[SISTEMA OPERACIONAIS 1](#_Toc287942568)

[GUI 2](#_Toc1150066507)

[OBJETIVO DE UM SO 3](#_Toc1191245207)

[METODOS DE ACESSO 3](#_Toc1399571364)

[COMANDOS PRIMARIOS 4](#_Toc1010878961)

[MODO DE CONFIGURAÇÃO 5](#_Toc659223500)

[NAVEGAR ENTRE MODOS 5](#_Toc1591228949)

[ESTRUTURA BÁSICA DE COMANDOS 6](#_Toc1459491708)

[VERIFICAÇÃO DA SINTAXE DE COMANDO 7](#_Toc1969786644)

[TECLAS E ATALHOS 8](#_Toc1282454480)

[NOMES DE DISPOSITIVOS 10](#_Toc1005268789)

[DIRETRIZES E SENHAS. 11](#_Toc2039080115)

[CONFIGURAR SENHA 12](#_Toc418392477)

[CRIPTOGRAR SENHAS 13](#_Toc1635695272)

[MENSAGEM DE BANNER 15](#_Toc722874450)

[ARQUIVO DE CONFIGURAÇÃO 15](#_Toc1786215565)

[ALTERAR CONFIGURAÇÃO ATIVA 16](#_Toc1329209585)

[ENDEREÇO IP 17](#_Toc699244736)

[INTERFACES E PORTAS 18](#_Toc2055938024)

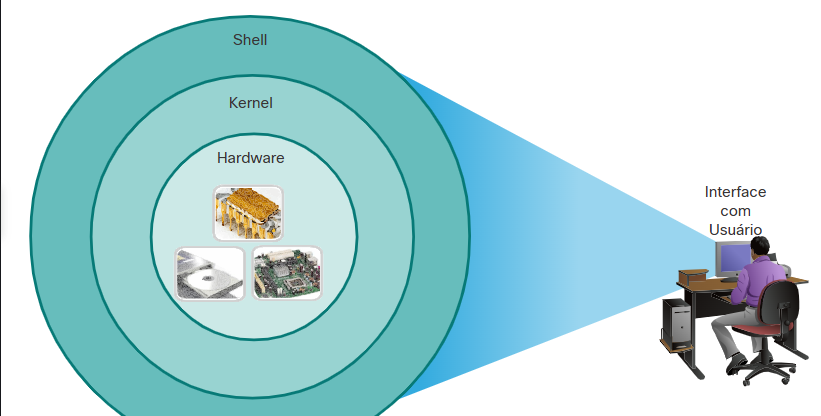
[CONFIGURAÇÃO MANUAL DE ENDEREÇO IP 19](#_Toc504500193)

[CONFIGURAÇÃO AUTOMATICA DE ENDEREÇO IP 20](#_Toc250349750)

[CONFIGURAÇÃODA INTERFACE VIRTUAL DO SWITCH 21](#_Toc299984917)

# SISTEMA OPERACIONAIS

A parte do sistema operacional que interage diretamente com o hardware do computador é conhecida como kernel. A parte que tem interface com aplicações e o usuário é conhecida como shell. O usuário pode interagir com a shell por meio de uma interface de linha de comando CLI (Interface de linha de Comando) ou uma interface gráfica de usuário GUI (Interface Gráfica do Usuário).



**Shell** - A interface de usuário que permite que os usuários solicitem tarefas específicas do computador. Essas solicitações podem ser feitas por meio da interface CLI ou GUI.

**Kerne**l - comunica-se entre o hardware e o software de um computador e gerencia como os recursos de hardware são usados para atender aos requisitos de software.

**Hardware** - A parte física de um computador, incluindo os componentes eletrônicos subjacentes.

# GUI

Uma GUI como Windows, macOS, Linux KDE, Apple iOS ou Android permite que o usuário interaja com o sistema usando um ambiente de ícones gráficos, menus e janelas. O exemplo da GUI na figura é mais fácil de usar e requer menos conhecimento da estrutura de comando subjacente que controla o sistema. Por esse motivo, a maioria dos usuários depende de ambientes da GUI.

