



Software-Defined Netzwerk im Campus Bereich

Studienarbeit

Abteilung Informatik
Hochschule für Technik Rapperswil

Frühjahrssemester 2018

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

Inhaltsverzeichnis

1	Aufgabenstellung	1
2	Abstract	2
2.1	Aufgabenstellung	2
2.2	Vorgehen	2
2.3	Fazit	2
3	Management Summary	3
3.1	Ausgangslage	3
3.2	Vorgehen und Technologien	3
3.3	Ergebnisse	3
3.4	Ausblick	4
4	Ausgangslage (Kontext)	5
5	Problembeschreibung (Stand der Technik)	6
6	Lösungskonzept	7
7	Technologien	8
7.1	Software Defined Access (SDA)	8
7.1.1	Campus Fabric	8
7.1.2	Architektur	12
7.2	Cisco Digital Network Architecture Center (Cisco DNA-Center)	12
7.3	Identity Service Engine (ISE)	15
7.4	Locator ID Separation Protocol (LISP)	16
7.4.1	Campus Fabric und LISP	18
7.5	Virtual Extensible LAN (VXLAN)	18
7.5.1	VXLAN Encapsulation	19
7.5.2	Fabric Data Plane	20
7.6	Slack	21
7.7	Infoblox	21
7.8	SDA Mechanismus Beispiel	22
8	Use Cases	24
8.1	Use Cases Brief	24
8.1.1	UC01: Definierung von Benutzer und Geräteprofilen	24
8.1.2	UC02: Gastzugang	24
8.1.3	UC03: Backup and Restore DNA Center	24
8.1.4	UC04: Reporting	24
8.1.5	UC05: Hardware Ersatz	24
8.1.6	UC06: Benutzermobilität	24
8.1.7	UC07: Degradation	24
8.1.8	UC08: Integration von nicht Fabric Komponenten	24
8.1.9	UC09: Migration von bestehenden klassischen Campus	24
8.1.10	UC10: Einsatz von SGT	25
8.1.11	UC11: Infoblox	25
8.2	Use Cases Fully dressed	26

8.2.1	UC01: Definierung von Benutzer und Geräteprofilen	26
8.2.2	UC02: Gastzugang	27
8.2.3	UC03: Backup and Restore DNA Center	28
8.2.4	UC04: Reporting	29
8.2.5	UC05: Hardware Ersatz	30
8.2.6	UC06: Benutzermobilität	31
8.2.7	UC07: Degradation	33
8.2.8	UC08: Integration von nicht Fabric Komponenten	34
8.2.9	UC09: Migration von bestehenden klassischen Campus	35
8.2.10	UC10: Einsatz von SGT	36
8.2.11	UC11: Infoblox	37
9	Testprotokolle	38
9.1	UC01	38
9.2	UC02	39
9.3	UC03-1 Backup DNA Center	40
9.4	UC03-2 Restore DNA Center	41
9.4.1	Zusammenfassung UC03	41
9.5	UC11: Infoblox	42
9.6	UC04: Reporting	43
9.7	UC05: Hardware Ersatz	44
9.8	UC06: Benutzermobilität	45
9.9	UC07: Degradation	46
9.10	UC08: Integration von nicht Fabric Komponenten	47
9.11	UC10: Gastzugang	47
9.12	UC10: Einsatz von SGT	48
9.12.1	Zusammenfassung UC10	49
10	Umsetzung	50
10.1	Labor Netzwerk Architektur	50
10.2	Netzwerkarchitekturen Vergleich	50
10.3	Maximale Skalierungen	51
10.4	Verkabelungsplan	54
11	Vorgehen Versuch 1	55
11.1	DNA Center Initiales Setup	55
11.1.1	Installation	55
11.1.2	Setup Accounts	57
11.2	DNA Center Updates	59
11.2.1	Fehlgeschlagene Updates reparieren	60
11.2.2	Update Reihenfolge	60
11.2.3	Schwierigkeit: CCO Credentials für Updates notwendig	61
11.2.4	Schwierigkeit: Unterschiedliche Versionsangabe	61
11.3	DNA Center Netzwerk Design	61
11.3.1	Network Hierarchy	61
11.4	LAN Automation	63
11.4.1	DHCP Konfiguration	63
11.5	Underlay Konfiguration	64
11.6	”Claim“ von Netzwerkgeräten	65

11.6.1 DNA Center Provision - Unclaimed Devices	65
11.7 Netzwerkgeräte zu Inventory hinzufügen	66
11.7.1 Manuell Geräte im DNA Center hinzufügen	66
11.8 Image Repository	67
11.9 Automatisches Softwareupdate von Netzwerkgeräten	68
11.10 Manuelles Softwareupdate	69
11.11 Lizenzen	69
11.12 Device Provisioning via DNA Center	72
11.13 Fabric Konfigurieren	72
11.14 DNA Center Reset	73
12 Vorgehen Versuch 2	76
12.1 Vorarbeiten	76
12.1.1 ISE reset	76
12.2 DNA Center Update	77
12.3 DNA Center Netzwerk Design	77
12.4 ISE Integration	77
12.5 LAN Automation	78
12.5.1 Verbindung zwischen Legacy Router und Border Switch	78
12.5.2 Discovery	79
12.6 LAN Automation PnP	80
12.7 Provisioning	83
12.7.1 Templates	83
12.7.2 Network Profile anlegen	84
12.7.3 Initial Provisioning	85
12.7.4 Geräte zur Fabric hinzufügen	87
12.7.5 Border BGP	90
12.7.6 IP Pools definieren	90
12.7.7 Host Onboarding	90
12.7.8 Authentifizierungsmethoden	90
13 Ergebnisdiskussion	91
14 Schlussfolgerungen	92
14.1 Erreichte Ziele	92
14.2 Mögliche Verbesserungen	92
14.3 Zukunft	92
15 Abkürzungsverzeichnis	93
A Installationsanleitung	I
A.1 DNA Center Setup	I
A.1.1 DNA Center Reset	I
A.2 DNA Center Network Discovery	I
B Benutzerhandbuch	II
B.1 Updates	II
B.2 Access Control Policies	II
B.2.1 Workflow	III

B.2.2	Erstellen eines virtuellen Netzwerkes	III
B.2.3	Erstellen einer Skalierbaren Gruppe	IV
B.3	Erstellen eines Zugriffskontrollvertrages	IV
C	Projektmanagement	V
C.1	Projektübersicht	V
C.1.1	Ziele der Projektes	V
C.2	Projektorganisation	V
C.2.1	Organisationsstruktur	V
C.3	Management Abläufe	V
C.3.1	Zeitliche Planung	VI
C.3.2	Meilensteine	VI
C.3.3	Arbeitspakete	VI
C.3.4	Besprechungen	VI
C.4	Infrastruktur	VII
C.5	Risiko Management	VII
C.5.1	Umgang mit Risiken	VII
C.5.2	Risiken	VIII
C.5.3	Eingetretene Risiken	XI
D	Bugs	XV
D.0.1	Backup Server hinzufügen	XV
D.0.2	Netzwerkgerät OS Update	XVI
D.0.3	DNA Center Update - Appliance nicht nutzbar während Update	XVII
D.0.4	Devices mit Namen "NULL" können nicht gelöscht werden	XVIII
D.0.5	https://dnacenter/mypnp Configurations nicht lösbar	XIX
D.0.6	9xxx Serie Lizenzzuordnung	XIX
D.0.7	PNP	XX
D.0.8	LAN Automation IP Vergab	XX
D.0.9	Manuelle Eingriffe Infoblox	XXI
E	Persönliche Summaries	XXII
E.1	Sandro Kaspar	XXII
E.2	Philipp Albrecht	XXII
E.3	Jessica Kalberer	XXII
F	Sitzungsprotokolle	XXIII
F.1	Sitzungsprotokoll 27.02.2018	XXIII
F.2	Sitzungsprotokoll 06.03.2018	XXIV
F.3	Sitzungsprotokoll 08.03.2018	XXVII
F.4	Sitzungsprotokoll 13.03.2018	XXIX
F.5	Sitzungsprotokoll 20.03.2018	XXXI
F.6	Sitzungsprotokoll 10.04.2018	XXXIII
F.7	Sitzungsprotokoll 17.04.2018	XXXV
F.8	Sitzungsprotokoll 24.04.2018	XXXVI
F.9	Sitzungsprotokoll 01.05.2018	XXXVII
F.10	Sitzungsprotokoll 02.05.2018	XXXVIII
F.11	Sitzungsprotokoll 08.05.2018	XXXIX
F.12	Sitzungsprotokoll 16.05.2018	XL

F.13 Sitzungsprotokoll 22.05.2018	XLI
F.14 Sitzungsprotokoll 29.05.2018	XLII
F.15 Sitzungsprotokoll 05.06.2018	XLIV
F.16 Sitzungsprotokoll 12.06.2018	XLV
G Erklärungen	XLVI
G.1 Eigenständigkeitserklärung	XLVI
G.2 Urheberrechtsvereinbarung	XLVII
Tabellenverzeichnis	XLVIII
Abbildungsverzeichnis	L
Literaturverzeichnis	LI

1 Aufgabenstellung

Die vom Betreuer abgegebene und unterschriebene Aufgabenstellung (eingescannt).

Zur Zeit ist nur die Aufgabenstellung aus dem AVT verfügbar. Die finale Aufgabenstellung folgt in den letzten zwei Wochen der Studienarbeit.

Software-Defined Netzwerk im Campus Bereich

Studiengang: Informatik (I)

Semester: FS 2018 (19.02.2018-16.09.2018)

Durchführung: Bachelorarbeit, Studienarbeit

Fachrichtung: Network Design and Security

Institut: INS: Institut für vernetzte Systeme

Gruppengrösse: 2-3 Studierende

Status: zugewiesen

Verantwortlicher: Metzger, Laurent

Betreuer: Metzger, Laurent

Gegenleser: Beat Stettler

Experte: Laurent Billas

Industriepartner: Führungsunterstützungsbasis (FUB) der Schweizer Armee

Ausschreibung: Das Netzwerk einer völlig neuen Ära.

Da Software-Defined Access Neuland im Campus Bereich ist, wollen wir die SD-Access Lösung von Hersteller Cisco ausarbeiten.

Aufgaben:

- Installation von DNA-Center und Integration vom bestehenden Campus Labor-Netzwerk.
- Definierung von Benutzer- und Geräteprofile, um basierend auf Geschäftsanforderungen die Zugriffsrechte und Netzwerksegmentierung zu verwalten und so das Netzwerk sicher zu halten.
- Verwendung von Erkenntnissen von DNA Analytics and Assurance für eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerks.
- Integration vom bestehenden IP Address Management Tool im DNA Center.
- Durch APIs, Erstellung von Wöchentlichen Reports über Campus Netzwerk-Status in einem E-Mail und in einem Slack Message.

Voraussetzungen: Routing & Switching, Python, REST APIs, JSON/XML, git/GitHub, Linux Skills

Abbildung 1.1: Aufgabenstellung aus AVT

2 Abstract

2.1 Aufgabenstellung

Ziel dieser Studienarbeit war die Evaluation des Cisco Digital Network Architecture (DNA) Center, der Software Defined Access Lösung von Cisco, für die Führungsunterstützungsbasis (FUB) der Schweizer Armee. Das DNA Center soll das Deployment und Management einer Campus Netzwerk Umgebung mit Hilfe von Technologien wie VXLAN und LISP automatisieren und vereinfachen.

Für die FUB sollte die Lösung unter anderem folgende Anforderungen abdecken:

- Definierung von Benutzer- und Geräteprofilen
- Gastzugang
- Reporting der Netzwerkaktivitäten
- Benutzermobilität
- Degradation, Backup, Restore
- Anbindung an externe Systeme wie ISE und Infoblox

2.2 Vorgehen

Der erste Teil der Arbeit war die Installation und Konfiguration des DNA Centers, die Anbindung an externe Systeme und das Deployment einer Fabric in einer Testumgebung. Die Inbetriebnahme des Campus Netzwerkes gestaltet sich schwieriger als erwartet. Viele der Schritte sind nur teilweise automatisiert und es ist sehr viel manueller Aufwand nötig. Als Beispiel kann hier die LAN Automation aufgeführt werden. Mit Hilfe dieser sollten sich Netzwerkgeräte automatisiert mittels Plug and Play (PnP) in Betrieb nehmen und konfigurieren lassen. Dieser Prozess ist allerdings sehr fehleranfällig und funktioniert nur unzuverlässig, sodass die Inbetriebnahme des Underlay Netzwerkes erst nach mehreren Versuchen korrekt ausgeführt werden konnte. Des Weiteren funktionieren viele Funktionen des DNA Centers nur mit spezifischen Versionen von ISE und IOS-XE. Dies führte zu weiteren Komplikationen, da dies vom Hersteller so nicht dokumentiert ist.

In einem zweiten Schritt ging es darum, Benutzer- und Geräteprofile zu definieren, sowie deren Zugriffe zentral zu verwalten. Des Weiteren sollte mit DNA Assurance eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerkes sichergestellt werden. Mit diesen Informationen sollten wöchentliche Reports über den Status des Netzwerks per E-Mail oder Slack Message versendet werden.

2.3 Fazit

Abschliessend kann gesagt werden, dass für die Installation und Konfiguration des DNA Centers mehrere Tage, wenn nicht Wochen eingerechnet werden müssen. Zudem muss im optimalen Fall ein Green Field vorliegen, da zur Zeit kein bestehendes Netzwerk ohne Unterbrüche migriert werden kann. Bei der Installation sollten die empfohlenen Softwareversionen genauestens eingehalten werden, da sonst die volle Funktionalität des DNA Centers nicht gewährleistet werden kann.

Unserer Meinung nach hat das DNA Center sehr grosses Potenzial, ist in der aktuellen Version aber noch nicht bereit für den produktiven Einsatz. Sollte dies dennoch angestrebt werden, macht es sicherlich Sinn, die Lösung mit Hilfe des Herstellers zu implementieren.

3 Management Summary

3.1 Ausgangslage

Diese Arbeit beschäftigt sich mit Software Defined Networking im Campus LAN für die Führungsunterstützungsbasis der Schweizer Armee. Die Lösung soll den Netzwerkzugriff der Mitarbeiter der FUB sicherstellen und die Zugriffsrechte der einzelnen Mitarbeiter oder Teams regeln können. Des Weiteren müssen Reportingfunktionen und eine proaktive Überwachung erstellt werden, um allfällige Fehler schnellstmöglich zu erkennen, das Netzwerk stets zu optimieren und dessen Funktion jederzeit sicherzustellen. Zusätzlich wird ein bestehends IP Management Tool in die Lösung integriert.

Da die Anforderungen an Campus Netzwerke aus verschiedensten Gründen, wie z.Bsp. modernen Arbeitsmodellen, neuen Sicherheitsanforderungen usw. ständig steigen, ist es äusserst schwierig und aufwändig, diese Anforderungen mit traditionellen Methoden zu erfüllen.

Um dies zu erreichen wird in dieser Arbeit daher ein Software Defined Network erstellt, dass diesen neuen Anforderungen gerecht werden soll. Vorteile zeigen sich insbesondere dadurch, dass eine derartige Lösung flexibler ist, also einfacher und schneller an neue Gegebenheiten angepasst werden kann und durch Schnittstellen einfach an bestehende Systeme anzubinden ist. Durch das zentrale Management und Monitoring der Komponenten sinkt zudem das Risiko für Fehler massiv und viele Aufgaben lassen sich einfach und schnell automatisieren. Schlussendlich kann durch diese Vorteile sehr viel Aufwand und damit Kosten eingespart werden.

Ziel ist es, die Vorteile dieser Lösung gegenüber einer traditionellen Netzwerkinfrastruktur aufzuzeigen, allfällige Risiken und mögliche Probleme früh zu erkennen und Lösungen für diese zu finden.

3.2 Vorgehen und Technologien

Die Lösung wird mit dem Produkt Software Defined Access von Cisco erstellt. Diese besteht aus mehreren Komponenten dies ist zum einem das DNA Center, welches die grundsätzliche Funktion des Netzwerks sicherstellt, sowie ISE (Identity Service Engine), welches die Benutzeridentitäten und Profile verwaltet. Zusätzlich muss das bestehende IP Management in die Lösung integriert werden und Reporting Funktionen mittels Slack und E-Mail implementiert werden. Diese Zusatzfunktionalitäten werden in Python implementiert und nutzen die in Ciscos SDA enthaltenen APIs.

3.3 Ergebnisse

Am Ende dieser Arbeit wird ein funktionierender Prototyp eines Software Defined Networks im Access Bereich zur Verfügung stehen, der alle Requirements des Industriepartners abdeckt. Der Prototyp besteht aus den Cisco Komponenten, sowie Eigenentwicklungen, die zusätzliche Features implementieren. Zudem steht eine Dokumentation des Systems zur Verfügung, die den Installationsprozess und die Handhabung des Systems erklärt. Des Weiteren zeigt die Dokumentation Vorteile, aber auch Risiken und mögliche Probleme im Vergleich zu einer traditionellen Netzwerklösung auf.

3.4 Ausblick

Die Resultate aus dieser Arbeit können dazu dienen, SDA in einer produktiven Umgebung in Betrieb zu nehmen. Zudem kann er Prototyp um zusätzliche Funktionen erweitert werden, an zusätzliche bestehende oder neue Systeme angebunden werden oder mit alternativen Lösungen verglichen werden.

4 Ausgangslage (Kontext)

- Beschreibung des Typs der Arbeit (Bsp. Fokus Lösungserstellung oder Machbarkeitsanalyse)
- Fachliche Domäne, Zielgruppe, heutige Praktiken bzw. Lösungen (Methoden, Tools, etc.)

Bei dieser Arbeit handelt es sich um eine Produktevaluation mit Ausführlichem Testing.

5 Problembeschreibung (Stand der Technik)

- Motivation für die Arbeit, z.B. aus den Schwächen der heutigen Praktiken bzw. Lösungen
- Funktionale Anforderungen beschrieben (z.B. als Use Cases (short) mit Akteuren oder in Form von User Stories mit Personas)
- Wichtigste NFA/Qualitätsattribute abgedeckt und überprüfbar beschrieben

Um den heutigen Anforderungen an Campus Netzwerke im Bezug auf Sicherheit, Wartbarkeit und Skalierbarkeit gerecht zu werden, steht man mit der isolierten Konfiguration einzelner Komponenten schnell vor verschiedenen Problemen. In erster Linie ist es extrem Aufwändig alle Konfigurationen manuell zu erstellen. Selbst das Hinzufügen von einfachen Richtlinien oder zum Beispiel neuen Firmenabteilungen können zu gewaltigem Aufwand führen. Des Weiteren verliert man schnell die Übersicht und ist gezwungen umfangreiche Dokumentationen zu erstellen. Häufig kommen selbstgeschriebene Script zum Beispiel mithilfe von NAPALM (Siehe: [18]) zur automatisierten Konfiguration zum Einsatz. Für das Monitoring des Netzwerkes sind zusätzlich Tools wie icinga2 (Siehe: [19]) oder ähnlich nötig.

Typische Herausforderungen bei den klassischen Campus Netzwerken:

- Zu wenig VLAN
- VLAN über ein Layer 3 Netzwerk
- Mobilität von Komponenten
- Mobilität von Benutzer (Netzwerk Teilnehmer)
- Durchsetzen von Sicherheitsregeln mithilfe von Firewalls
- Direkte Abhängigkeit von Berechtigungen und IP Subnetzen
- Mehrere Unabhängige Tools mit Informationsredundanz
- Komplexe Fehlersuche über verschiedene Komponenten/Geräte hinweg.

Genau hier setzt das Cisco DNA Center an. Es fasst alle diese Tools unter einem Dach zusammen und bietet eine übergreifende Plattform.

6 Lösungskonzept

- Dokumentation Architektur und Design (i.d.R. plattformneutral bzw. technologieübergreifend, z.B. in Form von UML-Diagrammen und Erläuterungen dazu)
- Architekturentscheidungen mit Begründungen
- Diskussion, wie Qualitätsattribute adressiert werden (welche Qualität kann erreicht werden?)

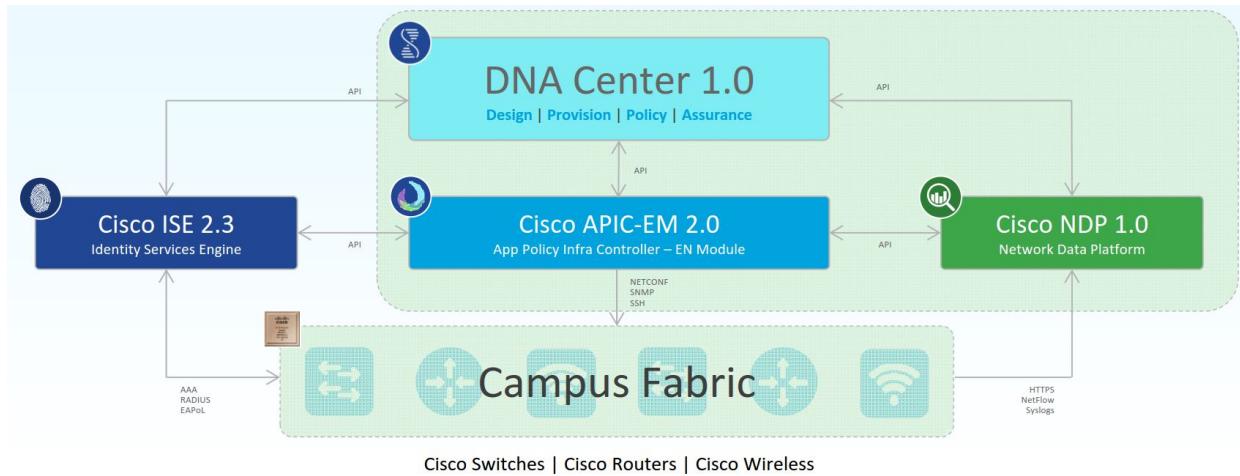


Abbildung 6.1: DNAC Komponenten

7 Technologien

7.1 Software Defined Access (SDA)

Cisco bietet mit SDA eine automatisierte End-to-End-Segmentierung um den Benutzer-, Gerät- und Anwendungsverkehr zu trennen, ohne das Netzwerk neu zu gestalten. Durch diesen automatisierten Benutzerzugriff ermöglicht SDA Einrichtungen innerhalb kürzester Zeit. Durch diese enorme Vereinfachung wird eine zusätzliche Sicherheit und Skalierung des Betriebs gewonnen. Ebenso wird die Transparenz deutlich erhöht und die schnelle Bereitstellung neuer Dienste gewährleistet. Durch die Automatisierung von täglichen Aufgaben wie Konfiguration, Bereitstellung und Troubleshooting reduziert SDA die Zeit für Netzwerkanpassungen, verbessert die Problemlösungszeit und reduziert die Auswirkungen von Sicherheitsverletzungen.

So können Organisationen sicherstellen, dass für jeden Benutzer oder jedes Gerät mit jeder Anwendung die richtigen Richtlinien festgelegt werden über das Netzwerk. Dies wird mit einer einzigen Netzwerkstruktur über LAN und WLAN erreicht, wodurch ein konsistente Benutzererfahrung überall ohne Kompromisse bei der Sicherheit.

SDA wird aus mehreren Komponenten zusammengesetzt. Dazu gehört das DNA-Center, welches die grundsätzliche Funktion des Netzwerks sicherstellt, sowie Identity Service Engine (ISE), welches die Benutzeridentitäten und Profile verwaltet. [5]

7.1.1 Campus Fabric

Um eine konsistente Benutzererfahrung zu erreichen, braucht man eine Switching-Infrastruktur mit der sich der Zugang zu bestimmten IP-Subnetzen ortsunabhängig realisieren lässt. [6]

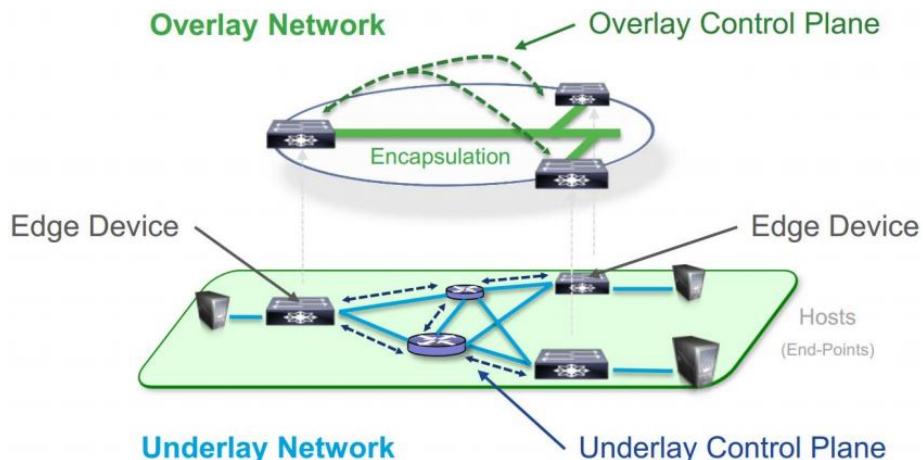


Abbildung 7.1: Die Aufteilung Campus Fabric in ein Underlay und Overlay Netzwerk

Die SDA Architektur wird durch die für den Campus implementierte Fabric Technologie unterstützt, welche die Verwendung virtueller Netzwerke (Overlay Network) in einem physischen Netzwerk (Underlay Network) ermöglicht, um alternative Topologien für die Verbindung von Geräten zu erstellen. Overlay Netzwerke werden in Data Center häufig verwendet, um die Mobilität von virtuellen Maschinen über Layer 2 und Layer 3 bereitzustellen (Beispiele: ACI, VXLAN und Fabric Path). Overlay-Netzwerke werden auch

in Wide-Area-Netzwerken verwendet, um sicheres Tunneling von Remote-Standorten aus zu ermöglichen (Beispiele: MPLS, DMVPN und GRE). [4]

Overlay Network Die Fabric bildet ein Overlay Netz. Das Overlay Netz bildet eine virtuelle Topologie um Geräte miteinander zu verbinden, welches auf einer beliebigen physischen Underlay Topologie aufgebaut ist. Das Overlay Netzwerk verwendet oft alternative Weiterleitungsattribute, um zusätzliche Dienste bereitzustellen, die nicht vom Underlay Netzwerk bereitgestellt werden. Die Datenebenenverkehrs- und Steuerungsebenen-Signalisierung ist in jedem virtualisierten Netzwerk enthalten, wobei zusätzlich zu der Isolation von dem Underlay Netzwerk eine Isolation zwischen den Netzwerken aufrechterhalten wird. Der SDA Fabric implementiert die Virtualisierung, indem er den Benutzerdatenverkehr über IP-Pakete einkapselt, die an den Grenzen des Fabrics bereitgestellt und abgeschlossen werden. Overlay Netzwerke können über alle oder eine Teilmenge der Underlay Netzwerkgeräte hinweg ausgeführt werden. Mehrere Overlay Netzwerke können aber auch über das gleiche Underlay Netzwerk laufen, um Multi-Tenancy durch Virtualisierung zu unterstützen. Die Netzwerkvirtualisierung, welche sich ausserhalb der Fabric erstreckt, wird mithilfe herkömmlicher Virtualisierungstechnologien wie VRF-Lite und MPLS VPN beibehalten. Die IPv4 Multicast wird gekapselt und an interessierte Fabric-Edge-Switches gesendet, welche den Multicast wiederrum entkapseln und an die Empfänger weiterleiten. Ist der Empfänger ein drahtloser Client, so wird der Multicast (genau wie ein Unicast) durch den Fabric-Edge in Richtung des AP mit dem Multicast-Empfänger gekapselt. Die Multicast-Quelle kann entweder innerhalb oder ausserhalb eines Overlay vorhanden sein. [4]

Underlay Network Das Underlay Netzwerk wird durch die physischen Switches und Router definiert, die Teil des SDA Netzwerks sind. Jegliche Geräte die dem Underlay Netzwerk angehören, müssen über ein Routing Protokoll eine IP Konnektivität herstellen. Obwohl auf dem Underlay beliebige Topologie- und Routing-Protokolle verwendet werden können, wird von Cisco die Implementierung einer gut überlegten Layer 3 Grundlage bis zur Campus Edge empfohlen, um die hohe Leistung, sowie Skalierbarkeit und Verfügbarkeit des Netzwerkes zu gewährleisten. Um dieses Ziel für Underlay Deployments zu erreichen, welche nicht manuell erstellt werden, werden bei der DNA Center LAN-Automatisierung neue Netzwerke mit einem IS-IS-Routing Access Design bereitgestellt. Obwohl es viele Alternativen gibt, bietet diese Auswahl betriebliche Vorteile wie zum Beispiel dem Nachbarschaftsaufbau ohne IP-Protokollabhängigkeiten, Peering-Fähigkeit unter Verwendung von Loopback-Adressen und agnostische Behandlung von IPv4-, IPv6- und Nicht-IP-Verkehr. [4]

Fabric Data Plane and Control Plane SDA konfiguriert das Overlay Netzwerk mit einer Fabric Datenebene mithilfe der VXLAN Technologie. VXLAN kapselt und durchtunnelt komplett Layer 2-Frames über das Underlay Netzwerk, wobei jedes Overlay-Netzwerk durch eine VXLAN-Netzwerk-ID (VNI) identifiziert wird. Der VXLAN-Header enthält auch die SGTs, die für die Mikrosegmentierung erforderlich sind.

Das Mapping und Auflösen von Endpunkten, die VXLAN-Tunnelendpunkten (VTEPs) zugeordnet sind, erfordert ein Steuerungsebenenprotokoll, und SD-Access verwendet das Locator / ID Separation Protocol (LISP) für diese Aufgabe. LISP bietet den Vorteil, dass das Routing nicht nur auf der IP-Adresse als Endpunkt kennung (EID) für ein Gerät basiert, sondern auch eine zusätzliche IP-Adresse als Routing Locator (RLOC)

zur Verfügung stellt, um den Netzwerkstandort dieses Geräts darzustellen. Die EID- und RLOC-Kombination bietet alle erforderlichen Informationen für die Weiterleitung von Datenverkehr, selbst wenn ein Endpunkt eine unveränderte IP-Adresse verwendet, wenn er an einem anderen Netzwerkstandort angezeigt wird. Gleichzeitig ermöglicht die Entkopplung der Endpunktidentität von ihrem Standort, dass Adressen in demselben IP-Teilnetzwerk hinter mehreren Layer-3-Gateways verfügbar sind, gegenüber der Eins-zu-eins-Kopplung von IP-Teilnetzwerk mit Netzwerk-Gateway in herkömmlichen Netzwerken. Beispiel für zwei Subnetze, die Teil des Overlay-Netzwerks sind. Die Subnetze erstrecken sich über physisch getrennte Layer 3-Geräte. Die RLOC-Schnittstelle ist die einzige routbare Adresse, die zum Herstellen der Verbindung zwischen Endpunkten desselben oder eines anderen Subnetzes erforderlich ist. Weitere detailliertere Informationen zu LISP und VXLAN folgen in den nächsten Kapiteln. [4]

In der nachfolgenden Abbildung ist der Aufbau eines Campus Fabric mit allen Komponenten etwas detaillierter aufgezeigt.

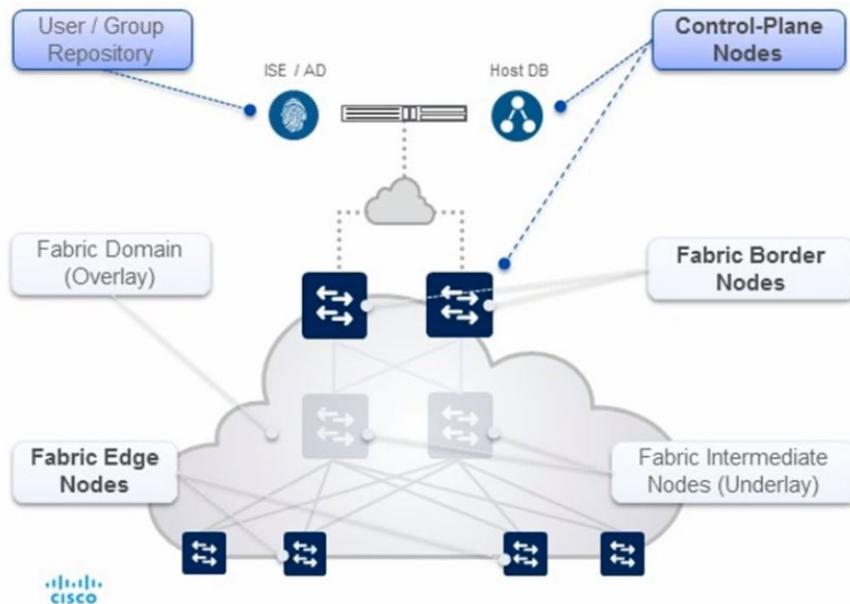


Abbildung 7.2: Fabric Rollen und Terminologie

Dieses Campus Fabric besteht aus folgenden Elementen:

- User/Group Repository: Ein externes ID-Speichergerät (z. B. ISE oder AD) kann verwendet werden, um eine dynamische Zuordnung von Benutzer/Gerät zu Gruppen bereitzustellen
- Control-Plane-Nodes: Ein Map System, das die Beziehung eines Endpoints zu einem Gateway (Edge oder Border) verwaltet
- Border-Nodes: Das L3-Gateway-Gerät (Core), das externe L3-Netzwerke mit dem Fabric verbindet
- Edge-Nodes: Das L3-Gateway-Gerät (Access oder Distribution), das Endpoints mit Fabric verbindet
- Intermediate Nodes: Normale L3 (IP) Forwarder im Underlay Netzwerk

Control-Plane Nodes Der SDA Fabric Control Plane basiert auf der LISP Map Server (MS) und LISP Map Resolver (MR), welche auf demselben Node kombiniert sind. Die

Funktion des Control Planes wird am Border Node oder Dedicated Node instanziert. Der Control Plane Node ermöglicht folgende Funktionen: [4]

- Host Tracking Database: Die Host Tracking Database (HTDB) ist ein zentrales Repository von EID zu Fabric Edge Nodes Verbindungen.
- Map Server: Der LISP-MS wird verwendet, um die HTDB mit Registrierungsnachrichten von Fabric-Edge-Geräten zu füllen.
- Map Resolver: Der LISP MR wird verwendet, um auf Map Abfragen von Fabric-Edge-Geräten zu reagieren, die RLOC-Mapping-Informationen für Ziel-EIDs anfordern.

Fabric Border Nodes Die Fabric Border Nodes dienen als Gateway zwischen der SDA Fabric Domäne und dem Netzwerk ausserhalb der Fabric. Der Fabric Border Node ist für die Netzwerkvirtualisierung und die SGT Propagierung vom Fabric zum Rest des Netzwerks verantwortlich. Die Fabric Border Nodes können entweder als Gateway für bestimmte Netzwerkadressen, z.B. ein Netzwerk für gemeinsam genutzte Dienste, oder in einer Standard-Border-Rolle, die für das Internet oder einen gemeinsamen Austrittspunkt aus einer Fabric nützlich ist. Border Nodes implementieren die folgenden Funktionen: [4]

- Advertisement von EID Subnetzen: SDA konfiguriert das Border Gateway Protocol (BGP) als bevorzugtes Routing-Protokoll zum Anbieten der EID-Präfixe ausserhalb der Fabric und der für EID-Subnetze von ausserhalb der Fabric bestimmte Verkehr durchläuft die Border Nodes. Diese EID-Präfixe werden nur in den Routingtabellen am Border angezeigt. Im gesamten Fabric werden die EID-Informationen über den Fabric Control Plane abgerufen.
- Fabric Domain Exit Point: Der Standard Fabric Border ist der Gateway für den letzten Exit Point für die Fabric Edge Nodes. Dies wird mithilfe der LISP Proxy Tunnel Funktionalität implementiert.
- Mapping von LISP Instanzen zu VRF: Der Fabric Border kann die Netzwerkvirtualisierung von innerhalb des Fabrics nach ausserhalb des Fabrics erweitern, indem externe VRF Instanzen verwendet werden, um die Virtualisierung beizubehalten.
- Policy Mapping: Der Fabric Border Node bildet auch SGT-Informationen aus dem Fabric ab, die beim Verlassen des Fabric entsprechend gepflegt werden. Tags aus dem VXLAN-Header werden Cisco Meta Data (CMD) zugeordnet, wenn Inline-Tagging-Funktionen verwendet werden, oder alternativ werden die Tags über das SGT-Austauschprotokoll (SXP) transportiert, sodass eine nahtlose Integration in die Cisco TrustSec-Lösung möglich ist.

