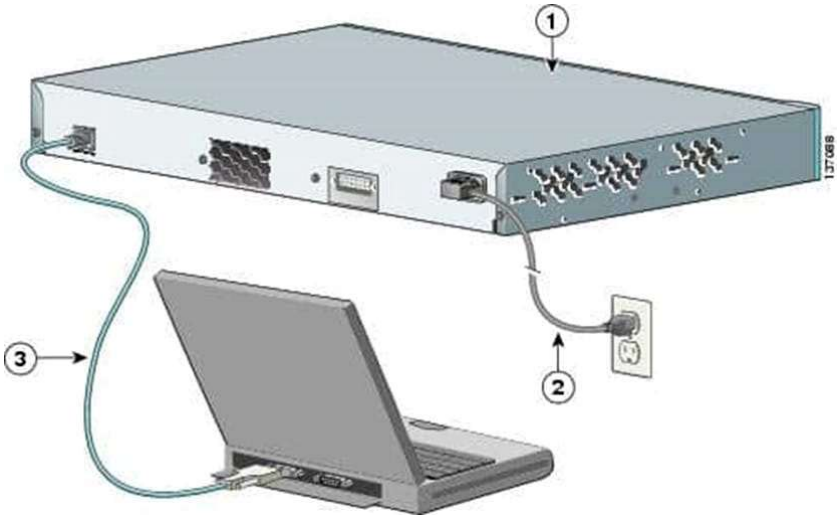

1
2
3
137068


www.labcisco.com.br
AUX
CONN
CONSOLE
Porta de Console RJ-45 (Cabo Serial)
Porta de Console Mini-USB B

Métodos de Acesso

Um switch encaminhará o tráfego por padrão e não precisa ser explicitamente configurado para operar. Por exemplo, dois hosts configurados conectados ao mesmo novo switch seriam capazes de se comunicar.

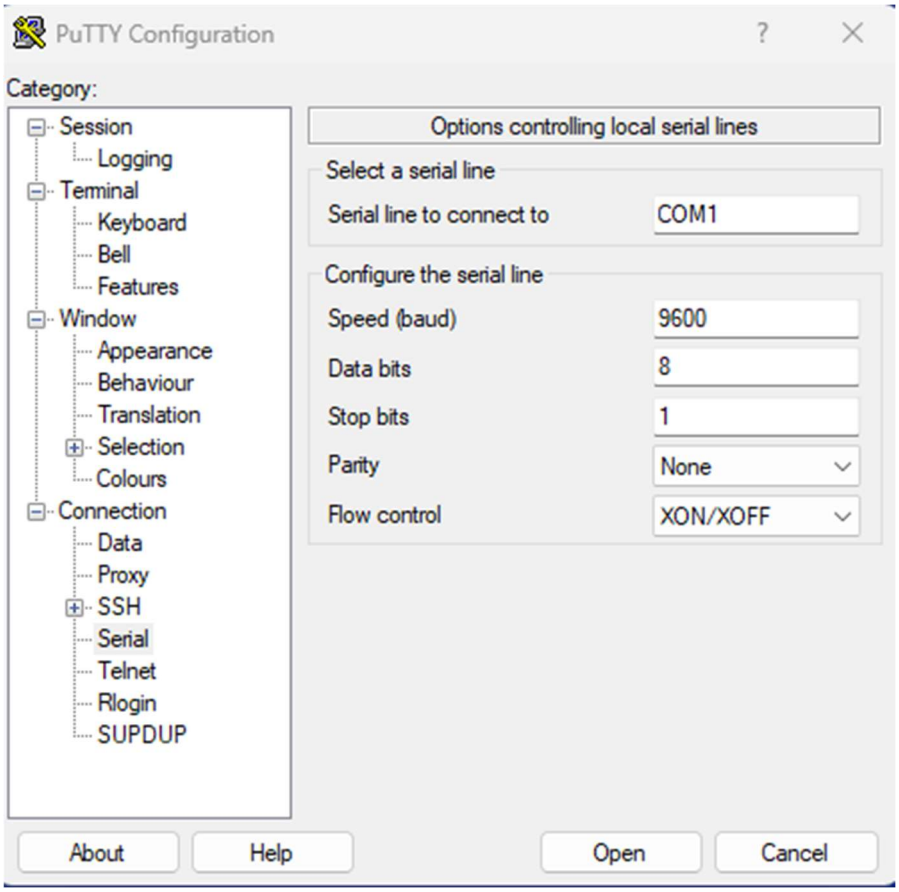
Já um roteador precisa ser configurado para poder iniciar o seu correto funcionamento.

Independentemente do comportamento padrão de um novo switch ou de um roteador, todos os switches e roteadores devem ser configurados e protegidos.

