Laboratório - Configurar acesso administrativo seguro

Topologia

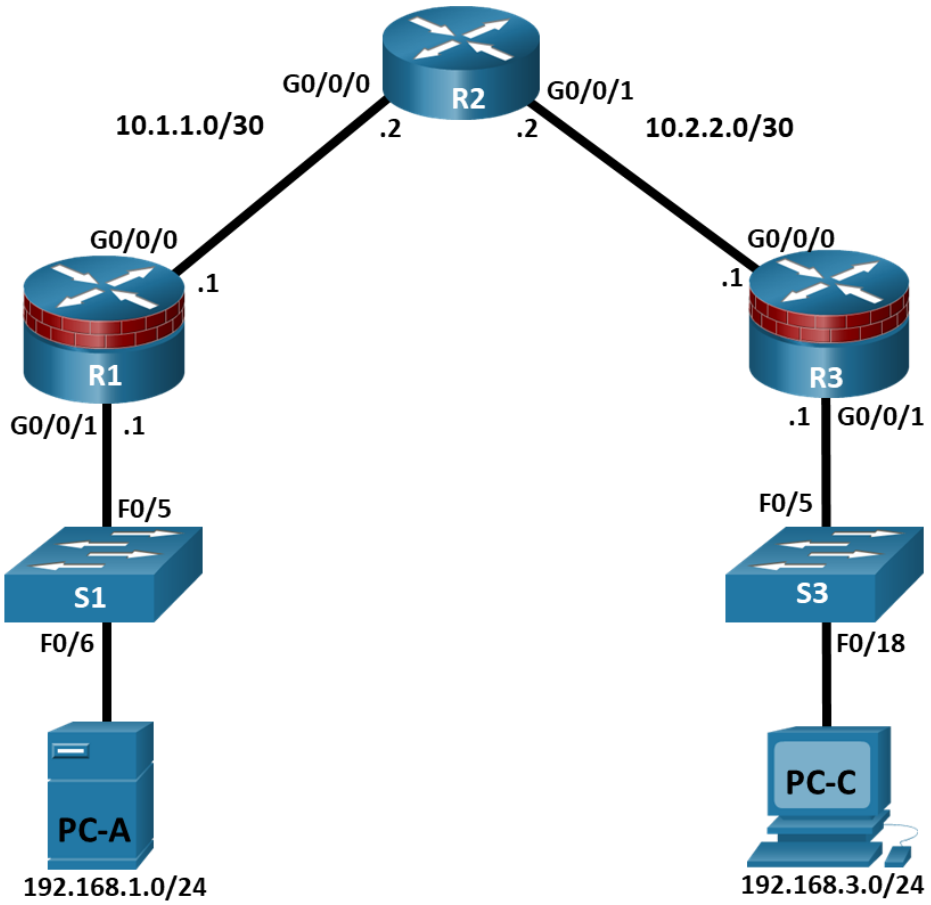

Tabela de endereçamento

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
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
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

- Cabeie a rede conforme mostrado na topologia.
- Configure o endereçamento IP básico para roteadores e PCs.
- Configure o roteamento de OSPF.
- Configure os PCs hosts.
- Verifique a conectividade entre hosts e roteadores.

Parte 2: Configurar e criptografar senhas nos roteadores R1 e R3

- Configure a senha criptografada para linhas de acesso virtual, porta auxiliar e console.
- Criptografar senhas em texto não criptografado
- Configurar um banner de mensagem de aviso

Parte 3: Configurar a segurança aprimorada da senha do nome de usuário nos roteadores R1 e R3

- Criar novas contas de usuário
- Faça login usando as contas de usuário

Parte 4: Configurar o servidor SSH no Roteadores R1 e R3

- Configure um nome de domínio
- Gerar chave de criptografia RSA
- Configure e verifique as configurações SSH

Histórico/Cenário

O roteador é um componente crítico em qualquer rede. Ele controla o movimento de dados para dentro e fora da rede e entre dispositivos dentro da rede. É particularmente importante proteger o Roteadores de rede porque a falha de um dispositivo de roteamento poderia tornar as seções da rede, ou de toda a rede, inacessíveis. Controlar o acesso aos roteadores e permitir relatórios sobre roteadores é fundamental para a segurança da rede e deve fazer parte de uma política de segurança abrangente.

