Laboratório - Configurar autenticação AAA local

Topologia

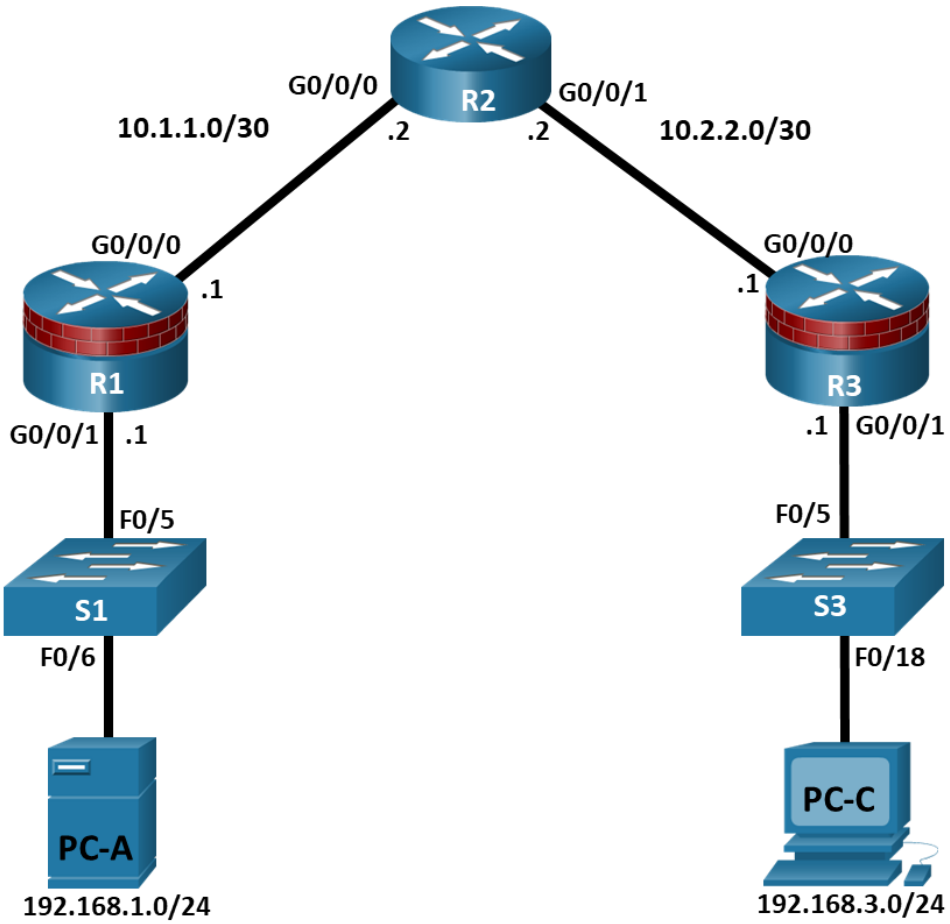

Tabela de endereçamento

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

- Defina as configurações básicas, como nome do host, endereços IP de interface e senhas de acesso.
- Configure o roteamento estático.

Parte 2: Configurar a autenticação local para o acesso do console

- Configurar um usuário de banco de dados local e acesso local para a linha de console.
- Teste a configuração.

Parte 3: Configurar a autenticação local para acesso remoto

- Configure o nome de domínio
- Configure a chave de criptografia
- Permita o SSH em vty

Parte 4: Configurar a autenticação local usando o AAA no R3

- Configurar o banco de dados de usuário local usando o Cisco IOS.
- Configurar a autenticação local AAA usando o Cisco IOS.
- Teste a configuração.

Parte 5: Observe a autenticação AAA usando o Cisco IOS debugar

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 um modo EXEC privilegiado habilitar senha secreta melhora ainda mais a segurança, mas ainda assim apenas uma senha básica é necessária para cada modo de acesso.

