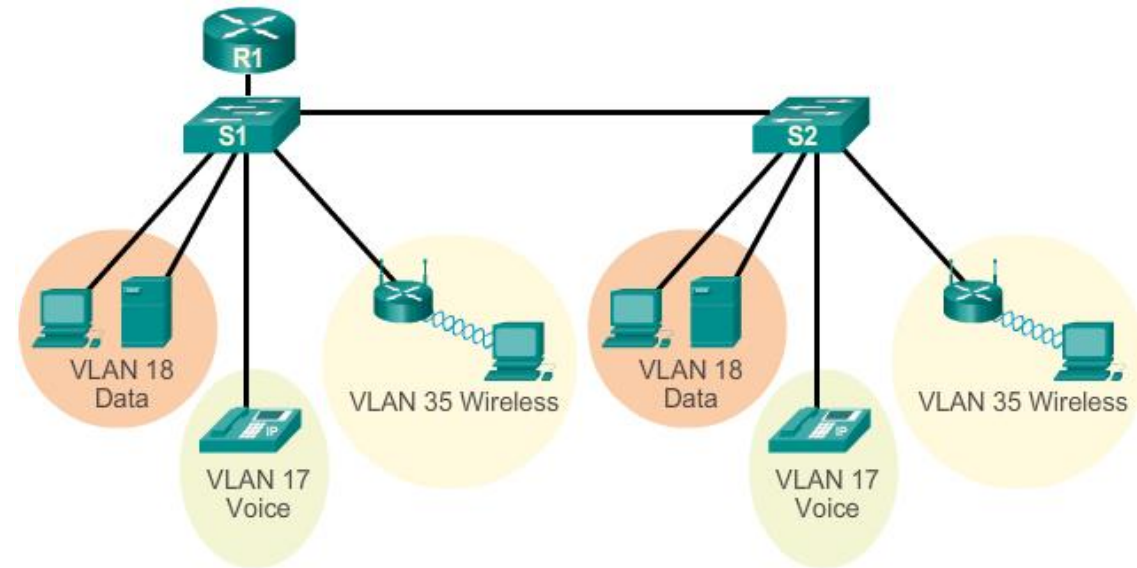




IPS

Instituto
Politécnico de Setúbal

Escola Superior de
Tecnologia de Setúbal



Switching Básico

Slides do CCNA Routing & Switching revistos e atualizados por
Luísa Caeiro, Jorge Martins e Teles Rodrigues

ESTSetúbal (v1)

Tipos de memórias dos Switches

- EPROM - utilizada para armazenar o ROM Monitor Software, e o boot loader/helper software, que permite acessar o equipamento mesmo se ele estiver sem o IOS
- NVRAM – armazena o startup-config e também o configuration-register.
- FLASH - armazena o IOS e outros arquivo
- DRAM - utilizada para manter a tabela de roteamento, o running-config (arquivo de configuração em uso), e o IOS, que é carregado nela quando o equipamento liga. Na segunda parte (shared) temos o buffer das interfaces de rede

Sequência de Boot dos Switches

- Teste de Power on - *Power-on self test* (POST).
- Execução do software *boot loader*:
 1. inicialização de baixo nível do CPU;
 2. inicialização do sistema de ficheiros na flash;
 3. localização e carregamento em memória da imagem de software por omissão do sistema operativo Cisco IOS;
 4. Transferência do controlo do switch para o Cisco IOS.

Sequência de Boot dos Switches




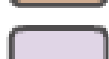
- Para encontrar uma imagem adequada do Cisco IOS, o switch efetua os seguintes passos:
 1. Tenta iniciar automaticamente usando a informação existente na variável de ambiente de BOOT.
 2. Se a variável não está definida, o switch faz uma procura em profundidade no sistema de ficheiros da flash. Se possível carrega e executa o primeiro ficheiro executável.
- O IOS inicializa então as interfaces usando os comandos Cisco IOS constantes do ficheiro de configuração file, ***startup-config***, gravado na NVRAM.

Sequência de Boot dos Switches

O comando ***boot system*** pode ser usado para definir a variável de ambiente de BOOT.



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

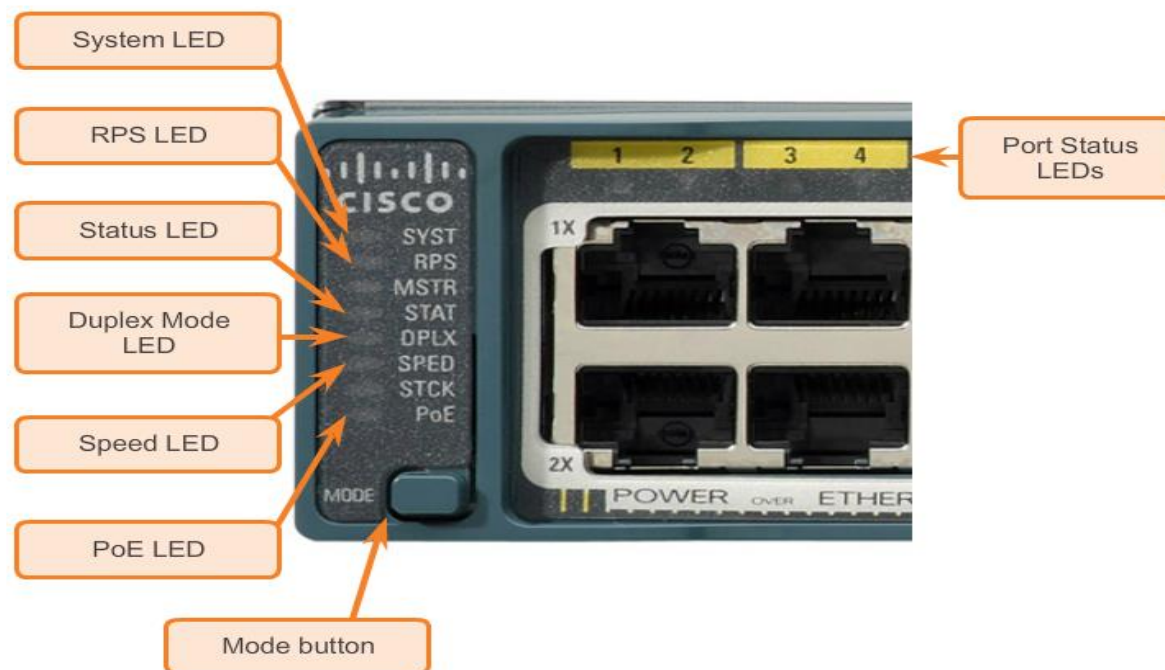
-  Command
-  Storage Device
-  Path to location in file system
-  Filename of IOS

