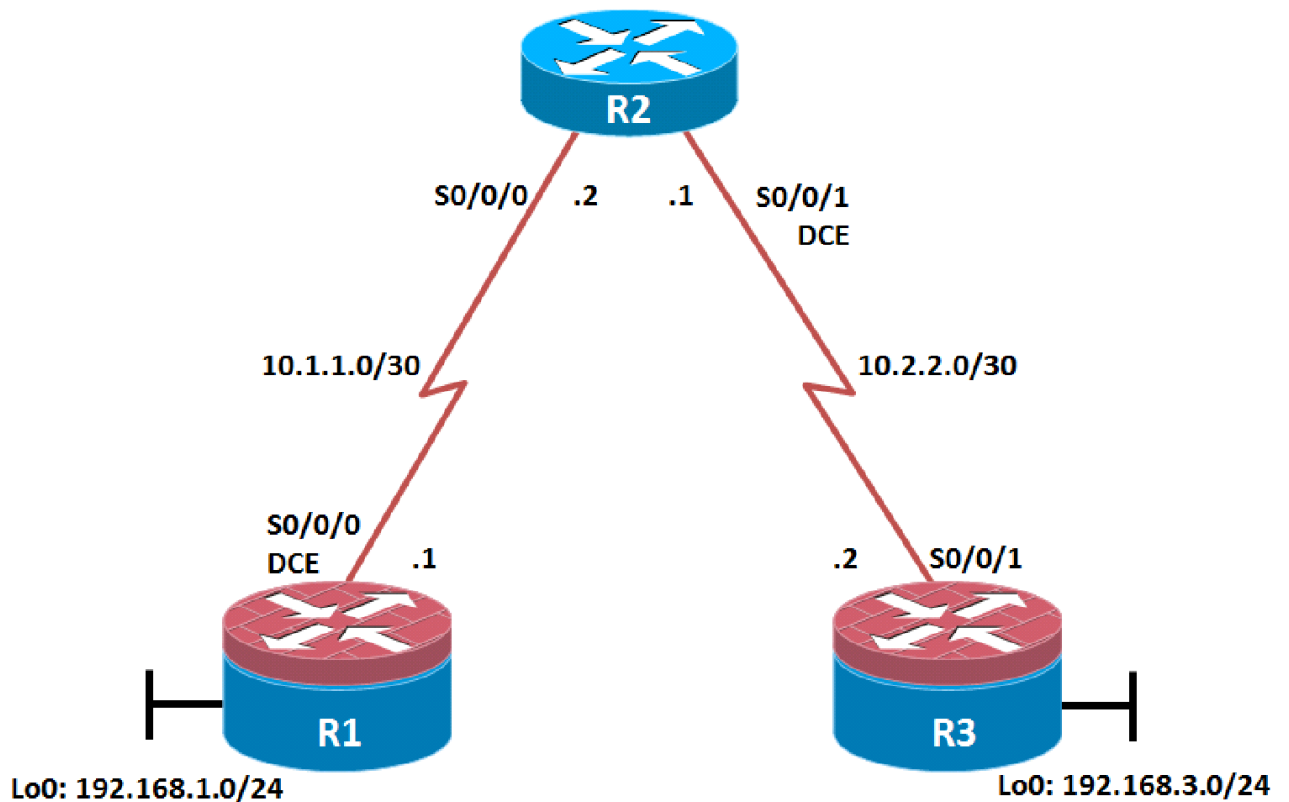


Practical No: 4

Aim: Secure the Management Plane

Topology



Objectives

- Secure management access.
- Configure enhanced username password security.
- Enable AAA RADIUS authentication.
- Enable secure remote management.

Background

The management plane of any infrastructure device should be protected as much as possible. Controlling access to routers and enabling reporting on routers are critical to network security and should be part of a comprehensive security policy.

In this lab, you build a multi-router network and secure the management plane of routers R1 and R3.

Note: This lab uses Cisco 1941 routers with Cisco IOS Release 15.2 with IP Base. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

3 routers (Cisco IOS Release 15.2 or comparable)
Serial and Ethernet cables

Step 1: Configure loopbacks and assign addresses.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the R1, R2, and R3 routers.

You can copy and paste the following configurations into your routers to begin.

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

R1

```
hostname R1
```

```
interface Loopback 0
```

```
description R1 LAN
```

```
ip address 192.168.1.1 255.255.255.0
```

```
exit
```

```
!
```

```
interface Serial0/0/0
```

```
description R1 --> R2
```

```
ip address 10.1.1.1 255.255.255.252
```

```
clock rate 128000
```

```
no shutdown
```

```
exit
```

```
!
```

```
end
```

R2

hostname R2

!

interface Serial0/0/0

description R2 --> R1

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface Serial0/0/1

description R2 --> R3

ip address 10.2.2.1 255.255.255.252

clock rate 128000

no shutdown

exit

!

end

R3

hostname R3

!

interface Loopback0

description R3 LAN

ip address 192.168.3.1 255.255.255.0

exit

```
interface Serial0/0/1
description R3 -> R2
ip address 10.2.2.2 255.255.255.252
no shutdown
exit
!
end
```

Step 2: Configure static routes.

