Laboratório – Configuração de Recursos de Segurança do Switch

Topologia

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway Padrão
R1	G0/1	172.16.99.1	255.255.255.0	N/D
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: Configurar a topologia e inicializar os dispositivos

Parte 2: Definir configurações básicas do dispositivo e verificar a conectividade

Parte 3: Configurar e verificar o acesso SSH no S1

- Configure o acesso SSH.
- Modifique os parâmetros do SSH.
- Verifique a configuração do SSH.

Parte 4: Configurar e verificar recursos de segurança em S1

- Configure e verifique os recursos de segurança gerais.
- Configure e verifique a segurança de portas.

Histórico/Cenário

É prática comum bloquear o acesso e instalar bons recursos de segurança em computadores e servidores. É importante que os dispositivos de infraestrutura de sua rede, como switches e roteadores, também sejam configurados com recursos de segurança.

Neste laboratório, você seguirá algumas práticas recomendadas para configurar recursos de segurança nos switches de LAN. Você somente permitirá sessões de SSH e HTTPS seguras. Você também configurará e verificará a segurança de portas para bloquear qualquer dispositivo com um endereço MAC não reconhecido pelo switch.

Observação: o roteador utilizado nos laboratórios práticos CCNA é o ISR do Cisco 1941 com software Cisco IOS versão 15.2(4) M3 (imagem universalk9). O switch usado é o Cisco Catalyst 2960 com software IOS Cisco versão 15.0(2) (imagem lanbasek9). Outros roteadores, switches e versões do Cisco IOS podem ser usados. De acordo com o modelo e da versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado no laboratório. Consulte a Tabela de Resumo das Interfaces dos Roteadores no final do laboratório para saber quais são os identificadores de interface corretos.

Observação: certifique-se de que os roteadores e switches tenham sido apagados e que não haja nenhuma configuração de inicialização. Se estiver em dúvida, contate o instrutor ou consulte o laboratório anterior para obter os procedimentos de inicialização e reload de dispositivos.

.

Recursos Necessários

- 1 roteador (Cisco 1941 com Cisco IOS versão 15.2(4)M3 imagem universal ou similar)
- 1 switch (Cisco 2960 com Cisco IOS versão 15.0(2) imagem lanbasek9 ou similar)
- 1 PC (Windows 7, Vista ou XP com o programa de emulação de terminal, como o Tera Term)
- 1 Cabos de console para configurar os dispositivos Cisco IOS pelas portas de console
- 2 Cabos ethernet conforme mostrado na topologia

Parte 1. Configurar a Topologia e Inicializar os Dispositivos

Na Parte 1, você configurará a topologia da rede e limpará todas as configurações, se necessário.

Etapa 1. Cabeie a rede conforme mostrado na topologia.

Etapa 2. Inicialize e recarregue o roteador e o switch.

Se os arquivos de configuração foram salvos anteriormente no roteador ou no switch, inicialize e recarregue esses dispositivos com as configurações básicas.

Parte 2. Definir configurações básicas do dispositivo e verificar a conectividade

Na Parte 2, você define configurações básicas no roteador, no switch e no computador. Consulte a topologia e a Tabela de Endereçamento no início deste laboratório para obter nomes de dispositivos e informações de endereço.

Etapa 1. Configurar um endereço IP no PC-A.

Consulte a Tabela de endereçamento para obter as informações de endereço IP.

Etapa 2. Defina configurações básicas em R1.

a. Use o console para se conectar ao R1 e entre no modo de configuração global.

b. Copie as seguintes configurações básicas e cole-as na configuração em execução do R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (O acesso não autorizado é
estritamente proibido.) #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
interface g0/1
```



```
 ip address 172.16.99.1 255.255.255.0
 no shutdown
end
```

c. Salve a configuração em execução na configuração de inicialização.

Etapa 3. Defina configurações básicas em S1.

a. Use o console para se conectar ao S1 e entre no modo de configuração global.

b. Copie as seguintes configurações básicas e cole-as na configuração em execução do S1.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (O acesso não autorizado é
estritamente proibido.) #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

c. Crie a VLAN 99 no switch e nomeie-a **Gerenciamento**.

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

d. Configure o endereço IP da interface de gerenciamento VLAN 99, como mostrado na Tabela de Endereçamento, e habilite a interface.

```
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#
```

e. Emita o comando **show vlan** em S1. Qual é o status da VLAN 99? _____ Ativo

f. Execute o comando **show ip interface brief** no S1. Qual é o status e o protocolo da interface de gerenciamento da VLAN 99?

_____

O status está ativo e o protocolo está inativo.

Por que o protocolo continua inativo depois que você emitiu o comando **no shutdown** para a interface VLAN 99?

_____

Nenhuma porta física no switch foi atribuída à VLAN 99.

g. Atribua as portas F0/5 e F0/6 à VLAN 99 no 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
```

h. Salve a configuração em execução na configuração de inicialização.

i. Execute o comando **show ip interface brief** no S1. Quais status e protocolo são mostrados na interface de gerenciamento da VLAN 99? _____ Up and up (Ativo e ativo)

Observação: pode haver um atraso enquanto os estados das portas convergem.

