RD Press

Guia Básico para Configuração de Switches

Segurança

Switches 3Com, H3C e HP baseados no Comware

Diego Dias

RD PRESS

Guia Básico para Configuração de Switches – Segurança

Rotadefault.com.br
Comutadores.com.br
2018

Autor: Diego Dias
Revisão: Millena Mota/Ricardo Amaral

Índice

Quem deve ler esse livro?

A segurança em redes de computadores pode ser um assunto bastante complexo e extenso e que envolve diversos appliances e serviços. Nesse ebook direcionamos o conteúdo para as principais funcionalidades de proteção e de encaminhamento do tráfego legítimo na rede local.

Esse livro pode ser utilizado por técnicos ou administradores de switches da 3Com, H3C e HP, baseados no Comware e familiarizados com a configuração de VLANs e na comunicação entre as redes. O conteúdo e os comandos apresentado nesse material podem também ser aplicados por administradores de rede que gerenciam equipamentos de diversos fabricantes, visto que as principais funcionalidades citadas são utilizadas por quase todos os *vendors* do mercado.

Apesar do título do livro ser **Guia Básico para Configuração de Switches – Segurança**, o conteúdo abordado no eBook poderá ser relacionado também a materiais de Certificação, mas o foco do ebook não são os exames, e sim, os comandos e cenários do dia-a-dia de um administrador de Redes.

Agrego a esse material minhas experiências como administrador de redes de pequeno e médio porte, incluindo a administração de datacenters e projetos de segurança.

Agradecimentos

Gostaria de agradecer a minha familia pelo apoio e suporte, assim como aos meus amigos do Rota Default, por participarem direta e indiretamente desse projeto.

Louvo a Deus por tudo o que Ele tem me permitido viver.

'Porque Deus é o que opera em vós tanto o querer como o efetuar, segundo a sua boa vontade'. **Filipenses 2:13**

Capítulo

1

Introdução à segurança

Este capítulo é uma breve introdução a conceitos de Segurança da Informação como a tríade Confidencialidade, Integridade e Disponibilidade e o conceito de ameaças, riscos e vulnerabilidades.

A necessidade da alta disponibilidade dos serviços e o fornecimento de infraestrutura para os mais diversos tipos de dispositivos refletem aos administradores de rede novas preocupações referente a segurança dos dados.

Os equipamentos como notebooks, servidores, telefones IP, impressoras, *access points*, *smartphones*, IoT, entre outros necessitam da infraestrutura disponível para uso dos aplicativos relevantes para o negócio de cada empresas. Os switches da LAN, do ponto de vista dos negócios, são considerados como um agregador de portas para vazão do tráfego da rede local e por serem equipamentos de "fácil" configuração, dificilmente é pensando na segurança da informação durante a implantação de novos *switches*.

Existem inúmeras vulnerabilidades nos *switches* Ethernet e as ferramentas de ataque para explorá-los existem há mais de uma década. Um atacante pode desviar qualquer tráfego para seu próprio PC para quebrar a confidencialidade, privacidade ou a integridade desse tráfego.

A maioria das vulnerabilidades são inerentes aos protocolos da Camada 2 e não somente aos switches. Se a camada 2 estiver comprometida, é mais fácil criar ataques em protocolos das camadas superiores usando técnicas comuns como ataques de *man-in-the-middle* (MITM) para coleta e manipulação do conteúdo.

Para explorar as vulnerabilidades da camada 2, um invasor geralmente deve estar mesma rede local do alvo. Se o atacante se utilizar de outros meios de exploração, poderá conseguir um acesso remoto ou até mesmo físico ao equipamento. Uma vez dentro da rede, a movimentação

lateral do atacante torna-se mais fácil para conseguir acesso aos dispositivos ou tráfego desejado.

Caso o atacante esteja dentro o limite físico das organizações, é relativamente fácil encontrar um cabo Ethernet livre para conectar um *notebook* e obter acesso não autorizado à rede.

