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

Switching Advanced

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

Autoren: A. Vogt, D. Krummenacher, N. Lardieri, Prof. Dr. B. Hämmerli, D. Nadezhdin, P. Muff, C.Di Battista., M. Schröder
Version: 5.2
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		Erledigt	Erstellung Dokument	AV
Nr. 1.5	24.03.05	Erledigt	Anpassungen IOS	D. Krummenacher
Nr. 2.0	28.09.05	Erledigt	Versuch in zwei Teile gesplittet	D. Krummenacher
Nr. 3.0	19.02.08	Erledigt	Komplette Überarbeitung	N. Lardieri
Nr. 3.1	29.05.09		Neues Layout	N. Lardieri
Nr. 3.2	05.01.10	Erledigt	Update, Fehlerkorrektur	N. Lardieri
Nr. 4.0	01.05.12	Erledigt	Aktualisierung des Versuches unter Berücksichtigung von Win7 und IOS 12.2, Kapitel 8 (Stacking) ergänzt	D. Nadezhdin, P. Muff
Nr. 5.0	23.09.12	Erledigt	Überarbeitung – Layout und Inhalt	C. Di Battista, M. Schröder
Nr. 5.1	15.07.14	Erledigt	Interswitchlink neu mit SFP für Glasverbindung	P. Gertsch
Nr. 5.2	06.11.15	Erledigt	Überarbeitung Kapitel „8 Security Zusatzkapitel B“	C. Banzer
Nr. 5.3	08.03.15	Erledigt	Anpassung Password/Secret setzen, IOS-Version anpassen, Diagramm Kapitel 6 korrigieren	C. Banzer, E. Fux

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

In diesem Dokument werden folgende Abkürzungen verwendet:

Abkürzung	Beschreibung
IP	Internet Protokoll
SFP	Small Form-factor Pluggable
SPAN	Switch Port Analyzer
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
VTP	VLAN Trunking Protocol

Einleitung

Dieser Laborversuch vermittelt den Studierenden einen tieferen Einblick in den Umgang mit Switches und die Konfiguration von VLANs. Dieser Versuch baut auf dem Vorwissen des Basisversuchs auf.

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.

Unbedingt 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.

Versuchsaufbau

Der Versuch ist in mehrere Teile aufgeteilt. Der Hauptteil (Kapitel 1 bis 6) ist obligatorisch zu bearbeiten. Anschliessend teilt sich der Versuch in zwei Teile auf. Man kann entweder das Zusatzkapitel A zu Stacking oder das Zusatzkapitel B zu Security bearbeiten. Die Challenge-Aufgaben des Kapitels 9 sind unabhängig bearbeitbar.

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. Welches ist der dritte Layer im OSI Modell, welche Geräte sind typisch dafür und was beinhaltet diese Schicht?
2. Was ist Port mirroring, alias SPAN (Switch Port Analyzer)?
3. Was ist ein VLAN und wofür braucht man dieses?
4. Was ist das Spanning Tree Protokoll und was verhindert es?

1.2 Antworten

Frage 1: Lesen Sie Kapitel 1.4.1 auf Seite 56 vom Buch Computernetzwerke von A.S. Tanenbaum.

Frage 2: Lesen Sie Kapitel 11 Anhang A – Theorie.

Frage 3: Lesen Sie Kapitel 4.7.6 auf Seit 365 vom Buch Computernetzwerke von A.S. Tanenbaum.

Frage 4: Lesen Sie Kapitel 4.7.3 auf Seit 360 vom Buch Computernetzwerke von A.S. Tanenbaum.

1.3 Materialiste

Für die Durchführung dieses Laborversuches benötigen Sie folgendes Material:

- 2x Cisco Catalyst 3560 Switches mit Firmware-Version 12.2 oder höher
- 2x Cisco Catalyst 3750 Switches mit Firmware-Version 15.02 oder höher für Zusatzkapitel B (Kapitel 8)
- 2x Gigabit-SFP Module für Catalyst 3560
- 2x Workstations (1 Workstation mit Dualboot Windows / Ubuntu mit installiertem Wireshark und Macof)
- 2x Studierenden-Notebooks
- diverse Kabel

2 Aufgabenstellung

Damit der Laborversuch möglichst praxisnah durchgeführt werden kann, wird anhand eines KMU's der Einsatz von Switches und VLANs aufgezeigt.

Sie sind stets bei der gleichen Firma eingestellt, wie im Versuch „Switching Basic". Der Verwaltungsrat hat Ihnen ein höheres Budget genehmigt, so dass Sie die momentane Infrastruktur erneuern können. Sie haben vorgeschlagen die zwei Layer-2 Switches und den Router, der das InterVLAN-Routing übernimmt, mit zwei Cisco Catalyst 3560 Switches zu ersetzen. Diese Switches besitzen Layer 3 Fähigkeiten, d.h. das Routing erfolgt direkt auf dem Switch.

Ihre Aufgabe besteht darin, die gewachsenen Abteilungen Verkauf und Marketing logisch zu trennen und daraus eigene Broadcast-Domains zu machen. Es sollte anschliessend möglich sein, dass z.B. Marketingangestellte vom ersten Stock mit den Angestellten vom zweiten Stock kommunizieren können. Ein zusätzlicher Router ist also für die Kommunikation unterhalb der VLANs nicht mehr notwendig, da dies gleich ein Layer 3 Switch übernimmt.

Weil die Ports eines einzelnen Switches nicht ausreichen, müssen Sie einen zweiten zur Hilfe nehmen und diesen über einen Gigabit-Trunk mit dem ersten verbinden.

Während des Aufbaus untersuchen Sie das STP und die Entstehung eines Broadcast Sturmes. Zudem konfigurieren Sie SPAN Ports. Dadurch ist es möglich, den Datenfluss von einem Port zu analysieren. Sie werden in diesem Teil verstehen, wie das Trunking von VLANs funktioniert.

In einem Zusatzkapitel werden die Grundlagen des Stacking anhand von geänderten Anforderungen bei Ihrer Firma angewendet. Da die Firma mehr Mitarbeiter und neue Computer hat, muss der Haupt-Switch ersetzt werden. Sie werden mittels spezieller Konfiguration zwei Switches zu einer logischen Einheit verbinden und konfigurieren. Zudem werden Sie sich mögliche Ausfall-Szenarien überlegen und versuchen diese durch den Einsatz von Stacking zu verhindern.

Am Ende werfen Sie im Zusatzkapitel B noch einen Augenmerk auf die Sicherheit des Netzwerkes. Sie werden die MAC-Flooding Technik kennen lernen und mit den passenden Massnahmen unterbinden.

3 Grundkonfiguration (30 min)

Dieses Kapitel beschreibt die Grundkonfiguration von Switches. Sie werden Schritt für Schritt durch die Konfiguration geführt. In diesem Dokument sind alle neuen 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 Switch DLSwitch1

Konfigurieren Sie DLSwitch1 und erstellen Sie eine Grundkonfiguration. Sie umfasst:

- Hostname DLSwitch1
- Passwort "cisco" für privileged EXEC Mode (verwenden Sie den Befehl „secret”)
- Passwort "cisco" für Console-Verbindung
- Passwort "cisco" für Telnet-Verbindung

Kontrollieren Sie die Konfiguration in der Running-Config. Danach sichern Sie die Konfiguration.

```
DLSwitch1#show running-config
Building configuration...

Current configuration : 3245 bytes
!
version 12.2
...✂...
!
hostname DLSwitch1
!
enable secret 5 $1$z73H$wl1TW.KYlh7BKrxN0r9IF1
...✂...
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

```
line vty 5 15
 login
end
```

3.1.1 VLAN

Konfigurieren Sie VLAN 10 für Verkauf und VLAN 20 für Marketing.

- VLAN 10 Verkauf
- VLAN 20 Marketing

Weisen Sie Switchport 0/1 bis 0/6 dem VLAN 10 und Switchport 0/7 bis 0/12 dem VLAN 20 zu. Verwenden Sie den Range-Operator (z.B. ***interface range fastEthernet 0/1 – 6***)

- VLAN 10 FastEthernet-Port 0/1 bis 0/6
- VLAN 20 FastEthernet-Port 0/7 bis 0/12

Aktivieren Sie die Option **spanning-tree portfast** auf den Interfaces 0/1 – 0/12.

Tipp: Befehle zur Konfiguration der VLANs können dem Dokument „Switching Basic“ entnommen werden.

Kontrollieren und vergleichen Sie Ihre Konfiguration. Die Ausgabe des Befehls ***show vlan*** sollte folgendes zeigen.

