem Google DNS Server, mit der Adresse 8.8.8.8, die Adresse google.ch aufzulösen. Wie aus der Abbildung ersichtlich ist, konnte das nicht durchgeführt werden, Grund dafür ist das die Firewall nur DNS Anfragen nach aussen zulässt welche vom DNS Server kommen.

Die Funktion des DNS Servers konnte mit diesen Schritten belegt werden.

Testbeschreibung	
Beschreibung	DNS Server
Testvoraussetzungen	Notebook, Konfigurierter Switch, Router und DNS/DHCP Server
Testschritte	Notebook mit DHCP einstellen Anschluss mittels Kat 5 Ethernet Kabel an Client VLAN Internet Browser für Domänen Auflösung CMD für nslookup abfragen an unerwünschte Server
Erwartetes Ergebnis	Namen werden in IP Adressen aufgelöst, jedoch nur über internen DNS

Tabelle 45 Testbeschreibung DNS

Testergebnis	
Tester	
Testergebnis	Die Namensauflösung funktioniert, jedoch wie erwünscht nur über internen DNS
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 46 Testergebnis DNS

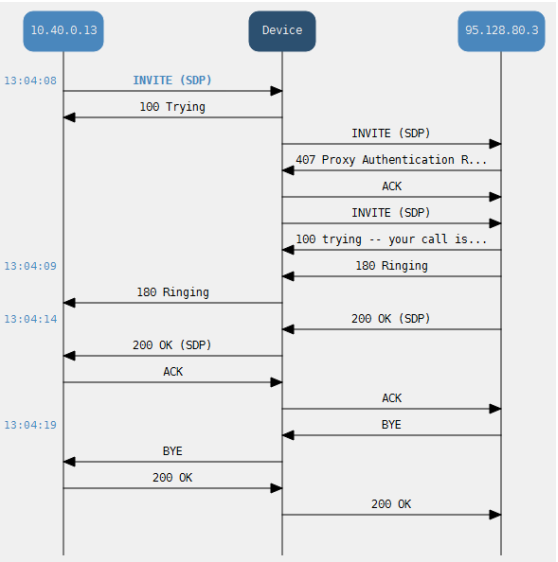
9.7 Telefonie Test

9.7.1 Ein-/Ausgehender Anruf

Um die ein- und ausgehenden Anrufe zu prüfen, hilft mir der eingerichtete Syslog Viewer. Hiermit kann die ganze SIP Signalisierung zwischen Call Server und SBC, sowie SBC und Provider überprüft werden. Der RTP Stream wird nicht angezeigt, da für die Performance „direct RTP“ aktiviert wurde. Nach dem zweiten ACK zwischen SBC (Device) und 95.128.80.3 (Provider) findet das Gespräch in Form von RTP Stream statt.

Die Verhandlung der Medien findet mit dem Session Description Protokoll (SDP) statt, hier werden Codec, Media Port und Art der Kommunikation ausgehandelt.

Ausgehend:



Eingehend:

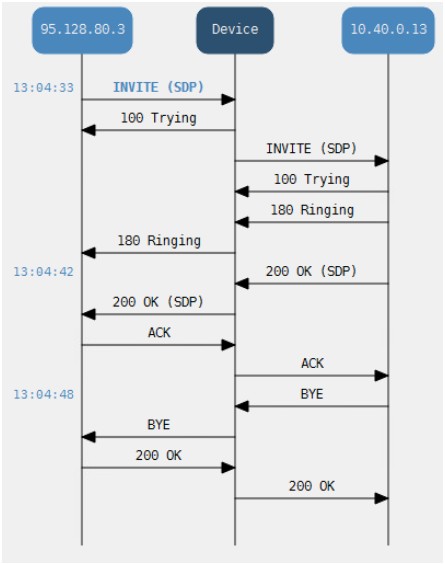


Abbildung 26 Telefonie Test 1

Abbildung 27 Telefonie Test 2

Testbeschreibung	
Beschreibung	Router
Testvoraussetzungen	VoIP Telefon, Mobile, Konfigurierter Call Server, Netzwerkinfrastruktur, DHCP und DNS Server Syslog Server und SBC mit Amtsanschluss
Testschritte	VoIP Telefon mit DHCP konfigurieren Anschluss mittels Kat 5 Ethernet Kabel an Voice VLAN Telefonate durchführen (ausgehend/ eingehend) Prüfen der Logfiles
Erwartetes Ergebnis	Anrufe können getätigt werden

