HSR Cloud Infrastructure Lab 2

Design an enterprise network based on customer specifications

Emanuel Duss, Roland Bischofberger

16. Oktober 2014

Inhaltsverzeichnis

1 Aufgabenstellung **2**
- 1.1 Ziele des Datacenters . . . 2
- 1.2 Beschreibung der gewünschten Ziel (Desired Goals) . . . 2

2 Datacenter Access Layer **3**
- 2.1 Access Layer Design für HR und IT . . . 3
- 2.2 3 Tier Modell Trading . . . 3
- 2.3 Layer 2 Topologie . . . 3
- 2.4 Topologie . . . 3
  - 2.4.1 VLAN . . . 4

3 Datacenter Aggregation Layer **5**
- 3.1 Benötigte Funktionen und Services . . . 5
- 3.2 Routing . . . 5
- 3.3 Firewall . . . 5

4 Datacenter Core Layer **6**

5 Multitenant Datacenter **7**

6 Layer 2 **7**

7 Layer 3 Topologie **7**
- 7.1 Namenskonzept und IP-Adresskonzept . . . 7
- 7.2 Routing Protokolle . . . 7

8 Report **8**
- 8.1 Erklärung . . . 8
- 8.2 Physikalische Topologie . . . 8
- 8.3 Logische Topologie . . . 8
- 8.4 Traffic Flow Beispiele . . . 8
- 8.5 Skalierbarkeit . . . 8

1 Aufgabenstellung

1.1 Ziele des Datacenters

- Voll redundant
- Hochverfügbar
- Skalierbar
- "Schnelle" Antwortzeiten

1.2 Beschreibung der gewünschten Ziel (Desired Goals)

- Im Campus LAN hat jede Abteilung ihr eigenes Subnetz/VLAN
- Alle Applikationen von BetaHouse Inc. werden im Datacenter gehostet
- Jede Abteilung hat ihre eigenen Server
  - Abteilungen dürfen die Server von anderen Abteilungen nicht erreichen
- Jede Applikation wird auf einem eigenen physischen Server betrieben (keine Virtualisierung)
- Anzahl Server (Total 90 Server)
  - HR hat 30 Server
  - IT hat 30 Server
  - Trading hat 10 Applikationen mit 3-Tier Architektur auf 30 Server
    - Kommunikation zwischen den Tiers mit TCP/IP und zwischen den Tiers je eine Firewall

2 Datacenter Access Layer

2.1 Access Layer Design für HR und IT

Das Netzwerk basiert auf Layer drei bis zum Accesslayer hinunter. Das heisst, dass der Netzwerktraffic bis zum Access Layer geroutet wird.

Die Server werden mit je zwei Gigabit Kupfer Kabel an die Access Switches angeschlossen. Auf dem Server sind beide Interfaces mit der selben IP Adresse konfiguriert. Bei einem Unterbruch eines Links erwacht die sich im Hot Standby befindliche Karte und übernimmt den defekten Link. In der Map sind die Hot Standby Links grau eingezeichnet.

Der Default Gateway der Server ist jeweils der jeweilige Access Switch. Beim Acces Switch ist das Routing so eingerichtet, dass dort über den Aggregation Switch geroutet werden muss, um in ein anderes VLAN zu kommen.

Will nun ein Server auf ein VLAN einer anderen Abteilung zugreifen, sendet dieser das IP Paket an den Default Gateway. Dieser sendet es an den Aggregation Switch weiter, bis es dort von der Firewall blockiert wird.

Die Redundanz der Access Switches wird nicht mit dem Spanning Tree Protocol umgesetzt. Spanning Tree bleibt jedoch auf den Switches aktiviert, um Loops bei falscher Verkabelung zu verhindern.

2.2 3 Tier Modell Trading

Auch dies Server des Trading sind mit je zwei Gbps Kupfer Kabeln angebunden. Auch werden hier zwei Netzwerkkarten im Active-Standby Modus eingesetzt.

Das logische Modell einer 3-Tier Applikation und ein Beispiel eines Traffic Flows ist im Anhang.

