HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

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

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 Erkenntnisse 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 Wochentlichen 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

Der Abstract richtet sich an den Spezialisten auf dem entsprechenden Gebiet und beschreibt daher in erster Linie die (neuen, eigenen) Ergebnisse und Resultate der Arbeit. Es umfasst nie mehr als eine Seite, typisch sogar nur etwa 200 Worte (etwa 20 Zeilen). Es sind keine Bilder zu verwenden.

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 Reportingfunktionion 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 verschiensten 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.)

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 Aktoren oder in Form von User Stories mit Personas)
- Wichtigste NFA/Qualitätsattribute abgedeckt und überprüfbar beschrieben

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?)

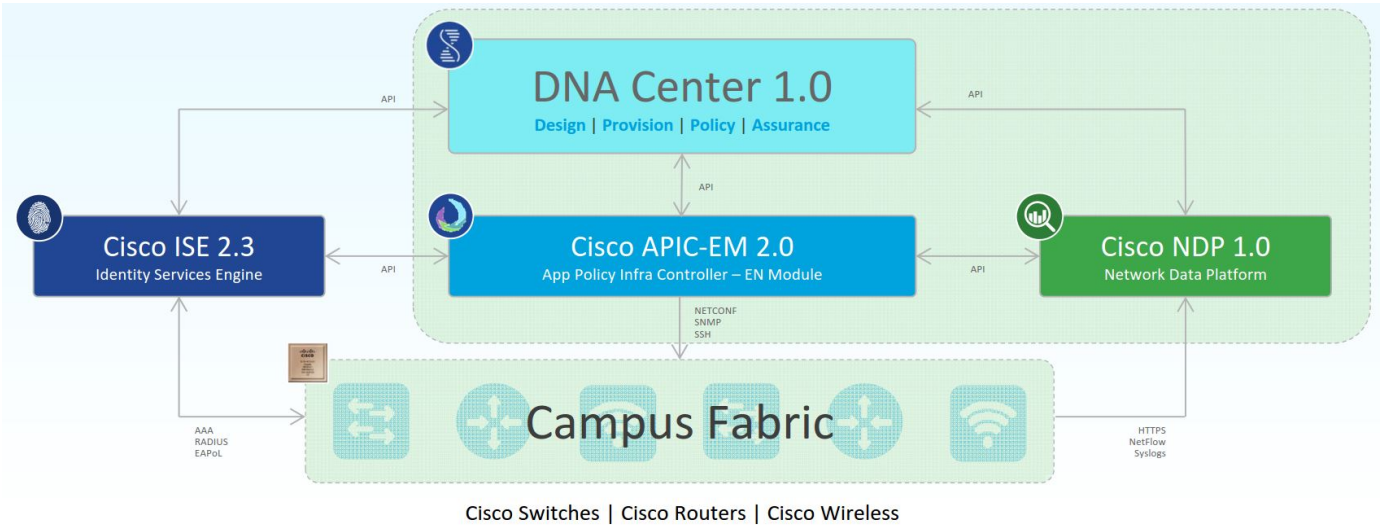


Abbildung 6.1: DNAC Komponenten

7 Technologien

7.1 Software Defined Access (SDA)

Cisco bietet mit SDA eine automatisierte End-to-End-Segmentierung um den Benutzer-, Geräte- und Anwendungsverkehr zu trennen, ohne das Netzwerk neu zu gestalten. Durch diesen automatisierten Benutzerzugriff ermöglicht SDA Einrichtungen innert 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. [1]

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.
Cisco hat nun ein neues Overlay für diesen Zweck erfunden, die "Campus Fabric". Das Overlay ist hierbei eine Kombination aus LISP und VXLAN. [2]

