

Studienarbeit  
Dokumentation

# Neue Netzwerkarchitektur für Infrastrukturanlagen des EW Buchs

Semester: Herbst 2022



Version: 1.0

Datum: 23. Dezember 2022

**Studierende:** Jan Untersander  
Luzia Kündig

**Betreuer:** Laurent Metzger



School of Computer Science  
OST Eastern Switzerland University of Applied Sciences

## Abstract

Der Bereich Infrastruktur des Elektrizitäts- und Wasserwerk der Stadt Buchs (EWB) betreibt zurzeit mehrere physisch komplett separierte Netzwerke, um ihre Kraftwerksanlagen, Trafostationen und verschiedenen weiteren Standorte und Dienste untereinander zu verbinden. Die physischen Leitungen sind teilweise stark veraltet und entsprechen keinem einheitlichen Standard. Gleichzeitig wurde vom EWB in den letzten Jahren der Neubau eines FTTx Glasfasernetzwerks in ganz Buchs vorangetrieben. Dieses Grossprojekt ist aktuell in der Abschlussphase.

Auf Basis dieser neuen physikalischen Grundlage analysiert die vorliegende Arbeit mögliche Varianten eines neuen Netzwerkdesigns für die bestehenden Anwendungsfälle der Infrastruktur. Dabei wurde auch die potentielle Zusammenarbeit mit dem internen Provider "Rii Seez Net" geprüft, welcher bereits Nutzer des Glasfasernetzes ist. Dies wurde jedoch aus technischen und organisatorischen Gründen ausgeschlossen.

Für folgende drei providerunabhängige Varianten wurde ein Designentwurf erstellt:

- VLAN-basiert:  
Virtuelle Isolation der bestehenden mehreren Netzwerke auf einer physikalischen Grundlage
- L2 over L3 Ansatz BGP EVPN (MPLS / VXLAN):  
Optimierung der grossen Layer 2 Netzwerke mittels Overlay auf einer gerouteten Layer 3 Basis
- Cisco Software Defined Access:  
Zur Basis von Variante 2 zusätzliche Funktionalität im Bereich Automatisierung, Analyse und Sicherheit

Unsere Analyse ergibt, dass besonders mit Augenmerk auf Funktionalität, Einfachheit im Betrieb und Sicherheit die Variante 3: Cisco Software Defined Access am besten abschneidet. Als offensichtlicher Nachteil dieser Variante den beiden anderen gegenüber können die höheren einmaligen und wiederkehrenden Kosten genannt werden.

Variante 1: VLANs dagegen ist eine kostengünstige Alternative, welche aber viel weniger Funktionalität und Sicherheit bietet und somit wenig zukunftsorientiert ist.

Variante 2: BGP EVPN bietet auch gewisse erweiterte Funktionalität, welche jedoch auf Kosten von hoher Betriebskomplexität erreicht wird.

Aus diesen Gründen empfehlen wir, in einer Pilotphase vor Ort in Buchs mit Cisco Software Defined Access weiterzufahren, um das Zusammenspiel der Infrastrukturanlagen mit diesem Design zu testen. Der Aufbau eines Proof of Concept der Variante 3 in Rapperswil und das ausgearbeitete Testkonzept bieten die Grundlage, damit die Pilotphase erfolgreich durchgeführt werden kann.

# Management Summary

## Ausgangslage

Der Bereich Infrastruktur des Elektrizitäts- und Wasserwerk der Stadt Buchs (EWB) betreibt zur Zeit mehrere physisch komplett separierte Netzwerke, um ihre Kraftwerksanlagen, Trafostationen und verschiedenen weiteren Standorte und Dienste untereinander zu verbinden. Die physischen Leitungen sind teilweise stark veraltet und entsprechen keinem einheitlichen Standard. Gleichzeitig wurde vom EWB in den letzten Jahren der Neubau eines Glasfasernetzwerks in ganz Buchs vorangetrieben. Dieses Grossprojekt ist aktuell in der Abschlussphase, sämtliche Infrastrukturanlagen sind an diesem neuen Netz angeschlossen.



Abbildung 1.: Wasserkraft

## Vorgehen und Technologien

Auf Basis dieser neuen physikalischen Grundlage analysiert die vorliegende Arbeit mögliche Varianten eines neuen Netzwerkdesigns für die bestehenden Anwendungsfälle der Infrastruktur. Dabei wurde auch die potentielle Zusammenarbeit mit dem internen Provider "Rii Seez Net" geprüft, welcher bereits Nutzer des Glasfasernetzes ist. Dies wurde jedoch aus technischen und organisatorischen Gründen ausgeschlossen.

Deshalb wurden drei providerunabhängige Varianten für das neue Netzwerkdesign erarbeitet.

- Variante 1 basiert mit VLAN auf einer relativ simplen, über 20 Jahre alten Technologie, welche noch immer in vielen Unternehmen eingesetzt wird.
- Variante 2 bietet Optimierungen in der Netzwerkauslastung dank der Verwendung von BGP EVPN und weiteren Protokollen.
- Variante 3 basiert auf der Vorherigen, erweitert diese jedoch um zusätzliche Funktionalität, welche von Cisco Software Defined Access angeboten werden.

## Ergebnisse

Variante 1 ist sehr einfach zu implementieren, bietet jedoch wenig Funktionalität und ist darum nicht zukunftsorientiert. Variante 2 hat mehr zu bieten als Variante 1, jedoch ist sie komplexer zu implementieren und zu betreiben. Variante 3 bietet die meisten Funktionalität und somit auch die beste Zukunftsperspektive, vor allem auf Grund der mitgelieferten Sicherheitsfunktionen.

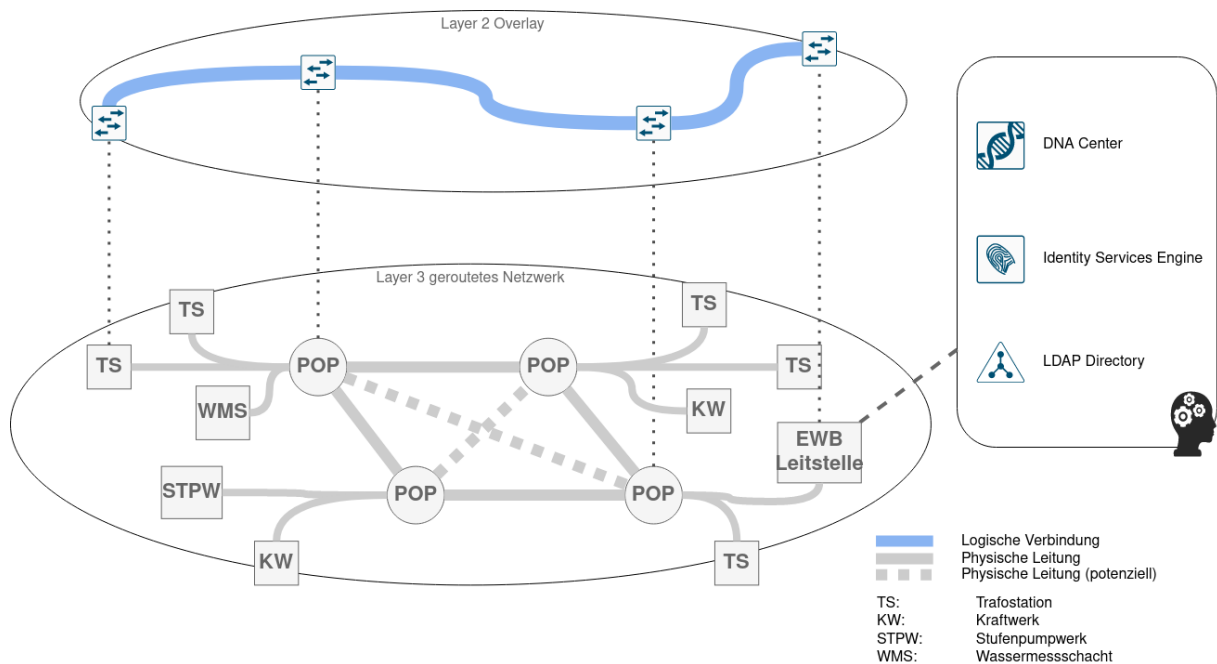


Abbildung 2.: Logisches Schema Variante 3

Auf Grund dieser Erkenntnisse wurde Variante 3 als beste Lösung für das neue Netzwerkdesign ausgewählt und in einem Proof of Concept in Rapperswil aufgebaut und getestet. Nach erfolgreicher Implementierung des PoC wurde ein Testkonzept für eine spätere Pilotphase in Buchs erarbeitet.

## Ausblick

In Anbetracht der steigenden Gefahr von Cyberangriffen ist Sicherheit ein wichtiges Thema, vor allem da die Infrastruktur des EWB die Bevölkerung der Stadt mit Strom und Wasser versorgt. Mit der neuen Netzwerkarchitektur wird das EWB in der Lage sein, die Sicherheit ihrer Netzwerke zu erhöhen und somit die Gefahr von Cyberangriffen zu reduzieren.

# Danksagung

Wir danken den folgenden Personen für die Unterstützung:

- Laurent Metzger (Institut für Netzwerke und Sicherheit)
- Jürg Göldi (EW Buchs)
- Niklaus Müller (EW Buchs)
- Donat Vetsch (EW Buchs)
- Patrick Mosimann (Cisco)
- Raphael Holenweger (EW Buchs)

# Inhaltsverzeichnis

<b>I. Produktdokumentation</b>	<b>9</b>
<b>1. Bisherige Situation</b>	<b>10</b>
1.1. Bestehendes Netzwerk "Infrastruktur"	10
1.2. Anwendungsfälle	11
1.2.1. TS LAN	12
1.2.2. KW LAN	12
1.2.3. MMI LAN	13
1.2.4. Firewall	15
1.2.5. Übersicht aller genutzten/bekannten Protokolle	16
<b>2. Anforderungskatalog</b>	<b>17</b>
2.1. Strategische Anforderungen	17
2.2. Funktionale Anforderungen	17
2.3. Technische Anforderungen	18
2.4. Designeinschränkungen	19
<b>3. Design</b>	<b>20</b>
3.1. Zusammenarbeit Providergeschäft	20
3.2. Schematischer Entwurf (Physikalisch)	20
3.3. Grundlagen Netzwerktechnik	21
3.3.1. Layer 2 Transport	21
3.3.2. Layer 3 Transport	22
3.3.3. Tunneling	23
3.3.4. Netzwerk Fabric	24
3.3.5. Control Plane und Data Plane	24
3.3.6. Zero Trust und Port-based Network Access Control (IEEE 802.1X)	24
3.4. Variante 1 – VLAN-basiert	26
3.4.1. VLAN – 802.1Q	26
3.4.2. VLAN Tags, Access- und Trunk Ports	26
3.4.3. Spanning Tree	27
3.4.4. Analyse	28
3.5. Variante 2 – L2 over L3 Ansatz BGP EVPN (MPLS / VXLAN)	29
3.5.1. Data Plane Protokolle	29
3.5.2. MPLS	29
3.5.3. VXLAN	30
3.5.4. Control Plane Protokoll	31
3.5.5. Analyse	32
3.6. Variante 3 – Cisco Software Defined Access	33
3.6.1. Grundlagen Software Defined Networking	33
3.6.2. Cisco DNA	34
3.6.3. Authentifizierung: Identity Services Engine	35
3.6.4. Software Defined Access	36
3.6.5. Segmentierung	37
3.6.6. Netzwerkdesign EWB	39
3.6.7. Analyse	41
3.7. Variantenvergleich	42

<b>4. Aufbau Proof of Concept</b>	<b>43</b>
4.1. Planung des Deployment	43
4.1.1. IP Konfiguration	44
4.1.2. Zugangsdaten	45
4.2. Installation der Appliance	45
4.3. Vorbereiten der Appliance für die Konfiguration	45
4.4. Vorbereitung der Catalyst 9300 Switches	45
4.4.1. Stack auflösen	46
4.4.2. Factory Reset	46
4.5. Grundkonfiguration der Appliance	46
4.5.1. Maglev Einrichtungsassistent	46
4.6. Grundkonfigurationen im DNA Center	48
4.6.1. Allgemeine Informationen	49
4.6.2. Software Image Management	50
4.6.3. Device Templates	51
4.7. LAN Automation	53
4.7.1. Phase 1: Device Onboarding und Provisionierung	53
4.7.2. Phase 2: Interface Configuration	56
4.8. Fabric	59
4.8.1. Konfiguration der Fabric	59
4.9. Konfiguration Extended Nodes	62
4.9.1. Voraussetzungen	62
4.9.2. Erstellung des IP-Adresspools und der Credentials	62
4.9.3. Zuweisen des IP-Adresspools zum Virtuellen Netzwerk	62
4.9.4. Erstellen der Port Channels	63
4.9.5. Konfiguration DHCP Server	64
4.9.6. Finalisierung der Konfiguration	64
4.10. Statische VLAN-Port Zuweisung	65
<b>5. Testkonzept für Pilotphase in Buchs</b>	<b>67</b>
5.1. Grundlegende Kommunikation	67
5.2. Anwendungsspezifische Kommunikation	67
5.3. DNA Center Funktionalität	67
5.4. Aussenstellen: Extended Node vs. Policy Extended Node	68
5.4.1. Extended Node	68
5.4.2. Policy Extended Nodes	68
<b>II. Projektdokumentation</b>	<b>70</b>
<b>1. Projektplanung</b>	<b>71</b>
1.1. Phasen/Meilensteine	71
1.2. Meetings	71
1.3. Rollen	72
1.4. Risikomanagement	72
1.5. Arbeitspakete	73
<b>III. Anhang</b>	<b>74</b>
<b>A. Aufgabenstellung</b>	<b>75</b>

<b>B. Einrichtungsassistent - Screenshots</b>	<b>77</b>
<b>C. Projektplan</b>	<b>92</b>
<b>D. Glossar</b>	<b>93</b>



**Teil I.**

# **Produktdokumentation**

# 1. Bisherige Situation

Diese Studienarbeit befasst sich mit dem Infrastrukturnetzwerk des Elektrizitäts- und Wasserwerk der Stadt Buchs (EWB). Dieses verbindet unter anderem Kraftwerke, Pumpwerke, Reservoirs und Trafostationen untereinander und mit der zentralen Leitstelle. Das Ziel ist die Erhebung der Anforderungen an das Netzwerk und die Erarbeitung eines neuen Designs.

Dieses soll einfach, sicher und zukunftsgerichtet sein. Als physikalische Grundlage dient dabei das neu erstellte Glasfasernetz in Buchs.

## 1.1. Bestehendes Netzwerk “Infrastruktur”

**Für öffentliche  
Version entfernt**

Abbildung 1.1.: Leittechnikkonzept des EW Buchs (Firma Rittmeyer)

Die Zeichnung zeigt die aktuelle Situation mit Fokus auf die Leitstelle im EW Buchs. Es bestehen komplett separate physische Netzwerke für die verschiedenen Anwendungsfälle, und somit auch redundante Aktivkomponenten und Leitungen.

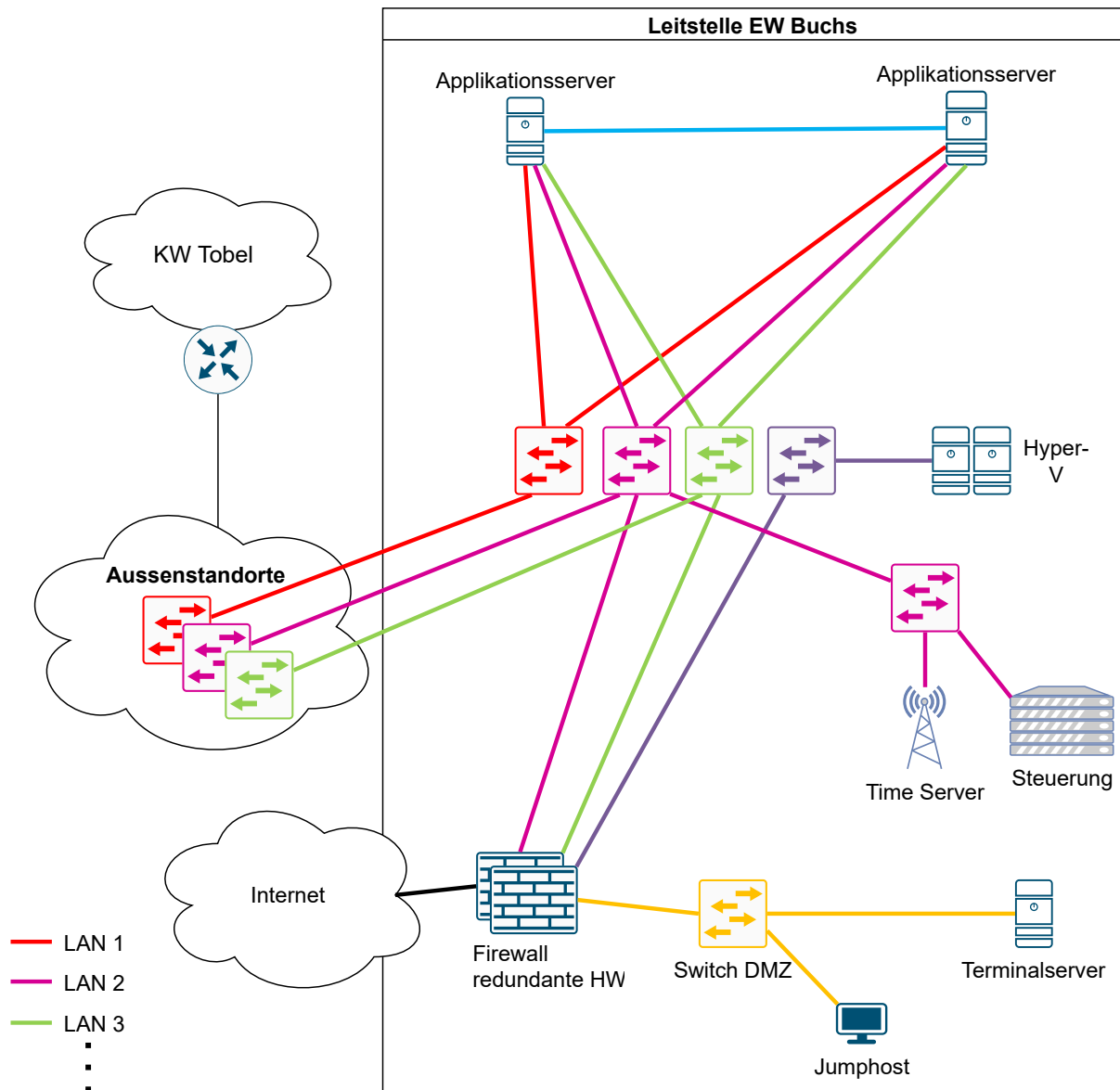


Abbildung 1.2.: Netzwerkschema physisch Leitstelle EWB

## 1.2. Anwendungsfälle

Die bisherigen Anwendungsfälle des Netzwerks für den Bereich Infrastruktur lassen sich am besten anhand der verschiedenen Subnetze erklären. Jedes Subnetz erfüllt eine andere Funktion, welche für das Design der neuen Lösung nach bestimmten Kriterien eingestuft werden soll.

Der operative Hauptfokus liegt einerseits auf dem Netzwerk *KW-LAN*, das bisher ausschliesslich durch Rittmeyer betrieben wurde und die autonome Kommunikation der Anlagen untereinander sicherstellt, andererseits auf den beiden *TS-LAN* (*OPC und IEC*), welches zur Steuerung und Überwachung der Anlagen durch Mitarbeitende des EW Buchs dient.

Die weiteren logischen Netzwerke (*im bisherigen MMI-LAN*) ermöglichen zusätzliche Dienste, die hinter der Anlagentechnik an zweiter Stelle stehen.

Die Adressbereiche der bestehenden Netze sollen wo immer möglich beibehalten werden. Das Neudressieren aller Anlagen wäre ein manueller Aufwand, der vermieden werden soll.

Grafiken der Netzwerkanalysen sind interaktiv als [PowerBI App](#)<sup>1</sup> verfügbar.

### 1.2.1. TS LAN

Zwei Subnetze, die komplett separiert nur die Verbindung zwischen Server und Aussenstationen sicherstellen. Auf der Firewall nicht bekannt, kein Zugang ins Internet. Dies ist keine zwingende Anforderung, jedoch bestand bisher kein Bedarf. *Adresskonflikt mit anderen Netzen möglich!*

#### TS-OPC

IP-Bereich: 192.168.1.0/24

Beinhaltet ca. 120 Geräte: Siemens SPS, verschiedene optische Switch-Modelle

Beschreibung / Zweck: Anbindung der Stationstechnik an RITOP (Software) über SPS Geräte.

#### TS-IEC

IP-Bereich: 192.168.3.0/24

Beinhaltet ca. 110 Geräte: SPS IEC, verschiedene Switchmodelle, Ritop Server

Beschreibung / Zweck: Anbindung der Stationstechnik an RITOP (Software) über SPS Geräte.

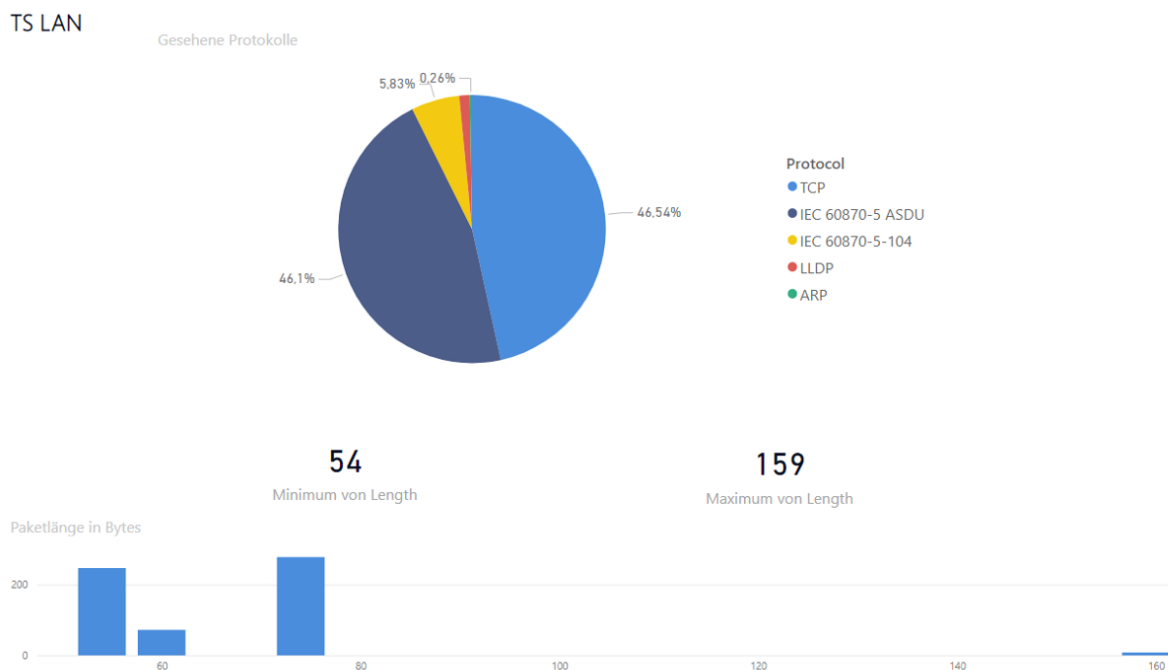


Abbildung 1.3.: Analyseergebnisse TS LAN

### 1.2.2. KW LAN

Auf der Firewall bekannt, Internetzugang möglich.

IP-Bereich: 192.168.2.0/2

Beinhaltet ca. 30 Geräte: "RIFLEX", Switches (Moxa), Ritop Server

Beschreibung / Zweck: Kraftwerksteuerung, RIFLEX, Kommunikation der Systeme untereinander

<sup>1</sup><https://app.powerbi.com/Redirect?action=OpenApp&appId=d3da1630-42d4-4b7d-86a1-dbe52199e65a&ctid=a6e70fa3-1c7a-4aa2-a25e-836eea52ca22>

## KW LAN

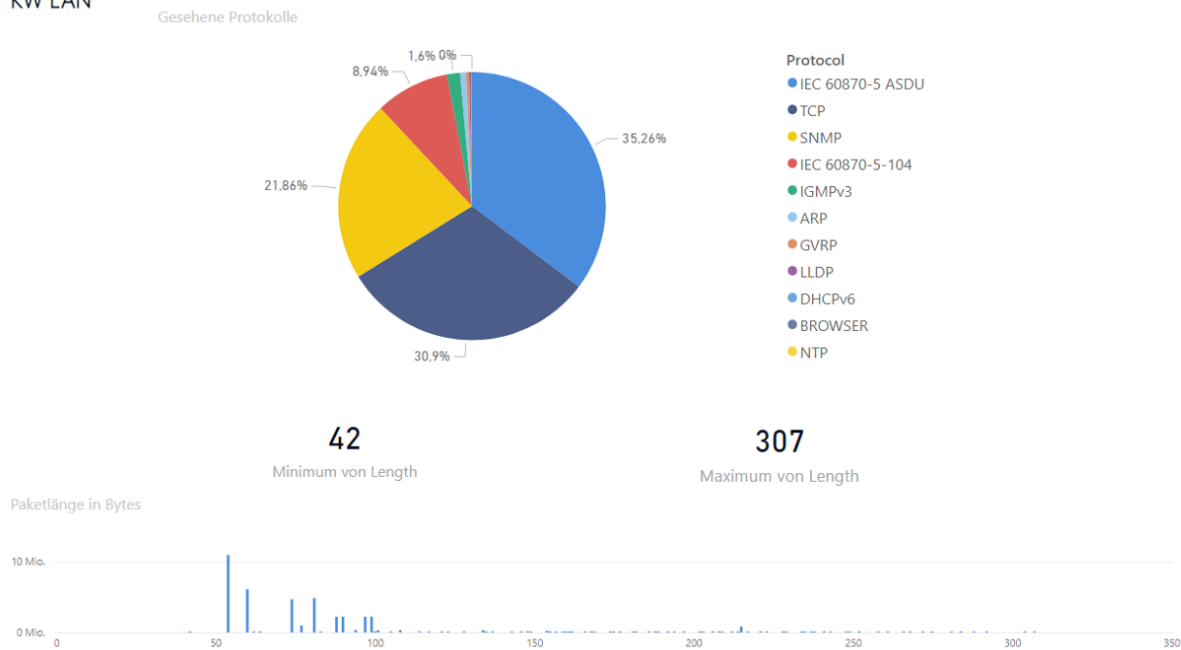


Abbildung 1.4.: Analyseergebnisse KW LAN

### 1.2.3. MMI LAN

Aufgeteilt in verschiedene Subnetze für verschiedene kleinere Anwendungszwecke. Grösstenteils auf der Firewall bekannt.

#### Rundsteueranlage

IP-Bereich: 192.168.1.0/24

Beinhaltet ca 10 Geräte: Server, Arbeitsplatz, Rundsteuerung, Backup NAS

Beschreibung / Zweck: Rundsteuerung in TS-Fuchsbühl und Software in Leitstelle (Hyper-V Host).

IP Wechsel bei Konflikt mit TS-LAN wäre möglich.

#### Telefon

IP-Bereich: 192.168.4.0/24

Beinhaltet 2 Geräte: Telefone Vorderberg und Malschüel

Beschreibung / Zweck: Telefonie Verbindung, Rückbau kurzfristig geplant. Wird durch Festnetzanschluss Rii Seez Net ersetzt, sobald der FTTH Anschluss erstellt ist.

#### Power-Quality Messungen

IP-Bereich: 192.168.5.0/24

Beinhaltet ca. 15 Geräte (wachsend?): UMG 512-PRO, Terminalserver, Arbeitsplatz

Beschreibung / Zweck: Qualitätsmessungen UMG 512 in Trafostationen, Anbindung an GridVis-Software

## ZFA

IP-Bereich: 192.168.6.0/24

Beinhaltet ca. 40 Geräte: Stromzähler, Programmiergerät, Firewall (Gateway)

Beschreibung / Zweck: Zählerfernauslesung, Rückbau mittelfristig geplant.

## KW Tobel

IP-Bereich: 192.168.3.0/24

Beinhaltet ca. 5 Geräte, 1 Router am Standort Vorderberg. Beschreibung / Zweck: Logisch durch separaten Router getrenntes Netz. Anforderung besteht durch Rittmeyer, dass die Anlage vom restlichen Netzwerk getrennt ist, da sie von einem anderen Lieferanten stammt. Wechsel vom IP Range wäre machbar.

## DMZ CKW

IP-Bereich: 192.168.8.0/24

Beinhaltet 2 Geräte: Firewall und UCD Box

Beschreibung / Zweck: Systemdienstleistung Wasserkraft

## KOM CKW-RAG

IP-Bereich: 192.168.9.0/24

Beschreibung / Zweck: Kommunikation Systemdienstleistung zwischen Rittmeyer und CKW

## RAG / RITOP

IP-Bereich: 192.168.10.0/24

Beschreibung / Zweck: RITOP

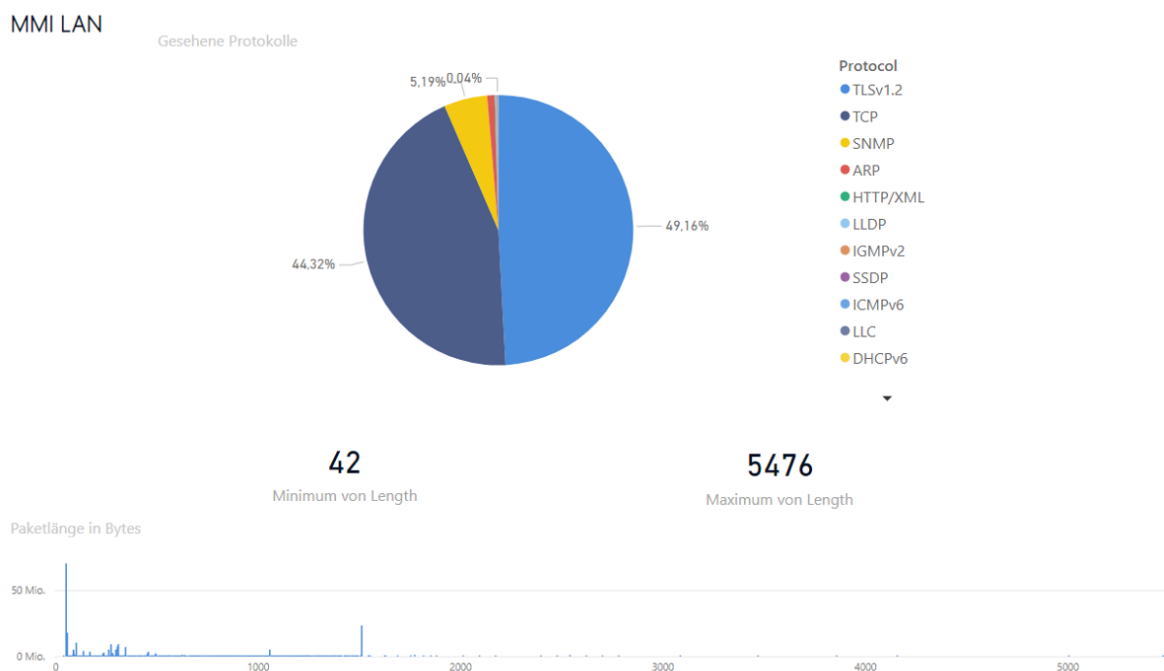


Abbildung 1.5.: Analyseergebnisse MMI LAN

## **DMZ RAG**

IP-Bereich: 192.168.20.0/24

Beschreibung / Zweck: DMZ PLS

## **ServReduLink**

IP-Bereich: 192.168.101.0/24

Beschreibung / Zweck: Synchronisierung der Server untereinander. Direkte Ethernet Verbindung, ohne Gerät dazwischen. Höchste Priorität ist die Unabhängigkeit von Hardwareausfällen (Switches).

## **Alarmserver**

IP-Bereich: 192.168.200.0/24

Beschreibung / Zweck: SMS-Butler und ADAM-Modul vom Alarmserver

## **1.2.4. Firewall**

Das **TS-LAN** ist ein von den anderen Netzwerken komplett getrennt. Die verschiedenen anderen Netzwerke sind miteinander über eine Firewall verbunden und können teilweise miteinander kommunizieren.

**Für öffentliche  
Version entfernt**

Abbildung 1.6.: Logisches Netzwerkschema der Firma Rittmeyer

## **VPN Verbindungen**

Aktuell sind auf der vorhandenen Firewall zwei VPN Verbindungen konfiguriert:

- Zugriff Rittmeyer Service
- Zugriff EWB Pikett

Beide Verbindungen terminieren auf einem Gerät in der DMZ Netzwerkzone, einem Konfigurations-Rechner bzw. Terminalserver respektive.