Etapa 4. Verifique a conectividade entre os dispositivos.

a. Do PC-A, faça ping no endereço de gateway padrão em R1. Os pings foram bem-sucedidos? _____ Sim

b. Do PC-A, faça ping no endereço de gerenciamento da S1. Os pings foram bem-sucedidos? _____ Sim

c. Da S1, faça ping no endereço do gateway padrão em R1. Os pings foram bem-sucedidos? _____ Sim

d. Do PC-A, abra um navegador e acesse http://172.16.99.11. Se você for solicitado a inserir um nome de usuário e senha, deixar o nome de usuário em branco e utilize **class** como senha. Se for solicitada uma conexão segura, responda **Não**. Você conseguiu acessar a interface da Web no S1? _____ Sim

e. Feche o navegador.

Observação: a interface não segura da Web (servidor HTTP) em um switch Cisco 2960 é habilitada por padrão. Uma medida de segurança comum consiste em desativar esse serviço, conforme descrito na Parte 4.

Parte 3. Configure e verifique o acesso SSH em S1

Etapa 1. Configure o acesso SSH em S1.

a. Habilite SSH em S1. No modo de configuraçãoglobal, crie um nome de domínio de **CCNA-Lab.com**.

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

b. Crie uma entrada no banco de dados de usuário local para ser usada quando você se conectar ao switch via SSH. O usuário deve ter acesso de nível administrativo.

Observação: a senha usada aqui NÃO é uma senha forte. Ela está sendo usada apenas para fins de laboratório.

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

c. Configure a entrada de transporte para as linhas vty a fim de permitir apenas conexões SSH e use o banco de dados local para autenticação.

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



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

d. Gere uma chave de criptografia RSA usando um módulo de 1024 bits.

```
S1(config)#crypto key generate rsa modulus 1024
O nome das chaves será: 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 a configuração do SSH.

```
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==
```

Qual versão do SSH o switch está utilizando? _____ 1.99

Quantas tentativas de autenticação o SSH permite? _____ Três

Qual é a configuração de tempo limite padrão para SSH? _____ 120 segundos

Etapa 2. Modifique a configuração do SSH em S1.

Modifique a configuração padrão do 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==
```

Quantas tentativas de autenticação o SSH permite? _____ Duas

Qual é a configuração de tempo limite para SSH? _____ 75 segundos

Etapa 3. Verifique a configuração do SSH em S1.

a. Utilizando o software cliente SSH no PC-A (como o Tera Term), abra uma conexão SSH para S1. Se você receber uma mensagem no cliente SSH com referência à chave do host, aceite-a. Conecte-se utilizando o nome de usuário **admin** e a senha **sshadmin**.

A conexão teve êxito? _____ Sim

Qual prompt foi exibido em S1? Por quê?

_____

_____

_____

O S1 está mostrando o prompt do modo EXEC privilegiado porque a opção de privilégio 15 foi usada durante a configuração do nome de usuário e senha

b. Digite **exit** para terminar a sessão SSH em S1.

Parte 4. Configurar e verificar recursos de segurança em S1

Na Parte 4, você desativará as portas não utilizadas, desconectará determinados serviços executados no switch e configurará a segurança de portas com base nos endereços MAC. Os switches podem estar sujeitos a ataques de sobrecarga na tabela de endereços MAC, ataques de falsificação de MAC e conexões não autorizadas com as portas do switch. Você configurará a segurança de portas para limitar o número de endereços MAC que podem ser aprendidos em uma porta do switch e desativar a porta se esse número for excedido.

Etapa 1. Configure recursos de segurança gerais em S1.

a. Altere a faixa de MOTD no S1 para "O acesso não autorizado é proibido. Os invasores serão processados de acordo com a lei."

b. Emita um comando **show ip interface brief** em S1. Quais portas físicas estão ativas?

_____

Portas F0/5 e F0/6

c. Desative todas as portas físicas não utilizadas no switch. Use o 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. Execute o comando **show ip interface brief** no S1. Quais são os status das portas F0/1 a F0/4?

_____

Administrativamente desativado.

e. Emita o 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
```

Qual é o status do servidor HTTP? _____Habilitado

Qual porta do servidor ele está usando? _____ 80

Qual é o status do servidor seguro HTTP? _____Habilitado

Qual porta do servidor seguro ele está usando? _____ 443

f. As sessões HTTP enviam tudo em texto não criptografado. Você desabilitará o serviço HTTP em execução em S1.

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

g. Do PC-A, abra um navegador e acesse http://172.16.99.11. Qual foi o resultado?

_____

A página da web não abriu. As conexões HTTP são, agora, recusadas por S1.

h. No PC-A, abra um navegador da Web e acesse https://172.16.99.11. Aceite o certificado. Faça login sem o nome de usuário e com uma senha de **class**. Qual foi o resultado?

_____

A sessão web segura foi bem-sucedida.

i. Feche o navegador da Web.

Etapa 2. Configure e verifique a segurança de portas em S1.

a. Registre o endereço MAC G0/1 de R1. Da CLI de R1, use o comando **show interface g0/1** e anote o endereço MAC da interface.