Além das senhas básicas, nomes de usuário específicos ou contas com níveis de privilégio variados podem ser definidos no banco de dados do roteador local que pode se aplicar ao roteador como um todo. Quando o console, vty, ou linhas auxiliares são configuradas para se referir a este base de dados local, o usuário é alertado para um nome de usuário e uma senha ao usar qualquer uma dessas linhas para acessar o roteador.

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. 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 usará então comandos CLI configurar o Roteadores com autenticação local básica por meio do AAA.

Nota: Os roteadores usados com laboratórios hands-on são Cisco 4221 com a versão 16.9.6 do Cisco Ios Xe (Universife9). 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 (SO Windows com um programa de emulação de terminal, como Tera Term ou PuTTy 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 do laboratório, você configura a topologia da rede e define as configurações básicas, como os endereços IP da interface, roteamento estático, acesso ao dispositivo e senhas.

Todas as etapas devem ser executadas no Roteadores R1 e R3. Somente as etapas 1, 2, 3 e 6 precisam ser executadas no R2. O procedimento para R1 é mostrado aqui como exemplo.

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: Defina as configurações básicas de cada Roteador.

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

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

c. Para evitar que o roteador tente traduzir comandos inseridos incorretamente como se fossem nomes de host, desative a pesquisa de DNS.

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

Etapa 3: Configure o roteamento estático nos roteadores.

a. Configurar uma rota padrão estática do R1 ao R2 e do R3 ao R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

b. Configurar uma rota estática do R2 à LAN R1 e do R2 à LAN R3.

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

Etapa 4: 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 5: Verifique a conectividade entre PC-A e R3.

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. Execute ping de PC-A na LAN R1 para 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 puder executar ping de PC-A para PC-C, você demonstrou que o roteamento estático está configurado e funcionando corretamente. Se você não puder fazer ping, mas as interfaces do dispositivo estiverem ativas e os endereços IP estiverem corretos, use os comandos **show run** e **show ip route** para ajudar a identificar problemas relacionados ao protocolo de roteamento.

Etapa 6: Salve a configuração básica de execução de cada roteador.

Etapa 7: Configure e criptografe senhas em R1 e R3.

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.

Para esta etapa, defina as mesmas configurações para R1 e R3. O roteador R1 é mostrado aqui como um exemplo.

a. Configure um comprimento mínimo de senha.

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

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

b. Configure uma senha para o modo EXEC privilegiado em ambos os roteadores. Use o algoritmo de hash tipo 8 (PDKDF2).

```
R1(config)# enable algorithm-type sha256 secret cisco12345
```

Etapa 8: Configurar o console básico, a porta auxiliar e as linhas vty.

a. Configure uma senha de console e habilite o login para o roteador R1. 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 inícios de sessão repetitivos durante este laboratório, o timeout do exec pode ser ajustado a 0, que o impede de expirar. No entanto, isso não é considerado uma boa prática de segurança.

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

b. Configurar uma senha para a porta auxiliar 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
```


c. Configure 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)# login
```

d. Criptografe as senhas do console, aux e vty.

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

e. Entre com o comando **show run | section line** .

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

Não. As senhas agora estão criptografadas

Etapa 9: Configurar um banner de aviso de login nos roteadores R1 e R3.

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

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

b. Saia do modo EXEC privilegiado usando o comando **disable** ou **exit** e pressione **Enter** para começar.

Se o banner não aparecer corretamente, recrie-o usando o comando **banner motd** .

Etapa 10: Salve as configurações básicas em todos os roteadores.

Salve a configuração em execução na configuração de inicialização a partir do prompt EXEC privilegiado.

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

Parte 2: Configurar a autenticação local para o acesso ao console

Nesta parte do laboratório, você configura um nome de usuário e uma senha locais e altera o acesso para as linhas do console, aux, e vty para referenciar o banco de dados local do roteador para nomes de usuário e senhas válidos. Execute todas as etapas no R1 e no R3. O procedimento para o R1 é mostrado aqui.