### 1.2.5. Übersicht aller genutzten/bekannten Protokolle

#### Applikationen

Protokoll	Beschreibung
HTTP / HTTPS	Web Traffic
SMTP	E-Mail
FTP	Übertragen von Dateien über Netzwerk
SIP	IP Telefonie
TCP	Applikationsdaten, Session-basiert (bidirektional)
UDP	Applikationsdaten, unidirektional (streaming)
IEC 60870-5-104, IEC 60870-5 ASDU	Anwendungsbezogene Norm für Fernwirkaufgaben in IP-Netzen [20]
OPC UA	IEC 62541 plattformunabhängiger Standard für Datenaustausch zwischen Sensoren und Applikationen [18]

#### Verwaltung / Remotezugriff

Protokoll	Beschreibung
VNC	Bildschirm-Zugriff auf entfernte Geräte, plattformunabhängig
SSH	Gesicherte Verbindung auf Kommandozeile von entfernten Geräten
RDP	Remotedesktop-Verbindung (Microsoft-Standard)
SNMP	Abfragen von Geräte-Informationen, Monitoring
NTP, SNTP	Zeitsynchronisation im Netzwerk

#### Netzwerk Management / diverses

Protokoll	Beschreibung
ARP	Address Resolution Protocol
ICMPv4 / ICMPv6	Internet Control Message Protocol: Ping, etc.
DHCPv6	Dynamische Adressvergabe für IPv6
IGMPv3	Internet Group Management Protocol, Verwaltung von Multicast Empfängergruppen (Quelle 192.168.3.80)
LLC	Logical Link Control
LLMNR	Link Local Multicast Name Resolution
MDNS	Multicast Domain Name System
NBNS	NetBIOS Name Service
SSDP	Simple Service Discovery Protocol
LLDP	Link Layer Discovery Protocol, Austausch von Informationen zwischen Nachbargeräten
GVRP	Generic VLAN Registration Protocol (MOXA Switches)



## 2. Anforderungskatalog

Die Anforderungen an das neue Netzwerk werden in diesem Kapitel aufgeführt. Diese werden für die Erarbeitung mit dem Industriepartner in zwei Kategorien unterteilt: strategische und funktionale Anforderungen. Aus diesen Anforderungen, Informationen der Anlagenhersteller und eigener Analysen des Netzwerks werden die technischen Anforderungen und Designeinschränkungen abgeleitet.

### 2.1. Strategische Anforderungen

Die folgenden Punkte wurden zusammen mit dem EWB erarbeitet und bilden die Grundlage für die restlichen Anforderungen an das neue Netzwerk.

Tabelle 2.1: Strategische Anforderungen

Priorität	Ziel
1	Modernisierung des Netzwerks durch Wechsel auf neues Glasfasernetz
2	Mehr Sicherheit
3	Vereinfachung/Vereinheitlichung der genutzten Technologien
4	Nutzung von Synergien mit klar geregelten Verantwortlichkeiten
5	Wachstum & Veränderungen im Netz vereinfachen

### 2.2. Funktionale Anforderungen

Genauere Beschreibungen der Anwendungsfälle, auf denen diese Anforderungen basieren, finden sich im Abschnitt 1.2.

Tabelle 2.2: Funktionale Anforderungen

ID	Anforderung	Erklärung
A1	Fernwirkaufgaben	Steuerungssoftware auf Server und steuert Anlagen an entfernten Standorten
A2	Anlagenkommunikation	Die Anlagen kommunizieren untereinander und mit dem zentralen Server
A3	Störmeldungen	Störmeldungen verschiedener Anlagen werden an zentralen Server gesendet
A4	Alarmierung	Es werden Alarmer bei Störungen ausgelöst und über verschiedene Wege weitergeleitet
A5	Messungen	Messdaten verschiedener Anlagen werden an zentralen Server gesendet
A6	VPN Zugriff	Es wird von Extern via VPN auf zwei Server in der DMZ zugegriffen
A7	Fernzugriff	Es wird via Teamviewer, VNC und RDP auf verschiedene Rechner zugegriffen

Fortsetzung auf der nächster Seite

Tabelle 2.2: Funktionale Anforderungen (Fortsetzung)

ID	Anforderung	Erklärung
A8	Web Traffic	Einige Anlagen/Steuerungen haben ein Web Interface, auf das zugegriffen werden kann
A9	E-Mail	Es findet E-Mail Kommunikation statt
A10	Remote-Backup	Ein Backup der Server wird auf ein NAS an einem anderen Standort übermittelt
A11	IP Telefonie	Ein Telefon kommuniziert übers Netzwerk (Abbau geplant)
A12	Benötigt Multicast	NTP Services und weitere kommunizieren via Multicast
A13	Verwendete Protokolle	Die Protokolle im Unterabschnitt 1.2.5 werden verwendet
A14	Bandbreiten	Anwendungen benötigen nur wenig der bereits verfügbaren Bandbreite
A15	Basiert auf Ethernet	Alle verwendeten Protokolle basieren auf Ethernet
A16	Performance	Wurde bei Rittmeyer angefragt, keine spezifischen Anforderungen erhalten. Beim Testen der Use Cases im Rahmen des Pilots nochmals zu klären.

## 2.3. Technische Anforderungen

Technische Anforderungen sind Qualitätseigenschaften, die das Netzwerk erfüllen muss, um den Anwendungen einen reibungslosen Betrieb zu ermöglichen. Diese technischen Anforderungen haben sich aus den funktionalen Anforderungen ergeben und sind in der folgenden Tabelle aufgelistet.

Tabelle 2.3: Technische Anforderungen

ID	Anforderung	Erklärung
T1	Wartbarkeit	Netzwerk soll von der IT gewartet werden können
T2	Sicherheit	Unterstützt die Integration von Netzwerksicherheitsdiensten
T3	Veränderbarkeit	Es soll möglichst einfach bestehende Subnetze an verschiedenen Standorte verfügbar gemacht oder entfernt werden können
T4	Erweiterbarkeit	Es soll möglichst einfach neue Subnetze an beliebigen Standorten verfügbar gemacht werden können
T5	Segmentierung	Netzwerk soll logisch in mehrere Subnetze aufgetrennt werden können
T6	Verfügbarkeit	Netzwerkausfälle, die weniger als 30 Minuten dauern, sind vertretbar. Somit sind jegliche Konvergenz-Szenarien grundsätzlich ausreichend, überall dort wo im Netzwerk Redundanz besteht. Für Hardware-Ausfälle soll vom Picketdienst Infrastruktur (nicht IT Mitarbeiter) ein Ersatz eingebaut werden können, nötige Konfigurationen übernimmt die EWB Informatik.
T7	Verlässlichkeit	Keine spezifischen Anforderungen betreffend Ausfälle pro Jahr. Verlässlichkeit (Lebensdauer) der Geräte nach Vorgaben vom Hersteller.

## 2.4. Designeinschränkungen

Designeinschränkungen sind Faktoren und Entscheidungen, die bereits getroffen wurden und nicht mehr geändert werden können oder sollen und direkten Einfluss auf das Design des Netzwerks haben.

Tabelle 2.4: Designeinschränkungen

<b>ID</b>	<b>Anforderung</b>	<b>Erklärung</b>
F1	FTTx Netz	Das neue FTTx Glasfasernetz wird als physisches Layer verwendet
F2	Cisco Geräte	Aufgrund des Partnerstatus bei Cisco soll wo möglich auch deren Hardware verwendet werden

## 3. Design

Für das Design werden folgende drei Varianten in Betracht gezogen, welche sich aus den gesammelten Anforderungen, Recherchen und Gesprächen mit unserem Advisor und dem EWB ergeben haben. [9, 10]

- Variante 1 – VLAN-basiert
- Variante 2 – L2 over L3 Ansatz BGP EVPN (MPLS / VXLAN)
- Variante 3 – Cisco Software Defined Access

### 3.1. Zusammenarbeit Providergeschäft

Eine Zusammenarbeit mit dem eigenen Provider Rii Seez Net wurde nicht weiter verfolgt, da deren Infrastruktur innerhalb Buchs lediglich mit Layer 2 erschlossen ist. Ein einzelner Core Router implementiert MPLS zur Kommunikation mit anderen Gemeinden. Für den vorliegenden Anwendungsfall hat dies jedoch keinen Nutzen.

Somit wird bevorzugt eine Lösung direkt auf der physikalischen Ebene umgesetzt, welche von der EWB Informatik betreut werden kann und nicht unnötig weitere Stellen involviert im späteren Betrieb.

### 3.2. Schematischer Entwurf (Physikalisch)

Die nachfolgenden Designs basieren auf dem durch das EWB gebauten FTTx Netz. Ein grobes Schema zeigt den Ring der vier Hauptknotenpunkte (Point of Presence bzw. POPs) sowie einen Stich in Ringform für die verschiedenen Anlagen am Buchserberg.

**Für öffentliche  
Version entfernt**

Abbildung 3.1.: FTTx Netz

### 3.3. Grundlagen Netzwerktechnik

Im folgenden Unterkapitel werden kurz die wichtigsten Begriffe erklärt, die zum Verständnis der vorgeschlagenen Varianten nötig sind.

Die Unterscheidung zwischen Netzwerkverkehr auf Layer 2 und Layer 3 des OSI Schichtenmodells ist für die behandelte Thematik zentral. Die jeweiligen Vor- und Nachteile spielen eine grosse Rolle bei der Architektur eines solchen Netzwerks.

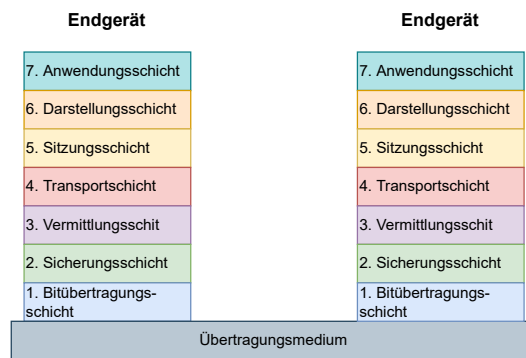


Abbildung 3.2.: OSI Schichtenmodell

#### 3.3.1. Layer 2 Transport

Auf Layer 2 des OSI Modells kommunizieren Netzwerkgeräte nur via MAC Adressen. Grundsätzlich werden alle Pakete im Netzwerk für alle Geräte hörbar verschickt. Layer 2 Switches mit MAC Learning speichern ab, welche MAC Adressen an welchen Ports verbunden sind und leiten Pakete nur noch an den richtigen Ort weiter.

Pakete an unbekannte Ziele werden jedoch in jedem Fall auf allen Ports ausser dem Empfängerport weitergeleitet. Sobald das gesuchte Gerät selber kommuniziert, wird es ebenfalls vom Switch mittels MAC Learning abgespeichert.

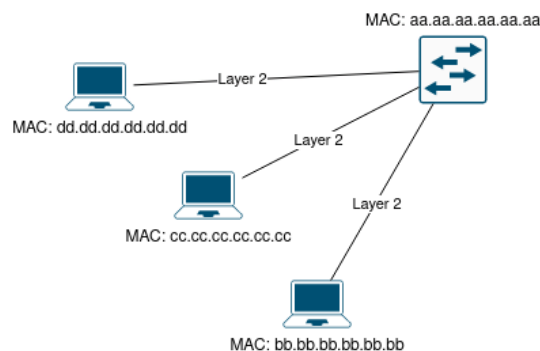


Abbildung 3.3.: Beispiel Layer 2

#### Spanning Tree

Wird in einem reinen Layer 2 Netzwerk physisch irgendwo ein geschlossener Ring erstellt, resultiert dies in einem sogenannten Broadcast Storm. Pakete werden von denselben Switches mehrfach empfangen und aufgrund fehlender Kontrollmechanismen auch genauso weitergeleitet. Dies führt zu endlos steigender Auslastung der Bandbreite und schlussendlich zum kompletten Verbindungsunterbruch.

Das Spanning Tree Protokoll verhindert solche Probleme, indem aus der gesamten Topologie nur gewisse Verbindungen verwendet werden. Das Ergebnis ist ein eindeutiger, loop-freier Baum. Redundante Wege werden deaktiviert und können im Falle eines Unterbruchs an anderer Stelle automatisch wieder aktiviert werden.

Das Protokoll definiert ein Netzwerkgerät als sogenannte Root Bridge, welche die Berechnung dieses Baumes übernimmt. Informationen zu diesem Prozess werden in Bridge Protocol Data Units, sogenannten BPDU verschickt. Dort, wo auf einem einzelnen Link von mehreren Switches BPDUs verschickt werden, wird die Verbindung deaktiviert.

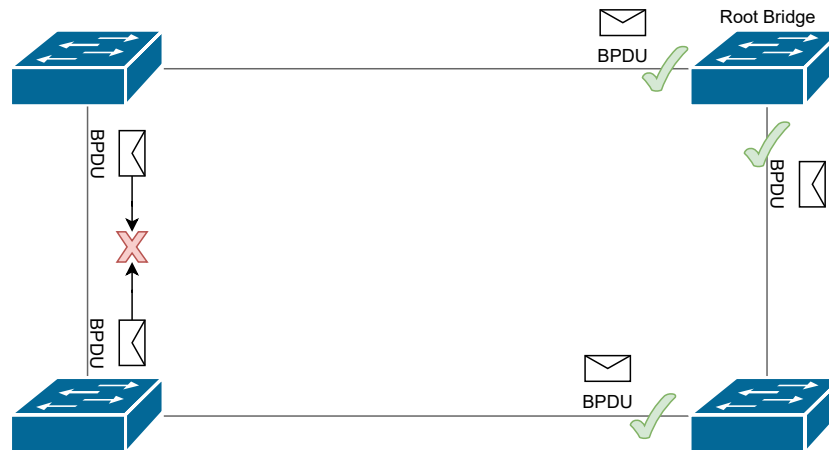


Abbildung 3.4.: Spanning Tree

Spezielle Kontrollmechanismen wie BPDU Guard erlauben es zudem, diese Kontrollpakete auf Access Ports zu verbieten. Somit kann verhindert werden, dass ein falsch angeschlossener Switch zur Root Bridge wird und die Berechnung des kompletten Baumes übernimmt.

### 3.3.2. Layer 3 Transport

Um einen Übergang zwischen verschiedenen Layer 2 Netzwerken zu schaffen, wird im OSI Modell eine Ebene höher auf Layer 3 gewechselt. Der sogenannte Standardgateway (ein Gerät, welches Routing-Funktionen ausführen kann), dient als Austrittspunkt aus dem eigenen Layer 2 Netzwerk. Diese Adresse ist die einzige Information, welche die Endgeräte benötigen, um ausserhalb ihres Netzes kommunizieren zu können. Alle weiteren Informationen muss der Gateway besitzen.

Mittels dynamischen Routing-Protokollen werden alle Netze sowie deren Standort unter sämtlichen Routern des Netzwerks ausgetauscht. So wird auf jedem Gerät eine Routing-Tabelle erstellt, welche die zentrale Datenbank eines Layer 3 Netzwerks ist und als Basis für alle Steuerungs-Entscheidungen dient.

Loops können in seltenen Fällen auch in Layer 3 Netzwerken entstehen. Diese sind jedoch unproblematisch, da ein Netzwerkpaket von Routern nicht unendlich weitergeleitet wird (Steuerungslogik). Zudem sind dies meist zeitlich beschränkte Phänomene aufgrund einer Änderung in der Topologie, wie einem Verbindungsausfall. Sobald das Netzwerk wieder konvergiert, also einen stabilen Zustand erreicht, ist der Loop nicht mehr vorhanden.

Ebenfalls können in Layer 3 Netzwerken mehrere Pfade zum selben Ziel gleichzeitig aktiv sein und erlauben somit unter anderem auch das Netzwerk gleichmässiger auszulasten.

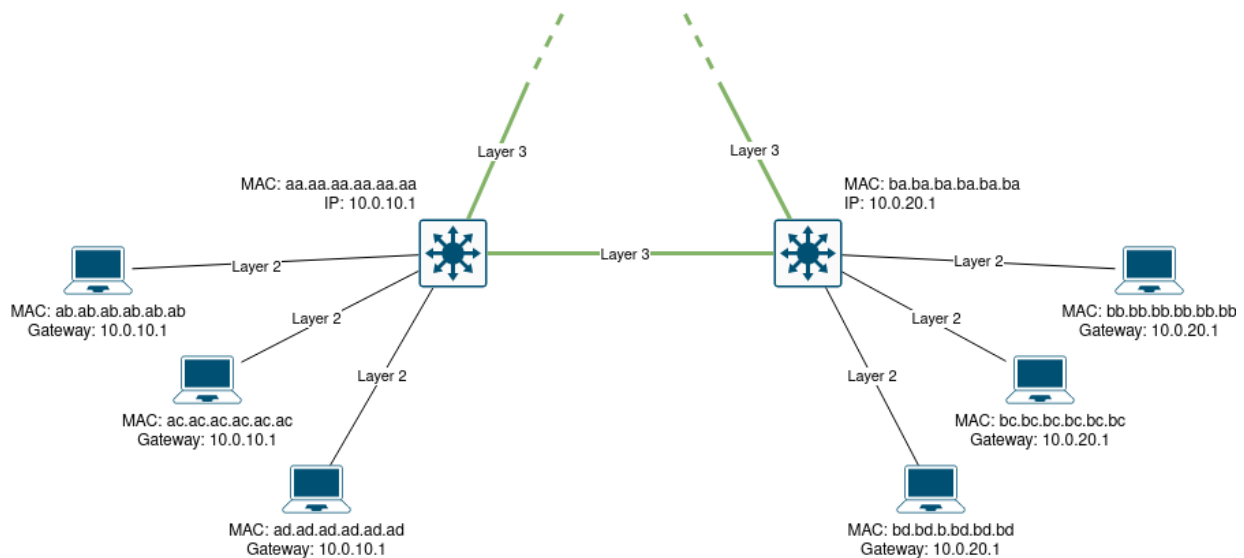


Abbildung 3.5.: Beispiel Layer 3

Tabelle 3.1: Vergleich Layer 2 und Layer 3

Aspekt	Layer 2	Layer 3
Konfigurationsaufwand	Hoch, komplett manuelle Konfiguration	Mittel, Routing Protokolle arbeiten selber
Skalierbarkeit	Begrenzt durch Broadcast	Benötigt Planung von Netzwerkadressen
Anzahl Geräte	Begrenzt durch Broadcast	Unbeschränkt
Komplexität	Tief: Spanning Tree benötigt bei redundanten Wegen	Mittel: Routing-Protokolle, Konvergenz, Timer
Steuerung	keine Möglichkeit	Routing ermöglicht Steuerung und Filterung von Traffic
Segmentierung	keine Möglichkeit	Firewall und Filtering
Ausfallsicherheit	Von Spanning Tree blockierte Links können aktiv geschaltet werden	Erlaubt mehrere aktive Pfade zu einem Ziel (Equal Cost Multipath)

### 3.3.3. Tunneling

Ein Tunnel ist eine Verbindung, die es erlaubt, Daten einer tieferen OSI-Schicht über ein Netzwerk zu versenden, welches eigentlich auf einer höheren Schicht kommuniziert.

Die Datenpakete werden dazu mit zusätzlichen Headern versehen, welche Informationen zu Herkunft und Ziel des Pakets beinhalten, die vom transportierenden Netzwerk verstanden werden. Das originale Paket wird so verpackt oder enkapsuliert und am Ende des Tunnels wieder entpackt bzw. dekapsuliert, bevor es dem Zielnetzwerk/Zielgerät übergeben wird.

Bei einem Layer 2 Tunnel wird dabei das komplette Layer 2 Paket in ein Tunneling-Protokoll verpackt. Es gibt eine Vielzahl von Protokollen und Standards, die es erlauben, Layer 2 Verkehr durch ein Layer 3 Netzwerk zu tunneln.

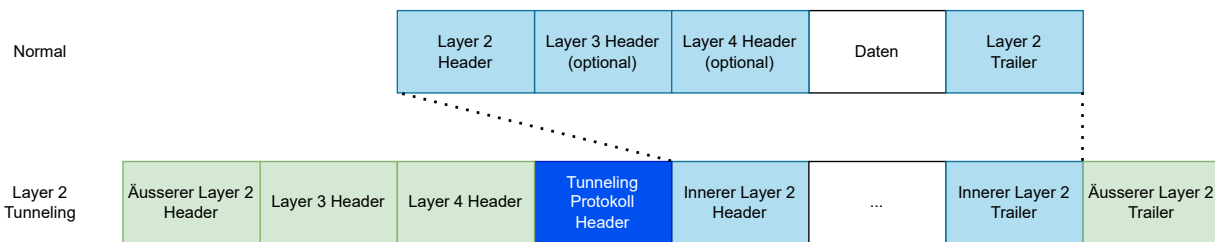


Abbildung 3.6.: Layer 2 over Layer 3 Tunnel

### 3.3.4. Netzwerk Fabric

Der Begriff Fabric beschreibt eine Architektur, welche die grundlegende Konnektivität von A nach B in ein Underlay und ein Overlay aufteilt.

Ein Underlay Netzwerk bezeichnet das physikalische Netz, das auf Layer 3 ein internes Routing Protokoll (Interior Gateway Protocol, IGP) verwendet. Das Ziel ist es, alle Endpunkte möglichst einfach und performant miteinander zu verbinden.

Im Overlay können dann separate logische Netzwerke für einzelne Services erstellt werden, die zwei oder mehr Endpunkte untereinander verbinden.

### 3.3.5. Control Plane und Data Plane

Diese Funktionalität einer Fabric wird mit einer Kombination von verschiedenen Protokollen erreicht. Diese lassen sich wiederum auf zwei Ebenen aufteilen. Während die Data Plane für das Weiterleiten von Paketen zuständig ist, trifft die Control Plane basierend auf gewissen Informationen die Entscheidungen, wie auf der Data Plane weitergeleitet wird.

### 3.3.6. Zero Trust und Port-based Network Access Control (IEEE 802.1X)

In einer Netzwerkkumgebung, die nach dem Zero Trust Prinzip konfiguriert ist, wird jedes Endgerät beim ersten Kontakt als unsicher eingestuft. Zugriff auf das Netz wird erst erteilt, wenn sich das Gerät erfolgreich authentifiziert. [8]

Folgende Funktionalität ermöglicht es, diese Herangehensweise zu automatisieren.

- Identifizieren der Endgeräte
- Netzwerksegmentierung mittels Richtlinien
- Trust Monitoring zur fortlaufenden Analyse des Verhaltens

Zur Erkennung und dadurch möglichen Authentifizierung der Endgeräte wird verbreitet der IEEE Standard 802.1X (Port-based Network Access Control) genutzt. Dieser Standard beinhaltet verschiedene Protokolle, um das Ziel zu erreichen. [22]

- EAP-TLS: Austausch von Zertifikaten
- MSCHAPv2: Übermittlung von Username und Passwort
- MAC-Bypass: Authentifizierung via MAC-Adresse (für Endgeräte, welche 802.1X nicht unterstützen)

Diese verschiedenen Varianten der Authentifizierung werden alle im Protokoll EAPoL (Extended Authentication Protocol over LAN) gekapselt.

Die Rollen, welche für eine solche Authentifizierung benötigt werden, sind die folgenden:



- Supplicant: Endgerät, welches sich am Netzwerk authentifizieren will
- Authenticator: Das Netzwergerät, welches die Anfrage vom Supplicant entgegennimmt und diese an den Authentication Server weiterleitet (Switch oder WLAN Access Point)
- Authentication Server: Datenbank, die Identitäten und Zugangsrichtlinien verwaltet (zum Beispiel Cisco ISE)

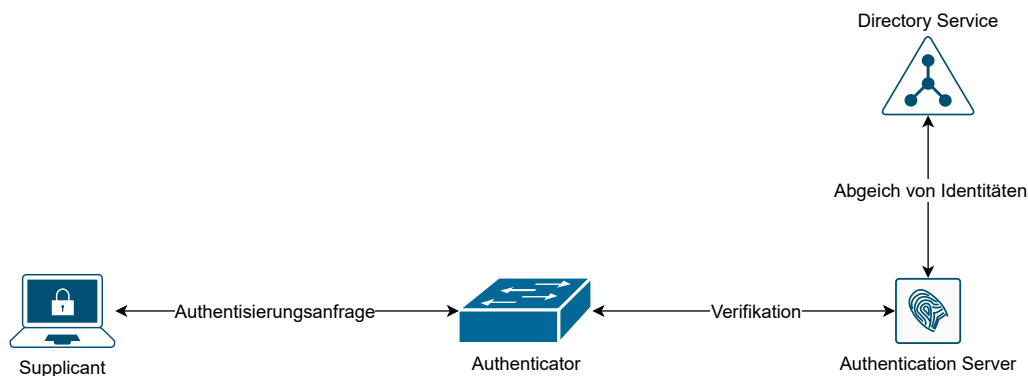


Abbildung 3.7.: Authentifizierung via 802.1X

Ein mittels 802.1X gesichertes Netzwerkgerät (Authenticator) kennt zwei verschiedene Status auf jedem einzelnen Port. Im unautorisierten Status wird jeglicher Netzwerkverkehr blockiert, nur eine Authentifizierung über EAPoL wird akzeptiert.

Vom Authenticator wird die Anfrage des Endgerätes an einen Authentifizierungs-Server weitergeleitet, welcher ein Verzeichnis von bekannten Identitäten führt. Dies kann ein alleinstehender Server sein, oder aber mit verschiedenen bestehenden Verzeichnissen abgeglichen werden, beispielsweise dem Active Directory von Microsoft. [14]

### 3.4. Variante 1 – VLAN-basiert

Die erste vorgeschlagene Variante fokussiert sich ausschliesslich darauf, die aktuell vorhandene Hardwarelandschaft zu vereinfachen, während die Komplexität des Setups möglichst gering gehalten wird. Dies wird erreicht, indem die verschiedenen Netze logisch getrennt auf derselben Leitung geführt werden.

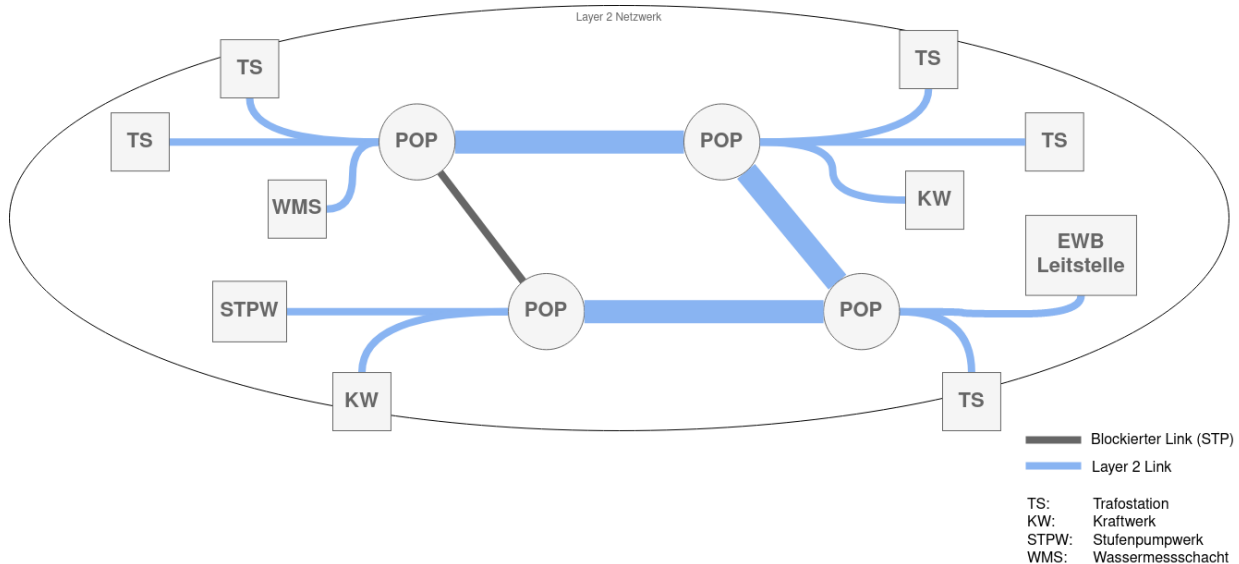


Abbildung 3.8.: Variante VLAN

#### 3.4.1. VLAN – 802.1Q

Der Standard [IEEE 802.1Q](#) (Virtual Local Area Network) [21] beschreibt eine bewährte Technologie zur Kategorisierung bzw. Segmentierung von Netzwerk-Paketen. Er definiert im Ethernet-Header eines Paketes ein zusätzliches Datenfeld, welches unter anderem eine sogenannte VLAN ID beinhaltet. Mithilfe dieses Tags kann jeglicher Netzwerktraffic von Geräten, die den Standard unterstützen, kategorisiert und logisch getrennt werden.

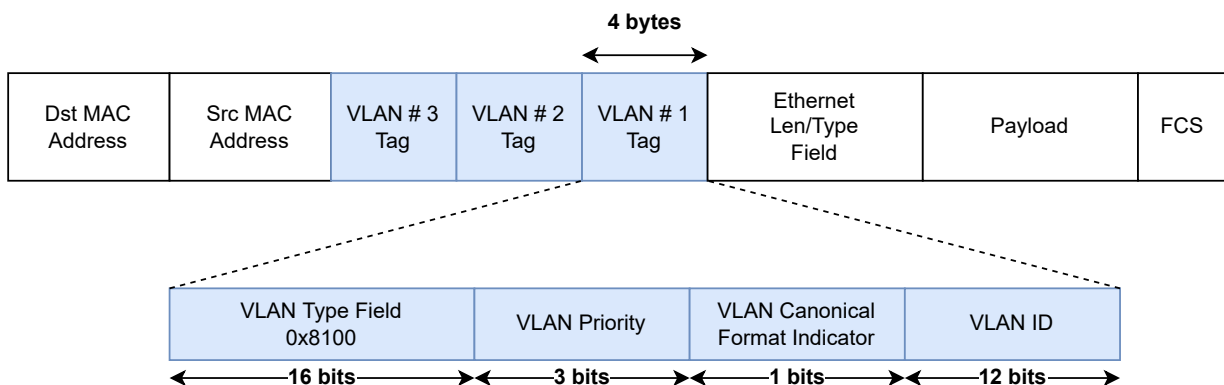


Abbildung 3.9.: VLAN Teil im Ethernet Header

#### 3.4.2. VLAN Tags, Access- und Trunk Ports

Mit dieser Erweiterung des Ethernet-Headers ergeben sich verschiedene Konstellationen, welche die eingesetzten Netzwerkgeräte handhaben müssen.

Kein VLAN Tag (*untagged*) oder "Native VLAN" Tag 1: Diese zwei Varianten werden gleich behandelt. Grundsätzlich sind sämtliche Pakete, welche beim Endgerät ankommen oder von diesem verschickt werden, untagged. Dies aus dem Grund, dass das Endgerät einerseits keine VLAN Tags verstehen muss, andererseits diese auch nicht von einem Angreifer verändert werden können. Ein Switchport, welcher *untagged* Pakete entgegennimmt und diesen einen VLAN Tag hinzufügt, wird als **Access-Port** bezeichnet. Empfängt dieser Pakete, welche bereits einen Tag enthalten, werden sie verworfen.

Ein VLAN Tag zwischen 2 und 4096 bedeutet, der Traffic ist einem entsprechenden virtuellen LAN zugeordnet und wird von einem Switch nur auf denjenigen Ports weitergegeben, welche auch im selben VLAN kommunizieren.

Ein Port, welcher der Kommunikation zwischen zwei Switches dient, muss normalerweise Pakete mit verschiedenen VLAN Tags transportieren. Ein sogenannter **Trunk Port** akzeptiert nur *tagged* Pakete derjenigen VLANs, welche in der Konfiguration explizit erlaubt sind.

### 3.4.3. Spanning Tree

Die erste Designvariante spannt das Netz auf Layer 2 über sämtliche Standorte. Redundante Wege wie der Ring zwischen den vier zentralen POPs führen zu Loops im Netzwerk und müssen zwingend mittels Spanning Tree abgesichert werden.

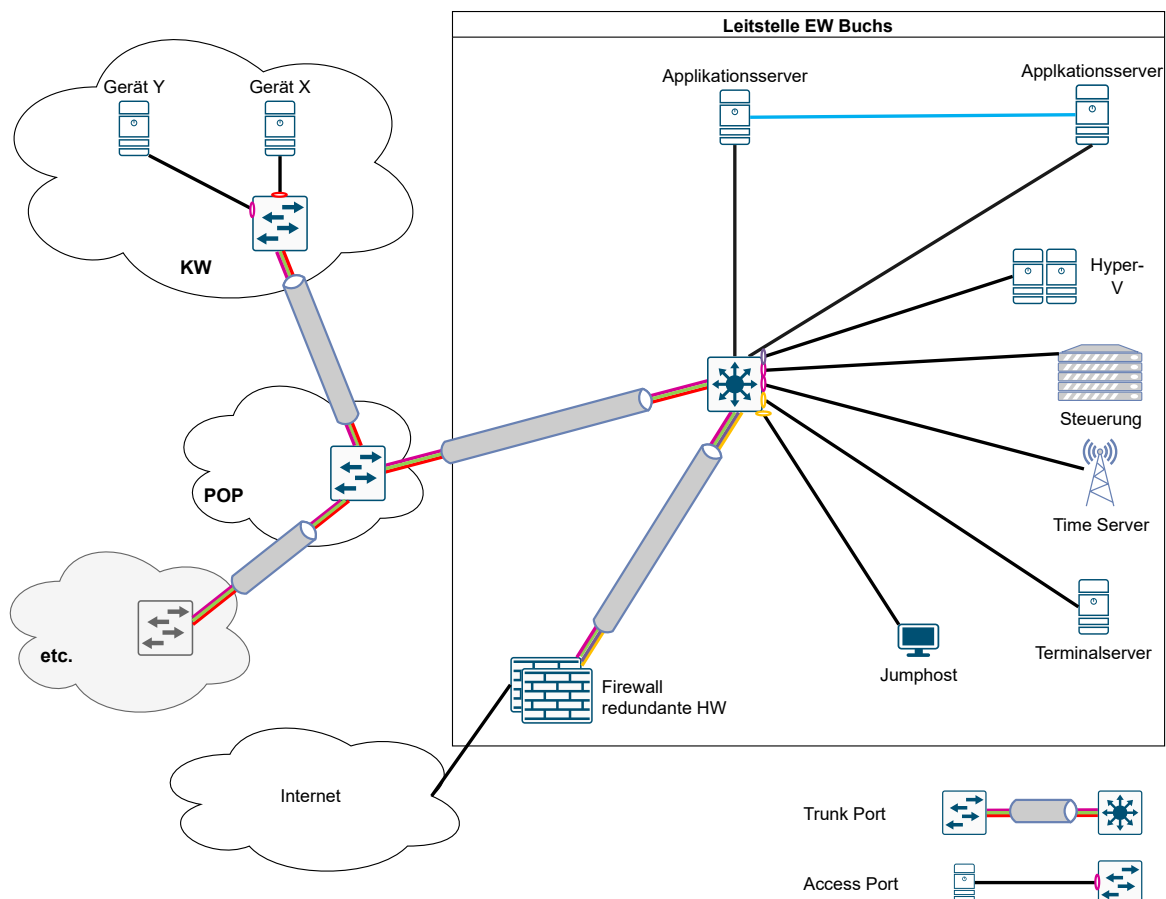


Abbildung 3.10.: Mögliche Architektur mit VLAN

In der gegebenen Netzwerktopologie bietet sich ein Per VLAN Spanning Tree (PVST) Setup an, um

den Ring der vier POPs abzusichern. Damit wird in jedem VLAN ein anderes Gerät als Root Bridge definiert und deshalb ein anderer Link blockiert. Dies verbessert die Auslastung im Netz.