No entanto, nem sempre as GUIs podem fornecer todos os recursos disponíveis com a CLI. As GUIs também podem falhar, congelar ou simplesmente não funcionar como especificado. Por esses motivos, os dispositivos de rede geralmente são acessados por meio de uma CLI. A CLI consome menos recursos e é muito estável, em comparação com uma GUI.



# OBJETIVO DE UM SO

Os sistemas operacionais de rede são semelhantes a um sistema operacional de PCs. Por meio de uma GUI, um sistema operacional de PC permite que o usuário faça o seguinte:

Utilizar um mouse para fazer seleções e executar programas;

Inserir texto e comandos baseados em texto;

Exibir a saída em um monitor.

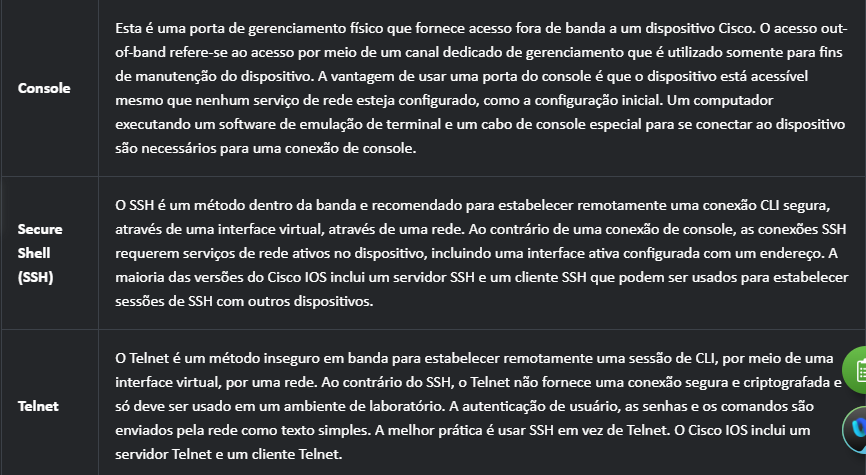
Um sistema operacional de rede baseado em CLI (por exemplo, o Cisco IOS em um switch ou roteador) permite que um técnico de rede faça o seguinte:

Use um teclado para executar programas de rede baseados na CLI;

Use um teclado para inserir texto e comandos baseados em texto;

Exibir a saída em um monitor.

# METODOS DE ACESSO

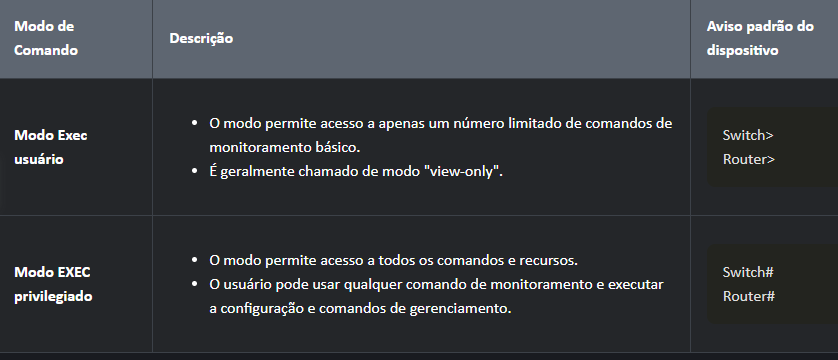


# COMANDOS PRIMARIOS

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.



# MODO DE CONFIGURAÇÃO

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)#.

