

# Telekommunikationsnetze Praktika 1

Eschreiter, 5.5.2017

## Hintergrund

- Netzwerkgeräte Infrastruktur und Endpunkte (Router, Switch, Server, AP ...) sollen aus der Ferne administriert werden, dafür müssen sie eine Grundkonfiguration erhalten
- Auch für Notfall, wenn etwas verstellt ist, falsch konfiguriert wurde → Zugriff muss möglich sein
- Mit physikalischem Zugriff auf Gerät ist Zugriff/Übernahme möglich, evtl. unter Verlust der Einstellungen! (Zurücksetzen mit Löschen der Konfiguration und Passwörtern)
- Deswegen: Passwort Schutz!

## Inhalt des Praktikums

- Kennenlernen der Menü/ Kommandostruktur im Betriebssystem der Geräte
- Vorbereiten eines Geräts für Fernzugriff über Netzwerk (Achtung: hier nur mit Telnet = Unverschlüsselt; im Praxiseinsatz per SSH = Verschlüsselt)
- Verschiedene Modi / Menüeinträge / Befehlskontexte
- Hilfesystem mit ?
- Redundanz der Befehle, Aliases
- History
- Hier: kein „copy running-config startup-config“ → kein dauerhaftes Speichern in den FLASH durchführen
- Gerät für Zugriff per Telnet vorbereiten und testen

## Unterlagen: Vorlesung Prof. Scharf

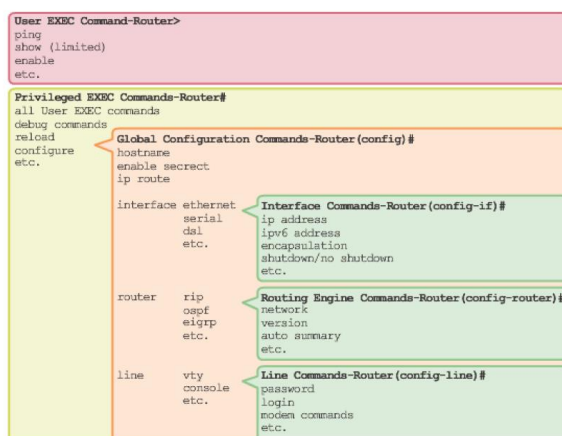


Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>Change terminal settings.</li> <li>Perform basic tests.</li> <li>Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>Issue <b>show</b> and <b>debug</b> commands.</li> <li>Copy images to the device.</li> <li>Reload the device.</li> <li>Manage device configuration files.</li> <li>Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router (config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router (config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router (config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual terminal lines.

Quelle: Cisco, ITN\_instructorPPT\_Chapter2\_final.pptx Seite 14

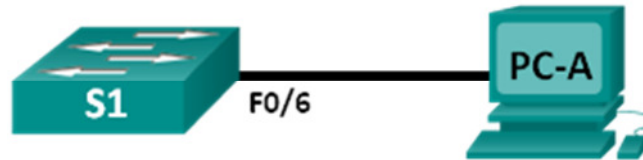
[http://www.cisco.com/c/en/us/td/docs/ios/iproute\\_bfd/configuration/guide/15\\_1/1rb\\_15\\_1\\_book.pdf](http://www.cisco.com/c/en/us/td/docs/ios/iproute_bfd/configuration/guide/15_1/1rb_15_1_book.pdf) Seite 17

Am Ende des Praktika, Telnet-Zugriff und erfolgreiche PING-Ausführung demonstrieren.

Dokumentieren Sie sich die genutzten Befehle für den 2. Versuch. Es ist kein Protokoll abzugeben.

## Lab - Configuring a Switch Management Address

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	N/A

### Objectives

#### Part 1: Configure a Basic Network Device

- Cable the network as shown in the topology.
- Configure basic switch settings including hostname, management address, and Telnet access.
- Configure an IP address on the PC.

#### Part 2: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capability with Telnet.
- Save the switch running configuration file.

### Background / Scenario

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address that is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings and IP addressing, and demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

**Note:** The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the available commands and output produced might vary from what is shown in the labs.

**Note:** Make sure that the switch has been erased and has no startup configuration. If you are unsure, contact your instructor.

### Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

## Lab - Configuring a Switch Management Address

---

- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

### Part 1: Configure a Basic Network Device

In Part 1, you will set up the network and configure basic settings, such as hostnames, interface IP addresses, and passwords.

#### Step 1: Cable the network.

- a. Cable the network as shown in the topology.
- b. Establish a console connection to the switch from PC-A.

#### Step 2: Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname and configuring an IP address for the SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and Secure Shell (SSH) are two of the most common management methods; however, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), you will be at the user EXEC mode prompt on the switch with a prompt of `Switch>`. Enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

- b. Verify a clean configuration file with the `show running-config` privileged EXEC command. If a configuration file was previously saved, it will have to be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address set. If your switch does not have a default configuration, ask your instructor for help.

