

ZSL

Zentrum für Schulqualität
und Lehrerbildung
Baden-Württemberg



Networking
Academy

Basic Device Configuration



Andreas Grupp

Andreas.Grupp@zsl-rstue.de

Carina Haag

haag.c@lanz.schule

Tobias Heine

tobias.heine@springer-schule.de

Uwe Thiessat

uwe.thiessat@gbs-sha.de

- Einen Switch mit den grundlegenden Einstellungen konfigurieren
- Switch-Ports konfigurieren, passend zu den Netzwerkanforderungen
- Einen sicheren Management-Zugriff für einen Switch konfigurieren

- Einen Router über CLI so konfigurieren, dass Routing bei direkt angeschlossenen Netzwerken funktioniert
- Verbindungen zwischen zwei direkt am Router angeschlossenen Netzwerken überprüfen

Bootfolge – Was passiert nach dem Einschalten?

- Schritt 1: Ein power-on-self-test Programm wird aus dem ROM geladen und ausgeführt. Getestet werden die CPU, DRAM und Teile des Flash (Flash Dateisystem aufbauen)
- Schritt 2: Nach erfolgreichem POST wird die boot-loader-software aus dem ROM geladen und ausgeführt.
- Schritt 3: Der boot loader ruft die CPU-Register auf, welche den Hardwarespeicher kontrollieren, ebenso dessen Größe und Zugriffsgeschwindigkeit.
- Schritt 4: Vom boot loader wird das flash Dateisystem auf dem Systemboard aufgerufen.
- Schritt 5: Schlussendlich ermittelt der boot loader ein vorgesehene IOS software image, lädt es in den Speicher und gibt die Kontrolle über den Switch an das IOS ab.

Der Befehl: „boot system“

Ein Switch bootet üblicherweise mittels der Informationen aus der BOOT-Variablen. Ist diese nicht gesetzt, versucht der Switch die erste ausführbare Datei, die er finden kann, zu laden.

In der startup-config Datei, welche als „**config.text**“ im flash liegt, werden die IOS Kommandos gefunden und aufgerufen.

