Práctica de laboratorio: configuración de características de seguridad de switch

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los parámetros básicos de los dispositivos y verificar la conectividad

Parte 3: configurar y verificar el acceso por SSH en el S1

- Configurar el acceso por SSH.
- Modificar los parámetros de SSH.
- Verificar la configuración de SSH.

Parte 4: configurar y verificar las características de seguridad en el S1

- Configurar y verificar las características de seguridad general.
- Configurar y verificar la seguridad del puerto.

Información básica/situación

Es muy común bloquear el acceso e instalar buenas características de seguridad en computadoras y servidores. Es importante que los dispositivos de infraestructura de red, como los switches y routers, también se configuren con características de seguridad.

En esta práctica de laboratorio, seguirá algunas de las prácticas recomendadas para configurar características de seguridad en switches LAN. Solo permitirá las sesiones de SSH y de HTTPS seguras. También configurará y verificará la seguridad de puertos para bloquear cualquier dispositivo con una dirección MAC que el switch no reconozca.

Nota: el router que se utiliza en las prácticas de laboratorio de CCNA es un router de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). El switch que se utiliza es Cisco Catalyst 2960 con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers,

switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, solicite ayuda al instructor o consulte las prácticas de laboratorio anteriores para conocer los procedimientos de inicialización y recarga de dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1. establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, si fuera necesario.

Paso 1. realizar el cableado de red tal como se muestra en la topología.

Paso 2. inicializar y volver a cargar el router y el switch.

Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos.

Parte 2. configurar los parámetros básicos de los dispositivos y verificar la conectividad

En la parte 2, configure los parámetros básicos en el router, el switch y la computadora. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica de laboratorio para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1. configurar una dirección IP en la PC-A.

Paso 2. configurar los parámetros básicos en el R1.

a. Configure el nombre del dispositivo.

b. Desactive la búsqueda del DNS.

c. Configure la dirección IP de interfaz que se muestra en la tabla de direccionamiento.

d. Asigne **class** como la contraseña del modo EXEC privilegiado.

e. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

f. Cifre las contraseñas de texto no cifrado.

g. Guarde la configuración en ejecución en la configuración de inicio.

Paso 3. configurar los parámetros básicos en el S1.

Una buena práctica de seguridad es asignar la dirección IP de administración del switch a una VLAN distinta de la VLAN 1 (o cualquier otra VLAN de datos con usuarios finales). En este paso, creará la VLAN 99 en el switch y le asignará una dirección IP.

a. Configure el nombre del dispositivo.

b. Desactive la búsqueda del DNS.

c. Asigne **class** como la contraseña del modo EXEC privilegiado**.**

d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y luego habilite el inicio de sesión.

e. Configure un gateway predeterminado para el S1 con la dirección IP del R1.

f. Cifre las contraseñas de texto no cifrado.

g. Guarde la configuración en ejecución en la configuración de inicio.

h. Cree la VLAN 99 en el switch y asígnele el nombre **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. Configure la dirección IP de la interfaz de administración VLAN 99, tal como se muestra en la tabla de direccionamiento, y habilite la interfaz.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. Emita el comando **show vlan** en el S1. ¿Cuál es el estado de la VLAN 99? _____ Active

k. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo para la interfaz de administración VLAN 99?

_____

El estado es up y el protocolo figura como down.

¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando **no shutdown** para la interfaz VLAN 99?

_____

No se asignaron puertos físicos en el switch a la VLAN 99.

l. Asigne los puertos F0/5 y F0/6 a la VLAN 99 en el switch.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```


m. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99? _____ Up y up

Nota: puede haber una demora mientras convergen los estados de los puertos.

Paso 4. verificar la conectividad entre los dispositivos.

a. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? _____ Sí

b. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente? _____ Sí

c. En el S1, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? _____ Sí

d. En la PC-A, abra un navegador web y acceda a http://172.16.99.11. Si le solicita un nombre de usuario y una contraseña, deje el nombre de usuario en blanco y utilice la contraseña **class**. Si le solicita una conexión segura, conteste **No.** ¿Pudo acceder a la interfaz web en el S1? _____ Sí

e. Cierre la sesión del explorador en la PC-A.

