Laboratório - Configurar a autenticação baseada no servidor com RADIUS

Topologia

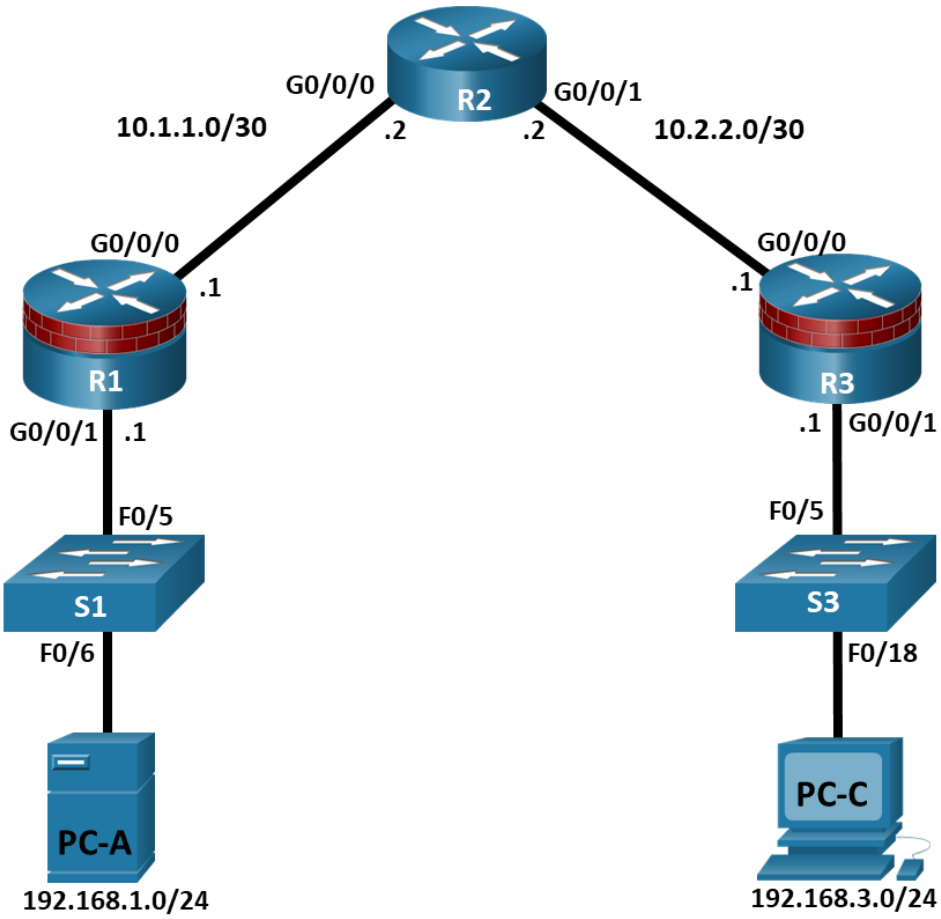

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
R1	G0/0/0	10.1.1.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.1.1	255.255.255.0	N/D	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/D	N/D
	G0/0/1	10.2.2.2	255.255.255.252	N/D	N/D
R3	G0/0/0	10.2.2.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.3.1	255.255.255.0	N/D	S3 F0/5

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
RADIUS Server no PC-A	Placa de rede	192.168.1.11	255.255.255.0	192.168.1.1	N/D
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objetivos

Parte 1: Implementar as Configurações Básicas do Dispositivo

Parte 2: Configurar a autenticação centralizada usando o AAA e o RAIO

- Enable AAA.
- Configurar a lista de autenticação de login padrão.
- Especifique um servidor Radius.

Parte 3: Configurar a autenticação centralizada usando o AAA e o RAIO

- Teste a configuração do RAIO AAA.
- Alterar os números de porta RADIUS

Histórico/Cenário

A forma mais básica de segurança de acesso ao roteador é criar senhas para o console, vty e linhas auxiliares. Um usuário é solicitado apenas uma senha ao acessar o roteador. Configurar uma senha secreta do modo EXEC privilegiada melhora ainda mais a segurança, mas ainda assim apenas uma senha básica é necessária para cada modo de acesso. Bancos de dados locais com nomes de usuário com diferentes níveis de privilégio também podem ser usados e os usuários serão solicitados para que nomes de usuário e senhas acessem os dispositivos.

