

Lab – Configuring Basic Router Settings with IOS CLI (Instructor

Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 information to the PC interfaces.
- Configure basic router settings.
- Verify network connectivity.
- Configure the router for SSH.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

Part 4: Configure IPv6 and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and IPv4 interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize IOS commands to retrieve information from the device to answer questions about the router. In Part 4, you will configure IPv6 on the router so that PC-B can acquire an IP address and then verify connectivity.

For review purposes, this lab provides the commands necessary for specific router configurations.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (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

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable can be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

- a. Attach the devices as shown in the topology diagram, and cable as necessary.
- b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Note: Appendix A details the steps to initialize and reload the devices.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

a. Console into the router and enable privileged EXEC mode.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Router> enable

Router#

b. Enter into global configuration mode.

```
Router# config terminal
Router(config)#
```

c. Assign a device name to the router.

```
Router(config) # hostname R1
```

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

```
R1(config) # no ip domain-lookup
```

e. Require that a minimum of 10 characters be used for all passwords.

```
R1(config) # security passwords min-length 10
```

Besides setting a minimum length, list other ways to strengthen passwords.

Use capital letters, numbers, and special characters in passwords.

f. Assign **cisco12345** as the privileged EXEC encrypted password.

```
R1(config) # enable secret cisco12345
```

g. Assign ciscoconpass as the console password, establish a timeout, enable login, and add the logging synchronous command. The logging synchronous command synchronizes debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

```
R1(config) # line con 0
R1(config-line) # password ciscoconpass
R1(config-line) # exec-timeout 5 0
R1(config-line) # login
R1(config-line) # logging synchronous
R1(config-line) # exit
R1(config) #
```

For the exec-timeout command, what do the 5 and 0 represent?

The session will timeout in 5 minutes and 0 seconds.

h. Assign **ciscovtypass** as the vty password, establish a timeout, enable login, and add the **logging synchronous** command.

```
R1(config) # line vty 0 4
R1(config-line) # password ciscovtypass
R1(config-line) # exec-timeout 5 0
R1(config-line) # login
R1(config-line) # logging synchronous
R1(config-line) # exit
R1(config) #
```

i. Encrypt the clear text passwords.

```
R1(config) # service password-encryption
```

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

```
R1(config) # banner motd #Unauthorized access prohibited!#
```

k. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config) # int g0/0
R1(config-if) # description Connection to PC-B
R1(config-if) # ip address 192.168.0.1 255.255.255.0
R1(config-if) # no shutdown
R1(config-if) # int g0/1
R1(config-if) # description Connection to S1
R1(config-if) # ip address 192.168.1.1 255.255.255.0
R1(config-if) # no shutdown
R1(config-if) # exit
R1(config) # exit
R1#
```

I. Set the clock on the router; for example:

```
R1# clock set 17:00:00 18 Feb 2013
```

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

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

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

The contents of the running configuration would be erased. In this lab, the router would have no startup configuration. Upon a reboot, a user would be asked if they would like to enter initial configuration dialog.

Step 3: Verify network connectivity.

a. Ping PC-B from a command prompt on PC-A.

Note: It may be necessary to disable the PCs firewall.

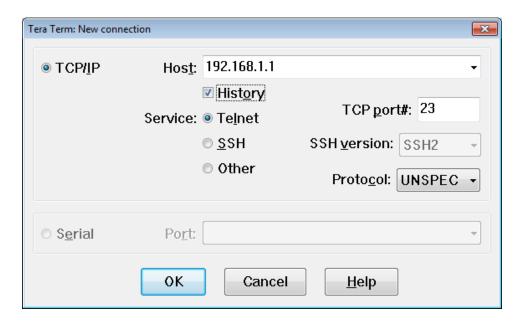
Were the pings successful? Yes

After completing this series of commands, what type of remote access could be used to access R1?

Telnet

b. Remotely access R1 from PC-A using the Tera Term Telnet client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **Telnet** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? Yes

Why is the Telnet protocol considered to be a security risk?

A Telnet session can be seen in clear text. It is not encrypted. Passwords can easily be seen using a packet sniffer.

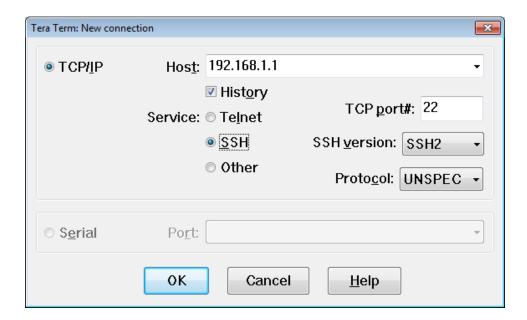
Step 4: Configure the router for SSH access.

a. Enable SSH connections and create a user in the local database of the router.