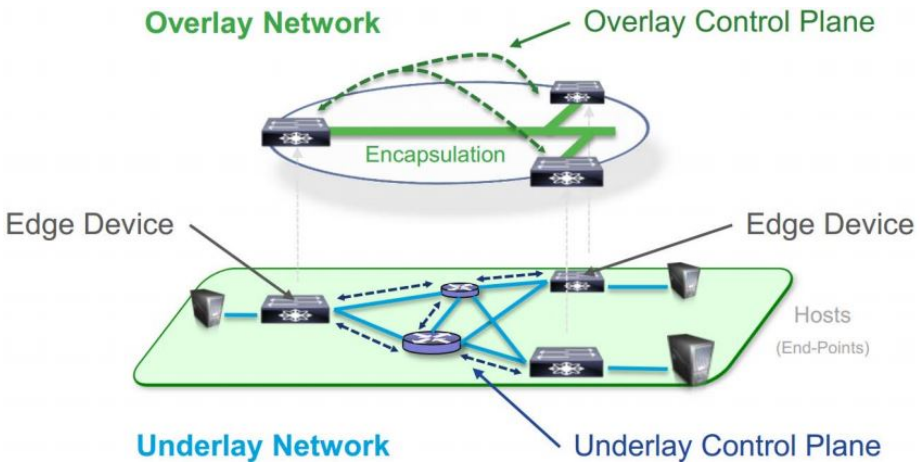


Abbildung 7.1: Campus Fabric

[1] SDA Cisco Definition: https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html

[2] Campus Fabric: https://www.cisco.com/c/dam/m/hr_hr/training-events/2017/cisco-connect/pdf/Cisco-Campus-Fabric-Introduction.pdf

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

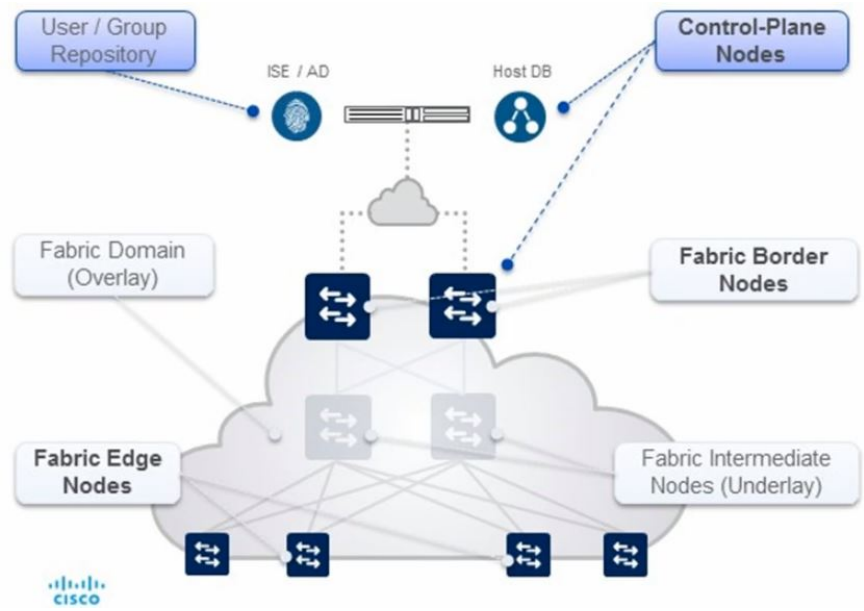


Abbildung 7.2: Fabric Rollen und Terminologie

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

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

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 7.3: 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 zB Infoblox werden nur über die DNA Center Oberfläche konfiguriert.

SD-Access ist die Grundlage von Cisco DNA. Es ermöglicht Netzwerkzugriff in Minuten für jeden Benutzer oder jedes Gerät für jede Anwendung, ohne Kompromisse. Bei SD-Access folgen die festgelegten Richtlinien automatisch dem Benutzer über alle Netzwerkdomänen hinweg.

7.3 Identity Service Engine (ISE)

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 Identity Services Engine (ISE) und ermöglicht den beiden Anwendungen, Daten auf sichere Weise miteinander zu teilen. 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 Site 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 was wachsende Problem des doppelten Verwendungszwecks der IP-Adressen zu bereinigen. 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 das sich bei einem Aufenthalsortwechsel auch die IP-Adresse des Hosts ändert, was bedeutet das die Identität verloren geht und die alten IP-Verbindungen verfallen.

Dies soll nun durch LISP geändert werden, in dem 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 prefices 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

7.5 Virtual Extensible LAN (VXLAN)

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

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. [1]

7.6 Slack

Slack ist ein webbasierter 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.

8 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.