Tabelle 47 Testbeschreibung Telefonie

Testergebnis	
Tester	
Testergebnis	Anrufen konnten ein- wie ausgehend erfolgreich auf- und abgebaut werden.
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 48 Testergebnis Telefonie

9.7.3 SBC

9.7.3.1 Authentifizierung mit Provider

Auf dem Kundenportal kann nachgeschaut werden, ob der SIP Trunk registriert wurde.

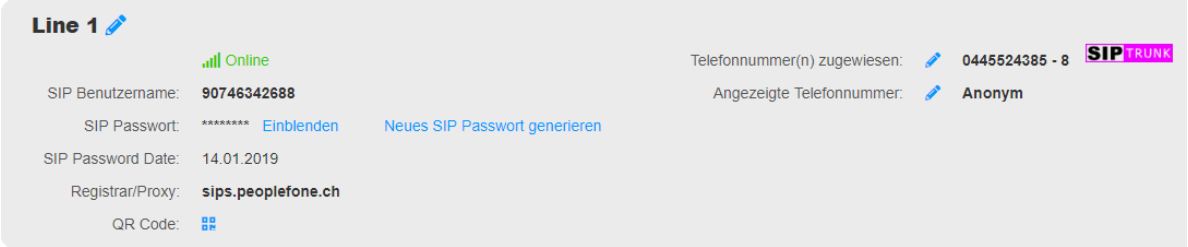


Abbildung 28 Trunk Test

Der genaue Verkehr für die Registrierung, kann aus den Logs entnommen werden. Mit dem ersten Register geben wir dem Provider an das wir uns Registrieren wollen, wobei dieser mit einem „401 Unauthorized“ antwortet. Diese Nachricht beinhaltet den WWW-Authentifizierungsheader und fordert somit die Authorisierungsdaten an, welche mit dem nächsten Register mitgesendet werden. Darauf werden diese vom Provider geprüft und bei Stimmigkeit folgt das 200 OK und der SIP Trunk ist angemeldet.

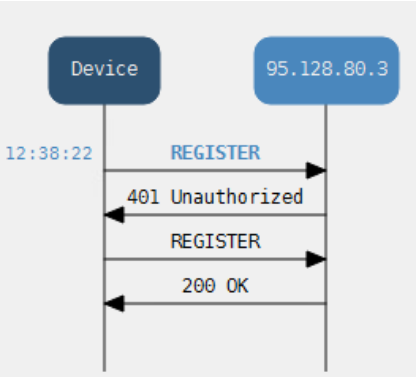


Abbildung 29 Test Authentifizierung

9.7.3.2 SIP Manipulation durch SBC

INVITE CS -> SBC

```
20:17:04.519  ---- Incoming SIP Message from 10.40.0.13:5060 to SIPInterface #1 (sipInterface1) TCP TO(#

INVITE sip:+4141798269288@10.40.0.10;user=phone SIP/2.0
Route: <sip:10.40.0.10;lr;transport=TCP>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, NOTIFY, SUBSCRIBE, OPTIONS, UPDATE, INFO
Supported: timer,path,100rel
User-Agent: OmniPCX Enterprise R12.2 m3.402.24.a
Session-Expires: 1800;refresher=uac
Min-SE: 900
P-Asserted-Identity: "Test 1" <sip:+41445524385@10.40.0.13;user=phone>
Content-Type: application/sdp
To: <sip:+4141798269288@10.40.0.10;user=phone>
From: "Test 1" <sip:+41445524385@10.40.0.13;user=phone>;tag=5cf5a981f2ee36d56add1e2de076235d
Contact: <sip:+41445524385@10.40.0.13;transport=TCP>
Call-ID: 187d366d0ca9649f755da36f9c621746@10.40.0.13
CSeq: 1146312163 INVITE
Via: SIP/2.0/TCP 10.40.0.13;branch=z9hG4bK9b2383f863f8e1ef2f96fb72cfb44f98
Max-Forwards: 70
Content-Length: 288

v=0
o=OXE 1550085436 1550085436 IN IP4 10.40.0.13
s=abs
c=IN IP4 10.10.64.102
t=0 0
m=audio 32514 RTP/AVP 8 18 101
a=sendrecv
a=rtpmap:8 PCMA/8000
a=ptime:20
a=maxptime:30
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=ptime:20
a=maxptime:40
a=rtpmap:101 telephone-event/8000
```