Fabric Edge Nodes Die SDA Fabric Edge Nodes entsprechen einem Access-Layer Switch in einem herkömmlichen Campus-Design. die Edge Nodes implementieren ein Layer 3 Access Design mit den folgenden Fabric Funktionen: [4]

- Endpunktregistrierung: Nachdem ein Endpunkt von der Fabric Edge erkannt wurde, wird er einem lokalen Host-Tracking Datenbank (EID Tabelle) hinzugefügt. Das Edge Gerät gibt auch eine LISP Map Register Nachricht aus, um den Control Plane Node über den erkannten Endpunkt zu informieren, damit dieser die Informationen in die HTDB einfügen kann.
- Zuordnung von Benutzer zu virtuellem Netzwerk: Endpunkte werden in virtuellen Netzwerken platziert, indem der Endpunkt einem VLAN zugewiesen wird, das einer LISP-Instanz zugeordnet ist. Die Zuordnung von Endpunkten zu VLANs kann statisch oder dynamisch mit 802.1X erfolgen. Eine SGT wird ebenfalls zugewiesen,

und eine SGT kann verwendet werden, um Segmentierung und Richtliniendurchsetzung an der Fabric Edge bereitzustellen.

- Anycast Layer 3 Gateway: Ein gemeinsamer Gateway (IP- und MAC-Adressen) kann an jedem Knoten verwendet werden, der sich ein gemeinsames EID-Subnetz teilt, um eine optimale Weiterleitung und Mobilität zwischen verschiedenen RLOCs zu gewährleisten.
- LISP Forwarding und VXLAN Encapsulation/De-Encapsulation: Anstelle einer typischen routingbasierten Entscheidung fragen die Fabric Edge Nodes den Map Server an, um den der Ziel-IP zugeordneten RLOC zu ermitteln und den Verkehr mit VXLAN-Headern zu kapseln. Schlägt die Abfrage fehl, so wird der Traffic an einen Default Fabric Border gesendet, auf dem die globale Routing-Tabelle für das Weiterleiten verwendet wird. Die von Map Server empfangene Antwort wird im LISP Map Cache gespeichert.

Fabric Intermediate Nodes (Underlay) Die Fabric Intermediate Nodes sind Teil des Layer 3 Netzwerk, das für Verbindungen zwischen den Edge Nodes zu den Border Nodes verwendet wird. Im Falle das ein 3 Tier Campus Design mit einem Core, Distribution und Access Layer verwendet wird, sind die Intermediate Nodes äquivalent zu Distribution Switches. Intermediate Nodes routen nur den IP-Verkehr innerhalb der Fabric. [4]

7.1.2 Architektur

Cisco SDA kann grob in fünf Layer aufgeteilt werden.

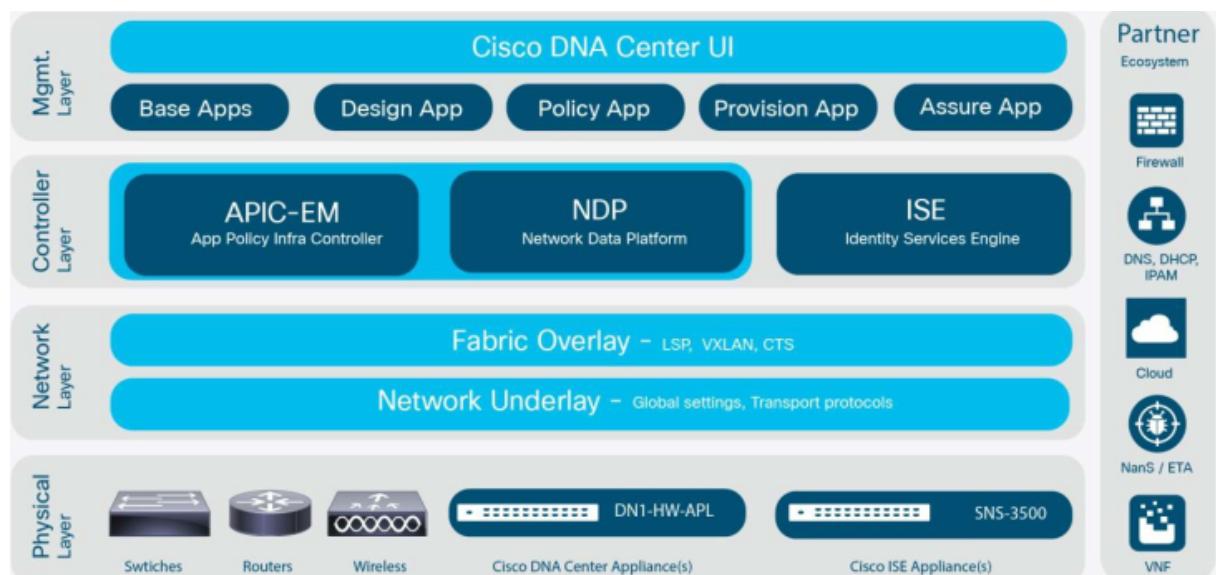


Abbildung 7.3: SDA Architektur

7.2 Cisco Digital Network Architecture Center (Cisco DNA-Center)

Im Zentrum der Automatisierung der SDA Lösung steht das Cisco DNA Center. DNA Center ist ein Controller für die Planung und Vorbereitung, Installation und Integration. SDA ist eines der vielen Softwarepakete, die auf dem DNA Center laufen und ist die

Grundlage des Cisco DNA. Es ermöglicht den Netzwerkzugriff in Minuten für jeden Benutzer oder jedes Gerät für jede Anwendung, ohne Kompromisse. Bei SDA folgen die festgelegten Richtlinien automatisch dem Benutzer über alle Netzwerkdomänen hinweg. DNA Center ist das zentrale Überwachungs-Dashboard für Netzwerke, mit dem alle Cisco DNA-Produkte und -Lösungen verwaltet werden können.

DNA Center gibt die Möglichkeit unter einem Grafischen Nutzer Interface direkt mit APIC(Application Policy Infrastructure Controller)-EM 2.x Applikationen mit der Identity Services Engine (ISE) und mit Network Data Plattform (NDP) unserer Assurance und Analytics Plattform zu sprechen. Alle Parameter die angezeigt oder konfiguriert werden müssen, kann man unter DNA Center ausführen und muss nicht zwischen den einzelnen Modulen und Oberflächen hin und her springen.

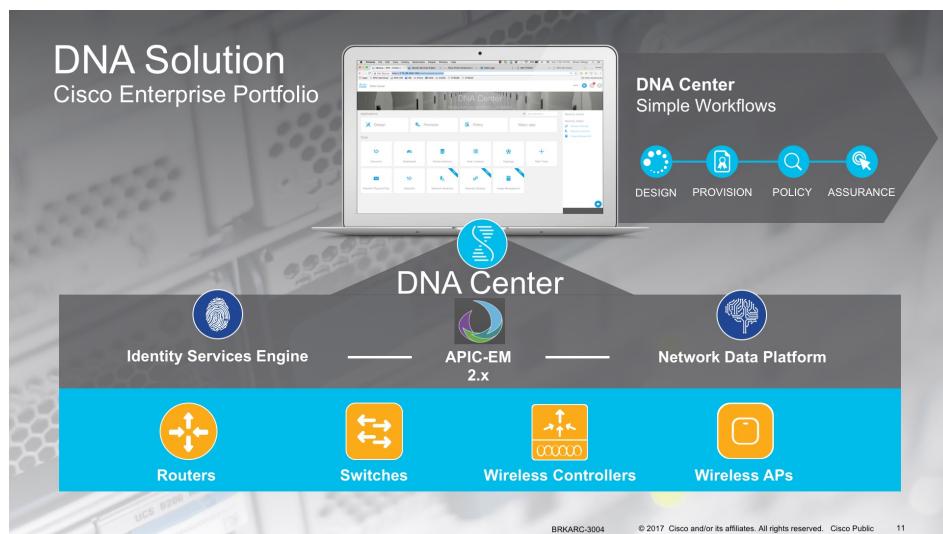


Abbildung 7.4: DNA Solution

APIC-EM 2.x automatisiert dann die notwendigen Konfigurationen und spricht mit dem Netzwerk. Auch die Integration von IP Address Management Lösungen wie z.B. Infoblox werden nur über die DNA Center Oberfläche konfiguriert. Dies geschieht über verschiedene API-basierte Datenaustauschmechanismen sowie einen automatisierten Zertifikataustausch für Partnersysteme (zum Beispiel Cisco ISE). [3]

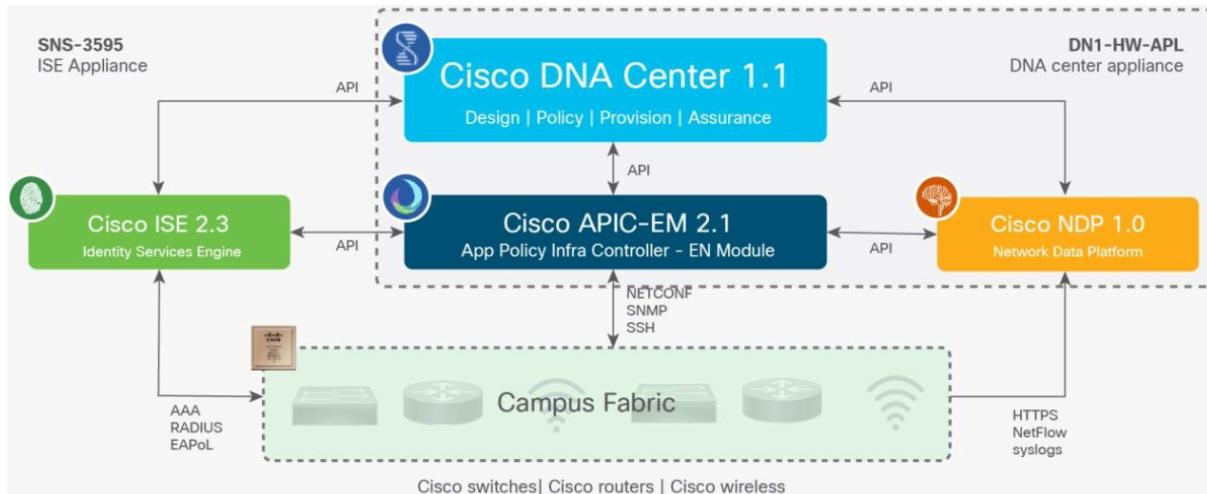


Abbildung 7.5: SDA Architektur

Das DNA Center verwaltet zentral folgende vier Hauptbereiche: [4]

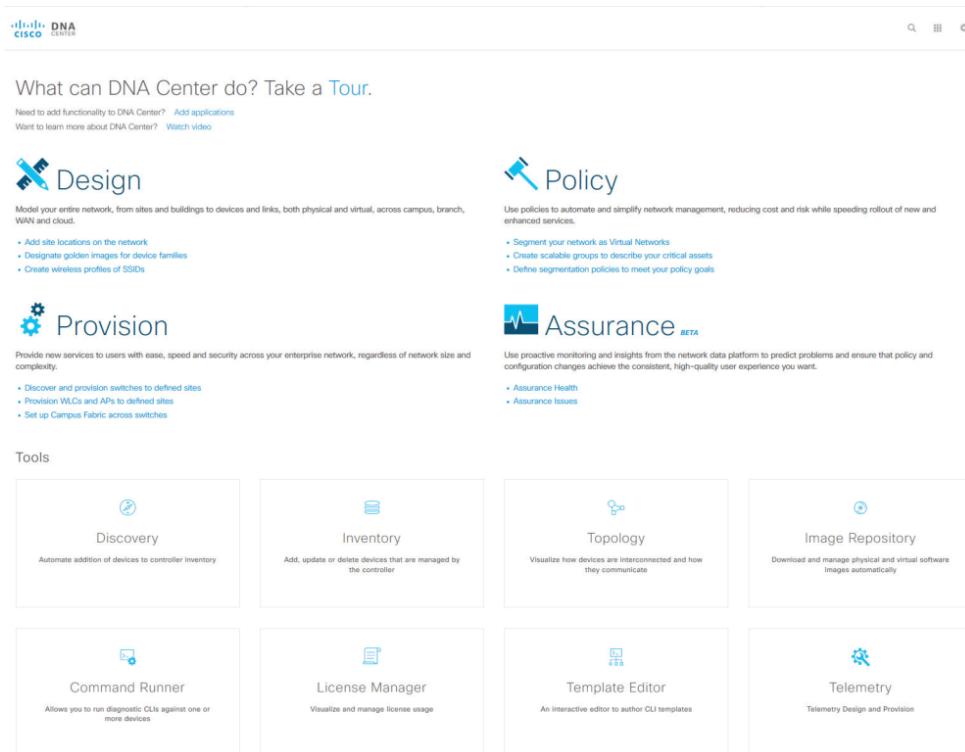


Abbildung 7.6: DNA Dashboard

Design Konfiguriert globale Geräteeinstellungen, Netzwerkstandortprofile für die physische Gerätelinventur, DNS, DHCP, IP-Adressierung, Software-Image-Verwaltung, Plug-and-Play und Benutzerzugriff.

Policy Definiert die Geschäftsabsicht für die Bereitstellung im Netzwerk, einschließlich der Erstellung virtueller Netzwerke, der Zuweisung von Endpunkten zu virtuellen Netzwerken und der Definition von Richtlinienverträgen für Gruppen.

Provision Stellt Geräte für das Management bereit und erstellt Fabric-Domänen, Control Plane Nodes, Border Nodes, Edge Nodes, Fabric-Wireless und externe Konnektivität.

Assurance Aktiviert das Health-Score-Dashboard, Client/Gerät-360 Grad-Ansichten, Knoten-, Client- und Pfad-Traces. DNA Center unterstützt die Integration mithilfe von APIs. Zum Beispiel ist die Integration von IP-Adressen von Infoblox und die Integration von Policy Enforcement mit ISE über DNA Center verfügbar. Ein umfassendes Set von Northbound-REST-APIs ermöglicht Automatisierung, Integration und Innovation.

7.3 Identity Service Engine (ISE)

Cisco ISE ist ein wesentlicher Bestandteil von SDA für die Richtlinienimplementierung. Mit der Cisco ISE können Benutzer und Geräte, die mit dem Unternehmensnetzwerk verbunden sind, angezeigt und gesteuert werden. Das alles von einer zentralen Stelle aus. ISE ermöglicht es einem Netzwerkadministrator, Zugriffsrichtlinien für kabelgebundene und drahtlose Endpunkte basierend auf Informationen zentral zu steuern, die über RADIUS-Nachrichten gesammelt werden, die zwischen dem Gerät und dem ISE-Knoten übertragen werden. Dies wird auch als Profiling bezeichnet. Die Profiling-Datenbank wird regelmäßig aktualisiert, um mit den neuesten und besten Geräten Schritt zu halten, so dass keine Lücken in der Gerätesichtbarkeit bestehen.

Im Wesentlichen hängt ISE eine Identität an ein Gerät an, basierend auf Benutzer-, Funktions- oder anderen Attributen, um Richtliniendurchsetzung und Sicherheitskonformität bereitzustellen, bevor das Gerät autorisiert wird, auf das Netzwerk zuzugreifen. Basierend auf den Ergebnissen einer Vielzahl von Variablen kann ein Endpunkt mit bestimmten Zugriffsregeln auf das Netzwerk zugelassen werden, die auf die Schnittstelle angewendet werden, mit der er verbunden ist. Andernfalls kann er vollständig verweigert oder basierend auf den spezifischen Unternehmensrichtlinien gewährt werden.

DNA Center bietet einen Mechanismus zum Erstellen einer vertrauenswürdigen Kommunikationsverbindung mit Cisco ISE und ermöglicht den beiden Anwendungen, Daten auf sichere Weise miteinander zu teilen. ISE integriert sich in DNA Center mit Hilfe von Cisco Platform Exchange Grid (pxGrid) und REST APIs zum Austausch von Client-Informationen und zur Automatisierung von Fabric-bezogenen Konfigurationen auf ISE. Sobald die ISE beim DNA Center registriert ist, wird jedes Gerät, das ISE entdeckt, zusammen mit der entsprechenden Konfiguration und anderen Daten an das DNA Center weitergeleitet. Benutzer können beide Anwendungen verwenden, um Geräte zu erkennen und dann sowohl DNA Center- als auch ISE-Funktionen auf sie anzuwenden, da diese Geräte in beiden Anwendungen verfügbar sind. DNA Center- und ISE-Geräte werden alle durch ihre Gerätenamen eindeutig identifiziert.

In ähnlicher Weise werden DNA-Center-Geräte sobald sie bereitgestellt werden und zu einer bestimmten Seite in der DNA Center-Standorthierarchie gehören, an ISE übergeben. Alle Aktualisierungen an einem DNA Center-Gerät (z. B. Änderungen an der IP-Adresse, SNMP- oder CLI-Anmeldeinformationen, gemeinsamer ISE-Schlüssel usw.) werden automatisch an die entsprechende Geräteinstanz auf der ISE weitergeleitet. Wenn ein DNA Center-Gerät gelöscht wird, wird es ebenfalls aus der ISE entfernt.

7.4 Locator ID Separation Protocol (LISP)

LISP ist das Produkt einer Arbeitsgruppe in der Internet Engineering Taskforce (IETF), um das wachsende Problem des doppelten Verwendungszwecks der IP-Adressen zu beseitigen. Zur Zeit wird die IP-Adresse benutzt um die Identität eines Hosts festzulegen und auch den Ort zu bestimmen, an dem er sich im Internet befindet. Dies hat zur Folge, dass sich bei einem Aufenthaltsortwechsel auch die IP-Adresse des Hosts ändert, was bedeutet, dass die Identität verloren geht und die alten IP-Verbindungen verfallen.

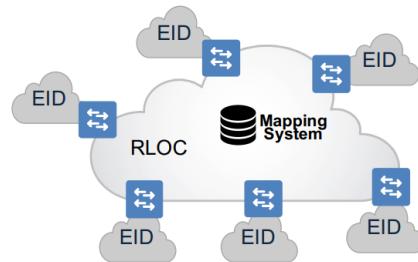


Abbildung 7.7: LISP Aufbau

Dies soll nun durch LISP geändert werden, indem es die Identität eines Gerätes, auch Endpoint Identifier (EID) genannt, von seinem Aufenthaltsort, auch Routing Locator (RLOC) genannt, in zwei separate Adressräume unterteilt. Das bedeutet, dass die Router in einer LISP-Architektur nur Routing-Informationen von RLOCs speichern müssen. Um Pfadinformationen eines Hosts abzurufen, kann der Router diese beim LISP-Mapping-Server abfragen, was analog wie das DNS-Mapping funktioniert.

LISP verwendet für SDA/Fabric eine VXLAN-Kapselung. Um die VXLAN-Kapselung für LISP zu aktivieren, muss auf dem Router der LISP Konfigurationsmodus, den Befehl für die VXLAN-Enkapsulierung verwendet werden. Dieser Befehl muss auf allen LISP-Edge-Geräten im Enterprise-Fabric konfiguriert werden: Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Proxy Ingress Tunnel Router (PITR), Proxy Egress Tunnel Router (PETR). Wenn dieser Befehl nicht auf einem der LISP-Edge-Geräte konfiguriert wird, führt dies zu einem Verlust der Kontrolle und des Datenverkehrs. [2]

LISP Device	Function
ALT (Alternative Logical Topology)	Collects EID data from Map Servers (MS) and advertise aggregate EID prefix. In a deployment of multiple Map Servers, it keeps all synchronized.
ETR (Egress Tunnel Router) and PETR (Proxy ETR)	Connects a LISP capable core network. Registers EID prefixes with Map Server (MS). Decapsulates LISP packets, received from LISP core. Responds to Map-request messages with a Map-Reply by giving appropriate EID prefix. Typically, this is a CPE (customer premise equipment) router. PETR works on behalf on non-LISP domain and provides LISP-non-LISP connectivity.
ITR (Ingress Tunnel Router) and PITR (Proxy Ingress Tunnel Router)	Responsible for forwarding local traffic to external destinations. Resolves RLOC for a given destination by sending Map-request to Map Resolver. Encapsulates (vxlan) traffic with LISP header. Typically, this is a Access Layer Switch. PITR works on behalf on non-LISP domain and provides LISP-non-LISP connectivity.
XTR (X Tunnel Router)	When both ITR and ETR functions are handled by one router, it is called XTR. This is typical in practice.
MR (Map Resolver)	Responds to Map-requests from ITR. Map-requests will be replied with a Negative Map-Reply or forwarded to appropriate ETR or ALT.
MS (Map Server)	Registers EID space upon receiving Map-register messages from ETR. Updates ALT and MR with EID and RLOC data.
MSMR (Map Server Map Reloader)	When a device acts as both Map Server and Map Resolver, it is called MSMR. This is typical in practice.
EID (Endpoint ID)	Endpoint Identifier. IP addresses hidden from core network routing table. RLOC acts next-hop to reach EID space.
RLOC (Routing Locator)	Routing Locator. Exists in global routing tables. Authoritative to reach EID space.

Tabelle 7.1: LISP Elements

7.4.1 Campus Fabric und LISP

Im Einzug mit dem Campus Fabric wurden für bestehende LISP Namenskonzepte neue Begriffsdefinitionen zugewiesen:

- ”Control-Plane Node” ≈ ”LISP Map-Server”
- ”Edge Node” ≈ ”LISP Tunner Router” (xTR)
- ”Border Node” ≈ ”LISP Proxy Tunnel Router” (PxTR)
- ”Intermediate Node” ≈ ”Non-LISP IP Forwarder”

Fabric Control-Plane Node basiert auf einem LISP Map Server / Resolver. Führt die LISP-Host-Tracking-Datenbank aus, um Overlay-Erreichbarkeitsinformationen bereitzustellen.

- Eine einfache Host-Datenbank, die die Endpunkt-ID zu Edge-Knoten-Bindungen zusammen mit anderen Attributen verfolgt
- Host-Datenbank unterstützt mehrere Endpoint-ID-Lookup-Schlüssel (IPv4 / 32, IPv6 / 128 oder MAC)
- Empfängt Präfix-Registrierungen von Edge Nodes mit lokalen Endpunkten
- Beheben von Suchanforderungen von Remote-Edge-Knoten, um lokale Endpunkte zu finden

Fabric Edge Node basiert auf einem LISP Tunnel Router (xTR). Bietet Konnektivität für Benutzer und Geräte, die mit dem Fabric verbunden sind.

- Verantwortlich für das Identifizieren und Authentifizieren von Endpunkten
- Registrieren von Endpunkt-ID mit dem Control-Plane Node(s)
- Bietet Anycast L3 Gateway für verbundene Endpunkte
- Host-Datenverkehr von und zu Endpunkten, die mit dem Fabric verbunden sind, verkapseln/entkapseln

Fabric Border Node basiert auf einem LISP Proxy Tunnel Router (PxTR). Der gesamte Verkehr, der das Fabric betritt oder verlässt, durchläuft diesen Knotentyp.

- Verbindet traditionelle L3-Netzwerke und / oder verschiedene Fabric-Domänen mit der lokalen Domäne
- Wo zwei Domains Endpoint Erreichbarkeit und Richtlinieninformationen austauschen
- Verantwortlich für die Übersetzung von Kontexten (VRF und SGT) von einer Domäne in eine andere
- Stellt einen Domänenexitpunkt für alle Edge-Knoten bereit

7.5 Virtual Extensible LAN (VXLAN)

VXLAN ist ein Encapsulation-Protokoll, um ein Overlay-Netzwerk auf einer existierenden Layer 3 Infrastruktur laufen zu lassen. VXLAN wurde ursprünglich von Cisco Systems, VMware und Arista Network entwickelt und ist einer der IETF festgelegten Standards (RFC 7348). [1]

Technisch gesehen erzeugt ein VXLAN logische Layer 2 Netzwerke, die dann in standardmässige Layer 3 Pakete eingepackt werden. VXLAN dient dazu um in sehr grossen Netzwerkumgebung die Probleme zu lösen, die durch beschränkte Anzahl von VLANs

betroffen sind. Mit VXLAN sind insgesamt 16'777'215 (24 Bit) Layer-2-Umgebungen möglich, die ihrerseits wieder jeweils 4096 VLANs beinhalten können.

7.5.1 VXLAN Encapsulation

Die Data Plane basiert auf VXLAN, im Gegensatz zur Control Plane, welche auf LISP basiert. Die VXLAN-Kapselung ist IP/UDP-basiert, was bedeutet, dass sie von jedem IP-basierten Netzwerk (Legacy- oder nicht-Cisco-Netzwerk) weitergeleitet werden kann und effektiv den Overlay-Aspekt des SD-Access-Fabric erzeugt. Die VXLAN-Kapselung wird (statt der LISP-Kapselung) aus zwei Hauptgründen verwendet. VXLAN umfasst den Source Layer 2 (Ethernet) -Header (LISP nicht) und bietet auch spezielle Felder für zusätzliche Informationen, wie die ID des virtuellen Netzwerks (VN) und die ID der Gruppe (Segment). [3]

Diese Technologie bietet mehrere Vorteile für SD-Access, z. B. Unterstützung für virtuelle Layer-2 und Layer-3-Topologien (Overlays) und die Möglichkeit, über jedes IP-basierte Netzwerk mit integrierter Netzwerksegmentierung (VRF/VN) und gruppenbasierter Richtlinie zu arbeiten.

In SD-Access wurden einige Verbesserungen der ursprünglichen VXLAN-Spezifikationen hinzugefügt, insbesondere die Verwendung von Sicherheitsgruppen-Tags (SGTs). Dieses neue VXLAN-Format ist derzeit ein IETF-Entwurf, der als Gruppenrichtlinienoption (oder VXLAN-GPO) bekannt ist.



Abbildung 7.8: VXLAN Encapsulation

Die Fabric Data-Plane bietet folgendes:

- Underlay Adressanzeige und -zuordnung
- Automatischer Tunnelaufbau (Virtuelle Tunnelendpunkte)
- Frame-Kapselung zwischen Routing-Locators

Unterstützung für das LISP- oder VXLAN-Header-Format

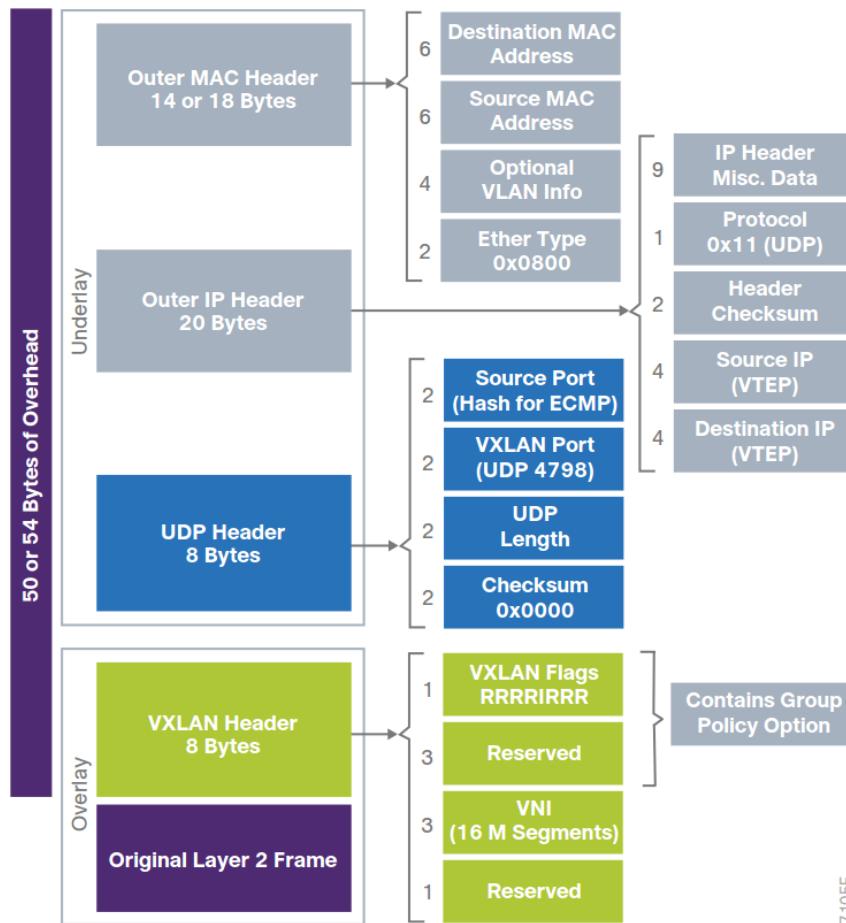
- Fast gleich, mit verschiedenen Feldern und Nutzlast
- LISP-Header trägt IP-Payload (IP in IP)
- VXLAN-Header trägt MAC-Payload (MAC in IP)

Ausgelöst durch LISP-Control-Plane-Ereignisse

- ARP oder NDP Learning auf L3 Gateways
- Map-Reply oder Cache auf Routing Locators

7.5.2 Fabric Data Plane

RFC 7348 definiert die Verwendung von Virtual Extensible LAN (VXLAN) als eine Möglichkeit, ein Layer 2-Netzwerk über einem Layer 3-Netzwerk zu überlagern. Mit VXLAN tunneln Sie den ursprünglichen Layer 2-Frame mit UDP/IP über das Layer 3-Netzwerk. Die Tunnelschnittstelle an jedem Knoten wird VXLAN-Tunnelendpunkt (VTEP) genannt. VTEPs beruhen auf dem Lernen der Data Plane oder Control Plane, um den entfernten Endpunkt für das VTEP-Mapping für die Verkapselung des Datenverkehrs zu bestimmen. Jedes Overlay-Netzwerk wird als VXLAN-Segment bezeichnet und mithilfe einer 24-Bit-VXLAN-Netzwerk-ID identifiziert, die bis zu 16 Millionen VXLAN-Segmente unterstützt.



7105F

Abbildung 7.9: RFC7348 VXLAN Header

Das SDA Fabric verwendet die VXLAN Data Plane, um das vollständige ursprünglichen Layer-2-Frame bereitzustellen und verwendet zusätzlich LISP als Control Plane, um die Endpunkt zu VTEP Zuordnungen aufzulösen. Das SDA Fabric ersetzt 16 der reservierten Bits im VXLAN-Header, um bis zu 64'000 SGTs zu transportieren. Dabei wird ein modifiziertes VXLAN-GPO-Format verwendet.

Der VNI wird einer virtuellen Routing- und Weiterleitungsinstanz für Layer-3-Overlays zugeordnet, während ein Layer-2-VNI einer VLAN-Broadcastdomäne zugeordnet wird. Beide bieten den Mechanismus zur Isolierung von Daten und Steuerungsebene für jedes einzelne virtuelle Netzwerk. Die SGT trägt Gruppenmitgliedschaftsinformationen von Benutzern und stellt eine Datenebenensegmentierung innerhalb des virtualisierten Net-

zwerks bereit. [4]

7.6 Slack

Slack ist ein webbasiertes Instant-Messaging-Dienst des US-amerikanischen Unternehmens Slack Technologies zur Kommunikation innerhalb von Arbeitsgruppen. Slack erlaubt, Nachrichten auszutauschen, mit Einzelpersonen oder in einer Gruppe zu chatten sowie gemeinsam Dokumente zu bearbeiten. Andere Online-Dienste wie Dropbox, Google Drive oder GitHub lassen sich in Slack integrieren.

7.7 Infoblox

Infoblox ist einer der führenden Hersteller für DNS-, DHCP-, TFTP und IP-Adress-Management Appliance (IPAM). Die Integration von Infoblox ermöglicht dem DNA Center die IPAM-Funktionen von Infoblox zu nutzen. Dafür werden beispielsweise die IP-Addresspools zwischen dem DNA Center und Infoblox synchronisiert. Mit dieser Integration können IP-Adresszuweisungen automatisiert werden, was einerichtlinienbasierte Bereitstellung in einer einzigen Operation ermöglicht und so die betriebliche Effizienz verbessert.

Infoblox ermöglicht die automatische Überprüfung der Netzwerkinfrastrukturen, die Konfiguration sowie Anpassung an die jeweiligen Compliance-Vorgaben. Mittels DNS-, DHCP-, TFTP und IP-Adress-Management Appliance (IPAM) werden wichtige Kontrollfunktionen für Endgeräte und Anwendungen bereitgestellt. Dank der DNS-Management-Software-Appliance kann stets der Überblick über Ihre IP-Adressbereiche behalten und die Verteilung der DNS- und DHCP-Daten überprüft und automatisiert werden. Reportings älterer sowie aktueller Daten können dank einer zuverlässigen Netzwerkdatenbank sowie Grid-Technologie erstellt werden.[15]

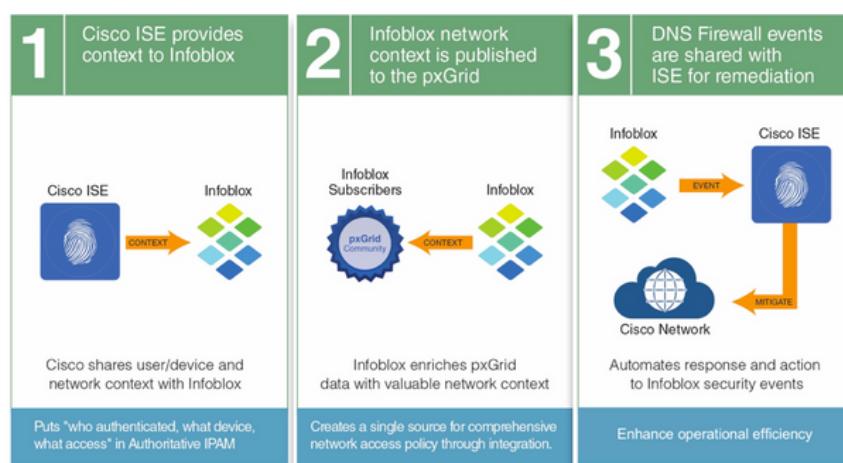


Abbildung 7.10: Zusammenspiel Infoblox und ISE

Die gemeinsame Lösung von Infoblox ActiveTrust und Cisco Identity Services Engine (ISE) verbessert die Genauigkeit und Aktualität von Sicherheitsmaßnahmen, erhöht die Sichtbarkeit und erleichtert den Austausch von Informationen zwischen Netzwerk- und Sicherheitsteams. Cisco teilt den Gerätekontext mit Infoblox, während der Infoblox-

Netzwerkkontext in pxGrid veröffentlicht wird, sodass Netzwerkadministratoren die Reaktionszeit für die Sicherheit automatisieren und verkürzen können. [16]

7.8 SDA Mechanismus Beispiel

Ausgangslage:

Wenn ein IP Paket über SD-A von PC1 172.16.1.1/24 nach PC2 10.0.2.34/24 geschickt wird, was passiert mit dem Paket?

