

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	4
2	Ausgangslage	5
2.1	Fallbeispiel	5
2.2	Praktikumsausrüstung	6
3	Konzept	7
3.1	Ipv4 Adresskonzept	7
3.2	Ipv6 Adresskonzept	8
3.3	Routingkonzept	9
3.4	NAT Konzept	9
3.4.1	IPv4	9
3.4.2	IPv6	9
3.5	Securitykonzept	10
3.5.1	ACL	10
3.5.2	Layer 2 Security	10
3.6	Serverservices	10
3.6.1	DHCP	10
3.6.2	DNS	10
3.7	Netzwerkplan	10
3.8	weitere Überlegungen	11
3.9	Stack	11
4	Planung	12
5	Umsetzung	12
5.0.1	Grundlegende Konfiguration Router	13
5.0.2	Grundlegende Konfiguration access Switches	13
5.0.3	Routing zwischen Standorten	13
5.0.4	NAT	13
5.0.5	ACL	13
5.0.6	DHCP	13
5.0.7	DNS	13
6	Fazit	14

Abbildungsverzeichnis

2.1	Netzwerkstruktur	6
3.1	Netzwerkplan	10
4.1	Zeitplan	12

Tabellenverzeichnis

Listings

5.1	Router Grund Konfig	13
5.2	Switch Grund Konfig	13

1 Abkürzungen

LACP Link Aggreaction Protocol

PagP Port Aggregation Protocol

2 Ausgangslage

2.1 Fallbeispiel

Sie sollen ein neues Netzwerk für die Mittelh grosse Firma HAC Home Audio Center AG aufbauen, 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 (durch einen einfachen Switch simuliert).

2.2 Praktikumsausrüstung

Die Netzwerkkomponenten sind bereits vorhanden, die physische Netzstruktur aufgrund der Gebäude-topographie 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 3750)
- 2x Layer-3 Switch (Cisco 3560)
- 2x Layer-2 Switch (Cisco 2960)

-Standort Buchs:

- 1x Router (Cisco 1920)
- 1x Layer-2 Switch (Cisco 2960)

-Standort St.Gallen:

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

Die vorgegebene Netzwerkstruktur ist in Abbildung 2.1 zu sehen:

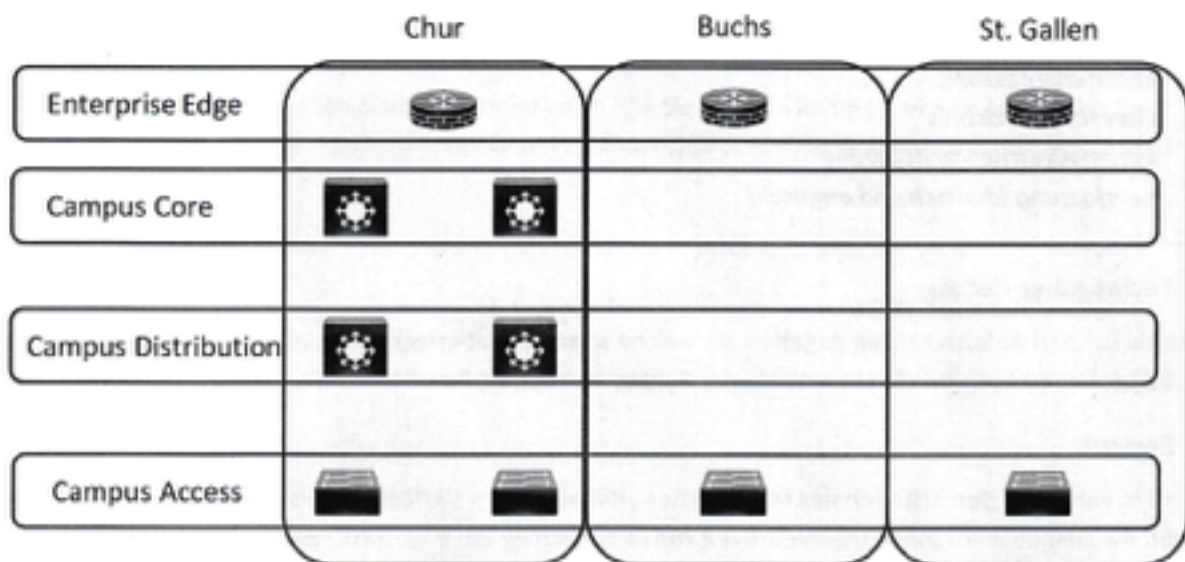


Abbildung 2.1: Netzwerkstruktur

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 Vlan werden die Netze der Standorte nochmals unterteilt, die gelben Sterne im Vlan-Plan stehen für die Standorte. Mit /24 Netzen stehen jeder Abteilung 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

