SEGURIDAD EN REDES

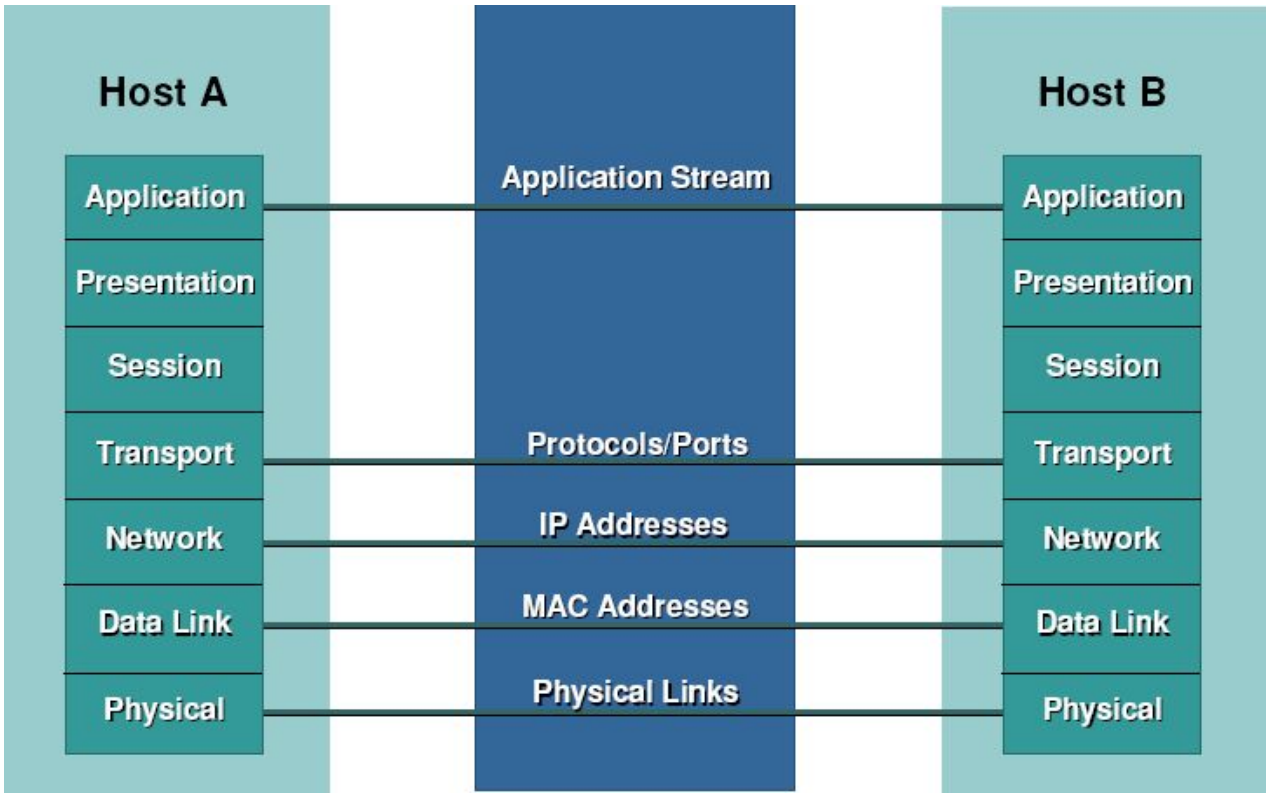
TABLA DE CONTENIDO

2. OBJETIVOS

- Tener un conocimiento acerca de los conceptos de VLAN, MAC, STP y ARP.
- Conocer los tipos de ataques que se pueden presentar en las VLAN, MAC, STP y ARP.
- Manejar diferentes herramientas de ataque.
- Conocer las diferentes características de seguridad.

1. INTRODUCCIÓN

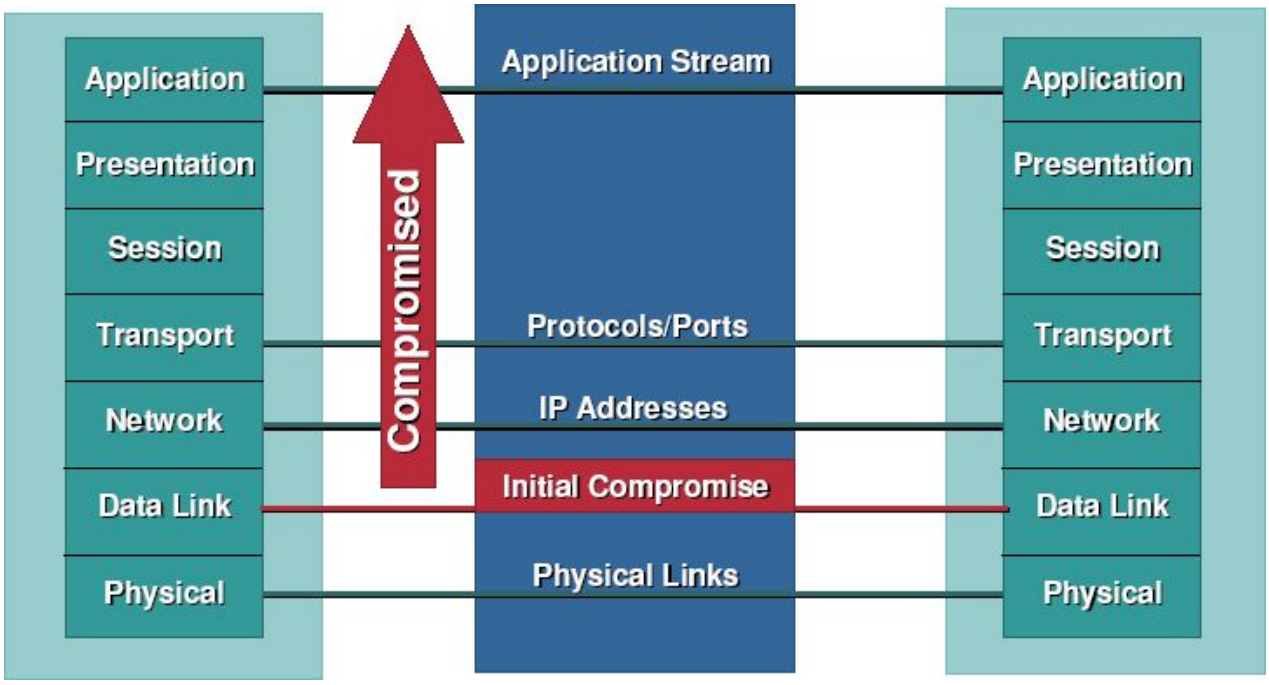
El modelo OSI (figura 1) se pensó para que cada capa opere independientemente de las demás. Esto quiere decir que cada capa puede ser comprometida sin que las otras lo



noten (figura 2).

Según el FBI el 80% de los ataques provienen al interior de la organización

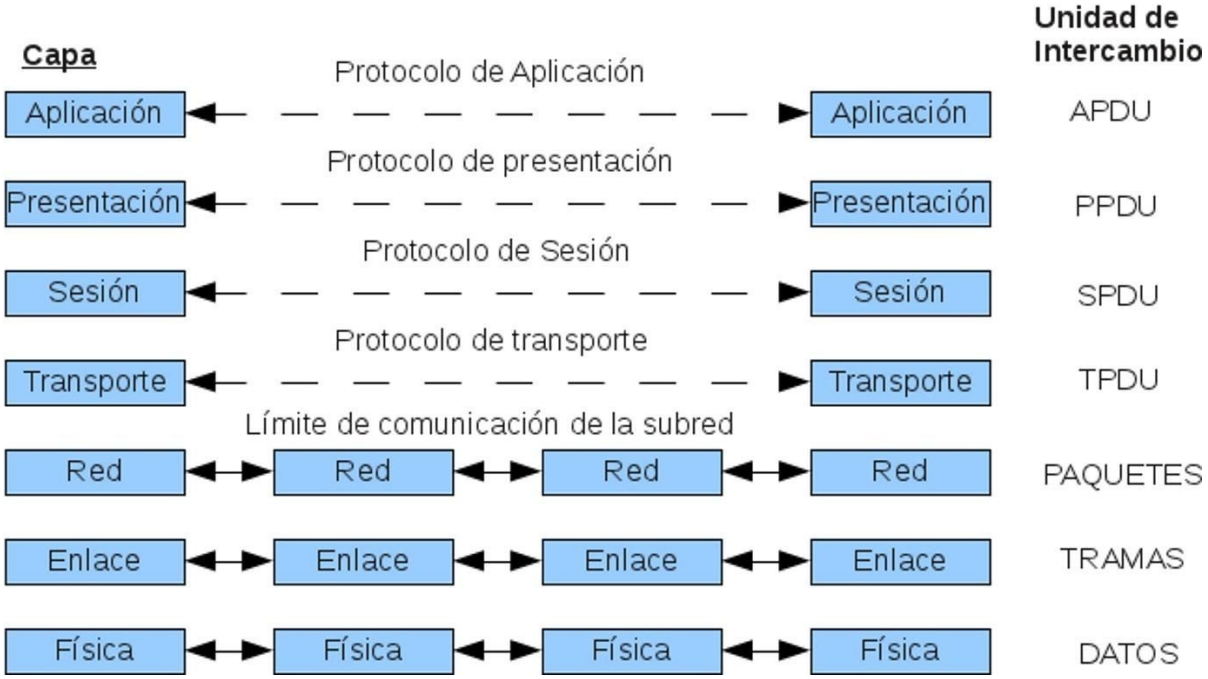
- El 99% de los puertos (o bocas) de las redes LAN corporativas están “desprotegidos”. Es decir, cualquiera puede conectarse a ellos.
- La mayoría de las empresas está desplegando redes inalámbricas (aunque no lo sepan).
- Las herramientas diseñadas para simplificar el trabajo de los administradores de red perjudican seriamente la seguridad de la red corporativa.