8.1 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 typsichen Gebäuden nicht möglich.

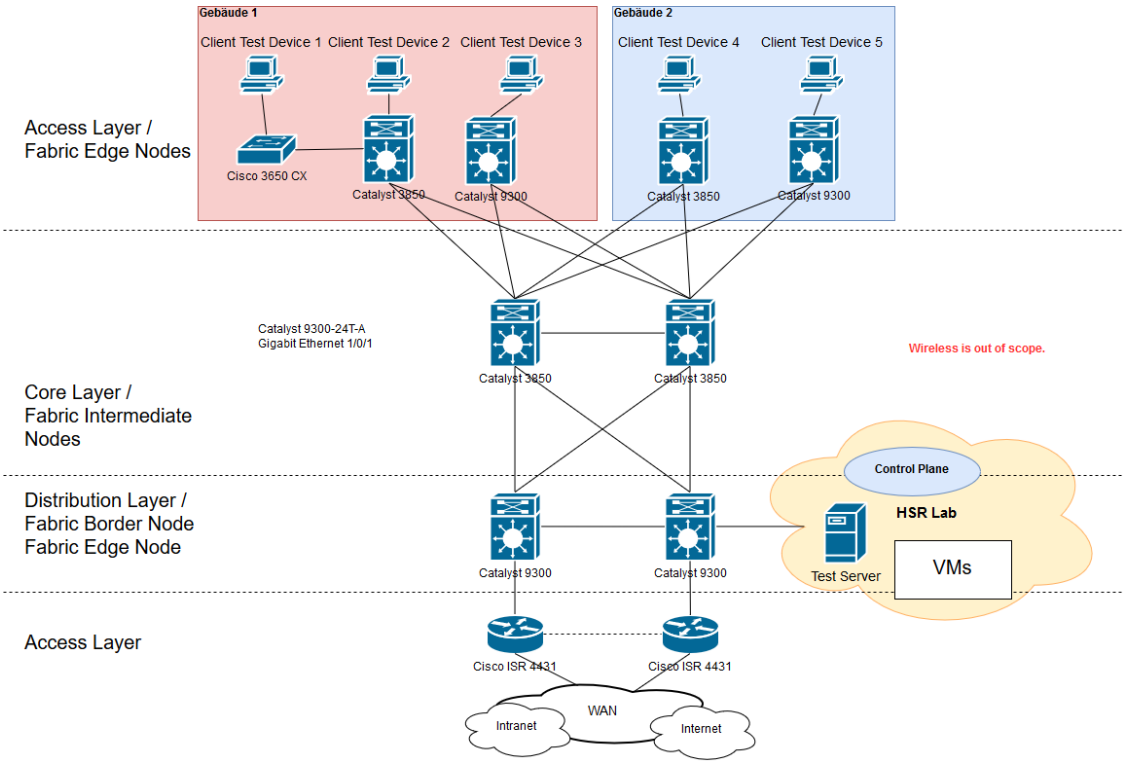


Abbildung 8.1: SDN Netzwerk Architektur

8.2 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 transporteuer 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 phykalische 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.