```
DLSwitch1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
10   Verkauf                          active    Fa0/1, Fa0/2,
                                                Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6
20   Marketing                        active    Fa0/7, Fa0/8,
                                                Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

...✂...
DLSwitch1#
```

3.1.2 VTP

Konfigurieren Sie DLSwitch1 als VTP Server in der Domäne OurFirm.

3.1.3 Verbindung der PCs

Schliessen Sie die PCs gemäss Schema an und konfigurieren Sie die entsprechenden IP-Adressen.

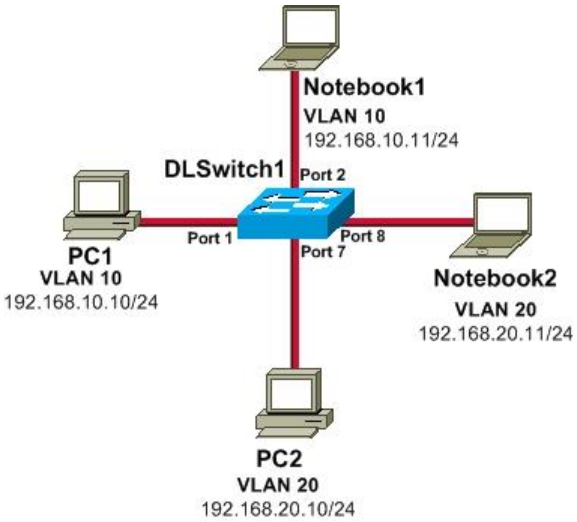

Abb. 1: Versuchsaufbau DLSwitch1

3.1.4 Kontrolle

Testen Sie die Erreichbarkeit innerhalb eines VLANs.

→ Innerhalb eines VLANs sollte alles funktionieren.

Testen Sie die Erreichbarkeit über die VLAN-Grenzen.

→ Dies sollte nicht gehen, da die VLANs momentan noch Grenzen bilden.

3.2 Layer 3 Fähigkeit

Für das Routing von VLANs wird ein Layer 3 fähiges Gerät benötigt. Normale Switches sind reine Layer 2 Geräte. Der Cisco Catalyst 3560 kann auch auf Layer 3, genau wie ein Router, agieren.

3.2.1 Aktivieren

Die Layer 3 Funktionalität ist standardmässig deaktiviert.

Aktivieren Sie auf DLSwitch1 die Layer 3 Funktionen.

```
DLSwitch1#configure terminal
DLSwitch1(config)#ip routing
```

Damit überhaupt etwas zum Routen bekannt ist, müssen Sie den VLANs eine IP-Adresse zuordnen. Konfigurieren Sie pro VLAN ein SVI (Switch Virtual Interface). Das aktiviert die Layer 3 Funktionalität für das angegebene VLAN.

```
DLSwitch1(config)#interface vlan 10
DLSwitch1(config-if)#ip address 192.168.10.1 255.255.255.0
DLSwitch1(config-if)#exit
DLSwitch1(config)#interface vlan 20
DLSwitch1(config-if)#ip address 192.168.20.1 255.255.255.0
DLSwitch1(config-if)#end
```

Konfigurieren Sie die Standardgateways auf den PCs. PCs im VLAN 10 erhalten den Standardgateway 192.168.10.1 und PCs im VLAN 20 den Gateway 192.168.20.1.

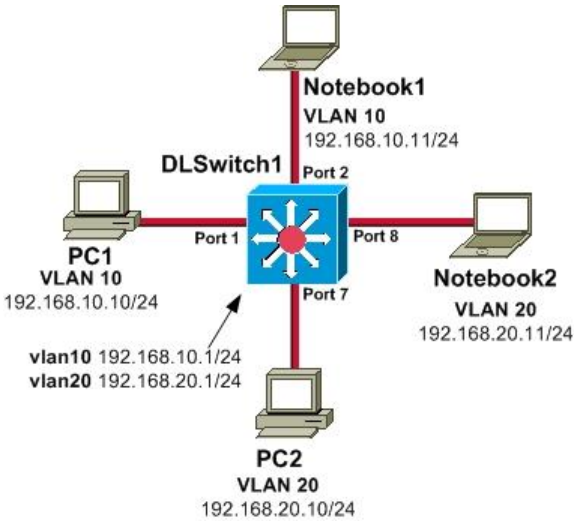

Abb. 2: Layer 3 Switch

Beachten Sie das Symbol eines Multilayer Switches.

3.2.2 Kontrolle

Kontrollieren Sie die Routingtabelle des Switches mit dem Befehl ***show ip route***.
Je nach IOS Version werden auch noch Zeilen mit einem „L“ dargestellt. Diese werden als Local Host Routes bezeichnet und dienen der schnelleren Weiterleitung von Paketen die für den Switch bestimmt sind.

```
DLSwitch1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
DLSwitch1#
```

Pingen Sie PC1 von PC2 an. Jetzt sollte dies ebenfalls funktionieren.

3.2.3 Up-Link zu Router

Ein Layer 3 Switch besitzt viele Funktionen, die ein Router auch hat. Der Hauptvorteil von Switches ist, dass sie ein Vielfaches mehr Ethernet-Ports als Router haben. Dagegen besitzt ein Switch keine seriellen Schnittstellen. Des Weiteren bietet die Catalyst 3560 Series keine NAT-Unterstützung.

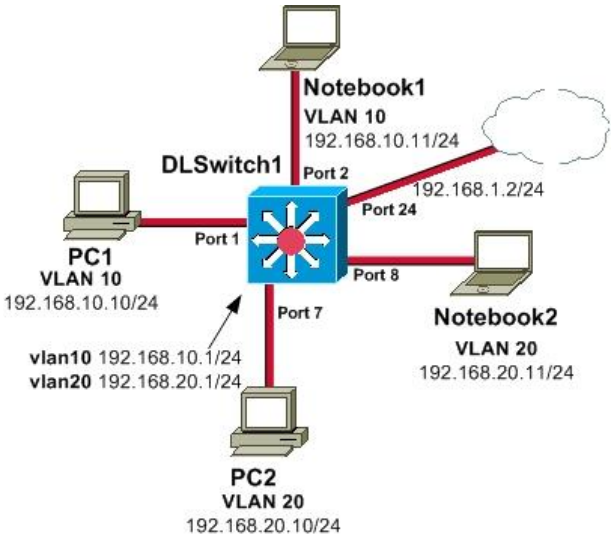

Abb. 3: Uplink zu Router

Konfigurieren Sie Port fastEthernet 0/24 so, dass er für den Uplink zu einem WAN-Router verwendet werden könnte. Versuchen Sie zuerst, einfach eine IP-Adresse zu konfigurieren.

```
DLSwitch1#configure terminal
DLSwitch1(config)#interface fastEthernet 0/24
DLSwitch1(config-if)#ip address 192.168.1.2 255.255.255.0
% IP addresses may not be configured on L2 links.
```

Wie Sie sehen, ist der Port momentan für Layer 2 konfiguriert. Aktivieren Sie Layer 3 für den Port. Dies geschieht durch Deaktivierung der L2-Eigenschaft.

```
DLSwitch1(config-if)#no switchport
01:03:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24,
changed state to down
```

Nun können Sie die IP-Adresse setzen.

```
DLSwitch1(config-if)#ip address 192.168.1.2 255.255.255.0
DLSwitch1(config-if)#exit
```

Setzen Sie gleich noch eine Default-Route auf den Pseudo-Router mit der IP-Adresse 192.168.1.1.