Além das senhas básicas e da autenticação local, o controle adicional sobre o processo de login pode ser alcançado usando autenticação, autorização e contabilidade (AAA). Para a autenticação básica, o AAA pode ser configurado para alcançar o base de dados local para logins do usuário, e os procedimentos de fallback também podem ser definidos. Contudo, esta aproximação não é muito escalável porque deve ser configurada em cada roteador. Para aproveitar ao máximo o AAA e conseguir a escalabilidade máxima, o AAA é usado conjuntamente com um banco de dados externo do servidor TACACS+ ou RADIUS. Quando um usuário tenta entrar, o roteador faz referência ao banco de dados de servidor externo para verificar se o usuário está fazendo login com um nome de usuário e senha válidos.

Neste laboratório, você constrói uma rede do multi-roteador e configura o Roteadores e os anfitriões. Você alcançará o software RADIUS em um computador externo e usará o AAA para autenticar usuários com o servidor RADIUS.

Nota: Os roteadores usados com laboratórios hands-on são Cisco 4221 com a versão 16.9.6 do Cisco IOS XE (imagem universersalk9). Os switches usados nos laboratórios são Cisco Catalyst 2960+ com a versão Cisco IOS 15.2 (7) (imagem lanbasek9). Outros roteadores, switches e versões do Cisco IOS podem ser usados. De acordo com o modelo e a versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado nos laboratórios. Consulte a Tabela de resumo de interfaces dos roteadores no final do laboratório para saber quais são os identificadores de interface corretos.

Nota: Antes de começar, verifique se os roteadores e os comutadores foram apagados e não têm configurações de inicialização.

Recursos necessários

- 3 roteadores (Cisco 4221 com a Cisco Xe Release 16.9.6 Imagem universal ou comparável com uma licença de pacote de tecnologia de segurança)
- 2 switches (Cisco 2960+ com lançamento do Cisco IOS 15.2 (7) imagem lanbasek9 ou comparável)
- 2 PCs (sistema operacional Windows com um aplicativo de emulação de terminal e software de virtualização, como VirtualBox instalado)
- 1 Máquina Virtual Security Workstation com servidor RADIUS já instalado
- Cabos de console para configurar dispositivos de rede Cisco
- Cabos ethernet conforme mostrado na topologia

Instruções

Parte 1: Implementar as Configurações Básicas do Dispositivo

Nesta parte, você configura a topologia da rede e define as configurações básicas, como os endereços IP da interface, roteamento estático, acesso ao dispositivo e senhas.

As configurações iniciais do roteador são fornecidas e as configurações para o Switches são opcionais.

Etapa 1: Cabeie a rede conforme mostrado na topologia.

Conecte os dispositivos conforme mostrado no diagrama de topologia e, a seguir, conecte os cabos conforme necessário.

Etapa 2: Carregue as configurações.

Nesta etapa, você copiará e colará as configurações em cada roteador.

Roteador R1

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R1
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.1.1.2
line con 0
```

```
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Roteador R2

```
enable
config terminal
no ip domain lookup
host R2
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
ip address 10.2.2.2 255.255.255.252
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 192.168.1.0 255.255.255.0 10.1.1.1
ip route 192.168.3.0 255.255.255.0 10.2.2.1
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
```

```
end
```

Roteador R3

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R3
interface GigabitEthernet0/0/0
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.2.2.2
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Etapa 3: Configurar computadores

O PC-A funcionará como o servidor Radius para este laboratório. Uma máquina virtual com um servidor RADIUS está configurada para uso neste curso. Você pode implantar a máquina virtual no PC-A seguindo **Lab - Instalando a máquina virtual** se você ainda não tiver feito isso. Você pode optar por transferir, instalar e configurar um servidor Radius para seu uso, se desejado.