Recuperação de um *Crash*

- O *boot loader* pode ser acedido através de uma ligação de consola, por ex., se o IOS não puder ser carregado.
- É usado o seguinte procedimento:
 - Ligar um PC através do cabo de consola à porta de consola do switch.
 - Desligar a alimentação do switch.
 - Voltar a ligar a alimentação do switch premindo o botão *Mode*.
 - O sistema de LEDs fica ambar por um período curto e em seguida fica verde.
 - Soltar o botão *Mode*.

Modos do Switch Cisco Catalyst 2960

- Cada porta do switch tem um LED que indica por omissão o seu estado de atividade.
- Ao premir o botão **Mode** pode alterar-se a indicação que os LEDs das portas fornecem (*port speed, port duplex,...*) .



Gestão Básica do Switch

- Para gerir remotamente um switch Cisco, é necessário configurá-lo para acesso à rede. Para isso:
 - atribuir um endereço IP e uma máscara de sub-rede;
 - configurar o gateway por omissão se se pretender aceder de uma rede remota.
- A informação IP (endereço, máscara de sub-rede, gateway) são atribuídas a uma interface virtual do switch, *Switch Virtual Interface (SVI)*.
- Estas definições IP permitem o acesso remoto ao switch, mas não permitem o encaminhamento de pacotes de nível 3.

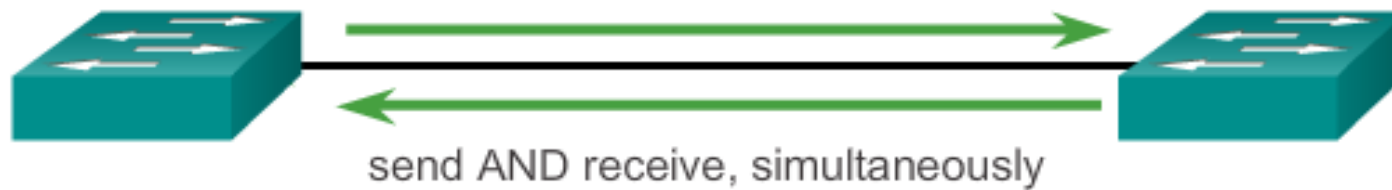
Gestão Básica do Switch

Cisco Switch IOS Commands

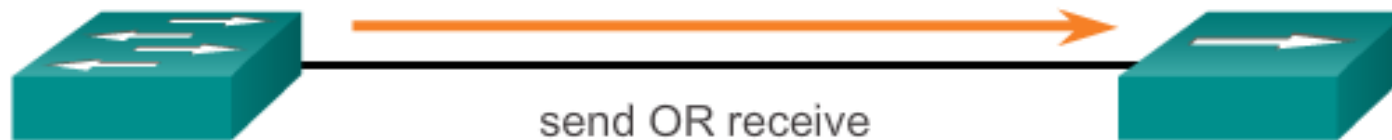
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface vlan99
Configure the management interface IP address.	S1(config-if)# ip address 172.17.99.11
Enable the management interface.	S1(config-if)# no shutdown
Return to the privileged EXEC mode.	S1(config-if)# end
Enter global configuration mode.	S1# configure terminal
Configure the default gateway for the switch.	S1(config)# ip default-gateway 172.17.99.1
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

Comunicação Duplex

Full-Duplex Communication

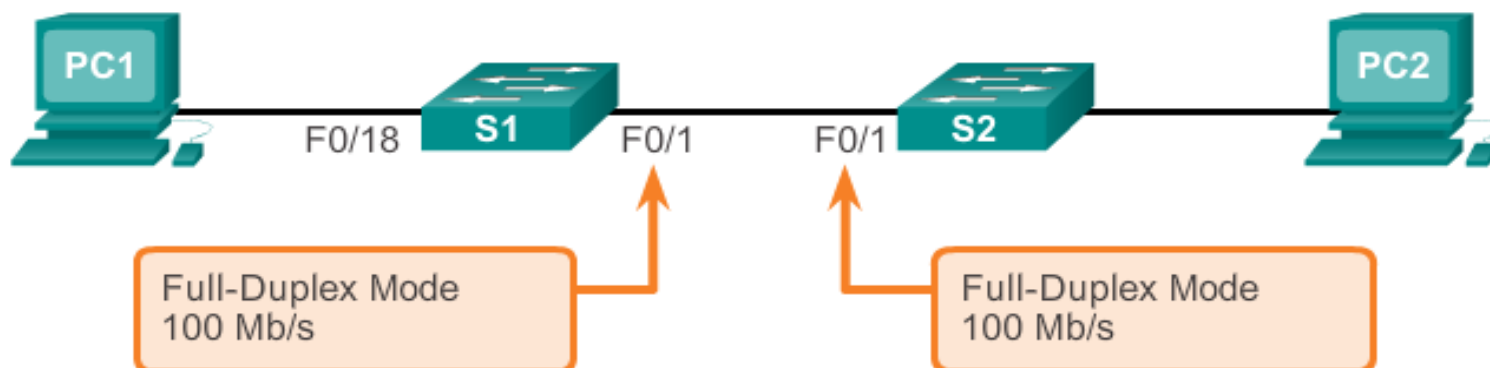


Half-Duplex Communication



Configurar Portas do Switch no Nível Físico

Configure Duplex and Speed



Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface FastEthernet 0/1
Configure the interface duplex.	S1(config-if)# duplex full
Configure the interface speed.	S1(config-if)# speed 100
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