# NAVEGAR ENTRE MODOS

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***

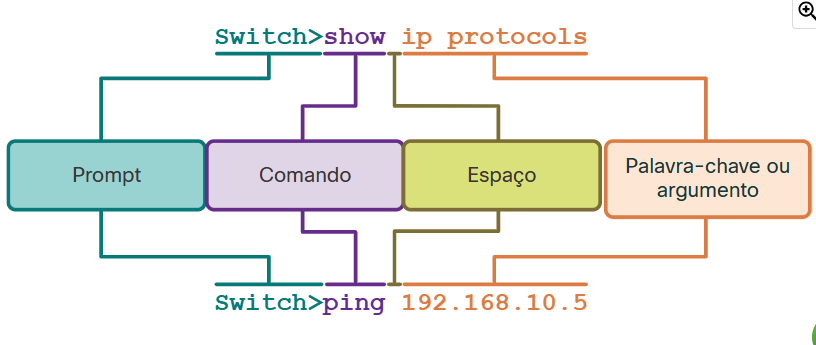
***Switch#***

Você também 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)#***

# ESTRUTURA BÁSICA DE COMANDOS



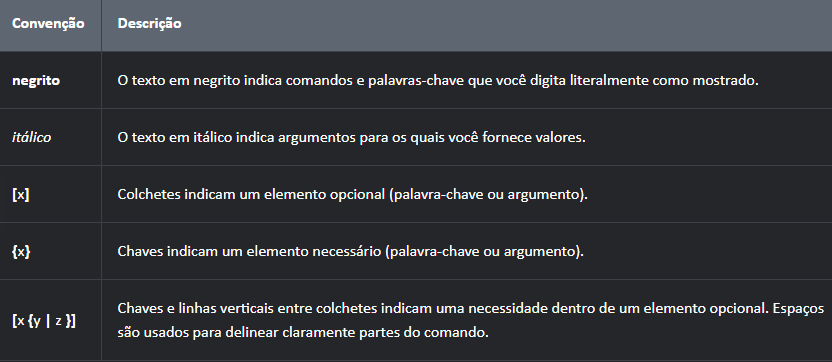
Palavra-chave – Este é um parâmetro específico definido no sistema operacional (na figura, protocolos ip)

Argumento – Isso não é predefinido; é um valor ou variável definido pelo usuário (na figura, 192.168.10.5)

# VERIFICAÇÃO DA SINTAXE DE COMANDO

Um comando pode exigir um ou mais argumentos. Para determinar as palavras-chave e os argumentos necessários para um comando, consulte a sintaxe de comando. A sintaxe fornece o padrão, ou formato, que deve ser usado ao inserir um comando.

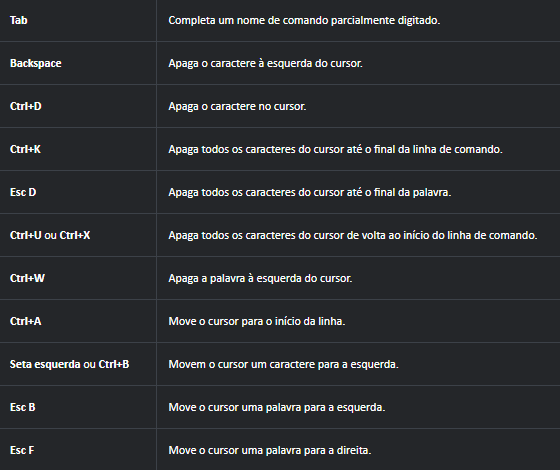
Por exemplo, a sintaxe para usar o comando description é description string. O argumento é um valor string fornecido pelo usuário. O comando description é normalmente usado para identificar a finalidade de uma interface. Por exemplo, digitando o comando,description Connects to the main headquarter office switch, descreve onde o outro dispositivo está no final da conexão.



Os exemplos a seguir demonstram as convenções usadas para documentar e utilizar comandos do IOS:

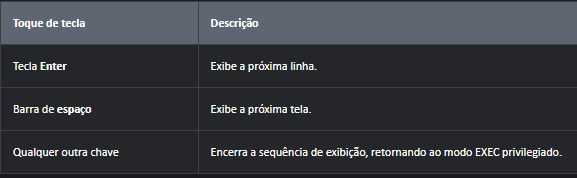
Ping ip-address – O comando é ping e o argumento definido pelo usuário é o endereço-IP do dispositivo de destino. Por exemplo ping ping 10.10.10.5.

# TECLAS E ATALHOS

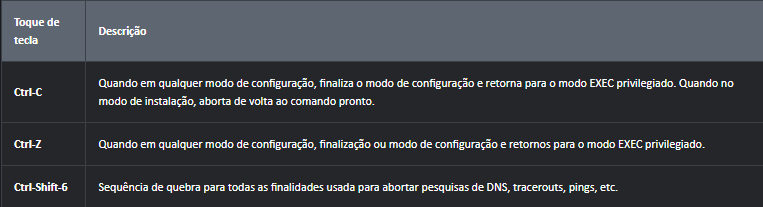


Observação: Embora a chave Delete exclua normalmente o caractere à direita do prompt, a estrutura de comando do IOS não reconhece a chave Delete.