```
DLSwitch1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
DLSwitch1(config)#end
```

Um die Konfiguration zu verifizieren, erstellen sie mit einem **gekreuzten** Ethernetkabel einen Loop vom Port 0/24 zu Port 0/23. Der Loop hat keine Funktion! Er wird lediglich dazu gebraucht, dass das Interface fa0/24 den Status up erhält. Erst dann sind die Einträge in der Routingtabelle ersichtlich.

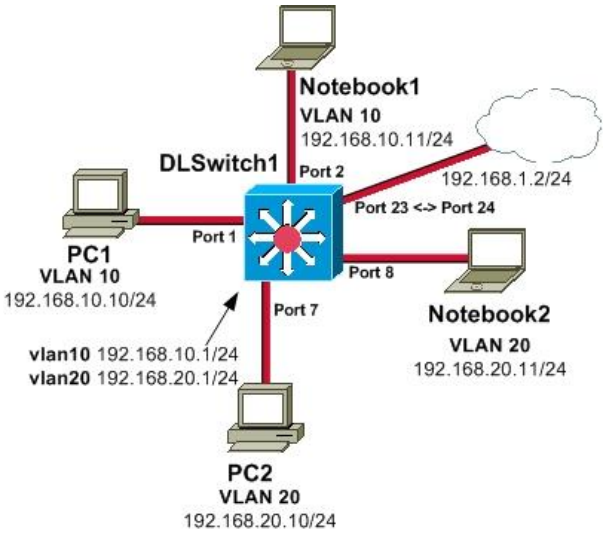

Abb. 4: Port 23⇔ Port 24

Kontrollieren Sie den Status der Interfaces.

```
DLSwitch1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan10                 192.168.10.1    YES NVRAM  up       up
Vlan20                 192.168.20.1    YES NVRAM  up       up
FastEthernet0/1        unassigned      YES unset  up       up
FastEthernet0/2        unassigned      YES unset  up       up
FastEthernet0/3        unassigned      YES unset  down     down
FastEthernet0/4        unassigned      YES unset  down     down
FastEthernet0/5        unassigned      YES unset  down     down
FastEthernet0/6        unassigned      YES unset  down     down
FastEthernet0/7        unassigned      YES unset  up       up
FastEthernet0/8        unassigned      YES unset  up       up
FastEthernet0/9        unassigned      YES unset  down     down
FastEthernet0/10       unassigned      YES unset  down     down
FastEthernet0/11       unassigned      YES unset  down     down
FastEthernet0/12       unassigned      YES unset  down     down
FastEthernet0/13       unassigned      YES unset  down     down
FastEthernet0/14       unassigned      YES unset  down     down
FastEthernet0/15       unassigned      YES unset  down     down
FastEthernet0/16       unassigned      YES unset  down     down
FastEthernet0/17       unassigned      YES unset  down     down
FastEthernet0/18       unassigned      YES unset  down     down
FastEthernet0/19       unassigned      YES unset  down     down
FastEthernet0/20       unassigned      YES unset  down     down
FastEthernet0/21       unassigned      YES unset  down     down
FastEthernet0/22       unassigned      YES unset  down     down
FastEthernet0/23       unassigned      YES manual up       up
FastEthernet0/24       192.168.1.2     YES manual up       up
GigabitEthernet0/1     unassigned      YES unset  down     down
GigabitEthernet0/2     unassigned      YES unset  down     down
DLSwitch1#
```

Kontrollieren Sie die Routingtabelle.

```
DLSwitch1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 192.168.1.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.1.0/24 is directly connected, FastEthernet0/24
S*   0.0.0.0/0 [1/0] via 192.168.1.1
DLSwitch1#
```

Haben Sie die Konfiguration bereits einmal gesichert? Sichern Sie die Konfiguration immer nach erfolgreichen Tests!

3.3 DLSwitch2

Erweitern Sie ihr Netzwerk um einen zusätzlichen Switch.

Konfigurieren Sie DLSwitch2 und erstellen Sie eine Grundkonfiguration. Sie umfasst:

- Hostname DLSwitch2
- Passwort "cisco" für privileged EXEC Mode (verwenden Sie den Befehl “secret“)
- Passwort "cisco" für Console-Verbindung
- Passwort "cisco" für Telnet-Verbindung

VTP
Konfigurieren Sie DLSwitch2 als VTP Client in der Domäne OurFirm.

Die richtigen VLAN-Namen erscheinen erst nach dem Verbinden der beiden Switches!

3.4 Verbindung DLSwitch1 – DLSwitch2

Erstellen Sie einen Trunk zwischen DLSwitch1 und DLSwitch2. Verwenden Sie dazu den Gigabit-Ethernetport Gi0/1. Erstellen Sie die Verbindung mit einer Glasfaserverbindung (fibre optic cable).

Abb. 5: Trunk

Konfigurieren Sie auf DLSwitch1 den Port gi0/1 als Trunk. Dies geschieht im Interface-Konfigurationsmodus des Interfaces mit dem Befehl ***switchport mode trunk***.

```
DLSwitch1#configure terminal
DLSwitch1(config)#interface gigabitEthernet 0/1
```

Bevor Sie den Trunk definieren können, müssen Sie die Encapsulation festlegen. Dieser Switch beherrscht neben dot1q auch ISL. Verwenden Sie dot1q!

```
DLSwitch1(config-if)#switchport trunk encapsulation replicate
DLSwitch1(config-if)#switchport mode trunk
DLSwitch1(config-if)#end
```

Konfigurieren Sie auf DLSwitch2 analog den Port gi0/1 als Trunk. Verwenden Sie wieder dot1q als Trunk-Encapsulation.

3.4.1 VLAN

Weisen Sie auf DLSwitch2 Switchport 0/1 bis 0/6 dem VLAN 10 zu. Switchport 0/7 bis 0/12 gehören zu VLAN 20. Verwenden Sie den Range-Operator (z.B. ***interface range fastEthernet 0/1 – 6***)

- VLAN 10 FastEthernet-Port 0/1 bis 0/6
- VLAN 20 FastEthernet-Port 0/7 bis 0/12

Die VLANs müssen Sie nicht benennen, da dies von VTP Server gelernt wird!

Aktivieren Sie die Option **spanning-tree portfast** auf den Interfaces 0/1 – 0/12.

Kontrollieren und vergleichen Sie Ihre Konfiguration. Die Ausgabe des Befehls ***show vlan*** sollte folgendes zeigen.

```
DLSwitch2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/2
10   VLAN0010                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6
20   VLAN0020                         active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

...✂...
DLSwitch1#
```

3.4.2 Kontrolle

Schliessen Sie die PCs gemäss Schema an.

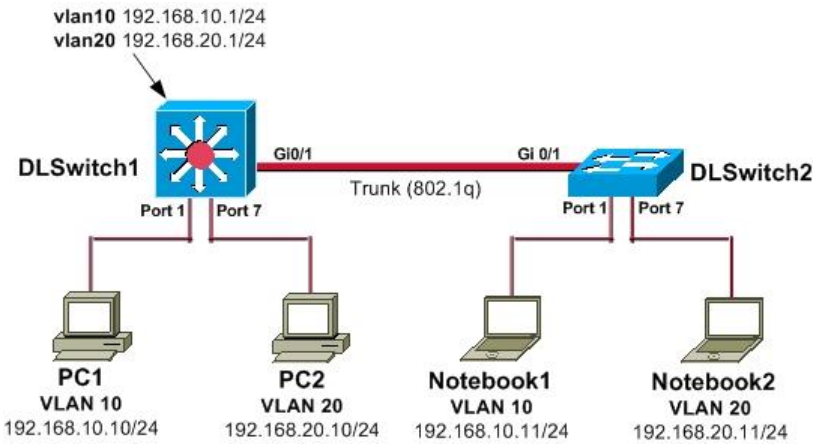

Abb. 6: Versuchsaufbau

Pingen Sie die PCs gegenseitig an. Testen Sie die Kommunikation innerhalb des gleichen VLANs und VLAN übergreifend.

3.5 Kontrollfragen

- Können Sie ein paar Unterschiede zwischen Routern und Switches aufzählen?
- Warum ist im Kapitel 3.1.1 VLAN der Port Gi 0/1 nicht mehr im Output des ***show vlan***-Befehls?
- Warum müssen die VLANs auf DLSwitch2 nicht benannt werden?

4 STP – Spanning Tree Protocol (15 min)

Bei einem grossen Netzwerk mit mehreren Switches ist eine gewisse Redundanz gewünscht. Ein Ausfall eines Switches hätte so keine grossen Folgen. Jedoch darf es keine Loops geben. Dies würde zu einem sogenannten Broadcast Sturm führen. Genauso einen Broadcast Sturm werden Sie jetzt erzeugen. Einfachheitshalber erstellen Sie einen Loop auf nur einem Switch.

Erstellen Sie den Loop. Dazu verbinden Sie auf DLSwitch1 den Port 0/5 mit dem Port 0/6. Verwenden Sie dazu ein **gekreuztes** Ethernetkabel.

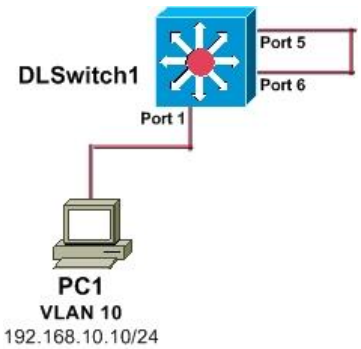

Abb. 7: Versuchsaufbau Loop (Ausschnitt)

Sichern Sie vorgängig Ihre Konfiguration!

Kontrollfrage
Warum funktioniert hier das Prinzip mit dem TTL-Eintrag im IP-Paket (in unserem Fall ein Ping-Paket) nicht?

4.1 STP deaktivieren

Vor der Deaktivierung führen Sie kurz einen Broadcast-Ping durch. Pingen Sie von PC1 die Broadcast-Adresse einmal an. Sie sehen, alle LEDs verhalten sich ruhig.

