Capítulo 2: Princípios das redes comutadas

Roteamento e Switching

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 2

2.0 Introdução

2.1 Configuração Básica de Switch

2.2 Segurança de switch: Gerenciamento e implementação

Capítulo 2: Objetivos

- Exemplificar as vantagens e desvantagens do roteamento estático
- Configurações iniciais em um switch Cisco
- Configurar as portas de switch para atender aos requisitos de rede
- Configurar a interface virtual de gerenciamento do switch
- Descrever ataques básicos à segurançaem um ambiente comutado
- Descrever as práticas recomendadas de segurança em um ambiente comutado
- Configurar o recurso de segurança da porta para restringir o acesso de dispositivos à rede

Sequência de inicialização de switch

1. POST
2. Executar o software carregador de inicialização
3. O carregador de inicialização executa a inicialização de CPU de baixo nível
4. O carregador de inicialização inicializa o sistema de arquivos flash
5. O carregador de inicialização localiza e carrega uma imagem de software de sistema operacional IOS padrão na memória e assume o controle do switch no IOS.

Sequência de inicialização de switch

Para localizar uma imagem do IOS apropriada, o switch passa pelas seguintes etapas:

1. Tenta inicializar automaticamente usando as informações na variável de ambiente BOOT
2. Se essa variável não estiver definida, o switch realiza uma pesquisa de cima para baixo pelo sistema de arquivos flash. Carregará e executará o primeiro arquivo executável, se possível.
3. O sistema operacional IOS então inicializa as interfaces usando os comandos do IOS Cisco encontrados no arquivo de configuração, a configuração de inicialização, armazenado na NVRAM.

Observação: o comando **boot system** pode ser usado para definir a variável de ambiente BOOT.

Recuperando-se de uma falha do sistema

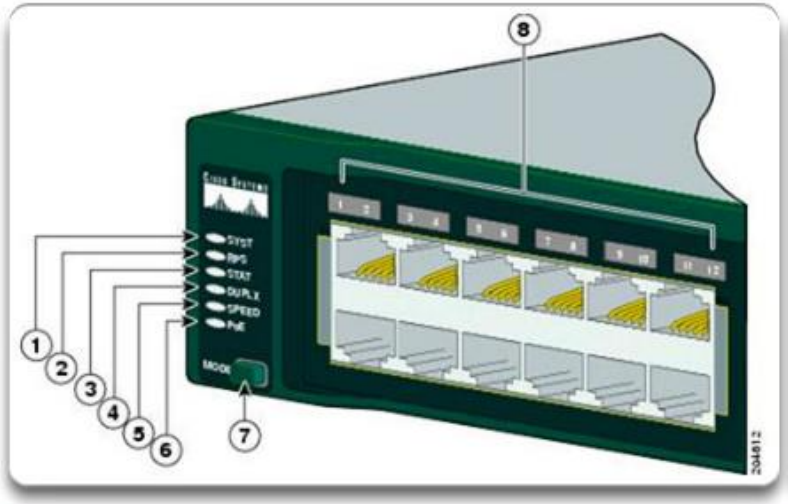
- O carregador de inicialização também pode ser usado para gerenciar o switch se o IOS não puder ser carregado.
- O carregador de inicialização poderá ser acessado por meio de uma conexão de console da seguinte forma:
  1. Conecte um PC por cabo de console à porta do console do switch. Desconecte o cabo de alimentação do switch.
  2. Reconecte o cabo de alimentação ao switch e pressione e segure o botão **Mode**.
  3. O LED do sistema muda rapidamente para a cor âmbar e depois para verde sólido. Solte o botão **Mode**.
- O carregador de inicialização **switch:prompt** aparece no software de emulação de terminal no PC.

Indicadores de LED do switch

- Cada porta nos switches Cisco Catalyst tem luzes indicadoras de LED de status.
- Por padrão, essas luzes de LED refletem a atividade da porta, mas também podem fornecer outras informações sobre o switch através do botão **Modo**
- Os seguintes modos estão disponíveis nos switches Cisco Catalyst 2960:
  - LED de Sistema
  - LED RPS (sistema de alimentação redundante)
  - LED de Status das Portas
  - LED Duplex de Porta
  - LED de Velocidade da Porta
  - LED do modo Power Over Ethernet (PoE)

Indicadores de LED do switch

- Modos do switch Cisco Catalyst 2960



Leds do switch Catalyst 2960

1	O LED do sistema	5	O LED de velocidade de porta
2	O LED de RPS (se o RPS for suportado no switch)	6	O LED de status do PoE (se PoE for suportado no switch)
3	O LED de status das portas (este é o modo padrão.)	7	O botão Mode
4	O LED de modo de porta duplex	8	Os LEDs de porta

Preparar-se para o gerenciamento de switch básico

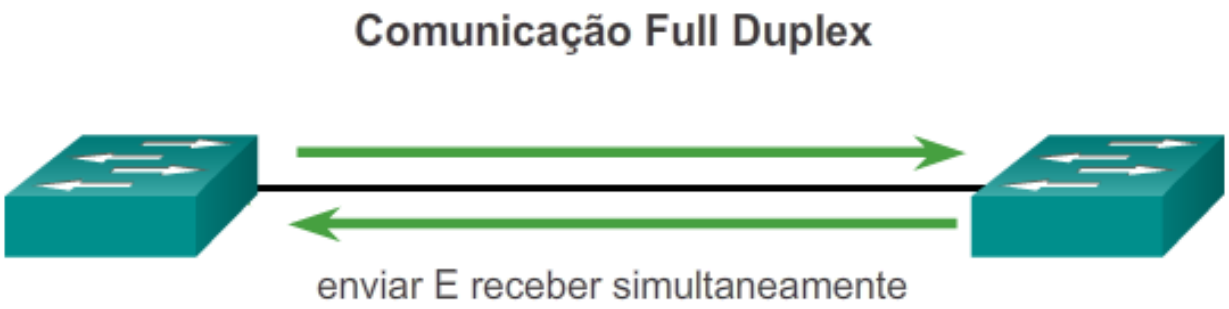
- Para gerenciar remotamente um switch Cisco, ele deve ser configurado para acessar a rede
- Um endereço IP e uma máscara de sub-rede devem ser configurados
- Se você estiver gerenciando o switch de uma rede remota, um gateway padrão também deverá ser configurado
- As informações de IP (endereço, máscara de sub-rede, gateway) devem ser atribuídas a uma SVI (interface virtual de switch) do switch
- Embora essas configurações IP permitam o gerenciamento remoto e o acesso remoto ao switch, elas não permitem que o switch roteie pacotes da camada 3.

