NTB
Interstaatliche Hochschule
für Technik Buchs

HTW Chur
Hochschule für Technik und Wirtschaft
University of Applied Sciences

NTB - Interstaatliche Hochschule für Technik Buchs

IuK_III_U-Konzeption und Aufbau eines Unternehmensnetzwerkes

Studierende: Benjamin Mosberger, Tobias Schoch

Dozent: Beat Bigger

Datum: Herbstsemester 2015

Zusammenfassung

Die Aufgabe dieser Projektarbeit ist ein Unternehmensnetzwerk im Labor der HTW Chur zu planen, aufzubauen und zu Dokumentieren. Das ganze Netzwerk soll redundant aufgebaut werden, um ausfallsicher zu sein, und ausserdem wird IPv4 und IPv6 verwendet.

Abstract

The goal of this project is to achieve a working corporate network. Beside redundancy, the clients should be able to use IPv4 and Ipv6. Clients from a department should only be able to communicate with users from the same department, even in other sites.

Inhaltsverzeichnis

1 Abkürzungen **5**

2 Ausgangslage **6**
2.1 Fallbeispiel 6
2.2 Praktikumsausrüstung 7

3 Konzept **8**
3.1 Ipv4 Adresskonzept 8
3.2 Ipv6 Adresskonzept 9
3.3 Routingkonzept 10
3.4 NAT Konzept 10
3.4.1 IPv4 10
3.4.2 IPv6 10
3.5 Securitykonzept 11
3.5.1 ACL 11
3.5.2 Layer 2 Security 11
3.6 Serverservices 12
3.6.1 DHCP 12
3.6.2 DNS 12
3.7 Netzwerkplan 12
3.8 weitere Überlegungen 13
3.9 Stack 13

4 Planung **14**

5 Umsetzung **14**
5.1 Grundlegende Konfiguration Router 15
5.2 Grundlegende Konfiguration access Switches 15
5.3 IP-Konfiguration 16
5.3.1 Router 16
5.3.2 Distribution 16
5.3.3 Access-Switches 16
5.4 Link-Aggregation 17
5.5 OSPF 17
5.5.1 IPv4 17
5.5.2 IPv6 18
5.6 NAT 18
5.7 ACL 19

5.8 DHCP 20
5.8.1 IPv4 20
5.8.2 IPv6 20
5.9 DNS 20

6 Fazit **21**

Abbildungsverzeichnis

2.1 Netzwerkstruktur 7

3.1 Netzwerkplan 12

4.1 Zeitplan 14

Tabellenverzeichnis

Listings

5.1 Router Grund Konfig 15
5.2 Switch Template Wechsel 15
5.3 Switch Grund Konfiguration 15
5.4 Router IP-Konfiguration 16
5.5 Distribution IP-Konfiguration 16
5.6 Access-Switch IP-Konfiguration 16
5.7 Switch Grund Konfiguration 17
5.8 OSPF IPv4 17
5.9 OSPF IPv6 18
5.10 NAT 18
5.11 ACL 19

1 Abkürzungen

ACL Access Control List

LACP Link Aggreagtion Protocol

PagP Port Aggregation Protocol

2 Ausgangslage

2.1 Fallbeispiel

Es soll ein neues Netzwerk für die Mittelgrosse Firma HAC Home Audio Center AG aufgebaut werden, welche 80 Mitarbeiter an den 3 Standorten Chur, Buchs, St. Gallen beschäftigt. Die Firma hat ihren Hauptsitz mit 70 Mitarbeitern in Chur und Niederlassungen mit je 5 Mitarbeitern in Buchs und St. Gallen. Die Standorte sind durch ein Layer-3 MPLS VPN miteinander verbunden (was durch einen einfachen Switch simuliert wird).

2.2 Praktikumsausrüstung

Die Netzwerkkomponenten sind bereits vorhanden, die physische Netzstruktur aufgrund der Gebäudetopographie und der Skalierbarkeit zu einem grossen Teil vorgegeben.