```
c:\>ping -n 1 192.168.10.255
Ping wird ausgeführt für 192.168.10.255 mit 32 Bytes Daten:
Antwort von 192.168.10.1: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.10.255:
    Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
c:\>
```

Beachten Sie, dass je nach Firewalleinstellungen keine Rückmeldung erfolgt.

Deaktivieren Sie nun das Spanning Tree Protokoll im VLAN 10.

```
DLSwitch1#configure terminal
DLSwitch1(config)#no spanning-tree vlan 10
DLSwitch1(config)#end
```

4.2 Broadcast-Sturm

Starten Sie auf PC1 eine Sniffingsoftware (z. B. Wireshark).

Unterbrechen Sie kurz den Loop und schicken Sie einen beliebigen Ping.

Kontrollieren Sie diesen mit der Sniffingsoftware. Nun können Sie erneut den Loop erstellen, in dem Sie das Kabel wieder einstecken.

Pingen Sie von PC1 nochmals die Broadcast-Adresse einmal an. Beobachten Sie den Sniffer und die LEDs des Switchs.

```
c:\>ping -n 1 192.168.10.255
```

Versuchen Sie irgendein Host zu pingen! Testen Sie auch das VLAN20 und das InterVLAN-Routing.

Kontrollieren Sie nun die Prozessorauslastung des Switchs.

```
DLSwitch1#show processes cpu
CPU utilization for five seconds: 97%/22%; one minute: 90%; five minutes: 21%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0       907          0  0.00%  0.00%  0.00%   0 Load Meter
...✂...
DLSwitch1#
```

4.3 STP aktivieren

Aktivieren Sie das Spanning-Tree auf VLAN 10 wieder.

```
DLSwitch1#configure terminal
DLSwitch1(config)#spanning-tree vlan 10
```

```
DLSwitch1(config)#end
```

Was bei diesem Schritt passiert ist, ist folgendes:

Der Switch kontrolliert, ob die aktuelle Verkabelung zu einem Loop führt. Sollte dies zutreffen, wird der Link (ein Switchport) für die Datenübertragung deaktiviert um den Loop zu vermeiden.

Welcher Port blockiert wurde, kann überprüft werden:

```
DLSwitch1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
...✂...
Interface        Port ID                     Designated                Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID            Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         4 32778 000b.be6b.0080 128.3
Fa0/5            128.5           19 FWD         4 32778 000b.be6b.0080 128.4
Fa0/6            128.6           19 BLK         0 32778 000b.be6a.bb00 128.26
Gi0/1            128.25           4 FWD         0 32778 000b.be6a.bb00 128.25
DLSwitch1#
```

Legende: (Fwd=Forwarding, BLK=Blocked, LIS=Listen)

Kontrollfrage
Überlegen Sie sich, wieso es zu einem Broadcast Sturm kam! Ideen protokollieren!

5 SPAN-Port (15 min)

Switches haben den Vorteil, dass es kaum zu Kollisionen kommt. Vergleicht man einen Switch mit einem Hub, so stört die Kommunikation zwischen zwei PCs keine anderen (Kollisionen). Jeder Link bildet ein Mikrosegment welches 100% kollisionsfrei ist (bei Full-Duplex).

Hubs dagegen machen Administratoren das Leben einfacher, wenn sie kontrollieren wollen, was für Datenverkehr überhaupt im Netzwerk vorhanden ist. Alle Daten, welche über einen Port an den Hub gelangen, werden auf alle anderen Ports propagiert.
Bei Switches ist es aufwendiger den Datenverkehr zu kontrollieren. Ein Switch muss speziell konfiguriert werden, damit man den Netzwerkverkehr aufzeichnen kann. Um dies zu erreichen, muss man die Technologie Switchport Analyzer (oder kurz SPAN) einsetzen.

5.1 Konfiguration DLSwitch1

5.1.1 Trunk

Konfigurieren Sie auf DLSwitch1 einen SPAN-Port so, dass er den Verkehr vom Gigabit-Ethernet 0/1 ebenfalls an den Port FastEthernet 0/19 sendet.

```
DLSwitch1#configure terminal
DLSwitch1(config)#monitor session 1 source interface Gi0/1
DLSwitch1(config)#monitor session 1 destination interface Fa0/19 encapsulation
replicate
DLSwitch1(config)#end
```

Schliessen Sie die PCs gemäss Schema an. Verschieben Sie PC1 von Port 1 auf Port 19.

Starten Sie (falls möglich) den PC1 mit Linux Ubuntu, da unter Windows nicht alle Pakete (802.1q) in Wireshark vollständig angezeigt werden.

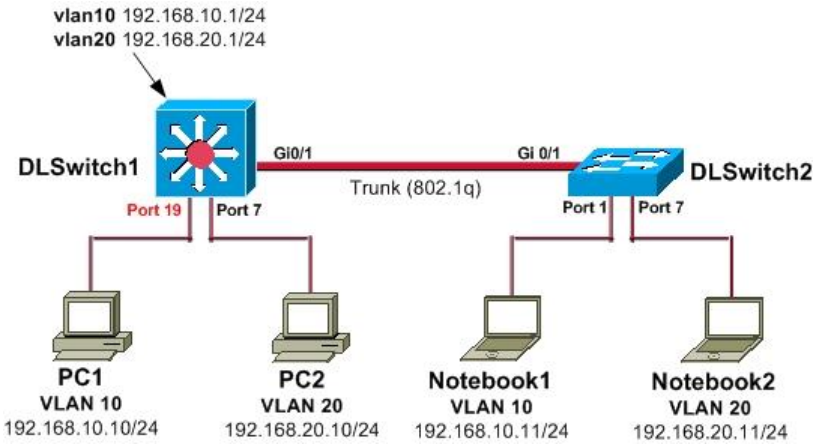

Abb. 8: Versuchsaufbau SPAN Session 1

Starten Sie auf PC1 Wireshark (unter Linux als root) im Promiscuous-Mode. Im Promiscuous-Mode werden nicht nur die an den Computer adressierten Pakete angezeigt sondern alle im Netzwerk sichtbaren Pakete.

Pingen Sie von Notebook2 den PC2 im VLAN20 an.

Analysieren Sie die aufgezeichneten Pakete. Achten Sie vor allem auf das Trunking-Protokoll! Auf welchem Layer befindet sich 802.1q und wo werden die VLAN-Informationen gesendet?

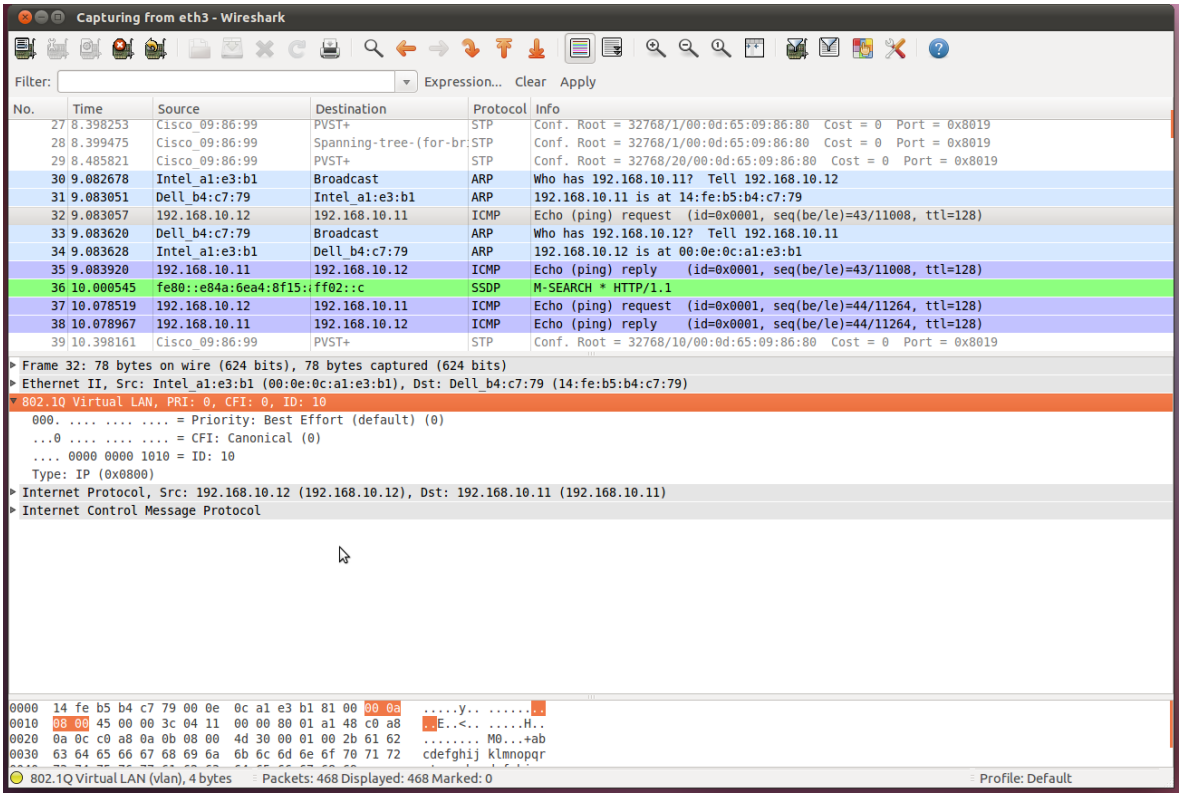

Abb. 9: Trunking-Protokoll 802.1q

Ein SPAN-Port verlangsamt das Netzwerk nicht.

5.1.2 Switchport

Konfigurieren Sie eine zweite Monitor Session. Diesmal soll jeder Verkehr, welcher zum Host am Port FastEthernet 0/7 angeschlossen ist, analysiert werden (z.B. durch ein IPS). Es interessiert Sie nur die Daten vom Netzwerk zum PC!