Legenda da tabela	
Método	**Descrição**
Console	Esta é uma porta de gerenciamento físico que fornece acesso fora de banda a um dispositivo Cisco. O acesso out-of-band refere-se ao acesso por meio de um canal dedicado de gerenciamento que é utilizado somente para fins de manutenção do dispositivo. A vantagem de usar uma porta do console é que o dispositivo está acessível mesmo que nenhum serviço de rede esteja configurado, como a configuração inicial. Um computador executando um software de emulação de terminal e um cabo de console especial para se conectar ao dispositivo são necessários para uma conexão de console.
Secure Shell (SSH)	O SSH é um método dentro da banda e recomendado para estabelecer remotamente uma conexão CLI segura, através de uma interface virtual, através de uma rede. Ao contrário de uma conexão de console, as conexões SSH requerem serviços de rede ativos no dispositivo, incluindo uma interface ativa configurada com um endereço. A maioria das versões do Cisco IOS inclui um servidor SSH e um cliente SSH que podem ser usados para estabelecer sessões de SSH com outros dispositivos.
Telnet	O Telnet é um método inseguro em banda para estabelecer remotamente uma sessão de CLI, por meio de uma interface virtual, por uma rede. Ao contrário do SSH, o Telnet não fornece uma conexão segura e criptografada e só deve ser usado em um ambiente de laboratório. A autenticação de usuário, as senhas e os comandos são enviados pela rede como texto simples. A melhor prática é usar SSH em vez de Telnet. O Cisco IOS inclui um servidor Telnet e um cliente Telnet.

Note: Alguns dispositivos, como roteadores, também podem suportar uma porta auxiliar herdada usada para estabelecer uma sessão CLI remotamente por uma conexão telefônica usando um modem. De modo semelhante a uma conexão de console, a porta AUX é do tipo fora de banda e não requer serviços de rede para ser configurada ou estar disponível.

Existem vários programas de emulação de terminal que você pode usar para conectar-se a um dispositivo de rede por uma conexão serial por uma porta do console ou por uma conexão SSH / Telnet. Esses programas permitem que você aumente sua produtividade ajustando tamanhos de janela, alterando tamanhos de fontes e alterando esquemas de cores.



Como recurso de segurança, o software Cisco IOS separa o acesso de gerenciamento nestes dois modos de comando:

- **Modo EXEC de usuário** - Este modo possui recursos limitados, mas é útil para operações básicas. Ele permite apenas um número limitado de comandos de monitoramento básicos, mas não permite a execução de nenhum comando que possa alterar a configuração do dispositivo. O modo EXEC usuário é identificado pelo prompt da CLI que termina com o símbolo >.
- **Modo EXEC privilegiado** - Para executar comandos de configuração, um administrador de rede deve acessar o modo EXEC privilegiado. Modos de configuração mais altos, como o modo de configuração global, só podem ser acessados do modo EXEC privilegiado. O modo EXEC privilegiado pode ser identificado pelo prompt que termina com o # símbolo.

A tabela resume os dois modos e exibe os prompts da CLI padrão de um switch e roteador Cisco.

Legenda da tabela		
Modo de Comando	**Descrição**	**Aviso padrão do dispositivo**
Modo Exec usuário	• O modo permite acesso a apenas um número limitado de comandos de monitoramento básico. • É geralmente chamado de modo "view-only".	Switch> Router>
Modo EXEC privilegiado	• O modo permite acesso a todos os comandos e recursos. • O usuário pode usar qualquer comando de monitoramento e executar a configuração e comandos de gerenciamento.	Switch# Router#

Para configurar o dispositivo, o usuário deve entrar no modo de configuração global, geralmente chamado de modo de configuração global.

No modo de config global, são feitas alterações na configuração via CLI que afetam o funcionamento do dispositivo como um todo. O modo de configuração global é identificado por um prompt que termina com (config)#após após o nome do dispositivo, como **Switch(config)#**.

Esse modo é acessado antes de outros modos de configuração específicos. No modo de configuração global, o usuário pode inserir diferentes modos de subconfiguração. Cada um desses modos permite a configuração de uma parte particular ou função do dispositivo IOS. Dois modos comuns de subconfiguração incluem:

- **Modo de configuração de linha -** Usado para configurar o acesso ao console, SSH, Telnet ou AUX.
- **Modo de configuração da interface -** Usado para configurar uma porta de switch ou interface de rede do roteador.

Quando a CLI é usada, o modo é identificado pelo prompt da linha de comandos exclusivo para esse modo. Por padrão, todo prompt começa com após após o nome do dispositivo. Após o nome, o restante do prompt indica o modo. Por exemplo, o prompt

padrão para o modo de configuração de linha é **Switch(config-line)#** e o prompt padrão para o modo de configuração da interface é **Switch(config-if)#**.

Vários comandos são usados para entrar e sair dos prompts de comando. Para passar do modo EXEC do usuário para o modo EXEC privilegiado, use o comando **enable** Use o comando **disable** do modo EXEC privilegiado para retornar ao modo EXEC do usuário.

Observação: O modo EXEC privilegiado às vezes é chamado de *enable mode*.

Para entrar e sair do modo de configuração global, use o comando **configure terminal** privilegiado do modo EXEC. Para retornar ao modo EXEC privilegiado, digite o comando **exit** global config mode.

Existem muitos modos diferentes de subconfiguração. Por exemplo, para entrar no modo de subconfiguração de linha, use o comando **line** seguido pelo tipo e número da linha de gerenciamento que deseja acessar. Use o comando **exit** para sair de um modo de subconfiguração e retornar ao modo de configuração global.

```
Switch(config)# line console 0
Switch(config-line)# exit
Switch(config)#
```

Para mover de qualquer modo de subconfiguração do modo de configuração global para o modo um passo acima na hierarquia de modos, digite o comando **exit**

Para passar de qualquer modo de subconfiguração para o modo EXEC privilegiado, insira o comando **end** ou a combinação de teclas **Ctrl+Z**.

```
Switch(config-line)# end
Switch#
```

Pode mover diretamente de um modo de subconfiguração para outro. Observe como depois de selecionar uma interface, o prompt de comando muda de **(config-line)#** para **(config-if)#**.

```
Switch(config-line)# interface FastEthernet 0/1
Switch(config-if)#
```

Quando uma saída de comando produz mais texto do que pode ser exibido em uma janela de terminal, o IOS exibirá um **“--More--”** prompt. A tabela a seguir descreve os pressionamentos de teclas que podem ser usados quando esse prompt é exibido.

