UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

RONALDO JOSÉ CZELUSNIAK

SEGURANÇA EM CAMADA 2

MONOGRAFIA

CURITIBA
2013

RONALDO JOSÉ CZELUSNIAK

SEGURANÇA EM CAMADA 2

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores
Orientador: Prof. MSc. Juliano De Mello Pedroso.

CURITIBA
2013

RESUMO

CZELUSNIAK, Ronaldo J. **Segurança em camada 2**. 2013. 32 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

A presente monografia se propõe a abordar a segurança na camada 2 dos modelos de referência OSI e TCP/IP, referenciando as melhores praticas em segurança destes equipamentos e protocolos, demostrando soluções aplicáveis a redes de pequeno a grande porte e demostrando na prática um ataque muito comum nos dias atuais, devido a crescente popularidade da internet.

Palavras-chave: Redes de Computadores. Segurança de Redes. Segurança em Camada 2, Enlace de Dados, Segurança da Informação.

LISTA DE SIGLAS

MAC - Media Access Control

DHCP - Dynamic Host Configuration Protocol

ARP - Address Resolution Protocol

STP - Spanning tree protocol

VLAN - Virtual Local Area Network

OSI - Open Systems Interconnection

ISO - International Organization for Standardization

HTTP - Hypertext Transfer Protocol

SMTP - Simple Mail Transfer Protocol

POP - post office protocol

IMAP - Internet Message Acess Protocol

DNS - Domanin Name System

RDP - Remote Desktop Protocol

TCP - Transmission Control Protocol

IP - Internet Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

UDP - User Datagram Protocol

FTP - File Transfer Protocol

ICMP - Internet Control Message Protocol

RIP - Routing Information Protocol

OSPF - Open Shortest Path First

IGMP - Internet Group Management Protocol

BGP - Border Gateway Protocol

RFC - Request for Comments

IEEE - Institute of Electrical and Eletronics Engineers

BPDUs - Bridge Protocol Data Units

CAM - content Addressable Memory

DTP - Dynamic Trunking Protocol

GARP - Gratuitous ARP

LDAP - Lightweight Directory Access Protocol

NTP - Network Time Protocol

LAN - Local Area Network

LLC - Logical Link Control

LISTA DE ILUSTRAÇÕES

SUMÀRIO

1. INTRODUÇÃO

Vivemos em mundo cada vez mais digital, onde paradigmas e costumes são desfeitos todos os dias, o jornal impresso perdeu seu espaço e o bombardeio de informação vem de todos os lados, a internet mudou o comportamento do mundo, o jeito de se comunicar, de se relacionar, de aprender, uma fonte de informação imensurável, e que pode estar no seu bolso, no seu escritório, na sua casa, na rua ou onde você desejar. Produzimos, compartilhamos e consumimos informação a uma velocidade incrível.

No meio corporativo não é diferente, o volume de dados cresce exponencialmente e o valor desses dados também, empresas inteiras estão dentro de storages locados nas próprias empresas ou em algum lugar do mundo em grandes data centers.

O grande valor desses dados para as corporações requer uma dose grande de segurança, porém nem todas as empresas tem esse cuidado, falta de profissionais qualificados, autoconfiança e cortes no orçamento são os principais fatores que colocam em risco a segurança da informação segunda a pesquisa *The Global State of Information Security® Survey* 2013 realizada pela PWC a pesquisa revela também que as empresas que verdadeiramente lideram na área de segurança da informação empregam, muito mais que as outras, estruturas integradas que combinam gestão de risco, compliance, segurança da informação, privacidade de dados, gestão de identidades digitais e gestão de continuidade de negócios. Além disso, entendem que os objetivos organizacionais devem impulsionar o programa de segurança da informação.

Neste trabalho iremos abordar a segurança da informação do âmbito interno das organizações, a rede interna e responsável pela maior parte dos ataques, devido a sensação de segurança que ele parece ter, mostrarei a seguir os principais riscos as redes internas e algumas formas de deixa-las mais seguras.

1.1 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.1.1. Objetivo Geral

O objetivo principal deste projeto e demonstrar os principais riscos a segurança na camada 2 e como mitiga-los.

1.1.2. Objetivos Específicos

- Embasamento Teórico;
- Ataques MAC;
- Ataques ARP;
- Ataques STP e VLANs;
- Ataques DHCP;
- Segurança física;
- Segurança de acesso;

2. REFERENCIAIS TEÓRICOS

2.1 REDES DE COMPUTADORES

2.1.1. Modelo de referência OSI

O modelo de referência OSi (*Open Systems Interconnection*) foi baseado na proposta desenvolvida pela ISO (*International Standards Organizition*), o modelo OSI foi desenvolvido a fim de padronizar a comunicação entre sistemas abertos possibilitando assim a comunicação entres dispositivos e aplicações de fabricantes distintos. A criação desse modelo se propõe a realizar a interoperabilidade, compatibilidade, portabilidade e escalabilidade nas redes de computadores.

O modelo e baseado em camadas ou níveis, cada camada oferece um conjunto de serviços a camada superior, para isso cada camada utiliza seus

próprios serviços e os serviços das camadas inferiores conforme figura 1, no total são 7 camadas que compõe o modelo, Fisica, enlace, rede, transporte, sessão, apresentação e aplicação.