Nota: la interfaz web no segura (servidor HTTP) en un switch Cisco 2960 está habilitada de manera predeterminada. Una medida de seguridad frecuente es deshabilitar este servicio, tal como se describe en la parte 4.

Parte 3. configurar y verificar el acceso por SSH en el S1

Paso 1. configurar el acceso por SSH en el S1.

a. Habilite SSH en el S1. En el modo de configuración global, cree el nombre de dominio **CCNA-Lab.com**.

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

b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al switch a través de SSH. El usuario debe tener acceso de nivel de administrador.

Nota: la contraseña que se utiliza aquí NO es una contraseña segura. Simplemente se usa a los efectos de esta práctica de laboratorio.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Configure la entrada de transporte para que las líneas vty permitan solo conexiones SSH y utilicen la base de datos local para la autenticación.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
```



```
S1(config)# end
```

e. Verifique la configuración de SSH y responda las siguientes preguntas.

```
S1# show ip ssh
SSH Enabled - version 1.99
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 AAAAB3NzaC1yc2EAAAADAQABAAAAgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcgqiKGeeluAu+iQ2drE+k
butnlLTGmtNhdEJMxri/ZeO3BsFcnHpO1hbB6Vsm4XRXGk7OfQ==
```

¿Qué versión de SSH usa el switch? _____ 1.99

¿Cuántos intentos de autenticación permite SSH? _____ 3

¿Cuál es la configuración predeterminada de tiempo de espera para SSH? _____ 120 segundos

Paso 2. modificar la configuración de SSH en el S1.

Modifique la configuración predeterminada de SSH.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
S1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcgqiKGeeluAu+iQ2drE+k
butnlLTGmtNhdEJMxri/ZeO3BsFcnHpO1hbB6Vsm4XRXGk7OfQ==
```

¿Cuántos intentos de autenticación permite SSH? _____ 2

¿Cuál es la configuración de tiempo de espera para SSH? _____ 75 segundos

Paso 3. verificar la configuración de SSH en el S1.

a. Mediante un software de cliente SSH en la PC-A (como Tera Term), abra una conexión SSH en el S1. Si recibe un mensaje en el cliente SSH con respecto a la clave de host, acéptela. Inicie sesión con el nombre de usuario **admin** y la contraseña **class**.

¿La conexión se realizó correctamente? _____ Sí

¿Qué petición de entrada se mostró en el S1? ¿Por qué?

El S1 muestra la petición de entrada en el modo EXEC privilegiado porque la opción privilege 15 se usó al configurar el nombre de usuario y la contraseña.

b. Escriba **exit** para finalizar la sesión de SSH en el S1.

Parte 4. configurar y verificar las características de seguridad en el S1

En la parte 4, desactivará los puertos sin utilizar, desactivará determinados servicios que se ejecutan en el switch y configurará la seguridad de puertos según las direcciones MAC. Los switches pueden estar sujetos a ataques de desbordamiento de la tabla de direcciones MAC, a ataques de suplantación de direcciones

MAC y a conexiones no autorizadas a los puertos del switch. Configurará la seguridad de puertos para limitar la cantidad de direcciones MAC que se pueden detectar en un puerto del switch y para deshabilitar el puerto si se supera ese número.

Paso 1. configurar las características de seguridad general en el S1.

a. Configure un aviso de mensaje del día (MOTD) en el S1 con un mensaje de advertencia de seguridad adecuado.

b. Emita un comando **show ip interface brief** en el S1. ¿Qué puertos físicos están activos?

_____

Los puertos F0/5 y F0/6

c. Desactive todos los puertos sin utilizar en el switch. Use el comando **interface range**.

```
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

d. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado de los puertos F0/1 a F0/4?

_____

Administratively down.

e. Emita el comando **show ip http server status**.