Auto-MDIX

- Para ligar dispositivos entre si usam-se cabos de tipos diferentes (diretos ou cruzados) consoante os dispositivos.
- A funcionalidade de *automatic Medium-Dependent Interface Crossover* (auto-MDIX) elimina a necessidade de se utilizarem cabos de tipos diferentes.
- Quando o auto-MDIX está ativo, a interface automaticamente deteta e configura adequadamente a ligação.
- Ao usar auto-MDIX numa interface, esta deve estar definida em modo auto para speed e duplex.

Configuração Auto-MDIX



Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1 (config) # interface fastethernet 0/1
Configure the interface to autonegotiate duplex with the connected device.	S1 (config-if) # duplex auto
Configure the interface to autonegotiate speed with the connected device.	S1 (config-if) # speed auto
Enable auto-MDIX on the interface.	S1 (config-if) # mdix auto
Return to the privileged EXEC mode.	S1 (config-if) # end
Save the running config to the startup config.	S1# copy running-config startup-config

Verificação do Auto-MDIX



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

Verificação da configuração do Switch

Cisco Switch IOS Commands

Display interface status and configuration.	S1# show interfaces [<i>interface-id</i>]
Display current startup configuration.	S1# show startup-config
Display current operating config.	S1# show running-config
Display information about flash file system.	S1# show flash
Display system hardware and software status.	S1# show version
Display history of commands entered.	S1# show history
Display IP information about an interface.	S1# show ip [<i>interface-id</i>]
Display the MAC address table.	S1# show mac-address-table OR S1# show mac address-table

Problemas do Nível de Acesso à Rede

Runts

Pacotes que são descartados por terem tamanho inferior ao mínimo permitido no meio.

Exemplo:

Output Errors

Soma de todos os erros que não permitem a transmissão final de pacotes na interface examinada.

Input Errors

Número total de erros. Inclui **runts**, **giants**, **no buffer**, **CRC**, **frame**, **overrun** e **ignored counts**.

Giants

Pacotes que são descartados excederem o máximo tamanho permitido no meio. Exemplo:
- Um pacote Ethernet maior que 1518 bytes é considerado **giant**.

Collisions

Número de mensagens retransmitidas devido a

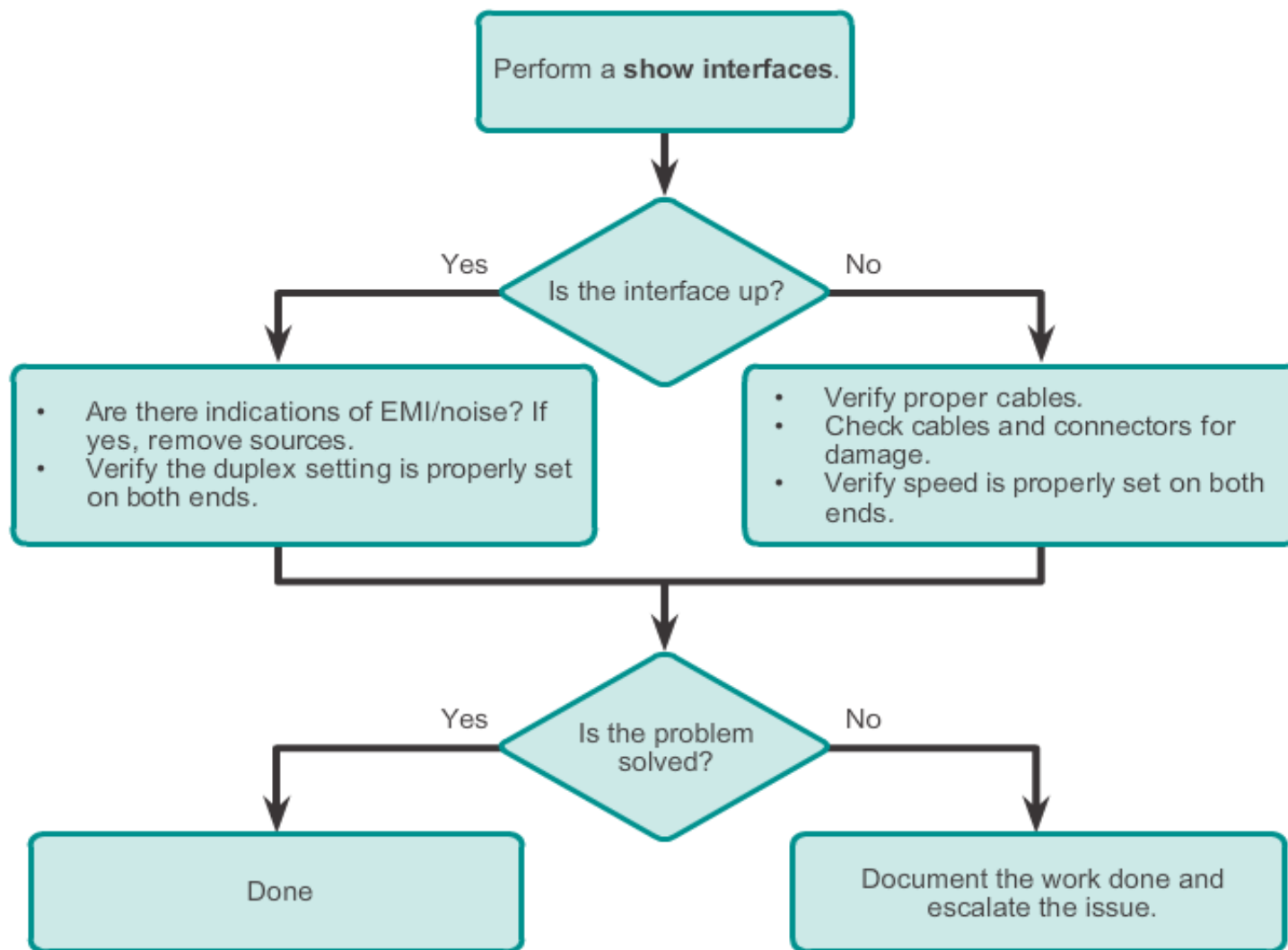
Late collisions

O Sinal Jam não pode chegar ao fim.