In folgendem Beispiel wird die BOOT Umgebung mit dem Befehl: „**boot system**“ gesetzt. Um die aktuelle IOS Bootdatei zu lokalisieren dient der Befehl: „**show boot**“

```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

globale
Config-
Ebene

Boot system
Haupt-
Befehl

flash:
Pysikalischer
Speicher

c2960-lanbasek9-mz.150-2.SE/
Der Pfad zum Dateisystem

c2960-lanbasek9-mz.150-2.SE.**bin**
Der IOS Dateiname

Die LED-Ampel – Bedeutung der Farbanzeigen

Je nach Switchmodell sind die LED-Anzeigen unterschiedlich!
Beispielanzeigen für den **Catalyst 2960**:

Vollfunktion!

Power ja, aber nur Teilfunktion

Remote Power System funktioniert.
Blinkt: RPS verbunden, versorgt selbst.

Standby oder Fehlermodus.
Blinkt: Eigenversorgung def.; Fremdvers.

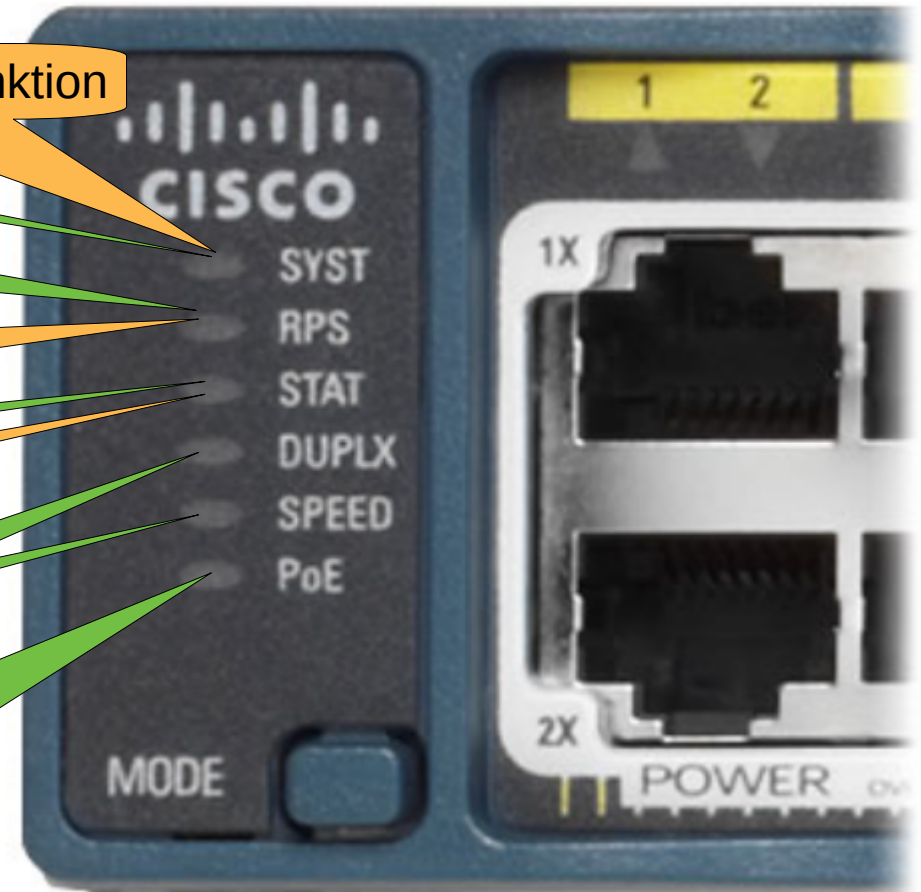
Link ok! Blinkend: Datenaustausch.

Geblockt beim Einschalten!
Blinkt: gelockt wegen LOOPS

Duplex
modus

100MBits/s Blinkt: 1GBits/s

PoE-Modus gewählt. Port-LEDs beachten!



Wiederherstellung nach einem Systemcrash

1. PC mit Konsolenkabel an den Konsolenport des Switch verbinden und Terminal-Software starten.
2. Den Switch von der Stromversorgung trennen.
3. Die Stromversorgung wieder anschliessen und innerhalb 15 Sekunden den Mode-Button drücken und halten während die System LED **grün blinkt**.
4. Solange Mode halten bis die System LED von **amber** zu **grün** wechselt → loslassen!
5. Nun erscheint der Terminalprompt **switch:** „help“ oder „?“ eingeben!

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
```

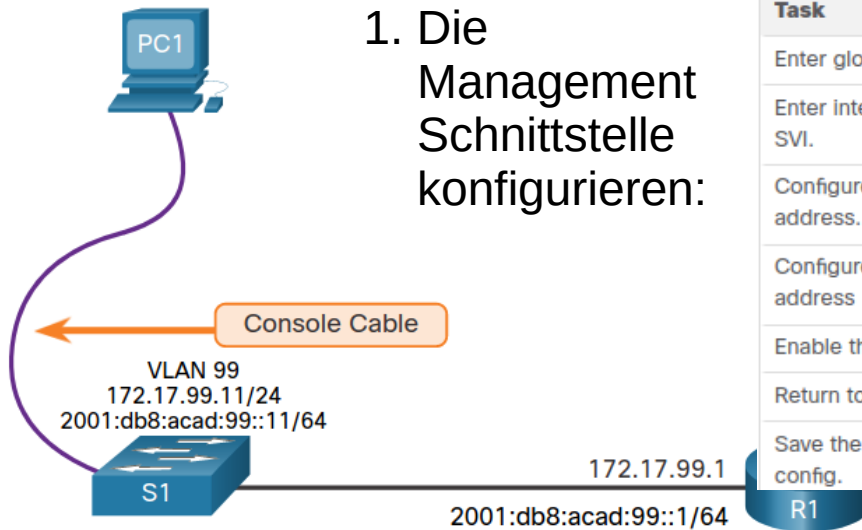
```
switch: dir flash:
Directory of flash:/
 2  -rw- 11834846      c2960-lanbasek9-mz.150-2.SE8.bin
 3  -rw- 2072         multiple-fs
```

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

Die Bootloader-Kommandos unterstützen:

- flash aufrufen;
- Flash formatieren;
- neues IOS installieren;
- Bootvariablen ändern;
- Passwortwiederherstellung;

Den Switch für Verwaltungszugriffe konfigurieren!