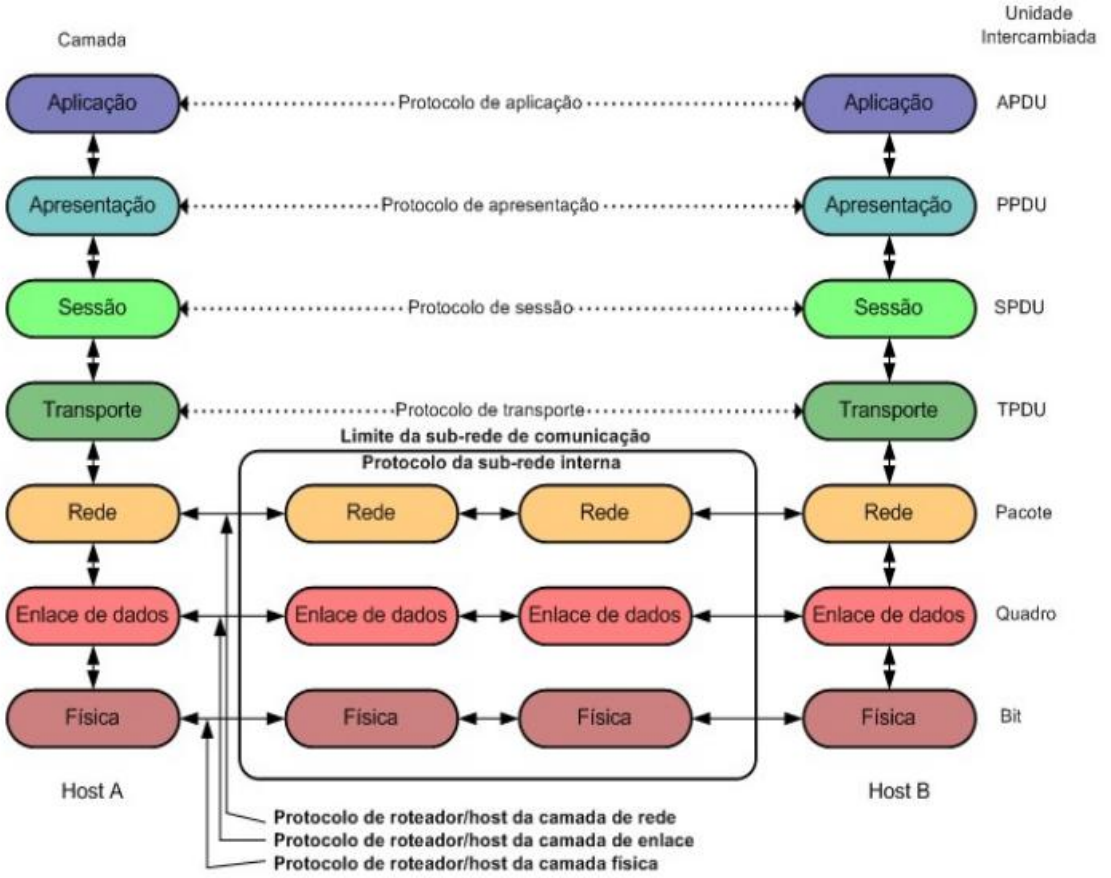

Figura 1 - Modelo OSI
Fonte: Tanenbaum, 2003

As figuras 2 e 3 mostram as funções exercidas por cada camada e a divisão entre camadas de host e camadas do meio.

Figura 2- Funções das camadas do modelo OSI
Fonte: Tanenbaum, 2003

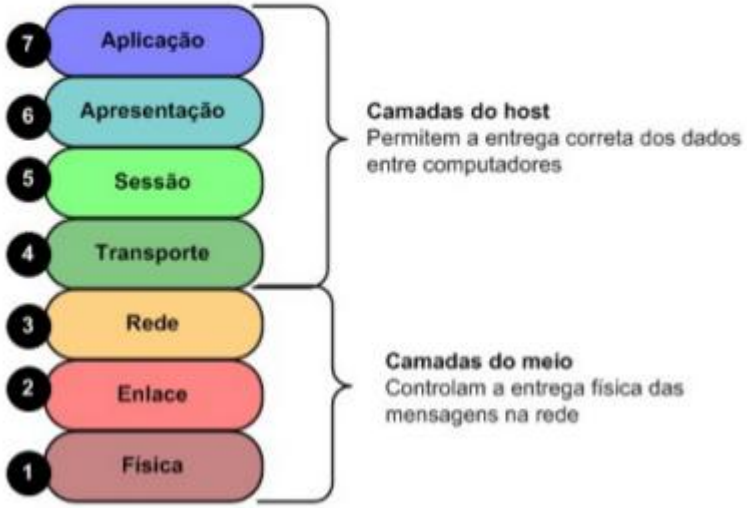

Figura 3 - Divisão das camadas de host e meio.
Fonte: Tanenbaum, 2003

A seguir descreverei brevemente a função de cada camada, com ênfase apenas na camada de enlace de dados por ser uma das partes mais relevante a esse trabalho.

2.1.1.1 Camada Física

Sua responsabilidade e transmitir e receber os bits em uma comunicação, segundo Tanenbaum, 2003 a camada física deve garantir que

quando um lado enviar um bit 1, o outro lado o receberá como um bit 1, não como um bit 0.

Principais funções da camada física são controle da voltagem durante a transmissão, ou seja quantos nano segundos um bit irá durar, se o comunicação será apenas em um sentido ou nos dois sentidos, controle quando será iniciada a transmissão do bits e quando será finalizada a transmissão e também define quantos pinos o cabo de rede terá e define a função para cada um dos pinos.

2.1.1.2 Camada de Enlace

A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruta em uma linha que pareça livre de erros de transmissão não detectados para a camada de rede. Para executar essa tarefa, a camada de enlace de dados faz com que o transmissor divida os dados de entrada em quadros de dados (que, em geral, têm algumas centenas ou alguns milhares de bytes), e transmita os quadros sequencialmente. Se o serviço for confiável, o receptor confirmará a recepção correta de cada quadro, enviando de volta um quadro de confirmação. (TANENBAUM, ANDREW S., 2003, p.46)

Outra função da camada de enlace e gerenciar o fluxo de dados para que um transmissor rápido não transmita mais dados que um receptor lento pode receber.

Uma sub-camada é responsável pelo controle de acesso ao meio, a sub-camada MAC (Media Access Control) tem a função de evitar colisões de pacotes gerenciando o acesso ao meio.

2.1.1.3 Camada de Rede

A camada de rede é responsável por determinar como os pacotes serão roteados da sua origem até o destino, para isso são utilizadas rotas, as rotas são os caminhos que o pacote irá trafegar até o seu destino, as rotas podem ser estáticas, adicionadas uma a uma manualmente ou rotas dinâmica que são atribuídas através de protocolos de roteamento.

O tratamento dos problemas encontrados nas rotas também faz parte da camada de rede, como a verificação de fluxo alto em um rota, um rota instável ou que não está mais disponível, problemas de endereçamento de rede.

2.1.1.4 Camada de Transporte

Sua função e receber os dados da camada superior dividi-los em segmentos menores caso seja necessário e garantir que os dados enviado cheguem até seu destino, fazendo isso de forma transparente para as camadas superior para que as alterações das camadas inferiores não interfiram nas superiores.
Também e função da camada de transporte garantir que a entrega sequencial e ordenada de bytes na mesma sequencia em que o segmento foi enviado.

2.1.1.5 Camada de sessão

A camada de sessão tem a função de estabelecer sessões entre o host de origem e o de destino, controlando quando cada um deve enviar, verificando em transmissões longas a fim de permitir que a transmissão continue de onde parou em caso de erros.

