HSR Cloud Infrastructure Lab 5

Implementing a data center with Hyper-V

Emanuel Duss, Roland Bischofberger

2014-11-04

Inhaltsverzeichnis

1 Abweichungen gegenüber der vorherigen Abgabe

In unserer vorherigen Abgabe haben wir den Layer 3 bis zum Access Switch geplant. Dies konnten wir in diesem Lab so nicht implementieren, da wir keine Layer 3 Access Switches zur Verfügung hatten. Deshalb geht der Layer 3 nun nur noch bis zum Aggregation Layer und auf den Aggegation Switches sind auch die VLANs terminiert. Auch wurde, aufgrund des vorgegebenen IP Adress Ranges, die Adressierung der Komponenten nochmals geändert. Auch konnten wir aus Zeitgründen HSRP nicht konfigurieren. Im Abschnitt HSRP unter Aggregation Switches ist dazu mehr zu lesen.

2 Dokumentation physikalischer und logischer Layer

2.1 Netzwerkübersicht

Vgl. Anhang.

2.2 Begründungen

2.2.1 OSPF

Als Routingprotokoll wählten wir OSPF, da dies Herstellerübergreifend funktioniert.

2.2.2 HSRP

HSRP sorgt für die Default Gateway Redundanz bei den Clients. Die Konfiguration von HSRP ist im Abschnitt Aggregation Switches näher beschrieben.

2.2.3 RSTP

Rapid STP ist im Aggregation wie auch Access Layer aktiviert. Wir haben RSTP aktiviert, da es einen Loop in Form einer "Acht" gibt zwischen den Aggregation und den Access Switches. Der Link zwischen dem Switch DS02-02 und dem Switch AS02-01 ist auf Seiten des Switches DS02-02 geblockt.

3 Konfiguration

3.1 Server

Folgende Server kamen in unserem Labor zum Einsatz:

Hostname	IP-Adresse	Beschreibung
srv-02-dc	10.2.110.10/24	Domain Controller
srv-02-01	10.2.110.11/24	Hyper-V Server 1
srv-02-02	10.2.110.12/24	Hyper-V Server 2
srv-02-scvmm	10.2.110.13/24	System Center Virtual Machine Manager
srv-02-v01	10.2.110.20/24	Virtueller Server 1 (GRML)

Weitere Netzwerkkonfiguration der Server:

- Nameserver: 10.2.1.10
- Windows Domain: `gr02.local`
- Username: `administrator`
- Passwort: `8640Rapperswil`

3.1.1 Namensschema Netzwerkkomponenten

- Unsere Gruppennummer 2.
- Typ der Komponenten
  - `CS` fü Core Switch
  - `DS` für Aggregation Switch
  - `AS` für Access Switches

Es wird das Schema `<Typ><Gruppennummer>-<Aufsteigende_Nummer>` angewendet:

Hostname	Beschreibung
CS02-01	Core Switch 1
CS02-02	Core Switch 2
DS02-01	Aggregation Switch 1
DS02-02	Aggregation Switch 2
AS02-01	Access Switch 1
AS02-02	Access Switch 2

3.1.2 VLANs

Folgende VLANs kommen bei uns zum Einsatz.

VLAN	Subnetz	Beschreibung
101	10.2.101.0/24	Management
110	10.2.110.0/24	Diverses

- Als Native VLAN benutzen wir `110 Diverses`.

3.2 ISP Switches

Laut der Aufgabenstellung wird jedes IP Paket mit unserer Destination Adresse `10.2.0.0/16` an unsere Core Switches weitergeleitet.

Wenn jetzt ein IP Paket in unserem Netz verschickt wird, für welches keinen eigenen Routing Eintrag existiert, wird für dieses IP Paket immer die Default Route gewählt. Angenommen wir verschicken ein IP Paket an das Netz `10.2.23.0/24`, welches bei uns nicht existiert, wird dies auch an die Default Route geschickt. Schlussendlich landet das IP Paket mit dieser Destination Adresse bei unseren Core Switches. Diese wissen mit dem Paket auch nichts anzufangen, und es wird ebenfalls an die Default Route weitergeleitet. Die Default Route auf den Core Switches zeigen zum ISP (vgl. Routingtabelle der Core Switches). Das IP Paket wird vom ISP entgegengenommen und anhand der Routingtabelle wird entschieden, wohin das IP Paket geht. Wala: `10.2.23.0/24` liegt in unserem Netz und wird deshalb wieder an uns weitergeleitet. Das Paket ist wieder bei uns. Der Core Switch denkt sich: Keine Route dazu, ich schicke es wider an den ISP... Das geht solange, bis die TTL abgelaufen.