Etapa 1: Configure o banco de dados do usuário local.

a. Crie uma conta de usuário local usando o algoritmo de hash tipo 8 (PDKDF2) para criptografar a senha.

```
R1(config)# username user01 algorithm-type sha256 secret user01pass
```

b. Saia do modo de configuração global e exiba a configuração em execução.

Você pode ler a senha do usuário?

Etapa 2: Configurar a autenticação local para a linha de console e o início de uma sessão.

a. Defina a linha do console para usar os nomes de usuário e senhas de login definidos localmente.

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


b. Saia para a tela inicial do roteador que exibe:

```
R1 con0 está agora disponível.

Press RETURN to get started. (con0 de R1 agora está disponível. Pressione
RETURN para começar.)
```

c. Faça login usando a conta **user01** e a senha previamente definidas.

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

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

Você conseguiu emitir o comando? Explique.

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

Foi solicitada uma senha? Explique.

Parte 3: Configurar a autenticação local para acesso remoto

Nesta parte, você usará SSH para acesso remoto ao R1 usando o banco de dados de usuário local.

Etapa 1: Configure um nome de domínio para o dispositivo.

Etapa 2: Configure o método de chave de criptografia.

Etapa 3: Habilite o SSH nas linhas vty.

a. Ative o SSH nas linhas vty de entrada usando o comando **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

b. Altere o método de login para usar o banco de dados local para a verificação de usuário.

c. Do PC-A, estabeleça uma sessão SSH com R1.

Você foi solicitado para uma conta de usuário? Explique.

d. Quando conectado ao R1 via SSH, acesse o modo EXEC privilegiado com o comando **enable**.

Que senha você usou?

e. Para maior segurança, defina a porta auxiliar para usar as contas de login definidas localmente.

```
R1(config)# line aux 0
R1(config-line)#login local
```

Etapa 4: Salve a configuração em R1.

Salve a configuração em execução na configuração de inicialização a partir do prompt EXEC privilegiado.

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

Etapa 5: Execute etapas 1 a 4 no R3 e salve a configuração.

Parte 4: Configurar a autenticação local usando o AAA no R3

Etapa 1: Configure o banco de dados do usuário local.

a. Crie uma conta de usuário local com hashing PDKDF2 para criptografar a senha.

```
R3(config)# username Admin01 privilege 15 algorithm-type sha256 secret Admin01pass
```

b. Saia do modo de configuração global e exiba a configuração em execução.

Você pode ler a senha do usuário?

Etapa 2: Permita serviços AAA.

No R3, permita serviços com o comando global configuration **aaa new-model**. Porque você está implementando a autenticação local, use a autenticação local como o primeiro método e nenhuma autenticação como o método secundário.

Se você estava usando um método de autenticação com um server remoto, tal como TACACS+ ou RADIUS, você configuraria um método de autenticação secundário para o fallback se o server é inalcançável. Normalmente, o método secundário é o banco de dados local. Neste caso, se nenhum nome de usuário estiver configurado no banco de dados local, o roteador permite que todos os usuários acessem o dispositivo.

```
R3(config)# aaa new-model
```

Etapa 3: Implemente serviços AAA para o acesso de console usando o base de dados local.

a. Crie a lista de autenticação de login padrão emitindo o comando **aaa authentication login default** *method1[method2] [method3]* com uma lista de métodos usando as palavras-chave **local** e **none**.

```
R3(config)# aaa authentication login default local-case none
```

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

Nota: O parâmetro **local-case** é usado para tornar os nomes de usuário com distinção entre maiúsculas e minúsculas.

b. Saia para a tela inicial do roteador que exibe:

```
R3 con0 já está disponível
```



```
Press RETURN to get started. (con0 de R1 agora está disponível. Pressione
RETURN para começar.)
```

Entre ao console como **Admin01** com uma senha de **admin01Pass**. Lembre-se de que nomes de usuário e senhas são ambos diferenciam maiúsculas e minúsculas agora.