- c. Enter global configuration mode and assign the switch hostname.

```
Switch# configure terminal  
Switch(config)# hostname S1  
S1(config)#
```

- d. Configure the switch password access.

```
S1(config)# enable secret class  
S1(config)#
```

- e. Prevent unwanted Domain Name System (DNS) lookups.

```
S1(config)# no ip domain-lookup  
S1(config)#
```

- f. Configure a login message-of-the-day (MOTD) banner.

```
S1(config)# banner motd #  
Enter Text message. End with the character `#'.  
Unauthorized access is strictly prohibited. #
```

## Lab - Configuring a Switch Management Address

---

- g. Verify your access setting by moving between modes.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

---

- h. Return to privileged EXEC mode from user EXEC mode.

```
S1> enable
Password: class
S1#
```

**Note:** Password will not show up on screen when entering.

- i. Enter global configuration mode to set the SVI IP address to allow remote switch management.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

- j. Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

- k. Configure the virtual terminal (VTY) line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to Telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

## Lab - Configuring a Switch Management Address

---

### Step 3: Configure an IP address on PC-A.

- a. Assign the IP address and subnet mask to the PC, as shown in the Addressing Table on page 1. The procedure for assigning an IP address on a PC running Windows 7 is described below:
  - 1) Click the **Windows Start** icon > **Control Panel**.
  - 2) Click **View By:** > **Category**.
  - 3) Choose **View network status and tasks** > **Change adapter settings**.
  - 4) Right-click **Local Area Network Connection** and select **Properties**.
  - 5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties** > **OK**.
  - 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

## Part 2: Verify and Test Network Connectivity

You will now verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the remote management capability of the switch.

### Step 1: Display the S1 device configuration.

- a. Return to your console connection using Tera Term on PC-A to display and verify your switch configuration by issuing the **show run** command. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
```

## Lab - Configuring a Switch Management Address

---

```
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

- b. Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port F0/6 is also up because PC-A is connected to it. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
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	up	up

## Lab - Configuring a Switch Management Address

FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
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	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

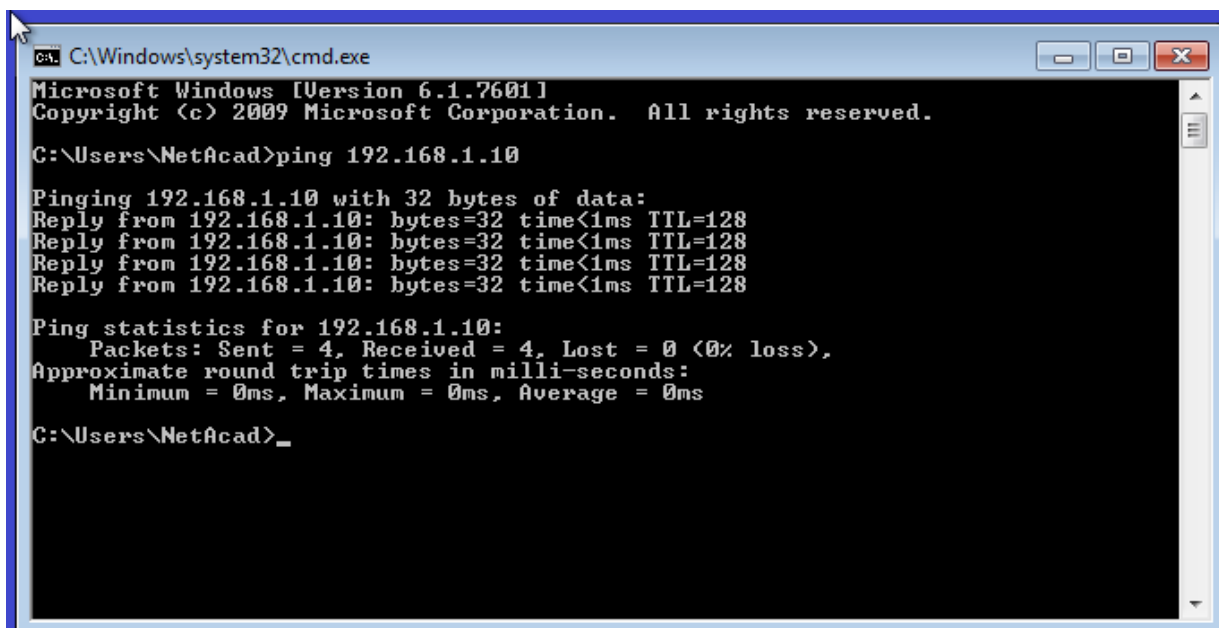
### Step 2: Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and enter **cmd** into the **Search for programs and files** field. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information. Ping PC-A's own address and the management address of S1.

