Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik
FH Zentralschweiz

NIS Labs
Networking+Services and
Information Security

Suurstoffi 41 b, CH-6343 Rotkreuz
T +41 41 757 68 64
www.hslu.ch

Informatik
Networking+Services and Information Security
Prof. Dr. Bernhard Hämmerli
T direkt +41 41 757 68 43
bernhard.haemmerli@hslu.ch

Routing Advanced

Dieses Dokument beinhaltet die Versuchsanleitung für die Durchführung des Laborversuches Routing Advanced im Labor Networking+Services. Bei Fragen zur Versuchsanleitung wenden Sie sich bitte direkt an das Laborpersonal.

Autoren: C. Di Battista, P.Gertsch, Prof. Dr. B. Hämmerli, D. Krummenacher, N. Lardieri, F. Pfanner, Ph. Schnyder, A. Suhl, A. Vogt
Version: 4.2
Letze Änderung: 22. Februar 2017

Laborbetreuung

Informatik
Networking+Services
Curdin Banzer

curdin.banzer@hslu.ch

Informatik
Networking+Services
Thomas Jösler

thomas.joesler@hslu.ch

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
Nr. 1.0	03.02.02	Erledigt	Versuch erstellt	Av
Nr. 1.1	22.03.03	Erledigt	Fehler korrigiert	Av
Nr. 1.2	27.04.05	Erledigt	IGRP durch OSPF ersetzt Fehler korrigiert	dk
Nr. 2.0	20.09.05	Erledigt	Versuch in Basics und Advanced aufgeteilt HSRP eingefügt	dk
Nr. 2.1	17.03.06	Erledigt	Fehler korrigiert	dk
Nr. 3.0	01.04.08	Erledigt	Komplette Überarbeitung	nl
Nr. 3.1	29.05.09	Erledigt	Neues Layout	nl
Nr. 3.2	07.01.10	Erledigt	Fehlerkorrektur/Update	nl
Nr. 3.3	14.10.10	Erledigt	Fehlerkorrektur/Update	nl
Nr. 3.4	09.05.12	Erledigt	Überarbeitung	C.Di Battista, F. Pfanner
Nr. 4.0	23.09.12	Erledigt	Überarbeitung	C.Di Battista, M. Schröder
Nr. 4.1	22.07.14	Erledigt	Kapitel 4 auf IPv6 umgeschrieben	Pg
Nr. 4.2	10.03.16	Erledigt	Algorithm-Type, Kontrollfrage bei 3.5 löschen	C. Banzer, E. Fux

Inhaltsverzeichnis

Änderungsverzeichnis I
Abbildungsverzeichnis III
Abkürzungsverzeichnis III
Vorwort 1
Feedback 1
Legende 1
Bemerkungen 1
1 Vorbereitung 2
1.1 Fragen zur Theorie 2
1.2 Antworten 2
1.3 Materialliste 2
2 Aufgabenstellung 2
2.1 Vorbereitende Arbeiten 2
2.2 Aufbau 2
2.3 Übersicht Versuche 3
2.3.1 Teil 1: Fortgeschrittene Routerkonfigurationen 3
2.3.2 Teil 2: Fortgeschrittenes Routing 3
2.3.3 Teil 3: Hot-Standby Routingprotokoll (HSRP) (optionales Kapitel) 3

2.4 Verwendung von USB-Datenträgern für die Routerkonfiguration ... 3
3 Fortgeschrittene Routerkonfigurationen (45 min) ... 5
3.1 Vorbereitung ... 5
3.1.1 Verkabelung ... 5
3.1.2 Computer-Konfigurationen ... 5
3.2 Grundkonfigurationen ... 6
3.2.1 Router Luzern ... 6
3.2.2 Router Bern ... 7
3.2.3 Router ISP ... 7
3.3 Interface-Konfigurationen ... 7
3.3.1 Router Luzern ... 7
3.3.2 Router Bern ... 7
3.3.3 Zwischenkontrolle ... 8
3.3.4 Konfiguration Routingprozess ... 8
3.3.5 Router ISP ... 10
3.4 Spezielle Konfigurationen ... 11
3.4.1 DHCP ... 11
3.4.2 NAT/PAT ... 12
3.4.3 Statisches PAT (Port Forwarding) ... 14
3.4.4 Access-lists ... 14
3.4.5 Konfigurationsdateien mittels USB-Datenträger auf den Router übertragen ... 17
3.5 Kontrollfragen ... 17
4 Fortgeschrittenes Routing (45 min) ... 19
4.1 Zurücksetzen Testumgebung ... 19
4.2 Vorbereitung ... 19
4.3 EIGRPv6 zwischen Bern-Luzern ... 20
4.4 OSPFv3 zwischen Luzern-ISP ... 20
4.5 OSPFv3 in EIGRPv6 ... 22
4.6 EIGRPv6 in OSPFv3 ... 24
4.7 Loopback in OSPFv3 ... 25
4.8 Kontrollfrage ... 26
5 Hot Standby Routing Protokoll (HSRP) (optional) (30 min) ... 27
5.1.1 Zurücksetzen Testumgebung ... 27
5.2 Vorbereitung ... 27
5.3 Vorbereitung ... 28
5.3.1 Kontrolle ... 28

5.4 HSRP 28
5.4.1 Theorie 28
5.4.2 Router Luzern 30
5.4.3 Router Bern 30
5.4.4 Konfiguration PCs 31
5.4.5 Kontrolle 31
5.5 Testen von HSRP 31
5.6 Kontrollfragen 33
6 Bemerkung Load Balancing 33
7 Anhang A - Vertiefung Access Control List ACL / Extended Access Lists ACE 34
8 Anhang B – DHCP 36
9 Anhang C – EIGRP 38
10 Anhang D - Passwort Recovery Prozedur 39

Abbildungsverzeichnis

Abb. 1: Versuchsaufbau Teil 1 5
Abb. 2: IIS-Manager 6
Abb. 3: Kontrolle IIS 6
Abb. 4: Versuchsaufbau Teil 2 inkl. EIGRPv6 AS 1 19
Abb. 5: OSPF Area 0 20
Abb. 6: OSPFv3 → EIGRPv6 22
Abb. 7: EIGRPv6 → OSPFv3 24
Abb. 8: Versuchsaufbau Teil 3 27
Abb. 9: Virtueller Router 29
Abb. 10: Physikalische Router 29
Abb. 11: Beispiel Load Balancing 33
Abb. 12: Funktionsweise des DHCPs 37

Abkürzungsverzeichnis

In diesem Dokument werden folgende Abkürzungen verwendet:

Abkürzung	Beschreibung
ACL	Access Control List
DCE	Data Communication Equipment (z.B. Modem)
DHCP	Dynamic Host Configuration Protokoll
DTE	Data Terminal Equipment (z.B. PC oder Router)
EIGRP	Enhanced Interior Gateway Routing Protocol
NAT	Network Address Translation
OSPF	Open Shortest Path First

PAT	Port Address Translation
HSRP	Hot-Standby Routingprotokoll

Vorwort

Dieser Versuch bringt den Studierenden den Umgang mit Routern näher. Er basiert auf dem Versuch IP Routing Basics. Es werden weiterführende Konfigurationen behandelt.

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 dies bitte direkt dem Laborpersonal oder erwähnen Sie es in Ihrem Laborbericht oder Protokoll. Die Geräte mit denen Sie den Laborversuch bestreiten, sind relativ teuer. Behandeln Sie diese mit der entsprechenden Umsicht. Die Syntax und die Ausgaben der einzelnen Befehle können je nach IOS-Version leicht verschieden sein. 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 werden hier erklärt.

Weiterführende Aufgaben. Dies sind Aufgaben, die nichts an den Versuchen ändern, aber ein vertieftes Wissen vermitteln.

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

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

Bemerkungen

Die Bezeichnung der Netzwerkschnittstelle kann unterschiedlich sein. Haben die Router 10/100Mbps-Port, dann werden die Interfaces mit FastEthernet bezeichnet. Sind es dagegen Gigabit Ports, dann sind es GigabitEthernet Interfaces.

Stellen Sie sicher, dass alle Firewalls und nicht benötigten Netzwerkinterfaces deaktiviert sind (Windows & Co).

Bitte entnehmen Sie die Muster-Konfigurationsdateien aus diesem PDF-Dokument, falls Sie die Konfigurationen aus Zeitgründen nicht selber vornehmen können oder um die Fehlersuche zu vereinfachen. Die Konfigurationsdateien sollten sich links in der Auflistung der angefügten Dokumente befinden.

1 Vorbereitung

Dieses Kapitel beschreibt die Vorbereitungsmassnahmen, die Sie zu Beginn des Laborversuches durchführen müssen.

1.1 Fragen zur Theorie

Beantworten Sie die folgenden Fragen richtig, können Sie den zugehörigen Theorieteil überspringen.

1. Erläutern Sie die Funktionsweise des DHCPs
2. Was ist EIGRP? Erläutern Sie die Funktionsweise.
3. Wieso und wie wird NAT eingesetzt?

1.2 Antworten

Frage 1: Anhang B – DHCP

Frage 2: Anhang C – EIGRP

Frage 3: Lesen Sie Kapitel NAT auf Seite 487 vom Buch Computernetzwerke von A.S. Tanenbaum

1.3 Materialliste

Für die Durchführung dieses Laborversuches benötigen Sie folgendes Material:

- 3x Cisco Router
- 2x Workstations
- 1x Studierenden-Notebook
- (optional) 1 Switch Catalyst 2950
- diverse Kabel

2 Aufgabenstellung

2.1 Vorbereitende Arbeiten

Prüfen Sie mittels ***show startup-config***, ob bei der Erstverwendung der Router noch alte Konfigurationen gespeichert sind und löschen Sie diese mittels ***erase startup-config***. Starten Sie, falls Sie eine noch vorhandene Konfiguration löschen mussten, danach den Router mittels ***reload*** neu.

2.2 Aufbau

Der Versuch ist in drei unabhängige Teile unterteilt. Nachdem ein Teil vollständig bearbeitet wurde, müssen Sie die Routerkonfiguration löschen und anschliessend den Router neu starten.

Bitte beachten Sie, dass für die Versuche jeweils Zeitlimits vorgegeben sind. Sollte es Ihnen nicht möglich sein, diese Zeitvorgaben einzuhalten, so überspringen Sie bitte die manuelle und zeitraubende Konfigurationseingabe und fügen Sie die zum Versuch und Router passende Konfigurations-Datei über die Konsole aus der Zwischenablage ein oder verwenden Sie einen FAT16 formatierten USB-Datenträger (Memorystick). Erweiterte Erklärungen dazu entnehmen Sie dem nachfolgenden Unterkapitel.

2.3 Übersicht Versuche

2.3.1 Teil 1: Fortgeschrittene Routerkonfigurationen

Der erste Teil des Versuchs steht im Thema "Anbindung einer Firma ans Internet". Sie schliessen ein kleines Firmennetzwerk an das Internet an. Die Firma ist auf zwei Standorte verteilt. Im Berner-LAN wird der Router als DHCP-Server verwendet und im Luzerner-LAN stehen nur Server mit statischen IP-Adressen.

Die Firma entschliesst sich, nur über den Standort Luzern mit einem ISP zu verbinden. Mittels NAT/PAT wird das Internet allen Angestellten ermöglicht. Die Firma hat zudem eine statische IP-Adresse gemietet und betreibt einen Web-Server.

Da die Firma noch keine Firewall besitzt (Lieferschwierigkeiten), erstellen sie einen rudimentären Zugriffsschutz des Netzwerks mittels Access-Listen konfigurieren.

2.3.2 Teil 2: Fortgeschrittenes Routing

Teil 2 des Versuchs beschäftigt sich ausschliesslich mit Routing-Protokollen und der Frage, wie Routen von und in andere Routingprotokolle ausgetauscht werden.

2.3.3 Teil 3: Hot-Standby Routingprotokoll (HSRP) (optionales Kapitel)

Im letzten Teil wird ein kleines Szenario aufgebaut, in dem das HSRP konfiguriert und getestet wird. Mit HSRP kann eine gewünschte Redundanz erreicht werden. Sie implementieren eine zweifache Redundanz. Zum einen sichern sie die Verbindung zum ISP und zum andern den Ausfall eines ganzen Routers.

2.4 Verwendung von USB-Datenträgern für die Routerkonfiguration

Im Rahmen der Routing-Advanced Labor-Versuche werden Router verwendet, die über USB-Anschlüsse verfügen. Diese können unter Berücksichtigung einiger Punkte zur Vereinfachung verwendet werden.

Um Konfigurationen für die Versuche nicht manuell erfassen zu müssen oder über eine Konsolenapplikation wie Putty einfügen zu müssen, bietet sich der schnelle und einfache Transfer mittels USB-Stick an.

Auch IOS-Binaries (Upgrades) können auf diesem Weg schnell eingelesen oder gesichert werden. Eine weitere Möglichkeit wäre die Verwendung von TFTP, wozu allerdings einige zusätzliche Arbeitsschritte nötig wären (Interface einrichten). TFTP kann zudem bei grösseren Datenmengen wie IOS-Binaries mehr Zeit in Anspruch nehmen, als dies mit USB-Datenträgern der Fall ist.