Vergleicht man das 3-Schichtenmodell der Softwarearchitektur (Verteilte Systeme) mit dem logischen Fluss der Netzwerkpaketen, stellt man ein Unterschied fest: Im 3-Schichtenmodell der Softwarearchitektur sieht es aus, als ob die Präsentationsschicht mit der Applikationsschicht und die Applikationsschicht direkt mit der Datenschicht verbunden wäre, ohne mehrmals über dieselben Netzwerkknoten zu gehen. Im logischen Modell sieht man jedoch, dass die Netzwerkpakete mehrfach bei den selben Router und Firewall vorbeikommen. Da sich die einzelnen Layers in verschiedenen VLANs und Subnetzen befinden, müssen diese geroutet werden. Wir führen das Routing im Aggregation Layer mit einem Firewall Modul durch, damit die Systeme korrekt voneinander getrennt werden können. Deshalb geht jeder Traffic vom Access Layer, welcher in ein anderes Netz muss durch die Firewall und wieder zurück auf den Access Layer. Dies kann sogar auf denselben Access Switch zurückgehen. Da es 3 Layer sind, kann eine Anfrage von einem Client bis zu sechs Routing-Aktionen auf den Access Switches führen. (vgl. Bild).

Die Clients kommunizieren nur mit den Servern in der Präsentationsschicht (Web-Tier). Zum Beispiel greift ein Client mit einem Webbrowser auf den Webserver im Web-Tier zu. Der Zugriff vom Internet auf die Web-Tiers wird über eine Firewall kontrolliert.

Die Business-Logik befindet sich im zweiten Layer (Application-Tier). Nur der Web-Tier darf auf den Application-Tier zugreifen. Dieser Zugriff wird ebenfalls durch eine Firewall geregelt.

Der Web-Tier darf nicht direkt auf den Data-Tier (Datenbanken) zugreifen. Dieser Zugriff hat nur der Application-Tier. Das wird ebenfalls durch eine Firewall geregelt.

2.3 Layer 2 Topologie

2.4 Topologie

Es wird keine spezielle Layer 2 Topologie benötigt. Für die Beschreibung, siehe "Access Layer Design für HR und IT".

2.4.1 VLAN

VLAN	Subnetz	Beschreibung
20	10.10.20.0/24	HR
30	10.10.30.0/24	IT
40	10.10.40.0/24	Trading
41	10.10.41.0/24	Trading Web
42	10.10.42.0/24	Trading Application
43	10.10.43.0/24	Trading Data

Die VLANs werden pro Abteilung in einem 10er Intervall inkrementiert. So sind die verschiedenen VLANs der einzelnen Abteilung gruppiert.

Dazu käme noch ein allgemeines VLAN für gemeinsame Services wie Mail- oder Nameserver, welche von allen Abteilungen genutzt werden. Dies wird in der Aufgabenstellung jedoch nicht thematisiert.

3 Datacenter Aggregation Layer

3.1 Benötigte Funktionen und Services

Folgende Datacenter Aggregation Layer Funktionen und Services werden benötigt, um die Businessanforderungen zu erfüllen:

3.2 Routing

Mit dem HSRP Protokoll soll sichergestellt werden, dass bei einem Ausfall eines Aggregation Switches der AG02 einspringt. Dabei wird das Multigroup HSRP von Cisco genutzt. Der Switch AG02 ist somit Standby für die HSRP Group1 mit dem Switch AG01 und zugleich auch Standby für die HSRP Group2 mit dem Switch AG03. Die Access Switches AC01-AC04 haben den DefaultGateway 10.33 konfiguriert, wobei die Access Switches AC05-AC06 den Default Gateway 10.34 definiert haben. Die Virtuelle IP für die HRSP group1 ist 10.10.10.33/26 und für die HRSP group2 10.10.10.34/26.

3.3 Firewall

Auf den Aggregation Layer Switches wird ein Firewall Modul eingesetzt. Jeder Traffic von den Core Switches zu den Access Switches und auch in der Gegenrichtung wird durch die Firewall geroutet.

Mit der Firewall wird ebenfalls verhindert, dass Geräte von verschiedenen VLANs der einzelnen Abteilungen miteinander kommunizieren. Das heisst, jeglicher Verkehr von einem VLAN in ein anderes muss die Firewall auf dem Aggregation Layer durchlaufen. Dies wird durch das Routing auf den Access und Aggregation Switches sichergestellt.

Die Firewall soll so nahe wie möglich beim Routing platziert werden. Da wir aber bereits im Access Layer routen, würde dies eine höhere Anzahl Firewalls bedeuten. Die Firewalls im Core aufzustellen ist ebenfalls eine schlechte Idee, weil dadurch der ganze Traffic hoch zum Core muss und dann wieder zurück. Die für uns optimalste Lösung ist das platzieren der Firewall im Aggreagation Layer.

