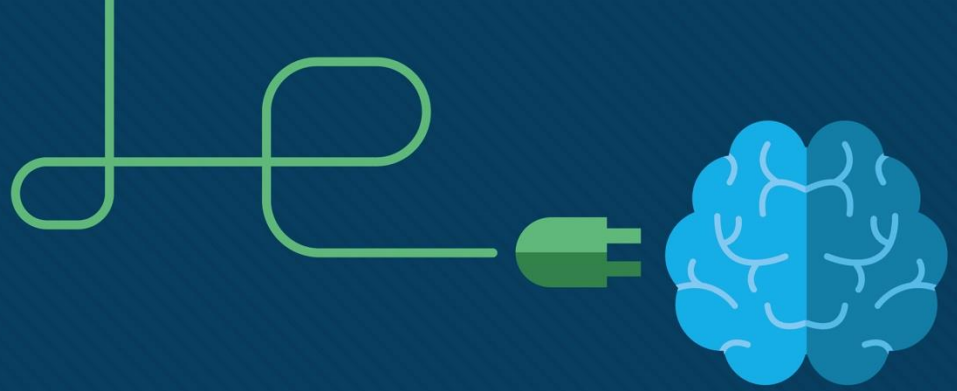


Módulo 1: Configuração básica do dispositivo

Versão original: Cisco Network Academy
Versão modificada: Eduardo Costa

Switching, Routing, e Wireless Essentials v7.0 (SRWE)

Objetivos do módulo

Título do Módulo Configuração básica do dispositivo

Objectivo do módulo: Configurar dispositivos usando as melhores práticas de segurança.

Título do Tópico	Objetivo do Tópico
Configurar um switch com definições iniciais	Configurar definições iniciais num switch Cisco.
Configurar portas do switch	Configurar as portas do switch para atender aos requisitos de rede.
Acesso remoto seguro	Configurar o acesso seguro de gestão num switch.
Configuração básica do router	Definir as configurações básicas de um router para encaminhar entre duas redes diretamente ligadas, usando o CLI.
Verificar redes conectadas diretamente	Verificar a conectividade entre duas redes diretamente conectadas a um router.

1.1 Configure um Switch usando as Configurações Iniciais

Sequência de arranque (boot) do Switch

Quando um switch Cisco é ligado, ele segue a seguinte sequência de inicialização de cinco etapas:

Etapa 1: Primeiro, o switch carrega um programa POST (Power-On Self-Test) armazenado na ROM. POST verifica o subsistema da CPU. Testa a CPU, DRAM e a parte do dispositivo flash que compõe o sistema de ficheiros da flash.

Etapa 2: a seguir, o switch carrega o software do boot loader. O carregador de inicialização (boot loader) é um programa pequeno armazenado na ROM que é executado imediatamente após a conclusão bem-sucedida do POST.

Etapa 3: O carregador de inicialização executa uma inicialização de baixo nível da CPU. Ele inicializa os registos da CPU, que controlam onde a memória física é mapeada, a quantidade de memória e sua velocidade.

Etapa 4: O carregador de inicialização inicializa o sistema de ficheiros da flash na placa do sistema.

Etapa 5: Finalmente, o carregador de inicialização localiza e carrega uma imagem padrão do software do sistema operativo IOS na memória e dá o controlo do switch através do IOS.

O comando do sistema de inicialização (boot system)