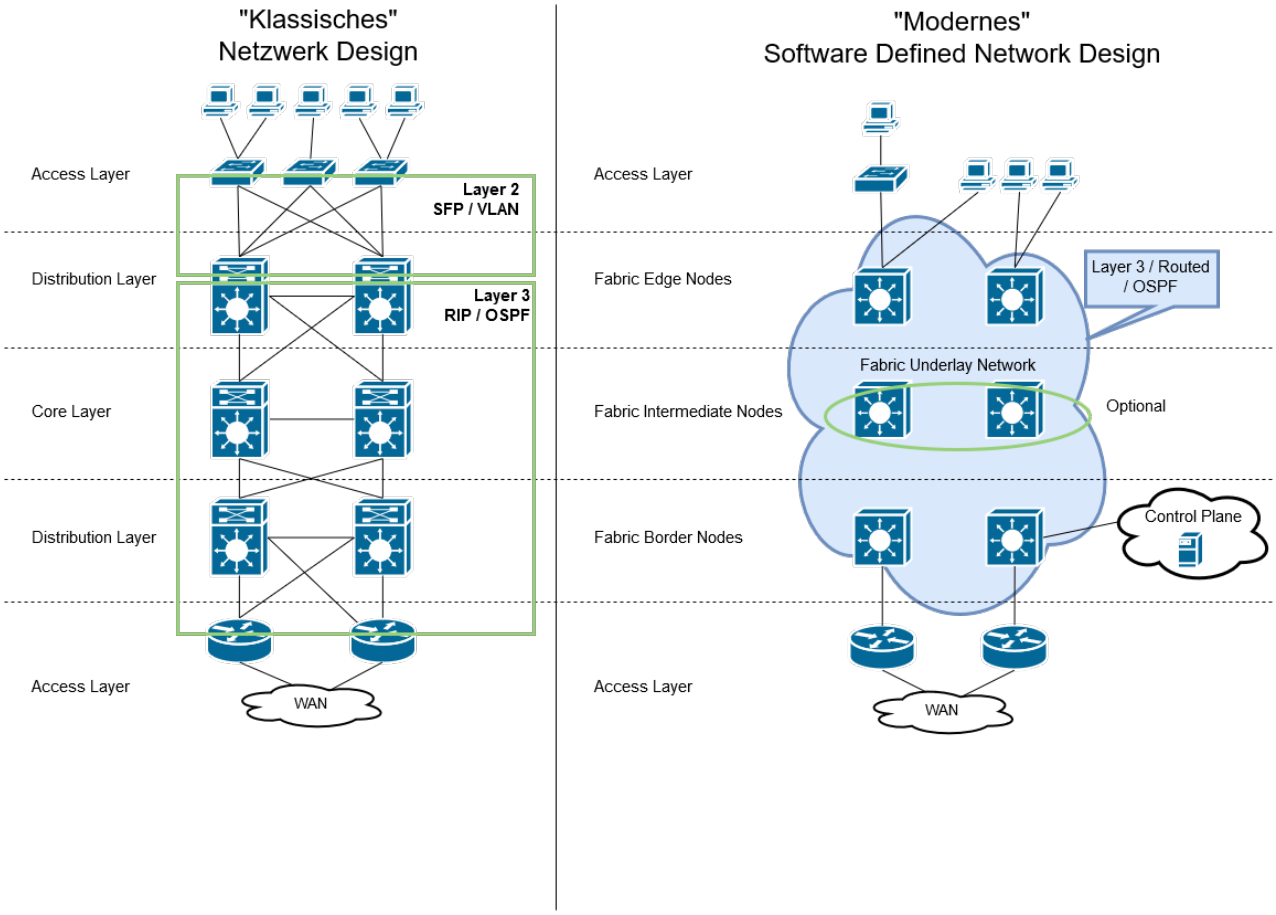


Abbildung 8.2: Netzwerk Architektur Vergleich

8.3 Verkabelungsplan

Verkabelung			
Seite A		Seite B	
isr4431-1.access	port1	WAN	-
isr4431-1.access	port2	isr4431-2.access	port2
isr4431-1.access	port3	c9300-1.dist	port1
isr4431-2.access	port1	WAN	-
isr4431-2.access	port2	isr4431-1.access	port2
isr4431-2.access	port3	c9300-2.dist	port1
c9300-1.dist	port1	isr4431-1.access	port3
c9300-1.dist	port2	c9300-2.dist	port2
c9300-1.dist	port3	c3850-1.core	port1
c9300-1.dist	port4	c3850-2.core	port1
c9300-2.dist	port1	isr4431-1.access	port3
c9300-2.dist	port2	c9300-1.dist	port2
c9300-2.dist	port3	c3850-1.core	port2
c9300-2.dist	port4	c3850-2.core	port2
c3850-1.core	port1	c9300-1.dist	port3
c3850-1.core	port2	c9300-2.dist	port3
c3850-1.core	port3	c3850-2.core	port3
c3850-1.core	port4	c3850-1.access	port1
c3850-1.core	port5	c9300-1.access	port1
c3850-1.core	port6	c3850-2.access	port1
c3850-1.core	port7	c9300-2.access	port1
c3850-2.core	port1	c9300-1.dist	port4
c3850-2.core	port2	c9300-2.dist	port4
c3850-2.core	port3	c3850-1.core	port3
c3850-2.core	port4	c3850-1.access	port2
c3850-2.core	port5	c9300-1.access	port2
c3850-2.core	port6	c3850-2.access	port2
c3850-2.core	port7	c9300-2.access	port2