On R1, configure a default static route to ISP.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

On R3, configure a default static route to ISP.

```
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

On R2, configure two static routes.

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

```
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.2
```

From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {
192.168.1.1
10.1.1.1
10.1.1.2
10.2.2.1
10.2.2.2
192.168.3.1
}{ ping $address }
```

R1# tclsh

```
R1(tcl)#foreach address {
```

```
+>(tcl)#192.168.1.1
```

```
+>(tcl)#10.1.1.1
```

```
+>(tcl)#10.1.1.2
```

```
+>(tcl)#10.2.2.1
```

```
+>(tcl)#10.2.2.2
```

```
+>(tcl)#192.168.3.1
```

```
+>(tcl)#} { ping $address }
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms

R1(tcl)#

Are the pings now successful?

Yes. If not, troubleshoot.

Step 3: Secure management access.

On R1, use the **security passwords** command to set a minimum password length of 10 characters.

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

Configure the enable secret encrypted password on both routers.

```
R1(config)# enable secret class12345
```

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Configure a console password and enable login for routers. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)# line console 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)#
```

Configure the password on the vty lines for router R1.

```
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)# exit
R1(config)#
```

The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port.

```
R1(config)# line aux 0
R1(config-line)# no exec
R1(config-line)# end
R1#
```

Enter privileged EXEC mode and issue the **show run** command.

Use the **service password-encryption** command to encrypt the line console and vty passwords.

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

Note: Password encryption is applied to all the passwords, including the **username** passwords, the authentication key passwords, the privileged command password, the console and the virtual terminal line access passwords, and the BGP neighbor passwords.

Issue the **show run** command.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign (\$) is used to start and end the message.

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

Issue the **show run** command. What does the \$ convert to in the output?

The \$ is converted to ^C when the running-config is displayed.

Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started.

Does the MOTD banner look like what you created with the **banner motd** command? If the MOTD banner is not as you wanted it, recreate it using the **banner motd** command.

Repeat the configuration portion of steps 3a through 3k on router R3.

Step 4: Configure enhanced username password security.

To increase the encryption level of console and VTY lines, it is recommended to enable authentication using the local database. The local database consists of usernames and password combinations that are created locally on each device. The local and VTY lines are configured to refer to the local database when authenticating a user.

To create local database entry encrypted to level 4 (SHA256), use the **username *name* secret *password*** global configuration command. In global configuration mode, enter the following command:

```
R1(config)# username JR-ADMIN secret class12345
```

```
R1(config)# username ADMIN secret class54321
```

Note: An older method for creating local database entries is to use the **username *name* password *password*** command.

Set the console line to use the locally defined login accounts.

```
R1(config)# line console 0
```

```
R1(config-line)# login local
```

```
R1(config-line)# exit
```

```
R1(config)#
```

Set the vty lines to use the locally defined login accounts.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# login local
```

```
R1(config-line)# end
```

```
R1(config)#
```

Repeat the steps 4a to 4c on R3.

To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

```
R1# telnet 10.2.2.2
```

```
Trying 10.2.2.2 ... Open
```

```
Unauthorized access strictly prohibited!
```


User Access Verification

Username: **ADMIN**

Password:

R3>

Step 5: Enabling AAA RADIUS Authentication with Local User for Backup.

Authentication, authorization, and accounting (AAA) is a standards-based framework that can be implemented to control who is permitted to access a network (authenticate), what they can do on that network (authorize), and audit what they did while accessing the network (accounting).

Users must authenticate against an authentication database which can be stored:

Locally: Users are authenticated against the local device database which is created using the username secret command. Sometimes referred to self-contained AAA.

Centrally: A client-server model where users are authenticated against AAA servers. This provides improved scalability, manageability and control. Communication between the device and AAA servers is secured using either the RADIUS or TACACS+ protocols.

In this step, we will configure AAA authentication to use a RADIUS server and the local database as a backup. Specifically, the authentication will be validated against one of two RADIUS servers. If the servers are not available, then authentication will be validated against the local database.

Always have local database accounts created before enabling AAA. Since we created two local database accounts in the previous step, then we can proceed and enable AAA on R1.

```
R1(config)# aaa new-model
```

Note: Although the following configuration refers to two RADIUS servers, the actual RADIUS server implementation is beyond the scope. Therefore, the goal of this step is to provide an example of how to configure a router to access the servers.

Configure the specifics for the first RADIUS server located at 192.168.1.101. Use **RADIUS-1-pa55w0rd** as the server password.