- O switch tenta inicializar automaticamente usando informações na variável de ambiente BOOT. Se esta variável não estiver definida, o switch tentará carregar e executar o primeiro arquivo executável que encontrar.
- O sistema operativo IOS inicializa as interfaces usando os comandos do Cisco IOS encontrados no ficheiro startup-config. O ficheiro startup-config é chamado **config.text** e está localizado na flash.
- No exemplo, a variável de ambiente BOOT é definida usando o comando **boot system** no modo de configuração global. Observe que o IOS está localizado em uma pasta distinta e o caminho da pasta é especificado. Use o comando **show boot** para ver como o ficheiro de inicialização IOS atual está definido.

```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

Comando	Definição
boot system	O comando principal
flash:	O dispositivo de armazenamento
C2960-lanbasek9- mz.150-2.se/	O caminho para o sistema de ficheiros
C2960-lanbasek9-mz.150-2.se.bin	O nome do ficheiro IOS

LEDs Indicadores do switch

System LED (SYST): Mostra se o sistema está a receber energia e a funcionar corretamente.
LED de Redundant Power Supply (RPS): Mostra o estado da fonte de alimentação redundante.
LED de Status de Porta (STAT): Quando está verde, indica que o modo de estado da porta está selecionado, que é o default. O estado da porta pode ser entendido pela luz associada a cada porta.
LED de Porta Duplex (DUPX): Quando verde, indica que o modo duplex da porta está selecionado. Porta duplex pode então ser entendida pela luz associada a cada porta.
LED de velocidade da porta (SPEED): quando verde, indica que o modo de velocidade da porta está selecionado. A velocidade da porta pode então ser entendida pela luz associada a cada porta.
Power over Ethernet LED (PoE): Presente se o switch suportar PoE. Indica o estado PoE das portas no switch.

O botão Mode é usado para mover entre os diferentes modos — STAT, DUPX, SPEED e PoE

LEDs Indicadores do Switch (Cont.)

	Desligado	Verde	Verde intermitente	Laranja	Laranja intermitente	Alternating Green/Amber
RPS	Desativado/ Sem RPS	Pronto para RPS	RPS pronto, mas não disponível	RPS em espera ou falha	O PS interno falhou, o RPS fornece energia	N/D
PoE	Não selecionado , sem problemas	selecionado	N/D	N/D	Não selecionado, problemas de porta presentes	N/D
Quando o modo nomeado é selecionado, a luz associada a cada porta física indica:						
STAT	Sem link ou desligado	Link Up	Atividade	Porta bloqueada evitando loop	Porta bloqueada evitando loop	Falha de link
DUPLEX	Half-duplex	Full-duplex	N/D	N/D	N/D	N/D
VELOCIDADE	10 Mbps	100 Mbps	1000 Mbps	N/D	N/D	N/D
PoE	PoE desligado	PoE em	N/D	PoE desativado	PoE desligado devido a falha	PoE negado (acima da capacidade)

Recuperar de uma falha no sistema

O boot loader fornece acesso ao switch se o sistema operativo não puder ser usado devido a ficheiros de sistema ausentes ou danificados. O boot loader tem uma linha de comando que fornece acesso aos ficheiros armazenados na memória flash. O boot loader pode ser acedido através de uma ligação de consola, seguindo estas etapas:

Etapa 1. Ligar um PC pelo cabo do consola à porta de consola do switch. Configure o software de emulação de terminal para a ligação ao switch.

Etapa 2. Desligar o cabo de alimentação do switch.

Etapa 3. Ligar novamente o cabo de alimentação do switch e, dentro de 15 segundos, pressionar e manter pressionado o botão Modo enquanto o LED do sistema ainda estiver a piscar verde.

Etapa 4. Continuar a pressionar o botão Modo até que o LED do sistema fique brevemente âmbar e verde sólido; em seguida, soltar o botão Modo.

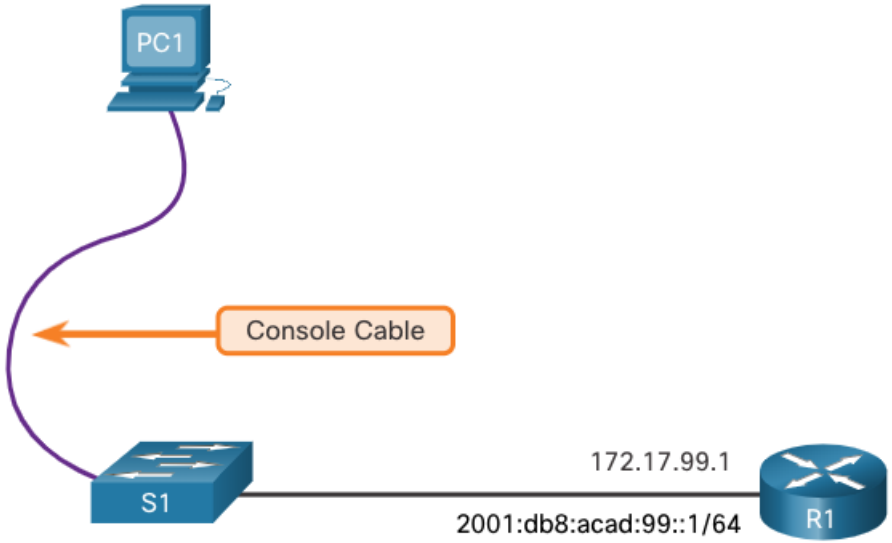
Etapa 5. Aparecerá a prompt do boot loader **switch:** no software de emulação de terminal no PC.