Um diesen Issue zu beheben, wird auf dem Core Switch eine Route vom Netz `10.2.0.0/16` auf das `Loopback0` Interface erstellt. Somit wird der ganze Traffic ins leere geroutet. Da zudem per OSPF weitere Routen auf den Core Switches verfügbar sind, und jeweils der best Match zählt, werden die bestehenden Netze wie anhin geroutet.

3.3 Core Switches

3.3.1 OSPF

OSPF wird für für folgende Netze aktiviert:

Switch	Subnetz
CS02-01	10.2.0.0/30
CS02-01	10.2.0.4/30
CS02-02	10.2.0.8/30
CS02-02	10.2.0.12/30

Verwendet wird überall die OSPF Area `0`.

Die Default-Route wird mittels `default-information originate` per OSPF den anderen Routern mitgeteilt.

3.3.2 Default Route

Die Default-Route wird auf den zwei Core Switches definiert. Die Routing Tabelle auf den Core Switches sieht somit so aus (Beispiel `CS02-01`):

```
CS02-01#show ip route
[...]
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.2.0.8/30 [110/2] via 10.2.0.2, 01:06:49, FastEthernet0/2
O       10.2.0.12/30 [110/2] via 10.2.0.6, 01:06:49, FastEthernet0/3
C       10.0.0.12/30 is directly connected, FastEthernet0/1
C       10.2.0.0/30 is directly connected, FastEthernet0/2
C       10.2.0.4/30 is directly connected, FastEthernet0/3
O       10.2.110.0/24 [110/2] via 10.2.0.6, 01:06:49, FastEthernet0/3
```

```
                    [110/2] via 10.2.0.2, 01:06:49, FastEthernet0/2
O       10.2.101.0/24 [110/2] via 10.2.0.6, 01:06:50, FastEthernet0/3
                    [110/2] via 10.2.0.2, 01:06:50, FastEthernet0/2
S*   0.0.0.0/0 is directly connected, FastEthernet0/1
```

Auf dem CS02-01 sind folgende OSPF Neighbors zu sehen:

```
CS02-01#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.110.2        1   FULL/BDR        00:00:35    10.2.0.6        FastEthernet0/3
10.2.110.1        1   FULL/BDR        00:00:39    10.2.0.2        FastEthernet0/2
```

Dies sind die zwei Switches vom Aggregation Layer. Auf dem zweiten Core Switch sind dieselben Aggregation Layer Switches eingetragen.

3.3.3 Redundanz

Interessant sind vor allem folgende Zeilen in der Routing tabelle:

```
O       10.2.110.0/24 [110/2] via 10.2.0.6, 01:06:49, FastEthernet0/3
                      [110/2] via 10.2.0.2, 01:06:49, FastEthernet0/2
O       10.2.101.0/24 [110/2] via 10.2.0.6, 01:06:50, FastEthernet0/3
                      [110/2] via 10.2.0.2, 01:06:50, FastEthernet0/2
```

Dort sieht man, gut, dass die zwei Netze `10.2.110.0/24` und `10.2.101.0/24` über zwei Pfade erreichbar sind.

3.3.4 Weitere Routing Einträge

Vgl. Abschnitt über die ISP Router, welche das Problem beschreiben.

3.3.5 Interfaces von CS02-01

Interface	Portmode	IP
FastEthernet0/1	N/A	10.0.0.14/30
FastEthernet0/2	N/A	10.2.0.1/30
FastEthernet0/3	N/A	10.2.0.5/30

3.3.6 Interfaces von CS02-02

Interface	Portmode	IP
FastEthernet0/1	N/A	10.0.0.18/30
FastEthernet0/2	N/A	10.2.0.9/30
FastEthernet0/3	N/A	10.2.0.13/30

3.4 Aggregation Switches

3.4.1 Spanning Tree

Rapid STP ist im Aggregation wie auch Access Layer aktiviert. Wir haben RSTP aktiviert, da es einen Loop in Form einer "Acht" gibt zwischen den Aggregation und den Access Switches. Der Link zwischen dem Switch DS02-02 und dem Switch AS02-01 ist auf Seiten des Switches DS02-02 geblockt.

3.4.2 HSRP

Im vorhergegangenen Lab haben wir auf Stufe der Aggregation Switches geplant, HSRP einzusetzen. Da das aktuelle Lab jedoch um eine Woche gekürzt wurde, kamen wir nicht dazu, dies zu konfigurieren. Deshalb beschreiben wir hier theoretisch, wie wir es eingerichtet hätten.