#### **3.4.4. Analyse**

Vorteile:

- Geringe Anforderungen an die Netzwerkgeräte, VLAN und STP wird von jedem in Frage kommenden Gerät unterstützt.
- Bewährte Technologien (20+ Jahre alt)
- Wenig "Überraschungspotenzial"

Nachteile:

- Durchgehend manuelle Konfiguration nötig
- Grosse Layer 2 Netze bedeuteten viel Broadcast Traffic
- Fehler im Netzwerk propagieren durch die gesamte Topologie

### 3.5. Variante 2 – L2 over L3 Ansatz BGP EVPN (MPLS / VXLAN)

Die zweite Variante geht einen Schritt weiter als Variante 1. Die vorhandene Hardwarelandschaft wird nicht nur vereinfacht, sondern auch optimiert genutzt. Das ist möglich, indem wir die Verbindungen zwischen den Core Switches mit Layer 3 herstellen und die bisherigen Layer 2 Netzwerke darüber als virtuellen Overlay aufbauen, basierend auf [RFC 8365](#) [27, 19].

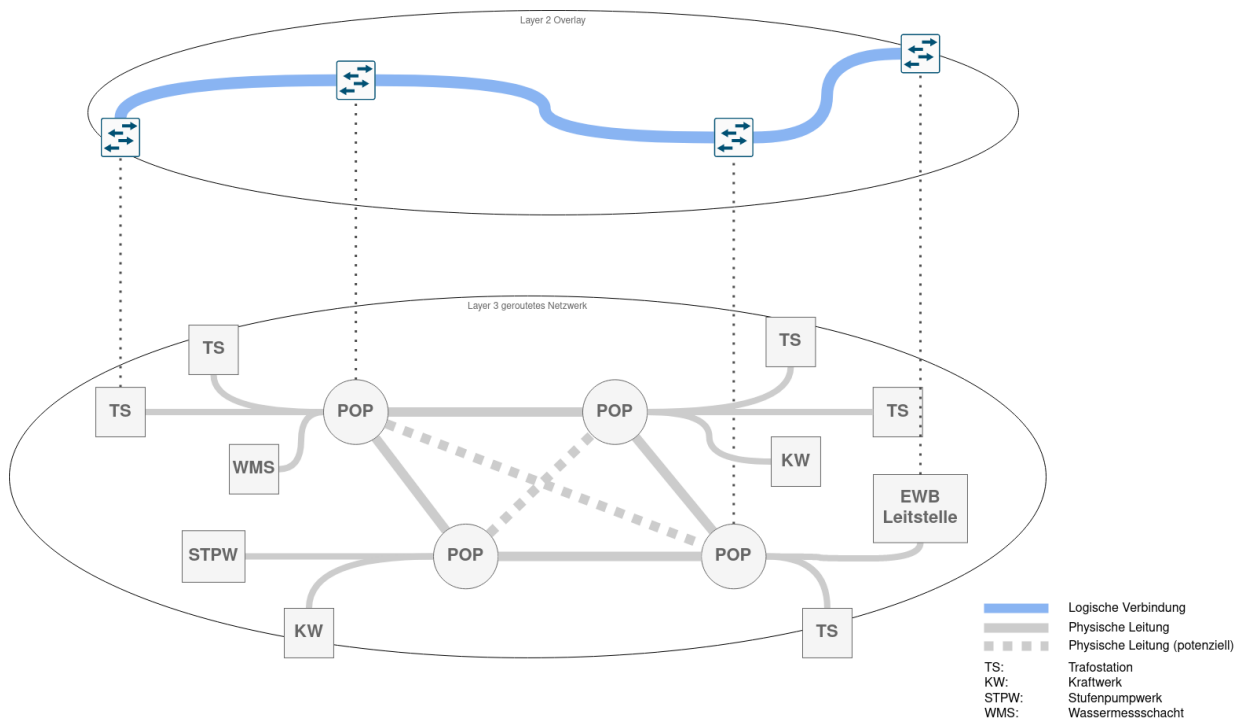


Abbildung 3.11.: Variante BGP EVPN

Dazu werden verschiedene Protokolle benötigt, die im Folgenden kurz erklärt werden.

#### 3.5.1. Data Plane Protokolle

Damit die Layer 2 Informationen nicht verloren gehen wenn der Netzwerkverkehr über ein Layer 3 Netz geschickt wird, benötigt es ein Protokoll, welches diese Informationen enkapsuliert und am Zielort wieder dekapuliert. Dazu kommen zwei Protokolle in Frage, MPLS oder VXLAN.

#### 3.5.2. MPLS

Multiprotocol Label Switching (MPLS), als erste Variante, wird definiert in [RFC 3031](#) [26]. MPLS ist ein Enkapsulierungsprotokoll, welches häufig von Internet Service Providern eingesetzt wird, um ihren Kunden eine virtuelle Layer 2 oder 3 Verbindung zwischen zwei Standorten zu ermöglichen.

Begriffe:

- P-Router    Provider MPLS Core Router
- PE-Router    Provider Edge Router, Provider Endpunkte der Layer 2 Tunnels
- CE-Router    Customer Edge Router, Kunden Endpunkte, Sender und Empfänger des Layer 2 Datenverkehrs

Den Datenpaketen eines Kundennetzwerks werden vor dem ursprünglichen Header eines oder mehrere Labels hinzugefügt. Anhand dieser Label wird das Paket durch das Provider-Netzwerk vom PE über einen oder beliebig viele P-Router zum Ziel-PE gesendet. Die Labels werden unterwegs von den Provider-Routern wieder entfernt, sodass das Paket beim Kundennetzwerk wieder seine ursprüngliche Form hat. Somit verhält sich das Netzwerk auf Kundenseite, als wären die beiden CE-Router direkt miteinander verbunden.

Dieses Routing innerhalb des Provider Netzes basiert dabei auf einem gängigen IGP.

Bei MPLS geschieht MAC Learning auf den PE Routern genauso wie auch auf Switches bei normaler Layer 2 Kommunikation.

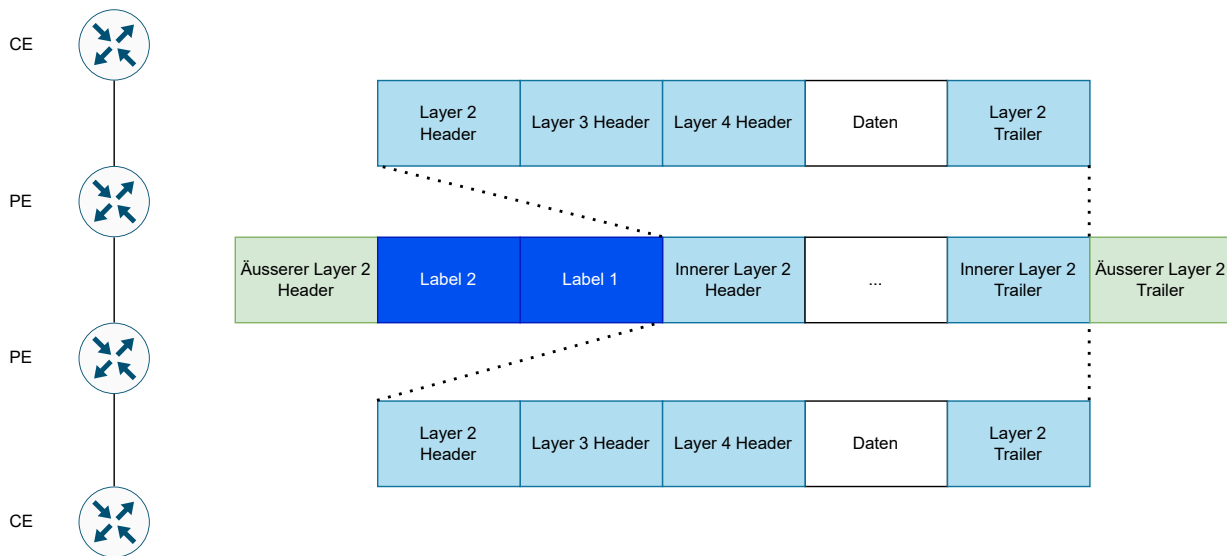


Abbildung 3.12.: MPLS Encapsulierung

### 3.5.3. VXLAN

Die Alternative Virtual eXtensible LAN (VXLAN, [RFC 7348](#) [24]) wird häufig innerhalb oder zum Verbinden von Rechenzentren eingesetzt, um Layer 2 Kommunikation über Layer 3 Netzwerke zu ermöglichen.

Begriffe:

VTEP Virtual Tunnel Endpoint, ein Switch der den VXLAN Tunnel terminiert

VNI VXLAN Network Identifier

VXLAN verpackt das ganze Ethernet Frame als Daten in ein weiteres Netzwerkpaket (UDP auf Layer 4) und erlaubt so, das Layer 2 Paket über ein Layer 3 Netz zu senden. Dadurch ist es auch möglich, Daten über Router zu senden, die keine VXLAN Funktionalität besitzen. Dies im Gegensatz zu MPLS, bei dem alle Router zwischen den Endpunkten das Protokoll verstehen müssen.

Ein Virtual Tunnel Endpoint (VTEP) kann man mit Provider Edge Routern bei MPLS vergleichen; sie sind zuständig für die Encapsulierung und Dekapsulierung der Layer 2 Pakete.

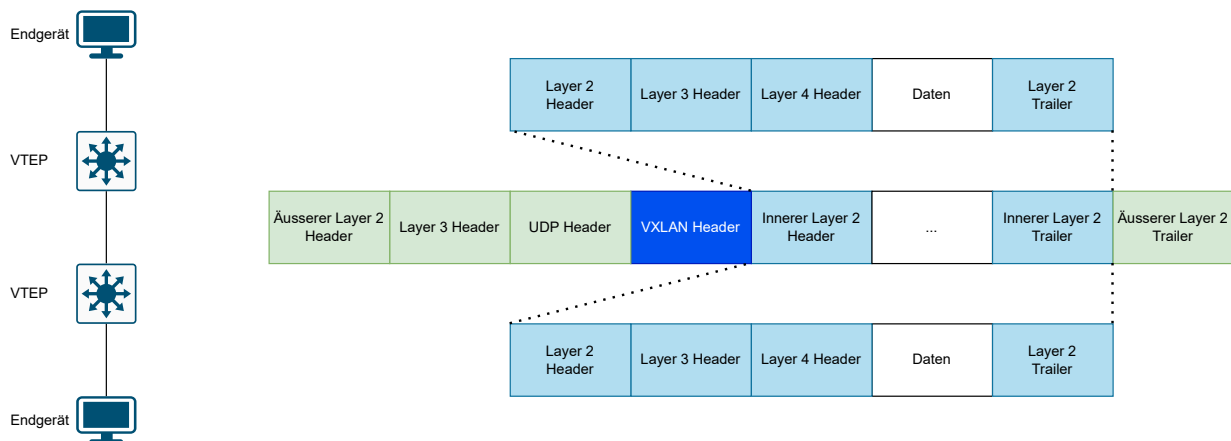


Abbildung 3.13.: VXLAN Encapsulierung

Bei VXLAN geschieht MAC Learning auf den VTEPs genauso wie auch auf Switches bei normaler Layer 2 Kommunikation.

### 3.5.4. Control Plane Protokoll

Layer 2 Kommunikation über ein Layer 3 Netz wird durch die Data Plane Protokolle gewährleistet, jedoch geschieht dies noch nicht optimal. Wenn ein Paket bei einem Tunnelendpunkt eintrifft, müsste dieses an alle anderen Tunnelendpunkte weitergeleitet werden damit sichergestellt ist, dass das Paket beim Empfänger auch ankommt. Wie man sich vorstellen kann, skaliert dies sehr schlecht.

Dieses Problem kann gelöst werden, indem eine Control Plane die Zuordnung der MAC Adresse zu Tunnelendpunkt übernimmt und diese Informationen an die Endpunkte verteilt. Der nächste Abschnitt beschreibt ein solches Control Plane Protokoll.

### BGP EVPN

Das Border Gateway Protocol (BGP, RFC 4271) [25] ist ein Routing Protokoll, welches erlaubt, IPv4 Routing Informationen zwischen zwei Endpunkten auszutauschen.

Eine Erweiterung davon ist Multiprotocol BGP (MP-BGP, RFC 4760) [2]. Dies bildet die Basis dafür, dass auch andere Typen von Adressen (Adressfamilien) über BGP ausgetauscht werden können. BGP Ethernet Virtual Private Network (EVPN, RFC 7432) [1] ist nun eine solcher Adresstyp, welcher es erlaubt, MAC Adressen oder MAC + IP Adresskombinationen effizient zwischen mehreren VTEPs oder MPLS PE Routern auszutauschen.

Das bedeutet, dass mittels EVPN eine Control Plane für VXLAN oder MPLS geschaffen werden kann. Die Endpunkt MAC und IP Adressen werden auf den VTEPs bei VXLAN oder PEs bei MPLS gelernt, bevor sie dann via EVPN an die jeweils anderen VTEPs/PEs verteilt werden.

EVPN bietet folgende Vorteile gegenüber Ansätzen nur mit MPLS / VXLAN:

- Bessere Skalierbarkeit: BGP bildet auch die Grundlage des gesamten Routings im Internet
- Einfacheres Deployment
- Mehrfach aktive Verbindung zwischen Tunnelendpunkt und Endgerät
- Lastverteilung (Load Balancing)
- Bessere Mobilität von Geräten zwischen Standorten

### **3.5.5. Analyse**

Vorteile:

- Layer 3 Design als Underlay bedeutet keine blockierten Links durch Spanning Tree
- Verbindung nach Netzwerkunterbrüchen kann schneller wiederhergestellt werden.
- Reduktion des Datenverkehrs insgesamt durch weniger Broadcast Traffic

Nachteile:

- Tiefe Kenntnis komplexer Protokolle nötig für Betrieb
- Konfiguration manuell auf jedem Switch nötig bei Änderungen
- Anforderungen an Switchhardware, müssen sämtliche benötigten Protokolle unterstützen (MPLS)



### 3.6. Variante 3 – Cisco Software Defined Access

Cisco Software Defined Access ist eine Applikation, die Teil der Cisco Digital Network Architecture (DNA) Software Suite ist. Zur Zeit kann diese Software nur auf einer dezidierten Appliance von Cisco betrieben werden, in Zukunft soll es jedoch auch möglich sein, dies in einer virtuellen Maschine zu installieren.

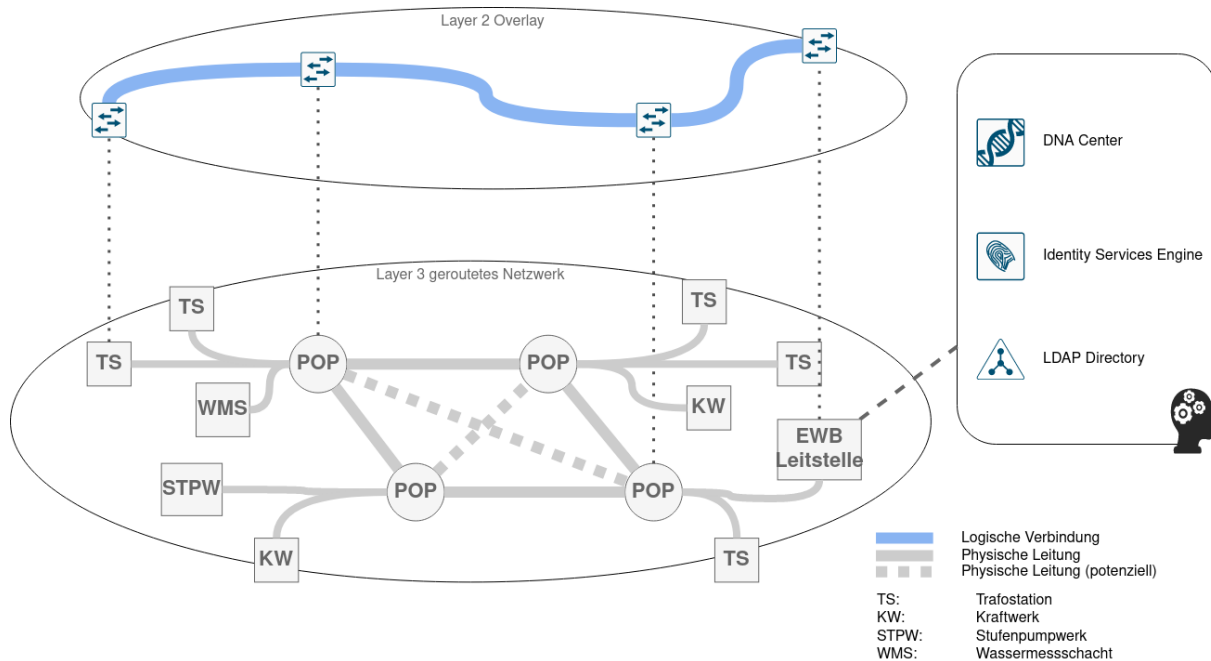


Abbildung 3.14.: Variante Software Defined Access

#### 3.6.1. Grundlagen Software Defined Networking

Traditionelle Netzwerkdesigns basieren darauf, dass jedes eingesetzte Gerät eine gewisse Intelligenz besitzt, und in Kommunikation mit anderen gleichartigen Geräten eine Gesamtsicht auf die Topologie erhält. Entscheidungen werden von jedem Gerät basierend auf diesen Informationen getroffen. Dabei wird klassisch zwischen der Control Plane und der Data Plane unterschieden.

Während die Control Plane für das Sammeln der Daten und fällen der Entscheidungen zuständig ist, beispielsweise welcher der möglichen Wege von A nach B der schnellste ist, kümmert sich die Data Plane um das effektive Weiterleiten von Paketen nach Vorgaben der Control Plane. Klassisch geschieht beides auf jedem Netzwerkgerät separat.

Im Software Defined Networking wird die Control Plane von der Data Plane getrennt und auf einem zentralen Controller betrieben. Dieser kommuniziert direkt mit den Geräten im Netzwerk, die selber keine Berechnungen mehr ausführen müssen, sondern alle nötigen Informationen vom Controller erhalten.

Dieser strikte Ansatz der Trennung wird im offenen Standard OpenFlow beschrieben. Damit wird im Netzwerk nur noch sehr einfache Hardware verwendet, die keine Logik mehr ausführt. Viele Hersteller setzen aber auf einen Kompromiss. Die eingesetzten Geräte besitzen eine gewisse Logik, um die Kommunikation im gesamten Netz herzustellen. Auf diesem Underlay Netzwerk kommuniziert jedes Gerät mit dem Controller und erhält von ihm gewisse Konfigurationen. Somit kann erweiterte Funktionalität zur Verfügung gestellt, welche in herkömmlichen Netzwerken mit verteilter Intelligenz nicht möglich wäre. [16, 17, 19]

### 3.6.2. Cisco DNA

Die von Cisco angebotene DNA Software bietet folgende Funktionalität [7]:

- **Automation**  
Ein automatisiertes Deployment von neuen Geräten bedeutet in jedem Fall konsistente Konfigurationen. Dies reduziert die Fehleranfälligkeit von sich wiederholenden Einrichtungsaufgaben. Ebenfalls kann die Zeit zur Einrichtung von einzelnen oder mehreren Geräten stark reduziert werden.
- **Policy und Segmentierung, Identifikation**  
Automatisierte Netzwerksegmentierung, Zugriffsrichtlinien basierend auf ganzen Netzen oder einzelnen User- bzw. Gerätegruppen. Herkömmliche Lösungen wie VLANs oder auch VRFs (Virtual Routing and Forwarding, Logische Segmentierung auf Layer 3) sind entweder komplex und sehr schnell aufwändig in der Konfiguration, oder bieten nicht die Möglichkeit, detaillierte Anforderungen des Unternehmens abzubilden. Statische Mappings von Zugriffsrechten auf Ebene von Switchports bedeuten wenig Flexibilität und wieder manuelle Konfiguration, wenn ein Gerät den Standort wechselt.
- **Assurance**  
Sammlung, Überwachung und Analyse von Informationen aus dem gesamten Netz, trägt zur einfacheren Problembekämpfung und Kapazitätsplanung bei.
- **Integration**  
Programmierbare Schnittstellen (API) zur Anbindung von Drittanbieter-Lösungen
- Hochverfügbarkeit: Hard- und Softwareseitig
- Backup und Restore Mechanismus
- RBAC: Rollenbasiertes Berechtigungskonzept

#### **Control Plane: Locator/ID Separation Protocol (LISP)**

In herkömmlichen Netzwerken definiert die IP Adresse eines Endpunktes die Identität sowie auch den Standort eines Gerätes im Netzwerk.

Mit LISP können diese beiden Aspekte voneinander getrennt werden, indem für jedes Gerät eine Zuordnung zwischen der *Identität des Endpunktes (EID)* und dem *Routing Locator (RLOC)* gemacht wird. Der Routing Locator beschreibt den Fabric Edge Node, an welchem das Endgerät verbunden ist.

Damit ist es möglich, dasselbe Layer 2 Netzwerk an verschiedenen Endpunkten eines Layer 3 Underlay verfügbar zu machen.

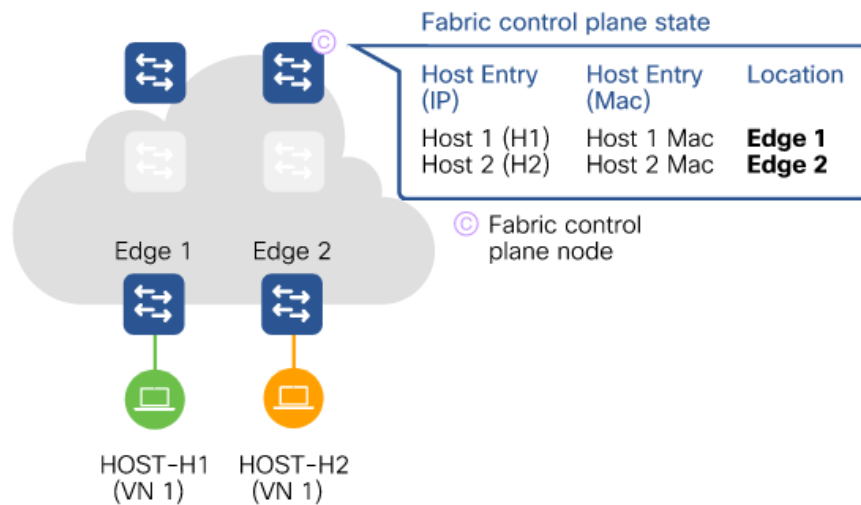


Abbildung 3.15.: Cisco SDA Fabric Control Plane [19]

### Data Plane: VXLAN

Mittels VXLAN werden Ethernet-Frames enkapsuliert und über die Netzwerk-Fabric verschickt. Fabric Edge Nodes übernehmen die En- sowie Dekapsulierung.

### Policy Plane: Cisco TrustSec mit Secure Group Tag SGT

In traditionellen Netzwerkarchitekturen sind die Berechtigungen von Personen bzw. Geräten an Informationen wie IP Adresse oder VLAN gebunden. Dies bewirkt, dass dasselbe Layer 2 Netz über verschiedene Standorte hinweg verteilt wird, damit die Zugangsrechte dieselben sind. Die Markierung von Traffic mittels Secure Group Tag (im VXLAN Header integriert) erlaubt einerseits die granulare Verwaltung von Gerätegruppen innerhalb derselben logischen Netze, andererseits auch die Entkopplung von Berechtigung und IP Adresse, da die Entscheidung Zugriff / kein Zugriff neu basierend auf dem Secure Group Tag gefällt wird.

Beispiel: Gruppe A darf mit Gruppe B kommunizieren, aber nicht mit Gruppe C oder anderen Geräten der Gruppe A.

### Management Plane: DNA Center

Mittels DNA Center kann ein Netzwerk auf einer zentralen Plattform Ende-zu-Ende konfiguriert und automatisiert werden. Als Netzwerkadministrator kann auf einem einzigen Dashboard das gesamte Management durchgeführt werden. Mittels Workflows können Anforderungen abgebildet und nach Vorgaben auf Devices ausgerollt werden. Gleichzeitig bietet die Plattform Monitoring-Informationen der Geräte und bietet somit Kontrolle über die gesamte Netzwerkinfrastruktur und deren Policies, sowie Unterstützung bei der Fehlersuche.

### 3.6.3. Authentifizierung: Identity Services Engine

Die Cisco Identity Services Engine (ISE) stellt einen Authentifizierungsserver dar und ermöglicht damit die Verwendung von 802.1X. Die ISE ist für die Verwaltung von Usern und Devices sowie den Zugriffsrichtlinien zuständig. Sie lässt sich mit verschiedensten Identity Providern wie beispielsweise dem Microsoft Active Directory verbinden, um die bestehenden Informationen abzuholen und darauf basierend Geräte zu authentifizieren.

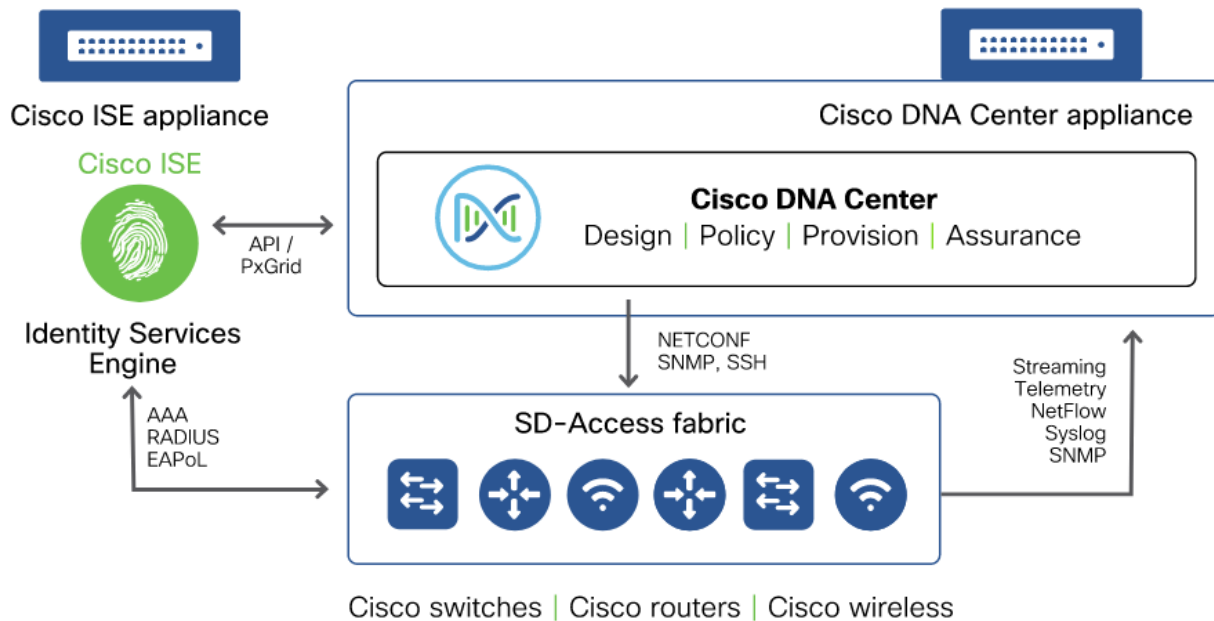


Abbildung 3.16.: Cisco DNA Center Schnittstellen [19]

### 3.6.4. Software Defined Access

Die Trennung vom physikalischen Underlay Netzwerk und der logischen Schicht des Overlays erlaubt es, die Anforderungen des Betriebs unabhängig von physikalischen Einheiten wie Ports, Subnetzen oder Access Control Lists umzusetzen. Änderungen an den Zugriffsrichtlinien haben keine direkte Auswirkung mehr auf die Physik, sondern werden via DNA Center rein in Software abgebildet.

Cisco Software Defined Access sieht die folgenden Geräterollen vor:

- **Control Plane Nodes**  
 Dienen als zentrale Datenbank der Fabric und somit als Vermittler zwischen Over- und Underlay. Hauptfunktion der Fabric Control Plane ist die Zuordnung von Endgeräten, die im Overlay Netz verbunden sind, auf Fabric Edge Nodes, welche den Übergabepunkt von der Fabric zum traditionellen Netz darstellen.
- **Intermediate Nodes**  
 Stellen die Layer 3 Konnektivität innerhalb der Fabric her. Kennen nur das Underlay Netzwerk und arbeiten strikt nach Routing Protokoll.
- **Border Nodes**  
 Verbinden die SD-Access Fabric mit traditionellen Layer 2 oder Layer 3 Netzwerken ausserhalb, beispielsweise dem Internet oder anderen Standorten.
- **Edge Nodes**  
 Stellen den Verbindungspunkt von Endgeräten mit der Fabric dar. Sie führen Einkapsulierung und Dekapsulierung von Traffic durch und implementieren die Sicherheitsrichtlinien.
- **Extended / Policy Extended Nodes**  
 Erlauben die Erweiterung der SDA Fabric über kleinere, via Layer 2 verbundene Switches. Zugangsrichtlinien werden an den Edge Nodes durchgesetzt. Beispiele dazu sind industrielle Switches die an Aussenstandorten eingesetzt werden und wenige Geräte mit der Fabric verbinden.

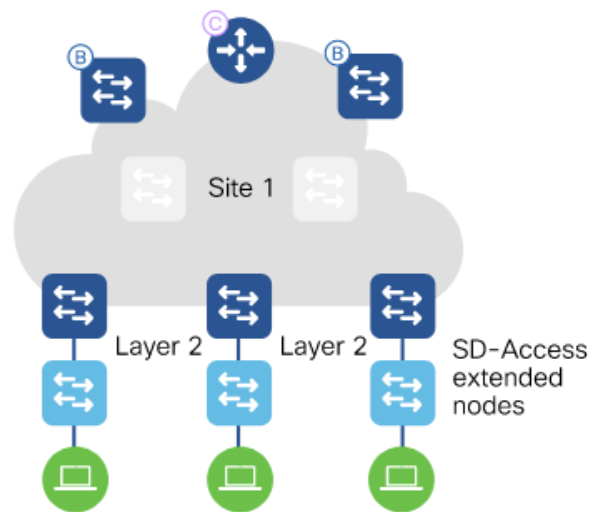


Abbildung 3.17.: Cisco SDA Fabric mit Extended Nodes [19]

### 3.6.5. Segmentierung

Das DNA Center ermöglicht die Aufteilung der Netzwerke in einer groberen Form (Makrosegmentierung) und zusätzlich in eine feingranulare Form (Mikrosegmentierung).

#### Makrosegmentierung: Virtuelle Netzwerke

Alle Geräte, welche miteinander kommunizieren müssen, sollten im selben virtuellen Netzwerk (VN) sein. Über die Grenzen der VNs hinaus kann nur via einer Firewall oder einem Router ausserhalb der Fabric kommuniziert werden. Die Separierung durch Virtuelle Netzwerke entspricht im traditionellen Netzwerkdesign der Trennung zwischen verschiedenen virtuellen Routing Domains (VRFs).

Diese Funktionalität wird von jedem Fabric Extended Node unterstützt.

#### Mikrosegmentierung: Secure Group Tag

Die Segmentierung mit Secure Group Tag (SGT) erlaubt es, einfache gruppenbasierte Richtlinien zu erstellen und unterstützt somit granulare Isolation auf der Data Plane zwischen einzelnen Endgeräte-Gruppen.

Diese erstellen Gruppen gelten innerhalb von einzelnen Virtuellen Netzen. Mit einer Matrix-Darstellung kann dabei definiert werden, welche Gruppen untereinander und gleichfalls ob die Geräte innerhalb der Gruppe miteinander kommunizieren dürfen.

