

Titel: Labor 02 – Einführung

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 20.10.2020 **Abgabe:** 10.11.2020

Inhaltsverzeichnis

1	Theorie-Teil.....	1
1.1	CDP (Cisco Discovery Protocol)	1
1.1.1	Meist benutzte Commands	1
1.2	Global Configuration Register Werte	2
2	Übung	3
2.1	CDP	3
2.1.1	Test von CDP	3
2.2	Passwort-Recovery	3
2.2.1	Setzen Sie ein unmerkbares Enable-Passwort.	3
2.2.2	Sichern Sie die Konfiguration und rebooten Sie den Router.....	4
2.3	Konfigurationsmanagement.....	5
2.3.1	Sichern Sie die Konfiguration im NV-RAM.....	5
2.3.2	Sichern Sie die Konfiguration aus dem Terminal.....	5
2.3.3	Reloaden über das Terminal.....	9
2.3.4	Erasen von NV-RAM	9
2.3.5	Sichern Sie die Konfiguration auf einem TFTP Server.	9
2.3.6	Stellen Sie die Konfiguration vom TFTP Server wieder her	10
2.3.7	Zeigen Sie den Inhalt Ihres Flash/NVRam Speichers an.	10
2.4	IOS-Management	11
2.4.1	Sichern Sie das IOS vom Flash auf einem TFTP Server.	11
2.4.2	Kopieren Sie eine aktuellere IOS Version vom TFTP Server auf den Router. Wie können Sie beeinflussen, von welcher Version sie booten (Testen!) (Hinweis: boot system)?.....	12
2.4.3	Booten Sie in den Rommon (über das Global Configuration Register).	13
2.4.4	Stellen Sie das IOS Image über den TFTP Server wieder her (tftpdnld).	13
2.5	Lizenzverwaltung / IOS	14
2.5.1	Welche IOS Version mit welchem Funktionsumfang haben Sie installiert?	14
2.5.2	Wie können zusätzliche Lizenzen installiert werden? Welche Funktionen können hinzugefügt werden?.....	14
2.5.3	Was versteht man unter einer Evaluation License? Wie wird sie aktiviert?	15
2.5.4	Wie unterscheiden sich die Versionen 12/15/16?	15

1 Theorie-Teil

1.1 CDP (Cisco Discovery Protocol)

Quelle 1: https://de.wikipedia.org/wiki/Cisco_Discovery_Protocol

Quelle 2: <https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x>

Das Cisco Discovery Protocol, auch CDP abgekürzt genannt, ist ein 1994 von Cisco entwickeltes Protokoll. Es agiert auf Layer 2 im OSI-Schichten-Modell und wird hauptsächlich auf Cisco-Geräten verwendet. CDP verwendet keine Sicherheitsmechanismen und lässt sich so leicht abhören und fälschen.

Jedes Gerät, das dafür konfiguriert ist, dass es CDP Nachrichten sendet, sendet periodische Nachrichten, auch Advertisements, an eine Ethernet-Multi-Cast Adresse (01-00-0C-CC-CC-CC).

Jede Nachricht enthält Informationen über das jeweilige Gerät (Router, Switch), z.B. Hostname, IOS-Version, IP-Adresse, Schnittstellen, die IP-Adressen der Management-Schnittstellen und die Holdtime des CDP Paketes. Findet keine periodische Aktualisierung der Geräteinformationen über das Netzwerk statt, so wird die alte Information aus dem CDP Paket nach der angegebenen Holdtime verworfen.

In der Standard-Einstellungen schicken Cisco-Geräte alle 60 Sekunden ein CDP Paket an die Ethernet-Multi-Cast Adresse mit einer Paket-Holdtime von 180 Sekunden (3 Minuten).

Eine aktuellere Version, CDPv2, bietet mehr Informationen und ist so hilfreicher bei der Diagnose und bei der Suche nach Fehlern.

Ist man auf der Suche nach einem vergleichbaren, herstellerunabhängigen Protokoll, bietet sich LLDP (Link Layer Discovery Protocol) an. LLDP und CDP sind nicht kompatibel zueinander.

