HSR Cloud Infrastructure Lab 2

Design an enterprise network based on customer specifications

Emanuel Duss, Roland Bischofberger

9. Oktober 2014

Inhaltsverzeichnis

1 Aufgabenstellung

1.1 Einleitung

Entnommen aus der Aufgabenstellung:

> The fictional company BetaHouse Inc. is specialized in the high-frequency trading sector. In this exercise you will design the LAN part of the network, based on customer specifications. Part two will focus on the WAN integration with several remote locations throughout Switzerland (10+). Start with analyzing and characterizing the desired goals. Then go ahead with a logical network design. Based on that define the physical network. Document, review and change if needed until you get a satisfying solution. It's important to describe your design decisions in your documentation.

1.2 Wichtige Angaben

- Firma BetaHouse Inc.
- LAN- und WAN-Design erstellen
- 10+ remote Lokationen mit WAN verbinden
- Datacenter nur als Building Block einzeichnen, da Task für nächste Woche
- Das Internet muss nicht nacht Herstellern und Preisen durchsucht werden

1.3 Aufbau des Kunden

1.3.1 Headquarter

- 4 stöckiges Gebäude
  - 1st floor banking employees and guest WLAN
  - 2nd floor banking employees
  - 3rd floor trading employees
  - 4th floor HR and IT employees
- Angestellte
  - Banking: 30 person
  - IT: 10 person
  - HR: 20 person
  - Trading: 30 person
  - Every user needs a VoIP phone
  - Every 10 users needs a printer
- Trading must be redundant
- Datacenter is a black box for the moment

1.3.2 Branch Office

- 50 Banking employees per branch
- Employees access the terminal server and private cloud application at the HQ.

1.4 Annahmen und Einschränkungen

- Die User führen alle Arbeiten auf dem Terminalserver aus (Office, Drucken, Mailing, Web, ...)
- Firewallregel Branch Office
  - Ausgehend nur Terminalserver und VoIP
  - Eingehend nur Druckjobs
- Die Mail- und Webserver stehen in der DMZ der Firma.

2 Requirements

2.1 Business Requirements

Die Firma BetaHouse Inc. möchte den Benutzern eine stabile Arbeitsumgebung bieten.

Da einige finanzkritische Situationen vorhanden sind, wie zum Beispiel die Arbeiten der Abteilung "Trading", müssen diese Netzwerkbereiche eine besonders hohe Verfügbarkeit aufweisen.

Ein Ausfall einer Branch für einen Tag kostet mindestens CHF 20'000.00. (Berechnung vgl. Kapitel "WAN Design → Redundanz und Verfügbarkeit")

2.1.1 Growth in 5 years

Im Headquater wie auch in den Branches ist ein Zuwachs von beinahe 50% der Angestellten möglich und ohne Probleme umsetzbar.

In den nächsten Jahren wird die Firma einen Branch Zuwachs erhalten. Da die Branches per MPLS an der Firmennetz angeschlossen werden, ist dies optimal skalierbar für die Zukunft.

Im Gegensatz zu einer Mietleitung kann MPLS viel dynamischer ausgebaut werden und ein neuer Branch einfach in die "MPLS-Wolke" eingehägt werden. Bei einer Mietleitung muss bei jedem neuen Branch eine neue eigene Mietleitung dazugekauft werden.

Im Gegensatz zu Frame Relay bietet MPLS eine höhere Bandbreite.

Die neu gekaufte Hardware soll auch den IPv6 Stack unterstützen, damit in Zukunft auch Services genutzt werden können, die nur per IPv6 angeboten werden. Durch die Unterstützung von IPv6 können in Zukunft auch die eigenen Services (Mail- und Webserver) mit IPv6 angeboten werden.

Im Gegensatz zu Nicht-IPv6 Hardware, könnten so in naher Zukunft enorme Kosten entstehen, wenn man die Hardware austauschen müsste.

2.2 Technical Requirements

2.2.1 Availability

Vgl. direkt in den Kapiteln LAN und WAN Design.

2.2.2 Redundancy

Vgl. direkt in den Kapiteln LAN und WAN Design.

3 LAN Design

3.1 Anforderungen des Kunden

Vgl. Kapitel "Aufgabenstellung" und "Requirements".