```
R1# show interface g0/1
GigabitEthernet0/1 está ativa; o protocolo de linha está ativo
  Hardware CN Gigabit Ethernet, endereço 30f7.0da3.1821 (bia 3047.0da3.1821)
```

Qual é o endereço MAC da interface G0/1 de R1?

_____

No exemplo acima, ele é 30f7.0da3.1821

b. Da CLI de S1, emita um comando **show mac address-table** no modo EXEC privilegiado. Encontre as entradas dinâmicas para as portas F0/5 e F0/6. Anote-as abaixo.

Endereço MAC de F0/5: _____
30f7.0da3.1821

Endereço MAC de F0/6: _____
00e0.b857.1ccd

c. Configure a segurança de portas básica.

Observação: este procedimento seria executado normalmente em todas as portas de acesso do switch. F0/5 é exibida aqui como um exemplo.

1) Da CLI de S1, insira o modo de configuração de interface para a porta que se conecta ao R1.

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

2) Desative a porta.

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

3) Ative a segurança de portas em F0/5.

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

Observação: inserir o comando **switchport port-security** define o máximo de endereços MAC como 1 e a ação de violação como desligamento (shutdown). Os comandos **switchport port-security maximum** e **switchport port-security violation** podem ser utilizados para alterar o comportamento padrão.

4) Configure uma entrada estática para o endereço MAC da interface R1 G0/1 registrada na Etapa 2a.

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

(xxxx.xxxx.xxxx é o endereço MAC real da interface G0/1 do roteador)

Observação: se preferir, use o comando **switchport port-security mac-address sticky** para adicionar todos os endereços MAC seguros que forem dinamicamente aprendidos em uma porta (até o máximo definido) à configuração em execução do switch.

5) Habilite a porta do switch.

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

d. Verifique a segurança de porta em F0/5 de S1 emitindo um 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
```

Qual é o status da porta de F0/5?

_____

O status é "Secure-up", o que indica que a porta é segura, mas o status e o protocolo estão ativos.

e. Do prompt de comando R1, faça ping no PC-A para verificar a conectividade.

```
R1# ping 172.16.99.3
```

f. Agora, você violará a segurança, alterando o endereço MAC na interface do roteador. Entre no modo configuração de interface da G0/1 e o desative.

```
R1#config t
```



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

g. Configure um novo endereço MAC para a interface, usando **aaaa.bbbb.cccc** como o endereço.

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

h. Se possível, abra uma conexão de console em S1 de modo simultâneo às duas etapas a seguir. Eventualmente, você visualizará as mensagens exibidas na conexão do console para S1 indicando uma violação de segurança. Habilite a interface G0/1 em R1.

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

i. No modo EXEC privilegiado de R1, faça o ping de PC-A. O ping foi executado com sucesso? Por que usar esse cabo ou por que não usar esse cabo?

_____

Não, a porta F0/5 no S1 está desativada em decorrência da violação de segurança.

j. No switch, verifique a segurança da porta com os seguintes comandos.

```
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. No roteador, desative a interface G0/1, remova o endereço MAC codificado do roteador e ative novamente a interface 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. Do R1, faça ping novamente no PC-A em 172.16.99.3. O ping obteve êxito? _____ Não

m. No switch, emita o comando **show interface f0/5** para determinar a causa da falha de ping. Anote suas descobertas.

_____

A porta F0/5 em S1 ainda está em um estado desativado por erro.

```
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. Limpe o status de erro da F0/5 do S1.

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

Observação: pode haver um atraso enquanto os estados das portas convergem.

o. Emita o comando **show interface f0/5** em S1 para verificar se F0/5 não está mais no modo de desativação por erro.

```
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. No prompt de comando do R1, faça novamente um ping no PC-A. O ping deve obter êxito.

Reflexão

1. Por que você ativaria a segurança de portas em um switch?

_____

Para evitar que dispositivos não autorizados acessem a sua rede quando se conectarem a um switch da rede.

2. Por que as portas não utilizadas em um switch devem ser desativadas?

_____

Uma excelente razão é que um usuário não conseguiria conectar um dispositivo ao switch em uma porta não utilizada e acessar a LAN.

Tabela de Resumo das Interfaces dos Roteadores

Resumo das Interfaces dos Roteadores				
Modelo do Roteador	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface Serial 1**	**Interface Serial 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)

Observação: para descobrir como o roteador está configurado, examine as interfaces para identificar o tipo de roteador e quantas interfaces ele tem. Não há como listar efetivamente todas as combinações de configurações para cada classe de roteador. Esta tabela inclui identificadores para as combinações possíveis de Ethernet e Interfaces seriais no dispositivo. Esse tabela não inclui nenhum outro tipo de interface, embora um roteador específico possa conter algum. Um exemplo disso poderia ser uma interface ISDN BRI. A string entre parênteses é a abreviatura legal que pode ser usada no comando do Cisco IOS para representar a interface.

Configurações de Dispositivos

Roteador R1

```
R1#sh run
Building configuration...
Configuração atual : 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...
Configuração atual : 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
```