DS02-01 Auf dem Interface Vlan 101 wird hsrp mit der IP 10.2.101.3 konfiguriert. Auf dem Interface Vlan 110 wird HSRP mit der IP Adresse 10.2.110.3 konfiguriert. Auf beiden Interfaces wird die Priorität auf 110 gesetzt.

DS02-02 Die Konfiguration ist identisch mit der Konfiguration für den Switch DS02-01, bis auf den Unterschied, dass die Priorität auf 100 gesetzt wird. Dies hat zur Folge, dass dieser Switch der Standby Router wird.

Für jedes VLAN das dazukommt, muss eine virtuelle IP konfiguriert werden. Es wird in jedem VLAN die ".3 Adresse" sein. Auf allen Servern wird dann die virtuelle IP Adresse des HSRP Verbundes als Default Gateway gesetzt.

3.4.3 OSPF

OSPF wird für folgende Netze aktiviert:

Switch	Subnetz
DS02-01	10.2.0.0/30
DS02-01	10.2.0.8/30
DS02-01	10.2.101.0/24
DS02-01	10.2.110.0/24
DS02-02	10.2.0.4/30
DS02-02	10.2.0.12/30
DS02-02	10.2.101.0/24
DS02-02	10.2.110.0/24

Verwendet wird überall die OSPF Area 0.

Die Default-Route bekommen die Aggregation Switches von den Core Switches via OSPF.

Die Aggregation Switches sehen je 4 Neighbors (Beispiel DS02-01). Die zwei ersten Einträge sind die Core Switches CS02-01 und CS02-02. Die zwei letzten Einträge gehören dem anderen Aggregation Switch DS02-02. Dieser ist zweimal aufgeführt, da dieser über zwei VLANs erreichbar ist.

```
DS02-01#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.0.13         1   FULL/DR         00:00:36    10.2.0.9        FastEthernet0/2
10.2.0.5          1   FULL/DR         00:00:37    10.2.0.1        FastEthernet0/1
10.2.110.2        1   FULL/DR         00:00:39    10.2.101.2      Vlan101
10.2.110.2        1   FULL/BDR        00:00:31    10.2.110.2      Vlan110
```

Die Routingtabelle sieht so aus (Beispiel DS02-01):

```
DS02-01# show ip route
[...]
Gateway of last resort is 10.2.0.9 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.2.0.8/30 is directly connected, FastEthernet0/2
O       10.2.0.12/30 [110/2] via 10.2.110.2, 01:22:14, Vlan110
                     [110/2] via 10.2.101.2, 01:22:14, Vlan101
                     [110/2] via 10.2.0.9, 01:22:14, FastEthernet0/2
C       10.2.0.0/30 is directly connected, FastEthernet0/1
O       10.2.0.4/30 [110/2] via 10.2.110.2, 01:22:14, Vlan110
                    [110/2] via 10.2.101.2, 01:22:14, Vlan101
                    [110/2] via 10.2.0.1, 01:22:14, FastEthernet0/1
C       10.2.110.0/24 is directly connected, Vlan110
C       10.2.101.0/24 is directly connected, Vlan101
O*E2 0.0.0.0/0 [110/1] via 10.2.0.9, 01:22:14, FastEthernet0/2
               [110/1] via 10.2.0.1, 01:22:14, FastEthernet0/1
```

Das Netz 10.2.0.4/30 ist dreimal erreichbar: Einmal über den Core Switch CS02-01 und zweinmal über die zwei verschiedenen VLANs via den anderen Aggregation Switch.

Der Zugang in das Internet ist über zwei Routen möglich.

3.4.4 VLANs

Auf den Aggregation Switches wurden die VLANs definiert. Die Ports Fa0/3 und Fa0/4 sind als Trunk definiert. Beispiel DS02-01:

```
DS02-01#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      110
Fa0/4       on           802.1q         trunking      110
[...]
```

Als native VLAN wurde das VLAN 110 definiert, da das Trunking im Zusammenhang mit dem virtualisierten Hyper-V Server nicht funktionierte. Somit sind befinden sich die HyperV Server im VLAN110.

3.4.5 Interfaces von DS02-01

Interface	Portmode	IP
FastEthernet0/1	N/A	10.2.0.2/30
FastEthernet0/2	N/A	10.2.0.10/30
Vlan101	N/A	10.2.101.1/24
Vlan110	N/A	10.2.110.1/24

Die VLANs werden auf den Aggregation Switches terminiert. Die Aggregation Switches dienen als Default-Gateway für dieses Netz.