Abbildung 30 SBC Test

INVITE SBC -> Provider

```
20:17:04.535  ---- Outgoing SIP Message to 95.128.80.3:5060 from SIPInterface #2 (sipInte

INVITE sip:+4141798269288@SIP;user=phone SIP/2.0
Via: SIP/2.0/TCP 192.168.0.200:5060;alias;branch=z9hG4bKac1486741166
Max-Forwards: 69
From: "Test 1" <sip:+41445524385@OXE;user=phone>;tag=1c695283196
To: <sip:+4141798269288@SIP;user=phone>
Call-ID: 9443754413220192017 3@192.168.0.200
CSeq: 1 INVITE
Contact: <sip:90746342688@192.168.0.200:5060;transport=tcp>
Supported: 100rel,timer,path,sdp-anat
Allow: INVITE, ACK, CANCEL, BYE, PRACK, NOTIFY, SUBSCRIBE, OPTIONS, UPDATE, INFO
Session-Expires: 1800;refresher=uac
Min-SE: 900
User-Agent: Mediant SW/v.7.20A.204.362
P-Asserted-Identity: "Test 1" <sip:+41445524385@OXE;user=phone>
Content-Type: application/sdp
Content-Length: 215

v=0
o=OXE 2041755901 35969238 IN IP4 192.168.0.200
s=abs
c=IN IP4 192.168.0.200
t=0 0
m=audio 7380 RTP/AVP 8 101
a=sendrecv
a=rtpmap:8 PCMA/8000
a=ptime:20
a=maxptime:40
a=rtpmap:101 telephone-event/8000
```

Abbildung 31 SBC Test

Um die Manipulationen des SBC zu prüfen, wurde ein INVITE vor und nach dem SBC aufgezeichnet und gegenübergestellt. Wie man sieht wird durch das Topology Hiding alles entfernt was auf das interne Netz dautet und mit der öffentlichen Adresse 192.168.0.200 ersetzt. Ebenfalls ist ersichtlich das die angebotenen Codecs nur noch auf G711 A-Law reduziert wurden. Somit konnte der Sicherheitsaspekt eines SBC belegt werden.

Testbeschreibung	
Beschreibung	SBC
Testvoraussetzungen	VoIP Telefon, Mobile, Konfigurierter Call Server, Netzwerkinfrastruktur, DHCP und DNS Server Syslog Server und SBC mit Amtsanschluss
Testschritte	Prüfen der Authentifizierung auf Provider Homepage Prüfen der Authentifizierung mittels Logfiles Vergleichen der SIP Manipulation vor und nach SBC
Erwartetes Ergebnis	Authentifizierung funktioniert und SIP Signalisierung wird angepasst

Tabelle 49 Testbeschreibung SBC

Testergebnis	
Tester	
Testergebnis	Authentifizierung hat erfolgreich funktioniert SIP Manipulation konnte anhand der Logs belegt werden
Fehlerbeschreibung	keine Fehler
Fehlerklasse	0

Tabelle 50 Testergebnis SBC

9.8 Testfazit

Testfazit	
Objekt	Ergebnis
VLAN	erfolgreich
Router	erfolgreich
Firewall	erfolgreich
DHCP	erfolgreich
DNS	erfolgreich
Call Server	erfolgreich
SBC	erfolgreich
WLAN	nicht testbar

Tabelle 51 Testfazit

Alle mir möglichen Test konnten erfolgreich durchgeführt werden und die Funktion der Bauteile technisch belegt werden.

