HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Krisenresistente Software Defined Netzwerke

Bachelorarbeit

Abteilung Informatik
Hochschule für Technik Rapperswil

Herbstsemester 2018

Autoren:	Sandro Kaspar, Jessica Kalberer
Betreuer:	Laurent Metzger
Projektpartner:	Führungsunterstützungsbasis (FUB) der Schweizer Armee
Experte:	Patrick Mosimann
Gegenleser:	Beat Stettler

Inhaltsverzeichnis

1 Aufgabenstellung

Dies ist die initiale Aufgabenstellung, welche zu Beginn der Bachelorarbeit vorlag.

1.1 Erster Teil (∼10%): Phase Analyse

Ziel: Analyse der SDA Lösung und Identifizierung der kritischen Elemente der Verfügbarkeit (LISP Database, Radius, SGT Access-list, etc.) und der Network Services (NTP, DNS, Lizenzen, etc.)

- Die Clients werden am Netz mit dot1x authentifiziert und mit Wired Access verbunden (Wireless Access ist nicht Teil der Bachelorarbeit)

1.2 Zweiter Teil (∼45%): Phase Absicherung

Ziel: Erstellung des technischen Designs und Ansätzen, um die SDA Lösung Krisenresistenter zu machen.

- Die Arbeiten umfassen:
  - Analyse und Gegenüberstellung der mögliche Optionen für die Verbindungen von zwei SDA Fabric (VRF-Lite, Transit Fabric, etc.)
  - Empfehlungen für das Deployment eines krisensicheren SDA
  - Aufbau eines Pilots mit mindestens zwei Standorten
  - Durchführung der definierten Vorgaben im Pilot
- Ein ECNS 5000 wird zur Verfügung gestellt und kann in der krisensicheren Lösung integriert sein.

1.3 Dritter Teil (∼45%): Phase Abstrahierung

Ziel: Entwicklung eines Operations Orchestrators für 2-3 Use Cases.

- Die Use cases werden von Betreuern und dem Industriepartner festgelegt.
- Der Operations Orchestrator wird bestimmte Operations Tätigkeiten vereinfachen und wird mit DNA Center, ISE und dem Fusion Router interagieren. (Wenn zwei VRFs zusammen kommunizieren, werden die Fabric und der Fusion Router gleichzeitig konfiguriert)
- Idealerweise gibt es ein Web Interfaces für Demozweck.

Notwendige Kenntnisse: Routing&Switching, VXLAN Overlays, Network Services, objektorientierte Programmierung (Python bevorzugt)

2 Abstract

2.1 Aufgabenstellung

Die Aufgabe dieser Bachelorarbeit war es, eine verteilte, krisenresistente Software-Defined Access (SDA) Lösung für die Führungsunterstützungsbasis der Armee (FUB) zu erstellen. Dies basierend auf dem DNA Center von Cisco, welches bereits in einer Studienarbeit in Betrieb genommen wurde. In einem ersten Schritt wurden die kritischen Komponenten der Lösung identifiziert und Ansätze entwickelt, wie diese Komponenten abgesichert werden können. Im darauffolgenden Schritt wurden diese Ansätze konkretisiert und umgesetzt. Der dritte Teil der Aufgabe war, ein Orchestrierungstool zu entwickeln, welches die gängigsten Operations Tasks vereinfacht und teilweise automatisiert. Folgende Use Cases soll die Anwendung abdecken:

- Netzwerke erstellen und verwalten
  - Netzwerke im DNA Center anlegen
  - Konfiguration der Fusion Router
  - Access Policies zwischen den Netzwerken konfigurieren
- Management der virtuellen Maschinen
- Anzeigen aller Konfigurationen und der dazugehörigen History

2.2 Vorgehen

In dieser Bachelorarbeit wurden grundlegende Ansätze zum Betrieb einer SDA Lösung erarbeitet, die in Zukunft weiterentwickelt werden können. Zu Beginn wurde das Lab, welches in der Studienarbeit erstellt wurde analysiert und die kritischen Komponenten, die für den Betrieb der Umgebung nötig sind, identifiziert. Zudem wurden Ideen entwickelt, wie diese kritischen Komponenten abgesichert und redundant betrieben werden können, sodass der Betrieb auch bei Ausfall von Komponenten oder Verbindungen gewährleistet ist. Ebenfalls wurde die Architektur der Umgebung analysiert und verbessert, sodass die Anforderungen an die Verfügbarkeit erfüllt sind. In einem nächsten Schritt wurden die zuvor erarbeiteten Ideen in der Testumgebung praktisch umgesetzt und getestet. Für viele Services, die in der verteilten Umgebung an allen Standorten verfügbar sein müssen, wurde eine Virtualisierungsplattform von Cisco verwendet. Im dritten Teil der Arbeit wurde ein Orchestrierungstool entwickelt. Mit Hilfe von diesem kann ein Operator die gängigsten Aufgaben über ein Web-Interface ausführen. Das Tool automatisiert zudem Arbeitsschritte, die im DNA Center noch nicht abgedeckt sind und manuell ausgeführt werden müssten.

2.3 Fazit

Es kann gesagt werden, dass die zentrale Struktur einer SDA Lösung die Sicherstellung der Verfügbarkeit in einer verteilten Umgebung erschwert. Die kritischen Komponenten, die in der Analyse definiert wurden, konnten dennoch zum grössten Teil erfolgreich abgesichert werden. Allerdings ermöglichen die zentralen Controller dieser Struktur ein programmatisches und automatisiertes Management der Infrastruktur über APIs. Nicht nur aus diesem Grund ist das Software-Defined Netzwerk (SDN) definitiv das Netzwerk der Zukunft.

3 Danksagung

Die Arbeit an diesem Projekt währe ohne die Hilfe die wir von verschiedenen Personen erhalten haben, nicht möglich gewesen. Dank ihrer Beiträge war es möglich, den Projektstand zu erreichen, den diese Arbeit jetzt hat.

- Prof. Laurent Metzger für seine ausgezeichnete Betreuung und die vielen hilfreichen Inputs
- Urs Baumann für seine wertvollen Beiträge und die ausgezeichnete Co-Betreuung
- Patrick Mosimann für die zeitnahe Beantwortung unserer vielen Fragen und Unterstützung
- Laurent Billas für die gute und konstruktive Zusammenarbeit
- Serge Pidoux für die gute und konstruktive Zusammenarbeit

Natürlich möchten wir uns auch bei den Menschen bedanken, die nicht namentlich erwähnt werden, die aber während der ganzen Bachelorarbeit mentale Unterstützung leistetenn, immer ein offenes Ohr für uns hatten und uns auf unserem Weg stets unterstützten, wie zum Beispiel unsere Familien.

4 Management Summary

4.1 Ausgangslage

Diese Bachelorarbeit ist eine Folgearbeit der Studienarbeit *Software-Defined Netzwerk im Campus Bereich* [1]. Ziel der Studienarbeit war die Evaluation des Cisco Digital Network Architecture (DNA) Center, der Software-Defined Network (SDN) Lösung von Cisco, für die Führungsunterstützungsbasis (FUB) der Schweizer Armee. In der Studienarbeit wurden mit den vorhandenen Geräten zwei Standorte geplant. Auf Grund von aufgetretenen Problemen und Bugs wurde entschieden, sich nur auf einen Standort mit mehreren Devices und zwei Gebäuden zu konzentrieren. Für diesen Standort wurde eine Fabric mit zwei Sites erstellt und diverse Policies implementiert. Somit konnten die vorgegebenen Use Cases, wie zum Beispiel die Definition von Benutzerprofilen, Benutzermobilität oder Reporting der Netzwerkaktivitäten umgesetzt und getestet werden.

4.2 Vorgehen

Nun soll in dieser Bachelorarbeit in einem ersten Schritt die SDN Lösung analysiert und sämtliche kritischen Elemente identifiziert werden. Zudem wurden Ideen entwickelt, wie diese kritischen Komponenten abgesichert und redundant betrieben werden können, sodass der Betrieb auch bei Ausfall von Komponenten oder Verbindungen jederzeit gewährleistet bleibt. In einem zweiten Schritt werden die kritischen Elemente wenn möglich abgesichert und eine Empfehlung für das Deployment eines krisensicheren SDN erarbeitet. Neu hinzu kam auch die Virtualisierungsplattform ENCS 5400, welche verwendet wurde, um einen autonomen Standort zu simulieren. Zum Abschluss erfolgt das Abstrahieren einzelner Elemente, welche im Verlauf der Bachelorarbeit noch in Use Cases definiert wurden, aus dem DNA Center in ein eigen entwickeltes Orchestrierungstool.

4.3 Ergebnisse

Als Ergebnis dieser Bachelorarbeit steht ein möglichst krisensicherer Prototyp zur Verfügung. Der Prototyp besteht aus den Cisco Komponenten sowie Eigenentwicklungen, die zusätzliche Features implementieren. Zudem steht eine Dokumentation des Systems zur Verfügung, welche eine Analyse der kritischen Komponenten, eine Empfehlung für das Deployment eines krisensicheren SDN, sowie eine Dokumentation über das entwickelte Orchestrierungstool beinhaltet. Über dieses Tool können ausserdem einzelne Standard-Aufgaben unabhängig vom DNA Center ausgeführt werden. Dies soll zum einen Aufgaben vereinfachen, in dem diese beispielsweise mit einem Wizard durchlaufen werden können.

4.4 Ausblick

Die Resultate dieser Arbeit können dazu dienen, eine möglichst krisensichere SDA Lösung in einer produktiven Umgebung in Betrieb zu nehmen. Zudem kann der Prototyp um zusätzliche Funktionen erweitert, an bestehende oder neue Systeme angebunden oder mit alternativen Lösungen verglichen werden. Durch das entwickelte Orchestrierungstool wurden die Möglichkeiten der DNA Center APIs aufgezeigt. Diese bieten schon viele Möglichkeiten. Allerdings sind viele API Endpoint noch nicht, oder nicht vollständig, dokumentiert. Dies soll in zukünftigen Releases aber verbessert werden.

5 Einführung

Wie schon erwähnt ist diese Bachelorarbeit eine Folgearbeit der Studienarbeit Software-Defined Netzwerk im Campus Bereich [1], was bedeutet, dass in dieser Arbeit nicht mehr auf die grundlegenden Technologien eingegangen wird. Es werden jedoch Technologien, welche für das krisenresistente Netzwerk besonders relevant sind, detaillierter analysiert und beschrieben.

5.1 Erkenntnisse aus der Studienarbeit

In der Studienarbeit hat sich klar gezeigt, dass bei einer so grossen Organisation wie der FUB ein besonderes Augenmerk auf die Skalierbarkeit gelegt werden muss. Auf Grund der aufgetretenen Probleme und Bugs, konnten diese Anforderungen jedoch nur kurz angeschnitten werden. Im Verlauf der Studienarbeit wurde eine laufende Fabric mit der höchsten Priorität definiert. Darauf folgend konnten die vom Industriepartner definierten Use Cases praktisch und wenn nicht anders möglich theoretisch abgedeckt werden. Die Use Cases lauteten folgendermassen [1]:

- Definition von Benutzerprofilen
- Benutzermobilität
- Reporting der Netzwerkaktivitäten
- Degradation der Infrastruktur
- Backup und Restore
- Anbindung an externe Systeme, wie ISE und Infoblox

Wie bei neuerer Software üblich, waren auch im DNA Center noch verhältnismässig viele Bugs vorhanden. Die Bugs wurden in der Studienarbeit dokumentiert und jeweils an die Cisco Experten weitergeleitet. Teilweise konnten die Bugs durch neue Releases schon behoben werden, wiederum andere sind noch ausstehend.

5.2 Krisenresistentes Software Defined Netzwerk

Nun soll in dieser Bachelorarbeit ein krisenresistentes Software Defined Netzwerk erstellt werden, welches mit Hilfe des DNA Centers und Technologien wie VXLAN und LISP umgesetzt wird. Diese Technologien wurden in der Studienarbeit genauer dokumentiert [1]. In der Bachelorarbeit wird zum einen ein möglichst krisenresistentes Netzwerk erstellt und für dies eine Empfehlung für das Deployment vorgestellt. Zum anderen sollen die APIs des DNA Centers genauer untersucht und in einem Orchestrierungstool verwendet werden. In der Studienarbeit waren bis anhin nur wenige Informationen zur API verfügbar, welche nun mit dem Release 1.2.5 aber relativ gut abgedeckt sein sollten. In der Analyse der ganzen SDA Lösung soll nun auch die Skalierbarkeit genauer untersucht werden. Es ist zu klären ob die aktuellen Skalierbarkeitsempfehlungen von Cisco, für so eine grosse Organisation wie der FUB genüben. Mit einem ECNS 5400 soll zudem ein autonomer Standort mit den nötigen Diensten wie Radius, DHCP, DNS und NTP simuliert werden können.

6 Analyse

Nachfolgend werden alle kritischen Elemente der SDA Lösung analysiert. Dazu gehören Dienste wie die LISP Datenbank, Radius und DNS.
Das Ziel ist die komplette Analyse der SDA Lösung und die Identifizierung der kritischen Elemente der Verfügbarkeit (LISP Database, Radius, SGT Access-list etc.) und der Network Services (NTP, DNS, DHCP etc.).

6.1 SDA Architektur und Design

Die Architektur der Lab Umgebung, welche in der Studienarbeit erarbeitet wurde, sah folgendermassen aus:

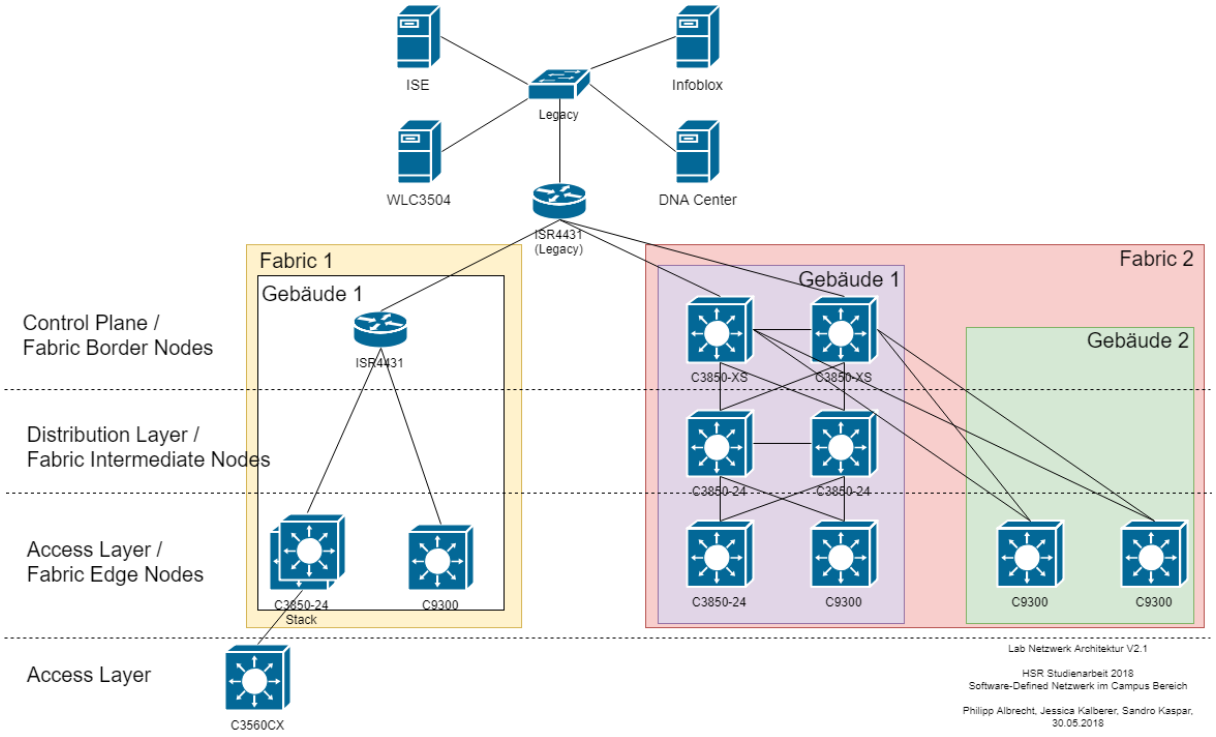

Abbildung 6.1: Architektur Studienarbeit

Die Analyse wird auf dieser Architektur aufbauen und die von der FUB gegebene Grössenordnung berücksichtigen.

Nachfolgend werden die derzeit von Cisco empfohlenen Design Entscheidungen, Grössenüberlegungen, sowie die Skalierungen gezeigt. Aktuelle und ausführliche Informationen hierzu, können direkt im SDA Design Guide von Cisco [3] eingesehen werden.

6.1.1 Platform Entscheidungen

Die Design Entscheidungen beruhen auf den aktuellen Empfehlungen von Cisco, welche sich jedoch laufend ändern können. Nachfolgende Cisco Validated Design (CVD) Empfehlungen sind für die Version 1.2.5 vom September 2018, welche für die zu verwendenden Geräte relevant sind. Ein Catalyst 9300 sollte zum Beispiel nicht als Border oder Control Plane

Node verwendet werden. Im Verlauf der Inbetriebnahme der einzelnen Geräte ist ausserdem darauf zu achten, welche IOS Versionen mit dem verwendeten DNA Center Release kompatibel sind.

Platform	Supported supervisor	Supported fabric-facing interfaces	Edge node	Border node	Control plane node
Cisco Catalyst 9300 Series	–	Onboard ports and network module ports	Yes–CVD verified	No	No
Cisco Catalyst 3850 Series	–	Onboard ports and 10G/40G network module ports	Yes–CVD verified	Yes–3850 XS 10-Gbps fiber versions CVD verified (small-scale deployments)	Yes–3850 XS 10-Gbps fiber versions CVD verified (small-scale deployments)

Abbildung 6.2: SDA Platforms and Deployment Capabilities [3]

Platform	Supported fabric-facing interfaces	Edge node	Border node	Control plane node
Cisco 4400 and 4300 Series Integrated Services Routers	Onboard LAN ports and routed LAN Network Interface Module and enhanced service Module Ports	No	Yes–CVD verified	Yes–CVD verified

Abbildung 6.3: SDA Platforms and Deployment Capabilities [3]

6.1.2 Grössenüberlegungen

Diese Grössenüberlegungen sind besonders für grosse Organisationen wichtig, da diese zur Zeit nur bis zu einer gewissen Anzahl von Cisco in der Praxis getestet wurden.

SD-Access component	CVD tested value for single DNA Center cluster (maximum may be higher)
Clients–across all fabric domains (wired clients and wireless clients)	25,000 validated
Edge, border, and control plane fabric nodes–across all fabric domains (switches/switch stacks, routers, WLCs)	500 validated
All fabric node types across all fabric domains, including fabric intermediate nodes and edge, border and control plane nodes	1,000 validated
Access points–across all fabric domains (each AP counts as an endpoint)	1,500 validated
IP pools–in a single fabric domain or split across all fabric domains	125 pools across 500 edges validated
Sites–each item in the DNA Center site hierarchy is additive (site, building, floor)	200 validated
Fabric domains	10 validated
Scalable group tags–across all fabric domains	4,000 validated
Access control policies–across all fabric domains	1,000 validated
Contracts–across all fabric domains	500 validated

Abbildung 6.4: DNA Center Management of SDA [3]

	Fabric edge platform validation	Fabric border validation
Cisco Catalyst 3850 and 3650 Series	40 validated	-
Cisco Catalyst 3850 XS (10 Gbps fiber)	-	40 validated
Cisco Catalyst 9300 Series	40 validated	40 validated

Abbildung 6.5: SDA Virtual Networks by Platform and Role [3]

6.1.3 Maximum Skalierungen

Folgende maximalen Skalierungen sollten berücksichtigt werden. Diese Daten sollten bei der Auswahl von Plattformen, die während der Planung für das aktuelle und zukünftige Wachstum des Netzwerks verwendet werden, berücksichtigt werden.
Die DNA Center Anzahlen sind pro Instanz, bei denen es sich um ein DNA Center mit einem einzelnen Server oder einem DNA Center Cluster mit drei Servern handeln kann. Die maximalen Zahlen sind entweder die absoluten Grenzen der Plattform oder die empfohlenen Höchstwerte aktueller Tests einer einzelnen Plattform.

SD-Access element	Maximum
Fabric domains	10
Fabric sites in one fabric domain or split across multiple domains	200
APs connected to fabric edge	4,000
Wired endpoints connected to fabric edge (includes APs counted as wired endpoints)	25,000
Fabric nodes including border, edge (switch or switch stack), and WLC	500
Non-fabric nodes including intermediate, subtended, and routers	1,000
Control plane nodes per fabric site	2
Default border nodes per fabric site	4
IP pools across all fabric domains	125
Sites across all fabric domains	200
Scalable groups	4,000
Policies	1,000
Contracts	500

Abbildung 6.6: DNA Center Maximum Scale Recommendations [3]

	Virtual networks	Attached wired endpoints	SGT/DGT table	SGACLs – security ACEs
Cisco Catalyst 3850 Series	64	4,000	4,000	1,500
Cisco Catalyst 9300 Series	256	4,000	8,000	5,000

Abbildung 6.7: Edge Node Maximum Scale Recommendations [3]

	Virtual networks	SGT/ DGT table	SGA-CLs– security ACEs	Fabric control plane entries – border collocated with control plane	IPv4 fabric routes	IPv4 fabric host entries
Cisco Catalyst 3850 XS (10 Gbps fiber)	64	4,000	1,500	3,000	8,000	16,000
4000 Series ISRs (8 GB memory)	4,000	64,000s	64,000	100,000	1,000,000	1,000,000
4000 Series ISR (16 GB memory)	4,000	64,000	64,000	100,000	4,000,000	4,000,000

Abbildung 6.8: Border Node Maximum Scale Recommendations [3]

6.2 Verfügbarkeit

Die Verfügbarkeit der nachfolgenden Dienste ist für den Betrieb eines SDA mit dem DNA Center wichtig, damit die volle Funktionalität des Netzwerkes bereitgestellt werden kann. Darum ist es von Vorteil, wenn die kritischen Server und Dienste redundant ausgelegt sind. Den einzelnen Komponenten werden jeweils mit einer Priorität (Severity) gewichtet. Die Definitionen der Severities werden von den *Cisco Severity and Escalation Guidelines* übernommen. [4]

6.2.1 DNA Center

Beschreibung Das DNA Center übernimmt verschiedene Funktionen im Netzwerk. Es verwaltet die Konfigurationen der Netzwerkgeräte, überwacht diese und stellt die Funktion der Fabrics sicher.

Impact Sollte das DNA Center ausfallen oder nicht erreichbar sein, hat dies keinen direkten Einfluss auf die Funktionalität des Netzwerks. Dies, da alle nötigen Konfigurationen auf den Netzwerkgeräten vorhanden sind. Es ist allerdings nicht mehr möglich, Änderungen am Netzwerk durchzuführen. Es ist beispielsweise nicht mehr möglich, Änderungen an einer Fabric vorzunehmen, Geräte hinzuzufügen oder Access Ports zu konfigurieren. Des Weiteren kann das DNA Center den Betrieb des Netzes nicht mehr monitoren.

Severity 3

Mögliche Ansätze für mehr Krisenresistenz Um die negativen Auswirkungen während eines Ausfalls möglichst gering zu halten, können verschiedene Massnahmen getroffen werden. Dies sind:

- DNA Center Betrieb im Cluster
- DNA Center an verschiedenen Standorten
- Regelmässige Backups damit ein schneller Restore möglich ist

6.2.2 LISP Map Server / Control Plane Node

Beschreibung Der LISP Map Server auf dem Control Plane Node verwaltet die RLOCs aller Clients in einer Fabric. Die entsprechenden Edge Nodes melden ihr bekannte Clients an den Control Plane Node, welcher diese Information in der LISP Database speichert. Benötigt ein Edge Node die RLOC eines Clients, kann er diesen auf der LISP Database abfragen.