1.1.1 Meist benutzte Commands

- Status des CDP anzeigen
`show cdp`
- Aktivieren von CDP für spezifisches Interface
`cdp enable`
- Benachbarte CDP-Geräte anzeigen
`show cdp neighbors`
- Löschen der CDP Informationstabelle
`clear cdp table`
- Informationen über bestimmtes CDP-Gerät anzeigen
`show cdp entry`
- CDP-Traffic Informationen anzeigen
`show cdp traffic`

- CDP Holding-Time verändern
`cdp holdtime`
- CDP Intervall, in dem Pakete gesendet werden, verändern
`cdp timer`
- Globale Aktivierung v. CDP Prozess
`cdp run`

1.2 Global Configuration Register Werte

Bit Number	Hex	Meaning
00-03	0x0000-0x000F	Boots Field Parameters:
		• 0x0000 - Stays at the system bootstrap prompt.
		• 0x0001 - Boots the first system image in onboard
		Flash memory (EPROM).
		• 0x0002-0x000F- Specifies a default netboot filename.
		Enables boot system commands that override the default netboot filename.
6	0x0040	Ignore NVRAM contents
7	0x0080	Disable boot messages
8	0x0100	Break disabled
9	0x0200	Causes the system to use the secondary bootstrap.
		This is typically not used (set to 0).
10	0x0400	IP broadcast with all zeros
5,11,12	0x0020, 0x0800, 0x1000	Console line speed
13	0x2000	Boots default ROM software if network boot fails
14	0x4000	IP broadcasts do not have net numbers
15	0x8000	Enables diagnostic messages
		Ignores NVRAM contents

Quelle: <https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html>

2 Übung

2.1 CDP

2.1.1 Test von CDP

```
HAIDEN#show cdp neighbors detail
-----
Device ID: AlarkhanovRaid
Entry address(es):
  IP address: 192.168.0.2
Platform: Cisco CISCO2901/K9, Capabilities: Router Source-Route-
Bridge Switch IGMP
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime : 178 sec
Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.4(3)M, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Mon 21-Jul-14 19:29 by prod_rel_team
advertisement version: 2
Management address(es):
  IP address: 192.168.0.2
Total cdp entries displayed : 1
```

2.2 Passwort-Recovery

2.2.1 Setzen Sie ein unmerkbares Enable-Passwort.

```
HAIDEN(config)#enable password C450C3204C432^@
HAIDEN(config)#exit
HAIDEN#show runn
*Oct 20 05:40:45.011: %SYS-5-CONFIG_I: Configured from console by
console
Building configuration...
Current configuration : 1214 bytes
!
! Last configuration change at 05:40:45 UTC Tue Oct 20 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 password C450C3204C432
```

Passwort wurde gesetzt und ist nicht verhasht bzw. verschlüsselt.

2.2.2 Sichern Sie die Konfiguration und rebooten Sie den Router.

Um die Konfiguration zu sichern, kopiert man die running-config in die Startup-config.

```
HAIDEN#copy running-config startup-config
```

Danach schaltet man den Router aus und startet ihn neu. Während des Boot Vorgangs muss man bei „Readonly ROMMON intialized“ die CTRL und „Unterbrechen“ Taste gedrückt halten. Nachdem man dies getan hat, landet man im ROMMON Modus des Cisco Routers.

Dort setzt man

```
rommon 3 > confreg 0x2142
rommon 4 > reset
```

Zurück im normalen IOS CLI Screen, wechselt man in den Privileged Modus. Dieser hat nun kein Passwort mehr davor und so kann man ohne Passworteingabe wechseln. Danach kopiert man die Startup-Config in die running-Config.

```
Router#copy startup-config running-config
Destination filename [running-config]?
1214 bytes copied in 0.132 secs (9197 bytes/sec)
```

Da sich das Prompt ändert weiß man, dass man nun auf der alten Konfiguration, welche man vorher gesichert hat, arbeitet.