Task	IOS Commands
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface vlan 99
Configure the management interface IPv4 address.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Configure the management interface IPv6 address	S1(config-if)# ipv6 address 2001:db8:acad:99::11/64
Enable the management interface.	S1(config-if)# no shutdown
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

2. Ein Default Gateway konfigurieren:

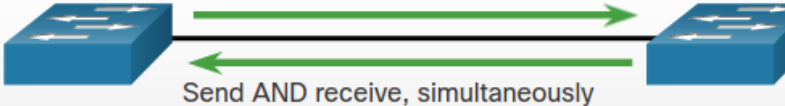
Task	IOS Commands
Enter global configuration mode.	S1# configure terminal
Configure the default gateway for the switch.	S1(config)# ip default-gateway 172.17.99.1
Return to the privileged EXEC mode.	S1(config)# end
Save the running config to the startup config.	S1# copy running-config startup-config

3. Die Konfiguration überprüfen:

```
S1# show ip interface brief
Interface      IP-Address      OK? M
Vlan99         172.17.99.11    YES m
(output omitted)
S1# show ipv6 interface brief
Vlan99         [down/down]
FE80::C27B:BCFF:FEC4:A9C1
2001:DB8:ACAD:99::11
```

Die Switchports konfigurieren 1


Full-Duplex Communication



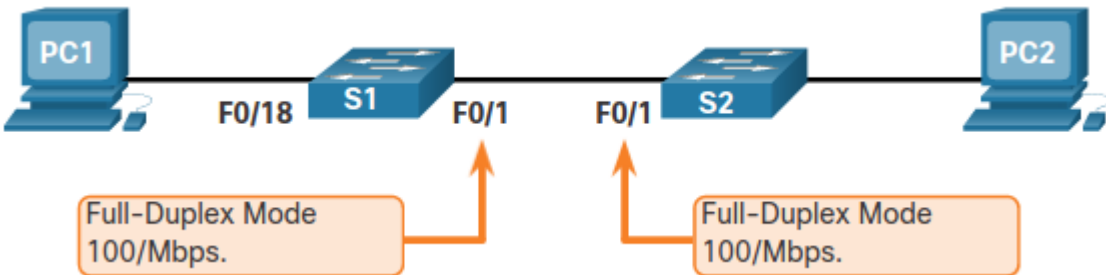
Send AND receive, simultaneously

Task	IOS Commands
Enter global configuration mode.	S1# <code>configure terminal</code>
Enter interface configuration mode.	S1(config)# <code>interface FastEthernet 0/1</code>
Configure the interface duplex.	S1(config-if)# <code>duplex full</code>
Configure the interface speed.	S1(config-if)# <code>speed 100</code>
Return to the privileged EXEC mode.	S1(config-if)# <code>end</code>
Save the running config to the startup config.	S1# <code>copy running-config startup-config</code>

Half-Duplex Communication



Send OR receive



Full-Duplex Mode 100/Mbps.

Full-Duplex Mode 100/Mbps.

Cat 2960 und 3560 mit duplex und speed „auto“;
Bei 1Gbps → full duplex; Für bestimmte Server und Workstations: Werte manuell festlegen!
Fehlersuche: beteiligte Ports benötigen gleiche Einstellungen!

Fiberoptikports wie 1000BASE-SX arbeiten mit einer Geschwindigkeit bei full duplex!

Automatic Medium Dependent Interface Crossover → auto-MDIX ist notwendig, damit sowohl straight through- als auch crossover- Kabel verwendet werden können. Mit auto-MDIX muss sowohl duplex als auch speed auf „auto“ gesetzt sein.

Kommando:

S1(config-if)#mdix auto

Bei Catalyst 2960 und 3560 standardmäßig! Nicht verfügbar bei älteren (2950; 3550)
Konfiguration der Ports überprüfen mit:

```
S1# show controllers ethernet-controller fa0/1 phy | include MDIX
Auto-MDIX           : On   [AdminState=1   Flags=0x00052248]
```

Wie können die Switch-Einstellungen überprüft werden?