Die verfügbaren Komponenten sind:

-Standort Chur:
- 1x Router (Cisco 1941) mit 2x FastEthernet und 2x GigabitEthernet Anschlüssen
- 2x Layer-3 Switch (Cisco 3750E)
- 2x Layer-3 Switch (Cisco 3560G)
- 2x Layer-2 Switch (Cisco 2960)

-Standort Buchs:
- 1x Router (Cisco 1921)
- 1x Layer-2 Switch (Cisco 2960)

-Standort St.Gallen:
- 1x Router (Cisco 2901)
- 1x Layer-2 Switch (Cisco 2960)

Die vorgegebene Netzwerkstruktur ist in Abbildung 2.1 zu sehen:

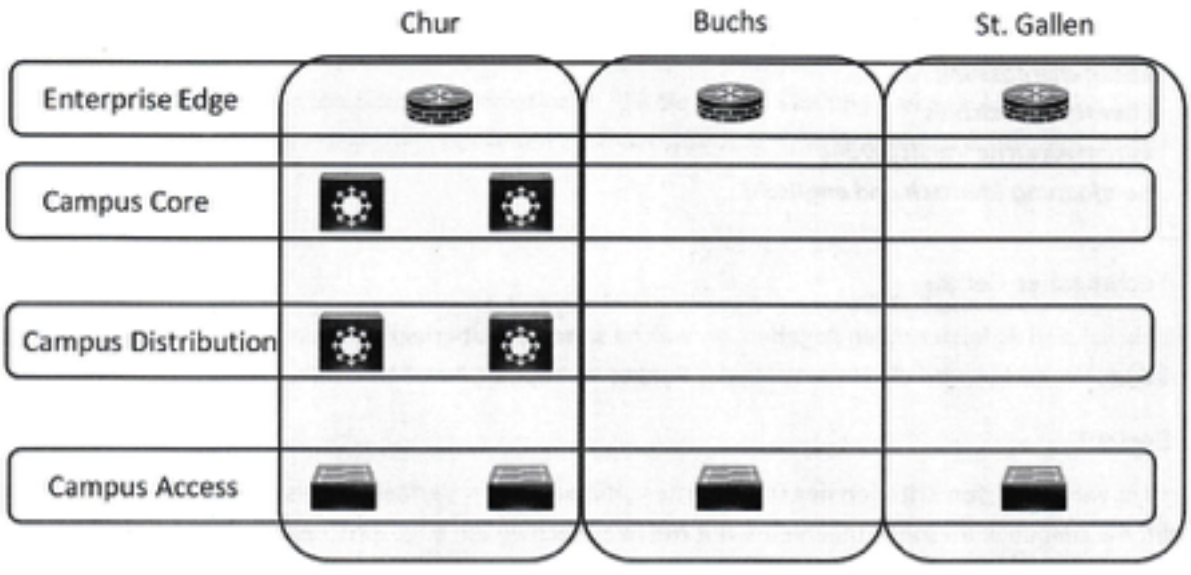

Abbildung 2.1: Netzwerkstruktur

3 Konzept

3.1 Ipv4 Adresskonzept

Das folgende Konzept gilt nur für IPv4, immer wenn von Adressen die Rede ist, sind nur IPv4 Adressen gemeint. Für das private Netz werde Adressen aus dem 10.0.0.0/8 Netz ausgewählt. Für jeden Standort und für die Netze welche nicht einem Standort zugeordnet werden können wird ein /16 Netz ausgewählt, so hat jeder Standort 65534 Ip-Adressen. Dies sollte für die nahe Zukunft genügen.

Die Aufteilung sieht folgendermassen aus:

Chur	10.1.0.0/16
St. Gallen	10.2.0.0/16
Buchs	10.3.0.0/16
Transfer	10.4.0.0/16

Für die Vlans werden die Netze der Standorte nochmals unterteilt, die gelben Sterne im Vlan-Plan stehen für die Standorte. Mit /24 Netzen stehen jeder Abteilund pro Standort 256 Adressen zur Verfügung.

Vlan 10	Geschäftsleitung	10.*.10.0/24
Vlan 20	Buchhaltung	10.*.20.0/24
Vlan 30	Entwicklung	10.*.30.0/24
	Transfer	10.*.40.0/24
Vlan 99	Management	10.*.99.0/24

3.2 Ipv6 Adresskonzept

Das folgende Konzept gilt nur für IPv6, immer wenn von Adressen die Rede ist, sind nur IPv6 Adressen gemeint. Die Aufgabenstellung besagt, dass ein /48 Netz zur Verfügung steht, das Ziel ist nun dies in einer ähnlichen Art wie bei IPv4 zu gestalten.