Preparar-se para o gerenciamento de switch básico

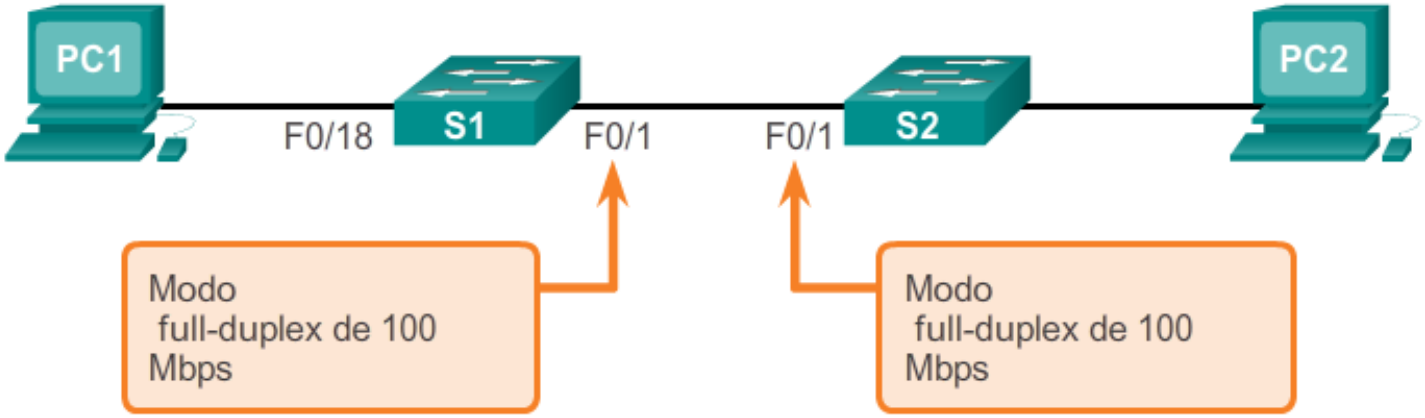
Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Entre no modo de configuração da interface para SVI.	`S1(config)# interface vlan 99`
Configure o endereço IP da interface de gerenciamento.	`S1(config-if)# ip address 172.17.99.11 255.255.0.0`
Ative a interface de gerenciamento.	`S1(config-if)# no shutdown`
Volte para o modo EXEC privilegiado.	`S1(config-if)# end`
Salve a configuração atual na configuração de inicialização.	`S1# copy running-config startup-config`

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

Comunicação duplex



Configurar portas de switch na camada física



Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Entre no modo de configuração da interface.	`S1(config)# interface FastEthernet 0/1`
Configure o duplex da interface.	`S1(config-if)# duplex full`
Configure a velocidade da interface.	`S1(config-if)# speed 100`
Volte para o modo EXEC privilegiado.	`S1(config-if)# end`
Salve a configuração atual na configuração de inicialização.	`S1# copy running-config startup-config`

Recurso de MDIX automático

- Certos tipos de cabo (direto ou cruzado) eram necessários para conectar dispositivos
- O recurso cruzado de interface dependente do meio automático (MDIX automático) elimina esse problema
- Quando o MDIX automático está ativado, a interface automaticamente detecta e configura a conexão adequadamente
- Quando o MDIX automático é usado em uma interface, a velocidade da interface e o duplex devem ser definidos como **automático**

Recurso de MDIX automático

Verificação de MDIX automático

Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Entre no modo de configuração da interface.	`S1(config)# interface fastethernet 0/1`
Configure a interface para negociar automaticamente o duplex com o dispositivo conectado.	`S1(config-if)# duplex auto`
Configure a interface para negociar automaticamente a velocidade com o dispositivo conectado	`S1(config-if)# speed auto`
Ative o MDIX automático na interface de WAN.	`S1(config-if)# mdix auto`
Volte para o modo EXEC privilegiado.	`S1(config-if)# end`
Salve a configuração atual na configuração de inicialização.	`S1# copy running-config startup-config`