Cisco IOS kann allerdings nur FAT-16 formatierte Datenträger lesen. Zudem muss ein Cisco IOS mit der Version 12.3 oder höher installiert sein. Formatieren Sie bitte einen allfälligen Memorystick mit FAT16 und speichern Sie anschliessend die zu transferierenden Daten. Entfernen Sie den USB-Datenträger mittels „sicherem Entfernen“ bzw. „auswerfen“. Von der Verwendung einer USB-Harddisk anstelle eines USB-Memorystickes, wird hier abgeraten. Die korrekte Grösse des Datenträgers kann evtl. unter FAT16 falsch angezeigt werden. Bei Dateigrössen einer Konfigurationsdatei oder einer IOS-Binary muss allerdings mit keinen Problemen gerechnet werden.

Beachten Sie dabei, dass die USB-Datenträger im realen Umfeld ein Sicherheitsrisiko darstellen könnten, fielen sie denn in falsche Hände. Dementsprechend sollten diese Datenträger nach Gebrauch fachgerecht gelöscht oder sicher verwahrt werden. Bedenken Sie, dass die Konfigurationsdatei nicht

verschlüsselt ist und allfällige MD5-Hash-Passwörter mit heutiger Software zurückberechnet und damit verwendbar gemacht werden können.

Zur einfacheren und schnelleren Verwendung der Konfigurationsdateien erstellen Sie diese bitte vorgängig auf ihrem Rechner oder übernehmen Sie dem PDF Routing Advanced direkt die Router-Advanced-Dateien. Eine Auflistung der zu verwendenden Konfigurationsfiles befindet sich immer am Ende eines Versuches.

Falls Sie eigene Konfigurationsdateien erstellen möchten, verwenden Sie bitte eindeutige Dateinamen. Beinhalten sollten diese jeweils den Routernamen und einen Kurznamen für den Versuch (Kapitel). Cisco IOS behandelt Dateinamen case-sensitiv. Beachten Sie daher die Gross-/Kleinschreibung und bevorzugen Sie wenn möglich die Grossschreibung.

Als Beispiel für ein Konfigurationsfile zu Router 1 Kapitel 4: R1_K4.txt

Danach kann der USB-Datenträger verwendet werden. Stecken Sie ihn in den USB-Anschluss.

Das Kopieren einer Konfigurationsdatei kann folgenden Beispielen entnommen werden:

```
Router#copy usbflash0:R1_K4.txt running-config
Router#copy running-config startup-config
```

Bitte halten Sie diese Reihenfolge ein. Das direkte Einfügen der Konfiguration in die startup-config kann unter Umständen anders ausgeführt werden, als das Kopieren mittels copy running-config startup-config, da das Cisco IOS in diesem Kopier-Schritt noch eigene interne Anpassungen beim Speichern in die startup-config übernimmt. Ein Neustart ist dabei nicht notwendig.

Allfällige Anpassungen können danach auch wieder auf dem USB-Datenträger gespeichert werden, falls gewünscht:

```
Router#copy running-config usbflash0:R1_K5_NEU.txt
```

Prüfen Sie die eingelesenen Konfigurationen! Einige erste Kontrollen führen Sie mit folgenden Befehlen durch (achten Sie dabei auf die Interfaces, ob diese der Aufgabenstellung des Versuches entsprechen):

```
Router#show running-config
Router#show ip interface brief
Router#show ip routing
```

Sollte es Probleme mit dem USB-Datenträger geben, so prüfen Sie mittels der folgenden Befehle den USB-Datenträger.

```
Router#show usb device
Router#show usb controllers
Router#show usb driver
Router#show usb port

Router#show file system
```

3 Fortgeschrittene Routerkonfigurationen (45 min)

3.1 Vorbereitung

3.1.1 Verkabelung

Verkabeln Sie die Router, PCs und Ihr Notebook gemäss Schema. Achten Sie bei den seriellen Verbindungen auf die DCE- und DTE-Seite! Verwenden Sie **gekreuzte Ethernet Kabel**, wenn Sie die Hosts direkt mit dem Router verbinden.

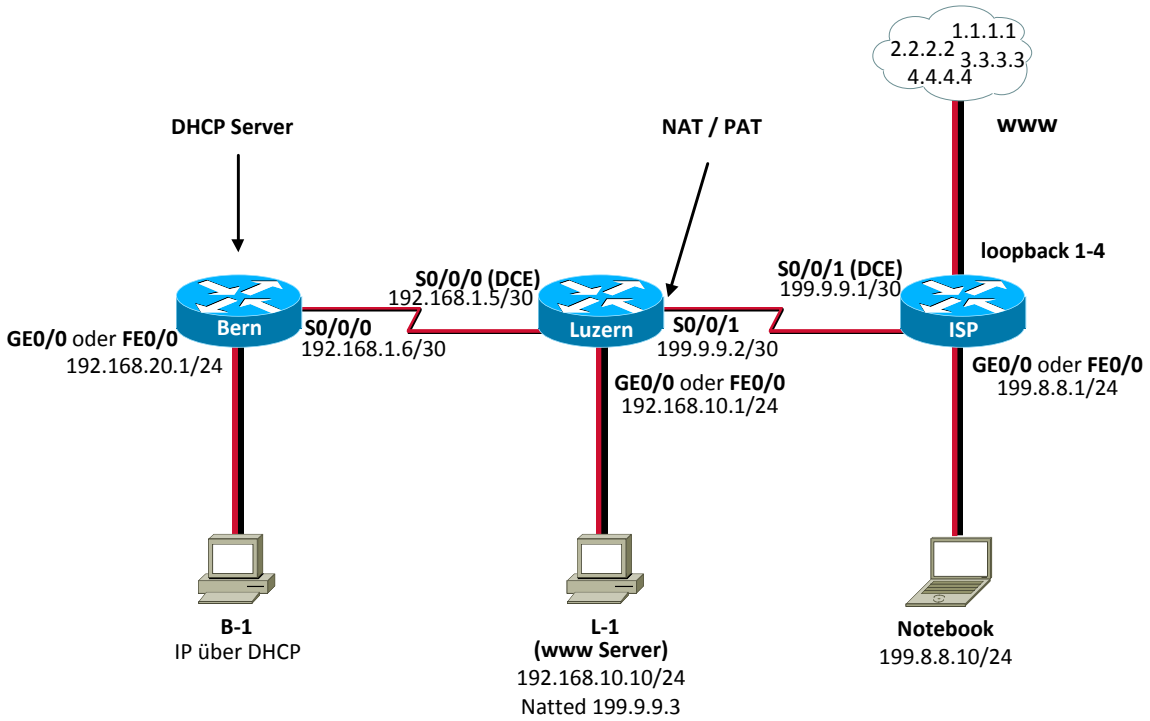

Abb. 1: Versuchsaufbau Teil 1

3.1.2 Computer-Konfigurationen

Bereiten Sie die PCs gemäss Schema vor. Konfigurieren Sie wo nötig die IP-Adresse und Standardgateways, oder stellen Sie die IP-Konfiguration auf DHCP ein. (NAT IP-Adresse wird später konfiguriert.)

Starten Sie den Webserver auf dem PC im LAN Luzern mit der IP-Adresse 192.168.10.10.

Klicken Sie auf **Start** und im Suchfeld geben Sie **inetmgr**.

Ist der Internet Information Server nicht installiert, kann er mit Systemsteuerung -> Programme und Funktionen -> Windows-Funktionen aktivieren oder deaktivieren -> Internetinformation installiert werden.

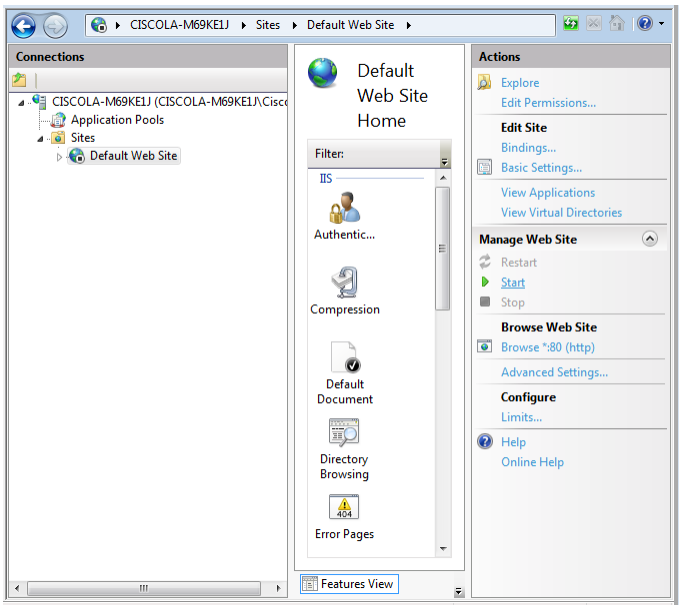

Abb. 2: IIS-Manager

Starten Sie nun die Standardwebsite, indem Sie auf der Symbolliste auf ▶ **Start** klicken.

Kontrollieren Sie, ob der IIS korrekt läuft. Starten Sie dazu auf PC1 einen Webbrowser und surfen Sie die Seite http://127.0.0.1 an.

Abb. 3: Kontrolle IIS

3.2 Grundkonfigurationen

3.2.1 Router Luzern

Erstellen Sie selbstständig die Grundkonfiguration vom Router Luzern. Konfigurieren Sie:

- Hostname
- Keine DNS-Abfragen
- Passwörter für Konsole- und Telnetverbindungen
- Passwort für Privilege Exec-Mode

3.2.2 Router Bern

Erstellen Sie selbstständig die Grundkonfiguration von Router Bern. Konfigurieren Sie:

- Hostname
- Keine DNS-Abfragen
- Passwörter für Konsole- und Telnetverbindungen
- Passwort für Privilege Exec-Mode

3.2.3 Router ISP

Die Grundkonfiguration von Router ISP ist vorbereitet. Kopieren Sie die folgenden Zeilen und fügen Sie sie in den globalen Konfigurationsmode des Routers ein.

```
hostname ISP
enable algorithm-type scrypt secret cisco
no ip domain-lookup
ip http server
line console 0
password cisco
login
line vty 0 4
password cisco
login
end
```

3.3 Interface-Konfigurationen

Alle Interfaces sind standardmässig deaktiviert. Sie müssen alle benötigten Interfaces manuell mit dem Befehl ***no shutdown*** aktivieren.

3.3.1 Router Luzern

Konfigurieren Sie das Interface FastEthernet0/0 von Router Luzern mit der IP-Adresse 192.168.10.1 und der Subnetmaske 255.255.255.0.

Konfigurieren Sie das Interface Serial0/0/0 von Router Luzern mit der IP-Adresse 192.168.1.5 und der Subnetmaske 255.255.255.252. Vergessen Sie nicht die Clock Rate von 128000 (bps) und die PPP-Encapsulation zu konfigurieren.

Konfigurieren Sie das Interface Serial0/0/1 von Router Luzern mit der IP-Adresse 199.9.9.2 und der Subnetmaske 255.255.255.252. Vergessen Sie nicht die PPP-Encapsulation.

Konfigurieren Sie auf Router Luzern eine statische Defaultroute, so dass alle unbekannten Zieladressen an Router ISP gesendet werden.

3.3.2 Router Bern

Konfigurieren Sie das Interface FastEthernet0/0 von Router Bern mit der IP-Adresse 192.168.20.1 und der Subnetmaske 255.255.255.0.

Konfigurieren Sie das Interface Serial0/0/0 von Router Bern mit der IP-Adresse 192.168.1.6 und der Subnetmaske 255.255.255.252. Vergessen Sie nicht die PPP-Encapsulation zu konfigurieren.

Testen Sie die serielle Verbindung zwischen Bern und Luzern. Verwenden Sie die Befehl show ip interface brief und ping.

3.3.3 Zwischenkontrolle

Kontrollieren Sie den Status der Interfaces und überprüfen Sie die serielle Verbindung mittels Ping.

Router Luzern:

```
luzern#show ip interface brief
Interface              IP-Address    OK?    Method Status Protocol
FastEthernet0/0        192.168.10.1 YES    manual up up
Serial0/0/0            192.168.1.5  YES    manual up up
Serial0/0/1            199.9.9.2    YES    manual up up
luzern#
```

Router Bern:

```
bern#show ip interface brief
Interface              IP-Address    OK?    Method Status Protocol
FastEthernet0/0        192.168.20.1 YES    manual up up
Serial0/0/0            192.168.1.6  YES    manual up up
Serial0/0/1            unassigned   YES    unset administratively down down
bern#
```

3.3.4 Konfiguration Routingprozess

Konfigurieren Sie EIGRP als Routingprotokoll zwischen Bern und Luzern. Konfigurieren Sie zuerst Router Luzern.