3.2 Campus LAN Design

3.2.1 Architektur und Topologie

Topologie vgl. Anhang. Beschreibung hier:

Cisco empfiehlt für Medium Campus eine 3-Tier Architektur.

Im Keller vom Headquarter befinden sich zwei Core Router, welche an die Distribution Switches im 2. und 3. Stock des Headquarters gehen. Diese Distribution Switches führen an die Access Switches, wo die Mitarbeiter angeschlossen werden.

Wir gehen mit dem Layer 3 bis zu den Access Switchen, damit wir das Spanning Tree Protocol nicht benötigen. Dies wollen wir in diesem kritischen Netz nicht einsetzen, da es bei einem Ausfall länger dauern kann, bis der Baum wieder aufgebaut wurde und das bei den Finanzkritischen Arbeiten nicht zu verantworten ist.

3.2.2 VoIP

Die VoIP Phones werden über die Single-Cable Methode angeschlossen. Sprich der Computer wird an das VoIP Phone und das VoIP Phone an den Switch angeschlossen. Somit spart man pro Mitarbeiter ein Kabel und ein Switchport. Da das Trading eine höhere Priorität hat und die Ausfälle so gering wie möglich sein sollen, wird dort das VoIP Phone und der Computer der Mitarbeiter separat angeschlossen. Somit kann der Mitarbeiter den Computer auch weiterhin benutzen, falls das VoIP Phone nicht mehr richtig funktioniert.

3.2.3 Verkabelung

Zwischen den Core Switches und von den Core Switches in das Datacenter wir dein MMF Kabel mit 10Gbps und einer Wellenlänge von 850nm verwendet. Zwischen den CS und den DS Switches werden pro Verbindung zwei Cat6 Twisted Pair Kabel mit je 1Gbps im Port Channel Modus verwendet. Alle anderen Verbindungen im HQ und in den Branches werden mit Cat6 Kabel (1Gbps) realisiert. Alle Endgeräte, die an den Access Switches angeschlossen sind, werden mit Cat5e Kabel verbunden.

3.2.4 Benötigte Accessports

Folgende minimale Anzahl der Accessports sind laut der Aufgabenstellung nötig:

Ort	Abteilung	Mitarbeiter	Printer	Benötigte Accessports
1. Stock	Bank	15	2	$15 + 2 = 17$
2. Stock	Bank	15	2	$15 + 2 = 17$
3. Stock	Trading	30	3	$30 \cdot 2 + 3 = 63$
4. Stock	HR, IT	$20 + 10 = 30$	2	$30 + 2 = 32$
Branch	Bank	50	5	$50 + 5 = 55$

3.2.5 Redundanz und Verfügbarkeit

Für die Trading Abteilung werden 4 · 24 Port Switches benötigt. Die 30 Mitarbeiter werden auf die 4 Switches aufgeteilt. Das gibt 8 Mitarbeiter pro Switch. Durch die doppelte Portbelegung (Computer + VoIP Phone) sind pro Switch also 16 Ports von den Mitarbeitern belegt. Bei einem Switchausfall können die 8 Mitarbeiter (mit 16 Ports) auf zwei andere Switches umverteilt werden.

Für die anderen Stockwerke ist jeweils nur ein Switch nötig. Dafür wird ein Backupswitch vom Support aufbewahrt, welcher in einem Ausfall schnell eingetauscht werden kann. Die Konfiguraiton aller Switches wird regelmässig gesichert und versioniert abgespeichert. Somit kann der Support bei einem Switchausfall die letzte Konfiguration auf den Backupswitch spielen und diesen installieren.

3.2.6 Major Traffic Flow

Die Benutzer arbeiten auf den Terminalservern. Das heisst, es muss nur das Bild von den Servern zu den Benutzern übertragen werden.

Druckaufträge werden von den Terminalservern auf einen Printserver verschickt und von dort aus auf die Drucker.

Der grösste Datenfluss findet somit zwischen dem Datacenter und den Access Switches im HQ und in den Branches statt.

3.2.7 Application QoS

Höchste Priorität im Netzwerk hat der Verkehr der Tradingapplikation und der Terminalsessions. Somit kann sichergestellt werden, dass die Tradingabteilung immer mit besten Antwortzeiten bedient werden kann.

3.3 Adressierungs- und Namensschema

Das Basisnetz ist `10.10.0.0/16`.