Nun setzt man mit `enable password` im Global Configuration Mode und setzt so das alte zurück.

```
HAIDEN(config)#enable password cisco
HAIDEN(config)#
```

Damit das Passwort und die anderen Einstellungen erhalten bleiben, kopiert man die derzeitige Konfiguration in die Startup-Konfiguration und speichert so das aktuelle Passwort und alle anderen Einstellungen.

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

Und zum Schluss setzt man das Global Configuration Register zurück auf den Standardwert:

```
HAIDEN(config)#config-register 0x2102
```

2.3 Konfigurationsmanagement

2.3.1 Sichern Sie die Konfiguration im NV-RAM

```
HAIDEN#copy running start
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.3.2 Sichern Sie die Konfiguration aus dem Terminal.

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

Current configuration : 1216 bytes
!
! Last configuration change at 07:02:50 UTC Tue Oct 20 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 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  
  ip address 192.168.0.1 255.255.255.0  
  shutdown  
  clock rate 64000  
!  
interface Serial0/0/1
```

```
no ip address
shutdown
clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
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
```

2.3.3 Reloaden über das Terminal

Um sie im Terminal zu reloaden, kopiert man diese einfach in das Putty (oder andere serielle Client) Fenster. Die Befehle müssen im Global Configuration Mode reingefügt werden, da es sonst einige Fehlermeldungen aufgrund fehlender Berechtigungen / Befehle gibt.

```
HAIDEN(config)#version 15.4
HAIDEN(config)#service timestamps debug datetime msec
HAIDEN(config)#service timestamps log datetime msec
HAIDEN(config)#no service password-encryption
HAIDEN(config)#!
HAIDEN(config)#hostname HAIDEN
HAIDEN(config)#!
HAIDEN(config)#boot-start-marker
HAIDEN(config)#boot-end-marker
HAIDEN(config)#!
```

2.3.4 Erasen von NV-RAM

Um den NVRAM zu löschen, gibt man im Terminal Fenster `write erase` ein.

```
HAIDEN#write erase

Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]

[OK]

Erase of nvram: complete
```

Ab hier wurde der Packet Tracer verwendet!

2.3.5 Sichern Sie die Konfiguration auf einem TFTP Server.

2.3.5.1 Packet Tracer Modell von Server & 2901-Router



Router und Server (dargestellt im Packet Tracer) sind durch ein Ethernet Kabel an den jeweiligen Ethernet-Schnittstellen verbunden. Hierbei nimmt der Router die IP-Adresse 192.168.0.1 und der Server die IP-Adresse 192.168.0.2 ein. Beide mit der Subnetzmaske 255.255.255.0 (/24).

2.3.5.2 TFTP

TFTP (Trivial File Transfer Protocol) ist eine vereinfachte Variante des populären FTP (File Transfer Protocol) Protokolls. Es unterstützt lediglich das Lesen und Schreiben von Dateien und unterstützt keine Mechanismen zur Authentifizierung, z.B. über Username & Passwort.

2.3.5.3 Sichern der Konfiguration

Laufende und Startup-Configs kann man zur späteren Verwendung, z.B. muss man den Router zurücksetzen, auf einen TFTP Server sichern um so das nächste Mal einen nicht alle Konfigurationsschritte erneut durchlaufen zu müssen.

Dies geschieht über den Befehl `copy`. Copy fragt nach dem Remote Host, d.h. wo die Datei hingeschickt werden soll und wie die Datei heißen soll.

Syntax: `copy <SOURCE> <TARGET>`

```
HAIDEN#copy running-config tftp
Address or name of remote host []? 192.168.0.2
Destination filename [HAIDEN-config]? HAIDEN-config
Writing running-config...!!
[OK - 623 bytes]
623 bytes copied in 0 secs
```

2.3.6 Stellen Sie die Konfiguration vom TFTP Server wieder her

Um die Konfiguration von einem TFTP Server herunterzuladen und wiederherzustellen, vertauscht man beim Copy Befehl einfach `running-config` und `tftp`:

```
ROUTER#copy tftp running-config
Address or name of remote host []? 192.168.0.2
Source filename []? HAIDEN-config
Destination filename [running-config]?
Accessing tftp://192.168.0.2/HAIDEN-config...
Loading HAIDEN-config from 192.168.0.2: !
[OK - 623 bytes]
623 bytes copied in 0.001 secs (623000 bytes/sec)
HAIDEN#
```

Die aktuelle Konfiguration wird dabei überschrieben, beispielhaft an dem Hostnamen aufgeführt.