Übersicht der wichtigsten „show-Befehle“:

Task	IOS Commands
Display interface status and configuration.	<code>S1# show interfaces [interface-id]</code>
Display current startup configuration.	<code>S1# show startup-config</code>
Display current running configuration.	<code>S1# show running-config</code>
Display information about flash file system.	<code>S1# show flash</code>
Display system hardware and software status.	<code>S1# show version</code>
Display history of command entered.	<code>S1# show history</code>
Display IP information about an interface.	<code>S1# show ip interface [interface-id]</code> OR <code>S1# show ipv6 interface [interface-id]</code>
Display the MAC address table.	<code>S1# show mac-address-table</code> OR <code>S1# show mac address-table</code>

Ein Überblick mit:

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
interface FastEthernet0/18
  switchport access vlan 99
  switchport mode access
!
(output omitted)
!
interface Vlan99
  ip address 172.17.99.11 255.255.255.0
  ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

Einen speziellen Port überprüfen:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

Probleme mit dem Network Access Layer?

Fehler und ihre Ursachen:

Error Type	Description
Input Errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output Errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late Collisions	A collision that occurs after 512 bits of the frame have been transmitted.

Fehlersumme, egal welcher Ursache:
runts, giants, CRC, etc.

Als „zu klein“ verworfene
Frames. Frame < 64Byte

Frames, welche die MTU
überschritten haben.
Frame >1518 Bytes

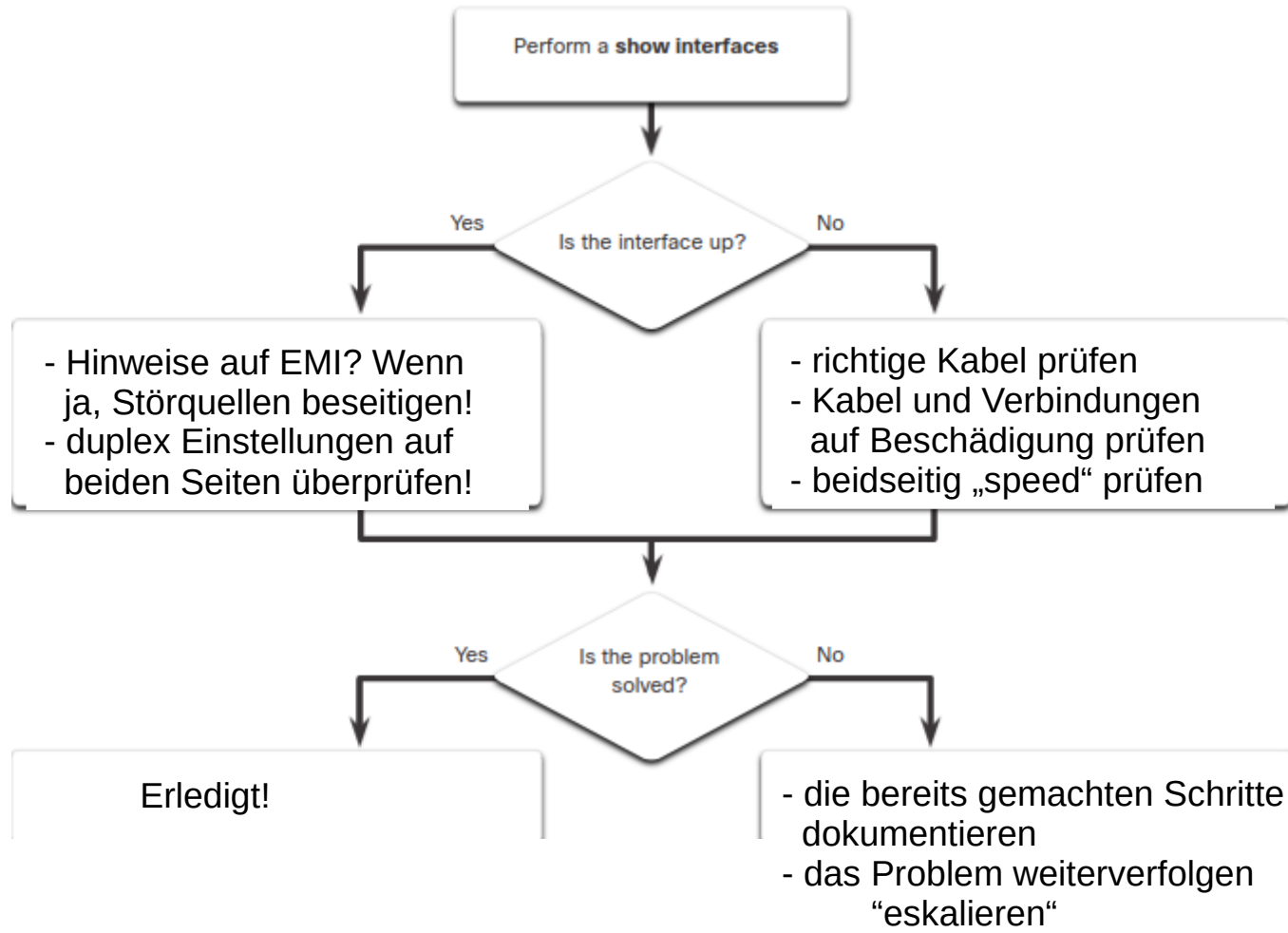
Die übermittelte Prüfsumme
Entspricht nicht der berechneten!