A linha de comando do boot loader aceita comandos para formatar o sistema de ficheiros flash, reinstalar o software do sistema operativo e recuperá-lo no caso de perda ou esquecimento da password. Por exemplo o comando **dir** pode ser usado para ver a lista de ficheiros dentro de uma directoria específica.

Acesso para Gestão do Switch

Para preparar um switch para o acesso de gestão remota, o switch deve ser configurado com um endereço IP e uma máscara de sub-rede.

- Para gerir o switch a partir de uma rede remota, o switch deve ser configurado com um gateway por omissão. De forma semelhante à configuração das informações de endereço IP em dispositivos finais.
- Na figura, o SVI (Switch Virtual Interface) no S1 deve receber um endereço IP. O SVI é uma interface virtual, não uma porta física no switch. Um cabo de consola é usado para conectar-se de um PC ao switch para a configuração inicial do switch.



Exemplo de Configuração da SVI do Switch

Por omissão, o switch está configurado para a gestão ser controlada pela VLAN 1. Todas as portas são atribuídas à VLAN 1 por defeito. Por motivos de segurança, é considerado uma prática recomendada usar uma VLAN diferente da VLAN 1 para a VLAN de gestão,

Etapa 1: **Configurar a interface de gestão:** Configurar um endereço IPv4 e a máscara de sub-rede na SVI de gestão do switch é feito a partir do modo de configuração da interface VLAN

Nota: o SVI para VLAN 99 não aparecerá como “Up/Up” até que a VLAN 99 seja criada e seja ativada ou exista uma interface associada a essa VLAN.

Nota: Se precisar configurar o switch com endereçamento IPv6, nesse caso serão necessárias configurações adicionais. Por exemplo, antes de configurar o endereçamento IPv6 num Cisco Catalyst 2960 com a versão 15.0 do IOS, é necessário executar o comando no modo de configuração global **sdm prefer dual-ipv4-e-ipv6 default** e, em seguida, deverá ser feito o **reload** do switch.

Exemplo de Configuração da SVI do Switch (Cont.)

Tarefa	Comandos IOS
Entre no modo de configuração global.	S1# **configure terminal**
Entre no modo de configuração da interface para SVI.	S1(config)# **interface vlan 99**
Configure o endereço IPv4 da interface de gestão.	S1(config-if)# **ip address 172.17.99.11 255.255.255.0**
Configurar o endereço IPv6 da interface de gestão	S1 (config-if) # **ipv6 address 2001:db8:acad:99: :1/64**
Ative a interface de gestão.	S1(config-if)# **no shutdown**
Volte para o modo EXEC privilegiado.	S1(config-if)#**end**
Salve a configuração atual no **startup-config**.	S1# **copy running-config startup-config**

Exemplo de Configuração da SVI do Switch (Cont.)

Step 2: Configure o Gateway por Omissão

- O switch deve ser configurado com um gateway por omissão se for gerido remotamente a partir de redes que não estão diretamente ligadas.
  - **Nota**: Relativamente ao gateway por omissão IPv6, uma vez que o switch receberá a informação do gateway por omissão de uma mensagem de anúncio de roteador (RA), não é necessário configurar manualmente o gateway por omissão IPv6.

Tarefa	Comandos IOS
Entre no modo de configuração global.	S1# **configure terminal**
Configure o gateway por omissão do switch.	S1(config)# **ip default-gateway 172.17.99.1**
Volte para o modo EXEC privilegiado.	S1(config-if)#**end**
Salve a configuração atual no **startup-config**	S1# **copy running-config startup-config**

Exemplo de Configuração da SVI do Switch (Cont.)

Step 3: **Verificar as configurações**

- Os comandos **show ip interface brief** e **show ipv6 interface brief** são úteis para determinar o estado das interfaces físicas e virtuais. A saída mostrada confirma que a interface VLAN 99 foi configurada com um endereço IPv4 e IPv6.

Nota: Um endereço IP aplicado ao SVI é apenas para acesso de gestão remoto do switch; isso não permite que o switch encaminhe pacotes da Camada 3.