a. Atribua o endereço IP e o gateway padrão no PC-C de acordo com a Tabela de endereçamento.

b. Se você ainda não implantou a máquina virtual **Security Workstation VM**, volte para **Lab - Instalando a máquina virtual**.

c. Inicie o VirtualBox e verifique se a estação de trabalho de segurança está usando o adaptador em ponte nas configurações de rede.

d. Inicie a VM da estação de trabalho de segurança. Entre na VM como **sec_admin** com a senha **Net_SecPW**. Selecione o usuário **sec_admin** na lista suspensa, se necessário.

e. Na barra de menus na parte inferior da Área de Trabalho, clique em **Emulador de terminal**.

f. Dentro da janela do emulador de terminal, você configurará esta máquina virtual com um endereço IP de 192.168.1.11 executando um script. Quando solicitado uma senha, use a senha **Net_SecPW**.

```
[sec_admin @Workstation ~] $ cd ~/lab.support.files/scripts/
[sec_admin @Workstation scripts] $ . Arquivo /configure_as_static.sh
[sudo] senha para sec_admin:
Configurando a NIC como:
IP: 192.168.11.1/24
GW: 192.168.1.1

Configuração de IP bem-sucedida.
```

g. Incorpore o **IP addr** na alerta para verificar o endereço IP estático atribuído na estação de trabalho VM da segurança.

```
[sec_admin @Workstation scripts] $ ip addr
<output omitted>
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 00:50:56:9 c:c 5:37 brd ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 escopo eth0 global
       valid_lft forever preferred_lft forever
    inet6 fe80:: 250:56 ff: fe9c: 5248/64 link de escopo
       valid_lft forever preferred_lft forever
```

h. Ping o endereço IP do gateway (G0/0/0 do R1, 192.168.1.1) da Security Workstation VM.

```
[sec_admin @Workstation scripts] $ ping -c 4 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.605 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.661 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.654 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.661 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0,605/0.640/0.661/0.021 ms
```

Etapa 4: Verifique a conectividade.

a. Teste a conectividade fazendo ping da Security Workstation VM para o PC-C. Se os sicos não são bem sucedidos, pesquise defeitos as configurações do roteador e do PC até que estejam.

b. No terminal de VM do Security Workstation, estabeleça uma sessão SSH com o R1 usando o username **user01** e a senha **user01pass**. Digite **sim** quando solicitado se tiver certeza de que deseja continuar conectando.

```
[sec_admin @Workstation scripts] $ ssh -l user01 192.168.1.1
```

c. Saia da sessão SSH quando terminar. Estabeleça um outro SSH com o R1 usando o username **admin** e a senha **cisco12345**.

d. Saia da sessão SSH quando terminar. Agora você verificou a conectividade de ponta a ponta e a Security Workstation VM pode se comunicar com o roteador R1.

Parte 2: Configurar a autenticação centralizada usando o AAA e o RAIO

Nesta parte, você configurará o R1 para usar serviços AAA para autenticar usuários. O servidor Radius já está configurado com um **usuário RadUser** com a senha **RadUserPass** e a chave compartilhada secreta **$trongKey**.

Etapa 1: Enable o AAA no R1.

Abra um console no R1 e use o comando **aaa new-model** no modo de configuração global permitir o AAA.

```
R1(config)# aaa new-model
```

Etapa 2: Configurar a lista de autenticação de login padrão.

Configurar a lista para usar primeiramente o RADIUS para o serviço de autenticação, e então o fallback, **nenhum**. Se nenhum servidor RADIUS puder ser alcançado e a autenticação não puder ser executada, o roteador permite globalmente o acesso sem autenticação. Esta é uma medida da salvaguarda caso que o roteador comece acima sem conectividade a um servidor Radius ativo.

```
R1(config)# aaa authentication login default group radius none
```

Nota: Você poderia alternativamente configurar a autenticação local como o método de autenticação de backup.