1.1. Mitos De La Capa 2

Las direcciones MAC no pueden ser falsificadas. Un switch no permite hacer sniffing. Las VLAN's están separadas unas de las otras .

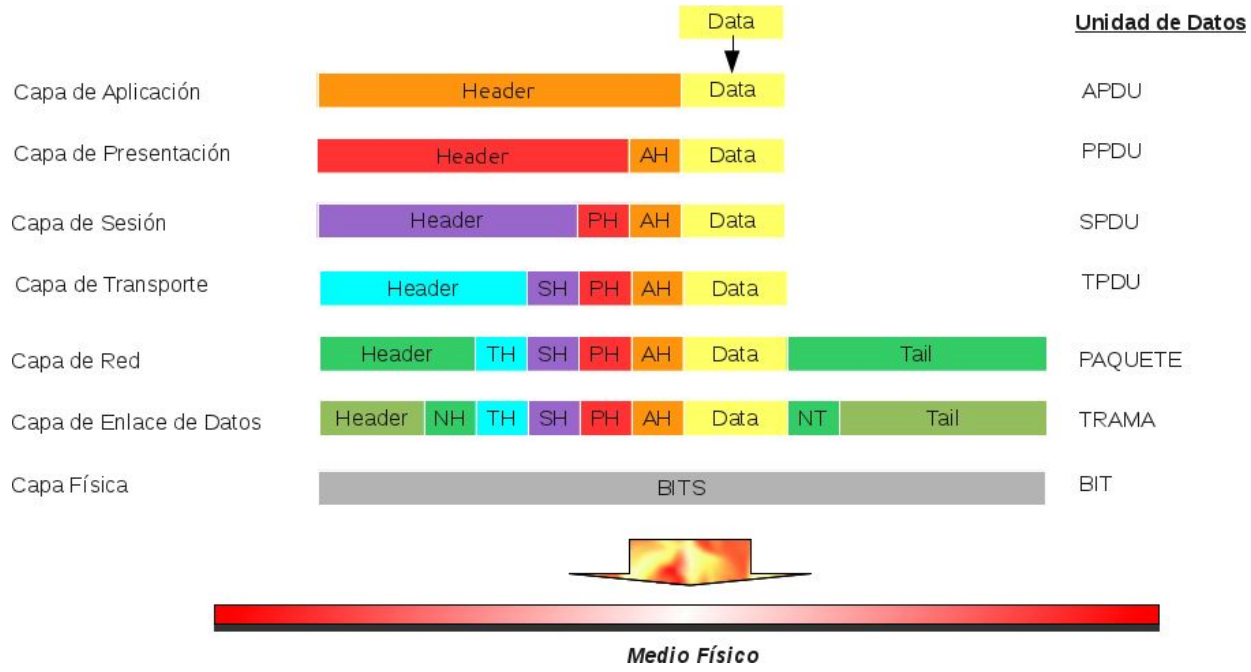
1.2. El Modelo OSI



El modelo OSI nace como una solución a la incompatibilidad de las redes en la década del 80; este modelo por capas o niveles permite que las comunicaciones se organicen en una "pila" de protocolos y que cada capa sea independiente de las demás.

El funcionamiento sería algo así: (Figura 3)

Desde la capa de aplicación se genera un "paquete"(PDU) como se muestra en (Figura 1.4). A este se le va agregando información en cada capa necesaria para la comunicación entre cada una de ellas sobre las diferentes máquinas:



El resultado obtenido en la capa de enlace de datos es la trama que enviaremos al medio físico para transmitirla. Como podemos ver en la (Figura 1.3) , la trama antes de llegar a la máquina destino va a pasar por switchs (capa 2) y routers (capa 3). En los routers la trama se va "abriendo", por decirlo de alguna manera y se obtiene la información que se necesita en cada nivel, ya sea la MAC (capa 2) en caso de los switchs o en los routers la MAC y la IP (capa 3) para poder hacer la redirección de las tramas por los caminos correctos. Una vez que se obtienen dichos datos, se vuelve a armar el paquete y a partir de los resultados obtenidos continúa su camino por la red hasta llegar a la máquina destino.

Bueno eso es OSI y así funciona, aclaremos que el modelo en sí mismo no es considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, por eso es que suele hablarse de modelo de referencia.

2. ATAQUES

2.1. Ataques Basados En MAC Y ARP

Para comprender el funcionamiento de este tipo de ataques hablaremos un poco del protocolo ARP. ARP son las siglas en inglés de *Address Resolution Protocol* (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = xx xx xx xx xx xx) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan. ARP está documentado en el RFC[1] 826

El protocolo RARP realiza la operación inversa.

En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC. ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

- Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
- Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router. Cuando
- un router necesita enviar un paquete a un host de la misma red.

2.1.1. Tablas ARP.

La filosofía es la misma que tendríamos para localizar al señor "X" entre 150 personas: preguntar por su nombre a todo el mundo, y el señor "X" nos responderá. Así, cuando a "A" le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su trama ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a "A" enviándole su dirección física. En este momento "A" ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla, o simplemente algún usuario de la red cambia de dirección IP).

2.1.1.1. **FUNCIONAMIENTO EN EL CASO 1.**

Si A quiere enviar una trama a la dirección IP de B (misma red), mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos la trama, no tendrán que deshacerla para comprobar si el mensaje es para ellos, sino que se hace con la dirección física.

2.1.1.2. **FUNCIONAMIENTO EN EL CASO 2.**

Si A quiere enviar un mensaje a C (un nodo que no esté en la misma red), el mensaje deberá salir de la red. Así, A envía la trama a la dirección física de salida del router. Esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP. Si esta entrada no está en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.

Una vez en el router, éste consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por la interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Aquí el proceso cambia: la interfaz del router tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP, y en caso de no existir la entrada correspondiente a la IP, la obtiene realizando una multidifusión.

Pare el ataque basado en MAC y ARP encontramos 3 tipos:

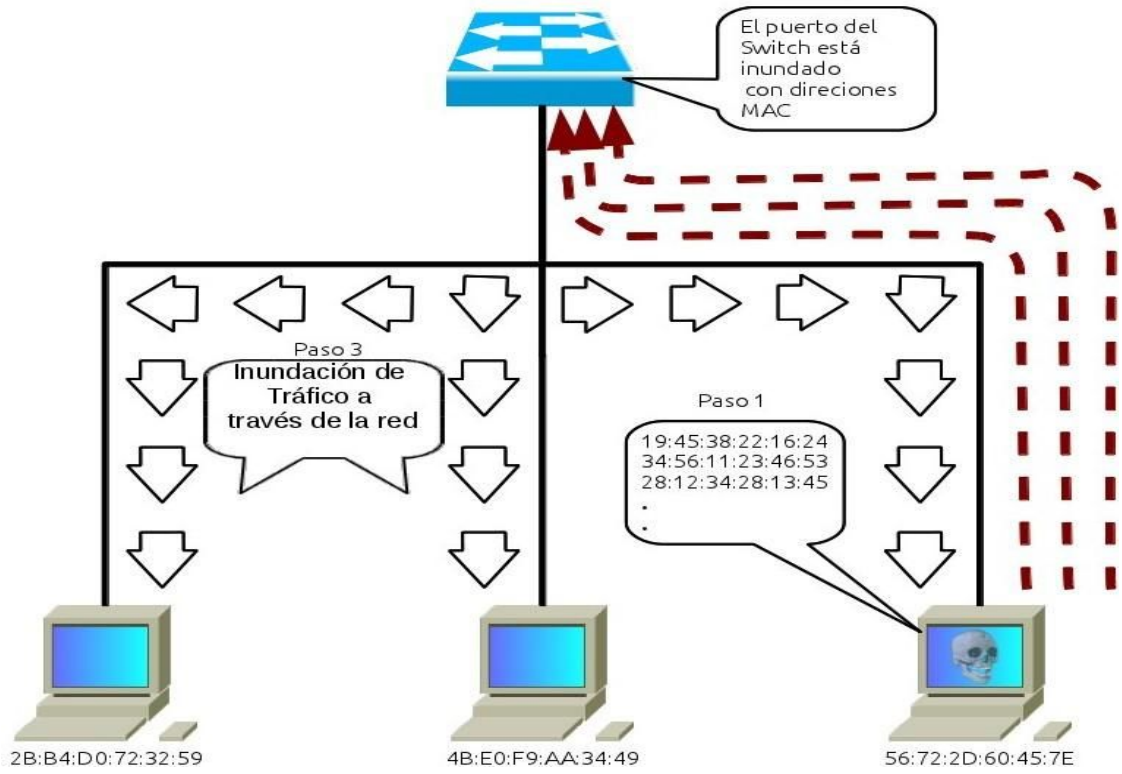
- CAM Table Overflow. ARP
- Spoofing
- Ataques que emplean ARP Spoofing.

