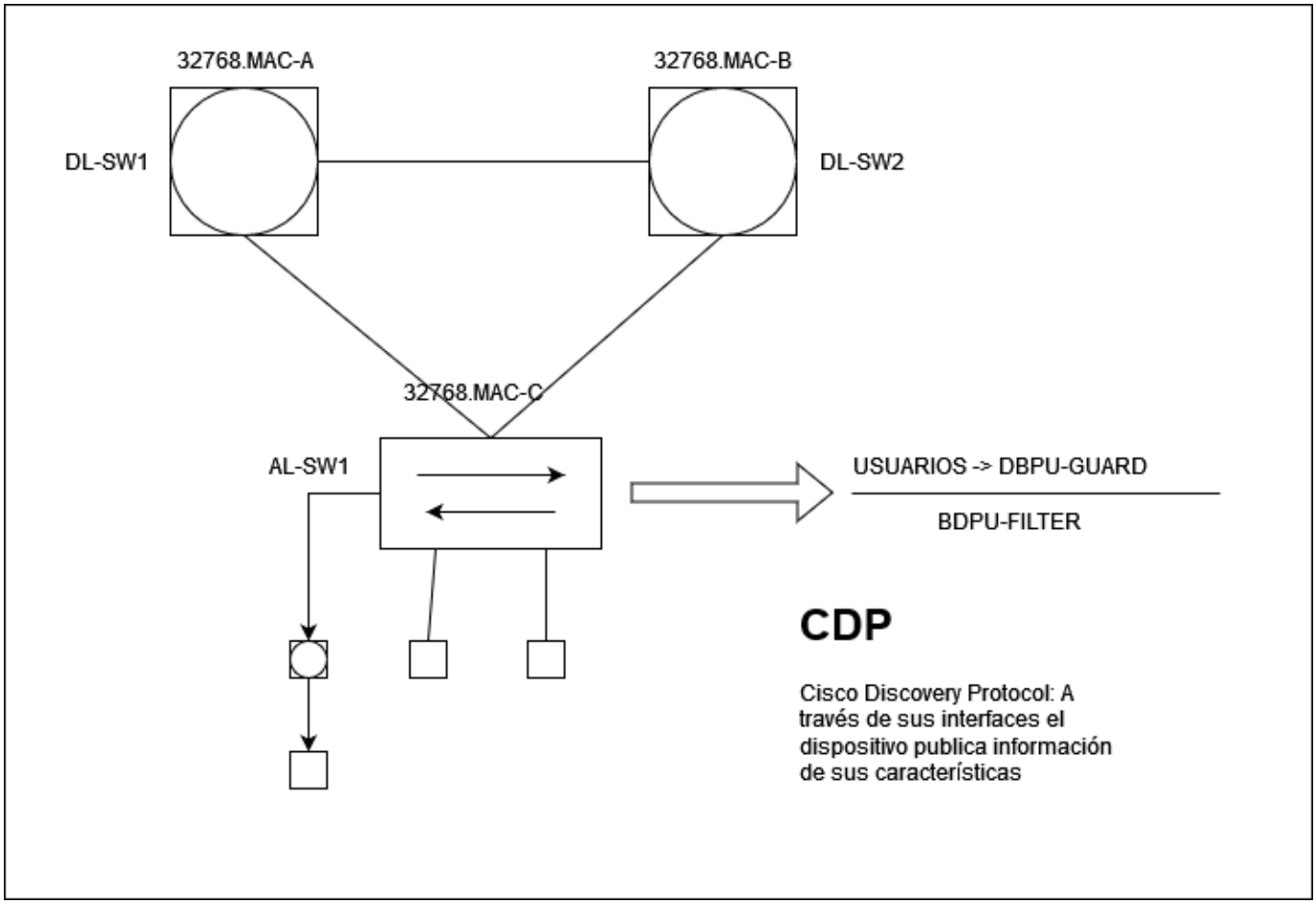
Seguridad LAN en entornos Ethernet

Configuridad de seguridad básica en Switches

- Contraseñas Seguras
  - Se debe usar siempre la opción secret, además de letras números y caracteres especiales.
  - Activar “service password-encryption” para evitar que las contraseñas se puedan descubrir mirando la configuración.
  - Utilizar gestión de usuarios AAA:
- Configuración de advertencias: Propósito disuasivo
  - “banner motd” o “banner login” como mensaje previo a la autenticación
  - Tanto para fines legales como administrativos, se configura un mensaje de advertencia.
- Acceso seguro a la consola: seguridad física y lógica configurando el control de acceso
- Acceso Seguro a través de líneas VTY:
  - Usar SSH2 en vez de telnet
  - Aplicar ACLs a las líneas VTY para limetar el acceso a solo las estaciones de gestión desde ciertas subredes. Se limita el acceso administrativo a determinadas IPs origen.
  - Uso de control de acceso AAA-NewModel
- Deshabilitar daemon HTTP:
  - Se recomienda su desactivación o, si no es posible, activar el modo HTTP secure con : “ip http secure-server”
  - Configurar ACLs para permitir acceso SOLO desde redes seguras.
- Deshabilitar servicios innecesarios
- Utilización de SNMPv3 con autenticaciín y privacidad y ACLs para limitar el acceso SNMP a las estaciones de trabajo y subredes de confianza

Asegurar topología de Spanning-Tree



- La introducción accidental o maliciosa de BPDUs puede bloquear un dispositivo o crear una denegación de servicio.
- Es necesario identificar al puente raiz configurando la prioridad