```
S1# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:html
HTTP server help root:
Maximum number of concurrent server connections allowed: 16
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

¿Cuál es el estado del servidor HTTP? _____ Enabled

¿Qué puerto del servidor utiliza? _____ 80

¿Cuál es el estado del servidor seguro de HTTP? _____ Enabled

¿Qué puerto del servidor seguro utiliza? _____ 443

f. Las sesiones HTTP envían todo como texto no cifrado. Deshabilite el servicio HTTP que se ejecuta en el S1.

```
S1(config)# no ip http server
```

g. En la PC-A, abra una sesión de navegador web a http://172.16.99.11. ¿Cuál fue el resultado?

_____

No se pudo abrir la página web. El S1 rechaza las conexiones HTTP.

h. En la PC-A, abra una sesión segura de navegador web en https://172.16.99.11. Acepte el certificado. Inicie sesión sin nombre de usuario y con la contraseña **class**. ¿Cuál fue el resultado?

_____

La sesión web segura se inició correctamente.

i. Cierre la sesión web en la PC-A.

Paso 2. configurar y verificar la seguridad de puertos en el S1.

a. Registre la dirección MAC de G0/1 del R1. Desde la CLI del R1, use el comando **show interface g0/1** y registre la dirección MAC de la interfaz.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

¿Cuál es la dirección MAC de la interfaz G0/1 del R1?

_____

En el ejemplo anterior, es 30f7.0da3.1821

b. Desde la CLI del S1, emita un comando **show mac address-table** en el modo EXEC privilegiado. Busque las entradas dinámicas de los puertos F0/5 y F0/6. Regístrelos a continuación.

Dirección MAC de F0/5: _____30f7.0da3.1821

Dirección MAC de F0/6: _____00e0.b857.1ccd

c. Configure la seguridad básica de los puertos.

Nota: normalmente, este procedimiento se realizaría en todos los puertos de acceso en el switch. Aquí se muestra F0/5 como ejemplo.

1) Desde la CLI del S1, ingrese al modo de configuración de interfaz para el puerto que se conecta al R1.

```
S1(config)# interface f0/5
```

2) Desactive el puerto.

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

3) Habilite la seguridad de puertos en F0/5.

```
S1(config-if)# switchport port-security
```

Nota: la introducción del comando **switchport port-security** establece la cantidad máxima de direcciones MAC en 1 y la acción de violación en shutdown. Los comandos **switchport port-security maximum** y **switchport port-security violation** se pueden usar para cambiar el comportamiento predeterminado.

4) Configure una entrada estática para la dirección MAC de la interfaz G0/1 del R1 registrada en el paso 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx es la dirección MAC real de la interfaz G0/1 del router)

Nota: de manera optativa, puede usar el comando **switchport port-security mac-address sticky** para agregar todas las direcciones MAC seguras que se detectan dinámicamente en un puerto (hasta el máximo establecido) a la configuración en ejecución del switch.

5) Habilite el puerto del switch.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Verifique la seguridad de puertos en F0/5 del S1 mediante la emisión de un comando **show port-security interface**.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

¿Cuál es el estado del puerto de F0/5?

_____

El estado es Secure-up, que indica que el puerto es seguro, pero el valor del estado y el protocolo es up.

e. En el símbolo del sistema del R1, haga ping a la PC-A para verificar la conectividad.

```
R1# ping 172.16.99.3
```

f. Ahora violará la seguridad mediante el cambio de la dirección MAC en la interfaz del router. Ingrese al modo de configuración de interfaz para G0/1 y desactívela.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Configure una nueva dirección MAC para la interfaz, con la dirección **aaaa.bbbb.cccc**.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. De ser posible, tenga una conexión de consola abierta en el S1 al mismo tiempo que realiza este paso. Verá que se muestran varios mensajes en la conexión de consola al S1 que indican una violación de seguridad. Habilite la interfaz G0/1 en R1.

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


i. En el modo EXEC privilegiado del R1, haga ping a la PC-A. ¿El ping se realizó correctamente? ¿Por qué o por qué no?