2.1.2. CAM Table Overflow.

El ataque se basa en la limitación del hardware del switch para mantener la tabla que relaciona las MAC con los puertos, dicha tabla se denomina CAM[2] Obviamente las tablas no son infinitas y cuando una llega a su tope un switch comienza a trabajar como un HUB, es decir que todo paquete que recibe el switch si la MAC destino no se encuentra en la tabla y ésta se encuentra llena, manda el paquete por todos sus puertos. Esto nos permitiría capturar todo el tráfico con un sniffer obviamente capturaríamos las tramas que se dirigen a MAC's que no se encuentren en la tabla, pero como sabemos que las

asignaciones son temporales, lo que se hace es mandar las MAC's falsas en intervalos de tiempo lo suficientemente chicos como para que se llene la tabla con MAC's falsas y cuando las verdaderas caen por vencimiento de tiempo, estos espacios se llenan con más MAC's falsas; y así lograríamos mantener el ataque. (Figura 2.2)

Bien para producir este *overflow* lo que se hace es enviar muchas tramas con direcciones MAC distintas a cualquier puerto del switch hasta que en un momento empecemos a



recibir las tramas que se dirigen a otras máquinas (esto lo detectamos con el sniffer).

Obviamente este tipo de cosas producen inestabilidad sobre la red, no sería raro que se encuentren con un DOS (*Denial of service*) en vez de empezar a recibir paquetes. Existe una herramienta para producir este tipo de ataques denominada macof, es parte del paquete Dsniff (GNU/Linux) y el código está escrito en perl. Para utilizarlo es suficiente con instalar el paquete d*sniff* y ejecutar *macof.*
Existen medidas contra este tipo de ataques, algunas de ellas son asignar a los puertos del switch un límite de MAC's a asignar, y en el caso que esa cantidad se supere producir el bloqueo de dicho puerto o directamente utilizando asignaciones estáticas de MAC a los puertos (que entre más grande la red requiere mucho trabajo).

2.1.3. ARP Spoofing

También conocido como ARP Poisoning o ARP Poison Routing. Para este ataque debemos tener claro el funcionamiento del protocolo ARP para cambiar la MAC. Para poder comunicarnos en un ámbito local necesitamos la MAC, para ello mandamos un pedido ARP que nos la retornara y luego se almacenará en la tabla durante cierto intervalo de tiempo, ahora bien también existen los GARP[3] estos son paquetes que contienen la MAC y la IP de un host y se mandan en broadcast a toda la red para que todos los hosts existentes en ella actualicen su caché ARP Importante¡ (todos los que estén configurados como dinámicos y acepten estos pedidos). Estos paquetes no generan una respuesta de parte de las máquinas que los reciben pero cuando una máquina lo recibe lo asigna a su tabla.

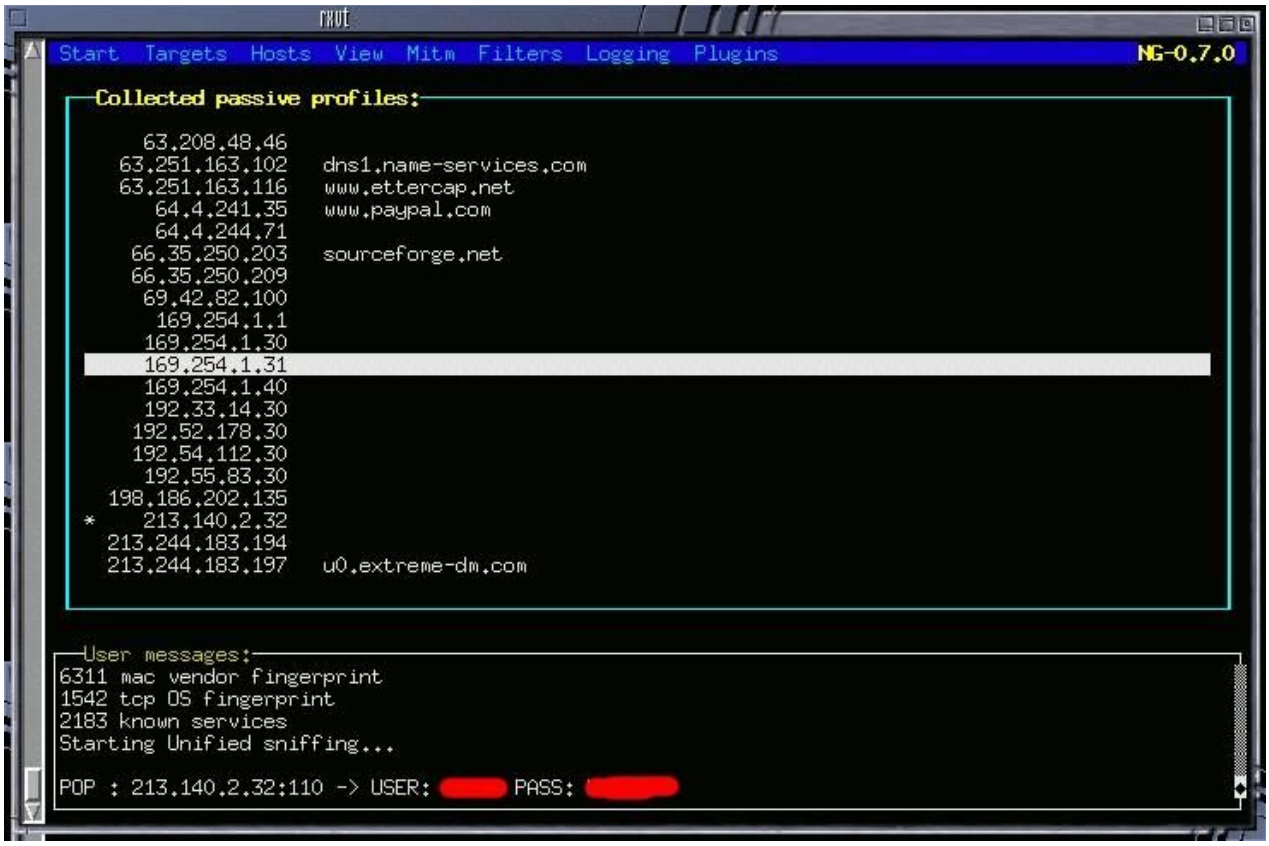
Al ser mensajes broadcast no están diseñados para proporcionar ninguna validación de identificación en la transacción, por ende falsificar la información que estos paquetes llevan sería muy sencillo, y manteniendo el envió de estos paquetes en intervalos de tiempos lo suficientemente cortos como para que las caches no borren las entradas, conseguimos generar conexiones virtuales distintas a las conexiones reales.

2.1.3.1. ¿COMO SERIA EL ATAQUE?