3.3.1 Adressbereich Netzwerkkomponenten

Die Punkt zu Punkt Verbindungen kommen in folgende Netze:

Subnetz	Beschreibung
`10.10.0.0/30`	Punkt-zu-Punkt Verbindung 1
`10.10.0.4/30`	Punkt-zu-Punkt Verbindung 2
`10.10.0.8/30`	Punkt-zu-Punkt Verbindung 3
`10.10.0.12/30`	Punkt-zu-Punkt Verbindung 4
...	Punkt-zu-Punkt Verbindung ...

Die Zuordnung der Subnetze zu den Switchen ist in der physikalischen Topologie zu sehen.

3.3.2 Adressbereich Headquarter

Folgende Netze sind im Headquarter vorhanden:

Subnetz	VLAN	Beschreibung
10.10.10.0/24	100	Server
10.10.20.0/24	200	Bank
10.10.21.0/24	201	Trading
10.10.22.0/24	202	HR
10.10.23.0/24	203	IT
10.10.28.0/23	210	VoIP
10.10.31.0/24	301	Management
10.10.40.0/24	400	Guest

3.3.3 Adressbereich Branches

Jeder Branch erhält ein eigenes Subnetz. Dies sind die Subnetze der Branches:

Subnetz	Beschreibung
10.10.101.0/24	Branch 01
10.10.102.0/24	Branch 02
...	...
10.10.109.0/24	Branch 9
10.10.110.0/24	Branch 10
...	...

Die Netze von jedem der Branches wird wieder in Subnetze unterteilt:

Subnetz	VLAN	Beschreibung
10.10.n.0/25	5n	Banking Clients und Drucker
10.10.n.128/25	6n	VoIP

Dabei steht *n* für die zweistellige Branch-Nummer. z.B. 01 oder 10.

3.4 Technologien

3.4.1 Layer 2 Protokolle

Auf das Spanning Tree Protocol wird verzichtet, da die Konvergenzzeit sehr gross ist, und das bei der Trading Abteilung nicht verantwortbar ist.

In den Branches wurden für das Banking und das VoIP je ein eigenes VLAN definiert, damit nicht eine grosse Broadcast Domäne über alle Branches und das HQ entsteht.

Folgende VLANs werden definiert:

Nummer	Name
100	Server

Nummer	Name
200	Bank
201	Trading
202	HR
203	IT
210	VoIP_HQ
301	Management
400	Guest
501	Bank_BR1
502	Bank_BR2
...	...
510	Bank_BR10
601	VoIP_BR1
602	VoIP_BR2
...	...
610	VoIP_BR10

3.4.2 Layer 3 Protokolle

Als dynamisches Routing Protokoll wird OSPF mit einer einzigen Area verwendet. Der Layer 3 wird bis auf den Access Layer gezogen, damit im Gegensatz zu einer Architektur mit STP, ein schneller Failover möglich ist.

3.4.3 Security

Das Guest WLAN im 1. Stock des Headquarters ist in einem separatem VLAN (400), damit die Gäste keinen Zugriff auf das interne Firmennetz haben.

Für die Verbindung ins Internet werden zwei Firewalls verwendet. Diese Firewalls sind für den Active/Active-Failover konfiguriert. Sobald eine Firewall der beiden ausfällt, übernimmt die andere die Aufgaben der anderen Firewall. Wenn beide Firewalls aktiv sind, wird ein Loadbalancing gemacht. Die somit redundanten Firewalls trennen die DMZ und das Intranet voneinander ab. In der DMZ stehen die Web- und Mailserver.

3.5 Liste mit Komponenten

3.5.1 Komponenten Headquarter

Anzahl	Ort	Komponente	Hostname	Beschreibung
1x	1. Stock	L3 Access Switch	HQ-AS1	48 · 100 Mbps, 2 · 1 Gbps
1x	2. Stock	L3 Access Switch	HQ-AS2	48 · 100 Mbps, 2 · 1 Gbps
4x	3. Stock	L3 Access Switch	HQ-AS3..AS4	24 · 100 Mbps, 2 · 1 Gbps
1x	4. Stock	L3 Access Switch	HQ-AS5	48 · 100 Mbps, 2 · 1 Gbps
1x	2. Stock	L3 Distribution Switch	HQ-DS1	11 · 1 Gbps Kupfer