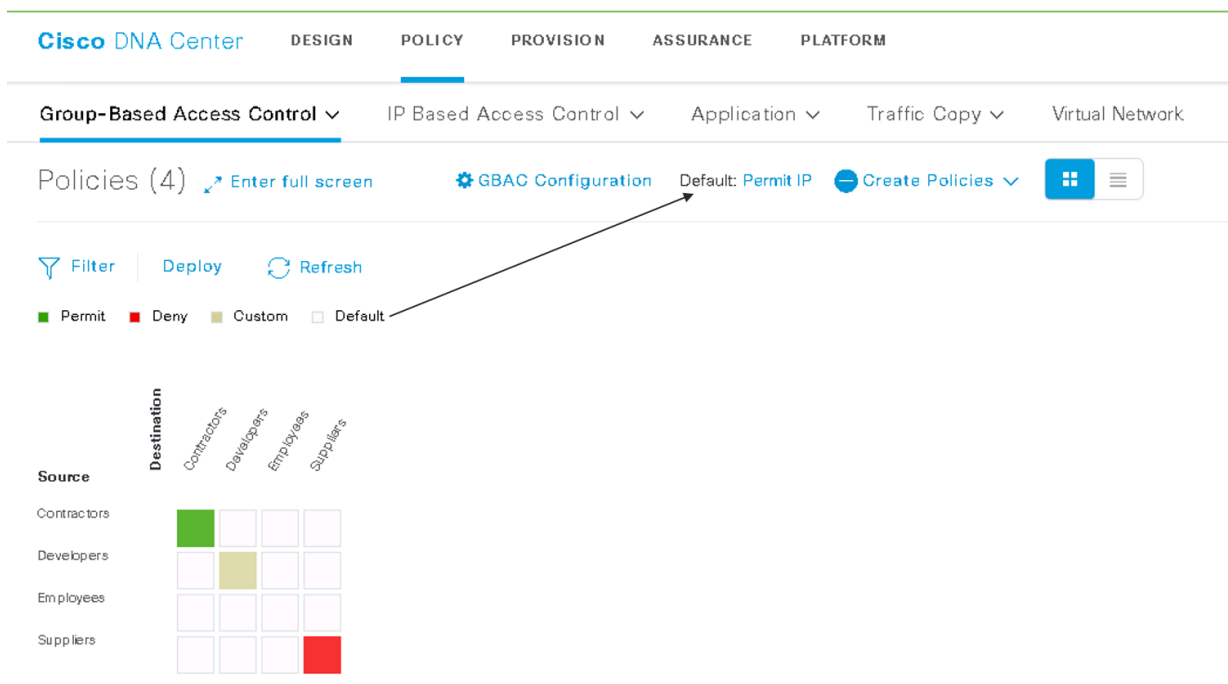


Abbildung 3.18.: SGT Matrix [23]

Die Anwendung von SGT ist nur mit Geräten möglich, die die Rolle eines Policy Extended Node ausführen können.

### Extended Node vs. Policy Extended Node

Cisco SDA unterscheidet für Anwendungsfälle wie Industrie- oder IoT Switches zwischen zwei verschiedenen Rollen. [29]

Ein Extended Node (IE3300 Geräteserie) unterstützt eine Segmentierung lediglich mittels Virtuellen Netzwerken. Der Switch verbindet sich zum Fabric Edge Gerät mit einem Layer 2 VLAN Trunk, welcher automatisch auf die verschiedenen VN gemappt wird. Secure Group Tags werden den Paketen erst am Fabric Edge hinzugefügt, was bedeutet, dass ein Policy Enforcement nur machbar ist, wenn Geräte über verschiedene Fabric Edges verbunden sind. Nicht möglich ist die Mikrosegmentierung unter Geräten am selben Extended Node, denn hier bewegt man sich in einem reinen Layer 2 Netzwerk.

Um die volle Funktionalität von Secure Group Tags zu ermöglichen, muss das Gerät mindestens ein Policy Extended Node sein (ab IE3400 Geräteserie). Diese Geräte sind in der Lage, den eingehenden Traffic direkt mit SGTs zu taggen und ermöglichen somit die volle Funktionalität der Mikrosegmentierung. [6]

Im Bereich Authentisierung mit 802.1X gibt es ebenfalls Unterschiede in der Funktionalität. Während ein Extended Node nur sich selber beim Identity Server authentisieren kann, ermöglicht ein Policy Extended Node jedem einzelnen Endgerät die Verwendung von 802.1X.

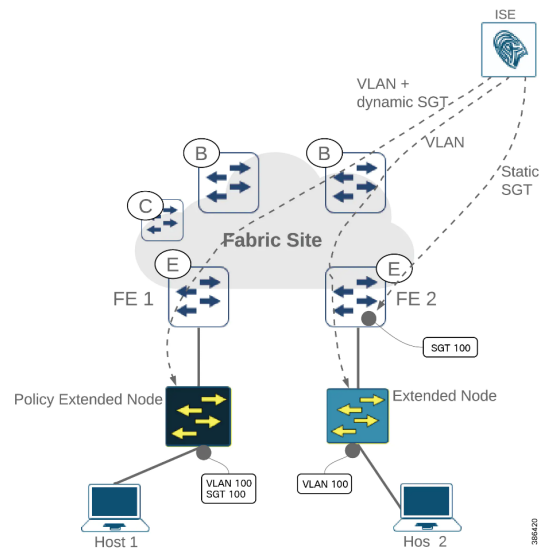


Abbildung 3.19.: Extended Node vs Policy Extended Node [6]

### 3.6.6. Netzwerkdesign EWB

Für eine Umsetzung von Cisco Software Defined Access im Rahmen der gegebenen Anforderungen schlagen wir das nachfolgende Design vor. Der Einfachheit halber werden in den Aussenstandorten jeweils Extended Nodes erwähnt. Die Entscheidung, ob allenfalls Policy Extended Nodes eingesetzt werden, liegt beim EWB.

#### Design Schritt 1

Dieses beschreibt in einem ersten Ausbauschnitt nur die Anforderungen der Infrastruktur, erlaubt aber einen späteren Ausbau zur gemeinsamen Nutzung der DNA Center Funktionalität mit der internen IT und deren Anwendungsfällen.

Die zentralen Elemente der Fabric (Control Plane Switches, DNA Center, ISE) befinden sich in der Leitstelle im EWB Bürogebäude. Ebenso ein DHCP Server, der zur Inbetriebnahme der Extended Nodes benötigt wird. Das Bürogebäude ist mit zwei verschiedenen Fasern an den FTTx Ring angeschlossen.

In den POPs befindet sich die effektive Fabric mit vier Fabric Edge Geräten, welche die Verbindungen zu allen Extended Nodes an den Aussenstandorten aggregieren.

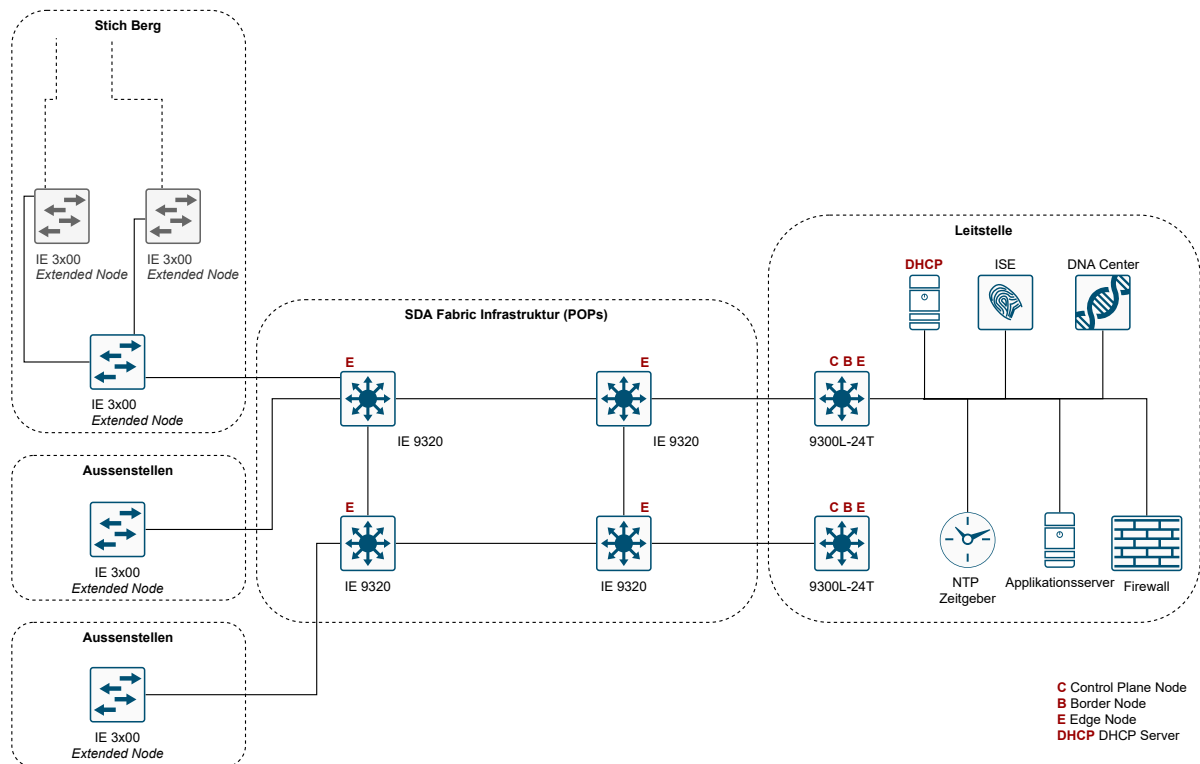


Abbildung 3.20.: Cisco SDA Ausbau Schritt 1

### Geräteauswahl

Folgende Geräte und Stückzahlen werden für das minimale Setup verwendet. Die Anzahl Extended Nodes stellt einen ungefähren Wert nach Anzahl Standorten dar und kann je nach örtlicher Situation leicht variieren.

Rolle	Standort	Anforderung	Modell	Anzahl
Control Plane	EWB Leitstelle	Control Plane Funktionalität	Catalyst 9300L-24T	2
Fabric Edge	POP Standorte	Hohe SFP Portanzahl	Catalyst IE9320	4
Extended Nodes	Aussenstellen	Kleiner Formfaktor, Hut-schienenmontage, variable Portanzahl	IE3300 / IE3400	ca. 70

### Design Schritt 2

In Schritt 2 können die beiden Rechencenter-Standorte der EWB Informatik zur Erhöhung der Redundanz sowie Verfügbarkeit im Core Bereich der Fabric genutzt werden. Die bestehenden Core Switches der IT sollen in absehbarer Zeit ersetzt werden, dabei kann ein Umbau der eigenen Infrastruktur in Richtung Cisco SDA in Betracht gezogen werden.



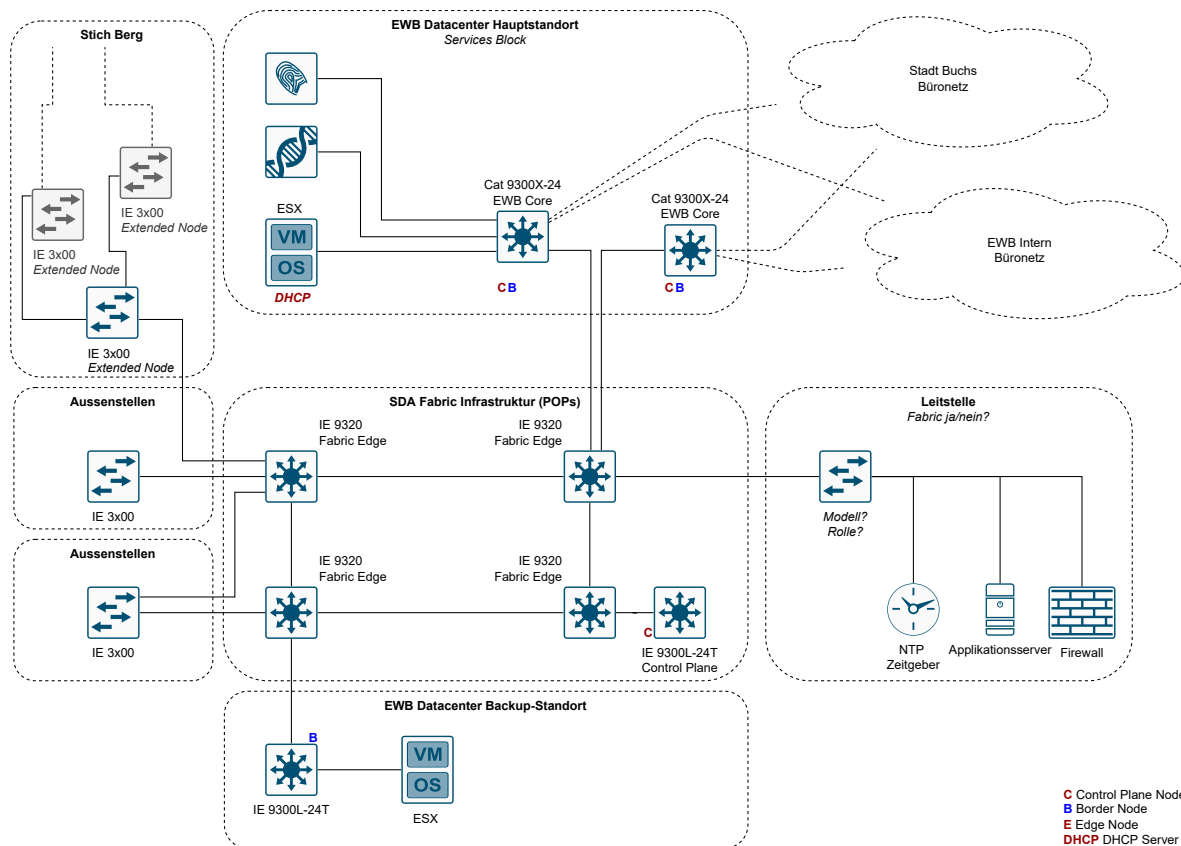


Abbildung 3.21.: Cisco SDA Ausbau Schritt 2

### 3.6.7. Analyse

Vorteile:

- Automatisierung in Deployment und Konfigurationen von Geräten
- Einfache Konfiguration von neuen Anforderungen
- Unterstützung bei Troubleshooting durch Datenauswertung
- Einfache Implementation von Security Features mit Cisco ISE
- Mögliche Erweiterung auf andere Netze, gemeinsame Nutzung mit EWB Informatik

Nachteile:

- Wiederkehrende Lizenzkosten für Cisco DNA Center, pro Switch
- Anforderungen an Switchhardware, müssen Fabric Funktionalität unterstützen

### 3.7. Variantenvergleich

Sämtliche Punkte sind 'je tiefer desto besser' zu lesen.

<b>Kriterien</b>	<b>Variante 1: VLAN</b>	<b>Variante 2: MP-BGP EVPN</b>	<b>Variante 3: Cisco SDA</b>
Einmalige Kosten	1	2	3
Wiederkehrende Kosten	0	0	3
Einrichtungsaufwand	3	5	4
Aufwand für Betrieb	3	5	2
Feature-Umfang	3	2	0
Erweiterbarkeit	3	3	0
<b>Summe</b>	<b>13</b>	<b>17</b>	<b>12</b>

## 4. Aufbau Proof of Concept

Dieses Kapitel bildet eine Dokumentation des Proof of Concept, welchen wir im Lab in Rapperswil aufgebaut haben. Da sich diese Dokumentation später als Anleitung an die EWB Informatik richtet, sind die fachspezifischen Begriffe jeweils auf Englisch erwähnt.

Dieser Proof of Concept fokussiert sich aufgrund der Resultate aus der Design-Analyse ausschliesslich auf Cisco Software Defined Access mit DNA Center. Ausgenommen ist dabei die Konfiguration der Cisco Identity Services Engine ISE, da kein Testgerät verfügbar ist.

Bei Variante 1 mit VLAN handelt es sich um bewährte Technologie, die von der EWB Informatik aktuell umgesetzt und betrieben wird.

Aufgrund der Ergebnisse der Vergleichstabelle in Kapitel 3.7 verzichten wir ebenfalls auf einen PoC der Variante 2 BGP EVPN. Diese Variante stellt einen verhältnismässig grossen Aufwand in Umsetzung und Betrieb für die EWB Informatik dar, während der Nutzen gegenüber Cisco SDA klar kleiner ist.

Zur Verfügung stehen uns folgende Netzwerkgeräte aus dem Bestand des INS:

- Cisco DNA Center Appliance (1st Generation)
- Cisco Catalyst 9300 Switches (4x)

Von Cisco zur Verfügung gestellt (Patrick Mosimann):

- Cisco IE3300 Switch (1x)
- Cisco IE3400 Switch (1x)

Die Schritte zur Umsetzung planen wir wie folgt:

- Setup Cisco DNA Center, Update auf neuste Version
- Reset und Grundinstallation der Catalyst Switches
- Basiskonfiguration zum Aufbau einer Netzwerk Fabric

Für die Vorbereitung der DNA Center Appliance und der Switches beziehen wir uns auf die [Installationsanleitungen](#) [5] von Cisco. Alle folgenden Anleitungen beziehen sich auf Version: 2.3.3.5-70134 des DNA Centers.

Eine Übersicht aller Dokumentationen vom DNA Center findet sich hier: [Documentation Overview](#) [4]

### 4.1. Planung des Deployment

Für die Planung ist es wichtig zu wissen, was für Netzwerkinterfaces das DNA Center besitzt und was deren Funktion ist. Folgend findet sich zuerst eine Erklärung zu den Interfaces und Subnets, die für die IP Konfiguration benötigt werden. Weiter Informationen findet man im [Plan the Deployment](#)[5] Kapitel der offiziellen Anleitung.

## DNA Appliance Netzwerkinterfaces

Die DNA Appliance besitzt insgesamt fünf Netzwerkinterfaces:

- Management: Dient dem Zugriff aufs Web Interface zwecks Management.
- Cluster: Dient der Kommunikation innerhalb eines DNA Center Clusters. Muss auch im Standalone Modus konfiguriert werden, und kann später nicht mehr geändert werden, ohne die Appliance neu zu installieren. Der Link Status muss Up sein, damit die Installation funktioniert.
- Enterprise: IP Optional. Dient der Kommunikation der DNA Appliance mit den Netzwerkkomponenten, die verwaltet werden sollen, sofern dies nicht via Management Interface möglich ist.
- Cloud: IP Optional. Kann zur Internetverbindung verwendet werden, nur falls diese nicht via Enterprise Port gegeben ist.
- Cisco Integrated Management Controller (CIMC): IP Optional aber wichtig. Erlaubt Integrated Management Controller Zugriff.

## Cluster Virtual IP

Eine Cluster Virtual IP Adresse muss nicht definiert werden, wenn eine Standalone Appliance eingesetzt wird, die auch später nicht in einen Cluster überführt werden soll. Dies ist im Rahmen des PoC-Setup nicht der Fall, müsste aber bei einer produktiven Implementation allenfalls beachtet werden.

## Intern verwendete Netzwerkbereiche

Container Subnet: reserviert für die Kommunikation zwischen DNA Center internen Applikations-Services (Assurance, Webfrontend, etc.). Cluster Subnet: reserviert für die Kommunikation zwischen DNA Center internen Infrastruktur-Services (db, message bus etc.).

Die Subnetze müssen mindestens 21 Bit gross sein, und zwingend aus IETF RFC 1918 Ranges, RFC 6598 Range oder RFC 3927 Range sein. Standardmässig und empfohlen sind die IP Ranges aus dem RFC 3927 Range.

Container Subnet: Standardmässig und empfohlen auf 169.254.32.0/20 Cluster Subnet: Standardmässig und empfohlen auf 169.254.48.0/20

### 4.1.1. IP Konfiguration

Für ein Pilot genügt es nur das CIMC und Management Interface zu konfigurieren, wir empfehlen jedoch das Enterprise Interface ebenfalls zu verwenden.

Verwendungszweck	Adresse/Subnetz
Cisco Integrated Management Controller (CIMC)	10.6.0.10/24
Management Interface	10.6.10.10/24
Management Default Gateway	10.6.10.1
Enterprise Interface	Nicht verwendet
Cluster Interface	Nicht verwendet
Container Subnet	10.7.64.0/21
Cluster Subnet	10.7.72.0/21
NTP Server	ch.pool1.ntp.org
DNS Server	8.8.8.8

### 4.1.2. Zugangsdaten

Für öffentliche Version entfernt.

## 4.2. Installation der Appliance

Die physische Installation der Appliance kann nach der Anleitung von Cisco durchgeführt werden: [Install the Appliance](#) [5]

## 4.3. Vorbereiten der Appliance für die Konfiguration

Als ersten Schritt konfiguriert man den Cisco Integrated Management Controller CIMC. Dieser ermöglicht ein Out-of-Band Management der Appliance ähnlich wie bei HP Servern das Integrated Lights-Out (iLo). Das bedeutet, dass man via des Webinterfaces des CIMC Zugriff auf folgende Funktionalität hat:

- Appliance Power Management (Einschalten, ausschalten, etc.)
- Übersicht über Appliance Status
- Appliance Auslastung
- Zugriff auf Konsole
- BIOS Einstellungen
- Netzwerkeinstellungen der physischen und virtuellen Netzwerkinterfaces
- Firmware Management
- Ping Tool zum testen der Connectivity

Zur Konfiguration benötigt man die CIMC IP, DNS Server Adresse, sowie einen NTP Server. Folgende Schritte dazu sind nötig:

1. Aktivieren des Browserzugangs zum CIMC
2. Zeitsynchronisierung der Appliance mittels NTP
3. Prüfen und konfigurieren der 10-Gbps Appliance Netzwerkinterfaces
4. DNA Center ISO Image herunterladen und bootbaren USB-Stick erstellen
5. Boot vom USB-Stick

Weitere Informationen findet man im Kapitel [Prepare the Appliance for Configuration](#) [5] der offiziellen Anleitung.

## 4.4. Vorbereitung der Catalyst 9300 Switches

Vier Geräte stehen aus dem Inventar des INS für diese Arbeit zur Verfügung. Zur Vorbereitung für den PoC müssen diese aus einem bestehenden Stack entfernt und auf Werkseinstellungen zurückgesetzt werden.

Die Switches sind uns mit Softwareversion: IOS XE 17.03.04 (Amsterdam) übergeben worden. Mit Hilfe des DNA Centers wird es möglich sein, diese auf die aktuellste empfohlene Softwareversion zu aktualisieren. Zur Zeit ist nur ein Switch mit einem Glasfaser Uplink Modul ausgerüstet, falls die Switches für eine Pilotphase nach Buchs gezügelt werden, wären 3 weitere Glasfaser Uplink Module und 4 Glasfaser SFPs nötig.

#### 4.4.1. Stack auflösen

Folgende Schritte sind notwendig um den Stack aufzulösen [13]:

1. Geräte ausschalten
2. Stackkabel entfernen
3. Gerät einschalten
4. Konfiguration entfernen

Die Konfiguration kann mit folgenden Befehlen entfernt werden:

```
Switch#show switch
Switch#switch x renumber 1
Switch#reload
Switch(config)#no switch x provision
Switch#reload
```

#### 4.4.2. Factory Reset

Die Geräte können nun auf Werkseinstellungen zurückgesetzt werden mit dem folgenden Befehl:

```
Switch#factory-reset config
```

### 4.5. Grundkonfiguration der Appliance

Das DNA Center kann Standalone oder in einem Cluster betrieben werden. Eine Standalone Einrichtung kann später immer noch erweitert werden zu einem Cluster. Für den Proof of Concept und den Pilot verwenden wir ein Standalone Setup.

#### 4.5.1. Maglev Einrichtungsassistent

In diesem Schritt werden die Daten aus den Planungsabschnitten IP Konfiguration und Zugangsdaten benötigt.

Nach erfolgreichem Boot vom USB-Stick sollte der Einrichtungsassistent (*Maglev Configuration Wizard*) erscheinen. Mit *Start a Cisco DNA Center Cluster* wird die Konfiguration gestartet.

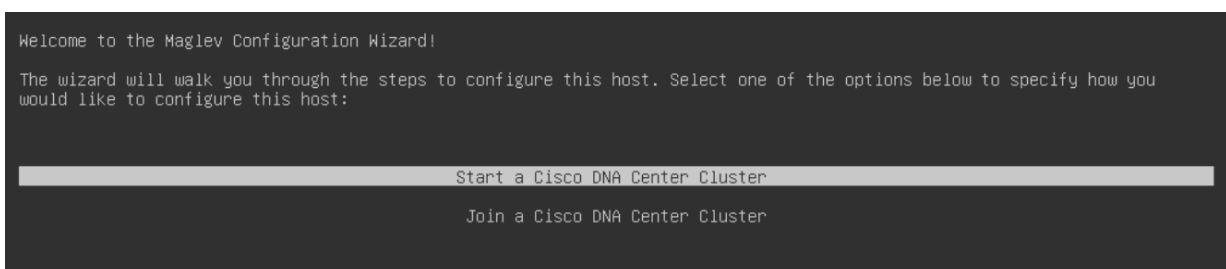


Abbildung 4.1.: DNA Center Setup Wizard

Es müssen 7 Schritte durchlaufen werden für die Konfiguration, diese sind allerdings nicht schön von 1 bis 7 nummeriert. Die folgenden Schritte referenzieren die im Einrichtungsassistent ersichtlichen Schritte in der Reihenfolge, wie sie erscheinen. Zur Hilfestellung befindet sich im Anhang B screenshots von jedem Schritt der Konfiguration.

## Step 2: IPv4/IPv6 Adressierung und Sicherheitsmodus

Hier kann man auswählen ob man IPv4 und/oder IPv6 Adressen verwenden möchte. Zudem kann man hier den Federal Information Processing Standard (FIPS) [28] mode aktivieren. Damit stellt man sicher, dass die Sicherheitsvorgaben an kryptographische module dem Standard genügen, der vom National Institute of Standards and Technology (NIST) vorgegeben wird.

Einstellungen:

- IPv4 mode: aktiviert
- IPv6 mode: deaktiviert
- FIPS mode: deaktiviert

Da in den Anforderungen viel Wert auf Sicherheit gelegt wird, empfiehlt es sich in einer Produktivumgebung den FIPS mode zu aktivieren.

## Step 2: Layer 2 Mode

Hier kann eingestellt werden ob VLANs benötigt werden über aggregiert Interfaces.

Einstellungen: Alles deaktiviert.

## Step 3: Netzwerkeinrichtung

In diesem Schritt können die IP Adressen der verschiedenen Interfaces des DNA Centers konfiguriert werden. Bei einem Interface, dass aktiv und mit dem Netzwerk verbunden ist, muss dabei Cluster Link aktiviert sein. Für ein Multi-Node Setup sollte dies das Cluster Interface sein, welches mit den anderen DNA Center Nodes kommuniziert.

Für den PoC wurde das Management Interface für alles verwendet. Alle anderen Network Adapter Einstellungen wurden übersprungen.

Einstellungen Management Interface:

- Host IPv4 Address: 10.6.10.10
- IPv4 Netmask: 255.255.255.0
- Default Gateway IPv4 Address: 10.6.10.1
- IPv4 DNS Servers: 1.1.1.1
- IPv4 Static Routes: (leer)
- Cluster Link: aktiviert

Für eine Produktivumgebung sollte das Enterprise sowie das Cluster Interface auch konfiguriert werden. Zudem sollte analysiert werden ob es sicherheitstechnisch macht es zudem Sinn das Internet Interface ebenfalls zu verwenden.

## Step 5: Cluster Details (Hostname / Virtual IP address)

In diesem Schritt kann man dem DNA Center (Cluster) einen Hostnamen geben und eine virtuelle IP Adresse über welche das Management und Enterprise Interface erreichbar sein sollen. Das ist vor allem nützlich um das DNA Center in einem Multi-Node-Setup über eine einheitliche Address/Hostnamen erreichbar zu machen.

Einstellungen: Übersprungen auf Grund des Single-Node-Setups des PoC

### Step 6: Benutzeraccount Einstellungen

In diesem Schritt setzt man die Passwörter für das Linux Login auf die Konsole der Appliance, sowie für den Administrator des Web GUIs. Falls man die Passwörter nicht manuell setzen möchte können diese auch automatisch generiert werden.

Einstellungen: Eingerichtet wie im Planungsabschnitt Zugangsdaten notiert

### Step 7: NTP Server Einstellungen

Hier können einer oder mehrere NTP Server konfiguriert werden. Es ist empfohlen mindestens drei oder mehr NTP Server zu konfigurieren für eine Produktivumgebung. Es muss mindestens einer der NTP Server erreichbar sein.

Einstellungen:

- NTP Servers: ch.pool.ntp.org

### Step 8: Erweiterte Einstellungen

In diesem Schritt kann man das Container Subnet sowie das Cluster Subnet konfigurieren und IPSec aktivieren für die Kommunikation innerhalb des DNA Center Cluster aktivieren. Für den PoC Aufbau haben wir einen Range der vom INS dafür vorgesehen war verwendet. Da uns nicht bewusst war dass es andere nicht geroutete empfohlenen IP Ranges dafür von Cisco vorgesehen sind. In einer Produktivumgebung sollte jedoch die empfohlenen Cluster und Container Subnet IP Ranges verwendet werden. Intracluster IPSec kann zur Erhöhung der Sicherheit ebenfalls aktiviert werden.

Einstellung PoC:

- Container subnet: 10.7.64.0/21
- Cluster subnet: 10.7.72.0/21
- Enable Intracluster IPSec: deaktiviert

Empfohlene Einstellung für Produktivumgebung:

- Container subnet: 169.254.32.0/20
- Cluster subnet: 169.254.48.0/20
- Enable Intracluster IPSec: aktiviert

Mit Schritt 8 sind alle Einstellungen gesetzt und der Installationsvorgang kann gestartet werden. Das DNA Center benötigt ca. 1.5h bis die Installation durchgelaufen ist und das Web GUI unter der Management IP Adresse erreichbar wird.

Für weitere Informationen kann die offizielle Anleitung [Configure the Appliance](#) [5] zur Hilfe gezogen werden. Das Kapitel [Complete First-Time Setup](#) [5] sollte jedoch übersprungen werden. Falls Probleme bei der Einrichtung auftauchen sollten gibt es Tipps zur Fehlerbehebung im Kapitel [Troubleshoot the Deployment](#) [5].

## 4.6. Grundkonfigurationen im DNA Center

Die Anleitung basiert auf dem [Cisco LAN Automation Deployment Guide](#) [11] von Cisco.



#### 4.6.1. Allgemeine Informationen

Als erster Schritt können im Menü unter Design / Network Hierarchy die einzelnen Standorte erfasst werden, welche später mit Geräten ausgestattet werden. Auf der angezeigten Karte können die Standorte genau platziert werden.

**Für öffentliche  
Version entfernt**

Abbildung 4.2.: Standorte im Cisco DNA Center

Als oberste Ebene wird eine Area definiert, welche weitere Areas oder Buildings beinhaltet. In einem Building können wiederum einzelne Floors definiert werden.

Unter Network Settings können allgemeine Informationen hinterlegt werden, die für alle Geräte gültig sind.

Folgende Informationen sind hier hinterlegt:

- Tab Network: Domain Name
- Tab Device Credentials: Verschiedene Zugangsdaten für CLI, SNMPv2 read, SNMPv2 write
- Tab IP Address Pools: Adressbereiche für Underlay, Extended Nodes und vom DNA Center verwaltete Hosts

IP Address Pools    SP Profiles    Wireless    Telemetry

---

IP Address Pools (2)

Subnet Type **All**    IPv4 only    Dual-Stack

Filter    0 Selected    Reserve    More Actions ▾

<input type="checkbox"/>	Name ▲	Type	IPv4 Subnet	IPv4 Used ⓘ
<input type="checkbox"/>	LAN-Infra	Generic	10.7.81.0/24	100% ⓘ
<input type="checkbox"/>	LAN-Underlay	LAN	10.7.80.0/24	12% ⓘ

Abbildung 4.3.: IP Adresspools

IP Bereiche müssen erst auf der Global Area erfasst werden. Import von CSV oder IPAM-Server ist möglich. Ein IPAM-Server muss aber erst konfiguriert werden. Dies wird im aktuellen PoC nicht abgedeckt.

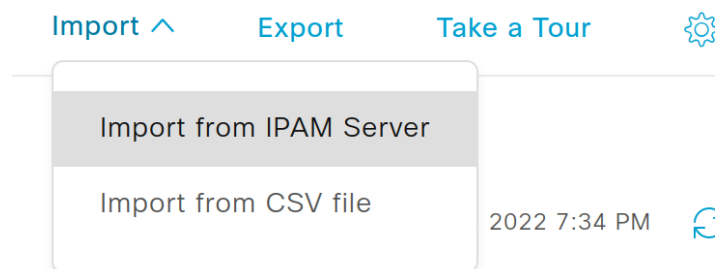


Abbildung 4.4.: IP Adressen Import Feature

Typ für den IP Pool ist LAN im Underlay, Generic für das Management Netz.

#### 4.6.2. Software Image Management

Unter Design / Image Repository kann für jeden Gerätetyp ein sogenanntes Golden Image definiert werden. Auf diesen Stand werden alle Geräte aktualisiert, falls sie noch auf einem älteren Softwarestand sind.

Ein vorhandenes Image muss als File hochgeladen oder von einer Web-Adresse importiert werden. Danach wird es nach Gerätefamilie geordnet angezeigt. Ebenfalls zeigt die Übersicht aktuelle Informationen von Cisco Advisories, zu Sicherheitslücken der Image Version. Das empfohlene Image für die im PoC verwendeten Catalyst 9300 Serie Switches ist: 17.6.4 [12]

Family Name ▾	Devices	Images	Advisories ⓘ		Images Marked Golden
Imported Images ⓘ	N/A	1	N/A		N/A
Cisco Catalyst 9300 Switch	4	1	0 Critical	0 High	1
Cisco IE-4000-4GC4GP4G-E Industrial Ethernet Switch	1	1	3 High	1 Medium	0
Cisco IE-4000-4GS8GP4G-E Industrial Ethernet Switch	1	1	3 High	1 Medium	0

Abbildung 4.5.: Software Image Repository

### 4.6.3. Device Templates

Im Bereich Design / Network Profiles können verschiedene Gerätekonfigurationen erfasst werden, die danach auf eine Auswahl von Geräten angewendet werden. Hier kann die im nächsten Kapitel folgende Konfiguration des Seed Device hinterlegt werden, um dieses automatisch einzurichten.