Supongan que 2 máquinas dentro de la red se quieren conectar,la *máquina1* con una *IP Y* y *MAC X, la máquina2* con una *IP Z y MAC M*, si estas quisieran comunicarse deberían utilizar un pedido para la MAC a menos que las tengan en sus tablas, pero ¿Que pasa si estuvieran "mal" cargadas? Suponga además que esta la máquina del atacante con *IP A* y *MAC B* y manda un paquete GARP en broadcast con la siguiente información (*IP Z, MAC B*) :O, este paquete le indicaría a la máquina1 que para llegar a la *IP Z* (de la *máquina 2*) debe mandar el paquete a la *MAC B* (máquina del atacante). De ahora en más todo paquete de máquina1 a máquina2 pasará por la máquina atacante, y si este último redireccionará dichos paquetes a la máquina2 generaríamos una conexión con nuestra máquina atacante en el medio y pasando por ella toda la comunicación (!*Excelente día para un sniffer*¡) bueno a este tipo de ataque se lo denomina *Switch Port Stealing*. Existe un ataque bastante similar denominado MITM[4] pero con un detalle más importante... que pasaría si mandamos el mismo GARP desde la máquina atacante y decimos que para la IP de gateway del router de la red la MAC es B :O, de ahora en más todo paquete de cualquier máquina en la red que quiera obtener información de una IP fuera de la red,

1 . (Gratuitous ARP o ARP announcement)

2 Siglas en Ingles: Man in the Middle



pasarían por la máquina atacante.(Otro Excelente día para sniffear). Para estos ataques existe Ettercap (*Figura 2.3).*

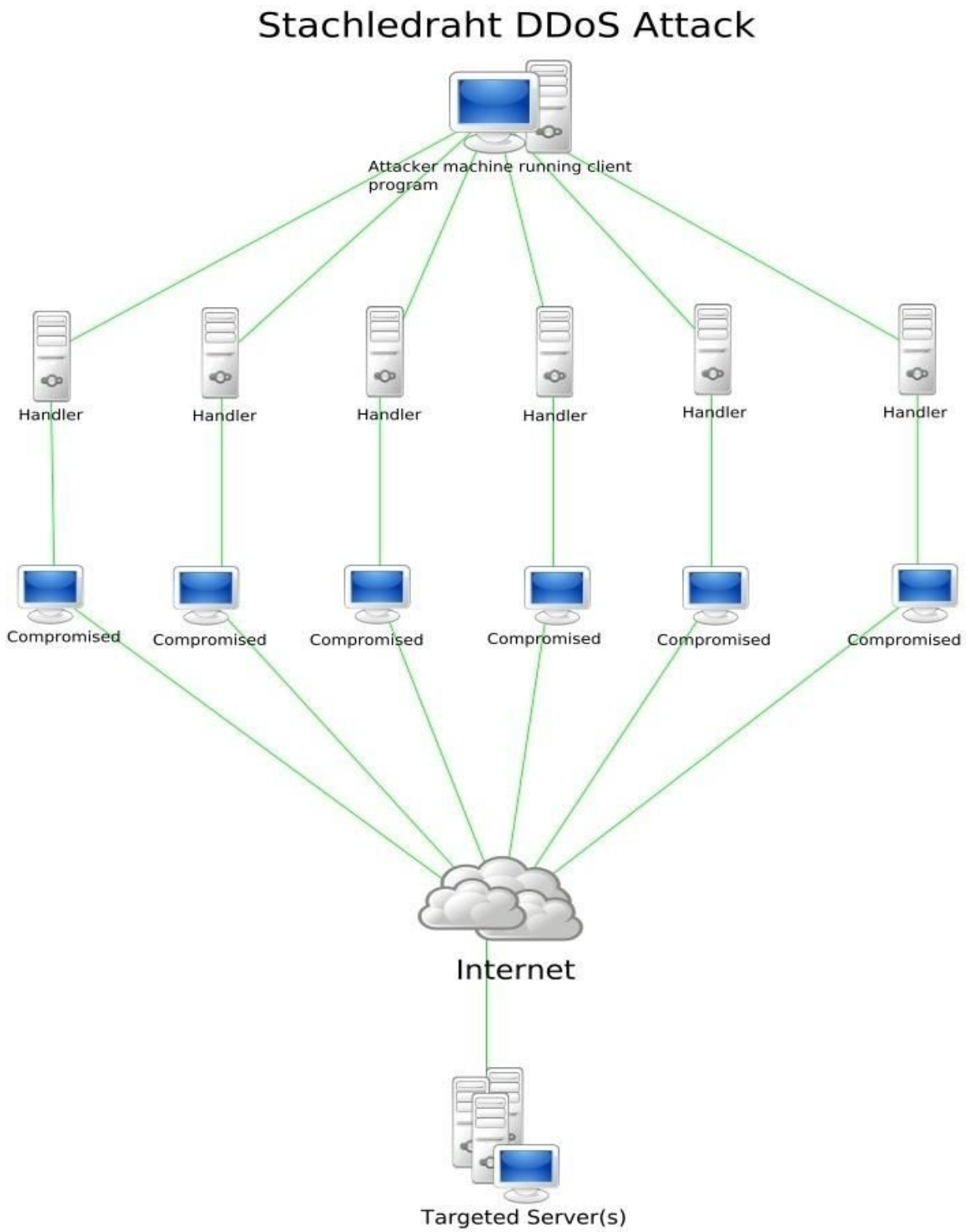
Y así podemos jugar con las MAC particulares como la de broadcast(FF:FF:FF:FF:FF), ¿Que pasaría si en vez de mandar la MAC de la máquina atacante (B), decimos que la IP de gateway se dirige a la MAC de broadcast? todos los paquetes de todas las máquinas que quieran salir de la red serán enviados a todas las máquinas de la red.

2.1.4. Ataques Que Emplean ARP Spoofing.

Figura 2.4: ARP Spoofing

Dentro de este tenemos:

- DoS (Denial of Service) la mas abajo figura 2.5 nos muestra un ejemplo de este ataque)



2.1.4.1. DOS (DENIAL OF SERVICE)

Bueno este es bastante sencillo, sigue siendo el mismo formato de los anteriores pero la diferencia es que quiere dejar sin servicio a alguna máquina de la red. Lo que hacemos para lograrlo es asignar en el paquete GARP[5] a una IP existente en la red una MAC inexistente por ende los paquetes se descartaran y esa máquina nunca va a recibir una

respuesta de ningún host en la red.

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta

técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DdoS *Figura 2.7* (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

2.1.4.1.1. Métodos de ataque.

Un ataque de "Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado en un numero de formas. Aunque básicamente consisten en :

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco,

3 Gratuitous ARP o ARP announcement Gratuitous
4 de las siglas en inglés Denial of Service

o tiempo de procesador.

- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

2.1.4.1.2. Inundación SYN (SYN Flood)

2.1.4.1.2.1. Principios de TCP/IP

Cuando una máquina se comunica mediante TCP/IP con otra, envía una serie de datos junto a la petición real. Estos datos forman la cabecera de la solicitud. Dentro de la cabecera se encuentran unas señalizaciones llamadas Flags (banderas). Estas señalizaciones (banderas) permiten iniciar una conexión, cerrarla, indicar que una solicitud es urgente, reiniciar una conexión, etc. Las banderas se incluyen tanto en la solicitud (cliente), como en la respuesta (servidor).

Para aclararlo, veamos cómo es un intercambio estándar TCP/IP:

1. Establecer Conexión: El cliente envía una Flag SYN, si el servidor acepta la conexión, este, debería responderle con un SYN/ACK luego el cliente debería responder con una Flag ACK.

```
-----------------------------------------------------
   1-Cliente ----------SYN    > 2 Servidor
   4-        Cliente <-----SYN/ACK   3 Servidor
   5-        Cliente ----------ACK       > 6 Servidor
-----------------------------------------------------
```

2. Resetear Conexión: Al haber algún error o pérdida de paquetes de envio se establece envío de Flags RST:

```
-----------------------------------------------------
   1-Cliente ---------Reset     > 2-servidor
   4-        Cliente <----Reset/ACK  3-Servidor
   5-        Cliente ----------ACK6-Servidor
-----------------------------------------------------
```

La inundación SYN[8] envía un flujo de paquetes TCP/SYN (varias peticiones con Flags SYN en la cabecera), muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías). Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la

respuesta. Estos intentos de conexión consumen recursos en el servidor y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

2.1.4.1.2.2. SYN cookies

provee un mecanismo de protección contra Inundación SYN, eliminando la reserva de recursos en el host destino, para una conexión en momento de su gestión inicial.

2.1.4.1.3. Inundación ICMP (ICMP Flood)

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que ésta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.
Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

2.1.4.1.4. SMURF

Existe una variante a ICMP Flood denominado Ataque Smurf que amplifica considerablemente los efectos de un ataque ICMP.

Existen tres partes en un Ataque Smurf: El atacante, el intermediario y la víctima (comprobaremos que el intermediario también puede ser víctima).

En el ataque Smurf, el atacante dirige paquetes ICMP tipo "echo request" (ping) a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando Echo reply, a la máquina origen (víctima).

Se dice que el efecto es amplificado, debido a que la cantidad de respuestas obtenidas, corresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.
Como se dijo anteriormente, los intermediarios también sufren los mismos problemas que las propias víctimas.

2.1.4.1.5. Inundación UDP (UDP Flood)

Básicamente este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.
Es usual dirigir este ataque contra máquinas que ejecutan el servicio Echo, de forma que se generan mensajes Echo de un elevado tamaño.

2.1.4.2. HIJACKING

Hijacking [9] hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. Es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontramos con el secuestro de conexiones de red, sesiones de terminal, servicios y un largo etc en cuanto a servicios informáticos se refiere.