Recurso de MDIX automático


```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Verificando a configuração de porta de switch

Comandos de verificação

Comandos do switch Cisco IOS	
Exibir o status e a configuração da interface.	S1# **show interfaces** [*interface-id*]
Exibir a configuração atual de inicialização.	S1# **show startup-config**
Exibir a configuração de trabalho atual.	S1# **show running-config**
Exibir informações sobre o sistema de arquivos da memória flash.	S1# **show flash**
Exibir o status de hardware e software do sistema.	S1# **show version**
Exibir o histórico dos comandos inseridos.	S1# **show history**
Exibir informações de IP sobre uma interface.	S1# **show ip** [*interface-id*]
Exibir a tabela de endereços MAC.	S1# **show mac-address-table** OU S1# **show mac address-table**

Problemas da camada de acesso à rede

Exiba o status e as estatísticas da interface

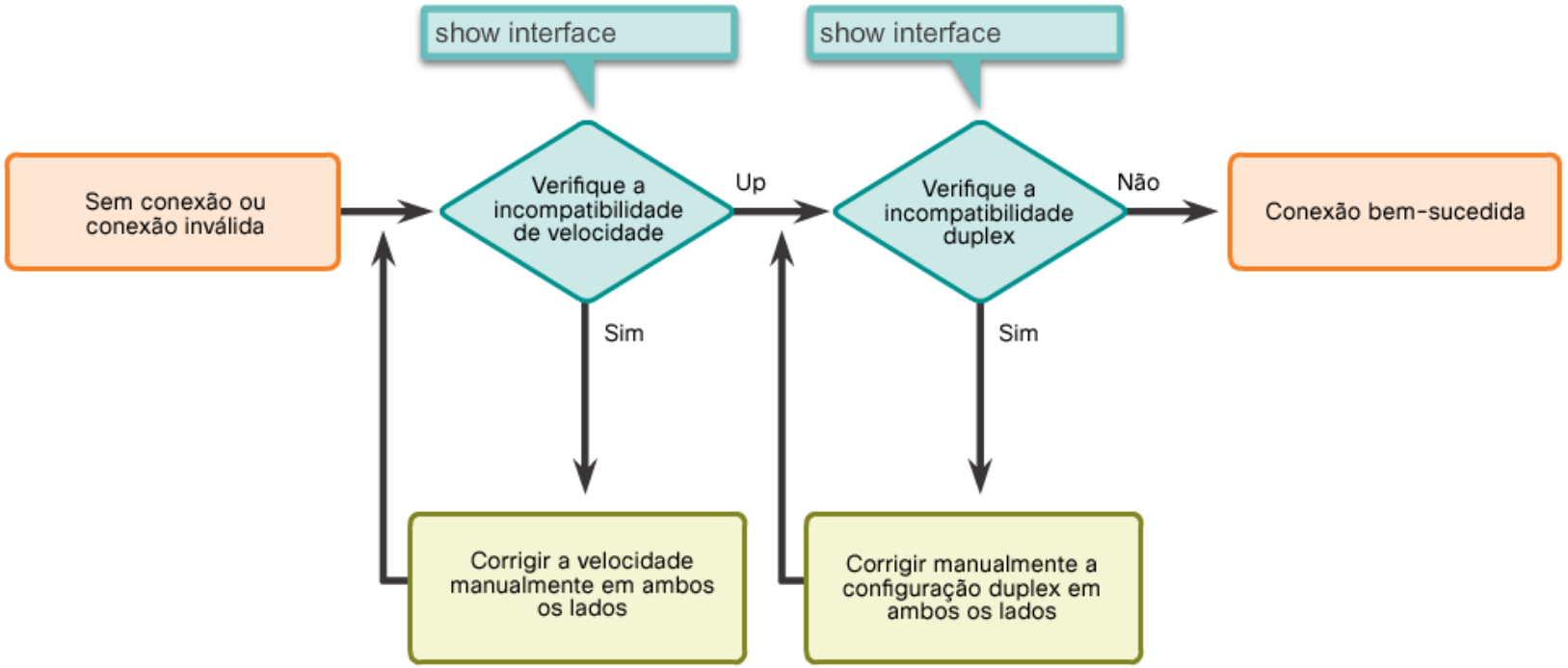
```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<saída omitida>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 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
<saída omitida>
```

Problemas da camada de acesso à rede

Tipo de erro	Descrição
Input Errors	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 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 do pacote para a mídia. Por exemplo, qualquer pacote Ethernet maior que 1.518 bytes é considerado um giant.
CRC	Os erros de CRC são gerados quando o checksum calculado não é igual ao checksum recebido.
Output Errors	Soma de todos os erros que impediram a transmissão final dos datagramas a partir da interface que está sendo examinada.
Collisions	Número de mensagens retransmitidas devido a uma colisão Ethernet.
Late Collisions	Um período que ocorre depois que 512 bits do quadro foram transmitidos.

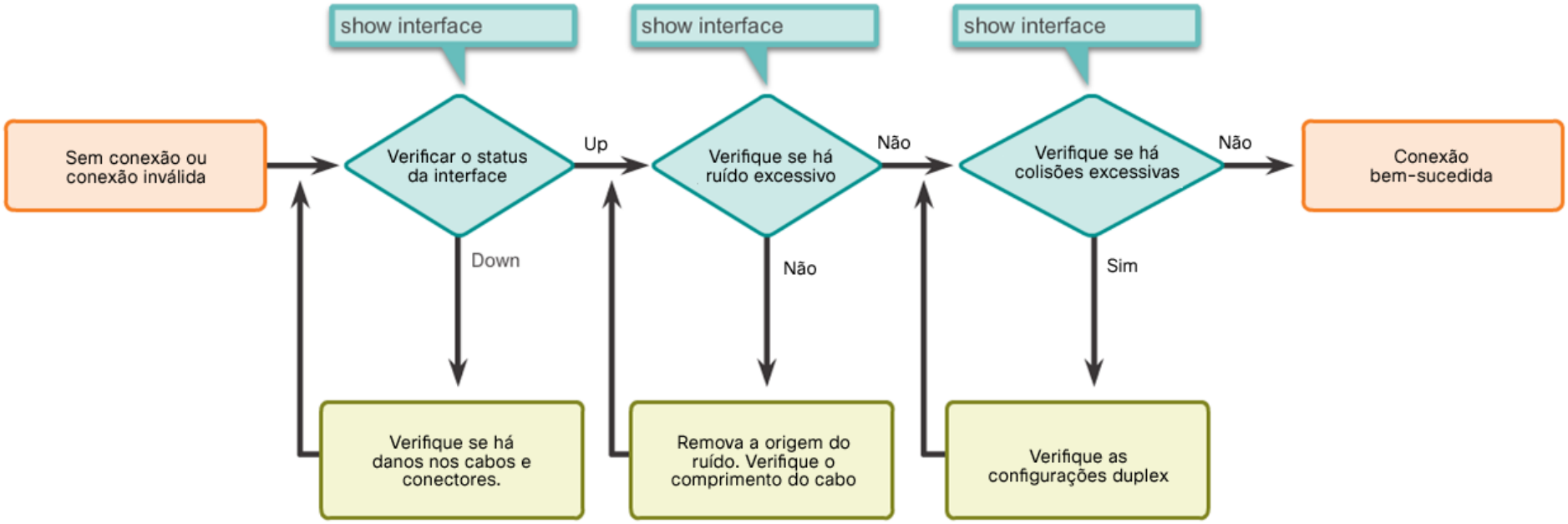
Problemas da camada de acesso à rede

- Identificando e solucionando problemas de meio do switch (conexão)



Problemas da camada de acesso à rede

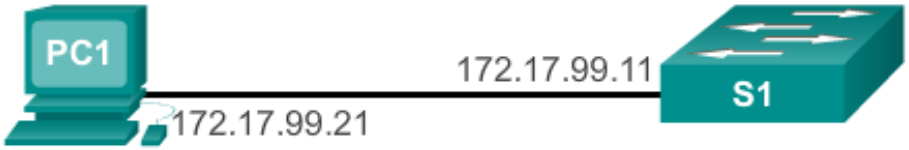
- Identificando e solucionando problemas relacionados à interface



Operação de SSH

- O Secure Shell (SSH) é um protocolo que fornece uma conexão baseada em linha de comando (criptografada) segura para um conexão baseada em um dispositivo remoto
- O SSH é comumente usado em sistemas baseados em UNIX
- O IOS Cisco também suporta SSH
- Uma versão do software IOS que inclui recursos e capacidades criptográficos é necessário para ativar o SSH nos switches Catalyst 2960
- Graças aos seus recursos de criptografia forte, o SSH deve substituir o Telnet para conexões de gerenciamento.
- O SSH por usa a porta 22 por padrão. O Telnet usa a porta TCP 23

Operação de SSH



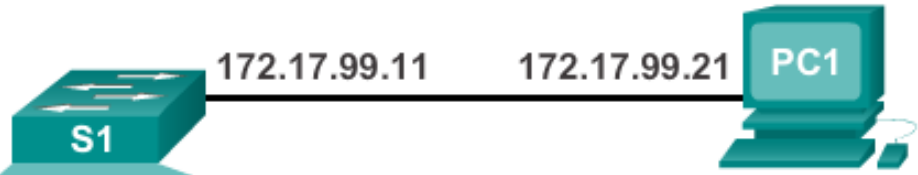
172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Acesso remoto seguro

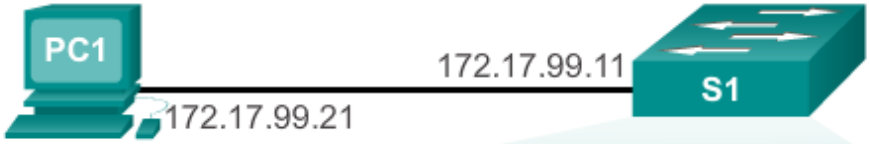
Configurando o SSH