Com o DHCP amplamente implantado nas empresas e a quase inexistência de configurações de portas de Switches na rede local com autenticação (por exemplo, utilizando IEEE 802.1X), o PC de um usuário interno da empresa pode obter facilmente um endereço IP e, na maioria dos casos, possuir o mesmo nível de acesso à rede que todos os outros usuários autorizados. Uma vez obtido um endereço IP de rede, o usuário malicioso poderá executar inúmeros ataques.

Mesmo com a mudança do mercado fornecendo conectividade através de dispositivos móveis e notebooks via rede wireless, ainda sim se faz necessário a utilização de *switches* Ethernet para conexão de equipamentos como *firewall*, *access point*, servidores e roteadores.

Quando falarmos da movimentação de serviços para nuvem, ainda temos uma parte das informações de uma empresa trafegando pela rede sem criptografia podendo assim ser facilmente capturada e visualizada por ferramentas utilizadas por script kiddie, resultando no vazamento de informações e exposições de dados que podem ser extremamente prejudiciais a uma empresa, em alguns casos, causar repercussões financeiras significativas.

Por outro lado, voltando aos switches Ethernet, há configurações que podem fornecer recursos específico para aumentar a postura de segurança da rede local como a identificação dos usuários via 802.1X, segmentação de VLANs, listas de acesso, criptografia, e assim por diante.

Princípios da Segurança

A segurança da informação é uma área de estudo da computação que visa proteger os ativos de uma empresa ou indivíduo, com base na preservação de três princípios básicos: a **confidencialidade**, **integridade** e a **disponibilidade** das informações.

Esses três princípios básicos nos darão um norte para o estabelecimento de uma política de segurança.

Exemplo 1-1 *Principios Fundamentais da Segurança da Informação*

A Segurança deve cobrir os três aspectos e nenhum sistema ou protocolo pode ser considerado seguro, desde que a tríade não é cumprida. A falta de uma propriedade torna todo o sistema sem garantia.

Dependendo do propósito ou do uso de um sistema, uma parte da tríade pode ser mais importante do que outra; no entanto, nenhuma parte pode ser negligenciada.

Confidencialidade

Ter confidencialidade na comunicação é a capacidade de garantir que o que foi dito a alguém ou escrito em algum lugar será escutado ou lido apenas por que tiver direito.

A confidencialidade deve ser considerada com base no valor que a informação tem para a empresa ou para uma pessoa e os impactos que a sua divulgação indevida pode causar.

O acesso deve ser considerado com base no grau de sigilo, pois nem todas as informações sensíveis são confidenciais.

Integridade

Uma informação íntegra é aquela que não foi alterada de forma

indevida ou não autorizada. Para que as informações possam ser utilizadas, elas devem estar íntegras.

Quando há a alteração não autorizada de informações em um determinado documento, quer dizer que sua integridade foi perdida.

Se uma informação sofre alterações em sua versão original, então ela perde a sua integridade, ocasionando erros, fraudes e fazendo com que a comunicação e a tomada de decisões sejam prejudicadas.

A quebra de integridade ocorre quando as informações são corrompidas, falsificadas ou burladas.

Disponibilidade

Para que uma informação possa ser utilizada, ela deve estar disponível. A disponibilidade da informação considera toda a infraestrutura física e tecnológica que permite seu acesso, tráfego e armazenamento.

Garantir segurança na disponibilidade das informações é permitir que elas sejam utilizadas quando necessário e que estejam ao alcance de seus usuários e destinatários no momento em que precisam fazer uso.

Não basta que as informações estejam disponíveis: elas devem estar acessíveis de forma segura, para que possam ser usadas no momento em que são solicitadas, para que sua integridade e confidencialidade sejam garantidas.

Assim, o ambiente tecnológico e os suportes da informação devem estar funcionando corretamente e de forma segura, para que a informação neles armazenada e que por eles trafega possa ser utilizada pelos seus usuários.

Outros princípios que autores na área defendem que uma informação, para ser considerada segura, deve respeitar são: autenticidade, não repúdio, legalidade, privacidade e auditoria.