```
R1(config)# radius server RADIUS-1  
R1(config-radius-server)# address ipv4 192.168.1.101  
R1(config-radius-server)# key RADIUS-1-pa55w0rd  
R1(config-radius-server)# exit  
R1(config)#
```

Configure the specifics for the second RADIUS server located at 192.168.1.102. Use **RADIUS-2-**

pa55w0rd as the server password.

```
R1(config)# radius server RADIUS-2  
R1(config-radius-server)# address ipv4 192.168.1.102  
R1(config-radius-server)# key RADIUS-2-pa55w0rd  
R1(config-radius-server)# exit  
R1(config)#
```

Assign both RADIUS servers to a server group.

```
R1(config)# aaa group server radius RADIUS-GROUP  
R1(config-sg-radius)# server name RADIUS-1  
R1(config-sg-radius)# server name RADIUS-2  
R1(config-sg-radius)# exit  
R1(config)#
```

Enable the default AAA authentication login to attempt to validate against the server group. If they are not available, then authentication should be validated against the local database..

```
R1(config)# aaa authentication login default group RADIUS-GROUP local  
R1(config)#
```

Note: Once this command is configured, all line access methods default to the default authentication method. The **local** option enables AAA to refer to the local database. Only the password is case sensitive.

Enable the default AAA authentication Telnet login to attempt to validate against the server group. If they are not available, then authentication should be validated against a case sensitive local database.

```
R1(config)# aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case  
R1(config)#
```

Note: Unlike the **local** option that makes the password is case sensitive, local-case makes the username and password case sensitive.

Alter the VTY lines to use the TELNET-LOGIN AAA authentication method.

```
R1(config)# line vty 0 4  
R1(config-line)# login authentication TELNET-LOGIN  
R1(config-line)# exit  
R1(config)#
```

Repeat the steps 5a to 5g on R3.

To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

```
R1# telnet 10.2.2.2
```

```
Trying 10.2.2.2 ... Open
```

```
Unauthorized access strictly prohibited!
```

```
User Access Verification
```

```
Username: admin
```

```
Password:
```

```
% Authentication failed
```

```
Username: ADMIN
```

```
Password:
```

```
R3>
```

Note: The first login attempt did not use the correct username (i.e., ADMIN) which is why it failed.

Note: The actual login time is longer since the RADIUS servers are not available.

Step 6: Enabling secure remote management using SSH.

Traditionally, remote access on routers was configured using Telnet on TCP port 23. However, Telnet was developed in the days when security was not an issue; therefore, all Telnet traffic is forwarded in plaintext.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

In this step, you will enable R1 and R3 to support SSH instead of Telnet.

SSH requires that a device name and a domain name be configured. Since the router already has a name assigned, configure the domain name.

```
R1(config)# ip domain-name ccnasecurity.com
```

The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Although optional it may be wise to erase any existing key pairs on the router.

```
R1(config)# crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.

Generate the RSA encryption key pair for the router. Configure the RSA keys with **1024** for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

The name for the keys will be: R1.ccnasecurity.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
R1(config)#
```

Jan 10 13:44:44.711: %SSH-5-ENABLED: SSH 1.99 has been enabled

```
R1(config)#
```

Cisco routers support two versions of SSH:

SSH version 1 (SSHv1): Original version but has known vulnerabilities.

SSH version 2 (SSHv2): Provides better security using the Diffie-Hellman key exchange and the strong integrity-checking message authentication code (MAC).

The default setting for SSH is SSH version 1.99. This is also known as compatibility mode and is merely an indication that the server supports both SSH version 2 and SSH version 1. However, best practices are to enable version 2 only.

Configure SSH version 2 on R1.

```
R1(config)# ip ssh version 2
```

```
R1(config)#
```

Configure the vty lines to use only SSH connections.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input ssh
```

```
R1(config-line)# end
```

Note: SSH requires that the **login local** command be configured. However, in the previous step we enabled AAA authentication using the TELNET-LOGIN authentication method, therefore **login local** is not necessary.

Note: If you add the keyword **telnet** to the **transport input** command, users can log in using Telnet as well as SSH. However, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

Verify the SSH configuration using the **show ip ssh** command.

```
R1# show ip ssh
```

```
SSH Enabled - version 2.0
```

```
Authentication timeout: 120 secs; Authentication retries: 3
```

```
Minimum expected Diffie Hellman key size : 1024 bits
```

```
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGC3Lehh7ReYlgyDzls6wq+mFzxqzoaZFr9XGx+Q/yi  
o
```

```
dFYw00hQo80tZy1W1Ff3Pz6q7Qi0y00urwddHZ0kBZceZK9EzJ6wZ+9a87KKDETCWrGSLi6c  
8IE/y4K+
```

```
Z/oVrMMZk7bpTM1MFdP41YgkTf35utYv+TcqbsYo++KJiYk+xw==
```

```
R1#
```

Repeat the steps 6a to 6f on R3.