```
S1# show ip interface brief
Interface      IP-Address      OK? Method   Status     Protocol
Vlan99         172.17.99.11    YES manual   down       down
(output omitted)
S1# show ipv6 interface brief
Vlan99                  [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::1
(output omitted)
```

1.2 Configurar Portas do Switch

Comunicação Duplex

- A comunicação full-duplex aumenta a eficiência da largura de banda, permitindo que ambas as extremidades de uma ligação transmitam e recebam dados simultaneamente. Isso também é conhecido como comunicação bidirecional e requer microssegmentação.
- Uma LAN microssegmentada é criada quando uma porta do switch tem apenas um dispositivo conectado e está operando no modo full-duplex. Não há domínio de colisão associado a uma porta de switch operando no modo full-duplex.
- Ao contrário da comunicação full-duplex, a comunicação half-duplex é unidirecional. A comunicação half-duplex cria problemas de desempenho porque os dados apenas podem fluir numa direção de cada vez, geralmente resultando em colisões.
- A Ethernet Gigabit e as NICs de 10 Gb requerem conexões full-duplex para operar. No modo full-duplex, o circuito de detecção de colisão na NIC está desativado. O full-duplex oferece 100% de eficiência em ambas as direções (transmissão e recepção). O que resulta numa duplicação do uso potencial da largura de banda declarada.

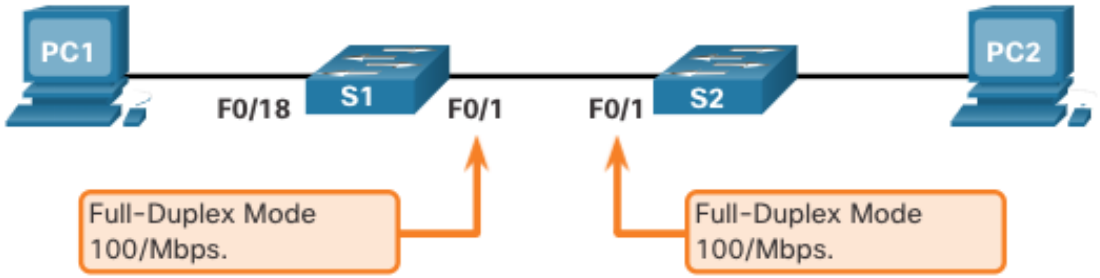
Configurar Portas de Switch na Camada Física

- As portas do switch podem ser configuradas manualmente com configurações de duplex e velocidade específicas. Os respectivos comandos de configuração de interface são **duplex** e **speed** .
- A configuração por omissão para duplex e velocidade para portas de switch nos switches Cisco Catalyst 2960 e 3560 é automática. As portas 10/100/1000 operam no modo half-duplex ou full-duplex quando estão definidas para 10 ou 100 Mbps e operam apenas no modo full-duplex quando está definido para 1000 Mbps (1 Gbps).
- A negociação automática é útil quando as configurações de velocidade e duplex de dispositivos desconhecidos. Na ligação de dispositivos conhecidos, como servidores, estações de trabalho dedicadas ou dispositivos de rede, uma prática recomendada é definir manualmente as configurações de velocidade e duplex.
- Na resolução de problemas de porta do switch, é importante que as configurações duplex e de velocidade sejam verificadas.

Nota: Configurações incompatíveis para o modo duplex ou para a velocidade das portas do switch podem causar problemas de conectividade. Falha de negociação automática cria configurações incompatíveis.

Todas as portas de fibra óptica, como as portas 1000BASE-SX, funcionam apenas numa velocidade predefinida e são sempre full-duplex

Configurar Portas do Switch na Camada Física (Cont.)



Tarefa	Comandos IOS
Entrar no modo de configuração global.	S1# **configure terminal**
Entrar no modo de configuração da interface.	S1(config)# **interface FastEthernet 0/1**
Configurar o duplex da interface.	S1(config-if)# **duplex full**
Configurar a velocidade da interface.	S1(config-if)# **speed 100**
Voltar para o modo EXEC privilegiado.	S1(config-if)#**end**
Salve a configuração atual no startup-config.	S1# **copy running-config startup-config**

Auto-MDIX

- Quando o automatic médium-dependente interface crossover (auto-MDIX) está habilitado, a interface do switch detecta automaticamente o tipo de ligação de cabo necessário (direto ou cruzado) e configura a ligação de forma adequada.
- Na ligação de switches sem o recurso auto-MDIX, os cabos straight-through (diretos) devem ser usados para ligar a dispositivos como servidores, estações de trabalho ou routers. Os cabos crossover (cruzados) devem ser usados para ligar a outros switches ou repetidores.
- Com o auto-MDIX habilitado, qualquer tipo de cabo pode ser usado para ligar a outros dispositivos e a interface irá ajustar-se automaticamente para uma comunicação bem-sucedida.
- Nos switches Cisco mais recentes, o comando **mdix auto** no modo de configuração de interface ativa esta característica. Ao usar o auto-MDIX **n**uma interface, a velocidade e o duplex da interface devem ser configurados para que o recurso funcione corretamente.

Nota: O recurso Auto-MDIX é ativado por omissão nos switches Catalyst 2960 e Catalyst 3560, mas não está disponível nos switches Catalyst 2950 e Catalyst 3550 mais antigos.

Para examinar a configuração Auto-MDIX para uma interface específica, use o comando **show controllers ethernet-controller** com a palavra-chave **phy** para examinar a configuração aoto-MDIX de uma interface específica. Usar o filtro **include Auto-MDIX,** para limitar a saída às linhas que fazem referência ao Auto-MDIX, .

Comandos de Verificação do Switch

Tarefa	Comandos IOS
Exibir o estado e a configuração da interface.	S1# **show interfaces** [*interface-id*]
Exibir a configuração atual no **startup-config**.	S1# **show startup-config**
Exibir a configuração atual no **running-config**.	S1# **show running-config**
Exibir informações sobre o sistema de ficheiros da memória flash.	S1# **show flash**
Exibir o estado do hardware e software do sistema.	S1# **show version**
Exibe o histórico dos comando digitados.	S1# **show history**
Exibir informações IP numa interface.	S1# **show ip interface** [*interface-id*] OU S1# **show ipv6 interface** [*interface-id*]
Exibir a tabela de endereços MAC.	S1# **show mac-address-table** OU S1# **show mac address-table**

Verificar a configuração das portas do switch

O comando **show running-config** pode ser usado para verificar se o switch foi configurado corretamente. A partir da saída abreviada da amostra em S1, algumas informações importantes são mostradas na figura:

- A interface VLAN foi configurada com a VLAN de Gestão com o ID 99
- A VLAN 99 configurada com o endereço IPv4 e máscara de sub-rede 172.17.99.11 255.255.255.0
- O switch foi configurado com o default gateway 172.17.99.1

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
(output omitted)
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

Verificar a configuração das portas do switch (Cont.)

O comando **show interfaces** é outro comando usado frequentemente, que permite visualizar informações do estado e estatísticas das interfaces de rede do switch. O comando **show interfaces** é frequentemente usado ao configurar e monitorizar dispositivos de rede.

A primeira linha da saída para o comando **show interfaces FastEthernet 0/18** indica que a interface FastEthernet 0/18 está up/up, o que significa que está operacional. Mais abaixo, a saída mostra que o duplex está full-duplex e a velocidade é de 100 Mbps.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

Problemas na camada de acesso à rede

A saída do comando **show interfaces** é útil para detectar problemas frequentes no meio físico. Uma das partes mais importantes dessa saída é a apresentação do estado do protocolo de linha e da ligação de dados, conforme mostrado no exemplo.

O primeiro parâmetro (FastEthernet0/18 está ativo) refere-se à camada de hardware e indica se a interface está recebendo um sinal de detecção de portadora. O segundo parâmetro (line protocol is up) refere-se à camada de ligação de dados e indica se os protocolos keepalive da camada de ligação de dados estão a ser recebidos. Com base na saída do comando **show interfaces**, possíveis problemas podem ser corrigidos da seguinte forma:

- Se a interface estiver ativa e o protocolo de linha estiver inativo, existe um problema. Pode haver uma incompatibilidade de tipo de encapsulamento, a interface na outra extremidade pode estar desativada por erro ou pode haver um problema de hardware.
- Se o protocolo de linha e a interface estiverem ambos desligados, um cabo não está ligado ou existe algum outro problema de interface. Por exemplo, numa ligação back-to-back, a outra extremidade da conexão pode estar administrativamente inativa.
- Se a interface estiver administrativamente desativada, ela foi desativada manualmente (o comando **shutdown** foi emitido) na configuração ativa.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW
100000 Kbit/sec, DLY 100 usec,
```

