# Übungsaufgaben
## Routing Basics

Dieses Dokument beinhaltet die Versuchsanleitung für die Durchführung des Laborversuches Routing Basics.

Bei Fragen zur Versuchsanleitung wenden Sie sich bitte direkt an das Laborpersonal.

**Autoren:** T. Jösler, S.Küng
**Version:** 1.3
**Letze Änderung:** 23.November 2022

## Änderungsverzeichnis

| Version | Datum | Status | Änderungen und Bemerkungen | Bearbeitet von |
|---|---|---|---|---|
| 1.0 | 22.02.19 | Erledigt | Neugestaltung Versuch Routing Basics | T. Jösler |
| 1.1 | 10.05.19 | Erledigt | Fehlerkorrektur | T. Jösler |
| 1.2 | 22.11.21 | Erledigt | Anpassung, Ergänzungen | S. Küng |
| 1.3 | 23.11.22 | Erledigt | Update Links | S. Küng |

# Inhaltsverzeichnis

## Abbildungsverzeichnis



## Abkürzungsverzeichnis

In diesem Dokument werden folgende Abkürzungen verwendet:

| Abkürzung | Beschreibung |
|---|---|
| IP | Internet Protokoll |
| VLAN | Virtual Local Area Network |
| ACL | Access Control List |
| SSH | Secure Shell |
| DHCP | Dynamic Host Configuration Protocol |
| NAT | Network Address Translation |

# Vorwort

Diese Laborübung soll den Studierenden den praktischen Umgang mit Cisco Hardware zeigen, wie sie auch in einem KMU Umfeld vorkommt. Die Studierenden sollen nach Abschluss dieser Übung fähig sein, ein kleines KMU Netzwerk aufzubauen.

## Feedback

Mit Ihrer Mithilfe kann die Qualität des Versuches laufend den Bedürfnissen angepasst und verbessert werden.

Falls in diesem Versuchsablauf etwas nicht so funktioniert wie es beschrieben ist, melden Sie diese bitte direkt dem Laborpersonal. Die Geräte, mit denen Sie den Laborversuch bestreiten, sind relativ teuer. Behandeln Sie die diese mit der entsprechenden Umsicht.

Bei Problemen wenden Sie sich bitte ebenfalls an das Laborpersonal.

## Legende

In den Versuchen gibt es Passagen, die mit den folgenden Zeichen markiert sind. Diese sind wie folgt zu verstehen:

Dringend beachten. Was hier steht, unbedingt merken oder ausführen.

Beantworten und dokumentieren Sie die Antworten im Laborprotokoll.

Ergänzender Hinweis / Notiz / Hilfestellung.

Weiterführende Informationen. Dies sind Informationen, die nicht zur Ausführung der Versuche benötigt werden, aber bekannt sein sollten.

# 1 Vorbereitung

Dieses Kapitel beschreibt Vorbereitungsmassnahmen, die vor Beginn der Übung durchzuführen sind.

## 1.1 Theorie

Beantworten Sie die Fragen in Kapitel 1.2 und notieren Sie Ihre Antworten. Sie finden die nötigen Informationen, um die Fragen zu beantworten an den unten erwähnten Stellen oder auch im grossen bösen Internet.

**Achtung:** Um die unten verlinkten Bücher öffnen zu können, müssen Sie sich zuerst einloggen unter https://www.oreilly.com/library-access/. Als Institution wählen Sie «Bibliotheken der Hochschule Luzern»

Frage1+2: Kapitel 6.1.- VLAN Segmentation:
https://learning.oreilly.com/library/view/routing-and-switching/9780134669632/ch06.html#ch06lev3sec1

Frage 3: Kapitel 7.1.4 - Types of IPv4 Addresses:
https://learning.oreilly.com/library/view/introduction-to-networks/9780134655604/ch07.html#ch07lev2sec4

Frage 4: Kapitel 7.1 - ACL Operation:
https://learning.oreilly.com/library/view/routing-and-switching/9780134669632/ch07.html#ch07lev3sec1

Frage 5: Kapitel 9.1 – NAT Operation:
https://learning.oreilly.com/library/view/routing-and-switching/9780134669632/ch09.html#ch09lev3sec1a

## 1.2 Fragen zur Theorie

✍ *1. Warum werden VLANs verwendet? Nennen Sie mindestens 3 Vorteile!*

.....

.....

.....

.....

✍ *2. Warum gibt es VLAN Tagging (802.1Q)? Wo wird das verwendet und warum?*

.....

.....

.....

.....

✍ *3. Was sind private und public IP Adressen? Wie unterscheiden sich diese?*

.....

.....

.....

.....

✍ *4. Sie kennen Access Control Lists (ACLs) bereits. Geben Sie hier zur Repetition wieder, was den Access Control Lists machen und wofür diese verwendet werden können.*

.....

.....

.....

.....

✍ *5. In der Übung werden wir Network Address Translation (NAT) konfigurieren.*
*Aus welcher Notwendigkeit heraus wurde NAT erfunden?*

.....

.....

.....

.....

# 2 Was wir heute lernen

Dieser Laborversuch vermittelt den Studierenden einen ersten Eindruck wie in einem KMU ein Netzwerk umgesetzt werden kann. Dabei wird als erstes das Netzwerk in drei logische VLANs unterteilt. Damit die Geräte in den verschiedenen VLANs miteinander sprechen können, muss mittel Hilfe eines Router-on-a-Stick Routing ermöglicht werden.