10 Abschlussbericht

10.2 Betreuersitzungen

10..1 Protokoll „Erste Betreuersitzung“

Höhere Fachschule Uster ***HFU***

Protokoll Betreuungssitzung Nr: ☒ 1 / ☐ 2 / ☐ 3 / ☐ 4

Art der Arbeit	O Vordiplomarbeit O Diplomarbeit O Abschlussarbeit NDS
Student	Perez Simon
Betreuer	Kubli Ruedi
Thema	Netzwerk / Telefonie Infrastruktur für Unternehmen mit 3 Standorten
Ort, Datum, Zeit	Dietikon, 18.12.2018, 16.15

Arbeitsstand	Grobe Zeitplanung und Pflichtenheft vorhanden. Architektur der Lösung ist definiert, Geräte sind grösstenteils beschafft / vorhanden.
Probleme, Fragen	
Weiteres Vorgehen	Zeitplanung finalisieren, Pflichtenheft noch ergänzen, WLAN Komponenten beschaffen. Dokumentenstruktur erstellen, min. Inhaltsverzeichnis.
Beschlüsse	
Nächster Termin	3. Januar, 16.00

Der Betreuer gibt dem Studenten jeweils eine Kopie. Er sammelt die ausgefüllten Protokolle und bewahrt sie auf bis 1 Monat nach der Präsentation (Ablauf Rekursfrist).

Unterschrift Betreuer

Unterschrift Student

Freigabe: Schulleitung HFU / 05.11.2018 H40405-10 1 von 1
C:\Users\kun\Dropbox\Eigene Dokumente\HFU\DA-2019\16T_Perez_Simon\Protokoll_Betreuungssitzung_Simon_Perez_18122018.doc

Abbildung 32 Sitzungsprotokoll 1

10.1.2 Protokoll „Zweite Betreuersitzung“

Höhere Fachschule Uster HFU

Protokoll Betreuungssitzung Nr: ☐ 1 / ☒ 2 / ☐ 3 / ☐ 4

Art der Arbeit	O Vordiplomarbeit ☒ Diplomarbeit O Abschlussarbeit NDS
Student	Perez Simon
Betreuer	Kubli Ruedi
Thema	Netzwerk / Telefonie Infrastruktur für Unternehmen mit 3 Standorten
Ort, Datum, Zeit	Wallisellen, 04.01.2019, 14:30

Arbeitsstand	Dokumentenstruktur erstellt, Zeitplanung in Bearbeitung, Pflichtenheft tabellarisch erstellt, Evaluation WLAN Komponenten und Server Umgebung für Netzwerk-Dienste. Remote-Zugriff mit OpenVPN eingerichtet, für Zugriff auf ESXi.
Probleme, Fragen	keine
Weiteres Vorgehen	Dokument weiterbearbeiten. Bearbeitung Detailstudie und Abschluss Evaluation (Hauptstudie). Netzwerkplanung (Routing / Switching), WLAN Evaluation (Guest und Company), Installation PBX
Beschlüsse	
Nächster Termin	Februar, nach Absprache

Der Betreuer gibt dem Studenten jeweils eine Kopie. Er sammelt die ausgefüllten Protokolle und bewahrt sie auf bis 1 Monat nach der Präsentation (Ablauf Rekursfrist).

Unterschrift Betreuer

Unterschrift Student

Freigabe: Schulleitung HFU / 05.11.2018 H40405-10 1 von 1
C:\Users\kur\Dropbox\Eigene Dokumente\HFU\DA-2019\16T_Perez_Simon\Protokoll_Betreuungssitzung_Simon_Perez_04012019.doc

Abbildung 33 Sitzungsprotokoll 2

10.1.3 Protokoll „Dritte Betreuersitzung“

Höhere Fachschule Uster **HFU**

Protokoll Betreuungssitzung Nr: ☐1 / ☐2 / ☒3 / ☐4

Art der Arbeit	O Vordiplomarbeit ☒ Diplomarbeit O Abschlussarbeit NDS
Student	Perez Simon
Betreuer	Kubli Ruedi
Thema	Netzwerk / Telefonie Infrastruktur für Unternehmen mit 3 Standorten
Ort, Datum, Zeit	Zürich, 31.01.2019, 18:00

Arbeitsstand	Dokumentenstruktur erstellt, Zeitplanung erstellt, Pflichtenheft ausgeschrieben, Evaluation WLAN Komponenten und Server Umgebung für Netzwerk-Dienste erfolgt. Realisierung erfolgt.
Probleme, Fragen	SIP Trunk Anbindung zu peoplefone, Liefertermine Meraki WLAN
Weiteres Vorgehen	Probleme beheben, WLAN, Test, Dokumentation fertigstellen
Beschlüsse	
Nächster Termin	nach Absprache

Der Betreuer gibt dem Studenten jeweils eine Kopie. Er sammelt die ausgefüllten Protokolle und bewahrt sie auf bis 1 Monat nach der Präsentation (Ablauf Rekursfrist).

