Report

Cloud Infrastructre Lab 3

Fabian Hauser and Michael Wieland

Hochschule für Technik Rapperswil

14. Oktober 2016

Inhaltsverzeichnis

1. Datacenter Design

1.1. Grundlegendes

Wie auch im Campus Network wird auch das Datacenter in drei Layer unterteilt.

Access Layer
Verbindet die Endgeräte mit dem weiteren Netzwerk. Regelt Port Security, VLAN's und PoE.

Aggregation Layer
Switches fassen Datenströme aus dem Access Layer zusammen. Regelt das Routing zwischen den VLANs und QoS.

Core Layer
Regelt den Verkehr im Backbone

1.2. Anforderungen

Für die Firma BetaHouse Inc. muss ein hochverfügbares, skalierbares und redundantes Datacenter designed werden, welches Platz für folgende Geräte bietet.

Anzahl	Typ	Bereich
30	Server	IT
30	Server	HR
30	Server	Trading
2	Core Switch	Core Tier
3	Aggregation Switch	Aggregation Tier
6	Access Switch	Access Tier

Tabelle 1: Server und Switches

1.2.1. Sicherheit

Die einzelnen Netze der Abteilungen müssen strikt getrennt werden. Es darf keine Konnektivität zwischen den Abteilungen ohne explizite Ausnahme stattfinden.

1.2.2. Verfügbarkeit und Redundanz

In Punkto Ausfallsicherheit wird ein Tier-3 Datacenter angestrebt, was eine Verfügbarkeit von 99.982% verspricht. Das Datencenter muss rund um die Uhr betriebsbereit zur Verfügung stehen und Wartungen müssen unbemerkt bleiben. Das Netzwerk besteht aus mehreren Pfaden, wobei durch STP immer nur ein Pfad aktiv verwendet wird.

Geo Redundanz Bei Datacenter von diesem Umfang, sollte eine geografische Redundanz in Betracht gezogen werden. Dabei wird ein zweites Datacenter an einem anderen Standort aufgebaut. Im Fehlerfall kann auf dieses umgeschalten werden.

Beschreibung	Anforderung
Versorgungswege Elektro/Kühlung	1 aktiv, 1 passiv
Redundanz Aktivkomponenten	N + 1
Backbone Redundanz	ja
Redundanz Horizontaltverkabelung	nein
USV und Generator	ja
Unterbruchsfreie Wartung	ja
Verfügbarkeit	99.982%

Tabelle 2: Tier 3 Infrastruktur

1.3. Skalierbarkeit

Das Datacenter sollte so skalierbar sein, dass es dem Wachstum einer Firma nachkommen kann. Dies bedingt den Einsatz eines Core Layers, damit der Aggregation Layer ohne weiteres ausgebaut werden kann.

1.3.1. Infrastruktur

Ein Datacenter stellt naturgemäss folgende Anforderungen an die Gebäudeinfrastruktur.

- Geeignetes Kühlungssystem
- Schutz gegen Stromausfälle mittels USV und Dieselgeneratoren
- Erdung und Schutz gegen Spannungsschwankungen
- Zugangsschutz gegen unerlaubten Zutritt
- Schutz gegen externe Gefahrenfaktoren wie Naturkatastrophen, Luftverkehr und andere Gefahren die von der Umgebung ausgehen können.

1.3.2. Core Layer

Im Core Layer geht es im speziellen um die Geschwindigkeit sowie Hochverfügbarkeit und Redundanz. Da im Core die Daten des Aggregation Layer zusammengefasst werden, müssen grosse Datenmengen performant verarbeitet werden können. Dadurch entstehen hohe Betriebstemperaturen, weshalb die Geräte im Core permanent herunter gekühlt werden müssen.

1.3.3. Verkabelung

Bei der Verkabelung wird bis zu den Access Switches Glasfasern eingesetzt. Um Kosten zu sparen werden die Server aber mit Kupferkabel angeschlossen.