Impact Fällt der Control Plane Node aus und die LISP Database steht nicht mehr zur Verfügung, ist die Kommuikation im Netzwerk nur noch eingeschränkt möglich. Clients die sich am selben Edge Node befinden, können weiterhin ohne Einschränkung miteinander kommunizieren. Verbindungen zu Geräten an anderen Edge Nodes sind nur noch möglich, sofern sich die entsprechenden RLOCs im Map-Cache des Source Edge Nodes befinden. Dies gilt ebenfalls für Ziele ausserhalb der Fabric, beispielsweise den Internetzugriff.

Severity 1

Mögliche Ansätze für mehr Krisenresistenz Es ist möglich mehrere Control Plane Nodes in einer Fabric zu betreiben. Im DNA Center Release 1.2.5 sind dies bis zu sechs Nodes pro Fabric Site. Damit kann eine sehr hohe Redundanz gewährleistet werden. Solange mindestens eine Control Plane Node pro Fabric funktioniert, hat der Ausfall der restlichen keinen Einfluss auf den Netzwerkbetrieb. Bei einer Fabric über mehrere Standorte ist es sinnvoll, die LISP Databases dezentral zu positionieren, also über die verschiedenen Standorte zu verteilen, sodass diese lokal noch verfügbar sind, sollte die

Kommunikation zum Hauptsitz unterbrochen sein. Ebenfalls ist denkbar, die Map Caches der einzelnen Geräte zu konfigurieren, sodass der letzte funktionierende Stand auch bei einem Ausfall des Map Servers noch auf den Netzwerkgeräten vorhanden ist.

6.2.3 ISE / Radius

Beschreibung Die ISE, bzw. ein Radius Server übernimmt alle AAA Aufgaben im Netzwerk. Er ist dafür zuständig, dass sich Clients am Netzwerk authentifizieren können, sowie für die Authentifizierung des DNA Centers auf den Netzwerkgeräten.

Impact Fällt dieser Service aus, kann das DNA Center keine Änderungen mehr auf den Devices ausführen. Des Weiteren können sich keine neuen Clients am Netzwerk anmelden. Bereits angemeldete Clients können das Netzwerk solange nutzen, wie Ihre Authentifizierung gültig ist.

Severity 1

Mögliche Ansätze für mehr Krisenresistenz Der Radius Server oder ISE kann redundant betrieben werden. Es können mehrere Instanzen in einem Cluster betrieben werden. Des Weiteren ist eine dezentrale Lösung denkbar. Es kann in Aussenstellen eine Read-Only Kopie des Radius Servers betrieben werden, damit diese autonom funktionieren können, sollte die Verbindung zum Hauptsitz unterbrochen sein.

6.2.4 SGT Access List

Beschreibung Der Secure Group Tag (SGT) weist jeder Sicherheitsgruppe eine eindeutige 16-Bit Sicherheitsgruppennummer zu, deren Geltungsbereich in einer TrustSec-Domäne global ist. Die Nummern werden automatisch generiert, wenn ein SGT auf der ISE erstellt wird. Die Anzahl der Sicherheitsgruppen im Switch ist auf die Anzahl der authentifizierten Netzwerkeinheiten beschränkt.
Die SGTs ermöglichen es der ISE, Richtlinien für die Zugriffssteuerung durchzusetzen, indem es dem Endgerät ermöglicht auf die SGT zu reagieren, um den Datenverkehr zu filtern.
Die Sicherheitsgruppen Access Control List (SGACL) ermöglicht die Steuerung der Zugriffe und der Berechtigungen basierend auf den zugewiesenen SGTs.

Impact bei Ausfall DNA Center: Auf dem DNA Center sind die Sicherheitsgruppen nicht mehr verfügbar und können auch nicht neu erstellt werden. Netzwerk: Die definierten Policies stehen nicht mehr zur Verfügung. Es werden also nur noch gecachte Policies angewendet, was den Netzwerkbetrieb stark einschränkt.

Severity 1

Mögliche Ansätze für bessere Krisenresistenz

- Redundanz der ISE
- Read-Only Kopien der ISE / Radius an Aussenstandorten
- SGT Access Lists mittels SXP auf alle Nodes statisch deployen (Limitierungen müssen abgeklärt werden)

6.2.5 Border Node

Beschreibung Der Border Node stellt die Verbindung der Fabric zu externen Netzwerken sicher. Unter anderem ermöglicht der Border Node den Internetzugriff oder den Zugriff auf andere Fabric Sites.

Impact Fallen alle Border Nodes einer Fabric Site aus, können die Clients der Fabric nur noch innerhalb dieser Fabric Site kommunizieren. Es ist nicht mehr möglich, mit Devices in anderen Sites oder Devices ausserhalb der Fabric oder dem Internet zu kommunizieren.

Severity 2

Mögliche Ansätze für mehr Krisenresistenz Es können pro Fabric Site maximal zwei Border Nodes definiert werden. Damit kann eine Redundanz sichergestellt werden, sodass beim Ausfall eines Nodes keine Einschränkungen für die Clients entstehen.

6.2.6 Fusion Router

Beschreibung Der Fusion Router stellt die Kommunikation zwischen den verschiedenen Fabric Sites, Fabrics, sowie zwischen den Fabrics und der Aussenwelt sicher. Dies ist somit eine sehr zentrale Komponente, die für den Betrieb des Netzwerks sehr wichtig ist.

Impact Fällt der Fusion Router aus, ist keine Kommunikation zwischen verschiedenen Fabrics mehr möglich. Ebenfalls sind die Verbindungen zu Legacy Netzwerken und dem Internet unterbrochen. Dies kann einen sehr grossen Einfluss haben, da sich DNA Center, ISE und weitere zentrale Komponenten in Legacy Netzwerken befinden können.

Severity 2

Mögliche Ansätze für mehr Krisenresistenz Der Fusion Router sollte redundant vorhanden sein. Dabei ist zu beachten, dass die Border Nodes dann Verbindungen zu mehreren Fusion Routern haben müssen.

6.2.7 DHCP

Beschreibung Der DHCP Service, in der Lab Umgebung ist dies Infoblox, stellt sicher, dass die Clients im Netzwerk die korrekten IP Adressen erhalten.

Impact Fällt der DHCP Service aus, erhalten neue Clients keine IP Adressen mehr. Die Netzwerkkommunikation ist für diese daher unmöglich. Bestehende Clients können ihre bereits bezogene IP Adresse weiter verwenden, bis die Lease Time abgelaufen ist. Danach sind auch diese Clients offline.

Severity 2

Mögliche Ansätze für mehr Krisenresistenz Infoblox kann als High-Availability Cluster mit zwei Nodes betrieben werden. Damit ist die nötige Redundanz gegeben, sodass ein Node ohne Impact ausfallen kann. Mit dem DNA Center können für Aussenstandorte separate DHCP Server konfiguriert werden, sodass diese bei einem Unterbruch zum Hauptsitz autonom funktionieren können.

6.2.8 NTP

Beschreibung Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung der Zeit auf den verschiedenen Systemen.

Impact bei Ausfall Bei einem Ausfall des NTP Services kann es zu Problemen bei der Validierung von Zertifikaten kommen. Zudem können auf Grund von falschen Zeiten Events oder Logeinträge fehlerhaft generiert werden. Dies kann eine spätere Fehlersuche stark erschweren.

Severity 3

Mögliche Ansätze für bessere Krisenresistenz Es können mehrere NTP Server unabhängig voneinander betrieben werden. Um eine möglichst genaue Zeit zu erreichen, ist es sinnvoll, an jedem Standort eigene NTP Server zu haben.

6.2.9 DNS

Beschreibung Das Domain Name System (DNS) ist eine wesentliche und oft unterschätzte Komponente in einem Netzwerk. Es ist wichtig, dass DNS im Netzwerk korrekt funktioniert und jederzeit zur Verfügung steht.

Impact bei Ausfall Namensauflösung der Geräte funktioniert nicht mehr. Dies kann dazu führen, dass Services und Geräte nicht mehr erreichbar sind, sofern der Zugriff über Domainnamen und nicht über IPs funktioniert.

Severity 1

Mögliche Ansätze für bessere Krisenresistenz

- Redundante DNS Server im Infoblox HA Cluster
- Read-Only DNS Server an Aussenstandorten zum Beispiel mittels Zone Transfer

6.2.10 Lizenzen

Beschreibung Die Lizenzen der Geräte können über das DNA Center verwaltet werden. Dazu ist jedoch ein Cisco Smart Account nötig, der über alle Lizenzen verfügt. Sind die Lizenzen einmal auf dem DNA Center synchronisiert und ersichtlich, so muss keine Internetverbindung bestehen, da kein Lizenzenforcement besteht.
Die Lizenzen für die einzelnen Switches müssen beim Kauf unbedingt beachtet werden.

Impact bei Ausfall Keine, da Lizenzen nicht enforced werden und alle Funktionen weiter laufen, auch wenn die Lizenz dafür nicht mehr vorhanden oder abgelaufen ist.

Severity 4

Mögliche Ansätze für bessere Krisenresistenz Richtige Lizenzen für alle Geräte bereits zu Beginn einplanen.

6.2.11 Hardware

Beschreibung Bei der Hardware handelt es sich, abhängig vom Dienst der darauf bereitgestellt wird, um eines der wichtigsten Komponenten. Läuft die Hardware nicht mehr, so können auch die Dienste welche darauf laufen nicht mehr ausgeführt werden.

Impact bei Ausfall DNA Center, ISE, Netzwerk nicht mehr verfügbar

Severity Abhängig von der Komponente

Mögliche Ansätze für bessere Krisenresistenz Bei der Hardware ist zu beachten, dass sowohl die Stromversorgung, als auch die Netzwerkverbindungen redundant vorhanden sind. Ebenfalls sollte die Hardware bei einem Stromausfall durch eine USV eine gewisse Zeit weiter betrieben werden können. Dies ermöglicht ein saubers Herunterfahren der Geräte, was die Wahrscheinlichkeit von verlorenen oder korrupten Daten verringert. Ein Backup für den Notfall ist immer zu empfehlen, damit bei einem Hardwaredefekt ein schneller Restore möglich ist. Ersatzgeräte sind ebenfalls von Vorteil.

Wireless Controller

Beschreibung Der Wireless Controller verwaltet die Access Points und stellt den Betrieb des Wireless LAN sicher. Da Wireless aber kein Bestandteil dieser Arbeit ist, wird nicht genauer darauf eingegangen.

Impact bei Ausfall Bei einem Ausfall aller WLCs stehen keine Wireless Netzwerke mehr zur Verfügung. Die Kommunikation für drahtlose Clients ist somit nicht mehr möglich.

Severity 2

Mögliche Ansätze für bessere Krisenresistenz

- Wireless Controller redundant auslegen
- Ersatzgeräte bereithalten

7 Absicherung

7.1 Architektur und Design

Die SDA Topologie sollte nach den gleichen Designprinzipien und Best Practices aufgebaut werden, welche auch ein traditionelles Campus-Design verfolgt. Das folgende Beispiel zeigt die physikalische Topologie eines dreistufigen Campus-Designs, bei dem alle Komponenten innerhalb der Fabric redundant sind.

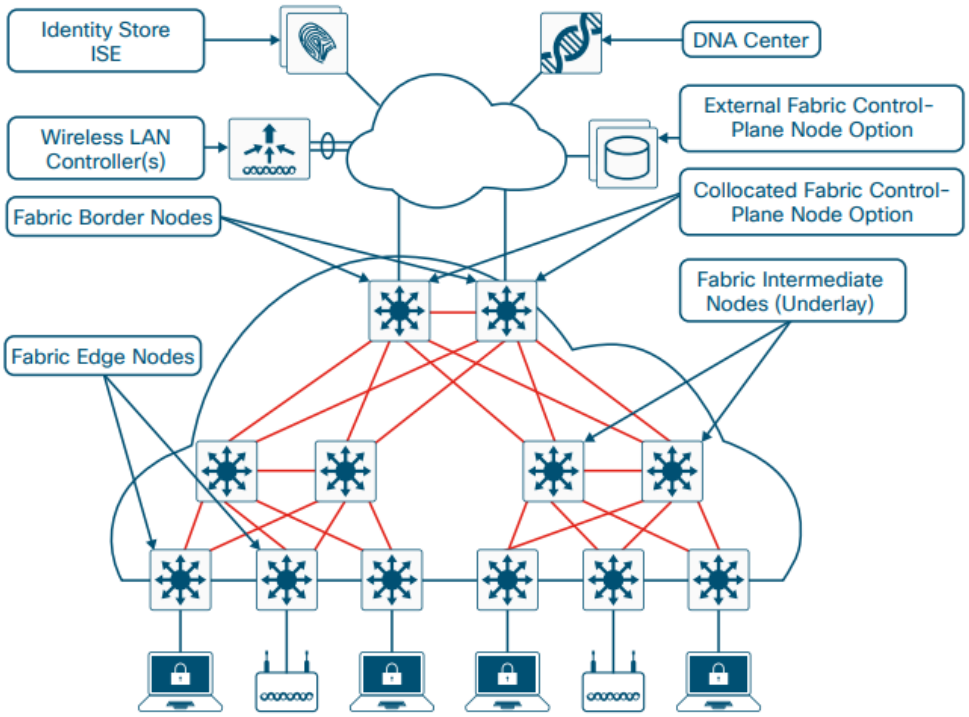

Abbildung 7.1: SDA Topologie [3]

Analog zu dieser wurde die von der Studienarbeit übernommene Architektur (siehe Abbildung 6.1: Architektur Studienarbeit) weiter angepasst und wenn möglich die Komponenten inklusive Verkabelung redundant ausgelegt. Ebenfalls zu beachten sind die Deployment Capabilities, welche als Border und Control Plane Node die Catalyst 3850 empfehlen. Darum werden in der Architektur die Catalyst 9300 als Intermediate oder Edge Nodes eingesetzt. Extended Nodes wie der C3560CX werden zudem nur unterstützt, wenn sie an einem C9300 Edge angeschlossen sind.

Diese neu erarbeitete Architektur (siehe Abbildung 7.2: Architektur Bachelorarbeit) verfügt über eine grosse Fabric *Deutschschweiz*, welche die zwei Sites *Dübendorf* und *Emmen* beinhaltet. Der Standort *Dübendorf* beinhaltet ein Gebäude der *Luftwaffe*. Der Standort *Emmen* beinhaltet den *Flugplatz*, sowie eine *Kaserne*.

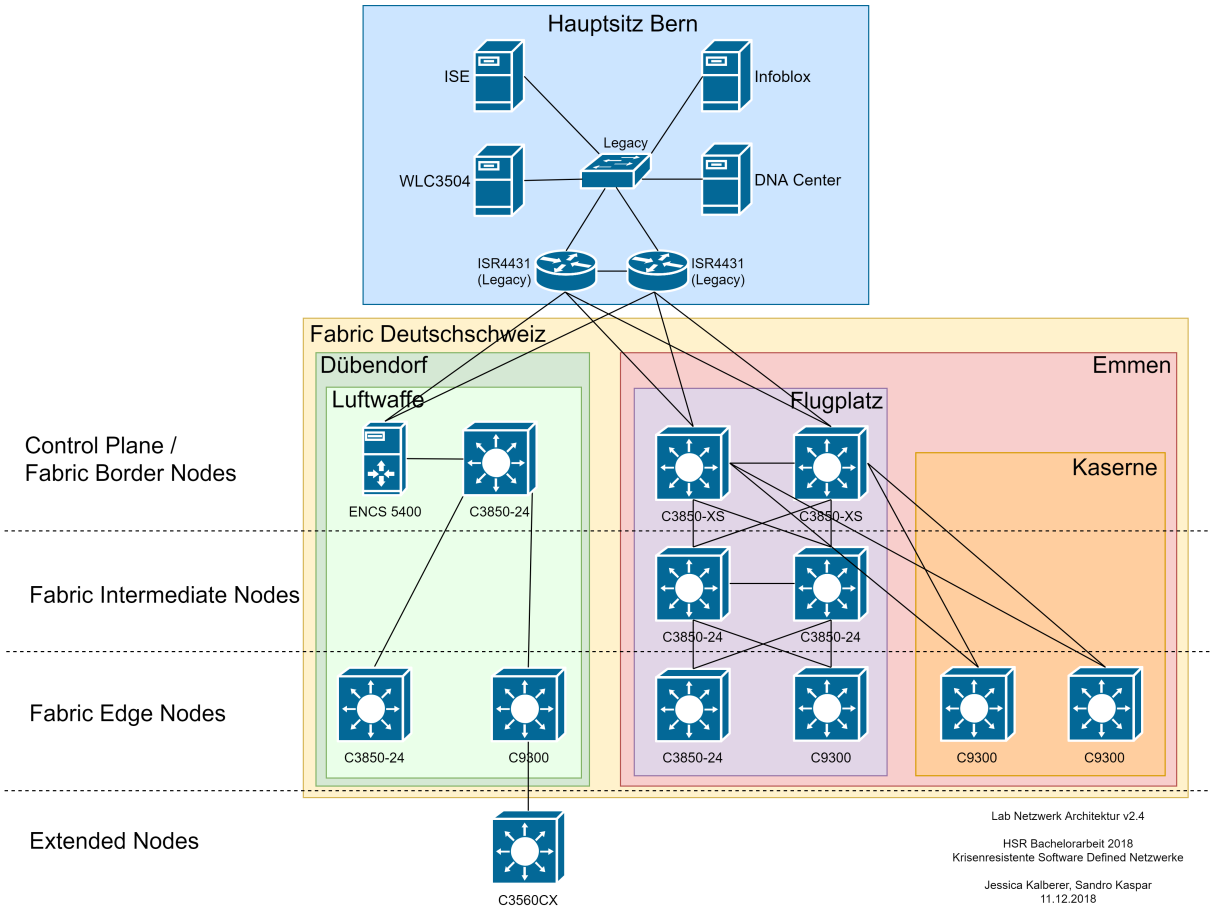

Abbildung 7.2: Architektur Bachelorarbeit

7.1.1 Extended Nodes

In einer SDA-Lösung werden Netzwerkgeräte wie der Catalyst 3560CX als Extended Nodes bezeichnet. Der Extended Node wird verwendet, um Non-Fabric Layer 2 Netzwerkgeräte an die SDA-Fabric anzuschliessen und somit die Fabric zu erweitern. Extended Nodes sind dazu geeignet, Geräte wie Access Point oder IoT Geräte mit der Fabric zu verbinden. Der Extended Node ist ein Gerät wie zum Beispiel ein kleiner Switch (Compact Switch, Industrial Ethernet Switch oder Building Automation Switch), der eine Verbindung zum Fabric Edge Node über Layer 2 herstellt. Geräte, die mit dem Extended Node verbunden sind, verwenden den Fabric Edge Node für die Kommunikation mit externen Subnetzen.

Um einen Extended Node zu integrieren, sind zur Zeit noch einige manuelle Schritte notwendig.

IP Address Pool Damit der Extended Node implementiert werden kann, ist ein IP Address Pool an der dafür vorgesehenen Site notwendig. Im DNA Center unter *Design* → *Network Settings* → *IP Address Pools* kann mit *Reserve IP Pool* ein neuer IP Pool reserviert werden. Als Type muss zwingend *LAN* ausgewählt werden.

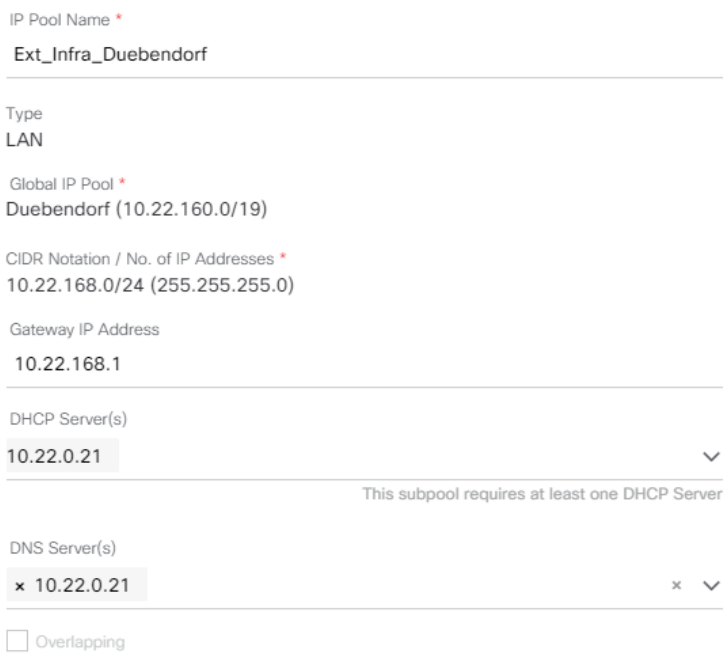

Abbildung 7.3: Reserve IP Address Pool

Host Onboarding für Extended Nodes Als nächstes muss der IP Pool dem dazugehörigen VN zugeordnet werden, damit Extended Nodes am Edge Node erkannt werden. Unter *Provision* → *Fabric* die gewünschte Fabric Domain auswählen. Anschliessend zu der Site navigieren, in welcher sich der Extended Node befindet und dort *Host Onboarding* auswählen. Unter *Virtual Networks* das *Infra_VN* auswählen und den vorher erstellten IP Address Pool als *Extended* Pool Type zuweisen.

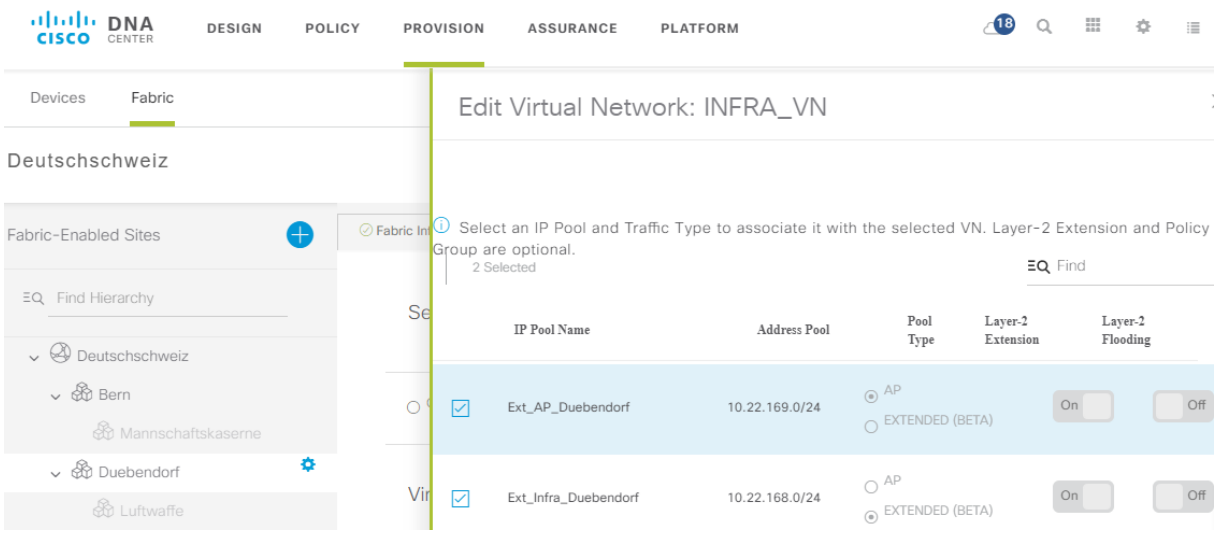

Abbildung 7.4: Virtual Network IP Pool zuweisen

Wichtig ist, das dem INFRA_VN schon ein IP Pool mit dem Pool Type *AP* zugewiesen ist. Ansonsten muss noch ein IP Pool für dies reserviert und dem Infra_VN zugewiesen werden, bevor dem Infra_VN der *Extended* Pool Type zugewiesen werden kann.

Port Assignment Unter *Provision* → *Fabric* muss die gewünsche Fabric ausgewählt und zur Site navigiert werden. Nun kann unter *Host Onboarding* → *Select Port Assignment* der Edge Node, an dem der Extended Node angeschlossen ist, ausgewählt werden. Anschliessend wird das Interface ausgewählt und mit *Assign* wird dem Interface ein Device Type mit dazugehörigem IP Pool zugewiesen.