Você conseguiu fazer logon? Explique.

Nota: Se sua sessão com a porta de console do roteador cronometra para fora, você pôde ter que entrar usando a lista de autenticação padrão.

c. Saia para a tela inicial do roteador que exibe:

d. Tente fazer login no console como **baduser** com qualquer senha.

Você conseguiu fazer logon? Explique.

Se nenhuma conta de usuário estiver configurada no banco de dados local, quais usuários têm permissão para acessar o dispositivo?

Etapa 4: Crie um perfil de autenticação AAA para o SSH usando o base de dados local.

a. Crie uma lista de autenticação exclusiva para o acesso SSH ao roteador. Isso não tem o fallback de nenhuma autenticação, portanto, se não houver nomes de usuário no banco de dados local, o acesso SSH está desabilitado. Para criar um perfil de autenticação que não seja o padrão, especifique um nome de lista de SSH_LINES e aplique-o às linhas vty.

```
R3(config)# aaa authentication login SSH_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication SSH_LINES
```

b. Verifique que este perfil de autenticação está usado abrindo uma sessão SSH do PC-C ao R3. Faça login como **Admin01** com uma senha de **admin01Pass**.

Você conseguiu fazer o login? Explique.

c. Saia da sessão SSH.

d. Tente fazer login como **baduser** com qualquer senha.

Você conseguiu fazer o login? Explique.

Parte 5: Observe a autenticação AAA usando o Cisco IOS debugar

Nesta parte, você usa o comando **debug** observar tentativas de autenticação bem-sucedidas e mal sucedidas.

Etapa 1: Verifique que o pulso de disparo do sistema e debuga carimbos de hora estão configurados corretamente.

a. Do usuário R3 ou do prompt privilegiado do modo EXEC, use o comando **show clock** determinar qual é a hora atual para o roteador. Se a hora e a data estiverem incorretas, defina a hora do modo de EXEC privilegiado com o comando **clock set HH: MM:SS DD month YYYY.** Um exemplo é fornecido aqui para R3.

```
R3# clock set 14:15:00 03 February 2021
```

b. Verifique se a informação detalhada do time-stamp está disponível para sua saída de depuração usando o comando **show run**. Este comando exibe todas as linhas na configuração em execução que incluem o texto “carimbos de data/hora”.

```
R3# show run | include timestamps
service timestamps debug datetime msec
service timestamps log datetime msec
```

c. Se o comando **service timestamps debug** não está presente, incorpore-o no modo de configuração global.

```
R3(config)# service timestamps debug datetime msec
R3(config)# exit
```

d. Salve a configuração em execução na configuração de inicialização a partir do prompt EXEC privilegiado.

```
R3# copy running-config startup-config
```

Etapa 2: Use debugar para verificar o acesso do usuário.

a. Ative a depuração para autenticação AAA.

```
R3# debug aaa authentication
AAA Authentication debugging is on
```

b. Inicie uma sessão SSH do R2 ao R3. Faça login com nome de usuário **Admin01** e senha **admin01Pass**.

```
R2# ssh -l Admin01 10.2.2.1
```

c. Navegue para trás R3. Observe os eventos de autenticação AAA na janela de sessão do console. Mensagens de depuração semelhantes às seguintes devem ser exibidas.

```
R3#
Feb 3 14:15:57.653: AAA/BIND(00000FB5): Bind i/f
Feb 3 14:15:57.653: AAA/AUTHEN/LOGIN (00000FB5): Pick method list 'SSH_LINES'
R3#
Feb 3 14:16:01.966: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source: 10.2.2.2] [localport: 22] at 14:16:01 UTC Wed Feb 3 2021
```