Although a user can SSH from a host using the SSH option of TeraTerm or PuTTY, a router can also SSH to another SSH enabled device. SSH to R3 from R1.

```
R1# ssh -l ADMIN 10.2.2.2
```

```
Password:
```

```
Unauthorized access strictly prohibited!
```

```
R3>
```

```
R3> en
```

```
Password:
```

```
R3#
```

Device Configurations

Router R1

```
service password-encryption
```

!

hostname R1

!

security passwords min-length 10

enable secret 5 \$1\$t6eK\$FZ.JdmMLj8QSgNkpChyZz.

!

aaa new-model

!

!

aaa group server radius RADIUS-GROUP

server name RADIUS-1

server name RADIUS-2

!

aaa authentication login default group RADIUS-GROUP local

aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

!

ip domain name ccnasecurity.com

!

username JR-ADMIN secret 5 \$1\$0u0q\$lwimCZIAuQtV4C1ezXL1S0

username ADMIN secret 5 \$1\$NSVD\$/YjzB7Auyes1sAt4qMfpd.

!

ip ssh version 2

!

interface Loopback0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

!

interface Serial0/0/0

description R1 --> R2

ip address 10.1.1.1 255.255.255.252

no fair-queue

!

ip route 0.0.0.0 0.0.0.0 10.1.1.2

!

radius server RADIUS-1

address ipv4 192.168.1.101 auth-port 1645 acct-port 1646

key 7 107C283D2C2221465D493A2A717D24653017

!

radius server RADIUS-2

address ipv4 192.168.1.102 auth-port 1645 acct-port 1646

key 7 03367A2F2F3A12011C44090442471C5C162E

!

banner motd ^CUnauthorized access strictly prohibited!^C

!

line con 0

exec-timeout 5 0

password 7 070C285F4D061A0A19020A1F17

logging synchronous

!

line aux 0

no exec

!

```
password 7 060506324F411F0D1C0713181F
```

```
login authentication TELNET-LOGIN
```

```
transport input ssh
```

```
!
```

```
end
```

Router R2

```
hostname R2
```

```
!
```

```
enable secret 5 $1$DJS7$xvJDW87zLs8pSJDFUICPB1
```

```
!
```

```
interface Serial0/0/0
```

```
description R2 --> R1
```

```
ip address 10.1.1.2 255.255.255.252
```

```
no fair-queue
```

```
clock rate 2000000
```

```
!
```

```
interface Serial0/0/1
```

```
description R2 --> R3
```

```
ip address 10.2.2.1 255.255.255.252
```

```
clock rate 128000
```

```
!
```

```
ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

```
ip route 192.168.3.0 255.255.255.0 10.2.2.2
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```



```
logging synchronous
```

```
!
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
!
```

```
end
```

Router R3

```
service password-encryption
```

```
!
```

```
hostname R3
```

```
!
```

```
security passwords min-length 10
```

```
enable secret 5 $1$50Y4$4J6VFlvGNKjwQ8XtajgUk1
```

```
!
```

```
aaa new-model
```

```
!
```

```
!
```

```
aaa group server radius RADIUS-GROUP
```

```
server name RADIUS-1
```

```
server name RADIUS-2
```

```
!
```

```
aaa authentication login default group RADIUS-GROUP local
```

```
aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case
```

```
!
```

ip domain name ccnasecurity.com

!

username JR-ADMIN secret 5 \$1\$b4m1\$RVmjL9S3gxKh1xr8qzNqr/

username ADMIN secret 5 \$1\$zGV7\$pVgSEbinvXQ7f7uyxeKBj0

!

ip ssh version 2

!

interface Loopback0

description R3 LAN

ip address 192.168.3.1 255.255.255.0

!

interface Serial0/0/1

description R3 --> R2

ip address 10.2.2.2 255.255.255.252

!

ip route 0.0.0.0 0.0.0.0 10.2.2.1

!

radius server RADIUS-1

address ipv4 192.168.1.101 auth-port 1645 acct-port 1646

key 7 01212720723E354270015E084C5000421908

!

radius server RADIUS-2

address ipv4 192.168.1.102 auth-port 1645 acct-port 1646

key 7 003632222D6E384B5D6C5C4F5C4C1247000F

!

banner motd ^CUnauthorized access strictly prohibited!^C

!

line con 0

exec-timeout 5 0

password 7 104D000A0618110402142B3837

logging synchronous

!

line aux 0

no exec

!

line vty 0 4

exec-timeout 5 0

password 7 070C285F4D060F110E020A1F17

login authentication TELNET-LOGIN

transport input ssh

!

End