2.1.1.6 Camada de Apresentação

Trata a sintaxe e a semântica dos dados, responsável por converter os dados recebidos da camada de aplicação em um formato padrão para transmissão desse dado, também realiza a compactação dos dados para serem envias mais rapidamente.

2.1.1.7 Camada de Aplicação

No topo do modelo OSI essa camada faz a interação entre o host e usuário, neles estão os aplicativos utilizados pelos usuários como HTTP, SMTP, POP, IMAP, DNS, RDP entre outros.

2.1.2 Modelo TCP/IP

O TCP/IP é baseado num modelo de referência de quatro camadas. Todos os protocolos pertencentes ao conjunto de protocolos TCP/IP estão localizados nas três camadas superiores deste modelo.

Conforme a figura 4, cada camada do modelo TCP/IP corresponde a uma ou mais camadas do modelo de referência OSI.

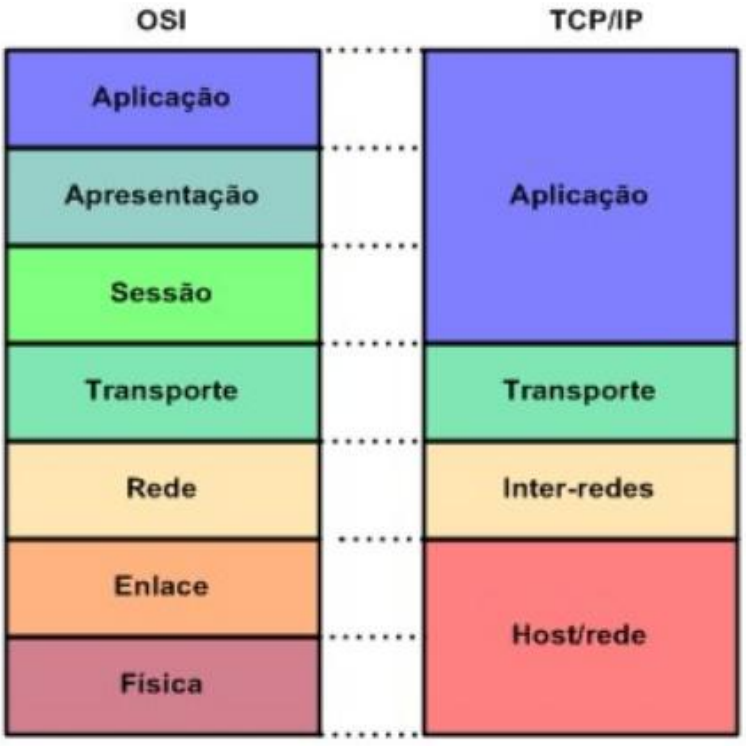

Figura 4 – Comparativo modelo OSI e TCP/IP.
Fonte: Tanenbaum, 2003

De acordo com Tanenbaum (2003), o modelo TCP/IP não possui as camadas de sessão e apresentação por serem pouco usadas na maioria das aplicações.

A figura 5 exibe o modelo TCP/IP com suas camadas e protocolos, que são descritos a seguir.

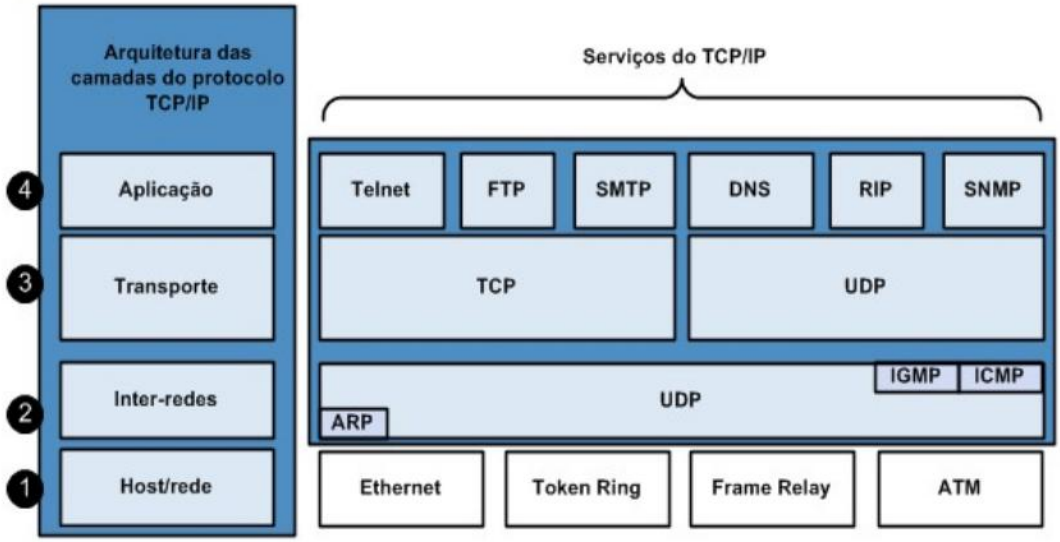

Figura 5 - Camadas e os protocolos no modelo TCP/IP.
Fonte: Tanenbaum, 2003

2.1.2.1 Camada inter-redes

A camada inter-redes integra toda a arquitetura. É responsável por permitir envio de pacotes pelos hosts em qualquer rede garantindo que eles trafeguem independentemente até o destino, talvez em uma rede diferente, entregando pacotes IP onde eles são necessários. Também conhecida com camada internet, a sua função é de endereçamento, roteamento e controle de envio e recepção de pacotes, não é orientada a conexão e faz sua comunicação através de datagramas.

2.1.2.2 Camada de transporte

Esta é uma camada fim a fim, ou seja, as entidades se comunicam em pares formados pelo host de origem e outro de destino, da mesma forma como é realizada no modelo OSI.

Dois protocolos fim a fim são definidos nesta camada, o *Transmission Control Protocol* (TCP) e *o User Datagram Protocol* (UDP). O TCP é um protocolo orientado a conexão que permite a entrega sem erros de fluxo de

bytes, retransmitindo-os se for necessária, cuida do controle de fluxo, impedindo que um emissor rápido sobrecarregue um receptor lento com um volume de mensagens maior do que pode processar.

O UDP não é orientado a conexão e não confiável destina-se a aplicações que não desejam o controle do fluxo e nem que se preocupem com a ordem da mensagem enviada. Desta forma o UDP é um protocolo mais rápido por requerer menos processamento.

2.1.2.3 Camada de aplicação

Compostos pelos protocolos utilizados das diversas aplicações do modelo TCP/IP não possui um padrão comum, sendo o padrão estabelecido por cada aplicação, ou seja, o FTP possui suas próprias regras, assim como o TELNET, SMTP, POP, DNS, etc.