Unterschrift Betreuer

Unterschrift Student

Freigabe: Schulleitung HFU / 05.11.2018 H40405-10 1 von 1
C:\Users\kun\Dropbox\Eigene Dokumente\HFU\DA-2019\16T_Perez_Simon\Protokoll_Betreuungssitzung_Simon_Perez_31012019.doc

Abbildung 34 Sitzungsprotokoll 3

10.1.4 Protokoll „Vierte Betreuersitzung“

Höhere Fachschule Uster **HFU**

Protokoll Betreuungssitzung Nr: ☐1 / ☐2 / ☐3 / ☒4

Art der Arbeit	O Vordiplomarbeit ☒ Diplomarbeit O Abschlussarbeit NDS
Student	Perez Simon
Betreuer	Kubli Ruedi
Thema	Netzwerk / Telefonie Infrastruktur für Unternehmen mit 3 Standorten
Ort, Datum, Zeit	Dietikon, 26.02.2019

Arbeitsstand	Dokument enthält wesentliche Punkte. Im Kapitel Test fehlen entsprechende Informationen zu Testszenarien, Testumfeld, durchgeführte Tests und deren Resultate.
Probleme, Fragen	WLAN Accesspoint konnte nicht rechtzeitig angeliefert werden. Realisation kann nicht umgesetzt werden.
Weiteres Vorgehen	Das Kapitel der Tests entsprechend überarbeiten.
Beschlüsse	
Nächster Termin	nach Absprache

Der Betreuer gibt dem Studenten jeweils eine Kopie. Er sammelt die ausgefüllten Protokolle und bewahrt sie auf bis 1 Monat nach der Präsentation (Ablauf Rekursfrist).

Unterschrift Betreuer Unterschrift Student

Freigabe: Schulleitung HFU / 05.11.2018 H40405-10 1 von 1
C:\Users\kur\Dropbox\Eigene Dokumente\HFU\DA-2019\16T_Perez_Simon\Protokoll_Betreuungssitzung_Simon_Perez_26022019.doc

Abbildung 35 Sitzungsprotokoll 4

10.2 Zielerreichung

10.2.1 Zielerreichung „Muss“-Kriterien

Zielerreichung Muss-Ziele			
Tätigkeit	ok	nok	Bemerkung
Netzwerkkonzept erstellen	x		
Sicherheitskonzept erstellen	x		
Telefonie Konzept erstellen	x		
WLAN-Konzept erstellen	x		
Server für Dienste aufsetzen	x		
DHCP Server konfigurieren	x		
DNS konfigurieren	x		
Router konfigurieren	x		
Switch konfigurieren	x		
WLAN-Konfiguration		x	Konnte durch Lieferverzug nur auf Demo umgesetzt werden. Test nicht möglich
Anbindung an Heimnetz / Internet	x		
NAT-Konfiguration	x		
PBX aufsetzen und konfigurieren	x		
Telefone konfigurieren	x		
SIP Trunk anbinden	x		
Firewall konfigurieren	x		

Tabelle 52 Zielerreichung Muss-Kriterien

10.2.2 Zielerreichung „Wunsch“-Kriterien

Zielerreichung Wunsch-Ziele			
Tätigkeit	ok	nok	Bemerkung
TFTP/ConfigFile Server		x	Keine übrigen Ressourcen
SBC	x		
ACL konfigurieren	x		
VPN einrichten		x	Nur für Demo an Präsentation, kein User VPN
Monitoring		x	Keine übrigen Ressourcen
Syslog	x		

Tabelle 53 Zielerreichung Wunsch-Kriterien

10.2.3 Fazit zur Zielerreichung

Es konnten alle mir möglichen Muss-Kriterien umgesetzt werden und erfolgreich getestet werden, ebenfalls konnten zusätzliche noch einige Wunsch-Kriterien umgesetzt werden. Insgesamt bin ich mit dem Erreichen der Ziele zufrieden.