c3850-1.access	port1	c3850-1.core	port4
c3850-1.access	port2	c3850-2.core	port4
c3850-1.access	port3	c3650-1.access	port1
c3650-1.access	port1	c3850-1.access	port3
c9300-1.access	port1	c3850-1.core	port5
c9300-1.access	port2	c3850-2.core	port5
c3850-2.access	port1	c3850-1.core	port6
c3850-2.access	port2	c3850-2.core	port6
c9300-2.access	port1	c3850-1.core	port7
c9300-2.access	port2	c3850-2.core	port7

9 Ergebnisdiskussion

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

10 Schlussfolgerungen

Zusammenfassung und Ausblick

10.1 Erreichte Ziele

Erreichte Ziele im Bezug auf Aufgabenstellung

10.2 Mögliche Verbesserungen

Was könnte man am erreichten verbessern?

10.3 Zukunft

Ausbaumöglichkeiten

A Installationsanleitung

B Benutzerhandbuch

C Projektmanagement

C.1 Projektplan

C.2 Risiko Management

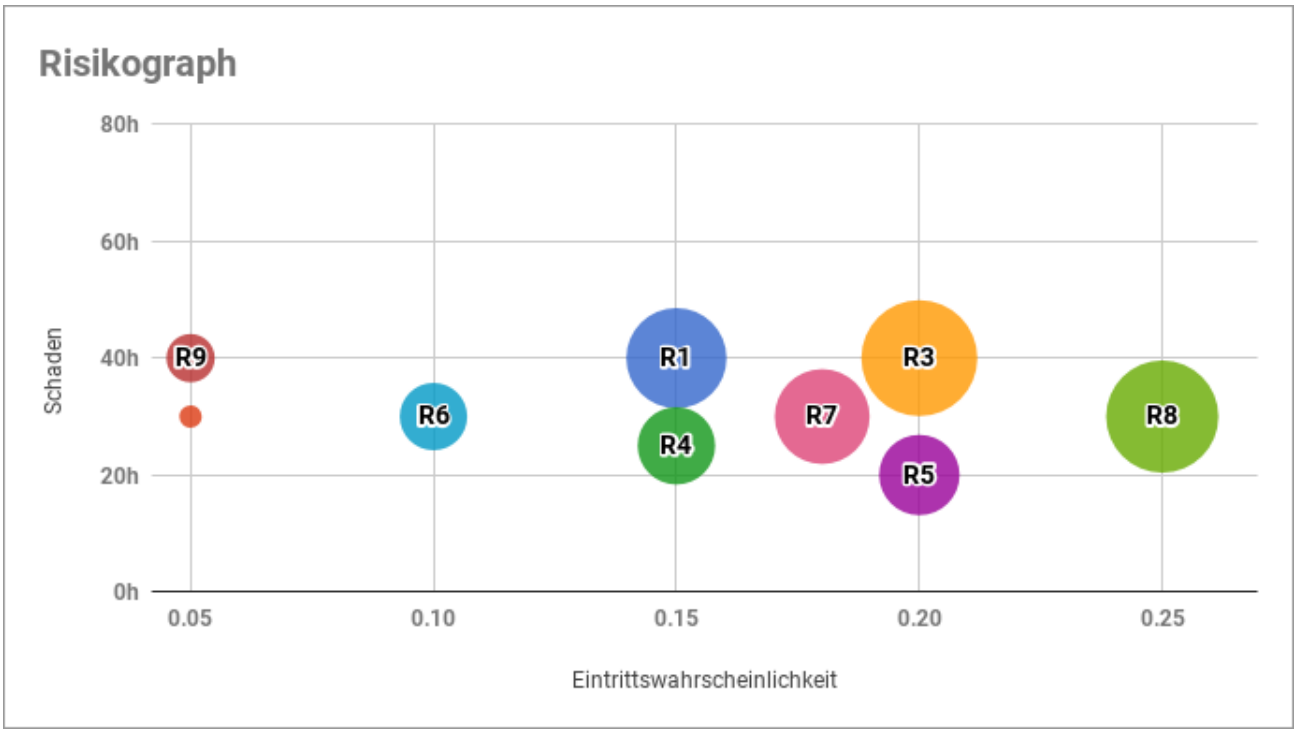
C.2.1 Umgang mit Risiken

Risiken lassen sich leider nicht immer vermeiden. Aus diesem Grund sind nachfolgend mögliche Risiken aufgeführt. Des Weiteren wurden vorbeugende Massnahmen definiert um die Eintretenswahrscheinlichkeit 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.2.2 Risiken

Nummer	Titel	Beschreibung	maximaler Schaden [h]	Eintrittswahrscheinlichkeit	Gewichteter Schaden [h]	Vorbeugung	Verhalten beim Eintreten
1	Ausfall eines Teammiglieds	Ausfall auf Grund unvorhergesehener Erreignisse wie Krankheit, Unfall etc.	40	15%	6	Reserven einplanen, Kommunikation sicherstellen, sodass der Rest Aufgaben übernehmen kann	Tasks des ausgefallen Mitglieds möglichst auf den Rest des Teams aufteilen.
2	Hardwareausfall DNA-Center	DNA-Center Appliance fällt durch Hardwaredefekt aus	30	5%	1.5	keine Verbeugenden Massnahmen möglich	Austausch im Rahmen der Garantie veranlassen
3	Fehlendes Know How	Da viele der Themen neu sind, kann entsprechendes Wissen fehlen	40	20%	8	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	25	15%	3.75	Entscheidungen stets mit Begründung dokumentieren	Kann auch mit Hilfe der Doku keine Einigung gefunden werden, fachnlichen Rat des Betreuers einholen
5	Missverständnisse im Team	Im Team herscht Uneinigkeit über bereits getroffene Entscheidungen	20	20%	4	Protokolle führen und Entscheidungen klar dokumentieren	Protokolle und Dokumentationen beiziehen