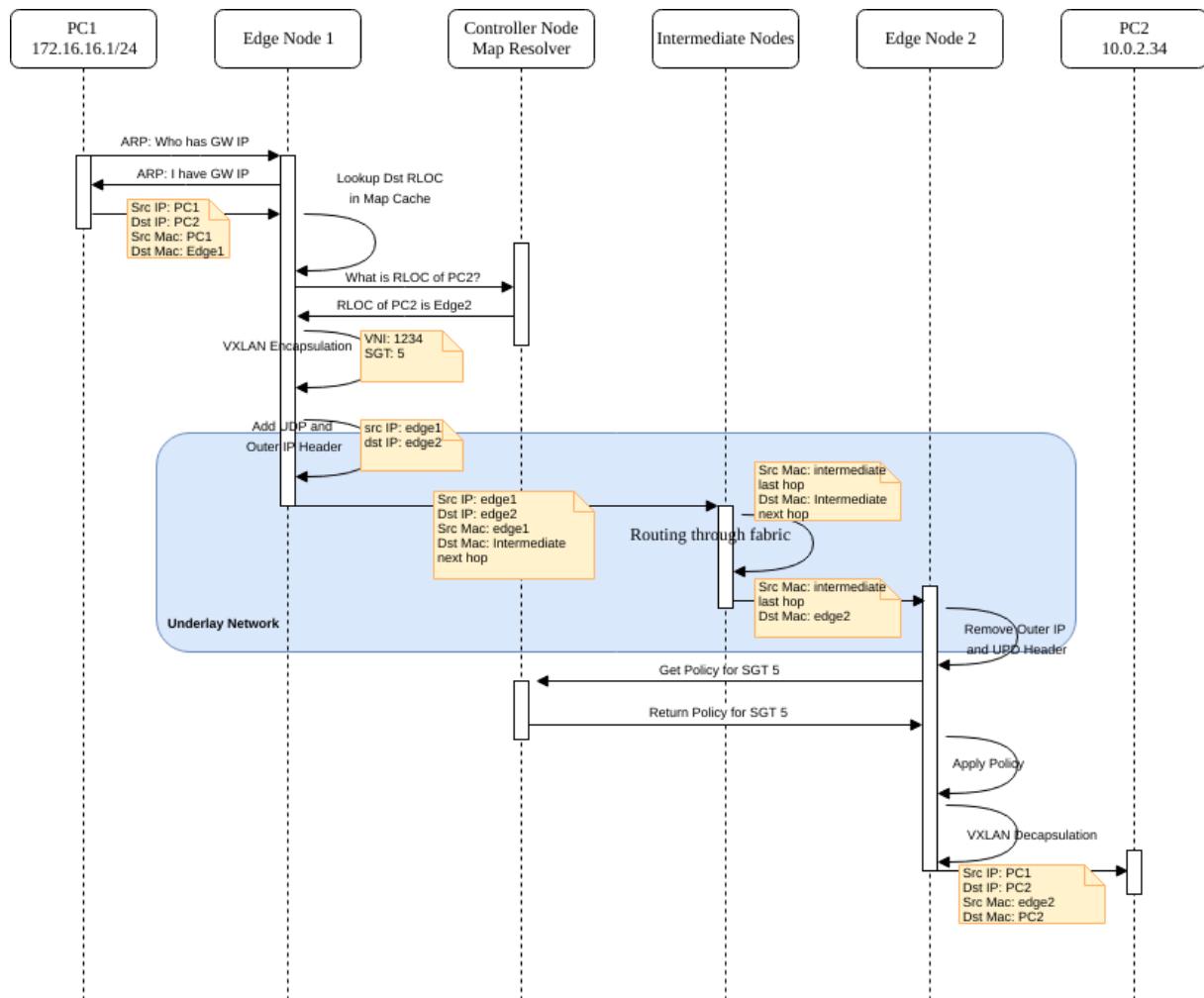


Abbildung 7.11: DNA Solution

- ARP Lookup für Default GW
- Antwort von Edge Node 1 (GW ist anycast Adresse und wird von jedem Edge Node beantwortet)
- Paket an GW
- RLOC Lookup im lokalen Map Cache
- Falls kein Eintrag im Lokalen Cache:
 - RLOC Lookup an Map Resolver senden
 - Map Resolver antwortet mit RLOC falls vorhanden
 - * Falls RLOC nicht bekannt, wird Border Node verwendet
- VXLAN Encapsulation (SGT 5, VNI1234)
- UDP und Outer IP Header hinzufügen (Underlay Network)

- Senden an RLOC IP (Destination Edge Node)
- Paket durch Intermediate Nodes routen
- Edge Node 2 erhält Paket
- Outer IP und UDP Header entfernen (Underlay Network)
- Policy für SGT 5 beim Map Resolver anfragen
- Policy auf Paket anwenden:
 - Je nach Policy ok oder Paket droppen
- VXLAN Decapsulation
- Paket an PC2 weiterleiten

8 Use Cases

8.1 Use Cases Brief

8.1.1 UC01: Definierung von Benutzer und Geräteprofilen

Ein Administrator definiert die Profile für Benutzer, Gruppen oder Geräte, sodass diese auf alle nötigen Ressourcen zugreifen können, unberechtigter Zugriff aber verhindert wird.

8.1.2 UC02: Gastzugang

Ein Guest (unbekannter User mit unbekanntem Gerät) steckt sich im Netzwerk an. Er erhält Zugriff auf alle definierten Ressourcen. Im einfachsten Fall einfach Internetzugriff.

8.1.3 UC03: Backup and Restore DNA Center

Auf Grund eines Problems des DNA-Centers muss die Appliance ausgetauscht oder auf einen vorherigen Konfigurationsstand zurückgesetzt werden. Um eine Neukonfiguration des Systems zu verhindern, wird eine zuvor gesicherte Konfiguration wiederhergestellt.

8.1.4 UC04: Reporting

Es werden regelmässig Reports über relevante Netzwerkaktivitäten erstellt und den zuständigen Personen via Mail und/oder Slack zugestellt.

8.1.5 UC05: Hardware Ersatz

Ein Switch muss auf Grund eines Hardwaredefekts oder ähnlichen Gründen ausgetauscht werden.

8.1.6 UC06: Benutzermobilität

Ein User ändert seinen Arbeitsplatz, das Gebäude oder den Arbeitsort. Er muss an allen Standorten dieselben Policies erhalten und auf dieselben Ressourcen zugreifen können.

8.1.7 UC07: Degradation

Bearbeitung von möglichen Degradations-Szenarios mit den entsprechenden Degradationstests.

8.1.8 UC08: Integration von nicht Fabric Komponenten

Netzintegration von „nicht Campus-Fabric Netzkomponenten“ (zum Beispiel traditionelle Access und Distribution Switches).

8.1.9 UC09: Migration von bestehenden klassischen Campus

Migrationskonzept bestehende CampusLAN Lösung zu einem Campus-Fabric Lösung mit DNA-Center

8.1.10 UC10: Einsatz von SGT

Einsatz von SGT zusammen mit VXLAN (Netzdesign, Design-Rules, Transport innerhalb und aussehlab des Fabrics, Schnittstelle L2/L3 und Überführung des IP-Konnektivität an einem IP-Backbone zB MPLS VPN).

8.1.11 UC11: Infoblox

Integration Infoblox DDI (DNS, DHCP and IP address management) mit dem DNA-Center für die Provisionierung von IP-Adresse für das Management von neuen Netzkponenten in die Fabric (zB Access-Switches, usw).

8.2 Use Cases Fully dressed

8.2.1 UC01: Definierung von Benutzer und Geräteprofilen

Primary Actor	Administrator
Beschreibung	Ein Administrator definiert die Profile für Benutzer, Gruppen oder Geräte, sodass diese auf alle nötigen Ressourcen zugreifen können, unberechtigter Zugriff aber verhindert wird.
Stakeholders	<ul style="list-style-type: none"> • Administrator • User
Preconditions	<ul style="list-style-type: none"> • DNA Center komplett konfiguriert • ISE konfiguriert und mit DNA Center verbunden
Postconditions	<ul style="list-style-type: none"> • User kann auf all nötigen Ressourcen zugreifen • Zugriffe auf nicht berechtigte Ressourcen werden blockiert
Main Success Story	<ol style="list-style-type: none"> 1. Profil wird definiert 2. Profil wird Usern oder Geräten zugewiesen 3. Entsprechende Geräte und Benutzer haben Zugriff auf benötigte Ressourcen (und keine zusätzlichen)
Alternative Flows	<ol style="list-style-type: none"> 1a. Definitionen fehlen <ol style="list-style-type: none"> 1. Netzwerksegmente oder Ressourcen definieren 2. Profil definieren 2a. User oder Geräte fehlen <ol style="list-style-type: none"> 1. User oder Geräte erfassen 2. Profil wird Usern oder Geräten zugewiesen

Tabelle 8.1: UC01 Fully Dressed

8.2.2 UC02: Gastzugang

Primary Actor	Guest
Beschreibung	Ein Guest (unbekannter User mit unbekanntem Gerät) steckt sich im Netzwerk an. Er erhält Zugriff auf alle definierten Ressourcen. Im einfachsten Fall einfach Internetzugriff.
Stakeholders	-
Preconditions	<ul style="list-style-type: none"> • Profil für Gastzugriff definiert • Guest ist mit dem Netzwerk verbunden
Postconditions	<ul style="list-style-type: none"> • Guest hat Zugriff auf definierte Ressourcen • Guest hat keinen Zugriff auf interne Ressourcen
Main Success Story	<ol style="list-style-type: none"> 1. Guest verbindet sich mit dem Netzwerk 2. Guest erhält Zugriff auf definierte Ressourcen 3. Guest verlässt das Netzwerk
Alternative Flows	-

Tabelle 8.2: UC02 Fully Dressed

8.2.3 UC03: Backup and Restore DNA Center

Primary Actor	Netzwerkadministrator
Beschreibung	Auf Grund eines Problems des DNA-Centers muss die Appliance ausgetauscht oder auf einen vorherigen Konfigurationsstand zurückgesetzt werden. Um eine Neukonfiguration des Systems zu verhindern, wird eine zuvor gesicherte Konfiguration wiederhergestellt.
Stakeholders	Alle Netzwerkbenutzer
Preconditions	<ul style="list-style-type: none"> • Ein Backup der DNA Center Konfiguration existiert
Postconditions	<ul style="list-style-type: none"> • Appliance läuft mit einer zuvor gesicherten Konfiguration
Main Success Story	<ol style="list-style-type: none"> 1. Passendes Backup wählen 2. Appliance auf den Stand des Backups zurücksetzen
Alternative Flows	-

Tabelle 8.3: UC03 Fully Dressed

8.2.4 UC04: Reporting

Primary Actor	Netzwerkadministrator
Beschreibung	Es werden regelmässig Reports über relevante Netzwerkaktivitäten erstellt und den zuständigen Personen via Mail und/oder Slack zugestellt
Stakeholders	<ul style="list-style-type: none"> • Netzwerkadministratoren • Management
Preconditions	<ul style="list-style-type: none"> • Alle nötigen Daten zur Erstellung der Reports stehen im DNA Center zur Verfügung.
Postconditions	<ul style="list-style-type: none"> • Definierte Benutzer erhalten regelmässige Reports
Main Success Story	<ol style="list-style-type: none"> 1. Relevante Informationen aus dem DNA Center werden erfasst 2. Informationen werden aufbereitet, Report wird generiert 3. Report wird per Mail an alle definierten Personen
Alternative Flows	<p>3a. Alternativer Messenger</p> <ol style="list-style-type: none"> 1. Report wird via Slack an alle definierten Personen gesendet

Tabelle 8.4: UC04 Fully Dressed

8.2.5 UC05: Hardware Ersatz

Primary Actor	Netzwerkadministrator
Beschreibung	Ein Switch muss auf Grund eines Hardwaredefekts oder ähnlichen Gründen ausgetauscht werden.
Stakeholders	<ul style="list-style-type: none"> • Netzwerkadministratoren • User am betroffenen Switch
Preconditions	<ul style="list-style-type: none"> • Ersatzhardware verfügbar
Postconditions	<ul style="list-style-type: none"> • Ersatzhardware hat die Funktionalität des auszutauschenden Geräts vollständig übernommen
Main Success Story	<ol style="list-style-type: none"> 1. Auszutauschendes Gerät wird entfernt 2. Neues Gerät wird installiert 3. Neues Gerät wird verkabelt 4. Neues Gerät wird im DNA Center erfasst 5. DNA Center installiert Konfiguration des alten Geräts auf das neue 6. Neues Gerät übernimmt Funktion des alten Geräts 7. Altes Gerät im DNA Center entfernen
Alternative Flows	<p>4a. Andere Hardware</p> <ol style="list-style-type: none"> 1. Ersatzhardware ist nicht identisch mit dem alten Gerät 2. Konfiguration wird im DNA Center angepasst

Tabelle 8.5: UC05 Fully Dressed

8.2.6 UC06: Benutzermobilität

Primary Actor	Mobiler Benutzer
Beschreibung	Ein User ändert seinen Arbeitsplatz, das Gebäude oder den Arbeitsort. Er muss an allen Standorten dieselben Policies erhalten und auf dieselben Ressourcen zugreifen können.
Stakeholders	<ul style="list-style-type: none"> • User
Preconditions	<ul style="list-style-type: none"> • User / Gerät erfasst und entsprechende Policies definiert
Postconditions	<ul style="list-style-type: none"> • User kann nach einem Standortwechsel alle Ressourcen verwenden, die ihm auch vor dem Wechsel zur Verfügung standen
Main Success Story	<ol style="list-style-type: none"> 1. User trennt Verbindung am alten Standort 2. User verbindet sich am neuen Standort 3. User authentifiziert sich 4. Die SDA Lösung gewährt dem User Rechte gemäss Policies 5. User kann auf dieselben Ressourcen zugreifen wie am alten Standort
Alternative Flows	<p>4a. Während des Standortwechsels wurden die Policies angepasst</p> <ol style="list-style-type: none"> 1. User erhält Rechte gemäss aktualisierten Policies

Tabelle 8.6: UC06 Fully Dressed

8.2.7 UC07: Degradation

Primary Actor	Netzwerkadministrator
Beschreibung	Es soll aufgezeigt werden, wie sich das System beim Ausfall von verschiedenen Komponenten verhält, wo Single Point of Failures liegen und wie diese allenfalls eliminiert werden können.
Stakeholders	<ul style="list-style-type: none"> • Netzwerkadministrator • Netzwerkbenutzer
Preconditions	<ul style="list-style-type: none"> • Netzwerkinfrastruktur läuft einwandfrei
Postconditions	<ul style="list-style-type: none"> • Ausfall oder Probleme bei einer oder mehreren Komponenten
Main Success Story	<ol style="list-style-type: none"> 1. Netzwerk funktioniert einwandfrei 2. Eine oder mehrere Komponenten fallen aus oder weisen sonstige Probleme auf 3. Netzwerkfunktionalität ist durch den Ausfall nicht beeinträchtigt 4. Fehler wird behoben, System wieder im Sollzustand
Alternative Flows	<ol style="list-style-type: none"> 3a. Durch den Ausfall kommt es zu einer Störung im Netzwerk <ol style="list-style-type: none"> 1. Was sind die genauen Auswirkungen? Wer ist betroffen? 2. Wie kann die Funktionalität wiederhergestellt werden? 3. Kann die Fehlerursache verhindert werden? 3b. Es kommt zum kompletten Ausfall des Netzwerks <ol style="list-style-type: none"> 1. Was sind die genauen Auswirkungen? 2. Wie kann die Funktionalität wiederhergestellt werden? 3. Kann die Fehlerursache verhindert werden?
Mögliche Szenarien	<ul style="list-style-type: none"> • Ausfall eines Edge Nodes • Ausfall eines Intermediate Nodes • Ausfall eines Border/Controller Nodes <ul style="list-style-type: none"> Wenn 1 Node vorhanden ist Wenn 2 Nodes vorhanden sind • Ausfall DNA Center Appliance • Ausfall ISE • Ausfall Infoblox • Ausfall WLC • Ausfall einer physischen Netzwerkleitung

8.2.8 UC08: Integration von nicht Fabric Komponenten

Primary Actor	Netzwerkadministrator
Beschreibung	Die Fabric muss mit Komponenten, die nicht der Fabric angehören kommunizieren können.
Stakeholders	<ul style="list-style-type: none"> • Netzwerkadministrator • Benutzer
Preconditions	<ul style="list-style-type: none"> • Fabric funktioniert • Es sind Komponenten oder Teile des Netzwerks vorhanden, die nicht zu einer Fabric gehören.
Postconditions	<ul style="list-style-type: none"> • Kommunikation funktioniert auch über nicht-Fabric Komponenten hinweg • Policies können auch bei Kommunikation über nicht-Fabric Komponenten angewendet werden
Main Success Story	<ol style="list-style-type: none"> 1. Ein User kommuniziert mit Ressourcen ausserhalb der Fabric 2. Kommunikation funktioniert einwandfrei 3. Policies können wie bei der Kommunikation innerhalb der Fabric angewendet werden
Alternative Flows	<ol style="list-style-type: none"> 1a. Ein User ausserhalb der Fabric will mit Ressourcen innerhalb der Fabric kommunizieren 2a. Kommunikation funktioniert einwandfrei 3a. Policies können wie bei der Kommunikation innerhalb der Fabric angewendet werden

Tabelle 8.8: UC08 Fully Dressed

8.2.9 UC09: Migration von bestehenden klassischen Campus

Primary Actor	Netzwerkadministrator
Beschreibung	Ein bestehendes Netzwerk nach klassischem Campusdesign soll in eine moderne Fabric migriert werden
Stakeholders	<ul style="list-style-type: none"> • Netzwerkadministrator • Netzwerkbenutzer
Preconditions	<ul style="list-style-type: none"> • Netzwerk nach klassischem Campusdesign existiert und funktioniert einwandfrei • DNA Center Appliance inkl. aller Abhängigkeiten ist vorhanden • Netzwerkkomponenten sind fähig in einer Fabric verwendet zu werden
Postconditions	<ul style="list-style-type: none"> • Fabric ist erstellt • DNA Center läuft und verwaltet Fabric(s) • Policies, die in der traditionellen Infrastruktur vorhanden waren funktionieren weiterhin
Main Success Story	<ol style="list-style-type: none"> 1. Bestehende Infrastruktur wird analysiert und inventarisiert 2. DNA Center wird aufgesetzt (inkl. aller Abhängigkeiten) 3. User, Gruppen, Policies etc. werden in DNA Center übernommen 4. Falls nötig wird das Netzwerkdesign angepasst 5. Downtime wird geschätzt und organisatorische Massnahmen werden getroffen. 6. Bestehende Netzwerkgeräte werden in die Fabric übernommen 7. Benutzer können Fabric analog der traditionellen Infrastruktur nutzen
Alternative Flows	-

Tabelle 8.9: UC09 Fully Dressed

8.2.10 UC10: Einsatz von SGT

Primary Actor	Administrator
Beschreibung	Im DNA Center können über das ISE Panel definierte SGT Gruppen hinzugefügt und angepasst werden.
Stakeholders	<ul style="list-style-type: none"> • Administrator
Preconditions	<ul style="list-style-type: none"> • DNA Center muss mit dem ISE verbunden sein und alle ISE SGT-Gruppen und -Geräte müssen im DNA Center vorhanden sein
Postconditions	<ul style="list-style-type: none"> • SGT Gruppen ersichtlich
Main Success Story	<ol style="list-style-type: none"> 1. Login auf DNA Center 2. Unter Systemeinstellungen Cisco ISE Panel auswählen 3. Unter Policy / Registry / Scalable Groups können neue SGT Gruppen hinzugefügt werden
Alternative Flows	1a. 1.

Tabelle 8.10: UC10 Fully Dressed

8.2.11 UC11: Infoblox

Primary Actor	Administrator
Beschreibung	Infoblox ist die IP-Adressmanagement-Lösung (IPAM) für das Cisco Digital Network Architecture (DNA) Center. IP-Adresspools werden zwischen DNA Center und Infoblox synchronisiert. Mit dieser Integration kann die Zuweisung von IP-Adressen automatisiert werden, was einerichtlinienbasierte Bereitstellung in einem einzigen Vorgang ermöglicht und so die Betriebseffizienz verbessert.
Stakeholders	<ul style="list-style-type: none"> • Administrator
Preconditions	<ul style="list-style-type: none"> • Infoblox Server ist eingerichtet
Postconditions	<ul style="list-style-type: none"> • Unter Design / Network Settings / IP Address Pools sind nun die IP-Adressen ersichtlich. • Anpassungen an Addresspool werden zwischen DNA Center und Infoblox synchronisiert • Infoblox verwendet die im DNA Center erstellten Infos für weitere Dienste wie DNS oder DHCP
Main Success Story	<ol style="list-style-type: none"> 1. Login auf DNA Center 2. Unter Settings / IP Adress Manager kann ein Infoblox Server hinterlegt werden. 3. Unter Design / Network Settings / IP Address Pools können nun die IP-Adressen angezeigt werden
Alternative Flows	<ol style="list-style-type: none"> 1a. Direkt nach Installation Infoblox Server bei erstem Konfigurations-Wizard hinzufügen <ol style="list-style-type: none"> 1. Login auf DNA Center 2. IP Adress Manager angeben (Server Name, Server URL, Username, Password, Provider) 1b. Schritt in erstem Konfigurations-Wizard überspringen und Infoblox mit nachfolgenden Schritten hinzufügen.

Tabelle 8.11: UC11 Fully Dressed

9 Testprotokolle

9.1 UC01

Kurzbeschreibung

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	TheBeschreibung	TheShould	TheHls	TheStatus

9.2 UC02

Kurzbeschreibung

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	TheBeschreibung	TheShould	TheIs	TheStatus

9.3 UC03-1 Backup DNA Center

Sämtliche Konfigurationen des DNA Centers sollen gebackcuped werden, sodass diese im Notfall wiederhergestellt werden können.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu den Backup Einstellungen navigieren <i>Settings</i> → <i>System Settings</i> → <i>Backup and Restore</i>	Backup Einstellungen anzeigen	Backup Einstellungen erscheinen	OK
3a	Backup Server hinzufügen via <i>Add</i> → SSH IP Address: 217.26.58.9, SSH Port: 22, Server Path: /home/dnacenter/backup, Username: dnacenter, Password: xxx, Encryption Passphrase: xxx. Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden angenommen, führt zu Absturz des DNA Centers	NOT OK
3b	Backup Server hinzufügen via <i>Add</i> → SSH IP Address: 217.26.58.9, SSH Port: 22, Server Path: /home/dnacenter/backup, Username: dnacenter, Password: xxx, Encryption Passphrase: xxx. Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden angenommen.	OK
4b	Regelmässiges Backup einrichten via <i>Schedule</i> → <i>Add Schedule Later</i> , Weekday: Wednesday, Time: 10:30 AM. Mittels Schedule die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden angenommen.	OK
5b	Backup wird regelmässig zum definierten Zeitpunkt ausgeführt.	Backup wird zum definierten Zeitpunkt ausgeführt	Backup wird nicht ausgeführt	NOT OK

9.4 UC03-2 Restore DNA Center

Sämtliche Konfigurationen des DNA Centers sollen aus einem zuvor erstellten Backup wiederhergestellt werden.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu den Backup Einstellungen navigieren <i>Settings → Backup and Restore</i>	Zuvor erstellte Backups werden angezeigt	Backups werden angezeigt	OK
3	Restore erstellen via <i>Restore</i> neben dem gewünschten Backup	DNA Center wird auf den Stand vom gewählten Backup zurückgesetzt	DNA Center wurde auf den gewünschten Stand zurückgesetzt	OK

9.4.1 Zusammenfassung UC03

Es kann ein Backup erstellt werden und auch ein Restore eines zuvor erstellten Backups ist möglich. Leider ist das Erfassen, Bearbeiten und Löschen eines Backupservers enorm unzuverlässig und hat mehrfach zu kompletten Abstürzen des DNA Centers geführt. Zudem funktioniert der Backup Schedule nicht. Backups werden nicht automatisch ausgeführt, sind also nur manuell möglich. Auch ein Restore einzelner Komponenten des DNA Centers ist nicht vorgesehen und es gibt kein komplettes Backup des DNA Centers. Einzelne Teile wie z.Bsp. Assurance werden nicht gebackedup. Da die Backup Funktionalität des DNA Centers sehr eingeschränkt ist und nur unzuverlässig funktioniert, wird der Use Case "Backup und Restore" nicht vollständig erfüllt.

9.5 UC11: Infoblox

Durch die Integration des Infoblox DDI im DNA Center soll das IP-Adressen Management für neue Netzwerkkomponenten vereinfacht werden.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu IP Adress Manager Einstellungen über <i>Settings</i> → <i>System Settings</i> → <i>Settings</i> → <i>IP Address Manager</i>	IP Adress Manager Einstellungen anzeigen	IP Address Manager Einstellungen erscheinen	OK
3	Infoblox Informationen hinterlegen → Server Name: Infoblox, Server Url: https://10.22.0.21 , Username: admin, Password: xxx, Provider: INFOBLOX). Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen. Eingaben werden angenommen. Eingaben werden angenommen.	Eingaben wurden angenommen und Verbindung zu Infoblox Server erfolgreich hergestellt.	OK
4	IP Adress Pools anzeigen über <i>Design</i> → <i>Network Settings</i> → <i>IP Adress Pools</i> .	IP Address Pools sollten angezeigt werden.	Es werden vorher definierte IP Address Pools angezeigt.	OK

9.6 UC04: Reporting

Andere Use Cases haben eine höhere Priorisierung erhalten. Aus Zeitmangel konnte dieser Use Case nicht behandelt werden.

9.7 UC05: Hardware Ersatz

Offene Frage an Ivan Caduff via Slack

9.8 UC06: Benuttermobilität

Um diesen Use Case zu testen braucht es eine funktionierende Fabric, zwei Gebäude oder besser zwei Standorte und 802.1X Authentifizierung. Da dies leider nicht der Fall ist, konnte dieser Use Case nicht getestet werden.

9.9 UC07: Degradation

In der Main Success Story dieses Use Cases steht „1. Netzwerk funktioniert einwandfrei.“. Da dies zu diesem Zeitpunkt noch nicht der Fall ist, konnte dieser Use Case nicht getestet werden.

9.10 UC08: Integration von nicht Fabric Komponenten

Andere Use Cases haben eine höhere Priorisierung erhalten. Aus Zeitmangel konnte dieser Use Case nicht behandelt werden. Insbesondere, weil nebst einer funktionierenden Fabric auch ein Mapping zwischen den SGT im Legacy Netzwerk konfiguriert hätte werden müssen.

9.11 UC10: Gastzugang

Gemäss *Sitzungsprotokoll der Sitzung mit Cisco vom 23.05.2018* im Anhang ist „(...)Gast-Netz(…)Nur möglich mit separatem Border exklusiv für Gast Netz → Internet(...“). Der Use Case konnte nicht getestet werden, da kein uns kein zusätzlicher Border zu Verfügung stand und andere Use Cases eine höhere Wichtigkeit hatten.

9.12 UC10: Einsatz von SGT

Erstellen einer neuen Scalable Group.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu den Einstellungen navigieren <i>Policy → Registry → Scalable Groups</i>	Liste der <i>Scalable Groups</i> wird angezeigt, inklusive der <i>Add Group</i> Schaltfläche.	Liste der <i>Scalable Groups</i> wird angezeigt, inklusive der <i>Add Group</i> Schaltfläche. Weiterleitung zum Cisco ISE zur Ansicht <i>Components → Security Groups</i> . (Eventuell muss man sich zuvor beim ISE zusätzlich einloggen.) Dort muss <i>Add</i> ausgewählt werden. Es erscheint ein Dialog zum Hinzufügen einer <i>Security Group</i> .	NOT OK
2	Hinzufügen einer neuen Gruppe mithilfe der Schaltfläche <i>Add Group</i>	Neuer Dialog erscheint zum Anlegen einer <i>Scalable Group</i> .	Ein neuer Name, ein Symbol und eine Beschreibung kann hinterlegt werden. Zusätzlich muss <i>Propagate to ACI</i> angewählt werden. Der Dialog wird mit <i>Speichern</i> geschlossen.	OK
3	Neue Gruppe anlegen mit einem Namen	Im Dialog kann ein neuer Name für die <i>Scalable Group</i> eingegeben werden. Der Dialog wird mit <i>Speichern</i> geschlossen.	Der Dialog wird mit <i>Anlegen</i> geschlossen	OK

4	Die Scalable Group ist erstellt. In der Liste der Scalable Groups wird die neu erstellte Gruppe angezeigt.	Da man immer noch in der ISE Ansicht ist, muss zuerst zum alten Tab des DNA Centers gewechselt werden. Anschliessend muss die Seite neu geladen werden. Die neue erstellte Gruppe wird angezeigt.

9.12.1 Zusammenfassung UC10

Noch nicht alle Funktionen können komplett im DNA Center erledigt werden. Ein Teil der Funktionen erfolgt weiterhin über die GUI der anderen Komponenten.

10 Umsetzung

- Ausgewählte Implementierungsdetails (Bsp. Algorithmen, Datenstrukturen, Libraries, Architectural Hot Spots) Dokumentation Architektur und Design (i.d.R. plattformneutral bzw. technologieübergreifend, z.B. in Form von UML-Diagrammen und Erläuterungen dazu)
- Dokumentation, welche Experimente/Tests durchgeführt wurden und welche Lösungsoptionen aufgrund der Ergebnisse dieser Experimente/Tests verworfen wurden.

10.1 Labor Netzwerk Architektur

Mit der zur Verfügung gestellten Hardware ist die folgende Netzwerk Architektur entstanden.

Folgende zentrale Überlegungen sind eingeflossen:

- Campus Netzwerk mit mehreren Gebäuden, um das Wandern von Geräten zu simulieren.
- Mischung der zur Verfügung stehenden Switches (Catalyst 9300 & 3850) in der Fabric Edge Nodes, um Verhalten zu vergleichen.
- Management Netzwerk ist inbound. Kabelführung zu jedem Switch ist meistens von den Gegebenheiten in typischen Gebäuden nicht möglich.

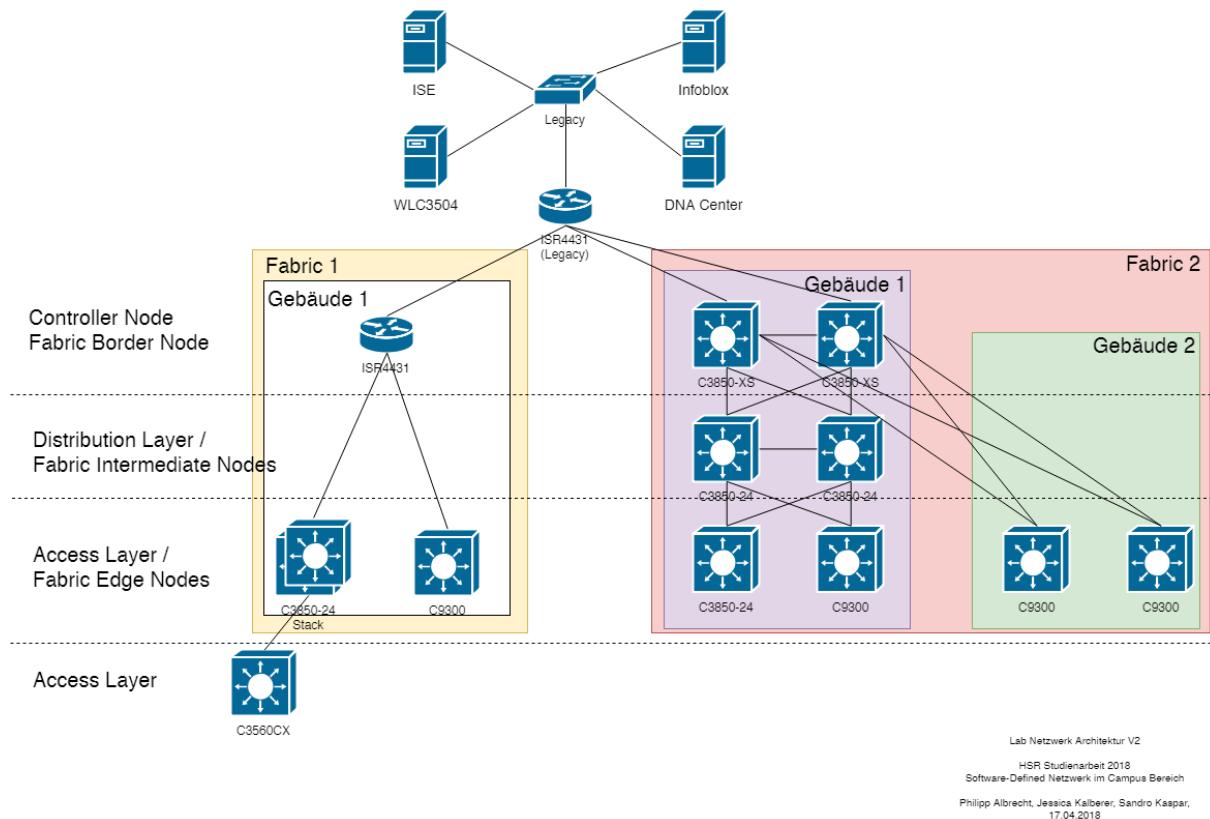


Abbildung 10.1: SDN Netzwerk Architektur

10.2 Netzwerkarchitekturen Vergleich

Hauptunterschiede zwischen der klassischen Netzwerkarchitektur und der "Modernen" Software-Defined Access Architektur.

- Bis zur Fabric Edge Nodes (Vergleichbar mit dem Access Layer) unterliegt ein Layer 3 Netzwerk.
- Kein Einsatz von STP oder VSS auf Distribution Layer notwendig, da das Underlay Netzwerk rein Layer 3 ist und Routing Protokolle (OSPF) zum Einsatz kommen.
- Der Distribution Layer nimmt neu als Fabric Intermediate Nodes nur noch die Funktion als Layer 3 Brücke bzw. VXLAN transportierer ein, anstatt die Grenze zwischen Layer 3 und Layer 2 zu sein. Die Fabric Intermediate Nodes sind optional.
- Während beim klassischen Design die logische Netzwerkarchitektur direkt Abhängig ist von der physikalischen Architektur, wird bei SDN die physische Netzwerkarchitektur von der logischen Architektur getrennt. Man spricht dann von der Physical Fabric Topology bzw. Underlay und den entsprechenden Layer 2 bzw. Layer 3 Overlay Network.

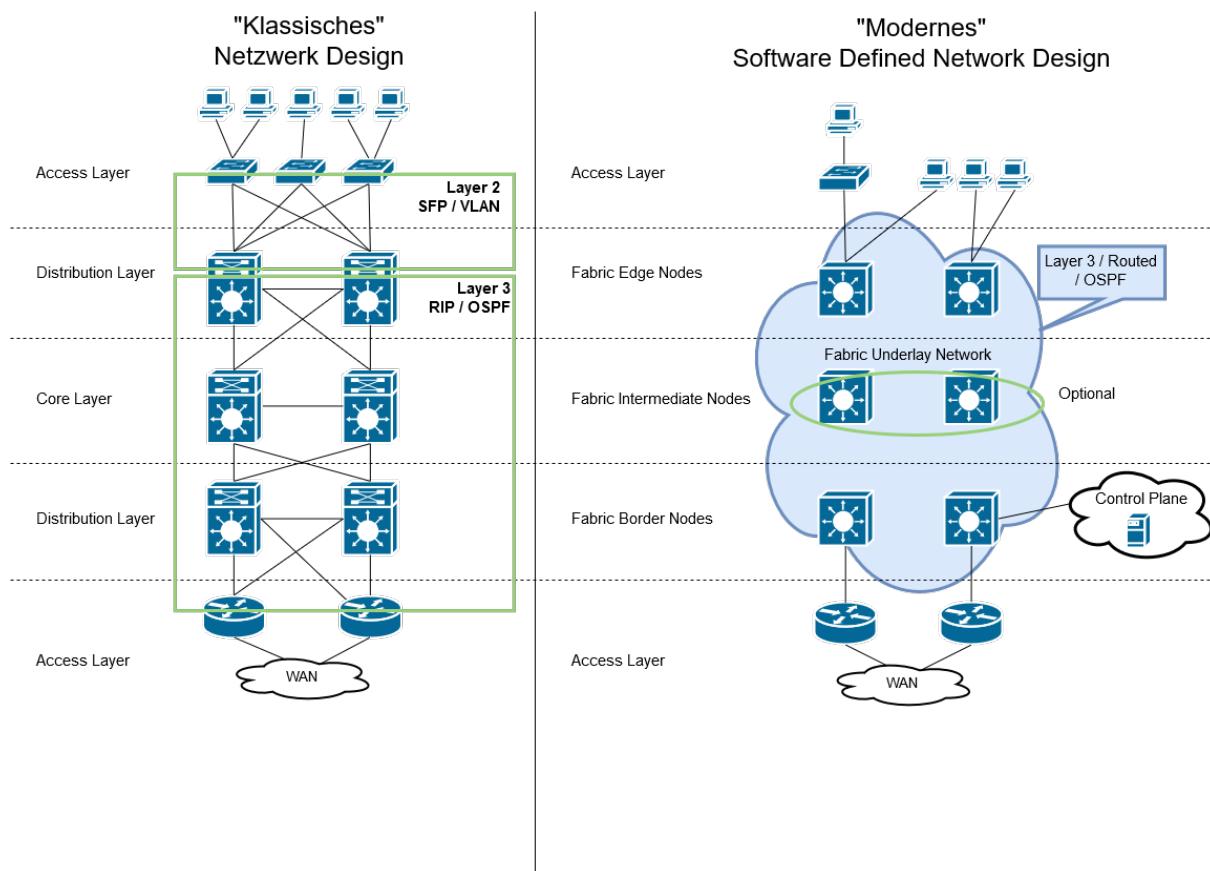


Abbildung 10.2: Netzwerk Architektur Vergleich

10.3 Maximale Skalierungen

Nachfolgend werden die aktuell maximalen Skalierungen des DNA Centers, sowie der Border und Edge Nodes aufgelistet.