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.



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



# NOMES DE DISPOSITIVOS

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;*

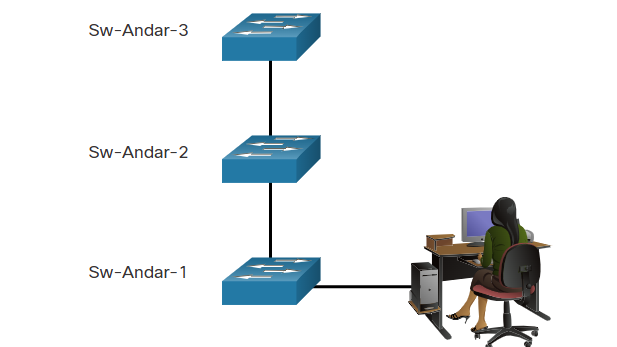
*Não conter espaços;*

*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.



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.

# DIRETRIZES E SENHAS.

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.

# CONFIGURAR SENHA

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 passwordpassword. 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#***

CRIPTOGRAR SENHAS

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.

***1(config)# endSw-Floor-***

***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***

MENSAGEM DE BANNER

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#

# ARQUIVO DE CONFIGURAÇÃO

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.

# ALTERAR CONFIGURAÇÃO ATIVA

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.

# ENDEREÇO IP

O uso de endereços IP é o principal meio de permitir que os dispositivos se localizem e estabeleçam comunicação ponto a ponto na Internet. Cada dispositivo final em uma rede deve ser configurado com um endereço IP. Exemplos de dispositivos finais incluem estes:

Computadores (estações de trabalho, laptops, servidores de arquivo, servidores Web);

Impressoras de rede;

Telefones VoIP;

Câmeras de segurança;

Smartphones;

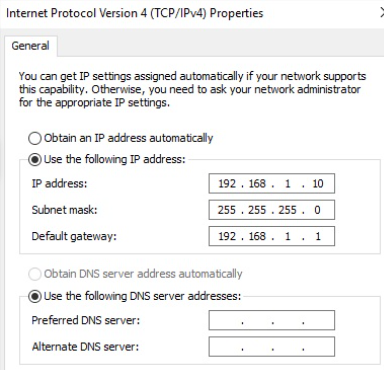
Dispositivos móveis portáteis (como scanners de códigos de barras sem fio).

A estrutura de um endereço IPv4 é chamada notação decimal com ponto e é representada por quatro números decimais entre 0 e 255. Os endereços IPv4 são atribuídos individualmente a dispositivos conectados a uma rede.

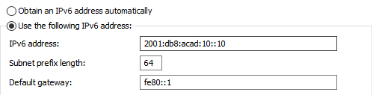
Observação: O IP neste curso refere-se aos protocolos IPv4 e IPv6. O IPv6 é a versão mais recente do IP e está substituindo o IPv4 mais comum.

Com o endereço IPv4, uma máscara de sub-rede também é necessária. Uma máscara de sub-rede IPv4 é um valor de 32 bits que diferencia a parte da rede do endereço da parte do host. Juntamente com o endereço IPv4, a máscara de sub-rede determina a qual sub-rede o dispositivo é membro.

O exemplo na figura exibe o endereço IPv4 (192.168.1.10), máscara de sub-rede (255.255.255.0) e gateway padrão (192.168.1.1) atribuído a um host. O endereço de gateway padrão é o endereço IP do roteador que o host usará para acessar redes remotas, incluindo a Internet.

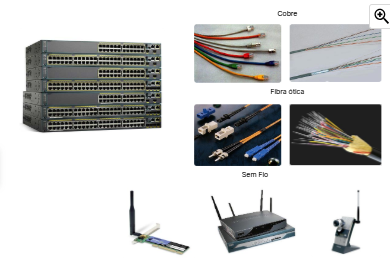


Os endereços IPv6 têm 128 bits e são escritos como uma sequência de valores hexadecimais. A cada quatro bits é representado por um único dígito hexadecimal; para um total de 32 valores hexadecimais. Grupos de quatro dígitos hexadecimais são separados por dois pontos (:). Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos tanto em minúsculas como em maiúsculas.



