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 Basics

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

**Autoren:** C. Di Battista, Prof. Dr. B. Hämmerli, D. Krummenacher, N. Lardieri, F. Pfanner, Ph. Schnyder, A. Suhl, A. Vogt, E. Fux, C. Banzer
**Version:** 4.5
**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 | 19.09.05 | Erledigt | Erstellung Dokument | D. Krummenacher |
| Nr. 2.0 | 07.02.05 | Erledigt | Diverse Überarbeitungen | D. Krummenacher |
| Nr. 3.0 | 09.10.07 | Erledigt | Komplette Überarbeitung des Versuches | D. Jossen |
| Nr. 3.1 | 16.04.08 | Erledigt | Erklärung der CHAP „bi-/unidirektionae“ Authentifizierung hinzugefügt | N. Lardieri |
| Nr 3.2 | 28.10.08 | Erledigt | Korrektur der CHAP Authentisierung | N. Lardieri |
| Nr. 3.3 | 29.05.09 | | Neues Layout | N. Lardieri |
| Nr. 3.4 | 07.01.10 | Erledigt | Fehlerkorrektur | N. Lardieri |
| Nr. 3.5 | 10.05.12 | Erledigt | Überarbeitung | C.Di Battista, F. Pfanner |
| Nr. 4.0 | 23.09.12 | Erledigt | Überarbeitung | C. Di Battista, M.Schröder |
| Nr. 4.5 | 10.03.16 | Erledigt | Aktualisierung IOS, Algorithm-Type | C. Banzer, E. Fux |

# Inhaltsverzeichnis

## Abbildungsverzeichnis



## Abkürzungsverzeichnis

In diesem Dokument werden folgende Abkürzungen verwendet:

| Abkürzung | Beschreibung |
|---|---|
| DCE | Data Communication Equipment |
| DTE | Data Terminal Equipment |
| IP | Internet Protokoll |
| NVRAM | Non volatile RAM |
| OSPF | Open Shortest Path First |
| WWW | World Wide Web |

# Vorwort

Dieser Laborversuch vermittelt den Studierenden einen ersten Einblick mit dem Umgang von Routern und Routingprotokollen. Weiterführende Routing Konfigurationen werden im Versuch IP Routing Advanced 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 diese 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 die 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. Was versteht man unter Routing?
2. Was ist OSPF?
3. Welche Vorteile bringen die seriellen Verbindungen  im Labor?

## 1.2 Theorie

Frage 1: Lesen Sie Kapitel 5.2 auf Seite 388 vom Buch Computernetzwerke von A.S. Tanenbaum

Frage 2: Lesen Sie Kapitel 5.6.4 auf Seit 498 vom Buch Computernetzwerke von A.S. Tanenbaum

Frage 3: Lesen Sie Anhang A - Nutzen von serielle Verbindungen

## 1.3 Materialiste

Für die Durchführung dieses Laborversuches benötigen Sie folgendes Material:

- 3x Cisco Router
- 2x Workstations
- Diverse Anschlusskabel

# 2 Aufgabenstellung

Dieser Laborversuch beschäftigt sich mit der Grundkonfiguration von Routern. Im Verlaufe dieses Versuches werden Sie lernen, wie Router mit einer elementaren Grundkonfiguration ausgerüstet werden können. In einem weiteren Schritt werden Sie die Möglichkeit haben, unterschiedliche Routing Schnittstellen konfigurieren zu können. Im Versuchsaufbau müssen Sie FastEthernet Interfaces, serielle Interfaces und logische Loopback Interfaces konfigurieren und entsprechend administrieren.

Nach der richtigen Konfiguration der Interfaces, müssen Sie die Routing Funktionalität auf den einzelnen Routern aktivieren. In diesem Laborversuch werden wir nur statisches Routing und das Routingprotokoll OSPF einsetzen.

Als Versuchsszenario verwenden wir ein Netzwerk einer kleinen Firma, die drei Standorte über entsprechende WAN-Verbindungen miteinander verbunden hat. Zudem besitzt die Firma einen Internetanschluss, über den alle angeschlossenen Standorte direkt mit dem Internet kommunizieren können.

Bitte beachten Sie die Zeitangaben bei den Kapiteln. Falls Sie merken, dass der Rahmen die vorgegebene Zeit sprengt, überspringen Sie die speziellen Aufgaben, die mit einer Brille markiert sind.

Falls Sie schon Erfahrungen haben und die Versuche vorzeitig abarbeiten, können Sie sich mit dem Advanced Routing befassen.

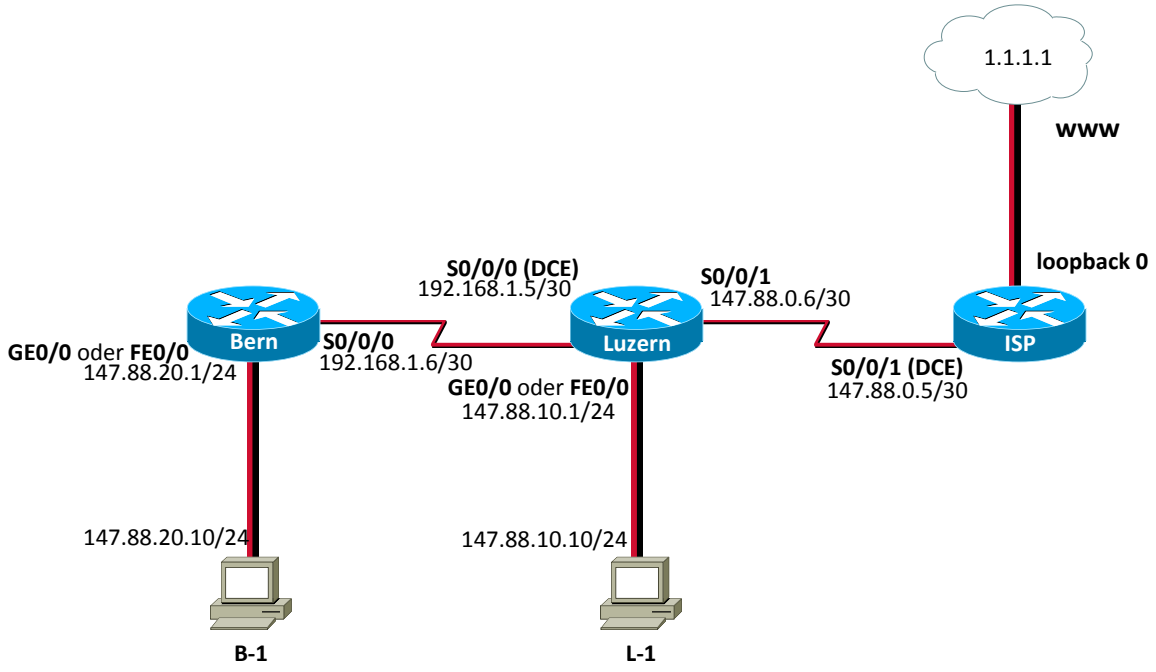



Abb. 1: Zielkonstellation des Basic Versuchs

# 3 Grundkonfiguration (20 min)

Dieses Kapitel beschreibt die Grundkonfiguration der Router. Sie werden Schritt für Schritt durch die Konfiguration geführt. In diesem Dokument sind alle Befehle komplett ausgeschrieben. Für die Konfiguration genügt es oft, wenn Sie nur die ersten Buchstaben des Befehls ausschreiben. Alternativ können Sie mit der Tabulatortaste das Kommando automatisch ergänzen.

