

HÖHERE TECHNISCHE BUNDESLEHRANSTALT HOLLABRUNN

Höhere Abteilung für Elektronik – Technische Informatik

Klasse/ Jahrgang: 5BHEL	Gruppe: 4b	Übungsleiter: Prof. Stoll
Übungsnummer: I / 5	Übungstitel: IP – Backup	
Datum der Übung: 06. 10. 2015	Teilnehmer: Baumhackl, Dräxler, Fleischmann, Uhl	
Datum der Abgabe: 20. 10. 2015	Schriftführer: Fleischmann	Unterschrift:

	Beurteilung
Aufgabenstellung	
Dokumentation	
Messschaltungen	
Messtabellen	
Berechnungen	
Programmlistings	
Auswertung	
Diagramme	
Berechnungen	
Simulationen	
Schlußfolgerungen	
Kommentare	
Inventarliste	
Messprotokoll	
Form	
Summe	

Allgemeiner Teil

Titel der Übung:	IP – Backup
Übungsnummer:	I / 5
Datum der Übung:	06.10.2015
Klasse:	5BHEL
Schritfführer:	Fleischmann Raphael
Übungsteilnehmer:	Baumhackl David Dräxler Stefan Fleischmann Raphael Uhl Sebastian

Inhaltsverzeichnis

1. Besprechung.....	3
2. Systembackup	3
2.1. Stromversorgung.....	3
2.2. Redundanz.....	4
3. Software-Backup	4
3.1. Aufgabenstellung.....	4
3.2. Grafische Darstellung	5
3.3. Durchführung	5
4. Layer 3 Backup.....	6
4.1. Aufgabenstellung.....	6
4.2. Grafische Darstellung	7
4.3. Durchführung	7
5. Erkenntnisse aus der Übung.....	8

1. Besprechung

Zu Beginn der Übung wurden die Inhalte der Vorbesprechung wiederholt, vor allem die verschiedenen Ebenen der Ausfallsicherheit:

- Systembackup
 - Stromversorgung
 - Hardware
 - Software
 - Konfiguration
- Layer 2 Backup
- Layer 3 Backup

2. Systembackup

Im Anschluss daran wurden im Netzwerktechniklabor die verschiedenen Anforderungen an das Systembackup theoretisch besprochen und die dafür notwendigen Geräte begutachtet.

2.1. Stromversorgung

Damit eine Störung in der Stromversorgung keinen Einfluss auf den laufenden Betrieb eines Rechenzentrums hat, müssen wichtige Geräte (z.B. Switches, Router, Server) mindestens zwei verschiedene Stromanschlüsse besitzen. Die beiden Spannungsquellen dürfen keinesfalls im selben Stromkreis sein.

Wichtig ist, dass die beiden Netztransformatoren jeweils für die volle Leistung ausgelegt sind, da sonst beim Abschalten einer Quelle der andere Trafo nicht genügend Leistung für den alleinigen Betrieb bereitstellen kann.

Bei einem Stromausfall gibt es verschiedene Stufen der Stromquellen, die sich nacheinander aktivieren:

- **Unterbrechungsfreie Stromversorgung (USV):**

Eine USV besteht aus Akkus und einer Ansteuerung, die bei einem Stromausfall die Last binnen Millisekunden phasenrichtig übernimmt. Die USV dient zur Überbrückung von kurzfristigen Ausfällen und der Zeitspanne, die zum Hochfahren der Generatoren benötigt wird. Wenn es nur eine USV, aber kein Stromaggregat gibt, sendet die USV kurz vor Ende der Akkulaufzeit ein Signal an die angeschlossenen Geräte (z.B. Server), damit sie sich zur Vermeidung von Datenverlust sicher herunterfahren.

- **Notstromaggregat**

Das Notstromaggregat besteht aus großen Dieselgeneratoren und –tanks, die die benötigte Leistung erzeugen. Auch sie sollten idealerweise redundant ausgeführt sein und die Last phasenrichtig von der USV übernehmen. Da auch die Dieselvorräte irgendwann zu Neige gehen, sollten Rechenzentren für mehrtägige Stromausfälle Lieferverträge vorbereitet haben.

Wenn das Stromnetz wieder vollständig funktioniert, muss die Last erneut phasenrichtig weitergegeben werden.

Die redundante Stromversorgung sollte mindestens einmal im Jahr getestet werden, was in der Praxis wegen der Fehlerhäufigkeit und des Ausfallrisikos oft nicht durchgeführt wird.

2.2. Redundanz

Wichtige Geräte sollten immer mindestens doppelt ausgeführt sein. Dazu zählen z.B. Server, Hauptschwitches, Router, usw. Auch wichtige Verbindungen, z.B. Ethernet-Kabel zwischen Switches sollten redundant vorhanden sein. Auch die Hardware in einem Server sollte doppelt eingebaut werden, z.B. mehrere CPUs, Netzwerkkarten, RAID-Festplatten, ...