_____

No, el puerto F0/5 en el S1 está desactivado debido a la violación de seguridad.

j. En el switch, verifique la seguridad de puertos con los comandos que se muestran a continuación.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-------------------------------------------------------------------------
      Fa0/5            1           1                 1         Shutdown
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                Ports      Remaining Age
                                                           (mins)
----     -----------       ----                -----   -------------
  99     30f7.0da3.1821    SecureConfigured    Fa0/5        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. En el router, desactive la interfaz G0/1, elimine la dirección MAC codificada de forma rígida del router y vuelva a habilitar la interfaz G0/1.


```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. Desde el R1, vuelva a hacer ping a la PC-A en 172.16.99.3. ¿El ping se realizó correctamente?
_____ No

m. Emita el comando **show interface f0/5** para determinar la causa de la falla del ping. Registre sus conclusiones.

_____

El puerto F0/5 en el S1 continúa en estado de inhabilitación por errores.

```
S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

n. Borre el estado de inhabilitación por errores de F0/5 en el S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Nota: puede haber una demora mientras convergen los estados de los puertos.

o. Emita el comando **show interface f0/5** en el S1 para verificar que F0/5 ya no esté en estado de inhabilitación por errores.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. En el símbolo del sistema del R1, vuelva a hacer ping a la PC-A. Debería realizarse correctamente.

Reflexión

1. ¿Por qué habilitaría la seguridad de puertos en un switch?

_____

Ayudaría a evitar que los dispositivos no autorizados accedan a su red en caso de que se conectaran a un switch en su red.

2. ¿Por qué deben deshabilitarse los puertos no utilizados en un switch?

_____

Una excelente razón es que un usuario no podría conectar un dispositivo al switch en un puerto sin utilizar para acceder a la LAN.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Configuraciones de dispositivos

Router R1

```
R1#sh run
Building configuration...
Current configuration : 1232 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain-lookup
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
```



```
!
interface GigabitEthernet0/1
 ip address 172.16.99.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!line con 0
 password 7 030752180500
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password 7 13061E01080344
 login
 transport input all
!
```

```
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#sh run
Building configuration...
Current configuration : 3762 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
no ip domain-lookup
ip domain-name CCNA-Lab.com
!
crypto pki trustpoint TP-self-signed-2530358400
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2530358400
 revocation-check none
 rsakeypair TP-self-signed-2530358400
!
crypto pki certificate chain TP-self-signed-2530358400
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32353330 33353834 3030301E 170D3933 30333031 30303030
  35395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35333033
  35383430 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100C0E3 1B8AF1E4 ADA4C4AD F82914AF BF8BCEC9 30CFBF54 D76B3940 38353E50
  A9AE0FCE 9CA05B91 24312B31 22D5F89D D249023E AEEC442D F55315F6 D456DA95
  16B758FB 8083B681 C1B3A3BF 99420EC7 A7E0AD11 CF031CD1 36A997C0 E72BE4DD
  1D745542 1DC958C1 443B6727 F7047747 D94B8CAD 0A99CBDC ADC914C8 D820DC30
  E6B70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 1464D1A8 83DEE145 E35D68C1 D078ED7D 4F6F0B82 9D301D06
  03551D0E 04160414 64D1A883 DEE145E3 5D68C1D0 78ED7D4F 6F0B829D 300D0609
  2A864886 F70D0101 05050003 81810098 D65CFA1C 3942148D 8961D845 51D53202
  EA59B526 7DB308C9 F79859A0 D93D56D6 C584AB83 941A2B7F C44C0E2F DFAF6B8D
  A3272A5C 2363116E 1AA246DD 7E54B680 2ABB1F2D 26921529 E1EF4ACC A4FBD14A
  BAD41C98 E8D83DEC B85A330E D453510D 89F64023 7B9782E7 200F615A 6961827F
  8419A84F 56D71664 5123B591 A62C55
```

```
        quit
!
ip ssh time-out 75
ip ssh authentication-retries 2
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address 30f7.0da3.1821
!
interface FastEthernet0/6
 switchport access vlan 99
 switchport mode access
!
interface FastEthernet0/7
 shutdown

interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
```



```
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.16.99.11 255.255.255.0
!
ip default-gateway 172.16.99.1
no ip http server
ip http secure-server
!
```



```
banner motd ^CWarning! Unauthorized Access is Prohibited.^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```