Neste laboratório, você construirá uma rede de vários roteadores e configurará os roteadores e hosts. Use várias ferramentas de CLI para proteger o acesso local e remoto aos roteadores, analisar potenciais vulnerabilidades e tomar medidas para atenuá-las. Ative o relatório de gerenciamento para monitorar as alterações de configuração do roteador.

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 programa de emulação de terminal, como PuTTY ou Tera Term 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, configure a topologia da rede e configure as configurações básicas, como endereços IP da interface.

Etapa 1: Conectar a rede.

Anexar os dispositivos, conforme mostrado no diagrama de topologia e cabo conforme necessário.

Etapa 2: Defina as configurações básicas de cada Roteador.

a. Use o console para se conectar ao roteador e ative o modo EXEC privilegiado.

```
Router> enable
Router# configure terminal
```

b. Configure os nomes de host conforme mostrado na topologia.

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

c. Configure endereços IP da interface conforme mostrado na tabela de endereçamento IP.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

d. Para evitar que o roteador tente traduzir comandos inseridos incorretamente como se fossem nomes de host, desative a pesquisa de DNS. R1 é mostrado aqui como exemplo.

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

Etapa 3: Configure o roteamento do OSPF nos roteadores.

a. Use o comando **router ospf** no modo de configuração global para ativar o OSPF em R1.

```
R1(config)# router ospf 1
```

b. Configure as instruções **network** para as rede em R1. Use um ID de área igual a 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure o OSPF em R2 e R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Emita o comando **passive-interface** Para alterar a interface G0/0/1 em R1 e R3 para passivo.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Etapa 4: Verifique os vizinhos OSPF e as informações de roteamento.

a. Emita o comando **show ip ospf neighbor** para verificar se cada roteador lista os outros roteadores na rede como vizinhos.

```
R1# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 1 FULL/BDR 00:00:37 10.1.1.2 GigabitEthernet0/0/0
```

b. Emita o comando **show ip route** para verificar se todas as redes são exibidas na tabela de roteamento em todos os roteadores.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set.

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O 10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, Gigabitethernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O 192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, Gigabitethernet0/0/0
```

Etapa 5: Defina as configurações de IP do host do PC.

Configure um endereço IP estático, máscara de sub-rede e gateway padrão para PC-A e PC-C, conforme mostrado na tabela de endereçamento IP.

Etapa 6: Verifique a conectividade entre PC-A e PC-C.

a. Faça ping de R1 para R3.

Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

b. Ping do PC-A, na LAN R1, ao PC-C, na LAN R3.

Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

Nota: Se você pode fazer o ping do PC-A ao PC-C você demonstrou que o roteamento OSPF está configurado e funcionando corretamente. Se você não pode executar o ping mas as interfaces de dispositivo estão acima e os endereços IP de Um ou Mais Servidores Cisco ICM NT estão corretos, use os comandos show run, show ip ospf neighbor, e show ip route ajudar a identificar problemas relacionados ao protocolo de roteamento.

Etapa 7: Salve a configuração básica de execução de cada roteador.

Salve a configuração de execução básica para os roteadores como arquivos de texto em seu PC. Esses arquivos de texto podem ser usados para restaurar configurações mais tarde no laboratório.

Parte 2: Configurar e criptografar senhas nos roteadores R1 e R3

Nesta parte, você irá:

- Configurar senhas criptografadas.
- Configurarum banner de aviso de login.
- Configurar a segurança aprimorada da senha do usuário
- Configurar a segurança de login virtual aprimorada.

Nota: Execute todas as tarefas no R1 e no R3. Os procedimentos e a saída para R1 são mostrados aqui.

Etapa 1: Configurar senhas criptografadas nos roteadores R1 e R3.

a. Configurar a senha criptografada segredo da possibilidade em ambos os roteadores. Use o algoritmo de hash tipo 9 (SCRYPT).

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

Como configurar uma senha secreta de habilitação ajuda a proteger um roteador de ser comprometido por um ataque?

b. Use o comando **security passwords** para definir um comprimento mínimo de senha de 10 caracteres.

```
R1(config)# security passwords min-length 10
```

Etapa 2: Configure o console básico, a porta auxiliar e as linhas de acesso virtual.

Nota: As senhas nesta tarefa são definidas com um mínimo de 10 caracteres, mas são relativamente simples para o benefício de realizar o laboratório. Senhas mais complexas são recomendadas em uma rede de produção.

a. Configure uma senha de console e habilite o login para roteadores. Para segurança adicional, o comando **exec-timeout** faz com que a linha seja desconectada após 5 minutos de inatividade. O comando **logging synchronous** impede que as mensagens do console interrompam a entrada do comando.

Nota: Para evitar logins repetitivos durante este laboratório, o comando exec-timeout pode ser ajustado a 0, que o impede de expirar. No entanto, esta não é considerada uma boa prática de segurança.

