Abteilung für INFORMATIK

HTL ST. PÖLTEN

Titel: Labor01 – Einführung

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 06.10.2020 Abgabe: 20.10.2020

Inhaltsverzeichnis

1 Theorie-Teil

1.1 Das Betriebssystem des Routers: Cisco IOS

IOS, auch Internetnetwork Operating System genannt, ist ein von Cisco entwickeltes und auf ihren Geräten (vor allem Switches und Routern) vertriebenes Betriebssystem. Es hat ein kommandozeilen-basiertes Interface auf das per SSH, Telnet oder über ein spezielles serielles Kabel zugegriffen wird. Es wird benutzt um verschiedene Dinge, wie Routing, Firewall & Switching an einem Cisco Router oder Switch zu konfigurieren und zu warten.

1.1.1 Architektur

IOS ist monolithisch aufgebaut, d.h. alle wichtigen Funktionen laufen im Kernel Modus. Da hier kein Kontext-Switching zwischen User-Mode und Kernel Mode notwendig ist, ist die Performance höher. Die Architektur ist auch den für damalige Verhältnisse langsamen Hardware-Spezifikationen der Router aus den 1980er-Jahren geschuldet. Es wurde damals auf Routern mit 256KB RAM betrieben.

Beim Start wird das IOS Image vom Flash Speicher in den Hauptspeicher entpackt und danach gestartet, bei älteren Modellen startet das IOS Image direkt vom Flash Speicher.

Um die maximale Performance aus der limitierten Hardware herauszuholen, haben Prozesse direkten Zugriff auf die Hardware. Es gibt keinen Speicherschutz zwischen Prozessen. Der Kernel von IOS macht kein Swapping oder Paging wie man es von heutigen, modernen Kernels (NT, Linux, Darwin,…) gewohnt ist. Der ganze physikalische Adressraum ist in einen einigen virtuellen Adressraum gemapped.

Der Vorteil dieser Architektur ist die Performance, die man so ohne Aufgaben wie Sheduling oder Speicherschutz rausholen kann. Der Nachteil darin liegt aber, dass ein einziger Prozess, welcher eine falsche Aktion ausführt, das ganze System zum Abstürzen bringen kann. Außerdem können Prozesse Daten von anderen Prozessen aufgrund des fehlenden Speicherschutzes überschreiben.

1.1.2 Release-Trains

Release-Trains gab es bis IOS Version 12.4. Sie waren einzelne, auf spezielle Anwendungsgebiete zugeschnittene Versionen der Software, z.B. eine Version zugeschnitten für ISPs (Internet Service Provider).

- Mainline-Train: Der stabilste Train, da er nur Bugfixes und Sicherheitsupdates in seiner Lebenszeit erhält.
- (T)-echnology-Train: bekommt immer die neusten Features und Bug Fixes in seinem Lebenszyklus, ist daher aber potenziell weniger stabil als der erprobte Mainline-Train. Wird nicht empfohlen für produktive Umgebungen, außer es wird dringend ein neues Feature gebraucht.
- S – Service Provider-Train: Speziell angepasste Version der Router-Software für Core-Router für Internet Service Provider.

Mit der Version 15 wurden alle Trains in einen einzigen vereint, in den M/T-Train.

Quelle: https://en.wikipedia.org/wiki/Cisco_IOS

1.2 Serielle Datenübertragung (RS232)

Quelle: https://kompendium.infotip.de/rs-232-die-serielle-schnittstelle.html

Serielle Schnittstellen dienen zum physischen Datenaustausch zwischen zwei Geräten, welche mit seriellen Schnittstellen ausgestattet sind. Die Datenbits werden dabei nicht parallel wie z.B. bei USB oder Firewire, sondern seriell, d.h. hintereinander, übertragen.

RS232 eignet sich zum Anschluss von Kassageräten, Druckern, Messgeräten und vielem mehr. Bis USB erschien, war quasi jeder PC mit so einer Schnittstelle ausgestattet. Die hohen Übertragungsraten von USB setzten RS232 jedoch ein Ende und so wird er Legacy Port nur noch in speziellen Anwendungsszenarien genutzt.

1.2.1 Prinzip der Datenübertragung

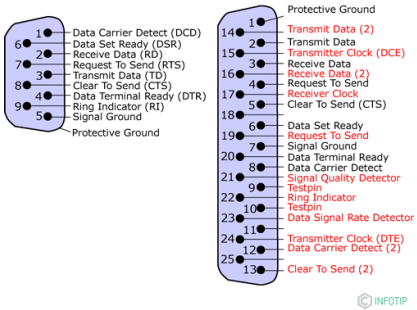
Bei der RS232-Verbindung erfolgt die Übertragung der Daten asynchron, das bedeutet, dass das Taktsignal nicht mitübertragen wird. Der Empfänger muss sich das Taktsignal aus dem Datenstrom wiedergewinnen.

