

Packet Tracer - Definir configurações iniciais do switch

Objetivos

Parte 1: Verificar a configuração padrão do switch

Parte 2: Configurar uma configuração básica do switch

Parte 3: Configurar um banner MOTD

Parte 4: Salvar os arquivos de configuração na NVRAM

Parte 5: Configurar S2

Histórico/Cenário

Nesta atividade, você executará tarefas básicas de configuração do comutador. Você protegerá o acesso à interface de linha de comando (CLI) e às portas de console usando senhas de texto simples e criptografadas. Você também aprenderá a configurar mensagens para usuários que se registram no switch. Esses banners de mensagens também são usados para avisar usuários não autorizados que o acesso é proibido.

Observação: No Packet Tracer, o switch Catalyst 2960 usa o IOS versão 12.2 por padrão. Se necessário, a versão do IOS pode ser atualizada a partir de um servidor de arquivos na topologia do Tracer de Pacotes. O switch pode então ser configurado para inicializar no IOS versão 15.0, se essa versão for necessária.

Instruções

Parte 1: Verificar a configuração padrão do switch

Etapa 1: Entrar no modo EXEC privilegiado.

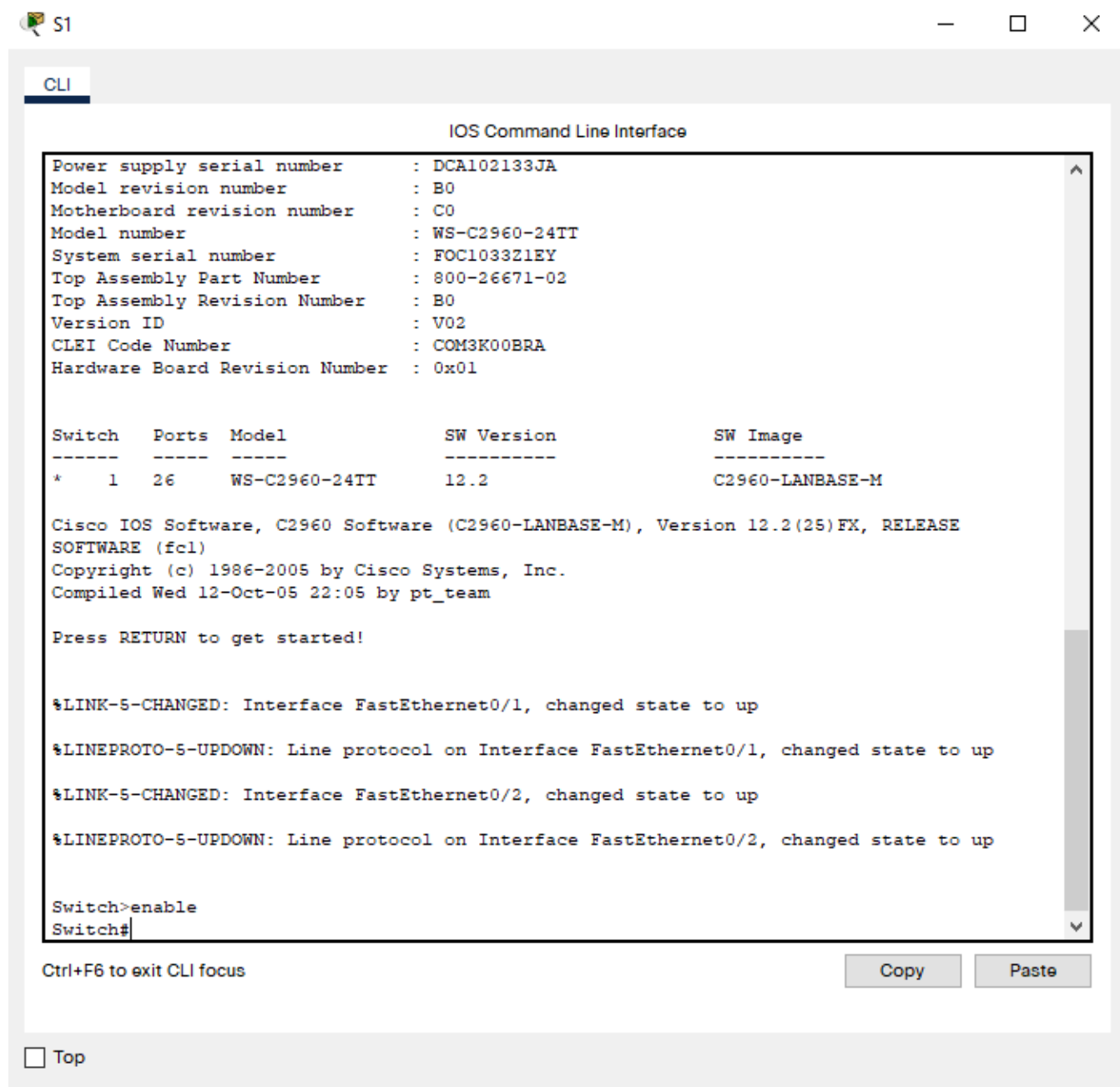
Você pode acessar todos os comandos do switch no modo EXEC privilegiado. No entanto, como muitos dos comandos privilegiados configuram parâmetros operacionais, o acesso privilegiado deve ser protegido por senha para evitar o uso não autorizado.