6	Ausfall Server / Netzwerkinfrastruktur	Ausfall der von der HSR zur Verfügung gestellten Infrastrukturkomponenten	30	10%	3	Keine Vorbeugenden Massnahmen möglich	Sobald die Infrastruktur wieder verfügbar ist, Systeme wieder 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 anpassen
8	Zeitaufwände falsch geschätzt	Auf Grund falscher Schätzungen kommt es zu Verzögerungen im Projekt	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


Risikograph
80h
60h
40h
20h
0h
Schaden
R9
R6
R1
R4
R7
R3
R5
R8
0.05
0.10
0.15
0.20
0.25
Eintrittswahrscheinlichkeit

D Persönliche Summaries

D.1 Sandro Kaspar

D.2 Philipp Albrecht

D.3 Jessica Kalberer

E Sitzungsprotokolle

E.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

E.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 für zwei Use Cases:
  - 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

E.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 Infrastuktur?

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 Switche 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 Netzwerklabor.
    - 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

E.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	Metzger
Verkabelungsplan erstellen (Switch Ports)	x
IP-Adressen Plan	x
Mapping zwischen SDA und LISP Name Definitions	x
Regelmässige Updates der Doku an Betreuer	x

Nächster Termin

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

Kommende Abwesenheiten

keine

E.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

Beschlüsse (Diskussion)

- x
  - x
- x
- x

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
x	x

Nächster Termin

- Meeting mit Betreuer: 27. März 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

Jessica Kalberer

E.6 Sitzungsprotokoll 27.03.2018

Sitzungsteilnehmer

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

Traktanden

- x
- x
- x
- x

Beschlüsse (Diskussion)

- x
  - x
- x
- x

Offene Punkte (erledigt vor nächster Sitzung)

Was	Verantwortlichkeit
x	x

Nächster Termin

- Meeting mit Betreuer: 03. April 2018, 15.10 Uhr, 60 Minuten

Kommende Abwesenheiten

keine

F Erklärungen

F.1 Eigenständigkeitserklärung

F.2 Urheberrechtsvereinbarung

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

[1] RFC7348 *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying 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)