## 3.1 Router Luzern

Verbinden Sie sich mit dem Konsolenkabel mit dem Router Luzern. Nach dem Sie den Router eingeschaltet haben, sehen Sie auf dem Konfigurationsterminal den untenstehenden Output. Sollt dies nicht der Fall sein, besitzt der Router noch eine gespeicherte Konfiguration. Löschen Sie bitte zu Beginn diese Konfiguration und starten das Gerät noch einmal neu auf. Falls es nach einem Passwort fragt und Sie mit ***cisco*** nicht hineinkommen gibt es im Anhang eine Einleitung für das Zurücksetzen.

```
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(9)T,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:47 by prod_rel_team
Image text-base: 0x6008FCB8, data-base: 0x62480000


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
```

```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Installed image archive
Cisco 1841 (revision 5.0) with 117760K/13312K bytes of memory.
Processor board ID FCZ094711ZR
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:no
```

Bestätigen Sie bitte den obigen Dialog mit no. Jetzt sollte die Kommandozeile erscheinen.

```
Router>
```

Sobald Sie Zugriff auf die Konsole des Routers haben, können wir mit der Grundkonfiguration beginnen. Cisco Router unterscheiden zwischen zwei Konfigurationsmodi. Wenn Sie sich das erste Mal anmelden, befinden Sie sich immer im user exec Modus. Dieser Modus besitzt eine eingeschränkte Zugriffsberechtigung auf die Kommandos des Routers. Damit wir auf dem Router einige Konfigurationen vornehmen können, müssen wir als Erstes in den privilege exec Modus wechseln. Geben Sie bitte dazu das untenstehende Kommando ein:

```
Router>enable
Router#
```

Bitte beachten Sie die unterschiedlichen Prompts. Nach der Eingabe das Kommandos sollte sich der Eingabeprompt in ein # ändern.

```
user-exec:         Router>
priviledged exec:  Router#
```

In priviledge exec Modus nimmt der Router keine Konfigurationskommandos entgegen. Damit wir den Router nun konfigurieren können, müssen wir als nächstes in den Konfigurationsmodus wechseln. Erst im Konfigurationsmodus können wir entsprechende Konfigurationen, wie das Setzen von IP-Adressen, das Konfigurieren von Routingprotokollen usw. vornehmen. Mit dem untenstehenden Befehl können Sie in den Konfigurationsmodus wechseln. Bitte beachten Sie auch wieder in diesem Fall, die Änderung des Eingabepromptes.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Als erstes konfigurieren wir nun den Hostnamen des Routers.

```
Router(config)#hostname luzern
luzern(config)#
```

Beachten Sie bitte, dass alle Konfigurationen, die Sie im Konfigurationsmodus durchführen, direkt wirksam werden! Damit Sie die Konfiguration aber dauerhaft auf einem Router abspeichern können, müssen Sie diese speziell abspeichern. Das werden wir aber später mit einander behandeln.

Im nächsten Schritt deaktivieren Sie die DNS-Auflösung des Routers. Dadurch verhindern Sie, dass der Router bei der Falscheingabe eines Befehles, die Eingabe als eine Hostadresse interpretiert und jedes Mal versucht, via DNS eine IP-Adresse für diesen Host aufzulösen.

```
luzern(config)#no ip domain-lookup
luzern(config)#
```

### 3.1.1 Zugriffschutz

Im nächsten Schritt schränken wir den Zugriff auf das Gerät ein. Auf den Cisco Routern können wir für jede Zugriffsart (Telnet / SSH / Konsole) unterschiedliche Passwörter definieren. Geben Sie dazu bitte die untenstehenden Befehle im Konfigurationsmodus ein.

#### *3.1.1.1 Zugriffschutz für Konsolenverbindungen*

```
luzern(config)#line console 0
luzern(config-line)#password cisco
luzern(config-line)#login
luzern(config-line)#logging synchronous
luzern(config-line)#exit
luzern(config)#
```

Das eingegebene Passwort wird erst durch den Login Befehl aktiviert.

Der Befehl logging synchronous aktiviert die synchrone Protokollierung um zu verhindern dass die Systemmeldungen bei einer Eingabe erscheinen.

Mit dem Befehl exit können Sie einen Konfigurationsmodus zurück springen.

#### *3.1.1.2 Zugriffschutz für Telnetverbindungen*

Router werden gerne über Telnetverbindungen konfiguriert. Mit Hilfe von Telnet können Sie sich Remote auf einen Gerät anmelden und Änderungen an der Konfiguration vornehmen. Damit Sie sich über Telnet auf einen Router verbinden können, müssen Sie zwingend ein Telnet Passwort konfigurieren. Sie können ein Telnet Passwort durch die Eingabe der untenstehenden Befehle konfigurieren.

```
luzern(config)#line vty 0 4
luzern(config-line)#password cisco
luzern(config-line)#login
luzern(config-line)#exit
luzern(config)#
```

Falls Sie die obigen Konfigurationskommandos nicht durchführen, können Sie sich nicht über Telnet mit dem Router verbinden.

#### *3.1.1.3 Zugriffsschutz für privilege exec Modus*

Im letzten Schritt konfigurieren wir nun ein Passwort für den privilege exec („enable“) Modus. Dieses Passwort wird bei jedem Wechsel in den privilege exec Modus abgefragt. Für die Konfiguration eines entsprechenden Passworts, geben Sie bitte die untenstehenden Befehle ein.

```
luzern(config)# enable algorithm-type scrypt secret cisco
luzern(config)#
```

Mit dem Befehl ***enable algorithm-type scrypt secret*** wird das Passwort mit einer starken Verschlüsselung (scrypt) abgespeichert. Sie könnten auch den alten Befehl ***enable passwort*** verwenden. Jedoch wird hierbei das Passwort unverschlüsselt in der Startup-Konfiguration abgespeichert. Wenn Sie nur ***enable secret*** verwenden, wird das Passwort als MD5-Hash in die Konfigurationsdatei gespeichert. Dieses Passwort kann sehr leicht mithilfe von Rainbow Tables herausgefunden werden.

### 3.1.2 Speichern der Konfiguration

Nun haben wir schon einige Konfigurationen am Router Luzern vorgenommen. Damit diese Konfigurationen bei einem allfälligen Stromausfall nicht verloren gehen, wird es Zeit, diese dauerhaft abzuspeichern.

Verlassen Sie nun den Konfigurationsmodus mit dem untenstehenden Befehl. Sie gelangen anschliessend in den privilege exec Modus.

```
luzern(config)#end
00:10:45: %SYS-5-CONFIG_I: Configured from console by console
luzern#
```

Mit dem untenstehenden Befehl können Sie Ihre vorgenommene Konfiguration dauerhaft auf dem Router abspeichern.

```
luzern#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
luzern#
```

Der Router kennt grundsätzlich zwei Konfigurationen:

Die running-configuration und die "startup-configuration". Beim Aufstarten des Routers wird die startup-config verwendet. Sie wird nach dem booten zur running-config, welche sich in einem flüchtigen Speicher (RAM) befindet. Wenn Änderungen an der Konfiguration gemacht werden, werden sie sofort aktiv, das heisst in die running-config übernommen.

Die startup-configuration wird die Konfiguration abgelegt, die der Router beim Neustart einliest und ausführt. Sie als Administrator müssen sämtliche Änderungen an der Konfiguration in die startup-configuration übernehmen. Nur so werden Ihre Einstellungen dauerhaft auf dem Router gespeichert und sind nach einem allfälligen Neustart des Routers wieder verfügbar. Die startup-config befindet sich in einem nichtflüchtigen Speicher (NVRAM: Non volatile RAM).

Damit wir sicher gehen können, dass die durchgeführten Konfigurationen tatsächlich auf dem Router gespeichert worden sind, können Sie sich auf dem Router abmelden und wieder neu anmelden. Führen Sie bitte dazu folgende Konfigurationsschritte gemäss der untenstehenden Anleitung durch:

Vom Router abmelden

```
luzern#exit
```

Neu Anmelden am Router

```
User Access Verification
Password:cisco
```

In den privilege exec Modus wechseln

```
luzern>enable
Password:cisco
luzern#
```

### 3.1.3 Verifizieren der Konfiguration

Wir haben jetzt diverse Dinge konfiguriert. Es ist an der Zeit die Konfiguration zu kontrollieren. Dies können sie über diverse show Kommandos im user exec oder privileged exec Modus durchführen. Alle heiklen Show-Kommandos können nur im privileged Modus aufgerufen werden, so auch diejenigen zum Betrachten der aktuellen Konfiguration.

Studieren Sie die Running-Config mit dem Befehl show running-config! Erkennen Sie die von Ihnen gemachten Konfigurationen? Was fällt Ihnen in Bezug auf Passwörter auf?

Studieren Sie auch die Startup-Config mittels des show startup-config Befehles!

Running-Config und Startup-Config sind identisch, da Sie seit dem letzten Sichern keine Änderungen an der Konfiguration gemacht haben. Ändern Sie etwas, so wird die Änderung gleich in die Running-Config übernommen und ist aktiv. Solange Sie dann die Running-Config nicht als Startup-Config speichern, verlieren Sie bei einem Neustart des Routers sämtliche Änderungen.

