

### Configuración del router.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
Router#
```

- b. Configure la hora correcta en el router.

```
Router# clock set 10:40:30 6 February 2013
Router#
```

- c. Ingrese al modo de configuración global.

```
Router# config t
Router(config)#
```

- 1) Asigne un nombre de host al router. Use la topología y la tabla de direccionamiento como pautas.

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

- 2) Desactive la búsqueda del DNS.

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

- 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd #Warning! Unauthorized Access is prohibited.#
```

- 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.

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

- 5) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

- 6) Encripte las contraseñas de texto no cifrado.

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

- 7) Cree un nombre de dominio **cisco.com** para el acceso por SSH.

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

- 8) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.

```
R1(config)# username admin secret cisco
```

- 9) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.

```
R1(config)# crypto key generate rsa modulus 512
```

- d. Configure el acceso a las líneas VTY.

- 1) Use la base de datos local para la autenticación de SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

- 2) Habilite SSH solo para el acceso de inicio de sesión.

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

- e. Vuelva al modo de configuración global.

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

- 1) Cree la interfaz Loopback 0 y asigne la dirección IP según la tabla de direcciones.

```
R1(config)# interface loopback 0
```

```
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

- 2) Configure y habilite la interfaz G0/1 en el router.

```
R1(config-if)# int g0/1
```

```
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)# no shut
```

- 3) Configure las descripciones de interfaz para G0/1 y L0.

```
R1(config-if)# description Connected to LAN
```

```
R1(config-if)# int lo0
```

```
R1(config-if)# description Emulate ISP Connection
```

- 4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

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

```
R1# copy run start
```

### Configuración del switch.

- a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
```

```
Switch#
```

- b. Configure la hora correcta en el switch.

```
Switch# clock set 10:52:30 6 February 2013
```

- c. Ingrese al modo de configuración global.

```
Switch# config t
```

- 1) Asigne un nombre de host al switch según la topología y la tabla de direccionamiento.

```
Switch(config)# hostname S1
```

- 2) Desactive la búsqueda del DNS.

```
S1(config)# no ip domain-lookup
```

- 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited.#
```

- 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.

```
S1(config)# enable secret class
```

- 5) Cifre las contraseñas de texto no cifrado.

```
S1(config)# service password-encryption
```

- 6) Cree un nombre de dominio **cisco.com** para el acceso por SSH.

```
S1(config)# ip domain-name cisco.com
```

- 7) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.

```
S1(config)# username admin secret cisco
```

8) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.

```
S1(config)# crypto key generate rsa modulus 512
```

9) Cree y active una dirección IP en el switch según la topología y la tabla de direccionamiento.

```
S1(config)# interface vlan 1
```

```
S1(config-if)# ip address 192.168.1.11 255.255.255.0
```

```
S1(config-if)# no shut
```

10) Configure el gateway predeterminado en el switch.

```
S1(config)# ip default-gateway 192.168.1.1
```

11) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.

```
S1(config-if)# line con 0
```

```
S1(config-line)# password cisco
```

```
S1(config-line)# login
```

d. Configure el acceso a las líneas VTY.

1) Use la base de datos local para la autenticación de SSH.

```
S1(config-line)# line vty 0 15
```

```
S1(config-line)# login local
```

2) Habilite SSH solo para el acceso de inicio de sesión.

```
S1(config-line)# transport input ssh
```

3) Ingrese al modo de configuración correspondiente para configurar las descripciones de interfaz de F0/5 y F0/6.

```
S1(config-line)# int f0/5
```

```
S1(config-if)# description Connected to R1
```

```
S1(config-if)# int f0/6
```

```
S1(config-if)# description Connected to PC-A
```

4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

```
S1(config-if)# end
```

```
S1# copy run start
```