htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Configure Basic Router Settings

Laboratory protocol Configure Basic Router Settings

Subject: NWT|ANGE
Class: 3AHITN
Name: Stefan Fürst, Marcel Raichle
Group Name/Number: Dumm und Dümmer/7
Supervisor: ANGE
Exercise dates: 8.11.2024 29.11.2024 6.12.2024
Submission date: 12.12.2024

Contents

1 Task definition **3**

2 Summary **3**

3 Complete network topology of the exercise **4**

4 Exercise Execution **5**

4.1 Set Up the Topology and Initialize Devices . . . 5

4.2 Configure Devices and Verify Connectivity . . . 5

4.2.1 Configure the PC interfaces . . . 5

4.3 Configure the router . . . 6

4.3.1 Verify network connectivity . . . 9

4.4 Display Router Information . . . 10

4.4.1 Retrieve important hardware and software information. . . . 10

4.4.2 Display the startup configuration . . . 11

4.4.3 Display the routing table on the router . . . 12

4.4.4 Display a summary list of the interfaces on the router . . . 12

4.5 Reflection Questions . . . 13

5 Complete configuration files **14**

6 List of figures **15**

1 Task definition

In this exercise, it is required to set up a basic router configuration, which includes configuring SSH for remote access, securing all other login methods, and setting IP addresses.

2 Summary

This exercise is about configuring router settings and verifying network connectivity. It involves assigning IPv4 and IPv6 addresses, setting up SSH for remote access, and applying security measures such as passwords and login protocols. Connectivity is tested through pings and SSH access. Router information is retrieved using commands like *show version* and *show ip route*, while interface and IPv6 settings are examined. The exercise emphasizes router configuration, network security, and troubleshooting. [1]

[1] This summary was created with ChatGPT.

3 Complete network topology of the exercise

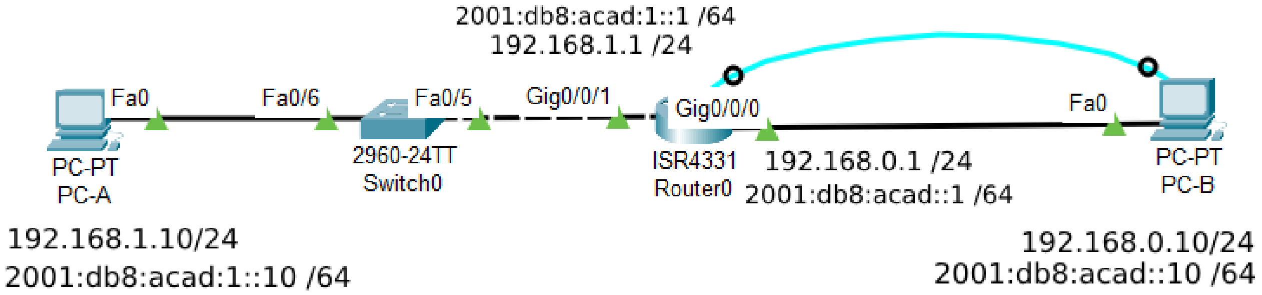


Figure 1: Complete network topology of this exercise

4 Exercise Execution

4.1 Set Up the Topology and Initialize Devices

This exercise was done in Cisco Packet Tracer and the devices were placed and wired using the automatic cabling type, as all the devices are Auto-MDIX compliant anyway.