Standortabhängigkeiten:

Chur	2001:620:3101:1::/64
St. Gallen	2001:620:3101:2::/64
Buchs	2001:620:3101:3::/64

Da es bei IPv6 keine Vlans gibt, sondern alles über Layer-3, sprich IP, geschieht. Muss auch ein "Vlan-Konzept" für IPv6 erstellt werden. Dies wird analog zu IPv4 gemacht. Die gelben Sterne stehen für die Standortadresse.

Netze der Abteilungen:

Vlan 10	Geschäftsleitung	2001:620:3101:*010::/64
Vlan 20	Buchhaltung	2001:620:3101:*020::/64
Vlan 30	Entwicklung	2001:620:3101:*030::/64
	Transfer	2001:620:3101:*040::/64
Vlan 99	Management	2001:620:3101:*099::/64

3.3 Routingkonzept

Innerhalb unseres Unternehmens werden die verschiedenen Standorte miteinander über OSPF geroutet. Am Hauptstandort in Chur wird ab dem Distributions-Switch (D) ebenfalls mit OSPF geroutet. Beim Interface mit dem Internetanschluss wird eine default-Route gesetzt, da diese immer die Gleiche ist. Damit die Clients immer den gleichen default-Gateway haben, ist auf R1 noch ein Loopback-Interface erstellt worden, dieses darf nicht vergessen werden bei der Konfiguration von OSPF.

3.4 NAT Konzept

Meistens ist es für ein Unternehmen nicht rentabel sich die gesamte Anzahl benötigter IP-Adressen zu kaufen. Deshalb werden private IP-Adressen verwendet und danach können mit einem NAT ganze Subnetze zu einer öffentlichen Adresse zugeordnet werden. Dies ist eine komfortable Lösung, ausserdem können dann die privaten Adressen so gestaltet werden, dass man nur schon beim anschauen weiss an welchem Standort und zu welchem Vlan die Adresse gehört.

3.4.1 IPv4

Für die öffentlichen Adressen steht ein /28 Netz zur Verfügung. Für die Verwendung von NAT können alle Adressen des Netzes benutzt werden, die Netz- und Broadcast-Adresse werden nicht benötigt. Somit stehen 16 öffentliche Adressen zur Benutzung, hier wurde für jeden Vlan an jedem Standort eine eigene Adresse verteilt. Dies ergibt 12 Adressen, die restlichen 4 Adressen sind für Reserven eingeplant.

3.4.2 IPv6

Bei IPv6 ist kein NAT notwendig, da ein öffentliches /48 Netz gebraucht wird. Es sind also mehr Adressen vorhanden als je in diesem Kleinunternehmen gebraucht werden.

3.5 Securitykonzept

3.5.1 ACL

Mit ACL's wird der Zugriff der Abteilungen untereinander verhindert, lediglich das Management-Vlan hat auf alles Zugriff, da dies für die reibungslose Verwaltung des Netzes erforderlich ist. Die ACL's werden auf den Routern R2, R3 und auf dem Switch D konfiguriert, für die 3 Vlans der Abteilungen wird je der Zugriff der anderen Vlans verboten, danach werden alle anderen IP und TCP Pakete erlaubt. Dies wird für IPv4 und IPv6 gleich gemacht, als erstes wird eine ACL pro Vlan erstellt, danach wird diese ACL dem Vlan-Interface zugewiesen.