Auf den Aggregation Layer Switches wird jeglicher Verkehr durch die Firewall geschläust. Bei den Access Switches ist der NextHop für den Verkehr in ein anderes VLAN oder Richtung Core immer der Aggregation Switch definiert, welcher dann den Verkehr an sein Firewallmodul weitergibt.

Alle Firewallmodule sind aktiv. Da jedoch der Switch AG02 nur als Standby eingesetzt wird, kommt die Firewall im AG02 erst zum Einsatzt, wenn dieser den Betrieb für einen ausgefallenen Switch übernimmt. Die Defaultrouten für die VLANs des Trading führen über die Firewall DC-AG03. Für die VLANs der HR und der IT führen die Defaultrouten standardmässig über den DC-AG01. Auch in der Gegenrichtung wird durch die Firewall geroutet, durch die auch der Verkehr raus geht. Somit kann verhindert werden, dass eine State-Synchronisation der Firewalls nötig wäre.

4 Datacenter Core Layer

Wir entscheiden uns für einen eigenen Core Layer im Datacenter, da dies besser skaliert als wenn die Core Switches vom Campus Netzwerk und vom Datacenter Netzwerk zusammen Full-Mesh verbunden sind. So kann der Aggregation-Layer ohne Probleme weiterwachsen. Das Troubleshooting und die Wartbarkeit wird einfacher.

Somit ist man für den Zugang ins Internet auf Core Switches des Campus angewiesen.

Die Netze der einzelnen Branches können summarisiert werden, damit hat man auf den Routern weniger Einträge in den Routing Tabellen.

5 Multitenant Datacenter

Jede Abteilung hat ihre Server in einem separaten VLAN. Da der Verkehr immer durch die Firewall auf dem Aggregation Layer geroutet wird, kann somit der Verkehr zwischen den VLANs kontrolliert werden. Mehr dazu im Abschnitt Firewall des Kapitels Aggregation Layer.

6 Layer 2

Vergleiche Abschnitt Layer 2 im Kapitel Datacenter Access Layer.

7 Layer 3 Topologie

7.1 Namenskonzept und IP-Adresskonzept

Für die Punkt-zu-Punkt Verbindungen werden die Netze 10.10.10.0/30 verwendet. Die IP Adressen können der physikalischen Topologie entnommen werden.

Auf den Access Switches muss aufgrund von HRSP ein für alle gültiger Default Gateway verfügbar sein. Deshalb wurde dort das Netz 10.10.10.32/26 gebildet. Somit haben die Aggregation Switches die virtuellen IP Adressen 10.10.10.33 und 10.10.10.34. Mehr dazu ist im Kapitel Data Center Aggregation Layer im Abschnitt Routing erklärt.

Hostname	Beschreibung
DC-CS01	Core Switch 1
DC-CS02	Core Switch 2
DC-AG01	Aggregation Switch 1
DC-AG02	Aggregation Switch 2
DC-AG03	Aggregation Switch 3
DC-AC01	Access Switch 1
DC-AC02	Access Switch 2
DC-AC03	Access Switch 3

Dabei dienen folgende Abkürzungen:

- DC als Präfix für Datacenter
- CS als Präfix für Core Switch
- AG als Präfix für Aggregation Switch
- AC als Präfix für Access Switch

7.2 Routing Protokolle

Im Datacenter wird OSPF eingesetzt. Die Datacenter Area wird als Stub Area konfiguriert, weil es nur eine Default Route aus dem Datacenter gibt.

8 Report

8.1 Erklärung

Wir haben uns für eine Architektur entschieden, die den Layer 3 bis auf die Access Switches weiterzieht. Somit kann bei einem Ausfall eines Links zwischen Aggregation und Access Layer schneller auf eine Änderung reagiert werden wie in einer Architektur mit nur noch einem Layer 2 und STP zwischen Aggregation und Acces Layer. Ausserdem wollten wir die Broadcast Domänen auf dem Access Layer so klein wie möglich halten.

Wir haben uns bewusst für drei Aggregation Switches entschieden, da somit ein höherer Durchsatz auf den zwei Aktiven gefahren werden kann und ein Ausfall eines Switches trotzdem durch den dritten sich im Standby befindlichen Switch verhindert werden kann.