Problemas da camada de acesso à rede (Cont.)

A saída do comando **show interfaces** apresenta contadores e estatísticas para a interface FastEthernet0/18, conforme mostrado aqui:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2295197 packets input, 305539992 bytes, 0 no buffer
     Received 1925500 broadcasts (74 multicasts)
     0 runts, 0 giants, 0 throttles
     3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 74 multicast, 0 pause input
     0 input packets with dribble condition detected
     3594664 packets output, 436549843 bytes, 0 underruns
     8 output errors, 1790 collisions, 10 interface resets
     0 unknown protocol drops
     0 babbles, 235 late collision, 0 deferred
```

Problemas da camada de acesso à rede (Cont.)

Alguns erros no meio físico não são graves o suficiente para fazer com que o circuito falhe, mas causam problemas de desempenho da rede. A tabela explica alguns desses erros comuns que podem ser detectados usando o comando **show interfaces**.

Tipo de erro	Descrição
Erros de Input	Número total de erros. Inclui contagem de runts, giants, CRC, no buffer, frame, overrun e ignored.
Runts	Pacotes que são descartados porque são menores que o tamanho mínimo permitido de pacote para o meio físico. Por exemplo, qualquer pacote Ethernet com menos de 64 bytes é considerado um runt.
Giants	Pacotes que são descartados porque excedem o tamanho máximo permitido do pacote para o meio físico. Por exemplo, qualquer pacote Ethernet maior que 1.518 bytes é considerado um giant.
CRC	Erros de CRC são gerados quando o checksum calculado não é igual ao checksum recebido.
Erros de output	Soma de todos os erros que impediram a transmissão final dos datagramas a partir da interface que está a ser examinada.
Colisions	Número de mensagens retransmitidas devido a uma colisão Ethernet.
Late Collisions	Uma colisão ocorre após 512 bits do quadro terem sido transmitidos.

Erros de Entrada e Saída na Interface

"Erros de entrada" é a soma de todos os erros nos datagramas recebidos na interface que está sendo examinada. Isso inclui contagem de runts, giants, CRC, no buffer, frame, overrun e ignored. Os erros de entrada relatados pelo comando **show interfaces** incluem o seguinte:

- **Runt Frames** - quadros Ethernet que são mais curtos do que o comprimento mínimo permitido de 64 bytes são chamados de runts. NICs com funcionamento inadequado normalmente são a causa de quadros runt em excesso, mas sua causa também pode ter origem em colisões.
- **Giants** - os quadros Ethernet maiores que o tamanho máximo permitido são chamados gigantes.
- **CRC errors** - em interfaces Ethernet e serial, os erros CRC geralmente indicam um erro do meio físico ou cabo. As causas mais comuns incluem interferência elétrica, conexões soltas ou danificadas ou cablagem incorreta. Se houver muitos erros de CRC, há muito ruído no link, e você deve verificar o cabo. Também devem ser procuradas as causas do ruído e eliminá-las.

Erros de Entrada e Saída da Interface (Cont.)

"Erros de saída" refere-se à soma de todos os erros que impediram a transmissão final de datagramas para fora da interface que está sendo examinada. Os erros de saída relatados pelo comando **show interfaces** incluem o seguinte:

- **Collisions** - Colisões no funcionamento em half-duplex são normais. No entanto, jamais haverá colisões numa interface configurada para a comunicação de full-duplex.
- **Late collisions** - Uma colisão tardia refere-se a uma colisão que ocorre depois de 512 bits do quadro terem sido transmitidos. Comprimentos excessivos de cabos são a causa mais comum de colisões tardias. Outra causa comum é a configuração incorreta de duplex.

Solucionando problemas da camada de acesso à rede

Para solucionar problemas de cenários que não envolvem ligações ou ligações ruins entre um switch e outro dispositivo, siga o processo geral mostrado na figura.

1.3 Acesso Remoto Seguro

Acesso com Telnet

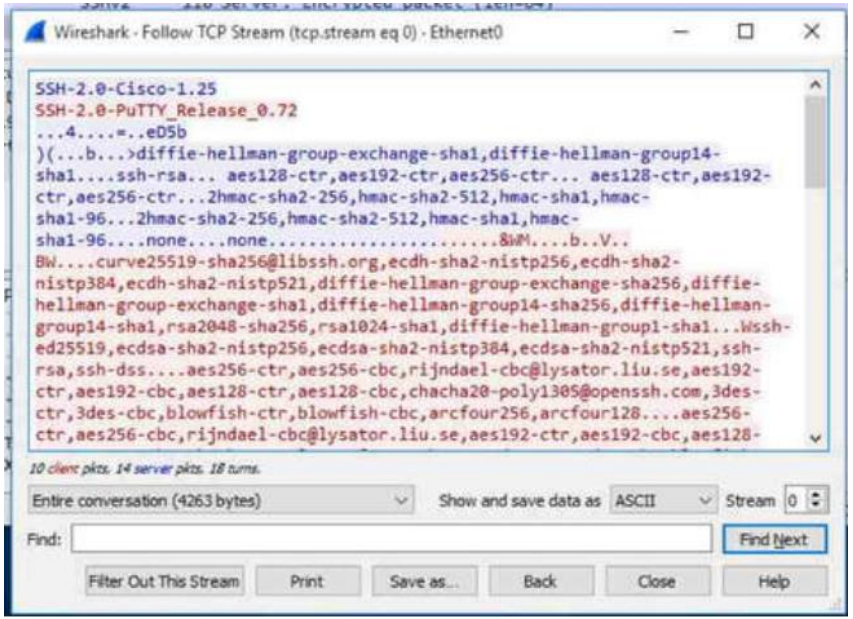
O Telnet usa a porta 23. É um protocolo mais antigo que utiliza transmissão não segura de texto sem encriptação da autenticação (nome de utilizador e password) e dos dados transmitidos entre os dispositivos de comunicação.

Um ator ameaça pode monitorizar pacotes usando o Wireshark. Por exemplo, na figura, o ator de ameaça capturou o nome de utilizador **admin** e password **ccna** de uma sessão Telnet.

Acesso com SSH

O Secure Shell (SSH) é um protocolo seguro que usa a porta TCP 22. Ele fornece uma conexão de gestão segura (encriptada) a um dispositivo remoto. O SSH deve substituir o Telnet nas conexões de gestão. O SSH fornece segurança para conexões remotas, fornecendo encriptação forte quando um dispositivo é autenticado (nome de utilizador e password) e também para os dados transmitidos entre os dispositivos que comunicam.

A figura mostra uma captura do Wireshark de uma sessão SSH. O ator de ameaça pode rastrear a sessão usando o endereço IP do dispositivo administrador. No entanto, ao contrário do Telnet, com SSH o nome de utilizador e password são encriptados.



Verificar se o switch suporta SSH

Para habilitar o SSH num switch Catalyst 2960, o switch deve ter uma versão do software IOS, que inclua recursos de encriptação. Use o comando **show version** no switch para ver qual a versão do IOS o switch está a executar no momento. Um nome de ficheiro IOS que inclui a combinação “k9” suporta recursos e recursos de encriptação.

O exemplo mostra a saída do comando **show version** .

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE
(fc1)
```

Configurar o SSH

Antes de configurar o SSH, o switch deve ser minimamente configurado com as definições corretas de um nome de host exclusivo e de conectividade de rede.

Etapa 1: Verificar o suporte SSH - Use o comando **show ip ssh** para verificar se o switch suporta SSH. Se o switch não estiver executando um IOS que ofereça suporte a recursos de encriptação, esse comando não será reconhecido.

Etapa 2: Configurar o domínio IP - Configure o nome de domínio IP da rede usando o comando **ip domain-name** *domain-name* no modo de configuração global.

Etapa 3: Gerar pares de chaves RSA - Gerar um par de chaves RSA habilita automaticamente o SSH. Use o comando **crypto key generate rsa** no modo de configuração global para ativar o servidor SSH no switch e gerar um par de chaves RSA.

Nota: Para excluir o par de chaves RSA, use o comando **crypto key zeroize rsa** no modo de configuração global. Quando o par de chaves RSA é excluído, o servidor SSH é desabilitado automaticamente.

Etapa 4: Configurar autenticação de utilizador - O servidor SSH pode autenticar utilizadores localmente ou usando um servidor de autenticação. Para usar um utilizador local, é necessário criar um utilizador use o comando **username** *username* **secret** *password* no modo de configuração global.