O conjunto de comandos EXEC privilegiados inclui os comandos disponíveis no modo EXEC do usuário, muitos comandos adicionais e o comando **configure** através do qual o acesso aos modos de configuração é obtido.

- a. Clique em S1 e depois na guia CLI. Pressione Enter.
- b. Entre no modo EXEC privilegiado inserindo o comando enable:

```
Switch> enable  
Switch#
```

Observe que o prompt foi alterado para refletir o modo EXEC privilegiado.



Etapa 2: Examinar a configuração atual do switch.

Insira o comando show running-config.

Switch# **show running-config**

Responda às perguntas a seguir:

Quantas interfaces Fast Ethernet o switch possui? **R: 24**

Quantas interfaces Gigabit Ethernet o switch possui? **R: 2**

Qual é a faixa de valores mostrados nas linhas VTY?

```
line vty 0 4
  login
line vty 5 15
  login
```

Que comando exibirá o conteúdo atual da memória de acesso aleatório não volátil (NVRAM)?

R: show startup-config

Por que o switch responde com "startup-config is not present?"

R: NVRAM não existe

Parte 2: Criar uma configuração básica do switch

Etapa 1: Atribuir um nome a um switch.

Para configurar parâmetros em um switch, pode ser necessário mover-se entre vários modos de configuração. Observe como o prompt muda à medida que você navega pelo switch.

```
Switch# configure terminal
Switch(config)#hostname S1
S1(config)# exit
S1#

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
|
```

Etapa 2: Acesso seguro à linha do console.

Para proteger o acesso à linha do console, acesse o modo config-line e defina a senha da console como **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. Termine com CNTL/Z.
S1(config)#line console 0
S1 (config-line) # senha letmein
S1 (config-line) # login
```

```
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Por que o comando **login** é necessário?

R: Para criar uma senha.

Etapa 3: Verificar se o acesso do console está protegido.

Saia do modo privilegiado para verificar se a senha da porta de console está em vigor.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Nota: Se o switch não solicitar uma senha, você não configurou o parâmetro de login na Etapa 2.

Press RETURN to get started.

User Access Verification

Password:

Ctrl+F6 to exit CLI focus

Copy

Paste

Etapa 4: Acesso seguro ao modo privilegiado.

Defina a senha de **enable** como **c1\$c0**. Essa senha protege o acesso ao modo privilegiado.

Nota: O **0** em **c1\$c0** é um zero, não um O maiúsculo. Essa senha não será classificada como correta até depois que você a criptografar na Etapa 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
```

```
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Etapa 5: Verificar se o acesso ao modo privilegiado é seguro.

- Insira o comando **exit** novamente para fazer logoff do switch.
- Pressione **<Enter>** e uma senha será solicitada a você:

User Access Verification
Password:
- A primeira é a senha do console que você configurou com **line con 0**. Digite essa senha para voltar ao modo EXEC usuário.
- Digite o comando para acessar o modo privilegiado.
- Digite a segunda senha que você configurou para proteger o modo EXEC privilegiado.
- Verifique sua configuração examinando o conteúdo do arquivo de configuração em execução:

```
S1# show running-config
```

Observe que o console e as senhas de habilitação estão em texto simples. Isso pode representar um risco de segurança se alguém estiver olhando por cima do seu ombro ou obtiver acesso a arquivos de configuração armazenados em um local de backup.

```
User Access Verification

Password:

SI>enable
Password:
SI#show running-config
Building configuration...

Current configuration : 1125 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SI
!
enable password c1$c0
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
--More--
```

Etapa 6: Configure uma senha criptografada para proteger o acesso ao modo privilegiado.