Wechseln Sie in den globalen Konfigurationsmodus.

```
luzern#configure terminal
```

Erstellen Sie einen EIGRP-Routingprozess mit der autonomen Systemnummer 1.

```
luzern(config)#router eigrp 1
```

Fügen Sie die lokalen privaten Netzwerke in den Routingprozess ein. Beachten Sie dabei, dass die Wildcard anstelle der Subnetmaske verwendet wird.

```
luzern(config-rtr)#network 192.168.10.0 0.0.0.255
luzern(config-rtr)#network 192.168.1.4 0.0.0.3
```

EIGRP soll die konfigurierte Defaultroute ebenfalls propagieren. Dies wird mit dem Befehl redistribute static gemacht.

```
luzern(config-rtr)#redistribute static
luzern(config-rtr)#exit
```

EIGRP benötigt ebenfalls die Bandbreite in seiner Metrik. Damit der Routing Prozess die effektiven Bandbreiten und nicht die maximalen Interface-Bandbreiten verwendet, müssen Sie auf allen seriellen Links die Bandbreite mit dem Befehl bandwidth angeben werden. Beachten Sie dabei, dass die Angaben in Kbits angegeben werden.

```
luzern(config)#interface serial0/0/0
luzern(config-if)#bandwidth 128
luzern(config-if)#end
```

Konfigurieren Sie nun Router Bern. Verwenden Sie zwingend die gleiche autonome Systemnummer 1! Sonst werden keine Neighbourbeziehungen aufgebaut und auch keine Updates ausgetauscht.

- EIGRP AS 1
- Netzwerk 192.168.1.4/30 und 192.168.20.0/24 (Wildcards!!)

Kontrollieren Sie die Routing-Konfigurationen mit dem Befehl ***show ip protocols***. Kontrollieren Sie ebenfalls die Routingtabelle.

Router Luzern:

```
luzern#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for Serial0/0/0
    192.168.1.0/24 for FastEthernet0/0
      Summarizing with metric 2169856
  Maximum path: 4
  Routing for Networks:
    192.168.1.4/30
    192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:02:32
    192.168.1.6           90      00:02:04
  Distance: internal 90 external 170
luzern#
luzern#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 199.9.9.1 to network 0.0.0.0
     199.9.9.0/24 is variably subnetted, 2 subnets, 2 masks
C       199.9.9.1/32 is directly connected, Serial0/0/1
C       199.9.9.0/30 is directly connected, Serial0/0/1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
D  192.168.20.0/24 [90/2195456] via 192.168.1.6, 00:02:10, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
D       192.168.1.0/24 is a summary, 00:02:39, Null0
C       192.168.1.4/30 is directly connected, Serial0/0/0
C       192.168.1.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 199.9.9.1
luzern#
```

Router Bern:

```
bern#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.20.0/24 for Serial0/0/0
    192.168.1.0/24 for FastEthernet0/0
      Summarizing with metric 2169856
  Maximum path: 4
  Routing for Networks:
    192.168.1.4/30
    192.168.20.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:00:40
    192.168.1.5           90      00:00:40
  Distance: internal 90 external 170
bern#
bern#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D  192.168.10.0/24 [90/2172416] via 192.168.1.5, 00:01:16, Serial0/0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
D       192.168.1.0/24 is a summary, 00:01:11, Null0
C       192.168.1.5/32 is directly connected, Serial0/0/0
C       192.168.1.4/30 is directly connected, Serial0/0/0
bern#
```

3.3.5 Router ISP

Die Interfacekonfiguration von Router ISP ist wieder vorbereitet. Kopieren Sie die folgenden Zeilen und fügen Sie sie in den globalen Konfigurationsmode des Routers ein. Die Loopback-Interfaces für die Simulation des Internet wird ebenfalls erstellt.

```
interface serial0/0/1
 description WAN-Link to Luzern
 ip address 199.9.9.1 255.255.255.252
 encapsulation ppp
 clock rate 128000
 no shutdown
```

```
interface loopback 1
 ip address 1.1.1.1 255.255.255.255
interface loopback 2
 ip address 2.2.2.2 255.255.255.255
interface loopback 3
 ip address 3.3.3.3 255.255.255.255
interface loopback 4
 ip address 4.4.4.4 255.255.255.255
! 10/100Mbs Interface-Konfiguration (Fehler ignorieren)
interface fastEthernet 0/0
 ip address 199.8.8.1 255.255.255.0
 no shutdown
end
```

Kontrollieren Sie den Status der Interfaces und überprüfen Sie die serielle Verbindung mittels Ping.

Router ISP:

```
ISP#show ip interface brief
Interface              IP-Address    OK? Method Status                Protocol
FastEthernet0/0        199.8.8.1        YES manual up                    up
Serial0/0/0            unassigned       YES unset  administratively down down
Serial0/0/1            199.9.9.1        YES manual up                    up
Loopback1              1.1.1.1          YES manual up                    up
Loopback2              2.2.2.2          YES manual up                    up
Loopback3              3.3.3.3          YES manual up                    up
Loopback4              4.4.4.4          YES manual up                    up
ISP#
```

3.4 Spezielle Konfigurationen

3.4.1 DHCP

Konfigurieren Sie Router Bern als DHCP-Server für das LAN-Segment von Bern.

Wechseln Sie in den globalen Konfigurationsmodus

```
bern#configure terminal
```

Verwenden Sie die ersten zwanzig IP-Adressen des 192.168.20.0-Netzes für allfällige Server im LAN. Konfigurieren Sie den Router, so dass die IP-Adressen von 1 bis 19 nicht verwendet werden.

```
bern(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.19
bern(config)#exit
```

Erstellen Sie einen neuen DHCP-Pool namens LanBern

```
bern(config)#ip dhcp pool LanBern
```

Definieren Sie das Netzwerk des DHCP-Pools

```
bern(dhcp-config)#network 192.168.20.0 255.255.255.0
```

Setzen Sie den DNS-Server, welcher die Clients erhalten sollten (DNS ist im Versuchsaufbau von keiner Bedeutung. Es ist nur der Vollständigkeit wegen angegeben.)

```
bern(dhcp-config)#dns-server 195.186.1.111
```

Setzen Sie das Standardgateway für die Clients

```
bern(dhcp-config)#default-router 192.168.20.1
```

Verlassen Sie die DHCP-Pool Konfiguration

```
bern(dhcp-config)#exit
```

Kontrollieren Sie, ob der PC im Berner-LAN bereits eine IP-Adresse des DHCP-Servers erhalten hat. Wenn nicht, dann forcieren Sie diesen Vorgang mit dem Befehl ***ipconfig /renew*** in der Eingabeaufforderung.

```
c:\>ipconfig /all
Windows-IP-Konfiguration
        Hostname. . . . . . . . . . . . : B-1
        Primäres DNS-Suffix . . . . . . . :
        Knotentyp . . . . . . . . . . . . : Hybrid
        IP-Routing aktiviert. . . . . . . : Nein
        WINS-Proxy aktiviert. . . . . . . : Nein

Ethernetadapter LAN-Verbindung:
        Verbindungsspezifisches DNS-Suffix:
        Beschreibung. . . . . . . . . . . : Realtek RTL8139
        Physikalische Adresse . . . . . . : 00-20-ED-4D-3A-47
        DHCP aktiviert. . . . . . . . . . : Ja
        IP-Adresse. . . . . . . . . . . . : 192.168.20.20
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.20.1
        DHCP-Server . . . . . . . . . . . : 192.168.20.1
        DNS-Server. . . . . . . . . . . . : 195.186.1.111
        Lease erhalten. . . . . . . . . . : Montag, 16. Mai 2005
        Lease läuft ab. . . . . . . . . . : Dienstag, 17. Mai 2005

c:\>
```

Auf dem Router sind die über DHCP vergebene IP-Adressen mit dem Befehl ***show ip dhcp bindings*** ersichtlich.

```
bern#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.20.20    0100.20ed.4d3a.47   Mar 01 1993 12:24 AM    Automatic
bern#
```

Mit ***ip helper*** können DHCP-Anfragen im LAN an einen DHCP-Server in einem anderen LAN weitergeleitet werden. Diese Funktion wird in diesem Versuch jedoch nicht benötigt.

3.4.2 NAT/PAT

Sicher ist es Ihnen bereits aufgefallen: Wir haben für unser internes Netz private IP-Adressen verwendet. Diese werden aber normalerweise beim Provider standardmässig geblockt! Wir kämen im Internet also nicht sehr weit!

Eine Lösung, die vor allem früher angewandt wurde, ist die Verwendung von öffentlichen Adressen. Dies führte zu einer Knappheit der IP Adressen. Wir dagegen implementieren die heute üblichere

Variante, wir verwenden NAT (Network Address Translation). Dabei werden auf unserem Corerouter Luzern alle ans Internet ausgehenden (und wieder einkommenden) IP-Pakete manipuliert. Wir lassen den Router die internen Source Adressen (SNAT – Source NAT) mit einer offiziellen (vom ISP zugewiesen), externen Adressen vertauschen. Die "incoming" Pakete werden genau umgekehrt manipuliert.

Genau genommen machen wir hier übrigens kein NAT, sondern PAT (Port Address Translation), auch IP-Masquerading genannt, da wir ja nur EINE externe IP haben – die des seriellen Interfaces gegen den Router ISP des Providers.

Alle Konfigurationen betreffend NAT müssen nur auf dem Router Luzern gemacht werden. Router ISP oder Bern "wissen" von der ganzen Adressmanipulationen nichts.

Konfigurieren Sie das Netzwerk resp. Port Address Translation auf Router Luzern.

Wechseln Sie auf Router Luzern in den globalen Konfigurationsmodus.

```
luzern#configure terminal
```

Erstellen Sie die NAT-Regel. Dabei werden interne Adressen (inside source) auf die Adresse des Interfaces Serial0/0/1 geändert. Overload gibt dabei an, dass Port Address Translation (PAT) verwendet wird.

```
luzern(config)#ip nat inside source list 1 interface serial0/0/1 overload
```

Erstellen Sie die Standard-Access-Liste 1. Sie wird verwendet, um die internen Host zu definieren, welche NAT resp. PAT berechtigt sind. In unserem Fall wählen wir das komplette private C-Klassennetzwerk 192.168.0.0 255.255.0.0 resp. die dazugehörige Wildcard 0.0.255.255.

```
luzern(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Zuletzt müssen Sie noch angeben, welche Interfaces intern oder extern verwendet werden. Die Address Translation wird dann automatisch zwischen intern und extern (und zurück) gemacht.

Konfigurieren Sie das Interface serial0/0/1 zum Router ISP als NAT outside.

```
luzern(config)#interface serial0/0/1
luzern(config-if)#ip nat outside
luzern(config-if)#exit
```

Konfigurieren Sie das Interface serial0/0/0 zum Router Bern und die lokale FastEthernet Schnittstelle als NAT inside.

```
luzern(config)#interface serial0/0/0
luzern(config-if)#ip nat inside
luzern(config-if)#exit
luzern(config)#interface fastEthernet 0/0
luzern(config-if)#ip nat inside
luzern(config-if)#exit
```

Kontrollieren Sie die konfigurierte Translation. Pingen Sie von den PCs das Internet mit der IP 1.1.1.1 an.

```
c:\>ping 1.1.1.1
```

Kontrollieren Sie die getätigten NAT-Translation auf Router Luzern

```
luzern#show ip nat translation
Pro Inside global  Inside local      Outside local      Outside global
icmp 199.9.9.2:513   192.168.10.10:512  2.2.2.2:512        2.2.2.2:513
icmp 199.9.9.2:512   192.168.20.20:512  1.1.1.1:512        1.1.1.1:512
luzern#
```

Bemerkung: Mit dieser Konfiguration benötigt Router ISP keine statische Routen oder ein Routing-Protokoll zu Router Luzern. Router ISP bekommt in Folge des NATs nur Pakete mit der Quell-IP-Adresse 199.9.9.2, welche eindeutig im Netzwerksegement zwischen Luzern und ISP ist.

3.4.3 Statisches PAT (Port Forwarding)

Im Luzerner LAN steht ein Webserver, welcher von aussen erreichbar sein sollte. Mit folgenden Schritten erreichen Sie die gewünschte Erreichbarkeit.

Konfigurieren Sie auf Router Luzern das statische PAT.

Wechseln Sie auf dem Router Luzern in den globalen Konfigurationsmodus

```
luzern#configure terminal
```

Erstellen Sie die statische NAT-Regel. Dabei wird die interne Adresse des Webservers 192.168.10.10 über die von extern erreichbare Adresse des Interfaces serial0/0/1 gelegt.

```
luzern(config)#ip nat inside source static tcp 192.168.10.10 80 interface
serial0/0/1 80
```

Kontrollieren Sie die Erreichbarkeit des Webservers von intern und von extern. Verwenden Sie für die externe Kontrolle ihr Notebook.

- Interne URL: http://192.168.10.10
- Externe URL: http://199.9.9.2.

Gibt Ihnen der Router oder der Web-Server Antwort, wenn Sie von Ihrem Notebook die IP-Adresse 199.9.9.2 anpingen?

Zur Kontrolle starten Sie auf dem Web-Server einen Sniffer. (WireShark)

3.4.4 Access-lists

In diesem Unterkapitel werden Sie einige einfache und nützliche Access-Listen erstellen. Eine Standard Access-Listen habe Sie bereits für das NAT/PAT konfiguriert. Es gibt neben Standard Access-Listen noch die anspruchsvolleren Extended Access-Listen. Einige weitere wichtige und nützliche Informationen zu diesem Thema entnehmen Sie bitte dem Anhang (Anhang A - Vertiefung Access Control List ACL / Extended Access Lists ACE)

Es kann eine Access-Liste pro Protokoll, pro Interface und pro Richtung gesetzt werden.

Jede Access-List hat am Ende der Regel ein implizites Deny, welches nirgends steht. Denken Sie immer daran!

Es gilt die Regel: Standard-ACL (1-99) so nahe am Ziel wie möglich (es wird nur der Sender überprüft). Extended-ACL (100-199), so nahe der Quelle wie möglich.

Im folgenden Beispiel werden nur mächtigere Extended Access-Lists verwendet. Zuerst werden zwei Beispiele vorgegeben. Anschliessend können Sie versuchen, selbstständig ACLs zu schreiben.

Aufgabe 1:

Sichern Sie ihr Netzwerk so, dass nur Anfragen an TCP Port 80 auf den Webserver gelangen (von intern und extern).

Lösung 1:

Für die Lösung wird eine Extended AccessList verwendet, da nur der Web-Traffic (TCP Port 80) erlaubt ist. Die Access-Liste wird mit folgender Syntax erstellt.

Konfigurieren Sie die Access-Liste.