Summe aller Fehler, die dazu
führen, dass ein Datagramm
portbezogen nicht gesendet
wird.

Eine Kollision, welche auftaucht nachdem
64 Byte des Frames übertragen wurden.
Siehe auch: „fragment free“

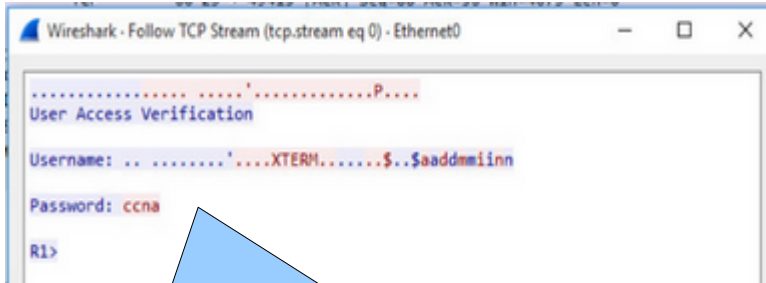
Anzahl der kollisionsbedingten
Zweitübertragungen.

Fehlersuche bei Network Access Layer Problemen.



Den Fernzugriff absichern von Telnet zu SSH

Bei Telnet:



```
.....P....
User Access Verification

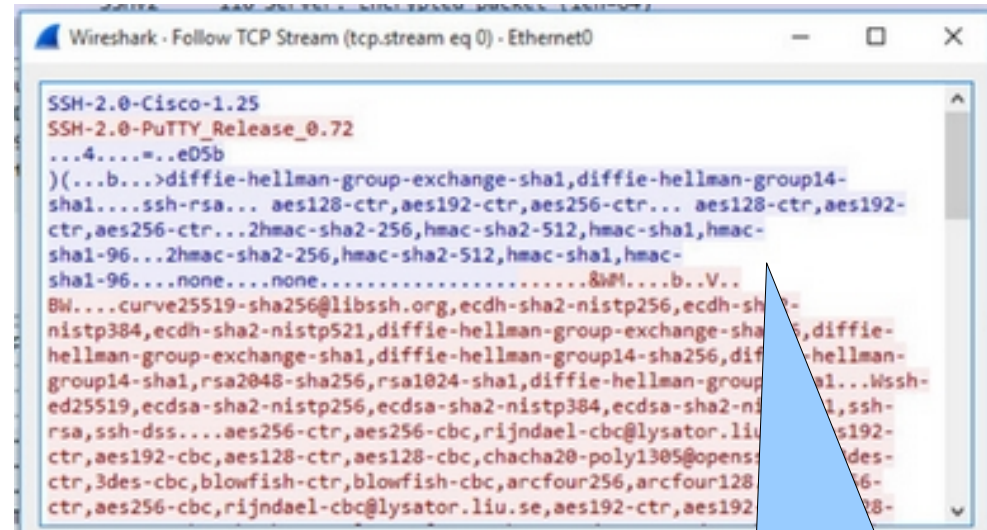
Username: .. .....XTERM.....$. $aaddmiinn

Password: ccna

R1>
```

Klartext Übertragung!