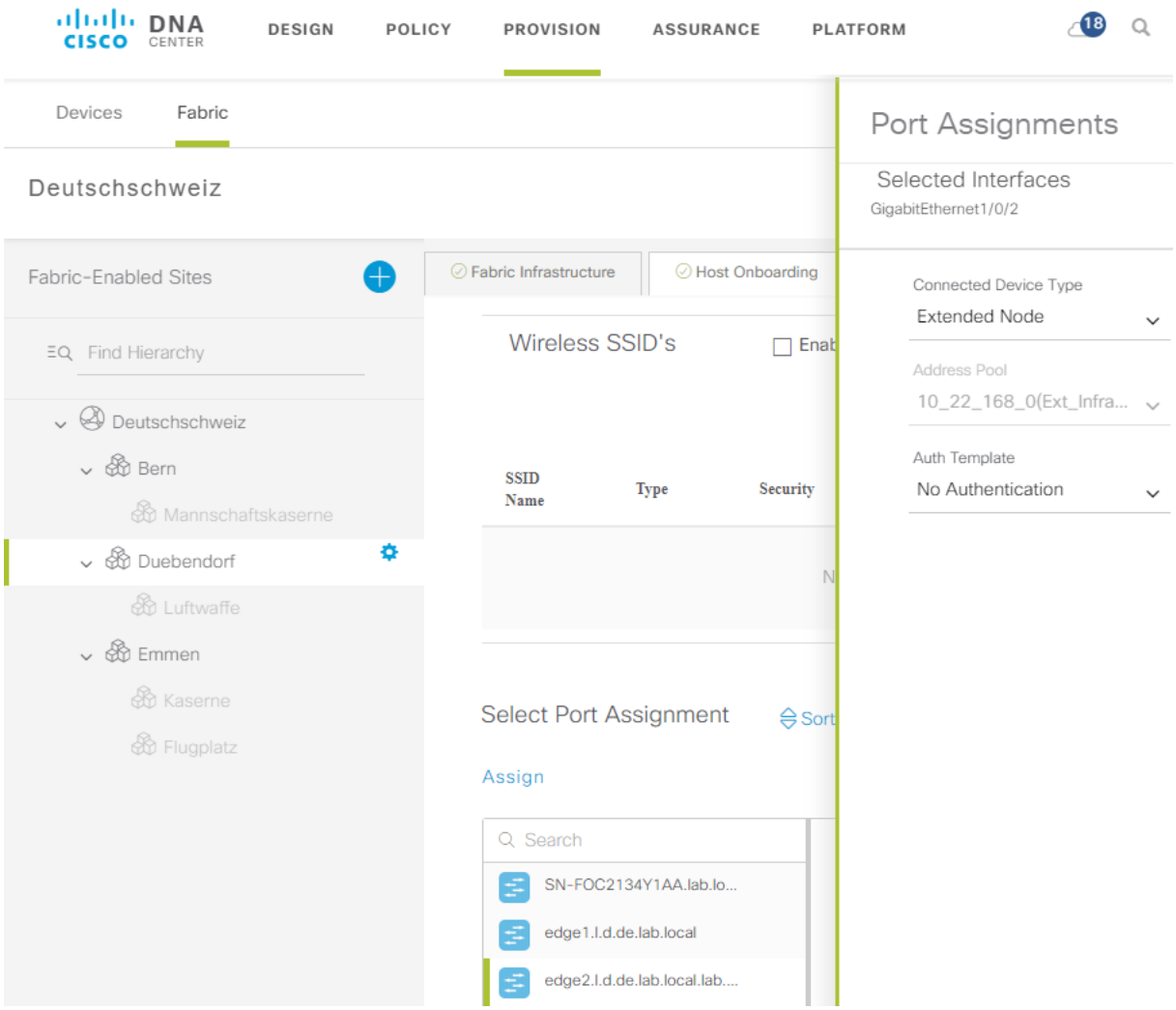

Abbildung 7.5: Port Assignment

DHCP Options Damit der Extended Node beim Starten erfolgreich mittels PnP im DNA Center erkannt wird, müssen für den IP Pool die entsprechenden DHCP Optionen gesetzt werden. Dafür im Infoblox *Data Management* → *DHCP* → *Networks* → *Networks* den IP Pool auswählen und mit *Edit* editieren. Hier wird unter *IPv4 DHCP Options* → *Custom DHCP Options* folgende Option hinzugefügt:

- Option 43 (vendor-encapsulated-option): 5A1D;B2;K4;I[*IP des DNA Center*];J80

Extended Node Am einfachsten ist es, wenn auf dem Extended Node die Konfiguration gelöscht und er neu gestartet wird. Nun sollte der mit dem Fabric Edge Node verbundene Extended Node automatisch erkannt werden und der PnP Prozess wird gestartet. Nach Abschluss des Discovery Prozesses wird der neue Extended Node in der Fabric Site Topologie und auch im Inventory erscheinen. Das Provision Inventory ist

unter *Provision* → *Devices* → *Inventory* zu erreichen. Die Site Topologie kann unter *Provision* → *Devices* → *gewünschte Fabric* → *gewünschte Site* angezeigt werden. Wie unten im Bild ersichtlich ist, wird der Extended Node in der Topologie mit *EX* gekennzeichnet.

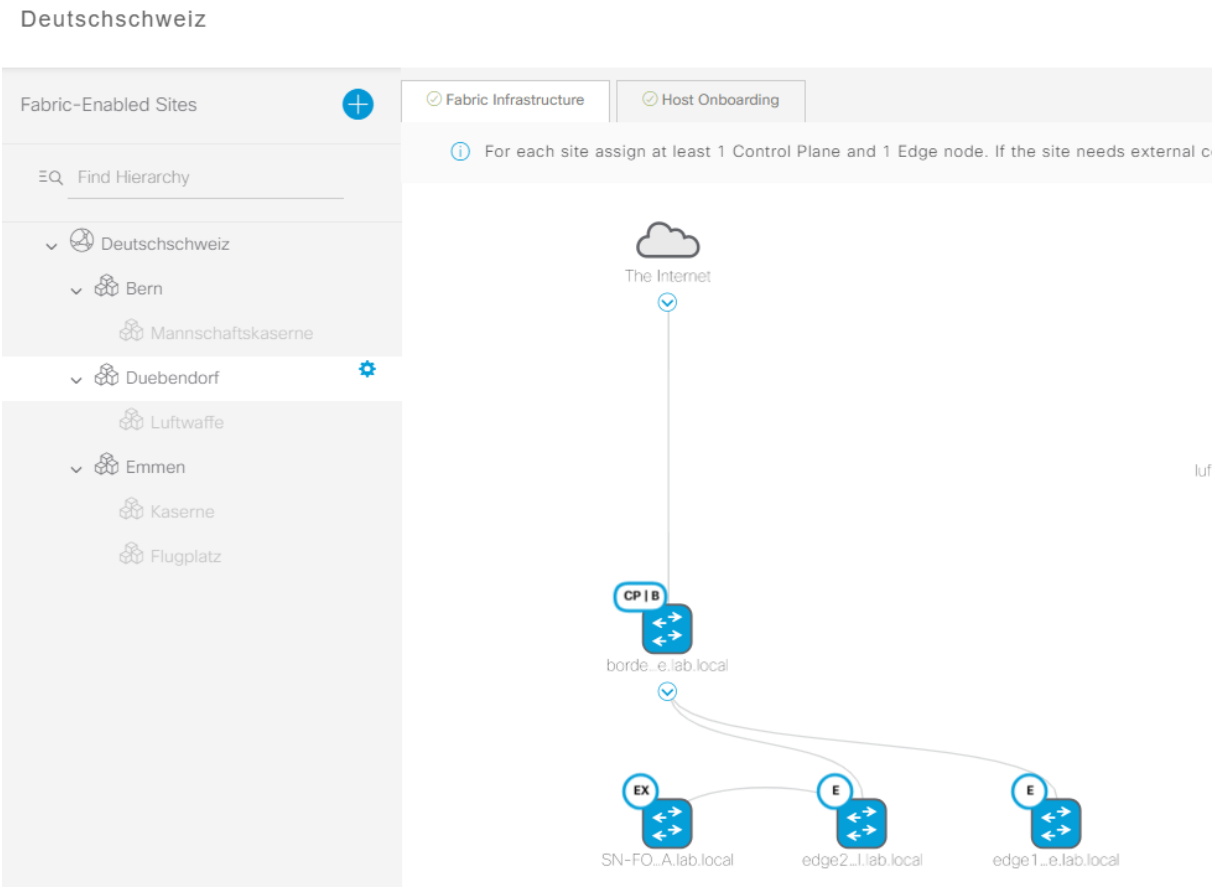

Abbildung 7.6: Fabric Infrastructure

7.2 Transit Fabric

Um die Kommunikation zwischen verschiedenen Fabric Sites innerhalb einer Fabric Domain zu ermöglichen, können Transit Fabrics eingesetzt werden. Diese verbinden die Sites und ermöglichen eine Ende-zu-Ende Segmentierung.

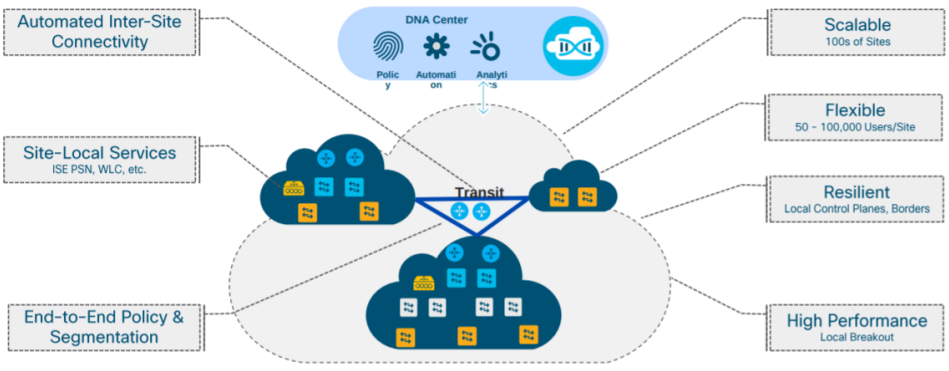

Abbildung 7.7: Transit Fabric [15]

7.2.1 IP Transit

Im IP Transit werden traditionelle Technologien, beispielsweise MPLS, BGP oder VRF-Lite, eingesetzt. Im Gegensatz zum SD Access Transit muss diese Transit Fabric grösstenteils manuell konfiguriert werden. Das DNA Center übernimmt lediglich die Konfiguration der externen Interfaces der Border Nodes. Dies bringt zum einen zusätzlichen Konfigurationsaufwand. Im Gegenzug kann die Transit Fabric aber flexibler konfiguriert werden. Zudem ist keine Control Plane nötig. Es gibt also keinen Single Point of Failure, sofern das Netzwerkdesign die nötige Redundanz bietet. Ein weiterer Vorteil ist, dass alle Geräte, welche die nötigen Protokolle unterstützen, verwendet werden können.

7.2.2 SD Access Transit

Im SD Access Transit wird die Kommunikation zwischen den Fabric Sites mittels Technologien wie VXLAN, LISP und CTS sichergestellt. In diesem Szenario wird ein Control Plane Node benötigt. Wie auch in einer normalen Fabric ist es ratsam, mehrere Control Plane Nodes zu definieren.

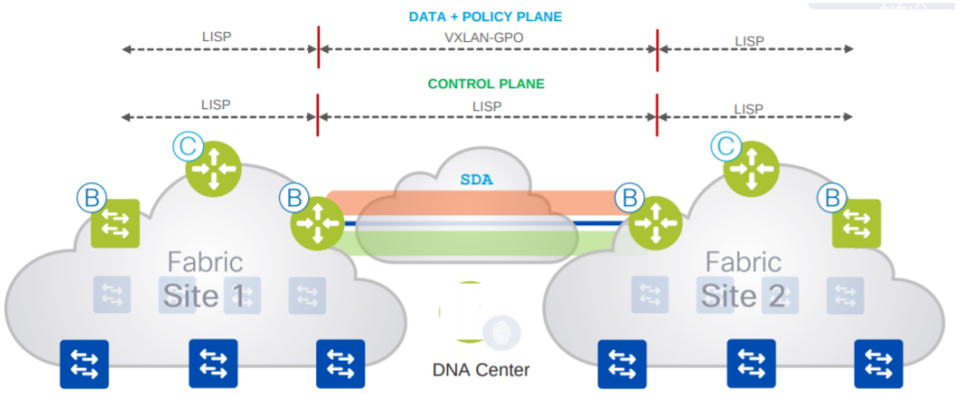

Abbildung 7.8: SD Access Transit [15]

Im Gegensatz zum IP Transit können in der SD Access Transit Fabric nur unterstützte Geräte verwendet werden. Zum jetzigen Zeitpunkt sind dies:

- C9K
- ASR1K
- ISR4K

7.3 ENCS 5400

Um mit möglichst kleinem Hardwareeinsatz eine maximale Autonomie der Aussenstandorte zu ermöglichen, wird pro Aussenstelle ein ENCS 5400 eingesetzt. Im Produktionsbetrieb können für wichtige Aussenstellen auch mehrere ENCS 5400 eingesetzt werden um die nötige Verfügbarkeit zu gewährleisten. Dabei handelt es sich um eine Virtualisierungsplattform von Cisco basierend auf KVM. Des Weiteren beinhaltet die Appliance einen Switch. Auf diesem System können virtuelle Router, Firewalls, WLCs und mittels Third Party Images viele weitere Dienste betrieben werden. Für spezifische Anwendungen können eigene Images erstellt werden, wodurch die Plattform enorm vielseitig einsetzbar ist.

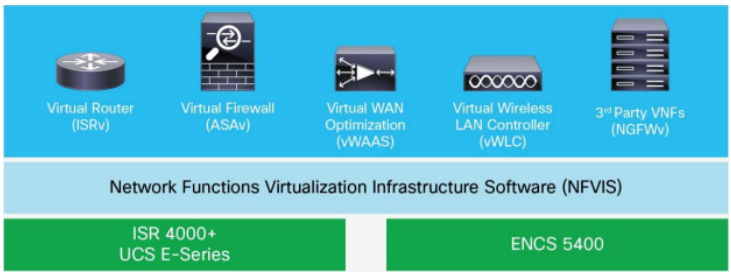

Abbildung 7.9: ENCS Architecture [11]

7.3.1 Image erstellen

In einem ersten Schritt muss ein Disk Image für den gewünschten Service vorliegen. In unserem Fall wurde dieses via Virtualbox erstellt, sodass alle nötigen Pakete bereits installiert werden konnten. Da das Image im Format qcow2 vorliegen muss, wird das vdi Image entsprechend konvertiert.

```
qemu-img convert -f vdi -O qcow2 Ubuntu18.04_Branch.vdi \
Ubuntu18.04_Branch.qcow2
```

Image Packaging Damit das Image verwendet werden kann, muss ein Package erstellt werden. Dabei handelt es sich um ein Archiv, bestehend aus dem Disk Image, sowie einem XML File, in welchem Metadaten wie die Hardwareanforderungen und die verschiedenen Profile definiert sind. Das Package kann manuell oder mittels NFVIS Web Interface erstellt werden.
Im Web-Interface wird dies unter *VM Life Cycle* → *Image Repository* → *Image Packaging* erstellt.

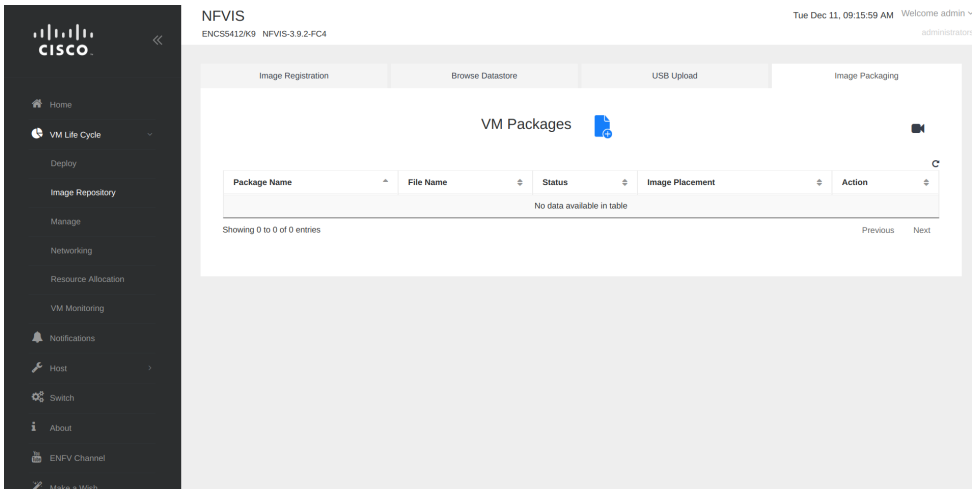

Abbildung 7.10: ENCS Image Packaging

Image Konfiguration Anschliessend werden die Metadaten für das Image definiert. Diese sind schlussendlich im XML File zu finden.

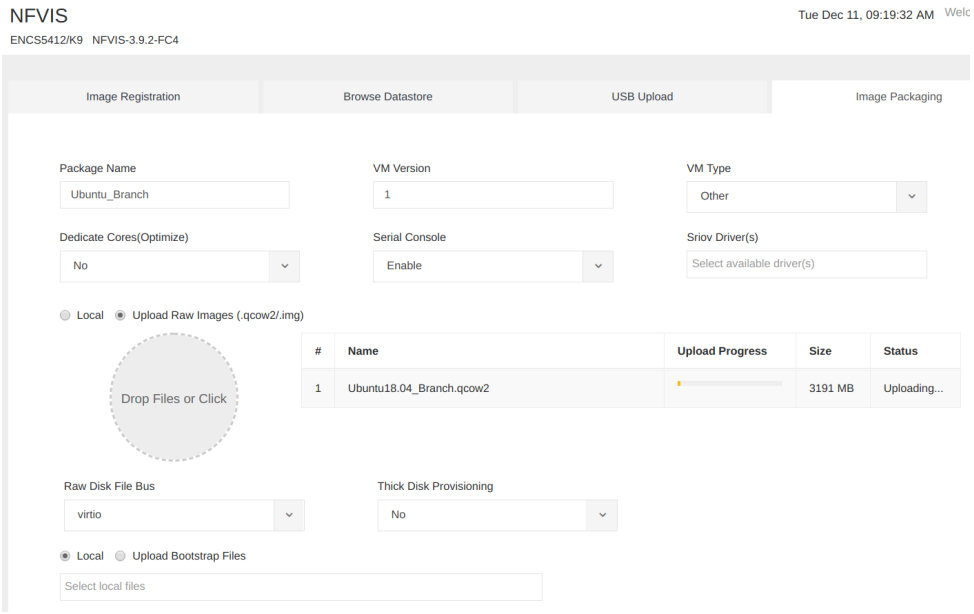

Abbildung 7.11: ENCS Image Konfiguration

Zudem werden die verschiedenen Profile definiert. Diese können später beim Deployment ausgewählt werden, sodass für verschiedene Grössen eines Branches ein passendes Profil ausgewählt werden kann.

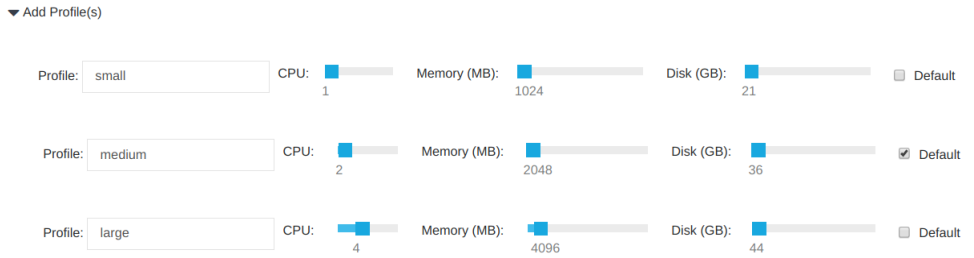

Abbildung 7.12: ENCS Image Profile

Image Deployment Das Deployment des Images soll via DNA Center funktionieren. Aus diesem Grund muss das zuvor erstellte Archiv heruntergeladen und anschliessend im DNA Center importiert werden. *Design* → *Image Repository* → *Virtual* → *Import*

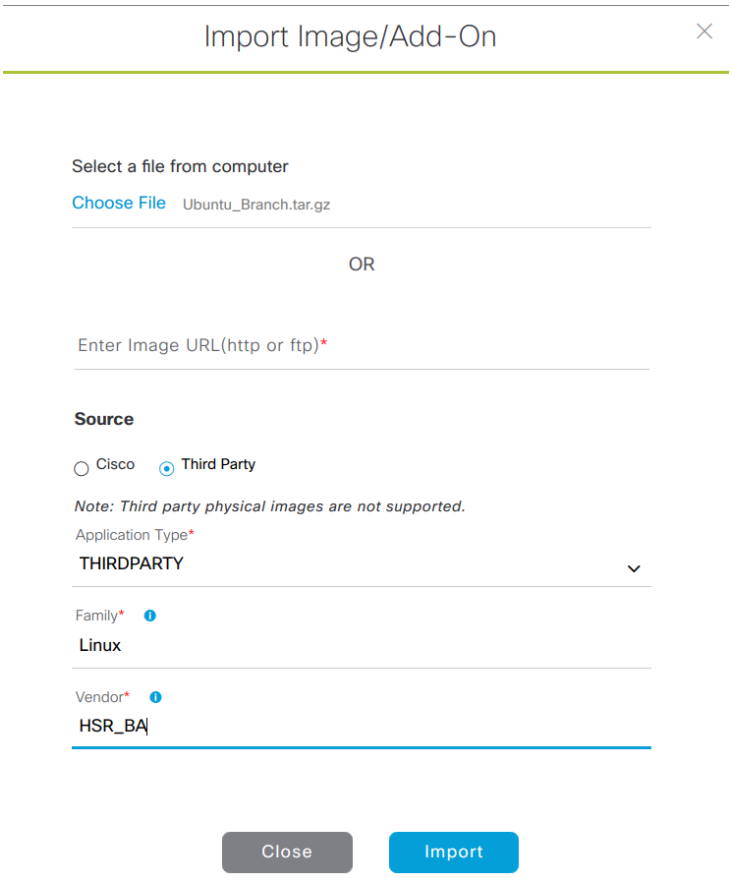

Abbildung 7.13: DNA Center Image Import

Im Lab hat ein Deployment über das DNA Center allerdings nicht funktioniert. Der Grund war, dass das DNA Center die Images als *Physical Images* und nicht als *Virtual Images* erkannte. Daher konnten diese nicht für virtuelle Maschinen verwendet werden.

7.4 DNA Center

Das DNA Center unterstützt den Standalone Betrieb oder eine Clusterkonfiguration mit drei Nodes. Im Optimalfall sollte das DNA Center in einem Cluster mit drei Nodes installiert werden. Der Cluster bietet sowohl Software als auch Hardware mit hoher Verfügbarkeit. Das DNA Center bietet einen Mechanismus zum Verteilen der Verarbeitung und Datenbankreplikation auf mehrere Nodes. Durch das Clustering werden Ressourcen und Funktionen gemeinsam genutzt, sowie eine hohe Verfügbarkeit und Skalierbarkeit ermöglicht.

Die folgende Abbildung zeigt die empfohlenen Verbindungen für einen DNA Center Cluster mit drei Nodes.