Die Adresskonfiguration von Endgeräten wird heute flächendeckend via DHCP gemacht. Auch Router können als DHCP Server agieren. Dies ist zwar nicht ihre primäre Aufgabe, für ein kleines Netzwerk reicht die vom Router bereitgestellte DHCP-Funktionalität jedoch absolut aus.

Um von einem internen Netzwerk ins Internet zu gelangen, benötigt man nicht nur eine Public IP Adresse sondern muss die intern verwendeten, privaten IP Adressen eine Network Adress Translation (NAT) einrichten. NAT übersetzt private Adressen in public Adressen, welche im Internet geroutet werden können.

Access Control Lists sind ein einfacher Mechanismus, um Zugriffe zu erlauben, respektive zu verbieten. Sie werden durch den Erstellungsprozess einer ersten Anforderung geführt. Danach sind Sie am Zug zwei weitere Anforderungen selbständig umzusetzen.

# 3 Vorbereitung der Laborumgebung

Dieses Kapitel beschreibt die vorbereitenden Massnahmen, die getroffen werden müssen, bevor mit der eigentlichen Konfiguration der Geräte begonnen werden kann.

## 3.1 Benötige Mittel

Verwenden Sie für diesen Versuch die Labor-Arbeitsstationen. Jedes Labor-Team benötigt einen Labor-Doppelarbeitsplatz.

- 1x Cisco Catalyst 2960 Switch
- 1x 1941 Router
- 2x Labor-PCs
- Diverse Anschlusskabel

## 3.2 Verkabelung

Für diesen Versuch müssen sie das folgende Netzwerk aufbauen.

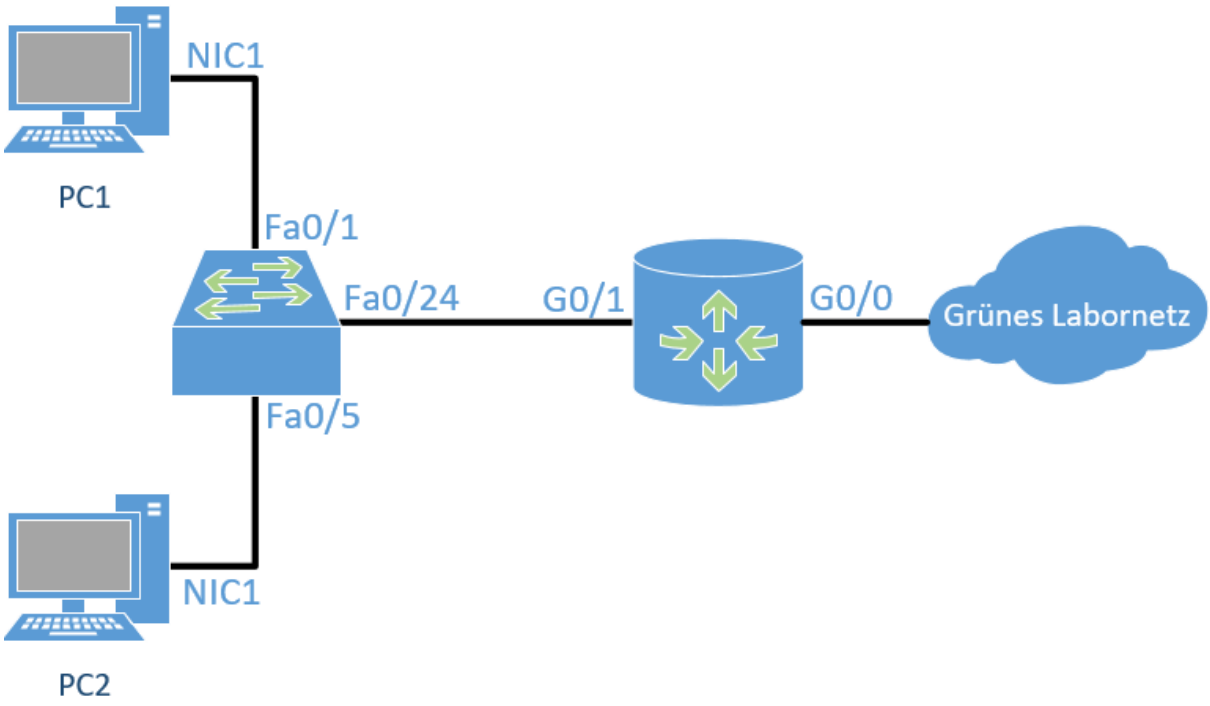


Abbildung 1: Netzwerkdiagramm - physikalische Sicht

Zum Ende dieser Übung werden Sie folgendes logisches Netzwerkdiagramm fertig implementiert haben. Sie können während der Übung auch immer wieder hier hin zurückkehren, um die Übersicht nicht zu verlieren.