3.5.2 Layer 2 Security

Port Security
Ports abschalten
switchport trunk allowed vlan 10,20,30,99

3.6 Serverservices

3.6.1 DHCP

3.6.2 DNS

3.7 Netzwerkplan

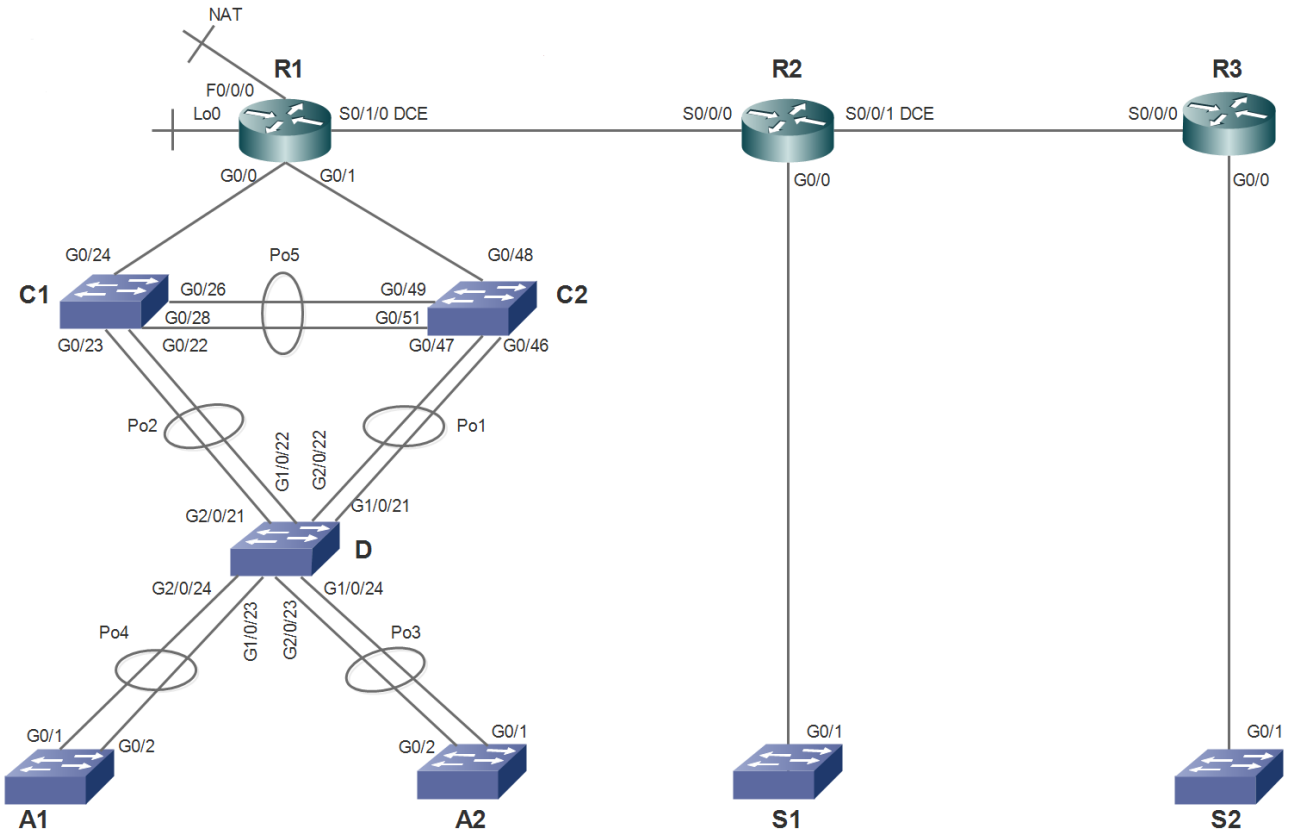

Abbildung 3.1: Netzwerkplan

3.8 weitere Überlegungen

Bei genügender Zeit hätte man noch einiges erreichen können. Einige Punkte welche wichtig sind werden nun erläutert:

- Passwort setzen: Im Moment ist auf keinem Gerät ein Passwort gesetzt, da es während der Konfiguration mühsam ist immer wieder das Passwort einzugeben, deshalb sollte dies ganz am Schluss geschehen.
- Fernwartung: Auf allen Geräten ist eine Management Adresse konfiguriert. Wenn jetzt der Fernzugriff aktiviert würde, müssten die Anzahl Zugriffe aus dem Internet begrenzt werden, damit nicht mit Bruteforce das Passwort geknackt werden kann.
- OSPF Areas: Die einzelnen Standorte hätten noch mit einem eigenen OSPF Area konfiguriert werden können, dies hätte den Vorteil dass nicht alle über OSPF Teilnehmer über das ganze Netz bescheid wissen müssen und so bedeutend weniger Traffic auf den Leitungen ist.
- Vlan: Es hätte noch ein GästeVlan eingerichtet werden können, welches nur zum Internet zugriff hat, dies ist jedoch nicht Teil der Aufgabenstellung und könne im Bedarfsfall schnell nachgerüstet werden.
- Device Backups: Wenn im Moment Device Backups gemacht werden müssen, muss jeder einzelne Router und Switch mittels kopieren der running-config gebackupt werden. Dabei könnte man mit einem Kron-Script die Backups zeitgesteuert auf einen TFTP Server speichern. So spart man sich wöchentliche Arbeit und man vergisst es auch sicher nicht.