SD-Access construct	Maximum for single DNA Center cluster
Endpoints (wired+APs, excluding wireless clients)—across all fabric domains	25,000
Fabric nodes—across all fabric domains (routers, switches/switch stacks, WLCs)	2,500
Non-Fabric Nodes (Intermediate, Extension)	10,000
Access points—across all fabric domains (each AP counts as an endpoint)	4,000
IP pools—across all fabric domains	500
Sites	500
Fabric domains	20
Scalable group tags—across all fabric domains	1,000
Policies—across all fabric domains	1,000
Contracts—across all fabric domains	500

Abbildung 10.3: DNA Center Maximum Scale Constraints HA Cluster

SD-Access construct	Maximum per fabric domain
Control plane nodes	2
Default border nodes	4

Abbildung 10.4: DNA Center Maximum Scale Constraints Fabric

	Catalyst 3850/3650	Catalyst 9300	Catalyst 4500 Supervisor 8-E and 9-E	Catalyst 9400 Supervisor Engine-1
Virtual Networks (limited fabric-wide by deployed devices having lowest capability)	64	256	64	256
Scalable group tags	4,000	8,000	2,000	8,000
Security group ACLs	1,500	5,000	32,000	18,000

Abbildung 10.5: SDA Edge Node Scale Constraints

	Catalyst 3850 (Fiber)	Catalyst 9300	Catalyst 9500	Catalyst 6800	Nexus 7700 Supervisor 2E	ASR 1000 and ISR 4000	CSR1000v
Virtual networks (limited fabric-wide by deployed devices having lowest capability)	64	256	256	512	500	4,000	–
Scalable group tags	4,000	8,000	8,000	30,000	64,000	64,000	–
Security group ACLs	1,500	5,000	18,000	30,000	64,000	64,000	–
Fabric control plane entries	4,000	4,000	96,000	25,000	Unsupported	200,000	200,000
IPv4 routes	8,000	8,000	48,000	1,000,000 (XL) 256,000 (non-XL)	1,000,000	4,000,000 (16GB) 1,000,000 (8GB)	–
IPv4 host entries	16,000	24,000	96,000	1,000,000 (XL) 256,000 (non-XL)	1,000,000	4,000,000 (16GB) 1,000,000 (8GB)	–

Abbildung 10.6: SDA Border Node Scale Constraints

10.4 Verkabelungsplan

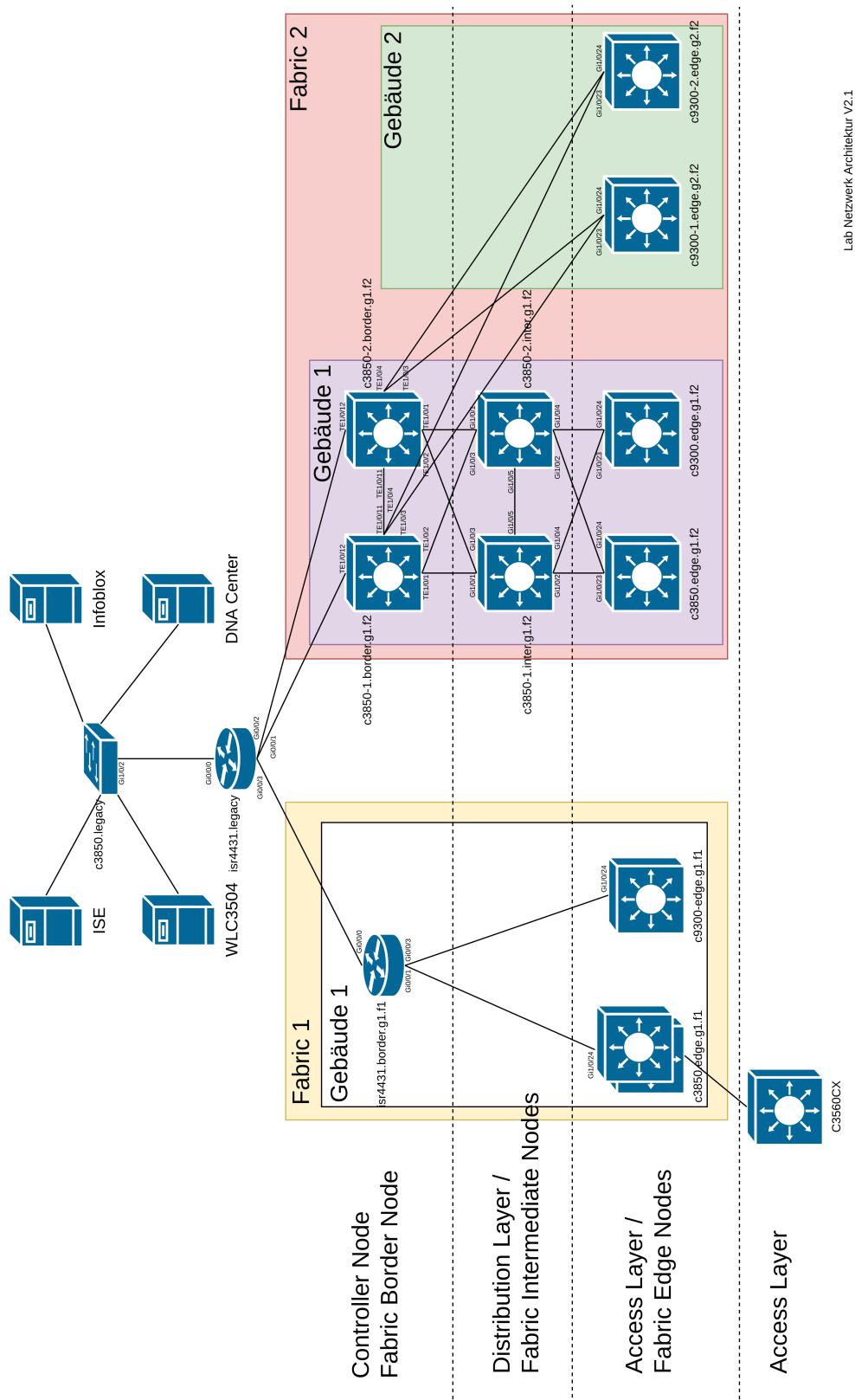


Abbildung 10.7: Lab Architecture with physical Interfaces

Lab Netzwerk Architektur V2.1

HSR Studierarbeit 2018
Software-Defined Netzwerk im Campus Bereich
Philip Albrecht, Jessica Kalberer, Sandro Kaspar,
30.05.2018

11 Vorgehen Versuch 1

Nachfolgend haben wir das Vorgehen von unserem ersten Versuch in einer Grafik übersichtlich dargestellt. Die Blitze deuten dabei auf ein Hindernis bei welchem mehr Aufwand benötigt wurde hin und das rote X als einen fehlgeschlagenen Versuch, welcher abgebrochen werden musste.

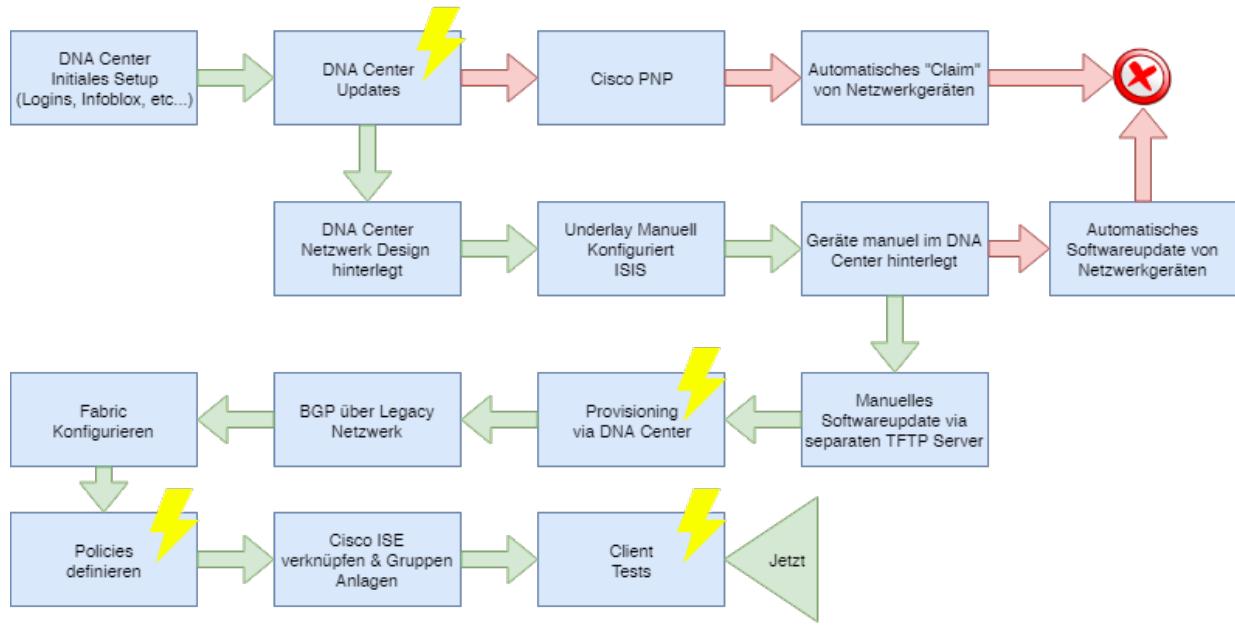


Abbildung 11.1: Grafische Übersicht über das Vorgehen beim ersten Versuch

11.1 DNA Center Initiales Setup

11.1.1 Installation

Die Installation des DNA Centers erfolgt direkt an der Konsole oder über die Cisco IMC. Dabei wird der maglev-config-wizard ausgeführt. Dieser Befehl kann zu einem späteren Zeitpunkt erneut ausgeführt werden, wenn die Konfiguration angepasst werden muss. Wie in Kapitel 2[8] beschrieben werden folgende Angaben benötigt:

- Host IP Adresse
- Netmask
- Default Gateway IP adress
- DNS Servers
- Static Routes
- HTTPS Proxy
- Maglev Master Node IP
- Username, Passwort und Linux Passwort
- Administration Passphrase für das Web-Interface
- NTP Server
- Service Subnets

Im ersten Schritt 11.2 wird gewählt, ob ein neuer Cluster erstellt werden soll oder einem beigetreten werden soll. Bei der Testumgebung dieser Arbeit war nur eine Appliance verfügbar, weshalb schliesslich "Start a DNA-C Cluster" ausgewählt wurde.

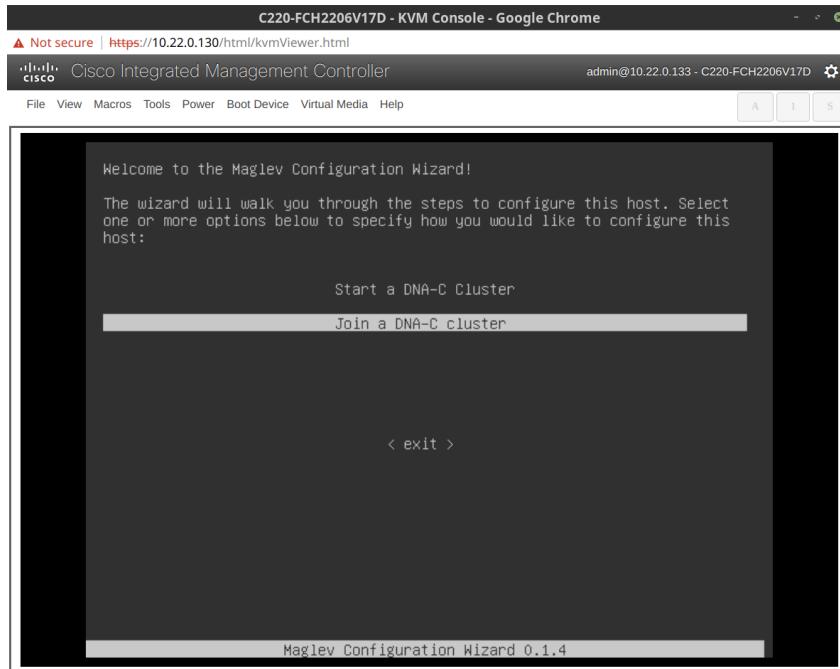


Abbildung 11.2: DNA Center Configuration Wizard - Start

Im nächsten Schritt muss die IP Konfiguration für die DNA Center Appliance angegeben werden. Es muss mindestens ein Interface konfiguriert werden und als Cluster Link definiert sein. Statische Routen können definiert werden, sind aber optional.

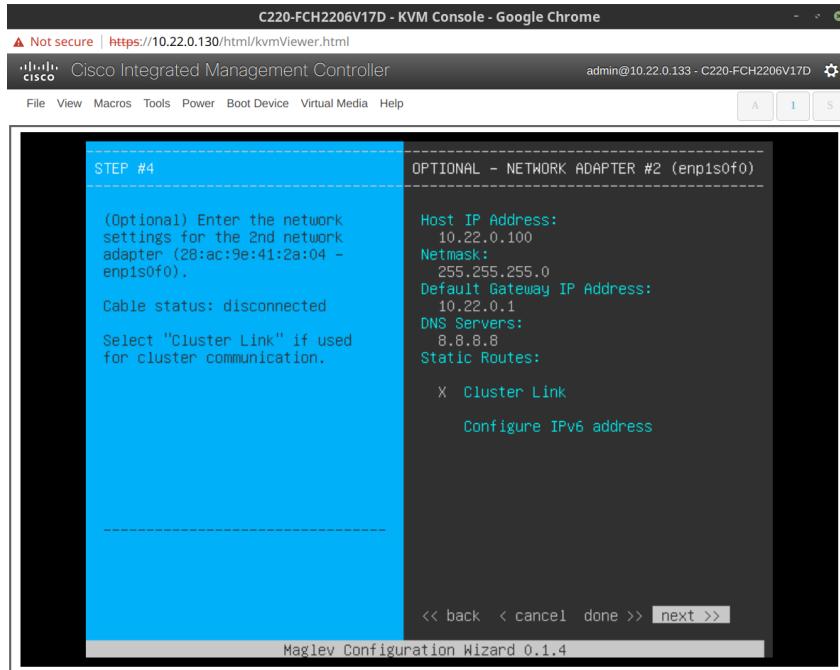


Abbildung 11.3: DNA Center Configuration Wizard - Entering Management IP

Im letzten Schritt des Wizards werden alle User Account Einstellungen festgelegt. Hierbei ist zu beachten, dass das "Linux Password" für den SSH Zugriff benötigt wird und die "Administrator Passphrase" für den Zugang zum Web Interface.

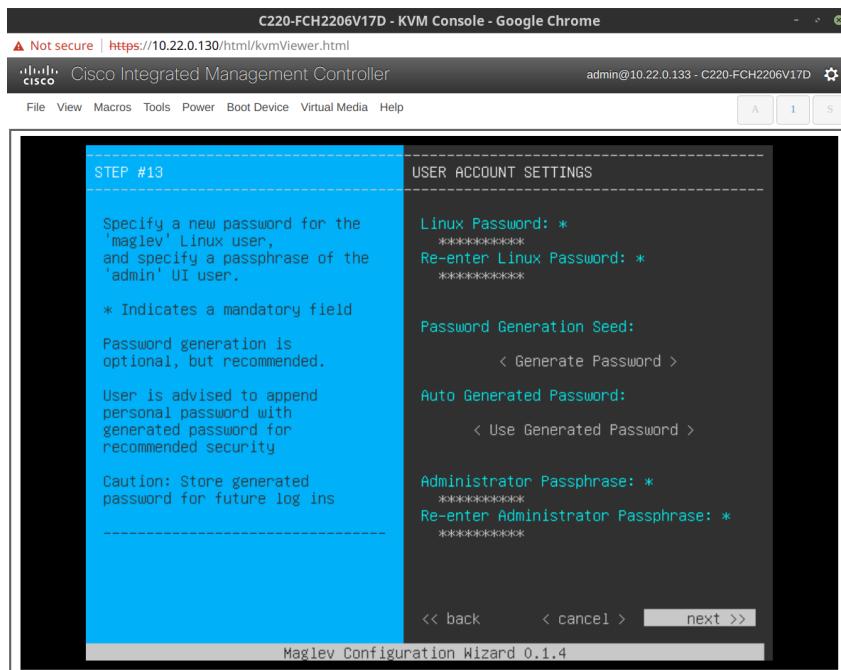


Abbildung 11.4: DNA Center Configuration Wizard - Entering Authentication Data

Nun wird das DNA Center aufgesetzt. Dieser Prozess dauert mehrere Stunden.

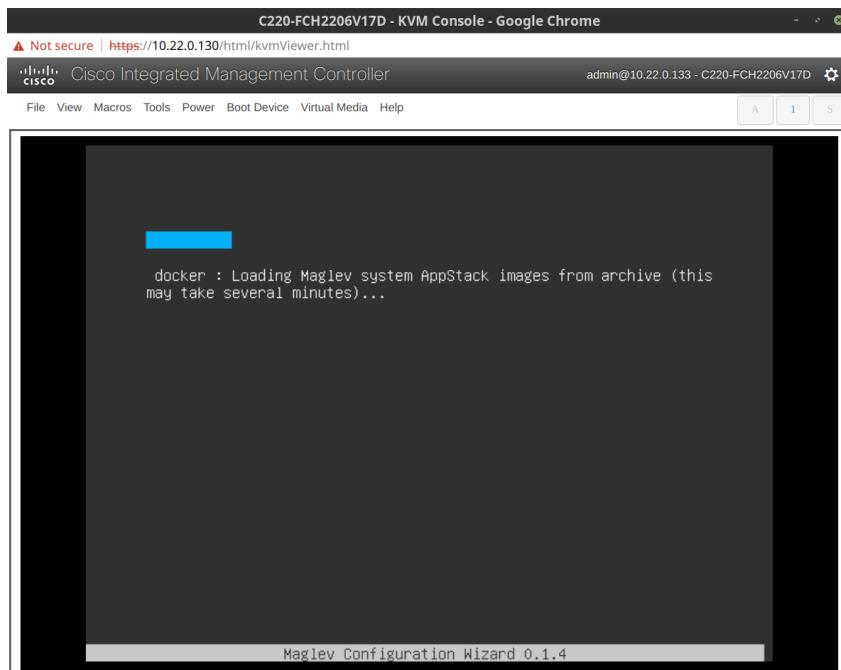


Abbildung 11.5: DNA Center Configuration Wizard - DNA Center uses docker

11.1.2 Setup Accounts

Nach dem der Wizard die Installation vollständig ausgeführt hat, ist das DNA Center Web-GUI verfügbar. Die Konfiguration kann nun über dieses weitergeführt werden.

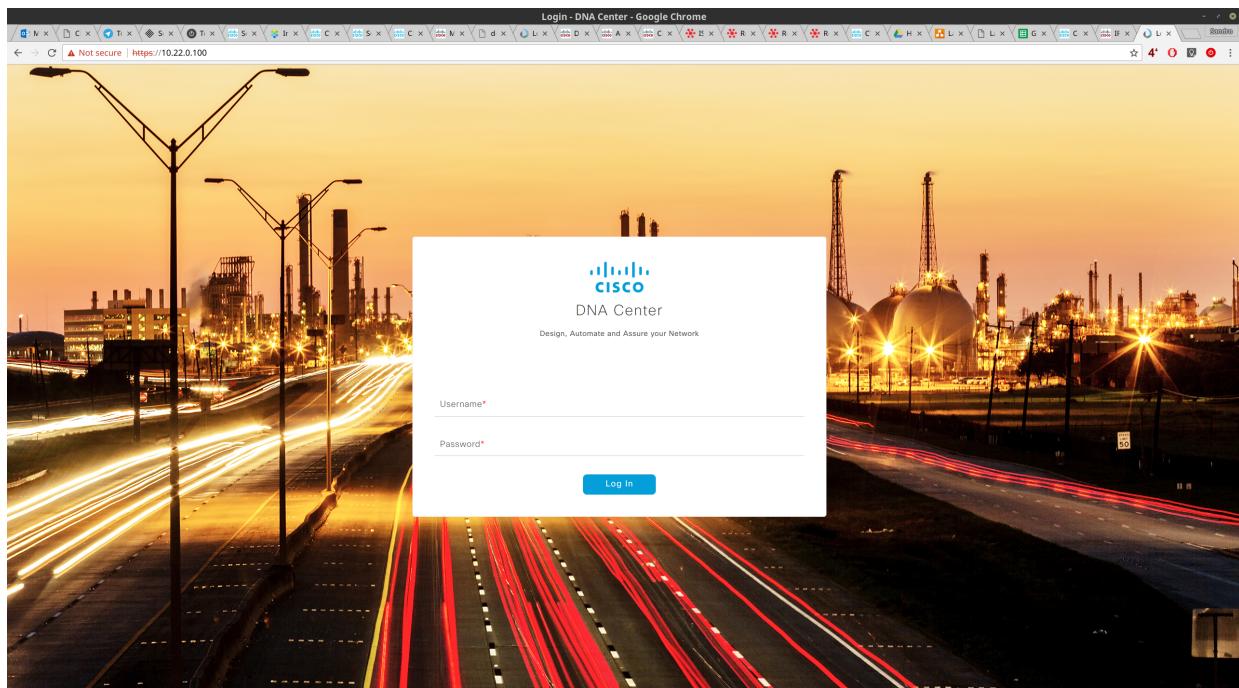


Abbildung 11.6: DNA Center Web GUI - Login Page

Gleich zu Beginn verlangt das DNA Center die Cisco Credentials die mit dem Smart Account verknüpft sind, in welchem die Lizenzen verwaltet werden. Diese Informationen können auch zu einem späteren Zeitpunkt noch eingetragen werden.

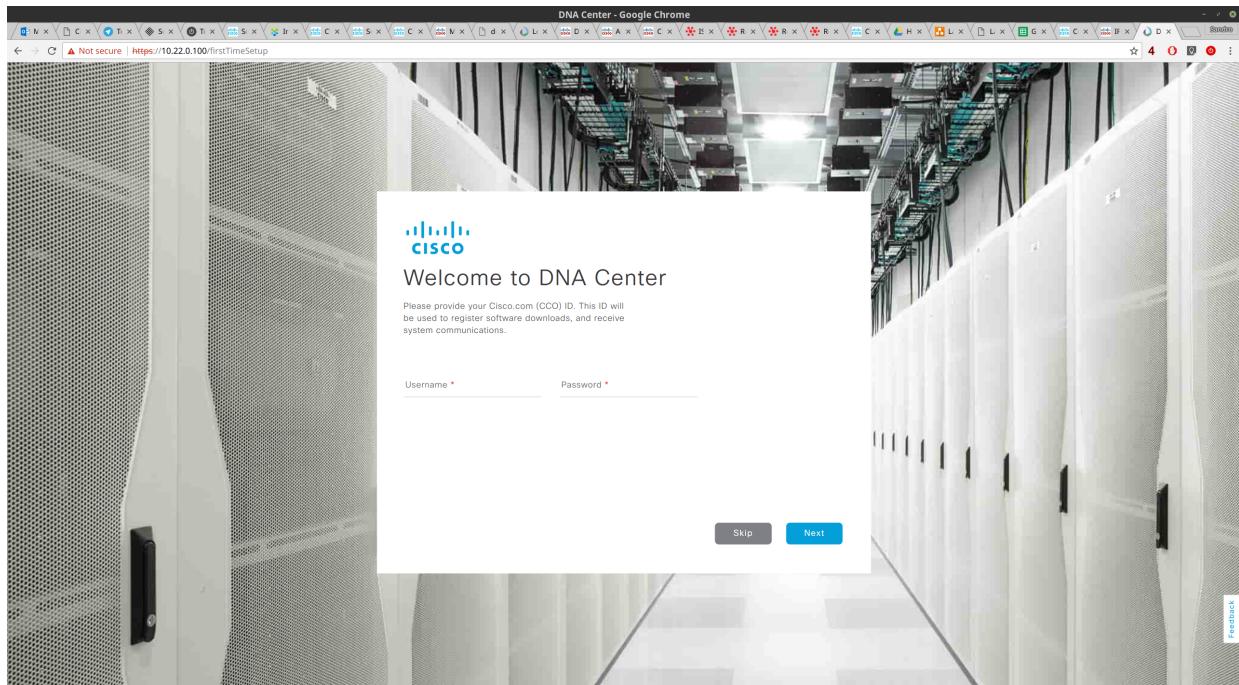


Abbildung 11.7: DNA Center Web GUI - Cisco Credentials for Licences

Im nächsten Schritt kann ein IPAM Server angegeben werden. Diese Einstellung kann ebenfalls später angepasst werden, weshalb wir diesen Schritt zu Beginn übersprungen haben.

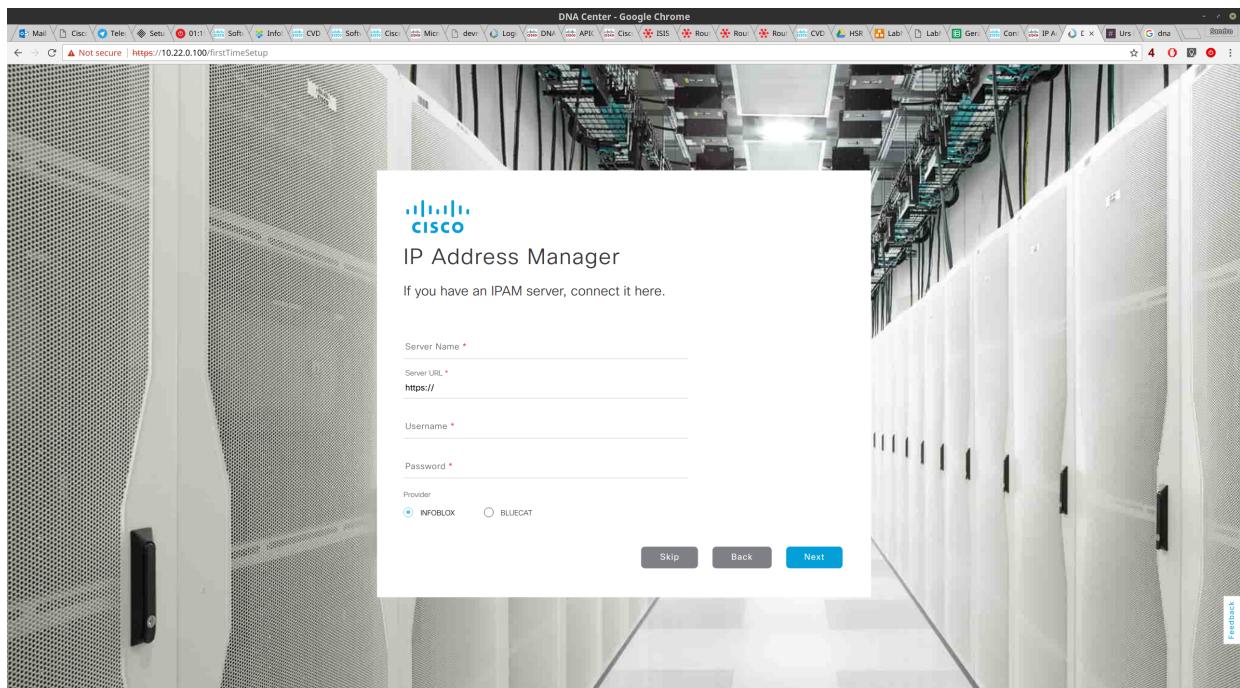


Abbildung 11.8: DNA Center Web GUI - Cisco IPAM

Danach ist die initiale Konfiguration beendet und das DNA Center Dashboard wird angezeigt.

Section	Description	Tasks/Links
Design	Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.	<ul style="list-style-type: none"> Add site locations on the network Designate golden images for device families Create wireless profiles of SSIDs
Provision	Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.	<ul style="list-style-type: none"> Discover and provision switches to defined sites Provision WLCs and APs to defined sites Set up Campus Fabric across switches
Assurance	Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.	<ul style="list-style-type: none"> Assurance Health Assurance Issues
Tools		<div>Discovery: Automate addition of devices to controller inventory</div> <div>Inventory: Add, update or delete devices that are managed by the controller</div> <div>Topology: Visualize how devices are interconnected and how they communicate</div> <div>Image Repository: Download and manage physical and virtual software images automatically</div>

Abbildung 11.9: DNA Center Web GUI - Dashboard

11.2 DNA Center Updates

Da sich das DNA Center während dem Setup Prozess nicht automatisch aktualisiert und die DNA Center Versionen in relativ kurzen Intervallen released werden, ist es ratsam, gleich zu Beginn die aktuellsten Updates zu installieren.

Der Updateprozess birgt jedoch einige Hürden:

- System Updates müssen vor den Package Updates heruntergeladen und installiert werden.

Werden die Package Updates vor dem System Update ausgeführt, können diese blockieren.

- Die Package Updates müssen in der richtigen Reihenfolge installiert werden.
- Die oben genannte Reihenfolge ist nicht direkt ersichtlich.
- Der Updatevorgang dauert mehrere Stunden.
- Der Updatefortschritt wird nicht angezeigt.
- Während dem Updateprozess können Teile des Web-GUIs Fehlermeldungen anzeigen oder überhaupt nicht mehr erreichbar sein.

Die Update Ansicht ist unter *Einstellungen (Zahnrad-Symbol)* → *System Settings* → *App Management* zu finden:

Application Management - System Updates			
Package	Status	Installed Version	Available Update
System	Running	1.0.4.741	1.0.4.807 Install

Abbildung 11.10: DNA Center App Management

11.2.1 Fehlgeschlagene Updates reparieren

Falls Updates in der falschen Reihenfolge installiert wurden oder aus anderen Gründen blockiert sind, können bereits heruntergeladene oder installierte Updates mit folgenden Befehlen entfernt und bereinigt werden. (am Beispiel von main-system-package:1.0.4.779):

```
$ maglev package status | awk '$3 ~ /[0-9]+/ { print $1 ":" $3 }' |
grep -v "system" | while read pkg;
do maglev catalog package delete $pkg; done
$ maglev system_update_package install main-system-package:1.0.4.779
```

11.2.2 Update Reihenfolge

Nach einem Update wurde die Reihenfolge von System und Package Updates angepasst. Vermutlich um den Administrator dazu zu bringen zuerst die System Updates zu installieren.

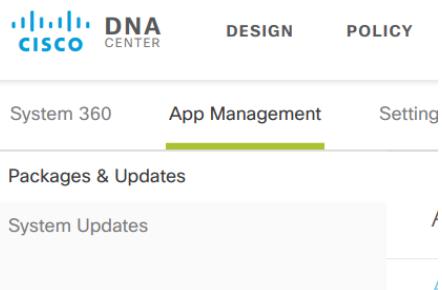


Abbildung 11.11: DNA Center App Management - Alte Menü Anordnung

11.2.3 Schwierigkeit: CCO Credentials für Updates notwendig

Application Packages und System Updates können nur installiert werden, wenn die CCO Credentials hinterlegt sind.



Cisco Connection On-line

CCO credentials were not found. Please enter your CCO credentials in Settings / [Cisco Credentials](#) and try again.

[OK](#)

Abbildung 11.12: DNA Center Upgrade - Cisco Credentials required

11.2.4 Schwierigkeit: Unterschiedliche Versionsangabe

Beim Updatevorgang kann es zu Verwirrungen kommen, weil die Versionangabe von der Funktion *About* von der Version des System Packages abweicht.



Abbildung 11.13: DNA Center - About - Version

Oben wurde bei *About* die richtige Version 1.1.4 angegeben. Nachfolgend die Anzeige unter *System Updates*, welche eine andere Version anzeigt.

Application Management - System Updates

Package	Status	Installed Version	Available Update
System	Running	1.0.4.807	1.0.4.824 Install

Abbildung 11.14: DNA Center - System Upgrade - Version

11.3 DNA Center Netzwerk Design

11.3.1 Network Hierarchy

Gemäss unserer Netzwerk Architektur wie in Kapitel 10.1 beschrieben, haben wir zwei Standorte. Rapperswil mit zwei Gebäuden und Jona mit einem Gebäude. In DNA Center können diese sehr einfach im Abschnitt *Design → Network Hierarchy* hinzugefügt werden.

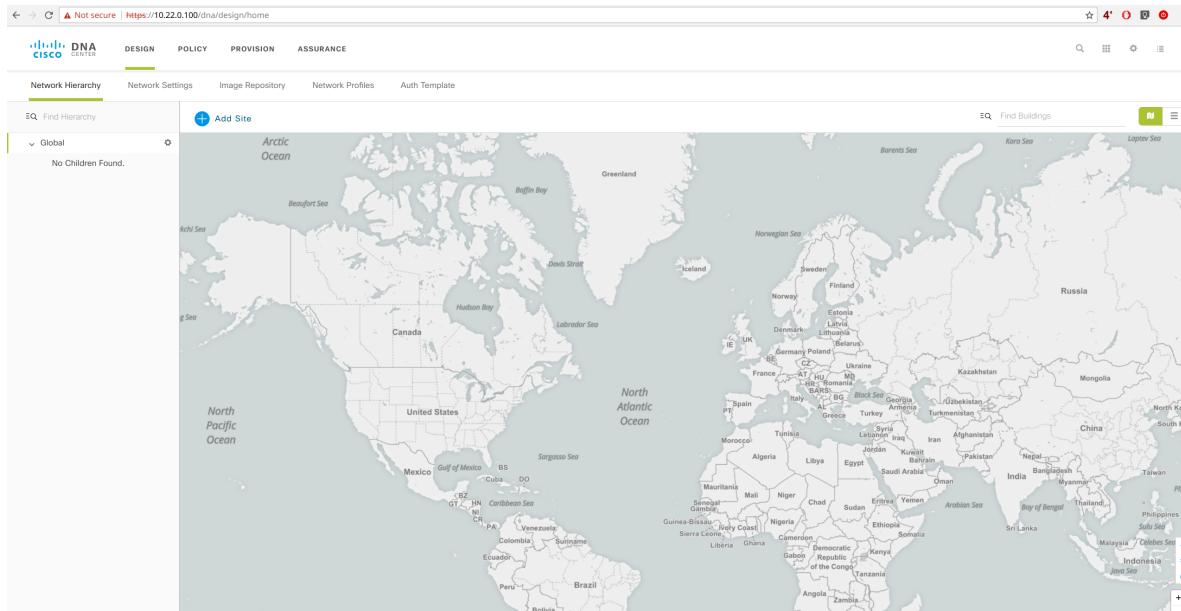


Abbildung 11.15: DNA Center Design Map

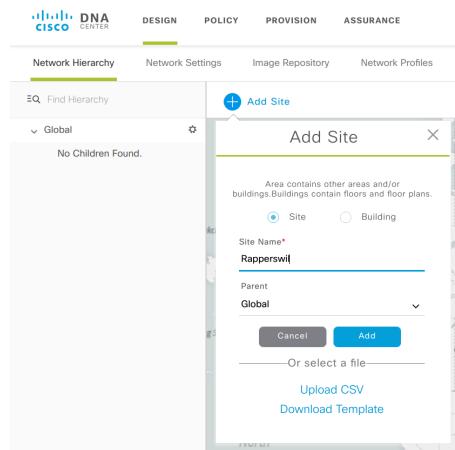


Abbildung 11.16: DNA Center Design - Standort hinzufügen

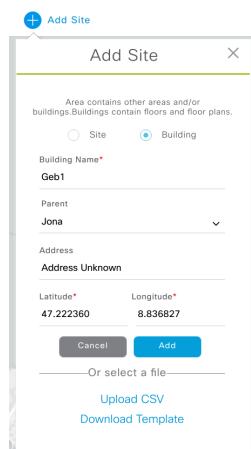


Abbildung 11.17: DNA Center Design - Gebäude können mit Koordinaten hinzugefügt werden.

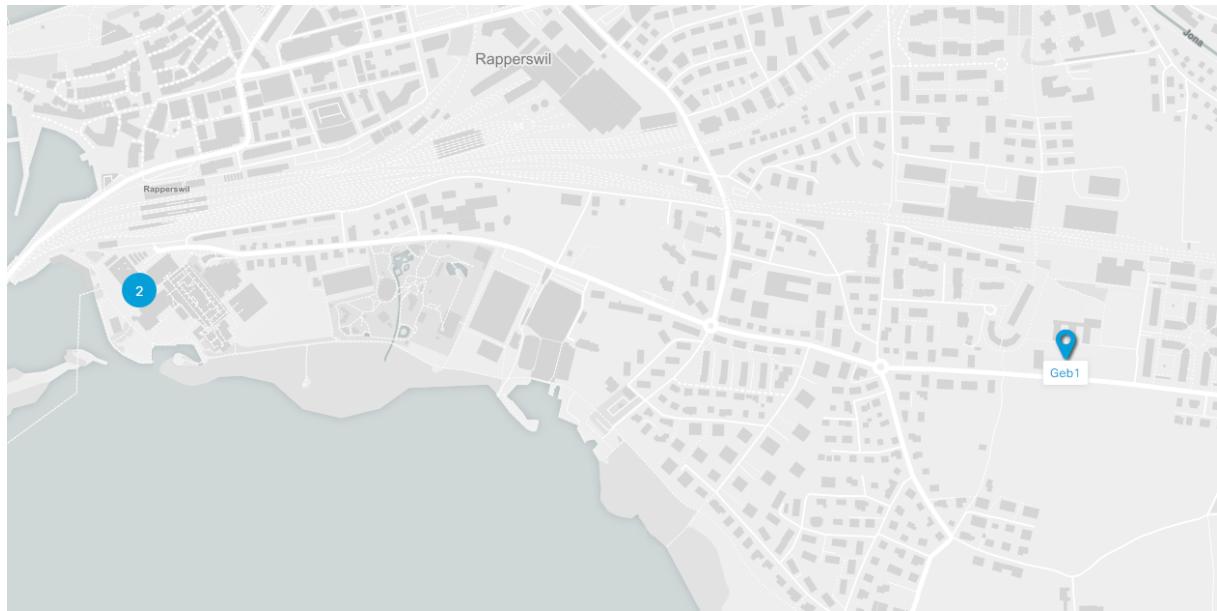


Abbildung 11.18: DNA Center Design - Übersicht über alle Standorte und Gebäude

11.4 LAN Automation

Das DNA Center nutzt Plug and Play um automatisch Netzwerkgeräte in Betrieb zu nehmen und initial zu konfigurieren.