1.3.4. Server

Auch bei den Server ist Redundanz gefordert, weshalb alle Server über 5 Anschlüsse verfügen müssen.

- 2 für das LAN
- 2 für das SAN (Fibre Channel übers Glas oder FCoE)
- 1 für KVM (Keyboard/Video/Mouse)

1.4. Physisches Design

Die Netzwerkgeräte werden gemäss der Top of Rack (ToR) Architektur organisiert. Diese eignet sich insbesondere für Hochgeschwindigkeitsverbindungen, welche im Highfrequency Trading gefordert sind. Mit der gewählten Architektur können 10Gib-Ethernet Anforderungen leicht bewältigt werden. Im oberen Bereich eines jeden Racks wird ein Access Switch positioniert. Die Architektur bietet klare Vorteile:

- kleineres Kabelvolumen, was das System wartbarer macht. Zusätzlich sind die Installationskosten geringer
- geeignet für hohe Serverdichte, wie dies bei 90 Server zuzüglich Switches der Fall ist
- neue Geräte lassen sich relativ einfach hinzufügen

Vorteile einer alternativen End of Row-Architektur wären:

- Hohe Flexibilität, Skalierbarkeit und Zukunftssicherheit
- Effizientere Belegung der LAN Ports und auslastung der Racks
- Konzentration von Access-Switches macht Belegung und Änderungen einfacher

Aufgrund der Anforderungen des Kunden überwiegen die Vorteile der ToR-Architektur.

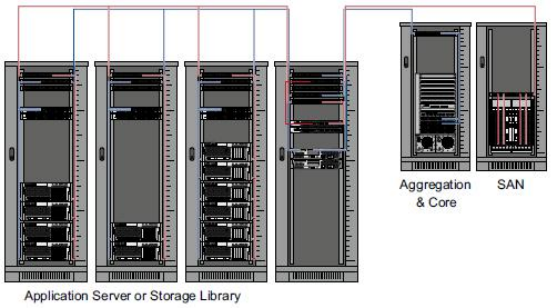


Abbildung 1: ToR Architektur in der Cisco Variante

Abteilung	Anzahl Racks	Gesamtzahl Server
HR	1	30
IT	1	30
Trading	1	30
Netzwerk-Switches	1	5

Tabelle 3: Racks und Server je Abteilung

1.5. Access Layer

Physical Die Server werden mit je zwei Gigabit Kupfer Kabel beim Access Switch angeschlossen. Die beiden Interfaces bekommen die selbe IP Adresse. Fällt ein Interfaces aus, gibt es ein Failover vom Primary zum Secondary.

Layer 2 Die Server im Access Layer sind als Looped Triangle organisiert. Dieser Design Ansatz ist weit verbreitet und verfügt über eine schnelle Konvergenz durch RSTP (802.1w) und MSTP (802.1s). Zusätzlich ist es einfach Load Balancer und Firewalls im Aggregation Layer zu deployen. Um Layer 2 Loops zu verhindern wird Rapid PVST+ eingesetzt. Ein Access Switch übernimmt die Funktion des Primary Root und der zweite dient als Backup (Standby). Um die Verfügbarkeit der Standardgateways hoch zu halten, wird das Cisco propertietäre HSRP (Hot Standby Routing Protocol) eingesetzt. Dabei werden mehrere physische Router zu einer logischen Gruppe zusammengefasst. Fällt ein Switch der logischen Gruppe aus, können die Server stets noch über den Standby Switch auf das Netzwerk zugreifen.

Layer 3 Der gesamte Traffic wird bis zum Access Layer mit OSPF geroutet. Dies erlaubt es, die Broadcast Domäne der einzelnen Subnetze so klein wie möglich zu halten.