### 3.1.4 Externe Sicherung der Konfiguration

Die Konfiguration lässt sich nicht nur im NVRAM des Routers sichern, sondern auch sehr einfach und gut lesbar in einem Textfile. Dieses Textfile kann zur (Neu-) Konfiguration eines Routers gleichen Typs verwendet werden. Die Sicherung selbst ist denkbar einfach. Kopieren Sie die jeweilige Ausgabe des ***show running-config*** Befehles und fügen Sie diese in ein Textfile ein.

Führen Sie bitte eine Datensicherung des Routers Luzern durch.
***copy running-config startup-config***

Das Wiederherstellen ist wieder sehr einfach. Kopieren Sie einfach den Inhalt des Textfiles und fügen Sie ihn in den globalen Konfigurationsmodus wieder ein. Beachten Sie allfällige Fehlermeldungen.

## 3.2 Router Bern

Erstellen Sie nun für den Router Bern die Grundkonfiguration analog dem Router Luzern. Konfigurieren Sie bitte folgende Tasks:

- Hostname
- Deaktivieren Sie die DNS-Auflösung
- Konfigurieren Sie die Passwörter für den Konsolen- und Telnetzugriff
- Konfigurieren Sie das Passwort für den priviledge exec Modus
- Sichern Sie Ihre Konfiguration ab

## 3.3 Kontrollfragen

- Wie kann die Konfiguration gesichert werden?
- Im welchen Modus ist es möglich die *running-config* mit dem Kommando *show* einzusehen?
- Was bringt den Befehl *logging synchronous* ?
- Für was stehen die 0 und die 4 beim Befehl *line vty 0 4* ? Was erzielt man damit?

# 4 Verkabelung der Router (20 min)

Im ersten Schritt bauen Sie das untenstehende Netzwerkschema auf. Bitte beachten Sie beim Aufbau die unterschiedlichen Kabeltypen.

Verwenden Sie ein gekreuztes Netzwerkkabel, um die beiden PC mit dem jeweiligen Router zu verbinden.

Verwenden Sie für die Verbindung zwischen dem Router Luzern und Bern ein serielles Kabel. Bei dieser Art von Verbindung handelt es sich um eine serielle Verbindung. Bei einer seriellen Verbindung müssen Sie immer darauf achten, dass auf dem DCE Gerät die Clock Rate konfiguriert wird. Unsere Kabel im Labor sind direkt mit der entsprechenden Bezeichnung ausgestattet.

Beachten Sie dass die Bezeichnung der Seriellen Interfaces nicht bei jedem Router gleich ist. Ist das 2T Modul im Slot 1 zu finden so ändert sich die Bezeichnung von S0/0/0 auf S0/1/0 usw.

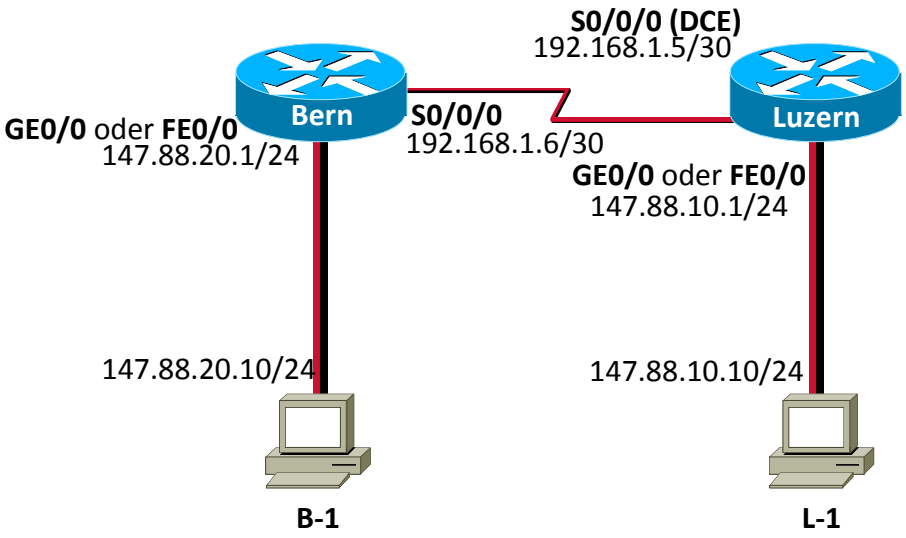



Abb. 2: Netzwerkschema Bern / Luzern

Nehmen Sie auf den angeschlossen Computern folgende IP-Konfigurationen vor:

| PC | IP Adresse | Subnetmaske | Standardgateway |
|---|---|---|---|
| L-1 | 147.88.10.10 | 255.255.255.0 | 147.88.10.1 |
| B-1 | 147.88.20.10 | 255.255.255.0 | 147.88.20.1 |

# 5 Konfiguration der Router Interfaces (30 min)

## 5.1 FastEthernet Interfaces

### 5.1.1 Router Luzern

Konfigurieren Sie das FastEthernet / Gigabit Interface vom Router Luzern. Konfigurieren Sie anschliessend die IP-Adresse 147.88.10.1/24 und aktivieren Sie danach das entsprechende Interface. (no shutdown)

```
luzern>enable
luzern#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
luzern(config)#interface fastEthernet 0/0
luzern(config-if)#ip address 147.88.10.1 255.255.255.0
luzern(config-if)#no shutdown
00:23:54: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:23:55: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
luzern(config-if)#
```

Nachdem Sie die obige Konfiguration vorgenommen haben, können Sie mit Befehl show ip int brief kontrollieren, ob das Interface richtig funktioniert ist.

```
luzern(config-if)#end
luzern#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0     147.88.10.1      YES manual up                    up
```

```
Serial0/0/0           unassigned      YES unset  administratively down down
Serial0/0/1           unassigned      YES unset  administratively down down
Luzern#
```

Testen Sie bitte die IP-Verbindung mit einem Ping.

```
luzern#ping 147.88.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
luzern#
```

Sicher Sie zum Schluss Ihre durchgeführte Konfiguration mit dem Befehl *copy running-config startup-config*.

```
luzern#copy running-config startup-config
```

### 5.1.2 Router Bern

Erstellen Sie für den Router Bern die Interfacekonfiguration analog der zuvor durchgeführten Konfiguration.

Konfigurieren Sie das FastEthernet-Interface von Router Bern und weisen Sie dem Interface die IP-Adresse 147.88.20.1/24 zu. Kontrollieren Sie die Konfiguration mit den gelernten show-Kommandos. Überprüfen Sie auch die Konfiguration selbst (show running-config).

Sichern Sie die Konfiguration von Router Bern

## 5.2 Serielle Interfaces

### 5.2.1 Router Luzern (Verbindung zu Bern)

Konfigurieren Sie das serielle Interface 0/0/0, welches Router Luzern mit Router Bern verbindet. Verwenden Sie das private IP-Netzwerk 192.168.1.0/30 (so verschwenden Sie keine teuren öffentlichen IP-Adressen).

Aktivieren Sie das Interface und wählen Sie PPP (Point to Point Protocol) als Übertragungsprotokoll.

Wählen Sie die Übertragungsgeschwindigkeit mittels clock rate. Die clock rate muss nur auf der DCE-Seite konfiguriert werden.

```
luzern#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
luzern(config)#interface serial 0/0/0
luzern(config-if)#ip address 192.168.1.5 255.255.255.252
luzern(config-if)#encapsulation ppp
luzern(config-if)#clock rate 128000
luzern(config-if)#no shutdown
luzern(config-if)#exit
luzern(config)#
```

Wenn Sie bei einem Befehl nicht mehr genau wissen wie er funktioniert, welche Paramter oder Optionen es gibt, dann benutzen Sie die Hilfefunktion, indem Sie ein Fragezeichen eingeben. Sie können es überall anwenden. Zum Beispiel beim Einstellen der clock rate. Wenn Sie nicht mehr

wissen, welche Geschwindigkeiten zulässig sind, tippen Sie am entsprechenden Ort ein Fragezeichen ein. Dabei generiert der Router Ihnen folgenden Output:

```
luzern(config-if)#clock rate ?
        Speed (bits per second)
  1200
  2400
  4800
  9600
  14400
  19200
  28800
  32000
  38400
  56000
  57600
  64000
  72000
  115200
  125000
  128000
  148000
  500000
  800000
  1000000
  1300000
  2000000
  4000000
  8000000
  <300-4000000>    Choose clockrate from list above
```

Finden Sie heraus, welche Übertragungsprotokolle für serielle Interfaces zulässig sind.

Die show Kommandos sind sehr wertvolle Diagnosefunktionen. Stöbern Sie mittels eines Fragezeichens in den show Kommandos herum und wenden Sie auch einige an.