Anzahl	Ort	Komponente	Hostname	Beschreibung
1x	3. Stock	L3 Distribution Switch	HQ-DS2	11 · 1 Gbps Kupfer
2x	Keller	Core Router	HQ-CO1..2	2 · 100 Mbps, 6 · 1 Gbps, 3 · 10 Gbps Glas
2x	Keller	ISP Router	HQ-ISP1..2	Von zwei unterschiedlichen ISPs bezogen
2x	Keller	Firewalls	HQ-FW1..2	Für DMZ, Intranet
1x	Eingang	802.11n Accespoint	HQ-WLANPUB	WLAN für die Gäste

3.5.2 Komponenten Branch

Anzahl	Ort	Komponente	Hostname	Beschreibung
2x	Branch Office	Access Switch	BRn-1..2	48 Port

Die Variable `n` steht für die Branches, welche durchnummeriert sind.

4 WAN Design

4.1 Design

Die Branch Offices werden via MPLS mit dem Headquarter verbunden. Dies hat den Vorteil gegenüber einer Mietleitung, dass das Netz so in Zukunft gut ausgebaut werden kann. Ein neues Branch Office kann schnell über MPLS in das bestehende Netz eingebunden werden.

4.2 Anforderungen des Kunden

Vgl. Kapitel "Aufgabenstellung" und "Requirements".

4.3 WAN Design

Topologie vgl. Anhang.

4.3.1 Redundanz und Verfügbarkeit

Auch die Branches werden redundant an das MPLS Netz angeschlossen. Wir gehen davon aus, dass ein Mitarbeiter der Bank CHF 8000.00 pro Monat verdient. Das ergibt pro Arbeitstag CHF 380.00. Fällt einmal pro Jahr ein Switch oder CERouter in irgendeinem Branch Office aus, ergibt das bei den 50 Mitarbeitern einen Verlust von mindestens CHF 20'000.00 (Lohnkosten). Deshalb lohnt es sich pro Branch zwei CE Router sowie zwei Switches zu beziehen.

4.4 Technologien

4.4.1 Layer 2 Protokolle

Auf Layer 2 werden im WAN Bereich keine speziellen Protokolle benötigt.

4.4.2 Layer 3 Protokolle

Als dynamisches Routing Protokoll wird OSPF mit einer einzigen Area verwendet.

4.4.3 Major Traffic Flow

Die Benutzer arbeiten auf den Terminalservern. Das heisst, es muss nur das Bild von den Servern zu den Benutzern übertragen werden.

Druckaufträge werden über den Terminalserver auf einen Printserver in den Branches verschickt. Dieser Printserver verarbeitet den Druckauftrag in der jeweiligen Branch.

Der grösste Datenfluss findet somit zwischen dem Datacenter und den Access Switches im HQ und in den Branches statt.

4.4.4 Application QoS

Damit die VoIP-Sprachqualität vom Traffic der Terminalserver und den Druckjobs nicht beeinträchtigt wird, bekommt der VoIP Traffic eine höhere Priorität als die Terminalserver und Druckjobs. Die Druckjobs bekommen die niedrigste Qualität, da es dort nicht stört, wenn dieser etwas verspätet ankommt.

4.5 Security

Da die Daten innerhalb von MPLS als Klartext übertragen werden, müssen die im OSI Modell darüberliegenden Schichten für eine Verschlüsselung sorgen. Zuerst einmal werden auf den CE Router folgende Regeln für eine Firewall mit stateful inspection definiert:

Nr.	From	To	Port	Protocol	Note
1	Internal	External	3389	TCP	Terminalserver
2	Internal	External	5060	TCP	SIP
3	External	Internal	5060	TCP	SIP
4	External	Internal	631	TCP	IPP

Die Session zum Terminalserver wird mit TLS verschlüsselt.

In jedem Branch Office gibt es einen Printserver, welcher die Druckaufträge vom Terminalserver entgegennimmt. Das IPP Protokoll wird ebenfalls TLS verschlüsselt.