Legenda da tabela	
Toque de tecla	**Descrição**
Tecla **Enter**	Exibe a próxima linha.
Barra de **espaço**	Exibe a próxima tela.
Qualquer outra chave	Encerra a sequência de exibição, retornando ao modo EXEC privilegiado.

Esta tabela lista os comandos usados para sair de uma operação.

Legenda da tabela	
Toque de tecla	**Descrição**
Ctrl-C	Quando em qualquer modo de configuração, finaliza o modo de configuração e retorna para o modo EXEC privilegiado. Quando no modo de instalação, aborta de volta ao comando pronto.
Ctrl-Z	Quando em qualquer modo de configuração, finalização ou modo de configuração e retornos para o modo EXEC privilegiado.
Ctrl-Shift-6	Sequência de quebra para todas as finalidades usada para abortar pesquisas de DNS, tracerouts, pings e outros comandos.

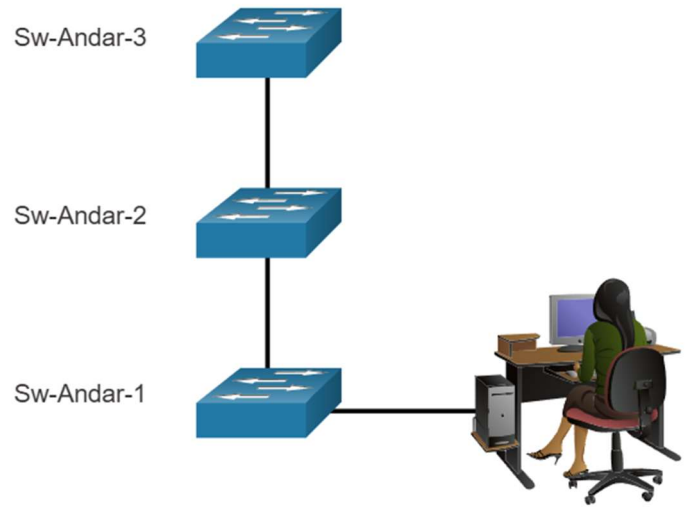
O primeiro comando de configuração em qualquer dispositivo deve ser dar a ele um nome de dispositivo exclusivo ou nome de host. Por padrão, todos os dispositivos recebem um nome padrão de fábrica. Por exemplo, um switch Cisco IOS é “Switch“.

O problema é que, se todos os comutadores em uma rede forem deixados com seus nomes padrão, seria difícil identificar um dispositivo específico. Por exemplo, como você saberia que está conectado ao dispositivo certo ao acessá-lo remotamente usando SSH? O nome do host fornece a confirmação de que você está conectado ao dispositivo correto.

O nome padrão deve ser alterado para algo mais descritivo. Com uma escolha sábia de nomes, é mais fácil lembrar, documentar e identificar dispositivos de rede. Aqui estão algumas diretrizes de nomenclatura importantes para hosts:

- Começar com uma letra;
- Não conter espaços;
- Terminar com uma letra ou dígito;
- Usar somente letras, números e traços;
- Ter menos de 64 caracteres.

Uma organização deve escolher uma convenção de nomenclatura que torne fácil e intuitivo identificar um dispositivo específico. Os nomes de host usados no IOS do dispositivo preservam os caracteres em maiúsculas e minúsculas. Por exemplo, a figura mostra que três comutadores, abrangendo três andares diferentes, estão interconectados em uma rede. A convenção de nomenclatura usada incorporou o local e a finalidade de cada dispositivo. A documentação de rede deve explicar como esses nomes foram escolhidos, de modo que outros dispositivos possam receber nomes apropriados.



Quando a convenção de nomenclatura for identificada, a próxima etapa é usar a CLI para aplicar os nomes aos dispositivos. Como mostrado no exemplo, no modo EXEC privilegiado, acesse o modo de configuração global digitando o comando **configure terminal** Observe a alteração no prompt de comando.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

No modo de configuração global, digite o comando **hostname** seguido pelo nome do comutador e pressione **Enter**. Observe a alteração no nome do prompt de comando.

Observação: Para retornar o switch ao prompt padrão, use o comando **no hostname** global config.

O uso de senhas fracas ou facilmente adivinhadas continua a ser a maior preocupação de segurança das organizações. Os dispositivos de rede, inclusive roteadores residenciais sem fio, sempre devem ter senhas configuradas para limitar o acesso administrativo.

O Cisco IOS pode ser configurado para usar senhas do modo hierárquico para permitir privilégios de acesso diferentes a um dispositivo de rede.

Todos os dispositivos de rede devem limitar o acesso administrativo protegendo EXEC privilegiado, EXEC de usuário e acesso remoto Telnet com senhas. Além disso, todas as senhas devem ser criptografadas e notificações legais fornecidas.