Bei SSH:



```
SSH-2.0-Cisco-1.25
SSH-2.0-PuTTY_Release_0.72
...4....=..e05b
)(...b...>diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1...ssh-rsa... aes128-ctr,aes192-ctr,aes256-ctr... aes128-ctr,aes192-
ctr,aes256-ctr...2hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-
sha1-96...2hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-
sha1-96...none...none.....8&M....b..V..
BW...curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha1,diffie-
hellman-group-exchange-sha1,diffie-hellman-group14-sha256,dif-
hellman-group14-sha1,rsa2048-sha256,rsa1024-sha1,diffie-hellman-group14-sha1...Wssh-
ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-
rsa,ssh-dss...aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-
ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.org,des-
ctr,3des-cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,
ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,des-

```

Verschlüsselte Übertragung
Mit Diffie-Hellman-Algorithmus

Unterstützt der Switch SSH?:

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE
SOFTWARE (fc1)
```

IOS „k9“ im Dateinamen

Minimale Voraussetzungen für die SSH Konfiguration sind ein eindeutiger Hostname und korrekte Netzwerk Verbindungseinstellungen.

Schritt 1: die SSH Unterstützung prüfen!

```
S1#show ip ssh
```

Schritt 2: die IP-Domäne konfigurieren!

```
S1(config)#ip domain-name meinedomain.com
```

Schritt 3: RSA Schlüsselpaare erzeugen!

```
S1(config)# crypto key generate rsa  
How many bits in the modulus [512]: 1024
```

Schritt 5: vty konfigurieren!

```
S1(config)# line vty 0 15  
S1(config-line)# transport input ssh  
S1(config-line)# login local  
S1(config-line)# exit
```

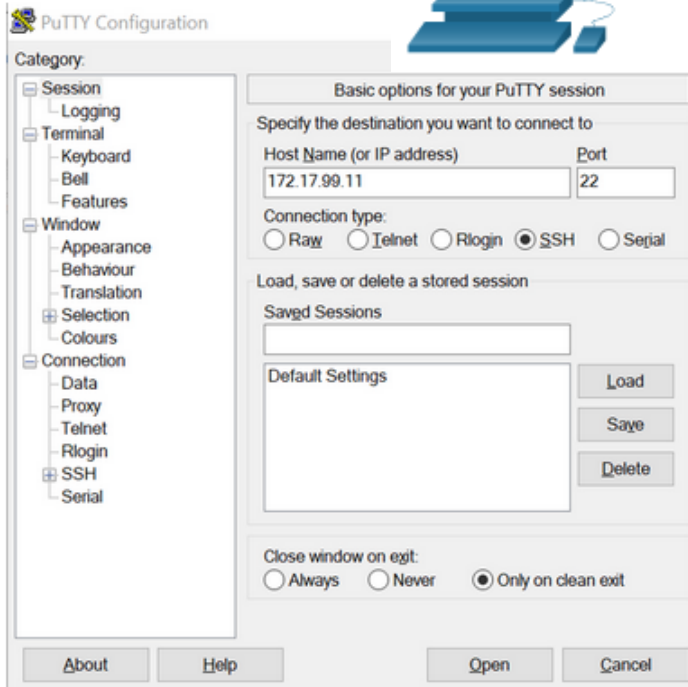
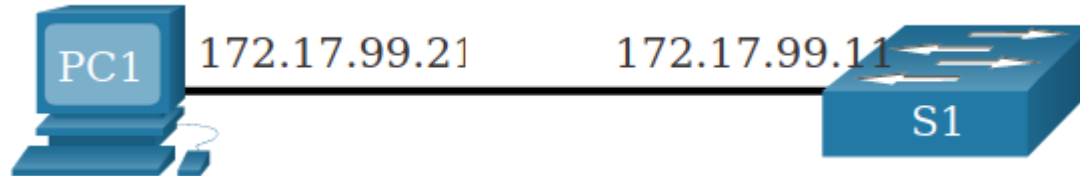
Schritt 6: SSH Version 2 aktivieren!

```
S1(config)# ip ssh version 2
```

Schritt 4: User Authentifizierung konfigurieren!