A **senha de enable** deve ser substituída pela senha secreta criptografada mais recente usando o comando **enable secret**. Defina a senha de enable secret como **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Nota: A **senha secreta** de ativação substitui a **senha de ativação**. Se ambos estiverem configurados no comutador, você deverá inserir a **senha secreta** de ativação para entrar no modo EXEC privilegiado.

Etapa 7: Verifique se a senha de enable secret é adicionada ao arquivo de configuração.

Digite o comando **show running-config** de novo para verificar se a nova senha de enable secret está configurada.

Nota: Você pode abreviar **show running-config** como

```
S1# show run
```

O que é exibido como a senha de enable secret?

```
SI#configure t
Enter configuration commands, one per line. End with CNTL/Z.
SI(config)#enable secret itsasecret
SI(config)#exit
SI#
%SYS-5-CONFIG_I: Configured from console by console

SI#show run
Building configuration...

Current configuration : 1172 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SI
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password cl$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
--More-- |
```

Por que a senha de enable secret é exibida de forma diferente do que configuramos? **R: Porque criamos uma senha criptografada.**

Etapa 8: Criptografar as senhas de enable e console.

Como você notou na Etapa 7, a **senha secreta** de ativação foi criptografada, mas as senhas de **ativação** e **console** ainda estavam em texto sem formatação. Nós criptografaremos agora essas senhas de texto simples com o comando **service password-encryption**.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Se você configurar mais senhas no switch, elas serão exibidas no arquivo de configuração como texto simples ou em formato criptografado? Explique.

R: Elas se mantêm criptografadas por conta do comando anterior.

Parte 3: Configurar um banner MOTD

Etapa 1: Configurar um banner da mensagem do dia (MOTD).

O conjunto de comandos do CISCO IOS inclui um recurso que permite configurar as mensagens que qualquer pessoa conectada no switch vê. Essas mensagens são chamadas de mensagem do dia ou banners MOTD. Insira o texto de banner entre aspas ou use um delimitador diferente de qualquer caractere que aparece na sequência MOTD.

```
S1# configuração t
S1(config)# banner motd "This is a secure system. Somente Acesso Autorizado!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Quando esse banner será exibido?

R: Ao iniciar o CLI.

Por que cada switch deve ter um banner MOTD?

R: Um aviso de segurança importante.

Parte 4: Salvar e verificar arquivos de configuração na NVRAM

Etapa 1: Verificar se a configuração é precisa usando o comando show run.

Salvar o arquivo de configuração. Você concluiu a configuração básica do switch. Agora, faça o backup do arquivo de configuração atual na NVRAM para garantir que as alterações feitas não sejam perdidas se o sistema for reinicializado ou se houver queda de energia.

```
S1# copy running-config startup-config
Nome do arquivo de destino [startup-config]? [Enter]
Building configuration...
[OK]
```

Qual é a versão mais curta abreviada do comando **copy running-config startup-config**?

R: copy running-config sta

Examinar o arquivo de configuração inicial.

Que comando exibirá o conteúdo da NVRAM?

R: show startup-config

Todas as alterações que foram digitadas foram registradas no arquivo?

R: Sim.

Parte 5: Configurar S2

Você concluiu a configuração em S1. Você vai configurar o S2 agora. Se você não se lembrar dos comandos, consulte as Partes 1 a 4 para obter ajuda.

Configure S2 com os seguintes parâmetros:

- Nome do Dispositivo: **S2**
- Proteja o acesso ao console com a senha **letmein**.
- Configure uma senha de habilitação de **c1\$c0** e uma senha secreta de habilitação de **seu segredo**.
- Configure uma mensagem apropriada para aqueles que fazem login no switch.
- Criptografe todas as senhas em texto claro.
- Verifique se a configuração está correta.
- Salve o arquivo de configuração para evitar perdas se o switch for desligado.


```
S2>enable
Password:
Password:
S2#enable
S2#show startup-config
Using 1204 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
enable secret 5 $l$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
!
!
!
```