Risco, Ameaça e Vulnerabilidade

É praticamente impossível monitorar e eliminar todas as brechas em uma rede ou em um sistema pois os atacantes necessitam apenas de um pequeno espaço para causar um bom estrago. Algumas dessas brechas

são nativas na arquitetura dos protocolos ou suscetíveis a engenharia social, explorando a fraqueza do fator humano.

Apesar dos termos serem bastante utilizados em literaturas de segurança, compreender o significado dos termos Risco, Ameaças e Vulnerabilidades, ajudará na compreensão, planejamento e execução de políticas de segurança e mitigação de ataques:

Risco: é a medida da probabilidade da ocorrência de uma ameaça, associada à ocorrência de algum incidente, que exploram uma ou várias vulnerabilidades provocando alterações isoladas ou em conjunto na confidencialidade, integridade e disponibilidade.

Ameaça: é algum fato que pode ocorrer e acarretar algum perigo a um bem, causando perdas. As ameaças podem ser classificadas como naturais, voluntárias e involuntárias.

Vulnerabilidade é a fraqueza no sistema de proteção, que cobre uma ou mais ameaças. A fraqueza pode estar desde procedimentos, em produtos ou na implementação.

Classes de ataques

A maioria dos atacantes não quer ser descoberto e se utilizam de uma variedade de técnicas para permanecerem ocultos ao comprometer uma rede. As seções a abaixo listam os tipos de ataques mais comuns:

Reconhecimento: O ataque de reconhecimento é o primeiro processo de intrusão e tem como objetivo encontrar informações sobre a rede, usuários e vítimas. Incluir a varredura (scanning) da rede para descobrir quais os endereços IP que respondem e examinam quais portas desses dispositivos estão abertas. Este é geralmente o primeiro passo para descobrir o que há na rede e determinar quais vulnerabilidades explorar. As varreduras podem ser passivas ou ativas. Uma pesquisa passiva, chamada de footprint, pode ser realizada por um invasor por apenas pesquisar informações sobre os registros públicos da vítima, sites de redes sociais e outras informações como DNS, whois, e assim por diante. As varreduras ativas são realizadas por ferramentas denominadas "scanners".

Engenharia social: os ataques de engenharia social focam na parte mais fraca da segurança, que é o usuário humano. Isso pode ser feito utilizando de técnicas para ganhar a confiança de um funcionário e assim obter vantagens ou a informação desejada, por e-mail (phishing ou whaling) ou no redirecionamento de páginas da web, o que resulta no usuário

clicando em algo que leva ao atacante a ganhar as informações desejadas, como as credenciais por exemplo.

Denial of service(DoS): Os ataques de negação de serviço e os ataques distribuídos de negação de serviço (DDoS) tem como intenção bloquear degradar, desabilitar ou corromper redes, sistemas ou serviços com a intenção de negar o serviço a usuários legitimos, atacando a disponibilidade do recurso ou serviço. Exemplos comuns de ataques DoS inclui TCP SYN Flood, ICMP ping flood e buffer overflow.