Ao escolher senhas, use senhas fortes que não sejam facilmente adivinhadas. Existem alguns pontos-chave a serem considerados ao escolher senhas:

- Use senhas com mais de oito caracteres.
- Use uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais e/ou sequências numéricas.
- Evite usar a mesma senha para todos os dispositivos.
- Não use palavras comuns porque elas são facilmente adivinhadas.

Use uma pesquisa na Internet para encontrar um gerador de senhas. Muitos permitirão que você defina o comprimento, conjunto de caracteres e outros parâmetros.

Observação: A maioria dos laboratórios deste curso usa senhas simples, como a maioria dos laboratórios deste curso usa senhas simples, como **classe** ou **cisco**. Essas senhas são consideradas fracas e facilmente adivinháveis e devem ser evitadas nos ambientes de produção. Usamos essas senhas apenas por conveniência em uma sala de aula ou para ilustrar exemplos de configuração.

Quando você se conecta inicialmente a um dispositivo, você está no modo EXEC do usuário. Este modo é protegido usando o console.

Para proteger o acesso ao modo EXEC do usuário, insira o modo de configuração do console de linha usando o comando de configuração global **line console 0**, conforme mostrado no exemplo. O zero é usado para representar a primeira interface de console (e a única, na maioria dos casos). Em seguida, especifique a senha do modo EXEC do

usuário usando o comando **password***password*. Por fim, ative o acesso EXEC do usuário usando o comando **login**

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

O acesso ao console agora exigirá uma senha antes de permitir o acesso ao modo EXEC do usuário.

Para ter acesso de administrador a todos os comandos do IOS, incluindo a configuração de um dispositivo, você deve obter acesso privilegiado no modo EXEC. É o método de acesso mais importante porque fornece acesso completo ao dispositivo.

Para proteger o acesso EXEC privilegiado, use o comando de configuração **enable secret** *password* global config, conforme mostrado no exemplo.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

As linhas de terminal virtual (VTY) permitem acesso remoto usando Telnet ou SSH ao dispositivo. Muitos switches Cisco são compatíveis com até 16 linhas VTY numeradas de 0 a 15.

Para proteger linhas VTY, entre no modo VTY de linha usando o comando de configuraão global **line vty 0 15**. Em seguida, especifique a senha do VTY usando o comando **password** *password*. Por fim, ative o acesso VTY usando o comando **login**

Um exemplo de segurança das linhas VTY em um switch é mostrado.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# 1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Os arquivos startup-config e running-config exibem a maioria das senhas em texto simples. Esta é uma ameaça à segurança, porque qualquer pessoa pode descobrir as senhas se tiver acesso a esses arquivos.

Para criptografar todas as senhas de texto simples, use o comando de configurção global **service password-encryption** conforme mostrado no exemplo.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

O comando aplica criptografia fraca a todas as senhas não criptografadas. Essa criptografia se aplica apenas às senhas no arquivo de configuração, não às senhas como são enviadas pela rede. O propósito deste comando é proibir que indivíduos não autorizados vejam as senhas no arquivo de configuração.

Use o comando **show running-config** para verificar se as senhas agora estão criptografadas.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
  password 7 094F471A1A0A
  login
line vty 5 15
  password 7 094F471A1A0A
  login
!
!
end
```

Embora a exigência de senhas seja uma maneira de manter pessoal não autorizado fora da rede, é vital fornecer um método para declarar que apenas pessoal autorizado deve tentar acessar o dispositivo. Para fazê-lo, adicione um banner à saída do dispositivo. Banners podem ser uma parte importante do processo legal caso alguém seja processado por invadir um dispositivo. Alguns sistemas legais não permitem processo, ou mesmo o monitoramento de usuários, a menos que haja uma notificação visível.

Para criar uma mensagem de faixa do dia em um dispositivo de rede, use o comando de configuração global **banner motd #***a mensagem do dia***#**. O “#” na sintaxe do comando é denominado caractere de delimitação. Ele é inserido antes e depois da mensagem. O

caractere de delimitação pode ser qualquer caractere contanto que ele não ocorra na mensagem. Por esse motivo, símbolos como “#” são usados com frequência. Após a execução do comando, o banner será exibido em todas as tentativas seguintes de acessar o dispositivo até o banner ser removido.

O exemplo a seguir mostra as etapas para configurar o banner no Sw-Floor-1.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #a mensagem do dia#
```

Agora você sabe como executar a configuração básica em um switch, incluindo senhas e mensagens de banner. Este tópico mostrará como salvar suas configurações.

Há dois arquivos de sistema que armazenam a configuração do dispositivo:

- **startup-config** - Este é o arquivo de configuração salvo armazenado na NVRAM. Ele contém todos os comandos que serão usados pelo dispositivo na inicialização ou reinicialização. O flash não perde seu conteúdo quando o dispositivo está desligado.
- **running-config** - Isto é armazenado na memória de acesso aleatório (RAM). Ele reflete a configuração atual. A modificação de uma configuração ativa afeta o funcionamento de um dispositivo Cisco imediatamente. A RAM é uma memória volátil. Ela perde todo o seu conteúdo quando o dispositivo é desligado ou reiniciado.