```
luzern(config)#access-list 100 permit tcp any any established
luzern(config)#access-list 100 permit tcp any host 192.168.10.10 eq www
```

Beachten Sie das implizites ***deny any any*** am Ende.

Dabei gilt folgender Befehlsaufbau/Syntax für die Erstellung der Extended ACL:

> *Router(config-if)#**access-list** access-list-name [line line_number] [extended] {**permit** |**deny**} protocol source_address mask [operator port] dest_address mask [operator port | ICMP_type] [inactive]*

Anschliessend müssen Sie die ACL an ein Interface binden. Binden Sie die ACL an das Interface von Router Luzern Richtung Webserver und lassen Sie den Inbound-Datenverkehr kontrollieren.

```
luzern(config)#interface fastEthernet 0/0
luzern(config-if)#ip access-group 100 out
```

Dabei gilt folgender Befehlsaufbau/Syntax für die Zuweisung der Extended ACL zu einem Interface:

> *Router(config-if)#{protocol} **access-group** access-list-number {in | out}*

Kontrolle 1:

Kontrollieren Sie nun die Korrektheit der ACL.

1. Versuchen Sie von PC B-1 die URL http://192.168.10.10 zu öffnen.
   ➔ Dies sollte funktionieren.
2. Versuchen Sie von Ihrem Notebook (angeschlossen beim ISP) die URL http://199.9.9.2 zu öffnen.
   ➔ Dies sollte funktionieren.
3. Versuchen Sie von PC B-1 die IP 192.168.10.10 zu pingen.
   ➔ Dies sollte nicht gehen.

Aufgabe 2:

Sichern Sie ihr Netzwerk so, dass der Web-Server nicht auf das interne Segment zugreifen kann. Ins Internet sollte alles möglich sein.

Lösung 2:

Erstellen Sie wieder eine neue Access-Liste auf dem Router Luzern und verknüpfen Sie die Liste wieder mit der LAN-Schnittstelle zum Web-Server. Diesmal kontrollieren Sie jedoch den Inbound-Verkehr.

Konfigurieren Sie die ACL.

```
luzern(config)#access-list 101 permit tcp any any established
luzern(config)#access-list 101 deny ip any 192.168.0.0 0.0.255.255
luzern(config)#access-list 101 permit ip any any
```

Dabei gilt folgender Befehlsaufbau/Syntax für die Erstellung der Extended ACL:

> *Router(config-if)#**access-list** access-list-name [line line_number] [extended] {**permit** |**deny**} protocol source_address mask [operator port] dest_address mask [operator port | ICMP_type] [inactive]*

Anschliessend müssen Sie die ACL an ein Interface binden. Binden Sie die ACL an das Interface von Router Luzern Richtung Webserver und lassen Sie den Inbound-Datenverkehr kontrollieren.

```
luzern(config)#interface fastEhternet 0/0
luzern(config-if)#ip access-group 101 in
```

Dabei gilt folgender Befehlsaufbau/Syntax für die Zuweisung der Extended ACL zu einem Interface:

> Router(config-if)#{protocol} access-group access-list-number {in | out}

Kontrolle 2:

Kontrollieren Sie nun die Korrektheit der ACL.

1. Versuchen Sie von PC B-1 die URL http://192.168.10.10 zu öffnen.
   ➔ Dies sollte funktionieren.
2. Versuchen Sie von Ihrem Notebook (angeschlossen beim ISP) die URL http://199.9.9.2 zu öffnen.
   ➔ Dies sollte funktionieren.
3. Versuchen Sie von PC B-1 die IP 192.168.10.10 zu pingen.
   ➔ Dies sollte nicht gehen.
4. Versuchen Sie vom Web-Server L-1 die IP 192.168.10.1 und die IP 192.168.20.1 zu pingen.
   ➔ Dies sollte nicht gehen.
5. Versuchen Sie vom Web-Server L-1 die URL http://1.1.1.1 zu öffnen.
   ➔ Dies sollte funktionieren.
6. Versuchen Sie vom Web-Server L-1 die IP 1.1.1.1 zu pingen.
   ➔ Dies sollte gehen, jedoch funktioniert es nicht. Der Grund liegt in den Antwortpaketen, welche bereits durch die Access-List 100 (Aufgabe 1) geblockt werden.
7. Korrigieren Sie die Access-Liste 100 so, dass die Echo-Antworten an den Webserver gesendet werden.

   ```
   luzern(config)#access-list 100 permit icmp any host 192.168.10.10 echo-reply
   ```

8. Korrigieren Sie anschliessend noch die Access-Liste 101, so dass Echo-Requests vom Webserver gesendet werden können.

```
luzern(config)#access-list 101 permit icmp host 192.168.10.10 any echo
```

9. Versuchen Sie vom Web-Server L-1 die IP 1.1.1.1 erneut zu pingen.
   Jetzt sollte dies funktionieren.

Implementieren Sie folgende Access-Listen selbstständig. Beachten Sie das implizite Deny am Ende jeder ACL.

Aufgabe 3:

Host von LAN Bern dürfen die Webseite von http://1.1.1.1 nicht erreichen (beliebte News-Seite der Angestellten). Die IP-Adresse 1.1.1.1 sollte aber anpingbar sein.

Lösung 3:

Erarbeiten Sie die ACL selbstständig. Überlegen Sie, wo Sie die ACL platzieren müssen (beachten Sie die Regel).

Kontrolle 3:

Kontrollieren Sie die Korrektheit der ACL.

1. Versuchen Sie von PC B-1 die URL http://1.1.1.1 zu öffnen.
   ➔ Dies sollte nicht gehen.
2. Versuchen Sie von PC L-1 die URL http://1.1.1.1 zu öffnen.
   ➔ Dies sollte funktionieren.
3. Versuchen Sie von PC B-1 die IP 1.1.1.1 zu pingen.
   ➔ Dies sollte funktionieren.

Aufgabe 4:

Überlegen Sie sich selbstständig eine weitere Access-Liste und konfigurieren Sie diese. Machen Sie sich Gedanken, wie Sie die ACL kontrollieren können.

3.4.5 Konfigurationsdateien mittels USB-Datenträger auf den Router übertragen

Bitte entnehmen Sie die Konfigurationsdateien aus diesem PDF-Dokument, falls Sie die oberen Konfigurationen aus Zeitgründen nicht selber vornehmen können. Die Konfigurationsdateien sollten sich links in der Auflistung der angefügten Dokumente befinden.

Folgende Dateien gehören zu diesem Kapitel 4:

1. BERN_K4.txt
2. LUZERN_K4.txt
3. ISP_K4.txt

Bitte löschen Sie am Ende dieses Versuches alle startup-configs mittels ***erase startup-config*** !

3.5 Kontrollfragen

- Wann muss bei EIGRP die autonome Systemnummer, zwischen zwei oder mehrere Routern, gleich sein? Wann nicht?
- Wann wird NAT/PAT eingesetzt?

- Was erzielt man mit Access-Listen?
- Was erzielt man mit *redistribute static* bei EIGRP?
- Was ist der Unterschied zwischen bandwith und clock-rate?

4 Fortgeschrittenes Routing (45 min)

4.1 Zurücksetzen Testumgebung

Löschen Sie auf allen Routern die Konfiguration und starten Sie die Router neu. Die Verkabelung können Sie belassen.

```
Router#erase startup-configuration
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm] [Enter]
[OK]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm] [Enter]
```

Machen Sie dies auf allen Routern und anschliessend können Sie eine kurze Pause machen, bis die Router bereit sind.

4.2 Vorbereitung

Installieren Sie mittels USB-Datenträger die Konfigurationsdateien auf den Routern. Überprüfen Sie die mittels Konfigurationsdatei angewandten Konfigurationen.

1. BERN_INIT_K4_IPv6.txt
2. LUZERN_INIT_K4_IPv6.txt
3. ISP_INIT_K4_IPv6.txt

Falls Sie gut in der Zeit liegen, ist es empfehlenswert, die Befehle von Hand einzugeben, anstatt sie einfach zu kopieren.

Nach den Vorbereitungen sieht Ihr Netzwerk wie folgt aus:

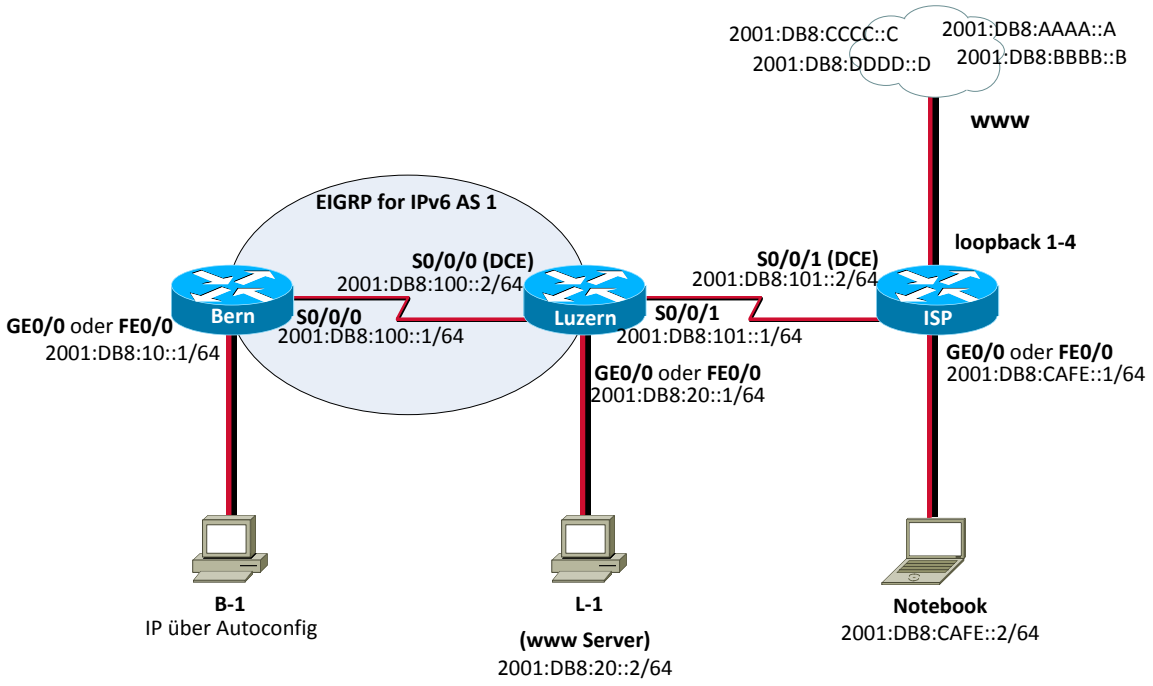

Abb. 4: Versuchsaufbau Teil 2 inkl. EIGRPv6 AS 1

Zur Vereinfachung wurden die Verkabelung und die Hostnamen beibehalten.

4.3 EIGRPv6 zwischen Bern-Luzern

Der EIGRPv6-Prozess (AS 1) wurde analog zum Teil 1vorkonfiguriert, jedoch mit dem Routing Protokoll EIGRP for IPv6 oder auch EIGRPv6 genannt.

Speziell ist zu erwähnen, dass man die Zuteilung der Interfaces zu den Routing Prozessen in IPv6 direkt auf den Interfaces vornimmt und das globale IPv6 Unicast-Routing vorgängig aktivieren muss.

Da die Router in der neuen Umgebung keine IPv4 Adressen mehr besitzen, mussten die Router IDs für das EIGRPv6 manuell konfiguriert werden. Diese müssen immer noch nach dem IPv4 Format erstellt werden. Auch muss das EIGRPv6 Protokoll mit dem Befehl „no shutdown“ im globalen „ipv6 router eigrp 1“-Konfigurationsmenü aktiviert werden.

Kontrollieren Sie die Routing-Tabelle der Router Bern und Luzern. Sehen Sie Routen, welche von EIGRPv6 gelernt wurden?

Beachten Sie, dass die IPv6 Routingtabelle unabhängig von der IPv4 Routingtabelle ist.

4.4 OSPFv3 zwischen Luzern-ISP

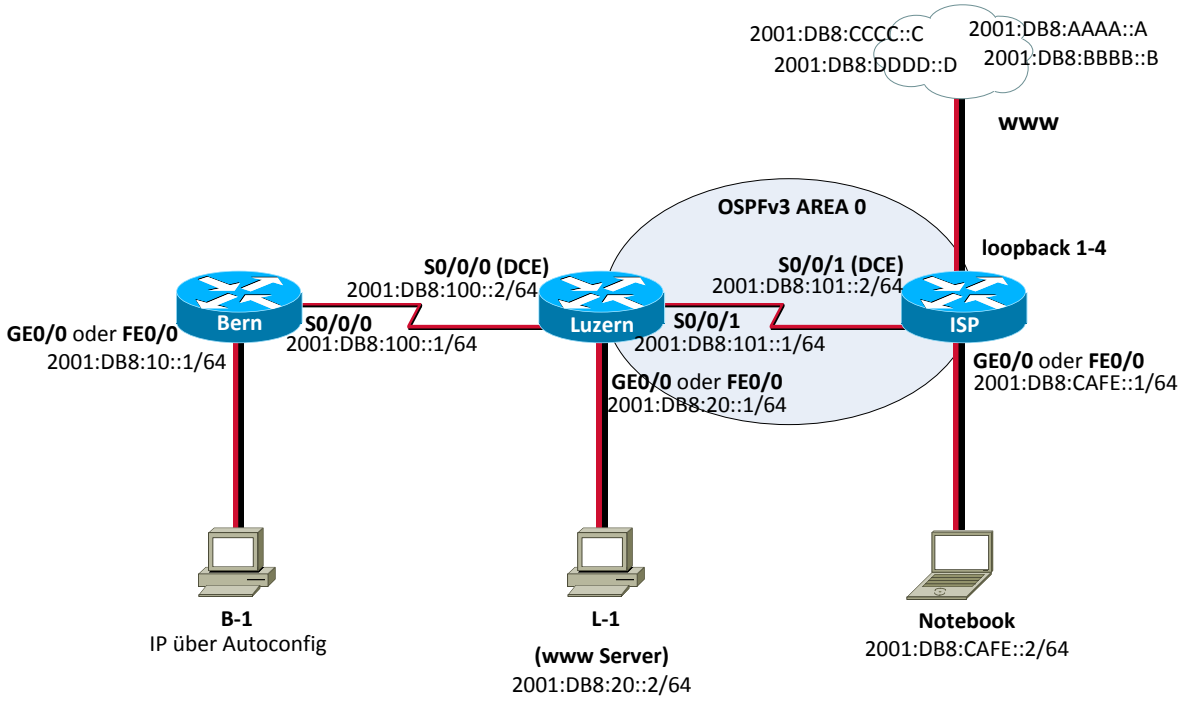

Abb. 5: OSPF Area 0

Konfigurieren Sie auf Router Luzern und ISP den OSPFv3-Prozess (Prozess-ID 1). Verwenden Sie ausschliesslich die Area 0.

Fügen Sie bei Router Luzern nur das Interface Serial0/0/1 in den Prozess ein. Beim Router ISP die Interfaces Serial0/0/1 und FastEthernet 0/0.

Router Luzern:

```
luzern#configure terminal
luzern(config)#interface serial 0/0/1
luzern(config-if)#ipv6 ospf 1 area 0

%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure
manually

luzern(config-if)#exit
luzern(config)#ipv6 router ospf 1
luzern(config-rtr)#router-id 1.1.101.1
luzern(config-if)#end
```

Router ISP:

```
ISP#configure terminal
ISP(config)#ipv6 router ospf 1
ISP(config-rtr)#router-id 1.1.101.2
ISP(config-rtr)#exit
ISP(config)#interface serial 0/0/1
ISP(config-if)#ipv6 ospf 1 area 0
ISP(config)#interface FastEthernet 0/0
ISP(config-if)#ipv6 ospf 1 area 0
ISP(config-if)#end
```

Kontrollieren Sie die Routing-Tabelle von Router Luzern. Er sollte nun Routen über OSPFv3 lernen!

```
luzern#show ipv6 route
IPv6 Routing Table - Default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D   2001:DB8:10::/64 [90/20514560]
     via FE80:100::1, Serial0/0/0
C   2001:DB8:20::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:DB8:20::1/128 [0/0]
     via FastEthernet0/0, receive
C   2001:DB8:100::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:100::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:101::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:101::1/128 [0/0]
     via Serial0/0/1, receive
O   2001:DB8:CAFE::/64 [110/65]
     via FE80:101::2, Serial0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

Kontrollieren Sie den Router ISP. Hat dieser Router ebenfalls eine Route gelernt?

Kontrollieren Sie den Router Bern. Kennt der Router Bern das Netzwerk 2001:DB8:CAFE::/64?

Bis jetzt kennt nur der Router Luzern alle Routen (von OSPFv3 und EIGRPv6). Router Bern hat keine Ahnung, wo das Netzwerk 2001:DB8:CAFE::/64 zu finden ist. Auch der Router ISP kennt keine Netzwerke von Bern.

4.5 OSPFv3 in EIGRPv6

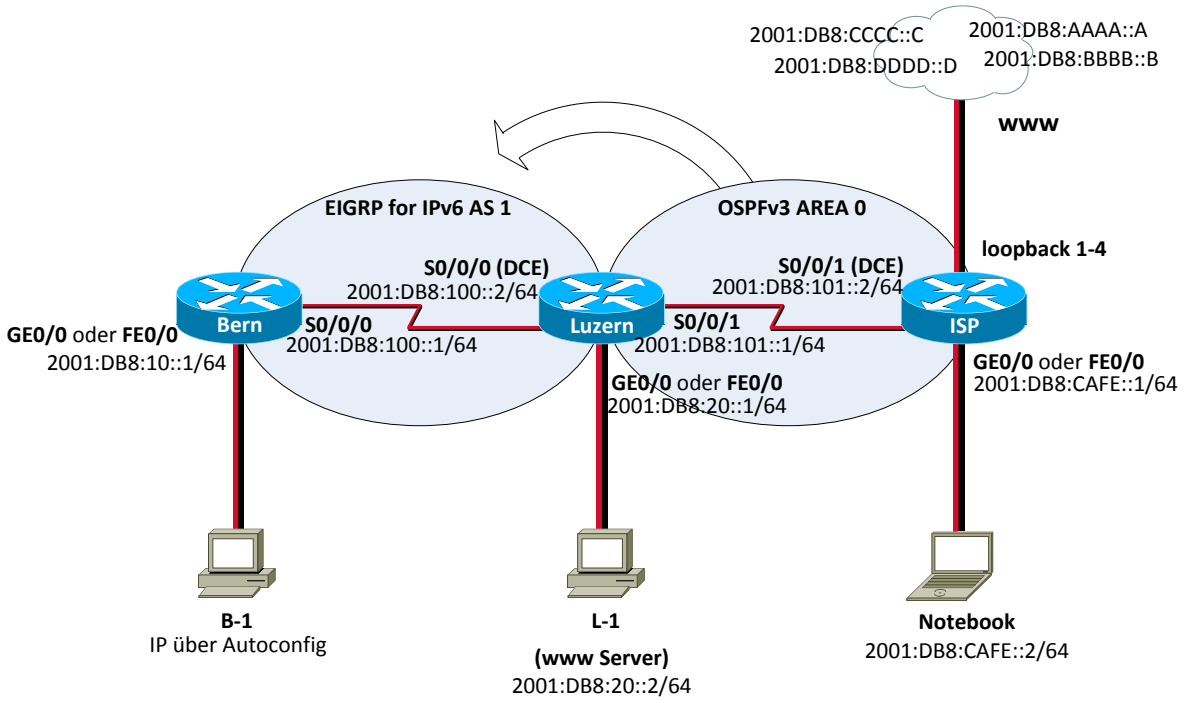

Abb. 6: OSPFv3 → EIGRPv6

Konfigurieren Sie auf Router Luzern die Weiterleitung der über OSPFv3 gelernten Routen in EIGRPv6. Das Stichwort hierbei ist ***redistribute***.

Wechseln Sie in den globalen Routing-Prozess von EIGRPv6 AS 1.

```
luzern#configure terminal
Luzern(config)#ipv6 router eigrp 1
```

Dem EIGRP-Prozess teilen wir nun mit, dass die über OSPFv3 gelernten Routen ebenfalls über EIGRPv6 propagiert werden sollten.

```
luzern(config-rtr)#redistribute ospf 1 metric ?
  <1-4294967295>  Bandwidth metric in Kbits per second

luzern(config-rtr)#redistribute ospf 1 metric 128 ?
  <0-4294967295>  EIGRP delay metric, in 10 microsecond units

luzern(config-rtr)#redistribute ospf 1 metric 128 50 ?
  <0-255>  EIGRP reliability metric where 255 is 100% reliable

luzern(config-rtr)#redistribute ospf 1 metric 128 50 255 ?
<1-255>  EIGRP Effective bandwidth metric (Loading) where 255 is 100% loaded

luzern(config-rtr)#redistribute ospf 1 metric 128 50 255 10 ?
  <1-65535>  EIGRP MTU of the path
```

```
luzern(config-rtr)#redistribute ospf 1 metric 128 50 255 10 1500
luzern(config-rtr)#redistribute connected
luzern(config-rtr)#end
```

Die Werte für Bandbreite, Delay, Verfügbarkeit, Load und MTU werden zur Berechnung der EIGRP-Routingmetrik verwendet.

Kontrollieren Sie Router Bern. Kennt er jetzt das Netzwerk 2001:DB8:CAFE::/64?

```
bern#show ipv6 route
IPv6 Routing Table - Default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:DB8:10::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:DB8:10::1/128 [0/0]
     via FastEthernet0/0, receive
D   2001:DB8:20::/64 [90/20514560]
     via FE80:100::2, Serial0/0/0
C   2001:DB8:100::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:100::1/128 [0/0]
     via Serial0/0/0, receive
EX  2001:DB8:101::/64 [170/21024000]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:CAFE::/64 [170/20524800]
     via FE80:100::2, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

4.6 EIGRPv6 in OSPFv3

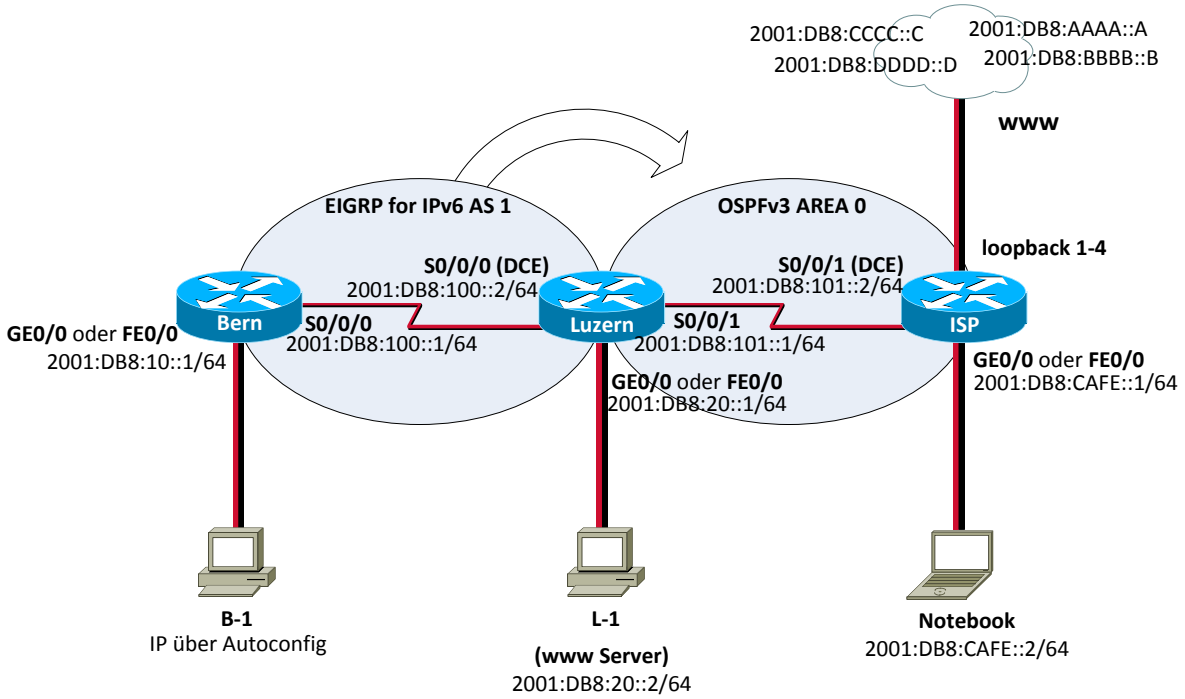

Abb. 7: EIGRPv6 → OSPFv3

Konfigurieren Sie auf Router Luzern die Weiterleitung der über EIGRPv6 gelernten Routen in OSPFv3. Das Stichwort ist wieder ***redistribute***.

Wechseln Sie in den globalen Routing-Prozess von OSPFv3 mit der Prozess-ID 1.

```
luzern#configure terminal
luzern(config)#ipv6 router ospf 1
```

Dem OSPF-Prozess teilen wir nun mit, dass die über EIGRPv6 gelernten Routen ebenfalls über OSPFv3 propagiert werde sollten.