Passo 5: Configurar as linhas vty - Habilite o protocolo SSH nas linhas vty usando o comando **transport input ssh** no modo de configuração de linha. Use o comando **line vty** no modo de configuração global e, em seguida, o comando **login local** no modo de configuração de linha para exigir autenticação local para conexões SSH usando a base de dados local de utilizadores.

Etapa 6: Ativar SSH versão 2 - Por padrão, SSH suporta ambas as versões 1 e 2. Ao suportar ambas as versões, isso é mostrado na saída **show ip ssh** como suportando a versão 2. Ative a versão SSH usando o comando de configuração global **ip ssh versão 2**.

Verificar a Operacionalidade do SSH

Num PC, usar um cliente SSH, como PuTTY, para conectar a um servidor SSH. Por exemplo, suponha que o seguinte esteja configurado:

- SSH está habilitado no switch S1
- Interface VLAN 99 (SVI) com endereço IPv4 172.17.99.11 no switch S1
- PC1 com endereço IPv4 172.17.99.21

Usando um emulador de terminal, inicie uma conexão SSH com o endereço IPv4 SVI VLAN de S1 a partir de PC1.

Quando conectado, o utilizador é solicitado a fornecer um nome de utilizador e password, conforme mostrado no exemplo. Usando a configuração do exemplo anterior, o nome de utilizador **admin** e password **ccna** são inseridos. Depois de inserir a combinação correta, o utilizador é conectado via SSH à interface de linha de comando (CLI) no switch Catalyst 2960.

```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

Verificar a Operacionalidade do SSH (cont.)

Para exibir a versão e a configuração do SSH num dispositivo que foi configurado com um servidor de SSH, usar o comando show ip ssh No exemplo, SSH versão 2 está habilitado.

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started       admin
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started       admin
S1#
```

1.4 Configuração básica do router

Definir configurações básicas do router

Routers e switches Cisco têm muito em comum. Eles suportam um sistema operativo modal semelhante, estruturas de comando semelhantes e muitos dos mesmos comandos. Além disso, os dois dispositivos têm etapas semelhantes de configuração inicial. Por exemplo, as seguintes tarefas de configuração devem ser sempre executadas. Nomeie o dispositivo para distingui-lo de outros routers e configure passwords, conforme mostrado no exemplo.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

Configurar Definições Básicas do Router (Cont.)

Configure um banner para fornecer uma notificação legal de acesso não autorizado, conforme mostrado no exemplo.

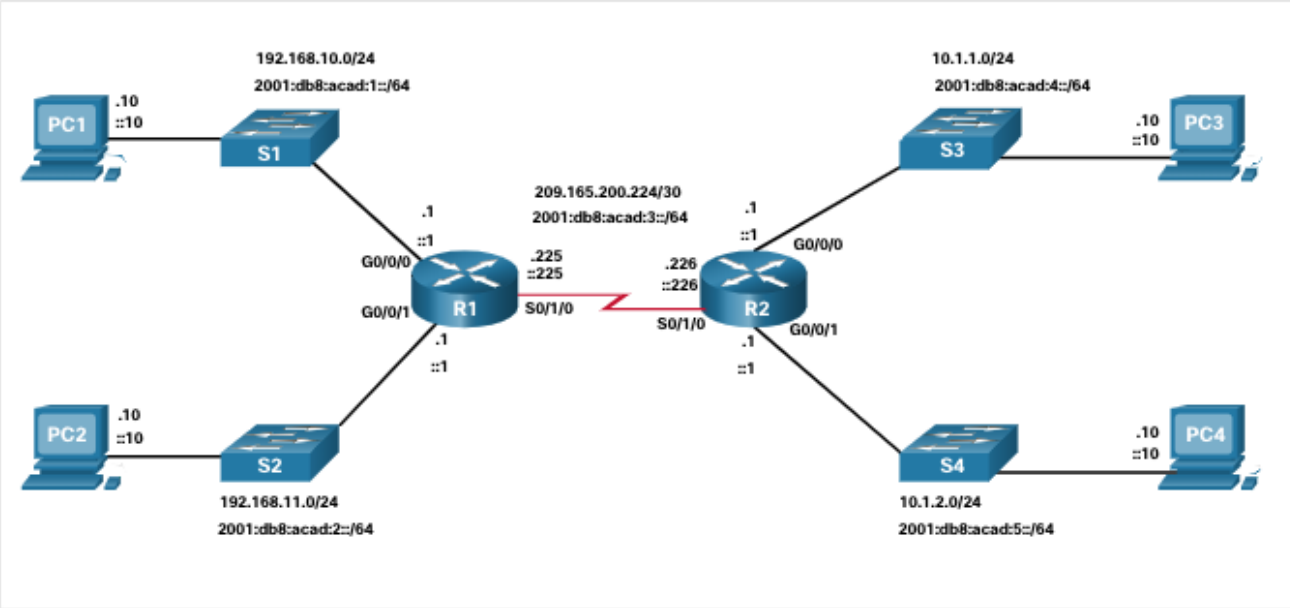
```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Salve as alterações num router, conforme mostrado no exemplo.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Topologia de Pilha Dupla

Um recurso diferenciador entre switches e routers é o tipo de interfaces suportadas por cada um. Por exemplo, os switches da camada 2 suportam LANs; portanto, eles têm várias portas FastEthernet ou Gigabit Ethernet. A topologia de pilha dupla na figura é usada para demonstrar a configuração das interfaces IPv4 e IPv6 do router.



Configurar interfaces do router

Os routers suportam LANs e WANs e podem interconectar diferentes tipos de redes; portanto, suportam muitos tipos de interfaces. Por exemplo, ISRs G2 têm uma ou duas interfaces Gigabit Ethernet integradas e slots High-Speed WAN Interface Card (HWIC) para acomodar outros tipos de interfaces de rede, incluindo serial, DSL e as interfaces do cabo.

Para estar disponível, uma interface deve estar:

- **Configurado com pelo menos um endereço IP** - Use os comandos **ip address** *ip-address sub-net-mask* e **ipv6 address** *ipv6-address/prefix* no modo de configuração de interface.
- **Ativado** - Por defeito, as interfaces LAN e WAN não são ativadas **(shutdown).** Para ativar uma interface deve ser usado o comando **no shutdown**. A interface também deve ser conectada a outro dispositivo (hub, switch ou outro router) para que a camada física esteja ativa.
- **Descrição** - Opcional, a interface deve configurada com uma pequena descrição com no máximo 240 caracteres. É uma boa prática configurar uma descrição em cada interface. Nas redes de produção, os benefícios das descrições de interface são percebidos rapidamente, pois são úteis na solução de problemas e na identificação de uma conexão e informações de contato de terceiros.

Configurar Interfaces do Router (Cont.)

O exemplo mostra a configuração para as interfaces em R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Interfaces de loopback IPv4

Outra configuração comum nos routers Cisco IOS é a ativação de uma interface de loopback.

- A interface de loopback é uma interface lógica interna ao router. Não está atribuído a uma porta física e nunca pode ser conectado a nenhum outro dispositivo. É considerada uma interface de software que é colocada automaticamente em um estado “up”, desde que o router esteja a funcionar.
- A interface de loopback é útil para testar e gerir um dispositivo Cisco IOS, pois assegura que pelo menos uma interface esteja sempre disponível. Por exemplo, ela pode ser usada para fins de teste, como o teste de processos de encaminhamentos internos, com a emulação de redes atrás do router.
- As interfaces de loopback também são comumente usadas em ambientes de laboratório para criar interfaces adicionais. Por exemplo, você pode criar várias interfaces de loopback num router para simular mais redes para fins de prática de configuração e teste. O endereço IPv4 de cada interface de loopback deve ser exclusivo e não utilizado por nenhuma outra interface. Neste currículo, muitas vezes usamos uma interface de loopback para simular um link para a internet.
- Permitir e atribuir um endereço de loopback é simples:

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
```