1.5.1. 3 Tier Organisation im Access Layer

Alle externen Zugriffe auf die einzelnen Tiers werden mit Firewalls im Aggregation Layer kontrolliert. Der Zugriffsfluss geht grundsätzlich von oben nach unten. Erlaubt sind nur Zugriffe auf den jeweils nächsten Tier. Also WEB → Application → Database. Die Kommunikation verläuft dann jedoch trotzdem über den Aggregation Layer, der die Zugriffe auf ihre Korrektheit überprüft.

1. WEB Tier Beinhaltet die Webserver

2. Application Tier Beinhaltet die bankenspezifischen Services fürs Trading

3. Database Tier Beinhaltet alle Datenbanken.

VLAN

VLAN	Subnetz	Beschreibung
21	10.200.2.1/26	Webserver
22	10.200.2.65/26	Application
23	10.200.2.129/26	Database

Tabelle 4: VLAN's

1.6. Aggregation Layer

Im Aggregation Layer ist die Security Logik (Firewall etc.) implementiert. Die Requests der Server werden über den Access Layer in den Aggregation Layer weitergeleitet und dort auf ihre Gültigkeit überprüft. Unerlaubte Zugriffe auf fremde Netze werden dort von der Firewall blockiert.

1.7. Core Layer

Bei einem Datacenter dieser Grösse ist der Einsatz eines Core Layers von Vorteil. Der Core bündelt die Geräte im Aggregation Layer, was zu einer besseren Skalierbarkeit führt. Ebenfalls kann im Core ein gewisses Load Balancing zwischen dem Campus Core und dem Aggregation Layer implementiert werden. Für das Routing bis zum Access Layer wird OSPF verwendet.

1.8. Multitenancy

Mittels VRF's können die einzelnen Tenands auf Layer 3 voneinander getrennt werden. Somit kann eine strikte Trennung der einzelnen Abteilungen End zu End umgesetzt werden. Auf Layer 2 kann dies zusätzlich mit VLAN's umgesetzt werden. Dies ist jedoch erst ab dem Access Layer nötig.

Eine alternative zu VRF's wäre es, den kompletten Backbone mit MPLS umzusetzen, welches eine saubere Trennung via VPNs erstellt.