2.1.2.4 Camada host/rede

O modelo TCP/IP não especifica muito bem o que acontece nesta camada, exceto pelo fato de que o host tem de se conectar à rede utilizando algum protocolo para que seja possível enviar pacotes IP. É um protocolo por não ser definido varia de host para host e de rede para rede. Esta camada além utilizar protocolo IP também faz uso de outros como o *Internet Control Message Protocol* (ICMP), *Routing Information Protocol* (RIP), *Internet Group Management Protocol* (IGMP), *Open Shortest Path First* (OSPF) e *Border Gateway Protocol* (BGP).

2.2 PROTOCOLOS

Serão descritos a seguir os protocolos mais vulneráveis as ataques na camada de enlace, além do funcionamento do endereçamento físico em uma LAN.

2.2.1 MAC

O *MAC-ADDRESS* é o endereço físico atrelado ao adaptador de rede de um host, ele e composto por 48bits e é responsável por identificar o host na rede.

Os Fabricantes de adaptadores solicitam a uma autoridade central uma faixa de endereços para serem utilizados em seus adaptadores, a fim de garantir que dois adaptadores não possam ter o mesmo *mac-address* em uma rede local, pois caso isso ocorra um conflito será gerado, Esses endereços de *mac-addres* são utilizados na comutação dos dados na rede local.

2.2.2 ARP

O protocolo ARP opera na camada de enlace, é definido pela RFC826 (*request for comments*) e é um protocolo utilizado pela pilha TCP/IP. Seu propósito é converter endereços IP da camada de rede que possuem 32 bits, em endereços físicos (camada1), de 48 bits, para transmissão de dados em uma rede Ethernet da mesma forma que em uma rede TCP/IP, cada elemento de uma rede Ethernet também deve possuir um endereço único para identificá-lo.

2.2.3 Spanning Tree

Spanning-Tree Protocol (STP), conforme definido na IEEE 802.1D é um protocolo de gerenciamento de link, que fornece redundância de caminhos, evitando loops indesejáveis na rede. Para uma rede Ethernet funcionar corretamente, apenas um caminho ativo pode existir entre duas estações. Loops ocorrem em redes por uma variedade de razões, a razão mais comum é gerar um loop na tentativa de criar caminhos redundantes entre os switches, para caso o link principal falhe o alternativo assuma o trafego.

O STP possibilita que switches se comuniquem a fim de evitar loops na rede, o algoritmo do STP fornece condições para que os switches troquem informações para criar uma topologia livre loops por mais que haja mais de um link entre dois switches, para isso o STP utiliza os pacotes BPDUs (*Bridge*

Protocol Data Units) para a troca de informações de status entre os switches, é através dessa comunicação que o STP elege um switch raiz e sua porta raiz, bem como a porta raiz e as portas designadas do outros switches da rede.

Após analisar a topologia toda, o STP então deixa apenas o melhor caminho habilitado e bloqueia todos os outros caminhos, porém caso o caminho que está encaminho o trafego para de funcionar, a topologia e refeita e outro caminho é ativo.

2.2.4 DHCP (Dynamic Host Configuration Protocol)

O Protocolo DHCP é responsável pela distribuição de endereços IPs dinamicamente a hosts de uma rede e foi definido através das RFCs a seguir:

- RFC 2131 - DHCP
- RFC 2132 - *DHCP Options and BootP Vendor Extensions*
- RFC 1534 - *Interoperation between DHCP and BootP*
- RFC 1542 - *Clarifications and Extensions for the BootP*
- RFC 2241 - *DHCP Options for Novell Directory Services*
- RFC 2489 - *Procedure for Defining New DHCP Options*

Conforme RFC 2132 o processo da distribuição de endereços funciona conforme figura 6.

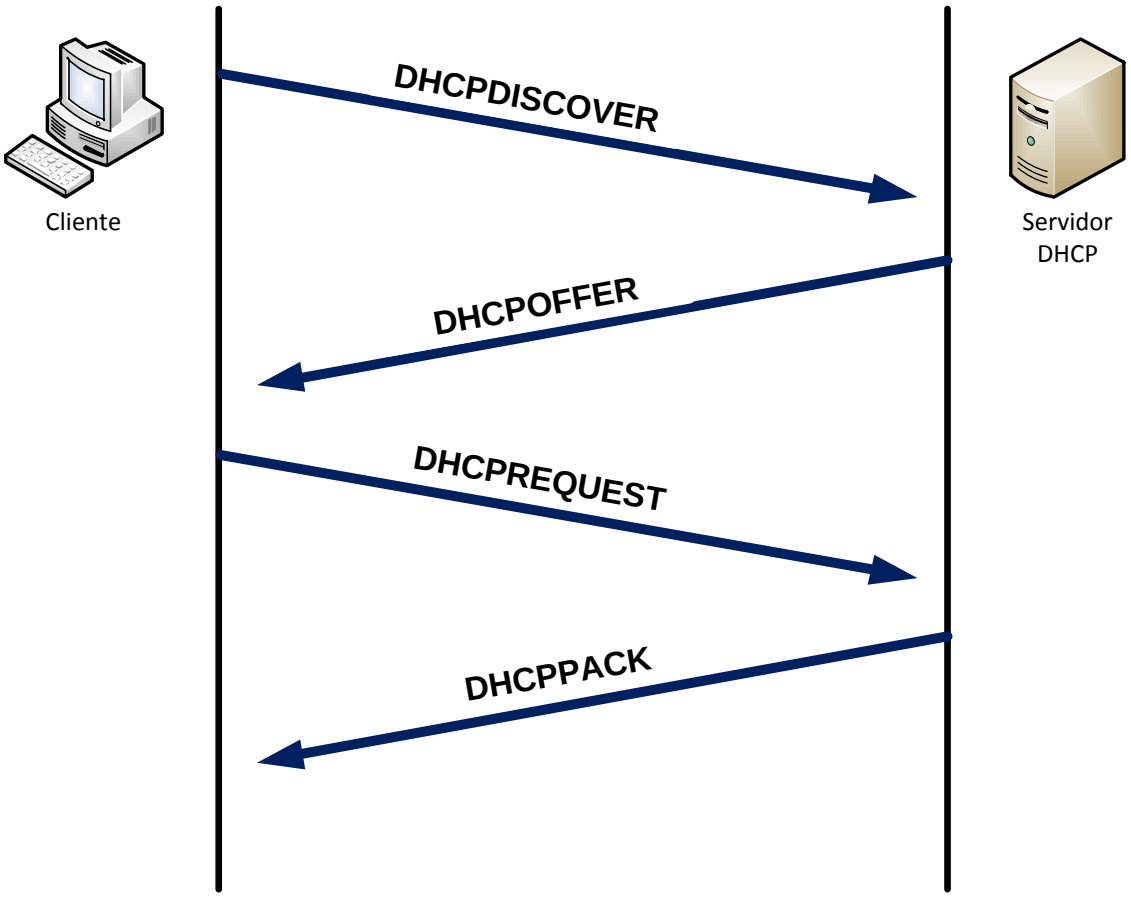

Figura 6 – Negociação de endereçamento DHCP.
Fonte: Autoria própria.