- Se debe activar la función “root-guard” para evitar que switches no autorizados se conviertan en raiz
- BDPU-Guard: Evita que los host envíen BPDUs de forma maliciosa de forma que si se recibe una BPDU maliciosa se desactiva el puerto hasta que sea reactivado por un administrador o hasta que pase cierta cantidad de tiempo.
- No se deben configurar BPDU guard y BPDU filter en el mismo puerto ya que podría generar bucles. Se reomienda que esté solo activa la funcionalidad BPDU filter
- Se debe reducir al mínimo el uso de CDP/LLDP.
- Configurar un sistema de log básico (Syslog)

Los switches Catalyst con Cisco IOS negocian automáticamente las capacidades de trunking:

	ACCESS	**Automatic**	**Desirable**	**Trunk**	**No Negotiate**
ACCESS	Acceso	Acceso	Acceso	ERROR	ERROR
Automatic	Acceso	Acceso	Trunk	Trunk	ERROR
Desirable	Acceso	Trunk	Trunk	Trunk	ERROR
Trunk	ERROR	Trunk	Trunk	Trunk	Trunk
No Negotiate	ERROR	ERROR	ERROR	Trunk	Trunk

- La negociación permite la introducción de un puerto de enlace troncal no autorizado en la red. Si uno de estos puertos no autorizados se usa para interceptar tráfico y generar ataques DDOS las consuecuencias pueden ser muchísismo peores que si se usa un puerto de acceso. Esto podría afectar a múltiples vlans.

- para evitar esto se desactiva la negociación automática de trunking en los puertos de acceso y en los troncales, además se eliminan las vlans no utilizadas en los troncales con “trunk allowed”

Para configurar esto existen los siguientes comandos:

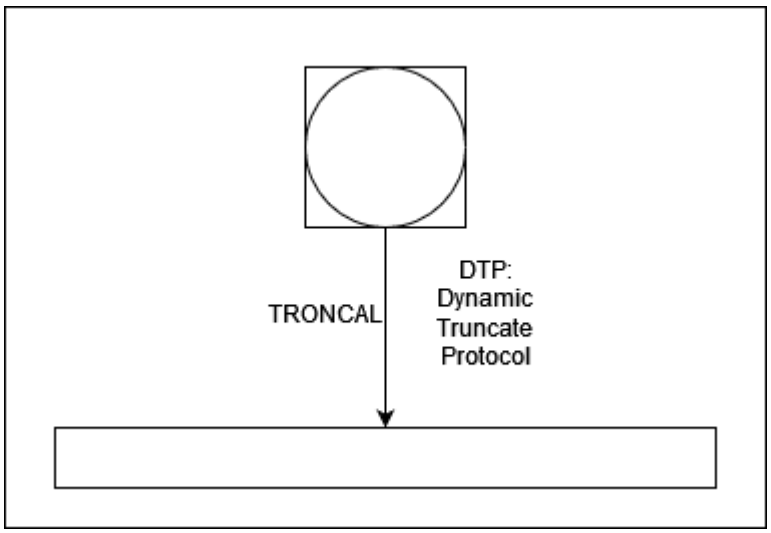
```
switchport mode trunk
switchport mode nonegotiate
switchport trunk vlan allowed
```

Configuración de puertos no utilizados:

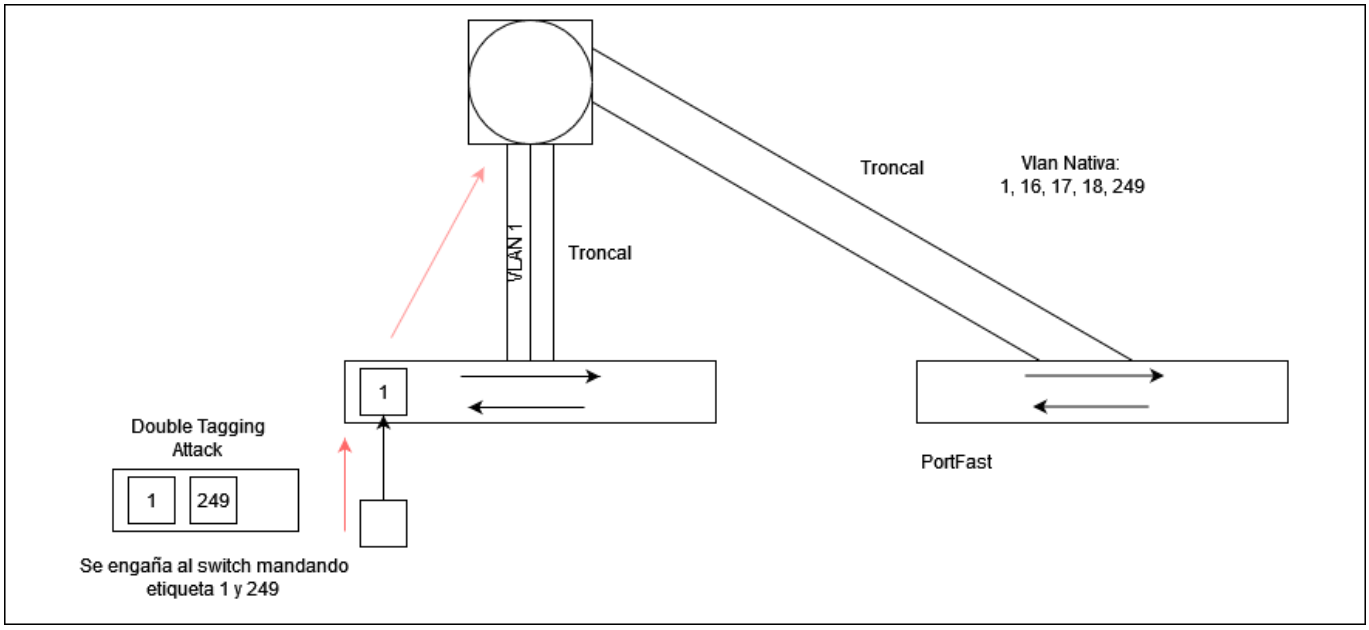
- “shutdown”
- Colocarlos en una VLAN que no se propague por puertos trunking o en una vlan que no exista
- Definirlos como puetos de acceso, desacviando la negociación automática de trunking

Elaces troncales:

- Configurar manualmente todas las acciones trunk y deshabiltiar DTP
- Configurar una VLAN nativa (VLAN sin etiqueta) que solo esté operativa en los enlaces troncales.
- Una VLAN nativa es una propiedad e los enlaces troncales que asigna una vlan sin etiqueta, lo normal es que estas no se utilicen, en switches modernos pueden ser deshabilitadas.



La VLAN 1 siempre está habilitada, el tráfico de servicio va por la VLAN 1, aunque se trate de deshabilitar el switch no va a obedecer.



Vulnerabilidades mitigables en capa 2

- Análisis Pasivo: Recopilación de información sin inyección de tráfico
  - Escucha el tráfico recibido en un puerto, es posible utilizar herramientas para descubrir información sin hacer mucho ruido (arpin, netdiscover, nmap)
- Análisis Activo: Se inyecta tráfico a nivel de capa 3 en la red, pero el ataque puede ser detectado más facilmente (ping, fping, hping3, nmap, metasploit...)

Ataques comunes

Accesos no autorizados desde dispositivos falsos

- Conexión de un punto de acceso no autorizado a la infraestructura de red: Brecha de seguridad ya que puede crear un punto de entrada tras el firewall.
  - Esta vulnerabilidad se abrava debido a que no suelen configurarse las medidas de seguridad en estos dispositivos
  - Acceso inalámbrico a redes abiertas: Ataque de suplantación
- Dispositivos de capa 2: Un tacante con acceso físisco puede colocar un switch para alterar el funcionamiento STP para provocar saltos de VLANS, snifar el tráfico, etc... Para evitar la manipulación de STP se portege para que no acepte BPDUs falsas y fijar la ubicación del switch raiz.

