

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/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: 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 porta.

Histórico/cenário

É prática comum bloquear o acesso e instalar bons recursos de segurança em PCs 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 porta para bloquear qualquer dispositivo com um endereço MAC não reconhecido pelo switch.

Observação: o roteador usado nos laboratórios práticos CCNA é o Roteador de Serviços Integrados (ISR) do Cisco 1941 com software IOS Cisco 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 IOS Cisco podem ser usados. Dependendo do modelo e da versão do IOS Cisco, os comandos disponíveis e a saída produzida podem diferir dos mostrados nos laboratórios. Consulte a tabela Resumo da interface do roteador no final deste laboratório para obter 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 software IOS Cisco versão 15.2(4)M3, imagem universal ou semelhante)
- 1 switch (Cisco 2960 com IOS Cisco versão 15.0(2), imagem lanbasek9 ou semelhante)
- 1 PC (Windows 7, Vista ou XP com um programa de emulação de terminal, como o Tera Term)
- Cabos de console para configurar os dispositivos IOS Cisco através das portas de console
- Cabos Ethernet conforme mostrado na topologia

Parte 1: Configure a topologia e inicialize os dispositivos

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

Etapa 1: Instale os cabos da 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 de volta às 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 PC. Consulte a topologia e a Tabela de Endereçamento no início deste laboratório para obter nomes de dispositivos e informações de endereço.

Etapa 1: Configure um endereço IP no PC-A.

Etapa 2: Defina configurações básicas em R1.

- Configure o nome do dispositivo.
- Desative a pesquisa DNS.
- Configure o endereço IP da interface conforme mostrado na Tabela de Endereçamento.
- Atribua **class** como a senha do modo EXEC privilegiado.
- Atribua **cisco** como senha de console e vty e habilite o login.
- Criptografe as senhas de texto não criptografado.
- Salve a configuração em execução na configuração de inicialização.

Etapa 3: Defina configurações básicas em S1.

Uma boa prática de segurança consiste em atribuir o endereço IP de gerenciamento do switch a uma VLAN diferente de VLAN 1 (ou qualquer outra VLAN de dados com usuários finais). Nesta Etapa, você criará a VLAN 99 no switch e atribuirá a ela um endereço IP.

- Configure o nome do dispositivo.
- Desative a pesquisa DNS.

- c. Atribua **class** como a senha do modo EXEC privilegiado.
- d. Atribua **cisco** como uma senha de console e de vty e, em seguida, habilite o login.
- e. Configure um gateway padrão para S1 usando o endereço IP de R1.
- f. Criptografe as senhas de texto não criptografado.
- g. Salve a configuração em execução na configuração de inicialização.
- h. Crie a VLAN 99 no switch e nomeie-a **Management**.

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

- i. 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#
```

- j. Emita o comando **show vlan** em S1. Qual é o status da VLAN 99? _____
- k. Execute o comando **show ip interface brief** no S1. Qual é o status e o protocolo da interface de gerenciamento da VLAN 99?

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

- l. 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
```

- m. Execute o comando **show ip interface brief** no S1. Quais status e protocolo são mostrados na interface de gerenciamento da VLAN 99? _____

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? _____
- b. Do PC-A, faça ping no endereço de gerenciamento da S1. Os pings foram bem-sucedidos? _____
- c. Da S1, faça ping no endereço do gateway padrão em R1. Os pings foram bem-sucedidos? _____

- d. Do PC-A, abra um navegador e acesse `http://172.16.99.11`. Se a tela lhe solicitar um nome de usuário e senha, deixe o nome de usuário em branco e utilize **class** como a senha. Se a tela perguntar se deseja uma conexão segura, responda **No**. Você conseguiu acessar a interface da web em S1? _____
- e. Feche a sessão do navegador no PC-A.

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 configuração global, crie um nome de domínio de **CCNA-Lab.com**.
`S1(config)# ip domain-name CCNA-Lab.com`
- b. Crie uma entrada de 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
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 a configuração do SSH e responda às perguntas abaixo.

```
S1# show ipssh
```

Qual versão do SSH o switch está utilizando? _____

Quantas tentativas de autenticação o SSH permite? _____

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

Etapa 2: Modifique a configuração do SSH em S1.

Modifique a configuração padrão do SSH.

```
S1# config t
S1(config)# ipssh time-out 75
```

```
S1(config)# ipssh authentication-retries 2
```

Quantas tentativas de autenticação o SSH permite? _____

Qual é a configuração de tempo limite para SSH? _____

Etapa 3: Verifique a configuração do SSH em S1.

- a. Usando 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. Faça login, usando **admin** para o nome de usuário e **cisco** para a senha.

A conexão teve êxito? _____

Qual prompt foi exibido em S1? Por quê?

- 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 porta 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 porta 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. Configure um banner de mensagem do dia (MOTD) em S1 com uma mensagem de aviso de segurança apropriada.
- b. Emita um comando **show ip interface brief** em S1. Quais portas físicas estão ativas?

- 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?

- e. Emita o comando **show ip http server status**.

Qual é o status do servidor HTTP? _____

Qual porta do servidor ele está usando? _____

Qual é o status do servidor seguro HTTP? _____

Qual porta do servidor seguro ele está usando? _____

- 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 uma sessão do navegador para `http://172.16.99.11`. Qual foi o resultado?
-

- h. Do PC-A, abra uma sessão de navegador segura em `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?
-

- i. Feche a sessão web no PC-A.

Etapa 2: Configure e verifique a segurança de porta 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 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)
```

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

- 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: _____

Endereço MAC de F0/6: _____

- c. Configure a segurança de porta 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 porta 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 usados 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?

- 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, deixe uma conexão de console aberta em S1 ao mesmo tempo em que executa esta Etapa. Você verá várias mensagens exibidas na conexão do console para o S1, indicando uma violação de segurança. Habilite a interface G0/1 em R1.

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

- i. Do modo EXEC privilegiado R1, faça ping no PC-A. O ping foi bem-sucedido? Por quê? Ou, por que não?
-

- j. No switch, verifique a segurança de porta por meio dos comandos exibidos abaixo.

```
S1# show port-security
Secure Port MaxSecureAddrCurrentAddrSecurityViolation 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 foi bem-sucedido? _____
- m. Emita o comando **show interface f0/5** para determinar a causa da falha de ping. Anote suas descobertas.

-
- 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. Agora você deve ser bem-sucedido.

Reflexão

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

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

Tabela Resumo das Interfaces dos Roteadores

Resumo da interface do roteador				
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, analise as interfaces para identificar o tipo de roteador e quantas interfaces ele possui. Não há como listar com eficácia todas as combinações de configuração de cada classe de roteador. Esta tabela inclui identificadores para as possíveis combinações de interfaces seriais e de Ethernet no dispositivo. A 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 sequência entre parênteses é a abreviatura legal que pode ser usada nos comandos do IOS Cisco para representar a interface.				