2.3.7 Zeigen Sie den Inhalt Ihres Flash/NVRam Speichers an.

2.3.7.1 Inhalt des Flash-Speichers

Zum Anzeigen des Inhaltes des Flash-Speichers kann man den Befehl `dir flash:` verwenden. Auf dem Flash-Speicherchip liegen ein paar Dateien, z.B. das IOS-System-Image welches beim Start des Routers in den Arbeitsspeicher entpackt wird.

```
HAIDEN#dir flash:
Directory of flash0:/
3 -rw- 33591768 <no date> c2900-universalk9-mz.SPA.151-4.M4.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml
255744000 bytes total (221896413 bytes free)
```

2.3.7.2 Inhalt des NVRAM-Speichers

```
HAIDEN#dir nvram:
Directory of nvram:/
No files in directory
```

2.4 IOS-Management

Wie Konfigurationen kann man auch IOS-Images sichern und wiederherstellen.

2.4.1 Sichern Sie das IOS vom Flash auf einem TFTP Server.

Wie bei der Konfiguration sichert man ein IOS-Image auch über den copy-Befehl.

[illegible]

2.4.2 Kopieren Sie eine aktuellere IOS Version vom TFTP Server auf den Router. Wie können Sie beeinflussen, von welcher Version sie booten (Testen!) (Hinweis: boot system)?

2.4.2.1 Kopieren von neuerer IOS-Version

Um eine neuere Version vom TFTP Server auf den Flash des Routers zu kopieren, braucht man nur den Dateinamen. Man vertauscht einfach Source und Ziel.

Version welche aktuell auf dem Router läuft

c2900-universalk9-mz.SPA.151-1.M4.bin

Neuere Version:

c2900-universalk9-mz.SPA.155-3.M4a.bin

Kopieren der Datei:

[illegible]

2.4.2.2 Einstellen des zu ladenden IOS-Images

```
Directory of flash0:/
3 -rw- 33591768 <no date> c2900-universalk9-mz.SPA.151-4.M4.bin
4 -rw- 33591768 <no date> c2900-universalk9-mz.SPA.155-3.M4a.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml
```

Der Router hat nun mehrere IOS-Images auf seinem Flash-Speicherchip gespeichert. Möchte man nun ein neueres IOS-Image booten, muss man den boot system Command benutzen. Er setzt das zu ladende IOS-Image.

Syntax: `boot system <TARGET-FILE>`

Das Target-File kann auf jedem beliebigen Speicherchip liegen. Man muss nur den Pfad hierzu angeben, in unserem Beispiel also:

```
HAIDEN(config)#boot system flash:c2900-universalk9-mz.SPA.155-3.M4a.bin
```

Danach lädt man den Router mit Reload neu und das neue IOS-Image wird vom Flash gebootet.

```
HAIDEN#show version

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE (fc1)
```

2.4.3 Booten Sie in den Rommon (über das Global Configuration Register).

Mit dem Setzen des 0x2120 Flags im Global Configuration Register bootet der Router automatisch beim nächsten Reload in den Rommon-Mode.

```
HAIDEN(config)#config-register 0x2120
HAIDEN(config)#reload
<neustart>

System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
rommon 1 >
```

2.4.4 Stellen Sie das IOS Image über den TFTP Server wieder her (tftpdnld).

Vor dem Zurücksetzen müssen einige Umgebungsvariablen wie IP des Servers, etc... gesetzt werden.