```
DLSwitch1#configure terminal
DLSwitch1(config)#monitor session 2 source interface fa0/7 tx
DLSwitch1(config)#monitor session 2 destination interface fa0/20
DLSwitch1(config)#end
```

Kontrollieren Sie die zweite Monitor Session. Verbinden Sie PC1 mit Port 0/20 und starten Sie die Sniffersoftware. Pingen Sie von PC2 das Notebook2 an. Wenn alles richtig konfiguriert und verkabelt ist, so sehen Sie auf dem Sniffer am Port fa 0/20 nur die Echo reply Pakete!

Die Richtung von rx (empfangen) oder tx (senden) ist aus der Sicht des Switchports und nicht vom Client.

Neben Trunks und einzelnen Ports können auch mehrere Ports oder ganze VLANs mit einem SPAN-Port analysiert werden.

5.2 Kontrollfragen

- Was sind Vor- und Nachteile zwischen Hub und Switch?
- Verlangsamt SPAN einen Switch?

6 Zusätzliches Netzwerk hinzufügen (15 min)

Die Abteilung Einkauf wechselt in Ihrem Unternehmen den Standort und ist neu in den gleichen Büros wie die Abteilungen Verkauf und Marketing. Sie werden beauftragt, die Konfiguration der bestehenden Switches anzupassen, damit die neuen Computer korrekt an das Netzwerk angeschlossen werden können.

Ihre Aufgabe ist es, ein neues VLAN für den Einkauf zu erstellen. Alle Einkäufer werden auf den DLSwitch2 Port 0/13 bis 0/18 an das Netzwerk angeschlossen. Natürlich sollten die Einkäufer auf die PCs von Verkauf und Marketing zugreifen können.

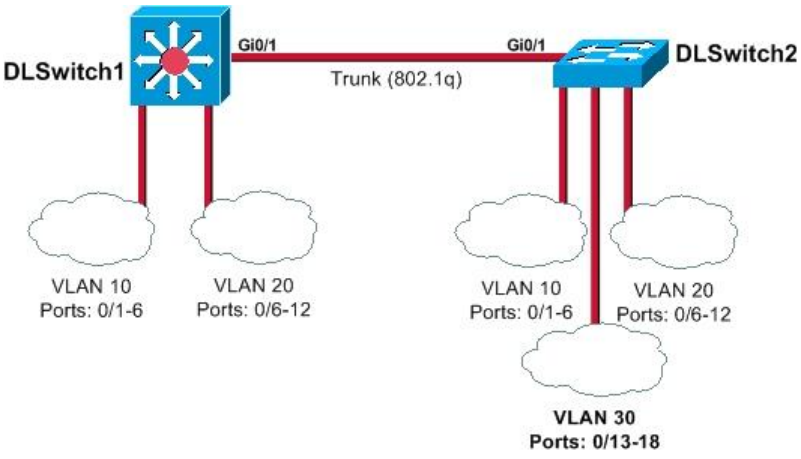

Abb. 10: Neues VLAN 30

Konfigurieren und testen Sie die neue Anforderung. Beachten Sie, dass PCs von VLAN 30 auch PCs von anderen VLANs erreichen.

- VLAN 30: Name: Einkauf | IP-Segment: 192.168.30.0/24
- Default Gateway: 192.168.30.1

Verkabeln Sie die PCs und vergeben Sie die IP-Adressen gemäss Schema. Passen Sie wo notwendig den Defaultgateway an.

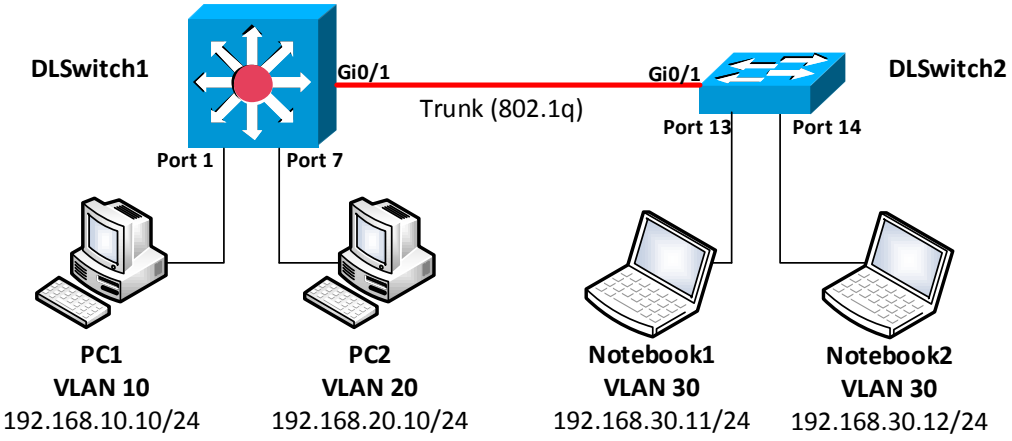

Abb. 11: Versuchsaufbau VLAN30

Versuchen Sie zuerst die Aufgabe selbstständig zu lösen. Schauen Sie erst zuletzt in die Lösung im nächsten Abschnitt!

6.1 Lösung

DLSwitch1: (Nur der VTP-Server kann neue VLANs erstellen!)