- a. Ping your own PC-A address first.

```
C:\Users\NetAcad> ping 192.168.1.10
```

Your output should be similar to the following screen:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>_
```

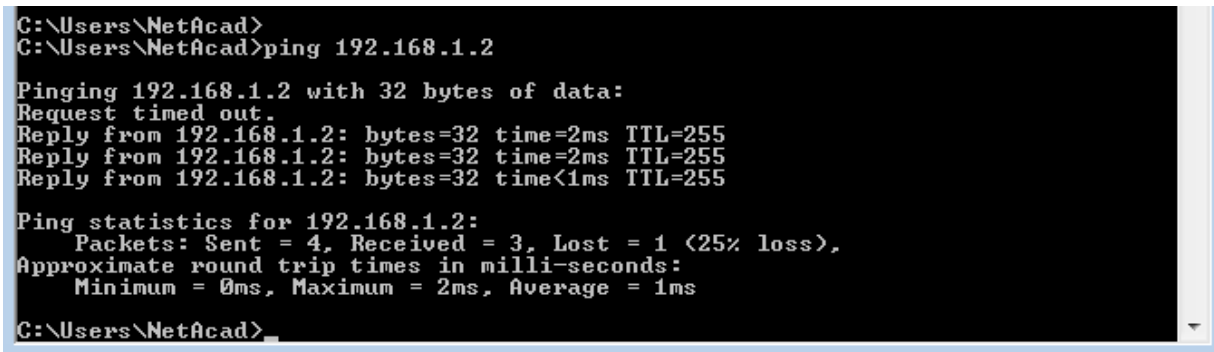
## Lab - Configuring a Switch Management Address

---

- b. Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

Your output should be similar to the following screen. If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing, if necessary.



```
C:\Users\NetAcad>
C:\Users\NetAcad>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

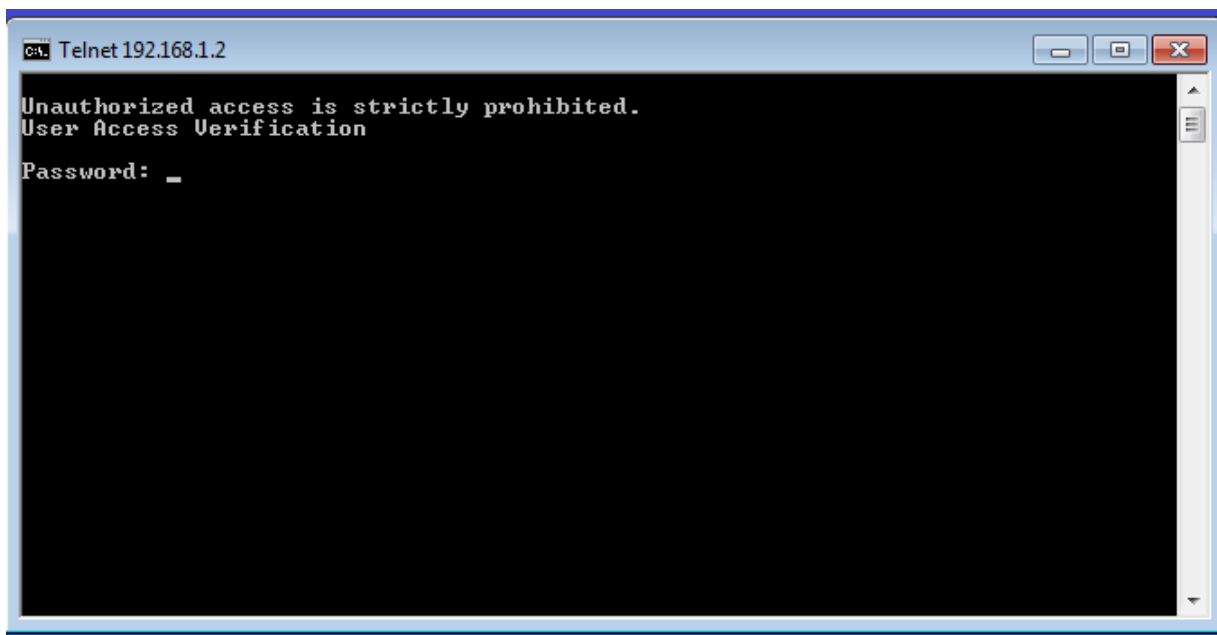
C:\Users\NetAcad>
```

### Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plain text. In real life, you should use Secure Shell (SSH) to remotely access network devices.

**Note:** Use TerraTerm to access S1 with Telnet. End the program and restart or start a second session and chose telnet with the IP address of S1.

Your output should be show a text similar to the following screen:



```
c:\ Telnet 192.168.1.2

Unauthorized access is strictly prohibited.
User Access Verification

Password: _
```



## Lab - Configuring a Switch Management Address

---

- a. After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

### Step 4: **For real live only, not in this lab!!!** Save the configuration file.

- a. From your Telnet session, issue the **copy run start** command at the prompt.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

### Reflection

Why must you use a console connection to initially configure the switch? Why not connect to the switch via Telnet or SSH?

---

---