```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

Acesso remoto seguro

Verificando o SSH




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started ricky
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started ricky
%No SSHv1 server connections running.
S1#
```

Preocupações com segurança na inundação de endereços MAC de LANs

- Os switches preenchem automaticamente suas tabelas CAM observando o tráfego que entra em suas portas
- Os switches encaminharão o tráfego por meio de todas as portas se não conseguirem encontrar o MAC de destino em sua tabela CAM
- Nessas circunstâncias, o switch atua como um hub. O tráfego unicast pode ser visto por todos os dispositivos conectados ao switch
- Um invasor pode explorar esse comportamento para obter acesso ao tráfego normalmente controlado pelo switch usando um PC para executar uma ferramenta de inundação de MAC.

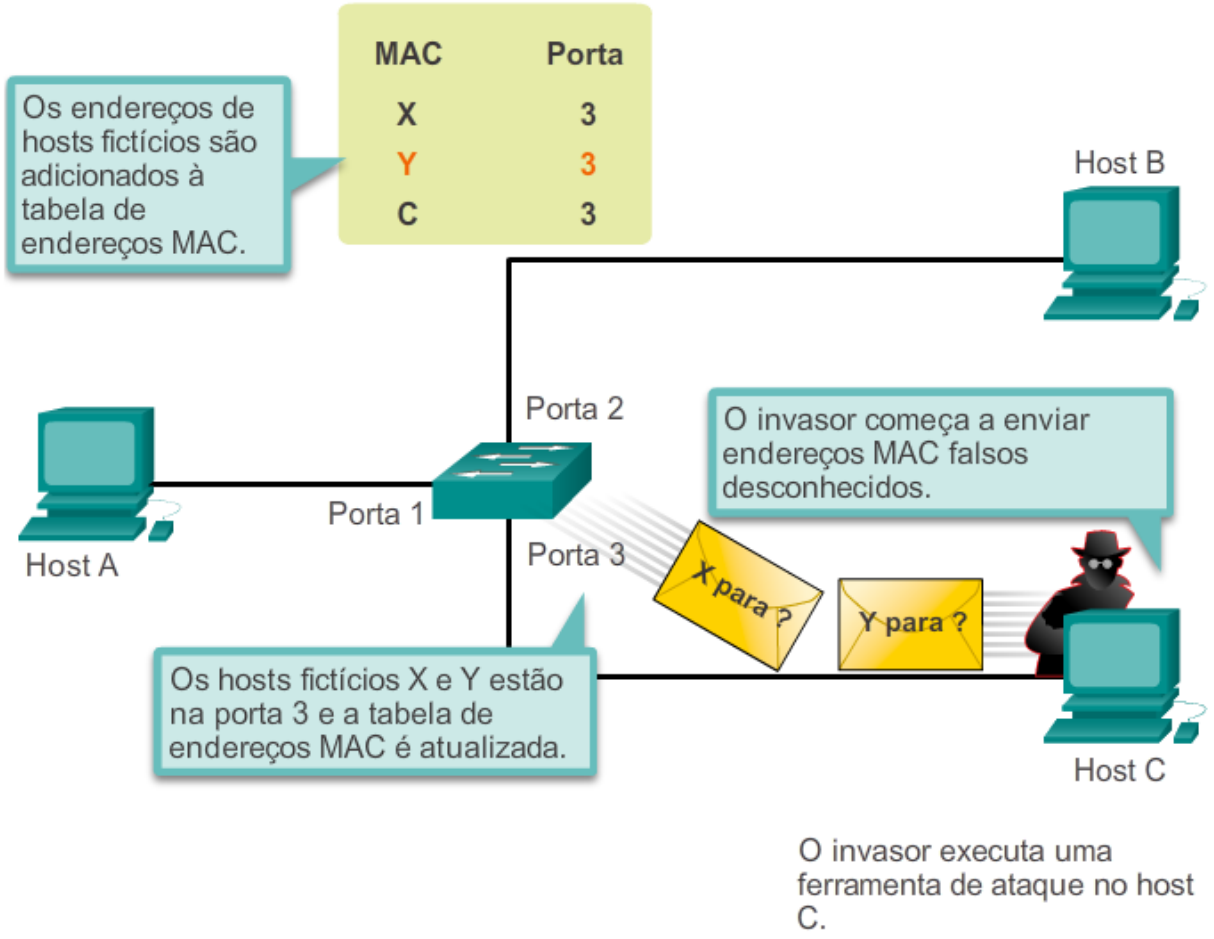
Preocupações com segurança na inundação de endereços MAC de LANs

- Essa ferramenta é um programa criado para gerar e enviar quadros com endereços MAC de origem falsos à porta do switch
- À medida que esses quadros acessam o switch, ele adiciona o endereço MAC falso à sua tabela CAM, anotando a porta em que os quadros chegaram
- Depois, a tabela CAM é preenchida com endereços MAC falsos
- Agora, a tabela CAM não tem espaço para os dispositivos legítimos presentes na rede e, portanto, nunca encontrarão os endereços MAC na tabela CAM.
- Todos os quadros são enviados agora para todas as portas, permitindo que o invasor acesse o tráfego para outros hosts

Preocupações com segurança na inundação de

endereços MAC de LANs

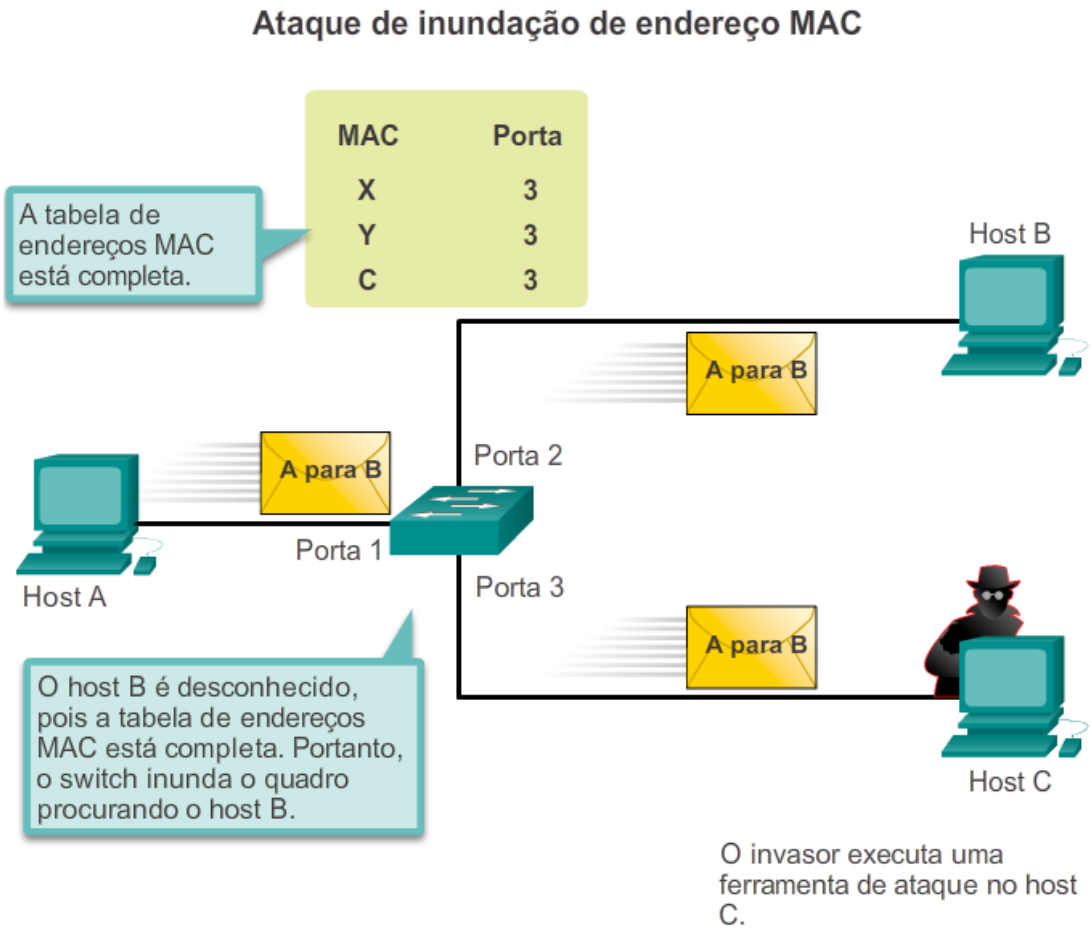
Invasor inundando a tabela CAM com as entradas falsas



Preocupações com segurança na inundação de

endereços MAC de LANs

Agora o switch se comporta como um hub

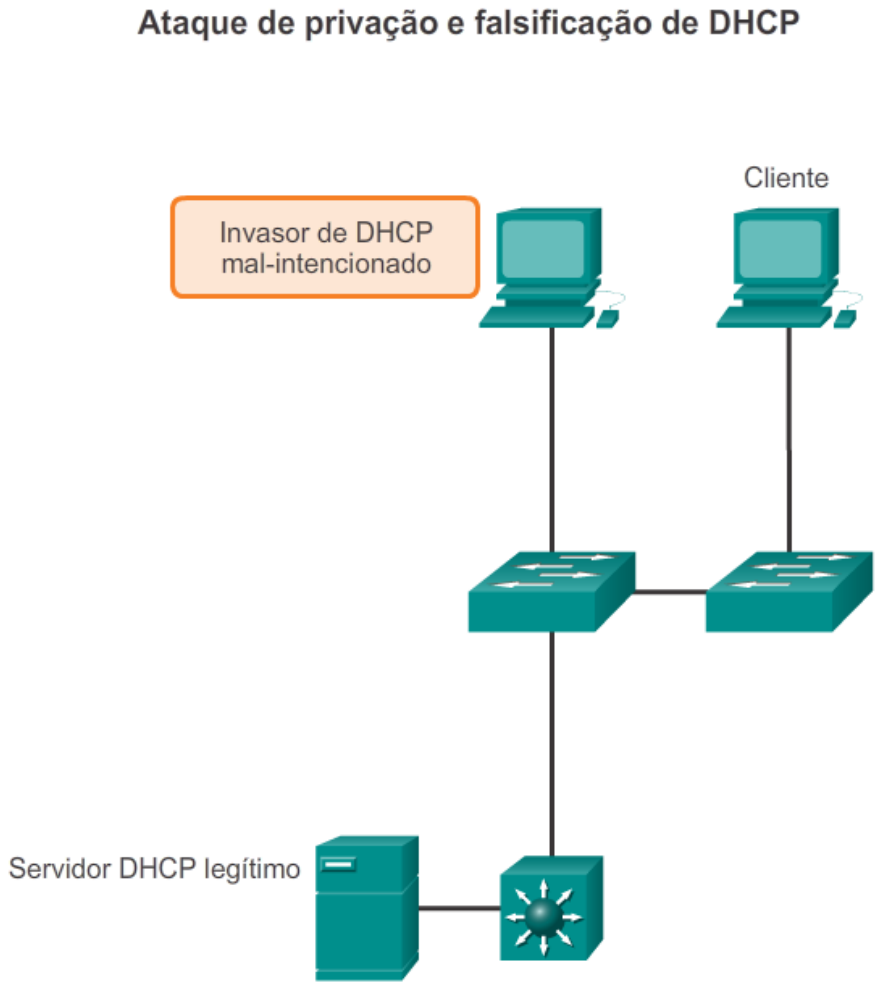


Falsificação de DHCP

- O DHCP é um protocolo de rede usado para atribuir automaticamente informações IP
- Há dois tipos de ataques DHCP:
  - DHCP Spoofing
  - DHCP starvation
- Nos ataques de spoofing do DHCP, um servidor DHCP falso é colocado na rede para emitir endereços DHCP aos clientes.
- O esgotamento do DHCP é usado geralmente antes de um ataque de spoofing do DHCP para negar o serviço ao servidor DHCP legítimo