```
R1(config)#line console 0
R1(config-line)# password ciscocon
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

Quando você configurou a senha para a linha de console, qual mensagem foi exibida?

b. Configure uma senha nova do **ciscoconpass** para o console.

c. Configurar uma senha para a porta AUX para o roteador R1.

```
R1(config)# line aux 0
R1(config-line) # password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Telnet de R2 para R1.

```
R2> telnet 10.1.1.1
```

Você foi capaz de fazer login? Explique.

Quais mensagens foram exibidas?

e. Configurar a senha nas linhas vty para o roteador R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# transport input telnet
R1(config-line)#login
```

f. Telnet do R2 ao R1 outra vez.

Você foi capaz de fazer login desta vez?

g. Entre no modo EXEC privilegiado e emita o comando **show run**.

Você consegue ler a senha secreta de enable? Explique.

Você pode ler as senhas do console, aux e vty? Explique.

Etapa 3: Criptografe as senhas em texto simples.

a. Use o comando **service password-encryption** para criptografar as senhas do console, aux e vty.

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

b. Execute o comando **show run**.

Você pode ler as senhas do console, aux e vty? Explique.

Em que nível (número) é o padrão enable senha secreta criptografada?

Em que nível (número) as outras senhas são criptografadas?

Qual nível de criptografia é mais difícil de quebrar. Explique.

Etapa 4: Configure uma mensagem de aviso a ser exibida antes do login.

a. Configurar um aviso para usuários não autorizados com um banner de mensagem do dia (MOTD) usando o comando **banner motd** . Quando um usuário conecta a um do Roteadores, a bandeira MOTD aparece antes da alerta de login. Neste exemplo, o sinal de dólar ($) é usado para iniciar e terminar a mensagem.

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Execute o comando **show run**.

O que o $ converte na saída?

c. Telnet para R1 de R2 novamente. Observe o banner MOTD.

d. Repita a parte da configuração das etapas anteriores no roteador R3.

Parte 3: Configure a segurança aprimorada de senha de nome de usuário nos roteadores R1 e R3

Etapa 1: Investigue as opções para o comando username.

No modo de configuração global, digite o seguinte comando:


```
R1(config)# username user01 algorithm-type ?
```

Que opções estão disponíveis?

Etapa 2: Crie uma nova conta de usuário com uma senha secreta.

a. Crie uma nova conta de usuário com hashing SCRYPT para criptografar a senha.

```
R1(config)# username user01 algorithm-type scrypt secret user01pass
```

b. Saia do modo de configuração global e salve sua configuração.

c. Exiba a configuração em execução.

Qual método de hashing é usado para a senha?

Etapa 3: Teste a nova conta fazendo login no console.

a. Defina a linha do console para usar as contas de login definidas localmente.

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#end
R1#exit
```

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

c. Faça login usando o **user01** nome de usuário definido anteriormente e a senha **user01pass**.

Qual é a diferença entre fazer login no console agora e anteriormente?

d. Depois de fazer login, emita o comando **show run**.

Conseguiram emitir o comando? Explique.

e. Entre no modo EXEC privilegiado usando o comando **enable**.

Foi solicitada uma senha? Explique.

Parte 4: Configurar o servidor SSH no Roteadores R1 e R3

Nesta parte, use o CLI para configurar o roteador a ser controlado com segurança usando o SSH em vez do telnet. O Shell Seguro (SSH) é um protocolo de rede que estabelece uma conexão segura de emulação de terminal para um roteador ou outro dispositivo de rede. O SSH criptografa todas as informações que passam no link de rede e fornece autenticação do computador remoto. O SSH está substituindo rapidamente o Telnet como ferramenta de login remoto favorita dos profissionais de rede.

Nota: Para que um roteador apoie SSH, deve ser configurado com autenticação local, (serviços AAA, ou nome de usuário) ou autenticação de senha. Nesta tarefa, você configura um nome de usuário SSH e uma autenticação local.

Etapa 1: Configure o nome de domínio.

Entre no modo de configuração global e defina o nome de domínio.