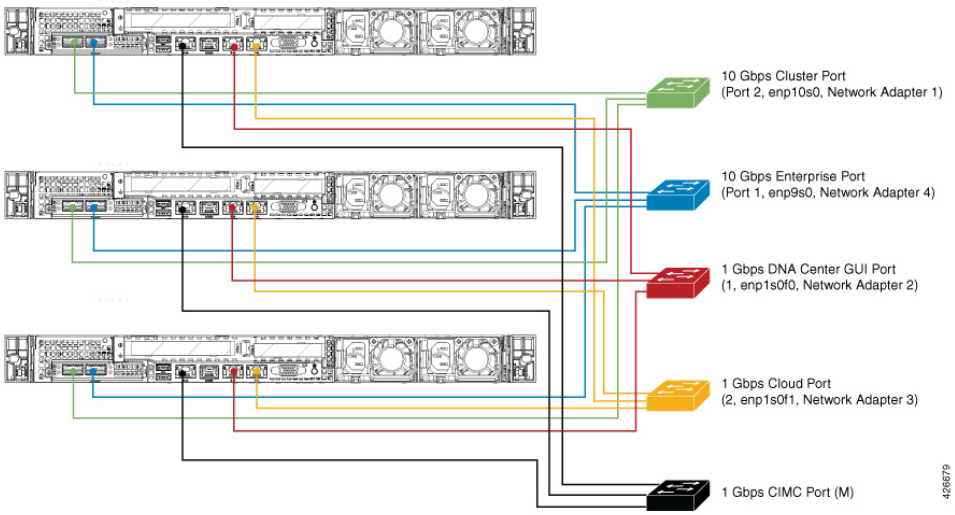

Abbildung 7.14: DNA Center Cluster [9]

Alle bis auf eine der Verbindungen sind für jeden Node im Cluster die gleichen, wie wenn ein Standalone Node eingesetzt werden würde. Die Ausnahme ist der Cluster-Port (Port 2, enp10so, Network Adapter 1), der erforderlich ist, damit jeder Node im Cluster mit den anderen kommunizieren kann.

Für Clusterbereitstellungen mit mehreren Nodes müssen sich alle Cluster Nodes im selben Netzwerk und am selben Standort befinden. Die Appliance unterstützt keine Verteilung von Nodes über mehrere Netzwerke oder Standorte. Diese Limitierung der Bereitstellung, sowie auch die maximale Anzahl der unterstützen Nodes wird sich hoffentlich in Zukunft noch ändern.
Wenn ein Node innerhalb einer Clusterkonfiguration ausfällt, beträgt die Zeit für die Wiederherstellung des Clusters in der Regel 20 Minuten. Fällt in einem Multi-Node Cluster mit drei Nodes ein Node aus und es fällt ein zweiter Node aus, so fällt auch der letzte Node sofort aus. Es müssen immer zwei der drei Nodes im Cluster einwandfrei funktionieren, damit ein funktionsfähiger Cluster gewährleistet werden kann.

7.5 LISP Map Server / Control Plane Node

Der Control Plane Node ermöglicht LISP und besteht aus folgenden Komponenten:

- Map Resolver (MR), der Map-Requests von einem ITR entgegennimmt und das EID-zu-RLOC-Mapping mit Hilfe der verteilten Mapping-Datenbank auflöst
- Map Server (MS), der autoritative EID-zu-RLOC-Mappings von einem ETR lernt und in der Datenbank veröffentlicht
- Host Tracking Database (HTDB), welche ein zentrales Repository für die EID-zu-Fabric-Edge-Nodes Bindings beinhaltet

Zur Bereitstellung gibt es zwei Varianten. Zum einem kann es einen redundanten globalen MS/MR geben, oder es wird pro Fabric Site ein MS/MR implementiert.

7.5.1 Redundante MS/MR Bereitstellung

Es wird empfohlen redundante Standalone MS/MR Systeme mit den MS/MR Funktionen auf demselben Gerät bereitzustellen. Wenn redundante eigenständige MS/MR implemen-

tiert werden, müssen sich alle xTRs bei beiden MS registrieren, sodass jeder eine konsistente Sicht auf den registrierten LISP EID-Namespace hat. Für die MR-Funktionalität ist die Verwendung einer Anycast-IP-Adresse wünschenswert, da dadurch die Mapping-Lookup-Leistung verbessert wird, indem der MR ausgewählt wird, der dem anfordernden ITR am nächsten ist.

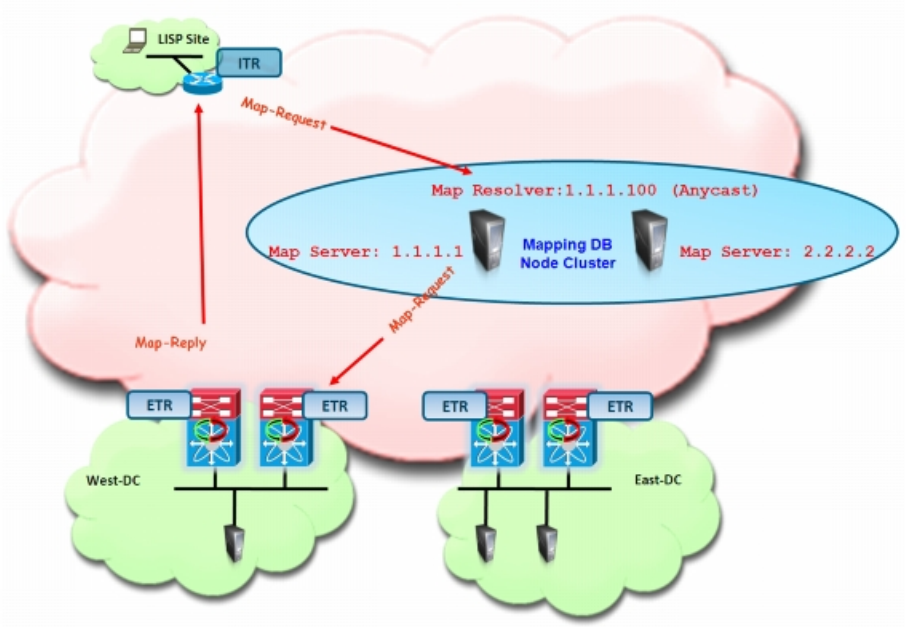

Abbildung 7.15: Redundante MS / MR Bereitstellung [5]

7.5.2 Co-Lokalisierung von MS/MR und xTR Funktionalitäten

Ein weiteres Beispiel ist die Co-Lokalisierung von MS/MR- und xTR-Funktionalitäten. Das co-lokalisierte Modell ist besonders vorteilhaft, da es die Gesamtzahl verwalteter Geräte reduziert, die zum Ausrollen einer LISP Host Mobility-Lösung erforderlich sind. Die erforderliche Konfiguration würde aber in beiden Szenarien identisch bleiben, indem eindeutige IP-Adressen genutzt werden um die MS und eine Anycast-IP-Adresse um die MR zu identifizieren.

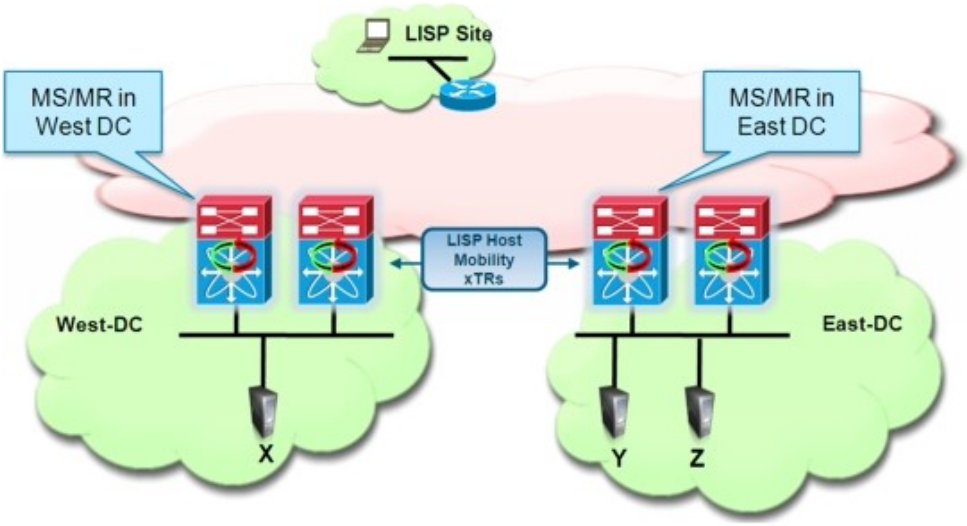

Abbildung 7.16: Co-Lokalisierung von MS/MR und xTR Funktionalitäten [5]

Es kann also ein redundantes eigenständiges MS/MR-Modell bereitgestellt werden, indem dedizierte Systeme zur Bereitstellung dieser Mapping-Funktionen genutzt werden (siehe Abbildung 2.9). Alternativ können die MS/MR Funktionen gleichzeitig auf dem Netzwerkgerät, welches bereits die xTR-Rolle ausführt, implementiert werden (siehe Abbildung 2.10).

7.5.3 Anwendung

Damit bei einem Ausfall eines MS/MR nicht alle Sites betroffen sind, macht es Sinn, pro Fabric Site einen redundanten MS/MR zu implementieren. So können auf einem xTR eine oder mehrere MS/MR-Adressen konfiguriert werden.
Abfragen, die ein EID-zu-RLOC-Mapping durchführen, sind datengesteuert. Dieses Verhalten bedeutet, dass ein neuer Datentransfer zwischen LISP-Sites einen Mapping-Lookup erfordert, was dazu führt, dass der Datenversand gestoppt wird, bis ein Mapping durchgeführt wurde. Dieses Verhalten ist analog zum DNS-Protokoll und ermöglicht LISP die Funktionen in einer dezentralen Datenbank mit EID-zu-RLOC-Mappings zu betreiben.
Die Replikation der gesamten, potenziell sehr umfangreichen, Datenbank ist unnötig, da nur bei Bedarf auf Mappings zugegriffen wird. Genau wie im DNS muss ein Host nicht die komplette Domänendatenbank kennen. TR verwalten den Map-Cache der zuletzt verwendeten Mappings, um die Performance des Systems zu verbessern.

LISP Client Registration Wird ein noch unbekannter Client an die Fabric angeschlossen, sendet der ITR einen Map-Request an einen bekannten MR, wenn es ein EID-zu-RLOC-Mapping benötigt, das noch nicht in seinem lokalen Map-Cache vorhanden ist.

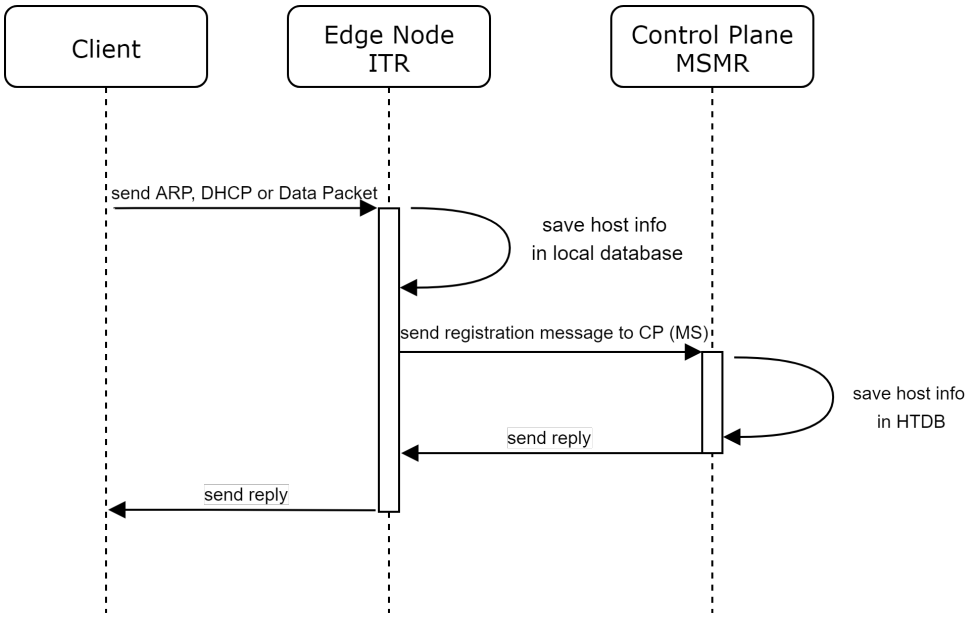

Abbildung 7.17: LISP Client Registration

LISP Host Resolution Will ein Client1 mit einem noch unbekannten Client2 kommunizieren, so sucht sein ITR zuerst in seinem lokalen Map-Cache nach einem Eintrag. Ist noch kein Eintrag zum Client2 vorhanden, so schickt der ITR einen Map-Request zu seinem MR. Der MS sendet dann den originalen Map-Reguest an den zuletzt registrierten ETR. Da Client2 noch am ETR angeschlossen ist, sendet dieser einen Map-Reply an den ITR, welcher die angefragten Mapping-Informationen enthält.
Bei einem Ping werden die initialen Pakete verworfen, bis die Host Resolution abgeschlossen ist.

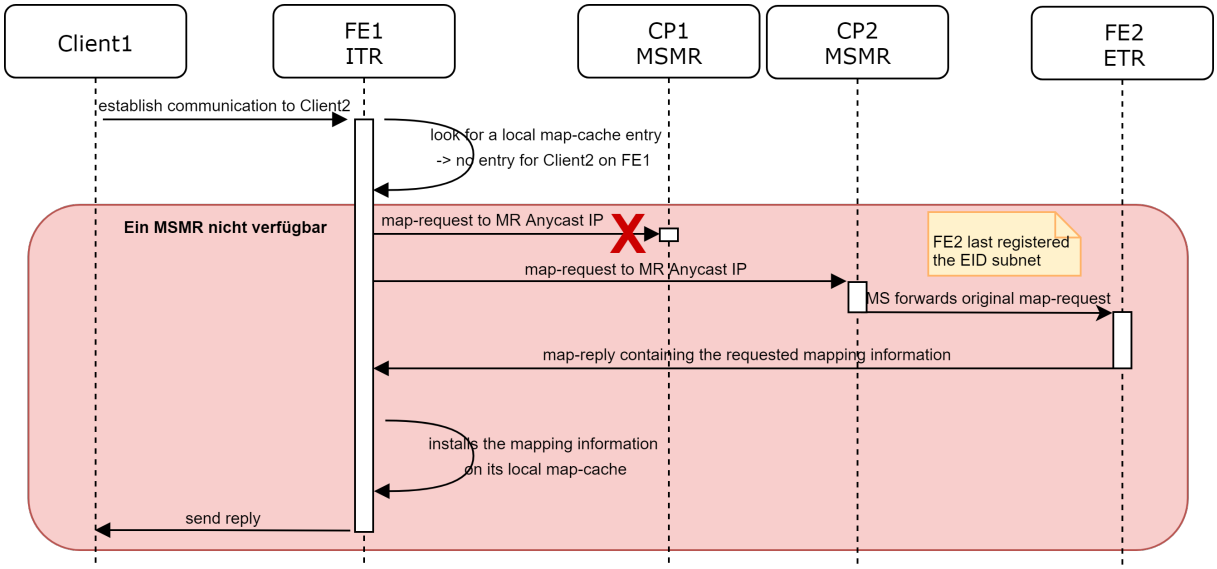

Abbildung 7.18: LISP Host Resolution

Host Mobility Die Host Mobility ist ähnlich wie die Client Registration, da der Client sich beim neuen FE2 zuerst registriert und die neuen Informationen schliesslich vom CP1 an den alten FE1 zur Aktualisierung weitergegeben werden.

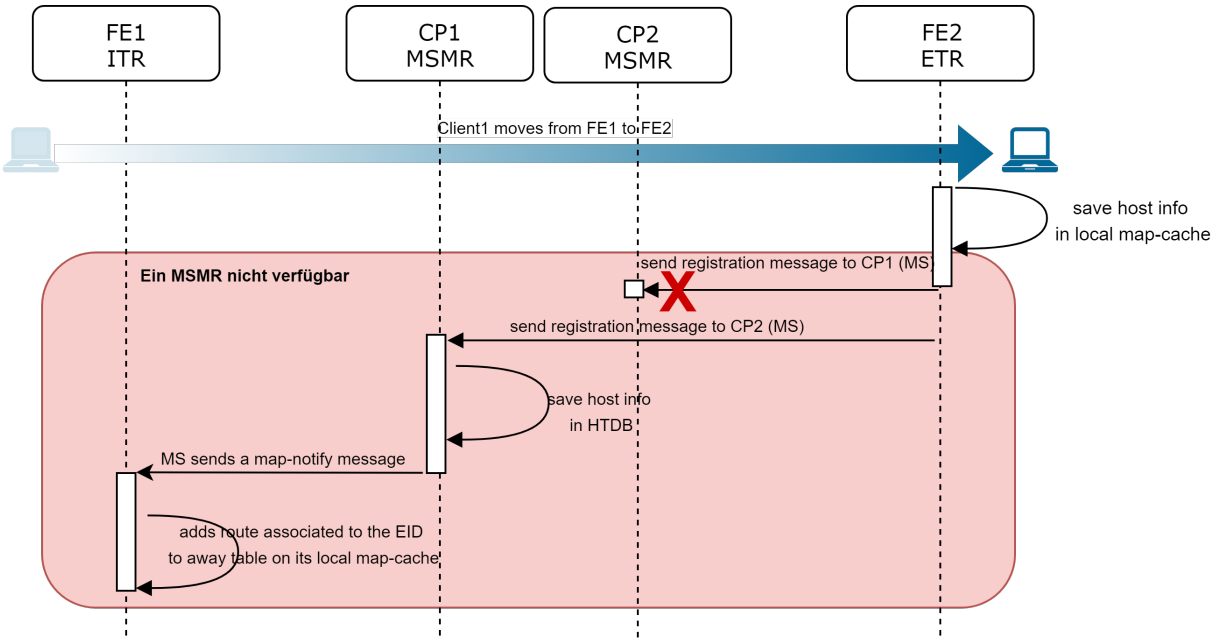

Abbildung 7.19: LISP Host Mobility

Wenn eine dynamischer EID zwischen Sites wechselt, müssen die lokalen LISP Host Mobility-xTRs ihre Existenz erkennen.
Das für LISP Host Mobility konfigurierte xTR erkennt ein Host Mobility Ereignis wenn:

1. Er empfängt ein IP-Datenpaket von einer Quelle, die aus Routing-Sicht nicht über die Schnittstelle erreichbar ist, auf der das Paket empfangen wurde.
2. Die Quelle entspricht der auf die Schnittstelle angewendeten Dynamic-EID-Konfiguration.

7.5.4 Ausfall MS/MR

Bei einem Ausfall des MS/MR kann keine Host Registration mehr vorgenommen werden. Das heisst, neue Clients können keine Verbindung zum restlichen Netzwerk aufbauen. Bestehende Clients können nur mit Clients, welche am selben FE angeschlossen sind, kommunizieren. Dies jedoch nur solange ihr Eintrag im lokalen Map-Cache bestehen bleibt. Die TTL der Einträge im Map-Cache beträgt per default einen Tag.
Da jeder xTR seinen eigenen Map-Cache hat, kann sich sein Inhalt innerhalb derselben LISP-Site unterscheiden. Daher können xTR leicht grosse Paketverluste erleiden oder mit LISP Control Messages geflutet werden.

MS Es sollten mehrere MS vorhanden und eingetragen sein. Im Optimalfall ist mindestens ein MS pro Site vorhanden. Sollte der erste MS nicht erreichbar sein, so wird der zweite MS verwendet.

MR Für den MR sollte eine Anycast IP-Adresse verwendet werden. So werden Pakete gesendet und über einen verfügbaren MR zum Ziel weitergeleitet. Auch hier ist es sinnvoll, mindestens einen MR pro Site bereitzustellen.

7.5.5 Analyse mittels LISP Commands

Es gibt viele LISP Befehle, welche die Analyse vereinfachen können. Nachfolgend werden die wichtigsten LISP Commands zusammen mit den ihren Ausgaben beschrieben. [13]

LISP EID-Table Auf einem Control Plane Node kann die EID-Tabelle mit folgendem Befehl ausgegeben werden:

`show lisp eid-table vrf <VRF Name> ipv4 map-cache`

```
border1.f.e.de#show lisp eid-table vrf Mitarbeiter ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf Mitarbeiter (IID 4099), 30 entries

10.22.0.0/24, uptime: 3d02h, expires: never, via site-registration, self, send-m
ap-request
  Negative cache entry, action: send-map-request
10.22.1.1/32, uptime: 3d02h, expires: never, via site-registration, self, send-m
ap-request
10.22.168.0/24, uptime: 2d04h, expires: never, via site-registration, self, send
-map-request
  Negative cache entry, action: send-map-request
10.22.169.0/24, uptime: 2d04h, expires: never, via site-registration, self, send
-map-request
  Negative cache entry, action: send-map-request
10.22.193.253/32, uptime: 3d01h, expires: 02:18:08, via map-reply, complete
  Locator        Uptime    State      Pri/Wgt     Encap-IID
  10.22.192.102  3d01h     up          10/10        -
```

Abbildung 7.20: LISP EID-Table

LISP EID-Table Map Cache Entry Ein Eintrag in der EID-Table im Map Cache kann mit folgender Abfrage detaillierter angezeigt werden:

`show lisp eid-table vrf <VRF Name> ipv4 map-cache <IP>`

```
border1.f.e.de#$id-table vrf Mitarbeiter ipv4 map-cache 10.22.193.253
LISP IPv4 Mapping Cache for EID-table vrf Mitarbeiter (IID 4099), 30 entries

10.22.193.253/32, uptime: 3d01h, expires: 02:17:42, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 3d01h, map-source: 10.22.30.1
  Idle, Packets out: 27(6230 bytes) (~ 21:12:40 ago)
  Locator        Uptime    State      Pri/Wgt     Encap-IID
  10.22.192.102  3d01h     up          10/10        -
    Last up-down state change:         3d01h, state change count: 1
    Last route reachability change:    3d01h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d04h (rtt 20ms)
```

Abbildung 7.21: LISP EID-Table Map Cache Entry

LISP Database EID-Table Der folgende Befehl kann verwendet werden, um die im ETR konfigurierten lokalen IPv4-EID-Präfixes und der zugehörigen Locator-Sets auszugeben:

`show ip lisp database eid-table <VRF Name>`

```
border1.f.e.de#show ip lisp database eid-table Mitarbeiter
LISP ETR IPv4 Mapping Database for EID-table vrf Mitarbeiter (IID 4099), LSBs: 0
x3
Entries total 29, no-route 0, inactive 0

10.22.0.0/24, route-import, inherited from default locator-set rloc_079cdd97-bfa
b-46be-89ae-da6d00334ea2, auto-discover-rlocs
  Locator         Pri/Wgt  Source     State
  10.22.30.1       10/10   cfg-intf   site-self, reachable
  10.22.192.103    10/10   auto-disc  site-other, report-reachable
10.22.1.1/32, route-import, inherited from default locator-set rloc_079cdd97-bfa
b-46be-89ae-da6d00334ea2, auto-discover-rlocs
  Locator         Pri/Wgt  Source     State
  10.22.30.1       10/10   cfg-intf   site-self, reachable
  10.22.192.103    10/10   auto-disc  site-other, report-reachable
10.22.1.2/32, route-import, inherited from default locator-set rloc_079cdd97-bfa
b-46be-89ae-da6d00334ea2, auto-discover-rlocs
  Locator         Pri/Wgt  Source     State
  10.22.30.1       10/10   cfg-intf   site-self, reachable
  10.22.192.103    10/10   auto-disc  site-other, report-reachable
10.22.2.0/30, route-import, inherited from default locator-set rloc_079cdd97-bfa
```

Abbildung 7.22: LISP Database EID-zu-RLOC

7.5.6 LISP Test

Um die Funktionalität von LISP zu überprüfen, wurde als erstes der Ausfall eines Control Plane Nodes simuliert. Die beiden Clients sind an zwei verschiedene Edge Nodes (C3850 und C9300) in der Site Emmen im Gebäude Flugplatz angeschlossen.
Als erstes wurde nun die LISP EID-Table auf dem Edge1 angezeigt und anschliessend mit dem nachfolgenden Befehl gelöscht:

```
clear ip lisp database eid-table <VRF Name>
```

```
edge1.f.e.de#sh ip lisp database eid-table Mitarbeiter
LISP ETR IPv4 Mapping Database for EID-table vrf Mitarbeiter (IID 4099), LSBs: 0x0
Entries total 1, no-route 0, inactive 1

*** ALL ACTIVE LOCAL EID PREFIXES HAVE NO ROUTE ***
***    REPORTING LOCAL RLOCS AS UNREACHABLE     ***

10.22.193.253/32, Inactive, expires: 23:59:43
edge1.f.e.de#
edge1.f.e.de#clear ip lisp database eid-table Mitarbeiter
edge1.f.e.de#
edge1.f.e.de#
edge1.f.e.de#
edge1.f.e.de#
edge1.f.e.de#sh ip lisp database eid-table Mitarbeiter
% No local database entries configured.
```

Abbildung 7.23: Clear LISP Database EID-Table

Nachdem die EID-Table gelöscht ist, sollen sich die zwei Clients pingen. Dieser Ping war sofort erfolgreich (Voraussetzung dafür ist natürlich, dass die Clients dies auch dürfen) und der Eintrag erschien wieder in der EID-Table.