Falsificação de DHCP

- Ataque de spoofing do DHCP



Aproveitando o CDP

- O CDP é um protocolo proprietário Cisco da camada 2 usado para descobrir outros dispositivos Cisco diretamente conectados
- Foi projetado para permitir que os dispositivos configurem automaticamente suas conexões
- Se um invasor estiver ouvindo mensagens de CDP, ele poderá aprender informações importantes, como o modelo do dispositivo e a versão do software em execução
- A Cisco recomendar desativar o CDP quando ele não estiver em uso

Aproveitar o Telnet

- Como mencionado, o protocolo Telnet não é confiável e deve ser substituído pelo SSH.
- No entanto, um invasor pode usar o Telnet como parte de outros ataques
- Dois desses ataques são Ataque de senha de força bruta e Ataque de Telnet DoS
- Quando as senhas não puderem ser capturadas, os invasores tentarão tantas combinações de caracteres quanto possível. Essa tentativa de adivinhar a senha é conhecida como ataque de senha de força bruta.
- O Telnet pode ser usado para testar a senha psumarizada no sistema.

Aproveitar o Telnet

- Em um ataque de Telnet DoS, o invasor explora uma falha no software do servidor Telnet em execução no switch que torna o serviço Telnet indisponível.
- Esse tipo de ataque impede um administrador de acessar remotamente as funções de gerenciamento do switch.
- Ele pode ser combinado com outros ataques diretos na rede como parte de uma tentativa coordenada de impedir o administrador de rede de acessar os dispositivos principais durante a violação.
- As vulnerabilidades no serviço Telnet que permitem a ocorrência de ataques DoS são abordadas nos patches de segurança que estão incluídos nas revisões mais recentes do IOS Cisco.

10 Práticas Recomendadas

- Desenvolva uma política de segurança por escrito para a organização
- Feche serviços e portas não usados
- Use senhas fortes e mude-as frequentemente
- Controle o acesso físico aos dispositivos
- Use HTTPS, em vez de HTTP
- Execute operações de backup regularmente.
- Informe os funcionários sobre ataques de engenharia social
- Criptografe e proteja dados confidenciais som uma senha
- Implemente firewalls.
- Mantenha o software atualizado

Ferramentas de Segurança de Rede: Opções