Nota: Se você não estabelece uma lista de autenticação de login padrão, você poderia obter travado fora do roteador e precisa de usar o procedimento de recuperação de senha para seu roteador específico.

Etapa 3: Especifique um servidor Radius.

a. Use o comando **Radius Server** incorporar o modo de configuração do servidor RADIUS.

```
R1(config)# radius server NetSec
```

b. Use o **?** para ver os comandos submode disponíveis para configurar um servidor RADIUS.

```
R1(config-radius-server)# ?
Comandos do submodo do servidor RADIUS:
  address Specify the radius server address
  automate-tester Configure server automated testing.
  backoff Retry backoff pattern(Default is retransmits with constant
                  )
  sair do modo de configuração do servidor RADIUS
  key Per-server encryption key
  no Negate a command or set its defaults
  non-standard Attributes to be parsed that violate RADIUS standard
  pac Protected Access Credential key
  retransmit Number of retries to active server (overrides default)
  timeout Time to wait (in seconds) for this radius server to reply
                  (overrides default)
```

c. Use o comando **address** configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius.

```
R1(config-radius-server)# address ipv4 192.168.1.11
```

d. O comando **key** é usado para a senha secreta que é compartilhada entre o servidor Radius e o roteador (R1 neste caso) e é usado para autenticar a conexão entre o roteador e o servidor antes que o processo

de autenticação do usuário ocorra. Use a senha secreta de **$TrongPass** que foi configurada no servidor Radius. Lembre-se de que as senhas diferenciam maiúsculas de minúsculas.

```
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# end
```

Nota: Para fins deste laboratório, uma senha não criptografada é configurada. No futuro, o IOS exigirá senhas criptografadas.

Parte 3: Teste a configuração do RAIO AAA.

Etapa 1: Inicie o servidor Radius e verifique a operação.

a. No terminal da estação de trabalho de segurança, inicie o servidor RADIUS inserindo o comando **sudo systemctl start freeradius.service**. Digite a senha **Net_SecPW** conforme necessário.

```
[sec_admin @Workstation ~] $ sudo systemctl iniciar freeradius.service
```

b. Verifique se o servidor está sendo executado, digite o comando **sudo systemctl status freeradius.service** no prompt do terminal.

```
[sec_admin @Workstation ~] $ sudo systemctl status freeradius.service
? freeradius.service - Servidor RADIUS de alto desempenho FreeRadius.
     Loaded: loaded (/usr/lib/systemd/system/freeradius.service; disabled; vendor
preset: disabled)
     Active: active (running) since Sun 2021-02-14 22:14:07 EST; 18min ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             https://wiki.freeradius.org/Página inicial
             https: //networkradius.com/freeradius-documentation/
    Process: 890 ExecStartPre=/usr/bin/radiusd -C (code=exited, status=0/SUCCESS)
    Process: 893 ExecStart=/usr/bin/radiusd -d /etc/raddb (code=exited,
status=0/SUCCESS)
   Main PID: 895 (radiusd)
      Tasks: 6 (limit: 1113)
     Memory: 77.5M
     CGroup: /system.slice/freeradius.service
             mq895 /usr/bin/radiusd -d /etc/raddb

Feb 14 22:14:07 Workstation systemd[1]: Starting FreeRADIUS high performance RADIUS
server....
Feb 14 22:14:07 Workstation systemd[1]: Started FreeRADIUS high performance RADIUS
server..
```

Etapa 2: Teste sua configuração.

Você pode testar e verificar suas configurações do servidor RADIUS em seu roteador antes de sair do roteador usando o comando **test aaa**. A mensagem de saída indica que não há nenhuma resposta autoritária do RAIO sever.

```
R1# test aaa group radius RadUser RadUserpass legacy
Attempting authentication test to server-group radius using radius
No authoritative response from any server
```

Você também pode ver mensagens semelhantes às seguintes podem ser exibidas após os testes tentados indicando que o servidor RADIUS em 192.168.1.11 não está se comunicando com o roteador.


```
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.11:1645,1646 is
not responding.
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.11:1645,1646 is
being marked alive.
```

Etapa 3: Pesquise defeitos a comunicação do servidor Router-to-Radius.