Idealerweise kommt ein zweites Rechenzentrum hinzu, welches alle oder die wichtigesten Produktivsysteme redundant abbildet. Für zusätzliche Sicherheit muss Strom von zwei Anbietern bezogen werden und Notstrom z. B. mittels eines Dieselmotors verfügbar sein. Auf diese Details mussten wir jedoch bei dieser Aufgabe nicht näher eingehen.

8.2 Physikalische Topologie

Physikalische Topologie siehe Anhang.

8.3 Logische Topologie

Logische Topologie siehe Anhang.

8.4 Traffic Flow Beispiele

Ein Beispiel für Traffic Flows mit einer kurzen Beschreibung dazu ist im Anhang unter Example Traffic Flow illustriert.

8.5 Skalierbarkeit

Die Skalierbarkeit um den Faktor 10 über die nächsten 5 Jahre:

Das Netzwerk für das Datacenter wurde so designed, dass es auch in 5 Jahren bei einer Skalierung um den Faktor 10 den Anforderungen gerecht wird.

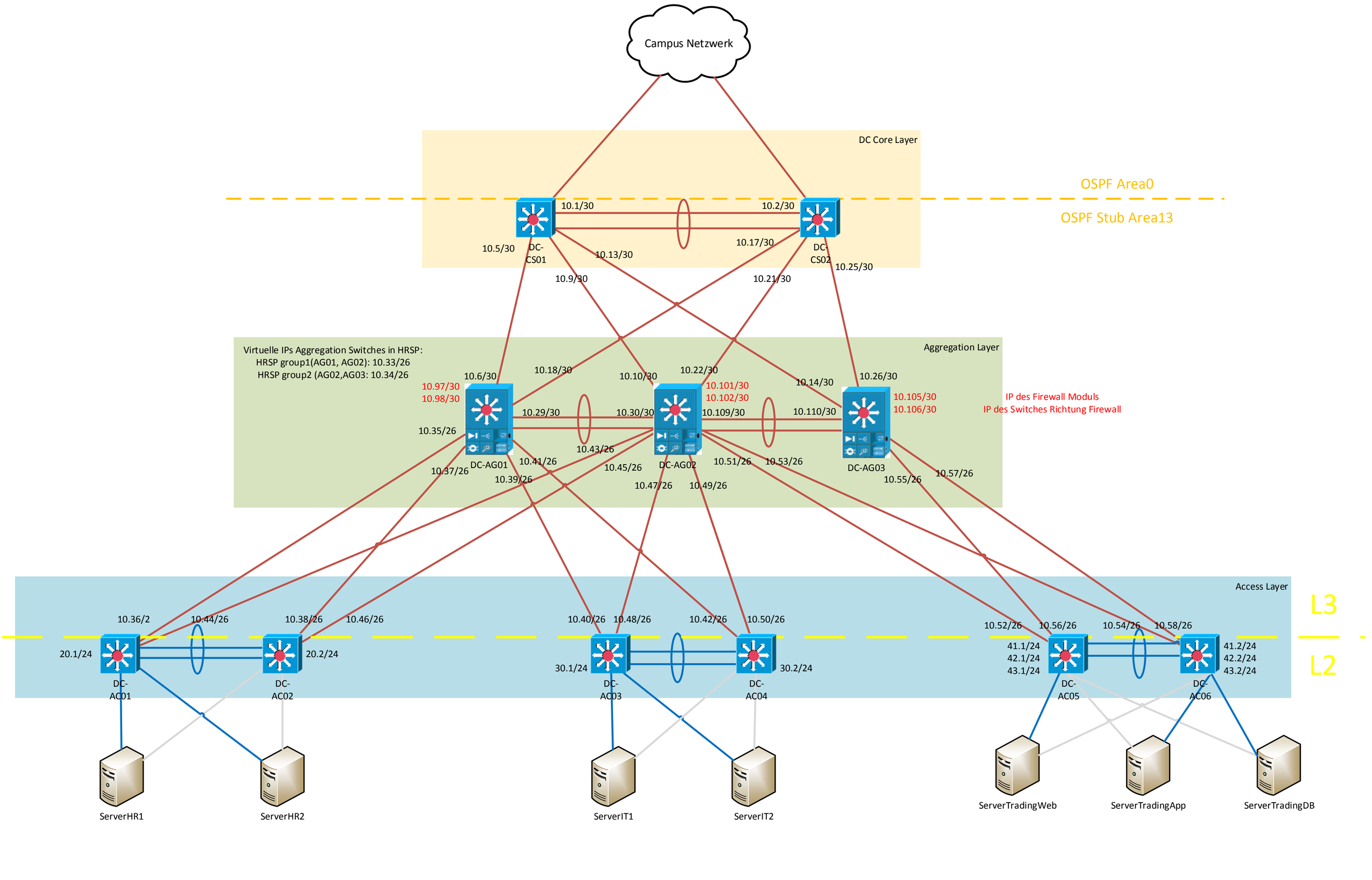
Dadurch, dass wir einen eigenen Core haben, kann dieser unabhängig vom Core des Campus LANs, der WAN Verbindungen und auch vom Internetanschluss der ISPs erweitert werden.