- As ferramentas de segurança de rede são muito importantes para os administradores de rede
- Essas ferramentas permitem que um administrador teste a força das medidas de segurança implementadas
- Um administrador pode iniciar um ataque contra a rede e analisar os resultados
- Também é útil para determinar como ajustar as políticas de segurança para atenuar esses tipos de ataques
- A auditoria segurança e o teste de penetração são duas funções básicas que as ferramentas de segurança de rede executam

Ferramentas de Segurança de Rede: Auditorias

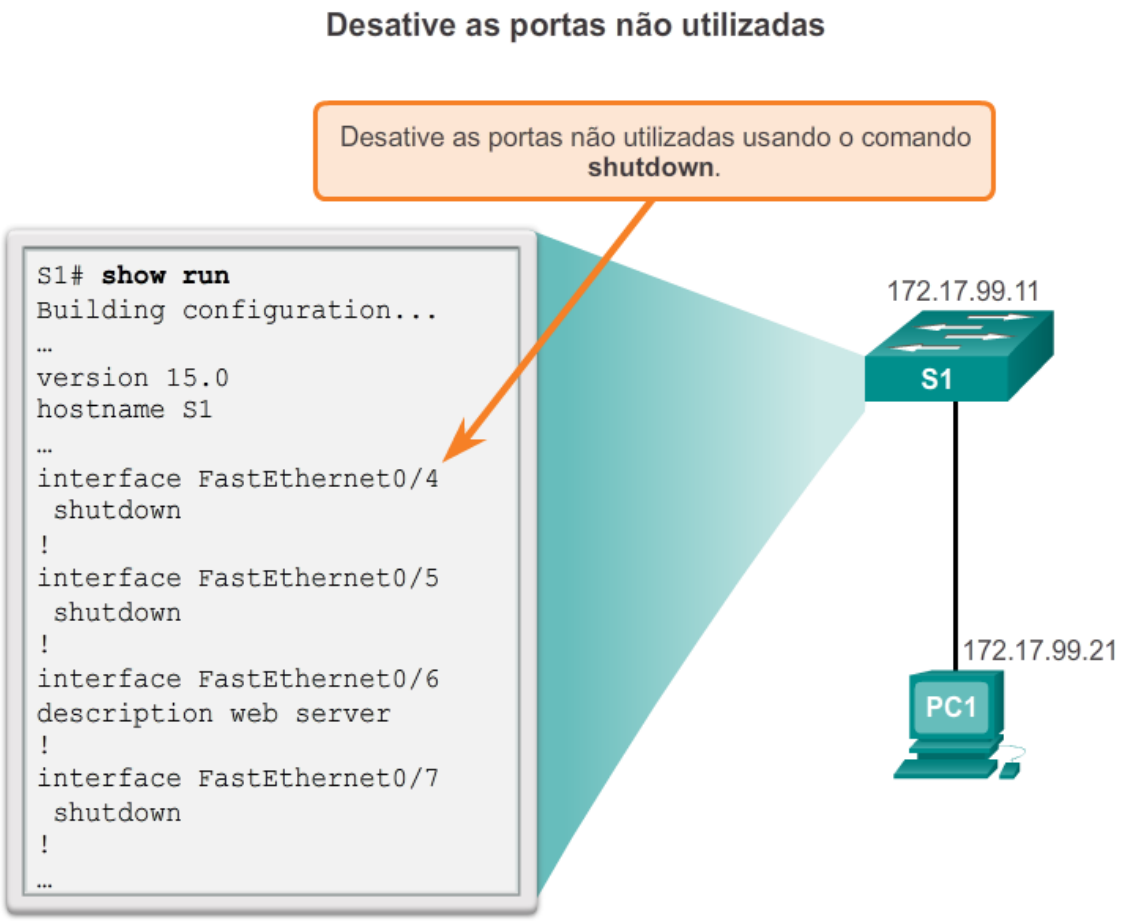
- As Ferramentas de Segurança de Rede podem ser utilizadas para auditar a rede
- Ao monitorar uma rede, um administrador pode avaliar que tipo de informações um invasor pode coletar
- Por exemplo, ao atacar e inundar a tabela CAM de um switch, um administrador identificaria que portas de switches estão vulneráveis à inundação de endereços MAC e poderia corrigir esse problema
- As ferramentas de segurança de rede também podem ser usadas como ferramentas de teste de penetração

Ferramentas de Segurança de Rede: Auditorias

- O teste de penetração é um ataque simulado
- Ele ajuda a determinar o quão vulnerável a rede fica quando está sofrendo um ataque real.
- Os pontos fracos na configuração de dispositivos de rede podem ser identificados com base nos resultados do teste de penetração
- As alterações podem ser feitas para tornar os dispositivos mais resistentes a ataques
- Esses testes podem danificar a rede e devem ser executados sob condições bastante controladas
- Uma rede off-line de teste que imite a rede de produção real é o ideal.

Portas não usadas seguras

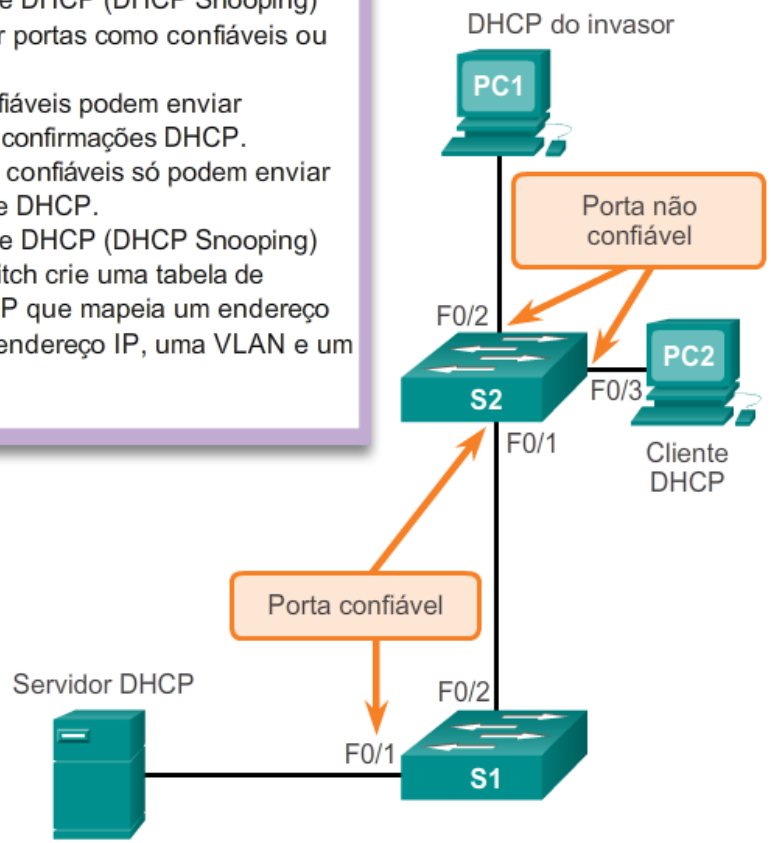
- As portas não usadas seguras constituem uma diretriz simples, porém eficiente de segurança



DHCP Snooping

- O DHCP Snooping especifica quais portas de switch podem responder às solicitações DHCP

- O rastreamento de DHCP (DHCP Snooping) permite configurar portas como confiáveis ou não confiáveis:
  - As portas confiáveis podem enviar solicitações e confirmações DHCP.
  - As portas não confiáveis só podem enviar solicitações de DHCP.
- O rastreamento de DHCP (DHCP Snooping) permite que o switch crie uma tabela de associações DHCP que mapeia um endereço MAC cliente, um endereço IP, uma VLAN e um ID de porta.