CRC

Erros de CRC são gerados quando se calcula o checksum e não é o mesmo que vem na frame.

Resolução de Problemas do Nível de Acesso



Acesso Remoto Seguro - SSH

- Secure Shell (SSH) é um protocolo que fornece acesso seguro (cifrado - *encrypted*) a um dispositivo remoto através de uma ligação baseada em linha de comando.
- SSH é de utilização comum em sistemas UNIX.
- O software Cisco IOS também suporta SSH.
- É necessário uma versão de IOS que inclua recursos e capacidades de criptografia (*encrypted*) para ativar SSH nos switches Catalyst 2960.
- SSH deve substituir Telnet em ligações de gestão porque tem fortes capacidades de cifra.
- SSH usa o porto TCP 22, por omissão e Telnet usa o 23.

Operação do SSH



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

S1>enable
Password:
S1#
```

Configuração de SSH no Switch



Gera um par de chaves RSA para ativar automaticamente o SSH.

Configura autenticação.

Configura as linhas de terminal virtual (vty).

Ativa SSH nas linhas vty.

Exige autenticação local.

Verificação do 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
AAAAB3NzaC1yc2EAAAADAQABAAQgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/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#
  
```

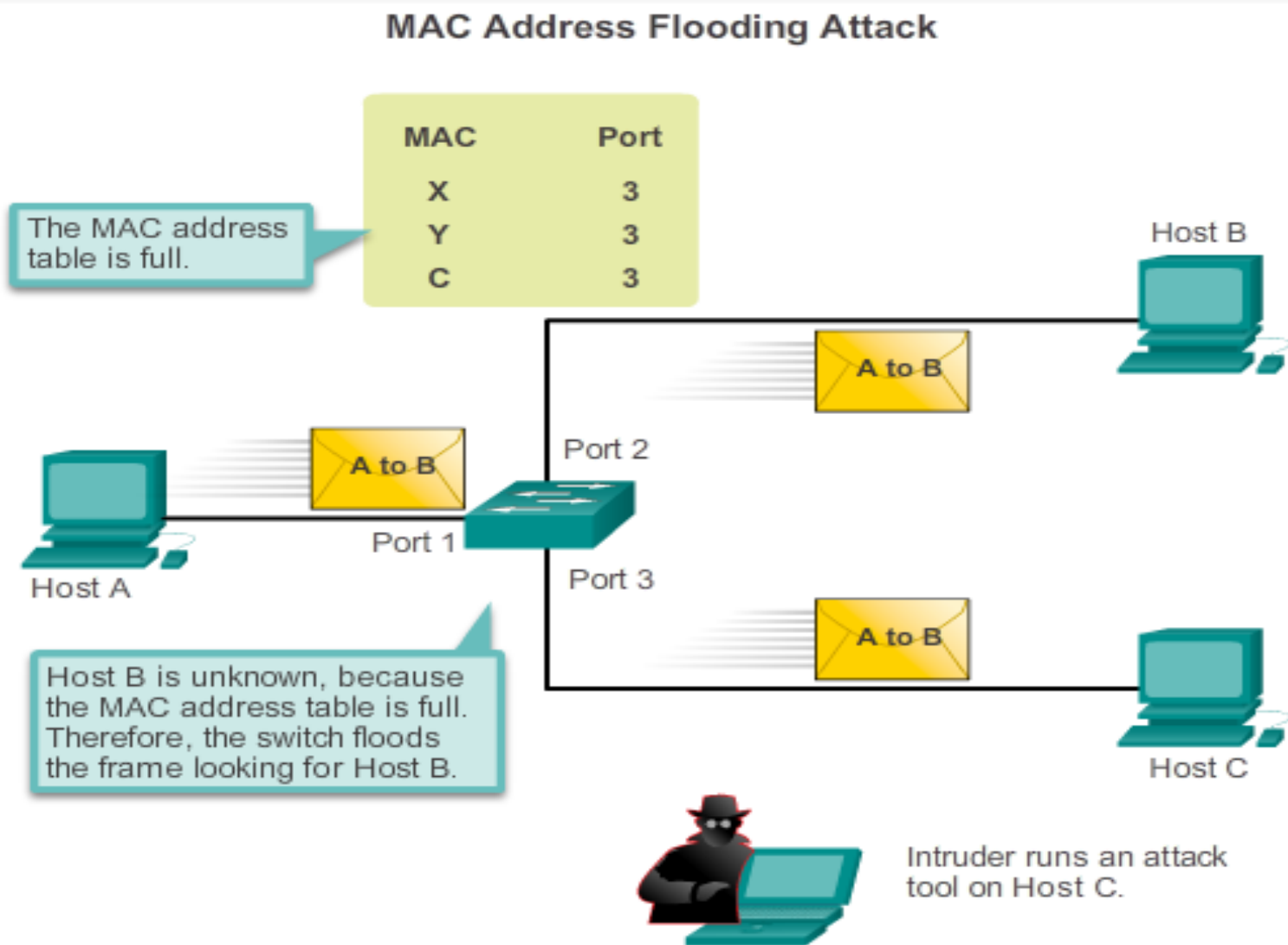
Inundação (Flooding) de MAC Addresses

- Os Switches preenchem automaticamente as suas tabelas de CAM observando o tráfego que passa nos suas portas.
- Switches transferem o tráfego para todas as portas quando não encontrarem o MAC de destino na sua tabela CAM.
 - Nestas circunstâncias o switch comporta-se como um hub.
- Um *attacker* pode explorar este comportamento para ganhar acesso ao tráfego normalmente controlado pelo switch, usando um PC que execute uma ferramenta de *MAC flooding*.
- Esta ferramenta é um programa criado para gerar e enviar *frames* com endereços MAC de origem falsos para a porta do switch:
 - O switch adiciona estes endereços MAC falsos à sua tabela CAM, registando a porta das *frames* recebidas.