Falls die Switches im Aggregation Layer an ihre Grenzen bzgl. der CPU Last kommen, können diese auch erweitert werden, indem man diese mit dem Core vernetzt und untereinander wie gehabt Channel Groups erstellt.

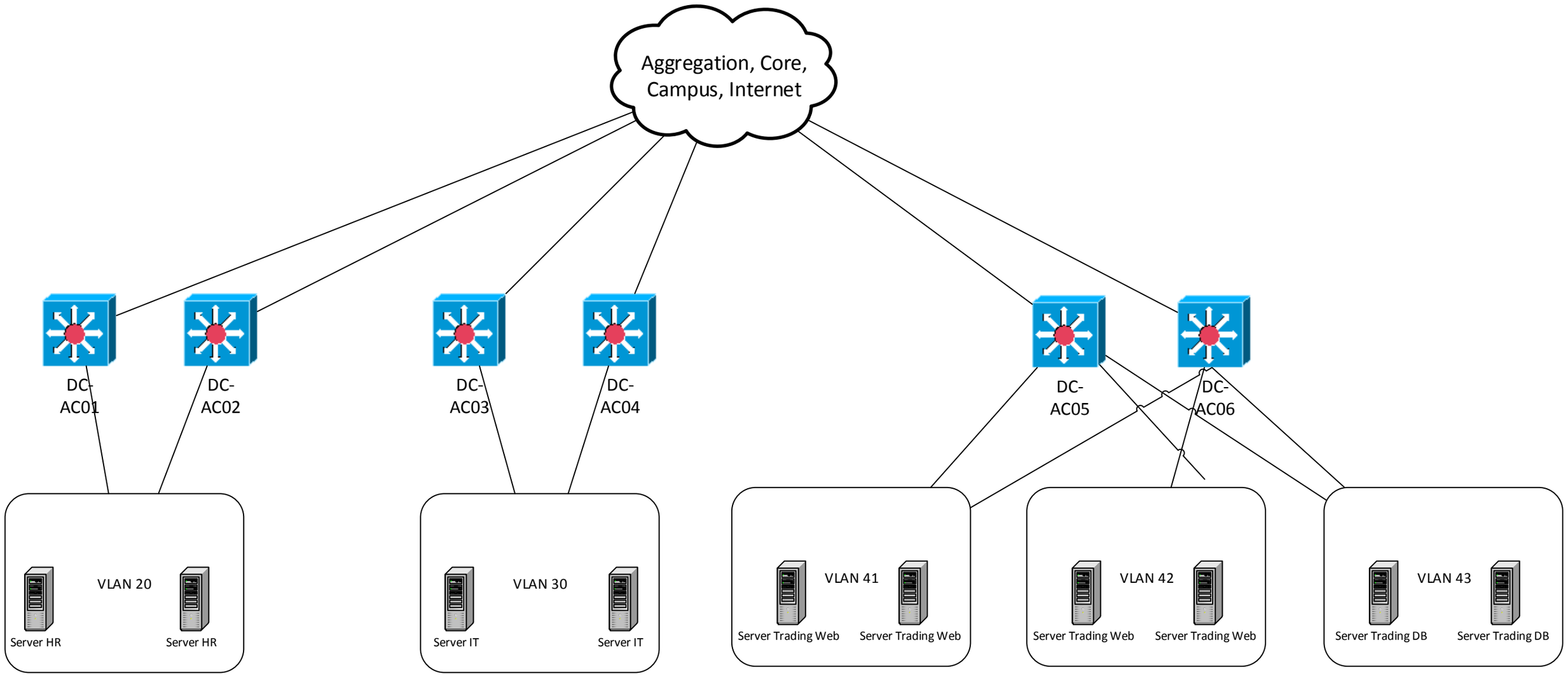
Der Access Layer kann ebenfalls durch mehr Switches aufgestockt werden.