```
S1(config)#username admin secret ccna
```

Testen, ob SSH Zugriff funktioniert



```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-sha1 Session started admin
0 2.0 OUT aes256-cbc hmac-sha1 Session started admin
```


Grundeinstellungen beim Router – schon bekannt?

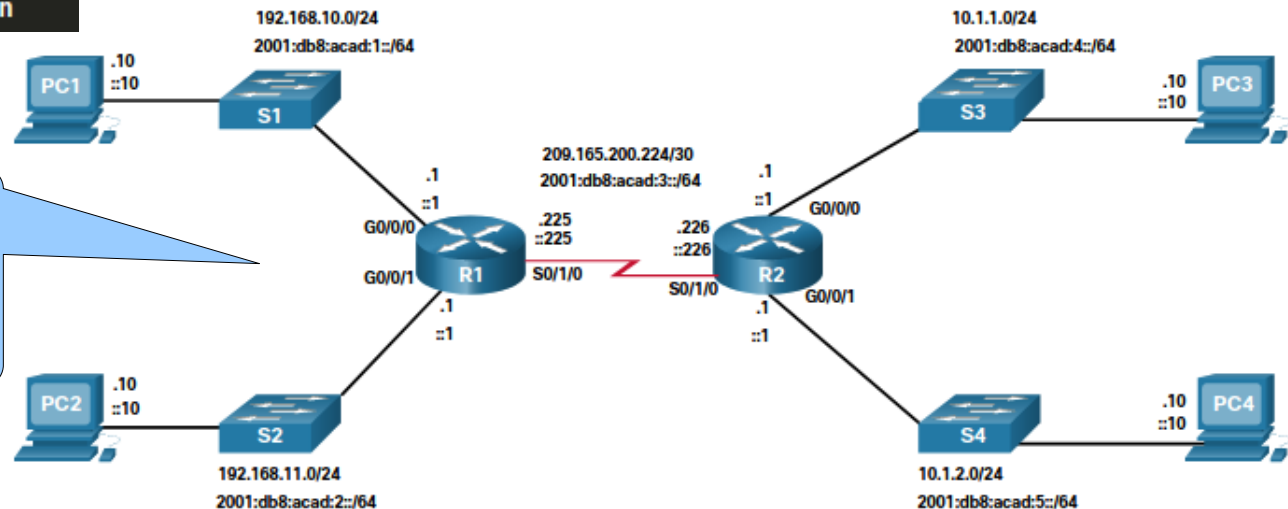
```
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
```

```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Bei Router
und Switch
Identisch!

Dual Stack Konfiguration.
IPv4 und IPv6 sind
Parallel konfiguriert.



Konfiguration der Router Schnittstellen – schon bekannt?

Sowohl LAN- als auch WAN-Schnittstellen sind zunächst deaktiviert und müssen mit „no shutdown“ aktiviert werden!

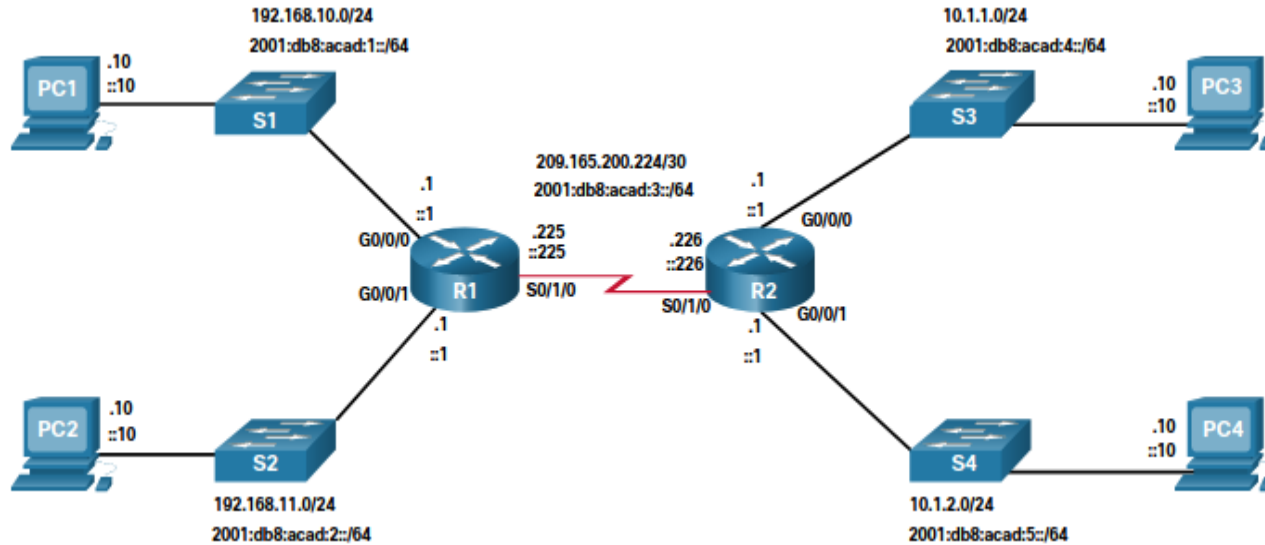
```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
```