11.4.1 DHCP Konfiguration

Bei unserem ersten Versuch ein Seed-Device festzulegen, wurde vom DNA Center kein DHCP Server konfiguriert, weshalb wir diesen manuell auf Infoblox eingerichtet haben.

Cisco PnP kann über die DHCP Optionen 43 und 60 konfiguriert werden (siehe [11]). In unserem Fall haben wir diese Optionen wie nachfolgend auf der Grafik ersichtlich auf dem Infoblox Server konfiguriert. Diese sind nötig, damit das Netzwerkgerät den PnP Server findet.

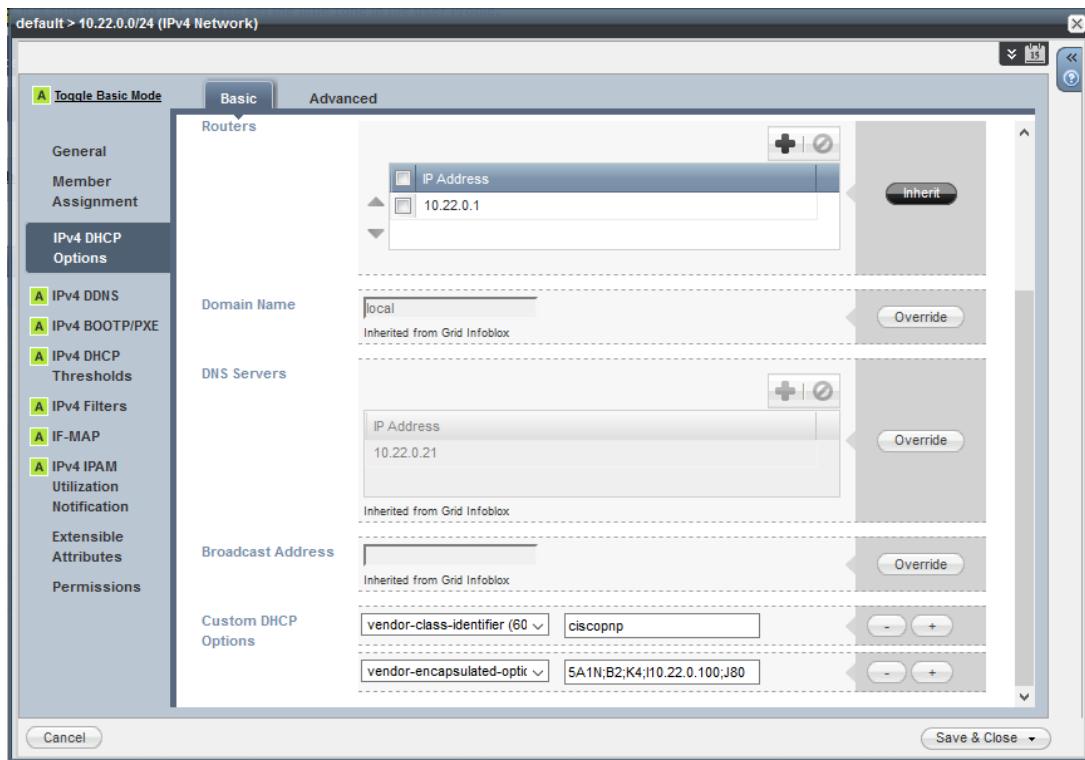


Abbildung 11.19: Infoblox Cisco PNP DHCP Option Konfiguration

Mit diesen Einstellungen hat PnP funktioniert. Allerdings nur sehr unzuverlässig und es kam oft zu Problemen, weshalb dies für viele Geräte mehrmals wiederholt werden musste. Hier ist zu empfehlen, nie mehr als ein Gerät gleichzeitig in Betrieb zu nehmen, damit es möglichst wenig Probleme gibt.

Uptime	First Seen	Status
2018-04-18 20:59:17.000382	2018-04-18 20:58:09.000507	UNCLAIMED
2018-04-18 21:10:11.000468	2018-04-18 21:10:04.000342	CERTIFICATE_INSTALL_REQUESTED
2018-04-18 21:00:21.000283	2018-04-18 20:59:12.000378	UNCLAIMED
2018-04-18 20:54:07.000560	2018-04-18 20:47:48.000666	ERROR_DURING_CERTIFICATE_INSTALL

Abbildung 11.20: DNA Center Provision - Fehlermeldungen in der "Unclaimed List"

11.5 Underlay Konfiguration

Das ISIS Routing im Underlay sollte vom DNA Center automatisch konfiguriert werden können. Da die entsprechende Funktion LAN Automation in unserem Versuch aber nicht funktionierte, wurde der Underlay manuell konfiguriert. Dazu wurden auf den Geräten IP Addressen auf den Loopback Interfaces und den P2P Links konfiguriert und entsprechende Router eingerichtet. Am Border wurde BGP verwendet, damit die Devices auch aus dem Legacy Netz erreichbar sind.

Dabei ist uns aufgefallen, dass die Geräte nur über eine IP-Base Lizenz verfügen. Für die Verwendung von BGP und VRF-lite ist aber die IP-Services Lizenz nötig.

Functions	LAN Base	IP Base	IP Services
Layer 2+	Enterprise access Layer 2 Wide range of Layer 2 access features for enterprise deployments supports Cisco StackPower technology	Complete Access Layer 2 Supports all Cisco Catalyst 2000 and Cisco Catalyst 3000 Layer 2 features, including hot standby protocols	
Layer 3	Static IP routing support Support for SVI	Enterprise access Layer 3 RIP, EIGRP stub, OSPF for routed access, PBR, IPv4 & IPv6 EIGRP stub routing, WCCP, IPv6 uRPF, IPv6 PBR, VRRPv3, Policy Classification Engine, HSRP v6	Complete access Layer 3 OSPF, EIGRP, BGP, IS-IS VRF-lite
Multicast	IGMP	IPv4 & IPv6 PIM routing	
Mobility	Supports Cisco Unified Wireless Networking mobility architecture	Supports Cisco Converged Access mobility architecture with CAPWAP termination at the access	
Manageability	Basic manageability Support for a wide range of MIBs, IPSLA Responder, and RSPAN, PnP, Autoconf, Interface Templates, Secure CDP	Enterprise access Layer 3, Flexible NetFlow for wired and wireless traffic EEM, GOLD-Lite, and Smart Install Director	
Security	Enterprise access security DHCP Snooping, IPSG, DAI, PACLs, Cisco Identity 4.0, NAC and 802.1x features	Complete access security Router and VLAN ACLs, private VLANs, complete identity and security; Cisco TrustSec® SXP and IEEE 802.1AE capable in hardware, Device Sensor	
QoS	Enterprise access QoS Ingress policing, Trust Boundary, AutoQoS, and DSCP mapping	Complete access QoS Support for all Cisco Catalyst 2000 and Cisco Catalyst 3000 QoS features, including per-VLAN policies	
Interoperability	Prime 2.1	Identity Services Engine (ISE 1.2/1.3), Mobility Services Engine (MSE 8.0), Improved WebUI	

Abbildung 11.21: IP Base and Services

Mit folgenden Befehlen war es möglich, eine IP-Services Test Lizenz zu aktivieren und somit die benötigten Features zu nutzen.

```
sh license right-to-use activate ipservices all acceptEULA
reload
show license right-to-use
```

11.6 "Claim" von Netzwerkgeräten

11.6.1 DNA Center Provision - Unclaimed Devices

Nachdem die Geräte via PnP eine initiale Konfiguration erhalten haben und die Konnektivität via ISIS und BGP sichergestellt war, wurden diese im Device Inventory als Unclaimed Devices angezeigt.

The screenshot shows the Cisco DNA Center interface under the 'PROVISION' tab. The main title is 'Device Inventory'. Below it, a sub-section titled 'Unclaimed Devices (8)' is selected. A table lists eight unclaimed switches, each with a checkbox, device name, serial number, product ID, IP address, location, OS image, uptime, first seen, and status (all marked as 'UNCLAIMED').

	Device Name	Serial Number	Product ID	IP Address	Location	OS Image	Uptime	First Seen	Status
<input type="checkbox"/>	Switch	FCW2130L0FH	C9300-24T	10.22.5.179	Unassigned	16.6.2	2018-04-18 20:59:17.0000382	2018-04-18 20:58:09.0000507	UNCLAIMED
<input type="checkbox"/>	Switch	FCW2129L02Z	C9300-24T	10.22.5.180	Unassigned	16.6.2	2018-04-18 21:00:21.0000283	2018-04-18 20:59:12.0000378	UNCLAIMED
<input type="checkbox"/>	Switch	FCW2122L01P	C9300-24T	10.22.5.178	Unassigned	16.6.2	2018-04-18 21:13:04.0000376	2018-04-18 21:11:45.0000906	UNCLAIMED
<input type="checkbox"/>	Switch	FCW2113F07N	WS-C3850-24P-S	10.22.5.173	Unassigned	16.6.3	2018-04-18 21:14:51.0000680	2018-04-18 21:13:36.0000232	UNCLAIMED
<input type="checkbox"/>	Switch	FOC2112X13T	WS-C3850-24P-S	10.22.5.174	Unassigned	16.6.3	2018-04-18 21:13:50.0000280	2018-04-18 21:12:29.0000997	UNCLAIMED
<input type="checkbox"/>	Switch	FOC2112X0PZ	WS-C3850-12XS-S	10.22.5.176	Unassigned	16.6.3	2018-04-18 22:14:20.0000476	2018-04-18 22:13:08.0000879	UNCLAIMED
<input type="checkbox"/>	Switch	FOC2113U08D	WS-C3850-24P-S	10.22.5.175	Unassigned	16.6.3	2018-04-18 21:13:15.0000783	2018-04-18 21:11:45.0000408	UNCLAIMED
<input type="checkbox"/>	Switch	FOC2112U0T1	WS-C3850-12XS-S	10.22.5.177	Unassigned	16.6.3	2018-04-18 22:13:54.0000227	2018-04-18 22:12:43.0000177	UNCLAIMED

Abbildung 11.22: DNA Center Provision - Alle Geräte erfolgreich in der "Unclaimed List"

11.7 Netzwerkgeräte zu Inventory hinzufügen

Der nächste Schritt wäre nun, die Devices zu "Claimen". Dies bedeutet, dass die Geräte einem Standort zugewiesen werden und somit erste Konfigurationen erhalten können. Der Claim Prozess hat leider gar nie funktioniert. Das DNA Center reagierte einfach nicht auf die Eingabe.

11.7.1 Manuell Geräte im DNA Center hinzufügen

Da alle Versuche die Geräte automatisch hinzuzufügen gescheitert sind, entschieden wir uns den Vorgang manuell durchzuführen.

Im Dashboard klickt man dazu auf *Inventory* (siehe 11.23)

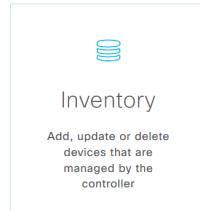


Abbildung 11.23: DNA Center Dashboard - Inventory Knopf

Anschliessend wählt man *Add* (siehe 11.24)

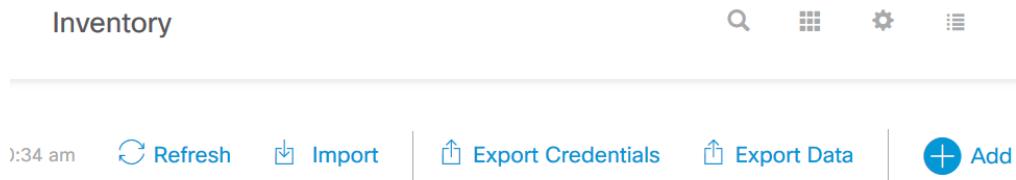


Abbildung 11.24: DNA Center Inventory - Gerät hinzufügen

Danach müssen folgende Informationen eingegeben werden:

- Device Type
- Device IP Name
- SNMP (Version, Read und Write Community)
- CLI (via SSH oder Telnet) *oder*
- NETCONF

Wir entschieden uns hier CLI via SSH zu wählen.

The form is titled "Add Device". It has a dropdown for "Type" set to "Network Device". The "Device IP / Name" field contains "10.22.20.248". Under "SNMP", the "Version" is set to "V2C" and the "Read Community" is "public". Under "CLI", the "Protocol" is "SSH2" and the "Username" is "dnadmin". There are "Cancel" and "Add" buttons at the bottom.

Abbildung 11.25: DNA Center Inventory - Formular Gerät hinzufügen

Danach erscheint das Gerät im Inventory. (siehe 11.26)

The table lists the inventory items. One item is shown: "Switch local 10.22.20.250" with IP address "10.22.20.250", reachability status "Reachable", up time "1 day", last updated time "1 day", resync interval "8 minutes ago", last inventory collection status "Managed", and location "Gb2".

Abbildung 11.26: DNA Center Inventory - Neue Geräte in der Liste

11.8 Image Repository

Im DNA Center können Netzwerkgeräte automatisch aktualisiert werden. Sobald ein Gerät im Inventory erfolgreich hinzugefügt worden ist, sucht das DNA Center automatisch nach Updates. Allerdings nur, wenn ein CCO Account konfiguriert ist. Die verfügbaren Images sind unter *Design* → *Global* → *Image Repository* zu finden.



Abbildung 11.27: DNA Center Design - Image Respository

In diesem Image Repository kann das gewünschte Image mit einem "Golden Tag" versehen werden, worauf dieses heruntergeladen wird.

11.9 Automatisches Softwareupdate von Netzwerkgeräten

Die Softwareupdates von Netzwerkgeräten können im DNA Center unter *Provision* → *Devices* → *Inventory* durchgeführt werden. Ebenfalls wird hier angezeigt, welche Softwareversion zur Zeit auf dem Gerät installiert ist und ob diese aktuell ist.

Abbildung 11.28: DNA Center Provision - Die OS Versionen sind outdated.

Das automatische Softwareupdate hat bei keinem von unseren Switches oder Routern geklappt. Nachfolgend eine kleine Übersicht über die verschiedenen Update Methoden und ausgeführten Versuche.

Methode	Resultat
DNA Center über HTTP und SFTP	Fehlgeschlagen (siehe 11.29)
CLI - HTTPS	Fehlgeschlagen (siehe 11.30)
CLI - SCP	Fehlgeschlagen (siehe ??)
CLI - TFTP	Erfolgreich (siehe 11.31)

Tabelle 11.1: Softwareupdate - Übersicht Methoden und ausgeführten Versuche
Beim Versuch die Softwareupdates im DNA Center über HTTP oder SFTP durchzuführen, wurden folgende Fehlermeldungen angezeigt.

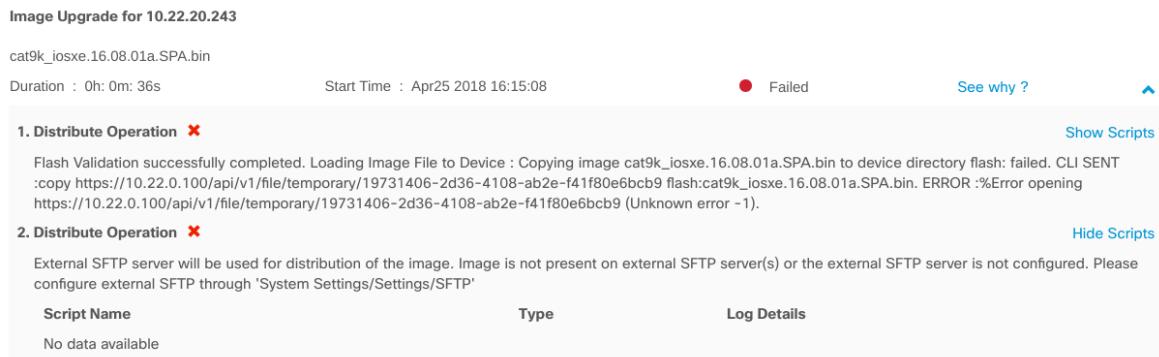


Abbildung 11.29: Fehlermeldung Updatevorgang via DNA Center

Die Upgrade Prozesse wurden schon beim Kopieren der einzelnen Images nach unterschiedlicher Dauer immer abgebrochen.

11.10 Manuelles Softwareupdate

Da wie oben beschrieben das automatische Update nicht funktionierte, wurde in einem nächsten Schritt versucht, die Updates manuell auf die Netzwerkgeräte zu installieren.

```
c3850-1.border.g1.f2#de flash:cat3k_caa-universalk9.16.08.01a.SPA.bin
Destination filename [cat3k_caa-universalk9.16.08.01a.SPA.bin]?
Accessing https://10.22.0.100/api/v1/file/temporary/ec66b36e-c629-4f3c-a79d-d633573130de...
Loading https://10.22.0.100/api/v1/file/temporary/ec66b36e-c629-4f3c-a79d-d633573130de !!!!!!!!
!!!!!!!■
```

Abbildung 11.30: Firmwareupdate Switch via CLI HTTPS

Das Kopieren via HTTPS und SCP war sehr unzuverlässig und wurde nach einer gewissen Dauer abgebrochen.

```
c3850-1.border.g1.f2#copy tftp:cat3k_caa-universalk9.16.08.01a.SPA.bin flash:
Address or name of remote host [10.22.0.15]?
Source filename [cat3k_caa-universalk9.16.08.01a.SPA.bin]?
Destination filename [cat3k_caa-universalk9.16.08.01a.SPA.bin]?
Accessing tftp://10.22.0.15/cat3k_caa-universalk9.16.08.01a.SPA.bin...
Loading cat3k_caa-universalk9.16.08.01a.SPA.bin from 10.22.0.15 (via TenGigabitEthernet1/0/12): !
!!!!!!!■
```

Abbildung 11.31: Firmwareupdate Switch via CLI TFTP

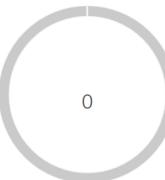
Mittels TFTP Server konnten die Devices schlussendlich erfolgreich aktualisiert werden.

11.11 Lizenzen

Die Lizenzen bezieht das DNA Center vom konfigurierten CCO Account.



Abbildung 11.32: Der Licence Manager ist über das Dashboard erreichbar.



Used DNA Licenses

⚠ Please configure your Cisco credentials to verify licensing compliance and view purchased licenses

[Configure CSSM](#)

Abbildung 11.33: Ohne verlinkten CSSM Account können keine Lizenzen zugewiesen werden.

Cisco Credentials

Cisco credentials are used for connecting to Cisco to verify access to software and services.

Cisco.com Credentials *

Username
laurent@nusystems.net

Password

Cisco.com connection check
 Cisco.com credentials check

Link your Smart Account *

Use Cisco.com user ID laurent@nusystems.net Use different credentials

Smart account connection check
 Smart account privilege check

Smart account credentials are incorrect or do not have access to the [Cisco software licensing account](#) for your organization. You can request a new smart account, request access to your organization Smart Licensing account, or enter credentials with the appropriate level of access.

[Retry](#)

Abbildung 11.34: Der im DNA Center hinterlegte Cisco Account muss Zugriff zum entsprechenden Smart Account haben.

Cisco Credentials

Cisco credentials are used for connecting to Cisco to verify access to software and services.

Cisco.com Credentials

Username	serge.pidoux
Password	***** 

Link your Smart Account 

Use Cisco.com user ID serge.pidoux Use different credentials

Abbildung 11.35: Der korrekt hinterlegte Account

 Filter	 Change DNA License	 Change Network License			
Device Name	Device Model	Device Type	DNA level	DNA License Expiry	License Mode
c9300.edge.g1.f2.local	Cisco Catalyst 9300 Series Switches	Switches and Hubs	Advantage	NA	RTU
c9300-1.edge.g2.f2.local	Cisco Catalyst 9300 Series Switches	Switches and Hubs	Advantage	NA	RTU
c9300-2.edge.g2.f2.local	Cisco Catalyst 9300 Series Switches	Switches and Hubs	Advantage	NA	RTU
c3850-1.edge.g1.f1.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	Advantage In-progress	Aug 9, 2018  90 Days	RTU
c3850.edge.g1.f2.local.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	In-progress	NA	RTU
c3850-1.border.g1.f2.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	In-progress	NA	RTU
c3850-1.inter.g1.f2.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	Advantage In-progress	Aug 9, 2018  90 Days	RTU
c3850-2.border.g1.f2.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	Advantage In-progress	July 31, 2018  81 Days	RTU
c3850-2.inter.g1.f2.local	Cisco Catalyst 3850 Series Ethernet Stackable Switch	Switches and Hubs	Advantage In-progress	Aug 9, 2018  90 Days	RTU

Abbildung 11.36: Übersicht über die den Netzwerkkomponenten zugewiesenen Lizenzen

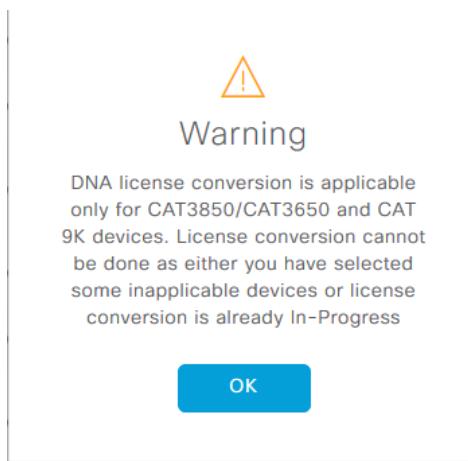


Abbildung 11.37: Nicht jedem Gerät kann eine Lizenz zugewiesen werden (Siehe Tabelle)

Geräteserie	Lizenzzuweisung möglich
Cisco Catalyst 9300 Series Switches	Ja
Cisco Catalyst 3850 Series Ethernet Stackable Switch	Ja
Cisco 4400 Series Integrated Services Routers	Nein

11.12 Device Provisioning via DNA Center

Um den einzelnen Netzwerkgeräten einen Namen und die Basis Konfiguration zu geben, werden im DNA Center unter *Provision → Devices* die zu provisioningierenden Geräte ausgewählt. Danach wird *Action → Provision Device* der Provision Vorgang gestartet. Dabei wird die komplette Konfiguration, die das DNA Center für ein Device vorsieht auf dem Gerät konfiguriert. Sind Templates für den entsprechende Devicetyp konfiguriert worden, werden diese ebenfalls angewendet. Templates können im Template Editor erstellt und entsprechenden Gerätetypen zugewiesen werden.

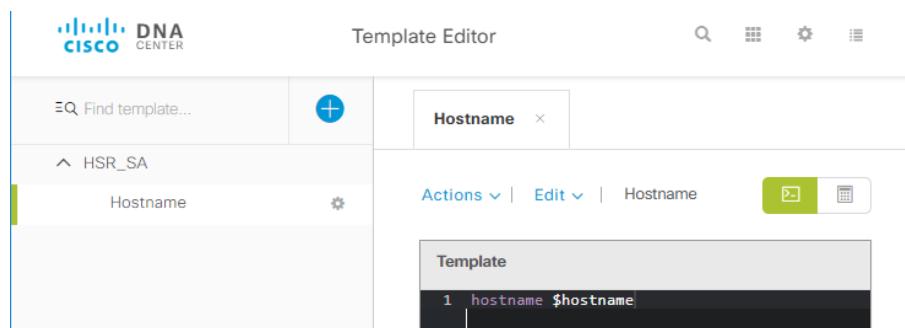


Abbildung 11.38: Template Editor

11.13 Fabric Konfigurieren

Nach der manuellen Konfiguration des Underlays, dem hinzufügen der Geräte, dem Update und dem Provisionieren, konnten wir endlich die Fabric konfigurieren.

Erreichbar ist das unter *Provision → Fabric*. Nachfolgend wird die Fabric des entsprechenden Standortes ausgewählt.

Den einzelnen Netzwerkgeräten werden nun mit Rechtsklick folgende Rollen zugeteilt:

- Border
- Border + CP (Control Plane)
- Edge

Nachdem alle Geräte der entsprechenden Fabric zugeteilt worden sind, kann die Konfiguration gespeichert werden und wird auf die Geräte geschrieben.

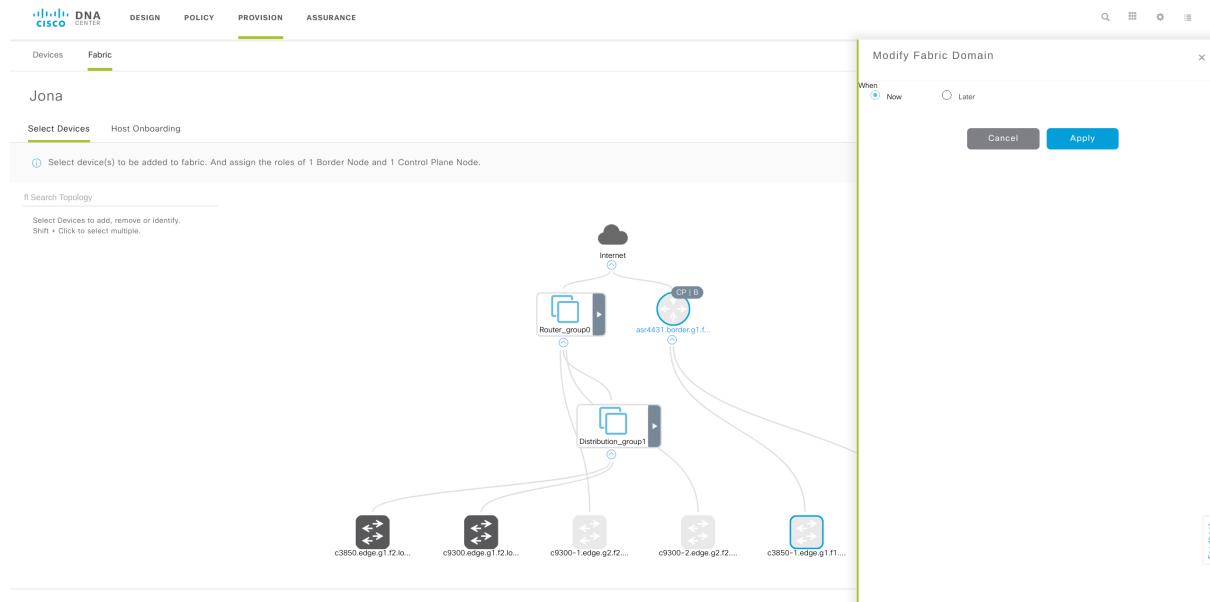


Abbildung 11.39: DNA Center Provision - Fabric - Nach der Zuteilung wird die Konfiguration auf die Geräte geschrieben.

Darstellung	Teil einer Fabric	Änderung ausstehend	Provisioniert	Bemerkung
Dunkelgrau	Ja	Nein	Nein	fremde Fabric
Hellgrau	Nein	Nein	Nein	
Grau mit blauem Rand	Ja	Ja	Nein	nicht deployed
Blau	Ja	Nein	Ja	aktuelle Fabric
Umrandung mit Pfeil	-	-	-	Gruppierte Geräte

Tabelle 11.2: DNA Center Provision - Fabric - Darstellung

11.14 DNA Center Reset

Da das Overlay Provisioning auch nach mehreren Versuchen nur teilweise funktioniert hatte, haben wir entschlossen, die Switches zusätzlich über das Out-of-Band Management zu verbinden, da dies in mehreren Videos von Cisco so erwähnt wird und im ersten Release zwingend nötig war.

Dazu benötigt das DNA Center ein zusätzliches Interface im Out-of-Band Management Netz. Um dieses einzurichten, muss der initiale Wizard erneut gestartet werden.

```
$ maglev-config-wizard #DO NOT EXECUTE THIS COMMAND
```

Als Folge dieses Befehls, nachdem alle Parameter eingegeben wurden, kam die folgende Meldung:



Abbildung 11.40: DNA Center - maglev-config-wizard - Fehlermeldung

Nach einem Neustart der Appliance erschien die folgende Meldung und das System bootete nicht mehr.

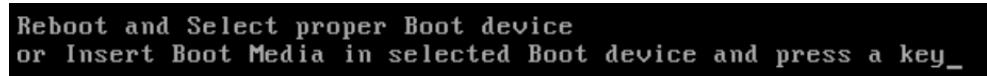


Abbildung 11.41: DNA Center - Boot Fehlermeldung

Es stellte sich heraus, dass wir den falschen Wizard gestartet hatten. Korrekt wäre der folgende Befehl gewesen:

```
$ sudo maglev-config update
```

Allerdings hätte auch der erste Befehl nicht dazu führen sollen, dass das System nicht mehr startet.

Neuinstallation

In der Folge war es nötig, dass DNA Center komplett neu zu installieren. Dazu ist ein entsprechendes ISO nötig, welches leider nicht mitgeliefert wird. Dieses kann bei Cisco via TAC Case angefordert werden. Mit dem ISO muss dann ein bootbarer USB Stick erstellt werden.

```
[kas@nbkas ~]$ ls -lah Downloads/DNAC-SW-1.1.4.iso
-rwxrwxr-x. 1 kas kas 11G May 17 09:36 Downloads/DNAC-SW-1.1.4.iso
[kas@nbkas ~]$ sudo dd if=Downloads/DNAC-SW-1.1.4.iso of=/dev/sda bs=4M status=p
rogress
[sudo] password for kas:
3212836864 bytes (3.2 GB, 3.0 GiB) copied, 265.085 s, 12.1 MB/s
```

Abbildung 11.42: DNA Center - Neuinstallation - Installations ISO wird auf USB Drive kopiert

Anschliessend kann der USB-Stick in die Appliance gesteckt und diese gestartet werden. Die initiale Installation ist in Abschnitt 11.1.1 gezeigt.

Nach der Neuinstallation sind alle Daten und die Konfiguration gelöscht. Eine Option die Konfiguration beizubehalten gibt es nicht.

12 Vorgehen Versuch 2

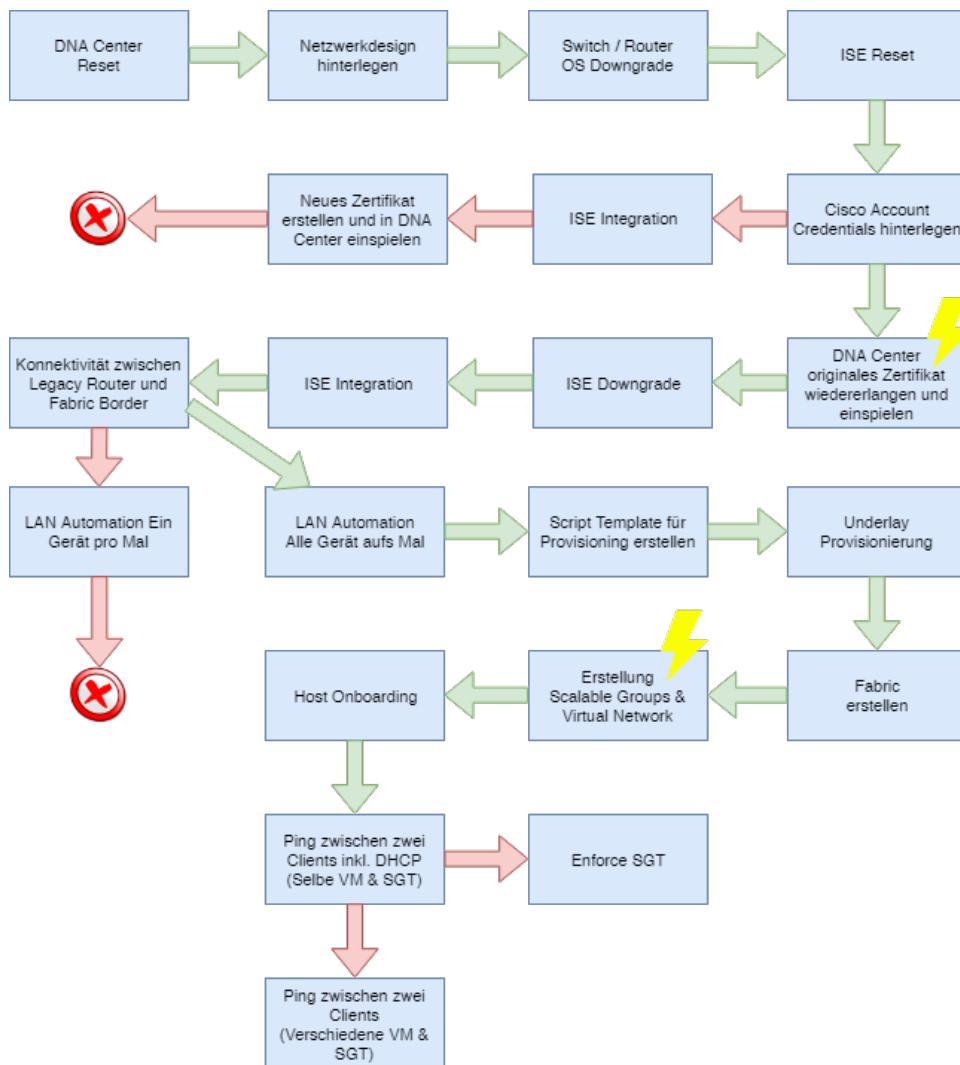


Abbildung 12.1: Grafische Übersicht über das Vorgehen beim zweiten Versuch

12.1 Vorarbeiten

Damit im zweiten Versuch keine Probleme mit bestehenden Konfigurationen entstehen, haben wir alle Konfigurationen in Infoblox gelöscht und ISE auf den Werkszustand zurückgesetzt.

Des Weiteren wurde auf allen Netzwerkdevices die IOS-XE Version 16.6.3 installiert, da gemäss Patrick Mosimann von Cisco nur diese Version mit dem aktuellen DNA Center kompatibel ist.

12.1.1 ISE reset

Um die Störungen durch alte Konfigurationen zu vermeiden, wurde das Cisco ISE Center ebenfalls zurückgesetzt. Dies kann einfach mittels eines Befehls durchgeführt werden.

```
ISE/admin# application reset-config ise
```

```
ISE/admin# application reset-config ise figured as
Initialize your Application configuration to factory defaults? (y/n): y
Leaving currently connected AD domains if any...
Please rejoin to AD domains from the administrative GUI
Retain existing Application server certificates? (y/n): y
Reinitializing local configuration to factory defaults...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping PassiveID WMI Service...
Stopping PassiveID Syslog Service...
Stopping PassiveID API Service...
Stopping PassiveID Agent Service...
Stopping PassiveID Endpoint Service...
Stopping PassiveID SPAN Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
Stopping ISE Sxp Engine Service...
Stopping TC-NAC Service ...
Error: No such container: irf-core-engine-runtime
irf-core-engine-runtime is not running
```

Abbildung 12.2: Cisco ISE Reset

12.2 DNA Center Update

Wie im ersten Versuch, haben wir das DNA Center nach der Installation auf den aktuellsten Stand geupdated. Dieser Vorgang wurde im Abschnitt 11.2 gezeigt. Dies war mittlerweile die Version 1.1.6. Im ersten Versuch arbeiteten wir mit den Versionen 1.1.4 und 1.1.5.

12.3 DNA Center Netzwerk Design

Das Netzwerkdesign wurde analog unserem ersten Versuch in Abschnitt 11.3 erstellt.

12.4 ISE Integration

Bei der Integration des ISE wollten wir gleich vorgehen, wie im ersten Versuch. Es stellt sich aber heraus, dass im Release 1.1.6 in Kombination mit ISE 2.4 geprüft wird, ob das DNA Center über ein Zertifikat verfügt, das den Hostname oder die IP des DNA Centers im Common Name hat. Aus diesem Grund haben wir das Zertifikat des DNA Centers durch eines ersetzt, dass diese Bedingung erfüllt.

Before You Begin

Before attempting to integrate ISE with Cisco DNA Center, be sure you have met the following pre-requisites:

- You have deployed one or more ISE version 2.3 hosts on your network. If you have a multi-host ISE deployment, integrating with the ISE admin node is recommended.

For information on installing ISE, see the [Cisco Identity Services Engine Installation Guide, Release 2.3](#).