Die VLAN Nummern und auch die Subnetze sind so gewählt, dass pro Abteilung 9 weitere VLANs bzw. Subnetze erstellt werden können. Im VLAN der IT sind zur Zeit 30 Server. Falls diese Infrastruktur weiter anwächst, wie etwa in der Abteilung Trading, können weitere VLANs mit den Nummern 31, 32, 33 erstellt werden.

Beta House Inc. 10.10.0.0/16



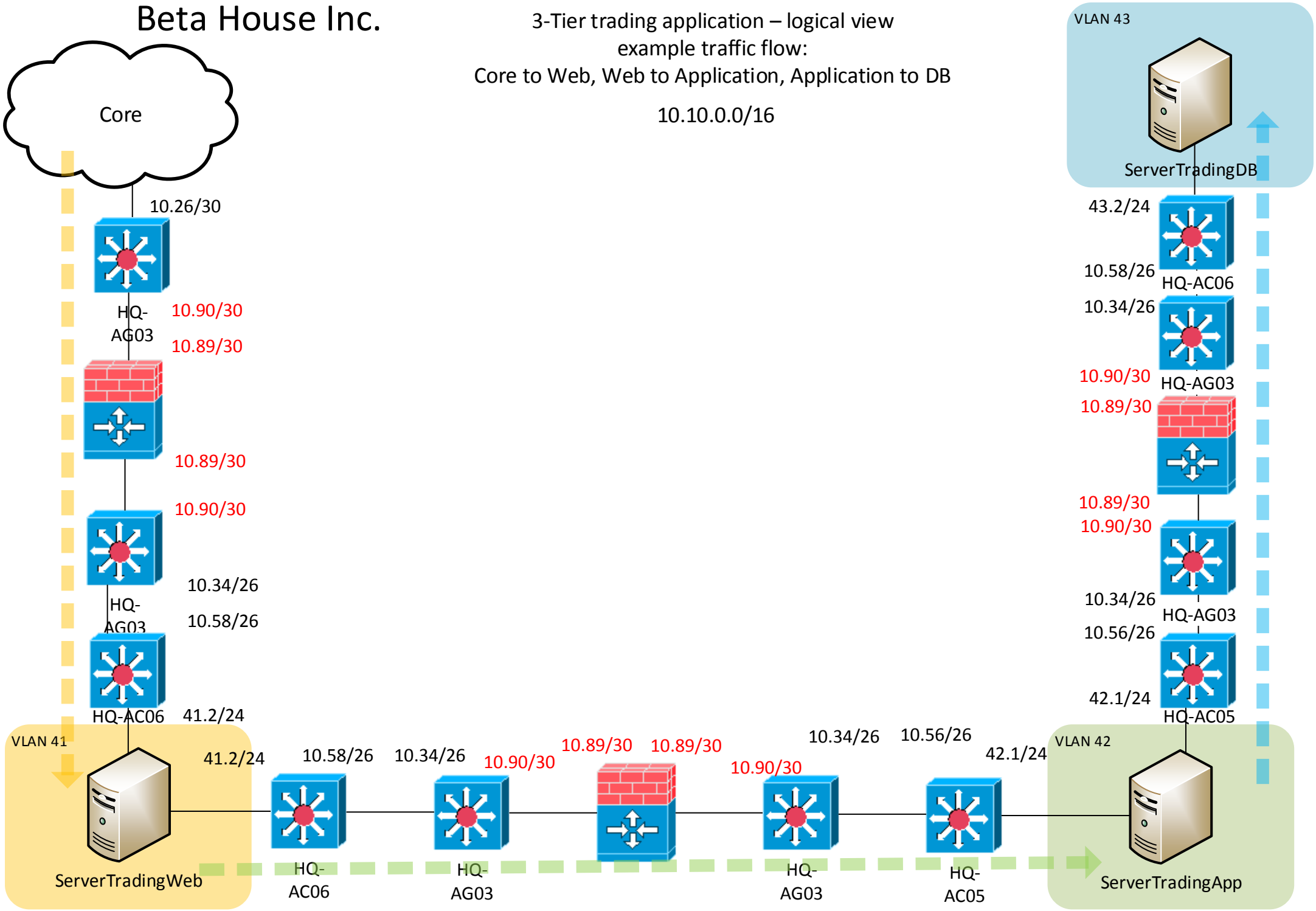
Beta House Inc.