Dazu wird im Menü unter Tools der Template Editor verwendet.

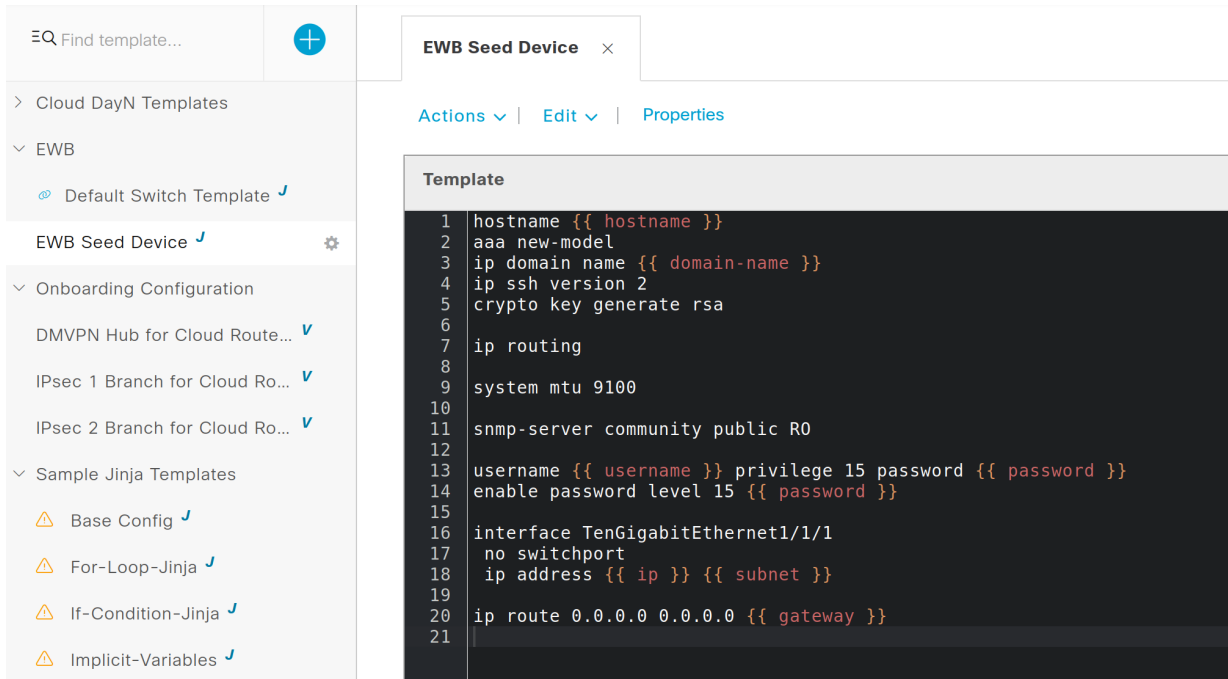
Bei einem neuen Template zwingend anzugeben sind die folgenden Informationen:


- Regular Template
- Name
- Project Name (Ordner)
- Device Type (Routing and Switching)
- Software Type IOS-XE


Die verfügbaren Template-Sprachen Velocity oder Jinja2 stellen erweiterte Funktionalität zur Verfügung wie die Verwendung von Variablen oder Kontrollfluss-Sequenzen wie Loops oder If-Else Statements. Der Template Editor ist eine eigene kleine Applikation, welche die Erstellung und Verwaltung von solchen Konfig-Snippets ermöglicht. Für gängige Logiken sind bereits Beispiele vorhanden.



Die Templates sind versioniert, deshalb muss jeweils Actions / Save und zusätzlich Actions / Commit ausgeführt werden.

In der folgenden Grafik 4.6 wird dargestellt, wie ein Template mit Variablen versehen werden kann. Diese Variablen werden jeweils beim Provisionieren eines Gerätes abgefragt und können individuell festgelegt werden.



Find template... 

EWB Seed Device 

Actions  | Edit  | Properties

**Template**

```
1 hostname {{ hostname }}
2 aaa new-model
3 ip domain name {{ domain-name }}
4 ip ssh version 2
5 crypto key generate rsa
6
7 ip routing
8
9 system mtu 9100
10
11 snmp-server community public R0
12
13 username {{ username }} privilege 15 password {{ password }}
14 enable password level 15 {{ password }}
15
16 interface TenGigabitEthernet1/1/1
17 no switchport
18 ip address {{ ip }} {{ subnet }}
19
20 ip route 0.0.0.0 0.0.0.0 {{ gateway }}
21
```

Abbildung 4.6.: Template Editor mit Beispielen

## 4.7. LAN Automation

LAN Automation bezeichnet das automatische entdecken von Switches inklusive der Konfiguration zu einem Layer 3 Underlay Netzwerk. [11]

### 4.7.1. Phase 1: Device Onboarding und Provisionierung

Der Layer 3 Underlay soll nach einer Grundkonfiguration vom Cisco DNA Center komplett automatisiert erstellt werden. Dabei werden die Geräte in zwei verschiedenen Rollen unterteilt.

#### Seed Device

Es wird ein konfigurierter Switch benötigt, von dem aus die LAN Automation gestartet werden kann. Dieser trägt die Rolle des Seed Device und muss als erstes ins Inventory aufgenommen werden. Falls das Gerät bereits aufgesetzt ist kann das via Discovery oder auch manuell geschehen. Falls es noch nicht aufgesetzt ist muss es zuerst konfiguriert werden, geschieht dies via Plug-n-Play zero-touch-provisioning wird das Gerät ebenfalls automatisch im Inventar aufgenommen.

Alle Geräte, die danach vom DNA Center konfiguriert werden sollen, müssen eine Layer 2 Verbindung zu diesem Device haben.

Die Konfiguration auf dem Seed Device kann manuell oder via Plug-n-Play zero-touch-provisioning durchgeführt werden. Damit die Konfiguration automatisch geschehen kann muss das Gerät im Inventory / Plug and Play über **Add Device** manuell mit seiner Seriennummer hinzugefügt werden. Beim ersten Gerätestart wird dann eine in den Onboarding Templates definierte Konfiguration automatisch auf den Switch gespielt.

Um das Seed Device via Discovery ins DNA Center Inventory einzubinden, haben wir initial die folgende Konfiguration vergeben.

Unsere Seed Device Konfiguration:

```
1
2 ! basics and connectivity
3 hostname sw1
4 ip domain name ewbuchs.ch
5 ip ssh version 2
6 crypto key generate rsa
7
8 ip routing
9
10 system mtu 9100
11
12 interface TenGigabitEthernet1/1/1
13 no switchport
14 ip address 10.6.20.162 255.255.255.224
15
16 ip route 0.0.0.0 0.0.0.0 10.6.20.161
17
18 ! user authentication
19 aaa new-model
20 aaa authentication login default local
21
22 username ewb privilege 15 password CiscoDna4EWBuchs
23 enable password level 15 CiscoDna4EWBuchs
24
25 ! snmp
26 snmp-server community public RO
```

```

27 snmp-server community <secret> RW
28
29 ! netconf
30 netconf-yang
31 netconf ssh
32 aaa authorization exec default local
  
```

Danach kann mit folgenden Einstellungen im Discovery das Device gefunden werden. Die verwendeten Credentials müssen in den globalen Einstellungen vom DNA Center hinterlegt sein und können dann fürs Discovery ausgewählt werden.

### New Discovery

Discovery Name\*  
Seed Device using IP

---

IP Address/Range\*

Discovery Type ⓘ

CDP
  IP Address/Range
  LLDP

From\* ⓘ 10.6.20.162 - To\* ⓘ 10.6.20.162 +

Subnet Filters ⓘ +

Preferred Management IP Address ⓘ

None
  Use Loopback

---

Credentials\*

ⓘ At least one CLI credential and one SNMP credential are required.  
 ⓘ Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.  
 ■ GLOBAL ■ Task-specific

CLI SNMPv2c Read

Global CLI EWB
  Global SNMP EWB

Abbildung 4.7.: Discovery Einstellungen für das vorkonfigurierte Seed Device

Auf das neu gefundene Device können nun weitere Einstellungen in den Device Templates via Provisioning angewendet werden.

## Plug and Play Agent Geräte

Cisco Guide: [Plug and Play Provisioning Overview](#) [15]

Als Plug and Play Agent bzw. PnP-Agent-Geräte werden alle weiteren bezeichnet, die via LAN Automation automatisiert aufgesetzt werden sollen. Neue Geräte starten ab Werk in einen Plug and Play Modus, der die Konfiguration durch ein DNA Center erlaubt.

Zur Vorbereitung und Bereinigung bei Geräten, die bereits konfiguriert sind, werden die folgenden Befehle verwendet. Diese versetzen das Gerät wieder in den ursprünglichen Werkszustand:

```
# Variante Automatisch
PnP-Switch# pnpa service reset
# Variante Manuell
PnP-Switch# delete /force nvram:*.cer
PnP-Switch# delete /force stby-nvram:*.cer (if a stack)
PnP-Switch# delete /force flash:pnp-reset-config.cfg
PnP-Switch# delete flash:vlan.dat
PnP-Switch# write erase
PnP-Switch# reload (enter no if asked to save)
```

```
Base Ethernet MAC Address      : 24:16:9d:ad:e5:00
Motherboard Assembly Number    : 73-18271-04
Motherboard Serial Number      : FOC2403017B
Model Revision Number          : A0
Motherboard Revision Number    : A0
Model Number                   : C9300-24P
System Serial Number           : FOC2404X0FH
CLEI Code Number               :

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1021
```

Abbildung 4.8.: Switch ist im initialen Setup Status

### Starten der LAN Automation

Gestartet wird die LAN Automation im Inventory über das Menü Actions / LAN Automation.

Dabei werden folgende Informationen benötigt:

- Primary Site:  
Site des Seed Devices
- Primary Device:  
Das vorkonfigurierte Seed Device
- Selected Ports of Primary Device:  
Auswählen, an welchen Ports des Seed Devices andere zu erkennende Geräte angeschlossen sind
- Discovered Device Site:  
Legt fest, welcher Site alle erkannten Geräte zugewiesen werden. Kann im Nachhinein pro Gerät angepasst werden.
- Main IP Pool:  
Der LAN-Underlay IP Bereich (aus dem Kapitel Allgemeine Informationen)

- **Enable Multicast:**  
Aktiviert eine Multicast Konfiguration auf allen neuen Geräten.
- **Hostname Mapping:**  
Hier kann ein Präfix angegeben werden um den Hostnamen automatisch zu generieren. Angehängt wird pro Gerät eine aufsteigende Zahl.

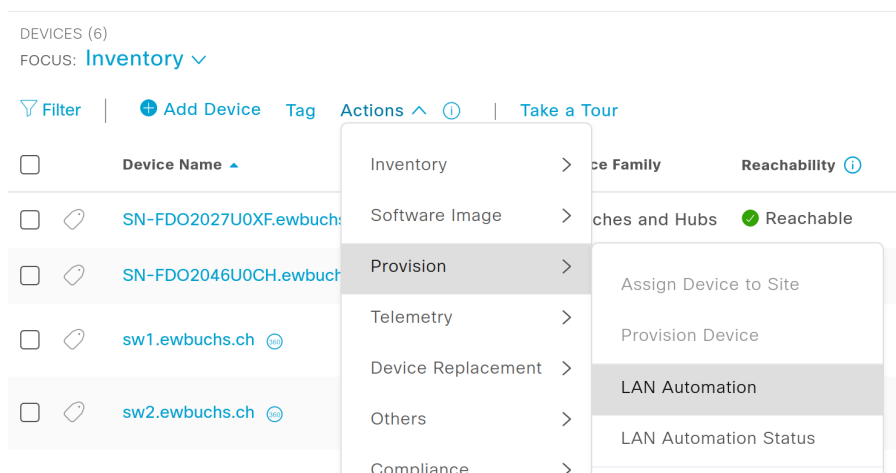


Abbildung 4.9.: Starten der LAN Automation

Auf das bereits hinzugefügte Seed Device wird eine erweiterte Konfiguration geschrieben, die das weitere Discovery ermöglicht. Dazu gehört unter anderem die Einrichtung von IS-IS als Routing Protokoll sowie ein DHCP Server, der den weiteren Geräten eine IP vergibt sowie mittels Option 43 die Adresse des DNA Centers mitteilt.

Folgende Aktionen werden beim Provisionieren von neuen Geräten automatisiert ausgeführt, teilweise basierend auf den bisher gemachten Einstellungen:

- Deployment des als “Golden Image” markierten Softwareimages
- Hinterlegen der Credentials aus den Globalen Network Settings (CLI und SNMP)
- SSHv2 und SCP Server aktivieren
- HTTP und HTTPS Server deaktivieren
- Bei Switches wird der “vtp mode transparent” aktiviert
- Eine Device Onboarding Configuration wird auf den Geräten ausgerollt
- Das Gerät wird zum Inventory hinzugefügt

#### 4.7.2. Phase 2: Interface Configuration

Im zweiten Schritt wird aus den nun verbundenen und eingerichteten Switches automatisiert ein Fabric Underlay Netzwerk gebaut. Dazu muss der Vorgang der LAN Automation gestoppt werden. Dies setzt voraus, dass alle angeschlossenen PnP-Geräte durch das Discovery entdeckt wurden und auf der Status Seite mit Completed markiert sind.



## LAN Automation Status ×

Last updated Nov 28, 2022 1:33 PM [Refresh](#)

[Summary](#)   [Devices](#)   [Logs](#)

Discovered Site	EWB Neubau
Primary Device	sw1.ewbuchs.ch
Peer Device	None
Primary Device Interfaces	GigabitEthernet1/0/2 GigabitEthernet1/0/1
IP Pool	LAN-Underlay
Link Overlapping IP Pool	None
Advertise LAN Automation summary route into BGP	Disabled
Multicast	Enabled
Device Prefix	None
Hostname File	None

Status In Progress  
 Discovered Devices 3  
✔ Completed : 3   🕒 In Progress : 0   ✘ Error : 0

Abbildung 4.10.: LAN Automation Status Seite

Dies bedeutet, die Geräte sind im Inventory vorhanden und im Status Reachable / Managed. In der Topologie-Ansicht des Inventory kann überprüft werden, ob auch die richtigen Interfaces angegeben worden sind.

[Provision](#) / [Network Devices](#) / [Inventory](#)

 Preview New Page 
 🔍 ? 🗄️ 🔔

---

📍 Global
 
 ☰ 🔄 📄

---

🔍 Find by device IP, type, role, family & MAC
📄 [Export](#)

---

[Collapse All](#)   [Custom Focus](#)   Dec 17, 2022 10:09 PM




Abbildung 4.11.: Topology View kann über die Buttons oben rechts aktiviert werden

Nach dem Stoppen der LAN Automation werden sämtliche Geräte umkonfiguriert und ein Layer 3 Underlay basierend auf IS-IS, VXLAN und LISP gebaut. Dies geschieht vollautomatisch.

Inventory | Plug and Play | Inventory Insights

Global / Buchs

DEVICES (6)  
FOCUS: Inventory

Filter | Add Device | Tag | Actions | Take a Tour

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score
SN-FDO2027U0XF.ewbuchs.ch	10.7.81.11	Switches and Hubs	Reachable	Not Scanned	Managed	Compliant	10
SN-FDO2046U0CH.ewbuchs.ch	10.7.81.12	Switches and Hubs	Reachable	Not Scanned	Managed	Compliant	10
sw1.ewbuchs.ch	10.7.80.65	Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed	Compliant	10
sw2.ewbuchs.ch	10.7.80.67	Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed	Compliant	10
sw3.ewbuchs.ch	10.7.80.73	Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed	Compliant	10

Abbildung 4.12.: Inventory Ansicht, Geräte sind im Status Reachable und Managed

## 4.8. Fabric

### 4.8.1. Konfiguration der Fabric

Cisco Anleitung: [Provision Fabric Networks](#) [15]

Nachdem sämtliche Geräte mittels LAN Automation gefunden und konfiguriert worden sind, kann mit dem Einrichten der Fabric begonnen werden.

Als erstes muss dazu SD Access als separate Software installiert werden. Dies geschieht im Menü unter System / Software Management.

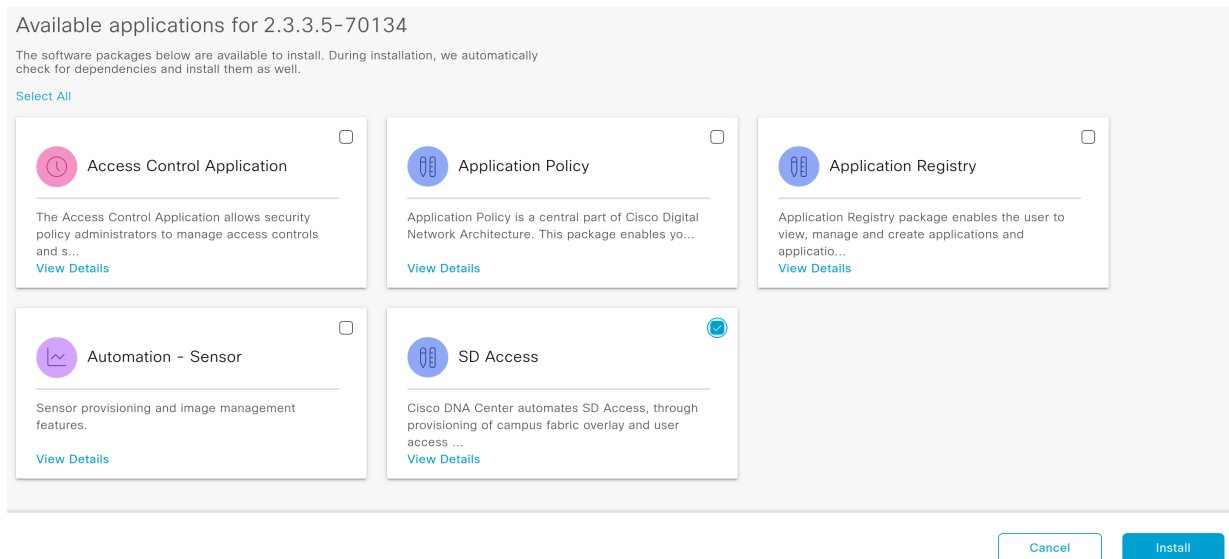


Abbildung 4.13.: Installation der SDA Applikation

Danach ist im Menü unter Provision die Unterkategorie SD-Access verfügbar.

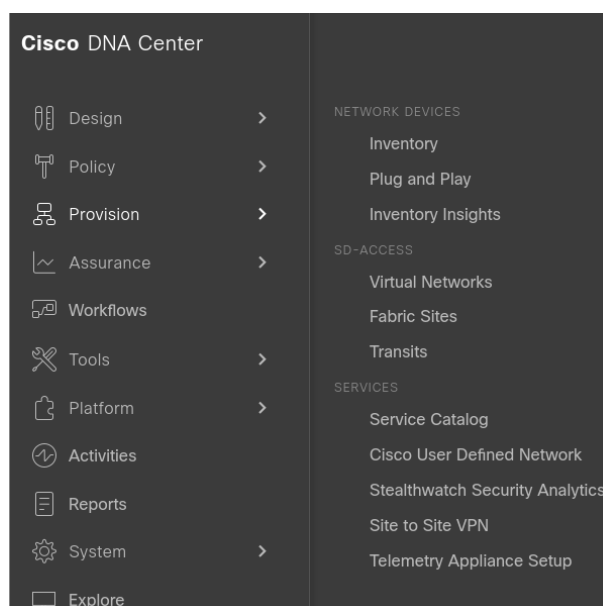


Abbildung 4.14.: SD Access

Die bestehenden Netzwerke können unter Provision / SD Access / Virtual Networks bereits erfasst

werden. Dazu wird nur ein Name für das Virtual Network benötigt.

Unter Provision / SD Access / Fabric Sites kann eine neue Fabric Site erstellt werden. Dies startet einen Wizard, der bei der Einrichtung unterstützt.

Die Einstellungen tätigen wir wie folgt:

- Fabric Site: Buchs
- Wired Endpoint Data Collection: Aktiviert
- Authentication Template: None (da aktuell keine Cisco ISE zur Verfügung steht)
- Fabric Zones: Setup later

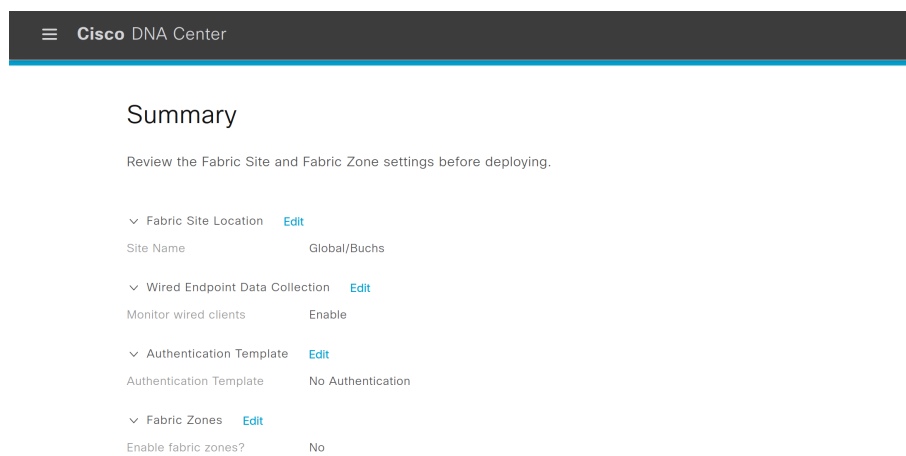


Abbildung 4.15.: Fabric Wizard Summary

Anschliessend wird in der Ansicht unter Provision / SD Access / Fabric Sites im Tab Fabric Infrastructure die aktuelle Topologie angezeigt. Hier kann den einzelnen Devices nun die entsprechende Rolle zugewiesen werden. Wichtig: Um die Fabric Edge Rolle zu erhalten, muss ein Switch im Inventory die Rolle ACCESS zugewiesen haben. Dies kann über Actions / Inventory / Edit Device im Tab Role gemacht werden.

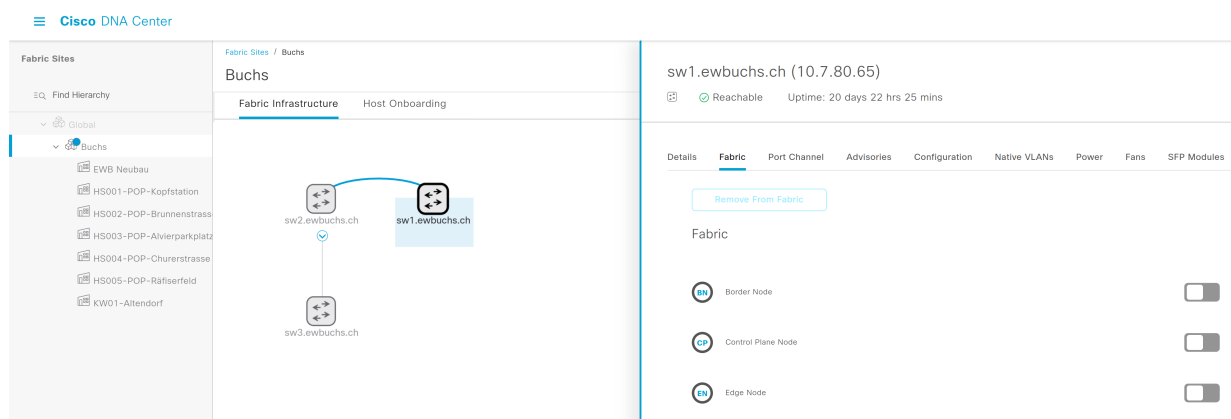


Abbildung 4.16.: Ansicht Fabric Infrastructure

Im Tab Authentication Templates unter Host Onboarding können im Nachhinein die Einstellungen zur Port-based Authentication angepasst werden.

Im Tab Host Onboarding kann ausgewählt werden, welche der vorkonfigurierten Virtuellen Netze in der Fabric zur Verfügung stehen sollen. Sobald die VNs hinzugefügt wurden, kann ihnen ein entsprechender IP Pool zugewiesen werden.

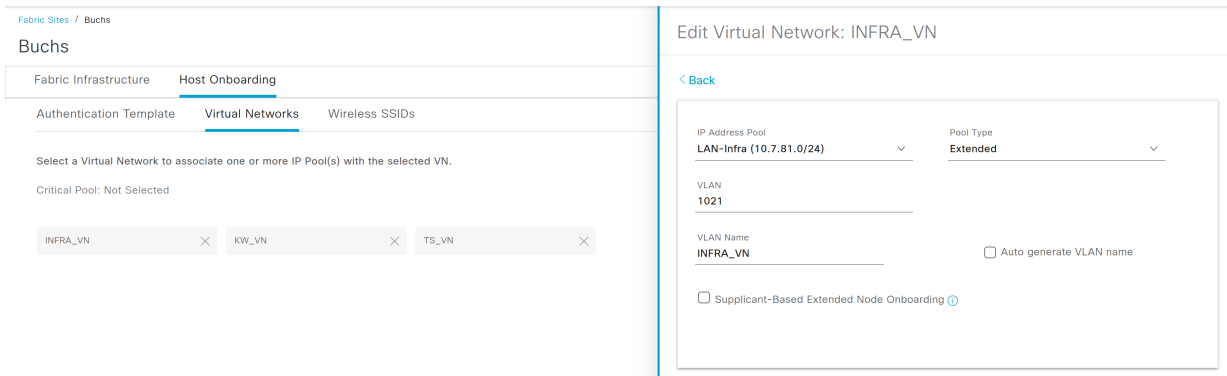


Abbildung 4.17.: Virtuelle Netze

## 4.9. Konfiguration Extended Nodes

Die Industrial Ethernet Switches der Cisco Catalyst IE3300 und IE3400 Serie, welche an den Ausenstandorten eingesetzt werden, können nur als Extended bzw. Policy Extended Nodes fungieren. Deshalb wurden sie nicht bereits bei der LAN Automation aufgesetzt. Allerdings können sie ähnlich wie das Seed Device via Plug-n-Play vom DNA Center konfiguriert werden. Die folgenden Schritte sind gültig für Extended Nodes und Policy Extended Nodes, solange nicht explizit etwas anderes angegeben ist. [15, 30]

### 4.9.1. Voraussetzungen

CLI und SNMP Credentials müssen für die Sites hinterlegt sein, an denen die Switches eingesetzt werden sollen. Diese können unter Design / Network Settings / Device Credentials hinterlegt werden. Die Switches müssen mit einem Fabric Edge Switch oder bereits konfigurierten Extended Node verbunden sein. Mehrere parallele Verbindungen zum selben Edge Switch sind möglich.

Folgende minimale Software Versionen sind nötig, damit die Switches als Extended Nodes eingesetzt werden können:

- Cisco Catalyst IE3300 Series: IOS XE 16.12.1s
- Cisco Catalyst IE3400 Series: IOS XE 17.1.1s

### 4.9.2. Erstellung des IP-Adresspools und der Credentials

Zuerst muss unter Design / Network Settings / IP Address Pools ein Generic IP-Adresspool für die Extended Nodes erstellt werden. Dieser entspricht einem Management-Netz bei traditionellen Netzwerken. Wichtig ist auch, dass der IP-Adresspool vom DNA Center erreichbar ist. Weitere Informationen zu IP Pools siehe Abschnitt 4.6.1.

### 4.9.3. Zuweisen des IP-Adresspools zum Virtuellen Netzwerk

Nun muss der IP-Adresspool dem speziellen Virtuellen Netzwerk **INFRA\_VN** zugeordnet werden, welches für Extended Nodes und Access Points gedacht ist. Dies geschieht unter Provision / SD-Access / Fabric Sites / Site / Host Onboarding / Virtual Networks Menu.

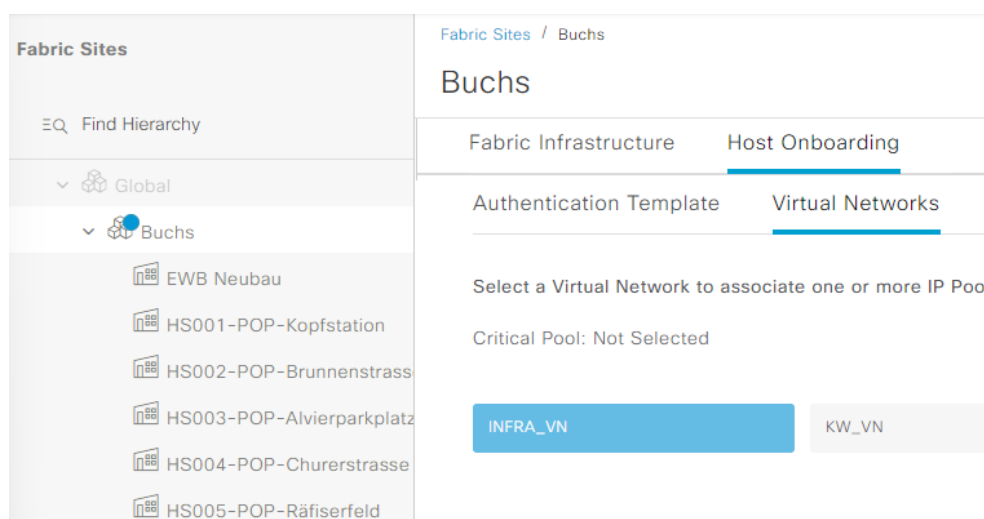


Abbildung 4.18.: Einstellungen Virtuelles Netzwerk innerhalb der Fabric

Hier kann man das **INFRA\_VN** auswählen und dann via **Add** den Adresspool hinzufügen. Wichtig ist, dass der Pool Type **Extended** gewählt wird. Das DNA Center konfiguriert dann den IP Address Pool und das VLAN auf dem Fabric Edge Switch.

Edit Virtual Network: INFRA\_VN ×

---

[< Back](#)

IP Address Pool  
LAN-Infrastructure (10.7.82.0/24) +

---

Pool Type  
Extended

---

VLAN  
100

---

VLAN Name  
extended  Auto generate VLAN name

---

Supplicant-Based Extended Node Onboarding ?

#### 4.9.4. Erstellen der Port Channels

Als nächstes muss auf dem Fabric Edge Switch ein Port Channel erstellt werden für die Ports, welche mit dem Extended Node Switch verbunden sind. Dies ist zwingend, auch wenn die Extended Nodes nicht mit mehreren Ports angeschlossen sind. Falls mehrere Extended Nodes hintereinander gehängt sind, muss dort ebenfalls jeweils ein Port Channel erstellt werden.

Dies geschieht unter Provision / SD-Access / Fabric Sites / Site / Fabric Infrastructure. Hier wählt man den Fabric Edge Switch aus und kann im gleichnamigen Menü einen neuen Port Channel erstellen. Wichtig ist hier, das Protokoll PAgP zu wählen.

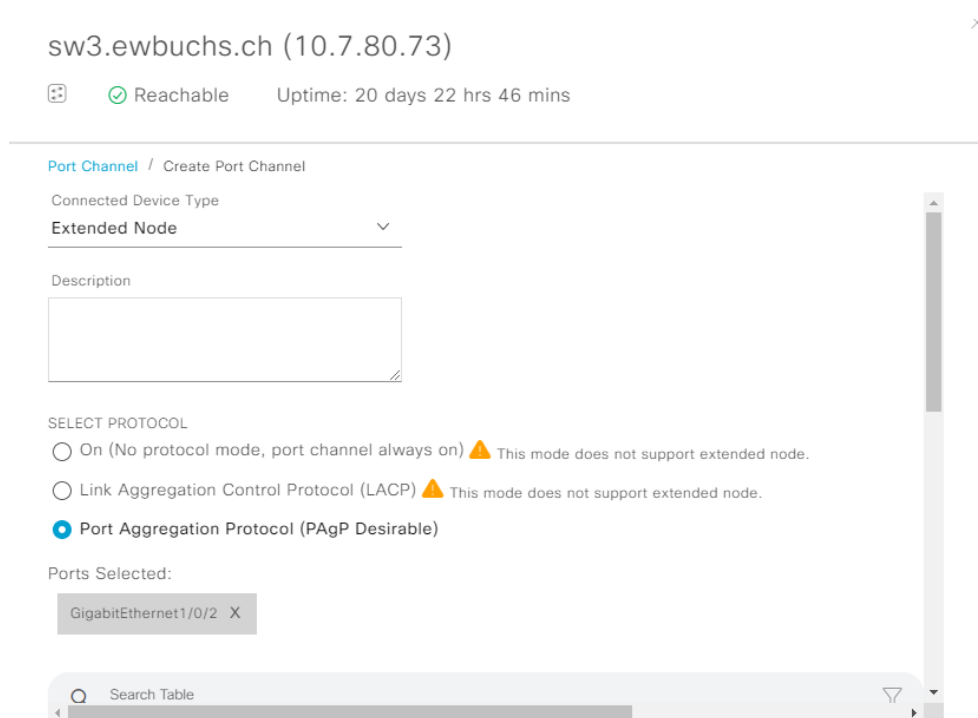


Abbildung 4.19.: Port Channel erstellen

#### 4.9.5. Konfiguration DHCP Server

Die Switches müssen nun beim Start eine IP erhalten, die im konfigurierten LAN\_Infra Adresspool ist. Wichtig ist es, in DHCP Option 43 die Adresse des DNA Centers mitzugeben. Damit das funktioniert, muss ein Scope auf einem vorhandenen DHCP Server konfiguriert werden. Nachfolgend eine Beispielkonfiguration eines DHCP Scopes für PnP Geräte auf einem Cisco Router, wobei 10.0.50.50 die IP Adresse des DNA Centers wäre.

```

1 ip dhcp pool pnp-device-pool
2   network 10.0.50.0 255.255.255.0
3   default-router 10.0.50.1
4   option 43 ascii "5A1N;B2;K4;I10.0.50.50;J58" ! Option 43: String in ASCII Format
  
```

#### 4.9.6. Finalisierung der Konfiguration

Die Extended Node Switches müssen sich in den Werkseinstellungen befinden, damit sie via DHCP die Adresse des DNA Centers für die Konfiguration erhalten können. Um die Switches zurückzusetzen, falls sie das nicht bereits sind, siehe Abschnitt 4.7.1.