O comando **show running-config** do modo EXEC privilegiado é usado para visualizar a configuração em execução. Como mostrado no exemplo, o comando irá listar a configuração completa atualmente armazenada na RAM.

```
Sw-Floor-1# show running-config
Building configuration...
Current configuration : 1351 bytes
!
! Last configuration change at 00:01:20 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Sw-Floor-1
!
(output omitted)
```

Para visualizar o arquivo de configuração de inicialização, use o comando EXEC privilegiado **show startup-config**.

Se a energia do dispositivo for perdida ou se o dispositivo for reiniciado, todas as alterações na configuração serão perdidas, a menos que tenham sido salvas. Para salvar as alterações feitas na configuração em execução no arquivo de configuração de inicialização, use o comando do modo EXEC privilegiado **copy running-config startup-config**.

Se as alterações feitas na configuração em execução não tiverem o efeito desejado e a configuração ainda não foi salva, você poderá restaurar o dispositivo para a configuração anterior. Remova os comandos alterados individualmente ou recarregue o dispositivo usando o comando de modo EXEC privilegiado **reload** para restaurar o startup-config.

A desvantagem de usar o comando **reload** para remover uma configuração em execução não salva é o breve período de tempo em que o dispositivo ficará offline, causando o tempo de inatividade da rede.

Quando um recarregamento é iniciado, o IOS detecta que a configuração em execução possui alterações que não foram salvas na configuração de inicialização. Um prompt será exibido para pedir que as alterações sejam salvas. Para descartar as alterações, insira **n** ou **no**.

Como alternativa, se alterações indesejadas foram salvas na configuração de inicialização, pode ser necessário limpar todas as configurações. Isso requer apagar a configuração de inicialização e reiniciar o dispositivo. A configuração de inicialização é removida usando o comando do modo EXEC privilegiado **erase startup-config**. Após o uso do comando, o switch solicitará confirmação. Pressione **Enter** para aceitar.

Após remover a configuração de inicialização da NVRAM, recarregue o dispositivo para remover o arquivo de configuração atual em execução da RAM. Ao recarregar, um switch carregará a configuração de inicialização padrão que foi fornecida originalmente com o dispositivo.

Para acessar o switch remotamente, um endereço IP e uma máscara de sub-rede devem ser configurados na SVI. Para configurar um SVI em um switch, use o comando **interface vlan 1** de configuração global. Vlan 1 não é uma interface física real, mas virtual. Em seguida, atribua um endereço IPv4 usando o comando **ip address** *ip-address subnet-mask* interface configuration. Por fim, ative a interface virtual usando o comando **no shutdown** de configuração da interface.

Após a configuração desses comandos, o switch terá todos os elementos IPv4 prontos para comunicação pela rede.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