```
luzern(config-rtr)#redistribute eigrp 1 metric ?
  <0-16777214>  OSPF default metric

luzern(config-rtr)#redistribute eigrp 1 metric 1000
```

Kontrollieren Sie die Routingtabelle des Routers ISP. Kennt Router ISP nun alle Netzwerke von Bern und Luzern?

```
ISP#show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2001:DB8:10::/64 [110/1000]
     via FE80:101::1, Serial0/0/1
C   2001:DB8:101::/64 [0/0]
     via Serial0/0/1, directly connected
```

```
...✂...
LC  2001:DB8:CCCC::C/128 [0/0]
     via Loopback3, receive
LC  2001:DB8:DDDD::D/128 [0/0]
     via Loopback4, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Auch hier fehlen die direkt an Router Luzern angeschlossenen Subnetze.

```
luzern#configure terminal
luzern(config)#ipv6 router ospf 1
luzern(config-rtr)#redistribute connected
```

```
ISP#show ipv6 route
IPv6 Routing Table - Default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2001:DB8:10::/64 [110/1000]
     via FE80:101::1, Serial0/0/1
OE2 2001:DB8:20::/64 [110/20]
     via FE80:101::1, Serial0/0/1
OE2 2001:DB8:100::/64 [110/20]
     via FE80:101::1, Serial0/0/1
C   2001:DB8:101::/64 [0/0]
     via Serial0/0/1, directly connected
...✂...
LC  2001:DB8:DDDD::D/128 [0/0]
     via Loopback4, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

4.7 Loopback in OSPFv3

Fügen Sie die Loopbacks von Router ISP ebenfalls in den OSPFv3-Routingprozess ein.

Wechseln Sie in den OSPFv3 Routing-Prozess mit der Prozess-ID 1 von Router ISP.

```
ISP#configure terminal
ISP(config)#ipv6 router ospf 1
```

Folgende Zeile bewirkt, dass alle verbundenen Interfaces in OSPFv3 propagiert werden.

```
ISP(config-rtr)#redistribute connected
ISP(config-rtr)#end
```

Sie könnten auch die Loopbacks auf dem jeweiligen Interface mit **ipv6 ospf 1 area 0** verbreiten lassen.

Kontrollieren Sie die Routingtabelle von Router Bern.

```
bern#show ipv6 route
IPv6 Routing Table - Default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:DB8:10::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:DB8:10::1/128 [0/0]
     via FastEthernet0/0, receive
D   2001:DB8:20::/64 [90/2172416]
     via FE80:100::2, Serial0/0/0
C   2001:DB8:100::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:100::1/128 [0/0]
     via Serial0/0/0, receive
EX  2001:DB8:101::/64 [170/2681856]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:AAAA::A/128 [170/20524800]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:BBBB::B/128 [170/20524800]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:CAFE::/64 [170/20524800]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:CCCC::C/128 [170/20524800]
     via FE80:100::2, Serial0/0/0
EX  2001:DB8:DDDD::D/128 [170/20524800]
     via FE80:100::2, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Überprüfen Sie die Erreichbarkeit von 2001:DB8:AAAA::A. Pingen Sie dazu diese IP-Adresse von allen PCs aus an.

Bitte löschen Sie am Ende dieses Versuches alle startup-configs mittels **erase startup-config** !

4.8 Kontrollfrage

- Wie kann man die Routing-Informationen von EIGRPv6 zu OSPFv3 weiterleiten? Erläutern Sie.

5 Hot Standby Routing Protokoll (HSRP) (optional) (30 min)

5.1.1 Zurücksetzen Testumgebung

Löschen Sie auf allen Routern die Konfiguration und starten Sie die Router neu.

```
Router#erase startup-configuration
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm] [Enter]
[OK]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm] [Enter]
```

Entfernen Sie die komplette Verkabelung.

5.2 Vorbereitung

Verkabeln Sie die Router und PCs gemäss Schema. Verwenden Sie **gerade Ethernetkabel**. Installieren Sie mittels USB-Datenträger die Konfigurationsdateien auf den Routern. Überprüfen Sie die mittels Konfigurationsdatei übernommenen Konfigurationen. Nach den Vorbereitungen sieht Ihr Netzwerk wie folgt aus:

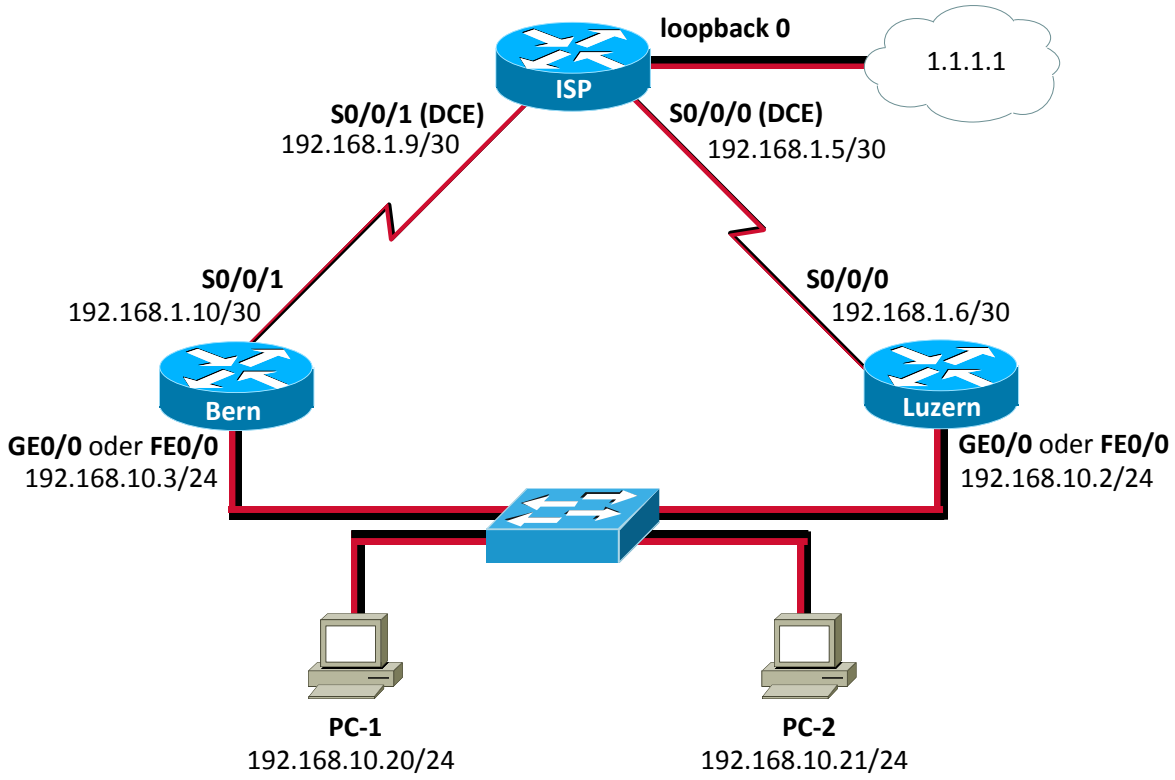

Abb. 8: Versuchsaufbau Teil 3

Konfigurieren Sie die PCs gemäss Schema. Setzen Sie ebenfalls das Defaultgateway (1x 192.168.10.2, 1x 192.168.10.3)

ACHTUNG: In diesem Szenario wird ein total neues Netzwerk aufgebaut! Ausser Hostname und Passwörter ändert sich alles.

5.3 Vorbereitung

Installieren Sie mittels USB-Datenträger die Konfigurationsdateien auf den Routern. Überprüfen Sie die mittels Konfigurationsdatei übernommenen Konfigurationen.

4. BERN_INIT_K6.txt
5. LUZERN_INIT_K6.txt
6. ISP_INIT_K6.txt

Falls Sie gut in der Zeit liegen, ist es empfehlenswert, die Befehle von Hand einzugeben, anstatt sie einfach zu kopieren.

5.3.1 Kontrolle

Pingen Sie von den PCs die IP 1.1.1.1 an. Dies sollte problemlos funktionieren.

5.4 HSRP

5.4.1 Theorie

Router Luzern sollte bei der Wahl als Standardgateway bevorzugt werden, da dieser Router eine schnellere Verbindung hat. Jedoch ist der Router nicht mehr der Jüngste und zudem gibt es ab und zu Probleme mit der seriellen Leitung zum ISP.

Ihre Aufgabe ist es nun, eine Redundanz im Netzwerk herzustellen, so dass die Verbindung zum ISP immer gewährleistet ist. Die Lösung bietet Ihnen das Hot Standby Routing Protocol (HSRP). Zwei damit konfigurierte Router überwachen den jeweils anderen und übernehmen dessen Funktion bei einem Ausfall.

Abstrakt gesehen existiert nach dem Konfigurieren nur ein "virtueller" Router, welcher physikalisch aus zwei oder mehreren besteht. In dieser abstrakten Sichtweise sieht das Netzwerk wie folgt aus:

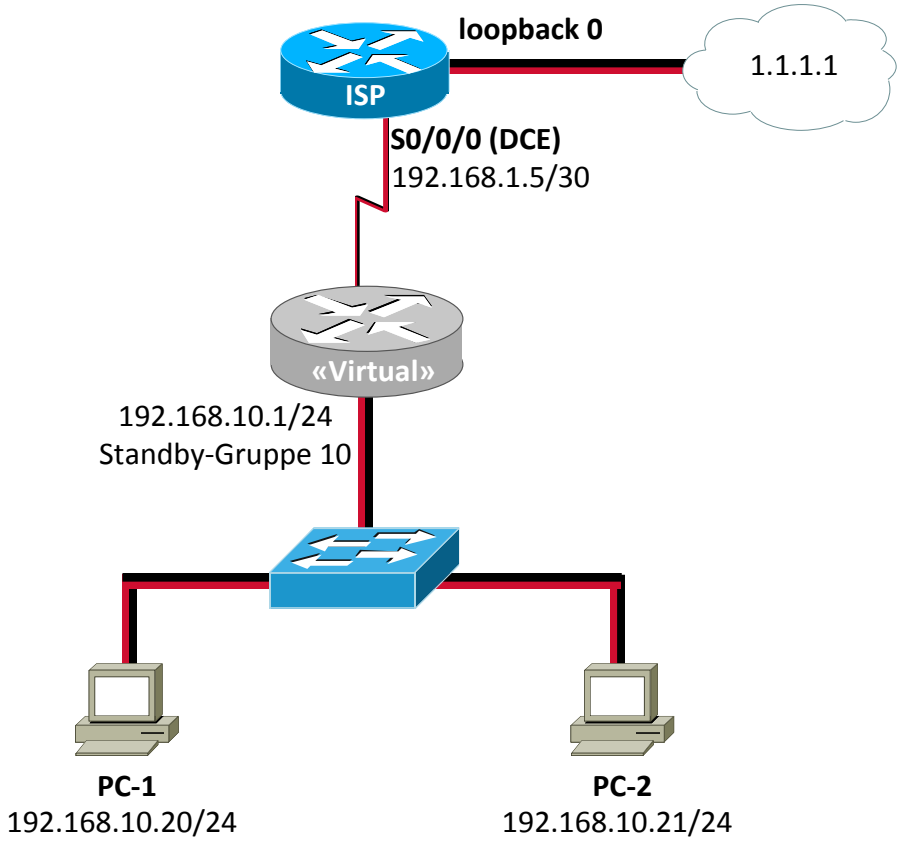

Abb. 9: Virtueller Router

Physikalisch gesehen sind es immer noch zwei Router.

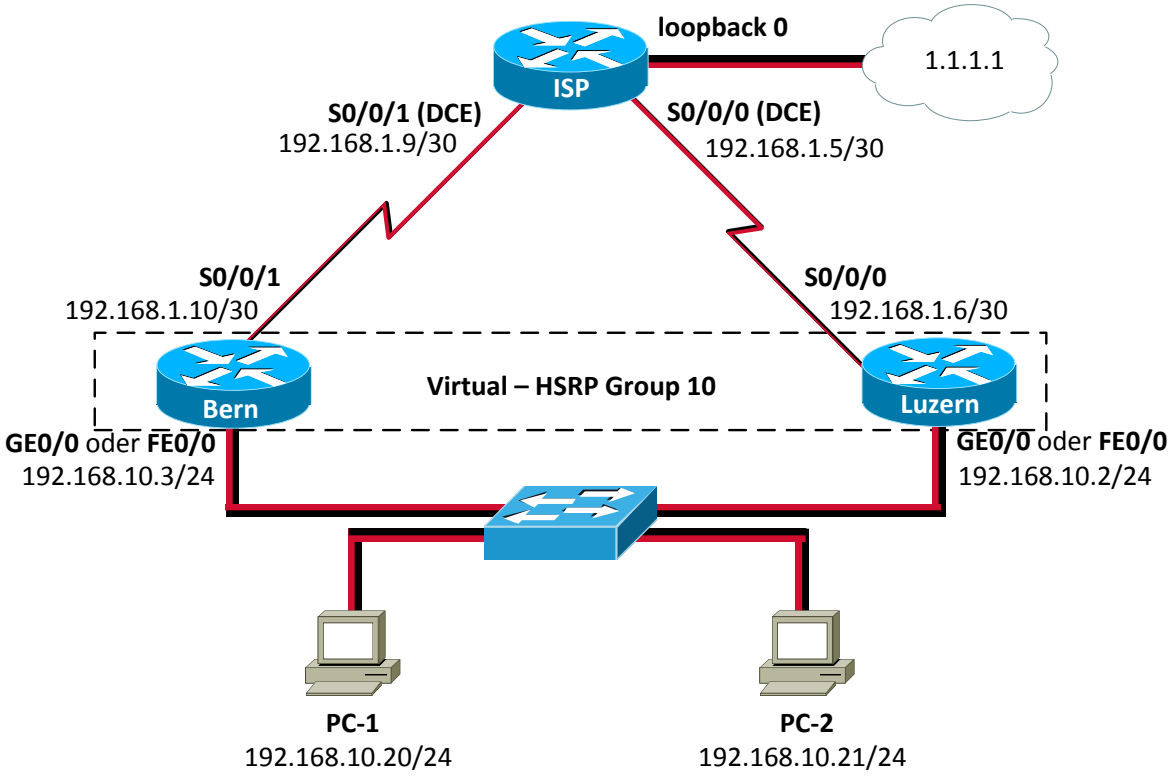

Abb. 10: Physikalische Router

5.4.2 Router Luzern

Konfigurieren Sie Router Luzern für HSRP.