Quando um novo host é conectado a rede e não possui um endereço IP o host envia um pacote DHCPDISCOVER para o endereço de broadcast (255.255.255.255) na porta 67 UDP (BOOTP) em sua sub-rede local, com o IP de origem 0.0.0.0 pois ainda não possui um IP, caso haja um servidor DHCP configurado nessa sub-rede, ele irá responder o host com um pacote DHCPOFFER, se o servidor DHCP estiver em outra sub-rede, será necessário um agente de retransmissão para que a comunicação entre host e servidor acontece, uma vez que a solicitação e feita através de broadcast, esse agente pode ser um servidor ou roteador por exemplo.

Após receber o pacote DHCPOFFER o host responde o servidor DHCP com um pacote DHCPREQUEST aceitando a oferta e requisitando assim um endereço IP, em seguida o servidor DHCP envia um pacote DHCPPACK com o endereço IP e suas opções como gateway padrão, DNS e etc.

3 Ataques a camada de enlace

3.1 Inundação da tabela CAM

A tabela CAM (*Content Addressable Memory*) num comutador contém informações como endereços MAC disponível em uma determinada porta física, assim como os parâmetros associados de VLAN. Quando um switch *Layer* 2 recebe um quadro, o switch verifica na tabela CAM para localizar o endereço MAC de destino. Se existe uma entrada para o endereço MAC na tabela CAM, o switch encaminha o quadro para a porta designada na tabela CAM para esse endereço MAC. Se o endereço MAC não existe na tabela CAM, o switch encaminha o quadro a cada porta do switch, atuando como se fosse um hub, se houver resposta, o switch atualiza a tabela CAM.

Na figura 7 o host A envia o tráfego para o host B, o switch recebe os quadros e procura o endereço MAC de destino em sua tabela CAM. Se o switch não pode encontrar o destino MAC na tabela CAM então copia o quadro e transmite-o de todas as portas do switch (i). O host B recebe o quadro e envia de volta uma resposta para o host A. O switch então vê que o endereço MAC do host B está localizado na porta 2 e grava essas informações na tabela CAM (ii). Agora, qualquer quadro enviado pelo host A (ou qualquer outro host) para o host B será simplesmente encaminhado à porta 2 do switch e não transmitir a todas as portas, como foi feito anteriormente (iii).

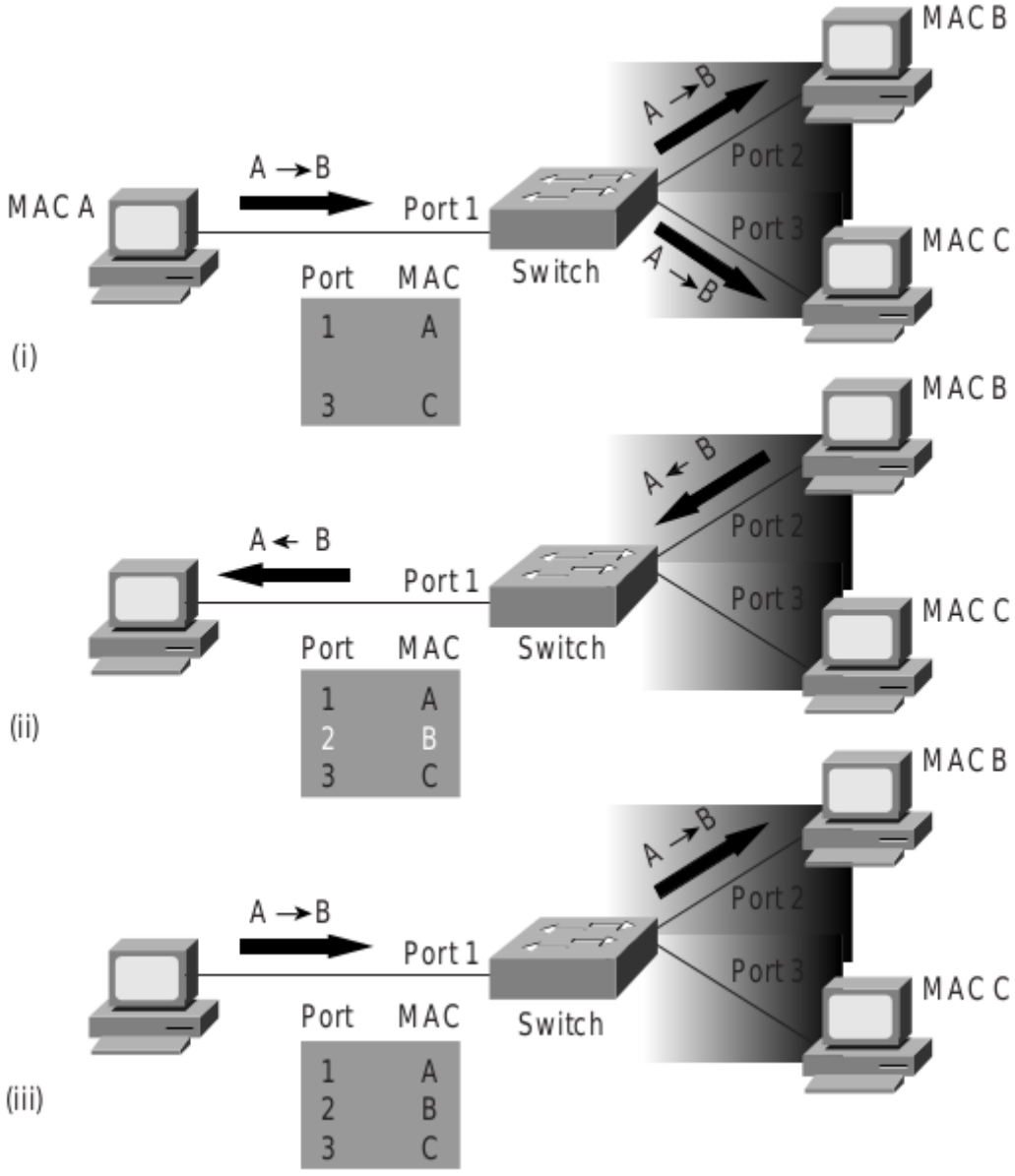

Figura 7 – Resolução de endereços físicos.
Fonte: Cisco Systems.