# INTERFACES E PORTAS

As comunicações em rede dependem de interfaces do dispositivo de usuário final, interfaces do dispositivo de rede e cabos que as conectam. Cada interface física tem especificações ou padrões que a definem. Um cabo conectado à interface deve ser projetado de acordo com os padrões físicos da interface. Os tipos de mídia de rede incluem cabos de cobre de par trançado, cabos de fibra óptica, cabos coaxiais ou sem fio



Diferentes tipos de meio físico de rede oferecem características e benefícios diferentes. Nem todas as mídias de rede têm as mesmas características. Nem todas as mídias são apropriadas para o mesmo propósito. Estas são algumas das diferenças entre os vários tipos de mídia:

A distância pela qual o meio físico consegue carregar um sinal com êxito;

O ambiente no qual o meio físico deve ser instalado;

A quantidade e a velocidade de dados nas quais eles devem ser transmitidos;

O custo do meio físico e da instalação.

Cada link na Internet não exige apenas um tipo de mídia de rede específico, mas também requer uma tecnologia de rede específica. Por exemplo, Ethernet é a tecnologia de rede local (LAN) mais comum usada atualmente. As portas Ethernet são encontradas nos dispositivos de usuário final, dispositivos de switch e outros dispositivos de rede que podem se conectar fisicamente à rede por meio de um cabo.

Os switches Cisco IOS de Camada 2 têm portas físicas para se conectarem a dispositivos. Essas portas não são compatíveis com endereços IP da Camada 3. Portanto, os switches têm uma ou mais interfaces virtuais de switch (SVIs). Essas interfaces virtuais existem porque não há hardware físico no dispositivo associado. Uma SVI é criada no software.

A interface virtual permite gerenciar remotamente um switch em uma rede usando IPv4 e IPv6. Todo switch tem uma SVI na configuração padrão pronta para uso A SVI padrão é a interface VLAN1.

Observação: Um switch da camada 2 não precisa de um endereço IP. O endereço IP atribuído à SVI é usado para acesso remoto ao switch. Um endereço IP não é necessário para o switch executar suas operações.

# CONFIGURAÇÃO MANUAL DE ENDEREÇO IP

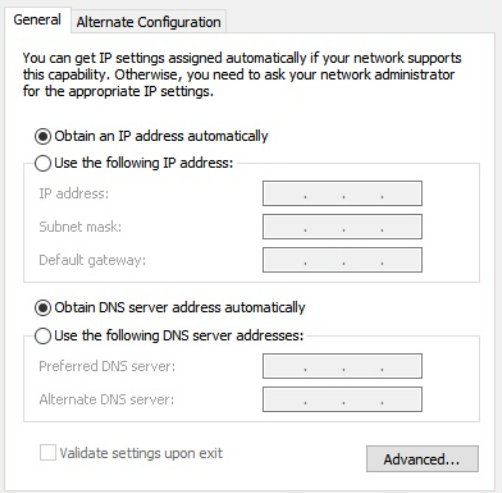
Os dispositivos finais da sua rede precisam de um endereço IP para que eles possam se comunicar com outros dispositivos na sua rede. Neste tópico, você implementará a conectividade básica configurando o endereçamento IP em comutadores e PCs.

As informações de endereço IPv4 podem ser inseridas nos dispositivos finais manualmente ou automaticamente usando o DHCP (Dynamic Host Configuration Protocol).

# CONFIGURAÇÃO AUTOMATICA DE ENDEREÇO IP

Os dispositivos finais geralmente usam o DHCP para configuração automática de endereço IPv4. O DHCP é a tecnologia usada em quase todas as redes. A melhor maneira de entender por que o DHCP é tão popular é analisando o trabalho extra que seria necessário sem ele.

Em uma rede, o DHCP habilita a configuração automática de endereço IPv4 para todos os dispositivos finais habilitados para DHCP. Imagine quanto tempo levaria se, toda vez que você se conectasse à rede, tivesse que inserir manualmente o endereço IPv4, a máscara de sub-rede, o gateway padrão e o servidor DNS. Multiplique isso por cada usuário e cada dispositivo em uma organização e você entenderá o problema. A configuração manual também aumenta a possibilidade de erros ao duplicar o endereço IPv4 de outro dispositivo.



# CONFIGURAÇÃODA INTERFACE VIRTUAL DO SWITCH

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***