2.1.4.2.1. Ejemplos de Hijacking

IP hijakers: secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.
web hijacking: secuestro de página web. Hace referencia a las modificaciones que un atacante realiza sobre una página web, normalmente haciendo uso de algún bug de seguridad del servidor o de programación del sitio web, también es conocido como defacement o desfiguración.
Reverse domain hijacking o Domain hijacking: secuestro de dominio
Session hijacking: secuestro de sesión
Browser hijacking: (Secuestro de navegadores en español). Se llama así al efecto de apropiación que realizan algunos spyware sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada etc. Es utilizado por un tipo de software malware el cual altera la configuración interna de los navegadores de internet de un ordenador. El termino "secuestro" hace referencia a que éstas modificaciones se hacen sin el permiso y el conocimiento del usuario. Algunos de éstos son fáciles de eliminar del sistema, mientras que otros son extremadamente complicados de eliminar y revertir sus cambios.

2.2. Ataques Basados En VLAN

Para entender este tipo de ataque vamos explicar que es una VLAN y como trabaja. Es un método para crear redes lógicamente independientes dentro de una misma red física Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

2.2.1. Protocolos Y Diseño.

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com.

Los primeros diseñadores de redes enfrentaron el problema del tamaño de los dominios de colision (Hubs) esto se logró controlar a través de la introducción de los switch o conmutadores pero a su vez se introdujo el problema del aumento del tamaño de los dominios de difusión y una de las formas más eficientes para manejarlo fue la introducción de las VLANs. Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad.

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

En el contexto de las VLANs, el término trunk ('troncal') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLANs, por lo que a menudo son enlaces conmutador a conmutador o conmutador a enrutador más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales»;. Un enrutador (conmutador de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP (Cisco) también permite «podar», lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino.

2.2.2. Ejemplo De Definición De VLAN

Imaginemos que en nuestra empresa tenemos una LAN corporativa con un rango de direcciones IP tipo 172.16.1.XXX. Se da el caso de que tenemos asignadas las casi 255 direcciones que como máximo nos permite el mismo y además notamos cierta saturación en la red. Una fácil solución a este problema sería crear unas cuantas VLAN por medio de un switch o conmutador de nivel 3.

Podemos asignar una VLAN a cada departamento de la empresa, así también controlamos que cada uno sea independiente (o no) del resto:
VLAN1: Contabilidad. Direcciones 172.16.2.XXX
VLAN2: Compras. Direcciones 172.16.3.XXX
VLAN3: Distribución. Direcciones 172.16.4.XXX

.

De esta forma liberamos direcciones de nuestra red origen 172.16.1.XXX pasándolas a las distintas VLAN que hemos creado. Gracias al switch de nivel 3 podremos gestionar la visibilidad entre las distintas VLAN y notaremos una mejora en el rendimiento de la red ya que las difusiones o broadcast de cada VLAN sólo llegarán a los equipos conectados a la

misma.

2.2.3. Gestión De La Pertenencia A Una VLAN

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLANs estáticas y VLANs dinámicas

Las VLANs estáticas también se denominan VLANs basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

En las VLANs dinámicas, la asignación se realiza mediante paquetes de software tales como el CiscoWorks 2000. Con el VMPS (acrónimo en inglés de VLAN Policy Server o Servidor de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el software FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

2.2.4. VLAN Basadas En El Puerto De Conexión

Con las VLANs con pertenencia basada en el puerto de conexión del switch, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una sub-red y que puede ser capaz de hablar con otros miembros de la sub-red simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de

puerto-a-VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es muy bueno. Un ASIC permite el mapeo de puerto-a-VLAN sea hecho a nivel hardware.

2.2.4.1. TIPOS DE ATAQUE

Dentro de este tipo de ataque encontramos 4 tipos:

- Dynamic Trunking protocol.
- VLAN Hopping Attack.
- Double Encapsulated VLAN Hopping Attack.
- VLAN Trunking Protocol.

2.2.4.2. DYNAMIC TRUNKING PROTOCOL.

Para hablar sobre este ataque hablaremos primero que es y cómo funciona el protocolo.

DTP[10] es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DISABLE y NON-NEGOTIATE.

2.2.4.2.1. Modos de trabajo de los puertos

- dynamic auto — Es el modo por defecto en switches Catalyst 2960 de Cisco. El puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Para ello envía periódicamente tramas DTP al puerto en el otro lado del enlace indicando que es capaz de establecer un enlace troncal. Esto no quiere decir

5 De las siglas en inglés: Dynamic Trunking Protocol

que lo solicita, sino que sólo lo informa. Si el puerto remoto está configurado en modo on o dynamic desirable se establece el enlace troncal correctamente. Sin embargo, si los dos extremos estan en modo dynamic auto no se establecerá el enlace como troncal, sino como acceso, lo que probablemente implique configuración adicional.

- on — Suele ser el modo por defecto. Fuerza al enlace a permanecer siempre en modo troncal, aún si el otro extremo no está de acuerdo.

- off — Fuerza al enlace a permanecer siempre en modo de acceso, aún si el otro extremo no está de acuerdo.

- dynamic desirable — Es el modo por defecto en switches Catalyst 2950 de Cisco. En este modo el puerto activamente intenta convertir el enlace en un enlace troncal. De este modo, si en el otro extremo encuentra un puerto en modo on, dynamic auto o

dynamic desirable pasará a operar en modo troncal.

- nonegotiate — Fuerza siempre al puerto a permanecer en modo troncal, pero no envía tramas DTP. Los vecinos deberán establecer el modo troncal en el enlace de forma manual.

2.2.4.2.2. Configuración de DTP

DTP[11] se habilita automáticamente en un puerto del switch cuando se configura un modo de trunking adecuado en dicho puerto. Para ello el administrador debe ejecutar el comando switchport mode adecuado al configurar el puerto: switchport mode {access | trunk | dynamic auto | dynamic desirable}. Con el comando switchport nonegotiate se desactiva DTP.

Su función es gestionar de forma dinámica la configuración del enlace troncal al conectar dos switches, introduciendo los comandos del IOS (sistema operativo de los switches y routers Cisco) en la configuración del dispositivo (running-config) de forma automática sin que el administrador intervenga.

Esto implica que si estamos configurando un puerto de un switch Cisco para DTP, el puerto del otro lado del enlace también debe tener DTP habilitado para que el enlace quede configurado correctamente.

La combinación de los modos asignados a los puertos define cuál va a ser el estado final del enlace asociado a éstos:

- o bien 'access', es decir, pasarán las tramas de una única VLAN y no necesitaremos etiquetarlas.
- o bien 'trunking', es decir, pasarán las tramas de todas las VLAN permitidas etiquetándolas adecuadamente (ISL o 802.1Q).

La *Tabla 2.1* describe las combinaciones de modos y el estado final del puerto al que se llega, asumiendo que ambos lados tienen DTP habilitado:

6 De las siglas en inglés: Dynamic Trunking Protocol

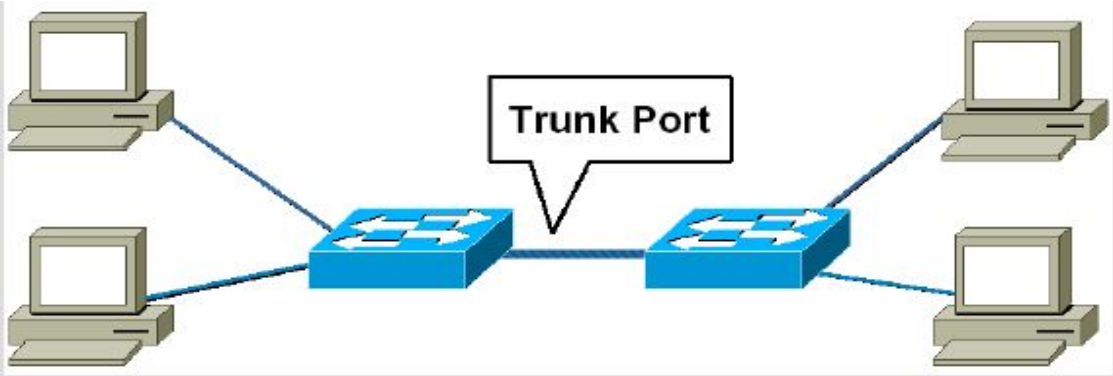
Table 2.1: Modos y combinaciones de los puertos DTP

\ Remoto ***Puerto local ***	**Dynamic Auto**	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	access	trunk	trunk	access
Dynamic Desirable	trunk	trunk	trunk	access
Trunk	trunk	trunk	trunk	**fallo**
Access	access	access	**fallo**	access

Este protocolo es una ayuda que facilita la vida del administrador de la red. Los switches no necesitan DTP para establecer enlaces troncales, y algunos switches y routers Cisco no soportan DTP.