3.4.6 Interfaces von DS02-02

Interface	Portmode	IP
FastEthernet0/1	N/A	10.2.0.6/30
FastEthernet0/2	N/A	10.2.0.14/30
Vlan101	N/A	10.2.101.2/24
Vlan110	N/A	10.2.110.2/24

3.5 Access Switches

Die Access Switches operieren ausschliesslich auf dem Layer 2. Layer 3 Protokolle wie OSPF werden nicht betrieben.

3.5.1 Spanning Tree

Siehe Aggregation Switches Abschnitt Spanning Tree.

3.5.2 VLANs

Auf den Access Switches werden ebenfalls all unsere VLANs definiert:

VLAN	Subnetz	Beschreibung
101	10.2.101.0/24	Management
110	10.2.110.0/24	Diverses

3.5.3 Interfaces von AS02-01

Die Interfaces Fa0/1 bis Fa0/3 sind als Trunk mit dem native VLAN 110 konfiguriert.

Interface	Portmode
FastEthernet0/1	trunk
FastEthernet0/2	trunk
FastEthernet0/3	trunk

3.5.4 Interfaces von AS02-02

Interface	Portmode
FastEthernet0/1	trunk
FastEthernet0/2	trunk
FastEthernet0/3	trunk

4 Konfiguration der Virtualisierungsumgebung

4.1 Aufgabe

Das Ziel der Aufgabe war es auf einem Hypervisor mehrere virtuelle Maschinen zu betreiben, welche sich in unterschiedlichen VLANs befinden. Der Hypervisor besitzt nur eine Netzwerkkarte, welche am Access Switch angeschlossen ist. Die Frage stellt sich, wie kommen verschiedene VLANs durch das Kabel zum Hypervisor? Um dieses Problem zu lösen, richteten wir auf dem Access Switch einen Trunk zum Server ein. Auf diesem Trunk können jetzt mehrere VLANs übertragen werden. Der Hypervisor empfängt die 802.1q getagten Frames und reicht diese an den virtuellen Switch vom Hypervisor weiter. An diesem Switch sind verschiedene virtuelle Maschinen eingerichtet, welche in unterschiedliche VLANs müssen. Die virtuelle Maschine kann einem VLAN zugeordnet werden und empfängt deshalb nur Pakete aus diesem VLAN. Der virtuelle Switch vom Hypervisor nimmt die Ethernet Frames vom Trunk entgegen und packt diese aus.

4.2 Experiment in der Laborumgebung

Durch das etwas komische Setup, welches wir in unserer Testumgebung hatten funktionierte es nicht. Der Hypervisor, in dem Fall HyperV von Microsoft, wurde nicht lokal auf dem Rechner installiert, sondern über eine virtuelle Maschine im VMWare Player gestartet. In dieser virtuellen Maschine befindet sich ein Windows Server mit der installierten HyperV Rolle. Die virtuelle Maschinen für die verschiedenen Abteilungen unserer Beispielfirma werden in dieser virtuellen Maschine erstellt. Quasi Inception.