A tabela CAM tem um tamanho limitado. Se todo o espaço disponível na tabela CAM for ocupado antes que outras entradas expirem, a tabela CAM enche a tal ponto que as novas entradas não poderão ser aceitas. Normalmente intrusos na rede inundam o switch com uma grande quantidade *mac-addres* inválidos até que a tabela CAM do switch esgote seu espaço, quando isso acontece o switch irá enviar a todas as portas todo o trafego de entrada, porque com a tabela CAM lotada ele não consegue encontrar o *mac-address* e a porta especifica, o switch então começa a funciona como um hub.

Caso o intruso não continue a enviar os endereços MAC inválidos após determinado período as entradas mais velhas na tabela irão expirar e o switch voltará a funcionar como um switch novamente. A inundação da tabela CAM irá funcionar apenas dentro da VLAN em que o intruso está conectado.

Na figura 8 o host com endereço MAC C está enviando vários pacotes com diferentes endereços MAC de origem, depois de um curto período de tempo na tabela CAM no switch enche até que ele não possa mais aceitar novas entradas, a tabela permanecerá lotada até que o host MAC C pare o ataque. Com a tabela cheia o switch começa a transmitir todos os pacotes que recebe para todas as portas conforme ilustração (ii) da figura 8, possibilitando ao atacante receber todo o trafego que passa por aquele switch.

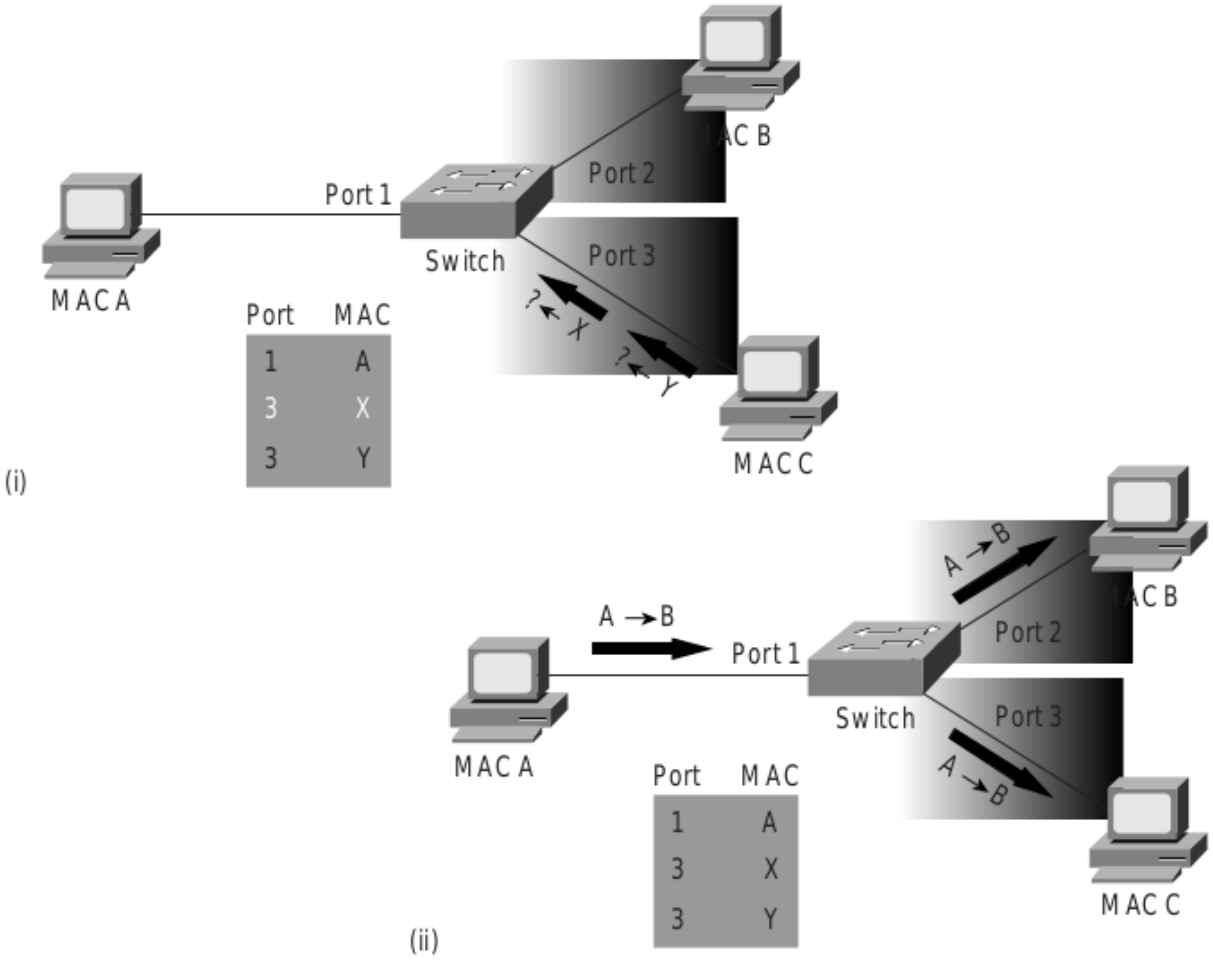

Figura 8 – Inundação da tabela CAM.
Fonte: Cisco Systems.

3.1.1 Como prevenir/mitigar

O ataque a tabela CAM podem ser mitigados através da configuração de segurança de porta no switch. Com a segurança de porta habilitada é possível especificar o MAC em uma porta ou limitar o números de endereços que podem ser associados a aquela porta, assim quando um endereço MAC inválido for detectado na porta, o switch pode bloquear o endereço MAC do agressor ou desligar a porta. Especificando endereços MAC de cada porta do switch pode ser muito trabalhoso em um ambiente grande, limitar o número de endereços MAC em uma porta do switch pode ser a opção mais viável em muitos casos.

3.2 VLAN Hopping

VLAN *hopping* é um ataque à rede em que o intruso envia pacotes

destinados a um host em uma VLAN diferente, que normalmente não podem ser alcançados pelo intruso. Este tráfego é marcado com um ID de VLAN diferente da que o intruso pertence. Ou então, o intruso pode estar tentando se comportar como um switch e negociar entroncamento para que ele possa enviar e receber tráfego entre outras VLANs diferente da dele.