10.3 Zeitaufwand Soll/Ist

10.3.1 Aufgliederung Soll/Ist Stunden

Aufwand Projektphasen im Detail			
Phase	Arbeitspaket	Schätzung (h)	Geleistet (h)
Vorstudie	Aufwandschätzung, Terminplanung	5	8
	Einarbeitung, Einführung	15	15
	Pflichtenheft	20	20
Hauptstudie	Evaluation HW, Planung	20	15
	Evaluation SW, Planung	20	20
Detailstudie	Auswahl HW, Detailplanung	30	30
	Auswahl SW, Detailplanung	30	35
Realisierung	HW Umgebung	20	20
	SW Installation	30	40
	Tests	10	15
Abschluss	Doku	60	80
	Rückblick / Ausblick	5	5
	Präsentation	5	2
		Total 270 h	305 h

Tabelle 54 Aufwand SOLL/IST

10.3.2 Fazit zum Soll / Ist Aufwand

Im Großen und Ganzen bin ich mit der Planung ziemlich genau an den Soll-Stunden, einzig das Erstellen der Dokumentation hat viel mehr Zeit beansprucht als erwartet. Dies liegt vor allem daran, dass ich noch keine Dokumentation mit diesem Umfang erstellt habe und die Schätzung daher schwer zu berechnen ist.

10.4 Rückblick / Ausblick

10.4.1 Hürden

10.4.1.1 WLAN

Leider gab es immer wieder Verspätungen mit der Lieferung meines Access Points, wobei ich die Lizenz bereits bekommen habe. Also habe ich mich im Internet nach gebrauchten Sendern umgeschaut und bin fündig geworden, jedoch stellte sich heraus das die gebrauchten Geräte nicht aus der alten Organisation entfernt wurden und somit nicht in meiner Organisation registriert werden konnten. Dazu kam noch die Meldung von Cisco das sie diese nur vom Eigentümer aus der Organisation entfernen können. Der Verkäufer hatte auch noch eine Ausrede, dass der alte Administrator nicht mehr bei ihnen arbeitet. Schlussendlich kam der Endtermin immer näher und die WLAN Infrastruktur konnte nicht wunschgemäss umgesetzt werden.

10.4.1.2 Telefonie

Ebenfalls hatte ich grosse Probleme mit der Installation des Call Servers, dies vor allem, weil ich den vSphere in der Version 6.7 verwende und das Tool zum ausrollen neuer Call Server noch nicht darauf abgestimmt ist. Ich musste auf den älteren PC Installer zurückgreifen und konnte nicht das Software Orchestration Tool nutzen. Dazu kommt noch das die Konfiguration des Call Servers sehr komplex ist und sehr viel Parameter stimmen müssen bis der erst Anruf endlich funktioniert hat.

10.4.1.3 Routing

Bei Routing hatte ich vor allem Schwierigkeiten bei dem statischen Routen im inter-VLAN Routing. Leider wurde in keiner Dokumentation oder Anleitung angegeben das man den VLAN eine IP vergeben muss welche als next-hop in der Route angegeben wird. Schlussendlich bin ich per Zufall darauf gestossen und das Routing hat funktioniert.

10.4.2 Verbesserungspotential

10.4.2.1 Netzwerk

Das grösste Verbesserungspotential birgt bestimmt die Lösung mit dem Router-on-a-Stick, durch die vielen Netze über ein 100 Mbit/s Port ist die Bandbreit doch ziemlich klein. Da dies jedoch keine Produktive Umgebung ist kann dies zu Übungszwecken so konfiguriert werden. Dies könnte zum Bespiel mit Link Aggregation etwas erweitert werden oder mit Gbit/S Ports.

10.4.2.2 Projekt Management

Das Projekt Management ist mir auch schwergefallen, da ich eher eine Affinität für die Technik habe und mich nicht gerne mit Projektleitungsaufgaben auseinandersetzte. Ich hoffe jedoch, dass ich dies im Rahmen dieser Arbeit zufriedenstellend umsetzten konnte.