3.9 Stack

Stacken ist das Zusammenschliessen zweier physischen Switches zu einem logischen. Dies ist nicht mit allen Switches möglich, doch in diesem Fall ist es bei den Beiden Distribution-Switches möglich, da diese ein Stack-Interface auf der Rückseite haben. Dies erspart eine Menge an Arbeit, wenn man weiss wie dies funktioniert. In diesem Fall war dies leider nicht der Fall, da noch nie mit gestackten Switches gearbeitet wurde, die Anweisungen zur Konfiguration des Stackes bezieht sich hier nur auf die Cisco Catalyst 3750 Switches, da nicht bekannt ist ob es noch Besonderheiten bei der Konfiguration anderer Switches gibt. Als erstes musste festgestellt werden, dass der 3750er nur LACP und kein PagP unterstützt.

4 Planung

In Abbildung 4.1 ist der geplante und der tatsächliche Ablauf des Projektes zu sehen.

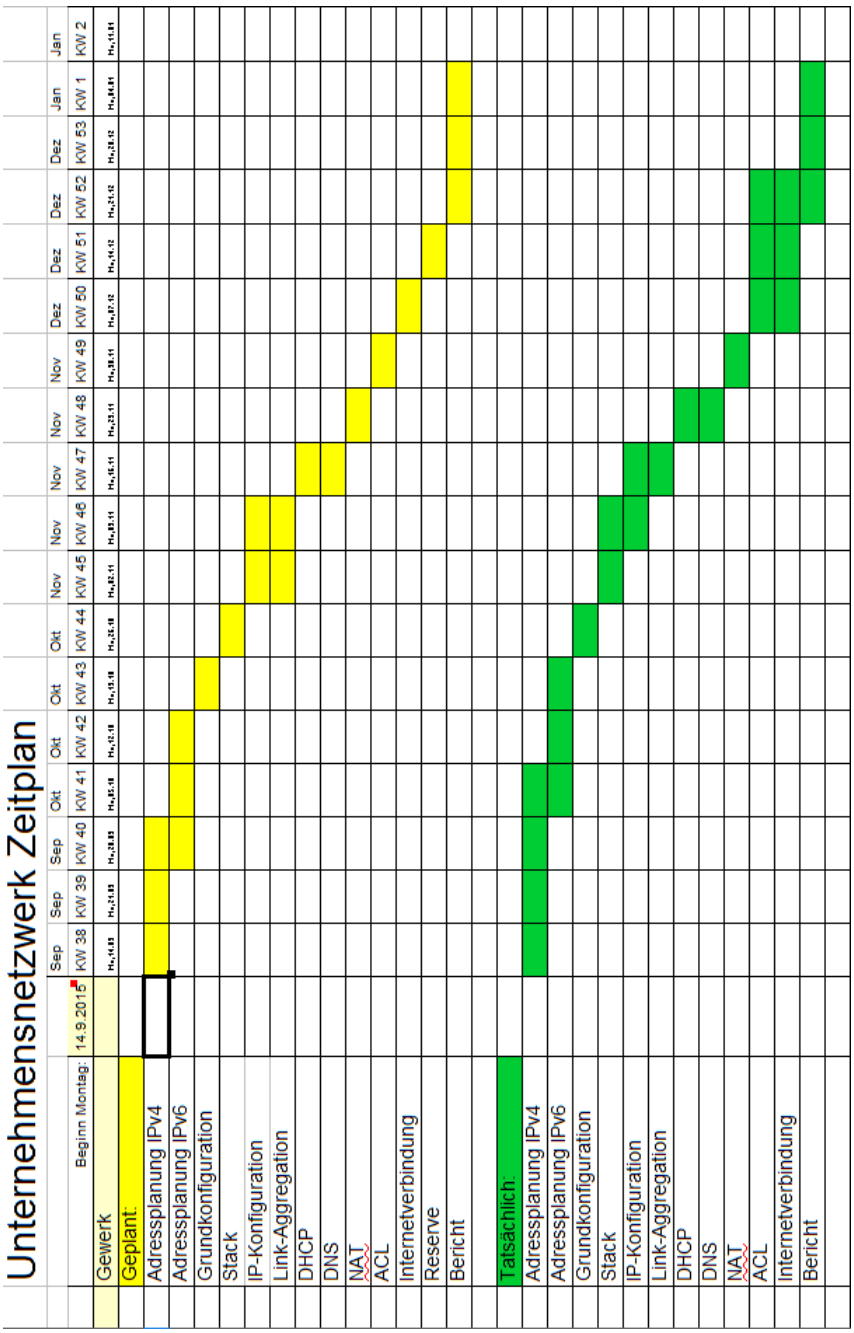

Abbildung 4.1: Zeitplan

5 Umsetzung

5.1 Grundlegende Konfiguration Router

```
R1(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#ipv6 unicast-routing
```