```
DLSwitch1#configure terminal
DLSwitch1(config)#vlan 30
DLSwitch1(config-vlan)#name Einkauf
DLSwitch1(config-vlan)#exit
DLSwitch1(config)#interface vlan 30
DLSwitch1(config-if)#ip address 192.168.30.1 255.255.255.0
DLSwitch1(config-if)#end
DLSwitch1#
```

DLSwitch2:

```
DLSwitch2#configure terminal
DLSwitch2(config)#interface range fastEthernet 0/13 -18
DLSwitch2(config-if-range)#switchport access vlan 30
DLSwitch2(config-if-range)#spanning-tree portfast
DLSwitch2(config-if-range)#end
DLSwitch2#
```

7 Stacking (Zusatzkapitel A) (30 min)

7.1 Aufgabenstellung

Durch einen Umzug ihrer Firma haben sich die Anforderungen geändert. Da nun alle Clients auf einem Stockwerk sind und die Firma neu noch zusätzliche Mitarbeiter angestellt hat, überzeugen Sie ihren Vorgesetzten zur Anschaffung neuer Switches. Um die Verwaltungsmöglichkeiten zu vereinfachen und einen einfachen Ausbau der Infrastruktur zu ermöglichen, entscheiden Sie sich für zwei Switches vom Typ Cisco Catalyst 3750 und verbinden diese mit der Cisco Stackwise Technologie zu einer logischen Einheit.

In diesem Versuch werden Sie eine einfache Stacking-Umgebung realisieren und die Reaktion bei einem möglichen Ausfall prüfen.

7.2 Versuchsaufbau

Für diesen Versuch brauchen Sie zwei Modelle vom Typ Cisco Catalyst 3750. Prüfen Sie bitte, dass noch keine Konfiguration auf den Geräten ist, und verkabeln Sie den ersten Switch gemäss Schema mit den Client-Computern.

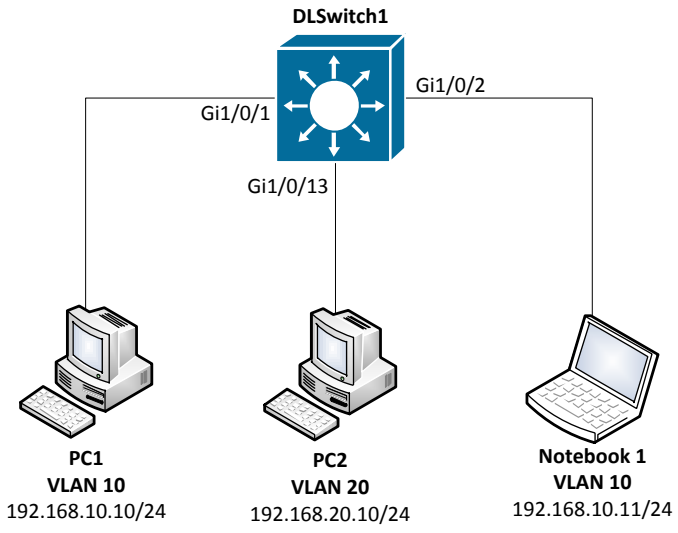

Abb. 12: Vorbereitungen Stacking-Versuch

Laden Sie für diesen Versuch die Konfiguration aus dem Anhang (DLSwitch1 Stacking) auf den Switch. **Achtung!** Vor dem Laden der Einstellungen unbedingt die Switch und **Stackwise** Konfigurationen löschen. Befolgen Sie dazu die **komplette** Anleitung im Kapitel 10 Zurücksetzen der Geräte zu Switches.

Vergessen Sie nicht die IP-Adressen auf den Computern zu konfigurieren!

7.3 Verbindungen prüfen

Durch das Laden der Konfiguration wurde auf dem Switch eine Konfiguration von VLANs geladen. Das VLAN 10 (Verkauf) ist auf den Ports 1 bis 12 verfügbar, das VLAN 20 (Marketing) auf den Ports 13 bis 24.

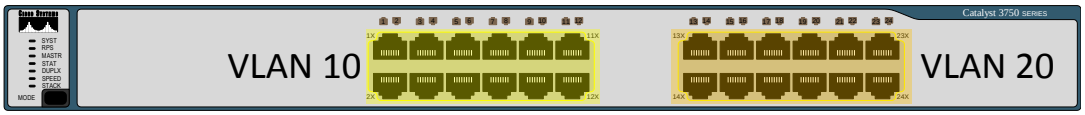

Abb. 13: VLAN Zuordnung Switchports

Pingen Sie von PC1 das Notebook 1. Diese Verbindung sollte funktionieren.

Pingen Sie von PC2 den PC1. Auch diese Verbindung sollte funktionieren, da über die Konfiguration neben den VLANs auch ein InterVLAN-Routing konfiguriert wurde.

7.4 Konfiguration des Stacking

Es soll nun ein zweiter Switch mit dem bestehenden Gerät zu einer logischen Einheit zusammengefasst werden. Damit kann man die Anzahl der Ports verdoppeln. Überprüfen Sie, dass die Switches die gleiche Firmware-Version installiert haben.

DLSwitch1:

```
DLSwitch1#show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE5,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 09-Feb-12 18:59 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000
```

Ist dies der Fall, können die Switches mit zwei Cisco Stackwise-Kabeln verbunden werden. Schalten Sie dazu den noch nicht konfigurierten zusätzlichen Switch aus. Der DLSwitch1 kann normal weiterlaufen.

Verbinden Sie die Switches gemäss folgender Grafik:

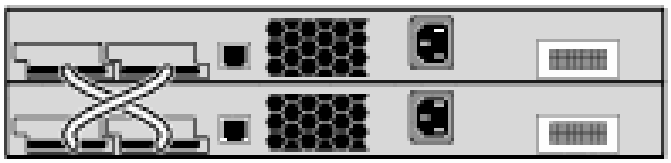

Abb. 14: Quelle: Creation and Management of Catalyst 3750 Switch (cisco.com, Doc-ID: 71925)

Starten Sie anschliessend den Switch 2 und lesen Sie die Terminalausgabe von Switch 1und 2 mit. Sie werden feststellen, dass der erste Switch, den zweiten Switch automatisch erkennt und eine Master- / Member-Beziehung ausarbeitet.

DLSwitch1:

```
DLSwitch1#
*Mar  1 01:10:11.248: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has
changed to state UP
```

```
*Mar  1 01:10:11.248: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has
changed to state UP
DLSwitch1#
```

Beachten Sie auch die Konsolenausgabe auf dem 2. Switch während dem Boot-Vorgang!

DLSwitch1:

```
Waiting for Stack Master Election...
POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Stack Port Loopback Tests : Begin
POST: PortASIC Stack Port Loopback Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

Election Complete
Switch 2 booting as Member, Switch 1 elected Master
HCOMP: Compatibility check PASSED
Waiting for feature sync....
Waiting for Port download...Complete
Stack Master is ready
```

Der Stack-Master wird nach den folgenden Kriterien ausgewählt:

1. Der Switch mit der höchsten Stackmember-Priorität
2. Der Switch mit einer bereits bestehenden Konfiguration (in diesem Versuch der Fall)
3. Der Switch mit der höheren Hardware- / Software-Priorität
4. Der Switch mit der längsten Uptime
5. Der Switch mit der kleinsten MAC-Adresse

Nachdem beide Switches laufen, werden Sie auf der Konsole des Switch 2 feststellen, wie die Konfiguration (z.B. der Hostname) von DLSwitch1 automatisch übernommen wurde.

Da die beiden Switches eine logische Einheit bilden, können Sie über die Konsolen-Ports beider Switches die Konfiguration des Gesamtsystems anpassen.

Die Stack-Ports und die Stack-Neighbours können über die folgenden Befehle geprüft werden:

DLSwitch1:

```
DLSwitch1#show switch stack-ports
  Switch #    Port 1       Port 2
  --------    ------       ------
    1           Ok           Ok
    2           Ok           Ok