Im Gegensatz dazu werden normale Workstations (Clients) nicht ausfallsicher gemacht, da der Aufwand zu groß wäre und im Normalfall genügend Ersatz-Clients zur Verfügung stehen.

3. Software-Backup

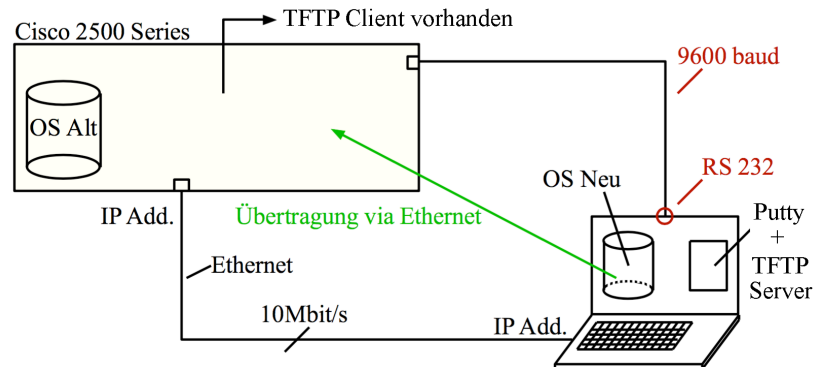
3.1. Aufgabenstellung

Die Software bzw. Firmware von Geräten sollte immer auf den neuesten Stand gebracht werden, um Probleme zu beheben und Sicherheitslücken zu schließen. Hierfür müssen laufend Updates durchgeführt werden.

Während der Laborübung war die Software eines Cisco 2500 Routers zu aktualisieren. Hierfür wurden die neue Software und eine Anleitung zur Aktualisierung zur Verfügung gestellt.

Die Übertragung des Updates sollte nicht über die serielle Schnittstelle (RS-232) erfolgen, da dies sehr lange dauern würde. Stattdessen wurde ein Ethernet-Port verwendet. Da der Switch nur einen TFTP-Client integriert hat, muss mit dem Übungs-Laptop ein TFTP-Server konfiguriert werden. TFTP benötigt keine Authentifizierung und ist daher leicht einzurichten.

3.2. Grafische Darstellung



3.3. Durchführung

Zunächst muss mit den Befehlen „enable“ und „conf t“ in den Konfigurationsmodus gewechselt werden. Anschließend wurde mit den Befehlen „interface [Interface-Name]“, „ip address [IP-Adresse] [Netzmaske]“ und „no shutdown“ das Netzwerk-Interface konfiguriert. Weiters wurde auch am Laptop eine IP-Adresse eingestellt (10.10.10.22).

Mit dem Befehl „show flash“ kann die aktuelle Softwareversion angezeigt werden, in diesem Fall handelte es sich um 1.121-21. Da dies bereits die neuere Version war, wurde zu Testzwecken eine ältere Version 1.121-17 eingespielt.

```
Router#show flash

System flash directory:
File Length Name/status
1 8034456 c2500-i-1.121-21.bin
[8034520 bytes used, 354088 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Im Anschluss wurden die notwendigen Befehle aus der Update-Anleitung durchgeführt. Zuerst musste der Rxboot-Mode im Configuration-Register gesetzt werden:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# config-register 0x2101
Router(config)# ^Z
Router# reload
```

Mit „show version“ kann der aktuelle Wert abgelesen werden. Nach dem Reload wurde das Register wieder auf den vorherigen Wert zurückgesetzt:

```
Router(boot)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(boot)(config)#config-register 0x****
Router(boot)(config)#^Z
Router(boot)#
```

Danach wurde der TFTP-Server auf dem Laptop installiert und konfiguriert. Hierbei muss der Pfad zur einzubindenden Datei angegeben werden.

Mit dem Befehl „copy tftp flash“ wird die Dateiübertragung gestartet. Zuvor wird noch die IP-Adresse des TFTP-Servers und der Name der Datei abgefragt. Sobald die Informationen eingegeben wurden, musste noch mehrfach das Löschen der aktuellen Software bestätigt werden, um das neue Update einzuspielen. Dann begann die Übertragung:

```
Router(boot)#copy tftp flash

System flash directory:
File Length Name/status
  1 8024584 c2500-i-1.121-17.bin
[8024648 bytes used, 363960 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 10.10.10.22
Source file name? c2500-i-1.121-21.bin
Destination file name [c2500-i-1.121-21.bin]?
Accessing file 'c2500-i-1.121-21.bin' on 10.10.10.22...
Loading c2500-i-1.121-21.bin from 10.10.10.22 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'c2500-i-1.121-21.bin' from server
as 'c2500-i-1.121-21.bin' into Flash WITH erase? [yes/no]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading c2500-i-1.121-21.bin from 10.10.10.22 (via Ethernet0): !!!!!
```

Die Übertragung via Ethernet und TFTP dauerte 4 Minuten und 1 Sekunde.