Acesso de equipamentos de rede não autorizados

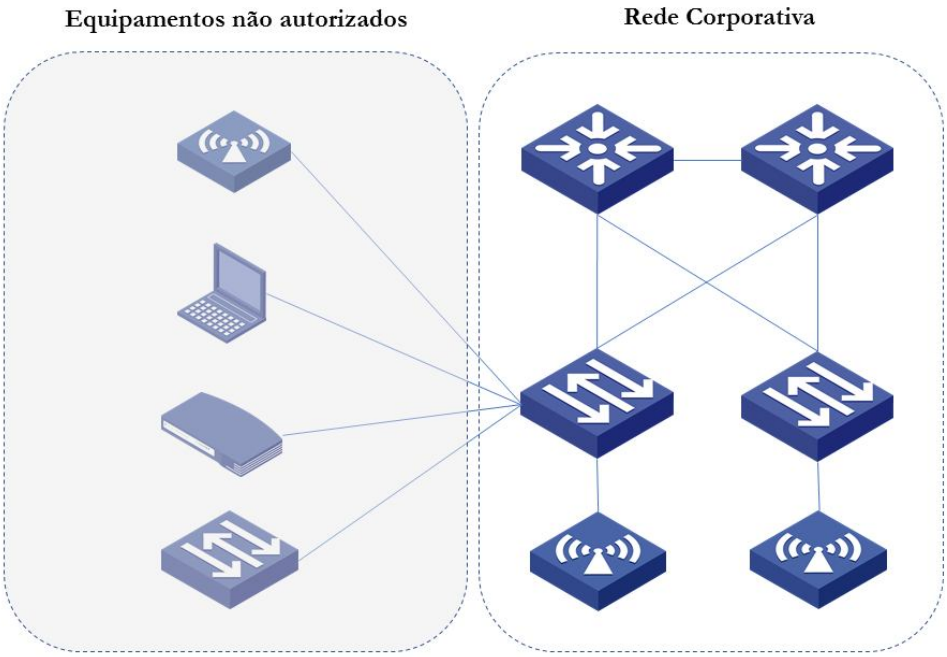
A utilização de equipamentos indevidos na rede é geralmente executada com equipamentos de baixo custo conectados a rede local sem consentimento do departamento de TI, por usuários locais devido a falta de uma política de segurança e/ou por atacantes internos (insider attackers). Entre esses equipamentos podemos listar:

Switches não gerenciados ou de baixo custo – esses equipamentos podem alterar a topologia STP da rede causando intermitência e indisponibilidade na convergência do protocolo, além de prover conectividade a dispositivos não previstos naquele determinado segmento da rede.

HUBs – podem causar os mesmos problemas de switches não gerenciados como também permitem ao atacante a interceptação bruta do trafego de rede, sequestro das sessões TCP, além de loop na rede.

Roteadores wireless - oferecem grandes riscos permitindo acesso indevido a rede local ou mesmo a interceptação de trafego pelo atacante.

Exemplo 1-2 *Conexão de equipamentos não autorizados a rede local*



Podemos também mencionar insider atackers que podem entrar em uma empresa (fisicamente) com um raspberryPi com um módulo Ethernet ou Wifi além de um modulo 3G/4G para o envio remoto dos dados (em casos de ataques de MITM ou spoofing). Há também bladeRF para exploração de vulnerabilidades em protocolos de voz e dados (3G, GSM e CDMA), apenas para citar.

Ataques específicos de Camada 2

Os ataques específicos disparados contra switches e protocolos de camada 2 do modelo OSI, podem ser agrupados da seguinte forma:

Ataques contra o gerenciamento e configuração - coletando informações do CDP, LLDP ou informações contidas em mensagens sem criptografia como SNMPv2, HTTP e Telnet.

Ataques utilizando endereços MAC - utilizando endereços únicos inválidos para “estourar” o limite de endereços MAC apreendidos por um Switch e transformar o Switch em um HUB.

Ataques Spoof - visam enganar alguns serviços como o DHCP, consumindo todos os endereços fornecido pelo Servidor, não permitindo que novas máquinas consigam endereços IP na rede gerando uma

negação de serviço(DoS) ou então uma máquina forjando um ser um servidor DHCP. A falsificação de endereços IP, MAC ou mensagens ARP também podem ser forjadas para ataques MITM.

Ataques de VLANs - forjam o VLAN ID para enganar Switches L3, burlando configurações de segurança. Os ataques de VLAN também podem buscar escutar mensagens validas dentro da própria VLAN para fins de movimentação lateral e etc.

Ataques de STP - visam causar indisponibilidades na rede, buscando alterar o root da rede.

Nos próximos capítulos daremos foco em grande parte dos ataques de camada 2 mencionados acima além de técnicas e configurações para mitigação de diversos ataques e as melhores práticas para hardening e envio de tráfego para ferramentas de analise e correlacionamento de logs.

Capítulo

2

Processo Learning e Forwarding

O processo de Learning e forwarding é responsável pelo aprendizado de endereços MAC e encaminhamento de quadros Ethernet por switches da rede local.