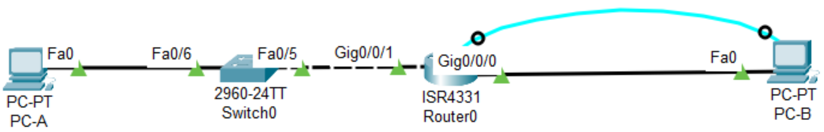


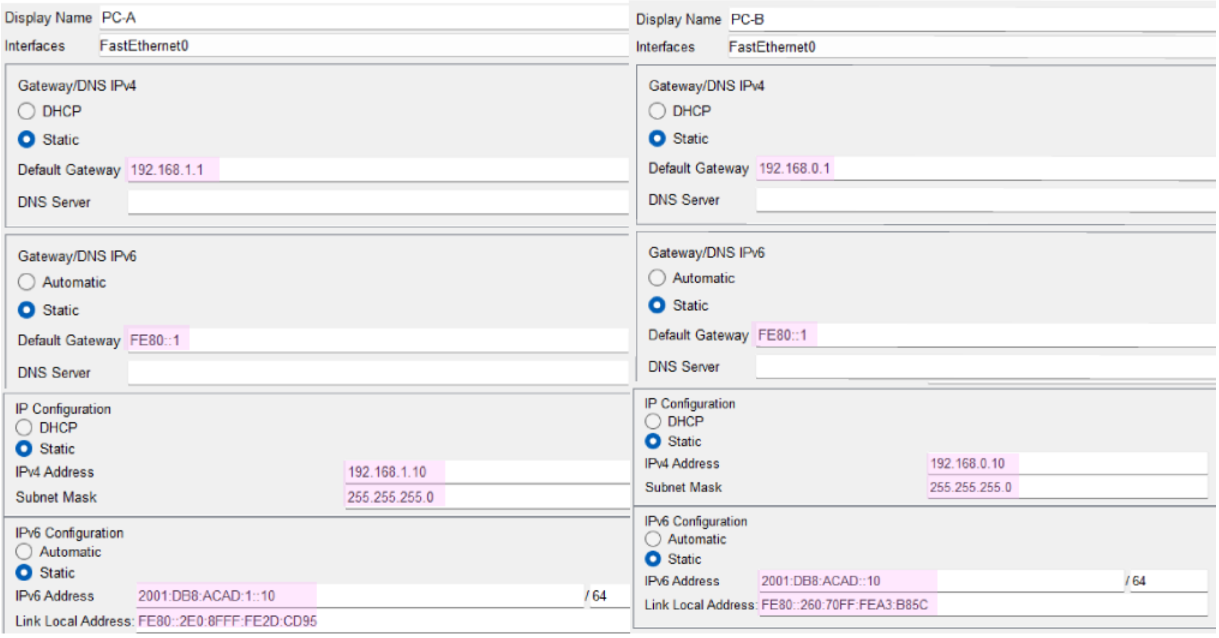
Figure 2: Network topology required for this exercise

After that, everything was turned on and the router and switch were both iniliazised and reloaded.

4.2 Configure Devices and Verify Connectivity

4.2.1 Configure the PC interfaces

The IP addresses for both PCs have been set in the IP Configuration application.



Display Name PC-A
Interfaces FastEthernet0

Gateway/DNS IPv4
○ DHCP
● Static
Default Gateway 192.168.1.1
DNS Server

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway FE80::1
DNS Server

IP Configuration
○ DHCP
● Static
IPv4 Address 192.168.1.10
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address 2001:DB8:ACAD:1::10 / 64
Link Local Address: FE80::2E0:8FFF:FE2D:CD95

Display Name PC-B
Interfaces FastEthernet0

Gateway/DNS IPv4
○ DHCP
● Static
Default Gateway 192.168.0.1
DNS Server

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway FE80::1
DNS Server

IP Configuration
○ DHCP
● Static
IPv4 Address 192.168.0.10
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address 2001:DB8:ACAD::10 / 64
Link Local Address: FE80::260:70FF:FEA3:B85C

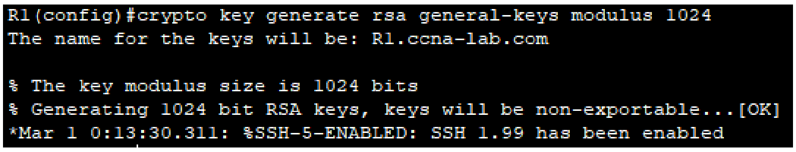
Figure 3: IP configuration for PC-A and PC-B