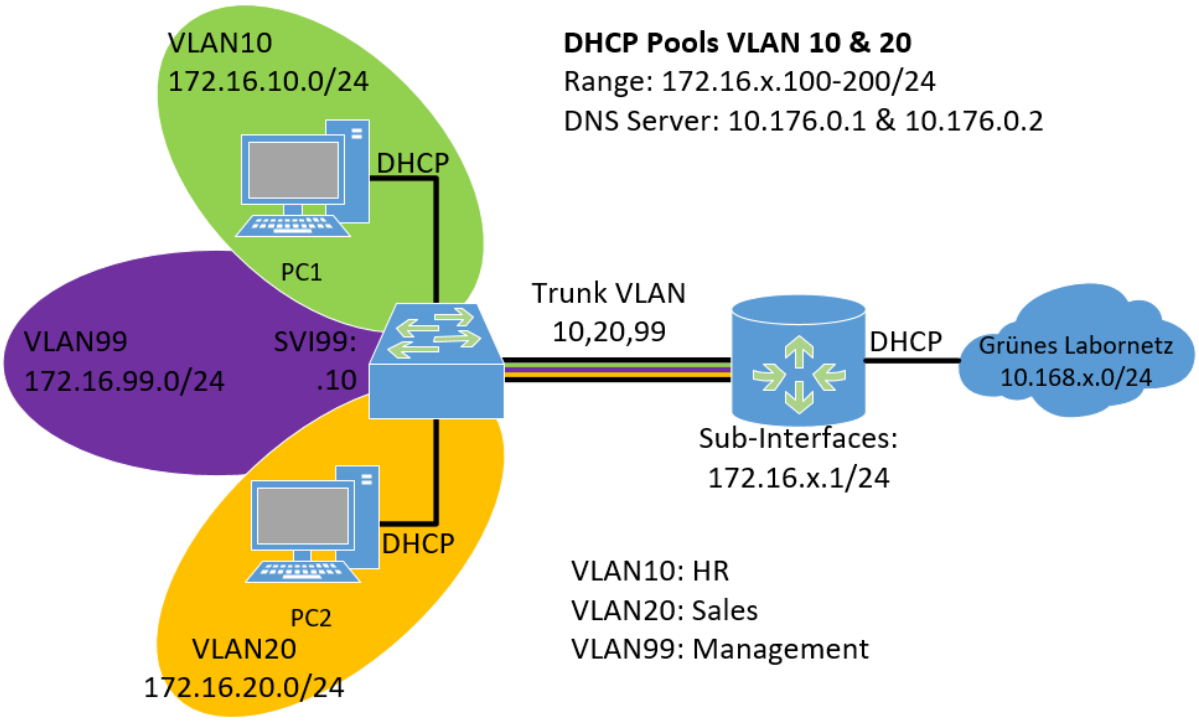


Abbildung 2: Netzwerkdiagramm - logische Sicht

## 3.3 Labor PCs

Führen Sie auf beiden PCs das Reset Script aus. Dieses setzt alle Netzwerkeinstellungen wieder auf Default zurück (DHCP).

## 3.4 Switch ALS1

Als erstes müssen wir verifizieren, dass Ihr Switch von Ihren Vorgängern korrekt auf die Werkeinstellungen zurückgesetzt wurden. Dazu müssen wir die folgenden zwei Konfigurationselemente eines Switches überprüfen: Startup-Config und vlan.dat File.

Lesen Sie den folgenden Abschnitt genau. Ist ihr Switch bereits auf die Werkeinstellungen zurückgesetzt, können Sie sich die folgenden Schritte sparen.

Um zu erkennen ob die Konfiguration von Ihrem Vorgänger zurückgesetzt wurde, müssten Sie die genaue Default-Konfiguration kennen und die running-config gegen diese vergleichen. Wir begnügen uns damit, zu überprüfen ob der Hostname des Switches der Default-Einstellung entspricht.

Der Hostname Ihres Switches muss "Switch" sein. Sie erkennen dies anhand der Terminaleingabe. Auch sollten Sie nicht aufgefordert worden sein, ein Passwort einzugeben oder ähnliches.

Sollte Ihr Hostname von "Switch" abweichen, müssen Sie folgenden Befehl absetzen, um die Startup-Config zu löschen.

```
*HOSTNAME*>enable
*HOSTNAME*#erase startup-config
```

Ein weiterer Teil der Konfiguration ist in der vlan.dat Datei gespeichert (VLANs). Die vlan.dat Datei ist im Flash abgespeichert. Kontrollieren Sie, ob die Datei vorhanden ist. Dies sollte auf einem korrekt zurückgesetzten Gerät **nicht** der Fall sein.

```
*HOSTNAME*#dir flash:
```

Falls die Datei **vlan.dat** dennoch vorhanden ist, löschen Sie diese Datei.

```
*HOSTNAME*#delete flash:vlan.dat
```

Damit die Werkeinstellungen geladen werden, muss der Switch neu gestartet werden.

```
*HOSTNAME*#reload
```

Sie müssen hier nicht warten bis das Gerät neu gestartet ist, sondern können bereits weiterfahren.

## 3.5 R1

Auch beim Router verifizieren wir, dass das Gerät von Ihren Vorgängern korrekt auf die Werkeinstellungen zurückgesetzt wurde. Die Konfiguration von Router besteht rein aus der Startup-Config.

Lesen Sie den folgenden Abschnitt genau. Ist Ihr Router bereits auf die Werkeinstellungen zurückgesetzt, können Sie sich den folgenden Schritt sparen.

Auch hier begnügen wir uns damit zu überprüfen, ob der Hostname des Routers der Default-Einstellung entspricht.