Inundação (*Flooding*) de MAC Addresses

- A tabela CAM ficará totalmente preenchida com os endereços MAC falsos e por isso:
 - deixa de ter espaço para os dispositivos legítimos presentes na rede
 - nunca encontrará os endereços MAC dos dispositivos legítimos na tabela CAM;
 - todas as *frames* passam a ser transferidas para todas as portas, permitindo ao *attacker* o acesso ao tráfego para outros hosts.

Inundação (Flooding) de MAC Addresses

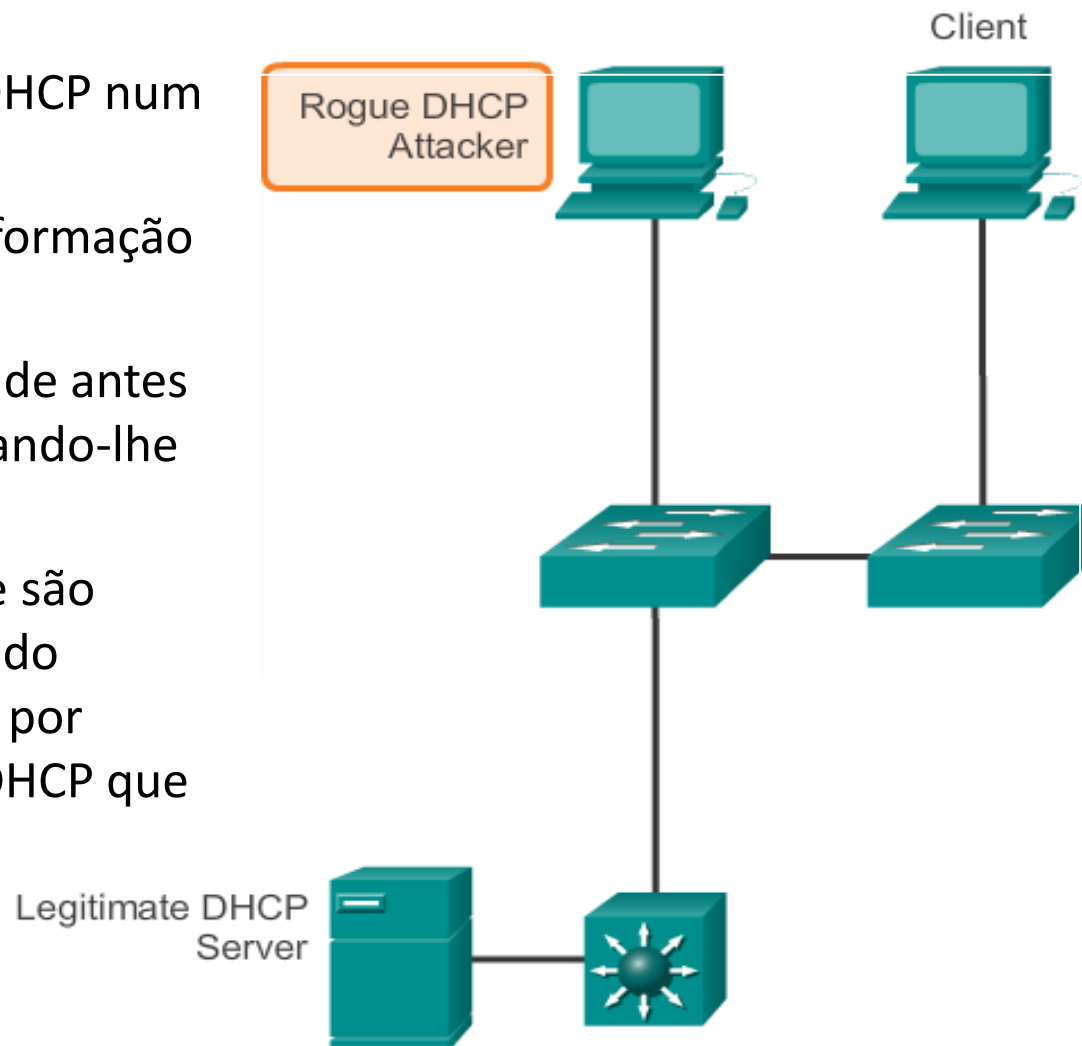


Ataques DHCP

- O DHCP é um protocolo de rede usado para atribuir informação IP de modo automático.
- Existem dois tipos de ataque DHCP:
 - DHCP *spoofing*;
 - DHCP *starvation*.
- Nos ataques DHCP *spoofing*, o falso servidor de DHCP é colocado na rede para atribuir endereços DHCP aos clientes.
- DHCP *starvation* é muitas vezes usado antes de um ataque DHCP *spoofing* para negar serviço aos servidores de DHCP legítimos.