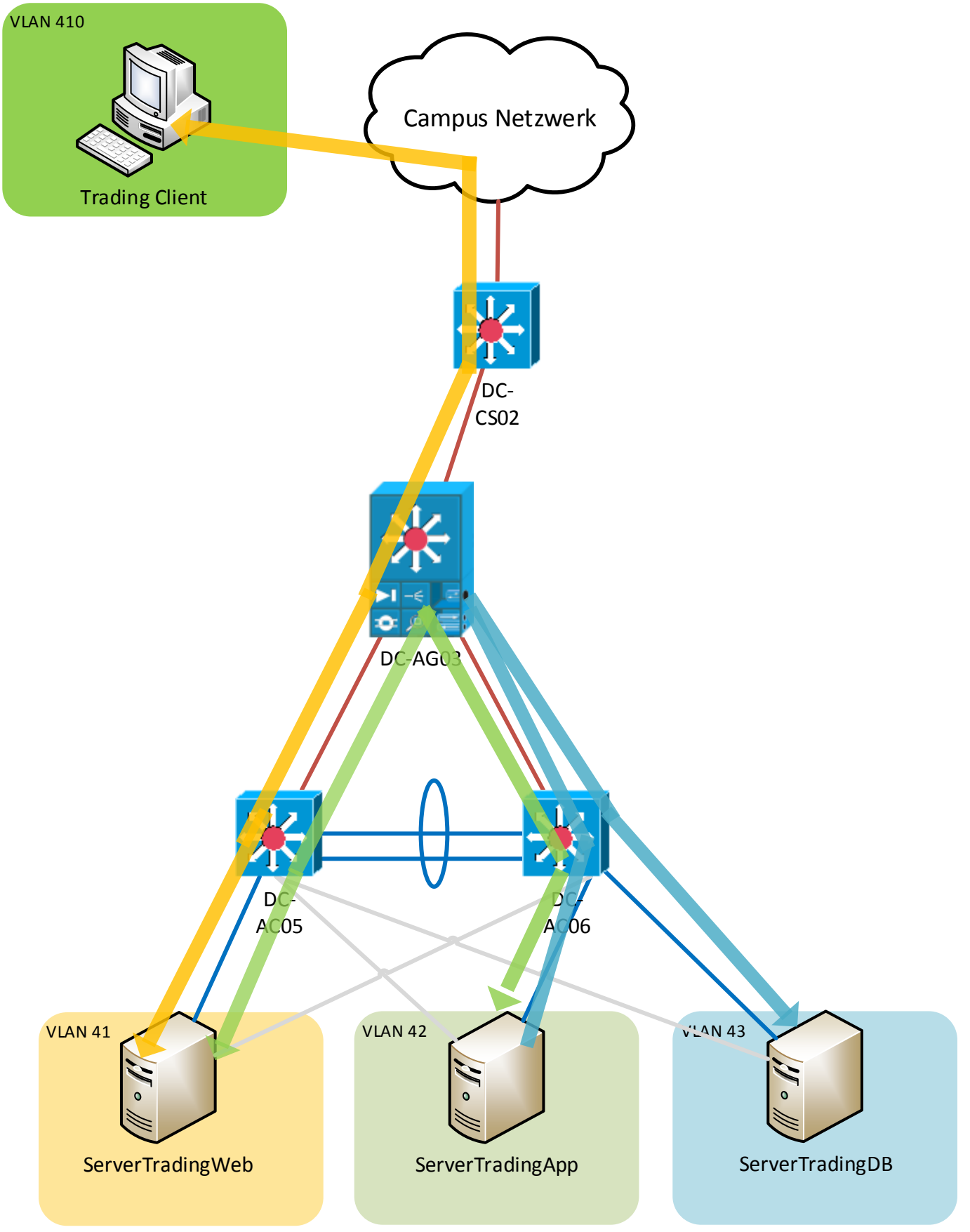
Beta House Inc.

3-Tier trading application – logical view
example traffic flow:
Core to Web, Web to Application, Application to DB

10.10.0.0/16



Physical view of example of 3-tier traffic flow:
Core to Web, Web to Application, Application to DB



Beta House Inc., Example Traffic Flow