Kontrollieren Sie anhand bereits gelernter show Kommandos die Funktion des seriellen Interfaces. Ist das Interface "up". Wenn nein, wieso nicht?

Das Interface ist nicht up, da die Gegenseite noch nicht konfiguriert wurde.

### 5.2.2 Router Bern (Verbindung zu Luzern)

Konfigurieren Sie nun die andere Seite der seriellen Verbindung (das "Berner" serielle Interface) analog der "Luzerner" Seite mit der IP 192.168.1.6/30.

```
bern#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bern(config)#interface serial 0/0/0
bern(config-if)#ip address 192.168.1.6 255.255.255.252
bern(config-if)#encapsulation ppp
bern(config-if)#no shutdown
bern(config-if)#exit
bern(config)#
```

Die clock rate muss nicht gesetzt werden, da Bern nicht DCE ist. Bern übernimmt die clock rate, welche Router Luzern als DCE vorgibt.

Kontrollieren Sie anhand bereits gelernter show Kommandos die Funktion des seriellen Interfaces. Jetzt sollte das serielle Interface auf beiden Routern up sein.

Überprüfen Sie anhand des ping Befehles die Verbindung zu Luzern.

Sichern Sie die Konfigurationen!

## 5.3 Testen des 1. Meilensteins

Nun haben wir den ersten Meilenstein erreicht. Damit wir im weiteren Verlauf dieses Laborversuchs auf den bisherigen Resultaten aufbauen können, führen Sie bitte folgende Tests und Verifikationen durch:

Testen Sie alle LANs. Bis jetzt sollten alle PCs ihre jeweiligen Standardgateways (Router Ethernet Interface) pingen können.

Können Sie vom PC L-1 den PC B-1 pingen? Wieso geht dies nicht?

Diskutieren Sie die Konfigurationen. Mit dem Befehl *show running-config* können Sie sich die Konfiguration anzeigen lassen.

Sichern Sie die Konfigurationen. Sie können die Konfiguration auch extern abspeichern, durch einfaches Kopieren in einen Texteditor.

## 5.4 Kontrollfragen

- Wieso wurden gekreuzte Netzwerkkabel verwendet, um die PCs mit dem Router zu verbinden?
- Mit dem Kommando show ip interface brief ist es möglich, den Status von den Interfaces einzusehen: Was ist, im Status, der Unterschied zwischen administratively down und down?
- Welche verschiedene Übertragungsprotokolle werden von den seriellen Verbindungen unterstützt? Welches ist defaultmässig aktiv? Recherchieren Sie.
- Was ist der Unterschied zwischen DCE und DTE? Wo werden Sie verwendet?

# 6 Konfiguration des Routing Prozesses (30 min)

Wie Sie in der obigen Frage, ob man PC B-1 von L-1 erreichen kann, richtig gemerkt haben, kann man dies nicht. Zum Verständnis der Problematik versetzen Sie sich in das Ping-Paket. Im PC L-1 wird das Paket an das Standardgateway geschickt, da der Empfänger nicht im gleichen Netzwerksegment wie der Sender ist (vergleichen von IP und Subnetmask der Interface-Konfiguration). Das Paket hat als Ziel die MAC des Routers und die IP von B-1. Der Router nimmt das Paket entgegen, da das Paket seine MAC-Adresse hat. Jedoch anhand der Ziel IP-Adresse merkt der Router, dass er nicht als Empfänger gemeint ist. Somit muss der Router das Paket weiterleiten, jedoch weiss er nicht, wohin. Der Router kennt das Netzwerk, welches am Router Bern angeschlossen ist nicht und verwirft das Paket.

Diesen Sachverhalt können Sie einfach verifizieren, in dem Sie die Routingtabelle des Routers Luzern betrachten.

Überprüfen Sie die Routing Table von Router Luzern mit dem Befehl *show ip route*. Sie werden sehen, dass der Router Luzern das angeschlossene LAN von Bern nicht kennt.

```
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 not set

     147.88.0.0/24 is subnetted, 1 subnets
C       147.88.10.0 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.4/30 is directly connected, Serial0/0/0
C       192.168.1.6/32 is directly connected, Serial0/0/0
luzern#
```

Überprüfen Sie auch die Routingtabelle von Router Bern. Was stellen Sie dort ebenfalls fest?

## 6.1 Router Luzern

Konfigurieren Sie den Router Luzern so, dass er über das dynamische Routing Protokoll OSPF Netzwerke lernt und seine angeschlossenen Netzwerke anderen Routern mitteilt.

Wechseln Sie in den globalen Konfigurationsmodus.

Konfigurieren Sie einen OSPF Routing Prozess (Prozess-ID 1) auf dem Router Luzern. Alle Netzwerke sind in der OSPF Area 0. Führen Sie alle nötigen Netzwerke (an den Router angrenzende!) in den Routing Prozess ein. Beim Befehl network muss bei OSPF die Wildcardmask des Netzwerkes angegeben werden.

```
luzern#configure terminal
luzern(config)#router ospf 1
luzern(config-router)#network 192.168.1.4 0.0.0.3 area 0
luzern(config-router)#network 147.88.10.0 0.0.0.255 area 0
luzern(config-router)#exit
luzern(config)#
```

Die Routing-Prozess-ID ist bei OSPF nicht relevant. Sie hat nur eine lokale Bedeutung. Hingegen ist die Area-Nummer  das entscheidende Kriterium, das die Router in ihrem Netzwerke austauschen. OSPF arbeitet mit der Metric Kosten. Damit die Pfadkosten der jeweiligen Links richtig einbezogen werden, müssen Sie mit dem Befehl bandwidth die effektiven Interface-Bandbreite angegeben. Vergessen Sie diesen Befehl, funktioniert das Routing, jedoch kann es zu suboptimalen Routingpfade kommen, da der Routing Prozess die maximale Interface-Bandbreite verwendet und nicht die effektiv zur Verfügung stehende Bandbreite.

Wechseln Sie in das konfigurierten seriellen Interface 0/0/0 und setzen Sie die effektive Bandbreite (= Clock rate) des Links.

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

## 6.2 Router Bern

Konfigurieren Sie einen OSPF Routing Prozess (der Einfachheit wieder Prozess-ID 1) auf Router Bern. Alle Netzwerke befinden sich wieder in der OSPF Area 0 (zwingend). Führen Sie alle nötigen Netzwerke (an den Router angrenzende!) in den Routing Prozess ein.

```
bern#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bern (config)#router ospf 1
bern (config-router)#network 192.168.1.4 0.0.0.3 area 0
bern (config-router)#network 147.88.20.0 0.0.0.255 area 0
bern (config-router)#exit
bern (config)#
```

Konfiguriere Sie auf Router Bern die effektiven Bandbreiten der seriellen Interfaces.

## 6.3 Kontrolle

Kontrollieren Sie erneut die Routing Tabellen von Router Luzern und Bern. Was stellen Sie fest?

```
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 not set

     147.88.0.0/24 is subnetted, 2 subnets
C       147.88.10.0 is directly connected, FastEthernet0/0
O       147.88.20.0 [110/65] via 192.168.1.6, 00:00:00, Serial0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.4/30 is directly connected, Serial0/0
C       192.168.1.6/32 is directly connected, Serial0/0
luzern#
```

Sie sehen, dass Router Luzern über OSPF (O) das LAN von Bern gelernt hat. Können Sie jetzt alle PCs in den LANs erreichen (PING)?

Wenn es nicht funktioniert, dann versetzen Sie sich wieder in das Ping-Paket und überlegen Sie sich, was mit dem Paket passiert. Kontrollieren Sie alle Routingtabellen und Interface-Konfigurationen.

## 6.4 Kontrollfragen

- Was ist der Unterschied zwischen subnetmask und wildcardmask und wo werden sie verwendet?
- Bei Kapitel 6.3 wurde mittels *show ip route* die Routing Tabelle dargestellt. Für was stehen die beiden Zahlen in den rechteckigen Klammern, bei der OSPF Zeile (O)?

# 7 Anbindung an Provider (30 min)

Dieses Kapitel beschreibt die Anbindung unseres kleinen Firmennetzwerkes an das Internet über einen ISP (Internet Service Provider).