Zuletzt muss noch ein „reload“ durchgeführt werden. Mittels „show flash“ kann nun die neue Softwareversion überprüft werden, welche jetzt 1.121-17 – also die eben eingespielte – war.

4. Layer 3 Backup

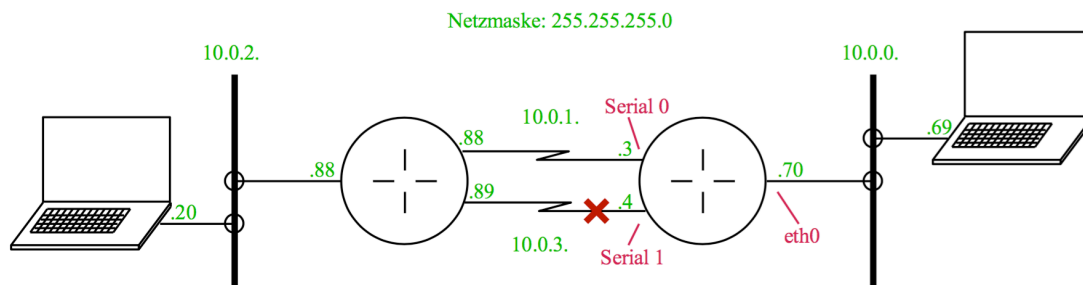
4.1. Aufgabenstellung

Als letzter Teil der Laborübung war noch ein Layer 3 Backupsystem aufzubauen. Hiermit ist gemeint, dass zwei Router mit mehreren Netzkabeln verbunden werden.

Mittels Spanning-Tree-Protokoll schalten die Router automatisch eine der beiden Leitungen ab, um keinen Broadcast-Loop zu erzeugen. Fällt eine Leitung aus, wird automatisch auf die andere umgeschaltet. Um einen derartigen Ausfall zu simulieren, war nach vollendeter Konfiguration eine der Leitungen abzustecken.

Jede der beiden Teilgruppen war für die Konfiguration eines Routers und eines Laptops zuständig.

4.2. Grafische Darstellung



4.3. Durchführung

Wie bereits in mehreren vorherigen Laborübungen musste zunächst das Netzwerk und die zugehörigen Routen konfiguriert werden (siehe Protokoll 4. Jahrgang).

```
Router(config)#interface Serial 0
Router(config-if)#ip address ?
  A.B.C.D      IP address
  negotiated   IP Address negotiated over PPP or via DHCP

Router(config-if)#ip address 10.0.2.88 255.255.255.0
Router(config-if)#interface Serial 1
Router(config-if)#ip address 10.0.1.89 255.255.255.0

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip route
Router(config)#no ip route 10.0.0.0 255.255.255.0 10.0.1.3
Router(config)#no ip route 10.0.0.0 255.255.255.0 10.0.3.4
Router(config)#interface Serial 0
Router(config-if)#ip address 10.0.1.88 255.255.255.0
Router(config-if)#interface Serial 1
```

Nachdem beide Router fertig konfiguriert waren, wurde zwischen den beiden Laptops ein kontinuierlicher Ping durchgeführt („ping [IP-Adresse] -t“). Anschließend konnte eines der beiden Verbindungskabel abgesteckt werden, um einen Ausfall zu simulieren. Nach einigen fehlgeschlagenen Pings, da das Umschalten einige Sekunden in Anspruch nimmt, funktionierte der Ping wieder. Das ausfallsichere System funktionierte also perfekt.

Als Erweiterung wurde letztlich ein dynamisches Routing mit dem Routing-Protokoll RIP durchgeführt, da statische Routen für diese Anwendung nicht optimal sind. Dafür muss im configure-Modus der Befehl „router rip“ ausgeführt und anschließend alle zu routenden Netzwerke angegeben werden:

```
Router(config-router)#network 10.0.2.0
Router(config-router)#network 10.0.1.0
Router(config-router)#network 10.0.3.0
Router(config-router)#exit
```

Auch mit dem dynamischen Routing funktionierte das Layer-3-Backup zuverlässig und ohne Probleme.

5. Erkenntnisse aus der Übung

In dieser Übung wurde erlernt, wie man ausfallsichere Systeme aufbaut, worauf besonders zu achten ist und welche Fehler in der Praxis häufig vorkommen. Weiters wurden die theoretischen Kenntnisse praktisch in einer Softwareaktualisierung und einem ausfallsicheren Layer-3-Backup umgesetzt.