Lab – Basic Device Configuration

Topology

Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0	192.168.1.1 /24	N/A
		2001:db8:acad::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1 /64	
		fe80::1	
S1	VLAN 99	192.168.1.10 /24	192.168.1.1
		2001:db8:acad::10 /64	fe80::1
PC-A	NIC	192.168.1.11 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure an SVI and verify its status

Part 3: Configure the SSH

Part 4: Configure the basic router settings and interfaces

Part 5: Verify the network connectivity

Background / Scenario

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch and router using the console and remote access methods.

You will examine default switch configurations, configuration the SSH on the switch and configuring basic router settings. These basic router settings include device name, interface description, local passwords, message of the day (MOTD) banner, IP addressing, and static MAC address.

You will also demonstrate the use of a management IP address for remote switch and router management.

Cable the Network and Verify the Default Switch Configuration

In Part 1, you will connect the console and network cable between the PC-A and the switch S1. Let's first have a look on the bootloader, then when the switch will be loaded, you will then verify the default switch settings.

a. Connect the console cable to the switch.

b. Start on the bootloader

c. List few commands that you can use:

Switch>?

d. What is the command you need to use to boot on the IOS?

The switch is now loading the IOS…

e. Examine the current running configuration file.

en
show running-config

- How many FastEthernet interfaces does the switch have?

  24

- How many Gigabit Ethernet interfaces does the switch have?

  2

- What is the range of values shown for the vty lines?

  5 15

f. Examine the startup configuration file in NVRAM.

Switch#show startup-config

- What message did you get and why?

  startup-config is not present

g. Examine the flash memory.

- What 2 commands could you use for that?

  Switch#dir flash:

  Switch#dir nvram:

h. Examine the Cisco IOS version information of the switch.

Switch#show version

- What is the version installed?

  Version 15.0(2)SE7

- What is the uptime of the switch?

  Switch uptime is 14 minutes

Configure an SVI and verify its status

In Part 2, you will configure an SVI and verify its status.

a. Examine the characteristics of the SVI for VLAN 1.

Switch#show interfaces vlan 1

- Is there an IP address assigned to VLAN 1?

  No

b. Examine the IP properties of the SVI VLAN 1.

Switch#show ip interface vlan 1

- What output do you see?

  Vlan1 is administratively down, line protocol is down

  Internet protocol processing disabled

- Why the line protocol is down?

  Parce que nous l'avons pas active et il y a rien qui est connecté au switch

c. Set the SVI IP address of the switch according to the addressing table

en

conf t

sdm prefer dual-ipv4-and-ipv6 default

interface vlan 99

ip address 192.168.1.10 255.255.255.0

ipv6 address 2001:db8:acad::10/64

ipv6 address fe80::1 link-local

no shutdown

exit

ip default-gateway 192.168.1.1

- What is the status of the VLAN 99?

- Why the VLAN 99 is down?

  Yes

d. Assign all user ports to VLAN99.

en

interface range fastEthernet 0/1-24

switchport access vlan 99

(% Access VLAN does not exist. Creating vlan 99)

e. Configure the default gateway for S1.

- What do you think it happens if you do not configure it?

Configure the SSH

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In Part 3, you will secure a remote switch with password encryption and SSH.

a. Create an **admin** user with cisco as the password.

Switch(config)#username admin password cisco

b. Create the EXEC password class.

Switch(config)#enable secret class

c. Show the current configuration.

Show running-config

- Are you able to see the admin's password in plain text?

  Yes

d. Enter the command to encrypts plain text password.

Switch(config)#service password-encryption

e. Verify that the password is encrypted.

Show running-config

- What type of encryption is used?

  7

f. Configure the domain name to be cpne.ch.

Switch(config)#ip domain name cpne.ch

g. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

Switch(config)#crypto key generate Rsa general-keys modulus 1024

h. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access.

Switch(config)#line vty 0 4

Switch(config-line)#login local

i. Are you able to ping S1 from PC-A?

OUI

j. Verify SSH implementation, connect to the switch with SSH from PC-A.

Configure the basic router settings and interfaces

In part 4, your task is to configure the basic settings of the router and the appropriate addressing on R1.

a. Assign a name to the router.

   Router(config)#hostname R1

b. Set the router's domain name as cpne.ch.

   R1(config)#ip domain name cpne.ch

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

   R1(config)#no ip domain lookup

d. Encrypt the plaintext passwords.

   R1(config)#service password-encryption

e. Configure the system to require a minimum 12-character password.

   R1(config)#security passwords min-length 12

f. Configure the username SSHadmin with an encrypted password of 55Hadm!n2024.

   R1(config)#username SSHadmin secret 55Hadmin!n2024

g. Generate a set of crypto keys with a 1024 bit modulus

   R1(config)#crypto key generate rsa modulus 1024

h. Assign the privileged EXEC password to $cisco!PRIV*

   R1(config)#enable secret $cisco!Priv*

i. Assign $cisco!!CON* as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.

   R1(config)#line console 0

   R1(config-line)#password $cisco!!CON*

j. Assign $cisco!!VTY* as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.

   R1(config)#line vty 0 4

   R1(config-line)#password $cisco!!VTY*

k. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

   R1(config)#banner motd 'Securized'

l. Enable IPv6 Routing.

   R1(config)#ipv6 unicast-routing

m. Configure all interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all interfaces with descriptions and activate them.

   R1(config)#interface g0/0

   R1(config-if)#ip address 192.168.1.1 255.255.255.0

   R1(config-if)#ipv6 address 2001:db:acad::1/64

   R1(config-if)#ipv6 address fe80::1 link-local

   R1(config-if)#no shutdown

(La même chose pour loopback0)

n. The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

o. Set the clock on the router.

p. Save the running configuration to the startup configuration file.

What would be the result of reloading the router prior to completing the copy running-config startup-config command?

Verify the network connectivity

In part 5, your task is to check the connectivity between PC-A, S1 and R1.

a. Examine the default properties of the FastEthernet interface used by PC-A on S1.
   - Is the interface up or down?
   - What is the speed and duplex setting of the interface?

b. Display the mac addresses of that port.

c. Using the command line at PC-A, ping the IPv4 and IPv6 addresses for R1.
   - Were the pings successful?

d. Remotely access R1 from PC-A using the Tera Term SSH client.
   - Was remote access successful?

e. Display the routing table on the router.
   - What code is used in the routing table to indicate a directly connected network?

f. Display a summary list of the interfaces on the router.

In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What show command could the technician use to troubleshoot this issue?

Jocker *(please contact instructor before doing it)*:

g. There is an issue while connecting directly to R1 from PC-A in SSH, find another way…