## 7.1 Übersicht

Die nächste Aufgabe von Ihnen ist es, unser kleines Firmennetz ans Internet anzubinden. Dies geschieht über eine serielle Verbindung zu einem ISP. Das Szenario sieht wie folgt aus:

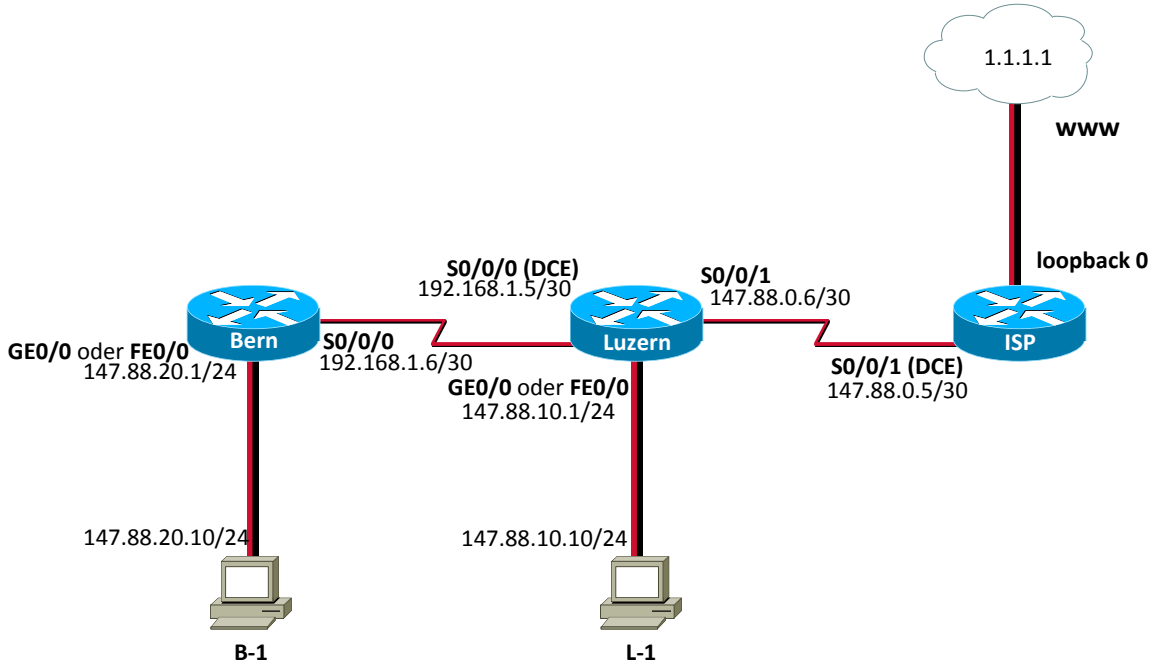



Abb. 3: Netzwerkschema mit Anbindung zum ISP

| Verbindung | WAN-ZI |
|---|---|
| Typ | Seriell/PPP |
| Kabel | V.35 |
| IP | 147.88.0.4/30 |

Erstellen Sie die benötigten Verbindungen. Achten Sie bitte auf DCE/DTE!

Das Loopback-Interface des ISP existiert nicht physikalisch. Es ist nur ein logisches Interface im Innern des Routers, das für administrative Aufgaben eingesetzt werden kann.

## 7.2 Grundeinstellung

Bitte achten Sie darauf, dass der Router, bevor Sie mit der Konfiguration beginnen, keine alte Konfiguration mehr besitzt. Falls der Router noch eine ältere Konfiguration besitzt, löschen Sie diese bitte und starten anschliessend das Gerät neu. Nehmen Sie auf dem ISP-Router folgende Grundkonfiguration vor:

Konfigurieren Sie den Hostnamen auf ISP

Deaktivieren Sie die DNS-Auflösung auf dem Router

Setzen Sie als Konsolenpasswort cisco

Setzen Sie als Telnetpasswort cisco

Konfigurieren Sie als Passwort für den Privilege Mode cisco

Speichern Sie anschliessend die erstellte Konfiguration ab.

## 7.3 ISP Loopback Interface

Damit wir in unserer Laborumgebung eine Internetverbindung simulieren können, erstellen wir auf dem Router mehrere Loopback Interfaces. Diese Interfaces sind nicht physikalisch vorhanden, sondern simulieren nur ein Ziel im Internet. Um ein Loopback Interface auf dem Router zu konfigurieren gehen Sie bitte wie folgt vor:

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface loopback 0
ISP(config-if)#ip address 1.1.1.1 255.255.255.255
ISP(config-if)#no shutdown
ISP(config-if)#end
ISP#
```

Nachdem Sie die Konfiguration vorgenommen haben, können Sie mit einen simplen ping überprüfen, ob das erstellte Interface verfügbar ist.

```
ISP#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
ISP#
```

Die Ausführung des Ping-Befehls sollte gemäss obiger Abbildung erfolgreich sein.

## 7.4 Konfiguration der serielle Verbindung zwischen ISP und Luzern

Nun wird es Zeit, die serielle Verbindung zwischen dem Router ISP und Luzern zu konfigurieren. Gehen Sie dazu wie folgt vor:

**Router ISP**

- Interface serial 0/0/1 (DCE)
- Encapsulation ppp
- IP-Adresse 147.88.0.5 /30
- Clock Rate 128000 bps
- Bandwidth 128kbps

**Router Luzern**

- Interface serial 0/0/1 (DTE)
- Encapsulation ppp
- IP-Adresse 147.88.0.6 /30
- Clock Rate 128000 bps
- Bandwidth 128kbps

Auf dem Router Luzern müssen Sie keinen neuen Routingprozess erstellen. Ändern Sie bitte nichts an der zuvor erstellten Konfiguration.

Verifizieren Sie mit den erlernten Kommandos, ob die beiden Interfaces der Router Luzern und dem ISP funktionsfähig sind und erreichbar sind.

## 7.5 Erstellen der Connectivity

Aus diversen Gründen ist es unsinnig, dass sich ein Firmennetzwerk in einen dynamischen Routing Prozess des Providers einklinkt. Die Firma interessiert sich nicht über die interne Vernetzung vom Provider und der Provider sollte auch nicht wissen, wie es im Innern der Firma aussieht. Man erstellt, sofern es die Komplexität (oder die Einfachheit) des eigenen Netzes zulässt, eine Defaultroute gegen den Provider (Defaultroute = Standardgateway). Wann immer der Router für ein Netzwerk keine Information in der Routingtabelle vorfindet, bedient er sich der Defaultroute. Bedingung dazu ist natürlich, dass das interne Netz sauber konfiguriert ist und für jedes interne Netz eine Route existiert. Ansonsten werden Datenpakete, die für Ziele im internen Firmennetzwerk bestimmt sind, direkt zum Provider weitergeleitet.

Erstellen Sie auf dem Router Luzern eine Defaultroute zum Provider. Geben Sie dazu folgenden Befehl ein:

```
luzern#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
luzern(config)#ip route 0.0.0.0 0.0.0.0 147.88.0.5
luzern(config)#exit
luzern#
```

Überprüfen Sie anschliessend die Routingtabelle. Was stellen Sie fest?

```
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 147.88.0.5 to network 0.0.0.0
147.88.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 147.88.10.0/24 is directly connected, FastEthernet0/0
C 147.88.0.5/32 is directly connected, Serial0/0/1
C 147.88.0.4/30 is directly connected, Serial0/0/1
O 147.88.20.0/24 [110/65] via 192.168.1.6, 00:09:29, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
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 147.88.0.5
luzern#
```

## 7.6 Zwischenkontrolle

Pingen Sie von Router Luzern das Loopback Interface von Router ISP an! Tun Sie dies mittels "extended ping" (siehe unten). Mit dem Extended-Ping können Sie angeben, welche Source IP-Adresse (der konfigurierten Interfaces) das ICMP Paket haben soll. Verwenden Sie die IP-Adresse des seriellen Interfaces vom Router ISP. Warum ist der Ping-Befehl erfolgreich?

```
luzern#ping
Protocol [ip]:
Target IP address: 1.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 147.88.0.6
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 147.88.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
luzern#
```

Pingen Sie anschliessend das Loopback Interface des ISP Routers noch einmal. Nehmen Sie aber dieses Mal als Absenderadresse die IP-Adresse des seriellen Interfaces zum Router Bern. Was stellen Sie fest?