```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
```

b. Remotely access R1 from PC-A using the Tera Term SSH client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? Yes

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to R1 at IP address 192.168.0.1 and log in as **admin** with the password **adminpass1**.

Step 2: Retrieve important hardware and software information.

a. Use the **show version** command to answer questions about the router.

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod rel team
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
R1 uptime is 10 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
Last reload type: Normal Reload
Last reload reason: power-on
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
```

```
Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.

Processor board ID FTX1636848Z

2 Gigabit Ethernet interfaces

2 Serial(sync/async) interfaces

1 terminal line

DRAM configuration is 64 bits wide with parity disabled.

255K bytes of non-volatile configuration memory.

250880K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

Device	# PID	SN	
*0	CISCO1941/K9	FTX1636848Z	

Technology Package License Information for Module: 'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

ipbase ipbasek9 Permanent ipbasek9

ipbase ipbasek9 Permanent ipbase security None None None data None None None

Configuration register is 0x2142 (will be 0x2102 at next reload)

What is the name of the IOS image that the router is running?

Image version may vary, but answers should be something like c1900-universalk9-mz.SPA.152-4.M3.bin. How much non-volatile random-access memory (NVRAM) does the router have?

Answers may vary, but the output from the **show version** on 1941 router is: 255K bytes of non-volatile configuration memory.

How much Flash memory does the router have?

Answers may vary, but the default output from the **show version** command on the 1941 router is 250880K bytes of ATA System CompactFlash 0 (Read/Write).

b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version** | **include register** to answer the following question.

```
R1# show version | include register
Configuration register is 0x2142
```

What is the boot process for the router on the next reload?

Answers may vary. In most cases (0x2102), the router will undergo a normal boot, load the IOS from the Flash memory, and load the startup configuration from the NVRAM if present. If the config register is 0x2142, the router will bypass the startup config and begin at the user-mode command prompt. If the initial boot fails, the router goes into ROMMON mode.

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

```
R1# show start
Using 1674 out of 262136 bytes
1
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname R1
boot-start-marker
boot-end-marker
security passwords min-length 10
enable secret 4 3mxoP2KRPf3sFHY16Vm6.ssJJi9t0Jqqb6DMG/YH5No
no aaa new-model
no ipv6 cef
ip source-route
```

```
1
no ip domain lookup
ip domain name CCNA-lab.com
ip cef
multilink bundle-name authenticated
1
license udi pid CISCO2911/K9 sn FTX1636848Z
username admin privilege 15 secret 7 1304131f020214B383779
interface Embedded-Service-Engine0/0
no ip address
shutdown
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0/0
no ip address
shutdown
clock rate 200 0000
interface Serial0/0/1
no ip address
shutdown
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
1
banner motd ^CUnauthorized access prohibited!^C
line con 0
```

```
exec-timeout 5 0
password 7 060506324F410A160B0713181F
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
exec-timeout 5 0
password 7 060506324F411F0D1C0713181F
logging synchronous
login local
transport input ssh
scheduler allocate 20000 1000
end
```

How are passwords presented in the output?

Passwords are encrypted due to the service password-encryption command. The line con password of ciscoconpass is encrypted as 060506324F410A160B0713181F. The line vty password of ciscovtypass is encrypted as 060506324F411F0D1C0713181F.

Use the **show startup-config | begin vty** command.

```
line vty 0 4
  exec-timeout 5 0
  password 7 060506324F411F0D1C0713181F
  login local
  transport input ssh
!
scheduler allocate 20000 1000
end
```

What is the result of using this command?

A user receives the startup configuration output beginning with the line that includes the first instance of the filtering expression.

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
        192.168.0.0/24 is directly connected, GigabitEthernet0/0
С
т.
        192.168.0.1/32 is directly connected, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C
         192.168.1.0/24 is directly connected, GigabitEthernet0/1
L
         192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

What code is used in the routing table to indicate a directly connected network?

The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.

How many route entries are coded with a C code in the routing table? _____ 2

Step 5: Display a summary list of the interfaces on the router.

Use the **show ip interface brief** command on the router to answer the following question.