Sobald die Extended Nodes nun gestartet werden, verbinden sie sich mit dem DNA Center für Plug and Play und erhalten dabei automatisch eine Konfiguration.

Weitere Informationen zur Konfiguration können im Cisco User Guide unter [Configure an Extended Node Device](#) [15] nachgeschlagen werden.



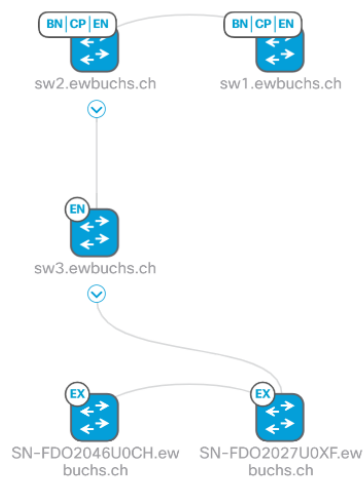


Abbildung 4.20.: Erfolgreich konfigurierte Extended Nodes

## 4.10. Statische VLAN-Port Zuweisung

Wenn die Switches der Fabric hinzugefügt wurden, können zuvor erstellte Virtuelle Netzwerke (Layer 2 Overlay Netze) statisch den Ports zugewiesen werden. Falls 802.1X verwendet wird, geschieht diese Konfiguration automatisch. Anderenfalls muss das manuell erfolgen. Unter Provision / SD-Access / Fabric Sites / Site / Host Onboarding / Port Assignment hat man eine Übersicht über alle Switches und deren Ports.

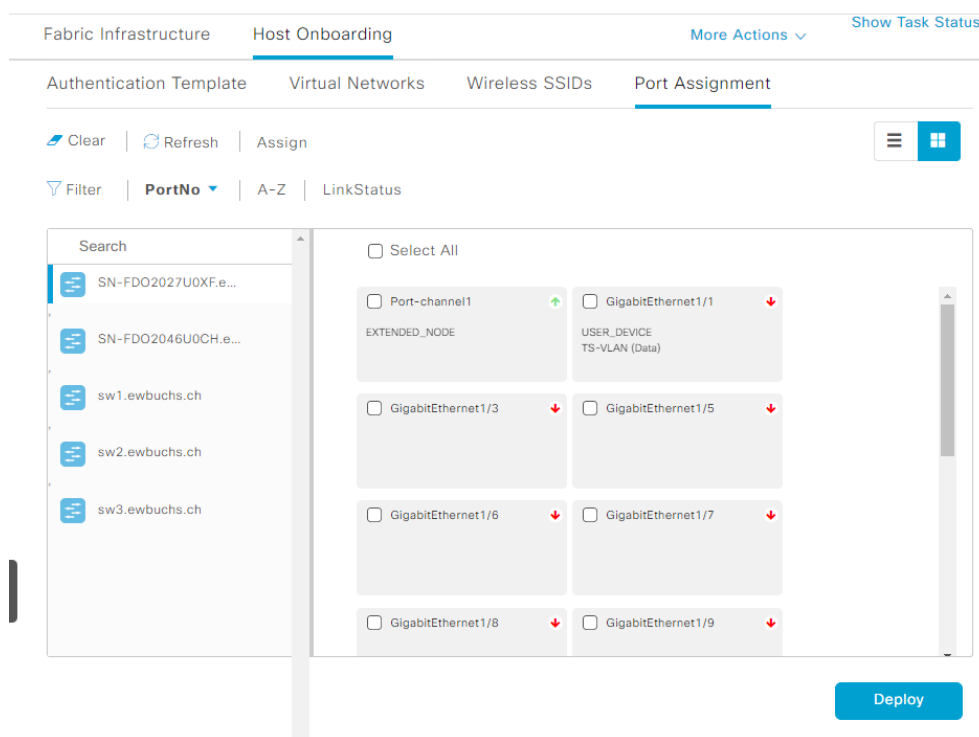


Abbildung 4.21.: Übersicht über alle Switches und deren Ports

Nun können alle Ports ausgewählt werden, die dieselbe Konfiguration bekommen sollen und mittels

**Assign** dem VN zuweisen. Für Endgeräte wie Infrastrukturanlagen, PCs, etc. wählt man den Device Type User Devices. Man hat hier auch unter **Authentication Template**, die Möglichkeit verschiedene Authentifizierungsmodus wie 802.1X zu aktivieren oder deaktiviert. Je nachdem, welcher Authentifizierungsmodus als Standard für das Gerät gewählt wurde.

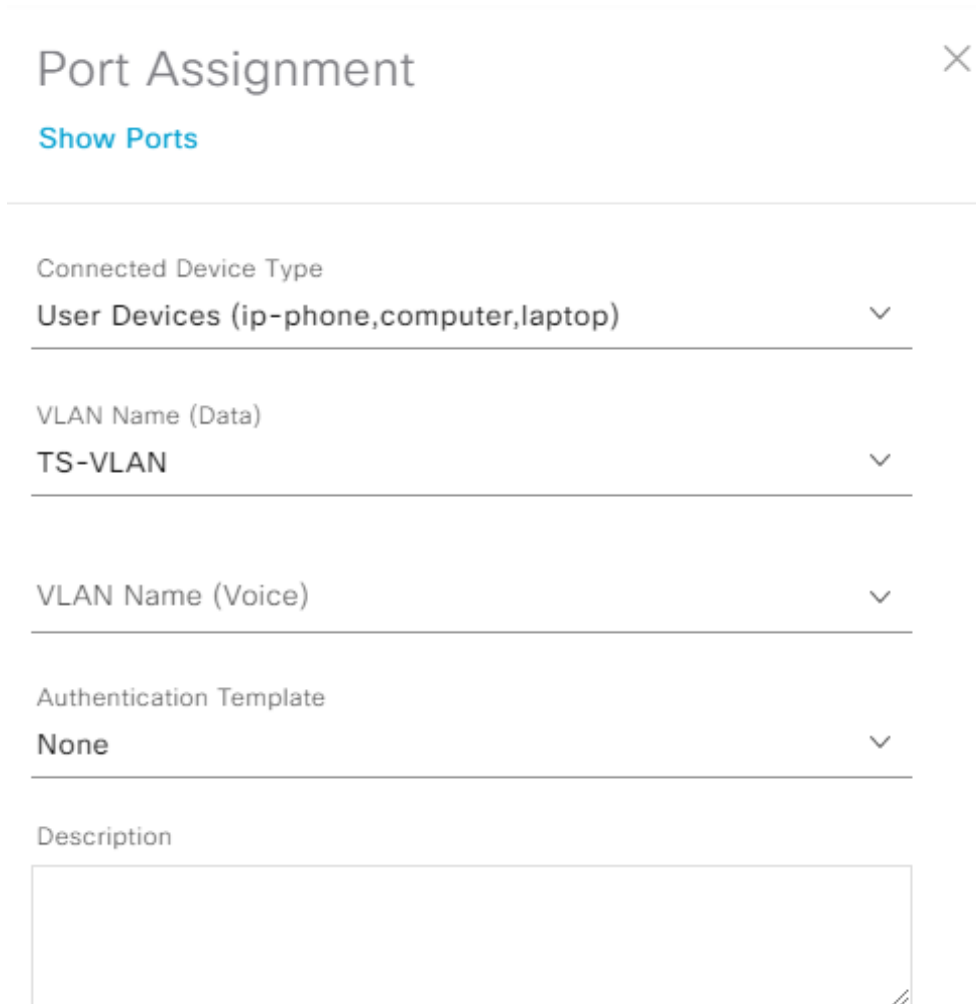


Abbildung 4.22.: Port Assignment Optionen

Damit die Änderungen aktiv werden, muss am Schluss noch auf **Deploy** geklickt werden.

## 5. Testkonzept für Pilotphase in Buchs

Erster Fokus der Tests sollen die realen Anwendungsfälle des Bereichs Infrastruktur sein. Grundlegende Kommunikation der Anlagen wie bisher muss zwingend funktionieren. Die korrekte funktionsweise der Rittmeyer und Siemens Anlagen werden am besten in Zusammenarbeit mit der jeweiligen Firma gemacht.

Als zweiter Punkt soll ebenso mit Priorität der Aspekt Sicherheit betrachtet werden. Insbesondere in Bezug auf Visibility sollen Anwendungsfälle definiert werden, die gegenüber der jetzigen Situation einen Mehrwert bringen.

Weiter soll das Konzept auch auf Wartbarkeit und Erweiterbarkeit geprüft werden.

Klar abgegrenzt werden folgende Themen, welche für den geplanten Anwendungsfall nicht relevant sind:

- Wireless Network
- Multi Site Fabric

Folgend sind Tests aufgelistet welche während des Proof of Concept vor Ort durchgeführt werden sollten.

### 5.1. Grundlegende Kommunikation

- Ping von allen angeschlossenen Anlagen/Servern

### 5.2. Anwendungsspezifische Kommunikation

- Rittmeyer
  - Erhalt von Messdaten in Leitstelle von Kraftwerken/Trafostationen
  - Steuerungsbefehle versenden von Leitstelle zu den Anlagen
  - Kommunikation der Anlagen untereinander
  - Weitere Tests von Rittmeyer
- Siemens
  - Erhalt von Messdaten in Leitstelle von Kraftwerken/Trafostationen
  - Steuerungsbefehle versenden von Leitstelle zu den Anlagen
  - Kommunikation der Anlagen untereinander
  - Weitere Tests von Siemens

### 5.3. DNA Center Funktionalität

- Austausch von Switches und automatisierte Konfiguration
- Provisionierung eines neuen PoP Switches
- Provisionierung eines Aussenstandort Switch
- Hinzufügen eines Switches zur Fabric inklusive Rolle

- Änderung der Rolle eines Switches in einer Fabric
- Erstellen eines neuen Layer 2 Virtual Networks
- Erkennung von Störungen im Netzwerk
- Unterbruch zwischen redundant verbundenen Switches in den PoPs stört die Kommunikation zwischen Endgeräten nicht
- Ein Verbindungsabbruch zwischen DNA Center und Switches hat keine Störung im restlichen Netzwerk zur Folge.
- Automatisierte E-Mail Benachrichtigung bei Störungen.
- Backup und Restore der DNA Center Konfiguration

## **5.4. Aussenstellen: Extended Node vs. Policy Extended Node**

Zur Auswahl zwischen Extended oder Policy Extended Node wurde in Kapitel 3.6.5 bereits die wichtigsten Punkte dargelegt. Hier listen wir deshalb für beide Varianten entsprechende Testszenarien auf.

Damit die folgenden Tests durchgeführt werden können wird zusätzlich ein AAA (Authentication, Authorization, Accounting) Server benötigt, der das RADIUS Protokoll unterstützt. Wir empfehlen, die Cisco Identity Services Engine (ISE) zu verwenden. [3, 30, 15]

### **5.4.1. Extended Node**

- Verbindung zur Fabric im Layer 2 Modus
- Extended Node Onboarding mit Cisco Plug and Play Technologie
- Konfiguration/Kommunikation über mehrere Nodes, welche als Ring an der Fabric angeschlossen sind
- Orchestrierung der AAA Konfiguration
- SGT-VLAN Mapping statisch auf dem Fabric-Edge Gerät
- Zuweisung des VLANs statisch auf Port, Konfiguration via DNA Center möglich
- Multicast Konfiguration am verbundenen Port
- 802.1X Authentifizierung zwischen Extended Node und NAC Server

### **5.4.2. Policy Extended Nodes**

- Verbindung zur Fabric im Layer 2 Modus
- Policy Extended Node Onboarding mit Cisco Plug and Play Technologie
- Konfiguration/Kommunikation über mehrere Nodes, welche als Ring an der Fabric angeschlossen sind
- Orchestrierung der AAA Konfiguration
- Anwendung der Secure Group-ACL

- VLAN und SGT werden dynamisch den Endgeräten zugewiesen
- Dynamische 802.1X Authentifizierung der Endgeräte

**Teil II.**

# **Projektdokumentation**

# 1. Projektplanung

Wir suchen für die hier beschriebene Arbeit einen angemessenen Kompromiss zwischen der statischen Wasserfall-Planung und den verschiedenen, auf die moderne Softwareentwicklung zugeschnittenen Vorgehensweisen wie Rational Unified Process (RUP) oder Scrum.

Einerseits sind die Anforderungen an ein Projekt im Bereich Netzwerkdesign sehr spezifisch und decken sich nicht zwingend mit der Softwareentwicklung, andererseits sind nachträgliche Anpassungen an Anforderungen oder Vorgehensweise doch möglich und sollten nicht von vornherein ausgeschlossen werden.

## 1.1. Phasen/Meilensteine

Zur groben Planung unseres Projektes verwenden wir vier Phasen, die wir basierend auf dem Rational Unified Process in der Bezeichnung auf unser Projekt anpassen. Der Projektplan befindet sich im Anhang C.

Phase	RUP	Ergebnis
Einstieg	Inception	<ul style="list-style-type: none"> <li>▪ Zielformulierung</li> <li>▪ Anwendungsfälle</li> <li>▪ Wesentliche Risiken formuliert</li> </ul>
Ausarbeitung	Elaboration	<ul style="list-style-type: none"> <li>▪ Detaillierte Beschreibung von Anwendungsfällen</li> <li>▪ Business- und technische Anforderungen</li> <li>▪ Kritische Risiken adressiert</li> </ul>
Design	Construction	<ul style="list-style-type: none"> <li>▪ Mehrere Designvorschläge zur Erfüllung der erarbeiteten Anforderungen</li> <li>▪ Empfehlung basierend auf diesen Anforderungen sowie Best Practices im Netzwerkkumfeld</li> <li>▪ Proof of Concept in Rapperswil</li> </ul>
Implementationsplan	Transition	<ul style="list-style-type: none"> <li>▪ Planung und Erarbeitung Testkonzept für Pilotphase in Buchs</li> </ul>

## 1.2. Meetings

### Internes Review Meeting mit Advisor

Zyklus: wöchentlich, Dauer: 1 Stunde

Inhalt:

- Präsentation des aktuellen Projektfortschritts
- Feedback und Inputs abholen
- Besprechen des weiteren Vorgehens

## Planungsmeeting im Projektteam

Zyklus: wöchentlich, Dauer: flexibel, max. 1 Stunde

Inhalt:

- Strukturieren der Ergebnisse vom Review Meeting
- Pflege des Backlogs und Planung des anstehenden Sprints

## Definierte Meetings mit dem Kunden

Zyklus: Definiert im Projektplan

Inhalt: Jeweils spezifisch nach Thema des entsprechenden Meilensteins.

## 1.3. Rollen

Aufgrund des kleinen Projektteams und eigenen Voraussetzungen in einem Netzwerkprojekt sind keine expliziten Rollen definiert. Der Backlog wird jeweils durch beide Studierenden in Abstimmung miteinander gepflegt und aktualisiert.

Dank des jeweiligen Arbeitsverhältnisses kann der Kontakt zum Kunden durch Luzia Kündig sichergestellt werden, der Kontakt zum Betreuer durch Jan Untersander.

## 1.4. Risikomanagement

Risiken werden bewertet in folgenden Schweregraden: **Hoch**, **Mittel**, **Klein**

- **Schweregrad / Risiko**
  - **Massnahmen**

1. **Klein** / Zusammenarbeit intern EW Buchs zwischen Infrastruktur und Provider nicht ideal
  - 1.1 04.10.22: Aktueller Stand der Informationen deutet darauf hin, dass eine eigene Lösung implementiert werden wird, ohne Verwendung von Provider-Infrastruktur.
2. **Klein** / Unterschiedliches Mass an Vorwissen im Bereich Netzwerk innerhalb des EWB.
  - 2.1 03.10.22: Es besteht die Möglichkeit dass die IT Abteilung den Support des neuen Netzwerks übernimmt.
3. **Mittel** / Vollständigkeit/Aktualität der bestehenden Netzwerkdokumentation ist unklar
  - 3.1 03.10.22: Alle vorhandenen Dokumente welche das EWB haben wir erhalten, zudem konnten wir Traffic in den verschiedenen Netzwerken sniffen.
  - 3.2 07.10.22: Eine Auskunftsanfrage an Rittmeyer wurde versendet, weitere Analysen stehen noch aus.
  - 3.3 18.10.22: Neue Bewertung: **Klein** / Auskunft von Rittmeyer ist eingetroffen, spezielle Qualitätsanforderungen an das Netzwerk sind ausschliesslich im Bereich Verfügbarkeit vorhanden. Der aktuelle Stand der Dokumentation ist für den erwarteten Projektscope ausreichend.
4. **Klein** / Wir als Studierende führen zum ersten Mal ein Projekt durch, bei welchem wir eine Netzwerkarchitektur designen müssen.
  - 4.1 04.10.22: Laurent Metzger hat langjährige Erfahrung in Projekten in diesem Bereich und kann uns deshalb sehr gut beraten.



4.2 25.11.22: Weitere Unterstützung durch Patrick Mosimann (Cisco) sowie Raphael Holenweger (EWB Informatik) ist gegeben.

## **1.5. Arbeitspakete**

Der aktuelle Stand der offenen und laufenden Aufgaben wird in [Jira](#) <sup>1</sup> geführt.

---

<sup>1</sup><https://sa-ewb.atlassian.net/jira/software/projects/SE/boards/1>

**Teil III.**

**Anhang**

## A. Aufgabenstellung

### Aktuelle Situation

Das Elektrizitäts- und Wasserwerk der Stadt Buchs beschäftigt ca. 120 Mitarbeitende, unter anderem in den Bereichen Infrastruktur (Strom und Wasser), Kommunikation (Providergeschäft Rii Seez Net) und Informatik.

Versorgungsgebiet der Infrastruktur ist die Kleinstadt Buchs im St. Galler Rheintal. Zur Verwaltung und Steuerung sämtlicher Anlagen besteht zurzeit ein innerhalb des Bereichs selbst verwaltetes, physisch komplett eigenständiges Glasfasernetzwerk.

### Eckdaten des aktuellen Netzwerks

**Für öffentliche  
Version entfernt**

Abbildung A.1.: Leittechnikkonzept

- Bestehende Glasfaserleitungen, teilweise bis zu 35 Jahre alt, teilweise direkt in Stromleitungen integriert
- Für drei logische Netzwerke werden physisch separate Geräte betrieben und eigene Glasfasern eingesetzt
- Ursprüngliche Architektur: mehrere Ringe
- 3 Verwendungszwecke
  - Überwachung, Alarmierung Infrastrukturanlagen (TS-LAN)
  - Kraftwerk-Steuerung (Rittmeyer-LAN)
  - Überwachung Steuerungs-Software, ZFA, diverses (MMI-LAN)
- Steuerungs-Stationen werden im Verwaltungsgebäude des EW Buchs ebenfalls in einem eigenen Netz verwaltet, unabhängig vom Büro-Netzwerk

## **Fertigstellung Glasfasernetzwerk Buchs**

Im Jahr 2021 konnte der Bereich Infrastruktur mit dem Ausbau ihres eigenen Glasfasernetzes in Buchs eine Abdeckung von 90 Prozent erreichen, 100 Prozent sind für das Jahr 2024 geplant. Dieses Netz besteht aus jeweils 4 Fasern pro Wohneinheit, die an Dritte zur Erbringung von Telekommunikationsdienstleistungen vermietet werden können. Zusätzlich dazu wurden pro Gebäude zwei separate Fasern zur eigenen Nutzung (Smart Metering, Gebäudetechnik etc.) verlegt.

An dieses neue Netzwerk werden auch sämtliche Infrastrukturanlagen angeschlossen. Somit besteht eine solide physische Grundlage, um eine neue Architektur zu planen und schlussendlich auch umzusetzen.

## **Ziel dieser Arbeit**

Erheben von Anforderungen in Bezug auf Funktion, Verfügbarkeit, Sicherheit und Wartbarkeit, Vereinfachung wo möglich.

Erarbeiten einer neuen Netzwerkarchitektur basierend auf den physischen und organisatorischen Gegebenheiten.

Gegenüberstellung der Möglichkeiten, Vor- und Nachteile von folgenden Varianten:

- Bezug Netzwerkdienstleistungen von Provider (Rii Seez Net)
- Selbst verwaltete, providerunabhängige Lösung