d. Na janela SSH em R2, entre no modo EXEC privilegiado. Use a senha secreta da possibilidade de **cisco12345**. Mensagens de depuração semelhantes às seguintes devem ser exibidas. Na terceira entrada, observe o nome de usuário (Admin01), o número de porta virtual (tty866), e o endereço de cliente SSH remoto (10.2.2.2). Observe também que a última entrada de status é “PASS”.

```
Feb 3 14:19:51.146: AAA: parse name=tty866 idb type=-1 tty=-1
Feb 3 14:19:51.146: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=866 channel=0
Feb 3 14:19:51.146: AAA/MEMORY: create_user (0x7FD084CE0FF0) user='Admin01' ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
```



```
Feb 3 14:19:51.146: AAA/AUTHEN/START (402765494): port='tty866' list='' action=LOGIN
service=ENABLE
Feb 3 14:19:51.146: AAA/AUTHEN/START (402765494): non-console enable - default to
enable password
Feb 3 14:19:51.147: AAA/AUTHEN/START (402765494): Method=ENABLE
R3#
Feb 3 14:19:51.147: AAA/AUTHEN (402765494): status = GETPASS
R3#
Feb 3 14:19:54.156: AAA/AUTHEN/CONT (402765494): continue_login (user='(undef)')
Feb 3 14:19:54.156: AAA/AUTHEN (402765494): status = GETPASS
Feb 3 14:19:54.156: AAA/AUTHEN/CONT (402765494): Method=ENABLE
Feb 3 14:19:54.259: AAA/AUTHEN (402765494): status = PASS
Feb 3 14:19:54.259: AAA/MEMORY: free_user (0x7FD084CE0FF0) user='NULL' ruser='NULL'
port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
```

e. Da janela SSH, saia do modo EXEC privilegiado usando o comando **disable**. Tente entrar no modo EXEC privilegiado novamente, mas use uma senha incorreta desta vez. Observe a saída de depuração no R3, observando que o status é “FAIL” desta vez.

```
Feb 3 14:24:20.274: AAA: parse name=tty866 idb type=-1 tty=-1
Feb 3 14:24:20.274: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=866 channel=0
Feb 3 14:24:20.274: AAA/MEMORY: create_user (0x7FD08991D130) user='Admin01'
ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE
priv=15 initial_task_id='0', vrf= (id=0)
Feb 3 14:24:20.274: AAA/AUTHEN/START (1943266075): port='tty866' list='' action=LOGIN
service=ENABLE
Feb 3 14:24:20.274: AAA/AUTHEN/START (1943266075): non-console enable - default to
enable password
Feb 3 14:24:20.274: AAA/AUTHEN/START (1943266075): Method=ENABLE
R3#
Feb 3 14:24:20.275: AAA/AUTHEN (1943266075): status = GETPASS
R3#
Feb 3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): continue_login (user='(undef)')
Feb 3 14:24:22.276: AAA/AUTHEN (1943266075): status = GETPASS
Feb 3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): Method=ENABLE
Feb 3 14:24:22.379: AAA/AUTHEN(1943266075): password incorrect
Feb 3 14:24:22.379: AAA/AUTHEN (1943266075): status = FAIL
Feb 3 14:24:22.379: AAA/MEMORY: free_user (0x7FD08991D130) user='NULL' ruser='NULL'
port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
R3#
```

f. Saia da sessão SSH ao roteador R3. Em seguida, tente abrir uma sessão SSH ao roteador novamente, mas desta vez tente entrar com o nome de usuário **Admin01** e uma senha ruim. Na janela do console, a saída de depuração deve ser semelhante ao seguinte.

```
Feb 3 14:26:40.960: AAA/BIND(00000FB9): Bind i/f
Feb 3 14:26:40.960: AAA/AUTHEN/LOGIN (00000FB9): Pick method list 'SSH_LINES'
```

Qual mensagem foi exibida na tela do cliente SSH?

g. Desative toda a depuração usando o comando **undebug all** no prompt EXEC privilegiado.

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)
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.