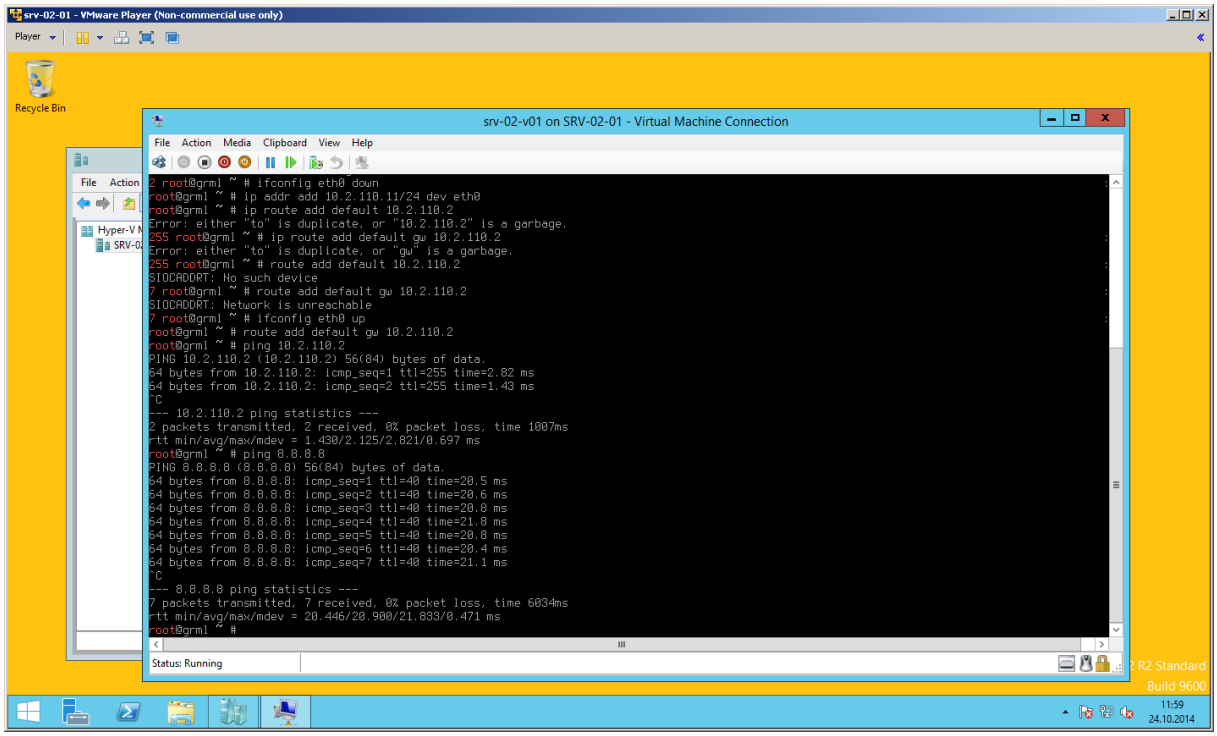
Wir erstellten eine neue Maschine und wiesen dieser ein zuvor auf dem Switch definiertes VLAN zu. Das wurde auf beiden HyperV Instanzen gemacht. Zum testen verwendeten wir GRML, was man live booten kann. Theoretisch hätten sich jetzt die zwei Maschinen über das zugewiesene VLAN anpingen können. Aber das klappte nicht. Liess man auf dem GRML `tcpdump` laufen und startete den Ping, sah man ausgehende ARP Requests, aber keine einkommenden Antworten auf diese. Das war das Problem: Die Kommunikation war nicht bidirektional. Der Verkehr konnte zwar aus der Netzwerkkarte raus, aber es kam nie etwas zurück. Startete man Wireshark auf dem Hostsystem, sah das etwas anders: Die ARP Requests kamen an und auch zurück, aber ohne 802.1q Tags. Das Betriebssystem Windows nahm einfach die 801.1q Tags vom Frame weg, ohne, dass wir das so konfigurierten. Wir haben sehr viel Zeit damit verbracht das Problem zu beheben, aber das gelang uns nicht. Die wohl beste Lösung wäre gewesen, den HyperV direkt auf einem System laufen zu lassen, wie es auch in der Praxis gemacht wird.

5 Testing

Wir haben die Umgebung vorallem mit Pings getestet. Wir haben auf jedem Switch im Core und Aggregation Layer überprüft, ob der Ping zu der Gegenseite funktioniert. Auch haben wir in der Virtuellen Maschine auf dem HyperV Server getestet, ob dieser in das Internet pingen kann. Zusätzlich dazu, haben wir alle Virtuellen Server der Domäne auf srv-02-dc hinzugefügt und haben getestet ob diese sich gegenseitig erreichen können. Alle diese Tests waren erfolgreich.

5.1 Ping grml → Internet

Hier sieht man einen Ping, welcher vom GRML System ins Internet durchgeführt wurde:



5.2 Routing

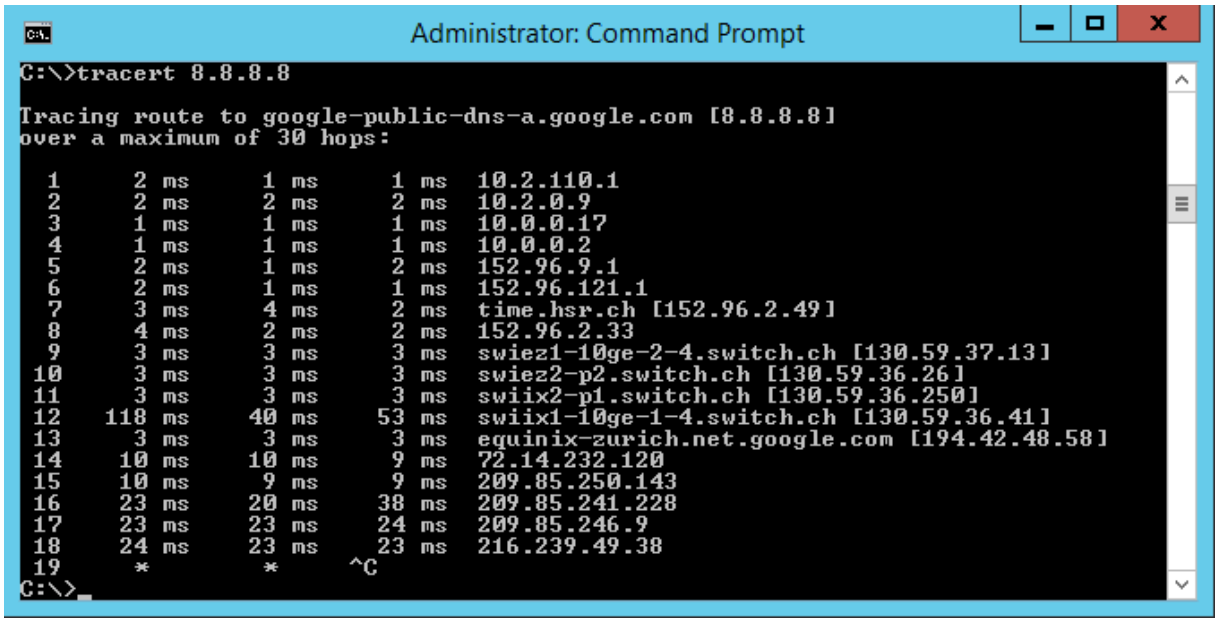
Die Routingtabellen wurden jeweils im Abschnitt über die Netzewrkkonfiguration beschrieben.

5.3 OSPF

Die OSPF Neighbor Tabellen können im Abschnitt über die Netzwerkkonfiguration entnommen werden.

5.4 Traceroute

Durch folgenden Traceroute kann man gut den Weg durch das Datacenter Netzwerk sehen:



Der Weg des IP Pakets durch das Datacenter Netzwerk ist im Anhang zu sehen.

5.5 Failover Testing

Das Szenario "Ausstecken von einem Access Switch" konnten wir nicht testen, da unser Labor PC nur ein Interface besitzt und somit nicht an zwei Access Switches angeschlossen war.

Das Szenario "Ausstecken von einem Aggregation Switch" konnten wir nicht testen, da wir das HSRP Protokoll nicht implementiert haben (eine theoretische Beschreibung) der Konfiguration liegt oben vor). Unsere Labor PCs haben den Aggregation Switch direkt als Default Gateway eingetragen und somit sind diese nicht für einen Ausfall ausgelegt.

Das Szenario "Ausstecken von einem Core Switch" konnten wir aber erfogreich testen, da die Route zu den Core Switches auf dem Aggregation doppelt eingetragen ist (vgl. dazu die Routing Tabellen der Aggregation Switches im Teil der Konfiguration). Der Core Layer ist deshalb auf zwei Wege erreichbar. Während dem Pingen ins Internet wurde die Route sekundenschnell angepasst.

6 Überlegungen zu den "Post-Studies"

6.1 Multitenancy

Unter Multitenancy versteht man die Abtrennung von mehreren Abteilungen in einer Firma. Die Abteilung Verkauf darf beispielsweise nicht auf die Server der Abteilung HR zugreifen.

Hierfür könnte man die Technik der VLANs nutzen, welche eine Abgrenzung auf Layer 2 vornimmt. Von einem VLAN in ein anderes kann ohne Routing nicht zugegriffen werden.

Mit ACLs könnte man die Zugriffe noch weiter einschränken. Will man noch detailliertere Einstellungen vornehmen, greift man zu einer Firewall.

6.2 VM Mobility

Unter VM Mobility versteht man, dass virtuelle Maschinen zur Laufzeit von einem Hostsystem auf ein anderes Hostsystem gezügelt werden kann, ohne dass es zu einem Unterbruch kommt.

Mittels VXLAN (Virtual Extensible LAN) kann dies umgesetzt werden: Dabei wird über das bestehende Layer 3 Netz ein Layer 2 Netz gelegt. Der Traffic fliesst weiterhin an den alten Standort, wird dort jedoch in ein UDP Tunnel gepackt und an den neuen Standort weitergeleitet. Der Vorteil daran liegt, dass man das auf das bestehende Netzwerk aufsetzen kann. Der Nachteil ist, dass zusätzlicher Verkehr vom ersten Standort zum zweiten Standort fliesst.