## B. Einrichtungsassistent - Screenshots

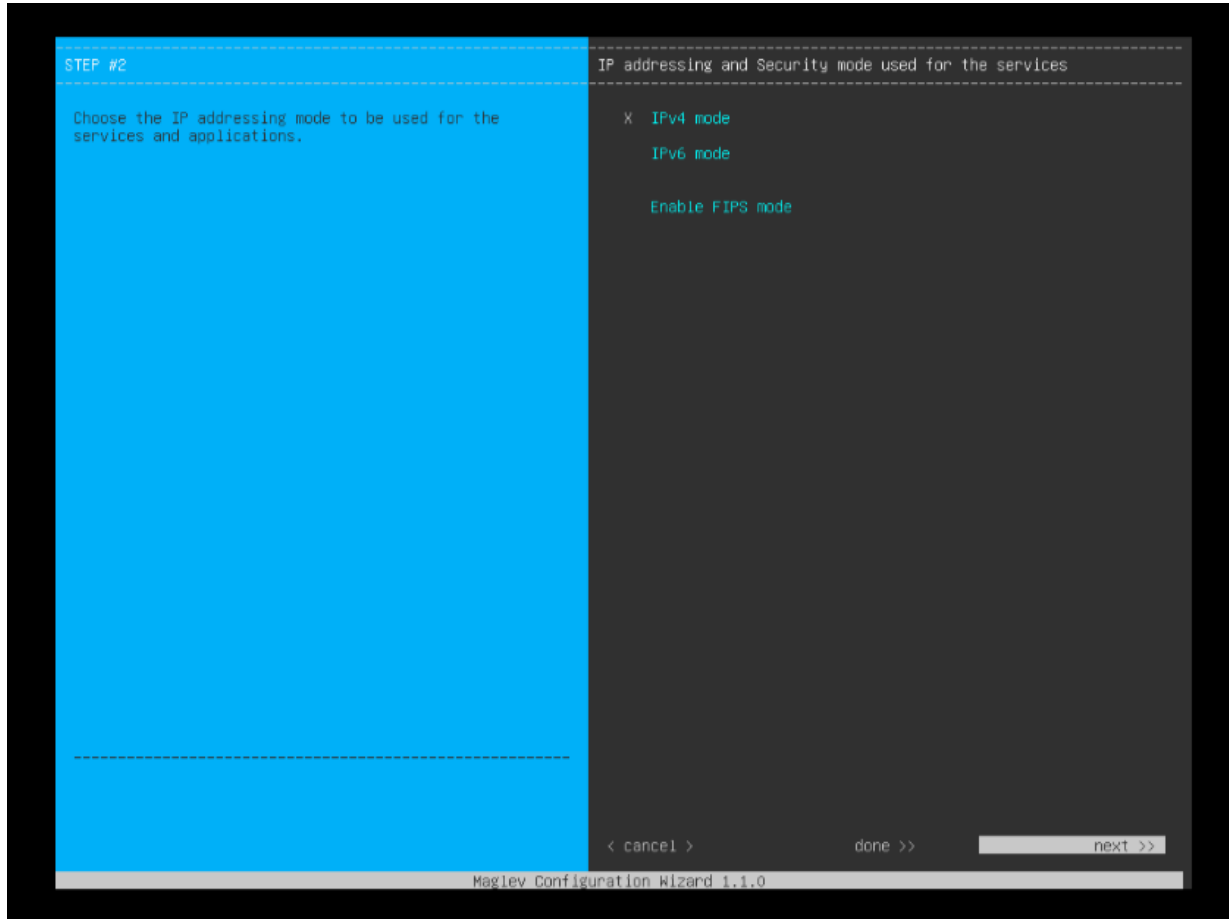


Abbildung B.1.: DNA Center Setup Wizard 2

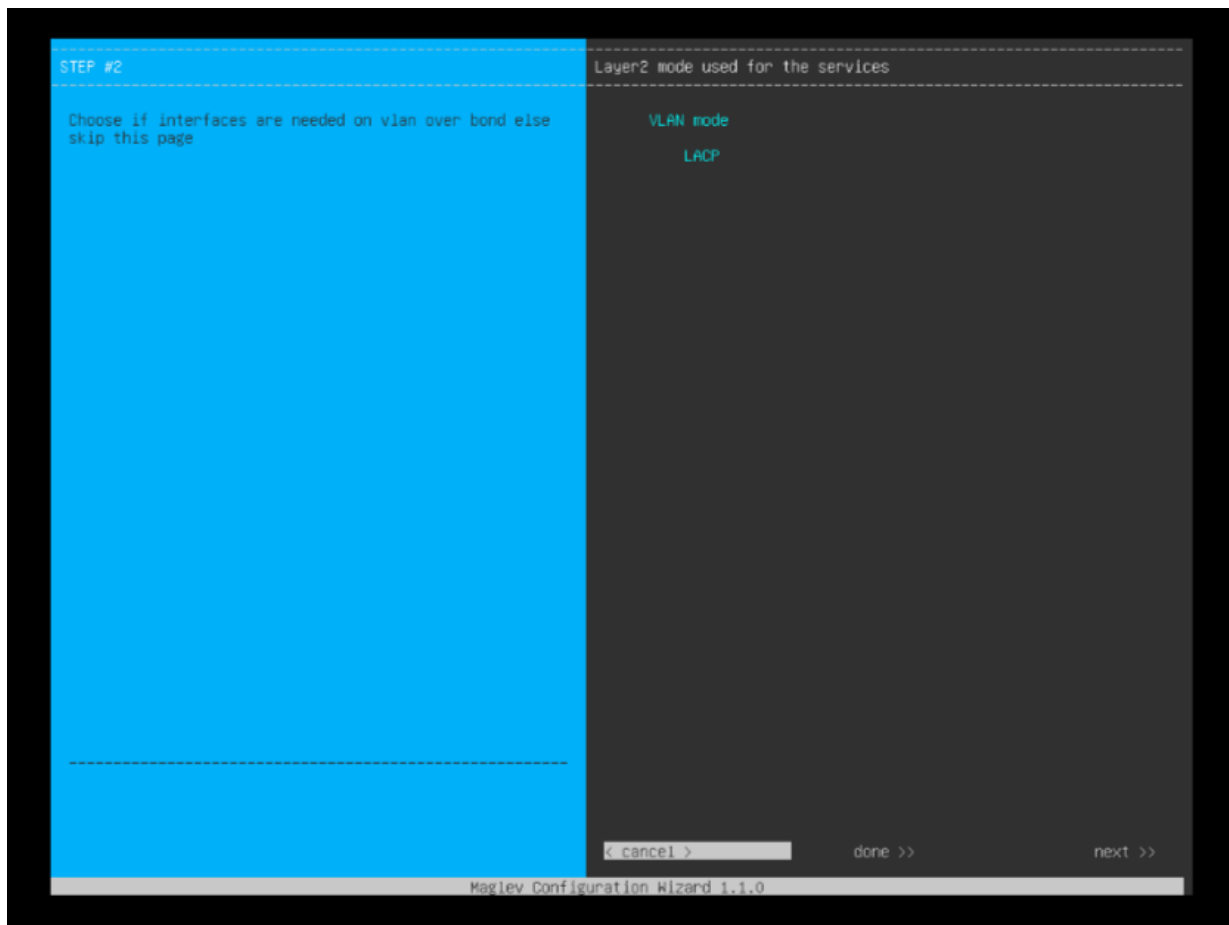


Abbildung B.2.: DNA Center Setup Wizard 3

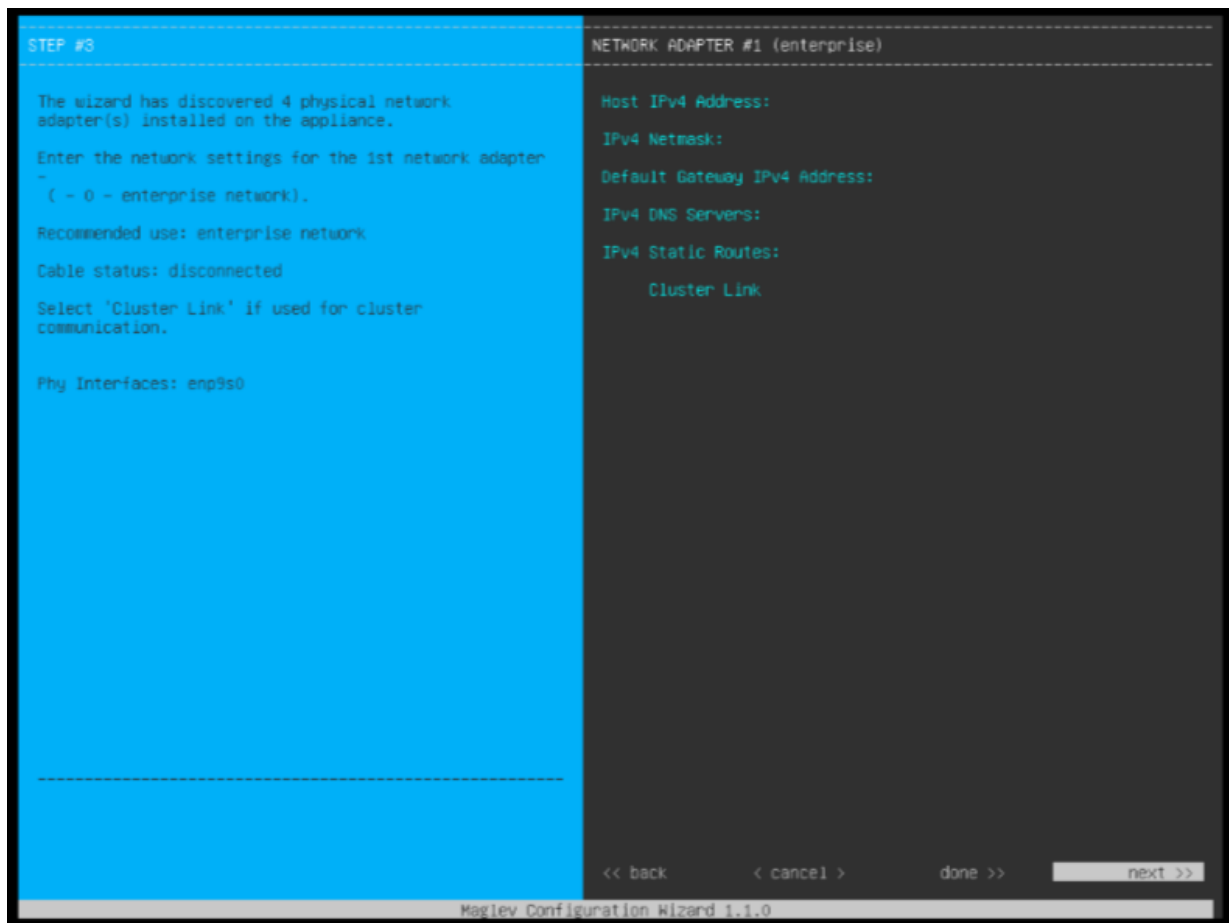


Abbildung B.3.: DNA Center Setup Wizard 4

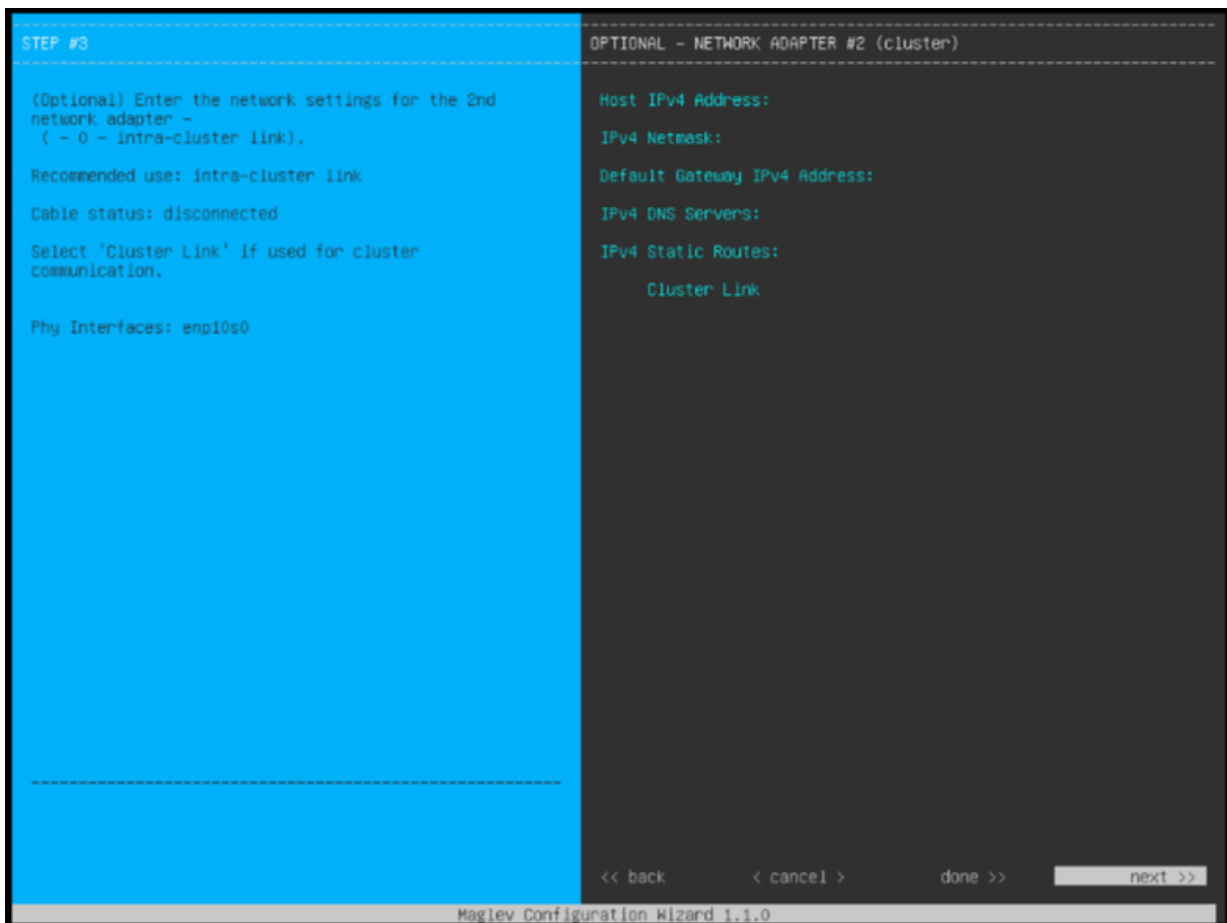


Abbildung B.4.: DNA Center Setup Wizard 5



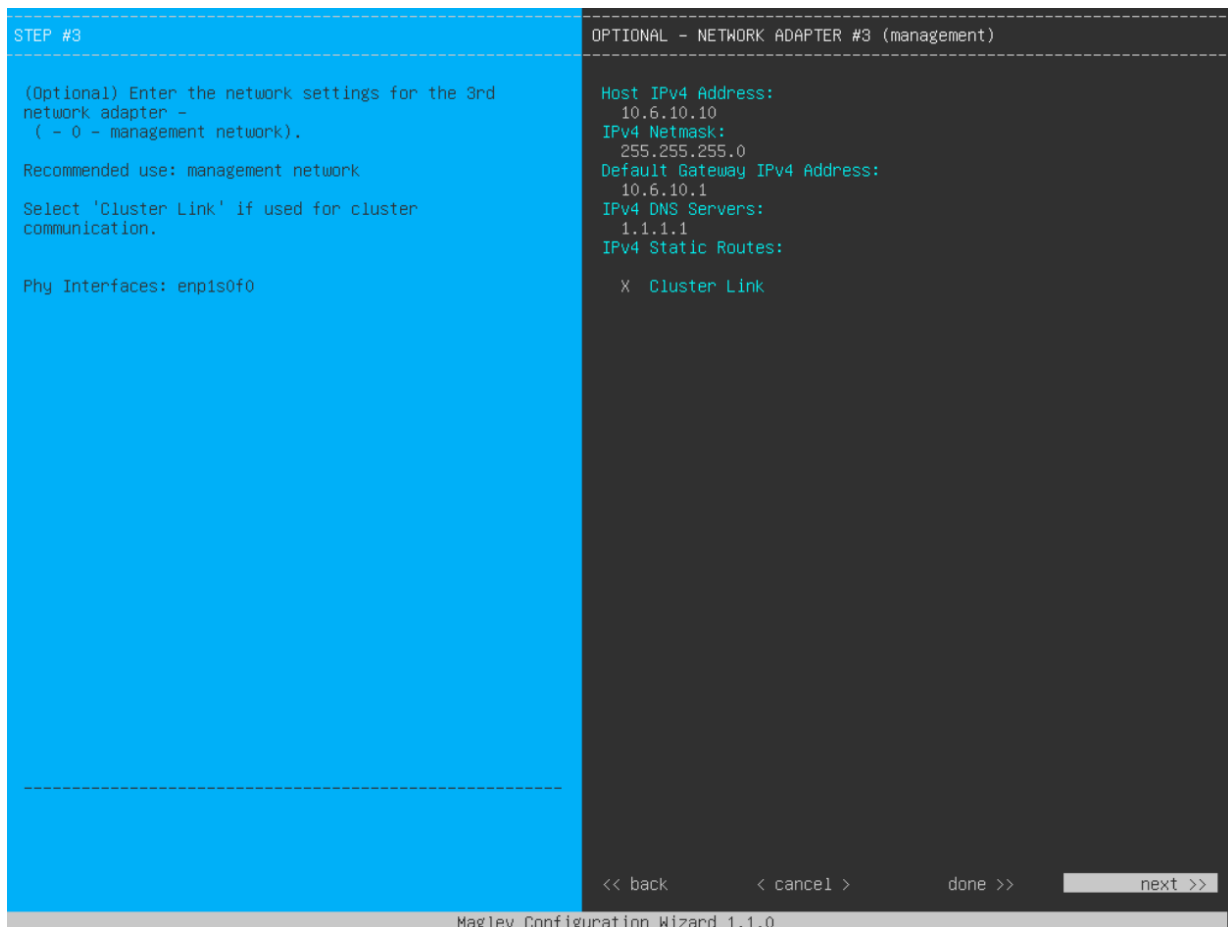


Abbildung B.5.: DNA Center Setup Wizard 6

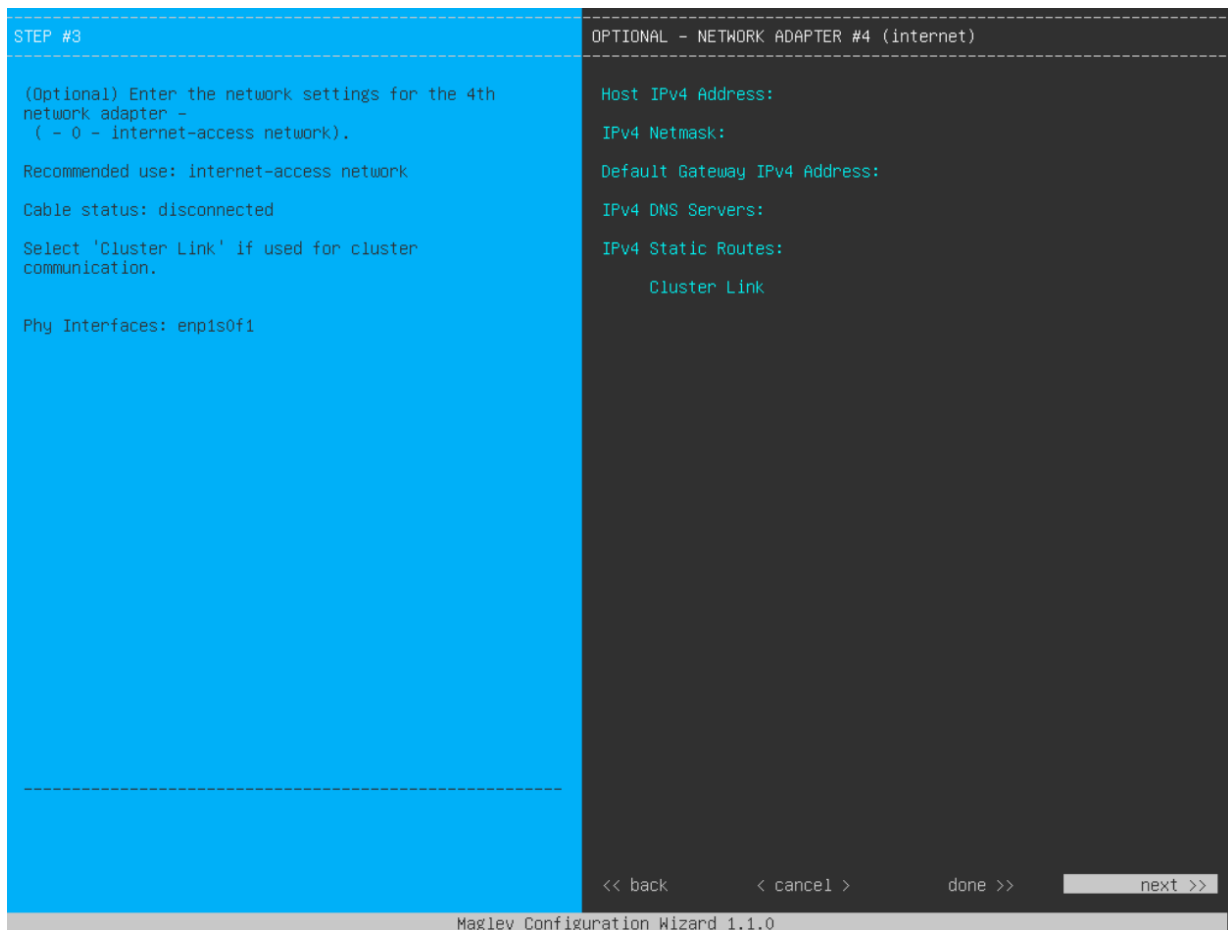


Abbildung B.6.: DNA Center Setup Wizard 7

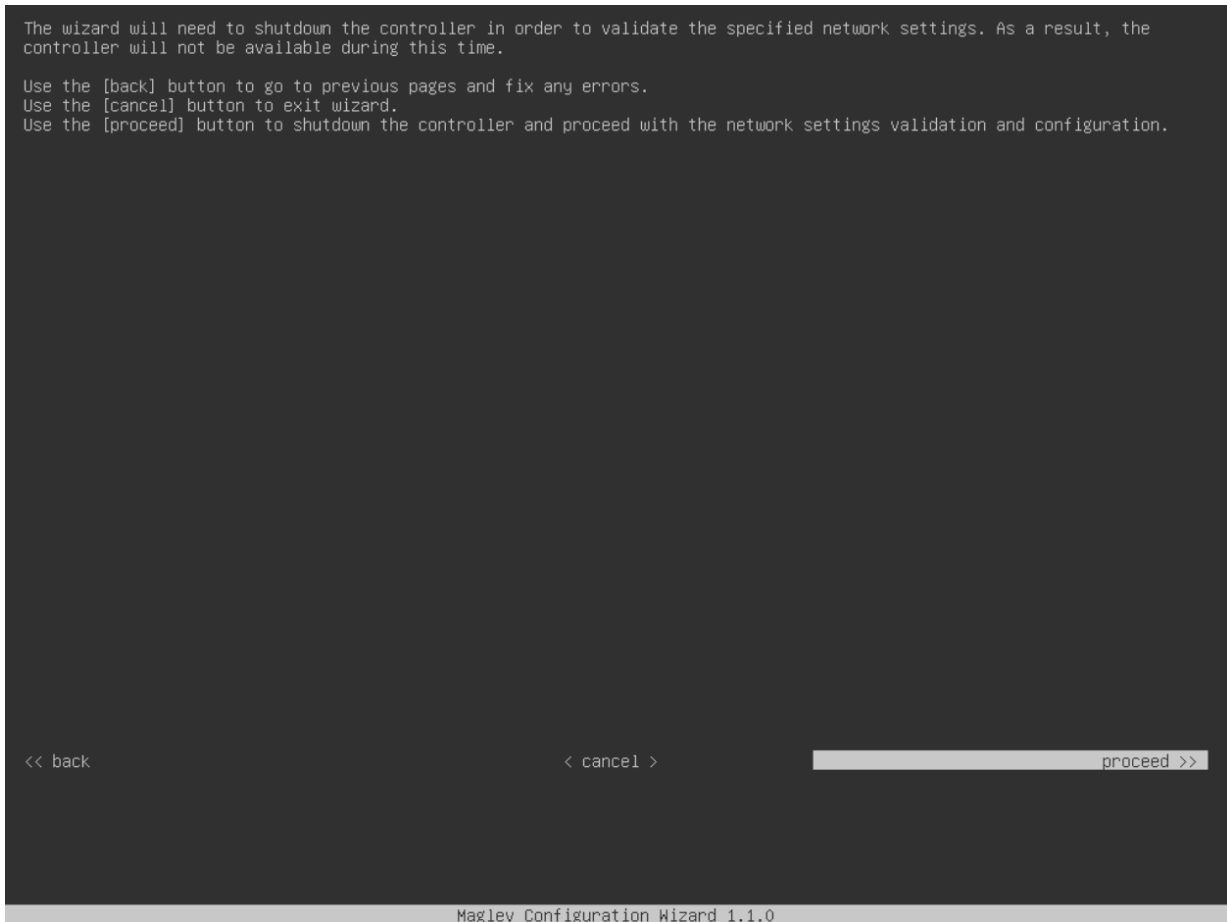


Abbildung B.7.: DNA Center Setup Wizard 8

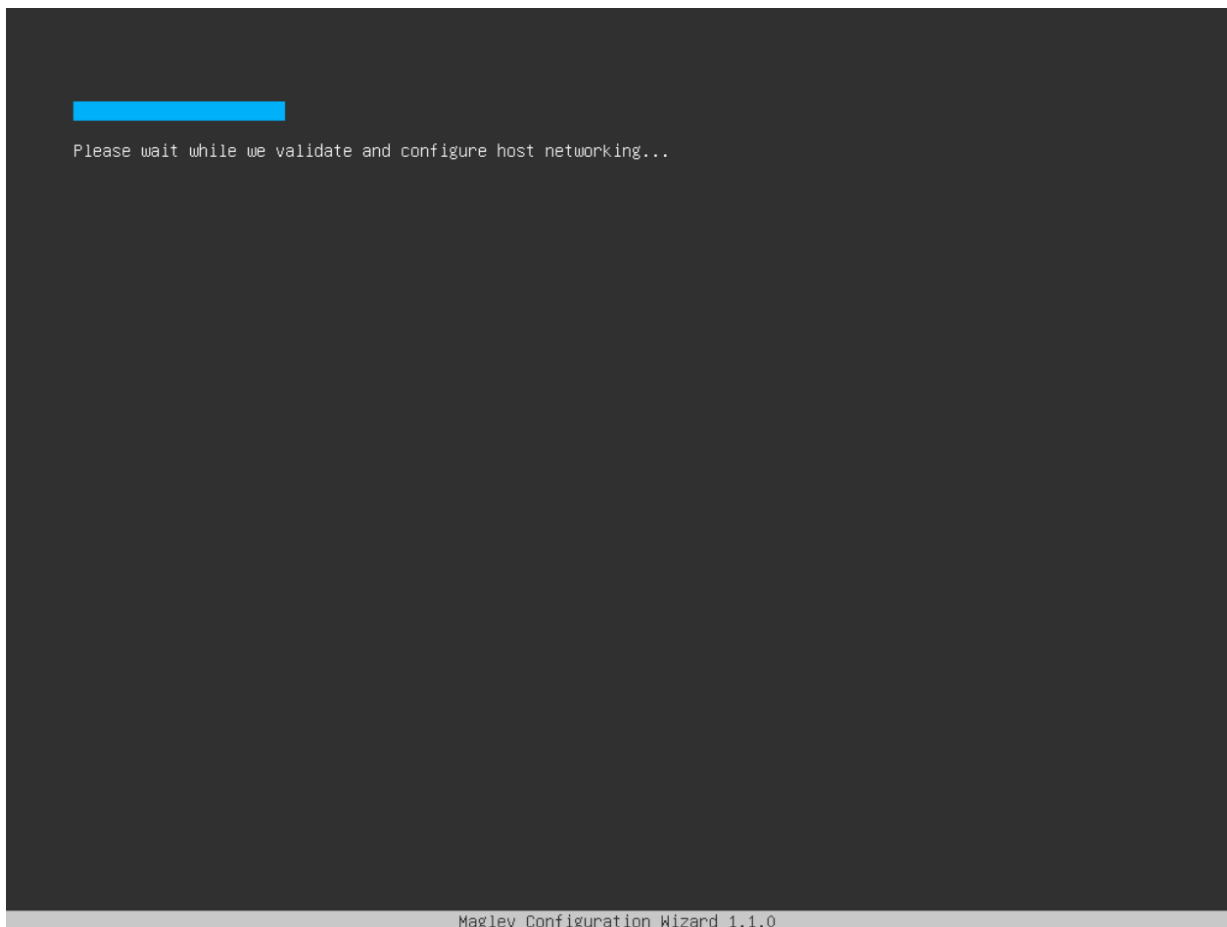


Abbildung B.8.: DNA Center Setup Wizard 9

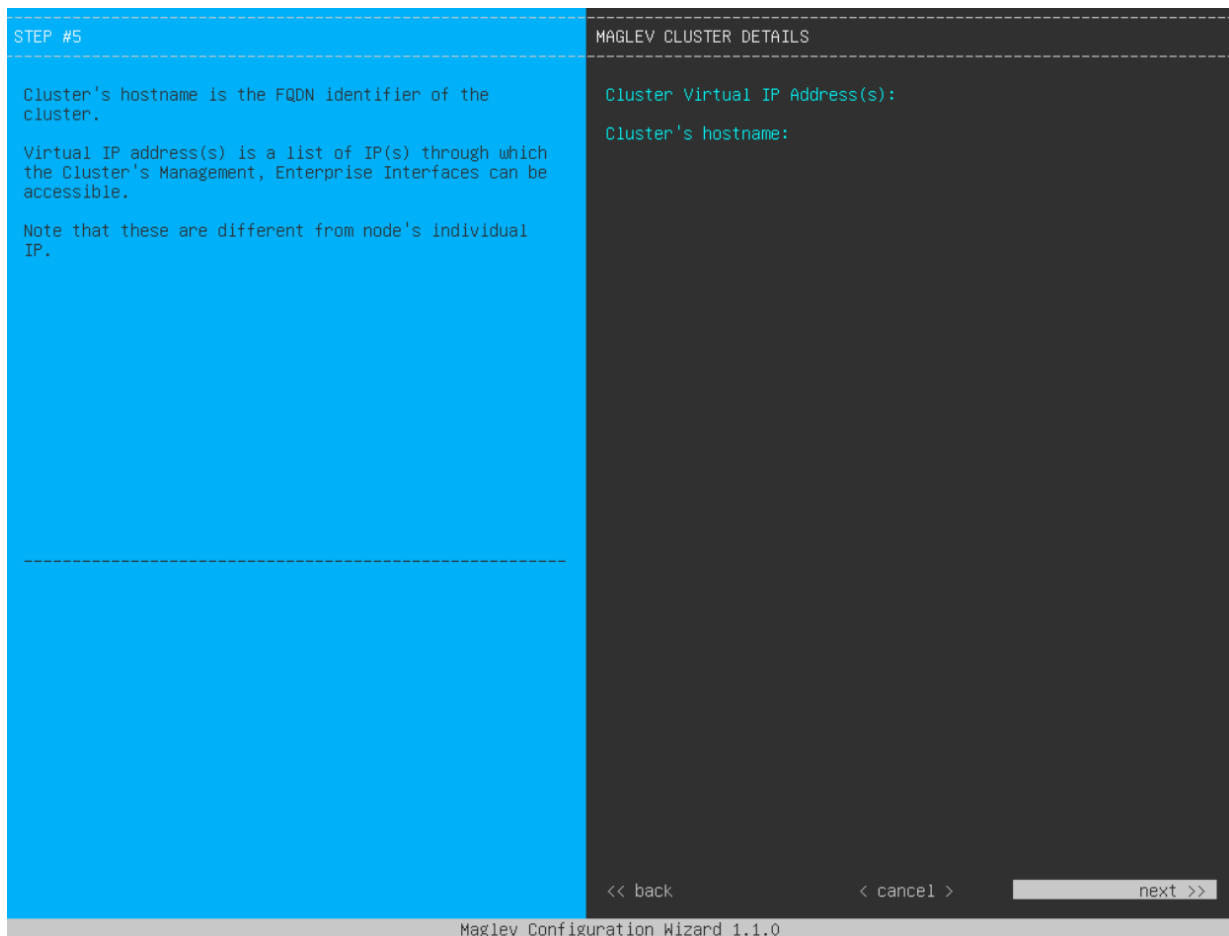


Abbildung B.9.: DNA Center Setup Wizard 10

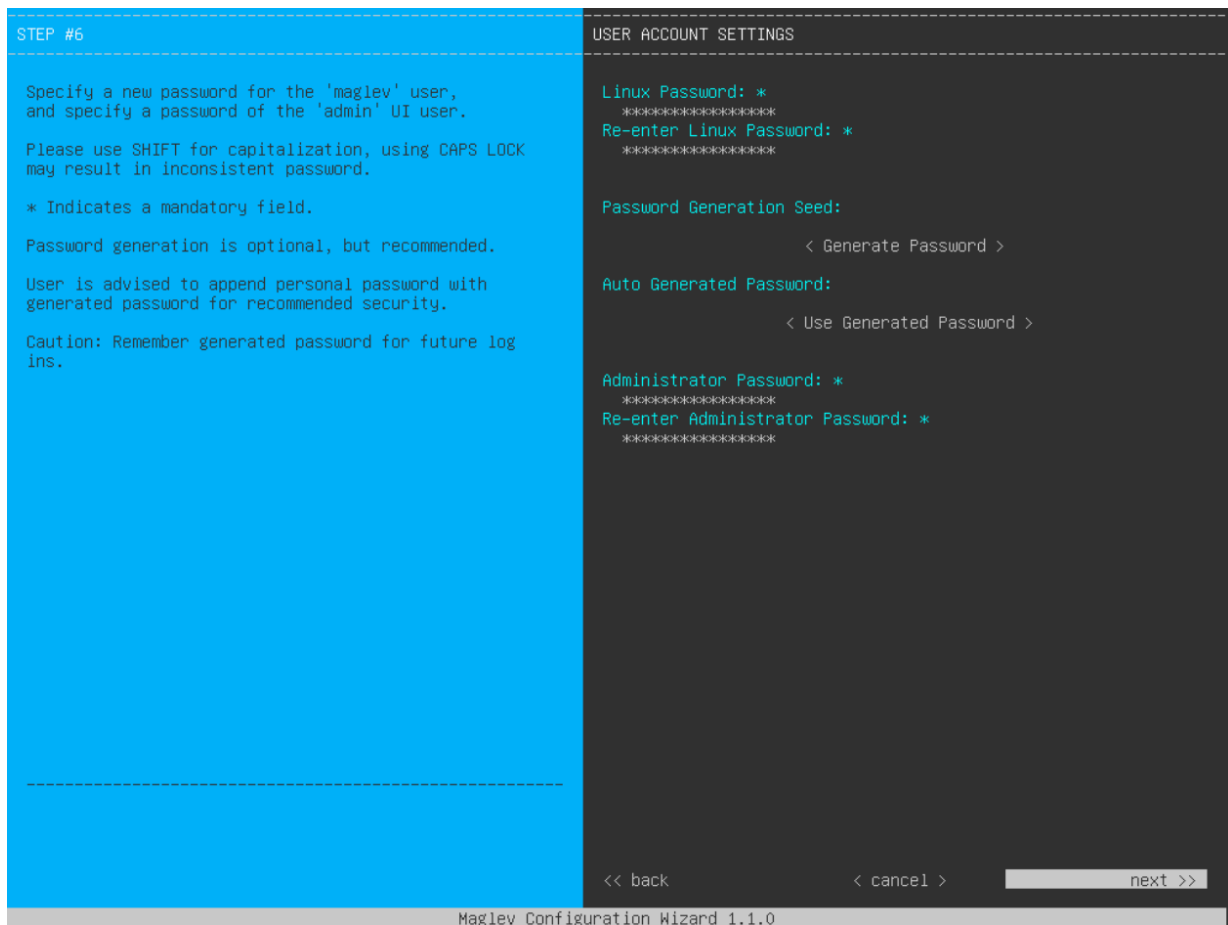


Abbildung B.10.: DNA Center Setup Wizard 11

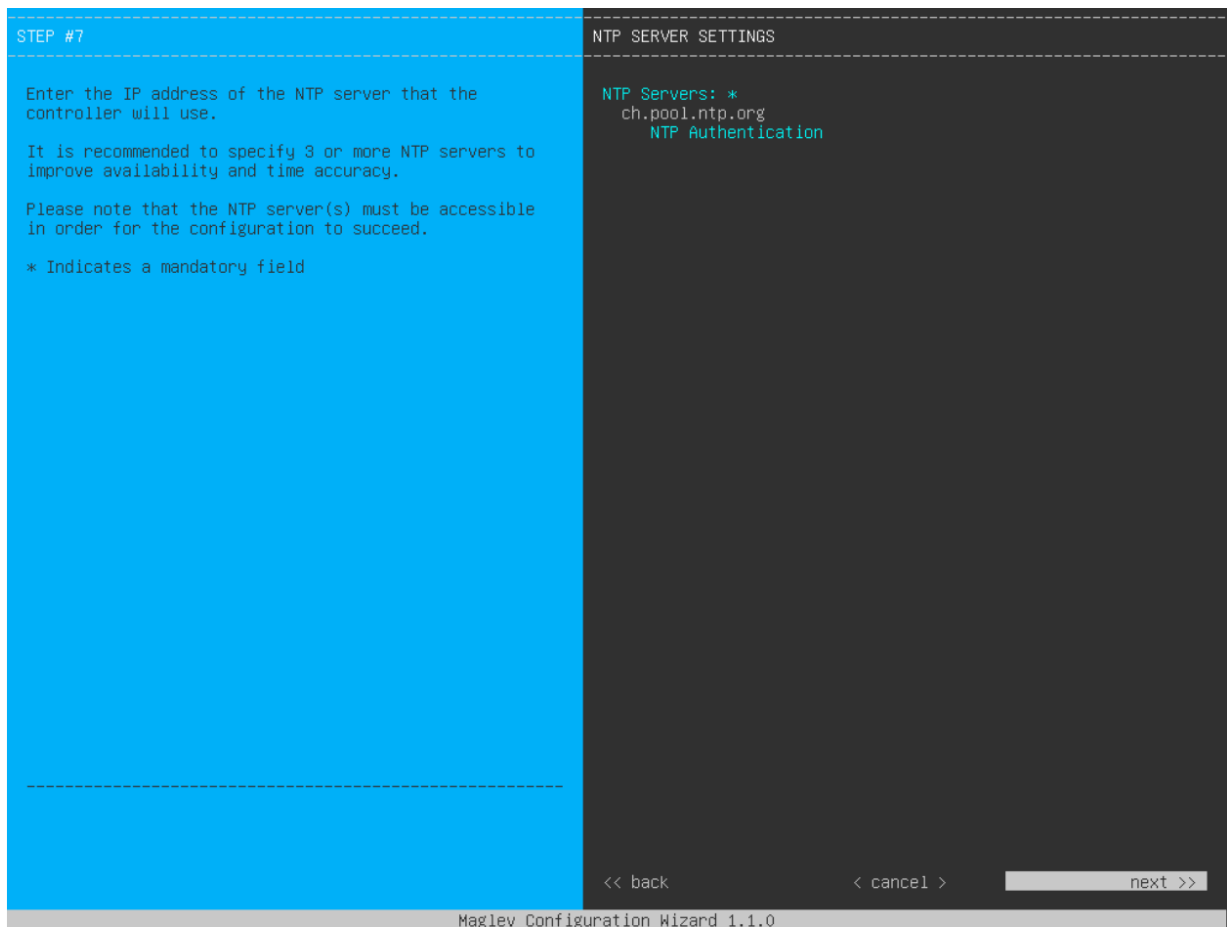


Abbildung B.11.: DNA Center Setup Wizard 12

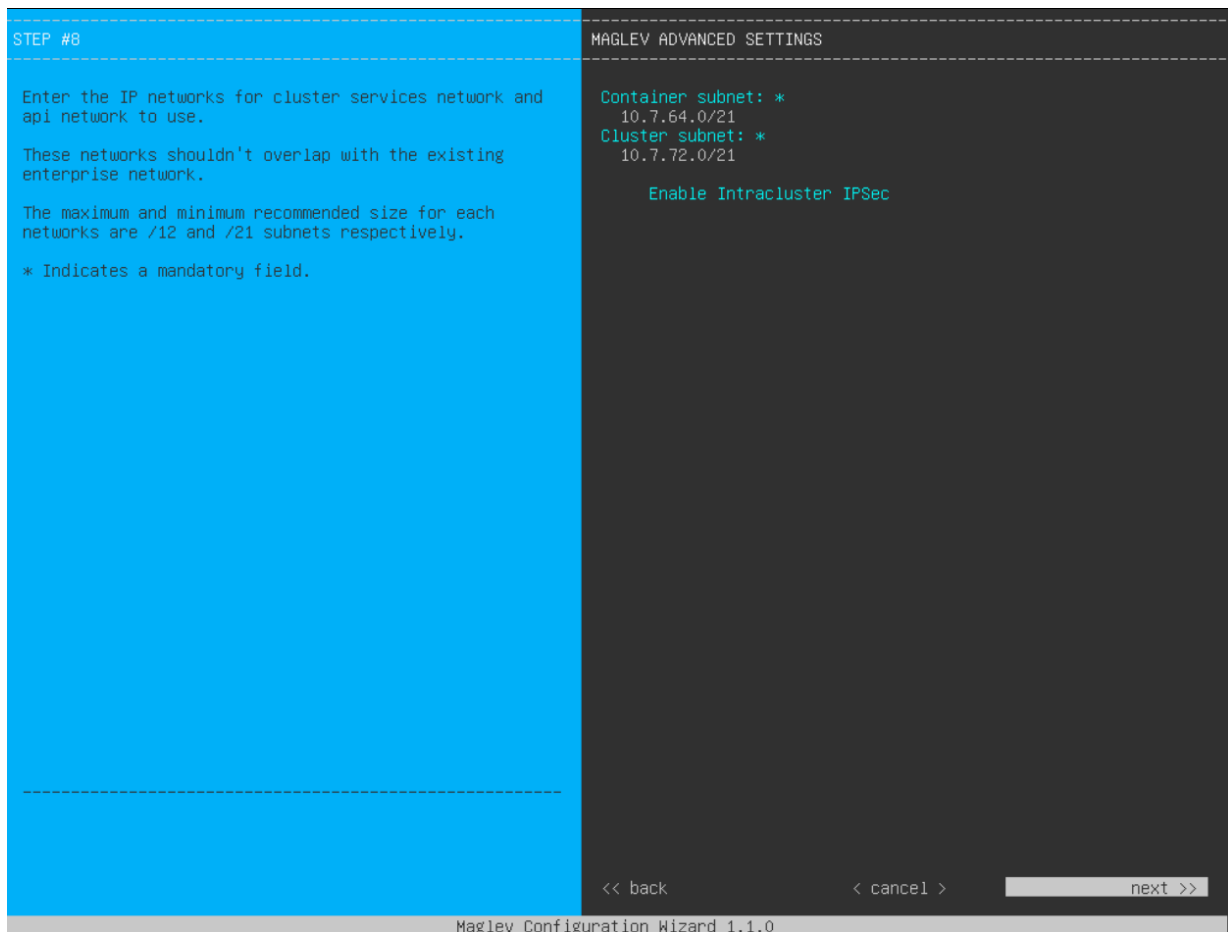


Abbildung B.12.: DNA Center Setup Wizard 13



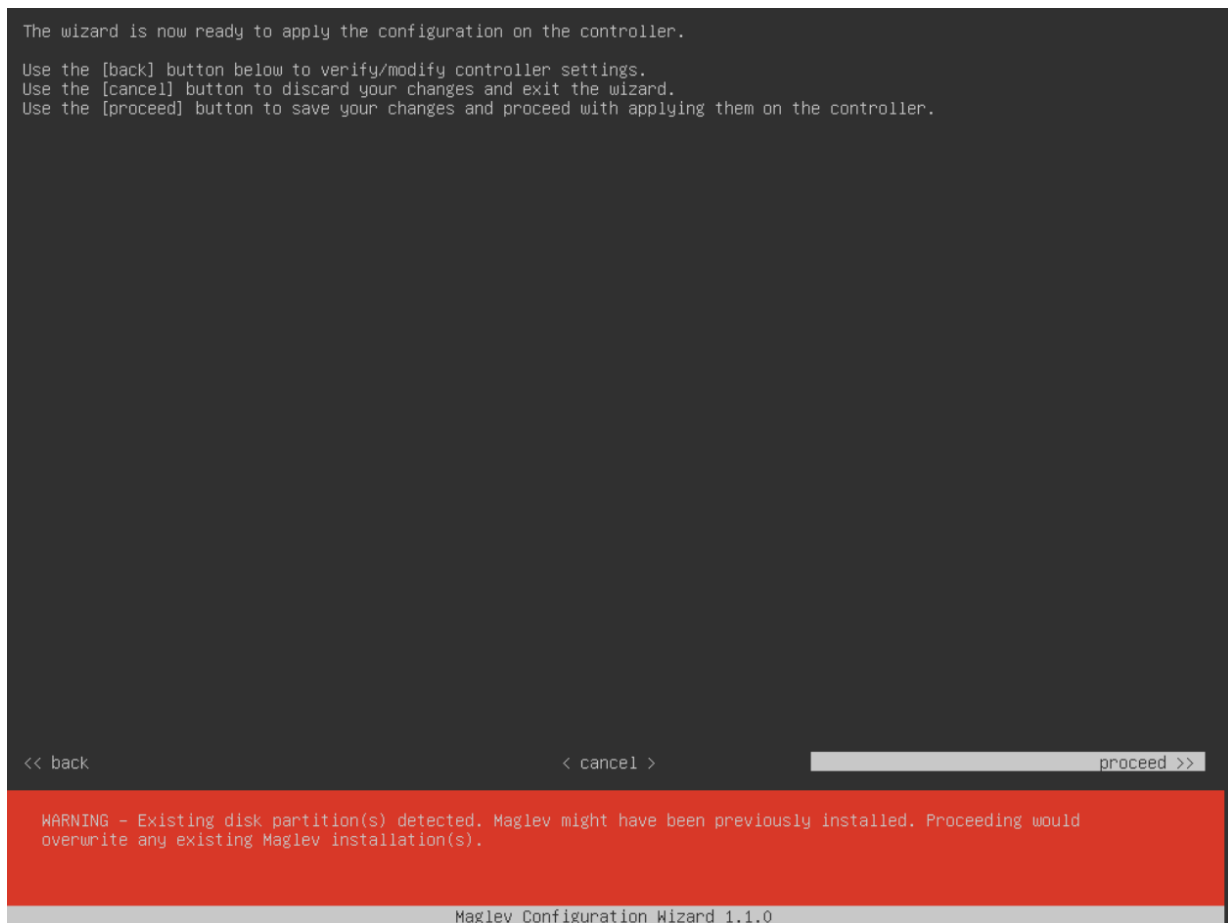


Abbildung B.13.: DNA Center Setup Wizard 14

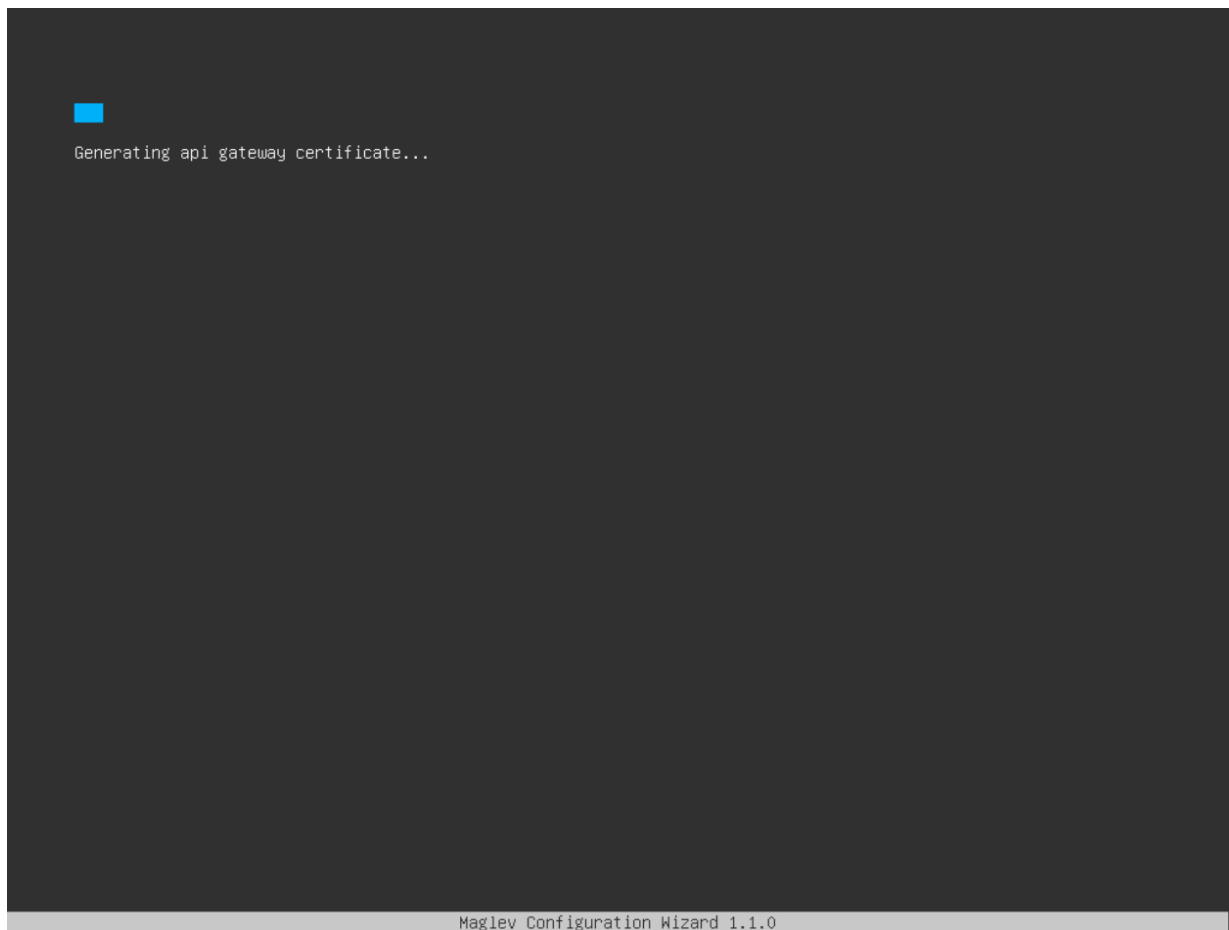


Abbildung B.14.: DNA Center Setup Wizard 15

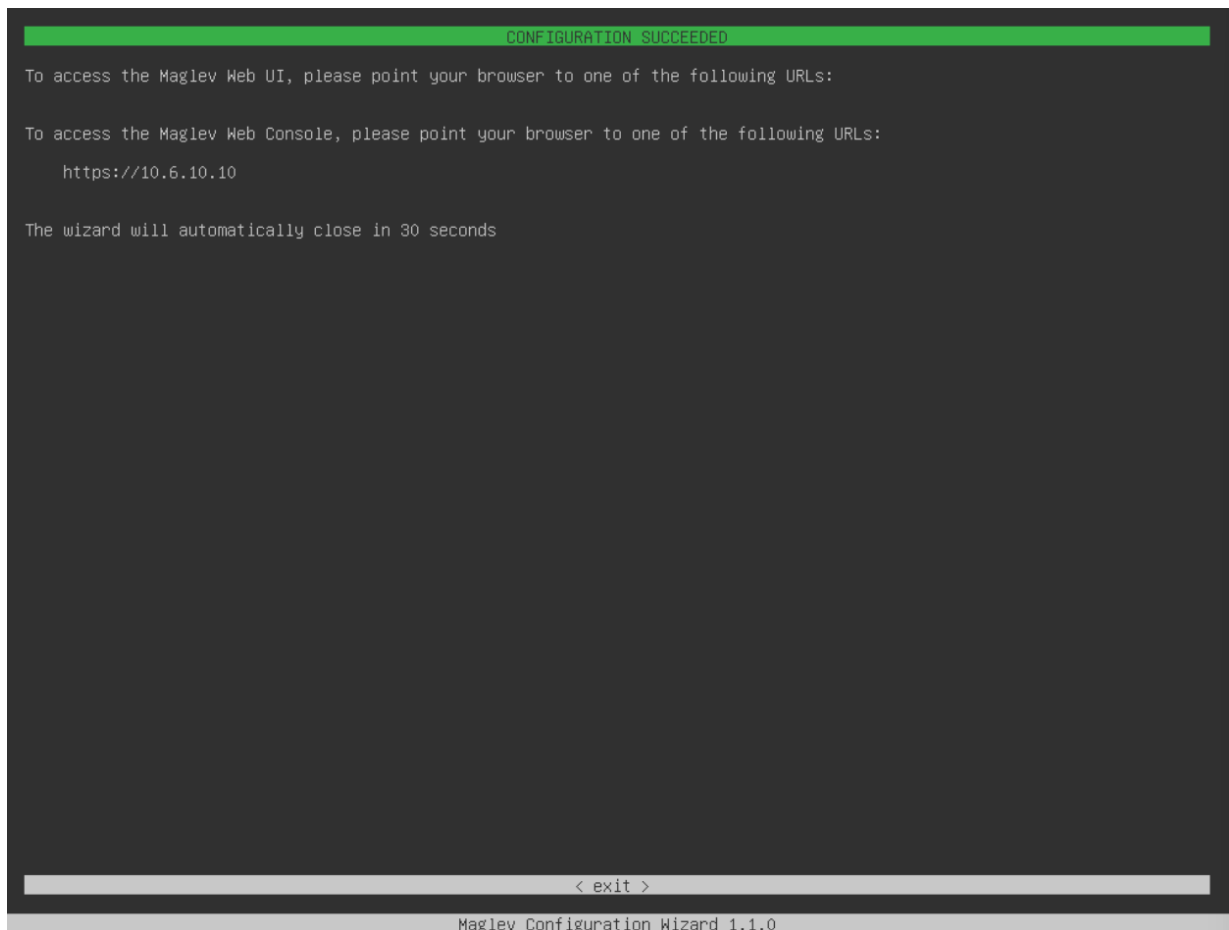
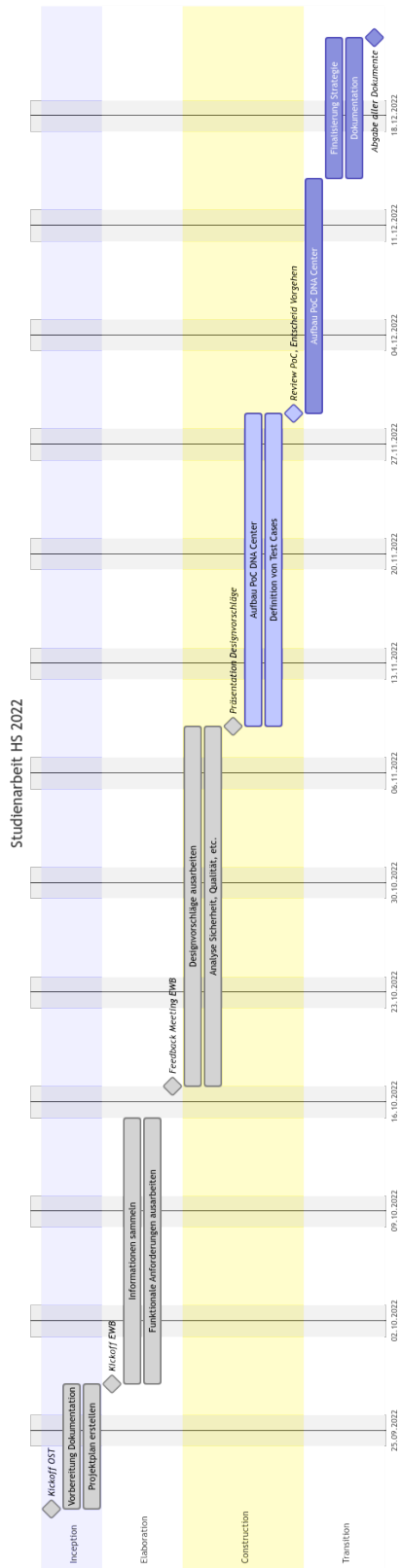


Abbildung B.15.: DNA Center Setup Wizard 16

# C. Projektplan



## D. Glossar

Tabelle D.1: Glossar

Begriff	Bedeutung
FTTx	Sammelbegriff für verschiedene Glasfaser-Ausbaustandards. Varianten sind Fiber To The Home (FTTH), Fiber To The Building (FTTB), Fiber To The Curb (FTTC).
Layer 2	Netzwerkkommunikation auf Layer 2 basiert auf MAC Adressen und Broadcast
Layer 3	Netzwerkkommunikation auf Layer 3 basiert auf IP Adressen und Routing
VLAN	Virtuelles LAN, wird zur logischen Trennung von verschiedenen Netzwerken verwendet.
MPLS	Multi Protocol Label Switching. Kann als Enkapsulierungsprotokoll zum Transport von Layer 2 oder Layer 3 Netzwerkpaketen z.B. über ein Providernetz verwendet werden.
VXLAN	Virtual eXtensible LAN. Enkapsuliert Layer 2 oder Layer 3 Pakete, bevorzugt im Datacenter-Umfeld.
BGP	Border Gateway Protocol. Wird im Internet verbreitet verwendet als stabiles, sehr gut skalierendes Routing-Protokoll. Standardmässig werden IPv4 Adressen übertragen.
MP-BGP	Multiprotocol Border Gateway Protocol. Erweiterung von BGP, erlaubt das gleichzeitige Austauschen von verschiedenen Adress-Typen, nicht nur IPv4.
EVPN	Ethernet VPN. Verwendet MP-BGP, um eine Control Plane für Layer 2 oder Layer 3 Overlay Netzwerke zu schaffen.
Konvergenz	Zeitdauer nach einer Netzwerkänderung, bis alle Geräte im gesamten Netz die aktualisierte Topologie kennen und ihre Routing-Tabellen entsprechend aktualisiert haben.
Unicast	Standard der Netzwerkkommunikation. Ein Paket ist an genau einen Empfänger gerichtet.
Multicast	Spezielle Art der Adressierung, spezielle IP-Adress-Bereiche werden für Multicast-Verkehr verwendet. Empfänger sind Gruppen von mehreren Geräten, die sich für den Empfang registrieren und abmelden können. Die Gruppen werden auf den Netzwerkgeräten verwaltet.
Broadcast	Netzwerktraffic, dessen Ziel nicht bekannt ist oder explizit an alle Geräte im Netz gerichtet ist. Verwendet spezielle MAC (ff.ff.ff.ff.ff) oder IP Adresse (Die jeweils letzte im Subnetz)
Ethernet	Standardprotokoll für Layer 2 Netzwerkverkehr.
VPN	Virtual Private Network. Ende zu Ende verschlüsselte Verbindung zwischen zwei Geräten. Varianten sind Client to Site (von einem Client zu einem Netzwerkgerät) oder Site to Site (zwischen zwei Netzwerkgeräten).
DMZ	DeMilitarisierte Zone. Bezeichnet ein Netzwerkbereich, der von ausserhalb des eigenen Firmennetzwerks für gewisse Dienste erreichbar ist.

Fortsetzung auf der nächster Seite

Tabelle D.1: Glossar (Fortsetzung)

<b>Begriff</b>	<b>Bedeutung</b>
POP	Point of Presence. Zentrale Verteilstelle eines Netzwerkproviders.
OSI Schichtenmodell	Grundlegende Theorie zur Netzwerkkommunikation. Verschiedene Funktionalität wird verschiedenen Schichten zugeordnet.
MAC Adresse	Dient zur Adressierung von Geräten auf OSI Schicht 2. Der Erste Teil bezeichnet den Hersteller, der zweite Teil ist die für den Hersteller eindeutige ID des Gerätes.
MAC Learning	Switches oder andere Netzwerkgeräte speichern in einer Tabelle, an welchem Port welche MAC-Adresse verbunden ist. So können sie eingehende Pakete direkt nur auf dem richtigen Port weiterleiten, anstelle von auf allen Ports.
Load Balancing	Verteilen von Last auf verschiedenen Wegen. Viele Varianten möglich.
Equal Cost Multipath	Wenn in einer Routing-Tabelle zwei verschiedene Wege ans selbe Ziel genau die selben Kosten haben, können die eingehenden Pakete zu Load Balancing Zwecken auf die beiden Wege verteilt werden.
Header, Headertypen	Für jede Schicht des OSI-Modells wird dem Netzwerkpaket ein Header hinzugefügt, der die relevanten Informationen zur Verarbeitung beinhaltet. Standardmässig wird ein Paket in Layer 2 (Ethernet), Layer 3 (IP) und Layer 4 (TCP oder UDP) mit einem Header versehen.
Underlay	Möglichst einfaches, performantes Layer 3 Netzwerk, dass auf einem Standard-Routingprotokoll oder auch MPLS basiert.
Overlay	Mittels Encapsulierung von Paketen und entsprechender Logik können Ende-zu-Ende Verbindungen über ein Underlay erstellt werden. Die beiden Endgeräte sehen das Underlay Netzwerk nicht.
En- / Dekapsulierung	Wird dann angewendet, wenn ein Paket mehrere Male einen Header derselben Schicht erhält. Ein soweit fertiges Netzwerkpaket erhält weitere Header von bestimmten Schichten, um eine Overlay / Underlay Funktionalität zu ermöglichen. Wird auch als Tunneling bezeichnet.
Netzwerkfabric, Fabric	Kombination von Overlay und Underlay, um verschiedenste Anwendungsfälle auf demselben Netzwerk abzudecken.
Data Plane	Netzwerkschicht, welche für das Weiterleiten der Pakete zuständig ist.
Control Plane	Netzwerkschicht, welche steuert, wie die Daten in der Data Plane weitergeleitet werden.
Zero Trust	Bezeichnet ein Zugriffsmodell, welches ein neues Gerät im Netzwerk grundsätzlich als unsicher einstuft. Erst, wenn es sich erfolgreich authentisiert hat, werden die entsprechenden Zugriffe freigeschaltet.
802.1X	Standard zur Port-basierten Authentifizierung von Geräten auf Netzwerkebene.
EAP-TLS	Protokoll zur Authentifizierung mittels Zertifikaten.
MSCHAPv2	Protokoll zur Authentifizierung unter Angabe von Benutzername und Passwort.
MAC-Bypass	Das Endgerät wird basierend auf der MAC Adresse authentifiziert.

Fortsetzung auf der nächster Seite

Tabelle D.1: Glossar (Fortsetzung)

<b>Begriff</b>	<b>Bedeutung</b>
Supplicant	Ein Endgerät, welches sich im Netzwerk authentifizieren will.
Authenticator	Netzwerkgerät, welches die Anfrage vom Supplicant entgegennimmt und diese an den Authentication Server weiterleitet.
Authentication Server	Datenbank, die Identitäten und Richtlinien verwaltet. Zum Beispiel Cisco ISE.
Access Port	Netzwerk-Port, an dem ein Endgerät angeschlossen ist.
Trunk Port	Netzwerk-Port, der zur Kommunikation zwischen zwei Switches dient.
VLAN Tag	Identifikator im Ethernet Header, der ein Netzwerkpaket einem VLAN zuordnet.
Spanning Tree Protokoll	Protokoll zur Vermeidung von Loops in Layer 2-Netzwerktopologien. Erstellt aus der Topologie einen eindeutigen Baum ohne Schleifen und blockiert die redundanten Verbindungen.
Root Bridge	Switch, der für die Berechnung des Spanning Tree zuständig ist. Wird nach einem bestimmten Algorithmus ausgewählt.
BPDU	Bridge Protocol Data Unit. Netzwerkpaket, dass zur Abstimmung des Spanning Tree Protokoll unter allen Switches ausgetauscht wird.
PVST	Per VLAN Spanning Tree. Definiert einen separaten Baum derselben Topologie für jedes logische Netz.
P-Router	Provider Router. Kommuniziert nicht direkt mit einem Kunden, ist für die Weiterleitung innerhalb eines Netzwerk-Underlays verantwortlich.
PE-Router	Provider Edge Router. Bildet den Übergang vom Providernetz zum Kunden. Führt normalerweise En- sowie Dekapsulierung durch.
CE-Router	Customer Edge Router. Kundengerät, das direkt mit dem Provider Edge Router kommuniziert.
MPLS Label	Das MPLS Label definiert innerhalb des MPLS Protokolls, wohin das Paket innerhalb vom Underlay weitergeleitet wird.
IGP	Interior Gateway Protocol. Gruppe von Routing-Protokollen, welche innerhalb von geschlossenen Netzwerken oder Organisationen verwendet werden. Verbreitete Beispiele davon sind Open Shortest Path First (OSPF) oder Intermediate System - Intermediate System (IS-IS).
VTEP	Virtual Tunnel Endpoint. In VXLAN Netzwerken für die En- oder Dekapsulierung verantwortlich. Verbindet die Endgeräte mit der Netzwerk-Fabric.
VNI	VXLAN Network Identifier. Ähnlich einer VLAN ID. Bei VXLAN steht mit dem VNI eine viel grössere Anzahl von virtuellen Netzen zur Verfügung.
TCP	Layer 4 Protokoll für Applikationsdaten, Session-basiert.
UDP	Layer 4 Protokoll für Applikationsdaten, unidirektional. Wird beispielsweise für Streaming verwendet.
Cisco SDA	Software Defined Access, eine Lösung von Cisco zur automatisierten Verwaltung von Overlay Netzwerken und weitere Funktionalität.

Fortsetzung auf der nächster Seite

Tabelle D.1: Glossar (Fortsetzung)

<b>Begriff</b>	<b>Bedeutung</b>
Cisco DNA	Cisco Digital Network Architecture,
OpenFlow	Standard der Open Networking Foundation, beschreibt die komplette Zentralisierung von Control Plane auf Netzwerkgeräten.
VRFs	Virtual Routing and Forwarding. Ein Mechanismus zum parallelen Betrieb von mehreren Routing Tabellen. Kann zur Trennung von verschiedenen Kunden auf derselben Layer 3 Netzwerk-Hardware verwendet werden.
RBAC	Role Based Access Control. Beschreibt die Steuerung von Zugriffsberechtigungen basierend auf Gruppen oder Rollen.
API	Application Programmable Interface. Definition, wie verschiedene Softwaresysteme untereinander interagieren können.
Microsoft Active Directory	Lösung von Microsoft zur Verwaltung verschiedenster Ressourcen innerhalb einer Domäne. Speziell Benutzer und Gerätekonten.
Identity Provider	Ein System, welches eine Datenbank an Usern oder Geräten führt. Beispielsweise Active Directory.
Identity Server	System, welches Antworten auf explizite Authentifizierungsanfragen gibt. Bezieht Informationen vom Identity Provider.
Cisco ISE	Identity Services Engine. Policy Management und Control Authentication Server von Cisco. Verwaltet User Identitäten und Zugriffsrechte.