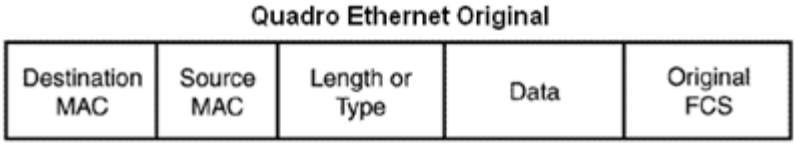
Uma rede de computadores consiste em dois ou mais dispositivos interligados entre si de modo a compartilhar recursos por um padrão de endereçamento lógico para comunicação, sendo o IP em suas versões IPv4 (endereços de 32 bits) e IPv6 (endereços de 128bits) o protocolo mais utilizado no mercado.

Utilizando um endereço IP e com o acesso devido para a Internet através de um roteador, um computador poderá comunicar-se com qualquer dispositivo conectado à Internet. De acordo com TANENBAUM (2003) “a Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns".

Nas últimas décadas, o padrão Ethernet se estabeleceu como protocolo dominante para as redes locais. A comunicação entre dispositivos em uma rede local utiliza-se dos endereços de hardware das placas de rede Ethernet, chamados de endereços MAC. Os Switches Ethernet fazem o encaminhamento de quadros (*frames*) baseado no endereço MAC de cada dispositivo. Essa atividade consiste em encaminhar os dados para o dispositivo correto.

Cada equipamento em uma rede Ethernet possui um endereço físico globalmente único. Um quadro Ethernet utilizado na comunicação entre os dispositivos possui em seu cabeçalho um campo para o endereço MAC de origem (*source* MAC) e o endereço MAC de destino (*destination* MAC). O *source* MAC contem o endereço da máquina de origem e o *destination* MAC contém o endereço que servirá para entregar os dados para um ou mais receptores.

***Exemplo 2-1** Formato quadro Ethernet*



Um switch Ethernet encaminha os quadros baseando-se na sua tabela de encaminhamento. Conforme inicia-se a comunicação entre os dispositivos, o Switch então aprende os endereços MAC ao escutar o tráfego da LAN. Essa tabela é zerada quando o equipamento é desligado.

O processo aprendizado de endereços MAC é feito de maneira dinâmica gerando a otimização e o consumo do link, tornando cada porta um domínio de colisão; ao invés de encaminhar o tráfego para todas as portas, como um HUB faz.

No exemplo 2-2 podemos visualizar o registro da tabela de endereços MAC aprendidos pelo Switch, assim como o mapeamento de cada porta.

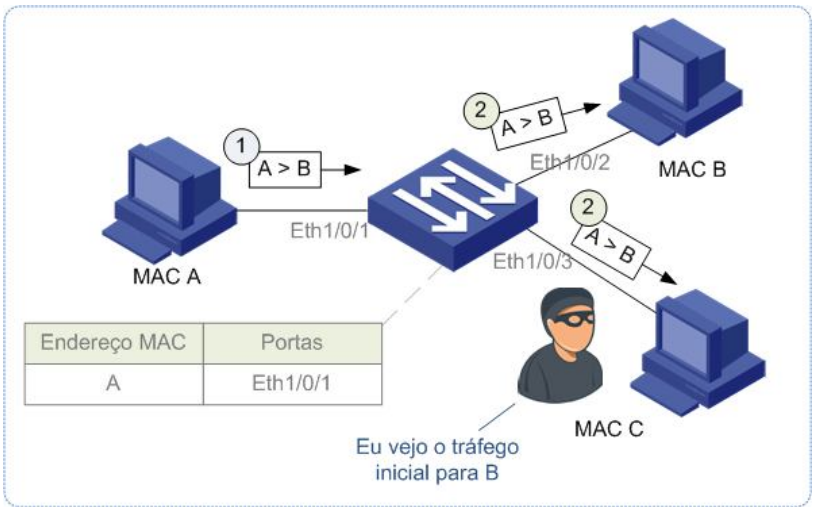
***Exemplo 2-2** Visualizando a tabela MAC de um Switch Comware*

```
[Switch] display mac-address
MAC ADDR       VLAN ID STATE    PORT INDEX    AGING TIME(s)

00e0-fc17-a7d6    1    Learned  Ethernet1/0/9   AGING
00e0-fc5e-b1fb    1    Learned  Ethernet1/0/8   AGING
00e0-fc55-f124    1    Learned  Ethernet1/0/8   AGING
```