Wechseln Sie in den spezifischen Konfigurationsmode der Fast-Ethernet Schnittstelle.

```
luzern#configure terminal
luzern(config)#interface fastEthernet 0/0
```

Unterbinden Sie dem Router die Möglichkeit, Redirects zu versenden.

```
luzern(config-if)#no ip redirects
```

Fügen Sie das Interface in die HSRP-Gruppe 10. Die virtuelle IP ist dabei 192.168.10.1.

```
luzern(config-if)#standby 10 ip 192.168.10.1
```

Mit ***preempt*** bekommt der Router das Recht, sich als Standard auszugeben und dies den anderen Routern zu entziehen.

```
luzern(config-if)#standby 10 preempt
```

Damit immer Router Luzern bevorzugt wird, wird die Priorität von den standardmässigen 100 auf 110 erhöht.

```
luzern(config-if)#standby 10 priority 110
```

Bei einem Unterbruch der seriellen Verbindung sollte nicht der Router Luzern aktiv sein, sondern der Router Bern sollte aktiv werden. Konfigurieren Sie, dass bei Unterbruch der seriellen Verbindung die Priorität um 20 reduziert wird und so unter die von Router Bern fällt.

Dazu definieren Sie auf dem Interface der HSRP-Gruppe 10 eine Track-Nummer (Bsp. 55). Ändert das getrackte Objekt (wird mit dem nächsten Befehl bestimmt) seinen Status, wird die HSRP-Priorität um den definierten Wert (Bsp. 20) vermindert.

```
luzern(config-if)#standby 10 track 55 decrement 20
luzern(config-if)#end
```

Erstellen Sie nun im globalen Konfigurationsmode das Track-Objekt und beachten Sie, dass die Track-Nummer mit der zuvor angegebenen korrespondiert (Bsp. 55). Bestimmen Sie das zu trackende Objekt und den zu überwachenden Status, in unserem Beispiel der Line-Protokoll Status des Interface Serial 0/0/0.

```
luzern(config)#track 55 interface Serial0/0/0 line-protocol
luzern(config-if)#end
```

Wechselt der Line-Protokoll Status des Interface Serial0/0/0 nun von Up zu Down, wird die HSRP-Priorität von Router Luzern um 20 vermindert.

5.4.3 Router Bern

Konfigurieren Sie Router Bern für HSRP analog Router Luzern.

- Redirects: no
- HSRP-Gruppe: 10

- Virtuelle IP: 192.168.10.1
- Preemptiv
- Priorität: 100

5.4.4 Konfiguration PCs

Ändern Sie auf den PCs das Standardgateway auf die IP-Adresse **192.168.10.1** (virtueller Router).

5.4.5 Kontrolle

Kontrollieren Sie auf den Routern die korrekte Konfiguration von HSRP mit dem Befehl ***show standby***. Vergleichen Sie die beiden Konfigurationen auf Unterschiede.

Router Luzern:

```
luzern#show standby
FastEthernet0/0 - Group 10
  State is Active
    9 state changes, last state change 00:00:40
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.572 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.3, priority 100 (expires in 9 sec)
  Priority 110 (configured 110)
    Track object 55 state Up decrement 20
  IP redundancy name is "hsrp-Fa0/0-10" (default)
luzern#
```

Router Bern:

```
bern#show standby
FastEthernet0/0 - Group 10
  State is Standby
    28 state changes, last state change 00:01:02
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.580 secs
  Preemption enabled
  Active router is 192.168.10.2, priority 110 (expires in 9 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0-10" (default)
bern#
```

5.5 Testen von HSRP

Speichern Sie die Konfiguration, bevor sie einen Router ausschalten!

Testen Sie das konfigurierte HSRP.

Trennen Sie temporär die serielle Verbindung zwischen Luzern und ISP.

Entfernen Sie temporär das LAN-Kabel von Router Luzern.

Pingen Sie von PC1 immer die IP 1.1.1.1 an (***ping –t 1.1.1.1***).

Führen Sie Traceroute (***tracert 1.1.1.1***) aus, um den Weg zu verfolgen.

Kontrollieren Sie auf dem Router Luzern und Bern, welcher Router aktiv ist. Verwenden Sie hierzu den Befehl ***show standby brief***.

Kontrollieren Sie den ARP-Cache der PCs (***arp –a***)

Bitte löschen Sie am Ende dieses Versuches alle startup-configs mittels **erase startup-config** !

5.6 Kontrollfragen

- Erläutern Sie kurz wie HSRP funktioniert.
- Wieso wurden zwei verschiedene Clock-Rate Werte bei ISP angegeben?

6 Bemerkung Load Balancing

Bei der Verwendung von RIP oder RIP V2 mit auto-summary (default bei Cisco) werden die Netze beim Erstellen der Routing-Routen als class-full behandelt. Dabei werden Netze unter Umständen zusammengefasst (siehe Abb. 11) und für den Router bei gleicher Metrik als gleichwertiger Pfad betrachtet. Das sollte erwartungsgemäss zu Load-Balancing führen. Den genauen Versuchsaufbau entnehmen sie der folgenden Grafik. Erwartet wird dabei, dass vom Notebook aus PC-2 oder PC-3 nicht vollständig mittels ***ping*** angepingt werden kann. Es ist eine Verteilung von 2:3 oder 3:2 zu erwarten. Das bedeutet, dass entweder 60% oder nur 40% der Pakete ankommen. Dies aufgrund der Verteilung der 5 Ping-Pakete (default). Es wird dabei jeweils abwechslungsweise ein Paket auf die eine Route geschickt, das nächste auf die andere (Packet Load-Balancing).

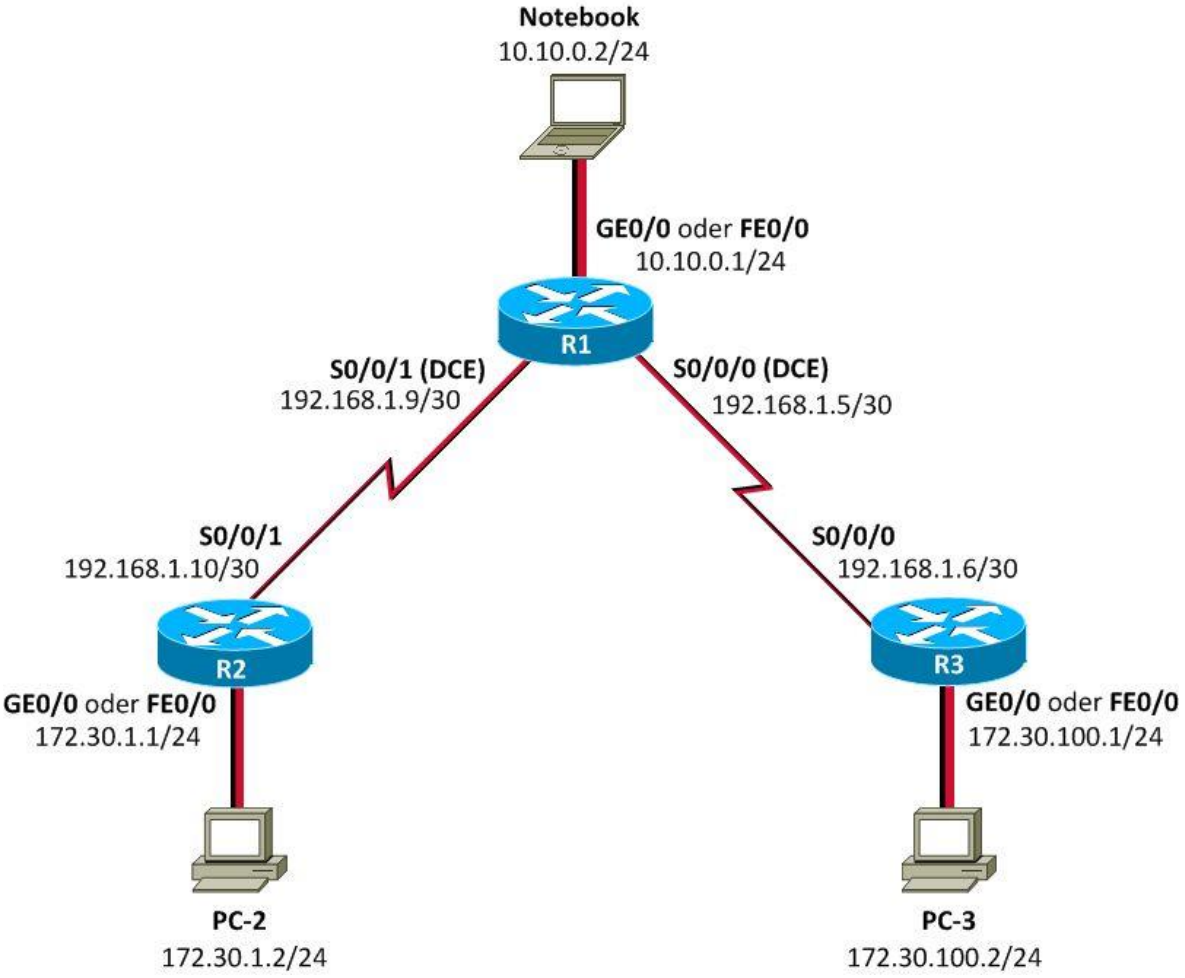

Abb. 11: Beispiel Load Balancing

Resultate

Im Labor konnte dieses erwartete Load-Balancing-Verhalten jedoch nicht festgestellt werden da CEF und FastSwitching defaultmässig aktiv sind und das zu per-destination-Load-Balancing führt.

Mit ***no ip cef*** kann dieses Verhalten abgeschaltet werden.

Für mehr Infos: https://learningnetwork.cisco.com/thread/12668

Packet Tracer

Parallel zu den Versuchen im Labor wurde der Versuchsaufbau auch in Packet Tracer von Cisco implementiert. Das erwartete Load-Balancing-Verhalten konnte simuliert werden. Allerdings gilt es zu beachten, dass dies keine grosse Bedeutung hat, da Paket Tracer nur eine Simulation des echten Verhaltens darstellt, CEF und Fast-Switching wurden dabei nicht implementiert. Die reale Welt bringt unterschiedliche IOS-Versionen und routerspezifische Einstellungen mit sich, die in Paket Tracer nicht berücksichtigt werden.

7 Anhang A - Vertiefung Access Control List ACL / Extended Access Lists ACE

Eine ACL/ACE konnte früher die Funktionalität einer Firewall teilweise übernehmen. Heutigen Standards kann der Zugriffsschutz mittels ACL nicht mehr entsprechen (z.B. Intrusion-detection). Daher werden ACL's heutzutage nur noch intern im Netzwerk zur Zugriffskontrolle des Datenverkehrs bei den Interfaces verwendet.

Die ACL/ACE besteht aus Anweisungen Pakete anzunehmen oder abzulehnen und wird beim betreffenden Interface und Protokoll eingerichtet. Eine solche ACL/ACE wirkt dabei nur in eine Richtung (entweder inbound oder outbound). Es kann nur eine ACL/ACE pro Interface und Protokoll und Richtung eingetragen werden. Standard-ACL's filtern nur nach der Source-IP. Erweiterte ACL's=ACE ermöglichen die Filterung nach Source-IP, Destination-IP, nach Protokoll (TCP / UDP), Port-Nummern oder weiteren Parametern.

Eine Standard-ACL wird wie folgt eingegeben (vorerfasst ohne Wirkung, muss später dann noch zugewiesen werden, um eine Wirkung zu erzielen):

*Router(config)#**access-list** access-list-number {**permit** | **deny**} {test-conditions}*

Test-conditions kann entweder durch eine IP-Adressen (mit wild-card-maske) oder durch das Schlüsselwort „any" (für alle IP-Adressen) ausgedrückt werden.

Die *access-list-number* 1-99 ist für die Standard-ACL (nur Source-IP Filtering) reserviert. Höhere Nummern können für erweiterte ACL's verwendet werden.