```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```

Segurança de porta: Operação

- A segurança de porta limita o número de endereços MAC válidos permitidos em uma porta
- Os endereços MAC de dispositivos legítimos podem acessar, enquanto outros endereços MAC são recusados
- Todas as tentativas adicionais de conexão com endereços MAC desconhecidos vão gerar uma violação de segurança
- Endereços MAC seguros podem ser configurados de várias maneiras:
  - endereços MAC seguros estáticos
  - endereços MAC seguros dinâmicos
  - endereços MAC seguros sticky

Segurança de porta: Modos de violação

- O IOS verá uma violação de segurança quando qualquer uma destas situações ocorre:
  - O número máximo de endereços MAC seguros para essa interface foi adicionado à tabela CAM e uma estação cujo endereço MAC não está na tabela de endereços tenta acessar a interface.
  - Um endereço aprendido ou configurado em uma interface segura é visto em outra interface segura na mesma VLAN.
- Há três a ações possíveis quando uma violação é detectada:
  - Proteger
  - Restrito
  - shutdown

Segurança de porta: Configurar

- Padrões de segurança de porta dinâmica

Recurso	Definição padrão
Segurança de porta	Desativada na porta
Número máximo de endereços MAC seguros	1
Modo de violação	Desativar. A porta é desativada quando o número máximo de endereços MAC seguros é excedido.
Aprendizagem do endereço sticky	Desativado

Segurança de porta: Configurar

- Configurando a segurança de porta dinâmica

Comandos CLI do CISCO IOS	
Especifique a interface a ser configurada para segurança de porta.	`S1(config)# interface fastethernet 0/18`
Defina o modo de interface para o acesso.	`S1(config-if)# switchport mode access`
Ative a segurança de porta na interface.	`S1(config-if)# switchport port-security`

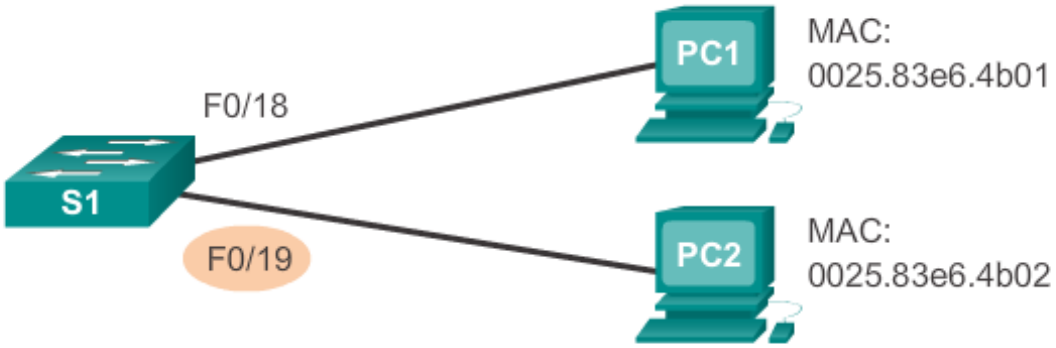
Segurança de porta: Configurar

- Configurando segurança de porta sticky

Comandos CLI do CISCO IOS	
Especifique a interface a ser configurada para segurança de porta.	`S1(config)# interface fastethernet 0/19`
Defina o modo de interface para o acesso.	`S1(config-if)# switchport mode access`
Ative a segurança de porta na interface.	`S1(config-if)# switchport port-security`
Defina o número máximo de endereços seguros permitidos na porta.	`S1(config-if)# switchport port-security maximum 50`
Ative a aprendizagem sticky.	`S1(config-if)# switchport port-security mac-address sticky`