```
luzern#ping
Protocol [ip]:
Target IP address: 1.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.5
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.5
.....
Success rate is 0 percent (0/5)
luzern#
```

**Problemstellung**

Wieso hat der obige Ping-Befehl nicht funktioniert? Überlegen Sie sich, wie der Ping-Befehl genau funktioniert und kontrollieren Sie anschliessend die Routingtabellen der einzelnen Router. Sie finden die Lösung für das Problem in der Routingtabelle.

**Lösung**

Wenn Sie ein Ping-Paket absenden, wird das Paket immer zwei Mal über das Netzwerk übertragen. Einmal vom Sender zum Empfänger und anschliessend wieder vom Empfänger der Nachricht zurück zum Sender. Wenn Sie vom Router Luzern ein ICMP Echo-Request los senden, kontrolliert der Router Luzern als erstes seine Routingtabelle nach einer Route für das Ziel.

```
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 147.88.0.5 to network 0.0.0.0

147.88.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 147.88.10.0/24 is directly connected, FastEthernet0/0
C 147.88.0.5/32 is directly connected, Serial0/0/1
C 147.88.0.4/30 is directly connected, Serial0/0/1
O 147.88.20.0/24 [110/65] via 192.168.1.6, 00:21:17, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
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 147.88.0.5
luzern#
```

Für das Ziel 1.1.1.1 ist kein spezifischer Eintrag in unserer Routingtabelle vorhanden. Jedoch besitzt der Router eine Default-Route. Alle Pakete, für die kein spezifischer Eintrag in der Routingtabelle vorhanden ist, werden an den Next-Hop der Default-Route versendet. Router Luzern sendet die ICMP-Pakete für das Ziel 1.1.1.1 über seine serielle Verbindung zum ISP Router. Der ISP Router anschliessend empfängt die Pakete und kontaktiert danach wieder seine Routingtabelle, um die Antwortpakete zurück zusenden.

```
ISP#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
1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1 is directly connected, Loopback0
147.88.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 147.88.0.6/32 is directly connected, Serial0/0/1
C 147.88.0.4/30 is directly connected, Serial0/0/1
ISP#
```

Auch der ISP Router besitzt keinen spezifischen Eintrag für das Ziel. Leider besitzt dieser Router auch keine Default-Route. Das heisst, der Router kann die Antwortpakete nicht mehr zurück senden. Der Ping-Befehl schlägt fehl.

Wenn wir jetzt aber vom seriellen Interace (mit der IP 147.88.0.5) pingen, geht das Ping nach gleichem Muster wie oben hin und auch wieder zurück, da in der Routingtabelle des ISP ein Eintrag für das Netz 147.88.0.4/30 steht!

**Problemstellung**

Was ist also zu tun, dass ein Echo-Reply in jedem Fall funktioniert? Können wir beim ISP ebenfalls eine Defaultroute zurück ins Firmen netz installieren? Bedenken Sie in dieser Sache, dass der Provider auf der einen Seite Ihr Firmennetz und auf der anderen Seite das Internet hat.

Wenn nein, wieso nicht und was können wir sonst tun? Wenn ja, welche "Nachteile" folgen daraus?

**Lösung**

Durch den Einsatz einer Defaultroute auf dem ISP-Router würde der Ping-Befehl tatsächlich funktionieren. Jedoch entsteht durch diese Massnahme für den Provider ein zusätzlicher Mehraufwand, für jeden Kunden eine eigene Route in der Routingtabelle zu erfassen. Wir werden also gezwungen, eine andere Lösung zu finden.

Die Lösung für unser Problem ist die Definition einer statischen Route, die nur unser Firmennetzwerk einschliesst. In unserem Fall müssen wir eine statische Route zum Ziel 147.88.0.0 auf dem ISP Router konfigurieren.

Konfigurieren Sie auf dem ISP Router eine statische Route.

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 147.88.0.0 255.255.0.0 147.88.0.6
ISP(config)#^Z
ISP#
```

Überprüfen Sie anschliessend die Routingtabelle des ISP-Routers.

```
ISP#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

1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1 is directly connected, Loopback0
147.88.0.0/16 is variably subnetted, 3 subnets, 3 masks
S 147.88.0.0/16 [1/0] via 147.88.0.6
C 147.88.0.6/32 is directly connected, Serial0/0/1
C 147.88.0.4/30 is directly connected, Serial0/0/1
ISP#
```

Führen Sie nun nochmals die Extended-Ping durch. Überprüfen Sie die Verwendung der Source IP-Adresse des FastEthernet Interfaces zu PC L-1 (IP 147.88.10.1). Können Sie vom Router ISP aus das FastEthernet Interface von Router Luzern (IP 147.88.10.1) pingen? Jetzt sollte alles funktionieren!

## 7.7 Router Bern

Pingen Sie vom FastEthernet Interface des Rotuers Bern die IP-Adresse 1.1.1.1. Was stellen Sie fest?

Sie werden feststellen, dass der Ping nicht erfolgreich ist. Wir haben wieder ein analoges Problem, wie vorher. Kontrollieren Sie die Routingtabelle des Routers in Bern. Sie werden feststellen, dass dieser Router keine Default-Route für das Internet besitzt.

Die Lösung für dieses Problem ist das Konfigurieren einer Default-Route auf jedem Router. Dies ist aber mit sehr viel Aufwand und Administration vorhanden. Anstelle bei jedem Router im Netzwerk eine Defaultroute zu setzen, gibt es eine einfachere Variante. Der Router Luzern, der die Schnittstelle zum Internet darstellt, soll den restlichen Routern in Ihrem Netzwerk eine Defaultroute mitteilen. Dadurch werden alle Router, welche keine Angaben zum Zielnetzwerk in der Routingtabelle haben, die Pakete an Router Luzern senden. Dieser weist anschliessend anhand seiner Routingtabelle, wohin er die Pakete in das Internet weiterleiten muss.

Loggen Sie sich auf den Router Luzern ein. Hier teilen wir anschliessend dem Routing-Prozess mit, dass er nun seine Defaultroute den anderen Routern mitteilen soll. Bei OSPF heisst dieser Befehl *default-information originate.* Beachten Sie bitte, dass bei anderen Routing-Protokollen der Befehl anders lautet!

```
luzern#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
luzern(config)#router ospf 1
luzern(config-router)#default-information originate
luzern(config-router)#[CTRL-Z]
luzern#
```

Kontrollieren Sie anschliessend auf dem Router Bern, ob dieser eine Default-Route erhalten hat. Sie sollten eine Routingtabelle nach dem untenstehenden Muster erhalten:

```
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 192.168.1.5 to network 0.0.0.0

147.88.0.0/24 is subnetted, 2 subnets
O 147.88.10.0 [110/74] via 192.168.1.5, 00:00:13, Serial0/0/0
C 147.88.20.0 is directly connected, FastEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.5/32 is directly connected, Serial0/0/0
C 192.168.1.4/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.5, 00:00:13, Serial0/0/0
bern#
```

Pingen Sie zur Kontrolle vom PC B-1 die IP-Adresse 1.1.1.1. Dieser Befehl sollte erfolgreich funktionieren.

Sichern Sie die Konfiguration aller Router ab.

### 7.8 Kontrollfragen

- Wie kann man IP-Verbindungen prüfen?
- Was erzielt man mit dem Kommando *default-information originate*?
- Wie erkennt man generell eine default Route in der Routing Tabelle?

# 8 Authentifizierung (optional)

## 8.1 Point-to-Point Protokoll

Punkt zu Punkt Datenverbindungen werden im Internet sehr oft eingesetzt. Jede ADSL, ISDN oder serielle Datenverbindung ist eine Punkt-zu-Punkt Verbindung. Bei öffentlichen Datenverbindungen ist es wichtig, dass sich nicht jeder mit der Gegenstelle verbinden kann. Aus diesem Grund werden Authentifizierungsprotokolle eingesetzt, die sicherstellen, dass sich nur Benutzer mit einem gültigen Benutzernamen und Passwort mit der Gegenstelle verbinden können. Auch in unserem Beispiel möchten wir die Verbindung zwischen dem ISP und Router Luzern gerne mit einer Authentifizierung sichern.

Damit wir diesen Mechanismus implementieren können, verwenden wir das PPP-Protokoll. Das PPP-Protokoll kennt folgende zwei Authentifizierungsprotokolle:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

**Bemerkung**

Das PAP-Protokoll ist unsicher. PAP sendet die Passwörter im Klartext über das Netzwerk.