7.6 ISE / Radius / SGT

7.6.1 Deployment Size and Scaling Recommendations

Die nachfolgenden Tabellen zeigen die Performance und Scalability Metriken für Radius Sessions, Passive Identity, Easy Connect, pxGrid und ISE Services.

Deployment Model	Platform	Max Number of Dedicated PSNs	Max RADIUS Sessions Per Deployment	Max Passive Identity Sessions Per Deployment	Max Merged and Easy Connect Sessions (Shared PSNs)	Max Merged and Easy Connect Sessions (Dedicated PSNs)
Standalone	3515	0	7500	100,000	1,000	N/A
	3595	0	20,000	300,000	2,000	N/A
PAN and MnT on same node and Dedicated PSNs	3515 as PAN and MnT	5	7,500	100,000	1,000	5,000
	3595 as PAN and MnT	5	20,000	300,000	2,000	10,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	3595 as PAN and MnT	50	500,000	300,000	N/A	50,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	Virtual Large SNS-3595 as PAN and MnT	50	500,000	300,000	N/A	50,000

Abbildung 7.24: ISE - Maximum RADIUS Scaling [10]

pxGrid Scaling Per Deployment	Platform	Max PSNs	Max PXGs	Max pxGrid Subscribers (Shared PSN+PXG)	Max pxGrid Subscribers (Dedicated PSN/PXG)
Standalone - All personas on same node (2 nodes redundant)	3515	0	0	2	N/A
	3595	0	0	2	N/A
• PAN, MnT, and PXG on same node and dedicated PSNs • PAN + MnT and dedicated PSN and PXG (Minimum 4 nodes redundant)	3515 as PAN + MnT/PXG	5*	2*	5	15
	3595 as PAN and MnT/PXG	5*	2*	5	15
Dedicated - All personas on dedicated nodes (Minimum 6 nodes redundant)	3595 as PAN and MnT	50	2	N/A	25
Scalability with pxGrid per PXG Node	**Platform**			**Max Subscribers per PXG Node**	
Dedicated pxGrid nodes (Max Publish Rate Gated by Total Deployment Size)	3515			15	
	3595			25	

Abbildung 7.25: ISE - Scalability with pxGrid Services [10]

Deployment Type	Platform	Max PSNs	Max PXGs	Max pxGrid Subscribers: Shared PAN+MNT+PXG	Max pxGrid Subscribers: Dedicated PSN/PXG
Standalone All personas on same node 2 nodes redundant	3515	0	0	20	N/A
	3595	0	0	30	N/A
Medium PAN+MnT+PXG on same node and dedicated PSNs -OR- PAN+MnT and dedicated PSN & PXG Minimum 4 nodes redundant	3515 as PAN+MNT/PXG	5*	2*	140	400
	3595 as PAN+MNT/PXG	5*	2*	160	400
	3595 as PAN+MNT/PXG	5*	3*	160	600
Dedicated All personas on dedicated nodes	3595 as PAN and MNT	50	4	N/A	800
Minimum 6 nodes redundant	3595 as PAN and MNT	50	4	N/A	800

Abbildung 7.26: ISE - pxGrid v2 Scaling per Dedicated pxGrid Node [10]

7.6.2 ISE Cluster

Um die Verfügbarkeit der ISE zu erhöhen, kann diese in einem Cluster, bestehend aus einem Primary Node und einem Secondary Node, betrieben werden. Dies erhöht die Ausfallsicherheit der ISE. Sollte der Primary Node ausfallen, kann der Secondary Node dessen Funktion übernehmen und es ist weiterhin möglich Konfigurationsänderungen vorzunehmen.

7.6.3 Distributed Deployment

Damit Aussenstandorte auch gegen einen Ausfall der Verbindung zum Hauptstandort abgesichert sind, macht ein Distributed Deployment Sinn. Dies bedeutet, dass an jedem Standort mindestens ein ISE Server betrieben wird.

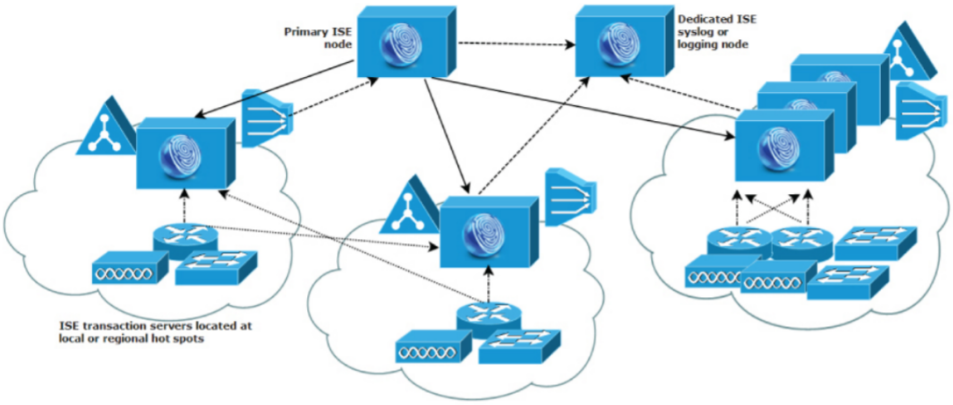

Abbildung 7.27: ISE - Distributed Deployment [14]

Alle Informationen des Primary Node werden auf die Secondary Nodes an den Aussenstandorten repliziert. Network Access Devices und Clients an diesen Standorten können also die lokale Instanz verwenden. Für wichtige Standorte kann die Ausfallsicherheit und Performance weiter erhöht werden, indem dort mehrere Instanzen betrieben werden.

Installation auf dem ENCS 5400 Die Installation der ISE auf dem ENCS 5400 funktioniert ähnlich, wie dies bereits in Kapitel 4.2 beschrieben wurde. Daher werden hier nur die Besonderheiten der ISE beschrieben.

Image Upload Für die ISE kann kein komplettes Disk Image importiert werden. Daher wird in diesem Fall das ISO auf den ENCS kopiert. Auf Grund der Grösse des ISOs kann dies aber nicht über das Web-Interface gemacht werden.

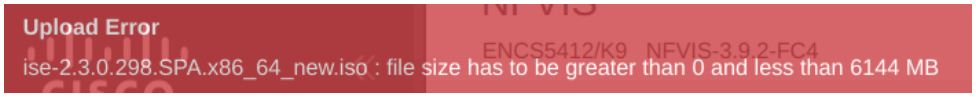

Abbildung 7.28: ENCS - Upload Limit

Ein Image oder ISO über 6 GB muss daher via USB, SCP oder NFS auf den ENCS kopiert werden.

```
nfvis# scp root@10.22.0.15:/root/isos/ise-2.3.iso intdatastore:
```

Nach dem Upload muss das ISO noch unter *VM Life Cycle* → *Image Repository* → *Browse Datastore* → *Register* registriert werden.

Image Deployment Falls noch kein passendes Profil existiert, muss dieses wie in der Abbildung 7.12 ersichtlich, erstellt werden. Hierbei sind die sehr hohen Hardwareanforderungen der ISE zu beachten. Die bei uns verwendete Version 2.3 stellt folgende Anforderungen:

CPU	4 Cores mit je 1.8 GHz
Memory	6 GB
Hard Disk	100 GB (Write IO 50 MB/s, Read IO 300 MB/s)

Tabelle 7.1: ISE Requirements

Die VM kann nun unter *VM Life Cycle* → *Deploy* erstellt werden. Es wird eine VM vom Typ *OTHER* benötigt. Es muss ein Name, das Image und ein Profil definiert werden. Zudem muss die VM mit allen nötigen Netzwerken verbunden werden.