A tarefa para configurar uma interface de roteador é muito semelhante a um SVI de gerenciamento em um switch. Especificamente, ele inclui a emissão dos seguintes comandos:

```
R1> enable
R1# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Proteger a infraestrutura de rede

A proteção da infraestrutura de rede é fundamental para a segurança geral da rede. A infraestrutura de rede inclui roteadores, switches, servidores, endpoints e outros dispositivos.

Considere um funcionário descontente olhando casualmente sobre o ombro de um administrador de rede enquanto o administrador estiver fazendo login em um roteador de borda. É uma maneira surpreendentemente fácil de um atacante obter acesso não autorizado.

Se um invasor obtém acesso a um roteador, a segurança e o gerenciamento de toda a rede podem ser comprometidos. Por exemplo, um invasor pode apagar a configuração de inicialização e fazer o roteador recarregar em cinco minutos. Quando o roteador reinicializa, ele não terá uma configuração de inicialização.

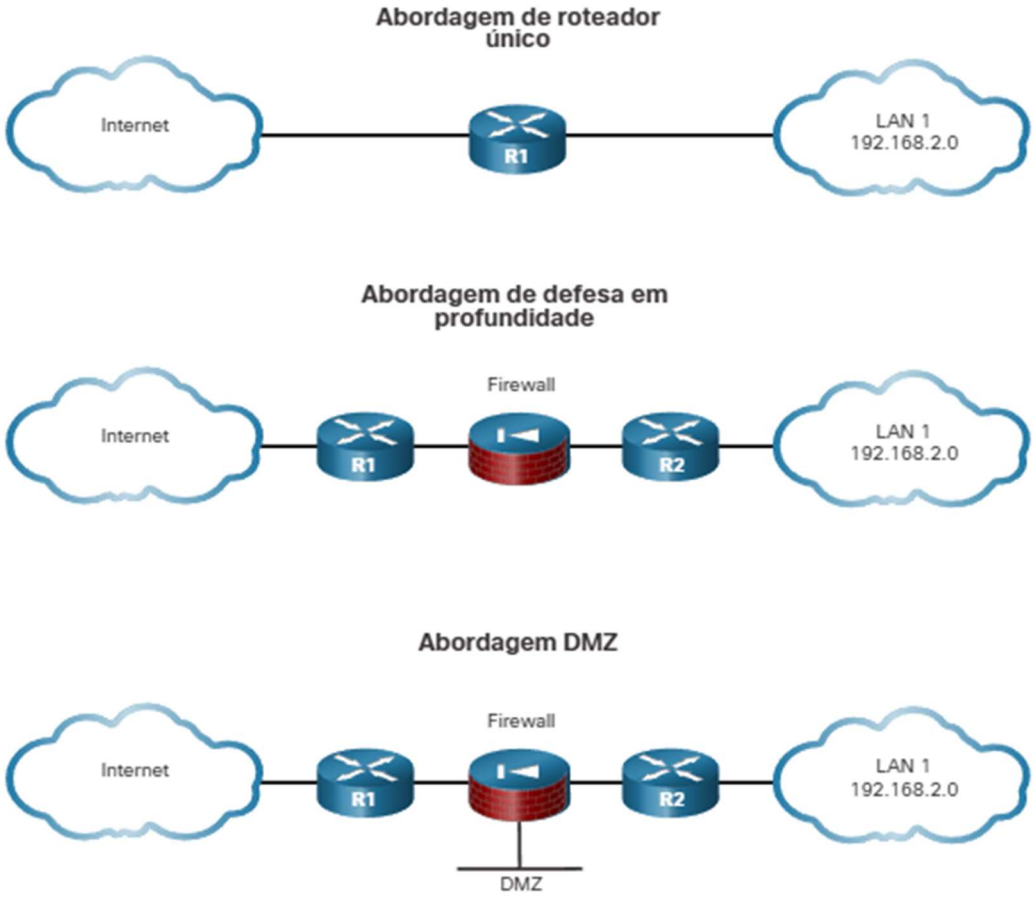
Para evitar o acesso não autorizado a todos os dispositivos de infraestrutura, políticas e controles de segurança adequados devem ser implementados. Os roteadores são o principal alvo de ataques porque esses dispositivos atuam como policiais de trânsito, que direcionam o tráfego para dentro, para fora e entre as redes.

O roteador de borda mostrado na figura é o último roteador entre a rede interna e uma rede não confiável, como a Internet. Todo o tráfego de internet de uma organização passa por um roteador de borda, que geralmente funciona como a primeira e última linha de defesa para uma rede. O roteador de borda ajuda a proteger o perímetro de uma rede protegida e implementa ações de segurança baseadas nas políticas de segurança da organização. Por estas razões, proteger os roteadores de rede é imperativo.

O Roteador de Borda

A implementação do roteador de borda varia dependendo do tamanho da organização e da complexidade do projeto de rede necessário. As implementações de roteador podem incluir um único roteador que protege uma rede interna inteira ou um roteador

funcionando como a primeira linha de defesa em uma abordagem de defesa aprofundada. Topologias simplificadas para as três abordagens são mostradas na figura:



Abordagem de roteador único

Na figura, um único roteador conecta a rede protegida ou a rede local interna (LAN), à Internet. Todas as políticas de segurança são configuradas neste dispositivo. Isso é mais comumente implantado em implementações de sites menores, como filiais e pequenos escritórios, escritórios domésticos (SOHO). Em redes menores, os recursos de segurança necessários podem ser suportados por ISRs (Integrated Services Routers) sem impedir as capacidades de desempenho do roteador.

Abordagem de defesa em profundidade

Uma abordagem de defesa em profundidade é mais segura do que a abordagem de roteador único. Ele usa várias camadas de segurança antes do tráfego que entra na LAN

protegida. Há três camadas primárias de defesa: o roteador de borda, o firewall e um roteador interno que se conecte à LAN protegida. O roteador de borda atua como a primeira linha de defesa e é conhecido como roteador de triagem. Depois de executar a filtragem de tráfego inicial, o roteador de borda passa todas as conexões que são pretendidas para a LAN interna para a segunda linha de defesa, que é o firewall.

O firewall normalmente pega onde o roteador de borda sai e executa filtragem adicional. Ele fornece controle de acesso adicional, rastreando o estado das conexões e atua como um dispositivo de ponto de verificação. Por padrão, o firewall nega o início de conexões das redes externas (não confiáveis) para a rede interna (confiável). Contudo, permite que os usuários internos estabeleçam conexões às redes não confiáveis e permite que as respostas voltem através do firewall. Ele também pode executar a autenticação do usuário (proxy de autenticação) em que os usuários devem ser autenticados para obter acesso a recursos de rede.

Os roteadores não são os únicos dispositivos que podem ser usados em uma abordagem de defesa em profundidade. Outras ferramentas de segurança, como sistemas de prevenção de intrusões (IPSs), dispositivos de segurança da Web (servidores proxy) e dispositivos de segurança de e-mail (filtragem de spam) também podem ser implementadas.

Abordagem DMZ

Uma variação da abordagem de defesa em profundidade é mostrada na figura. Esta abordagem inclui uma área intermediária, muitas vezes chamada de zona desmilitarizada (DMZ). A DMZ pode ser usada para servidores que devem ser acessíveis a partir do Internet ou de alguma outra rede externa. A DMZ pode ser configurada entre dois roteadores, com um roteador interno conectando à rede protegida e um roteador externo que conecta à rede desprotegida. Alternativamente, a DMZ pode simplesmente ser uma porta adicional fora de um único roteador. O firewall está localizado entre as redes protegidas e desprotegidas. O firewall é configurado para permitir as conexões necessárias, como HTTP, das redes externas (não confiáveis) aos servidores públicos na DMZ. O firewall serve como a proteção primária para todos os dispositivos na DMZ.

Protegendo o roteador de borda é um primeiro passo crítico para proteger a rede. Se houver outros roteadores internos, eles também devem ser configurados com segurança. Três áreas de segurança do roteador devem ser mantidas.

Segurança física

Forneça segurança física para os roteadores:

- Coloque o roteador e os dispositivos físicos que se conectam a ele em uma sala trancada segura que é acessível apenas ao pessoal autorizado, está livre de

interferência eletrostática ou magnética, tem supressão de fogo e tem controles de temperatura e umidade.