4.3 Configure the router

To access the router's configuration mode, connect to the router through the console port and execute the *en* and *conf t* commands.
The following basic settings are configured using the commands listed below:

```
#setting the hostname
hostname R1
#setting the domain name of the router
ip domain name ccna-lab.com
#disable DNS lookup on mistyped commands
no ip domain lookup
#encrypt plain text passwords
service password-encryption
#setting the minimum password length to 12 characters
security passwords min-length 12
```

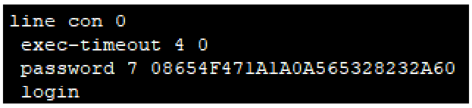
To set up SSH for configuring the router over the network, first, a user must be created with the *username SSHadmin secret 55Hadm!n2020* command, which creates a user named SSHadmin and sets an encrypted password.
Once the user has been created, an RSA key pair needs to be generated using the *crypto key generate rsa general-keys modulus 1024*[2] command.



```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:13:30.311: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Figure 4: Key pair generation

```
#setting a password to enter EXEC mode
enable secret $cisco!PRIV*
line console 0
#setting password for console access
password $cisco!!CON*
#termination of the session after four minutes of inactivity
exec-timeout 4 0
#enabeling login
login
```



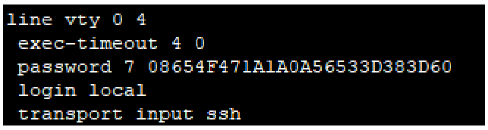
```
line con 0
 exec-timeout 4 0
 password 7 08654F471A1A0A565328232A60
 login
```

Figure 5: Viewing the configuration of VTY line 0

```
#entering the configuration for lines for vty lines 0 to 4
line vty 0 4
#setting a password to access the lines
password $cisco!!VTY*
#termination of the session after four minutes of inactivity
exec-timeout 4 0
#only allowing ssh connections
transport input ssh
```

[2] As this is done in Packet Tracer and the hardware in the lab is outdated, the keys are limited to 1024 bit length instead of the 4096 bit length that should be used in a production environment.

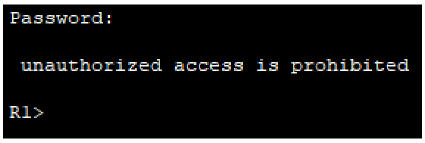
```
#enabeling login using the local database
login local
```



```
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
```

Figure 6: Viewing the configuration of VTY lines 0 4

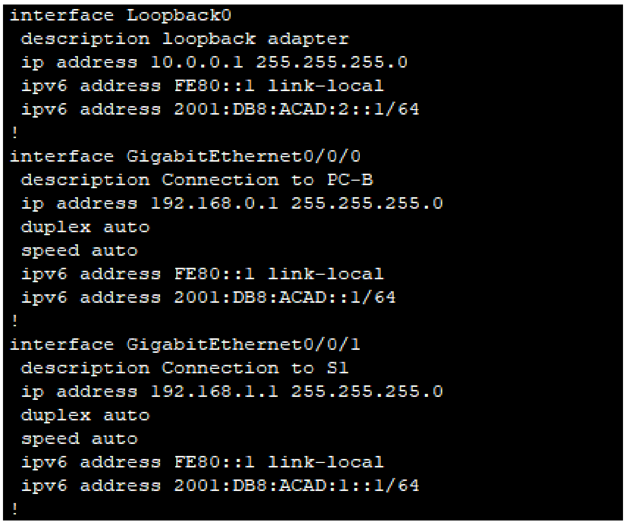
```
#createing a banner to warn that unauthorized access is prohibited
banner motd $ unauthorized access is prohibited $
```