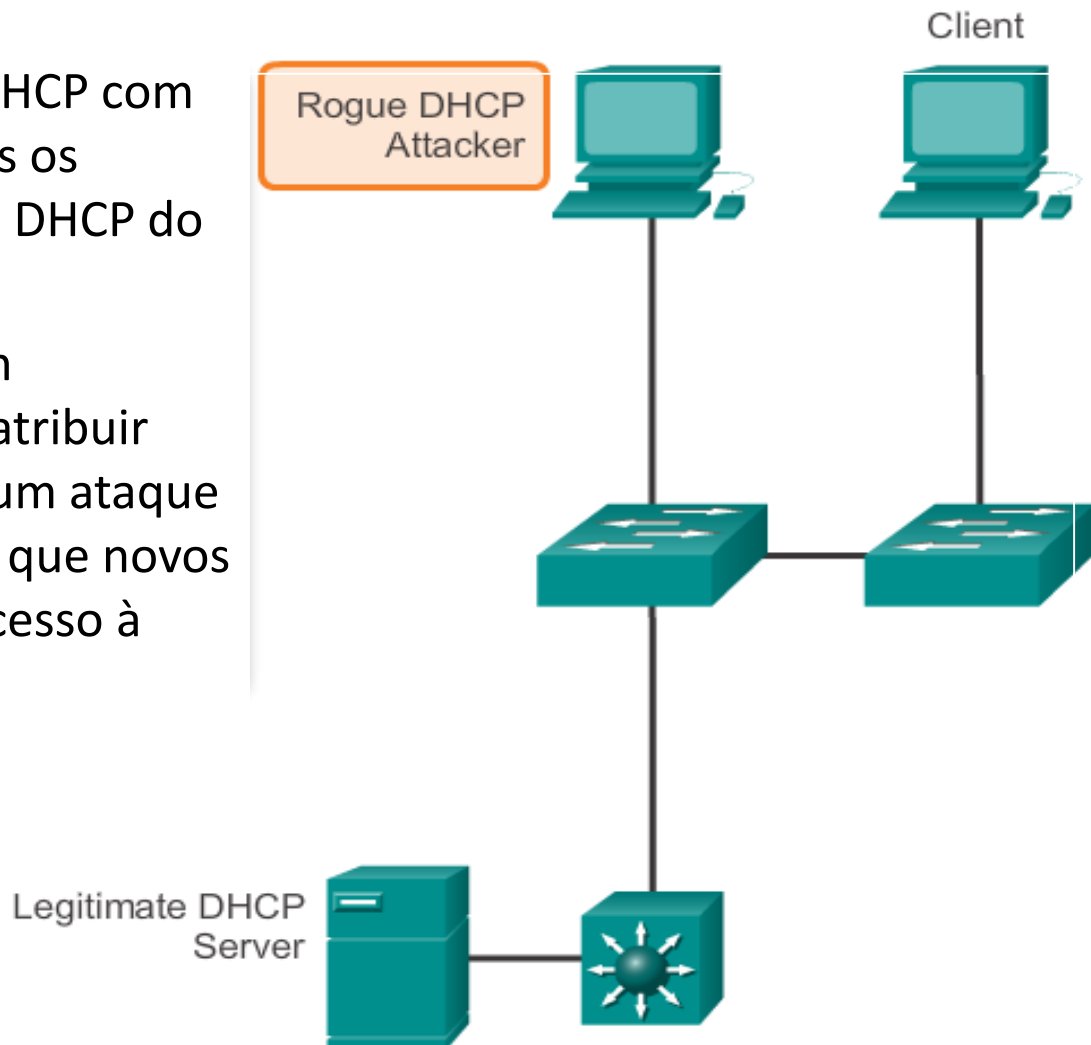
Ataque DHCP Spoofing

1. Um *attacker* ativa um servidor DHCP num segmento de rede.
2. O cliente envia um pedido de informação DHCP em difusão.
3. O falso servidor de DHCP responde antes do servidor DHCP legítimo enviando-lhe informação enganosa.
4. Os pacotes enviados pelo cliente são redirecionados para o endereço do *attacker* que emula um gateway por omissão para o falso endereço DHCP que este lhe forneceu.



Ataque DHCP Starvation

1. Um *attacker* inunda o servidor DHCP com pedidos de DHCP para usar todos os endereços IP disponíveis na pool DHCP do servidor.
2. Depois dos endereços IP estarem esgotados, o servidor não pode atribuir mais endereços consistindo em um ataque *Denial-of-Service* (DoS), uma vez que novos clientes não conseguem obter acesso à rede.



Vulnerabilidades do Cisco Discovery Protocol

- Cisco Discovery Protocol é um protocolo de nível 2 proprietário da Cisco usado para descobrir outros dispositivos Cisco diretamente ligados.
- O Cisco Discovery Protocol foi desenhado para permitir que os dispositivos auto-configurem as suas ligações.
- Se um *attacker* intercetar as mensagens do Cisco Discovery Protocol, pode aprender informação importante sobre o modelo do dispositivo e a versão de software que está em execução.
- A Cisco recomenda a desativação do CDP quando este não estiver em uso.

Vulnerabilidades do Telnet

- O protocolo Telnet é inseguro e deve ser substituído por SSH.
- Um *attacker* pode usar Telnet para suporte a outros ataques:
 - Ataque *Brute force password*
 - Ataque *Telnet DoS*
- Os *attackers* quando não conseguem capturar passwords, tentam todas as combinações de caracteres possíveis. Esta tentativa de adivinhar a password é conhecida como ataque *Brute Force Password*:
 - o Telnet pode ser usado para testar no sistema as passwords criadas deste modo.

Vulnerabilidades do Telnet

- Num ataque *Telnet DoS*, um *attacker* explora uma falha no software do servidor Telnet executado no switch, deixando o serviço Telnet indisponível.
- Este tipo de ataque impede que um administrador aceda remotamente ao switch para executar funções de gestão.
- O ataque *Telnet DoS* pode ser combinado com outros ataques diretos à rede, como parte de uma tentativa coordenada de impedir que o administrador da rede aceda a dispositivos de *core* durante uma violação de segurança.
- As vulnerabilidades do serviço Telnet que permitem a ocorrência de ataques de DoS são normalmente resolvidas por *patches* de segurança que estão incluídos em revisões mais recentes do Cisco IOS.