DLSwitch1#show switch neighbors
  Switch #    Port 1       Port 2
  --------    ------       ------
      1         2            2
      2         1            1
DLSwitch1#
```

7.5 Simulation des Master-Ausfalls

Stacking hat unter anderem den Vorteil, dass bei einem Systemausfall die ganze Konfiguration weiterhin verfügbar ist und nur das betroffene Gerät ausfällt. Dabei fallen nur die Verbindungen mit dem betroffenen Switch aus. Alle Verbindungen zu den anderen Switches im Stack laufen unterbruchsfrei weiter. Bei einem Ausfall des Masters wird automatisch die Master-Funktion übertragen.

Simulieren Sie einen Ausfall des Switch 1, indem Sie den Strom abstellen. Beobachten Sie die Ereignisse über die Konsolenverbindung zum Switch 2.

Starten Sie anschliessend den Switch 1 wieder und beachten Sie dabei, wie sich die Master-Einteilung verhält.

7.6 Konfiguration der VLANs

Durch das Stacking wurden auf diesem einen logischen Switch die Anzahl Ports verdoppelt. Prüfen Sie die Ports:

DLSwitch1:

```
DLSwitch1#show interface status
```

Beachten Sie dabei, dass nun auch die Ports des hinzugefügten Switches angezeigt werden. Die Ports haben nun den Präfixe 1 und 2 für Switch 1 und Switch 2 (1/0/1 für Switchport Nr. 1 auf Switch 1 und 2/0/1 für Switchport Nr. 1 auf Switch 2).

Es sollen nun den bestehenden VLANs (Verkauf, Marketing) zusätzlich die Ports auf der zweiten Switch-Einheit zugeordnet werden.

DLSwitch1:

```
DLSwitch1(config)#interface range gigabitEthernet 2/0/13 - 24
DLSwitch1(config-if-range)#switchport access vlan 20
DLSwitch1(config-if-range)#exit
DLSwitch1(config)#interface range gigabitEthernet 2/0/1 - 12
DLSwitch1(config-if-range)#switchport access vlan 10
DLSwitch1(config-if-range)#exit
```

Schliessen Sie die Computer nun nach folgendem Schema an:

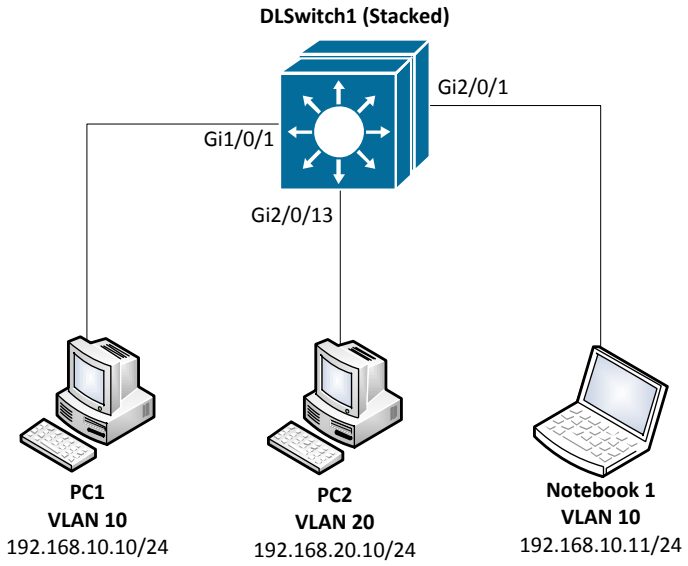

Abb. 15: Anschlussschema Kapitel 7.6

Versuchen Sie, die Computer gegenseitig zu pingen.

8 Security (Zusatzkapitel B) (30 min)

Bei diesem Versuch müssen Sie unbedingt beachten, dass es mit dem Cisco 3750 oder dem Cisco 3650 nicht möglich ist die Mac-Tabelle zu füllen. (40 bleiben immer frei), mit dem Cisco 3550 klappt es aber. Nehmen Sie deshalb einen Cisco 3550.

8.1 MAC-Flooding

Menschen mit weniger guten Absichten würden gerne einen Blick auf den Datenverkehr der anderen im Netzwerk haben. Jedoch haben diese Leute oft keinen administrativen Zugriff auf den Switch um sich SPAN-Ports einzurichten. Deshalb müssen sie andere Methoden entwickeln um an diese Daten zu kommen.

Durch MAC-Flooding kann die Funktion eines Switches so weit beeinträchtigt werden, dass er wie an Hub arbeitet. Die VLAN-Grenzen existieren jedoch immer noch!

8.1.1 Funktionsweise

Ein Switch führt eine Tabelle, welche die Zugehörigkeit der MAC-Adresse auf Switch-Ports zu finden ist. Dadurch kann der Switch die Frames genau und meistens auf einen Port beschränkt weiterleiten (Ausnahme z.B. Multicast).

Wie alles, hat diese Tabelle nicht unendlich viel Platz für die Einträge.

Kontrollieren Sie die Mac-Adresstabelle von DLSwitch1. Wie viele MAC-Adressen kann der Switch speichern?

```
DLSwitch1#show mac address-table count
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 3
Static  Address Count  : 0
Total Mac Addresses    : 3
```

```
Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2

Mac Entries for Vlan 20:
---------------------------
Dynamic Address Count  : 3
Static  Address Count  : 0
Total Mac Addresses    : 3

Total Mac Address Space Available: 5080
DLSwitch1#
```

Angenommen, die MAC-Adresstabelle ist bis auf den letzten Platz voll und ein neuer Host kommt dazu. Der Switch hat keine Möglichkeit die Information abzuspeichern bzw. kann er sich nicht mehr merken an welchem Port der Host mit der jeweiliger MAC-Adresse zu finden ist. Damit der Host trotzdem Antworten erhält, werden die Antwort-Pakete an alle anderen Switch-Ports im VLAN gesendet. Der Switch arbeitet innerhalb der VLANs wie ein Hub.

8.1.2 Das Tool: Macof

Macof ist ein UNIX-basiertes Programm, welches genau diesen Angriffspunkt ausnützt.

Booten Sie PC2 mit dem Linux Ubuntu.

Schliessen Sie die PCs und Notebooks gemäss Schema an und konfigurieren Sie die entsprechenden IP-Adressen und VLAN-Zuweisungen.

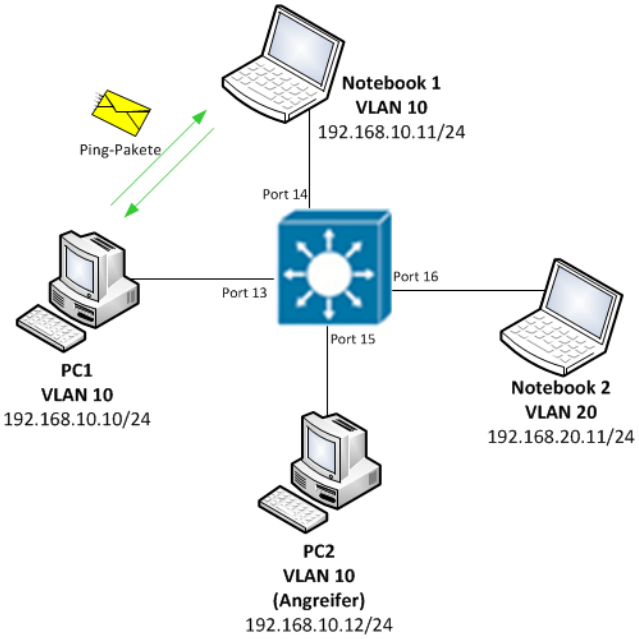

Abb. 16: Versuchsaufbau Macof

Starten Sie auf allen Geräten Wireshark. Setzen Sie den Capture Filter auf **icmp** und sniffen Sie im Promiscuous Mode.

Pingen Sie von PC1 das Notebook1 und umgekehrt. Auf welchen Geräten sehen Sie die Pakete im Sniffer? Wieso sehen Sie die Pakete nur auf den am Ping beteiligten Geräten?

Stoppen Sie alle laufenden Pings!

Starten Sie auf PC2 eine Konsole und geben Sie folgendes ein:

```
cisco@[ubuntu]#sudo -s
root@[ubuntu]#macof –i eth[x]
```

Nun wird die MAC-Adresstabelle des Switches gefüllt.

Kontrollieren Sie auf dem DLSwitch1, wie lange es geht, bis die MAC-Adresstabelle voll ist.

```
DLSwitch1#clear mac address-table dynamic
DLSwitch1#show mac address-table count
```

Pingen Sie von PC1 das Notebook1 an. Sehen Sie die Pakete nun im Sniffer auf dem Angreifer-PC2? Was hat sich im Vergleich zum vorherigen Ping-Versuch verändert?

Sehen Sie die Pakete im Sniffer auf dem Notebook2 und falls nein, wieso sehen Sie diese nicht?

Hinweis: Falls Sie die Ping-Pakete auf dem Angreifer-PC2 gar nicht, oder jeweils nur in eine Richtung sehen, sollten Sie nochmals die MAC-Adresstabelle löschen.