No exemplo 2-3 ilustramos a comunicação inicial entre a máquina com o endereço MAC A para o endereço MAC B (para exemplos didáticos representamos o endereço MAC de maneira simplificada ao invés dos 6bytes).

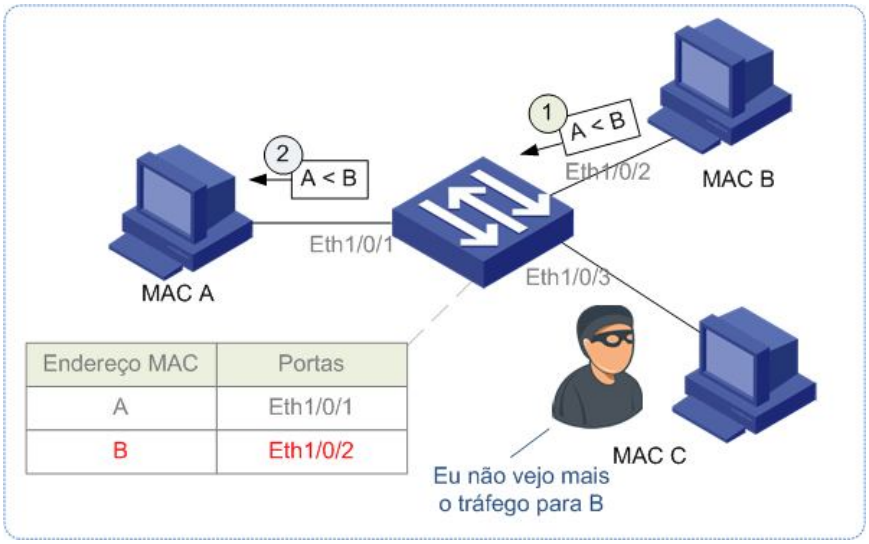
***Exemplo 2-3** Unknown Unicast Flooding*



Quando os dados enviados da máquina A para a máquina B chegam ao Switch é então adicionado o endereço MAC da máquina A (baseando-se no campo source MAC do cabeçalho Ethernet) na tabela de encaminhamento do Switch. Como ainda não há registro do endereço MAC B, o Switch encaminhará uma cópia do pacote para cada porta da VLAN onde o frame foi recebido (inclusive para outras máquinas).

A máquina com o endereço C poderá capturar com um sniffer apenas uma pequena porção do tráfego entre A e B (apenas as mensagens em broadcast utilizadas na detecção dos hosts), pois uma vez que a máquina B for retornar o tráfego para A, o switch terá em seus registros de endereços apenas os MACs aprendidos das portas Ethernet1/0/1 e Ethernet1/0/2 (máquina A e B respectivamente) e não encaminhará mais essa comunicação para todas as portas.

Exemplo 2-4 *Processo de aprendizado de endereços MAC*



Ataques de MAC Flooding

Todos os switches da LAN possuem uma tabela para aprendizado e encaminhamento de quadros Ethernet com um tamanho limitado e cada registro de endereço MAC ocupa um espaço de memória. Um switch pode armazenar centenas ou milhares de entradas MAC.

Quando determinado endereço MAC deixa de encaminhar ou receber tráfego na LAN, o switch remove a entrada (após um breve período). Dessa forma a tabela de endereços MAC recicla o espaço para entrada e registro de novos endereços ou mudança de endereços para outras portas, caso uma máquina mude de porta ou de Switch.

Em um ataque típico MAC Flooding, o atacante bombardeia o switch com quadros que contém diferentes endereços MAC, mudando randomicamente o endereço de origem em cada quadro. A intenção é consumir a memória que armazena a tabela de endereços.