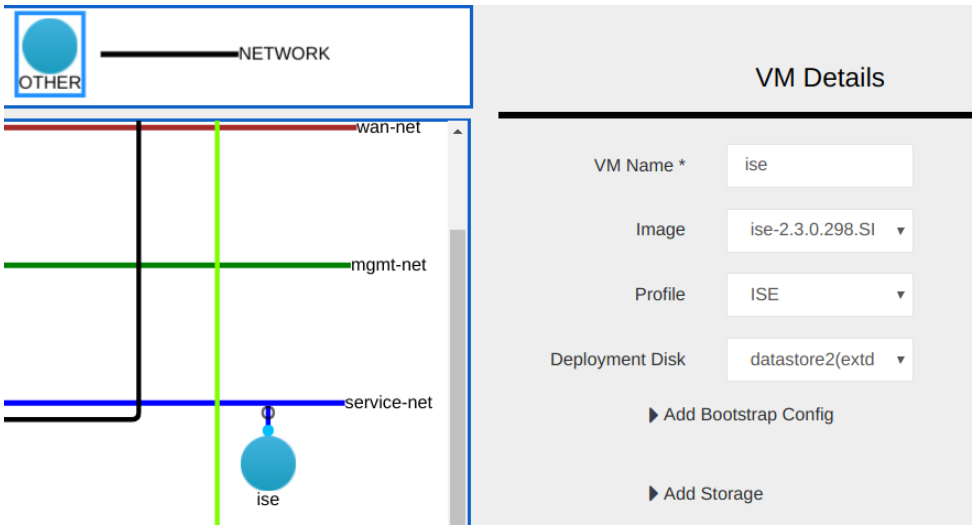

Abbildung 7.29: ENCS - ISE Deployment

ISE Konfiguration Sobald die VM deployed ist, wird das Setup gestartet. Es müssen grundlegende Informationen wie der Hostname und die Netzwerkeinstellungen konfiguriert werden.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise.l.d.de
Illegal characters in the hostname
Alphanumeric and '-' only in the hostname
Enter hostname[]: branch-ise
Enter IP address[]: 10.22.165.22
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.22.165.1
Enter default DNS domain[]: l.d.de.lab.local
Enter primary nameserver[]: 10.22.165.21
Add secondary nameserver? Y/N [N]: 10.22.0.21
Invalid input.  Please enter 'Y' or 'N' [N]: Y
Enter secondary nameserver[]: 10.22.0.21
Add tertiary nameserver? Y/N [N]: n
Enter NTP server[time.nist.gov]: 10.22.165.21
Add another NTP server? Y/N [N]: y
Enter additional NTP server[time.nist.gov]: 10.22.0.15
Add another NTP server? Y/N [N]: n
Enter system timezone[UTC]: CET
Enable SSH service? Y/N [N]: Y
Enter username[admin]:
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
```

Abbildung 7.30: ISE - Setup

Distributed Deployment Sobald die Installation des zweiten Nodes abgeschlossen ist, kann dieser auf dem Primary Node als Secondary Node hinzugefügt werden. Wichtig ist insbesondere, dass die beiden Nodes über dieselbe Zeit verfügen und miteinander kommunizieren können.
In einem ersten Schritt muss die CA des künftigen Secondary Node in den Primary Node importiert werden, sodass eine Trust Beziehung entsteht.

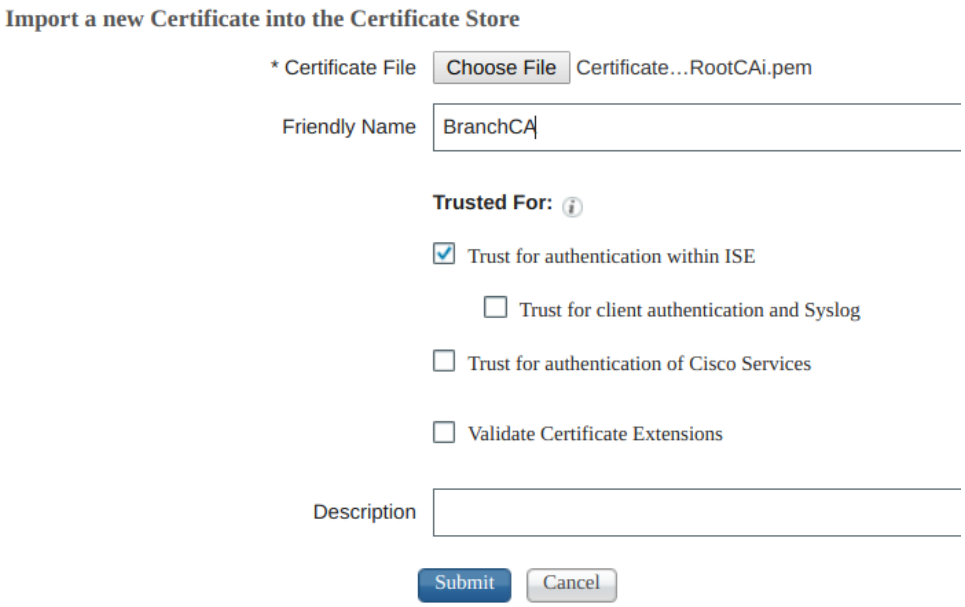

Abbildung 7.31: ISE - Zertifikat

Sofern der Primary Node noch im Standalone Modus ist, muss dieser zum Primary Node gewählt werden. Ist dieser bereits in der Rolle Primary Node, kann der nächste Schritt übersprungen werden.

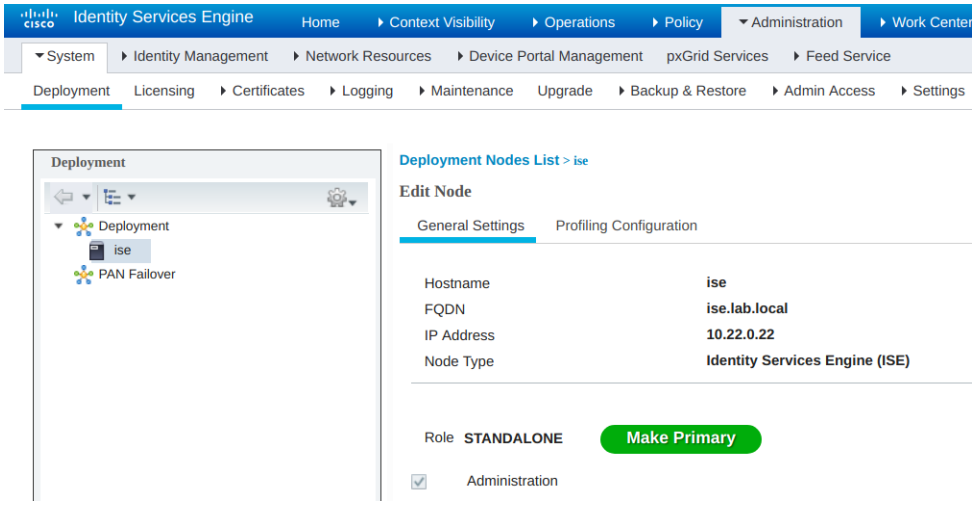

Abbildung 7.32: ISE - Primary Node

Danach wird der neue Node zum Deployment hinzugefügt. Dies wird auf dem Primary Node unter *Administration* → *System* → *Deployment* → *Deployment* → *Register* gemacht.

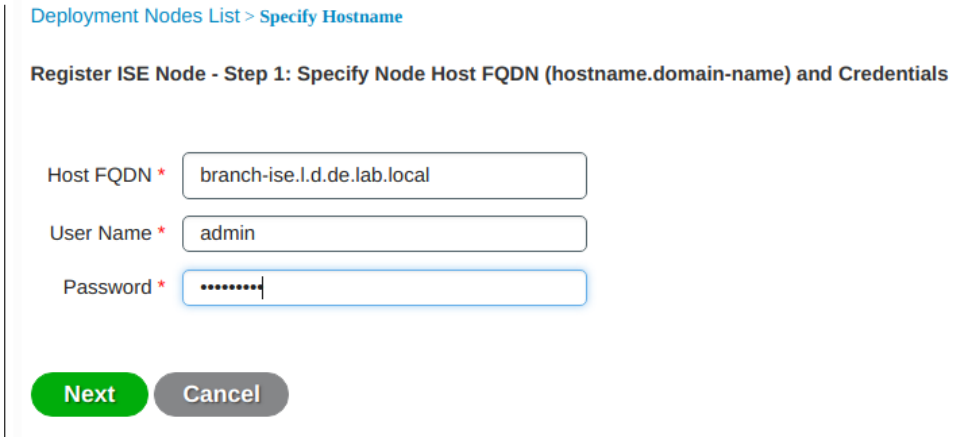

Abbildung 7.33: ISE - Add Node to Deployment

Zum Schluss werden die Rollen für den Secondary Node definiert. Die wichtigsten sind untenstehend aufgelistet. Es wird empfohlen, ressourcenintensive Services, wie zum Beispiel das Monitoring, auf dedicated Nodes auszulagern.

- Monitoring
- Policy Service
  - Session Service
  - Profiling Service
  - SXP Service
- pxGrid

In der Lab Umgebung wurde die Auswahl auf den Policy Service und SXP beschränkt, da dies die Dienste sind, die zwingend benötigt werden.
Nun beginnt die Primary ISE mit der Replikation der Konfigurationen auf den Secondary Node. Dies kann je nach Datenbestand mehrere Stunden dauern. Sobald diese Replikation abgeschlossen ist, können auf dem Secondary Node keine Konfigurationen mehr vorgenommen werden. Damit dieser wieder in den Standalone Mode wechselt, muss er aus dem Deployment entfernt werden.

Network Access Devices Auf den Network Devices muss der ISE Server vom jeweiligen Standort konfiguriert sein. Dies kann im DNA Center unter *Design* → *Network Settings* → *AAA Server* konfiguriert werden.

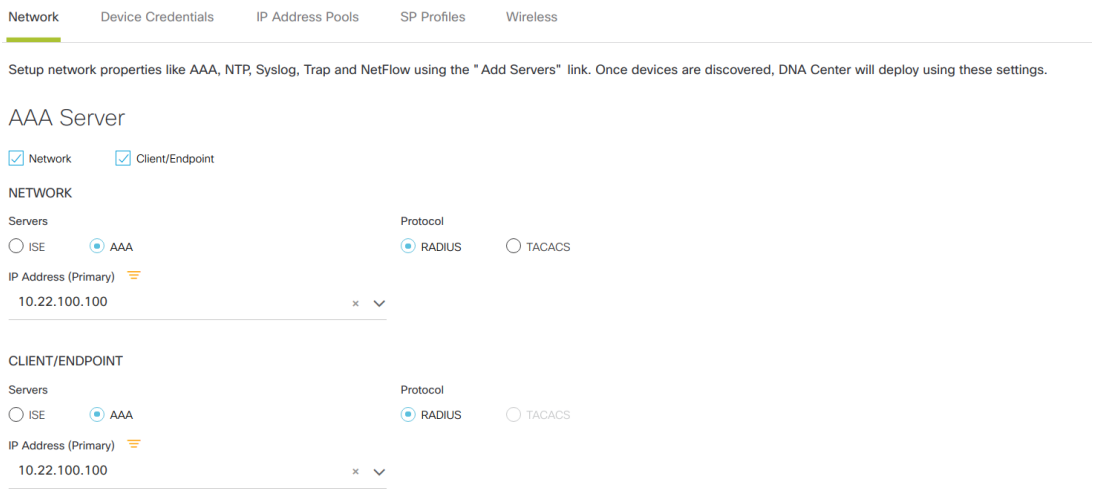

Abbildung 7.34: DNA Center - AAA Server

7.6.4 Third Party Software

Alternativ zum Distributed Deployment der ISE kann eine Replikation der Services auch mittels Third Party Software erreicht werden.

7.6.5 Read Only Radius Server an Aussenstandorten

In Aussenstellen wird ein Read Only Radius Server betrieben, damit die Network Access Devices auch im Falle eines Unterbruchs der Verbindung zum Hauptsitz einen Radius Server zur Verfügung haben. Hier könnte beispielsweise Freeradius eingesetzt werden. Da Freeradius seine Informationen nicht direkt vom ISE beziehen kann, muss vom ISE ein externer Radius Server verwendet werden, der eine Replikation unterstützt.

ISE An einem Hauptstandort wird der primäre ISE Node und ein Dedicated ISE Syslog oder Logging Node betrieben. In einem grossen zentralisierten Netzwerk sollte ein Load Balancer verwendet werden, der die Bereitstellung von AAA-Services vereinfacht. Die Verwendung eines Load Balancers erfordert nur einen einzigen Eintrag für die AAA-Server und der Load Balancer optimiert das Routing von AAA-Anfragen an die verfügbaren Server. Um einen Single Point of Failure zu vermeiden, sollten zwei Load Balancer mit Failover IP eingesetzt werden.
Weitere verteilte grosse Standorte können über eine eigene AAA-Infrastruktur für eine optimale AAA-Performance verfügen. Ein zentralisiertes Verwaltungsmodell hilft bei der Aufrechterhaltung einer konsistenten, synchronisierten AAA-Richtlinie. Ein zentralisiertes Konfigurationsmodell verwendet einen primären Cisco ISE Node mit einem sekundären Cisco ISE Node.

Freeradius Freeradius wird in einem Master/Slave Setup betrieben. Am Hauptstandort befindet sich der Radius Master und an allen Aussenstandorten ist ein Slave verfügbar. Die Replikation wird mittels MySQL Replikation sichergestellt.

7.7 SGT Access List

Beim Erstellen von SGTs über die DNA Center Benutzeroberfläche wird auf die ISE-Benutzeroberfläche weitergeleitet und die Aufgabe wird dort abgeschlossen. ISE verwaltet alle Gruppeninformationen, die später im DNA Center für die Richtlinienerstellung verwendet werden. Obwohl die Richtlinien und die entsprechenden Contracts im DNA Center erstellt werden, werden beide über die REST-API der ISE an die ISE zurückgemeldet. ISE dient dann als zentrale Anlaufstelle für SGTs, Richtlinien und SGACLs, die dann dynamisch an die Netzwerkinfrastruktur verteilt werden. Die Segmentierung innerhalb des SDA wird durch die kombinierte Verwendung von virtuellen Netzwerken (VN), die mit VRFs gleichgesetzt sind und TrustSec Scalable Group Tags (SGTs) ermöglicht. Während die Segmentierung durch die Verwendung von virtuellen Netzwerken allein erreicht werden kann, bieten die Cisco Trustsec SGTs eine logische Segmentierung basierend auf der Gruppenmitgliedschaft. Cisco bietet eine zusätzliche Granularitätsebene, mit der mehrere SGTs innerhalb eines einzigen VN verwendet können. Dies ermöglicht eine Mikrosegmentierung innerhalb des VN. Die Segmentierung erfolgt innerhalb des SDA sowohl auf Makro- als auch auf Mikroebene durch virtuelle Netzwerke beziehungsweise SGTs. Die Richtlinien und die damit verbundenen Contracts werden im DNA Center konfiguriert und dann über die REST-API an die ISE übermittelt. Diese aktualisiert dann die Edge Nodes mit den Richtlinien für SGTs, die den angeschlossenen Geräten zugeordnet sind. [8]
Es folgt eine kurze Zusammenfassung der damit benötigten Komponenten:

- Sicherheitsgruppe (SG) - Eine Gruppe von Benutzern, Endpunktgeräten und Ressourcen, die Zugriffssteuerungsrichtlinien gemeinsam nutzen. SGs werden vom Administrator in Cisco ISE definiert. Wenn neue Benutzer und Geräte zur TrustSec Domäne hinzugefügt werden, ordnet Cisco ISE diese neuen Entitäten den entsprechenden Sicherheitsgruppen zu.
- Security Group Tag (SGT) - Der TrustSec-Dienst weist jeder Sicherheitsgruppe eine eindeutige 16-Bit-Sicherheitsgruppennummer zu, deren Gültigkeitsbereich innerhalb einer TrustSec Domäne global ist. Die Anzahl der Sicherheitsgruppen im Switch ist auf die Anzahl der authentifizierten Netzwerkentitäten beschränkt. Die Sicherheitsgruppennummern müssen nicht manuell konfigurieren. Sie werden automatisch generiert, aber es gibt auch die Möglichkeit eine Reihe von SGTs für die IP-zu-SGT-Zuordnung zu reservieren.
- Security Group Access Control List (SGACL) - Mit SGACLs kann der Zugriff und die Berechtigung basierend auf den zugewiesenen SGTs gesteuert werden. Die Gruppierung von Berechtigungen in einer Rolle vereinfacht die Verwaltung von Sicherheitsrichtlinien. Beim Hinzufügen von Geräten wird einfach eine oder mehrere Sicherheitsgruppen zugewiesen und diese erhalten sofort die entsprechenden Berechtigungen. Die Sicherheitsgruppen können geändert werden, um neue Berechtigungen einzuführen oder die aktuellen Berechtigungen einzuschränken.
- Security Exchange Protocol (SXP) - Das SGT Exchange Protocol (SXP) ist ein Protokoll, das für den TrustSec Dienst entwickelt wurde, um die IP-SGT-Bindungen auf Netzwerkgeräte zu übertragen, die keine SGT-fähige Hardwareunterstützung für Hardware bieten, die SGT / SGACL unterstützt.

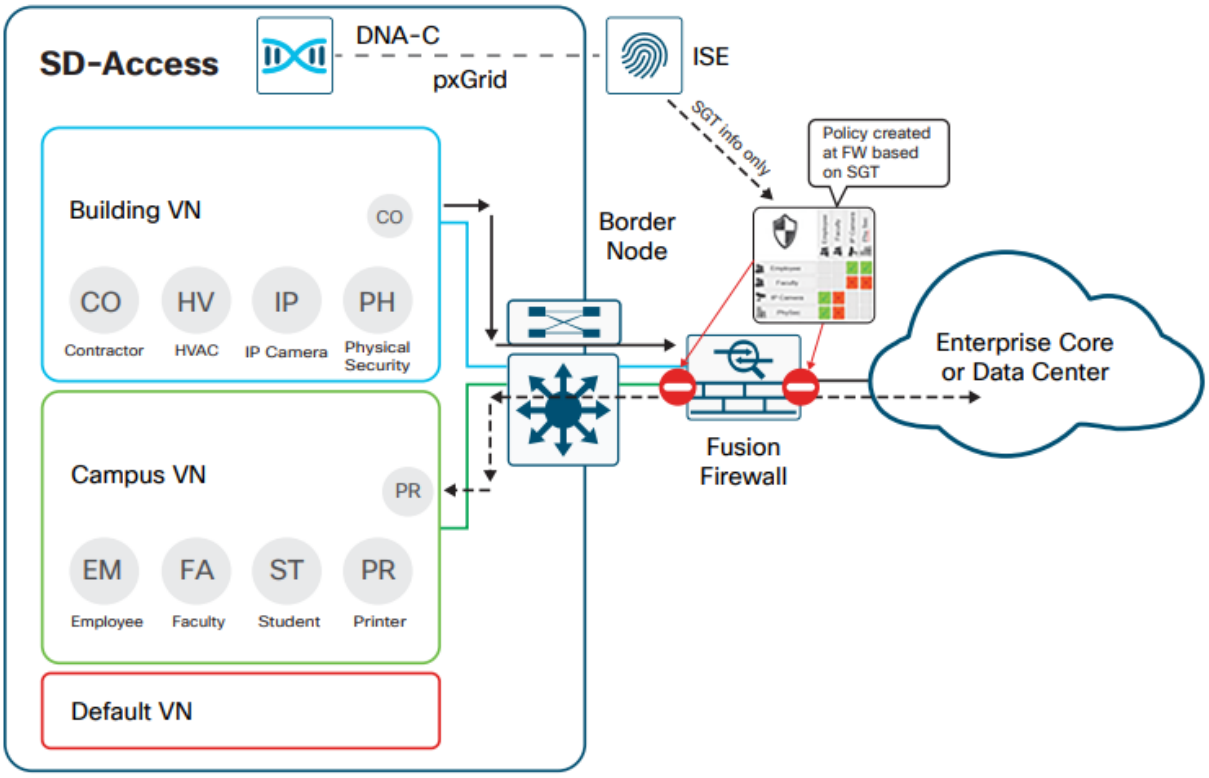

Abbildung 7.35: Policy Enforcement mit einer Fusion Firewall

Die obige Abbildung veranschaulicht die Verwendung einer Fusion Firewall, welche für die Kommunikation zwischen virtuellen Netzwerken sowie für den Verkehr an einem anderen Ort im Netzwerk. Mit Hilfe von Standard ACLs oder gruppenbasierten Richtlinien mit SGTs werden Firewall-Regeln in der Fusions-Firewall definiert, die den Datenverkehr zwischen Endpunkten steuert.

7.7.1 Failover

Die Absicherung der Access Listen kann beispielsweise nach folgenden Beispielen erarbeitet werden:

- Beispiel 1: Lokal auf 9300 SGACLs alle fünf Minuten sichern und diese bei Ausfall wieder eintragen. Nachteil: Host-Mobility funktioniert nicht, aber lokal kann weitergearbeitet werden.
- Beispiel 2: Global komplett alle SGACLs auf alle Geräte verteilen. Vorteil: Alle Geräten haben jederzeit alle Einträge. Nachteil: Die Maximum Scale Recommendations der SGACLs sind pro Gerät anders. C3850 - 1500 SGACLs, C9300 - 5000 SGACLs

Es können TrustSec SXP Speaker/Listener auf den Catalyst 3850 und C9300 definiert werden, indem die Catalyst 3850 als Gateway für die Catalyst 9300 Listener angegeben werden.

7.8 Border Node

Der gesamte Verkehr der die Fabric betritt oder verlässt, durchläuft diesen Knoten. Um einen Single Point of Failure zu vermeiden, sollten immer mindestens zwei Border Nodes

pro Site zur Verfügung stehen. Nach den aktuellen Maximum Scale Recommendations können maximal 4 Border Nodes Site implementiert werden.
Border Nodes implementieren die folgenden Funktionen, welche bei einem Ausfall in Mitleidenschaft gezogen werden könnten[3]:

- Ankündigung von EID-Subnetzen
- Fabric-Domänenausstiegspunkt
- Mapping der LISP-Instanz auf VRF
- Richtlinienzuordnung

7.8.1 Ankündigung von EID-Subnetzten

SD-Access konfiguriert Border Gateway Protocol (BGP) als bevorzugtes Routingprotokoll, das für die Ankündigung der EID-Präfixe außerhalb der Fabric verwendet wird, und der für EID-Subnetze von außerhalb der Fabric bestimmte Verkehr wird durch die Grenzknoten geleitet. Diese EID-Präfixe werden nur in den Routingtabellen am Rand angezeigt. Im gesamten Rest der Fabric wird auf die EID-Informationen über die Fabric-Steuerebene zugegriffen.

7.8.2 Fabric-Domänenausstiegspunkt

Der externe Fabric Border ist das Gateway des letzten Auswegs für die Fabric Edge Nodes. Dies wird mithilfe der LISP Proxy Tunnel Router-Funktionalität implementiert. Möglich sind auch interne Fabric Borders, die mit Netzwerken mit einem genau definierten Satz von IP-Subnetzen verbunden sind, wodurch die Ankündigung dieser Subnetze in der Fabric hinzugefügt werden muss.

7.8.3 Mapping der LISP-Instanz auf VRF

Der Fabric Border Node kann die Netzwerkvirtualisierung mithilfe von externen VRF-Instanzen von innerhalb der Fabric auf die Fabric-Außenseite ausweiten, um die Virtualisierung beizubehalten.

7.8.4 Richtlinienzuordnung

Der Fabric Border Node bildet auch SGT-Informationen aus der Fabric ab, die beim Verlassen dieser Fabric entsprechend verwaltet werden. SGT-Informationen werden vom Fabric Border Node an das ausserhalb der Fabric liegende Netzwerk weitergegeben, indem entweder die Tags mithilfe von SGT Exchange Protocol (SXP) zu Cisco-fähigen Geräten transportiert werden, oder indem SGTs direkt in einem Cisco-Metadatenfeld in einem Paket zugeordnet werden Inline-Tagging-Funktionen für Verbindungen zum Grenzknoten implementiert.

7.8.5 Absicherung Border Node

Damit die Beeinträchtigung des Netzwerks bei einem Ausfall eines Border Nodes minimal ist, muss dieser redundant ausgelegt sein. Konkret bedeutet dies, dass pro Site mindestens zwei Border Nodes vorhanden sind. Des Weiteren sind diese in einem Full Mesh zu den Fusion Routern verkabelt, sodass auch der Unterbruch einzelner Verbindungen keinen direkten Einfluss auf die Netzwerkservices hat.

7.8.6 Test Border Node (Stromausfall)

Um den Ausfall eines Border Nodes zu testen, wurde von einem Client aus ein Ping ins Internet gestartet. Während diesem Vorgang wurde das Interface auf dem zuständigen Border down genommen. Es gingen insgesamt ungefähr 27 Pings à je 0.1 Sekunden verloren, was bedeutet, dass ein Unterbruch von ungefähr 2.7 Sekunden resultierte, bevor die Verbindung über den anderen Border wieder aufgenommen wurde.

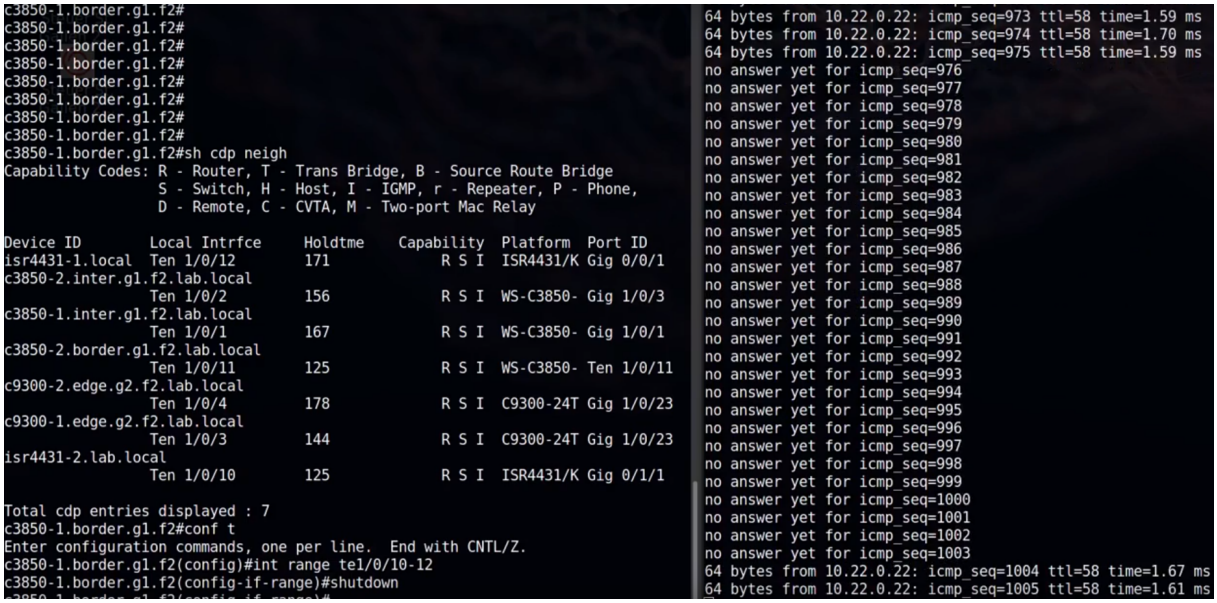

Abbildung 7.36: Border Ausfall Test

Der gleiche Test wurde auch mit einem effektiven Stromausfall an einem Border getestet. Dafür wurden zwei Clients an zwei verschiedene Edge Nodes (C3850 und C9300) in der Site Emmen im Gebäude Flugplatz angeschlossen. Nun wurde einem Border Node der Stromversorgung komplett entfernt und es resultierten die gleichen Ergebnisse. In der nachfolgenden Abbildung, sieht man das der linke Client über den noch funktionierenden Border eine Verbindung ins Internet hat. Der rechte Client jedoch war über den Border verbunden und hatte einen kurzen Unterbruch.

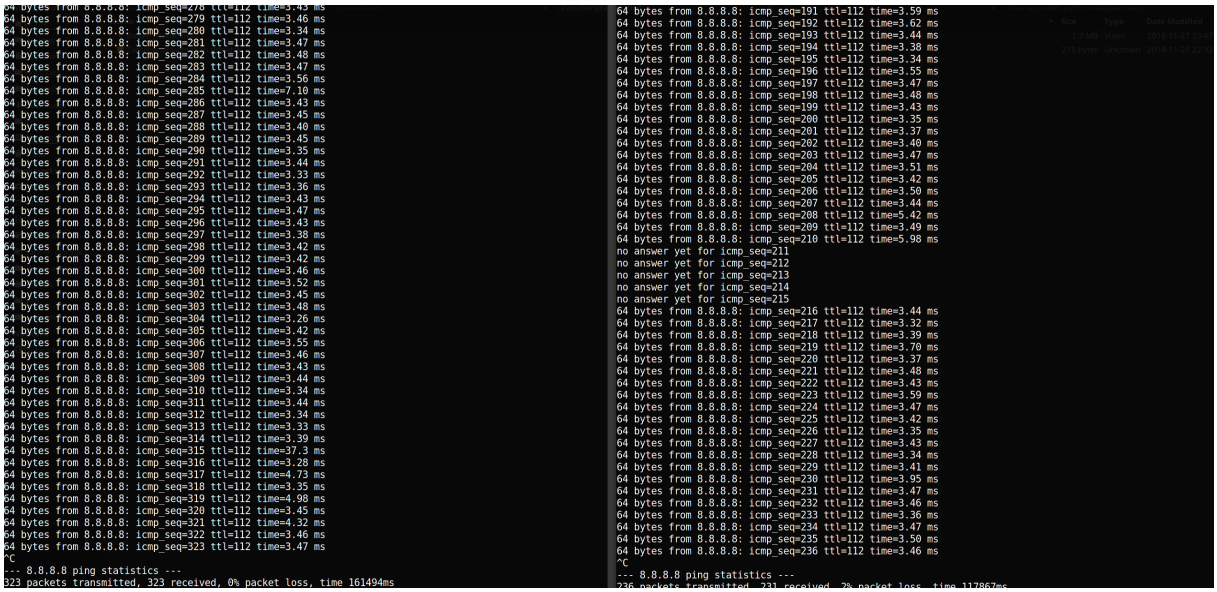

Abbildung 7.37: Border Ausfall Test 2

7.9 Fusion Router

Die Fusion Router stellen die Verbindungen zwischen den einzelnen Fabrics, dem Internet, sowie die Verbindung zum Legacy Netzwerk in dem sich beispielsweise das DNA Center und der ISE befinden.Es werden mehrere Fusion Router verwendet, um die nötige Ausfallsicherheit zu gewährleisten. Die Fusion Router und Border Nodes sind im Optimalfall in einem Full-Mesh verkabelt. Für das Routing zwischen den Fusion Routern, sowie den Border Nodes kommt BGP zum Einsatz.
Die Topologie wurde analog anhand der nachfolgenden Validation Topologie von Cisco aufgebaut.

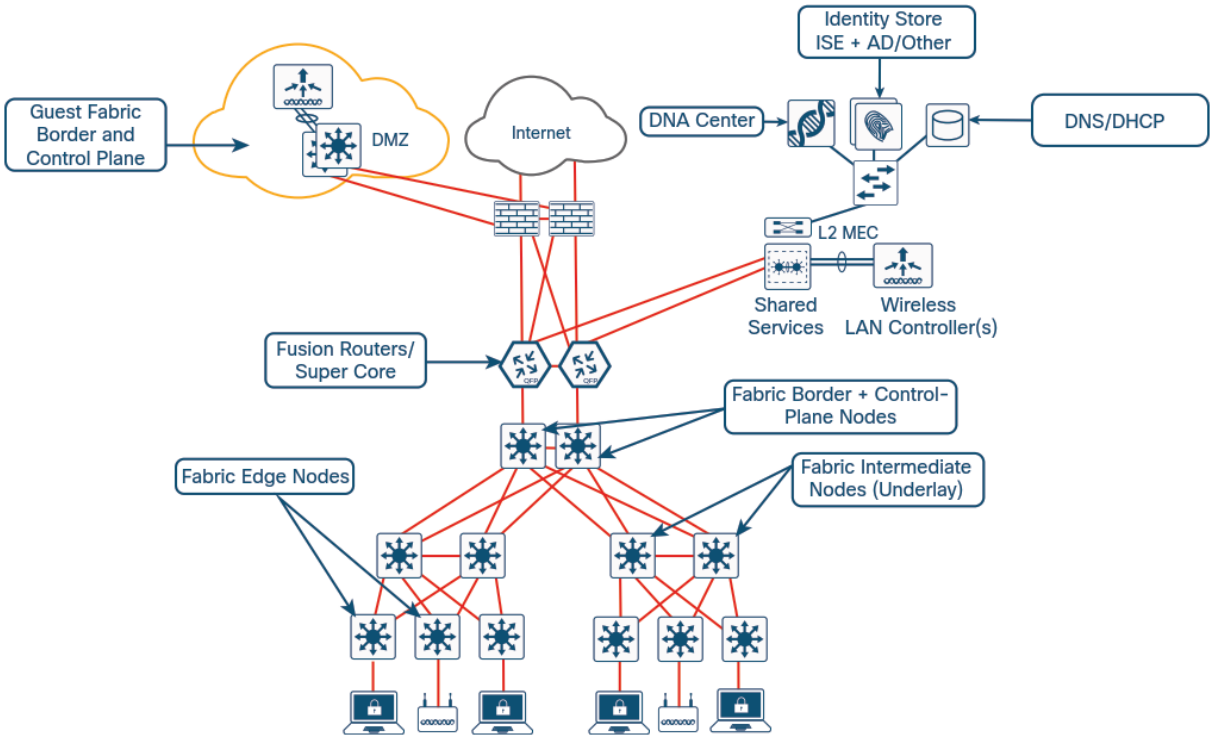

Abbildung 7.38: Fusion Router Validation Topology [7]

7.9.1 Absicherung Fusion Router

Wie auch beim Border Node ist darauf zu achten, dass pro Site mindestens zwei Fusion Router vorhanden sind. Dies ist insbesondere dann wichtig, wenn die Kommunkation zwischen den verschiedenen VNs gewährleistet sein muss. Um auch gegen einen Ausfall einer Verbindung abgesichert zu sein, müssen Verbindungen zu den Border Nodes, aber auch zu externen Netzwerken redundant ausgelegt sein.

7.9.2 Test Ausfall Fusion Router

Ein Ausfall eines Fusion Routers führt wie ein Ausfall eines Border Nodes zu einem teilweisen Verbindungsunterbruch im Bereich von wenigen Sekunden. In dieser Zeit kann BGP auf die neue Topologie reagieren und alle Pfade wiederherstellen.

7.10 Absicherung Infoblox

Infoblox stellt kritische Dienste wie DHCP, DNS und NTP für Netzwerkgeräte und Clients zur Verfügung. Aus diesem Grund muss die Verfügbarkeit dieser Services immer gewährleistet sein.

7.10.1 HA-Pairs

Zwei Infoblox Instanzen können in einem High-Availability Pair betrieben werden. Damit sind alle Services redundant und ein Ausfall einer einzelnen Instanz hat keinen Einfluss auf den Betrieb.

7.10.2 Grid