1.5 Verificar Redes Diretamente Ligadas

Comandos de Verificação da Interface

Existem vários comandos **show** que podem ser usados para verificar o funcionamento e a configuração de uma interface.

Os seguintes comandos são especialmente úteis para identificar rapidamente o estado de uma interface:

- **show ip interface brief** e **show ipv6 interface brief** - Exibem um resumo para todas as interfaces, incluindo o endereço IPv4 ou IPv6 da interface e o estado de funcionamento atual.
- **show running-config** *interface-id* da interface - Exibe os comandos aplicados à interface especificada.
- **show ip route** e **show ipv6 route** para ver o conteúdo da tabela de encaminhamento IPv4 ou IPv6 armazenada na RAM. No Cisco IOS 15, as interfaces ativas devem aparecer na tabela de encaminhamento com duas entradas relativas identificadas pelo código **'C'** (Conectado) ou **'L'** (Local). Nas versões anteriores do IOS, aparece apenas uma entrada com o código '**C**'.

Verificar estado da interface

A saída dos comandos **show ip interface brief** e **show ipv6 interface brief** podem ser usados para apresentar rapidamente o estado de todas as interfaces num router. Você pode verificar se as interfaces estão ativas e a funcionar conforme indicado pelo Status de “up” e Protocol de “up”, conforme mostrado no exemplo. Uma saída diferente indicaria um problema de configuração

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::7279:B3FF:FE92:3131
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]     Unassigned
```

Verificar Endereços Local e de Multicast numa Ligação IPv6

A saída do comando **show ipv6 interface brief** exibe dois endereços IPv6 configurados por interface. Um endereço é o endereço IPv6 unicast global que foi inserido manualmente. O outro endereço, que começa com FE80, é o endereço unicast link local para a interface. Um endereço link local será automaticamente adicionado a uma interface sempre que um endereço unicast global for atribuído. Uma interface de rede IPv6 é necessária para ter um endereço link local, mas não necessariamente um endereço unicast global.

O comando **show ipv6 interface gigabitethernet 0/0/0** exibe o estado da interface e todos os endereços IPv6 pertencentes à interface. Juntamente com o endereço local do link e o endereço unicast global, a saída inclui os endereços multicast atribuídos à interface, começando com o prefixo FF02, conforme mostrado no exemplo.

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

Verificar a configuração da interface

A saída do comando **show running-config interface** apresenta os comandos atuais aplicados à interface especificada, conforme mostrado.

Os dois comandos seguintes são utilizados para recolher informações mais detalhadas da interface:

- **show interfaces** - Exibe informações da interface e contagem de fluxo de pacotes para todas as interfaces no dispositivo.
- **show ip interface** e **show ipv6 interface** - Exibe as informações relacionadas ao IPv4 e IPv6 para todas as interfaces em um router.

```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

Verificar rotas

A saída dos comandos **show ip route** e **show ipv6 route** revelam as três entradas de rede diretamente conectadas e as três entradas de interface rota de host local, conforme mostrado no exemplo.

A rota do host local tem uma distância administrativa de 0. Também tem uma máscara de /32 para IPv4 e uma máscara de /128 para IPv6. A rota do host local é uma rota para uma interface do router que possui endereço IP. É usada para permitir que o router processe os pacotes destinados a esse IP.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Verificar rotas (cont.)

Um **'C'** ao lado de uma rota na tabela de encaminhamento indica que esta é uma rede diretamente conectada . Quando a interface do router é configurada com um endereço unicast global e está no estado "up / up", o prefixo IPv6 e o comprimento do prefixo são adicionados à tabela de encaminhamento IPv6 como uma rota conectada.

O endereço unicast global do IPv6 aplicado à interface também é instalado na tabela de encaminhamento como uma rota local. A rota local tem um prefixo /128. As rotas locais são usadas pela tabela de encaminhamento para processar, de modo eficiente, pacotes com o endereço da interface do router como destino.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Filtro de saída do comando Show

Por omissão, os comandos que geram várias ecrãs de saída são paradas após 24 linhas. No final da saída parada, o texto --More-- é apresentado. Pressione **Enter** para apresentar a próxima linha e pressionar a barra de espaço apresentar o próximo conjunto de linhas. Use o comando **terminal length** para especificar o número de linhas a serem apresentadas. Um valor de 0 (zero) impede o router de parar entre as ecrãs de saída.