Listing 5.1: Router Grund Konfig

5.2 Grundlegende Konfiguration access Switches

Da auf den access Switches das Default Template kein IPv6 unterstützt, muss zuerst das Template gewechselt werden, um IPv6 nutzen zu können. Nach dem Template Wechsel ist ein Neustart des Switches nötig. der Template Wechsel wird wie folgt durchgeführt:

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#reload
```

Listing 5.2: Switch Template Wechsel

Danach kann die Grundkonfiguration vorgenommen werden. Das Default-Gateway ist die jeweilige IP-Adresse des Management Vlans des jeweiligen Routers oder Distribution-Switches.

```
S1(config)#hostname A1
S1(config)#no ip domain lookup
S1(config)#spanning-tree mode pvst
S1(config)#ip default-gateway 10.2.99.1
S1(config)#ip http server
S1(config)#ip http secure-server
```

Listing 5.3: Switch Grund Konfiguration

5.3 IP-Konfiguration

5.3.1 Router

Auf den Routern wurde auf das jeweilige GigabitEthernet-Interface die dazugehörige IPv4 und IPv6 Addresse zugewiesen. Zusätzlich wurde pro Router noch eine Link-Local Adresse zugewiesen, welche jedem genutztem GigabitEthernet-Interface zugewiesen werden muss. Des weiteren muss auf dem Interface noch IPv6 aktiviert werden. Auf den Routern R2 und R3 werden die Konfigurationen auf den Subinterfaces vorgenommen.

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 10.1.40.1 255.255.255.252
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#ipv6 address 2001:620:3101:1040::1/64
R1(config-if)#ipv6 enable
```

Listing 5.4: Router IP-Konfiguration

5.3.2 Distribution

Auf den Distribution-Switches wird gleich wie bei den Routern vorgegangen, allerdings werden die IP-Adressen, wenn vorhanden, auf den Port-Channel konfiguriert (siehe Kapitel 5.4. Zusätzlich müssen hier noch die Vlan-Interfaces mit den zugehörigen IP-Adressen definiert werden.

```
D(config)#interface Vlan10
D(config-if)#description Geschaeftsleitung
D(config-if)#ip address 10.1.10.1 255.255.255.0
D(config-if)#ipv6 address FE80::6 link-local
D(config-if)#ipv6 address 2001:620:3101:1010::1/64
D(config-if)#ipv6 enable
```

Listing 5.5: Distribution IP-Konfiguration

5.3.3 Access-Switches

Auf den Acces-Switches wird eine IP-Adresse dem Management-Vlan zugewiesen.

```
interface Vlan99
 ip address 10.1.99.10 255.255.255.0
 ipv6 address 2001:620:3101:1099::11/64
```

Listing 5.6: Access-Switch IP-Konfiguration

5.4 Link-Aggregation

Bei der Konfiguration der Port-Channel war wichtig das zuerst der Port-Channel selbst definiert wird und erst danach die Zuweisung zum GigabitEthernet-Interface erfolgt. Des weiteren war darauf zu achten das sowohl der Port-Channel als auch das GigabitEthernet-Interface als no Switchport definiert wurden, sofern dies erwünscht ist.

```
D(config)#interface Port-channel1
D(config-if)#no switchport
D(config-if)#ip address 10.1.40.18 255.255.255.252
D(config-if)#ipv6 address FE80::6 link-local
D(config-if)#ipv6 address 2001:620:3101:1043::2/64
D(config-if)#ipv6 enable
D(config)#interface GigabitEthernet2/0/22
D(config-if)#no switchport
D(config-if)#no ip address
D(config-if)#channel-group 1 mode active
```