- The PxGrid service must be enabled on the ISE host with which you plan to integrate DNA Center. The procedure below explains how to enable this service.
- The ISE admin node on which PxGrid is enabled must be reachable on the IP address of the eth0 interface of ISE from DNA Center.
- The ISE node can reach the fabric underlay network via the appliance NIC.
- The ISE node has SSH enabled
- The ISE CLI and GUI user accounts must use the same username and password
- The ISE admin node certificate must contain the ISE IP address or fully-qualified domain name (FQDN) in either the certificate subject name or the SAN.
- The DNA Center system certificate must contain the DNA Center appliance IP or FQDN in either the certificate subject name or the SAN.

Abbildung 12.3: ISE Integration Prerequisites

[8]

Das Zertifikat kann unter *Settings* → *Settings* → *Certificate* → *Replace Certificate* ausgetauscht werden. Es ist möglich Zertifikate im PEM Format oder als PKCS Datei hochzuladen.

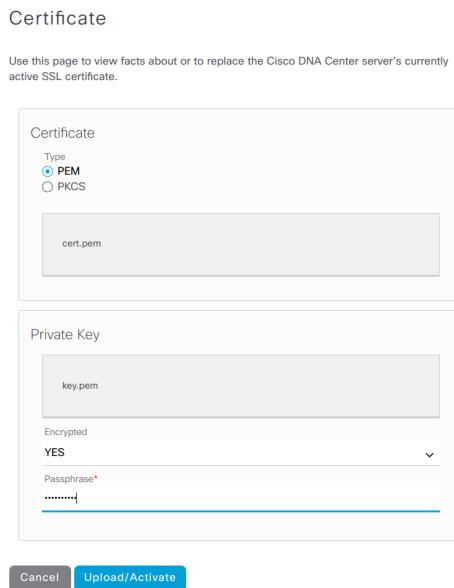


Abbildung 12.4: DNA Center Certificate Replacement

Nachdem das Zertifikat durch ein self-signed Zertifikat ausgetauscht wurde, welches die Bedingung erfüllt, dass die IP oder der Hostname im Common Name sein muss, funktionierte die ISE Integration ohne weitere Probleme.

12.5 LAN Automation

Bevor die LAN Automation gestartet werden kann, müssen folgende Bedingungen für das Seed Device erfüllt sein:

- Aktives SSH
- IP Konnektivität

12.5.1 Verbindung zwischen Legacy Router und Border Switch

Damit die LAN Automation gestartet werden kann, muss zuerst ein Seed Device eingerichtet werden, dass vom DNA Center aus erreichbar ist. Dies kann mit untenstehenden Befehlen über ein temporäres VLAN erreicht werden.

```
# interface lo0
#   ip address 10.22.30.1 255.255.255.255
#
# interface Te1/0/12
#   switchport trunk native vlan 100
#   switchport mode trunk
#
# interface vlan 100
#   ip address 10.22.31.1 255.255.255.252
```

```
#  
# ip route 10.22.0.0 255.255.255.0 10.22.31.2
```

```
# interface GigabitEthernet0/0/1.100  
# encapsulation dot1Q 100  
# ip address 10.22.31.2 255.255.255.252  
#  
# ip route 10.22.30.1 255.255.255.255 10.22.31.1
```

12.5.2 Discovery

Da der oben konfigurierte Border Router als Seed Device genutzt werden soll um die restlichen Geräte zu finden und zu deployen, muss dieses im DNA Center bekannt gemacht werden. Am einfachsten geht dies über die Discovery Funktion. Diese kann mittels *Discovery → New Discovery* eingerichtet werden. Die Discovery kann gemäss untenstehender Grafik konfiguriert werden.

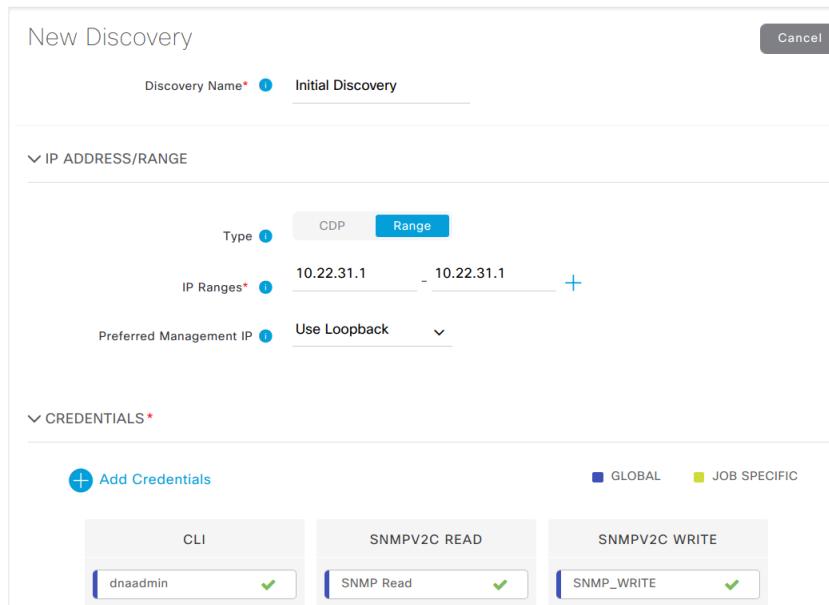


Abbildung 12.5: DNA Center Discovery

Sobald das Device gefunden wurde, erscheint dieses im Inventory. Damit dieses als Seed Device verwendet werden kann, ist zuerst ein Provisioning wie in 11.12 beschrieben nötig und das Device muss einer Fabric hinzugefügt werden 11.13.

Beim Provisioning ist aber aufgefallen, dass es Probleme mit der Verbindung zwischen dem Border Switch und dem ISE gibt. Patrick Mosimann hat uns dann erklärt, dass das DNA Center in den aktuell verfügbaren Versionen ausschliesslich mit ISE in der Version 2.3 kompatibel ist.

Unglücklicherweise war in unserer Lab Umgebung die Version 2.4 installiert. Ein Downgrade ist leider nicht möglich, weshalb die virtuelle Maschine ausgetauscht werden musste und der ISE erneut ins DNA Center integriert werden musste.

12.6 LAN Automation PnP

Nun konnte die eigentliche LAN Automation gestartet werden. Dabei wird, wie in untenstehender Grafik gezeigt ein Seed Device ausgewählt und definiert, auf welchen Interfaces DHCP Requests der anderen Devices beantwortet werden. Zudem muss ein IP Pool angegeben werden, der für folgende Zwecke verwendet wird:

- DHCP Pool während dem PnP Vorgang
- Loopback Interfaces der Devices
- Netze für Point to Point Links

Dabei ist zu beachten, dass die Unterteilung des IP Pools nicht optimal ist. Unabhängig von der Grösse des Pools werden beispielsweise nur 30 Adressen für den DHCP Pool reserviert, was in einer grossen Umgebung ein Problem darstellen könnte.

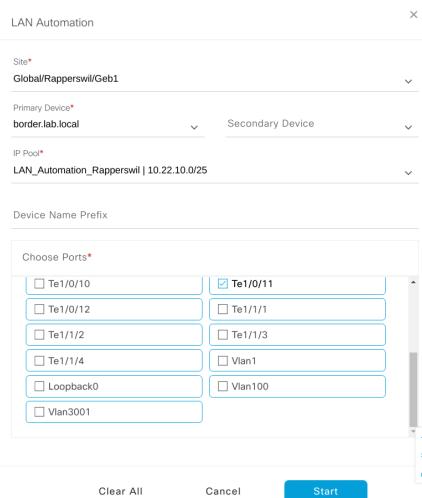


Abbildung 12.6: DNA Center - LAN Automation

Wir haben dann die LAN Automation gestartet. Dies konfiguriert auf dem Seed Device einen DHCP Server. Werden nun die Konfiguration auf anderen Netzwerkgeräten gelöscht und diese neu gestartet, senden diese DHCP Request, die vom Seed Device beantwortet werden. Die Antworten verweisen auf das DNA Center als PnP Server. Die Geräte senden nur DHCP Requests, wenn Sie im Zustand sind, der auf untenstehendem Bild ersichtlich ist.

```
Would you like to enter the initial configuration dialog? [yes/no]: |
```

Abbildung 12.7: Cisco Switch - Initial Config - Versucht DHCP und PnP zu machen, solange der Dialog aktiv ist.

Während des PnP Prozesses wird das Zertifikat, sowie die CA (Certificate Authority) des DNA Centers auf die Netzwerkgeräte kopiert. Dies ist nötig, damit die Verbindung auf HTTPS umgestellt werden kann. Nach diesem Schritt blieb der Setup Prozess jeweils mit folgender Meldung stehen:

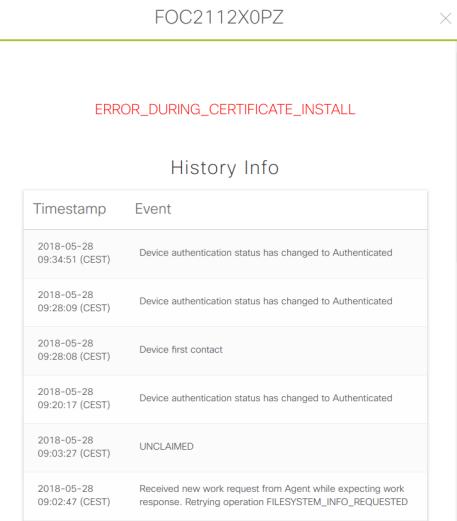


Abbildung 12.8: LAN Automation - PnP Error

Es stellte sich heraus, dass das Problem war, dass unser self-signed Zertifikat nicht von der DNA Center CA signiert war und die Netzwerkgeräte daher nicht validieren konnten ob dieses gültig ist. Leider konnte uns auch Patrick Mosimann von Cisco nicht sagen, wie wir dieses Zertifikat signieren können, das ursprüngliche Zertifikat wiederherstellen können oder das Problem anderweitig lösen können. Gemäss dem Installation Guide von Cisco [8] kann hier auch ein Zertifikat verwendet werden, dass von einer "Well-Known Certificate Authority" signiert ist. Aus diesem Grund haben wir das Zertifikat auch durch ein korrekt von Lets Encrypt signiertes Zertifikat ausgetauscht. Patrick konnte uns aber nicht sagen, ob diese Authority auf dem Gerät bekannt ist. Auch das korrekt signierte Zertifikat wurde nicht akzeptiert und der PnP Prozess konnte nicht weitergeführt werden. Aus diesem Grund haben wir uns via SSH auf die Appliance eingelogged und dort nach dem ursprünglichen Zertifikat oder der CA gesucht. Nach einer Weile wurden wir fündig und fanden das alte Zertifikat und die CA:

```
# $ sudo ls -lah /etc/maglev/.pki/
# [sudo] password for maglev:
# total 140K
# drwxr-xr-x 2 root 4.0K May 21 06:20 .
# drwxr-xr-x 4 root 4.0K May 21 06:20 ..
# -rw-r--r-- 1 root 1.3K May 17 09:09 apiserver.crt
# -rw----- 1 root 1.7K May 17 09:09 apiserver.key
# -rw-r--r-- 1 root 1.2K May 17 09:09 apiserver-kubelet-client.crt
# -rw----- 1 root 1.7K May 17 09:09 apiserver-kubelet-client.key
# -r--r--r-- 1 root 1.1K May 17 08:49 ca.crt
# -rw-r--r-- 1 root 1.7K May 17 08:49 ca.key
# lrwxrwxrwx 1 root 23 May 17 08:49 ca-key.pem -> /etc/maglev/.pki/ca.crt
# lrwxrwxrwx 1 root 23 May 17 09:09 ca.pem -> /etc/maglev/.pki/ca.crt
# -r----- 1 root 1.7K May 17 08:49 credentialmanager-key.pem
# -r----- 1 root 307 May 21 06:20 credentialmanager-openssl.cnf
# -r--r--r-- 1 root 1.1K May 17 08:49 credentialmanager.pem
# -r----- 1 root 1.7K May 17 08:49 encryptionmanager-key.pem
# -r----- 1 root 307 May 21 06:20 encryptionmanager-openssl.cnf
```

```
# -r--r--r  1 root 1.1K May 17 08:49 encryptionmanager.pem
# -r----- 1 root 1.7K May 17 08:49 encryption_seed-key.pem
# -r--r--r  1 root 981 May 17 08:49 encryption_seed.pem
# -rw-r--r  1 root 1.1K May 17 09:09 front-proxy-ca.crt
# -rw----- 1 root 1.7K May 17 09:09 front-proxy-ca.key
# -rw-r--r  1 root 1.1K May 17 09:09 front-proxy-client.crt
# -rw----- 1 root 1.7K May 17 09:09 front-proxy-client.key
# -r----- 1 root 1.7K May 17 08:49 kong-key.pem
# -r----- 1 root 299 May 21 06:20 kong-openssl.cnf
# -r--r--r  1 root 1.1K May 17 08:49 kong.pem
# -r----- 1 root 1.7K May 17 08:49 kube-admin-key.pem
# -r--r--r  1 root 977 May 17 08:49 kube-admin.pem
# -r----- 1 root 1.7K May 17 08:49 kube-worker-1-key.pem
# -r----- 1 root 336 May 21 06:20 kube-worker-1-openssl.cnf
# -r--r--r  1 root 1.1K May 17 08:49 kube-worker-1.pem
# -r----- 1 root 1.7K May 17 08:49 maglev-registry-key.pem
# -r----- 1 root 472 May 21 06:20 maglev-registry-openssl.cnf
# -r--r--r  1 root 1.3K May 17 08:49 maglev-registry.pem
# -r----- 1 root 36 May 17 08:49 passphrase.txt
# -rw-r--r  1 root 1.1K May 21 06:20 registry-ca.pem
# -rw----- 1 root 1.7K May 17 09:09 sa.key
# -rw----- 1 root 451 May 17 09:09 sa.pub
```

So konnten wir das alte Zertifikat wiederherstellen (sh. 12.4). Dies war kein Problem, da mit ISE Version 2.3 der Hostname und die IP nicht im Common Name sein müssen. Es wäre aber auch möglich gewesen, mit der CA ein neues zu signieren, da die Passphrase für den Private Key der CA in einem Textfile abgelegt ist.

Durch das erneute des Zertifikats wurde leider die Trust Verbindung zum ISE gebrochen, weshalb der ISE erneut ins DNA Center integriert werden musste.

Nun konnten wir die LAN Automation starten und der PnP Prozess auf den Netzwerkgeräten schien zu funktionieren.

Wir haben dann, wie von Patrick Mosimann vorgeschlagen, die ersten zwei Devices am Standort Rapperswil mit der LAN Automation konfiguriert, was einwandfrei funktioniert hat. Damit die Konfiguration auf die Geräte geschrieben wird, muss die LAN Automation beendet werden. Anschliessend wiederholten wir diesen Vorgang für die nächsten zwei Geräte. Dabei stellte sich heraus, dass die generierte Konfiguration unbrauchbar ist, da nur einzelne Point to Point Links konfiguriert wurden, aber nicht alle die nötig gewesen wären.

Da es sich bei der LAN Automation um ein Basisfeature handelt, wollten wir die Underlay Konfiguration nicht manuell erstellen und versuchten die Ursache für diesen Fehler zu finden. Schlussendlich hat uns folgendes Vorgehen zum Erfolg geführt:

- LAN Automation starten
- Ein Gerät nach dem anderen via PnP aufsetzen

Wenn mehrere Geräte gleichzeitig konfiguriert werden, bricht PnP meistens ab

- Erst wenn alle Devices via PnP aufgesetzt sind, die LAN Automation stoppen

So wurden alle Konfigurationen korrekt erstellt und der Underlay mit ISIS war korrekt konfiguriert. Ebenfalls waren nun alle Geräte im Inventory sichtbar.

Dieses Vorgehen verhindert aber natürlich das Hinzufügen weiterer Geräte zu einem

späteren Zeitpunkt, da damit zu rechnen ist, dass es wieder zu Problemen kommt, wenn für denselben Underlay erneut eine LAN Automation gestartet wird.

12.7 Provisioning

12.7.1 Templates

Damit der Hostname der Switches und Router via Provisioning gesetzt werden kann, muss ein Template angelegt werden.

Über das Hauptmenü *Tools* → *Template Editor* kann mit *Add (Pluszeichen)* → *Create Project* ein neues Projekt anlegt werden. (Siehe: 12.9)

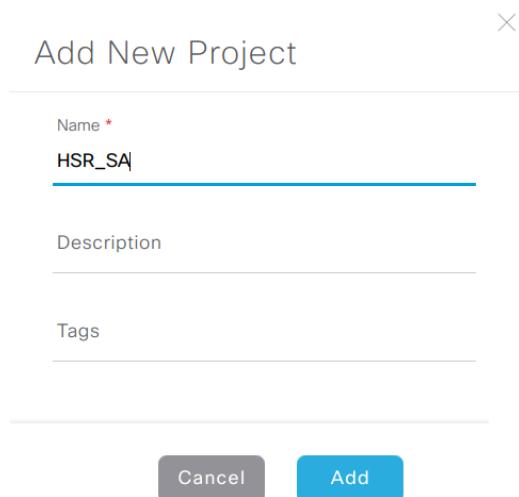


Abbildung 12.9: DNA Center - Templateeditor - Add Project

Weiter kann mit *Add (Pluszeichen)* → *Add Template* ein neues Template angelegt werden. (Siehe 12.10)

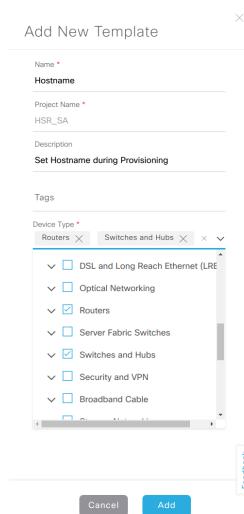


Abbildung 12.10: DNA Center - Templateeditor - Add Template

Wie in Abbilung 12.10 sind folgende Einstellungen festzulegen:

- Name des Templates
- Zugehörige Projekt
- Beschreibung
- Tags
- Für welche *Device Types* das Template verwendet werden soll.

Anschliessend wurde das Template befüllt. Hier kann die Script Sprache "velocity" verwendet werden. Da wir aber nur den Hostnamen setzen wollten, reicht das CLI Kommando und eine entsprechende Variable.

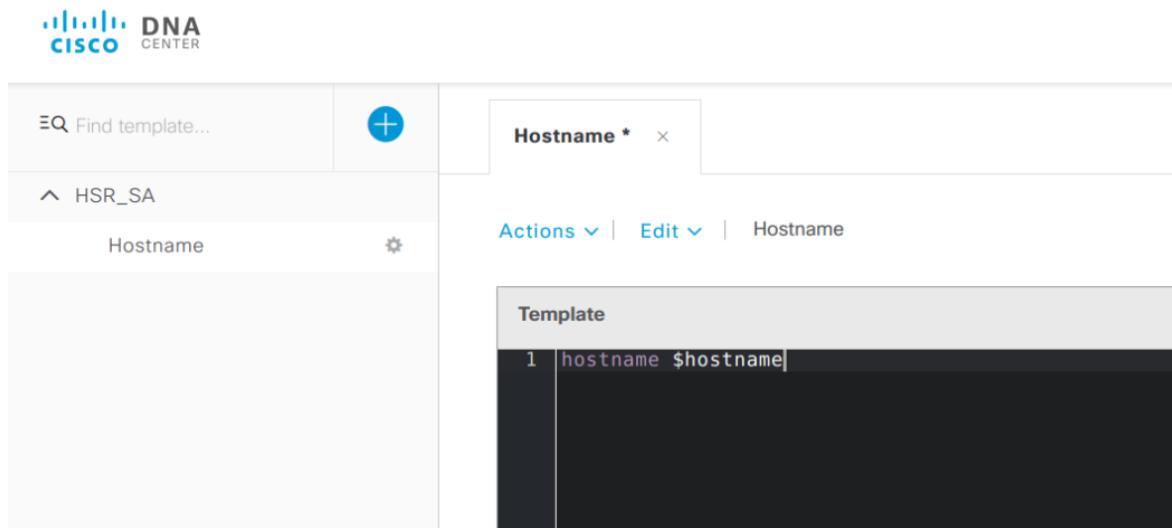


Abbildung 12.11: DNA Center - Templateeditor - Template um den Hostname bei der Provisionierung zu setzen.

12.7.2 Network Profile anlegen

Unter *Design* → *Network Profiles* → *Add Profile* konnte ein neues Profil angelegt werden. Dieses Profil wird während des Provisionierungsvorgang verwendet. Das Profil stellt das Bindeglied zwischen Site, Device Type, und Template dar.

The screenshot shows the 'Add a Network Profile' form. On the left, there are fields for 'Profile Name*' (with 'Default Switching Profile' selected) and 'Profile Type' (set to 'switching'). On the right, there's a table titled 'Attach Template(s)' with columns 'Device Type', 'Template', and 'Template'. Under 'Device Type', 'Switches and Hubs' is listed. Under 'Template', there's a row for 'Hostname'. At the bottom of the table, a note says 'Don't see the template you need? Create a new template in [Template Programmer](#)'.

Abbildung 12.12: Cisco DNA Center - Network Profile - New Profile

Weiter wird festgelegt für welche *Sites* das Netzwerkprofil verwendet werden soll.

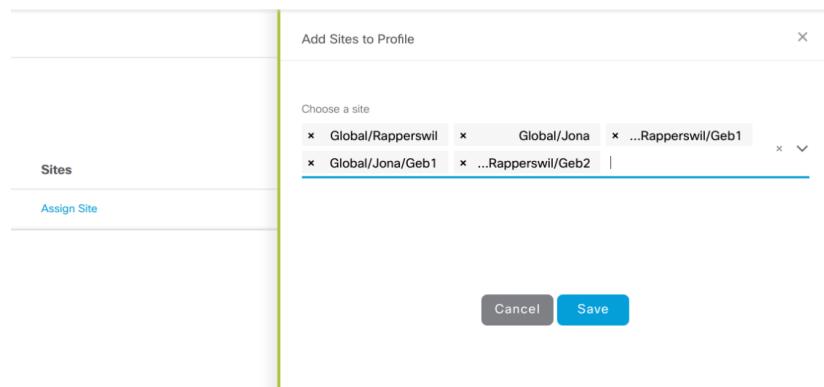


Abbildung 12.13: Cisco DNA Center - Network Profile - Assign Sites

12.7.3 Initial Provisioning

Nun kann ein initiales Provisioning der neuen Netzwerkgeräte durchgeführt werden. Dies ist im Modul *Provision* → *Devices* → *Inventory* zu finden. Das zu provisionierende Gerät wird in der Liste ausgewählt. Über *Action* → *Provision* wird das Provisioning gestartet.

Abbildung 12.14: Cisco DNA Center - Device Provisioning

Es folgt ein Wizard, der durch das Provisioning führt. Im ersten Schritt (Siehe: 12.15) wird die entsprechende *Site* ausgewählt.

Abbildung 12.15: Cisco DNA Center - Provision Step 1

Im zweiten Schritt gibt es keine wählbaren Optionen.

Im dritten Schritt kann das im Abschnitt 12.7.1 definierte Template ausgefüllt werden. Die Variablen (im Falle 12.16), in unserem Fall der Hostname des Geräts mussten angegeben werden.

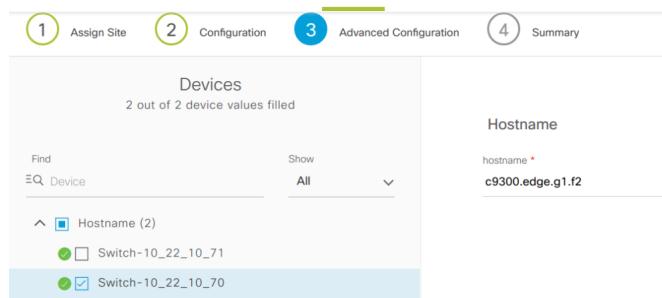


Abbildung 12.16: Cisco DNA Center - Provision Step 3

Im letzte Schritt erscheint eine Übersicht. Mit einem Klick auf *Deploy* wird das Device provisioniert. Die dabei automatisch ausgeführten Befehle durch das DNA Center sind in Listing 1 ersichtlich.

Listing 1: Befehle automatisch ausgeführt durch das DNA Center während der Provisionierung

```

enable
no ip domain-lookup
ip access-list extended ACL_WEAUTH_REDIRECT
180 permit tcp any any eq www
190 permit tcp any any eq 443
200 permit tcp any any eq 8443
210 permit udp any any eq domain
220 permit udp any eq bootpc any eq bootps
170 deny ip any host 10.22.0.22
exit
ip tacacs source-interface Loopback0
ip radius source-interface Loopback0
aaa new-model
ip radius source-interface Loopback 0
exit
aaa group server radius dnac-network-radius-group
server name dnac-radius_10.22.0.22
ip radius source-interface Loopback 0
exit
aaa accounting dot1x default start-stop group dnac-client-radius-group
aaa accounting update newinfo periodic 600
aaa accounting exec default start-stop group dnac-network-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa authorization exec VTY_author group dnac-network-radius-group local if-
aaa authorization exec VTY_author group dnac-network-radius-group local
aaa authentication login default local
aaa authentication dot1x default group dnac-client-radius-group
aaa authentication login VTY_authen group dnac-network-radius-group local
dot1x system-auth-control
radius server dnac-radius_10.22.0.22
address ipv4 10.22.0.22 auth-port 1812 acct-port 1813
pac key *
```

```

retransmit 1
radius-server deadtime 30
radius-server attribute 25 access-request include
radius-server attribute 8 include-in-access-req
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
cts authorization list dnac-cts-list
line vty 0 97
login authentication VTY_authen
authorization exec VTY_author
transport input all
banner motd #\i"Welcome to our SA Lab!"#
hostname c9300-2.edge.g2.f2

```

12.7.4 Geräte zur Fabric hinzufügen

TODO

Listing 2: Befehle automatisch ausgeführt durch das DNA Center während dem hinzufügen zur Fabric

```

!exec: enable
ip dhcp snooping
cts role-based enforcement
vrf definition DEFAULT_VN
address-family ipv4
vlan 4000
name VOICE_VLAN
exit
vlan 3999
name CRITICAL_VLAN
exit
interface GigabitEthernet1/0/3
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/4
no load-interval
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/7
no load-interval

```

```
no spanning-tree portfast
no switchport trunk native vlan
switchport
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/10
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
interface GigabitEthernet1/0/12
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/13
no load-interval
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/15
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/18
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/21
no load-interval
no spanning-tree portfast
```

```
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
switchport access vlan 1
exit
router lisp
ipv4 source-locator Loopback0
locator-set rloc_def9f1a7-9572-4e74-afaf-44215f0fbde
IPv4-interface Loopback0 priority 10 weight 10
exit
locator-table default
locator default-set rloc_def9f1a7-9572-4e74-afaf-44215f0fbde
service ipv4
etr map-server 10.22.10.67 proxy-reply
etr
sgt
use-petr 10.22.10.67
use-petr 10.22.30.1
exit
service ethernet
database-mapping limit dynamic 5000
map-cache-limit 25000
itr map-resolver 10.22.30.1
ipv4 locator reachability exclude-default
ip dhcp relay information option
banner motd #\"Welcome to our SA Lab!\"#
ip sla 1
icmp-echo 10.22.0.22 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 1 life forever start-time now
banner motd #\"Welcome to our SA Lab!\"#
ip sla 2
icmp-echo 10.22.10.67 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 2 life forever start-time now
banner motd #\"Welcome to our SA Lab!\"#
ip sla 3
icmp-echo 10.22.30.1 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 3 life forever start-time now
```

```
banner motd #\"Welcome to our SA Lab!\\"#
```

12.7.5 Border BGP

TODO

12.7.6 IP Pools definieren

TODO Infoblox vorgehen bei neuem Netzwerk!!!

12.7.7 Host Onboarding

TODO

12.7.8 Authentifizierungsmethoden

Type	Description
Closed Authentication	Based on 802.1X. Authentication MUST succeed prior to network access. Requires networks with complete 802.1x support.
Open Authentication	Based on 802.1x. Temporary access is granted (e.g. PXE, DHCP) prior to authentication. Optimal for networks with limited 802.1x support.
Easy Connect	Based on LDAP combined with MAC Address Bypass (MAB). Optimal for networks using Active Directory (AD) authentication.
No Authentication	Optimal for networks that do not support authentication or require static configuration.

Tabelle 12.1: Erklärung der Host Onboardning Authentifizierungsmethoden.[17]

13 Ergebnisdiskussion

Stärken und Schwächen der Konzepte, Verbesserungen für die Zielgruppe im Kontext

14 Schlussfolgerungen

Zusammenfassung und Ausblick

14.1 Erreichte Ziele

Erreichte Ziele im Bezug auf Aufgabenstellung

14.2 Mögliche Verbesserungen

Was könnte man am erreichten verbessern?

14.3 Zukunft

Ausbaumöglichkeiten

15 Abkürzungsverzeichnis

AAA	authentication, authorization, and accounting
ACL	access control list
AP	access point
BGP	border gateway protocol
CAPWAP	control and provisioning of wireless access points protocol
CCO	Cisco Connection On-line
CMD	Cisco Meta Data
DNA	Cisco Digital Network Architecture
EID	endpoint identifier
HTDB	host tracking database
IGP	interior gateway protocol
IPAM	IP-Adress-Management
ISE	Cisco Identity Services Engine
LAN	Local Area Network
LISP	Locator/ID Separation Protocol
MR	Map Resolver
MS	Map Server
MTU	maximum transmission unit
PnP	Plug and Play
RLOC	routing locator
SDA	Software-Defined Access
SGACL	scalable group access control list
SGT	scalable group tag
SXP	scalable group tag exchange protocol
VLAN	virtual local area network
VN	virtual network
VNI	virtual extensible LAN network identifier
VRF	virtual routing and forwarding

VTEP virtual extensible LAN tunnel endpoint

VXLAN virtual extensible LAN

IPAM IP Address Manager

A Installationsanleitung

A.1 DNA Center Setup

A.1.1 DNA Center Reset

A.2 DNA Center Network Discovery

Um die Netzwerkkomponenten zum DNA Center hinzuzufügen, wurde mehrere Versuche unternommen.

B Benutzerhandbuch

B.1 Updates

Es ist wichtig das DNA Center auf einem aktuellen Stand zu halten, da es noch eher in einem frühen Release steckt.

Auf folgender Webseite veröffentlicht Cisco die Sicherheitslücken und erklärt gleich zu welcher Version das DNA Center geupdatet werden muss:

<https://tools.cisco.com/security/center/publicationListing.x?resourceIDs=233151&apply=1&totalbox=terByProduct>

B.2 Access Control Policies

Virtual Network Virtuelle Netzwerke sind isolierte Routing- und Switching-Umgebungen. Standardmäßig können Hosts die in separaten virtuellen Netzwerken existieren nicht miteinander kommunizieren. Mit Hilfe von virtuellen Netzwerken kann das physische Netzwerk in mehrere logische Netzwerk geteilt werden. Ein typischer Anwendungsfall ist die Segmentierung von Gästen, Mitarbeitern und Kontraktor in getrennte Gruppen, so dass der Zugriff nur auf Teile des Netzwerkes erlaubt oder eingeschränkt werden kann. Die verschiedenen Arten von Netzwerken sind:

- **Gast-Netzwerk:** Netzwerkverbindungen, die von einem Unternehmen zur Verfügung gestellt werden, um seinen Gästen den Zugang zum Internet und zum eigenen Unternehmen zu ermöglichen, ohne die Sicherheit des Host-Unternehmensnetzwerks zu beeinträchtigen. Gäste können auf das Internet zugreifen, aber nicht auf interne Anwendungen, die im Rechenzentrum gehostet werden.
- **Mitarbeiter-Netzwerk:** Netzwerkverbindungen, die den Zugriff auf das Internet und interne Anwendungen ermöglichen. Diese Gruppe kann weiter segmentiert werden, um z.B. den Zugriff innerhalb des Unternehmensnetzwerks zu ermöglichen oder einzuschränken, für bestimmte interne Anwendungen, Laborumgebungen und Server. Ein Finanzangestellter z.B. braucht keinen Zugang zum Entwicklungslabor. Ebenso benötigt ein Entwickler keinen Zugriff auf eine Verkaufsprognose. Diese können ohne Probleme in weitere virtuelle Netzwerke segmentiert werden.
- **Kontraktor-Netzwerk:** Netzwerkverbindung, die es den Benutzern ermöglicht, auf das Internet und auf unternehmensspezifische Anwendungen innerhalb des Unternehmensnetzwerks zuzugreifen. Ein virtuelles Netzwerk kann sich über mehrere Standorte und Netzwerkdomänen (Wireless, Campus und WAN) erstrecken.

Scalable Group Skalierbare Gruppen umfassen eine Gruppierung von Benutzern, Endgeräten oder Ressourcen, die dieselben Anforderungen an die Zugriffskontrolle stellen. Diese Gruppen (in Cisco ISE als Sicherheitsgruppen oder SGs bekannt) werden auf dem Cisco ISE definiert. Eine skalierbare Gruppe kann nur ein Element (ein Benutzer, ein Endgerät oder eine Ressource) enthalten.

Access Control Contract Ein Zugriffsvertrag ist eine Security Group Access Control List (SGACL). Sie definiert das Regelwerk, dass die Netzwerkinteraktion zwischen Quelle und Ziel in einer Zugriffskontrollrichtlinie regelt.

Group-based Access Control Policy Gruppenbasierte Zugriffskontrollrichtlinien sind Security Group Access Control Lists (SGACLs). DNA Center hat den Cisco ISE integriert, um den Prozess der Erstellung und Pflege von SGACLs zu vereinfachen. Während der initialen Integration von DNA Center und Cisco ISE werden skalierbare Gruppen und Richtlinien, die in Cisco ISE vorhanden sind, an das DNA Center weitergegeben und in das standardmäßige virtuelle Netzwerk eingefügt.

Das folgende Beispiel zeigt den Prozess der Authentifizierung und Zugriffskontrolle, den ein Benutzer durchläuft, wenn er sich in das Netzwerk einloggt:

1. Ein Benutzer verbindet sich mit einem Port auf einem Switch und stellt seine Zugangsdaten zur Verfügung.
2. Der Switch kontaktiert Cisco ISE.
3. Cisco ISE authentifiziert den Benutzer und lädt die SGACLs auf den Port, mit dem der Benutzer verbunden ist.
4. Dem Benutzer wird der Zugang zu bestimmten Benutzern oder Geräten (Servern) auf der Grundlage des in die SGACL gewährt.

B.2.1 Workflow

Workflow zur Konfiguration einer gruppenbasierten Zugriffskontrollrichtlinie.

Schritt	Aktion	Zweck
1	Erstellen eines virtuellen Netzwerkes. Abhängig von der Konfiguration des Unternehmens und seinen Zugriffsanforderungen und -beschränkungen können die Gruppen in verschiedene virtuelle Netzwerke unterteilt werden, um eine weitere Segmentierung zu ermöglichen.	(Optional)
2	Erstellen einer skalierbaren Gruppe. Nach der Integration von Cisco ISE werden die in ISE vorhandenen skalierbaren Gruppen in das DNA Center übertragen. Wenn eine skalierbare Gruppe nicht besteht, kann diese direkt angelegt werden.	(Optional)
3	Erstellen eines Zugriffskontrollvertrag (access control contract). Ein Contract definiert eine Reihe von Regeln, die eine Aktion (erlauben oder verweigern), die Netzwerkgeräte basierend auf dem Datenverkehr durchführen, der bestimmten Protokollen oder Ports entspricht.	
4	Erstellen einer gruppenbasierten Zugriffskontrollrichtlinie (group-based access control policy). Die Zugriffskontrollrichtlinie definiert den Zugriffskontrollvertrag, der den Verkehr zwischen den skalierbaren Quell- und Zielgruppen regelt.	

Tabelle B.1: Workflow zur Erstellung der Access Control Policies

B.2.2 Erstellen eines virtuellen Netzwerkes

1. Wähle auf der DNA Center Homepage **Policy / Virtual Network**.

2. Klicke auf den **Add Button** und fülle die erforderlichen Informationen aus.
3. Klicke **Save**.

B.2.3 Erstellen einer Skalierbaren Gruppe

1. Wähle auf der DNA Center Homepage **Policy / Registry / Scalable Groups**. Alle skalierbaren Gruppen, die auf dem Cisco ISE erstellt wurden, erscheinen in der Registry.
2. Klick **Add**. DNA Center öffnet eine direkte Verbindung zum Cisco ISE Server, wo die skalierbaren Gruppen hinzugefügt werden können.
3. Erstelle in Cisco ISE skalierbare Gruppen (in Cisco ISE Sicherheitsgruppen genannt).
4. Gehe zum DNA Center zurück. Nun sollte die erstellte skalierbare Gruppe angezeigt werden.