```
Password:

 unauthorized access is prohibited

R1>
```

Figure 7: Viewing the MOTD banner

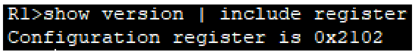
```
#enable ipv6 routing
ipv6 unicast-routing
#setting the ip addresses according to the addressing table
interface g0/0/0
ip address 192.168.0.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad::1/64
no shutdown
exit
interface g0/0/1
ip address 192.168.1.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:1::1/64
no shutdown
exit
interface loopback0
ip address 10.0.0.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:2::1/64
no shutdown
exit
```



```
interface Loopback0
 description loopback adapter
 ip address 10.0.0.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:2::1/64
!
interface GigabitEthernet0/0/0
 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::1/64
!
interface GigabitEthernet0/0/1
 description Connection to S1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
!
```

Figure 8: Displaying the IP addresses set

```
#setting a timeout of 2 minutes after 3 failed login attempts in 60 seconds
login block-for 120 attempts 3 within 60
exit
#setting the clock
clock set 9:22:40 08 Nov 2024
```



```
R1>show version | include register
Configuration register is 0x2102
```

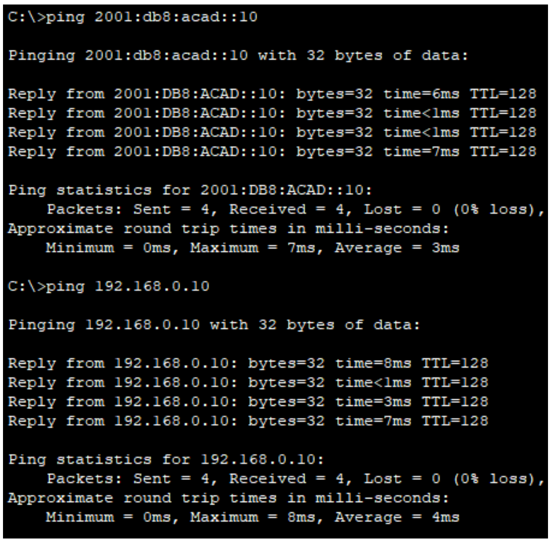
Figure 9: Display of current time

```
#copying the current running-config to the startup-config
copy run start
```

If the router is reloaded before running this command, the running configuration will be lost, as the RAM is erased during a reload.

4.3.1 Verify network connectivity

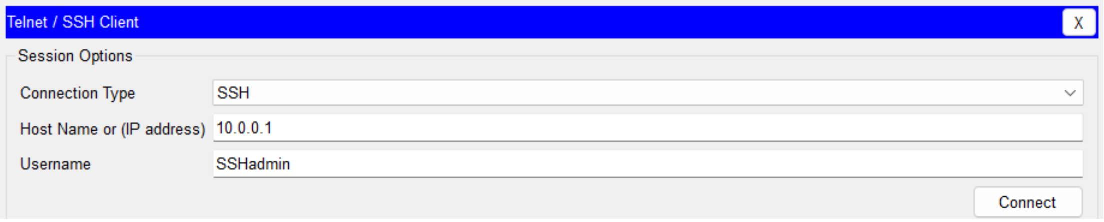
To test if everything was configured appropriately, PC-B will be pinged from PC-A to check if they can communicate.



```
C:\>ping 2001:db8:acad::10

Pinging 2001:db8:acad::10 with 32 bytes of data:

Reply from 2001:DB8:ACAD::10: bytes=32 time=6ms TTL=128
Reply from 2001:DB8:ACAD::10: bytes=32 time<1ms TTL=128
Reply from 2001:DB8:ACAD::10: bytes=32 time<1ms TTL=128
Reply from 2001:DB8:ACAD::10: bytes=32 time=7ms TTL=128

Ping statistics for 2001:DB8:ACAD::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 3ms

C:\>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:

Reply from 192.168.0.10: bytes=32 time=8ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time=3ms TTL=128
Reply from 192.168.0.10: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 4ms
```

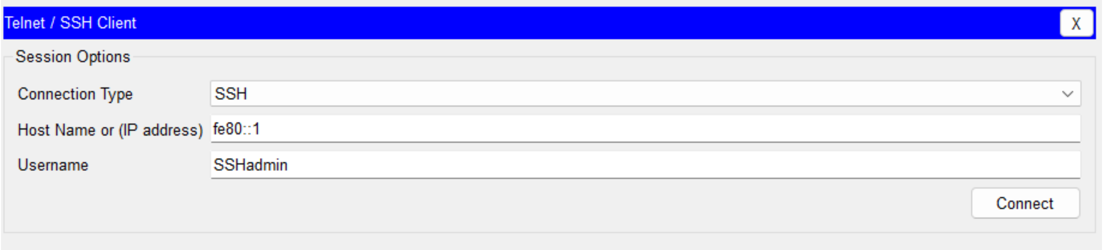
Figure 10: Pinging PC-B from PC-A

Next, the SSH connection will be tested by connecting from PC-A to the router using its IPv4 and IPv6 addresses on the loopback interface.



Connection Type: SSH
Host Name or (IP address): 10.0.0.1
Username: SSHadmin

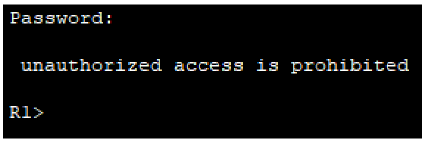
Figure 11: Connecting to the router via IPv4 using ssh



Connection Type: SSH
Host Name or (IP address): fe80::1
Username: SSHadmin

Figure 12: Connecting to the router via IPv6 using ssh

The Telnet protocol is considered a security risk because it is not encrypted, meaning that the entire session can be seen in clear text, allowing passwords to be easily exposed using a packet sniffer.



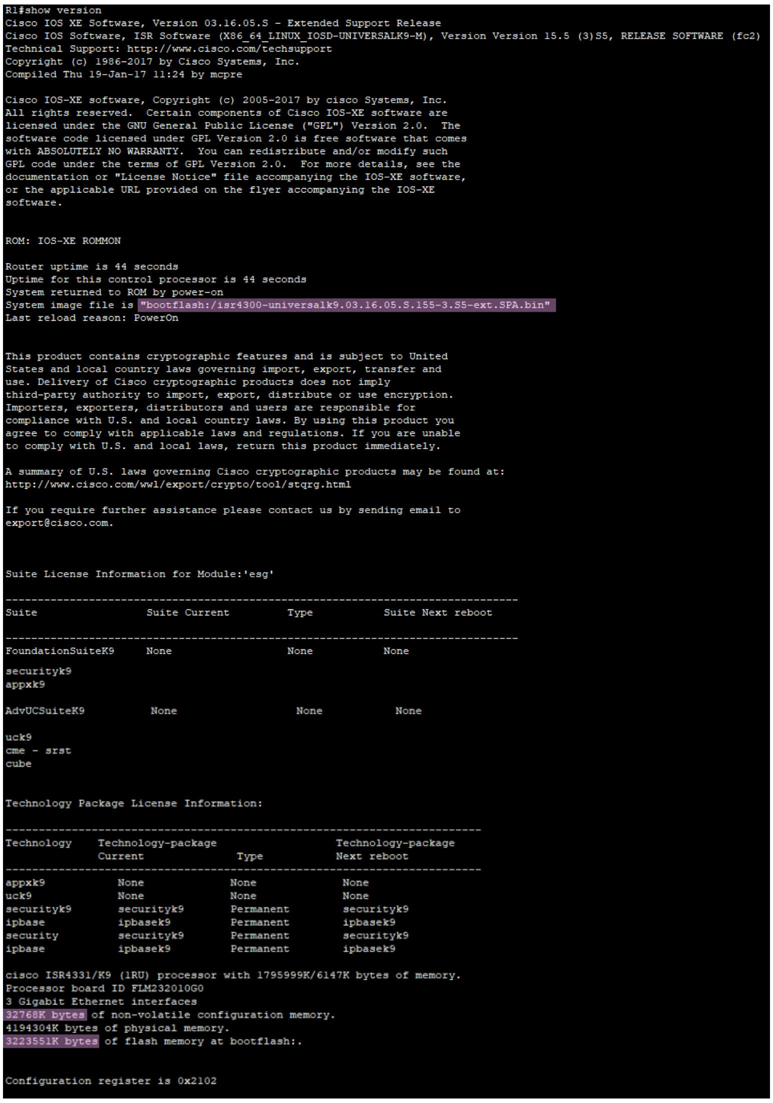
```
Password:

 unauthorized access is prohibited

R1>
```

Figure 13: Working login

4.4 Display Router Information

4.4.1 Retrieve important hardware and software information.

The *show version* command displays information about the hardware and software running on the router.

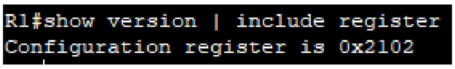


```
R1#show version
Cisco IOS XE Software, Version 03.16.05.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 19-Jan-17 11:24 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 44 seconds
Uptime for this control processor is 44 seconds
System returned to ROM by power-on
System image file is "bootflash:/isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin"
Last reload reason: PowerOn


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.



Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot

--------------------------------------------------------------------------------
FoundationSuiteK9     None                  None           None
securityk9
appxk9

AdvUCSuiteK9          None                  None           None

uck9
cme - srst
cube


Technology Package License Information:

--------------------------------------------------------------------------
Technology    Technology-package                  Technology-package
              Current              Type           Next reboot
--------------------------------------------------------------------------
appxk9           None             None             None
uck9             None             None             None
securityk9       securityk9       Permanent        securityk9
ipbase           ipbasek9         Permanent        ipbasek9
security         securityk9       Permanent        securityk9
ipbase           ipbasek9         Permanent        ipbasek9

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.


Configuration register is 0x2102
```

Figure 14: Displaying information about the hardware and software

The name of the IOS image is *isr4300-universalk9.03.16.05.S.155.3.S5-ext.SPA.bin*, and the router has 32 MB of NVRAM and 3.07 GB of flash memory.

Since the output of this command is long and can be difficult to navigate, it can be filtered by piping the command and using the *include* keyword with the desired search term.



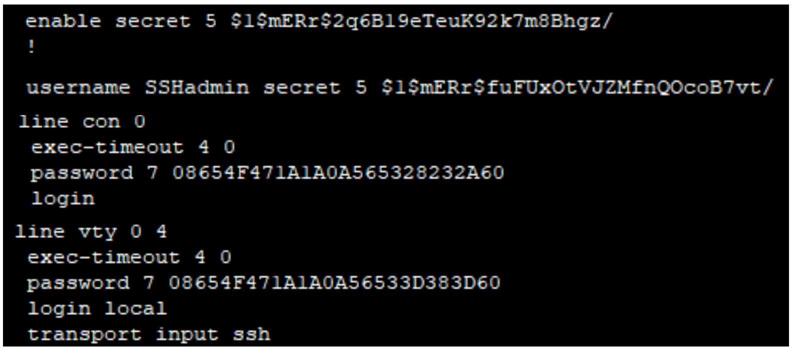
```
R1#show version | include register
Configuration register is 0x2102
```

Figure 15: Filtering the output of the show version command to show only the register

The register is *0x2142*, which means that the router will undergo the normal boot process: it will load the IOS image from flash memory and load the startup configuration from NVRAM if one is present.

4.4.2 Display the startup configuration

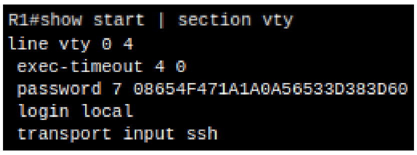
The startup configuration is shown with the *show startup-config* command, and due to the *service password-encryption* command, the passwords are displayed in an encrypted form.