Infoblox kann in einem Grid betrieben werden. Dies bedeutet, es gibt einen Grid Master und mehrere Grid Member. Alle Konfigurationen werden auf dem Grid Master definiert. Des Weiteren kann definiert werden, welche Member für spezifische Services zuständig sind. Somit kann sichergestellt werden, dass an Aussenstandorten nur die Services betrieben werden, die dort auch nötig sind. Um die Ausfallsicherheit weiter zu erhöhen, können Grid Master und Member zusätzlich als High-Availability Pair betrieben werden.

Grid Member hinzufügen Ein neuer Grid Member kann im UI von Infoblox unter *Grid* → *Grid Manager* → *Members* hinzugefügt werden.

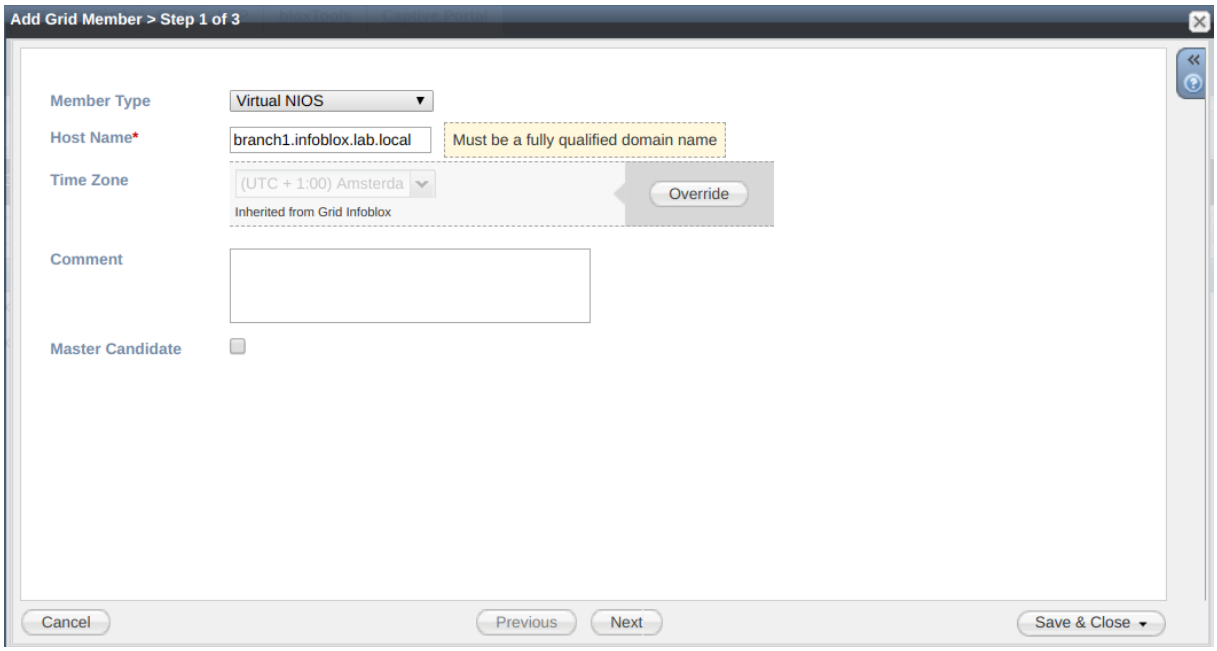

Abbildung 7.39: Infoblox - Add Grid Member

Member Assignment Sobald die Grid Member hinzugefügt wurden, kann definiert werden, für welche Services diese zuständig sind. Dies kann sehr granular definiert werden. Beispielsweise kann für eine einzelne DNS Zone oder einen einzelnen DHCP Pool definiert werden, welche Member zuständig sind.

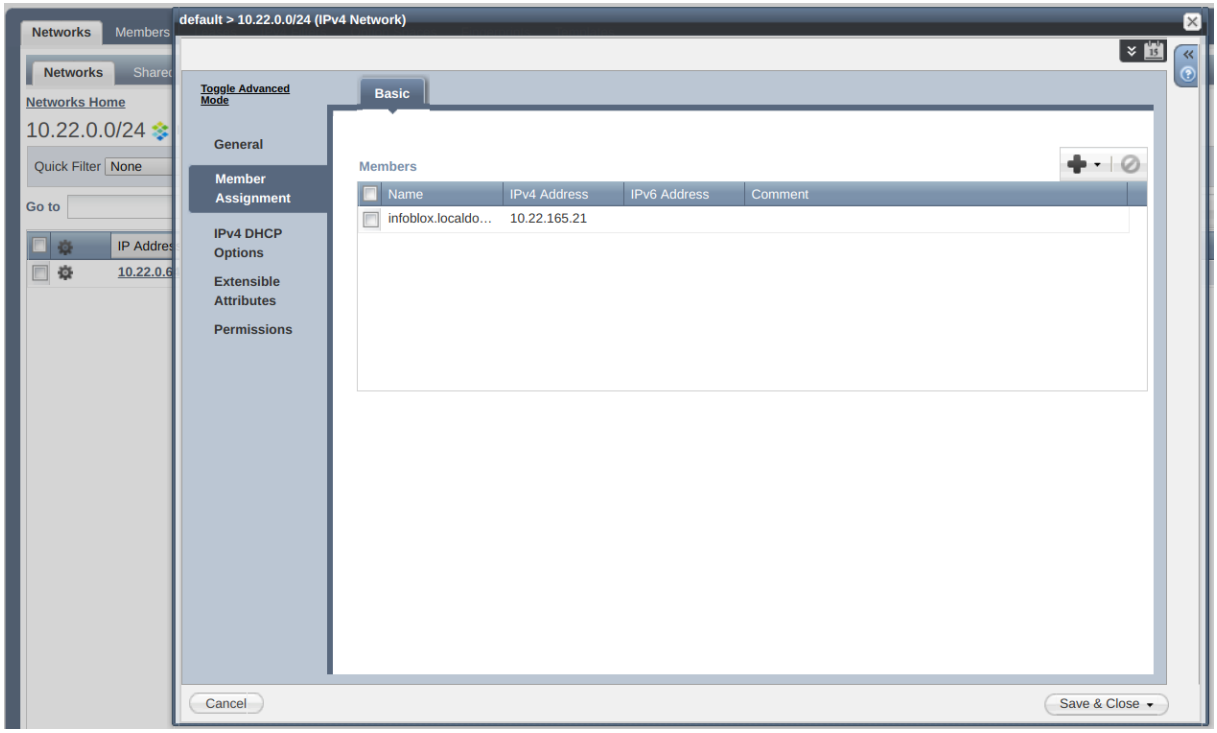

Abbildung 7.40: Infoblox - Member Assignment

Infoblox Services Damit alle Services, die Infoblox zur Verfügung stellt, stets an allen Standorten verfügbar sind, müssen die Clients primär die lokale Instanz von Infoblox verwenden. Diese kann auf einem ENCS 5400 oder einer anderen Virtualisierungsplattform betrieben werden.

DNS Werden an den Aussenstandorten Infoblox Instanzen verwendet, kann auf dem Grid Master definiert welche Instanzen was für Zonen zur Verfügung stellen. Somit können Clients an Aussenstellen alle nötigen Zonen auflösen. Im DNA Center müssen unter *Design* → *Network Settings* jeweils die DNS Server vom entsprechenden Standort konfiguriert werden. Der Server am Hauptstandort kann als zweiter Server eingetragen werden. Auch die Clients müssen die korrekten Server verwenden. Dies hat den Vorteil, dass die Antwortzeiten möglichst kurz sind und DNS auch im Falle eines Unterbruchs zum Hauptstandort zur Verfügung steht. Sofern diese ihre IP Adresse mittels DHCP beziehen, kann der DNS Server entsprechend gesetzt werden. Ansonsten muss diese Konfiguration manuell vorgenommen werden.

Abbildung 7.41: Infoblox - DNS Server

DHCP Wie auch bei DNS ist es wichtig, dass an Aussenstandorten stets der lokale DHCP Server verwendet wird. Dies kann im DNA Center unter *Design* → *Network Settings* für jeden Standort konfiguriert werden.

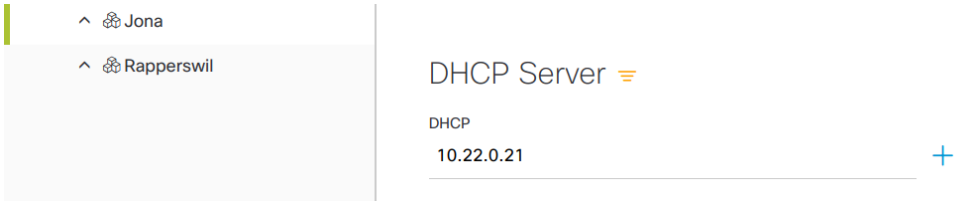

Abbildung 7.42: DNA Center - DHCP Server

Ist an einem Standort eine Hochverfügbarkeit des DHCP Services nötig, wird empfohlen, an diesem Standort ein High-Availability Pair zu betreiben.

NTP Für NTP ist es besonders wichtig, dass dieser Dienst stets verfügbar und möglichst nahe beim Client ist. Wird der NTP Dienst also an jedem Standort mit Infoblox betrieben kann die nötige Verfügbarkeit gewährleistet werden und die Zeitabweichungen sind minimal. Auch hier, kann der NTP Server für die Netzwerkgeräte im DNA Center unter *Design* → *Network Settings* individuell für jeden Standort konfiguriert werden. Für die Clients empfiehlt sich die DHCP Option 42. Mit dieser können den Clients die korrekten NTP Server mitgeteilt werden.

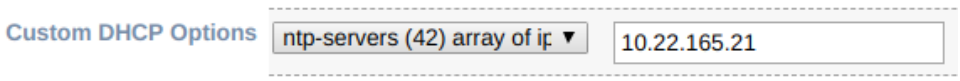

Abbildung 7.43: Infoblox - NTP Server

Die NTP Server an den Aussenstandorten verwenden als primäre Quelle die NTP Server am Hauptstandort. Um einen Ausfall der Verbindung zu diesem abzusichern, sollte aber auch mindestens ein externen NTP Server konfiguriert werden.

7.11 Third Party Software

Alternativ zu Infoblox Instanzen an allen Standorten können die Services auch mittels Third-Party Software angeboten werden.

7.11.1 DHCP

Aussenstellen Da sich Infoblox nicht in Kombination mit 3rd Party Software in einem Cluster oder einer Failoverlösung betreiben lässt, müssen an Aussenstandorten eigenständige DHCP Server betrieben werden, um deren Autonomie sicherzustellen. Da Infoblox den isc-dhcp-server für seine DHCP Services verwendet, sollte auch dieser an Aussenstandorten eingesetzt werden. Dieser kann auf einem Linux Server, optimalerweise virtualisiert auf dem ENCS 5400, betrieben werden. Für wichtige Aussenstandorte kann der isc-dhcp-server in einem Master-Slave Cluster betrieben werden. Somit ist an diesen Standorten ebenfalls eine Ausfallsicherheit gewährleistet.

7.11.2 DNS

Read Only DNS Server an Aussenstandorten Damit Aussenstellen nicht auf DNS Server des Hauptstandortes angewiesen sind, kann in jedem Standort ein Read-Only Server betrieben werden. Somit funktioniert die Namensauflösung auch im Falle eines Kommunikationsverlusts zum Hauptstandort.

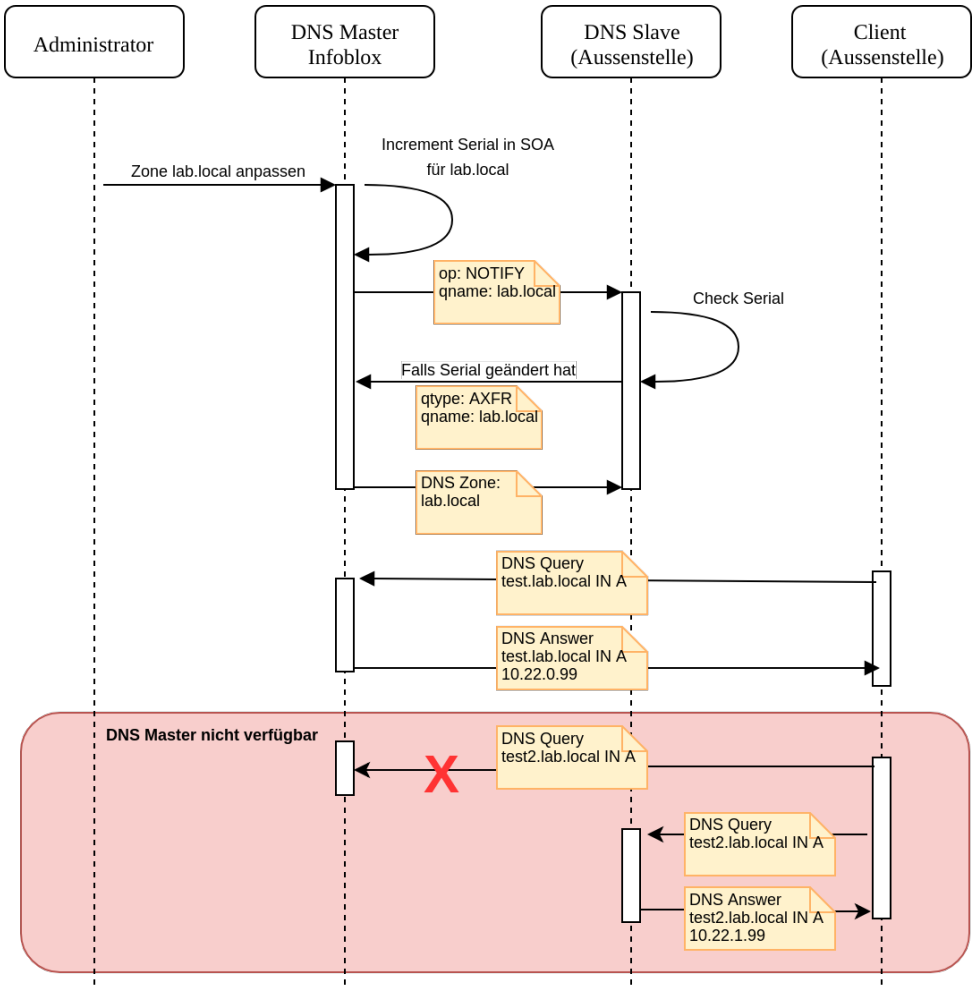

Abbildung 7.44: DNS Sequenzdiagramm

Infoblox Damit die Read-Only Server stets über die aktuellsten DNS Zonen verfügen, müssen die Informationen von Infoblox auf diese repliziert werden. In diesem Fall wird dafür der Zone Transfer verwendet. Dazu muss dies in Infoblox für alle Slave Server erlaubt werden.
Dies wird in Infoblox via *Grid* → *DNS* → *Infoblox Instanz* → *Edit* → *Zone Transfers* ausgeführt.

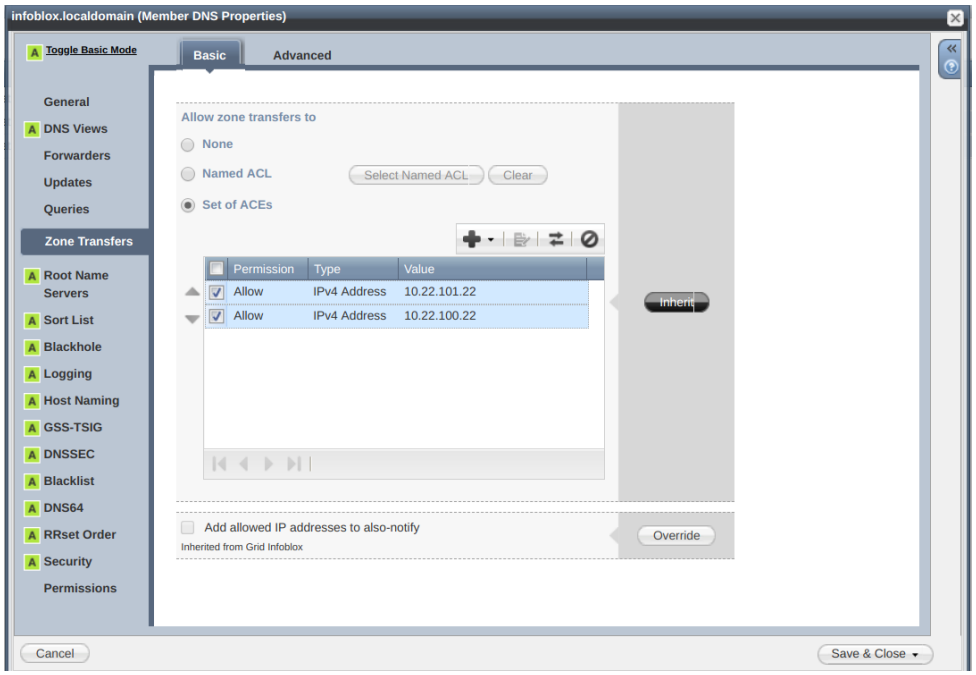

Abbildung 7.45: Infoblox Zone Transfer

DNS Slaves Auf den Slaves an den jeweiligen Aussenstandorten müssen die Zonen als Slave Zonen konfiguriert sein und Infoblox muss als Master konfiguriert werden. Dadurch können die Zonen vom Master auf den Slave transferiert werden. Der Slave aktualisiert alle Slave Zonen in regelmässigen Abständen. Dieser Intervall wird in der Zone im SOA Record mit dem "Refresh" Parameter definiert. Zusätzlich kann auf dem Master konfiguriert werden, dass alle Slaves mittels "Notify" informiert werden, sobald sich eine Zone ändert, worauf der Slave die aktuellsten Informationen für diese Zone abruft. Somit ist sichergestellt, dass alle Server an Aussenstandorten stets über eine aktuelle Konfiguration verfügen. Auf Grund der grossen Verbreitung sollte bind verwendet werden. Auch Infoblox setzt dieses Produkt ein. Dieses kann, wie auch der isc-dhcp-server auf einem Linux Server betrieben werden.

7.12 Scheduled Software Updates

Alle Netzwerk Devices die über das DNA Center verwaltet werden, erhalten ihre aktuellsten Software Images auch von diesem. Die Images haben teils sehr unterschiedliche Grössen (von 200 MB bis zu 1 GB), weshalb es wichtig ist, dass sich diese schon vor einem Upgrade auf den Geräten befinden.

7.12.1 Provision Software Images

Bevor ein Software Image auf ein Gerät übertragen wird, überprüft das DNA Center auf den einzelnen Geräten, ob dieses auch bereit für ein Update ist. Dazu gehören zum Beispiel das Überprüfen des Geräteverwaltungsstatus, Überprüfung der SCP- und HTTPS-Dateiübertragung, Festplattenspeicher usw. Wenn eine Vorprüfung fehlschlägt, kann die Aktualisierung des Software Images nicht durchgeführt werden.

Nun kann das Verteilen der Software Images nach folgendem Ablauf gestartet werden:

1. Das Verteilen der Software Images kann im DNA Center unter *Provision* konfiguriert werden.
2. Nun kann das Gerät, welches aktualisiert werden soll, ausgewählt werden. (Wenn der pre-check erfolgreich war, weisst der Link "Outdatet" in der Spalte "OS Image" ein grünes Häckchen auf.)
3. In der Dropdown-Liste unter *Actions* → *Update OS Image* wählen
   (a) Distribute: Mit einem Klick auf *Now* wird das Verteilen des Images sofort gestartet, oder es wird mit einem Klick auf *Later* an einem spezifischen Zeitpunkt ausgeführt. (Wenn sich das Image bereits auf dem ausgewählten Gerät befindet, wird der Distribute-Vorgang übersprungen und das Image kann direkt aktiviert werden.)
   (b) Activate: Mit einem Klick auf *Now* wird die Aktivierung sofort gestartet, oder es wird mit einem Klick auf *Later* an einem spezifischen Zeitpunkt ausgeführt. (Dieser Schritt kann übersprungen werden, wenn zum jetzigen Zeitpunkt nur das Image auf das Gerät verteilt werden sollte.)
   (c) Confirm: Mit einem Klick auf *Confirm* wird das Update bestätigt.
4. Nun kann unter *Upgrade Status* der aktuelle Vorgang des Image Upgrades beobachtet werden.

Sollte das Verteilen des Software Images nicht funktionieren, in dem es Beispielsweise die Übertragung immer wieder abbricht, so kann das Image auch manuell auf das Gerät kopiert werden. So würde dies bei dem vorher beschriebenen Vorgang *Distribute* automatisch erkennt werden, dass sich das Image schon auf dem Gerät befindet.

8 Abstrahierung

Im nachfolgenden Teil wird die Umsetzung der folgenden Use Cases beschrieben. Die Use Cases sind nach der Nummerierung priorisiert worden. Der UC01 soll auf jeden Fall umgesetzt werden. Der UC02 muss evaluiert werden, ob dies mit der API des DNA Centers im Zusammenspiel mit dem ENCS überhaupt möglich ist. Zum Schluss kommt der UC03, welcher nur optional ist und bei genügend verbleibender Zeit implementiert wird.

8.1 Use Cases Brief

8.1.1 UC01: Network Orchestration

Ein Administrator kann in einem Web Interface Netzwerke erstellen und verwalten. Des Weiteren ist die Möglichkeit gegeben, Policies, welche die Kommunikation zwischen diesen Netzen regeln zu erstellen. Die entsprechenden Konfigurationen werden auf allen beteiligten Geräten automatisch via APIs erstellt.

8.1.2 UC02: ENCS Virtual Machine Management

Ein Administrator kann in einem Web Interface die VMs auf einem ENCS System verwalten.

8.1.3 UC03: Configuration History

Ein Web Interface bietet die Möglichkeit, die Konfigurationen aller Geräte innerhalb einer Fabric anzuzeigen. Des weiteren kann die aktuelle Konfiguration mit älteren Versionen der Konfiguration verglichen werden.

8.2 Use Cases Fully Dressed

8.2.1 UC01: Network Orchestration

Primary Actor	Administrator
Beschreibung	Ein Administrator kann in einem Web Interface Netzwerke erstellen und verwalten. Des Weiteren ist die Möglichkeit gegeben, Policies, welche die Kommunikation zwischen diesen Netzen regeln zu erstellen. Die entsprechenden Konfigurationen werden auf allen beteiligten Geräten automatisch via APIs erstellt.
Stakeholders	• Administrator • User
Preconditions	• DNA Center komplett konfiguriert • Die Fabric läuft ohne Einschränkung • Web Interface steht zur Verfügung
Postconditions	• Änderungen an Netzen wurden auf den Netzwerkdevices umgesetzt • Policies sind korrekt umgesetzt
Main Success Story	1. Ein Netzwerk wird erstellt 2. Die Software erstellt das Netzwerk auf allen nötigen Netzwerkgeräten 3. Eine Policy für die Kommunikation mit anderen Netzen wird definiert 4. Die Konfiguration für die Policy wird automatisch auf allen nötigen Netzwerkgeräten erstellt
Alternative Flows	1a. Ein Netzwerk wird gelöscht 1b. Eine Policy wird verändert

Tabelle 8.1: UC01 Fully Dressed

8.2.2 UC02: ENCS Virtual Machine Management

Primary Actor	Administrator
Beschreibung	Ein Administrator kann in einem Web Interface die VMs auf einem ENCS System verwalten.
Stakeholders	• Administrator
Preconditions	• ENCS ist konfiguriert und mit dem DNA Center verbunden • VM Profile existieren
Postconditions	• VMs befinden sich im gewünschten Zustand
Main Success Story	1. Eine VM wird erstellt 2. Eine VM wird gestartet 3. VM wird einem Netzwerk zugewiesen
Alternative Flows	1a. VM wird gelöscht

Tabelle 8.2: UC02 Fully Dressed

8.2.3 UC03: Configuration History

Primary Actor	Administrator
Beschreibung	Ein Web Interface bietet die Möglichkeit, die Konfigurationen aller Geräte innerhalb einer Fabric anzuzeigen. Des weiteren kann die aktuelle Konfiguration mit älteren Versionen der Konfiguration verglichen werden.
Stakeholders	• Administrator
Preconditions	• Netzwerkgeräte sind erreichbar
Postconditions	• Konfiguration wird angezeigt
Main Success Story	1. Ein Netzwerkgerät wird gewählt 2. Ein Zeitpunkt wird gewählt 3. Konfiguration zum gewählten Zeitpunkt kann mit der aktuellen Version verglichen werden
Alternative Flows	

Tabelle 8.3: UC03 Fully Dressed

8.3 Technologien

Für das entwickeln des Orchestrierungstool wird Python verwendet. Für das Web Interface wird das Framework Flask eingesetzt. Mit diesen Technologien wird eine Web Anwendung entwickelt, die mit Hilfe der APIs des DNA Centers, des ENCS und der Netzwerkgeräte einzelne Prozesse vereinfacht oder automatisiert.

8.3.1 Python

Python ist eine objektorientierte Programmiersprache. Die einfache und leicht erlernbare Python-Syntax hebt die Lesbarkeit hervor und reduziert dadurch die Programmwartung. Python unterstützt Module und Pakete, was die Modularität von Programmen und die Wiederverwendung von Code fördert. Der Python-Interpreter und die umfangreiche Standardbibliothek sind in Quell- oder Binärform kostenlos für alle gängigen Plattformen verfügbar und können frei verteilt werden. [17]

8.3.2 Flask

Flask ist ein in Python geschriebenes Webframework. Der Fokus von Flask liegt auf Erweiterbarkeit und guter Dokumentation. Die einzigen Abhängigkeiten sind Jinja2, eine

Template-Engine und Werkzeug, eine Bibliothek zum Erstellen von WSGI-Anwendungen. [16]

8.3.3 DNA Center Platform

Cisco hat seit dem Sommer 2018 die DNA Center Platform zur Verfügung gestellt, über die nun auf den API Katalog und andere Ressourcen zugegriffen werden kann. So können beispielsweise die Platform Funktionen auch verwendet werden, um die Bereitstellung und Verwaltung von Netzwerken zu vereinfachen.
So soll das DNA Center nun eine 360 Grad Erweiterbarkeit durch vier verschiedene Platform Funktionen bereitstellen. Dazu gehören die Intent-based APIs, Process adapters, Domain adapters, sowie SDKs. [18]

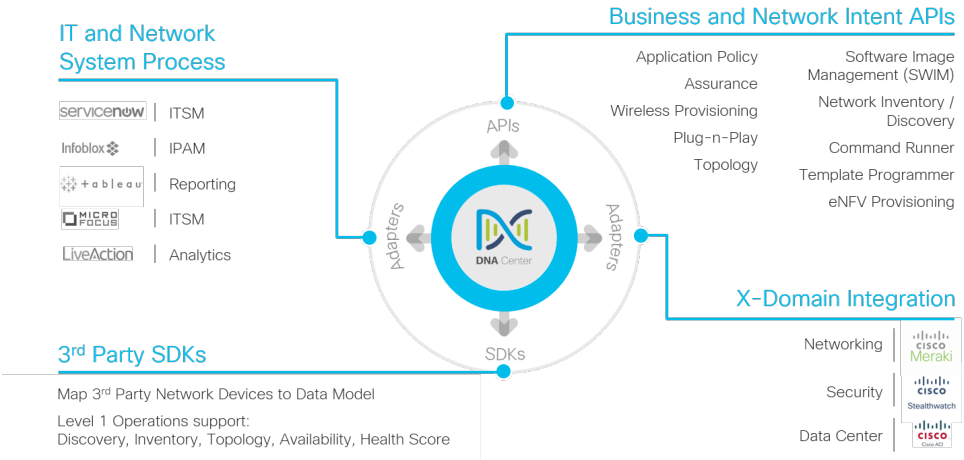

Abbildung 8.1: DNA Center Plattform [18]

Intent-API Die Intent-API ist eine Northbound REST API, welche bestimmte Funktionen des DNA Centers verfügbar macht. Mit der RESTful Intent API des DNA Centers können die HTTP- (GET, POST, PUT, DELETE) und JSON-Syntax verwendet werden, um das Netzwerk zu analysieren und zu konfigurieren. [18]
Diese APIs findet man im DNA Center unter *Platform* → *Developer Toolkit* → *APIs*

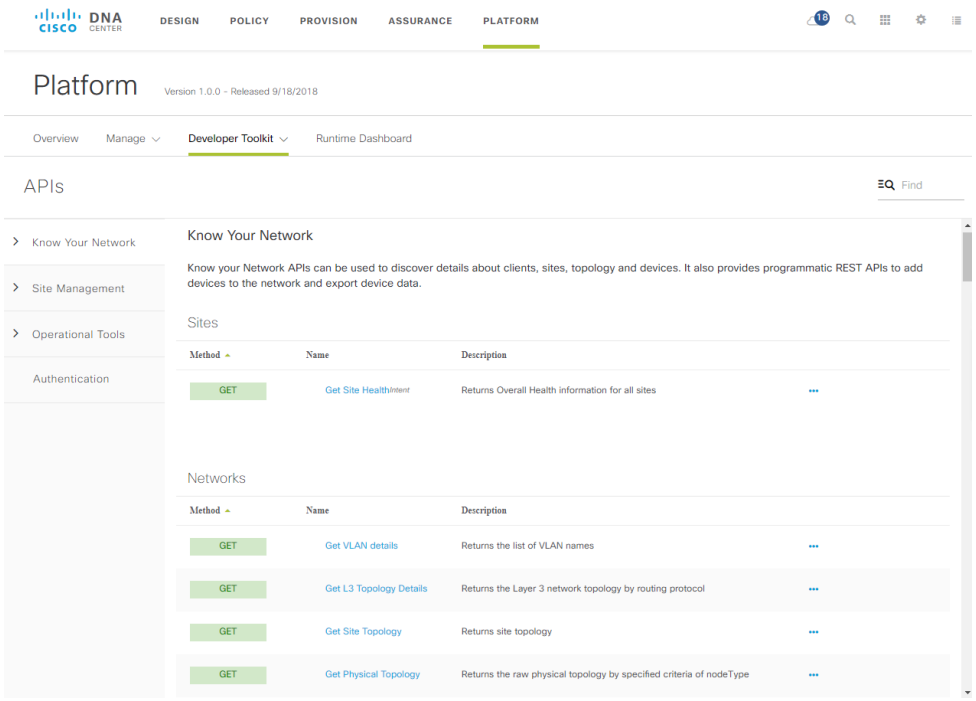

Abbildung 8.2: DNA Center Plattform APIs

8.3.4 ENCS/NFVIS API

Der ENCS beziehungsweise die NFVIS, welche auf dem ENCS läuft, stellt ebenfalls eine programmierbare API für Service Orchestration mittels REST- und NETCONF-API bereit.
Die API Dokumentationen sind bei NFVIS leider nicht direkt über dessen Applikation verfügbar. Es gibt jedoch eine Dokumentation von Cisco direkt, welche unter dem Namen *API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software* [19] zu finden ist.

8.4 Umsetzung

8.4.1 Ablauf Erstellung Netzwerk

Um die Erstellung eines Netzwerkes zu vereinfachen, wird ein Wizard erstellt, mit welchem folgende einzelnen Schritte vereinfacht auszuführen sind.

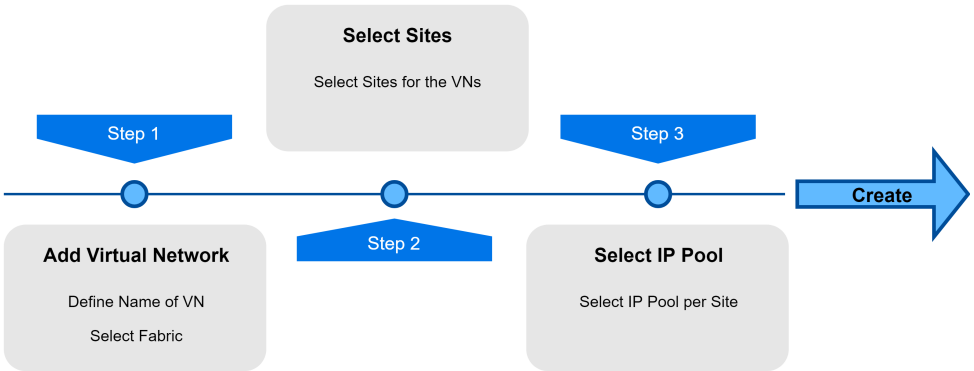

Abbildung 8.3: Add Virtual Network

Um den Wizard zu starten, kann im Orchestrationtool im Home *Virtual Networks* → *Add Virtual Networks* ausgewählt werden. So startet der Wizard mit den in der Abbildung (siehe Abbildung 8.3: Add Virtual Network) aufgezeigten Schritten und man kann Schritt für Schritt die gewünschten Informationen angeben.