Switch-Spoofing - Em um ataque de VLAN Hopping, o intruso da rede configura um sistema para se passar por um switch, isso exige que o intruso seja capaz de emular o protocolo ISL ou 802.1q juntamente com o DTP (*Dynamic Trunk Protocol*). Sendo assim capaz de simular uma porta trunking e negociar através do DTP com outro switch e caso obtenha sucesso, o intruso será membro de todas as outras vlans.

3.2.1 Como prevenir/mitigar

Desabilite o DTP em todas as portas e habilite manualmente apenas nas portas que forem necessárias.

3.3 VLAN - Marcação Dupla

Marcação Dupla ou *Double Tagging* é outra versão deste ataque de rede que envolve a marcação dos quadros transmitidos com dois cabeçalhos 802.1q, com a intenção de encaminhar os quadros para uma vlan a qual ele não pertence. Após encaminhar o quadro com dois cabeçalhos 802.1q o primeiro switch que receber o quadro retira o primeiro cabeçalho e encaminha o quadro para todas as portas na vlan correspondente ao primeiro cabeçalho, encaminhando também para as portas trunks, quando esse quadro chegar a uma porta trunk e for enviado ao próximo switch, o quadro chegará com o segundo cabeçalho e com a vlan que o atacante pretende alcançar, o switch então ira verificar o cabeçalho e encaminhará o quadro a todas as portas na vlan secundária.

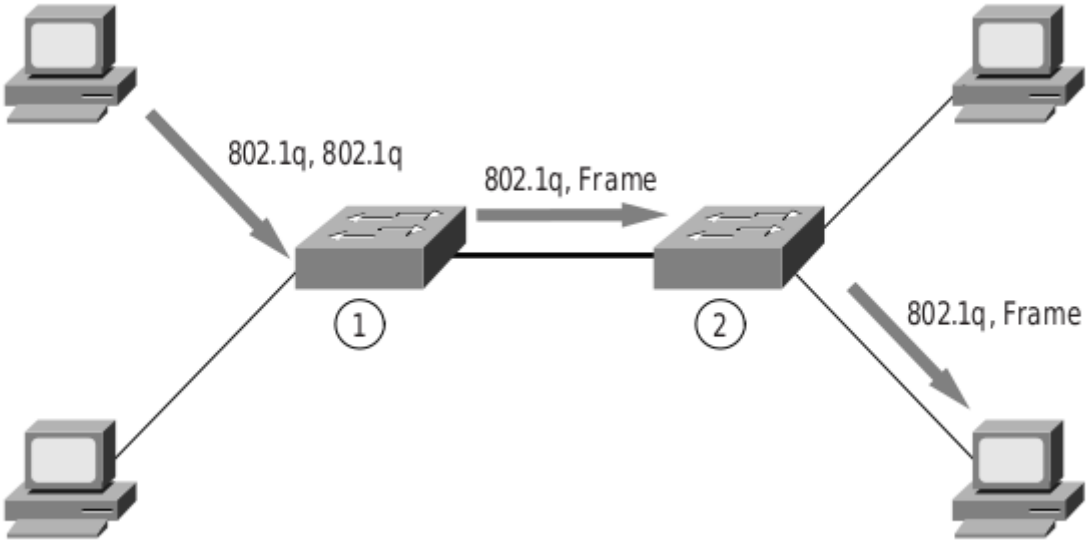

Figura 9 – ilustração marcação dupla de VLAN.
Fonte: Cisco Systems.

3.3.1 Como Prevenir/Mitigar

Para prevenir esse tipo de ataque além de habilitar o DTP apenas nas portas necessárias você pode também modificar a vlan nativa das portas trunks, pois só é possível executar um ataque de dupla marcação se a vlan nativa do intruso for a mesma da vlan nativa do trunk.

3.4 Manipulação de Spanning-Tree

Outro ataque contra switches consiste em interceptar o tráfego atacando o protocolo *Spanning-Tree.* Ao atacar o protocolo *Spanning-Tree*, o atacante se passa por um switch e começa enviar BPDUs de melhor prioridade, se o atacante obtiver sucesso o *Spanning-Tree* recalculará sua topologia e o atacante passará a ser a root bridge da topologia e passará a receber todo o trafego comutado entre os switches, Segundo Convery (2004) esse ataque é possível devido ao fato do STP não exigir autenticação dos BPDUs trocados entre os switches.

Os critérios para eleger uma root bridge são menor prioridade e em caso de empate vence o switch com menor MAC.

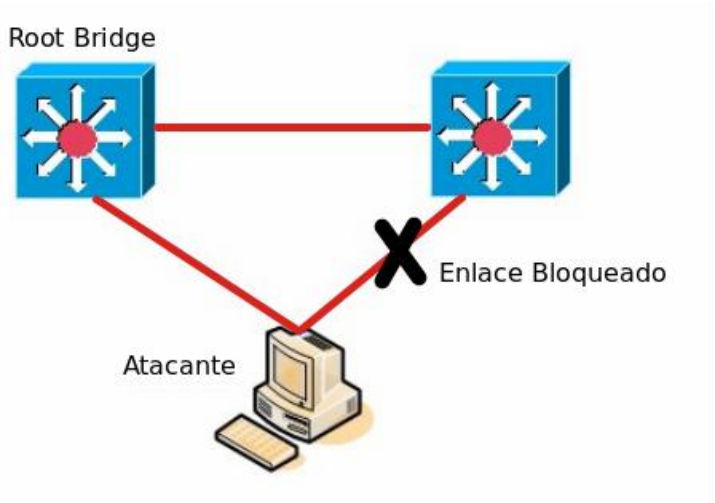

Figura 10 – STP Topologia normal.
Fonte: Autoria própria.

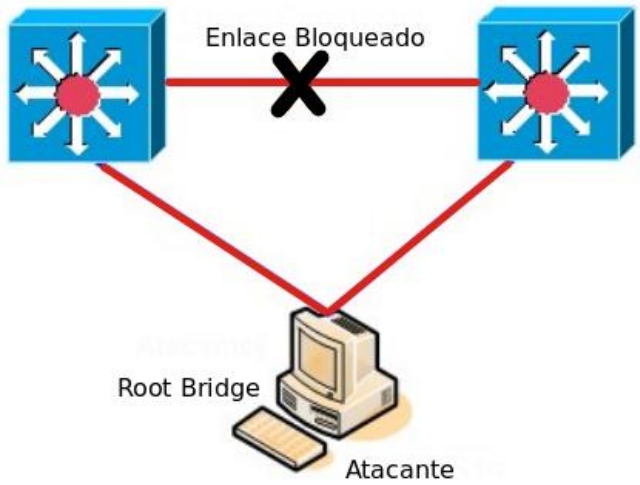

Figura 11 – STP Topologia em Ataque.
Fonte: Autoria própria.

