3.5.11 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/5/2025, 2:06:37 PM • **Time Spent:** 01:27

Score: 100%

Passing Score: 80%

[redacted]

Question 1. ✓ Correct

Which of the following is the most important thing to do to prevent console access to the router?

- Implement an access list to prevent console connections.
- → Keep the router in a locked room.
- Disconnect the console cable when not in use.
- Set the console and enable secret passwords.

Explanation

To control access to the router console, you must keep the router in a locked room. A console connection can only be established with a direct physical connection to the router. If the router is in a locked room, only those with access will be able to make a console connection. In addition, even if you had set console passwords, users with physical access to the router could perform router password recovery and gain access.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_01_ccna7.question.xml

Question 2. ✓ Correct

You want to prevent users from accessing a router through a Telnet session. What should you do?

→ ◉ For the VTY lines, add the **login** parameter and remove any passwords.

○ For the console line, add the **login** parameter and configure a password.

○ For the console line, set a password but remove the **login** parameter.

○ For the VTY lines, add the **login** parameter and configure a password.

○ For the console line, add the **login** parameter and remove any passwords.

○ For the VTY lines, set a password, but remove the **login** parameter.

Explanation

To prevent Telnet sessions with the router, configure the VTY lines with the **login** parameter, but without a password. This requires a password for login. But because no password has been configured, access will be denied with the message "Password required but not set."

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_02_ccna7.question.xml

Question 3. ✓ Correct

You want users to enter a password before being able to access the router through a Telnet session. You use the following commands:

```
router#config t
router(config)#line vty 0 4
router(config-line)#password cisco
router(config-line)#exit
router(config)#exit
```

You open a Telnet session with the router and discover that the session starts without being prompted for a password. What should you do?

- Use the **enable secret** command in line configuration mode to set the password.
- In global configuration mode, configure the **enable secret** password.
- → In line configuration mode, add the **login** parameter.
- Repeat the same configuration steps in **line con 0** mode.

Explanation

To require a password for a Telnet session, you must configure a password and add the **login** parameter. You can think of this command as turning password checking on. If a password is set but the **login** is missing, the password will not be required. If you add **login** but do not set a password, access will be denied (the prompt for a password will not be shown).

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_03_ccna7.question.xml

Question 4. ✓ Correct

What is the main security weakness associated with the **service password-encryption** command?

- Passwords are rendered as 4-digit hexadecimal values.
- → Passwords are easily broken.
- Passwords are kept in the configuration register.
- Password values are transposed.

Explanation

The **service password-encryption** command encrypts all passwords as type 7 passwords. Encrypted type 7 passwords are not secure and are easily broken. But the encrypted values do provide some level of protection from someone looking over your shoulder after having issued the **show running-config** command.

Passwords are never kept in the configuration register; they are kept in the startup-config file.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_04_ccna7.question.xml

Question 5. ✓ Correct

While configuring a new router, you use the following commands:

```
Router(config)#enable password cisco
Router(config)#enable secret highway
Router(config)#username admin password television
Router(config)#line con 0
Router(config-line)#password airplane
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password garage
Router(config-line)#login
```

Which password would you use to open a Telnet session to the router?

→ ◉ garage

○ airplane

○ cisco

○ highway

Explanation

The password set for VTY lines is used to establish the Telnet session. The password set for line con 0 is used to make a connection to the console. After you connect to the console or the Telnet connection, you are in user EXEC mode.

To enter privileged EXEC mode, use the enable secret password. If the enable secret password is not set, use the enable password.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_05_ccna7.question.xml

Question 6. ✓ Correct

Which of the following commands configures a password to switch to privileged EXEC mode and saves the password using MD5 hashing?

- **service password-encryption**
- **enable password**
- **password**
- → **enable secret**

Explanation

Use **enable secret** to configure a password for privileged EXEC mode that is stored using MD5 hashing.

enable password sets an unencrypted version of the password. **password** configures configure console and VTY passwords. **service password-encryption** adds simple encryption to the enable password. However, this encryption can be broken more easily than the MD5 hash used for the enable secret password.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_06_ccna7.question.xml

Question 7. ✓ Correct

You are at a customer site and need to access their router. The previous administrator left the company and did not document the password to the device. Which of the following would you access to start the password recovery process?

- IOS
- BIOS
- bootstrap
- → ROMmon

Explanation

To start the recovery process, access ROMmon mode on the device. ROMmon mode can be accessed via a console by using a break sequence during the boot process. Removing external flash memory while the device is powered off will also cause the device to boot in ROMmon mode.

Bootstrap is the boot loader software that loads from the ROM into RAM and loads the IOS operating system.

Accessing IOS does not provide the means to reset a lost or unknown password.

Accessing the BIOS does not provide a way to reset a lost or unknown password.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_01_ccna7.question.xml

Question 8. ✓ Correct

As part of the password recovery process on a router, you want the device to ignore the startup config file when the device is rebooted. Which of the following commands would you use to do this?

- **copy running-config startup-config**
- → **confreg 0x2142**
- **enable**
- **reset**

Explanation

You can use **confreg 0x2142** to change the configuration register to 0x2142. This instructs the device to ignore the startup-config file the next time your device starts.

The other commands do not accomplish the task. **copy running-config startup-config** will erase your startup configuration instead of telling the device to ignore the startup config.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_02_ccna7.question.xml

Question 9. ✓ Correct

After configuring a router to ignore the startup configuration when the device boots, what command would you use to tell the device to load the startup configuration upon boot?

- confreg 0x2142
- → confreg 0x2102
- restart
- copy startup-config running-config

Explanation

Using the command **confreg 0x2102** changes the configuration register to look for the startup configuration file on boot.

The command **confreg 0x2142** sets the configuration register to ignore the startup configuration file.

The other commands are not used to change the configuration register.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_03_ccna7.question.xml

Question 10. ✓ Correct

One of the steps in the password recovery process for a router is to access the ROM monitor. Which of the following methods will accomplish this? (Select two.)

- → ☑ Use a break sequence during the boot process.
- ☐ Run the **confreg 0x2142** command.
- → ☑ Remove the external flash memory while the device is powered off and then boot.
- ☐ Boot into the BIOS.
- ☐ Run the **confreg 0x2102** command.

Explanation

Access ROMmon mode on your device. You can access ROMmon mode via a console by using a break sequence during the boot-up process. Removing external flash memory while the device is turned off will also cause a device to boot in ROMmon mode.

Using the **confreg 0x2142** command sets the configuration register so the device will ignore the startup config file when the device is rebooted.

Using the **confreg 0x2102** command changes the configuration register so the device will look to the startup config file on restart.

Booting into the BIOS does not enable ROMmon mode.

References

3.5.1 Password Levels
3.5.2 Configure Line Level Passwords
3.5.4 Device Password Facts
3.5.5 Configure Enable Mode Passwords
3.5.8 Router Password Recovery
3.5.9 Recover a Forgotten Password
3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_04_ccna7.question.xml