- Instale uma fonte de alimentação ininterrupta (UPS) ou gerador de energia de backup a diesel. Use fontes de alimentação redundantes em dispositivos de rede, se possível. Isso reduz a possibilidade de uma falha de rede de perda de energia ou equipamentos de energia com falha.

Software de sistema operacional

Há alguns procedimentos envolvidos em proteger os recursos e o desempenho dos sistemas operacionais de roteador:

- Equipar roteadores com a quantidade máxima de memória possível. A disponibilidade de memória pode ajudar a reduzir os riscos para a rede de alguns ataques de negação de serviço (DoS) enquanto suporta a mais ampla gama de serviços de segurança.
- Use a versão mais recente e estável do sistema operacional que atenda às especificações de recurso do roteador ou dispositivo de rede. Os recursos de segurança e criptografia em um sistema operacional são aprimorados e atualizados ao longo do tempo, o que torna fundamental ter a versão mais atualizada.
- Mantenha uma cópia segura das imagens do sistema operacional do roteador e dos arquivos de configuração do roteador como backups.

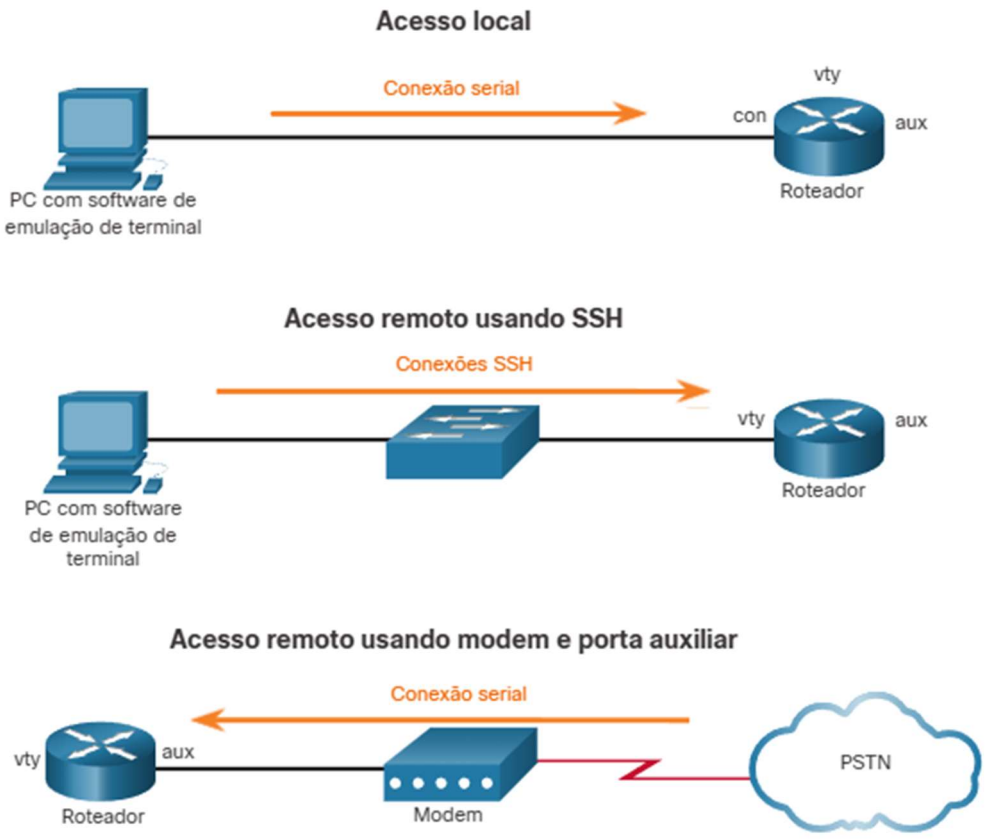
Endurecimento do roteador

Elimine o potencial abuso de portos e serviços não utilizados:

- Controle administrativo seguro. Certifique-se de que somente o pessoal autorizado tenha acesso e que seu nível de acesso seja controlado.
- Desativar portas e interfaces não utilizadas. Reduza o número de maneiras que um dispositivo pode ser acessado.
- Desativar serviços desnecessários. Semelhante a muitos computadores, um roteador tem serviços que são ativados por padrão. Alguns desses serviços são desnecessários e podem ser usados por um invasor para reunir informações sobre o roteador e a rede. Esta informação pode então ser usada em um ataque de exploração.

Um roteador pode ser acessado para fins administrativos local ou remotamente:

- **Acesso local** - Todos os dispositivos de infraestrutura de rede podem ser acessados localmente. O acesso local a um roteador geralmente requer uma conexão direta a uma porta de console no roteador Cisco e usando um computador que esteja executando o software de emulação de terminal, como mostrado na figura. O administrador deve ter acesso físico ao roteador e usar um cabo de console para se conectar à porta de console. O acesso local é usado tipicamente para a configuração inicial do dispositivo.
- **Acesso remoto** - Os administradores também podem acessar dispositivos de infraestrutura remotamente, como mostrado na figura. Embora a opção de porta auxiliar esteja disponível, o método de acesso remoto mais comum envolve permitir conexões Telnet, SSH, HTTP, HTTPS ou SNMP ao roteador a partir de um computador. O computador pode estar na rede local ou em uma rede remota. No entanto, se a conectividade de rede ao dispositivo estiver inativa, a única maneira de acessá-lo pôde ser sobre linhas telefônicas.



Alguns protocolos de acesso remoto enviam dados, incluindo nomes de usuário e senhas, para o roteador em texto simples. Se um invasor puder coletar o tráfego de rede enquanto um administrador estiver logando remotamente em um roteador, o invasor poderá capturar senhas ou informações de configuração do roteador. Por esta razão, é

preferível permitir somente o acesso local ao roteador. No entanto, em algumas situações, o acesso remoto ainda pode ser necessário. Precauções devem ser tomadas ao acessar a rede remotamente:

- Criptografe todo o tráfego entre o computador administrador e o roteador. Por exemplo, em vez de usar Telnet, use SSH versão 2; ou em vez de usar HTTP, use HTTPS.
- Estabelecer uma rede de gestão dedicada. A rede de gerenciamento deve incluir somente hosts de administração identificados e conexões a uma interface dedicada no roteador. O acesso a esta rede pode ser rigorosamente controlado.
- Configurar um filtro de pacote de informação para permitir que somente os anfitriões de administração identificados e os protocolos preferidos alcançam o roteador. Por exemplo, permita que somente solicitações SSH do endereço IP de um host de administração iniciem uma conexão com o Roteadores na rede.
- Configure e estabeleça uma conexão VPN à rede local antes de se conectar a uma interface de gerenciamento de roteador.

Essas precauções são valiosas, mas não protegem completamente a rede. Outros métodos de defesa também devem ser implementados. Um dos métodos mais básicos e importantes é o uso de senhas seguras.

A atribuição de senhas e autenticação local não impede que um dispositivo seja direcionado para ataque. Os aprimoramentos de login do Cisco IOS fornecem mais segurança diminuindo ataques, tais como ataques de dicionário e ataques DoS. Ativar um perfil de detecção permite que você configure um dispositivo de rede para reagir a tentativas repetidas com falha de login recusando solicitações de conexão adicionais (ou bloqueio de login). Este bloco pode ser configurado por um período de tempo, que é chamado de período silencioso. As listas de controle de acesso (ACLs) podem ser usadas para permitir conexões legítimas de endereços de administradores de sistema conhecidos.

Os banners são desativados por padrão e devem estar explicitamente ativados. Use o comando do modo de configuração global **banner** para especificar as mensagens apropriadas.

Router(config)# **banner motd** *delimiter message delimiter*

Exemplo:

R1(config)# banner motd $

Este equipamento e de propriedade privada e o acesso
e registrado. Desconecte-se imediatamente se voce
nao for um usuario autorizado. Os infratores serao
processados em toda a extensao da lei.
$

Os comandos de aprimoramentos de login do Cisco IOS, que são mostrados abaixo, aumentam a segurança das conexões de login virtuais.