Pegeländerungen werden durch das Abtasten des empfangenen Signals erkannt. Die Synchronisiation wird dann mit Start und Stopp Bits im Datenstrom vorgenommen. Vor dem Start der Übertragung gilt der Wert 1. Zu Beginn der Übertragung wird der logische Wert 0 gesendet und damit signalisiert man den Beginn der Übertragung, die Nutzerdaten werden gesendet und das Ende wird mit dem Stopp-Bit „1“ signalisiert. Die Dauer ist abhängig von der eingestellten Bitrate.

Der RS232 Standard definiert nicht, wie die zu übertragenden Daten genau übertragen werden. Dinge wie Datenrate, Zeichenkodierung usw… müssen vor Übertragung zwischen Sender und Empfänger ausgehandelt oder eingestellt werden. Die serielle Schnittstelle eines PCs verwendet sieben bis acht Bit lange ASCII-Werte als Nutzdaten. Diesen Nutzdaten folgt ein Paritätsbit zur Fehlererkennung.

1.3 Die Schnitstelle

DTE (Digital Terminal Equipment) sind Geräte, die die Daten empfangen oder senden können, aber nicht weiterleiten können. Der Anschluss ist immer als „male“, d.h. als Stiftleiste ausgelegt.



DCE sind Geräte, die Daten empfangen und sie ohne Verarbeitung an andere Geräte weiterleiten. Ihr Anschluss ist als Buchse, auch als „female“ bezeichnet, ausgelegt.

Die klassische RS232 ist 25-polig. Da aber in der EDV nicht alle Signale, die der Standard beherbergt, gebraucht werden, hat sich ein kleinerer, 9-poliger Anschluss durchgesetzt. Der Hauptunterschied besteht darin, dass der 25-polige Anschluss 2 Datenkanäle beinhaltet, der 9-polige nur einen zur Verfügung stellt.

1.3.1 Heute

Die Schnittstelle wird heutzutage nur mehr für spezielle Anwendungen, wie Industrieanlagen, eingesetzt und wurde durch schnellere Anschlüsse wie Firewire, Ethernet und USB ersetzt. Sie erlauben größere Übertragungsraten, größere Reichweiten und sind weitaus weniger störanfällig.

2 Übergabe

2.1 Verkabeln laut Angabe. Welche Kabel werden wo eingesetzt? Übernahme der Struktur ins Protokoll.

2.1.1 Eingesetzte Kabel

- Rollover-Kabel von Router zu PC.
- Serielles Kabel (DTE+DCE) von Router zu Router.

2.1.2 Struktur

Der Router und der Computer sind wie in folgendem Modell verkabelt:

2.2 Vergabe eines Routernamens

Damit man den Namen des Routers ändern kann, muss man zuerst mit `enable` in den Privileged Mode wechseln und dann per `configure terminal` in den Global Configuration Mode, wo man den Hostnamen (den Namen des Routers) ändern kann. Dies geschieht mit dem Befehl `hostname <NAME>.`

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

2.3 MOTD setzen

Um eine MOTD (Message Of The Day) zu setzen, gibt man `banner motd #<CUSTOM MODT>#` im Global Configuration Mode ein. Dabei ist es wichtig, die Message zwischen die beiden Delimiter `#` zu setzen, damit weiß die CLI wo die Message anfängt und aufhört.

```
HAIDEN(config)#banner motd #Dies ist meine eigene MOTD, lol.#
```

Nach einem erneuten Login:

```
Dies ist meine eigene MOTD, lol.

HAIDEN>
```

Um eine Login Nachricht zu setzen, gibt man den Befehl `banner login #<MSG>#` im Global Configuration Mode ein. Er wird beim Herstellen einer SSH Verbindung vor der Passwort-Abfrage angezeigt.

```
HAIDEN(config)#banner login #Dies ist eine Login Nachricht#

HAIDEN>ssh -l ciscossh 192.168.0.1

Dies ist eine Login Nachricht

Password:


Dies ist meine eigene MOTD, lol.


ROUTER2>
```

2.4 Führen Sie den Befehl „show version“ aus Welche IOS Version ist installiert? Welches File wird gebootet? Wo ist es gespeichert? Wieviel Speicher (RAM, Flash,…) hat Ihr Router?

Durch diesen Befehl bekommt man eine große Ausgabe.