```
R1#conf t
R1(config)# ip domain-name netsec.com
```

Etapa 2: Configurar um usuário privilegiado para login do cliente SSH.

a. Use o comando **username** para criar o ID de usuário com o nível de privilégio mais alto possível e uma senha secreta.

```
R1(config)# username admin privilege 15 algorithm-type scrypt secret cisco12345
```

Nota: Os nomes de usuário não diferenciam maiúsculas e minúsculas por padrão

b. Saia para a tela inicial de login do roteador. Entre com o admin do nome de usuário e a senha associada.

Qual foi o prompt do roteador depois que você inseriu a senha?

Etapa 3: Configure as linhas vty de entrada.

Especifique um nível de privilégio **15** para que um usuário com o nível de privilégio mais alto (15) seja padrão para o modo EXEC privilegiado ao acessar as linhas vty. Outros usuários serão padrão para o modo EXEC do usuário. Use as contas de usuário local para login e validação obrigatórios e aceite apenas conexões SSH.

```
R1(config)#line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)# exit
```

Nota: O comando local do **login deve ter sido configurado em uma etapa anterior. Ele está incluído aqui para fornecer todos os comandos se você estiver fazendo isso pela primeira vez.**

Nota: Se você adiciona a palavra-chave **telnet** ao comando **transport input**, os usuários podem entrar usando o telnet assim como o SSH, contudo, o roteador será menos seguro. Se apenas o SSH for especificado, o host de conexão deve ter um cliente SSH instalado.

Etapa 4: Apague pares de chaves existentes no roteador.

```
R1(config)# crypto key zeroize rsa
```

Nota: Se nenhuma chave existe, você pôde receber esta mensagem:% `nenhumas chaves da assinatura RSA encontradas na configuração.`

Etapa 5: Gere o par de chaves de criptografia RSA para o roteador.

O roteador usa o par de chaves RSA para autenticação e criptografia de dados SSH transmitidos.

a. Configurar as chaves RSA com **1024** para o número de bits de módulo. O padrão é 512 e o intervalo é de 360 a 2048.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
O nome para as chaves será: R1.netsec.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

a. Emita o comando **ip ssh version 2** forçar o uso da versão 2 do SSH.

```
R1(config)# ip ssh version 2
R1(config)# exit
```

Nota: Os detalhes dos métodos de criptografia são abordados no módulo posterior.

Etapa 6: Verifique a configuração do SSH.

a. Use o comando **show ip ssh** ver os ajustes atuais.

```
R1# show ip ssh
```

b. Preencha as seguintes informações com base na saída do comando **show ip ssh** .

Versão SSH ativada:

Tempo limite de autenticação:

Novas tentativas de autenticação:

Etapa 7: Configurar timeouts SSH e parâmetros de autenticação.

a. Os timeouts SSH padrão e parâmetros de autenticação podem ser alterados para serem mais restritivos usando os seguintes comandos.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2
```

b. Use o comando **show ip ssh** ver os ajustes atuais.

c. Salve o running-config no startup-config.

```
R1# copy running-config startup-config
```

d. Repita a parte da configuração das etapas anteriores no roteador R3.

Etapa 8: Verifique a conectividade SSH com R1 do PC-A.

a. Do PC-A, SSH no roteador R1 usando o software de emulação terminal selecionando a opção SSH e fornecendo o endereço IP de Um ou Mais Servidores Cisco ICM NT do R1. Confirme que você confiará no host (R1) quando solicitado no alerta de segurança.

b. Digite o nome de usuário **admin** e a senha de administrador **cisco12345** quando solicitado.

c. No prompt de exec privilegiado R1, incorpore o comando **show users** .

```
R1# show users
```

Quais usuários estão conectados ao roteador R1 neste momento?

d. Feche a janela de sessão SSH.

e. Tente abrir uma sessão Telnet para o seu roteador a partir do PC-A. Conseguiram abrir a sessão do Telnet? Explique.

f. Abra uma sessão SSH da massa de vidraceiro ao roteador do PC-A. Digite o **user01** username and password **user01pass** na janela PuTTY para tentar conectar para um usuário que não tenha o nível de privilégio de 15.

Se você foi capaz de fazer login, qual foi o prompt?

g. Use o comando **enable** incorporar o modo do privilégio EXEC e incorpore a senha secreta da possibilidade **cisco12345**.

Reflexão

1. Explique a importância de proteger o acesso ao roteador e monitorar dispositivos de rede.

2. Quais vantagens o SSH tem em relação ao Telnet?

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)
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.