Control Plane Node	Führt Informationen über Endgeräte und deren aktuellen Standort innerhalb der Fabric.
Intermediate Node	Fabric Node, der nur für die Weiterleitung innerhalb des Underlay Netzwerk zuständig ist. Hat keinerlei Berührung zu oder Kenntnis von Netzwerken außerhalb der Fabric.
Border Node	Stellt den Übergangspunkt von der Fabric zu externen Services, typischerweise Datacenter oder Internet, dar.
Fabric Edge Node	Stellt den Eintrittspunkt für Endgeräte in die Fabric dar, bei VXLAN gleich einem VTEP. Führt die En- und Dekapsulierung von Netzwerkpaketen durch.
Extended Node	Mit Fabric Edge Verbundener Switch an dem Endgeräte angeschlossen werden mit reduzierter Funktionalität.
Policy Extended Node	Bietet zusätzlich eine feingranulare Isolation von Endgerät-Gruppen.
LISP	Location Identity Separation Protocol. Führt eine Datenbank, welche Endgeräte an welchem Fabric Edge Node verbunden sind. Diese Informationen werden laufend von den Edge Nodes aktualisiert.
Cisco TrustSec / SGT	TrustSec bzw. Secure Group Tag: ID im Header eines Netzwerkpakets, die eine granulare Verwaltung von Zugriffsrechten bzw. Richtlinien ermöglicht.
Virtuelle Netzwerke VN	Analog zu VLANs innerhalb einer Cisco SDA Fabric.



## Literatur

- [1] Ed. A. Sajassi u. a. *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*. RFC 7432. RFC Editor, Feb. 2015. URL: <https://www.rfc-editor.org/rfc/rfc7432>.
- [2] T. Bates u. a. *Multiprotocol Extensions for BGP-4*. RFC 4760. RFC Editor, Jan. 2007. URL: <https://www.rfc-editor.org/rfc/rfc4760>.
- [3] Mike Cifelli. *SDA Extended Node Tips*. Nov. 2022. URL: <https://community.cisco.com/t5/software-defined-access-sd-access/sda-extended-node-tips/td-p/3994324>.
- [4] Cisco. *Cisco DNA Center 2.3.3 Documentation*. Okt. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/bulletins/b\\_cisco\\_dna\\_center\\_2\\_3\\_3\\_doc\\_roadmap.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/bulletins/b_cisco_dna_center_2_3_3_doc_roadmap.html).
- [5] Cisco. *Cisco DNA Center First-Generation Appliance Installation Guide, Release 2.3.3*. Okt. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/install\\_guide/1stgen/b\\_cisco\\_dna\\_center\\_install\\_guide\\_2\\_3\\_3\\_1stGen.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/install_guide/1stgen/b_cisco_dna_center_install_guide_2_3_3_1stGen.html).
- [6] Cisco. *Cisco Extended Enterprise non-fabric and SD-Access fabric Design Guide*. Sep. 2022. URL: <https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-dg/ee-dg.html>.
- [7] Cisco. *Cisco SD-Access Solution Design Guide (CVD)*. Sep. 2022. URL: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>.
- [8] Cisco. *Cisco SD-Access: Endpoint Analytics and Zero Trust Framework How to Demo*. Okt. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec\\_1-99/Dot1X\\_Deployment/Dot1x\\_Dep\\_Guide.html#wp386716](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386716).
- [9] Cisco. *Cisco Validated Designs*. Sep. 2022. URL: <https://www.cisco.com/go/cvd>.
- [10] Cisco. *Cisco Validated Designs for Power Utilities and Renewable Energy*. Sep. 2022. URL: <https://www.cisco.com/c/en/us/solutions/design-zone/industries/power-utilities.html>.
- [11] Cisco. *LAN Automation: Step-by-step deployment guide and Troubleshooting*. Nov. 2022. URL: <https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/215336-lan-automation-step-by-step-deployment.html>.
- [12] Cisco. *Recommended Releases for Catalyst 9200/9300/9400/9500/9600 and Catalyst 3650/3850 Platforms*. Okt. 2022. URL: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-series-switches/214814-recommended-releases-for-catalyst-9200-9.html>.
- [13] Cisco. *Stacking and High Availability Configuration Guide, Cisco IOS XE Bengaluru 17.5.x (Catalyst 9300 Switches)*. Okt. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-5/configuration\\_guide/stck\\_mgr\\_ha/b\\_175\\_stck\\_mgr\\_ha\\_9300\\_cg/managing\\_switch\\_stacks.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-5/configuration_guide/stck_mgr_ha/b_175_stck_mgr_ha_9300_cg/managing_switch_stacks.html).
- [14] Cisco. *Wired 802.1X Deployment Guide*. Sep. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec\\_1-99/Dot1X\\_Deployment/Dot1x\\_Dep\\_Guide.html#wp386716](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386716).
- [15] cisco. *Cisco DNA Center User Guide, Release 2.3.3*. Nov. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/user\\_guide/b\\_cisco\\_dna\\_center\\_ug\\_2\\_3\\_3.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/user_guide/b_cisco_dna_center_ug_2_3_3.html).
- [16] cisco. *Cisco Software-Defined Access FAQ*. Sep. 2022. URL: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-09-sda-faq-cte-en.html>.

- [17] cisco. *What Is a Network Fabric?* Sep. 2022. URL: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-fabric.html>.
- [18] OPC Foundation. *Unified Architecture*. Sep. 2022. URL: <https://opcfoundation.org/about/opc-technologies/opc-ua/>.
- [19] C. Hill u. a. *Cisco Software-Defined Access*. 2019.
- [20] *IEC 60870*. Sep. 2022. URL: [https://de.wikipedia.org/wiki/IEC\\_60870](https://de.wikipedia.org/wiki/IEC_60870).
- [21] «IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks». In: *IEEE Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014)* (2018), S. 1–1993. DOI: [10.1109/IEEESTD.2018.8403927](https://doi.org/10.1109/IEEESTD.2018.8403927).
- [22] «IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control». In: *IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018)* (2020), S. 1–289. DOI: [10.1109/IEEESTD.2020.9018454](https://doi.org/10.1109/IEEESTD.2020.9018454).
- [23] Fay Lee. *Allowed List Policy Considerations for SD-Access*. Sep. 2020. URL: <https://community.cisco.com/t5/networking-knowledge-base/allowed-list-policy-considerations-for-sd-access/ta-p/4048032>.
- [24] M. Mahalingam u. a. *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*. RFC 7348. RFC Editor, Aug. 2014. URL: <https://www.rfc-editor.org/rfc/rfc7348>.
- [25] Rekhter u. a. *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. RFC Editor, Jan. 2006. URL: <https://www.rfc-editor.org/rfc/rfc4271>.
- [26] E. Rosen, A. Viswanathan und R. Callon. *Multiprotocol Label Switching Architecture*. RFC 3031. RFC Editor, Jan. 2001. URL: <https://www.rfc-editor.org/rfc/rfc3031>.
- [27] A. Sajassi u. a. *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*. RFC 8365. RFC Editor, März 2018. URL: <https://www.rfc-editor.org/rfc/rfc8365>.
- [28] National Institute of Standards und Technology. *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*. FIPS. NIST, März 2019. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>.
- [29] Peter Welcher. *SD-Access and the Internet of Things (IOT)*. Dez. 2021. URL: <https://netcraftsmen.com/sd-access-and-the-internet-of-things-iot/>.
- [30] Jacob Zartmann. *SD-Access with Extended Nodes*. Nov. 2022. URL: [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/user\\_guide/b\\_cisco\\_dna\\_center\\_ug\\_2\\_3\\_3.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/user_guide/b_cisco_dna_center_ug_2_3_3.html).

# Abbildungsverzeichnis

1.	Wasserkraft . . . . .	3
2.	Logisches Schema Variante 3 . . . . .	4
1.1.	Leittechnikkonzept des EW Buchs (Firma Rittmeyer) . . . . .	10
1.2.	Netzwerkschema physisch Leitstelle EWB . . . . .	11
1.3.	Analyseergebnisse TS LAN . . . . .	12
1.4.	Analyseergebnisse KW LAN . . . . .	13
1.5.	Analyseergebnisse MMI LAN . . . . .	14
1.6.	Logisches Netzwerkschema der Firma Rittmeyer . . . . .	15
3.1.	FTTx Netz . . . . .	20
3.2.	OSI Schichtenmodell . . . . .	21
3.3.	Beispiel Layer 2 . . . . .	21
3.4.	Spanning Tree . . . . .	22
3.5.	Beispiel Layer 3 . . . . .	23
3.6.	Layer 2 over Layer 3 Tunnel . . . . .	24
3.7.	Authentisierung via 802.1X . . . . .	25
3.8.	Variante VLAN . . . . .	26
3.9.	VLAN Teil im Ethernet Header . . . . .	26
3.10.	Mögliche Architektur mit VLAN . . . . .	27
3.11.	Variante BGP EVPN . . . . .	29
3.12.	MPLS Enkapsulierung . . . . .	30
3.13.	VXLAN Enkapsulierung . . . . .	31
3.14.	Variante Software Defined Access . . . . .	33
3.15.	Cisco SDA Fabric Control Plane [19] . . . . .	35
3.16.	Cisco DNA Center Schnittstellen [19] . . . . .	36
3.17.	Cisco SDA Fabric mit Extended Nodes [19] . . . . .	37
3.18.	SGT Matrix [23] . . . . .	38
3.19.	Extended Node vs Policy Extended Node [6] . . . . .	39
3.20.	Cisco SDA Ausbau Schritt 1 . . . . .	40
3.21.	Cisco SDA Ausbau Schritt 2 . . . . .	41
4.1.	DNA Center Setup Wizard . . . . .	46
4.2.	Standorte im Cisco DNA Center . . . . .	49
4.3.	IP Adresspools . . . . .	50
4.4.	IP Adressen Import Feature . . . . .	50
4.5.	Software Image Repository . . . . .	51
4.6.	Template Editor mit Beispielen . . . . .	52
4.7.	Discovery Einstellungen für das vorkonfigurierte Seed Device . . . . .	54
4.8.	Switch ist im initialen Setup Status . . . . .	55
4.9.	Starten der LAN Automation . . . . .	56
4.10.	LAN Automation Status Seite . . . . .	57
4.11.	Topology View kann über die Buttons oben rechts aktiviert werden . . . . .	57
4.12.	Inventory Ansicht, Geräte sind im Status Reachable und Managed . . . . .	58
4.13.	Installation der SDA Applikation . . . . .	59
4.14.	SD Access . . . . .	59
4.15.	Fabric Wizard Summary . . . . .	60
4.16.	Ansicht Fabric Infrastructure . . . . .	60

4.17. Virtuelle Netze . . . . .	61
4.18. Einstellungen Virtuelles Netzwerk innerhalb der Fabric . . . . .	62
4.19. Port Channel erstellen . . . . .	64
4.20. Erfolgreich konfigurierte Extended Nodes . . . . .	65
4.21. Übersicht über alle Switches und deren Ports . . . . .	65
4.22. Port Assignment Optionen . . . . .	66
A.1. Leittechnikkonzept . . . . .	75
B.1. DNA Center Setup Wizard 2 . . . . .	77
B.2. DNA Center Setup Wizard 3 . . . . .	78
B.3. DNA Center Setup Wizard 4 . . . . .	79
B.4. DNA Center Setup Wizard 5 . . . . .	80
B.5. DNA Center Setup Wizard 6 . . . . .	81
B.6. DNA Center Setup Wizard 7 . . . . .	82
B.7. DNA Center Setup Wizard 8 . . . . .	83
B.8. DNA Center Setup Wizard 9 . . . . .	84
B.9. DNA Center Setup Wizard 10 . . . . .	85
B.10. DNA Center Setup Wizard 11 . . . . .	86
B.11. DNA Center Setup Wizard 12 . . . . .	87
B.12. DNA Center Setup Wizard 13 . . . . .	88
B.13. DNA Center Setup Wizard 14 . . . . .	89
B.14. DNA Center Setup Wizard 15 . . . . .	90
B.15. DNA Center Setup Wizard 16 . . . . .	91