Outro recurso muito útil que melhora a experiência do utilizador na CLI é a filtragem apresentação da saída. Os comandos de filtragem podem ser usados para apresentar seções específicas de saída. Para ativar o comando de filtragem, insira o caracter(**|**) depois do comando **show** e, em seguida, insira um parâmetro de filtragem e uma expressão de filtragem.

Existem quatro parâmetros de filtragem que podem ser configurados após o pipe (**|**):

- **section** - Mostra a seção inteira que começa com a expressão de filtragem.
- **include** - Inclui todas as linhas de saída que correspondem à expressão de filtragem.
- **exclude** - Exclui todas as linhas de saída que correspondem à expressão de filtragem.
- **begin** - Mostra todas as linhas de saída de um certo ponto, começando com a linha que corresponde à expressão de filtragem

Histórico de Comandos

O recurso ao histórico de comandos é útil porque armazena temporariamente a lista de comandos executados e que podem ser reutilizados.

- Para reutilizar comandos do buffer do histórico, pressione **Ctrl+P** ou a tecla **Seta para Cima** . A saída do comando começa com o comando mais recente. Repita a sequência de teclas para lembrar dos comandos mais antigos sucessivamente. Para retornar aos comandos mais recentes no buffer do histórico, pressione **Ctrl+N** ou a tecla **Seta para Baixo** . Repita a sequência de teclas para lembrar dos comandos mais recentes sucessivamente.
- Por omissão, o histórico de comandos está ativo e o sistema registra as últimas 10 linhas de comando no seu buffer de histórico. Use o comando no modo EXEC privilegiado **show history** para exibir o conteúdo do buffer.
- Também é prático aumentar o número de linhas de comando que o buffer de histórico regista durante a sessão do terminal atual apenas. Use o comando no modo EXEC privilegiado **terminal history size** para aumentar ou diminuir o tamanho do buffer.

1.6 - Sumário

O que aprendi neste módulo?

- Quando um switch Cisco é ligado, ele passa por uma sequência de inicialização de cinco etapas.
- A variável de ambiente BOOT é definida usando o comando de modo de configuração global do sistema de inicialização.
- Use os LEDs do switch para monitorizar a atividade e o desempenho do switch: SYST, RPS, STAT, DUPX, SPEED e PoE.
- O carregador de inicialização (boot loader) fornece acesso ao switch se o sistema operativo não puder ser usado devido a ficheiros de sistema ausentes ou danificados.
- Para preparar um switch para acesso de gestão remoto, o switch deve ser configurado com um endereço IP e uma máscara de sub-rede.
- Para gerir o switch a partir de uma rede remota, o switch deve ser configurado com um gateway por omissão.
- A comunicação full-duplex aumenta a largura de banda efetiva, permitindo que ambas as extremidades de uma conexão transmitam e recebam dados simultaneamente.
- As portas do switch podem ser configuradas manualmente com configurações de duplex e velocidade específicas.
- Use a negociação automática quando as configurações de velocidade e duplex do dispositivo que se conecta à porta forem desconhecidas ou podem ser alteradas.
- Quando o auto-MDIX está ativado, a interface detecta automaticamente o tipo de conexão de cabo necessário (direto ou cruzado) e configura a conexão adequadamente.

O que aprendi neste módulo? (Cont.)

- Existem vários comandos **show** a serem usados ao verificar as configurações do switch.
- O Telnet (usando a porta TCP 23) é um protocolo mais antigo que utiliza transmissão de texto sem segurança da autenticação de login (nome de utilizador e password) e dos dados transmitidos entre os dispositivos de comunicação.
- O SSH (usando a porta TCP 22) fornece segurança para conexões remotas, fornecendo encriptação forte quando um dispositivo é autenticado (nome de utilizador e password) e também para os dados transmitidos entre os dispositivos que se comunicam.
- Um nome de ficheiro do IOS que inclui a combinação “k9” suporta recursos e recursos de encriptação.
- Para configurar o SSH, você deve verificar se o switch o suporta, configurar o domínio IP, gerar pares de chaves RSA, configurar a autenticação de uso, configurar as linhas VTY e habilitar o SSH versão 2.
- Para verificar se o SSH está operacional, use o comando **show ip ssh** para exibir os dados de versão e configuração do SSH no dispositivo.
- As seguintes tarefas de configuração inicial devem sempre ser executadas: nomeie o dispositivo para distingui-lo de outros routers e configure passwords, configure um banner para fornecer notificação legal de acesso não autorizado e salve as alterações num router.

O que aprendi neste módulo? (Cont.)

- Um recurso diferenciador entre switches e routers é o tipo de interfaces suportadas por cada um.
- Os routers suportam LANs e WANs e podem interconectar diferentes tipos de redes; portanto, suportam muitos tipos de interfaces.
- A interface de loopback IPv4 é uma interface lógica interna ao router. Não está atribuída a uma porta física e nunca pode ser conectada a nenhum outro dispositivo.
- Use os seguintes comandos para identificar rapidamente o estado de uma interface:
  - **show ip interface brief** e **show ipv6 interface brief** para ver o resumo de todas as interfaces (endereços IPv4 e IPv6 e estado operacional),
  - **show running-config interface *interface-id*** para ver os comandos aplicados a uma interface especificada
  - **show ip route** e **show ipv6 route** para ver o conteúdo da tabela de encaminhamento IPv4 ou IPv6 armazenada na RAM.
- Filtrar a saída do comando show usando o caractere pipe (|). Use expressões de filtro: section, include, exclude e begin.
- Por omissão, o histórico de comandos está ativado e o sistema captura as últimas 10 linhas de comando em seu buffer de histórico.
- Use o comando no modo EXEC privilegiado **show history** para exibir o conteúdo do buffer.