## 8.2 CHAP

Der Challenge Handshake Authentication Protocol (CHAP) verifiziert die Identität des Peers mit einem three-way Handshake. Folgende Schritte werden durchgeführt:

1. Nachdem die LCP-Phase (Link Control Protocol) fertig ist und das CHAP Protokoll zwischen den Peers verhandelt und festgelegt wurde, sendet der ISP (authenticator) eine CHAP Nachricht dem Peer-Router.
2. Der Peer-Router antwortet mit einem MD5 Hashwert.
3. Der ISP überprüft die Antwort mit seinem eigenen Hashwert. Wenn die beiden Werte übereinstimmen, ist die Authentifizierung erfolgreich, sonst wird die Verbindung getrennt.

Die Authentifizierungsmethode basiert auf einem Passwort, welches nur den beiden Peers bekannt ist. Das Passwort wird nicht über den Link gesendet.

Unidirektionale und Bidirektionale Authentifizierung.

CHAP ist als unidirektionale Authentifizierungsmethode definiert. Doch Sie werden CHAP bidirektional implementieren, denn die Cisco CHAP Implementation unterstützt dies.

Per Default, authentifiziert sich die anrufende Partei beim ISP. Aber der anrufende Peer kann auch die Identität der “angerufenen” Seite verifizieren.

Eine unidirektionale Authentifizierung ist oft in Verbindung mit nicht-Cisco Geräten nötig.

In der unterstehenden Tabelle sind die Befehle für die uni-/bidirektionale Authentifizierung.

| Authentifications Typ | Client (calling) | ISP (called) |
|---|---|---|
| Unidirektional | ppp authentication chap callin | ppp authentication chap |
| Bidirektional | ppp authentication chap | ppp authentication chap |

Im Theorieteil wird der Authentifizierungs-Handshake näher erklärt.

## 8.3 Konfiguration: Bidirektional

Konfigurieren Sie eine bidirektionale Authentifizierung mit CHAP zwischen Bern und Luzern. Verwenden Sie dazu folgenden Benutzernamen und Passwörter. Achten Sie darauf, dass bei den Benutzernamen und Passwörtern Gross- und Kleinschreibung unterschieden wird.

| Router | Benutzername | Passwort |
|---|---|---|
| Bern | userBern | geheim |
| Luzern | userLuzern | geheim |

### 8.3.1 Bern

Für den Router Bern nehmen Sie bitte folgende Konfiguration vor:

```
Bern#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
```

Auf dem Router Bern wird der Router Luzern authentifiziert. Dazu wird der Benutzername und das Passwort für den Router Luzern konfiguriert.

```
Bern(config)#username userLuzern password geheim
```

Die PPP-Authentifizierung wird immer auf dem Interface konfiguriert.

```
Bern(config)#interface serial 0/0/0
```

Im nächsten Schritt wird dem Router mitgeteilt, dass er Verbindungen über dieses Interface mit CHAP authentifizieren soll.

```
Bern(config-if)#ppp authentication chap
```

Nun geben Sie an, mit welchem Passwort Router Bern an die Luzerner Türe klopft. Die Authentifizierung ist immer eine lokale Angelegenheit und könnte auch unidirektional konfiguriert werden. Geben Sie keinen Hostnamen an, so wird der Hostname des Routers verwendet. Mit ***ppp chap password*** kann man ein Passwort für die Verbindung angeben, jedoch kommt diese nicht zum Zuge! Studieren Sie zum Verständnis das Sequenzdiagramm.

```
Bern(config-if)#ppp chap hostname userBern
Bern(config-if)#end
Bern#
```

Konfigurieren Sie den Router Luzern analog Router Bern.

Kontrollieren Sie ihre Konfigurationen. Ist die Verbindung zwischen Luzern und Bern up? Wenn Probleme mit der Verbindung auftreten, so aktivieren Sie das Debug von PPP mit dem Befehl:

```
Bern#debug ppp authentication
```

Dieser Befehl liefert Ihnen den genauen Ablauf der Authentifizierung. Mit dem Befehl undebug all deaktivieren Sie das Debug wieder!

## 8.4 Unidirektional

Konfigurieren Sie zwischen dem Router Luzern und dem ISP eine unidirektionale CHAP-Authentifizierung. Dabei soll nur der Router ISP den Router Luzern authentifizieren. Bei der unidirektionalen Authentifizierung, muss sich nur der Client beim ISP authentifizieren.

Verwenden Sie dazu bitte die folgenden Angaben:

| Router | Benutzername | Passwort |
|---|---|---|
| ISP | userLuzern | Strenggeheim |
| Luzern | ISP | Strenggeheim |

Konfigurieren Sie das Interface des Routers Luzern wie folgt:

```
Luzern(config-if)# ppp authentication chap callin
--- Authentisierung nur auf einkommenden Anrufen
Luzern(config-if)# ppp chap hostname userLuzern
--- Alternatives CHAP Hostname, welcher auf dem ISP Router gespeichert ist
Luzern(config-if)# end
Luzern #
```

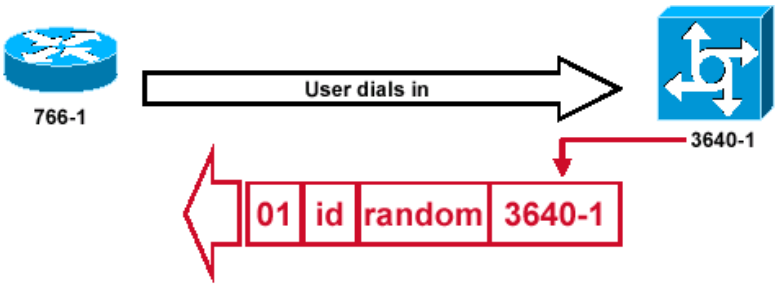
Die unidirektionale Authentisierung erfolgt folgendermassen:

- Luzern initialisiert den CHAP Vorgang.
- ISP antwortet mit einem CHAP Response, das mit „ISP“ gekennzeichnet ist.
- Luzern schaut in seiner lokalen Username-„Datenbank“ nach dem Eintrag „ISP“ und berechnet den MD5 Hash anhand des Shared Secrets.
- Luzern sendet den Hash zurück zu ISP, der seinerseits den Hashwert überprüft und Luzern authentisiert.

## 8.5 Wie funktioniert CHAP

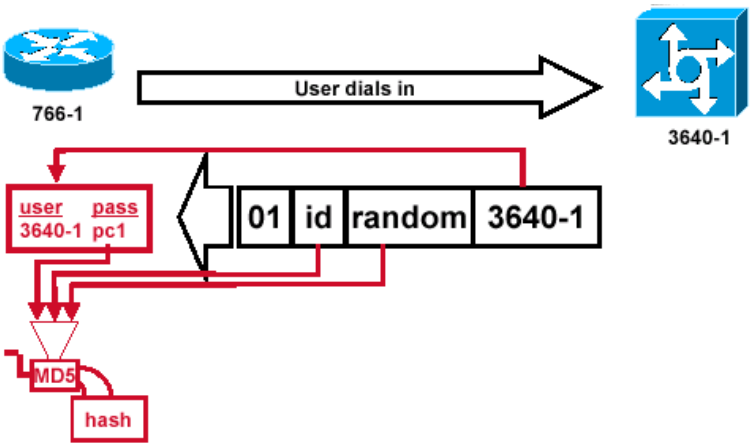
**Call**


1. 3640-1 wird angerufen. Das Interface ist mit dem Befehl **ppp authentication chap** konfiguriert.
2. LCP verhandelt CHAP und MD5.




1. Ein CHAP Challenge Paket wird erzeugt, mit diesen Merkmalen:
   - 01 = challenge packet type identifier.
   - ID = sequentielle Nummer, die das Challenge Packet identifiziert.
   - random = Eine zufällige vom Router erzeugte Nummer.
   - 3640-1 = Der Authentifizierungsname des Routers.
2. Die ID und der Randomwert werden auf dem Router 3640-1 zwischengespeichert.
3. Das Challenge Packet wird nun dem Client gesendet. Eine Liste der gesendete Challenge Pakete wird auf dem Router geführt.