Der Wizard verwendet die APIs des DNA Centers, sowie der Netzwerkgeräte. Beim DNA Center mussten teilweise undokumentierte API Endpoints verwendet werden, da die nötigen Funktionen ansonsten nicht verfügbar sind. Dies birgt das Risiko, dass sich diese in Zukunft ändern und die Applikation angepasst werden muss.
Dieser Use Case konnte nur teilweise implementiert werden. Es fehlt derzeit noch der letzte Schritt, also das Erzeugen und Schreiben der Konfiguration für die Fusion Router. Die Struktur für diese Schritte ist jedoch vorbereitet und kann ich Zukunft noch implementiert werden.

8.4.2 Virtual Machine Management

Das Virtual Machine Management zeigt alle virtuallen Maschinen auf NFVIS an. Des Weiteren wird der aktuelle Status der VMs, sowie die Netzwerkinterfaces angezeigt. Zudem ist es möglich, eine VM über das Web Interface zu starten oder zu stoppen.

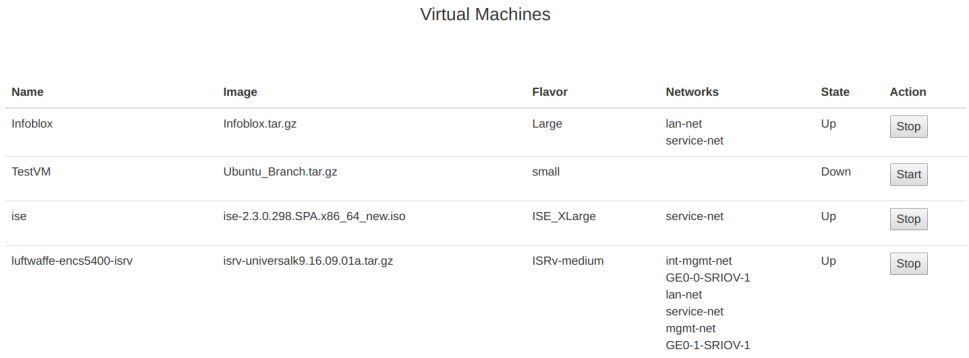

Abbildung 8.4: VM Management

8.4.3 Configuration History

Dieser Use Case konnte nicht mehr vollständig umgesetzt werden. Derzeit kann nur die aktuelle Konfiguration angezeigt werden. Die Anzeige einer History ist noch nicht implementiert.

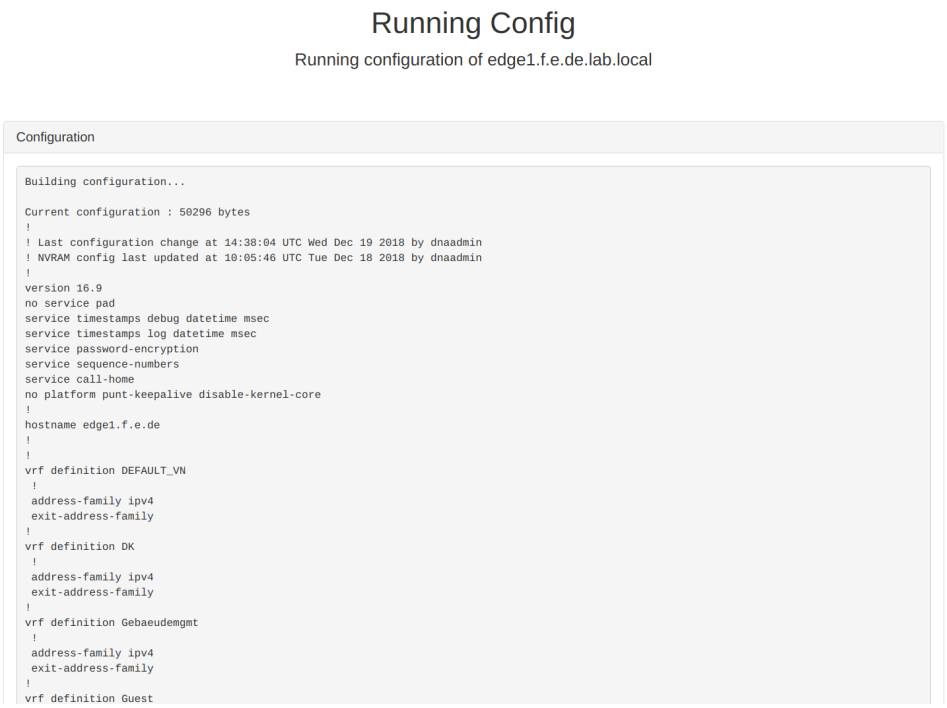

Abbildung 8.5: Running Config

9 Feature Requests und Bugs

Im Folgenden werden Feature Requests und Bugs aufgeführt, die während dieser Arbeit aufgetreten sind. Diese wurden mittesl "Make a Wish" Funktion des DNA Centers an Cisco gemeldet. Alle erwähnten Punkte beziehen sich auf das DNA Center in Version 1.2.5.

9.1 Template Zuweisung

Komponente	*Design → Network Profiles*
Beschreibung	Templates können nur Gerätetypen (z.Bsp. Switches oder Router) zugewiesen werden. Es wäre wünschenswert, wenn diese auch verschiedenen Rollen zugewiesen werden könnten. Beispielsweise allen Border Nodes.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.1: Feature Request: Template Zuweisung

9.2 Template Versionierung

Komponente	*Template Editor → Create Template*
Beschreibung	Templates können versioniert werden. Allerdings lassen sich ältere Versionen nur anschauen. Folgende Funktionen wären hilfreich: • Restore alter Templateversionen • Diffs zwischen verschiedenen Versionen anzeigen
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.2: Feature Request: Template Versionierung

9.3 Upload Image

Komponente	*Design → Image Repository → Import*
Priorität	Mittel
Beschreibung	Nach dem Uploaden eines Images, wird dieses nicht im WebGui angezeigt. Erst nach mehreren Minuten erscheint das zuvor hochgeladene Image.
Konsequenzen	Der User geht davon aus, dass der Upload fehlgeschlagen ist und versucht dies erneut.
Workaround	Keiner
Reproduzieren	1. *Design → Image Repository → Import* 2. File auswählen 3. Warten bis der Upload abgeschlossen ist 4. Image wird nicht angezeigt Nach mehreren Minuten erscheint das Image
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.3: Bug: Upload Image

9.4 Claim Device

Komponente	*Provision → Inventory*
Priorität	Niedrig
Beschreibung	Nach dem Hinzufügen oder Claimen eines Devices werden verschiedene Informationen als "null" angezeigt. Hier sollten die korrekten Informationen oder falls noch nicht verfügbar einfach nichts angezeigt werden.
Konsequenzen	Unschönes UI
Workaround	Keiner
Reproduzieren	1. *Provision → Inventory → Unclaimed Devices → Claim Device*
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.4: Bug: Claim Device

9.5 Image Checksum

Komponente	*Design → Image Repository*
Priorität	Mittel
Beschreibung	Wird auf ein Image geklickt, sodass die Detailinformationen angezeigt werden, wird die Checksumme vom "Make a Wish" Button überdeckt. Dies tritt bei FullHD Auflösung oder kleiner auf.
Konsequenzen	Checksumme nicht lesbar
Workaround	Grössere Auflösung
Reproduzieren	1. *Design → Image Repository → Auf Image klicken*
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.5: Bug: Image Checksum

9.6 Provision Status "Failed"

Komponente	*Provision → Devices → Inventory*
Priorität	Niedrig
Beschreibung	Der Provision Status wird als "Failed" angezeigt, auch wenn die Provisionierung funktioniert hat. Dies wird zur Zeit auf ewig so angezeigt, sollte im Verlauf irgendwann einmal etwas fehlgeschlagen sein. Dazu kommt, dass wenn man auf See Details klickt, die Einträge mit Success angezeigt werden. Zuerst muss also herausgefunden werden, bei welchem Workflow dies aufgetreten ist. Mit erneutem Klick auf See Details auf dem Workflow, werden die einzelnen Schritte des Workflows angezeigt.
Konsequenzen	Verwirrung das Problem vorhanden, obwohl keines besteht
Workaround	Keiner
Reproduzieren	
Reporter	Jessica Kalberer
Feedback Cisco	

Tabelle 9.6: Bug: Provision Status "Failed"

9.7 Provision Template Status Failed

Komponente	*Provision* → *Devices* → *Inventory*
Priorität	Niedrig
Beschreibung	Der Status des Schrittes im Workflow des Provisioning wird als Failed angezeigt, weil der Name schon gesetzt wurde. Es wird die Meldung "Template IOS Banner Template:2 is already deployed with same params,. Not deploying it." angezeigt. Der Name wurde zwar schon einmal mit dem Template deployed, jedoch handelte es sich nicht um den gleichen.
Konsequenzen	Verwirrung das Problem vorhanden, obwohl keines besteht
Workaround	Keiner
Reproduzieren	1. *Provision* → *Devices* → *Inventory* 2. Gewünschtes Device auswählen 3. *Actions* → *Provision* 4. Template für Namensänderung wählen 5. *Provision*
Reporter	Jessica Kalberer
Feedback Cisco	

Tabelle 9.7: Bug: Provision Template Status Failed

9.8 Fabric Custom View

Komponente	*Provision* → *Fabric* → *Layout*
Priorität	Mittel
Beschreibung	Wenn eine Custom View erstellt wird und diese ausgewählt wird, werden die Devices nicht mehr als Teil der Fabric angezeigt.
Konsequenzen	Fabric lässt sich in der Custom View nicht bearbeiten
Workaround	Keiner
Reproduzieren	1. *Provision* → *Fabric* → *Layout* 2. Custom View erstellen 3. Custom View anzeigen
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.8: Bug: Fabric Custom View

9.9 Fabric Default View

Komponente	*Provision* → *Fabric* → *Layout*
Priorität	Niedrig
Beschreibung	Wenn eine Custom View erstellt wird und anschliessend als Default View definiert wird, hat dies keinen Einfluss auf die Default View. Es wird weiterhin die Default View von Cisco angezeigt
Konsequenzen	Custom Views sind nutzlos, wenn jedes Mal die gewünschte View gewählt werden muss.
Workaround	Keiner
Reproduzieren	1. *Provision* → *Fabric* → *Layout* 2. Custom View erstellen 3. Custom View als Default setzen 4. Reload
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle 9.9: Bug: Fabric Default View

10 Ergebnisdiskussion

Die Analyse der kritischen Komponenten wurde abgeschlossen und diese sind identifiziert. Dazu wurden die kritischen Komponenten nach ihrer Prorität gewichtet.
Während der Absicherung wurden die kritischen Komponenten genauer analysiert, die Möglichkeiten zur Absicherung abgewägt und eine Empfehlung für ein krisensicheres Deployment erarbeitet. Anschliessend wurden die Empfehlungen wo möglich im eigenen Lab angewendet und somit die meisten Komponenten und Verbindungen redundant ausgelegt.
Die Abstrahierung konnte teilweise umgesetzt werden. Bei der Entwicklung des Orchestrierungstool kam es zu Problemen mit den DNA Center APIs. Diese waren teilweise falsch oder unvollständig dokumentiert. Zudem mussten viele API Endpoints verwendet werden, die in keiner Dokumentation enthalten sind. Aus diesem Grund nahm die Entwicklung des Tools mehr Zeit als geplant in Anspruch und es konnten nicht alle Use Cases komplett abgedeckt werden.

11 Schlussfolgerungen

11.1 Erreichte Ziele

Wie in den Ergebnissen erwähnt, konnten die gesetzten Ziele der Bachelorarbeit grösstenteils erreicht werden.

11.2 Mögliche Verbesserungen

Obwohl das DNA Center seit der Studienarbeit stark verbessert wurde, sind immer noch sehr viele Bugs vorhanden. Hier kann durch Fixes dieser Bugs eine grosse Verbesserung erreicht werden. Dasselbe kann für die ISE gesagt werden. Ebenfalls können einzelne Workflows im DNA Center optimiert oder durch Wizards erleichtert werden. Dies würde die Komplexität des Systems reduzieren. Bezüglich der APIs ist es wünschenswert, dass mehr API Endpoints zur Verfügung gestellt und dokumentiert werden.

11.3 Zukunft

Seit vielen Jahren betreiben viele Unternehmen ihre Netzwerke gleich, manuell mit Konsolenkabeln, Telnet, SHH, CLI oder anderen Tools. In der Zeit der Digitalisierung wird es immer schwieriger solch grosse Netze kosteneffizient zu warten. Vor fast zwei Jahren hat sich Cisco zum Ziel gesetzt das Campus Netzwerk neu zu erfinden und dabei das DNA Center entwickelt. Im Frühling 2018 hat Cisco die DNA Assurance eingeführt, um das Monitoring des gesamten Netzwerkes enorm zu vereinfachen. Im Sommer 2018 hat Cisco nun das DNA Center für Entwickler zugänglich gemacht. Dank der neuen offenen DNA Center Platform können über die APIs eigene Anwendungen entwickelt werden.

Das DNA Center wurde innerhalb der letzten Jahren stets weiterentwickelt und viele Bugs und Probleme wurden behoben. Es ist zu hoffen, dass dies so weitergeführt wird.

Nicht nur Cisco, sondern auch andere Hersteller fördern die Automatisierung des Netzwerkes, um Campus Netzwerke bereitzustellen. Dabei setzen sie ebenfalls auf eine zentrale Plattform, mit welcher das Monitoring und Provisioning ausserordentlich vereinfacht wird. Dies zeigt, dass die Zukunft auch für Campus Netze im Bereich SDN liegt.

12 Abkürzungsverzeichnis

AAA Authentication, Authorization, and Accounting

ACL Access Control List

AP Access Point

API Application Programming Interface

ARP Address Resolution Protocol

BGP Border Gateway Protocol

CA Certificate Authority

CCO Cisco Connection On-line

CIMC Cisco Integrated Management Controller

CLI Command-Line Interface

CMD Cisco Meta Data

CP Control Plane

CVD Cisco Validated Design

C3850 Catalyst 3850

C9300 Catalyst 9300

DHCP Dynamic Host Configuration Protocol

DNA Cisco Digital Network Architecture

DNS Domain Name System

dot1x IEEE 802.1X Standard zur Authentifizierung

ECNS Enterprise Network Compute System

EID Endpoint Identifier

ETR Egress Tunnel Router

FE Fabric Edge

FUB Führungsunterstützungsbasis

GW Gateway

HTDB Host Tracking Database

IEEE Institute of Electrical and Electronics Engineers

IGP Interior Gateway Protocol

IOS Internetworking Operating System

IoT Internet of Things

IP Internet Protocol

IPAM IP-Adress-Management

ISE Cisco Identity Services Engine

IS-IS Intermediate System to Intermediate System

ISR Integrated Service Routers

ITR Ingress Tunnel Router

KVM Kernel-based Virtual Machine

LAN Local Area Network

LISP Locator/ID Separation Protocol

MnT Monitoring and Troubleshooting Node

MS Map Server

MS/MR Map Server/Map Resolver

MR Map Resolver

NFS Network File System

NTP Network Time Protocol

NFV Network Functions Virtualization

NFVIS NFV Infrastructure Software

PAN Policy Administration Node

PETR Proxy Egress Tunnel Router

PITR Proxy Ingress Tunnel Router

PnP Plug and Play

PSN Policy Service Node

PXG PxGrid

pxGrid Platform Exchange Grid

qcow QEMU Copy On Write

RADIUS Remote Authentication Dial-In User Service

REST Representational State Transfer

RLOC Routing locator

SCP Secure Copy

SDA Software-Defined Access

SDK Software Development Kit

SDN Software-Defined Networking

SGACL Scalable Group Access Control List

SGT Security Group Tags

SNMP Simple Network Management Protocol

STP Spanning Tree Protocol

SXP Security Group Tag Exchange Protocol

TFTP Trivial File Transfer Protocol

TTL Time To Live

UDP User Datagram Protocol

URL Uniform Resource Locator

VLAN Virtual Local Area Network

VM Virtual Machine

VN Virtual Network

VNI Virtual Extensible LAN Network Identifier

VPN Virtual Private Network

VRF Virtual Routing and Forwarding

VSS Virtual Switching Systems

VTEP Virtual Extensible LAN Tunnel Endpoint

VXLAN Virtual Extensible LAN

VXLAN-GPO Virtual Extensible LAN Group Policy Option

WAN Wide Area Network

Web World Wide Web

WLAN Wireless Local Area Network

WLC Wireless LAN Controller

WSGI Web Server Gateway Interface

XML Extensible Markup Language

xTR x Tunnel Router

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

[1] Studienarbeit *Software-Defined Netzwerk im Campus Bereich*, FS2018 (URL: https://github.com/night28/HSR_BA/blob/master/Software-Defined_Netzwerk_im_Campus_Bereich_eprint.pdf), 18.09.2018

[2] SDA Design Guide *Software-Defined Access Design Guide August*, 2018 (URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2018AUG.pdf), 02.10.2018

[3] SDA Design Guide *Software-Defined Access Design Guide September*, 2018 (URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Sol1dot2-2018SEP.pdf)

[4] Severity Guidelines *Cisco Severity and Escalation Guidelines*, 2018 (URL: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Severity_and_Escalation_Guidelines.pdf), 11.10.2018

[5] LISP Host Mobility Solution *LISP Host Mobility Solution*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/5-0/LISPmobility/DCI_LISP_Host_Mobility/LISPmobile_3.html), 17.10.2018

[6] LISP Impact *Locator/ID Separation Protocol (LISP) Impact*, 2016, (URL: https://tools.ietf.org/html/rfc7834), 31.10.2018

[7] SDA Deployment Guide *SDA Deployment Guide Oktober*, 2018, (URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Deployment-Guide-Sol1dot2-2018OCT.pdf), 07.11.2018

[8] SDA Segmentation Design Guide *SDA Segmentation Design Guide May*, 2018 (URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf), 15.11.2018

[9] Cisco Digital Network Architecture Center Installation Guide *Release 1.2*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/install/b_dnac_install_1_2/b_dnac_install_1_2_chapter_0101.html), 08.12.2018

[10] Cisco Identity Services Engine Installation Guide *Network Deployments in Cisco ISE*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/install_guide/b_ise_InstallationGuide24/b_ise_InstallationGuide24_chapter_00.html), 10.12.2018

[11] Enterprise Network Functions Virtualization FAQ *Virtualization Architecture*, 2018 (URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-functions-virtualization-nfv/q-and-a-c67-736831.html), 09.12.2018

[12] Cisco DNA Center *Release Notes*, 2018 (URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html)

[13] LISP Command Reference *LISP Show Commands*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/command/ip-lisp-cr-book/ip-lisp-cr-book_chapter_01011.html), 16.12.2018

[14] ISE Install Guide *Deployment Models*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/install_guide/b_ise_InstallationGuide23/b_ise_InstallationGuide23_chapter_00.pdf), 17.12.2018

[15] Transit Fabric *Transit Fabric*, 2018 (URL: http://www3.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/SD-Access.pdf), 19.12.2018

[16] Flask *Microframework for Python*, 2018 (URL: http://flask.pocoo.org/), 19.12.2018

[17] Python *What is Python? Executive Summary*, 2018, (URL: https://www.python.org/doc/essays/blurb/), 19.12.2018

[18] DNA Center Platform *Übersicht*, 2018, (URL: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/cisco-dna-center-platform-overview), 19.12.2018

[19] NFVIS *API Reference*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/routers/nfvis/user_guide/b-api-reference-for-cisco-enterprise-nfvis.html), 20.12.2018