

Configure Initial Router Settings

10.1.1

Basic Router Configuration Steps

The following tasks should be completed when configuring initial settings on a router.

1. Configure the device name.

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

2. Secure privileged EXEC mode.

```
Router(config)# enable secret password
```

3. Secure user EXEC mode.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

4. Secure remote Telnet / SSH access.

```
Router(config-line)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

5. Secure all passwords in the config file.

```
Router(config-line)# exit
Router(config)# service password-encryption
```

6. Provide legal notification.

```
Router(config)# banner motd delimiter message delimiter
```

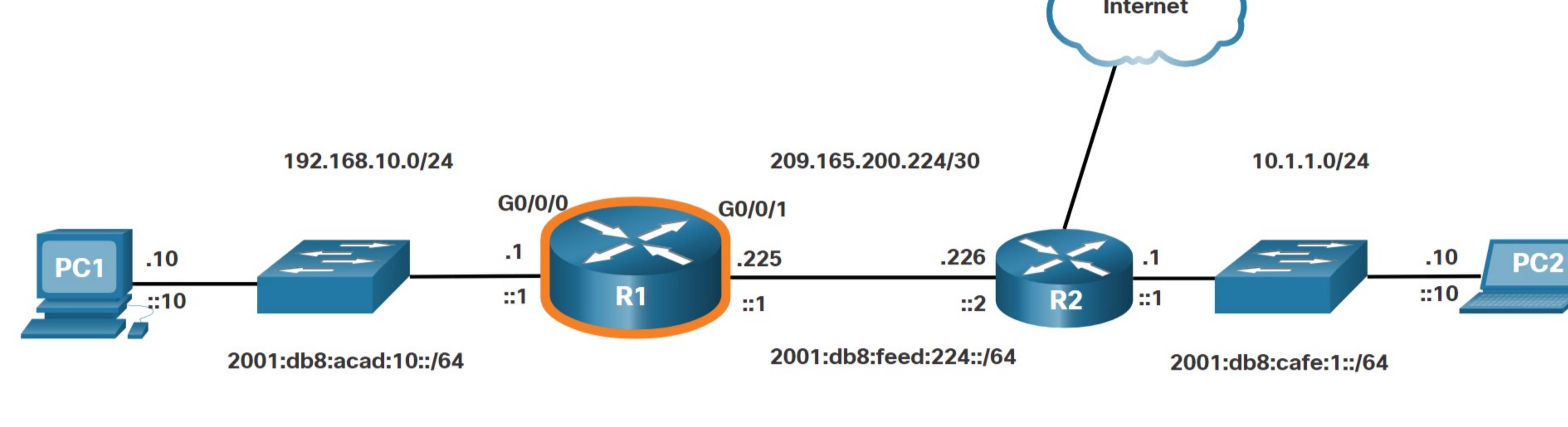
7. Save the configuration.

```
Router(config)# end
Router# copy running-config startup-config
```

10.1.2

Basic Router Configuration Example

In this example, router R1 in the topology diagram will be configured with initial settings.



To configure the device name for R1, use the following commands.

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Note: Notice how the router prompt now displays the router hostname.

All router access should be secured. Privileged EXEC mode provides the user with complete access to the device and its configuration. Therefore, it is the most important mode to secure.

The following commands secure privileged EXEC mode and user EXEC mode, enable Telnet and SSH remote access, and encrypt all plaintext (i.e., user EXEC and VTY line) passwords.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

The legal notification warns users that the device should only be accessed by permitted users. Legal notification is configured as follows.

```
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
*****WARNING: Unauthorized access is prohibited!*****
#
```

If the previous commands were configured and the router accidentally lost power, all configured commands would be lost. For this reason, it is important to save the configuration when changes are implemented. The following command saves the configuration to NVRAM.

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

10.1.3

Syntax Checker - Configure Initial Router Settings

Use this syntax checker to practice configuring the initial settings on a router.

- Configure the device name.
- Secure the privileged EXEC mode.
- Secure and enable remote SSH and Telnet access.
- Secure all plaintext passwords.
- Provide legal notification.

Enter global configuration mode to configure the name of the router as "R1".

```
Router>
```

Reset Show Me Show All

10.1.4

Packet Tracer - Configure Initial Router Settings

In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plaintext passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration.

Configure Initial Router Settings

Configure Initial Router Settings