**Response**

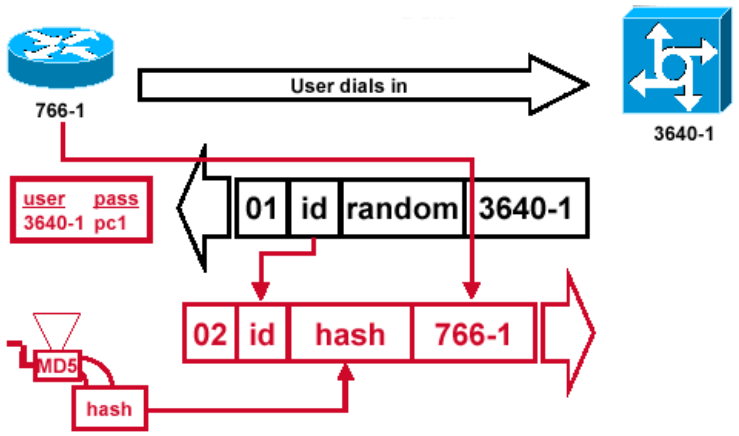



Der Client-Router verarbeitet das Challenge Packet wie folgt:

1. ID und Randomwert werden für das generieren des MD5 Hashes verwendet.
2. Anhand vom Namen 3640-1 wird nach einem passenden Eintrag gesucht:
   Hier: username 3640-1 password pc1

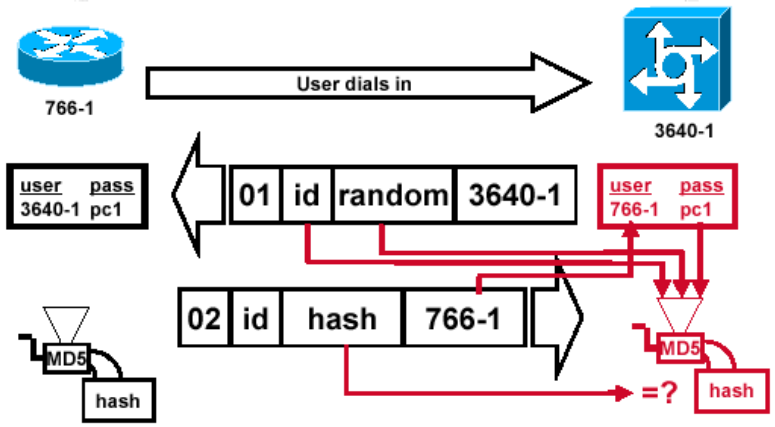
3. Das Passwort wird  für das Generieren des MD5 Hashes verwendet.
4. Der Client berechnet den MD5 Hash anhand des ID-Wertes, Random-Wertes und Passwortes.

**Response (2)**



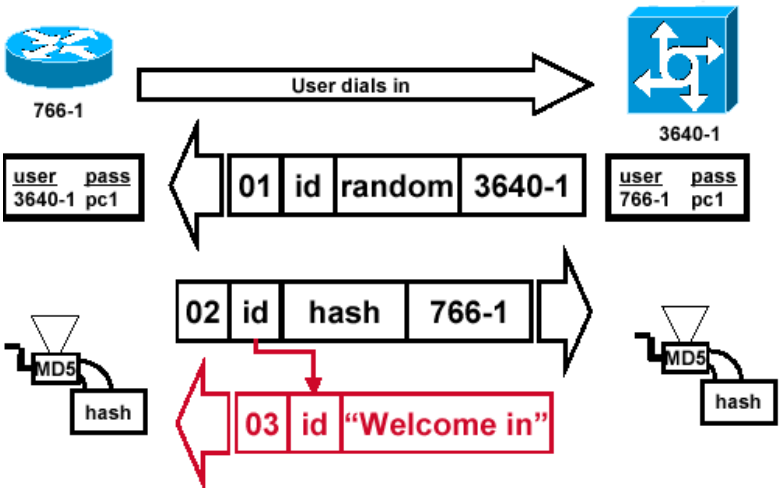

1. Der Client generiert das Antwortpaket mit diesen Komponenten:
   - 02 = CHAP response packet type identifier.
   - ID = Kopiert von Challenge Packet.
   - hash = Der berechnete MD5 Hashwert.
   - 766-1 = Der Authentifizierungsname des Clients.
2. Das Antwortpaket wird gesendet.

**Verify**




1. Mit der ID wird der CHAP-Authentifizierungsvorgang identifiziert und wird für das Generieren des MD5 Hashes verwendet.
2. Der gespeicherte Randomwert wird für das Generieren des MD5 Hashes verwendet.
3. Anhand vom Namen 3640-1 wird nach einem passenden Eintrag gesucht:
   Hier: username 766-1 password pc1
4. Das Passwort wird  für das Generieren des MD5 Hashes verwendet.
5. Der neuberechnete Hashwert wird mit dem Hashwet des Clients verglichen. Wenn die beiden Werte übereinstimmen, ist die Authentifizierung erfolgreich, sonst wird die Verbindung getrennt.

**Success**




Der ISP-Router sendet dem Client ein Success Message mit folgenden Eigenschaften.

1. Wenn die Authentifizierung erfolgreich war, erzeugt der ISP-Router ein CHAP success packet:
   - 03 = CHAP success message type.
   - ID = ID des ersten Challenge Packet.
   - "Welcome in" = Text.
2. Wenn die Authentifizierung fehlschlägt, erzeugt der ISP-Router ein CHAP failure packet:
   - 04 = CHAP failure message type.
   - ID = ID des ersten Challenge Packet.
   - "Authentication failure" = Text.
3. Des erzeugte Paket wird dann dem Client gesendet.

**Achtung:** Hier wurde nur die unidirektionale Authentifizierung behandelt. Bei der bidirektionalen Authentifizierung wird der ganze Vorgang noch einmal wiederholt (ISP ist dann der anrufende Router).

## 8.6 Kontrollfragen

- Wieso wird CHAP und nicht PAP als Authentifizierungsprotokoll verwendet?
- Was ist MD5?

# 9 OSPF Authentication (optional)

## 9.1 Konfiguration

Die meisten Routing Protokolle unterstützen ebenfalls eine Authentifizierung, um gefälschte Routing-Updates zu erkennen. Würde jemand erreichen, dass ein Router gefälschte Updates mit gefälschten Routen in die Routingtabelle einträgt, so könnte das ganze Netzwerk lahm gelegt oder der Verkehr umgeleitet werden. In unserem Fall konfigurieren wir OSPF mit Authentifizierung, damit wir ein Abändern der Routen verhindern können.

Konfigurieren Sie auf allen Routern die OSPF-Authentifizierung. Für den Router Bern sieht die Konfiguration wie folgt aus:

```
Bern#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bern(config)#router ospf 1
```

Anschliessend müssen Sie global für alle Router die Authentifizierung aktivieren. Ohne das Kommando *message-digest* wird das Passwort unverschlüsselt übertragen.

```
Bern(config-router)#area 0 authentication message-digest
Bern(config-router)#exit
```

Zum Schluss müssen Sie auf allen Schnittstellen das Passwort für OSPF aktivieren. Dies wird durch die Eingabe der folgenden Kommandos vorgenommen:

```
Bern(config)#interface serial 0/0/0
Bern(config-if)#ip ospf message-digest-key 1 md5 cisco
Bern(config-if)#end
Bern#
```

Führen Sie die oben aufgeführten Konfigurationsschritte ebenfalls für den Router Luzern durch. Erst nach dem Sie Konfiguration ebenfalls auf dem Router Luzern durchgeführt haben, sind die Routen wieder via OSPF auf beiden Routern verfügbar.

## 9.2 Kontrollfrage

- Was wird mit dem Kommando message-digest erzielt?

# 10 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*** |

# 11 Anhang A - Nutzen von serielle Verbindungen

In den Laborversuchen zwischen Routern werden die WANs mit seriellen Verbindungen simuliert. Dabei kommen HWIC-2T oder HWIC-2A/S Module mit „Smart Serial Kabeln“ zum Einsatz. Die Smart Serial Kabel sind nicht Cisco proprietär, aber praktisch, da man sonst die sperrigen/unhandlichen X.35 DCE und X.35 DTE Kabel verwenden muss.

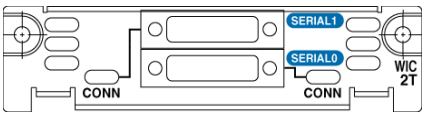



**Abb. 4: Front eines HWIC-2T Modul**

Die seriellen Verbindungen werden anstelle von FastEthernet verwendet.

Dadurch besteht die Möglichkeit mittels Clock-Rate die 2T Module zwischen 600bps und 115.2Kbps im Asynchronous Modus und bis max. 8Mbps im Synchronous Modus zu betreiben (2A/S sind im Synchronous Modus auf 128Kbps limitiert). Dies bringt einen wesentlichen Vorteil, wenn man

überladene Netze simulieren und testen will, da man die Clock-Rate herabsetzen kann, um einen Engpass oder eine Überlastung zu simulieren.

# 12 Anhang B - 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 Alt+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.