6.3 First Hop Redundancy Empfehlung

HSRP stellt eine virtuelle IP und MAC-Adresse zur Verfügung, welche von mehreren Geräten geteilt wird. Somit kann beim Ausfall eines Aggregation Switches der andere sich im Standby befindliche Switch einspringen. Der Vorteil von HSRP ist die schnelle Konvergenz bei einem Ausfall eines Routers und die First Hop Redundancy ist gewährleistet. Ein Nachteil ist, dass HSRP nur von Cisco unterstützt wird. Als offener Standard käme Virtual Router Redundancy Protocol in Frage. Wir würden HSRP empfehlen, da nur Cisco Geräte eingesetzt werden.

6.4 Full Automatic Cloud

Um eine automatische Skalierung zu erlauben, müsste ein Monitoring System eingesetzt werden, welches die aktuelle Auslastung auswerten kann. Mit einem Loadbalancing ist es dann möglich die Last der vielen Anfragen auf verschiedene virtuelle Hosts zu verteilen. Sollte nun ein gewisser Schwellwert überschritten werden, kann ein zusätzlicher virtueller Server in den Loadbalancingverbund aufgenommen werden.

6.5 Inter Datacenter Connection

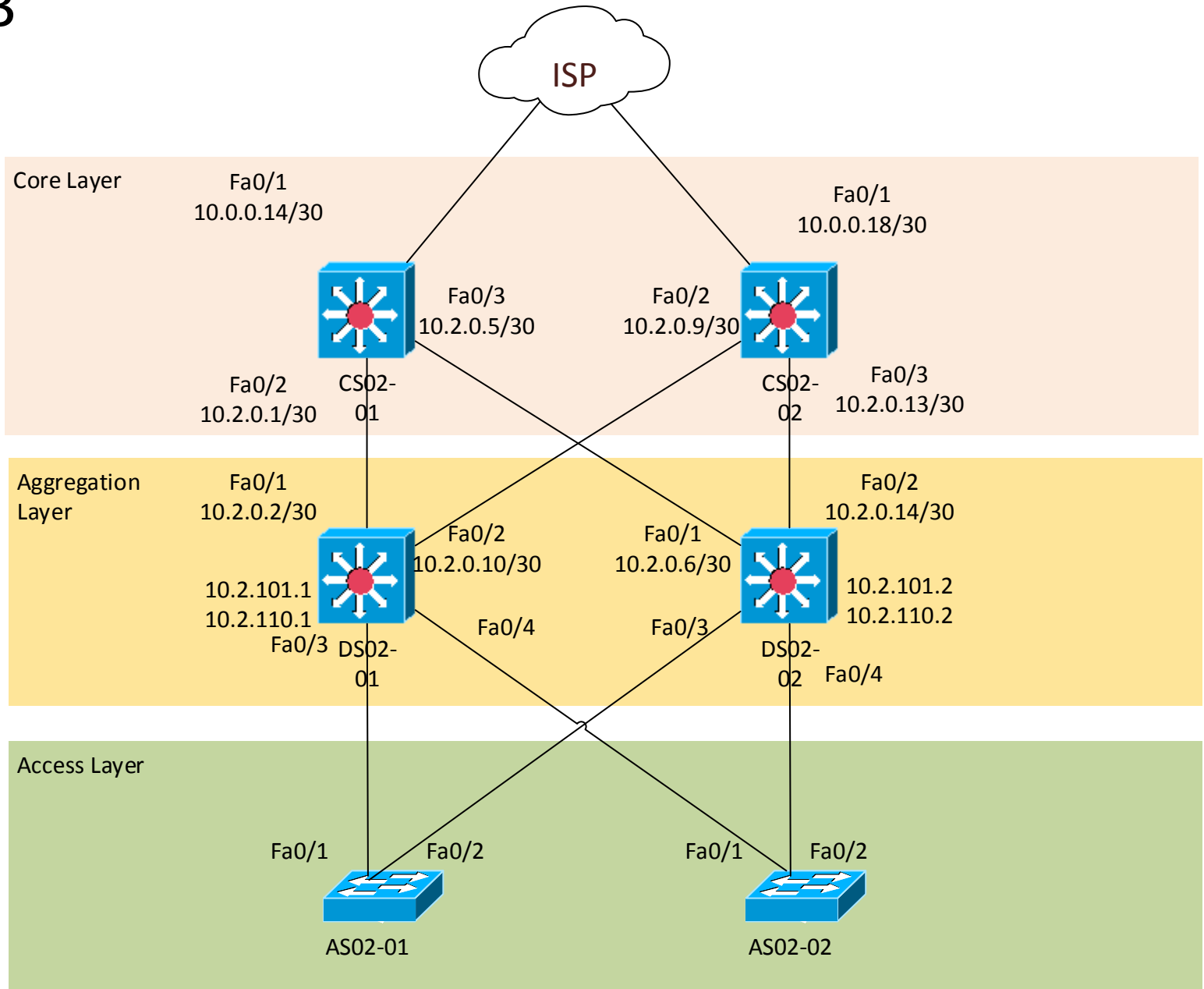
Cisco schlägt drei Varianten für eine Inter Datacenter Connection vor [1]:

- Dark Fiber: Eigene Kabel zwischen den Rechenzentren; Erlaubt auch SAN Traffic. Sehr teuer.
- Layer 2 Services: Ethernet Frames werden direkt an den ISP gesendet, welche an die remote Seite ausgeliefert werden. Es kann auch ein Layer 2 VPN eingesetzt werden.
- Layer 3 Services: ISP stellen IP oder MPLS Netz zur Verfügung.

[1] http://www.cisco.com/c/en/us/products/collateral/data-center-virtualization/data-center-interconnect/white_paper_c11_493718.html

Layer 1 / 3

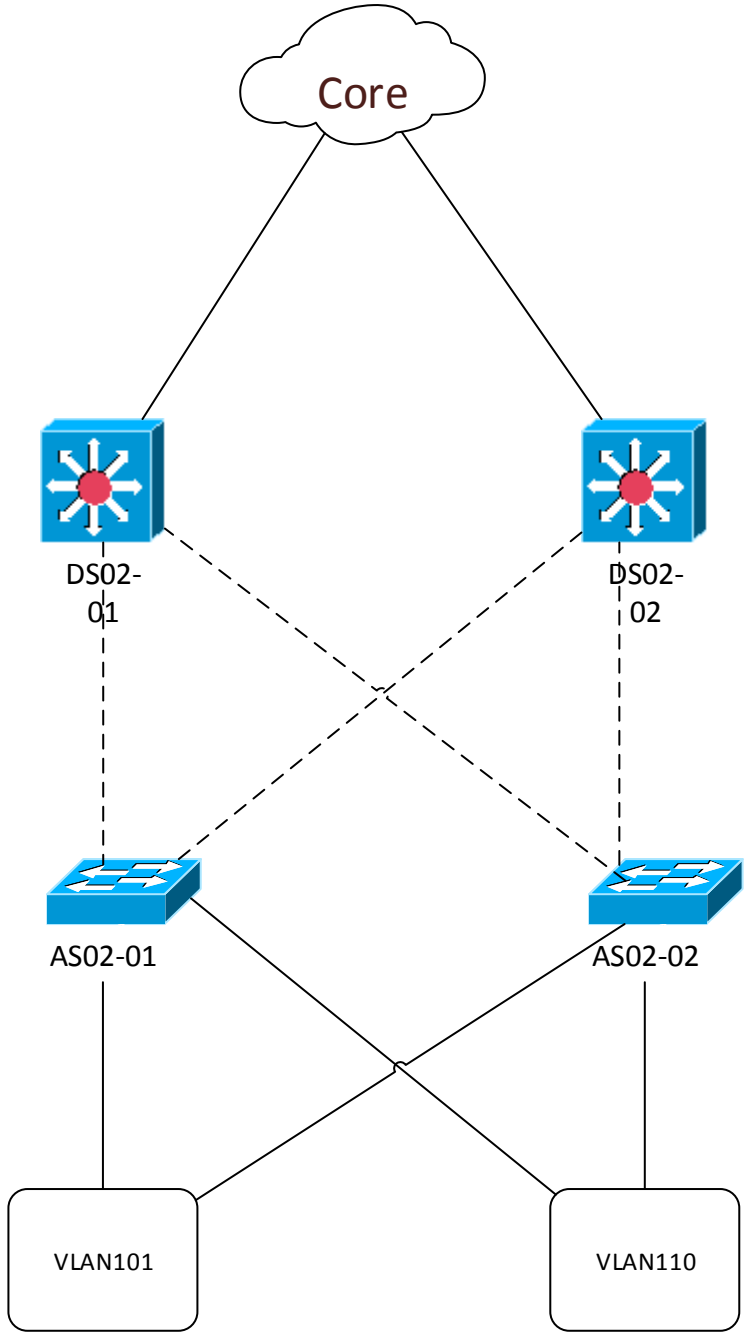
10.2.0.0/16



Layer 2 Map

Trunk, alle VLAN erlaubt

Access für VLAN



Traffic Flow
Traceroute