O comando **show radius server-group radius** indica que o roteador está usando as portas UDP 1645 e 1646 para comunicações.

```
R1# show radius server-group radius
Server group radius
    Sharecount = 1 sg_unconfigured = FALSE
    Type = standard Memlocks = 1
    Server(192.168.1.11:1645,1646) Transactions:
    authen: 32 Autor: 0 Acct: 0
    SERVER_AUTO_TEST_ENABLED: FALSE
     Keywrap enabled: FALSE
```

RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS. Isto indica que o roteador e o servidor Radius não estão se comunicando nas mesmas portas.

Etapa 4: Mude os números de porta RADIUS no R1 para combinar o servidor Radius.

A menos que especificado em contrário, a configuração do Cisco IOS RADIUS padroniza-se aos números de porta UDP 1645 e 1646. Os números de porta do Cisco IOS do roteador devem ser alterados para combinar o número de porta do servidor RADIUS ou os números de porta do servidor Radius devem ser alterados para combinar os números de porta do Cisco IOS Router.

a. Reemita novamente o comando address sub-mode novamente. Desta vez, especifique os números de porta **1812e 1813**, juntamente com o endereço IPv4**.**

```
R1(config)# radius server NetSec
R1(config-radius-server)# address ipv4 192.168.1.11 auth-port 1812 acct-port
1813
```

b. Teste o roteador às comunicações de servidor RADIUS novamente usando o comando **test aaa** .

```
R1# test aaa group radius RadUser RadUserpass legacy
Tentativa de teste de autenticação para raio de grupo de servidor usando raio
O usuário foi autenticado com sucesso.
```

Etapa 5: Teste sua configuração fazendo login no console no R1.

a. Sair para a tela inicial do roteador que exibe: R1 con0 está agora disponível, pressione **RETURN** para começar.

b. Entre novamente com o nome de usuário do **RadUser** e senha do **RadUserPass**.

Você conseguiu fazer o login? Houve algum atraso desta vez?

c. Faça login novamente usando um nome de usuário inválido de **Userxxx** e a senha de **Userxxxpass**.

Você foi capaz de fazer login?

Qual mensagem foi exibida no roteador?

d. Entre outra vez usando as credenciais do usuário local, **admin** / **cisco12345** ou **user01** / **user01pass**.

Você conseguiu fazer logon? Explique.

Etapa 6: Crie uma lista de métodos de autenticação para SSH e teste-a.

a. Faça login de volta no R1 conforme necessário.

b. Crie uma lista exclusiva do método de autenticação para o acesso SSH ao roteador. Isto não tem o fallback de nenhuma autenticação, assim que se não há nenhum acesso ao servidor Radius, o acesso SSH está desabilitado. Nomeie a lista de métodos de autenticação **SSH_LINES**.

```
R1(config)# aaa authentication login SSH_LINES group radius
```

c. Aplique a lista às linhas vty no roteador usando o comando **login authentication**.

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

d. Estabeleça uma sessão SSH do PC-C ao R1 (10.1.1.1) e entre com o nome de **usuário RadUser** e a senha do **RadUserPass**. Você foi capaz de obter acesso para fazer login? Explique.

e. Estabeleça uma sessão SSH de PC-C para R1 novamente. Entre com o username **user01** e a senha do **user01pass**. Você conseguiu fazer logon? Explique.

Reflexão

1. Por que uma organização gostaria de usar um servidor de autenticação centralizado em vez de configurar usuários e senhas em cada roteador individual?

2. Contraste a autenticação local e a autenticação local com o AAA.

Tabela de resumo das interfaces dos roteadores

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
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)

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para descobrir como o roteador está configurado, consulte as interfaces para identificar o tipo de roteador e quantas interfaces o roteador possui. 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.