4.6 Komponenten

4.6.1 Komponenten Headquarter

Für die Anbindung ans MPLS Netz wird folgende Hardware benötigt:

Anzahl	Ort	Komponente	Hostname	Beschreibung
2x	Keller	MPLS CE Router	HQ-CE1..2	2 Port

4.6.2 Komponenten Branch Office

Für die Anbindung ans MPLS Netz wird folgende Hardware benötigt:

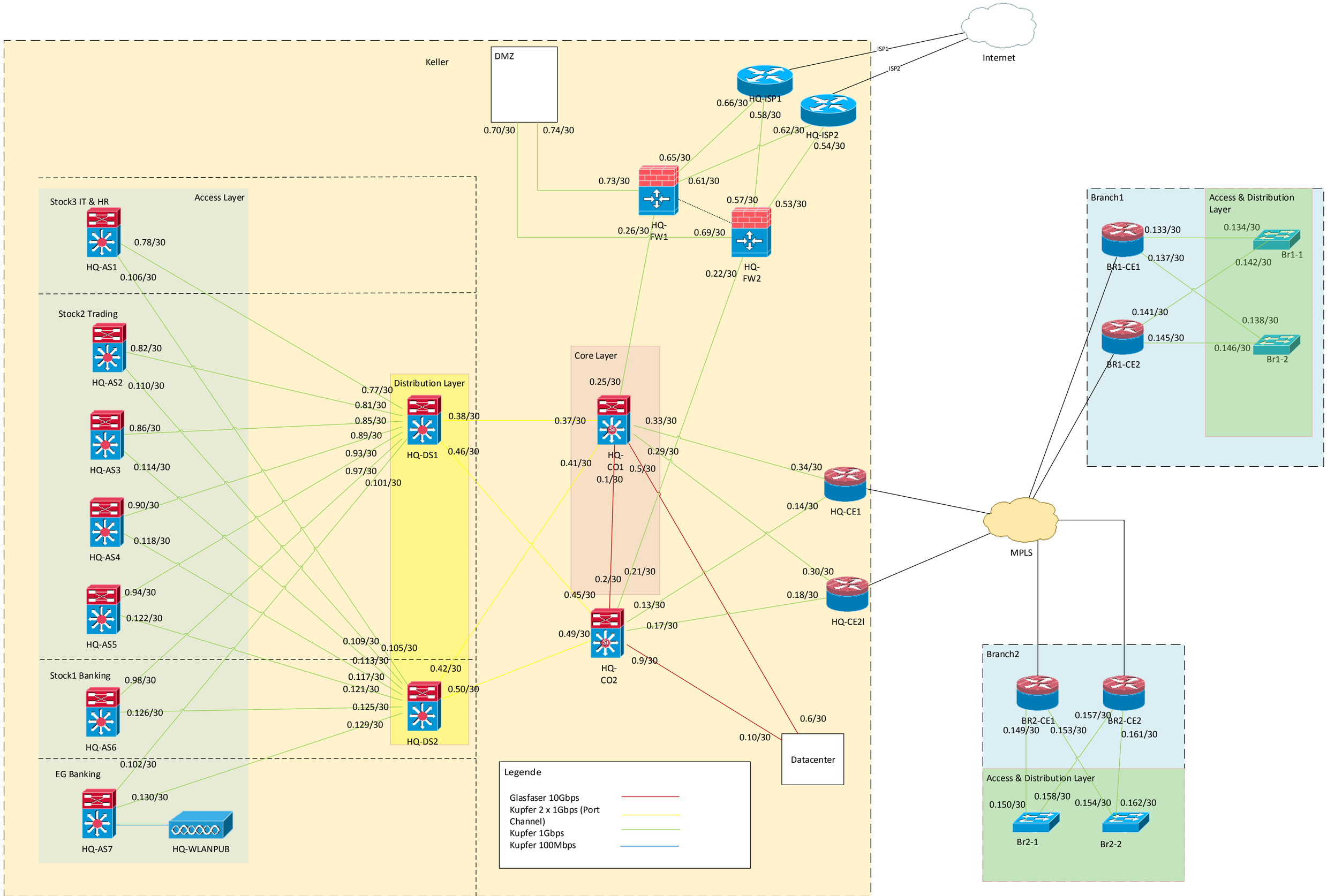
Anzahl	Ort	Komponente	Hostname	Beschreibung
2x	Keller	MPLS CE Router	BRn-CE1..2	2 Port

Die Variable `n` steht für die Branches, welche durchnummeriert sind.