Listing 5.7: Switch Grund Konfiguration

5.5 OSPF

5.5.1 IPv4

In Listing 5.8 ist die OSPF Konfiguration für IPv4 zu sehen. Dabei werden die angrenzenden Netzadressen angegeben. Access-Ports werden als Passive-Interface konfiguriert damit sie keine Hello-Packets empfangen.

```
R2(config)#router ospf 1
R2(config-router)#passive-interface GigabitEthernet0/0.10
R2(config-router)#passive-interface GigabitEthernet0/0.20
R2(config-router)#passive-interface GigabitEthernet0/0.30
R2(config-router)#passive-interface GigabitEthernet0/0.99
R2(config-router)#network 10.2.10.0 0.0.0.255 area 0
R2(config-router)#network 10.2.20.0 0.0.0.255 area 0
R2(config-router)#network 10.2.30.0 0.0.0.255 area 0
R2(config-router)#network 10.2.99.0 0.0.0.255 area 0
R2(config-router)#network 10.4.40.0 0.0.0.3 area 0
R2(config-router)#network 10.4.40.4 0.0.0.3 area 0
```

Listing 5.8: OSPF IPv4

5.5.2 IPv6

Bei IPv6 erfolgt die Konfiguration auf den einzelnen Interfaces.

```
R2(config)#interface GigabitEthernet0/0.10
R2(config-if)#ipv6 ospf 1 area 0
```

Listing 5.9: OSPF IPv6

5.6 NAT

Nat wird auf dem Router R1 konfiguriert. Hierzu werden die einzelnen Interfaces als ip nat outside oder inside konfiguriert. Zusätzlich werden noch pro VLAN und Standort NAT-Pools und ACL's definiert welche dann dem NAT zugewiesen werden. In Listing 5.10 sind die NAT-Pools und ACL's für das Vlan 10 definiert.

```
R1(config)#interface FastEthernet0/0/0
R1(config-if)#ip nat outside
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip nat inside
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip nat inside
R1(config)#interface Serial0/1/0
R1(config-if)#ip nat inside
R1(config)#ip nat pool chur10 195.176.242.17 195.176.242.17 netmask
   255.255.255.240
R1(config)#ip nat pool buchs10 195.176.242.21 195.176.242.21 netmask
   255.255.255.240
R1(config)#ip nat pool stgallen10 195.176.242.25 195.176.242.25 netmask
   255.255.255.240
R1(config)#access-list 101 permit ip 10.1.10.0 0.0.0.255 any
R1(config)#access-list 105 permit ip 10.2.10.0 0.0.0.255 any
R1(config)#access-list 109 permit ip 10.3.10.0 0.0.0.255 any
R1(config)#ip nat inside source list 101 pool chur10 overload
R1(config)#ip nat inside source list 105 pool buchs10 overload
R1(config)#ip nat inside source list 109 pool stgallen10 overload
```

Listing 5.10: NAT

5.7 ACL

Die Access-Listen werden wie in Kapitel 3.5.1 beschrieben konfiguriert. In Listing 5.11 ist die Konfiguration von R2 für das Vlan 10 zu sehen.

```
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.1.20.0
    0.0.0.255
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.1.30.0
    0.0.0.255
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.2.20.0
    0.0.0.255
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.2.30.0
    0.0.0.255
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.3.20.0
    0.0.0.255
R2(config)#access-list 116 deny   ip 10.2.10.0 0.0.0.255 10.3.30.0
    0.0.0.255
R2(config)#access-list 116 permit ip any any
R2(config)#access-list 116 permit tcp any any

R2(config)#ipv6 access-list b10
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:1020::/64
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:1030::/64
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:2020::/64
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:2030::/64
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:3020::/64
R2(config-ipv6-acl)#deny ipv6 2001:620:3101:2010::/64
    2001:620:3101:3030::/64
R2(config-ipv6-acl)#permit ipv6 any any
R2(config-ipv6-acl)#permit tcp any any
```

Listing 5.11: ACL

5.8 DHCP

5.8.1 IPv4

5.8.2 IPv6

5.9 DNS

6 Fazit

Wir taten uns am Anfang schwer mit dem Addresskonzept. Als wir das Addresskonzept aufgestellt hatten, folgten weitere Probleme welche nicht zuletzt aufgrund der gestackten Switches auftraten, was zu Zeitverzögerungen führte. Dies ist auch auf dem Zeitplan in Abbildung 4.1 zu sehen.