3.6 Serverservices

3.6.1 DHCP

3.6.2 DNS

3.7 Netzwerkplan

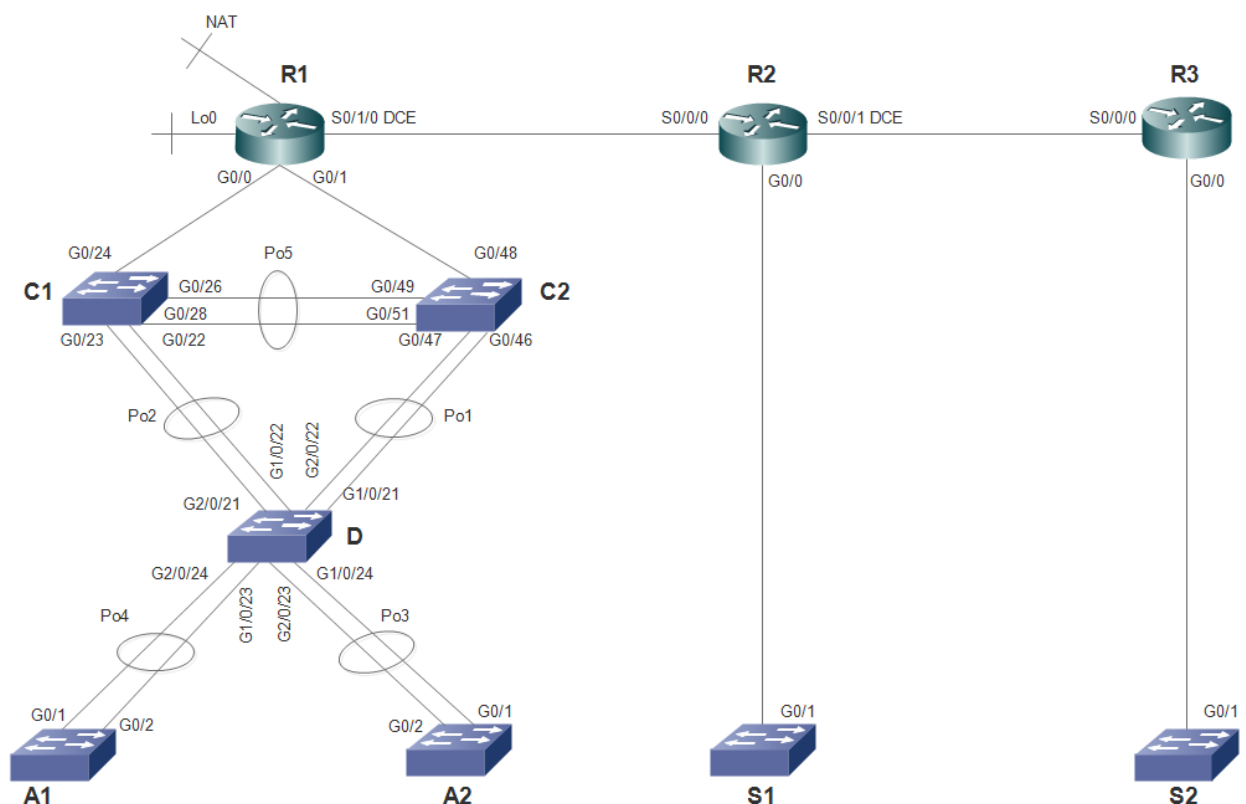


Abbildung 3.1: Netzwerkplan

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.

5 Umsetzung

5.0.1 Grundlegende Konfiguration Router

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

Listing 5.1: Router Grund Konfig

5.0.2 Grundlegende Konfiguration access 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 5.2: Switch Grund Konfig

5.0.3 Routing zwischen Standorten

5.0.4 NAT

5.0.5 ACL

5.0.6 DHCP

5.0.7 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.