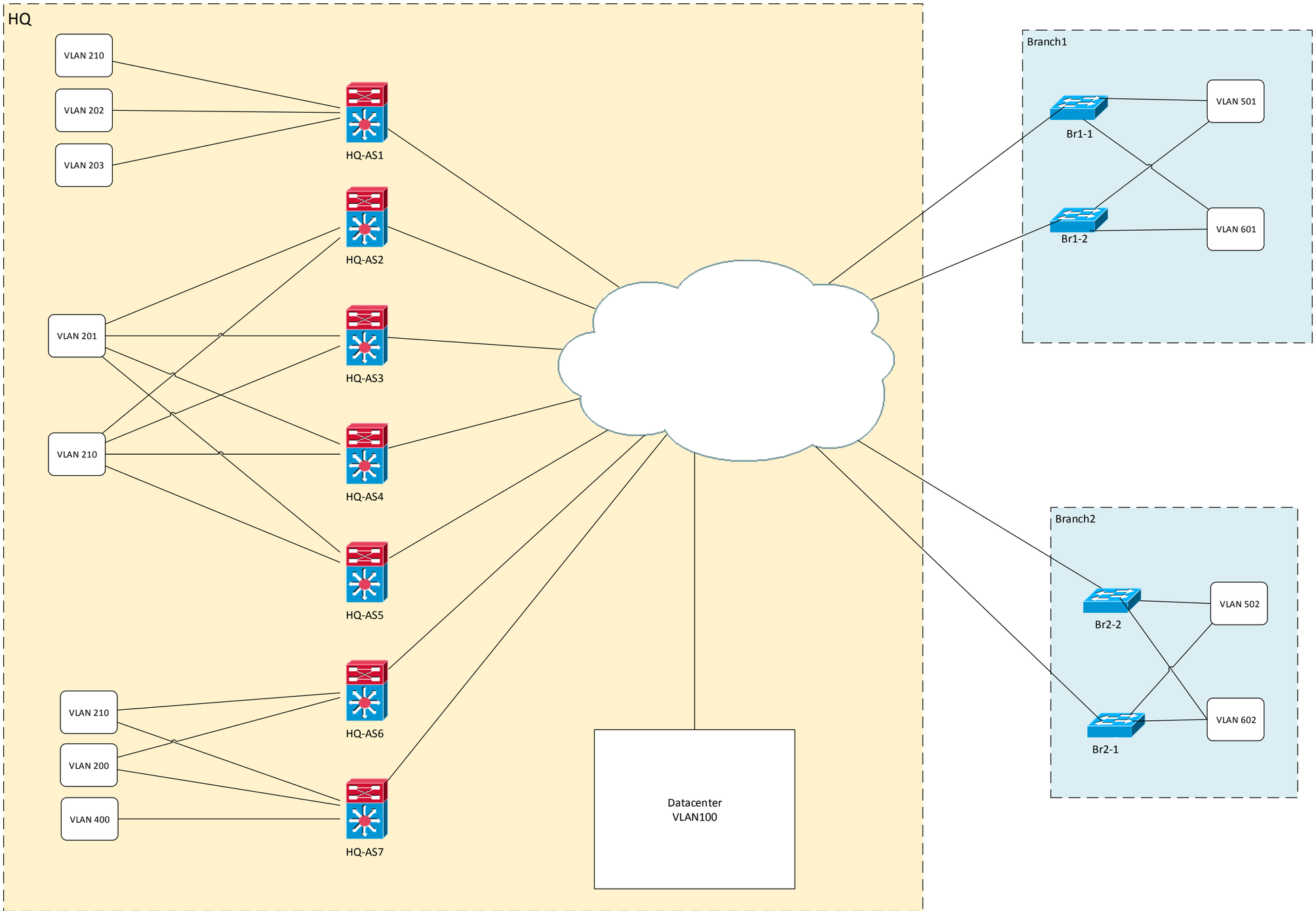
5 Links und weitere Informationen

- Cisco Design Guide: http://www.cisco.com/go/srnd → Infrastructure → Design Zone for Borderless Networkse
- Borderless Campus 1.0 Design and Deployment Models. Cisco. 2011.

Beta House Inc. 10.10.0.0/16



VLAN Übersicht



VLAN Übersicht

Nummer	Name
`100`	Server
`200`	Bank
`201`	Trading
`202`	HR
`203`	IT
`210`	VoIP_HQ
`301`	Management
`400`	Guest
`501`	Bank_BR1
`502`	Bank_BR2
`601`	VoIP_BR1
`602`	VoIP_BR2