Konkret müssen dabei die folgenden Umgebungsvariablen gesetzt werden:

`IP_ADDRESS`: Die IP des TFTP-Servers

`IP_SUBNET_MASK`: Die Subnetzmaske

`DEFAULT_GATEWAY`: Gateway

`TFTP_SERVER`: Die IP Adresse des TFTP Servers

`TFTP_FILE`: Welche Datei vom TFTP-Server heruntergeladen werden soll

```
rommon 9 > tftpdnld

IP_ADDRESS: 192.168.0.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.0.1
TFTP_SERVER: 192.168.0.2
TFTP_FILE: c2900-universalk9-mz.SPA.151-4.M4.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]:
...
program flash location 0x61f90000
program flash location 0x61fa0000
program flash location 0x61fb0000
program flash location 0x61fc0000
program flash location 0x61fd0000
program flash location 0x61fe0000
program flash location 0x61ff0000
program flash location 0x62000000
```

2.5 Lizenzverwaltung / IOS

2.5.1 Welche IOS Version mit welchem Funktionsumfang haben Sie installiert?

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE (fc1)

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

Copyright (c) 1986-2016 by Cisco Systems, Inc.

Compiled Thu 06-Oct-16 14:43 by mnguyen

Ich habe die Version 15.5 Milestone 4A installiert, in der Universal Variante, d.h. die Standard-Lizenz die bei jedem Router, der von Cisco verkauft wird, dabei ist.

2.5.2 Wie können zusätzliche Lizenzen installiert werden? Welche Funktionen können hinzugefügt werden?

Lizenzen können mit dem license Befehl hinzugefügt werden.

Syntax: `license <LOCATION-URL-TO-LICENSE-FILE>`

Danach den Router mit `reload` neustarten.

Beispiel von der Cisco-Dokumentation:

```
Router> enable
Router# license install flash0:uck9-C3900-SPE150_K9-FHH12250057.xml
Installing licenses from "uck9-C3900-SPE150_K9-FHH12250057.xml"
Installing...Feature:uck9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

Quelle: https://www.cisco.com/c/en/us/td/docs/routers/access/sw_activation/SA_on_ISR.html#pgfid-1097551

2.5.3 Was versteht man unter einer Evaluation License? Wie wird sie aktiviert?

Evaluation Licenses sind in einer Form begrenzte Lizenzen, häufig z.B. in Zeit, die dazu da sind, dass neue, potenzielle Nutzer, ein Feature oder eine Software austesten und evaluieren, d.h. ergründen können, ob die Software ihren Ansprüchen genügt und ob sie die erforderlichen Funktionen hat / bereitstellt.

Aktivieren einer Evaluations-Lizenz passiert auch mit dem Lizenz-Befehl:

Beispiel von der Cisco Dokumentation:

```
Router>enable
Router#configure terminal
Router(config)#license boot level advenenterprise
% use 'write' command to make license boot config take effect on
next boot
Router(config)#exit
Router#copy running-config startup-config
Router#reload
```

Quelle: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/csa/configuration/xe-16-6/csa-xe-16-6-book/csa-rtu.html>

2.5.4 Wie unterscheiden sich die Versionen 12/15/16?

Bis Version 12 gab es von Cisco IOS Release Trains.

- 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 Version 15 wurden alle Release Trains in einen einzigen vereint.

2.5.4.1 IOS 16 XE/XR

IOS 16 ist dagegen ein komplett neues Betriebssystem. IOS 16 ist ein auf Linux-basiertes Betriebssystem, wo der IOS Prozess als Daemon in einem eigenen Prozess neben Linux läuft. Alle Systemfunktionen laufen als separate Prozesse. Dies hat zur Folge, dass ein fehlerhafter Prozess nicht mehr ein ganzes System zum Absturz bringen kann wie bei der monolithischen Architektur von IOS.

Dies macht IOS auch modular und so muss man nicht mehr das ganze Rom-File herunterladen sondern nur einzelne Teile die man upgraden möchte.

XR ist eine Software-Plattform welche auf dem QNX Unix Kernel basiert.

Quelle: <https://networklessons.com/cisco/ccie-routing-switching-written/introduction-cisco-ios-xe>