A. Schemes

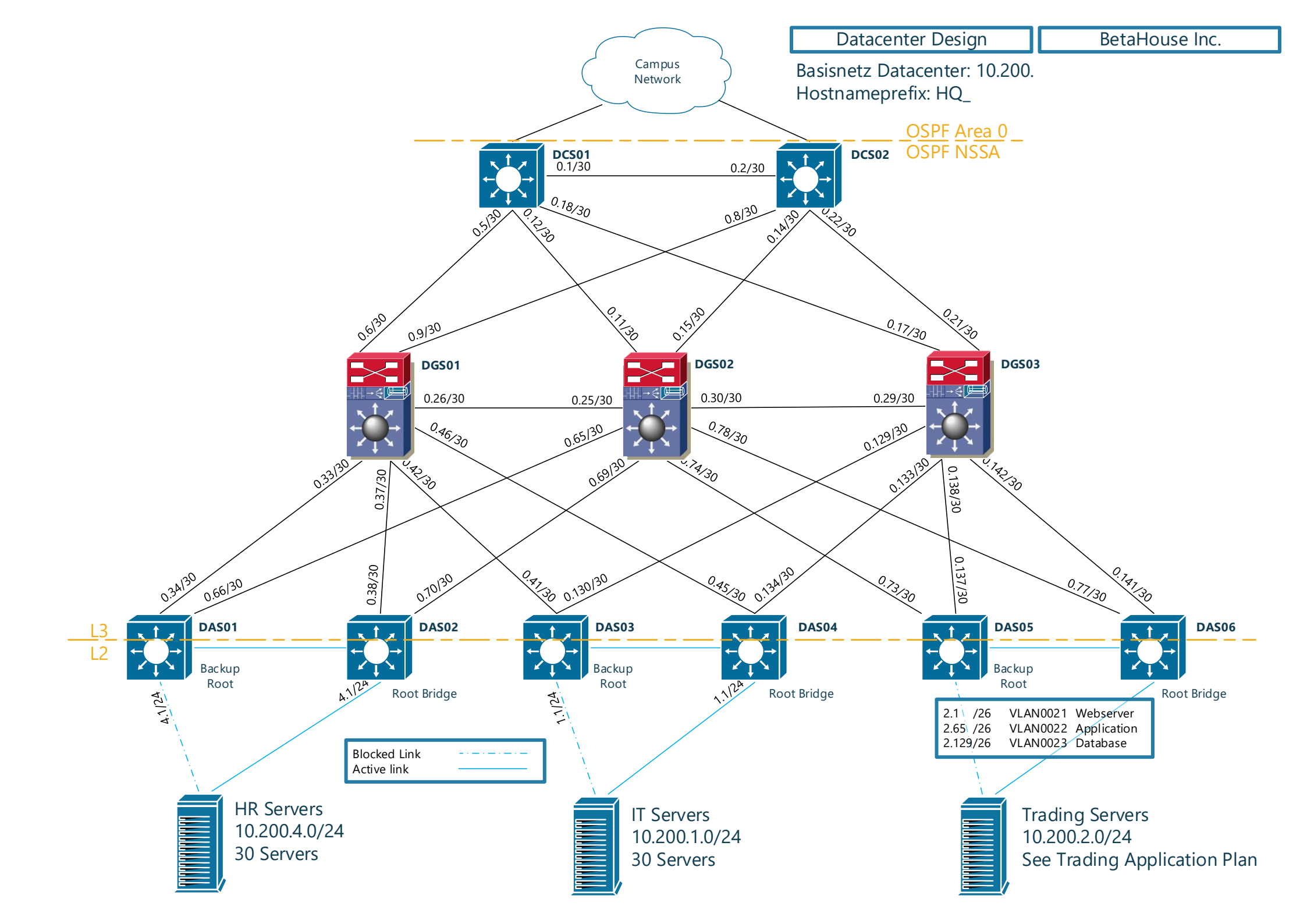
A.1. Datacenter Design

Das Schema ist im Anhang A.2 zu finden.

A.2. 3 Tier des Application Layers

Das Schema ist im Anhang A.2 zu finden.