B.3 Erstellen eines Zugriffskontrollvertrages

1. Wähle auf der DNA Center Homepage **Policy / Contracts / Access Contracts**.
2. Klick **Add Contract**.
3. Im Dialogfenster des **Contract Editor** kann ein Name und eine Beschreibung für den Vertrag erfasst werden.
4. Wähle in der Dropdown-Liste **Implicit Action** entweder **Deny** oder **Permit**.
5. Wähle aus der Dropdown-Liste in der Spalte **Port/Protocol** einen Port oder ein Protokoll aus. Hinweis: Wenn das DNA Center nicht über den Port oder das Protokoll verfügt welches benötigt wird, kann dies selbst erstellt werden. Klicke hierzu auf **Add Port/Protocol**, füge alle erforderlichen Informationen hinzu und klicke auf **Save**.
6. (Optional) Um weitere Regeln in den Vertrag aufzunehmen, klicke auf **Add** und wiederhole Schritt 5 und 6.
7. Klicke **Save**.

C Projektmanagement

C.1 Projektübersicht

Das Hauptziel dieser Studienarbeit ist die Installation von DNA-Center und Integration vom bestehenden Labor-Netzwerk.

C.1.1 Ziele der Projektes

Da Software-Defined Access Neuland im Campus Bereich ist, wollen wir die SD-Access Lösung vom Hersteller Cisco ausarbeiten. Dazu gehören folgende Ziele:

- Installation von DNA-Center und Integration vom bestehenden Campus Labor-Netzwerk.
- Definieren von Benutzer- und Geräteprofilen, um basierend auf Geschäftsanforderungen die Zugriffsrechte und Netzwerksegmentierung zu verwalten und so das Netzwerk sicher zu halten.
- Verwendung von Erkenntnissen von DNA Analytics and Assurance für eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerks.
- Integration vom bestehenden IP Address Management Tool im DNA Center
- Durch APIs, Erstellung von wöchentlichen Reports über den Campus Netzwerk Status in einem E-Mail und einer Slack Message.

C.2 Projektorganisation

Diese Studienarbeit wird von drei Personen umgesetzt und durch zwei Betreuer überwacht.

C.2.1 Organisationsstruktur

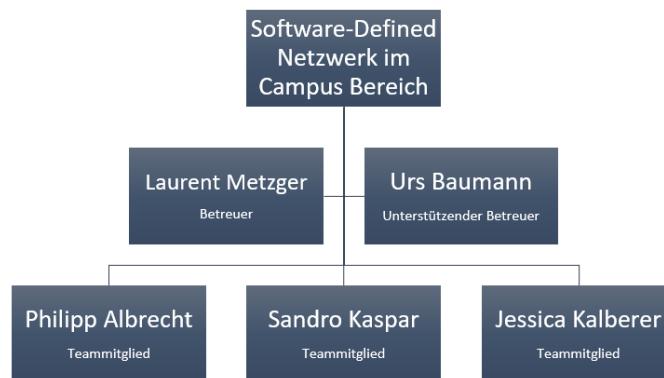


Abbildung C.1: Organisationsstruktur

C.3 Management Abläufe

Für die Umsetzung der Studienarbeit stehen insgesamt 15 Wochen und pro Person 240 Stunden zur Verfügung. In einer Woche liegt das Arbeitspensum von 16 Stunden pro Person vor. Das Projekt startet am 19. Februar 2018 und endet am 1. Juni 2018.

C.3.1 Zeitliche Planung

Die zeitliche Planung erfolgte in Gant und die Verwaltung der Arbeitspakete auf Waffle.io. Die Planung wird während dem Projekt laufend aktualisiert und angepasst. Die Zeiterfassung erfolgt während der Arbeitsausführung mit Toggle getrackt.

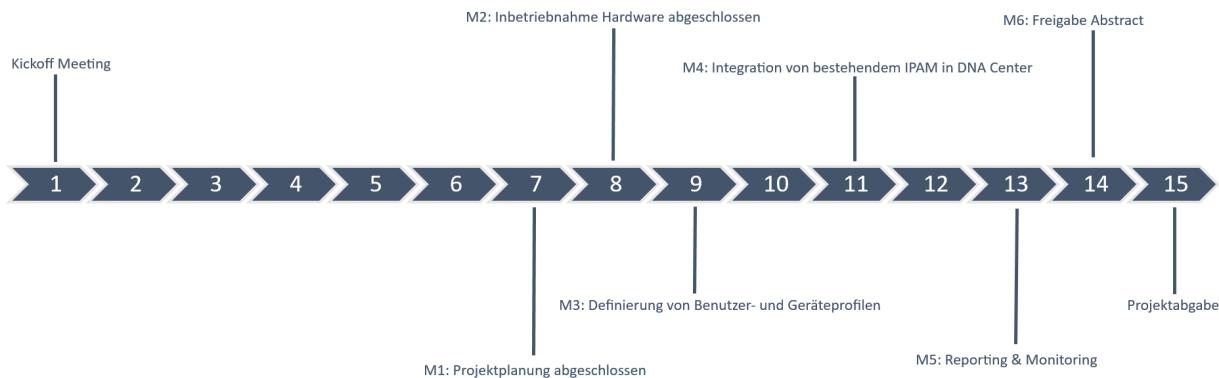


Abbildung C.2: Projektplanung

C.3.2 Meilensteine

Folgende Meilensteine sind für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	20.03.2018	Projektplanung abgeschlossen
M2	10.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	17.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	01.05.2018	Integration von bestehenden IPAM in DNA Center
M5	15.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.1: Meilensteine

C.3.3 Arbeitspakete

Alle Arbeitspakete werden in Waffle.io erfasst und sind unter folgendem Link ersichtlich:
https://waffle.io/night28/HSR_SA

C.3.4 Besprechungen

Die Besprechungen mit dem Betreuer finden an den nachfolgend aufgelisteten Tagen statt:

- jeden Dienstag zwischen 15.10 - 16.10 Uhr

Offene Traktanden und Probleme werden mit dem Betreuer kommuniziert und diskutiert. Nach dieser Besprechung wird jeweils in einem Team-Meeting das weitere Vorgehen geplant.

C.4 Infrastruktur

Die Organisation der Arbeit und Teammitglieder wird durch folgende Werkzeuge unterstützt:

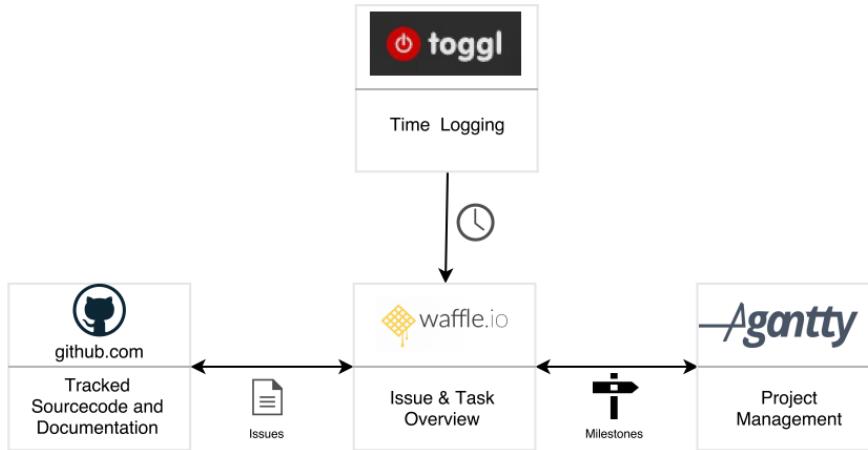


Abbildung C.3: Interne Organisationsstruktur

Unsere Tools sind unter folgenden Links ersichtlich:

GitHub https://github.com/night28/HSR_SA

Waffle.io https://waffle.io/night28/HSR_SA

Toggl <https://toggl.com/>

Agantty <https://app.agantty.com/#/project/203670>

C.5 Risiko Management

C.5.1 Umgang mit Risiken

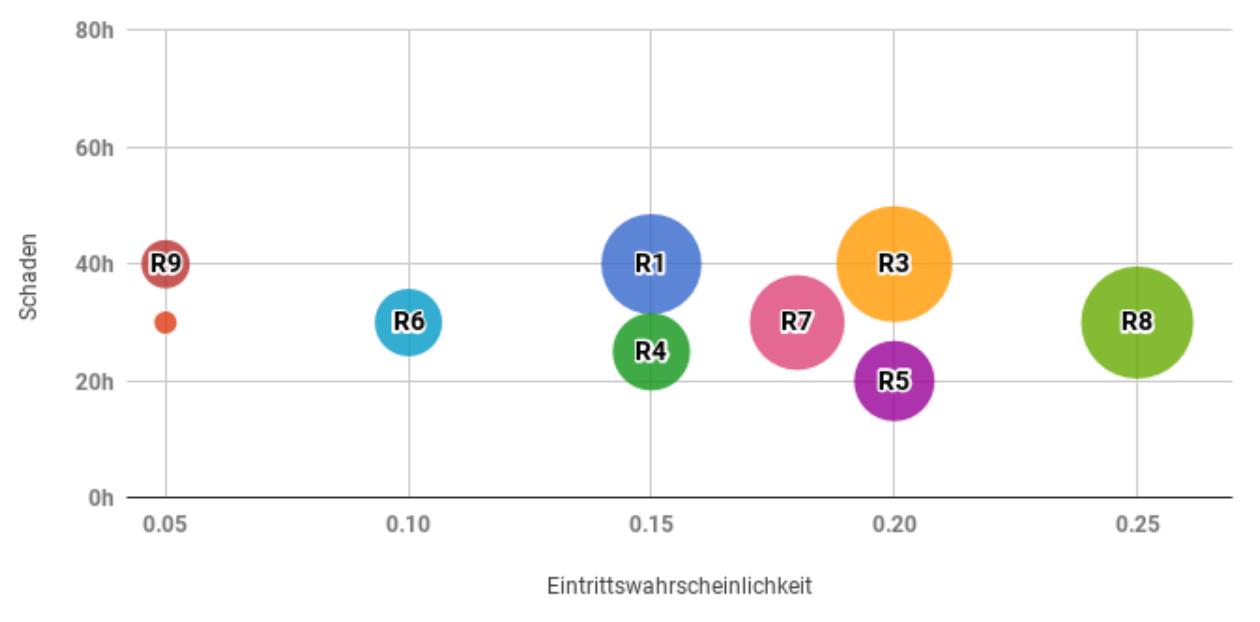
Risiken lassen sich leider nicht immer vermeiden. Aus diesem Grund sind nachfolgend mögliche Risiken aufgeführt. Des Weiteren wurden vorbeugende Massnahmen definiert, um die Eintrittswahrscheinlichkeit von Risiken mit schwerwiegenden Konsequenzen zu reduzieren. Für den Fall, dass ein Risiko dennoch eintreten sollte, sind entsprechende Massnahmen definiert um den Schaden möglichst gering zu halten. Sollten sich während dem Projekt neue potenzielle Risiken zeigen, wird dieses Dokument laufend aktualisiert.

C.5.2 Risiken

Nummer	Titel	Beschreibung	Vorbeugung	Verhältnis beim Eintreten
1	Ausfall eines Teammitglieds	Ausfall auf Grund unvorhergesehener Ereignisse wie Krankheit, Unfall etc.	Reserven einplanen, Kommunikation sicherstellen, damit andere Teammitglieder die Aufgaben übernehmen können	Tasks des ausgesfallenen Mitglieds möglichst auf die anderen Teammitglieder aufteilen.
2	Hardwareausfall DNA-Center	DNA-Center Appliance fällt durch Hardwaredefekt aus	keine Verbesserungen nahmen möglich	Austausch im Rahmen der Garantie veranlassen
3	Fehlendes Know-How	Da viele der Themen neu sind, kann entsprechendes Wissen fehlen	Zeit einplanen um sich in neue Themen einzuarbeiten	Fehlendes Wissen sobald wie möglich aneignen. Bei Bedarf Rat der Betreuer einholen
4	Konflikte oder Missverständnisse im Team	Das Team ist sich bezüglich wichtigen Entscheidungen uneinig	Entscheidungen stets mit Begründung dokumentieren	Kann auch mit Hilfe der Doku keine Einigung gefunden werden, fachlichen Rat des Betreuers einholen
5	Missverständnisse im Team	Im Team herrscht Uneinigkeit über bereits getroffene Entscheidungen	Protokolle führen und Entscheidungen klar dokumentieren	Protokolle und Dokumentationen beizeihen

6	Ausfall Server / Netzwerkinfrastuktur	Ausfall der von der HSR zur Verfügung gestellten Infrastrukturkomponenten	30	10%	3	Keine Vorbeugenden Massnahmen möglich	Sobald die Infrastruktur wieder verfügbar ist, Systeme erneut in Betrieb nehmen
7	Lieferverzögerung Hardware	Die von Cisco bestellte Hardware kommt später als angekündigt	30	18%	5.4	Keine Vorbeugenden Massnahmen möglich	Projektplanung an neue Gegebenheiten anpassen, notfalls Projektumfang im Absprache mit Betreuer anpassen
8	Zeitaufwände falsch geschätzt	Auf Grund falscher Schätzungen kommt es im Projekt zu Verzögerungen	30	25%	7.5	Laufende Kontrolle des Projektfortschritts um Probleme frühzeitig zu erkennen, Reserven einplanen	Verbleibende Schätzungen korrigieren, Planung anpassen
9	Datenverlust	Verlust von projektbezogenen Daten wie Dokumentationen, Konfigurationen etc.	40	5%	2	Regelmäßige und verteilte Backups aller Daten erstellen	Verlorenen Daten aus Backups wiederherstellen, fehlende Daten neu erarbeiten
10	Unausgereifte Software	Verzögerung des Projektes durch unvorhergesehene Hürden, da Software nicht genügend auf Funktionalität getestet und Dokumentiert. Software steht noch in einem frühen Release.	40	20%	8	Über aktualen und funktionalitäten informieren	Bugs reporten und bei Möglichkeit diese umgehen. Falls nötig Hilfe bei Cisco Support suchen.

Risikograph



C.5.3 Eingetretene Risiken

Nachfolgend werden die eingetretenen Risiken genauer erläutert.

Lieferverzögerung Hardware Leider wurde die Hardware nicht wie geplant geliefert.

Deshalb wurde die Projektplanung an die neuen Gegebenheiten angepasst.

Nachfolgend die alte Projektplanung:

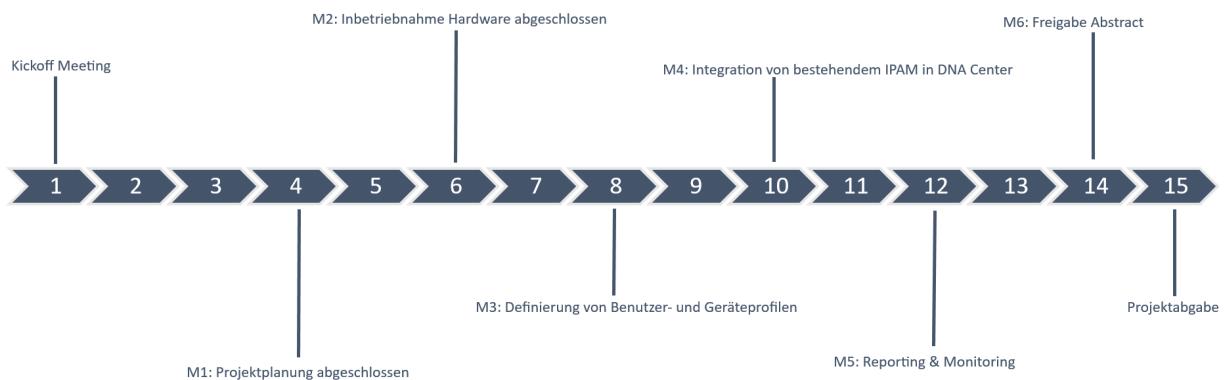


Abbildung C.4: alte Projektplanung

Folgende Meilensteine waren für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	20.03.2018	Projektplanung abgeschlossen
M2	03.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	17.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	01.05.2018	Integration von bestehenden IPAM in DNA Center
M5	15.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.3: alte Meilensteine

Die neue Projektplanung sieht nun folgendermassen aus: Nachfolgend die alte Projektplanung:

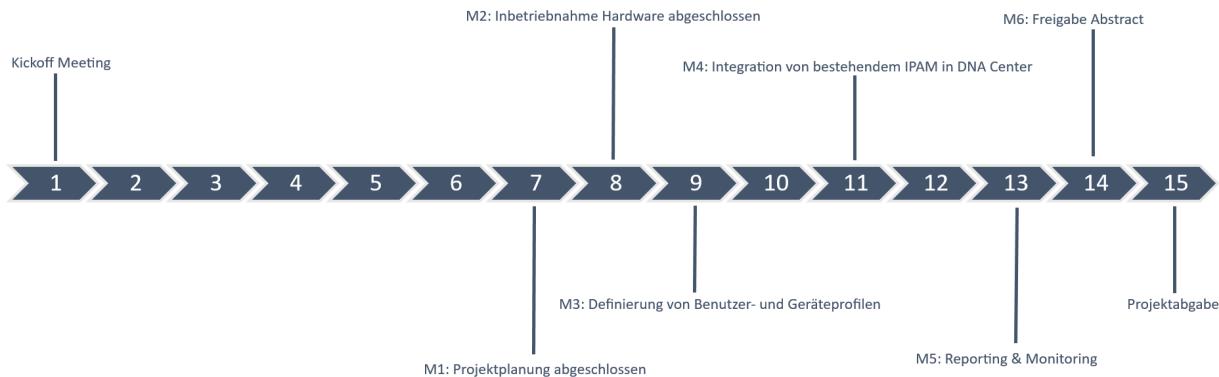


Abbildung C.5: neue Projektplanung

Folgende Meilensteine sind nun aufgrund der Lieferverzögerung für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	10.04.2018	Projektplanung abgeschlossen
M2	17.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	24.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	08.05.2018	Integration von bestehenden IPAM in DNA Center
M5	22.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.4: neue Meilensteine

Unausgereifte Software und fehlendes Know-How Das DNA Center befand sich beim Beginn unserer Studienarbeit noch in der Version 1.1.3. Bis zur Abgabe wurde die Version 1.1.6 veröffentlicht, auf welche wir unser DNA Center auch aktualisiert hatten.

Release Notes

View Documents by Topic Choose a Topic ▾

- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.6](#) 17/May/2018 NEW
- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.5](#) 11/May/2018 UPDATED
- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.4](#) 30/Mar/2018 NEW
- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.3](#) 18/Mar/2018
- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.2 Version 2](#) 12/Feb/2018
- [Release Notes for Cisco Digital Network Architecture Center, Release 1.1.2](#) 26/Jan/2018

Abbildung C.6: Release Notes

Das DNA Center enthält in diesen frühen Versionen noch viele Bugs und auch Beta Features, welche oft zu Problemen führen können. Die Funktionalitäten sind teilweise nur beschränkt so umsetzbar, wie sie angekündigt und beschrieben wurden. Bei unserem ersten Versuch mit der Version 1.1.3 stiessen wir auf das Problem, dass wir die Geräte über die LAN Automation nicht durchführen konnten, da nicht einmal ein DHCP Server auf den Geräten konfiguriert wurden. Weitere Probleme kamen auch beim Provisionierungsprozess hinzu. Geräte welche vorher verwaltet werden konnte, waren auf einmal nicht mehr erreichbar im DNA Center, obwohl dies manuell per SSH kein Problem darstellte. Ein Versuch das DNA Center per Backup zu sichern, brachte das ganze DNA Center zum Absturz. Nachdem viele solche Hürden und Probleme aufgetaucht waren, entschieden wir uns es mit einem Out of Band Management zu versuchen. Hierzu musste der Konfigurations-Wizard des DNA Centers nochmal gestartet werden, um das zweite Netzwerkinterface zu definieren. Das erneute Durchführen dieses Konfigurations-Wizard führte zum kompletten Absturz, so dass die ganze DNA Center Appliance gar nicht mehr bootete.

Nach einer zweiten Installation des DNA Centers versuchten wir erneut die LAN Automation, um ein Underlay zu bereitzustellen. Diesmal funktionierte das Hinzufügen eines Seed-Devices. Die LAN Automation soll nach der Konfiguration eines Seed-Devices so oft wie nötig gestartet und gestoppt werden können. Sollte später ein weiterer Switch hinzukommen, so könnte diese erneut für dieses Device gestartet werden. In unserem Fall führt dies zu Problemen mit der Konfiguration des IS-IS Protokolls. Es wurden nur die Routen der ersten Geräte zum Border hinzugefügt. Die Routen aller nachfolgenden Geräte wurden nur beliebig oder gar nicht hinzugefügt, so dass diese keine Kommunikation zum DNA Center aufbauen konnten. Dies führte bei einigen Konfigurationen zur Verwirrung, da wir teilweise nicht wussten ob es sich um ein falsches Verhalten der Software oder einen Fehler unsererseits handelte. Aus diesem Grunde wurde beschlossen uns für einen Tag einen Cisco Experten zur Verfügung zu stellen. Wir konnten mit ihm die Konfiguration nochmal von Grund auf durchführen und kamen bis zur Konfiguration eines Seed-Devices für die LAN Automation. An diesem Punkt stiessen wir aber wieder auf diverse Hindernisse, bei welchen uns der Cisco Experte zu dieser Zeit nicht weiterhelfen konnte. Nach eigenen weiteren Versuchen gelang es uns jedoch, die LAN Automation auf einem weiteren Gerät durchzuführen.

Des Weiteren Fehlen Dokumentationen zu der Verwendung von Policies oder der genauen Verwendung der Authentication Templates für das Onboarding. Bei dieser Bedeutung der verschiedenen Authentication Templates konnte uns jedoch jemand von Cisco Auskunft geben.

Da bei uns bereits zwei eher schwerwiegende Risiken eingetreten waren, wurde entschieden das der Abgabetermin um knapp zwei Wochen, auf den 13. Juni 2018 verschoben wird. Das hat folgende Anpassungen in der Projektplanung zur Folge:

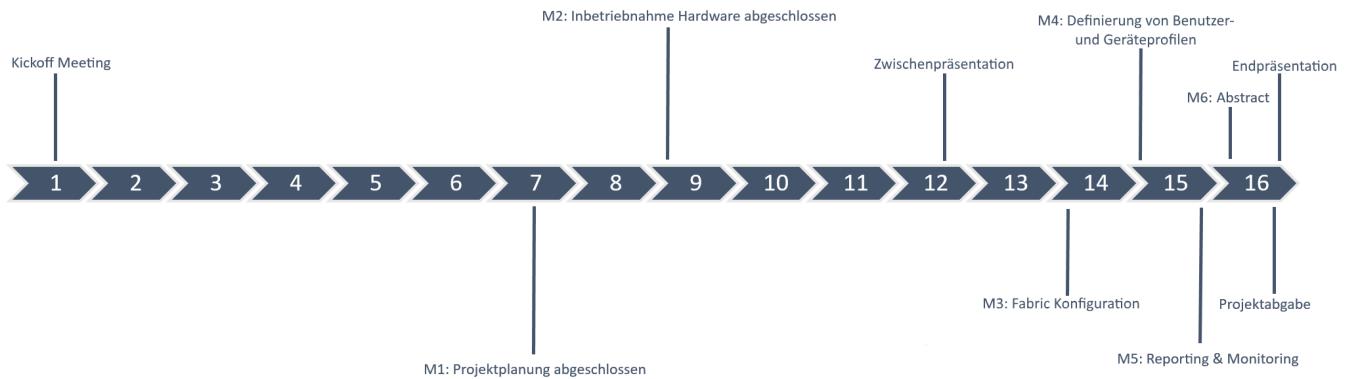


Abbildung C.7: Erweiterte Anpassung der Projektplanung

Folgende Meilensteine sind nun aufgrund der Lieferverzögerung für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	10.04.2018	Projektplanung abgeschlossen
M2	17.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	24.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	08.05.2018	Integration von bestehenden IPAM in DNA Center
M5	22.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.5: Erweiterte Anpassung der Meilensteine

D Bugs

Im folgenden werden Bugs aufgeführt, die während unserer Arbeit aufgetreten sind.

D.0.1 Backup Server hinzufügen

Komponente	Einstellungen → System Settings → Backup & Restore
Dringlichkeit	Hoch
Beschreibung	Nach der Eingabe der Backup Server Einstellungen und den klick auf <i>Apply</i> geschieht nichts. Nach einer Weile werden immer mehr Docker Container gestoppt, bis das DNA Center nicht mehr gebraucht werden kann. Ein Neustart ist erforderlich. Nachtrag: Nach mehreren Versuchen hat es geklappt. Über die genaue Ursache kann keine Aussage gemacht werden. Wir vermuten der Bug wurde in Updates gefixt.
Konsequenzen	Beim Ausfall der Appliance können die Einstellungen nicht wiederhergestellt werden
Workaround	Keiner
Reproduzieren	<ol style="list-style-type: none"> 1. Einstellungen → System Settings → Backup & Restore 2. Im Popup <i>Configure</i> wählen. 3. SSH Servereinstellungen eingeben 4. <i>Apply</i> drücken.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.1: Bug: Backup Server hinzufügen

D.0.2 Netzwerkgerät OS Update

Komponente	Provision → Devices → Inventory
Dringlichkeit	Mittel
Beschreibung	Im DNA Center können OS Images automatisch auf Netzwerkgeräte aufgespielt werden. Dieser Funktion hat bei allen Versuchen immer zu Fehler geführt. Wichtig: Im Imagerepository muss das Image verfügbar sein.
Konsequenzen	OS Updates müssen manuell durchgeführt werden.
Workaround	Update manuell via TFTP direkt via CLI auf dem Netzwergerät ausführen.
Reproduzieren	<ol style="list-style-type: none"> 1. Provision → Devices → Inventory 2. Gewünschtes Gerät anwählen 3. Action → Update OS Image 4. Im Popup Gerät auswählen → Update
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.2: Bug: Netzwerkgerät OS Update

D.0.3 DNA Center Update - Appliance nicht nutzbar während Update

Komponente	Einstellungen → App Management
Dringlichkeit	Mittel
Beschreibung	Wenn ein <i>System Update</i> oder ein <i>Package Update</i> durchgeführt wird, kann das GUI des DNA Center nicht verwendet werden. Problematisch: Der Zugriff ist trotzdem möglich. Jedoch sind dann zufällig Funktionen nicht vorhanden oder benutzbar.
Konsequenzen	Appliance nicht nutzbar während Update
Workaround	Während Update GUI nicht verwenden.
Reproduzieren	Bedingung: Updates sind Verfügbar. 1. Einstellungen → App Management 2. <i>System Update</i> oder <i>Package Update</i> wählen. 3. Packages auswählen 4. Install oder Update wählen.
Reporter	Philipp Albrecht
Feedback Cisco	Siehe Workaround

Tabelle D.3: Bug: DNA Center Update - Appliance nicht nutzbar während Update

D.0.4 Devices mit Namen ”NULL” können nicht gelöscht werden

Komponente	Provision → Devices → Inventory
Dringlichkeit	Mittel
Beschreibung	Nach der LAN-Automation kommt es vor, dass Devices mit dem Namen ”NULL” erscheinen. Diese können nicht über das Action Menü gelöscht werden.
Konsequenzen	Wenn die Synchronisation nicht funktioniert und das Device neu hinzugefügt werden muss, kann es nicht entfernt werden.
Workaround	”NULL-Device” zusammen mit funktionierendem Netzwerkgerät markieren. Die <i>Action</i> Schaltfläche wird dann klickbar. Das funktionierende Device deselektieren. Die Schaltfläche bleibt danach weiterhin klickbar und das ”NULL-Device” kann über <i>Action → Delete</i> gelöscht werden.
Reproduzieren	Bedingung: ”NULL-Device” in <i>Inventory</i> vorhanden. 1. Provision → Devices → Inventory 2. ”NULL-Device” anwählen 3. Probieren <i>Action</i> Schaltfläche anzuwählen
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.4: Bug: Devices mit Namen ”NULL” können nicht gelöscht werden

D.0.5 <https://dnacenter/mypnp> *Configurations* nicht lösbar

Komponente	https://dnacenter/mypnp → Configurations
Dringlichkeit	Mittel
Beschreibung	Im myPNP können Konfigurationen nicht gelöscht werden.
Konsequenzen	Annahme: Von dort kommen veraltete Informationen die auf die Netzwerkgeräte geschrieben wird.
Workaround	Nicht vorhanden.
Reproduzieren	Bedingung: In myPNP sind Konfigurationen vorhanden. 1. https://dnacenter/mypnp → Configurations 2. Beliebige Konfiguration anwählen 3. Delete klicken
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.5: Bug: <https://dnacenter/mypnp> *Configurations* nicht lösbar

D.0.6 9xxx Serie Lizenzzuordnung

Komponente	Licence Manager → Switches
Dringlichkeit	Mittel
Beschreibung	In der Tabelle <i>Switch Licence Usage</i> werden redundante Einträge für Switches der 9xxx Serie angezeigt. Einerseits gibt es den Eintrag <i>Cisco Catalyst 9300 Series Switches</i> andererseits <i>Cisco Catalyst 9xxx Series Switches</i> . Ein Gerät mit der Version 9300 fällt demnach in zwei Verschiedenen Model.
Konsequenzen	Die Lizenzen können nicht zugewiesen werden.
Workaround	Nicht vorhanden.
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.6: Bug: 9xxx Serie Lizenzzuordnung

D.0.7 PNP

Komponente	Provision → LAN Automation
Dringlichkeit	Mittel
Beschreibung	Während der LAN Automation machen die Switch und Router PNP auf das DNA Center. Dies klappt teilweise nicht und der Switch muss zurückgesetzt und neu gestartet werden.
Konsequenzen	Die LAN Automation braucht viel manuelle Eingriffe und ist sehr aufwändig.
Workaround	Siehe Beschreibung
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.7: Bug: PNP

D.0.8 LAN Automation IP Vergab

Komponente	Provision → Devices → Inventory
Dringlichkeit	Mittel
Beschreibung	Wir haben die LAN Automation ein zweites Mal mit einem grösseren IP Pool gestartet. Bei einzelnen Geräten wird aber im DNA Center weiterhin die alte IP angezeigt nachdem diese PNP versucht haben.
Konsequenzen	Die IP Adresse ist ungültig und die Geräte nicht erreichbar.
Workaround	Geräte löschen und Vorgang wiederholen bis die IP Adresse stimmt.
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.8: Bug: LAN Automation IP Vergab

D.0.9 Manuelle Eingriffe Infoblox

Komponente	Design → Network Settings → IP Address Pool
Dringlichkeit	Niedrig
Beschreibung	Wenn etwas an den IP Pools geändert wird (Hinzufügen oder Bearbeiten) werden diese Änderungen nicht aktiv.
Konsequenzen	Beim Adressbereich muss der Infoblox als DHCP Server hinterlegt werden und die Services auf dem Infoblox müssen neu gestartet werden.
Workaround	Siehe Konsequenzen
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle D.9: Bug: Manuelle Eingriffe Infoblox

E Persönliche Summaries

E.1 Sandro Kaspar

E.2 Philipp Albrecht

Mit der Vorstellung wie klassische Netzwerke konfiguriert werden, bin ich an das DNA Center mit grossen Erwartungen gestossen. Network Orchestration mit zentralen Kontrollern habe ich bisher nur von Ubiquiti und Cisco Meraki gekannt. Als wir nach langen warten endlich die Hardware mitte April bekommen haben, merkte ich, dass meine Erwartungen viel zu hoch waren. Während ich mir wie bei Cisco Meraki eine einfache intuitive "Clicki-Bunti" Lösung vorgestellt habe, stiess ich an ein unintuitives Etwas, komplizierten Lizzenzen und haufenweise Bugs. Alle Operationen und Versuche waren geprägt vom langen warten bis irgendwelche Geräte ihren Reboot durchgeführt haben und durchstöbern von als Marketingunterlagen strukturierte Bedienungsanleitungen. Schnell merkte ich zwei Dinge. Einerseits den Mangel an Erfahrungen und Wissen mit Cisco ISE, LISP, VXLAN und andererseits, dass das effektive Erlebnis mit dem DNA Center weit abweicht von den farb-freudigen Marketing Videos auf der Webseite von Cisco. Im persönlichen Zeitmanagement kam mit dem späten Eintreffen der nicht funktionierend Appliance noch ein weiteren Problem. Seit beginn der Arbeit waren nun schon fast zwei Monate vergangen und plötzlich musste ich viel mehr Zeit in die Semesterarbeit investieren. Da ich Teilzeit studiere, nebenbei Arbeite und jeweils von Zürich nach Rapperswil pendle, konnte ich nicht einfach plötzlich mehr Zeit für die Semesterarbeit investieren. Alles in allem fand ich unsere Arbeit sehr spannend. Das Ergebnis hingegen ist sehr ernüchternd und nicht zufriedenstellend. Das DNA Center ist nicht wie Erwartet ein fertiges ausgereiftes Produkt, sondern eine riesige Baustelle.

E.3 Jessica Kalberer

Das Themengebiet Network Design and Seurity hat mich schon seit Anfang des Studiums interessiert und mich nun in der Studienarbeit vor neue Herausforderungen gestellt. Als ich zum ersten mal von Cisco DNA Center hörte, war ich fasziniert von der ganzen Appliance. Der Gedanke das nun alles über eine einzige Appliance konfiguriert und verwaltet werden konnte, war einfach traumhaft. Am Anfang des Projektes musste ich mich einige Stunden in die Technologien einlesen, da vieles für mich neu war. Bisher konnte ich nur die traditionellen Netzwerk Design die aus einem Acces, Distribution und Core Layer bestanden. Leider verschob sich unsere ganze Arbeit etwas, da die Hardware relativ spät bei uns ankam. Mitte April konnten wir dann mit der ganzen Installation und Konfiguration starten. Die Konfiguration des DNA Center war relativ Ernüchternd, da vieles noch nicht fehlerfrei funktionierte und darum manuell konfiguriert werden musste.

Die Arbeit im dreier Team empfand ich als angenehm. Es war jedoch teilweise etwas schwierig, wenn Konfigurationen im DNA Center gemacht wurden und nicht alle in einem Raum sassen, so das nicht jeder wusste was gerade gemacht wird. Da das DNA Center fehleranfällig war, musste immer genau abgesprochen werden, wer was Konfiguriert und wann etwas neu gestartet wird. Teilweise funktionierten Ansichten nicht mehr genau oder der ISE wurde wahllos nicht mehr angezeigt. Die Arbeit im Team hatte aber zum Vorteil, das viele Probleme besprochen werden konnten und fast immer jemand wusste wie man es anders probieren könnte.

F Sitzungsprotokolle

F.1 Sitzungsprotokoll 27.02.2018

Sitzungsteilnehmer

- Laurent Metzger
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Projektstart
- Besprechung genaue Aufgabenstellung und nächste Schritte

Beschlüsse (Diskussion)

- Evaluieren eines Software Defined Network im Campus Bereich für FUB.
- Anleitung für FUB für die Erstellung eines SD Networks mittels DNA Center.
- Freie Hand bei Gestaltung wöchentlicher Reports, da nicht alle Möglichkeiten bekannt.
- Geräte werden erst Mitte März 2018 geliefert
- Offene Frage: Vorgaben auf welcher Plattform Projekt laufen soll (Dropbox, GitHub)?

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Projektplan mit Meilensteinen erstellen	Philipp
Sitzungsprotokoll vom 27.02.2018 erstellen	Jessica
Beschreibung der SD-A Lösung mit Vorteilen im Vergleich zu klassischem Campus Design (Management Summary)	Sandro
Module 2 Lesson 2 auf Cisco Learning Library anschauen (Part 1 und Part 2)	Philipp, Sandro, Jessica
Dokumentation vorbereiten (Latex) anhand Strukturierungsbeispiel 2	Jessica
Zeiterfassung Tool vorbereiten	Jessica

Nächster Termin

- Meeting mit Betreuer: 06. März 2018, 10 Uhr, 60 Minuten
- Meeting mit Industriepartner: 08. März 2017, 14 Uhr, 120 Minuten

Kommende Abwesenheiten

keine

F.2 Sitzungsprotokoll 06.03.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Aufgabenstellung schriftlich vom Betreuer erhalten? Bekommen wir diese noch?
 - erhalten wir in den letzten zwei Wochen
- Zeiterfassung mit Toggl / Waffle.io / GitHub Issues so sinnvoll oder anders gewünscht?
 - Tools passen, jedoch den Betreuern noch Zugang zu allen Tools geben
- Business Dresscode für Besprechung mit Industriepartner gewünscht?
 - Nein, normale anständige Kleidung reicht
- Teilnehmer Besprechung Industriepartner und deren Rollen?
 - FUB Leiter vom Netzwerk mit einem Mitarbeiter
- Was muss für die Besprechung mit dem Industriepartner vorbereitet werden?
 - wir werden in erster Linie Informationen von FUB erhalten
 - Grafik vorbereiten um eine Übersicht über unsere Tools zu zeigen
- Arbeit auf GitHub private oder public? Waffle.io wenn private 5 Dollar / Monat
 - Industriepartner am Donnerstag nochmals darauf ansprechen
- Technologien einzeln genauer beschreiben notwendig?
 - Technologien im technischen Bericht genauer beschreiben (SDA, DNA,..)