```
 enable secret 5 $1$mERr$2q6B19eTeuK92k7m8Bhgz/
 !
 username SSHadmin secret 5 $1$mERr$fuFUxOtVJZMfnQOcoB7vt/
line con 0
 exec-timeout 4 0
 password 7 08654F471A1A0A565328232A60
 login
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
```

Figure 16: Passwords displayed in encrypted form

Like with any other command, the output can be piped and filtered to show only specific sections. In this case, it is filtered to display only the VTY section of the startup configuration.[3]



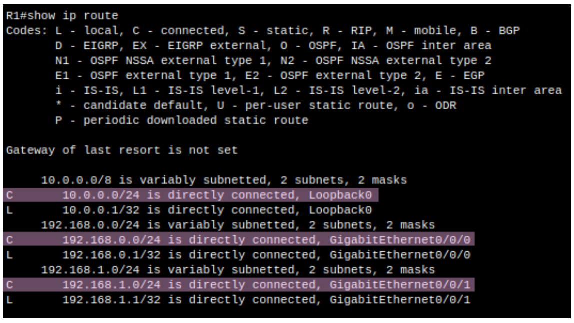
```
R1#show start | section vty
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
```

Figure 17: Filtering the output of show run to only display the VTY section

[3] In Cisco Packet Tracer, piping the output of the show run command doesn't work, so this screenshot was created using Photoshop. The output was taken from the show startup-config command without any filtering and edited to appear as if it was filtered.

4.4.3 Display the routing table on the router

The routing table of the router can be displayed with the *show ip route* command.



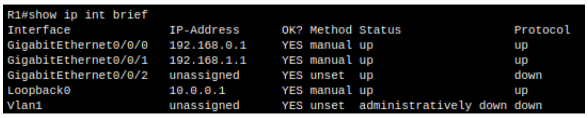
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Loopback0
L       10.0.0.1/32 is directly connected, Loopback0
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
```

Figure 18: Displaying the ip routes

The *C* code is used in the routing table to indicate a directly connected network, which corresponds to three entries in the routing table.

4.4.4 Display a summary list of the interfaces on the router

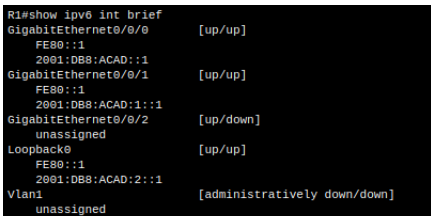
The IPv4 configuration of the interfaces is displayed with the *show ip interface brief* command.



```
R1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.0.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  up                    down
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Figure 19: Displaying a summary of the IPv4 configuration of interfaces

The *no shutdown* command is used to change the Ethernet ports from administratively down to up.
The IPv6 configuration of the interfaces is displayed with the *show ipv6 interface brief* command.

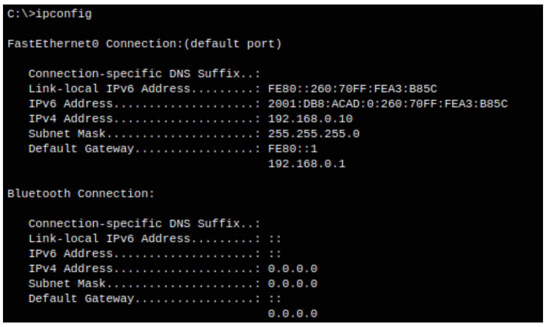