2.2.4.2.3. Puertos TRUNK.

Los puertos trunk por defecto tienen acceso a todas las VLANs. Se los emplea para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar switches). La encapsulación puede ser IEEE 802.1Q o ISL[12]. *Figura 2.4*



2.2.4.2.4. Principales características empleadas en el ataque.

- Automatiza la configuración de los trunk 802.1Q/ISL.
- Sincroniza el modo de trunking en los extremos.
- Hace innecesaria la intervención administrativa en ambos extremos.
- El estado de DTP en un puerto trunk puede ser “Auto”, “On”, “Off”, “Desirable”, o “Non-Negotiate”. Por default en la mayoría de los switchs es “Auto”.

Para este ataque podemos usar el frame work para el ataque en capa 2 llamado *Yersinia.*

2.2.5. VLAN Hopping Attack.

VLAN Hopping (*virtual local area network hopping*) es un método de atacar a los recursos en red en una VLAN. El concepto básico detrás de todos los ataques de salto de VLAN es para un host atacante en una VLAN para tener acceso al tráfico en otras VLAN que normalmente no serían accesibles. Hay dos métodos principales VLAN Hopping: switch

spoofing y doble etiquetado.

2.2.5.1. ATAQUE SWITCH SPOOFING.

En un ataque de switch spoofing, un host atacante que sea capaz de hablar de etiquetado y protocolos Trunking utilizados en el mantenimiento de una VLAN que imita un conmutador trunking. El Tráfico para varias VLAN es entonces accesible a la máquina atacante.

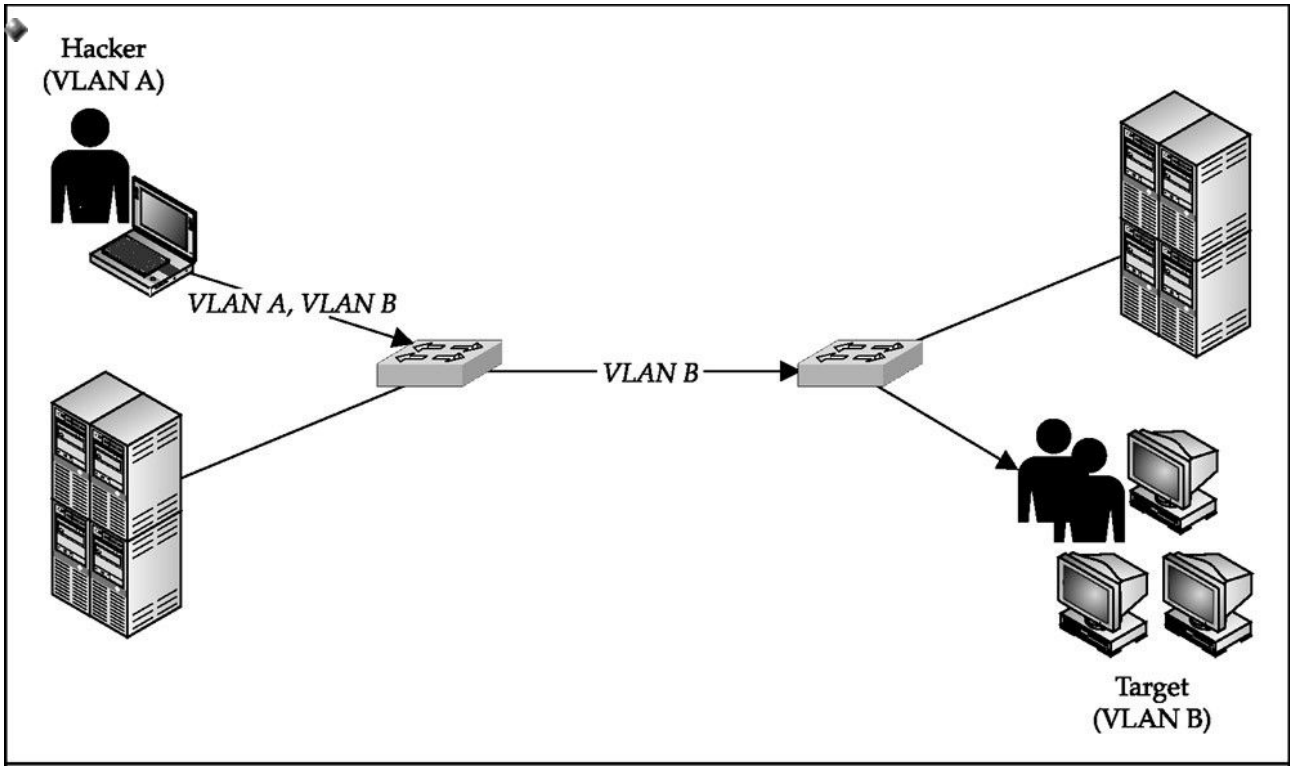
2.2.5.2. DOUBLE TAGGING ATTACK.

En un ataque de etiquetado doble, un host atacante antepone dos etiquetas VLAN a paquetes que transmite. El primer encabezado (que corresponde a la VLAN que el atacante es realmente un miembro de) es despojado por un primer conmutador que encuentre el paquete, y entonces el paquete se envía. El segundo, falso, el encabezado es entonces visible para el segundo conmutador que se encuentra con el paquete. Este falso encabezado VLAN indica que el paquete está destinado para un host en un segundo, VLAN de destino. El paquete es enviado al host de destino como si se tratara de tráfico en la capa 2. Mediante este método, la máquina atacante puede pasar por alto medidas de seguridad de la capa 3 que se utilizan para aislar lógicamente los host de los demás.

Como un ejemplo de un ataque de doble etiquetado, considere un servidor web seguro en una VLAN llamada VLAN1. Los hosts de la VLAN1 permite el acceso al servidor web, los host de fuera de la VLAN están bloqueados por los filtros de la capa 3. Un host atacante en una VLAN separada, llamada VLAN2, crea un paquete especialmente creado para atacar el servidor web. Se coloca una encabezado de etiqueta del el paquete como perteneciente a VLAN2 en la parte superior de otro encabezado de etiqueta del paquete como perteneciente a la VLAN1. Cuando el paquete es enviado, el interruptor de VLAN2 ve la cabecera VLAN2 y lo elimina, y envía el paquete. El interruptor VLAN2 espera que el paquete será tratado como un paquete del estándar de TCP por el conmutador en VLAN1. Sin embargo, cuando el paquete llega a VLAN1, el interruptor ve una etiqueta que indica que el paquete es parte de la VLAN1, y así evita la capa 3, tratándolo como un paquetes en la red capa de 2 en la misma VLAN lógica. El paquete por lo tanto llega al servidor de destino como si fuera enviado desde otro host en VLAN1, haciendo caso omiso de cualquier filtrado de capa 3 que podría estar en su lugar.

2.2.5.3. ¿COMO SE PRODUCE ESTE ATAQUE? (*FIGURA 2.9*)

- Un equipo puede hacerse pasar como un switch con IEEE802.1Q/ISL y DTP, o bien se puede emplear un switch.



El equipo se vuelve miembro de todas las VLAN.

- Requiere que el puerto este configurado con trunking automático.

2.2.6. Ataque De VLAN De Doble-Encapsulamiento 802.1Q/Nested .

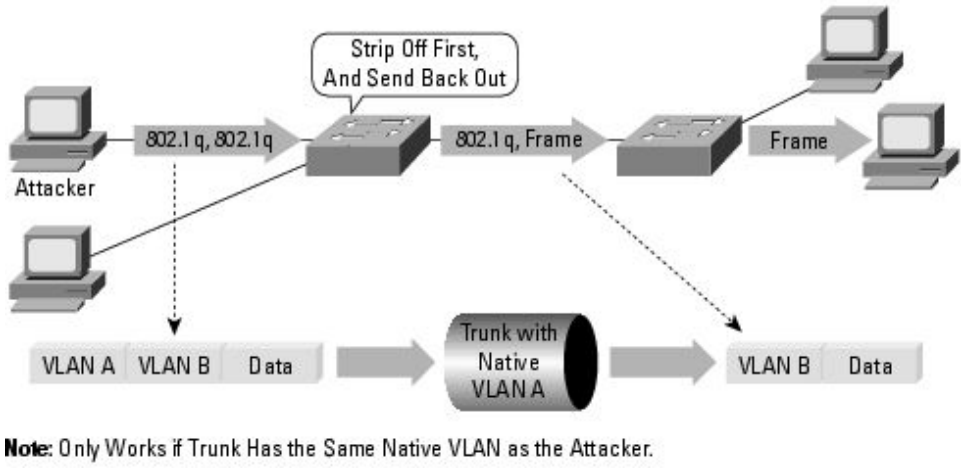
Mientras interno a un Switch, los números de VLAN y la identificación se llevan en un formato especial extendido que permite la ruta de transmisión para mantener el aislamiento de VLAN de extremo a extremo sin ninguna pérdida de información. En cambio, fuera de un conmutador, las normas de etiquetado son dictados por las normas ISL o 802.1Q.