```
R1# show ip interface brief
Interface
                         IP-Address
                                        OK? Method Status
Embedded-Service-Engine0/0 unassigned
                                       YES unset administratively down down
                         192.168.0.1
GigabitEthernet0/0
                                      YES manual up
GigabitEthernet0/1
                        192.168.1.1
                                       YES manual up
Serial0/0/0
                         unassigned
                                        YES unset administratively down down
Serial0/0/1
                        unassigned
                                        YES unset administratively down down
```

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

no shutdown

Part 4: Configure IPv6 and Verify Connectivity

Step 1: Assign IPv6 addresses to R1 G0/0 and enable IPv6 routing.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking, because both the IPv4 and IPv6 protocol stacks are active. By enabling IPv6 unicast routing on R1, PC-B receives the R1 G0/0 IPv6 network prefix and can autoconfigure its IPv6 address and its default gateway.

a. Assign an IPv6 global unicast address to interface G0/0, assign the link-local address in addition to the unicast address on the interface, and enable IPv6 routing.

```
R1# configure terminal
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit
```

b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

```
R1#show ipv6 int brief
```

```
Em0/0 [administratively down/down]
unassigned

GigabitEthernet0/0 [up/up]
FE80::1
2001:DB8:ACAD:A::1

GigabitEthernet0/1 [up/up]
unassigned

Serial0/0/0 [administratively down/down]
unassigned

Serial0/0/1 [administratively down/down]
Unassigned
```

If no IPv6 address is assigned to G0/1, why is it listed as [up/up]?

The [up/up] status reflects the Layer 1 and Layer 2 status of the interface and does not rely on Layer 3 for status.

c. Issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

Answers will vary. IPv6 address of 2001:db8:acad:a:d428:7de2:997c:b05a

What is the default gateway assigned to PC-B? _______ fe80::1

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful? _____ Yes

rcessful?

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad:a::1. Was it successful? ___Yes

Reflection

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

Answers may vary. However, show ip interface brief or show startup-config would provide the information.

2. 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?

show startup-config or show running-config

3. After configuring IPv6 on the R1 G0/0 PC-B LAN, if you were to ping from PC-A to the PC-B IPv6 address, would the ping succeed? Why or why not?

The ping would fail because R1 interface G0/1 was not configured with IPv6 and PC-A only has an IPv4 address.

Router Interface Summary Table

Router Interface Summary						
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2		
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)		
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Appendix A: Initializing and Reloading a Router and Switch

Step 1: Initialize and reload the router.

a. Console into the router and enable privileged EXEC mode.

Router> enable
Router#

b. Type the erase startup-config command to remove the startup configuration from NVRAM.

Router# erase startup-config

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

Erase of nvram: complete

Router#

c. Issue the **reload** command to remove an old configuration from memory. When prompted to **Proceed with reload**, press Enter to confirm the reload. (Pressing any other key aborts the reload.)

```
Router# reload

Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

Note: You may be prompted to save the running configuration prior to reloading the router. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

e. You are prompted to terminate autoinstall. Type **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 2: Initialize and reload the switch.

a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

```
Directory of flash:/
```

```
2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text
3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text
4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat
```

```
32514048 bytes total (20886528 bytes free) Switch#
```

c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. At this point, you can change the filename or just press Enter if you have entered the name correctly.
- e. You are prompted to confirm deleting this file. Press Enter to confirm deletion. (Pressing any other key aborts the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to confirm removing the configuration file. Press Enter to confirm to erase this file. (Pressing any other key aborts the operation.)

```
Switch# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

g. Reload the switch to remove any old configuration information from memory. You are prompted to confirm reloading the switch. Press Enter to proceed with the reload. (Pressing any other key aborts the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may be prompted to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

h. After the switch reloads, you should be prompted to enter the initial configuration dialog. Type **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no Switch>
```

Device Configs

Router R1

```
R1#show run
Building configuration...
Current configuration: 1742 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R1
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 4 3mxoP2KRPf3sFHY16Vm6.ssJJi9t0Jqqb6DMG/YH5No
no aaa new-model
!
!
!
!
!
!
no ip domain lookup
```

```
ip domain name CCNA-lab.com
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
license udi pid CISCO1941/K9 sn FTX1636848Z
license accept end user agreement
!
username admin privilege 15 password 7 1304131F0202142B383779
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:A::1/64
interface GigabitEthernet0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
interface Serial0/0/1
no ip address
shutdown
ip forward-protocol nd
no ip http server
```

```
no ip http secure-server
!
!
!
!
control-plane
!
!
banner motd ^CUnauthorized access prohibited!^C
line con 0
exec-timeout 5 0
password 7 03075218050022434019181604
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
exec-timeout 5 0
password 7 14141B180F0B3C3F3D38322631
logging synchronous
login local
transport input ssh
scheduler allocate 20000 1000
end
```