Die Versionsnummer, die auf meinem Router installiert ist, ist die Nummer 15.4:

```
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.4(3)M1, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2014 by Cisco Systems, Inc.

Compiled Sat 25-Oct-14 03:34 by prod_rel_team
```

Es wird folgende Datei gebootet:

```
System image file is "flash0:c2900-universalk9-mz.SPA.154-3.M1.bin"
```

Die Datei ist auf dem Flash Speicher des Routers gespeichert und wird beim Start dekompressiert.

Der RAM ist insgesamt 512MB groß, er ist aufgeteilt in I/O und Processor Memory:

```
Cisco CISCO2901/K9 (revision 1.0) with 446464K/77824K bytes of
memory.
```

Er hat insgesamt 256MB an Flash-Speicher:

```
255488K bytes of ATA System CompactFlash 0 (Read/Write)
```

2.4.1 Global Configuration Register

```
Configuration register is 0x2102
```

Bedeutung:

- Ignores Break
- Lädt das CISCO IOS Image von der Flash Disk
- 9600 baud Konsolenrate

2.5 Konfigurieren der IP Adressen und der seriellen Verbindungen. Welcher Seite ist DCE/DTE. Wer liefert den Clock? Zeichen Sie die Struktur ins Protokoll. Erklären Sie die Begriffe!

Ich bin DCE, mein Nachbar ist DTE. Da ich DCE bin, liefere ich die Clockrate.

2.5.1 Struktur

```
HAIDEN(config)#interface Serial0/0/1
HAIDEN(config-if)#clock rate 64000
HAIDEN(config-if)#ip address 192.168.0.2 255.255.255.0
HAIDEN(config-if)#no shutdown
HAIDEN(config-if)#description link to isp
HAIDEN(config-if)#exit
```

2.5.2 Ping Test:

```
HAIDEN#ping 192.168.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28
ms
```

2.6 Vergabe von Passwörtern

Secret Passwort: class

Enable Passwort: cisco

Consolen Passwort: ciscocon

2.6.1 Aktivieren sie den ssh Zugang.

SSH User: ciscouser

Passwort: ciscossh

```
HAIDEN#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HAIDEN(config)#username ciscouser
HAIDEN(config)#username ciscouser password ciscossh
HAIDEN(config)#ip domain name nvs.lan
HAIDEN(config)#crypto key generate rsa
The name for the keys will be: HAIDEN.nvs.lan
Choose the size of the key modulus in the range of 360 to 4096 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
```

```
  a few minutes.


How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)


HAIDEN(config)#
*Oct  6 07:49:31.319:  RSA key size needs to be atleast 768 bits for
ssh version 2
*Oct  6 07:49:31.319: %SSH-5-ENABLED: SSH 1.5 has been enabled
HAIDEN(config)#line vty 0 4
HAIDEN(config-line)#login local
HAIDEN(config-line)#transport input ssh
```

2.7 Maximale Clock-Rate herausfinden

Um die maximale CLock Rate herauszufinden, gibt man im Interface Konfigurations-Modus `clock rate ?` ein. Dann bekommt man eine Liste von Clock-Rates ausgegeben. Die höchste Clock Rate ist hierbei 8000000.

```
HAIDEN(config-if)#clock rate ?
        Speed (bits per second)
  1200
  …
  64000
  …
  8000000
  <300-8000000>    Choose clockrate from list above
```

2.8 Speichern der aktuellen Konfiguration

```
HAIDEN#show run
Building configuration...


Current configuration : 1397 bytes
!
! Last configuration change at 07:31:53 UTC Tue Oct 6 2020
!
```

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HAIDEN
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$3D3K$1taJaNBnAF/Y2dmTa.eM30
enable password cisco
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
```

```
multilink bundle-name authenticated
!
!
cts logging verbose
!
!
license udi pid CISCO2901/K9 sn FCZ1850C2DC
!
!
!
redundancy
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 description link to isp
 ip address 192.168.0.2 255.255.255.0
 clock rate 64000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner login ^CDies ist eine Login Nachricht
^C
banner motd ^CDies ist meine eigene MOTD, lol.^C
!
line con 0
 password ciscocon
 login
line aux 0
line 2
```

```
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

2.9 Testen Sie die Routerverbindung mit SSH. Ist ein Zugriff per Telnet noch möglich? Wenn ja, deaktivieren sie diesen.

2.9.1 Telnet:

```
HAIDEN>telnet 192.168.0.1
Trying 192.168.0.1 ...Open


[Connection to 192.168.0.1 closed by foreign host]
```

Der Router am anderen Ende (Packet Tracer) verweigert die Verbindung per Telnet und schließt diese.

2.9.2 Testen von SSH

```
HAIDEN>ssh -l ciscouser 192.168.0.1


Password:


dies ist eine motd


ROUTER2>
```