Der Hostname Ihres Routers muss "Router" sein. Sie erkennen dies anhand der Terminaleingabe. Auch sollten Sie nicht aufgefordert worden sein, ein Passwort einzugeben oder ähnliches.

Sollte Ihr Hostname von "Router" abweichen, müssen Sie folgenden Befehl absetzen, um die Startup-Config zu löschen.

```
*HOSTNAME*#erase startup-config
```

Damit die Werkeinstellungen geladen werden, muss der Router neu gestartet werden.

```
*HOSTNAME*#reload
```

*Was ist der Unterschied zwischen Startup- und Running-Config? Beschreiben Sie die Unterschiede und wie diese zwei Konfigurationen zusammenhängen.*

.....

.....

.....

.....

.....

# 4 Konfiguration VLAN Segmentierung

Dieses Kapitel beschreibt die Konfiguration von VLANs um ein physisches Netz in mehrere, kleinere logische Netzwerke zu unterteilen.

In einem ersten Schritt werden die VLANs auf unserem Switch erzeugt und Ports entsprechend konfiguriert. Um die Kommunikation zwischen verschiedenen VLANs zu erlauben, benutzen wir das "Router on a Stick" Konstrukt um Inter-VLAN Routing zu betreiben.

## 4.1 Konfiguration ALS1

Folgendes Kapitel deckt die Konfiguration des Switches ALS1 ab.

### 4.1.1 Basiskonfiguration

Konfigurieren Sie als erstes den Namen des Switches. Wechseln Sie dazu in den global config mode und führen Sie folgenden Befehl aus.

Um zwischen den Konfigurationsmodi hin und her zu switchen, benötigen Sie die folgenden Commands. Diese werden hier einmalig erwähnt. Danach wird erwartet, dass Sie selbst zwischen den Modi hin und her navigieren können.

| | |
|---|---|
| enable | Wechsel User exec Mode (>) nach Priviledged Exec Mode (#) |
| Configure terminal | Wechsel von nach Priviledged Exec Mode (#) nach Global Config Mode ((config)) |
| Exit | Mit Exit kann eine Stufe zurück navigiert werden. |

```
Switch(config)#hostname ALS1
```

Ein Switch kann grundsätzlich nicht nur über die Konsole konfiguriert werden, sondern auch Remote via Telnet oder SSH.

*Was ist der primäre Unterschied zwischen Telnet und SSH in Bezug auf Sicherheit?*
*Hint: Abschnitt "Summary"* *http://www.differencebetween.net/technology/internet/difference-between-telnet-and-ssh/*

.....

.....

.....

.....

Damit Sie einen Switch über SSH konfigurieren können, müssen Sie zuerst einige Konfigurationen vornehmen. Als erstes erstellen wir einen Benutzer, den wir zum Einloggen verwenden werden.

```
ALS1(config)#username cisco secret cisco
```

SSH benötigt ein RSA-Schlüsselpaar. Damit dieses generiert werden kann, wird ein Domain-Name benötigt. Setzen Sie als Domain-Name "networkinglab.ch" und generieren Sie das RSA-Schlüsselpaar. Das Generieren kann einige Sekunden dauern.

```
ALS1(config)#ip domain-name networkinglab.ch
ALS1(config)#crypto key generate rsa modulus 2048
```

Generieren Sie in der Praxis keine RSA Keys mit Modulus kleiner 4096!

Nun haben wir alle notwendigen Komponenten erstellt und können SSHv2 aktivieren.

```
ALS1(config)#ip ssh version 2
```

Nun ist SSH an sich aktiviert. Jedoch muss der Zugriff auf das Gerät noch separat erlaubt werden. Folgende Commands erlauben nur SSH Zugriff. Als Logindaten-Quelle wird "login local" definiert. Bedeutet, dass die User in der gerätinternen Datenbank genutzt werden.

```
ALS1(config)#line vty 0 4
ALS1(config-line)#transport input ssh
ALS1(config-line)#login local
```

*Können Sie sich nun per SSH auf den Switch verbinden? Oder fehlt noch etwas?*
*Hint: der Show command "show ip interface brief" zeigt Ihnen die Lösung auf.*

.....

.....

.....

.....

### 4.1.2 VLANs erstellen

Als nächstes erstellen wir drei VLANs. Eines für die HR Abteilung, eines für die Sales Abteilung und ein VLAN für das Management der Netzwerkkomponenten (Switch).

```
ALS1(config)#vlan 10
ALS1(config-vlan)#name HR
ALS1(config-vlan)#vlan 20
ALS1(config-vlan)#name Sales
ALS1(config-vlan)#vlan 99
ALS1(config-vlan)#name DeviceManagement
ALS1(config-vlan)#end
```

Kontrollieren Sie die erstellte Konfiguration mit dem folgenden Befehl:

```
ALS1#show vlan
```

Mit dem Befehl ***show vlan*** sehen Sie die unteranderem die Zuordnung der physikalischen Ports zu den entsprechenden VLANs. Momentan sind alle Ports im Default-VLAN. Die von Ihnen konfigurierten VLANs haben im Moment noch keine Ports zugeordnet.

*Welches ist denn das Default VLAN?*

.....

Je nach Switch können weitere VLANs vorhanden sein, welche zur Standardkonfiguration gehören.