Segurança de porta: verificar

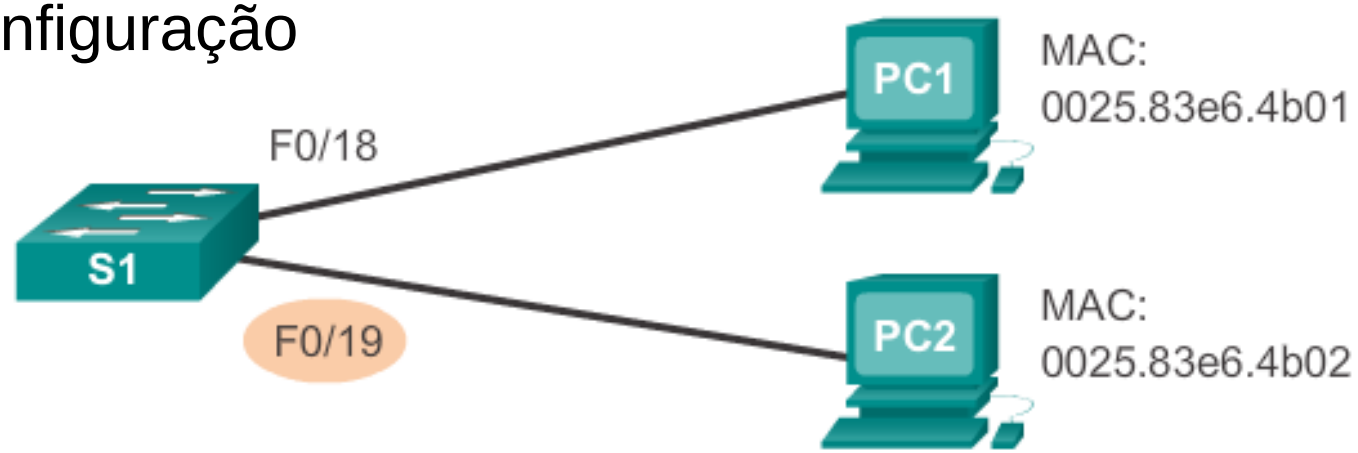
- Verificando a segurança de porta sticky




```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

Segurança de porta: verificar

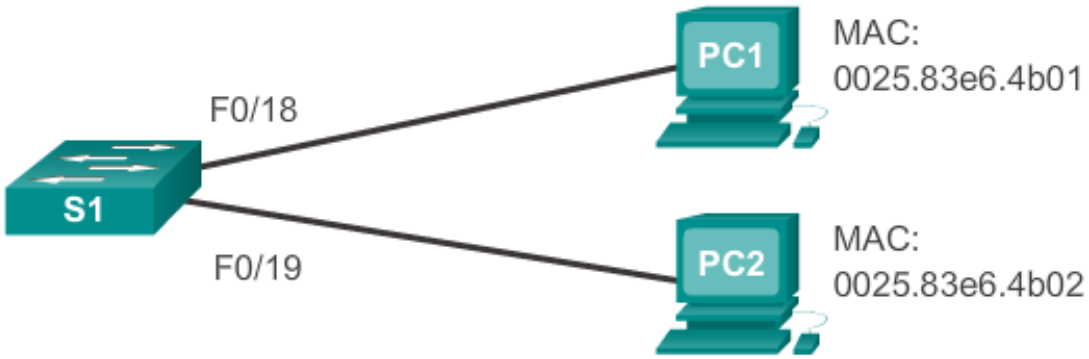
- Verificando a segurança de porta sticky – executando a configuração




```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Segurança de porta: verificar

- Verificando endereços MAC protegidos de segurança de porta




```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports    Remaining Age
                                                       (mins)
----    -----------       ----              -----    -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18       -
1       0025.83e6.4b02    SecureSticky      Fa0/19       -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Portas No estado de erro desativado

- Uma violação da segurança de portas pode colocar um switch no estado de erro desativado
- Uma porta no estado de erro desativada é realmente desativada
- O switch comunicará esses eventos por meio de mensagens de console

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Portas No estado de erro desativado

- O comando show interface também revela uma porta do switch no estado de erro desativado

```
S1# show interface fa0/18 status
Port Name   Status         Vlan   Duplex   Speed    Type
Fa0/18      err-disabled   1      auto     auto     10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security               : Enabled
Port Status                 : Secure-shutdown
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 000c.292b.4c75:1
Security Violation Count    : 1
```

Segurança de porta do switch

Portas No estado de erro desativado

- Um comando de interface shutdown/no shutdown precisa ser emitido para reativar a porta

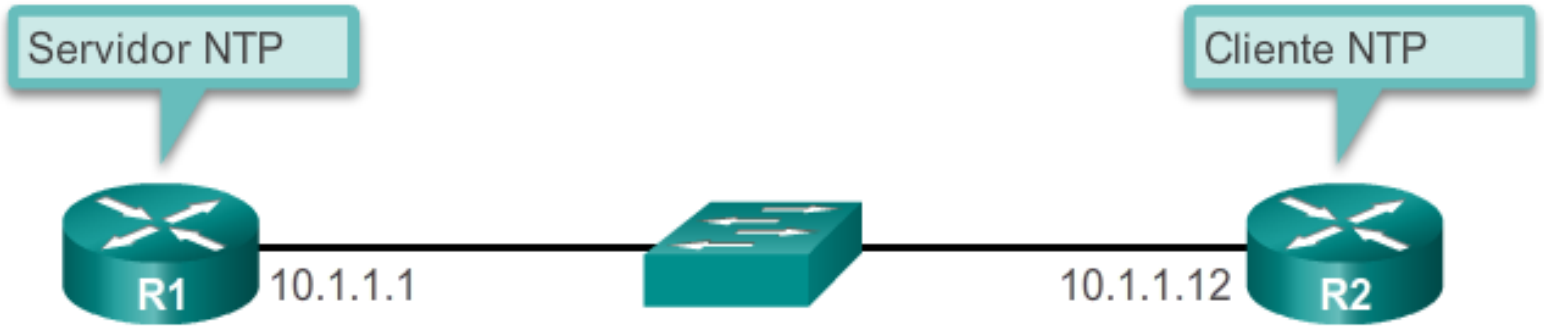
```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

Network Time Protocol (NTP)

- O NTP é um protocolo usado para sincronizar os relógios de redes de dados de sistemas
- O NTP pode obter o horário correto de uma fonte interna ou externa de tempo
- As fontes de tempo podem ser:
  - Master Clock local
  - Master Clock na Internet
  - GPS ou relógio atômico
- Um dispositivo de rede pode ser configurado como um servidor NTP ou um cliente NTP
- Consulte as anotações de slides para obter mais informações sobre o NTP

Network Time Protocol (NTP)

- Configuração do NTP




```
R1(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.1.1
```

Network Time Protocol (NTP)

- Verificando NTP

```
R2# show ntp associations
  address         ref clock       st   when   poll reach   delay   offs
*~10.1.1.1        .LOCL.           1     13     64   377    1.472   6.07
sys.peer,    # selected,    + candidate, - outlyer,   x falsetick
```

```
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.1.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz,
precision is 2**17reference time is D40ADC27.E644C776
(13:18:31.899 UTC Mon Sep 24 2012)clock offset is 6.0716
msec,
root delay is 1.47 msecroot dispersion is 15.41 msec,
peer dispersion is 3.62 msecloopfilter state is 'CTRL'
(Normal Controlled Loop), drift is 0.000000091 s/ssystem poll
interval is 64, last update was 344 sec ago.
```

Capítulo 2: Resumo

- Este capítulo abordou:
- Sequência de inicialização do switch de LAN da Cisco
- Modos do LED do switch de LAN da Cisco
- Como acessar e gerenciar remotamente um switch de LAN da Cisco por meio de uma conexão segura
- Modos duplex de porta do switch de LAN da Cisco
- Segurança de porta do switch de LAN da Cisco, modos de violação e ações
- Práticas Recomendadas para Redes Comutadas