10 Regras de Boas Práticas

1. Ter uma política de segurança documentada para a organização.
2. Desativar portas e serviços não usados.
3. Usar passwords fortes e alterá-las frequentemente.
4. Controlar o acesso físico aos dispositivos.
5. Usar HTTPS em vez de HTTP.
6. Efetuar operações de backup numa base regular.
7. Educar os trabalhadores sobre os possíveis ataques.
8. Cifrar e proteger com passwords dados sensíveis.
9. Implementar firewalls.
10. Manter o software atualizado.

Ferramentas de Segurança na Rede: Opções

- Ferramentas de segurança na rede são importantes para os administradores da rede:
 - Permitem que o administrador teste a eficácia das medidas de segurança implementadas.
 - Um administrador pode desencadear um ataque à rede e analisar os resultados, podendo determinar como ajustar as políticas de segurança para evitar esses tipos de ataques.
- Os **auditos à segurança** e os **testes de penetração** são duas funções básicas que as ferramenta de segurança na rede executam.

Ferramentas de Segurança na Rede: Auditos

- As ferramentas de segurança na rede podem ser usadas para auditar a rede.
- Monitorando a rede, um administrador pode aceder a todo o tipo de informação que um *attacker* é capaz de recolher.
- Por exemplo, através do ataque de inundação da tabela de CAM de um switch, um administrador determina quais as portas do switch que estão vulneráveis a ataques de *MAC flooding* e pode corrigir esse problema.

Ferramentas de Segurança na Rede: Auditos

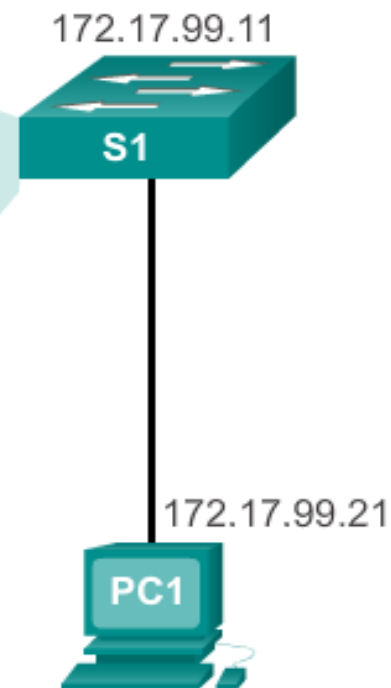
- As ferramentas de segurança na rede podem ser usadas para simular ataques e ajudar a determinar quão vulnerável a rede é em caso de ataque.
- Podem ser identificadas fraquezas na configuração dos dispositivos de rede com base nos resultados dos testes de penetração.
- Podem ser feitas alterações para que os dispositivos sejam mais resistentes aos ataques.
- No entanto, estes testes podem deteriorar a rede e devem ser feitos sob condições bem controladas.
- Uma rede de teste *offline* que reproduza a rede de produção atual é o ideal.

Desativar as Portas não Usadas

Disable unused ports using the **shutdown** command.

```
S1# show run
Building configuration...

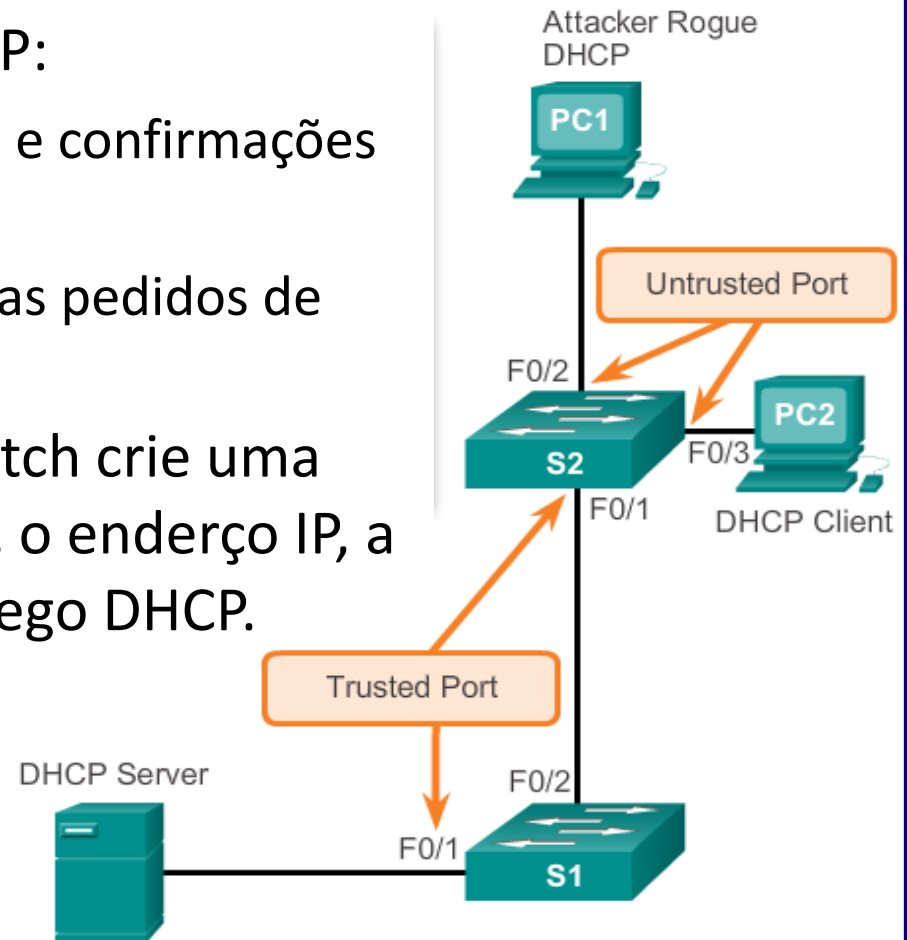
...
version 15.0
hostname S1
...
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 description web server
!
interface FastEthernet0/7
 shutdown
!
...
```