10.4.3 Fazit

Die grössten Schwierigkeiten hatte ich bei der Umsetzung der Telefonie. Diese hat mich jedoch nicht aus dem Zeitplan geworfen.

Um die Arbeit zu schreiben hatte ich teilweise Mühe, da diese doch mehr Zeit in Anspruch genommen hat als ich kalkuliert habe.

Insgesamt konnte ich jedoch vieles dazulernen und mein Wissen in Planung und im technischen Bereich erweitern.

Zusätzlich konnte ich noch folgende Zertifizierungen machen:

CCENT Cisco Certified Entry Network Technician

ACA Audiocodes Certified Associate

ACFE Alcatel Certified Field Engineer

10.5.4 Ausblick

Mit der Umsetzung der Arbeit kommen auch immer Ideen, wie die Infrastruktur erweitert werden kann. Für den produktiven Betrieb währe vor allem eine Redundanz im Netzwerk und die Erstellung eines HA Cluster der ESXi Umgebung ein wichtiges Thema.

Für mich persönlich konnte ich vieles im Zusammenhang mit Virtualisierung und Netzwerktechnik lernen und werde mich beruflich auch mehr versuchen in diese Richtung zu orientieren.

11 Verzeichnisse und Glossar

11.1 Tabellenverzeichnis

11.2 Abbildungsverzeichnis

11.3 Glossar

A

ACK ..... *Acknwledge*
ACL ..... *Access Control List*
ARS ..... *Automatic Route Selection*

B

BYOD ..... *Bring your own Device*

C

CLI ..... *Command Line Interface*
CPU ..... *Central Processing Unit*

D

DCE ..... *Data Communication Equipment*
DHCP ..... *Dynamic Host Configuration Protocol*
DTE ..... *Data Terminal Equipment*
DynDNS ..... *Dynamic Domain Name Server*

E

ESX ..... *ESX Virtualisierungssoftware*

F

FTP ..... File Transfer Protocol

G

GUI ..... *Grafical User Interface*

H

HA ..... High Availability
HDLC ..... *High Level Data Link Control*
HE ..... *Höheneinheit*
HTTP ..... *Hypertext Transfer Protocol*
HTTPS ..... *Hypertext Transfer Protocol Secure*

I

ISDN ..... *Integrated Services Digital Network*
ISP ..... *Internet Service Provider*

K

KMU ..... *Klein- und mittlere Unternehmen*

M

MAC ..... *Media Access Control Adresse*

N

NAT ..... *Network Address Translation*
NTP ..... *Network Time Protocol*

P

PBX ..... *Private Branch Exchange*
POE ..... *Power over Ethernet*

R

RTP ..... *Real Time Protocol*

S

SBC ..... *Session Border Controller*
SDP ..... *Session Description Protocol*
SFP ..... *Small Form Factor Pluggable*
SIP ..... *Session Initiation Protocol*
SSID ..... *Service Set Identifier*

T

TFTP ..... *Trivial File Transfer Protocol*

U

URL ..... *Uniform Recource Locator*
USB ..... *Universal Serial Bus*
UTM ..... *Unified Threat Management*

V

VLAN ..... *Virtual Local Area Network*
VoIP ..... Voice over IP
VPN ..... *Virtual Private Network*
vSwitch ..... *Virtual Switch*

W

WAN ..... *Wide Area Network*
WLAN ..... *Wireless Local Area Network*

12 Quellen

12.1 Internet

Alcatel	https://businessportal.alcatel-lucent.com
Fortigate	https://cookbook.fortinet.com/
Aruba	https://www.arubanetworks.com
Extreme	https://www.extremenetworks.com
Ruckus	https://www.ruckuswireless.com
Meraki	https://meraki.cisco.com

12.2 Bücher

Cisco	CCNA Powertraining: ICND1/CCENT (100-105)	ISBN: 978-3-95845-480-4
PM	Projektmanagement für Führungsfachleute	ISBN: 978-3-7155-9810-9

13.3 Kursunterlagen

Audiocodes	SBC Essentials & Configuration v7.2.200
Alcatel	CPU Loading – Issue 02 ENTPCTE301
	IP_SIP Security – Issue 02 ENTPCTE302
	Starter – Issue 03 ENTPCTE300