### 4.1.3 Konfiguration der Access Ports

Ihre nächste Aufgabe ist nun die Switch-Ports zu konfigurieren und den entsprechenden VLANs zuzuweisen. Beachten Sie, dass ein Switch Access-Port jeweils nur einem VLAN zugeordnet werden kann.

Weisen Sie das VLAN 10 dem Port 0/1 zu.

```
ALS1(config)#interface range fastEthernet 0/1-4
ALS1(config-if-range)#switchport mode access
ALS1(config-if-range)#switchport access vlan 10
ALS1(config-if-range)#spanning-tree portfast
ALS1(config-if-range)#spanning-tree bpduguard enable
ALS1(config-if-range)#exit
ALS1(config)#
```

Weisen Sie dem VLAN 20 die Ports 0/5 bis 0/8 zu. Dazu verwenden wir den Range-Operator. Nachfolgend das Beispiel für die Ports 0/5 bis 0/8.

```
ALSwitch1(config)#interface range fastEthernet 0/5-8
ALS1(config-if-range)#switchport mode access
ALS1(config-if-range)#switchport access vlan 20
ALS1(config-if-range)#spanning-tree portfast
ALS1(config-if-range)#spanning-tree bpduguard enable
ALS1(config-if-range)#end
ALS1#
```

Kontrollieren Sie die getätigten Konfigurationen mit dem Befehl **show vlan**:

```
ALS1#show vlan
VLAN Name                              Status    Ports
---------------------------------- --------- -----------------------
...✂...
10   HR                                active    Fa0/1, Fa0/2, Fa0/3,
                                                 Fa0/4
20   Sales                             active    Fa0/5, Fa0/6, Fa0/7,
                                                 Fa0/8
...✂...
```

✍ *Wir haben Portfast und BPDU-Guard auf den Access Ports aktiviert. Was machen diese zwei Funktionen? Wieso sollte man diese aktivieren, bzw. wo kann es zu Problemen kommen, wenn man dies nicht macht?*

.....

.....

.....

.....

### 4.1.4 Erstellen eines Management Interfaces

Damit der Switch (Layer 2 Gerät) über das Netzwerk angesprochen werden kann, muss dieser über eine IP verfügen. Mit Hilfe von Switch Virtual Interfaces (SVI) können virtuelle Layer 3 Interfaces auf einem Switch erzeugt werden. Diesen kann eine IP zugeordnet und das Gerät danach darüber administriert werden.

Wechseln Sie wieder in den global Configuration Mode und geben sie folgende Commands ein.

```
ALS1(config)#interface vlan 99
ALS1(config-if)#ip address 172.16.99.10 255.255.255.0
ALS1(config-if)#no shutdown
```

Auch ein Switch benötigt ein Default-Gateway, damit er mit der Aussenwelt ausserhalb seines lokalen Netzwerkes kommunizieren kann.

```
ALS1(config)#ip default-gateway 172.16.99.1
```

Es ist weiterhin nicht möglich auf den Switch per SSH zuzugreifen. Das SVI befindet sich im VLAN 99, unsere Switchports jedoch in den VLANs 1, 10 und 20. Damit der Zugriff funktioniert, müssen wir zuerst Routing zwischen den verschiedenen VLANs konfigurieren.

### 4.1.5 Verbindung zu Router R1 konfigurieren

Als letztes Konfigurieren wir die Verbindung vom Switch ALS1 zum Router R1. Da mehrere VLANs über das gleiche Kabel gesendet werden sollen, müssen wir VLAN Tagging aktivieren. Dies bedeutet, dass wir die Verbindung als Trunk konfigurieren müssen. Dabei erlauben wir nur Pakete, welche aus unseren drei VLANs stammen, den Trunk verwenden zu können.

```
ALS1(config)#interface fastEthernet0/24
ALS1(config-if)#switchport mode trunk
ALS1(config-if)#switchport trunk allowed vlan 10,20,99
```

Somit ist die Konfiguration auf Seiten des Switches ALS1 abgeschlossen.

## 4.2 Konfiguration R1

Dieses Kapitel kümmert sich um die Router-Konfiguration. Um zwischen den verschiedenen VLANs kommunizieren zu können, konfigurieren wir Inter-VLAN Routing mittels Router-on-a-Stick Prinzip.

### 4.2.1 Basiskonfiguration

Als erstes werden wir wie auch schon auf dem Switch den Hostnamen für den Router konfigurieren.

```
Router(config)#hostname R1
```

Als nächstes möchten wir den Router auch per SSH administrieren können. Die Konfiguration erfolgt analog zur Switch-SSH-Konfiguration.

```
R1(config)#username cisco secret cisco
R1(config)#ip domain-name networkinglab.ch
R1(config)#crypto key generate rsa modulus 2048
R1(config)#ip ssh version 2
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
```

### 4.2.2 Sub-Interface konfigurieren

Damit die verschiedenen VLANs, welche über den Trunk geschickt werden, auf dem Router separiert werden können, müssen wir für jedes VLAN ein Sub-Interface erstellen. Dabei wird jedem Sub-Interface sein VLAN zugeordnet.