Se o atacante conseguir manter a tabela de endereços MAC cheia, ele efetivamente transforma o Switch em um hub, permitindo que qualquer máquina possa coletar o tráfego daquela VLAN - inclusive conversas em unicast.

Alguns modelos de switches apenas travam e deixam de funcionar, mas a maioria entra no modo fail-open e começa a atuar como um hub.

Uma vez que o switch atua como um hub, o atacante pode assim usar um sniffer de pacote para capturar dados de outros computadores (como senhas não criptografadas, mensagens, VoIP e outros).

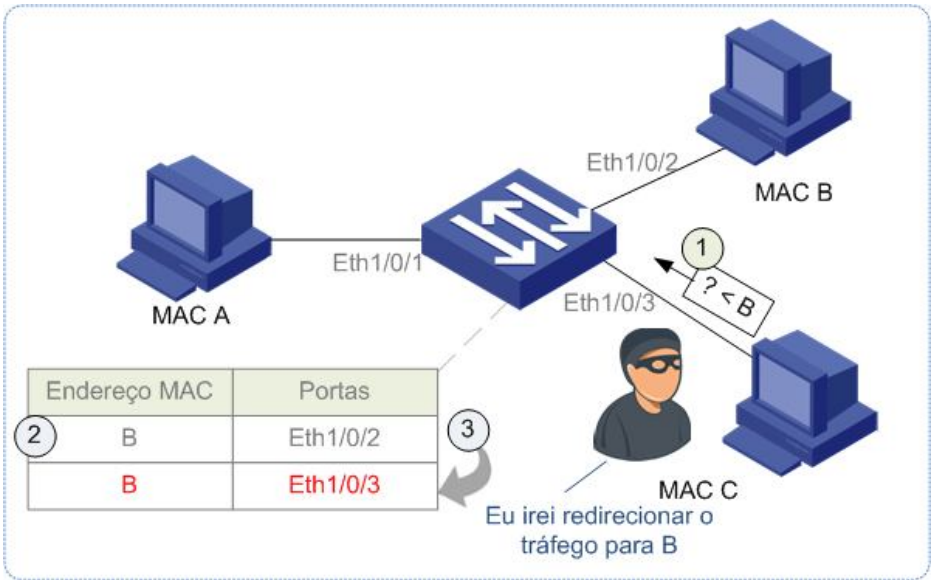
A ferramenta ***macof*** pode executar esse tipo de ataque e pode ser obtida no pacote ***dsniff***.

Ataques de MAC Spoofing

O ataque de MAC spoofing consiste em gerar um frame malicioso falsificando o endereço MAC da máquina alvo. O atacante gera registros falsos do endereço MAC de origem. Esse tipo de ataque gera um ataque de negação de serviço (DoS) ao host dono do endereço MAC verdadeiro.

O switch automaticamente troca a entrada do registro do MAC do host verdadeiro para a porta do ofensor (entrada mais recente), pois um mesmo endereço MAC unicast não pode residir em diversas portas de uma VLAN.

***Exemplo 2-5** Ataque MAC Spoofing*



Utilizando o Port Security para mitigar alguns ataques

O **port security** é uma funcionalidade de camada 2 que impõe limites para o número de endereços MAC permitidos (aprendidos) por uma determinada porta do switch e faz o registro dos endereços MAC válidos para aquela interface, de maneira estática ou dinâmica.

A feature **port security** permite o aprendizado dinâmico de endereços MAC vinculados a uma determinada interface Ethernet de um host para fins de segurança, não permitindo que outros dispositivos funcionem naquela interface; ou que aquele endereço MAC registrado funcione em outra porta. Se a condição não for satisfeita (a utilização do MAC correto), a porta entrará em estado de violação e não trafegará dados. A endereço MAC fica registrado na configuração da porta junto com o comando Port Sercurity.