```
R1#show ipv6 int brief
GigabitEthernet0/0/0       [up/up]
    FE80::1
    2001:DB8:ACAD::1
GigabitEthernet0/0/1       [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/2       [up/down]
    unassigned
Loopback0                  [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Vlan1                      [administratively down/down]
    unassigned
```

Figure 20: Displaying a summary of the IPv6 configuration of interfaces

The *[up/up]* status indicates the Layer 1 and Layer 2 status of the interface and does not provide information about Layer 3.

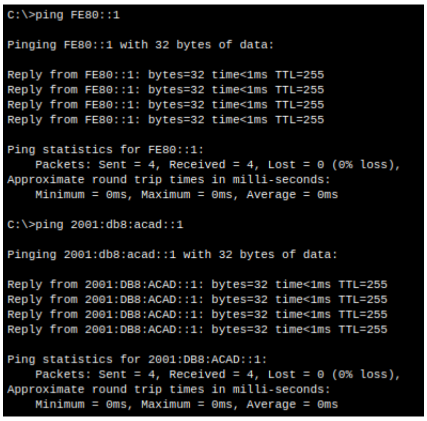
After changing the IPv6 configuration of PC-B to Automatic, the active configuration can be viewed in the command prompt with the *ipconfig* command.



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:70FF:FEA3:B85C
   IPv6 Address....................: 2001:DB8:ACAD:0:260:70FF:FEA3:B85C
   IPv4 Address....................: 192.168.0.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: FE80::1
                                     192.168.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

Figure 21: Displaying the IP configuration of PC-B after setting the IPv6 configuration to automatic

PC-B was assigned *2001:DB8:ACAD:0:260:70FF:FEA3:B85C* as its address and *FE80::1* as the default gateway.
After pinging both the default gateway's link-local and IPv6 unicast addresses, it shows that both were successful, and the automatic configuration worked.



```
C:\>ping FE80::1

Pinging FE80::1 with 32 bytes of data:

Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255

Ping statistics for FE80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad::1

Pinging 2001:db8:acad::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 22: Pinging both the default gateway link local and IPv6 unicast address

4.5 Reflection Questions

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?
   (a) To check if an interface is not enabled, either the *show interface brief* or *show running-config/startup-config* command can be used.
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?
   (a) To check if an interface is assigned the wrong subnet mask, either the *show protocols* or *show running-config/startup-config* command can be used.

5 Complete configuration files

```
Current configuration : 1613 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname R1
!
login block-for 120 attempts 3 within 60
!
enable secret 5\
$1$mERr$2q6B19eTeuK92k7m8Bhgz/
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
username SSHadmin secret 5 \
$1$mERr$fuFUx0tVJZMfnQ0coB7vt/
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
!
interface Loopback0
 description loopback adapter
 ip address 10.0.0.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:2::1/64
!
interface GigabitEthernet0/0/0
 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::1/64
!
interface GigabitEthernet0/0/1
 description Connection to S1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip classless
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
banner motd \
$ unauthorized access is prohibited $
!
line con 0
 exec-timeout 4 0
 password 7 08654F471A1A0A565328232A60
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
!
end
```

6 List of figures

List of Figures

1 Complete network topology of this exercise 4
2 Network topology required for this exercise 5
3 IP configuration for PC-A and PC-B 5
4 Key pair generation 6
5 Viewing the configuration of VTY line 0 6
6 Viewing the configuration of VTY lines 0 4 7
7 Viewing the MOTD banner 7
8 Displaying the IP addresses set 8
9 Display of current time 8
10 Pinging PC-B from PC-A 9
11 Connecting to the router via IPv4 using ssh 9
12 Connecting to the router via IPv6 using ssh 9
13 Working login 10
14 Displaying information about the hardware and software 10
15 Filtering the output of the show version command to show only the register 11
16 Passwords displayed in encrypted form 11
17 Filtering the output of show run to only display the VTY section 11
18 Displaying the ip routes 12
19 Displaying a summary of the IPv4 configuration of interfaces 12
20 Displaying a summary of the IPv6 configuration of interfaces 12
21 Displaying the IP configuration of PC-B after setting the IPv6 configuration to automatic 13
22 Pinging both the default gateway link local and IPv6 unicast address 13