Beschlüsse (Diskussion)

- Use Cases Bereiche (ca. 10 Use Cases generieren). Unterscheidung welche Änderung das DNA Center bringt. Welche Use Cases sind neu? Use Cases müssen anfangs nicht komplett ins Detail beschrieben werden. Vielleicht zuerst User Stories generieren und daraus dann die Use Cases ableiten. Diese können dann mit Industriepartner abgeglichen werden, ob diese mit ihm übereinstimmen. Beispiele:
 - Definierung von Benutzer- und Geräteprofile, um basierend auf Geschäftsanforderungen die Zugriffsrechte und Netzwerksegmentierung zu verwalten und so das Netzwerk sicher zu halten
 - Durch APIs, Erstellung von wöchentlichen Reports per E-Mail
- GitHub private oder public?
 - Wird mit Industriepartner am nächsten Donnerstag direkt abgeklärt, aber wahrscheinlich ist es egal das wir es public machen
 - Zugriffe für GitHub, Toggl, Waffle.io für Betreuer einrichten
- Technologien welche für unsere Arbeit essentiell sind im technischen Bericht festhalten, wie beispielsweise DNA Center, VXLAN, LISP. Doch Technologien wie BGP müssen nicht weiter dokumentiert werden, da genügend Cisco Quellen verfügbar sind und bekannt sein sollte.
- Projektmanagement gewünschter Inhalt:
 - Projektplan
 - Arbeitspakete

- Risikomanagement
- Testprotokoll (um Use Cases zu überprüfen)
- Sitzung am Donnerstag mit Industriepartner für uns erst um 15:30 Uhr
 - Dresscode für Meeting normal wie immer
 - Präsentation mit Industriepartner Dresscode edel erwünscht mit Hemd etc.
- Netzwerk-Umgebung: es muss noch eine passende Netzwerk-Topologie erstellt werden
 - Hardware
 - * 4 x Catalyst 9300
 - * 4 x Catalyst 3850
 - VMs werden von Betreuer erstellt und wir erhalten VPN Zugriff auf die Server, falls wir Hardware Zugriff benötigen, befinden sich die Switches im Netzwerklabor.
 - * ISE, Infobox (Betreuer)
 - * DHCP, DNS, NTP (Ubuntu VM)
- Traktanden jeweils am Montagabend vorher an Betreuer senden.
- Kosten des Projektes
 - Hardware DNA Center um die 90'000 Fr, Switch je à 10'000 Fr. Grundsätzlich wird alles von Urs im Netzwerklabor installiert. Softwaretechnisch kann alles an Cisco retourniert werden, wenn etwas nicht mehr bootet

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Zugriffe auf GitHub, Waffle.io und Toggl an Betreuer senden	Sandro
Grafik vorbereiten für Übersicht über unsere Tools	Philipp
GitHub private oder public mit FUB abklären am Donnerstag	Philipp, Sandro, Jessica
Eingesetzte Technologien dokumentieren	Jessica
Netzwerk-Topologie Vorschlag	Philipp
Risiko-Management Tabelle	Sandro
Use Cases vorbereiten (ca. 10 Use Cases generieren)	Philipp, Sandro, Jessica
Sitzungsprotokoll in Latex übernehmen	Jessica
Sitzungsprotokoll Traktanden jeweils spätestens Montagabend an Betreuer	Jessica
Testprotokoll Vorlage erstellen anhand von Use Cases	Jessica

Nächster Termin

- Sitzung mit Industriepartner: 08. März 2018, 15.30 Uhr, 30 Minuten
- Sitzung mit Betreuer: 13. März 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.3 Sitzungsprotokoll 08.03.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Laurent Billas FUB
- Serge Pidoux FUB
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Arbeit auf GitHub private oder public? Waffle.io wenn private 5 Dollar / Monat
- Vorstellung unserer internen Organisationsstruktur
- Wird SDA zur Zeit schon benutzt?
- Aktuelle Infrastruktur
 - Anzahl Benutzer
 - Anzahl Netzwerkgeräte
 - Wie viele Personen betreuen zur Zeit diese Infrastruktur?

Beschlüsse (Diskussion)

- Sicherheit ist der Mittelpunkt bei der FUB. Entsprechende Use Cases definieren:
 - Benutzer- und Geräteprofile Definition ist ein sehr wichtiger Punkt für die FUB. Sie möchten gerne wissen wie diese Definition auf einem ISE aussehen
 - Use Case: Austausch eines Switches oder Netzwerk-Gerätes
 - sicherstellen das wir die erhaltenen Use Case richtig verstanden haben und dies mit ihnen nochmals abklären, falls etwas nicht ganz klar oder unpräzise
 - wir werden mind. 4 Use Cases von der FUB erhalten, welche Ihnen besonders wichtig sind. Spätestens bis Ende März 2018.
- Netzwerk-Umgebung: es muss noch eine passende Netzwerk-Topologie erstellt werden
 - Hardware
 - * 4 x Catalyst 9300
 - * 4 x Catalyst 3850
 - * 1 Cisco 3650CX - Büro-Switch (herausfinden wie diese Switches im DNAC integriert werden können)
 - * 2 ISR4431
 - VMs werden von Betreuer erstellt und wir erhalten VPN Zugriff auf die Server, falls wir Hardware Zugriff benötigen, befinden sich die Switches im Netzwerk-labor.
 - * ISE, Infobox (Betreuer - Lizenzen erhalten wir von der FUB)
 - * DHCP, DNS, NTP (Diese Dienste sind nicht separat, sondern auf der Infobox vorhanden und können dort eingerichtet werden.)
- DNA-Center inkl. Material sollte ca. in 1-2 Wochen gesendet werden.
- Dimensionen des aktuellen FUB Netzes:
 - Ganzes Führungsnetz Schweiz mittels MPLS
 - Anzahl User permanent ein paar Tausend, aber ist sehr variabel je nach Einsatz. Wichtiger Punkt der abzuklären gilt wäre, werden die maximal erlaubten

Geräte überschritten? Wo liegen die Limiten?

- Kennenlernen der Tools und abklärung ob diese Technologien
- GitHub kann public genutzt werden, da Informationen von FUB schon vorher gefiltert.
- SDA wird noch nicht benutzt, wir sollen diese Technologien für die Evaluieren.

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Netzwerktopologie mit zusätzlichen Geräten	Philipp
Risiko-Management Tabelle	Sandro
Sitzungsprotokoll Traktanden spätestens Montagabend an Betreuer	Jessica

Nächster Termin

- Meeting mit Betreuer: 13. März 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.4 Sitzungsprotokoll 13.03.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Genauigkeit der Dokumentation der Technologien
- Wie ist es mit Quellen umzugehen?
- Netzwerktopologie besprechen

Beschlüsse (Diskussion)

- Netzwerktopologie
 - Core Layer kommt darauf an welche Modelle wir bekommen, um dies genauer spezifizieren zu können
 - * 9300-24T-A (Lizenz: Cisco DNA Advantage für 3 Jahre) ohne Uplinks
 - * Die genauen Modelle werden uns von Herrn Metzger noch bekannt gegeben
 - Green: Out of Bound Management
 - 3650CX kann selbst kein VXLAN und muss an 9300 angeschlossen werden
 - Unterschiedliche Gebäude in Netzwerktopologie erwähnen
 - 9300 zwischen Border und Control Node
 - zwischen den Switchen L3 Routing Protokolle
 - mit L2 auf Server zugriff vom 9300 Distribution Core her
 - 9300 Unterschied der einzelnen Modelle mehr nur Perfomance
 - Anmerkung: 3850XS nicht der beste Router in Core in einer Produktiven Umgebung
 - 3850 aktuell bei FUB in Verwendung
 - 9300 sind neu geplant
- Wireless = Out of Scope, sollte unbedingt in der Dokumentation erwähnt und als optional definiert werden.
- DNAC Konfiguration von Switches (theoretisch ein Use Case)
 - Bleibt die Verbindung bestehen bei Änderungen?
 - Port Konfigurationen werden nicht kontrolliert
 - Route Policies werden fix überschrieben
- Netzwerktopologie wird von Herrn Metzger noch FUB gezeigt (informell)
- Verkabelungsplan erstellen: da keine Uplinks vorhanden, werden wahrscheinlich Port 1-4 für das verwendet
- Regelmässige Updates per Mail mit Dokumentation an Betreuer
- Quellen HSR intern keine Vorgaben, so wie angefangen weiterführen

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Genaue Modelle der Switche bekanntgeben	Laurent Metzger
Verkabelungsplan erstellen (Switch Ports)	Sandro
IP-Adressen Plan	Philipp, Sandro, Jessica
Mapping zwischen SDA und LISP Name Definitions	Jessica
Regelmässige Updates der Doku an Betreuer	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 20. März 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.5 Sitzungsprotokoll 20.03.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Use Cases Industriepartner
- Verkabelungsplan
- LabNetzwerkArchitektur
- Zwischenstand aktuelle Dokumentation
- Dokumentatorisches: Quellenangaben
- Genaue Modelle der Switche (Laurent Metzger) - kommt noch
- IP Adress Plan - Vorgabe von Lab Infrastruktur (Urs Baumann) - kommt noch
- IPv6 Unterstützung? (Out of Scope - es werden private IPv4 Adressen verwendet RFC1918)

Beschlüsse (Diskussion)

- Use Cases werden bis 27.März 2018 vom Industriepartner übergeben (Herr Metzger wird nochmal bei FUB nachhaken, damit diese wirklich geliefert werden)
- Netzwerk Architektur wurde nach Besprechung mit FUB noch angepasst. Es werden zwei weitere Router im Core Layer hinzugefügt und die Catalyst 3850 in den Distribution Layer hoch geschoben
- Im Core Layer wird für den Cisco ISR 4431 ein Modul hinzugefügt. Zu beschreiben als Port 01-0 (mittleres bedeutet Modul 1)
- Hardware Aufbau inkl. Installation beginnt nach Ostern (1. April 2018) - Zeitaufwand wird exponentiell steigen
- Voranalyse Technologien (LISP Komponenten, Skalierbarkeit, Ablauf Kommunikation...)
 - Single Point of Failure
 - mögliche Topologien (mehrere Gebäude, Standorte, etc.), wo macht was Sinn?
Große Instanzen, mehrere kleinere, etc.
 - Skalierungsprobleme
 - Abläufe: was passiert wann (ARP Request, Abfolge, Zuständigkeiten, etc.)
- IPv6 Unterstützung -> Out of Scope - es werden private IPv4 Adressen verwendet RFC1918
- Materialliste inkl. den genauen Switch/Router Spezifikationen wird noch geliefert
- SDA Mechanismus
 - Wie lange hält der Map Cache auf einem Edge Node, kann dieser fürs Troubleshooting angeschaut werden?
 - Für die Evaluierung des genauen Ablaufes sollen die Pakete nachher mit Wireshark mitgeschnitten werden.
 - Werden die SGT immer mit dem Controller Node abgeglichen? (Wahrscheinlich für die Synchronisation der SGT, damit immer alle Fabrics über die Zugriffe Bescheid wissen.)

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Quellenangaben in Literaturverzeichnis übernehmen	Jessica
Meilensteine anpassen	Philipp, Sandro, Jessica
Analysephase	Philipp, Sandro, Jessica
Topologie korrigieren	Philipp
Design Guide lesen	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 27. März 2018, 15.10 Uhr, 60 Minuten (abgesagt)
- Meeting mit Betreuer: 03. April 2018, 15.10 Uhr, 60 Minuten (abgesagt)
- Meeting mit Betreuer: 10. April 2018, 15.10 Uhr, 120 Minuten

Kommende Abwesenheiten

Jessica Kalberer am 27. März 2018

F.6 Sitzungsprotokoll 10.04.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Use Cases Industriepartner
- Use Cases von uns besprechen
- Hardware nun eingetroffen? Erste Schritte besprechen
- Mechanismus von SDA in Details eventuell anschauen

Beschlüsse (Diskussion)

- Hardware ist bereits in Bern, wird diese Woche noch an die HSR geliefert und steht ab nächster Woche bereit.
 - bei nächstem Meeting erhalten wir alle Informationen
 - Geräte werden von Urs vorbereitet, aber nicht Konfiguriert
 - Zugriff auf Geräte und Infrastruktur ist nach nächstem Meeting möglich (sie werden schauen ob wir einen Schlüssel bekommen, um auch ausserhalb der Zugangszeiten Zugriff zu erhalten)
- Netzwerktopologie
 - wurde erneut mit Industriepartner besprochen und festgestellt, dass die aktuelle Netzwerktopologie zu weit von der Three-Tier Topologie entfernt ist.
 - es gibt neu 2 Fabrics, um den Use Case 4 "Einsatz von SGT zusammen mit VXLAN" und den Use Case 2 "Degradation Szenarien"
 - Switche wurde angepasst, da 9300 nur Capable sind. Darum sind nun zwei 3850XS Border Nodes, da diese von Cisco CVD Certifies sind. 3850-24 werden als L3-Switch fürs Routing eingesetzt und sind zu den 3850XS mit Kupfer verbunden.
 - Wireless Antennen wurden im Kit mitgesendet und können bei ausreichender Zeit
 - bei der Definitions der Fabrics muss darauf geachtet werden, dass die Anzahl Maximaler Control plane nodes per Fabric Domain nicht überschritten wird (siehe DNA Center Maximum Scale Constraints Fabric)
- Fünf Use Cases von FUB
 - Testprotokolle erstellen (Use Case 2: verschiedene Testprotokolle für diverse Szenarien, damit herausgefunden werden kann wie alles genau funktioniert)

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Netzwerk-Topologie anpassen	Philipp
DNA Installationsvideo anschauen	alle
Installationsguide lesen	alle
Use Cases FUB dokumentieren	alle
Testprotokolle für Use Case erstellen	Jessica

Nächster Termin

- Meeting mit Betreuer: 17. April 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.7 Sitzungsprotokoll 17.04.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann (telefonisch)
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Use Cases Review
- VMs bereit (Infoblox, ISE)
- Schlüsselübergabe Serverraum
- Übernahme / Besichtigung Hardware

Beschlüsse (Diskussion)

- Schlüssel für Raum erhalten und Raum wurde besichtigt
 - 10.22.0.0 /24 für uns reserviert (Security Rules vom HSR Netzwerk)
 - am einfachsten statische route auf 10.22.0.0/16, dann würde es kein NAT brauchen
 - GW 10.22.0.1 (HSRP 10.22.0.2, 10.22.0.3)
 - 10.22.0.11 PDU Rack 1
 - 10.22.0.12 PDU Rack 2
 - 10.22.0.13 PDU Rack 3
 - 10.22.0.254 Router
 - Terminalserver für Access auf alle Geräte siehe Mail
- VMs noch ausstehend, werden wir bis Freitag noch erhalten
 - Infoblox ab Mittwoch, 18.04.2018
 - ISE ab Freitag, 19.04.2018
- Zwischenpräsentation findet am 16. Mai 2018 um 13.30 Uhr mit den Industriepartnern statt (wird nicht bewertet für SA Notengebung)

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
In Betriebnahme des DNA Centers, Infoblox, ISE	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 24. April 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.8 Sitzungsprotokoll 24.04.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht (telefonisch)
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Aktueller Stand
- VPN Zugriff auf DNA Center
- Use Cases besprechen (nächste Woche)

Beschlüsse (Diskussion)

- Probleme sauber dokumentieren mit Screenshots
- Assurance Teil war ausgeblendet, bis der ISE verbunden wurde (Dokumentieren)
- Provisioning mit laufender Fabric bis Ende Woche versuchen, ansonsten Cisco Support oder manuell
- Jump Host wird von Urs eingerichtet (anstelle von VPN)
- Use Cases werden bis nächste Woche von Betreuer angeschaut

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Provisioning von Underlay	Philipp, Sandro, Jessica
Fabric Domain erstellen	Philipp, Sandro, Jessica
Spezialfälle und Fehler dokumentieren	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 1. Mai 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.9 Sitzungsprotokoll 01.05.2018

Sitzungsteilnehmer

- Laurent Metzger (telefonisch)
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Use Cases besprechen (werden besprochen sobald Lizenzproblem behoben)
- Lizenzprobleme (Lizenzen nicht vorhanden, DNA & ISE)
- OS-Upgrade geht nicht
 - 3850: Bug? kein BGP
 - 9300: SFTP Server nicht erreichbar
- 3850: Out of Memory (wahrscheinlich wegen PnP)

Beschlüsse (Diskussion)

- Mittwoch 2. Mai 2018 werden die generellen Probleme mit Herrn Metzger und Urs angeschaut
- Use Cases werden besprochen sobald die generellen Probleme gelöst sind

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Spezialfälle und Fehler dokumentieren	Philipp, Sandro, Jessica

Nächster Termin

- Meeting um Probleme zu besprechen/beheben: 2. Mai 2018, 10 Uhr, 120 Minuten
- Meeting mit Betreuer: 8. Mai 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.10 Sitzungsprotokoll 02.05.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Lizenzprobleme DNA Center
- Lizenzprobleme Switches (IP Base statt IP Services)

Beschlüsse (Diskussion)

- Lizenzprobleme DNA Center: anscheinend sind auf dem hinterlegten Account die Lizenzen nicht verfügbar.
- Lizenzen für 9300 Switches sind von der HSR und müssten demnach auf einem Account der HSR verwaltet werden. Dies wird noch besprochen wie weiter verfahren wird. Wir werden bis dahin mit den 90 Tage Evaluation Lizenzen arbeiten und sollten so wie es aussieht dadurch keine Einschränkungen haben.
- Lizenzprobleme Switches (IP Base statt IP Services) konnten gelöst werden. Auf den Switches kann durch ein Befehl die Lizenz auf IP Services gestellt werden. Dies ist aber ebenfalls eine 90 Tage Evaluation Lizenz.

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Underlay und Overlay komplett abschliessen	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 8. Mai 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.11 Sitzungsprotokoll 08.05.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Zwischenpräsentation
 - Dauer der Präsentation (ca. 1 Stunde, egal wie aufgeteilt)
 - Gewünschter Fokus
 - rein DNA Center oder auch unsere Ergebnisse, Fehler?
 - Bewertung der Präsentation (Benotung wie BA)
- Erläuterung des Fehlers mit ISE und Backup
- Problembeschreibung

Beschlüsse (Diskussion)

- Underlay funktioniert
- Ausprobieren ob zwei Computer Verbindung hinbekommen
 - ping von zwei Computern für Zwischenpräsentation wäre super
 - Syslog Server dazwischen, damit alle Befehle angefangen werden
 - Zeigen was genau der APIC-EM dazwischen macht
 - SDN zeigen mit ein bisschen Theorie, warum VXLAN, LISP.. Sequenzdiagramm, am besten Live vorzeigen
 - Live Demo im DNA Center vorzeigen
- Zwischenpräsentation
 - Aktueller Stand
 - Probleme
 - Screenshots von Bugs
- eventuell Verlängerung der Studienarbeit um eine Woche

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Bescheid geben ob bis am Montag Konnektivität von zwei Clients funktioniert	Philipp, Sandro, Jessica
Vorbereitung Präsentation	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 15. Mai 2018, 15.10 Uhr, 60 Minuten (abgesagt)
- Zwischenpräsentation: 16. Mai 2018, 13.30 Uhr, 90 Minuten

Kommende Abwesenheiten

keine

F.12 Sitzungsprotokoll 16.05.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer
- Laurent Billas
- Serge Pidoux

Traktanden

- Zwischenpräsentation
- Verlängerung Studienarbeit
- Besprechung weiteres Vorgehen

Beschlüsse (Diskussion)

- Es wird ein Cisco Mitarbeiter hinzugezogen, um angefallene Probleme zu besprechen
- Die Studienarbeit wird verlängert
 - Endabgabe: 13. Juni 2018 um 17 Uhr
 - Endpräsentation: 15. Juni 2018 um 10 Uhr
- Es wird eine weiterführende Bachelorarbeit geben, welche uns reserviert und zugeteilt wird

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Vorbereitungen für Besprechung mit Cisco Mitarbeiter	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 22. Mai 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.13 Sitzungsprotokoll 22.05.2018

Sitzungsteilnehmer

- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Besprechung der Vorbereitungen für Meeting mit Patrick Mosimann (Cisco)
 - Ankunftszeit Cisco bekannt?
- Use Cases priorisieren
 - Integration von nicht Fabric Komponenten streichen?
 - Migration von bestehendem klassischen Campus streichen?
 - Reporting evtl. abspecken (python script, dass Infos holt und per Mail versendet)

Beschlüsse (Diskussion)

- Besprechung mit Patrick Mosimann (Cisco)
 - Ankunftszeit: Keine genaue Zeit bekannt, wir werden ihm noch ein Mail schreiben
 - Urs wäre morgen den ganzen Tag erreichbar falls etwas ist
 - Schauen das wir alles zum laufen kriegen, ansonsten fragen ob er nochmals Zeit einrichten könnte um ausstehende Probleme und Fragen zu klären
- Use Cases
 - Ausfall von DNA Center, wie verhält es sich mit den SGT Tags
 - Migration von bestehendem klassischen Campus streichen (Patrick fragen wie der Prozess aussieht und wie Machbarkeit aussieht)
 - Integration von nicht Fabric Komponenten streichen? (wäre nicht schlecht dies auch noch abdecken zu können wegen dem ganzen PGP) - 3650 als Verlängerter Arm implementieren - wie funktioniert Kommunikation zwischen Fabric und nicht Fabric (extended Fabric)
 - Degradation fast grösster Punkt

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Vorbereitung Besprechung mit Patrick Mosimann	Philipp, Sandro, Jessica
Use Cases abdecken	Philipp, Sandro, Jessica

Nächster Termin

- Cisco Support Tag: 23. Mai 2018, 08.30 Uhr bis 17.00 Uhr
- Meeting mit Betreuer: 29. Mai 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.14 Sitzungsprotokoll 29.05.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Endabgabe als PDF oder ausgedruckt? Wie viele Versionen?
- Plakat gewünscht oder nicht nötig?
- Abgabe Abstract: Genauer Abgabetermin und Abgabe per abstract.hsr.ch oder möchte Herrn Metzger oder Urs dies zuerst gegenlesen?
- Abgabe und Unterzeichnung der definitiven Aufgabenstellung, damit diese in Abstract erwähnt werden kann
- Sitzungsprotokoll Cisco Support Tag wenn gewünscht
- Besprechung aktueller Stand
- Was kommt in den Anhang?
 - Installationsanleitung
 - Vorgehen
- Wurden an den Lizzenzen etwas geändert oder liegt das am neusten Update?

Beschlüsse (Diskussion)

- Aktueller Stand
 - LAN Automation nochmals neu angefangen (ausser Seed-Device)
 - LAN Automation nur einmal starten
 - Jedes Device (1 Stunde) Konfiguration löschen und neu starten
 - Fabric deployt (IP Services auf allen Switchen aktivieren)
 - Zwei Geräte können sich pingen
 - Geräte kommen aber mit einem tracert nur zu 10.22.0.
 - DNA-C Assurance hat beide Clients erkannt
- Nächste Schritte
 - Definieren der Benutzer- und Geräteprofilen
 - Analyse mit Wireshark (SNMP Write herausfinden wo genutzt)
 - Parallel mit Use Cases anfangen
 - Ausfall eines Borders testen
 - Zertifikatfehler nachfolziehen (show crypto ca)
- Präsentation
 - Demo vom Hinzufügen eines Gerätes (gewünscht)
 - Video von der LAN Automation (gewünscht)
 - Eventuell wird jemand von Cisco für die Endpräsentation eingeladen
 - Dauer ca 20 Minuten mit anschliessender Diskussion
 - Besprechung der Benotung zwischen Betreuer und Experte (Gegenleser gibt ebenfalls Empfehlung)
 - Eventuell anschliessend gemeinsames Mittagessen
- Endabgabe Dokument
 - Abgabe an Herrn Metzger mit PDF auf Medium

- 1 Exemplar gedruckt für INS
- 2 Exemplare gedruckt für FUB
- Plakat muss abgegeben werden
- Dokument, Abstract, Plakat am Mittwoch eine Woche vor Abgabe für Review an Herrn Metzger und Urs
- Abstract vorher per Mail an Herrn Metzger und Urs, damit sie es anschauen und korrigieren können. Anschliessend dann auf abstract.hsr.ch hochladen
- Aufgabenstellung gibt uns Herrn Metzger in einer Woche, damit wir im Abstract dieses erwähnen können
- Sitzungsprotokoll des Cisco Tages Link des Google Docs an Herrn Metzger und Urs senden
- Anhang
 - Selbst definieren nach Gefühl was am besten ist
 - Installationsanleitung, Benutzeranleitung, ..
 - Zeiterfassung in Anhang und vorne allenfalls referenzieren
 - Sitzungsprotokoll Cisco Tag eventuell in Anhang
- Lizenzen
 - Es ist möglich das die FUB was an ihrem Account geändert hat. Sie sind dabei Geräte zu erfassen.
 - Lizenzen werden neu angezeigt

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Use Cases testen und Testprotokolle erfassen	Philipp, Sandro, Jessica
Dokumentation vorbereiten für Review	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 05. Juni 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.15 Sitzungsprotokoll 05.06.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

- Abgabe Abstract für Feedback
- Besprechung Abgabe Dokumente
- Aktueller Stand

Beschlüsse (Diskussion)

- Abstract wird am 6. Juni 2018 an Betreuer gesendet, das Feedback gegeben werden kann
- Dokument und Plakat wird am 6. Juni an Betreuer zur Durchsicht gesendet
- Schwerpunkt bis Ende Arbeit auf UC01

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
Abstract überarbeiten	Philipp, Sandro, Jessica
Dokumentation strukturieren und weiterführen	Philipp, Sandro, Jessica
Plakat erstellen	Philipp, Sandro, Jessica

Nächster Termin

- Meeting mit Betreuer: 12. Juni 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F.16 Sitzungsprotokoll 12.06.2018

Sitzungsteilnehmer

- Laurent Metzger
- Urs Baumann
- Philipp Albrecht
- Sandro Kaspar
- Jessica Kalberer

Traktanden

-
- —
-
-
-

Beschlüsse (Diskussion)

-
- —
-
-
-
-

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
x	x
x	x

Nächster Termin

- Endabgabe Studienarbeit: 13. Juni 2018, 17 Uhr
- Endpräsentation Studienarbeit: 15. Juni 2018, 10 Uhr

Kommende Abwesenheiten

keine

G Erklärungen

G.1 Eigenständigkeitserklärung

G.2 Urheberrechtsvereinbarung

Tabellenverzeichnis

7.1	LISP Elements	17
8.1	UC01 Fully Dressed	26
8.2	UC02 Fully Dressed	27
8.3	UC03 Fully Dressed	28
8.4	UC04 Fully Dressed	29
8.5	UC05 Fully Dressed	30
8.6	UC06 Fully Dressed	31
8.7	UC07 Fully Dressed	33
8.8	UC08 Fully Dressed	34
8.9	UC09 Fully Dressed	35
8.10	UC10 Fully Dressed	36
8.11	UC11 Fully Dressed	37
11.1	Softwareupdate - Übersicht Methoden und ausgeführten Versuche	68
11.2	DNA Center Provision - Fabric - Darstellung	73
12.1	Erklärung der Host Onboardning Authentifizierungsmethoden	90
B.1	Workflow zur Erstellung der Access Control Policies	III
C.1	Meilensteine	VI
C.3	alte Meilensteine	XI
C.4	neue Meilensteine	XII
C.5	Erweiterte Anpassung der Meilensteine	XIV
D.1	Bug: Backup Server hinzufügen	XV
D.2	Bug: Netzwerkgerät OS Update	XVI
D.3	Bug: DNA Center Update - Appliance nicht nutzbar während Update	XVII
D.4	Bug: Devices mit Namen "NULL" können nicht gelöscht werden	XVIII
D.5	Bug: https://dnacenter/mypnp Configurations nicht löschenbar	XIX
D.6	Bug: 9xxx Serie Lizenzzuordnung	XIX
D.7	Bug: PNP	XX
D.8	Bug: LAN Automation IP Vergab	XX
D.9	Bug: Manuelle Eingriffe Infoblox	XXI

Abbildungsverzeichnis

1.1	Aufgabenstellung aus AVT	1
6.1	DNAC Komponenten	7
7.1	Die Aufteilung Campus Fabric in ein Underlay und Overlay Netzwerk	8
7.2	Fabric Rollen und Terminologie	10
7.3	SDA Architektur	12
7.4	DNA Solution	13
7.5	SDA Architektur	14
7.6	DNA Dashboard	14
7.7	LISP Aufbau	16
7.8	VXLAN Encapsulation	19
7.9	RFC7348 VXLAN Header	20
7.10	Zusammenspiel Infoblox und ISE	21
7.11	DNA Solution	22
10.1	SDN Netzwerk Architektur	50
10.2	Netzwerk Architektur Vergleich	51
10.3	DNA Center Maximum Scale Constraints HA Cluster	52
10.4	DNA Center Maximum Scale Constraints Fabric	52
10.5	SDA Edge Node Scale Constraints	52
10.6	SDA Border Node Scale Constraints	53
10.7	Lab Architecture with physical Interfaces	54
11.1	Grafische Übersicht über das Vorgehen beim ersten Versuch	55
11.2	DNA Center Configuration Wizard - Start	56
11.3	DNA Center Configuration Wizard - Entering Management IP	56
11.4	DNA Center Configuration Wizard - Entering Authentication Data	57
11.5	DNA Center Configuration Wizard - DNA Center uses docker	57
11.6	DNA Center Web GUI - Login Page	58
11.7	DNA Center Web GUI - Cisco Credentials for Licences	58
11.8	DNA Center Web GUI - Cisco IPAM	59
11.9	DNA Center Web GUI - Dashboard	59
11.10	DNA Center App Management	60
11.11	DNA Center App Management - Alte Menü Anordnung	60
11.12	DNA Center Upgrade - Cisco Credentials required	61
11.13	DNA Center - About - Version	61
11.14	DNA Center - System Upgrade - Version	61
11.15	DNA Center Design Map	62
11.16	DNA Center Design - Standort hinzufügen	62
11.17	DNA Center Design - Gebäude können mit Koordinaten hinzugefügt werden.	62
11.18	DNA Center Design - Übersicht über alle Standorte und Gebäude	63
11.19	Infoblox Cisco PNP DHCP Option Konfiguration	64
11.20	DNA Center Provision - Fehlermeldungen in der "Unclaimed List"	64
11.21	IP Base and Services	65
11.22	DNA Center Provision - Alle Geräte erfolgreich in der "Unclaimed List"	66
11.23	DNA Center Dashboard - Inventory Knopf	66
11.24	DNA Center Inventory - Gerät hinzufügen	67
11.25	DNA Center Inventory - Formular Gerät hinzufügen	67
11.26	DNA Center Inventory - Neue Geräte in der Liste	67

11.27DNA Center Design - Image Repository	68
11.28DNA Center Provision - Die OS Versionen sind outdated.	68
11.29Fehlermeldung Updatevorgang via DNA Center	69
11.30Firmwareupdate Switch via CLI HTTPs	69
11.31Firmwareupdate Switch via CLI TFTP	69
11.32Der Licence Manager ist über das Dashboard erreichbar.	70
11.33Ohne verlinkten CSSM Account können keine Lizenzen zugewiesen werden.	70
11.34Der im DNA Center hinterlegte Cisco Account muss Zugriff zum entsprechenden Smart Account haben.	70
11.35Der korrekt hinterlegte Account	71
11.36Übersicht über die den Netzwerkkomponenten zugewiesenen Lizenzen	71
11.37Nicht jedem Gerät kann eine Lizenz zugewiesen werden (Siehe Tabelle)	71
11.38Template Editor	72
11.39DNA Center Provision - Fabric - Nach der Zuteilung wird die Konfiguration auf die Geräte geschrieben.	73
11.40DNA Center - maglev-config-wizard - Fehlermeldung	74
11.41DNA Center - Boot Fehlermeldung	74
11.42DNA Center - Neuinstallation - Installations ISO wird auf USB Drive kopiert	74
12.1 Grafische Übersicht über das Vorgehen beim zweiten Versuch	76
12.2 Cisco ISE Reset	77
12.3 ISE Integration Prerequisites	77
12.4 DNA Center Certificate Replacement	78
12.5 DNA Center Discovery	79
12.6 DNA Center - LAN Automation	80
12.7 Cisco Switch - Initial Config - Versucht DHCP und PnP zu machen, solange der Dialog aktiv ist.	80
12.8 LAN Automation - PnP Error	81
12.9 DNA Center - Templateeditor - Add Project	83
12.10DNA Center - Templateeditor - Add Template	83
12.11DNA Center - Templateeditor - Template um den Hostname bei der Provisionierung zu setzen.	84
12.12Cisco DNA Center - Network Profile - New Profile	84
12.13Cisco DNA Center - Network Profile - Assign Sites	85
12.14Cisco DNA Center - Device Provisioning	85
12.15Cisco DNA Center - Provision Step 1	85
12.16Cisco DNA Center - Provision Step 3	86
C.1 Organisationsstruktur	V
C.2 Projektplanung	VI
C.3 Interne Organisationsstruktur	VII
C.4 alte Projektplanung	XI
C.5 neue Projektplanung	XII
C.6 Release Notes	XII
C.7 Erweiterte Anpassung der Projektplanung	XIV

Literaturverzeichnis

- [1] RFC7348 *Virtual eXtensible Local Area Network (VXLAN): A Framework for Over-laying Virtualized Layer 2 Networks over Layer 3 Networks*, RFC 7348, 2014 (URL: <https://tools.ietf.org/html/rfc7348>)
- [2] RFC6830 *The Locator/ID Separation Protocol (LISP)*, RFC 6830, 2014 (URL: <https://tools.ietf.org/html/rfc6830>)
- [3] SDA White Paper *Software-Defined Access 1.0 Solution White Paper*, 2017 (URL: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/white-paper-c11-739642.html>)
- [4] SDA Design Guide *Software-Defined Access Design Guide*, 2018 (URL: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2018JAN.pdf>)
- [5] SDA Cisco Definition *Software Defined Access Cisco Definition*, 2018 (URL: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html>)
- [6] Campus Fabric *Cisco Campus Fabric Introduction*, 2017 (URL: https://www.cisco.com/c/dam/m/hr_training-events/2017/cisco-connect/pdf/Cisco-Campus-Fabric-Introduction.pdf)
- [7] Cisco Digital Network Architecture Center Appliance Installation, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_0P2.pdf)
- [8] Cisco Digital Network Architecture Center Appliance Installation, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_0P2.pdf)
- [9] Cisco Digital Network Architecture Center User Guide, Release 1.1, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/user_guide/b_dnac_ug_1_1.pdf)
- [10] Release Notes for Cisco Digital Network Architecture Center, Release 1.1.3 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/rn_release_1_1_3/b_dnac_release_notes_1_1_3.html), 2018
- [11] Cisco Open Plug-n-Play Agent Configuration Guide - DHCP Option-based Discovery (URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pnp/configuration/xe-3e/pnp-xe-3e-book.html#concept_4A3D8AD59EAE4339B5E7FC7DA73C3594), 10.05.2018
- [12] Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.0 - Install a New ISO on the Appliance (URL: <https://www.cisco.com/c/en/>)

us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-0-x/app_install_guide/b_dnac_install_1_0/b_dnac_install_1_0_chapter_010.html#concept_dxd_tfy_k1b), 19.05.2018

[13] *Cisco Catalyst 3850 Series Switches FAQ* (URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/qa_c67-722110.html), 22.05.2018

[14] *Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.1* (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_OP2/b_dnac_install_1_1_OP2_chapter_010.html), 28.05.2018

[15] *Infoblox Information* (URL: <https://www.infoblox.com/>), 04.06.2018

[16] *Infoblox Community Blog about Cisco Integrations* (URL: <https://community.infoblox.com/t5/Community-Blog/Infoblox-Cisco-integrations-will-make-you-a-Networking-and/ba-p/12264>), 04.06.2018

[17] *Ivan Caduff via Slack, 01.06.2018*

[18] *NAPALM (Network Automation and Programmability Abstraction Layer with Multivendor support) Python Library* (URL: <https://napalm.readthedocs.io/en/latest/index.html>)

[19] *icinga2 - Icinga Open Source Monitoring* (URL: <https://www.icinga.com/products/icinga-2/>)