Die Interface Nummern können je nach Router Modell abweichen. Bei den neueren Routern im Lab (ISR4221) sind die Interfaces mit 3 Zahlen definiert (Bsp. GigabitEthernet0/0/1)

```
R1(config)#interface GigabitEthernet0/1
R1(config-if)#no shutdown
R1(config-if)#interface GigabitEthernet0/1.10
R1(config-subif)#description VLAN10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.16.10.1 255.255.255.0
```

Konfigurieren Sie analog die Sub-Interfaces für die VLANs 20 und 99.

```
R1(config-subif)#interface GigabitEthernet0/1.20
R1(config-subif)#description VLAN20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.16.20.1 255.255.255.0
R1(config-subif)#interface GigabitEthernet0/1.99
R1(config-subif)#description VLAN99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 172.16.99.1 255.255.255.0
```

*Was ist dieses "dot1q"? Woher kommt das?*

.....

.....

*Was fehlt zum jetzigen Zeitpunkt noch, damit ein Ping von PC1 zu PC2 möglich wird?*

.....

.....

.....

.....

# 5 Automatisierte Adressverteilung mittels DHCP

Um die IP Adressvergabe zentral zu steuern, werden wir R1 als DHCP Server konfigurieren. Für unsere Kleinunternehmung reicht der Router als DHCP Server völlig. In grösseren Unternehmen werden DHCP Server Lösungen oft in Verbindung mit einem IPAM (IP Address Management) System eingesetzt.

Als erster Schritt definieren wir, welche Adressen nicht via DHCP vergeben werden dürfen. Wir definieren, dass die ersten 10 Adresse jedes Subnetzes bereits reserviert sein sollen.

```
R1(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.10
R1(config)#ip dhcp excluded-address 172.16.20.1 172.16.20.10
```

Als nächstes definieren wir für jedes Subnetz, welches per DHCP IP Adressen erhalten soll, einen eigenen DHCP Pool. In der DHCP Pool Konfiguration können neben der Netzwerk-Definition auch zusätzliche Parameter wie Default Gateway oder DNS Server mitgegeben werden.

```
R1(config)#ip dhcp pool VLAN10
R1(dhcp-config)#network 172.16.10.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.10.1
R1(dhcp-config)#dns-server 10.176.0.1 10.176.0.2
```

Analog dazu erfolgt die Konfiguration des DHCP Pools für VLAN20.

```
R1(config)#ip dhcp pool VLAN20
R1(dhcp-config)#network 172.16.20.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.20.1
R1(dhcp-config)#dns-server 10.176.0.1 10.176.0.2
```

✍ *Warum erstellen wir keinen DHCP Range für das VLAN99? Was könnten die Gründe sein?*

.....

.....

.....

.....

✍ *Überprüfen Sie, dass die beiden PCs eine IP Adresse erhalten haben und notieren Sie die IP Adressen.*

.....

.....

.....

.....

☝ Welche IP Adressen eines DHCP Pools zuerst vergeben wird (höchste oder tiefste) ist Implementationssache und kann von Hersteller zu Hersteller unterschiedlich sein.

# 6 Testing der momentanen Konfiguration

Wir sind nun an einem Punkt angelangt, wo wir unsere momentane Konfiguration testen können.

Hier sind ein paar beispielhafte Testfälle, um unsere bis jetzt getätigte Konfiguration zu prüfen.

| Was | Wie testen? | Erwartetes Resultat | Effektives Resultat |
|---|---|---|---|
| Verbindung PC1 <-> PC2 | ping | funktioniert | |
| SSH Zugriff auf Switch | PuTTY | funktioniert | |
| SSH Zugriff auf Router | PuTTY | funktioniert | |
| Internet Zugriff | Ping 8.8.8.8 | Funktioniert nicht | |

# 7 Konfiguration Internetzugang

Im folgenden Kapitel werden wir den Zugang zum Internet einrichten.

## 7.1 Konfiguration WAN Interface R1

Ihre Internet-IP Adresse erhalten Sie von Ihrem Service Provider (hier dem Labornetzwerk). Dementsprechend konfigurieren wir das WAN Interface als DHCP Client.

```
R1(config)#interface gigabitethernet0/0
R1(config-if)#description WAN interface
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
R1(config-if)#end
```

Verifizieren Sie, dass das WAN Interface von R1 eine IP via DHCP erhalten hat.

```
R1#show ip interface brief
```

## 7.2 Einrichten Network Address Translation (NAT)

Im Folgenden werden wir NAT konfigurieren. Doch warum brauchen wir überhaupt NAT? Beantworten Sie die folgende Frage!

✍ *Warum braucht es NAT gegenüber dem Internet?*
*Hint: Überlegen Sie sich, wie private IP Adressen im Internet gehandhabt werden.*

.....

.....

.....

.....