B. Tabellenverzeichnis

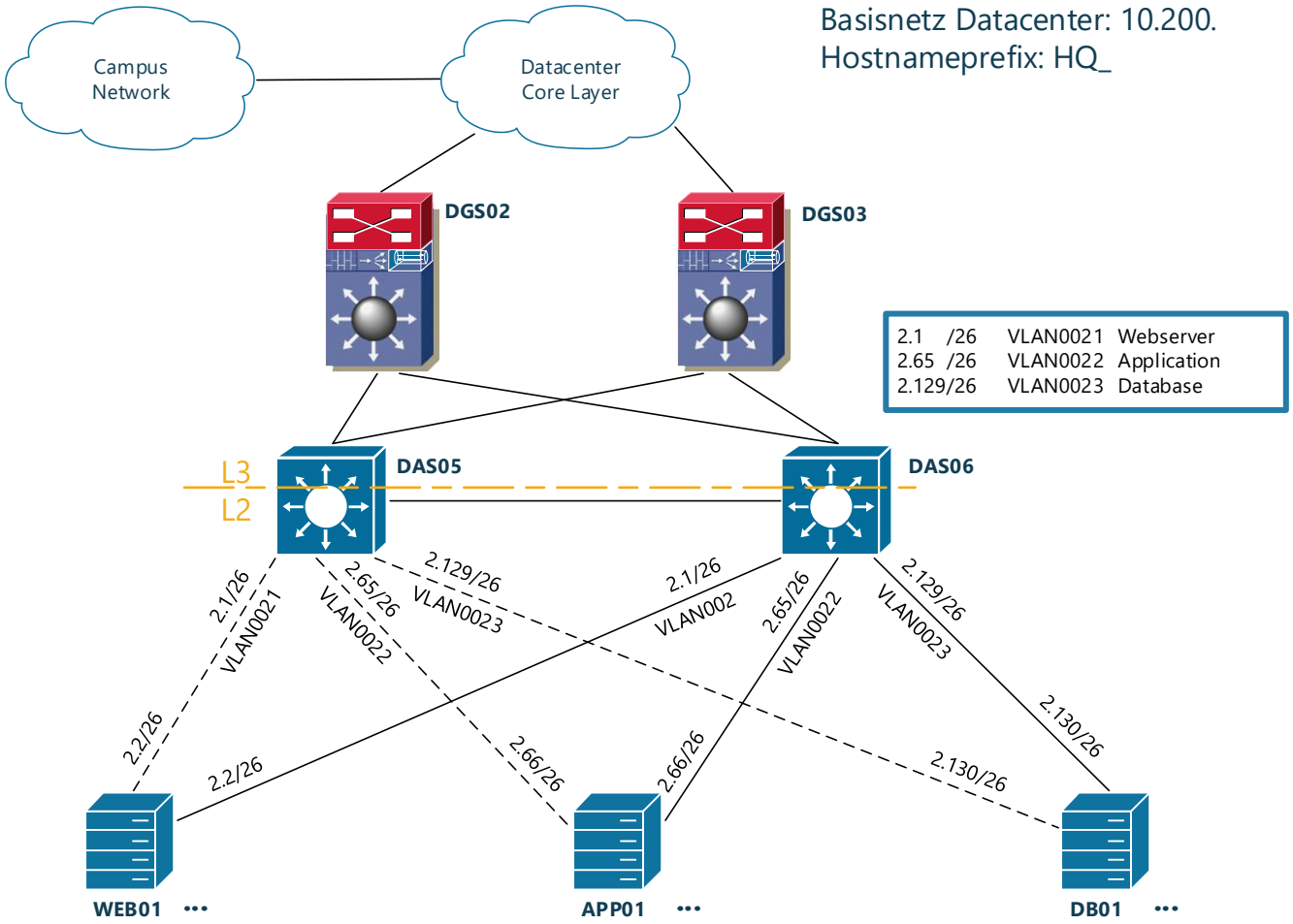

Datacenter Design
BetaHouse Inc.
Basisnetz Datacenter: 10.200.
Hostnameprefix: HQ_
Campus Network
OSPF Area 0
OSPF NSSA
DCS01
DCS02
0.1/30
0.2/30
0.18/30
0.5/30
0.12/30
0.8/30
0.14/30
0.22/30
DGS01
DGS02
DGS03
0.6/30
0.9/30
0.11/30
0.15/30
0.17/30
0.21/30
0.26/30
0.25/30
0.30/30
0.29/30
0.46/30
0.65/30
0.78/30
0.129/30
0.33/30
0.37/30
0.42/30
0.69/30
0.74/30
0.133/30
0.138/30
0.142/30
L3
L2
DAS01
DAS02
DAS03
DAS04
DAS05
DAS06
0.34/30
0.66/30
0.38/30
0.70/30
0.41/30
0.130/30
0.45/30
0.134/30
0.73/30
0.137/30
0.77/30
0.141/30
Backup Root
Root Bridge
Backup Root
Root Bridge
Backup Root
Root Bridge
4.1/24
4.1/24
1.1/24
1.1/24
2.1 /26 VLAN0021 Webserver
2.65 /26 VLAN0022 Application
2.129/26 VLAN0023 Database
Blocked Link
Active link
HR Servers
10.200.4.0/24
30 Servers
IT Servers
10.200.1.0/24
30 Servers
Trading Servers
10.200.2.0/24
See Trading Application Plan

Physische Struktur

3 Tier Application

BetaHouse Inc.

Basisnetz Datacenter: 10.200.
Hostnameprefix: HQ_



Beispiel Datenfluss