Nun etwas Neues, das Loopback-Interface. Nicht physikalisch, rein virtuell. Mehrere auf einem Router konfigurierbar.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
```

Wozu dieses?
Management,
Testen,
Simulation,
dyn. Routing,
Die Adresse muss einzigartig sein!

Schnittstellen Konfigurationen überprüfen – schon bekannt?



```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
description Link to LAN 1
ip address 192.168.10.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:1::1/64
end
```

```
R1# show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0  192.168.10.1    YES manual up          up
GigabitEthernet0/0/1  192.168.11.1    YES manual up          up
Serial0/1/0       209.165.200.225 YES manual up          up
Serial0/1/1       unassigned      YES unset  administratively down down

R1# show ipv6 interface brief
GigabitEthernet0/0/0  [up/up]
FE80::7279:B3FF:FE92:3130
2001:DB8:ACAD:1::1
GigabitEthernet0/0/1  [up/up]
FE80::7279:B3FF:FE92:3131
2001:DB8:ACAD:2::1
Serial0/1/0          [up/up]
FE80::7279:B3FF:FE92:3130
2001:DB8:ACAD:3::1
Serial0/1/1          [down/down] Unassigned
```

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
FF02::1
FF02::1:FF00:1
FF02::1:FF92:3130
MTU is 1500 bytes
```

IPv6-
Multicastadressen

Die Routingtabelle überprüfen mit „show ip route“ und show „ipv6 route“

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
 192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/30 is directly connected, Serial0/1/0
L    209.165.200.225/32 is directly connected, Serial0/1/0

R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C    2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L    2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C    2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L    2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C    2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/0, directly connected
L    2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/0, receive
L    FF00::/8 [0/0]
    via Null0, receive
```

Direct connected mit zugehörigem Routerinterface. AD=0

Local Host Route mit /32 bei IPv4
AD=0

Direct connected mit zugehörigem Routerinterface. AD=0

Local Host Route mit /128 bei IPv6
AD=0

```
R1# ping 2001:db8:acad:1::10
```

ping für IPv6

Filter für die „show“ Befehle – gezielte Auswahl treffen

```
R1# show running-config | section line vty
line vty 0 4
password 7 110A1016141D
login
transport input all
```

Zeigt den gesamten Bereich, der mit Dem Bereichsbegriff beginnt.

```
R1# show ip interface brief | include up
GigabitEthernet0/0/0 192.168.10.1 YES manual up
GigabitEthernet0/0/1 192.168.11.1 YES manual up
Serial0/1/0 209.165.200.225 YES manual up
```

Alle Ausgabezeilen, welche den Filterausdruck beinhalten.

```
R1# show ip interface brief | exclude unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up
GigabitEthernet0/0/1 192.168.11.1 YES manual up
Serial0/1/0 209.165.200.225 YES manual up
```

Zeilen mit diesem Ausdruck werden nicht angezeigt.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
```

Die Ausgabe beginnt ab Diesem Begriff (einschliesslich)

```
R1# terminal history size 200
R1# show history
show ip int brief
show interface g0/0/0
show ip route
show running-config
show history
terminal history size 200
```

Standardmäßig werden 10 CLI-Kommandos gespeichert, dieser Wert kann angepasst werden.
Durchscrollen der Befehle mit Pfeiltasten.

- 1.1.7 Lab – Basic Switch Configuration
- 1.3.6 PT – Configure SSH
- 1.4.7 PT – Configure Router Interfaces
- 1.5.10 PT – Verify Directly Connected Networks
- 1.6.1 PT – Implement a Small Network
- 1.6.2 Lab – Configure Basic Router Settings