Die NAT Konfiguration besteht grundsätzlich aus drei Komponenten:

| **Komponente** | **Funktion** |
|---|---|
| Access Control List | Gibt an, welche Source IP Adressen (Endgeräte) per NAT übersetzt werden dürfen. |
| Deklaration inside / outside | Gibt an, welche Interfaces des Routers auf der Inside Seite und welche auf der Outside Seite des NATs stehen. |
| NAT Definition | Definiert die NAT Regel. Verbindet die Access Control List mit der Outside IP Adresse. |

Zuerst konfigurieren wir die Access Control List. Dabei erlauben wir die drei Netzwerke (VLANs), welche wir zuvor konfiguriert haben. Wir verwenden hier eine Standard Access Control List. Im Gegensatz zu den Extended Access Control Lists, kann in Standard Access Control Lists nur die Source angegeben werden.

```
R1(config)#ip access-list standard NAT
R1(config-std-nacl)#permit 172.16.10.0 0.0.0.255
R1(config-std-nacl)#permit 172.16.20.0 0.0.0.255
R1(config-std-nacl)#permit 172.16.99.0 0.0.0.255
```

✍ *Lassen sich die ACE auch zusammenfassen, wenn ja, wie?*
*Was wären die Vor- und Nachteile der Zusammenfassung?*
*Hint: Sehen Sie sich die Wildcard Maske an.*

.....

.....

.....

Als nächstes rüsten wir die verschiedenen Interfaces mit Inside/Outside Deklaration aus. Dies müssen wir auf allen Sub-Interfaces (Inside) und dem WAN Interface (Outside) tun.

```
R1(config)#interface gigabitethernet0/1.10
R1(config-if)#ip nat inside
```

**Wiederholen** Sie den Schritt oben für die **beiden anderen Sub-Interfaces**.

Als nächstes konfigurieren wir das WAN Interface mit der ip nat outside Deklaration.

```
R1(config)#interface gigabitethernet0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

Als letzter Schritt aktivieren wir die NAT Regel.

```
R1(config)#ip nat inside source list NAT interface gigabitethernet0/0
```

## 7.3 Testen des NATs

Als nächstes wollen wir die NAT Konfiguration auf Ihre Funktionstüchtigkeit überprüfen. Nehmen Sie PC1 und öffnen Sie eine Webseite. Zum Beispiel https://www.google.com.

Dies muss funktionieren. Falls dies nicht der Fall ist, müssen Sie die vorherigen Schritte nochmals prüfen.

Nun wollen wir diesen Test auch noch auf PC2 durchführen. Öffnen Sie wieder die Google Webseite. Auch dies muss funktionieren.

Herzlichen Glückwünsch, Sie haben erfolgreich eine funktionierende Grundkonfiguration eines KMU Netzwerkes erstellt!

# 8 Zugriffe mittels Access Control Lists einschränken

In diesem Kapitel wenden wir uns ein wenig der Sicherheit zu. Access Control List sind ein sehr einfacher Mechanismus, mit welchem Zugriff erlaubt oder verweigert werden kann.

## 8.1 Anforderung 1

Zuerst wollen wir folgende Anforderung umsetzen:

"Aus dem Management Netzwerk heraus, sollen keine Verbindungen ins Internet möglich sein."

Im Folgenden wird die ACL hergeleitet und die Entwicklung davon ausführlich beschrieben. Wenn das für Sie langweilig ist, können Sie auch gleich mit der Implementierung weiterfahren und die beiden anderen Anforderungen umsetzen.

### 8.1.1 Theoretische Entwicklung der ACL

Im Folgenden sind die notwendigen Gedankengänge, welche zur Lösung zum obigen Problem führen, beschrieben.

Als erstes überlegen wir uns, wie wir testen können, ob wir die Anforderung oben erfüllen. Zudem müssen wir aufpassen, dass wir nicht zu restriktiv Zugriffe verweigern, sondern nur, dass umsetzen, was gefordert ist. Aus der Anforderung können wir folgende Testfälle ableiten.

**Testfälle:**

| **Test** | **Funktioniert?** |
|---|---|
| Ping PC1 nach ALS1 | Ja |
| Ping PC2 nach ALS1 | Ja |
| Ping ALS1 nach 8.8.8.8 | Nein |

Wir legen die Testfälle fürs erste auf die Seite. Diese werden wir für die Verifikation unserer ACL später wieder gebrauchen.

Tragen wir die Fakten, welche bereits klar sind, zusammen:

| | |
|---|---|
| Source: | VLAN99: 172.16.99.0/24 |
| Destination: | Alle ausserhalb unseres Ranges 172.16.0.0/16, welchen wir in unserem Adresskonzept verwenden. |
| Interface: | ? |
| Richtung: | ? |

Es gibt nun zwei Möglichkeiten wie wir diese ACL beschreiben können: Entweder verwenden wir das Source Netzwerk oder das Destination Netzwerk. Auch eine Kombination von beidem ist möglich.

Die Umsetzung via Source Netzwerk scheint intuitiv, jedoch macht uns da das NAT und die Reihenfolge, in welcher Routing, NAT und ACL in einem Cisco Router angewandt werden einen Strich durch die Rechnung. Hier finden Sie bei Interesse mehr Informationen dazu: https://cciethebeginning.wordpress.com/2010/06/08/order-of-operations-nat-routing-acl/

Aus oben genanntem Grunde konzentrieren wir uns auf die Destination Variante. Aus der Fakten-Tabelle oben leiten wir ab, dass alle Pakete die eine Destination IP Adresse ausserhalb des Netzwerk-Ranges 172.16.0.0/16 haben verboten sind. Dies lässt sich in einer ACL wie folgt abbilden.

| | |
|---|---|
| Source: | Any |
| Destination: | 172.16.0.0/16 |
| Aktion: | permit |

Übersetzt in einen ACL Command ergibt das folgendes Statement.