ISL es una tecnología propietaria de Cisco y en cierto sentido es una forma compacta de la cabecera del paquete ampliada utilizados en el interior del dispositivo: desde que todos los paquetes adquieran una etiqueta, no hay riesgo de pérdida de identidad y por lo tanto de las vulnerabilidades de seguridad. Por otra parte, la IEEE que definió 802.1Q decidió que, debido a la compatibilidad anterior era conveniente apoyar la bien llamada VLAN nativa, es decir, una VLAN que no se asocia explícitamente a cualquier etiqueta en un enlace 802.1Q . Esta VLAN es implícitamente usada para todo el tráfico sin etiquetar recibido en un puerto 802.1Q capaz de recibirlo.

Esta capacidad es deseable porque permite a los puertos 802.1Q capaces de hablar con los viejos puertos 802,3 directamente mediante el envío y recepción de tráfico sin etiquetar. Sin embargo, en los demás casos, puede ser muy perjudicial porque los paquetes asociados con la VLAN nativa pierden sus etiquetas, por ejemplo, su aplicación de identidad, así como su clase de servicio (802.1p bits) cuando se transmiten a través de un enlace 802.1Q.

Por estas razones exclusivas la pérdida de medios de identificación y la pérdida de la clasificación, el uso de la VLAN nativa debe ser evitado. Hay una razón más sutil, sin embargo. Si bien interno a un conmutadorr, los números de VLAN y la identificación se llevan en un formato especial extendido que permite la ruta transmisión para mantener el aislamiento de VLAN de extremo a extremo sin ninguna pérdida de información. En cambio, en las afueras de un interruptor, las normas de etiquetado son dictados por las normas ISL o 802.1Q.

La (*figura 2.6*) describe cómo trabaja este ataque.



Se envía una trama 802.1Q de la VLAN de la víctima dentro de otra trama 802.1Q de nuestra VLAN.
Los switchs realizan un solo nivel de desencapsulado.
Solo permite tráfico en una sola dirección.
Sólo funciona si la VLAN nativa del trunk es la misma a la que pertenece el atacante.
Funciona aunque el puerto del atacante tenga desactivado el trunking.

2.2.7. VLAN Trunking Protocol

VTP son las siglas de *VLAN Trunking Protocol,* un protocolo usado para configurar y administrar VLANs en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor - Transparente

Los administradores de red solo pueden cambiar la configuración de VLANs en modo Servidor. Después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos, sin embargo los dispositivos en modo transparente que usan la versión 2 del protocolo VTP enviarán la información que reciban

(publicaciones VTP) a otros dispositivos a los que estén conectados, actualmente (año 2009) dichas publicaciones se envían cada 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP, en el modo cliente NO se podrán crear VLAN, sino que sólo podrá aplicar la información que reciba de las publicaciones VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat. Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio.

2.2.8. Seguridad VTP

VTP puede operar sin autenticación, en cuyo caso resulta fácil para un atacante falsificar paquetes VTP para añadir, cambiar o borrar la información sobre las VLANs. Existen herramientas disponibles gratuitamente para realizar esas operaciones. Debido a eso se recomienda establecer un password para el dominio VTP y usarlo en conjunto con la función hash MD5 para proveer autenticación a los paquetes VTP. y tan importante es para los enlaces troncales de la vlan.

- Se lo emplea para distribuir configuraciones de VLAN a través de múltiples

dispositivos.

- VTP se emplea únicamente en puertos trunk.
- VTP puede causar muchos inconvenientes.
- VTP emplea autenticación considere usar MD5.
- Si un atacante logra que su puerto se convierta en trunk, puede enviar mensajes VTP como si fuera un servidor VTP sin VLANs configuradas. Cuando los demas switches reciban el mensaje eliminarán todas sus VLANs.

2.3. Ataques basados en STP

Spanning Tree Protocol (SmmTPr) es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles. STP es transparente a las estaciones de usuario.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay bucles en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, Tiempo de Vida) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos caso la red queda inutilizada. Un router, por el contrario, sí podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de bucles. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

Existen múltiples variantes del Spaning Tree Protocol, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

2.3.1. Funcionamiento

Este algoritmo cambia una red física con forma de malla, en la que existen bucles, por una red lógica en árbol en la que no existe ningún bucle. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (B.P.D.U).

El protocolo establece identificadores por puente y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el puente raíz. Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos los puentes que conectan un segmento de red, se elige un puente designado, el de menor coste (en el caso que haya mismo coste en dos puentes, se elige el que tenga el menor identificador "direccion MAC"), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el puerto designado y el que ofrece un camino de menor coste hacia la raíz, el puerto raíz. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

2.3.2. Elección Del Puente Raíz

La primera decisión que toman todos los switches de la red es identificar el puente raíz ya que esto afectará al flujo de tráfico. Cuando un switch se enciende, supone que es el switch raíz y envía las BPDU que contienen la dirección MAC de sí mismo tanto en el BID raíz como emisor. Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de BID raíz es el más bajo será el puente raíz. El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto (32768), lo que hace que el BID sea más pequeño. Esto sólo se debe implementar cuando se tiene un conocimiento profundo del flujo de tráfico en la red.

2.3.3. Elección De Los Puertos Raíz

Una vez elegido el puente raíz hay que calcular el puerto raíz para los otros puentes que no son raíz. Para cada puente se calcula de igual manera, cual de los puertos del puente

tiene menor coste al puente raíz, ese será el puerto raíz de ese puente.

2.3.4. Elección De Los Puertos Designados

Una vez elegido el puente raíz y los puertos raíz de los otros puentes pasamos a calcular los puertos designados de cada LAN, que será el que le lleva al menor coste al puente raíz. Si hubiese empate se elige por el ID más bajo.

2.3.5. Puertos Bloqueados

Aquellos puertos que no sean elegidos como raíz ni como designados deben bloquearse.

2.3.6. Mantenimiento del Spanning Tree

El cambio en la topología puede ocurrir de dos formas:

- El puerto se desactiva o se bloquea
- El puerto pasa de estar bloqueado o desactivado a activado

Cuando se detecta un cambio el switch notifica al puente raíz dicho cambio y entonces el puente raíz envía por broadcast dicha cambio. Para ello, se introduce una BPDU especial denominada notificación de cambio en la topología (TCN). Cuando un switch necesita avisar acerca de un cambio en la topología, comienza a enviar TCN en su puerto raíz. La TCN es una BPDU muy simple que no contiene información y se envía durante el intervalo de tiempo de saludo. El switch que recibe la TCN se denomina puente designado y realiza el acuse de recibo mediante el envío inmediato de una BPDU normal con el bit de acuse de recibo de cambio en la topología (TCA). Este intercambio continúa hasta que el puente raíz responde.

2.3.7. Estado De Los Puertos

Los estado en los que puede estar un puerto son los siguientes:

- Bloqueo: En este estado se pueden recibir BPDU's pero no las enviará. Las tramas de datos se descartan y no se actualizan las tablas de direcciones MAC (mac-address-table).
- Escucha: A este estado se llega desde Bloqueo. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualizan las tablas ARP. Se procesan las BPDU.
- Aprendizaje: A este estado se llega desde Escucha. Las tramas de datos se descartan pero ya se actualizan las tablas de direcciones MAC (aquí es donde se aprenden por primera vez). Se procesan las BPDU.

- Envío: A este estado se llega desde Aprendizaje. Las tramas de datos se envían y se actualizan las tablas de direcciones MAC (mac-address-table). Se procesan las BPDU.
- Desactivado: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