A funcionalidade é bastante útil também em ambientes onde hosts e servidores precisam ser vinculados obrigatoriamente a uma porta (em ambientes como em CPDs e DataCenters) ou em localidades onde o usuário costuma migrar a estação sem comunicar a equipe de suporte!

Outro objetivo do **port security** é prevenir ataques de flooding de endeços MAC. Os ataques de flooding de endereços MAC consiste em forçar o Switch a popular a sua tabela de endereços MAC originando inumeras mensagens com endereço de origem falsos para superpopular a tabela MAC e forçar o Switch a atuar como hub.

O total de entradas permitidas para aquela interface com port security pode ser configurada com o comando '**port-security** *max-mac-count'.*

Configurando Port Security

Apesar do **port security** poder trabalhar com o 802.1X e/ou autenticação baseada em endereços MAC, ele pode ser configurado de maneira simples para validar e permitir o funcionamento de endereços MAC registrados localmente na porta do Switch, conforme exemplo abaixo:

Passo 1 - Acesse o modo system-view:

```
<Switch> system-view
```

Passo 2 - Habilite o processo port-sercurity globalmente

```
[Switch] port-security enable
```

Passo 3 - Acesse a interface e habilite o port-security

```
[Switch] interface interface x/y/z
[Switch-interface x/y/z] port-security max-mac-count [nº end. MAC]
[Switch-interface x/y/z] port-security port-mode autolearn
```

Passo 4 - Saia do modo de configuração

```
[Switch--interface x/y/z] quit
```

Exemplo 2-6 *Exemplo de configuração com port-security*

```
! Configurando o port-security
[Switch] port-security enable
! Habilitando o port-security no Switch
!
[Switch] interface gigabitethernet 1/0/1
[Switch-Ethernet1/0/1] port-security max-mac-count 1
! Habilitando o port-security para o aprendizado dinamico de
! apenas 1 endereço MAC (o primeiro descoberto)
!
[Switch-Ethernet1/0/1] port-security port-mode autolearn
! Habilitando o port-security para aprendizado dinamico do endereço
! MAC para interface Ethernet 1/0/1
```

Exemplo 2-7 *Validando a configuração e o erro após a troca de máquina da porta com port-security.*

```
! Validando a configuração
[Switch-Ethernet1/0/1] display this
```

```
#
interface GigabitEthernet1/0/1
port access vlan 10
port-security max-mac-count 1
port-security port-mode autolearn
port-security mac-address security 000a-aab2-a33b vlan 10
! Endereço MAC 000a-aab2-a33b aprendido dinâmicamente pela porta
#

! O log abaixo demonstra uma violação após substituir a máquina real
! por uma máquina com outro endereço MAC

%Apr 26 17:23:01:527 2000 SBSSWCOR03 PORTSEC/1/VIOLATION:
OID: 1.3.6.1.4.1.43.45.1.10.2.26.1.3.2
An intrusion occurs!
IfIndex: 9437189
Port:Ethernet1/0/1
MAC Addr: 00:0F:DF:B4:FA:49
VLAN id:10
IfAdminStatus: 1
```

Após o aprendizado do endereço MAC, a porta não permitirá a conexão de outra máquina na interface Ethernet 1/0/1. O endereço aprendido na interface não poderá ser utilizado em outra interface no mesmo Switch. Sugerimos não configurar o Port-Security em interfaces trunk.

Manipulando a entrada de endereços MAC.

Há também a possibilidade (um pouco mais limitada) de somente restringir a quantidade de endereços MAC aprendidos em uma porta com o comando **mac-address max-mac-count** [*quantidade*].

No exemplo abaixo executamos um ataque de mac flooding contra um Switch 3Com que possui sua tabela MAC para até 8k (oito mil) endereços MAC. Demonstramos um ataque executado com a ferramenta *macof* ao switch da rede local com a configuração padrão.

Exemplo 2-8 *Executando o mac flooding*

```
linux:/# macof -i eth0 -n 10000
! Disparando mac flooding com 10k endereços MAC

[Switch]display mac-address count
 ---  8191 mac address(es) found
! Validando a quantidade de endereços MAC aprendidos pelo Switch
```