```
permit any 172.16.0.0 0.0.255.255
```

Wie Sie wissen, steht am Ende jeder ACL "unsichtbar" ein sogenannten implicit deny Statement. Dieses verbietet jeglichen Traffic, welchen wir weiter oben nicht erlaubt haben.

Als nächstes müssen wir das Interface bestimmen, auf welches wir die ACL anwenden. Da die ACL das Netzwerk des Interfaces G0/1.99 betreffen soll, ist es naheliegend, es mit diesem zu versuchen.

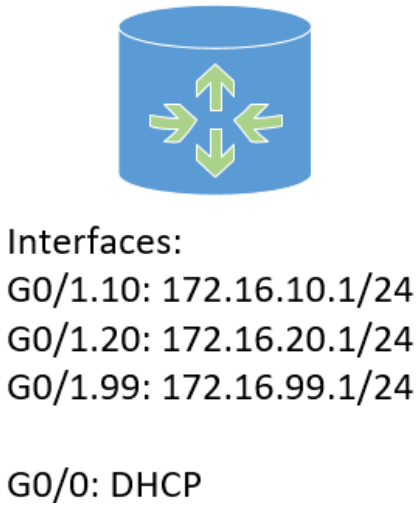


**Abbildung 3: Interfaces R1**

Applizieren wir gedanklich die obige ACL auf das Interface G0/1.99. Wir müssen entscheiden, in welche Richtung (in oder out) wir die ACL anwenden. Dabei betrachten wir die Richtung immer aus Sicht des betroffenen Interfaces.

Versuchen wir zuerst die ACL in out Richtung anzuwenden. Was bedeutet dies nun ausgeschrieben:

"Pakete welche das Interface G0/1.99 verlassen (also von aussen in Richtung Netzwerk 172.16.99.0/24 fliessen) sind betroffen."

Wir möchten jedoch, dass die Geräte des VLAN99 keinen Internet Zugang haben und nicht Zugriffe von aussen auf das Netzwerk 172.16.99.0/24 einschränken. Richtung "out" ist also die falsche Variante.

Machen wir das gleiche Gedankenexperiment mit Richtung "in". Ausgeschrieben bedeutet die ACL auf "in" angewandt:

"Pakete welche vom Netzwerk 172.16.99.0/24 her das Interface G0/1.99 erreichen sind betroffen".

Das ist das was wir brauchen. Wir haben nun also alle Informationen um die ACL umzusetzen:

| | |
|---|---|
| Source: | VLAN99: 172.16.99.0/24 |
| Destination: | Alle ausserhalb unseres Ranges 172.16.0.0/16, welchen wir in unserem Adresskonzept verwenden. |
| Interface: | G0/1.99 |
| Richtung: | in |

### 8.1.2 Umsetzung

Nun konfigurieren wir die ACL und applizieren sie auf dem passenden Interface.

```
R1(config)#ip access-list extended block-vlan99-internet
R1(config-ext-nacl)#permit ip any 172.16.0.0 0.0.255.255
R1(config-ext-nacl)#interface gigabitethernet0/1.99
R1(config-subif)#ip access-group block-vlan99-internet in
```

Führen Sie die zuvor definierten Testfälle durch. Überprüfen Sie, ob die Tests alle den erwarteten Resultaten entsprechen.

**Testfälle:**

| **Test** | **Funktioniert?** |
|---|---|
| Ping PC1 nach ALS1 | Ja |
| Ping PC2 nach ALS1 | Ja |
| Ping ALS1 nach 8.8.8.8 | Nein |

## 8.2 Anforderung 2

Nun sind Sie gefragt. Setzen Sie die folgende Anforderung selbstständig um. Es gibt mehrere Möglichkeiten das geforderte umzusetzen.

"Nur die HR Abteilung soll auf das DeviceManagement VLAN zugreifen können."

Mittels ping Command können Sie die Funktion ihrer ACL testen.

✍ *Notieren Sie die aus der obigen Aufgabe entstandene ACL. Schreiben Sie auch auf, auf welches Interface, sowie die Richtung, Sie die ACL angewandt haben.*

.....

.....

.....

.....

.....

.....

.....

## 8.3 Anforderung 3 (Challenge)

In dieser Challenge sollen Sie Ihr internes Netz gegen Anfragen vom Internet her mit Absenderadressen, welche im Internet-Kontext nicht vorkommen können, schützen.

Blockieren Sie folgende Netzwerk Ranges. Die restlichen IP Adressen sollen erlaubt sein.

- Multicast Adressen
- Broadcast Adressen
- Private IP Adressen
- Localhost Adressen
- Bogon Netzwerke (ungenutzte IP Address Ranges)

Nutzen Sie das Internet, um die nötigen Informationen zusammenzutragen.

✍ *Notieren Sie die aus der obigen Aufgabe entstandene ACL. Schreiben Sie auch auf, auf welches Interface, sowie die Richtung, Sie die ACL angewandt haben.*

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

# 9 Zurücksetzen der Geräte

Sie sind am Ende angekommen. Stellen Sie sicher, dass Sie Ihre Konfigurationen auf allen Geräten, mit den folgenden Befehlen gelöscht haben.

| | |
|---|---|
| Router Startup Konfiguration | ***write erase*** |
| Switch Startup Konfiguration | ***write erase*** |
| Switch VLAN Konfigurationen | ***delete flash:vlan.dat*** |