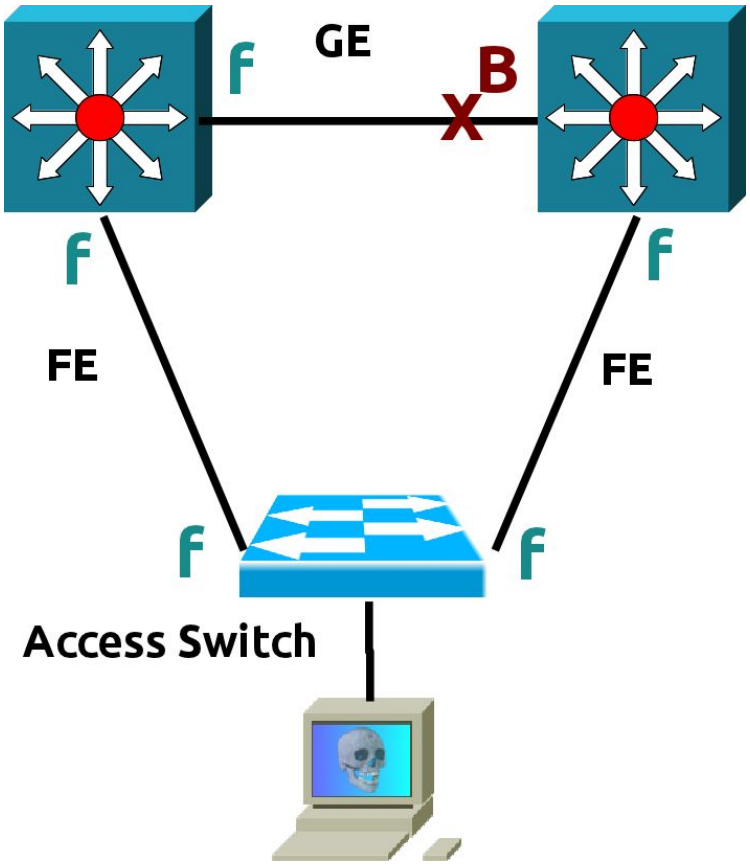
2.3.8. Ataques Basados En STP

- El atacante envía mensajes BPDU forzando recálculos STP.
-

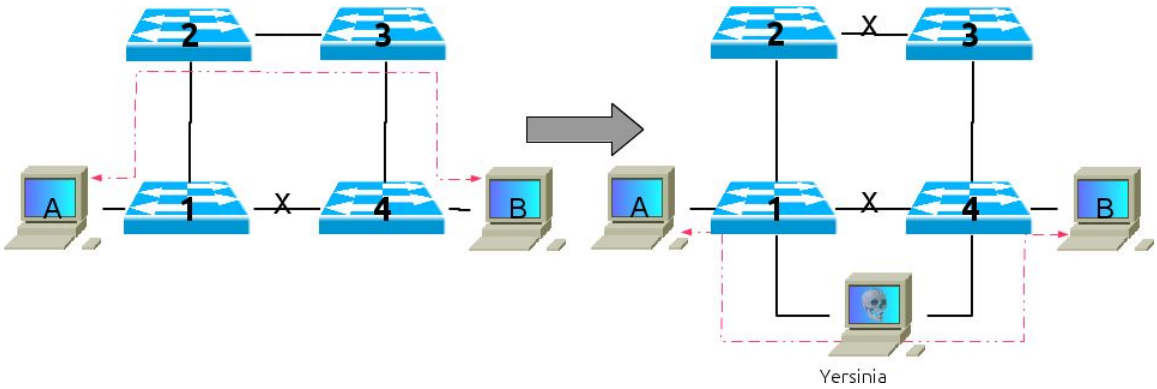
El atacante envía mensajes BPDU para convertirse en root.

- El atacante se convierte en root con lo cual puede ver tramas que no debería (esto permite ataques MiM, DoS, etc)
- Hace falta que el atacante esté conectado a dos switches simultáneamente.

2.3.9. ¿Como Trabaja?.



- El atacante envía mensajes BPDU anunciándose como bridge con prioridad 0.
- El atacante se vuelve root.
- El backbone pasa de ser GE a ser FE.
- Si se lo combina con MAC flooding este ataque puede permitir capturar más tramas.



3. CONTRAMEDIDAS

3.1. Ataques MAC Y ARP

3.1.1. Storm Control.

Una tormenta de paquetes ocurre cuando se reciben en un puerto gran número de paquetes broadcast, unicast o multicast. Reenviar esos paquetes puede causar una reducción de la performance de la red e incluso la interrupción del servicio. Storm Control usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast. Usa un método basado en ancho de banda. Los umbrales se expresan como un porcentaje del total de ancho de banda que puede ser empleado para cada tipo de tráfico.

3.1.1.1. CONFIGURACIÓN STORM-CONTROL

Deseamos configurar el puerto 15 del switch para que si el tráfico broadcast supere el 45% del ancho de banda disponible envíe una alerta.

Las opciones completas son:

Table 3.1: Configuración Storm Control

	Comando	Propósito
Paso 1	*Router(config)#* ***interface*** *{{type[1] slot/port} | {****port-channel*** *number}}*	Seleciona una interfaz para configurar.
Paso 2	*Router(config-if)#* ***storm-control broadcast level*** *level[.level]*	Habilita el tráfico broadcast storm-control en la interfaz, configura el nivel de tráfico storm-control y aplica el nivel de tráfico storm-control a todos los modos de tráfico storm-control habilitados en el puerto.
	Router(config-if)# ***no storm-control broadcast level***	Deshabilita el tráfico broadcast storm-control en el puerto.
Paso 3	*Router(config-if)#* ***storm-control multicast level*** *level[.level]* ***Note*** *The* ***storm-control multicast*** *command is supported only on Gigabit Ethernet interfaces.*	Habilita el tráfico multicast storm-control en la interfaz, configura el nivel de tráfico storm-control y aplica el nivel de tráfico storm-control a todos los modos de tráfico storm-control habilitados en el puerto.
	Router(config-if)# ***no storm-control multicast level***	Deshabilita el tráfico multicast storm-control en el puerto.
Paso 4	*Router(config-if)#* ***storm-control unicast level*** *level[.level]* ***Note*** *The* ***storm-control unicast*** *command is supported only on Gigabit Ethernet interfaces.*	Habilita el tráfico unicast storm-control en la interfaz, configura el nivel de tráfico storm-control, y aplica el nivel de tráfico a todos los modos de tráfico storm-control habilitados en la interfaz.
	Router(config-if)# ***no storm-control unicast level***	Desabilita el tráfico unicast storm-control en la interfaz.
Paso 5	*Router(config-if)#* ***end***	Sale del modo de configuración.
Paso 6	*Router#* ***show running-config*** *interface*	Verifica la configuración.

3.1.2. Puertos Protegidos.

Ciertas aplicaciones requieren que nos se reenvíe tráfico entre puertos en un mismo switch de manera que un equipo no ve el tráfico generado por otro (inclusive tráfico broadcast y
multicast).

- No se puede reenviar tráfico entre puertos protegidos a nivel de capa 2.
- El tráfico entre puertos protegidos debe ser reenviado a través de un dispositivo de capa 3.
- El reenvío de tráfico entre puertos protegidos y no protegidos se realiza de manera normal.

3.1.2.1. CONFIGURACIÓN PARA UN PUERTO PROTEGIDO.

Table 3.2: Para configurar un puerto como protegido.

	Comando	Propósito
Paso 1	***Configure terminal***	Entra al modo de configuración global.
Paso 2	***Interface*** *interface id*	Especifica el puerto a ser configurada, y entra al modo de configuración de el puerto.
Paso 3	***Switchport protected***	Configura el puerto para ser un puerto protegido.
Paso 4	***end***	Retorna al modo EXEC privilegiado.
Paso 5	***Show interfaces*** *interface-id switchport*	Verifica tus entradas.
Paso 6	***Copy*** ***running-config*** ***start-up config***	(Opcional) Guarda tus entradas y el archivo de configuración.

3.1.3. Port Security.

Conjunto de medidas de seguridad a nivel de puertos disponibles en la mayoría de los switchs de gama media y alta. La funciones provistas dependen de la marca, el modelo y la versión de firmware del switch en cuestión. Permite entre otras cosas:

- Restringir el acceso a los puertos según la
- MAC. Restringir el número de MACs por puerto.
- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
- Establecer la duración de las asociaciones MAC-Puerto.

3.1.3.1. **CONFIGURACION PORT-SECURITY**

Deseamos configurar el puerto 15 del switch para que no acepte más de dos direcciones MAC.

- No se puede activar port security en puertos dynamic access o trunk.
- Port Security está desactivado por default.
- Por default port security sólo almacena una sola MAC por puerto.

Además podemos especificar qué hacer si ese número de direcciones MAC es superado (por default deshabilitar el puerto):

- Que deje de aprender
- Que envíe una alerta administrativa
- Que deshabilite el puerto

	Comando	Propósito
Paso 1	*Switch(config)#* ***interface*** *interface_id*	Entra en el modo de configuración de el puerto para configurar, por ejemplo gigabitethernet 3/1.
Paso 2	*Switch(config-if)#* ***switchport mode access***	Coloca el modo de el puerto en access; un puerto en el modo por defecto (dynamic desirable) no puede ser configurada como puerto seguro
Paso 3	*Switch(config-if)#* ***switchport port-security***	Habilita Port-security en la interfaz.
Paso 4	*Switch(config-if)#* ***switchport port-security maximum*** *value*	(Opcional) Coloca el máximo número de direcciones MAC seguras para el puerto. El rango es de 1 a 1024: por defecto está en 1.

Tabla 3.3: Configuración Port-security

3.2. Seguridad Capa 2: VLAN Privadas.

Para prevenir este tipo de ataques debemos hacer lo siguiente:

- Deshabilitar auto trunking para todos los puertos:
- Deshabilitar VTP:
- Si es realmente necesario, usar la versión 2.
- Siempre utilizar una VLAN dedicada para los puertos trunk.
- Deshabilitar los puertos no utilizados y colocarlos en una VLAN no utilizada.
- No utilizar la VLAN 1 para nada.
- Colocar todos los puertos de los usuarios como non-trunking (Deshabilitar DTP).

3.3. Ataques STP

- No deshabilitar STP (introducir un loop puede convertirse en una forma de ataque).
- Habilitar BPDU Guard.
- Habilitar Root Guard.