```
R1(config)# login block-for 15 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)#
```

O comando **login block-for** pode se defender contra ataques DoS desativando logins após um número especificado de tentativas de login com falha. O comando **login quiet-mode** mapeia a uma ACL que identifique os hosts permitidos. Isto assegura-se de que somente os anfitriões autorizados possam tentar fazer login no roteador. O comando **login delay** especifica um número de segundos que o usuário deve esperar entre tentativas de login mal sucedidas. Os comandos **login on-success** e **login on-failure** registram tentativas de login bem-sucedidas e malsucedidas.

Esses aprimoramentos de login não se aplicam a conexões de console. Ao lidar com conexões de console, supõe-se que somente o pessoal autorizado tenha acesso físico aos dispositivos.

Para ajudar um dispositivo Cisco IOS a fornecer detecção de DoS, use o comando **login block-for**. Todos os outros recursos de aprimoramento de login são desabilitados até que o comando **login block-for** esteja configurado.

Especificamente, o comando **login block-for** monitora a atividade do dispositivo de login e opera em dois modos:

- **Modo normal** - Isso também é conhecido como modo de relógio. O roteador mantém a contagem do número de tentativas de login falhadas dentro de uma quantidade de tempo identificada.
- **Modo silencioso** - Este também é conhecido como o período de silêncio. Se o número de logins com falha exceder o limite configurado, todas as tentativas de login usando telnet, ssh e http são negadas para o tempo especificado no comando **login block-for**.

Quando o modo silencioso está ativado, todas as tentativas de login, incluindo acesso administrativo válido, não são permitidas. No entanto, para fornecer hosts críticos, como acesso de hosts administrativos específicos em todos os momentos, esse comportamento pode ser substituído usando uma ACL. O ACL é criado e identificado usando o comando **login quiet-mode access-class**. Somente os anfitriões identificados no ACL têm o acesso ao dispositivo durante o modo silencioso.

O exemplo na figura mostra uma configuração que use uma ACL que seja nomeada PERMIT-ADMIN. Os hosts que combinam as condições PERMIT-ADMIN estão isentos do modo silencioso.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
```

```
R1(config)# login delay 3
```