3.4.1 Como Prevenir/Mitigar.

Utilize as opções de root guard e BPDU guard, ao utilizar o root guard você impõe um switch como root da topologia evitando que uma porta designada receba BPDUs superiores, que indicam outro switch com melhor prioridade, ele bloqueia esse trafego de BPDUs e a porta só volta a encaminhar pacotes normalmente quando o trafego de BPDUs parar. Já o BPDU guard evita que

uma porta configurada em modo de acesso possa receber BPDUs, caso receba a porta e bloqueada.

3.5 MAC Spoofing e ARP Spoofing

O protocolo ARP é responsável por mapear endereços MAC em uma rede local, dessa forma quando um *mac-address* não e conhecido um pacote ARP-REQUEST e envia para todo a conforme RFC826 porém é possível que um host envie seu MAC a todos sem que um solicitação seja feita, nesse caso o pacote enviado e um GARP (***Gratuitous ARP***), dessa forma o atacante se aproveita dessa possibilidade e identifica o MAC do host alvo, o qual deseja se passar por ele, e envia um GARP com o *mac-address* do host alvo, ao receber isso o switch irá atualizar sua tabela cam com o novo IP correspondente ao *mac-address* recebido e também adicionará a informação ao seu cache da tabela ARP, assim todo trafego que for destinado ao *mac-address* do host alvo será encaminhado ao host do atacante.

O trafego só voltará ao normal quando o host alvo enviar algum pacote para a rede e seu *mac-address* for atualizado na tabela CAM e na tabela de cache do ARP.

3.5.1 Como Prevenir/Mitigar.

Uma solução seria ativar a segurança de porta e atrelar o *mac-address* do usuário a porta do switch, porém isso é uma opção muito trabalhosa, e quase impossível de se administrar em grandes redes. Outra solução, porém também trabalhosa seria utilizar ARP estático, porém impraticável em grandes redes, alterar o tempo em que os endereços mac permanecem na tabela cam e na tabela de cache do ARP poderia ajudar mas isso não evitaria o ataque.

3.6 DHCP Starvation

O ataque de DHCP *Starvation* funciona através de pedidos DHCP com endereços MAC falsificados que são enviados via broadcast, se os pedidos enviados forem suficientes, o atacante pode esgotar o espaço de endereços

disponíveis no servidor DHCP por um período. O Atacante então pode se passar por um servidor de DHCP clandestino e começar a responder as requisições DHCP na rede, como normalmente os pacotes DHCP incluem Gateway padrão e os endereços de DNS o atacante pode enviar o seu endereço como Gateway e DNS caracterizando assim um ataque "man-in-the-middle".

3.6.1 Como Prevenir/Mitigar.

Da mesma forma que o ataque a tabela CAM, este ataque pode ser mitigado com segurança de porta, limitando o número de *mac-address* nas portas do switch, outro ponto que pode dificultar esse ataque é a autenticação DHCP definido na RFC3118.

3.7 Segurança física

Além da segurança lógica dos equipamentos é necessário cuidarmos da segurança física dos mesmos, de nada adianta utilizarmos as melhores praticas de segurança para evitar ataques lógicos se deixarmos os equipamentos fisicamente vulneráveis.

O local onde os equipamentos estão locados deve ser seguro, permanecer trancado e com acesso restrito aos profissionais responsáveis pelos equipamentos, climatizado para evitar possíveis danos ao equipamento devido às altas temperaturas, ocasionando até mesmo perca de equipamentos e falhas na rede.

Outro ponto que deve ser considerado é a rede elétrica ele deve ser estabilizada para que os equipamentos estejam sempre disponíveis e não sofram danos em quedas e oscilações elétricas.

Para aumentar a segurança no caso de datacenters, leitores biométricos e fechaduras que possuem alguma forma de identificação pessoal além de câmeras aumentam a segurança e podem ajudar na identificação de responsáveis por possíveis problemas.

3.8 Segurança de acesso

O acesso aos equipamentos deve ser restrito a pessoas autorizadas e capacitadas, o primeiro passo para garantir a segurança de acesso, e alterar as senhas padrões dos equipamentos e nunca deixe-as em branco, se possível altere até mesmo os usuários, utilizar sempre senhas criptografadas.

Uma boa pratica é fazer com que os equipamentos autentiquem via Radius, assim poderá utilizar uma base LDAP como *o Active Directory* da Microsoft por exemplo, isso facilita o controle de usuários, e diminui a probabilidade de dois ou mais usuários utilizarem o mesmo login.

Para fins de auditoria utilize NTP para sincronizar a data dos equipamentos, para caso seja necessário efetuar uma auditoria seja fácil identificar a data de acessos e alterações de configurações.

4 CONSIDERAÇÕES FINAIS

Com ênfase na segurança de camada 2, os administradores devem cuidar da segurança da rede interna assim como olham os perigos externos, e que muitos protocolos básicos em redes ethernet possuem muitas vulnerabilidades que devemos ter cuidado.

Manter a segura a rede interna requer um trabalho árduo e cansativo, mas com pequenas mudanças já podemos melhorar muito a segurança dos dados em nossas empresas, com esse trabalho foi possível verificar a importância da segurança nas redes internas e que quanto mais segurança mais trabalho o administrador terá para manter sua rede segura, porém esse sempre será o preço a ser pago.

REFERÊNCIAS

WATKINS, M; WALLACE, K**.** ***CCNA Security.*** Cisco Press, 2008.

CISCO, Networking Academy. ***CCNA Exploration*** **– Fundamentos de Rede.** Cisco Systems, Inc., 2007-2009.

FILIPPETTI, Marco Aurélio. CCNA 4.1 – **Guia Completo de Estudos.** Florianópolis: Editora Visual Books, 2008.

PWC**, Pesquisa Global de Segurança da Informação**, São Paulo, 2013.

SÊMOLA, M. **Gestão de segurança da informação**. Campus, 2003. 156 p.

TANENBAUM, A. S. **Redes de computadores**. Campus, 2003. 945 p.

KUROSE, J. F; ROSS, K. W. **Redes de computadores e a internet**, 5. Ed. Downtronica, São Paulo,