```
DLSwitch1#clear mac address-table dynamic
```

Wie Sie sehen können, kann der Angreifer (PC2) bei einem Ping von PC1 zum Notebook1 die Pakete mitverfolgen, wenn die MAC-Adresstabelle geflutet wurde. Bedingung ist, dass in der MAC-Adresstabelle auf DLSwitch1 keine Einträge mehr von PC1 und Noteboo1 vorhanden sind. (Ansonsten muss gewartet werden, bis diese auslaufen, oder die MAC-Adresstabelle manuell gelöscht werden).

Auf Notebook2 können jedoch keine Pakete mitverfolgt werden, da sich der Notebook2 im VLAN 20 und nicht wie die anderen Geräte im VLAN 10 befindet. Die VLAN Grenze hält also der Attacke stand. Da sich aber alle VLANs den Speicherplatz für die MAC-Adresstabelle teilen, können auch in den anderen VLANs aufgrund des Platzmangels keine neuen MAC-Adresseinträge mehr angelegt werden. Somit werden allenfalls auch in anderen VLANs Pakete über alle Ports verteilt.

Der Zustand, in dem der Switch aufgrund der gefluteten MAC-Adresstabelle wie ein Hub agiert, wird als `“Fail Open Mode“ bezeichnet. Der Switch versendet in diesem Zustand Pakete über alle Ports (ausser den Ursprungsport), statt wie im normalen Zustand lediglich über den korrekten Port.

Stoppen Sie Macof! Nun geht es eine Weile, bis die gespeicherten Dummy-MAC-Adressen gelöscht werden (Timeout: 300 Sekunden). Beschleunigen können Sie dies, wenn Sie manuell die MAC-Adresstabelle löschen.

```
DLSwitch1#clear mac address-table dynamic
```

Macof funktioniert auch über den Trunk. DLSwitch2 hat ebenfalls die MAC-Adresstabelle gefüllt.

Die nachfolgende Tabelle dient als zusammenfassende Übersicht, an welche Clients/Switchports die Pakete in welchem Zustand versendet werden.

Zustand	Ping-Pakete sichtbar auf PC1	NB1	PC2	NB2	Begründung
Normal	Ja	Ja	Nein	Nein	Ping-Pakete werden nur an Ports der beteiligten Geräte versendet.
MAC Flooding Attack	Ja	Ja	Ja	Nein	Ping-Pakete werden über alle Ports im selben VLAN versendet. Deshalb sieht auch PC2 die Pakete. NB2 befindet sich in einem anderen VLAN und sieht die Pakete nicht.

8.2 PortSecurity

Das MAC-Flooding ist eine bekannte Technik, deshalb wurden gleich auf den Switchs Funktionen implementiert, welche dies aktiv verhindern.

8.2.1 Aktivieren

Aktivieren Sie auf DLSwitch1 die Port-Security auf den Ports fa0/7 bis fa0/12.

```
DLSwitch1#configure terminal
DLSwitch1(config)#interface range fastEthernet 0/7 - 12
DLSwitch1(config-if-range)#switchport mode access
DLSwitch1(config-if-range)#switchport port-security
DLSwitch1(config-if-range)#end
```

Kontrollieren Sie die Konfiguration:

```
DLSwitch1#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
--------------------------------------------------------------------------------
     Fa0/7           1               0             0               Shutdown
     Fa0/8           1               0             0               Shutdown
     Fa0/9           1               0             0               Shutdown
     Fa0/10          1               0             0               Shutdown
     Fa0/11          1               0             0               Shutdown
     Fa0/12          1               0             0               Shutdown
--------------------------------------------------------------------------------
Total Addresses in System : 1
Max Addresses limit in System : 128
DLSwitch1#
```

Die Schutzfunktion ist standardmässig auf Shutdown. Insgesamt gibt es drei Methoden:

Protect *– when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until secure MAC addresses are manually removed from the port's address table to create a free slot.*

Restrict *– a port security violation causes a trap notification to be sent to the SNMP network management station.*

Shutdown *– a port security violation causes the interface to shut down immediately and send an SNMP trap notification. Once shut down, the interface must be manually re-enabled by using the no shutdown interface configuration command. This is the default mode.*

By default, port security is disabled on a port. Port security defaults are a maximum of 128 secure MAC addresses per port, and shutdown on security violation.

[Quelle: Curriculum CCNP 3]

8.2.2 Testen

Testen Sie nun nochmals, ob Sie auf dem DLSwitch1 die MAC-Adresstabelle füllen können. Beachten Sie, momentan sind nur die Ports 0/7 bis 0/12 geschützt!

Kurz nach dem erneuten Starten von macof erscheint folgender Hinweis auf der Konsole:

```
01:31:02: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/9, putting
Fa0/9 in err-disable state
01:31:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed
state to down
```

Um den Port wieder zu aktiveren, müssen Sie in den Interface-Konfigurationsmodus wechseln, den Port herunterfahren und wieder hochfahren.

```
DLSwitch1#configure terminal
DLSwitch1(config)#interface fastEthernet 0/9
DLSwitch1(config-if)#shutdown
DLSwitch1(config-if)#no shutdown
DLSwitch1(config-if)#end
```

Testen Sie die Methode port-security violation protect. Kontrollieren Sie die Zustände der Ports mit folgenden Show-Befehlen:

```
DLSwitch1#show port-security
DLSwitch1#show port-security address
DLSwitch1#show ip interface brief
```

Konfigurieren Sie ein Netzwerk das sicher gegenüber MAC-Flooding ist. Testen Sie ihr Netzwerk!

9 Challenge

Sie haben vor sich zwei Layer 3 Switches, jedoch die Layer 3 Funktionalitäten sind nur auf DLSwitch1 konfiguriert.

Überlegen Sie sich, ob es Sinn macht, wenn der DLSwitch2 ebenfalls routen würde (Geschwindigkeit, Netzwerkbelastung, Redundanz).

Gibt es für die PCs ebenfalls Änderungen? Wenn ja, welche?

Wo sind die Rahmenbedingungen ihrer Lösung.

Überlegen Sie sich, was Hot Standby Routingprotokoll zur Effektivität beitragen würde (Siehe Versuch IP Routing Advanced).

Versuchen Sie, Ihre Lösung zu implementieren.

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***
Switch Startup Konfiguration	***write erase***
Switch VLan Konfigurationen	***delete flash:vlan.dat***

Das Zurücksetzen der Switches ist noch nicht komplett, da das Stacking immer noch vorhanden ist.

Prozedur:

1. Zuerst wie beschrieben alle Konfigurationen löschen.
2. Den als letzter hinzugefügte Switch (Switch 2) ausschalten und die StackWise Kabel entfernen.
3. Dann bei Switch 1:
    a. ***conf t***
    b. ***no switch 2 provision***
    c. ***end***
4. Switch 2 einschalten und:
    a. ***conf t***
    b. ***switch 2 renumber 1***
    c. ***end***
    d. ***reload***

11 Anhang A – Theorie

SPAN

Hier finden Sie die Theorie zu diesem Versuch. Weiter werden in im Folgenden die Fragen aus dem Kapitel 1.1 Fragen zur Theorie beantwortet.

Was ist SPAN und warum ist sie nötig? Die Funktion SPAN wurde wegen eines grundlegenden Unterschieds zwischen Switchen und Hubs eingeführt. Wenn ein Hub ein Paket an einem Port empfängt, sendet er eine Kopie dieses Pakets zu allen Ports ausser zu dem, auf dem er es empfangen hat.

Nach dem ein Switch gebootet hat, erstellt er eine Layer 2 forwarding Tabelle, aufgrund der Source MAC Adressen, der verschiedenen Pakete, die er erhält. Dank dieser Tabelle, kann der Switch Pakete gezielt verschicken, anstatt an alle Ports.

SPAN sorgt dafür, dass eine Kopie der gewünschten Pakete zusätzlich an einen bestimmten Port geschickt wird. Dadurch kann das Netzwerk trotz eines Switches überwacht werden.

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 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.