DHCP Snooping

- O *DHCP Snooping* especifica que portas do switch podem responder a pedidos de DHCP:
 - Portas *trusted* podem enviar pedidos e confirmações de DHCP;
 - Portas *untrusted* podem enviar apenas pedidos de DHCP.
- O *DHCP Snooping* permite que o switch crie uma tabela que mapeia o endereço MAC, o endereço IP, a VLAN e o ID da porta para filtrar tráfego DHCP.

```
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
```



Operação do *Port Security*

- O *Port security* limita o número de endereços MAC permitidos numa porta.
- Os endereços MAC dos dispositivos legítimos têm acesso à rede, enquanto aos outros é-lhes negado o acesso.
- Qualquer tentativa de ligação adicional efetuada por um endereço MAC desconhecido gera uma violação de segurança.
- Endereços MAC seguros podem ser configurados como:
 - Endereços MAC estáticos;
 - Endereços MAC dinâmicos;
 - Endereços MAC aprendidos (*Sticky*).

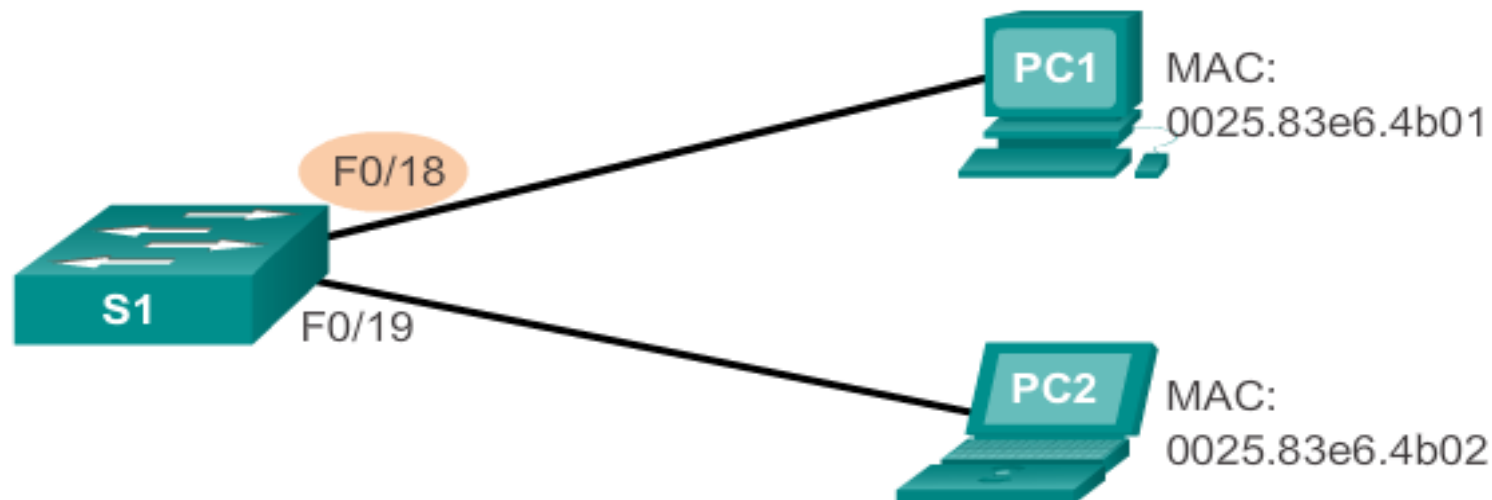
Port Security: Modos de Violação

- O IOS considera uma violação de segurança quando ocorre uma destas situações:
 - O número máximo de endereços MAC seguros para uma dada interface foi adicionado à tabela CAM.
 - Um endereço aprendido ou configurado numa interface segura foi detetado numa outra interface da mesma VLAN.
- Existem três ações possíveis que se podem tomar quando é detetada uma violação:
 - Proteger (*Protect*) – Não há notificação de violação;
 - Restringir (*Restrict*) - Há notificação de violação;
 - Desativar (*Shutdown*).

Dynamic Port Security por Omissão

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Configuração do *Dynamic Port Security*



Cisco IOS CLI Commands

S1(config) # interface fastethernet 0/18	Specify the interface to be configured for port security.
S1(config-if) # switchport mode access	Set the interface mode to access.
S1(config-if) # switchport port-security	Enable port security on the interface.

Configuração do *Port Security Sticky*



Cisco IOS CLI Commands

S1 (config) # interface fastethernet 0/18	Specify the interface to be configured for port security.
S1 (config-if) # switchport mode access	Set the interface mode to access.
S1 (config-if) # switchport port-security	Enable port security on the interface.
S1 (config-if) # switchport port-security maximum 50	Set the maximum number of secure addresses allowed on the port.
S1 (config-if) # switchport port-security mac-address sticky	Enable sticky learning.

Verificação do *Port Security Stick*



```
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
```

Verificação do *Port Security Stick*



```
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
```

Verificação do *Port Security*



```
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 *Error Disabled*

- Uma violação de segurança da porta pode colocá-la no estado de *error disabled*.
- Uma porta em *error disabled* está efetivamente desativada.
- O switch comunica estes eventos através de mensagens que envia para a consola.

```
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 *Error Disabled*

- O comando **show interface** revela a porta do switch num estado de *error disabled*.

```
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
```

Portas no Estado *Error Disabled*

- Para reativar a porta deve ser emitido um comando **shutdown** seguido de **no shutdown** na configuração da interface.

```
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
```