- IP (Standard-IP) 1-99
- IP (Extended-IP) 100-199
- AppleTalk 600-699
- IPX 800-899
- Extended IPX 900-999
- IPX Service Adv. Prot. 1000-1099

Ab Cisco IOS 11.2 können auch eigene Namen anstelle der Nummern verwendet werden (z.B.):

NO_NAT oder *VPN* oder *EDUCATION_GROUP*

Die Erfassung einer Extended Access List ACE sieht wie folgt aus:

*Router(config)#**access-list** access-list-name [line line_number] [extended] {**permit | deny**} protocol source_address mask [operator port] dest_address mask [operator port | ICMP_type] [inactive]*

ACL mittels Namen zu verwalten ermöglicht zudem, ohne vorgängiges Löschen neue Einträge am Ende der ACL einzufügen oder bestehende zu entfernen. Weitere Bearbeitung ist jedoch ohne Neuerstellung nicht möglich. Beachten sie die Wichtigkeit der Reihenfolge. Das vorgängige Erstellen/Ändern einer ACL in einem externen Editor wird empfohlen.

Danach folgt die notwendige Zuweisung zu einem Interface und zu einem vorgesehenen Protokoll (ab hier nun mit Wirkung auf den Betrieb) unter Angabe der Richtung:

*Router(config-if)#{protocol} **access-group** access-list-number {In | Out}*

Ein und dieselbe *access-list-number* kann mehreren Interfaces zugewiesen werden. Eine Zuweisung kann mittels vorangesetztem no wieder entfernt werden. *Protocol* kann dabei bspw. IP, TCP, UDP, ICMP oder andere sein.

Zu beachten:

1. Falls man alte Regeln durch neue ersetzen möchte, sollte man zuerst die neuen Regeln hinzufügen und erst danach die alten entfernen. Ginge man umgekehrt vor, bestünde für den Zeitraum bis zum Hinzufügen der neuen Regeln eine Sicherheitslücke!

2. Die ACL-Listen werden linear von oben nach unten abgearbeitet. Beim ersten Zutreffen einer Regel wird diese verwendet und alle folgenden Regeln werden ignoriert. Soll z.B. zur generellen Erlaubnis ein spezielles Verbot eingerichtet werden, muss dies also vor der Erlaubnis stehen, da sonst die Erlaubnis das Verbot wirkungslos macht. Der Reihenfolge kommt also eine bedeutende Rolle zu!

3. Wenn ein Paket durch eine ACL geblockt wird, dann wird eine ICMP „Destination unreachable“-Nachricht ausgelöst (mit „administratively prohibited“ als Vermerk).

4. Am Ende einer ACL-Liste steht ein implizites „implied deny“ (deny IP any), das alle Pakete blockiert. Es muss also mindestens eine Erlaubnis mittels „permit“ eingetragen sein.

5. Die wildcard-mask gibt lediglich an, wie viele Stellen für die Betrachtung relevant sind (Nullen sind relevant, Einsen nicht). Mittels wildcard-masks (z.B. 0.0.255.255) kann mitgeteilt werden, wie viel einer IP-Adresse bei den „test-conditions“ übereinstimmen muss. Wildcard-masks sollen nicht mit subnet-mask verwechselt werden – sie sind nur strukturell gleich aufgebaut.

Mittels

*Router#**show ip interface***

Oder

*Router#**show access list***

Oder

*Router#**show access-lists***

kann die Erfassung der ACL/ACE kontrolliert werden.

8 Anhang B – DHCP

[Quelle: http://www.elektronik-kompendium.de/sites/net/0812221.htm]

DHCP ist ein Protokoll, um IP-Adressen in einem TCP/IP-Netzwerk zu verwalten und an die Stationen zu verteilen. Mit DHCP ist jede Netzwerk-Station in der Lage sich selber vollautomatisch zu konfigurieren.

Warum DHCP?

Um ein Netzwerk per TCP/IP aufzubauen ist es notwendig jede einzelne Station zu konfigurieren. Für ein TCP/IP-Netzwerk müssen folgende Einstellungen bei jeder Station vorgenommen werden:

- Vergabe einer eindeutigen IP-Adresse
- Zuweisen einer Subnetzmaske (Subnetmask)
- Zuweisen des Default- bzw. Standard-Gateways
- DNS-Serveradressen

In den ersten IP-Netzen wurden IP-Adressen noch von Hand vergeben und fest in die Systeme eingetragen. Die dazu erforderliche Dokumentation war jedoch nicht immer fehlerfrei und schon gar nicht aktuell und vollständig. Der Ruf nach einer einfachen und automatischen Adressverwaltung wurde deshalb besonders bei Betreibern großer Netze lauter. Hier war sehr viel Planungs- und Arbeitszeit notwendig. Um dem zu entgehen, wurde DHCP entwickelt. Mit DHCP kann jede Netzwerk-Station die Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

DHCPv6

Bei IPv6 gibt es die Stateless Autoconfiguration. Doch diese berücksichtigt keine Informationen über Host-, Domainnamen und DNS. Diese Angaben und noch mehr können durch den Einsatz eines DHCPv6-Servers ergänzt werden. Dieser liefert die gewünschten Zusatzinformationen, kümmert sich dabei aber nicht um die Adressvergabe. Man spricht von Stateless DHCPv6.

Funktionsweise von DHCP

DHCP ist eine Client-Server-Architektur. Der DHCP-Server verfügt über einen Pool von IP-Adressen, die er den DHCP-Clients zuteilen kann. Bei größeren Netzen muss der DHCP-Server zudem wissen, welche Subnetze und Standard-Gateway es gibt. In der Regel ist der DHCP-Server ein Router.

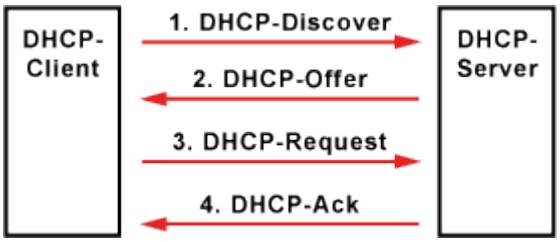

Abb. 12: Funktionsweise des DHCPs

Wird eine Station gestartet und ist dort ein DHCP-Client aktiviert, wird ein in seiner Funktion eingeschränkter Modus des TCP/IP-Stacks gefahren. Dieser hat keine gültige IP-Adresse, keine Subnetzmaske und kein Standard-Gateway. Das einzige, was der Client machen kann, ist IP-Broadcasts verschicken. Der DHCP-Client verschickt ein UDP-Paket mit der Ziel-Adresse 255.255.255.255 und der Quell-Adresse 0.0.0.0. Dieser Broadcast dient als Adressanforderung an alle verfügbaren DHCP-Server. Im Optimalfall gibt es nur einen DHCP-Server. So vermeidet man Konflikte bei der Adressvergabe. Der DHCP-Server antwortet auf den Broadcast mit einer freien IP-Adresse und weiteren Parametern. Danach wird die Datenübergabe bestätigt.

Mit DHCP werden nicht nur die IP-Adressen verteilt. Bei der Gelegenheit werden weitere Parameter übergeben, um die IP-Konfiguration im Client zu vervollständigen. Jeder angesprochene DHCP-Server schickt ein UDP-Paket mit folgenden Daten zurück:

- MAC-Adresse des Clients
- mögliche IP-Adresse
- Laufzeit der IP-Adresse
- Subnetzmaske
- IP-Adresse des DHCP-Servers / Server-ID

Aus der Auswahl von evt. mehreren DHCP-Servern sucht sich der DHCP-Client eine IP-Adresse heraus. Daraufhin verschickt er eine positive Meldung an den betreffenden DHCP-Server. Alle anderen Server erhalten die Meldung ebenso und gehen von der Annahme der IP-Adresse zugunsten eines anderen Servers aus. Anschließend muss die Vergabe der IP-Adresse vom DHCP-Server bestätigt werden. Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal ab. Abschließend wird der TCP/IP-Stack vollständig gestartet. Doch nicht nur die Daten zum TCP/IP-Netzwerk kann DHCP an den Client vergeben. Sofern der DHCP-Client weitere Angaben auswerten kann, übermittelt der DHCP-Server weitere Optionen:

- Time Server
- Name Server
- Domain Name Server (Alternative)
- WINS-Server
- Domain Name
- Default IP TTL
- Broadcast Address
- SMTP Server
- POP3 Server

9 Anhang C – EIGRP

[Quelle: Wikipedia]

Das Enhanced Interior Gateway Routing Protocol (EIGRP) ist ein 1992 von Cisco veröffentlichtes proprietäres Routing-Protokoll. Bei EIGRP handelt es sich um eine verbesserte Version des früheren IGRP, zu welchem weiterhin Kompatibilität besteht.

EIGRP ist ein erweitertes Distance-Vector-Routingprotokoll, welches sich beim Austausch mit benachbarten Geräten sowie bei der Speicherung von Routing-Informationen wie ein Link-State-Routingprotokoll verhält. Aufgrund der umfangreichen Merkmale, welche eher bei Link-State-Protokollen anzutreffen sind wird EIGRP daher oft auch als Balanced-Hybrid-Routingprotokoll klassifiziert. Mit Hilfe jener Link-State-Eigenschaften erreicht EIGRP im Verhältnis zu konventionellen Distance-Vector-Routingprotokollen eine sehr schnelle Konvergenz und ist immun gegenüber Routing-Schleifen. Die schnelle Konvergenz und vor allem Zuverlässigkeit in Umgebungen mit dynamisch durch NHRP quervernetzten GRE-Tunneln lassen EIGRP als interessante Alternative zu OSPF erscheinen.

Funktion

Bei EIGRP werden benachbarte Router in einer Neighbour Table (Nachbarschaftstabelle) gespeichert. Sämtliche Routen, welche über diese Nachbarn bekanntgegeben werden, werden wiederum in einer Topology Table (Topologietabelle) gesammelt. Die beste Route zu einem Zielnetzwerk wird bei EIGRP mit dem Diffusing Update Algorithm (DUAL) ermittelt.

Die Berechnung der Metrik für unterschiedliche Routen basiert bei EIGRP auf dem gleichen Verfahren wie bei IGRP, aufgrund des längeren Feldes für die Speicherung der Metrik skaliert EIGRP jedoch, gegenüber IGRP, den Wert um den Faktor 256. Bei der manuellen Konvertierung von Werten zwischen EIGRP- und IGRP-Routern muss dies berücksichtigt werden, in der Praxis erfolgt die Umrechnung automatisch.

Multiprotokolleigenschaften

Primär unterstützt EIGRP das Internet Protocol (IP), IPX und Appletalk als zu routende Protokolle der 3. Schicht des OSI-Referenzmodells. Aufgrund seines modularen Aufbaus ist es jedoch mit Hilfe von sogenannten Protocol-dependent modules (PDM) möglich, neuere Protokolle wie etwa IPv6 einzusetzen ohne EIGRP selbst aktualisieren zu müssen.

Ein Router, der mit EIGRP arbeitet, verwaltet für jedes Protokoll der OSI-Schicht 3 eine separate Routingtabelle, eine Nachbarschaftstabelle und eine Topologie-Tabelle.

Allerdings werden die Multiprotokolleigenschaften von EIGRP in den aktuellen Versionen von IOS nicht mehr voll unterstützt. Somit verbleiben nur IP und IPX als zu routende Protokolle.

Ausblick

Als Neuerung gegenüber IGRP werden auch die Verfahren Classless Inter-Domain Routing (CIDR) sowie Variable Length Subnet Mask (VLSM) unterstützt. Da diese Merkmale in modernen Netzen inzwischen Standard sind, spielt IGRP in der Praxis keine nennenswerte Rolle mehr.

10 Anhang D - Passwort Recovery Prozedur

Es kann vorkommen, dass die Router mit einem anderen Passwort als cisco versehen sind. Folgen Sie in diesem Fall der unten stehenden Anleitung.

Router

1. Verwenden Sie immer cisco als Passwort.
2. Bevor Sie mit der Recovery-Prozedur anfangen versuchen Sie folgende Passwörter zuerst:
   a. Cisco
   b. cisco (mit Leerschlag am Ende)
   c. class
   d. cisco12345
   e. user01 / user01pass
   f. admin01 / admin01pass
   g. admin / adminpa55
3. Falls keine der oben genannten Passwörter funktioniert, starten Sie mit der Password Recovery Prozedur.
4. Starten Sie den Router neu.
5. In den ersten 10 Sekunden des Boot-Vorganges senden Sie mit dem Terminal-Client einen Break (die Break Sequenz kann von Terminal zu Terminal unterschiedlich sein. (Mit TeraTerm ist sie Ctrl+B)
6. Der Router wird in das rommon: booten
7. Setzen Sie den Configuration Register auf 0x2142 und starten Sie den Router erneut:

```
rommon 1 > confreg 0x2142
rommon 2 > reset
```

8. Nach dem Bootvorgang löschen Sie den startup-config und setzen Sie den Configuration Register auf 0x2102 zurück:

```
Router# delete nvram:startup-config
Router# conf t
Router(config)# config-register 0x2102
Router(config)# end
Router# write
```

9. Starten Sie mit dem Versuch.