MAC flooding attack (Saturación de la Tabla de Envío)

Consiste en sobrecargar la tabla CAM para que las tramas convencionales se envíen por todos los puertos en vez de solo por el puerto que esté conectado al dispositivo de destino, esto permite recibir todo el tráfico que circula por una red y hacer ataques DDOS. Las tablas CAM tienen un tamaño limitado, por lo que si se introducen un número muy alto de direcciones MAC en esta tabla, este no podrá aprenderse las direcciones mac correctas asignadas a cada puerto, por lo que cada vez que se

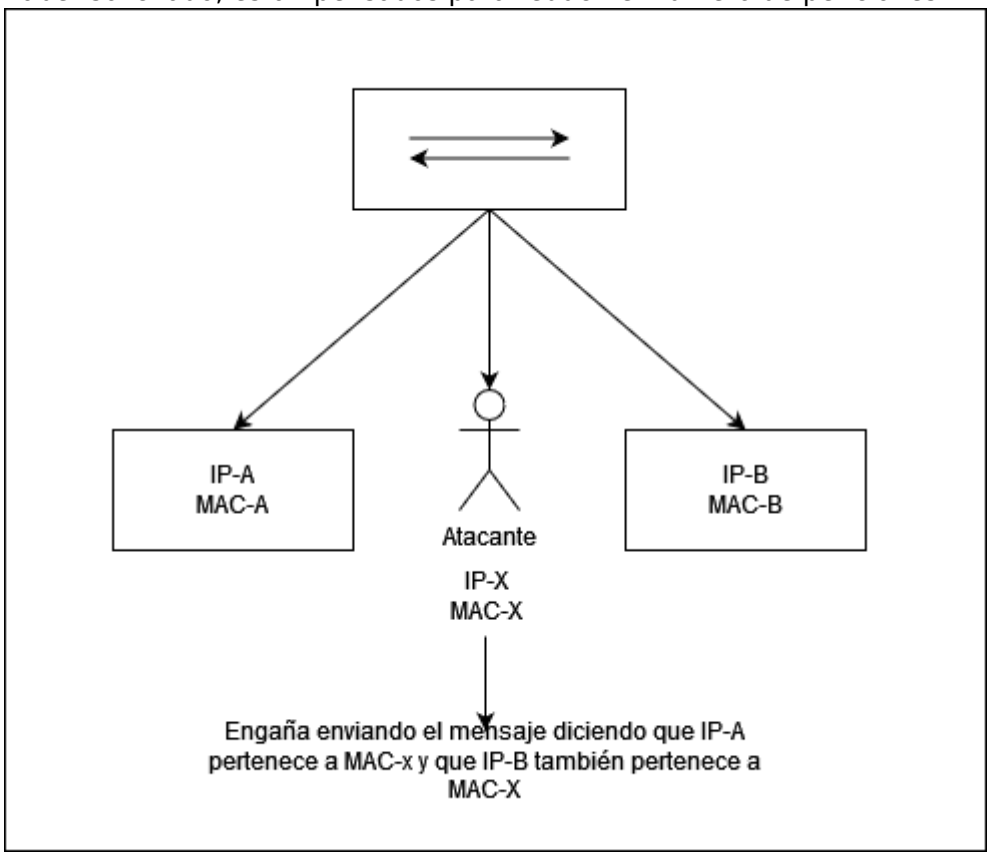
deba enviar tráfico a un dispositvo, se enviará por todos los puertos menos por el que entró ya que el switch no tendrá el dispositivo en cuestión en su tabla mac. Algunos efectos adeversos de esto son que el sitch envía tráfico de forma ineficiente y que un intruso podría recibir información a la que normalmente no podría acceder.

Si el ataque se realiza una sola vez, cuando expiren las entradas no válidas de la tabla CAM el switch podrá aprender las direcciones correctas, por lo que desaparecerá el flooding y el intruso no será detectado. Se recomienda la siguiente contramedida:

- Configuración de Port Security: Define un numero máximo de MACS que se pueden aprender por puerto y se define que direcciones MAC están permitidas en el puerto

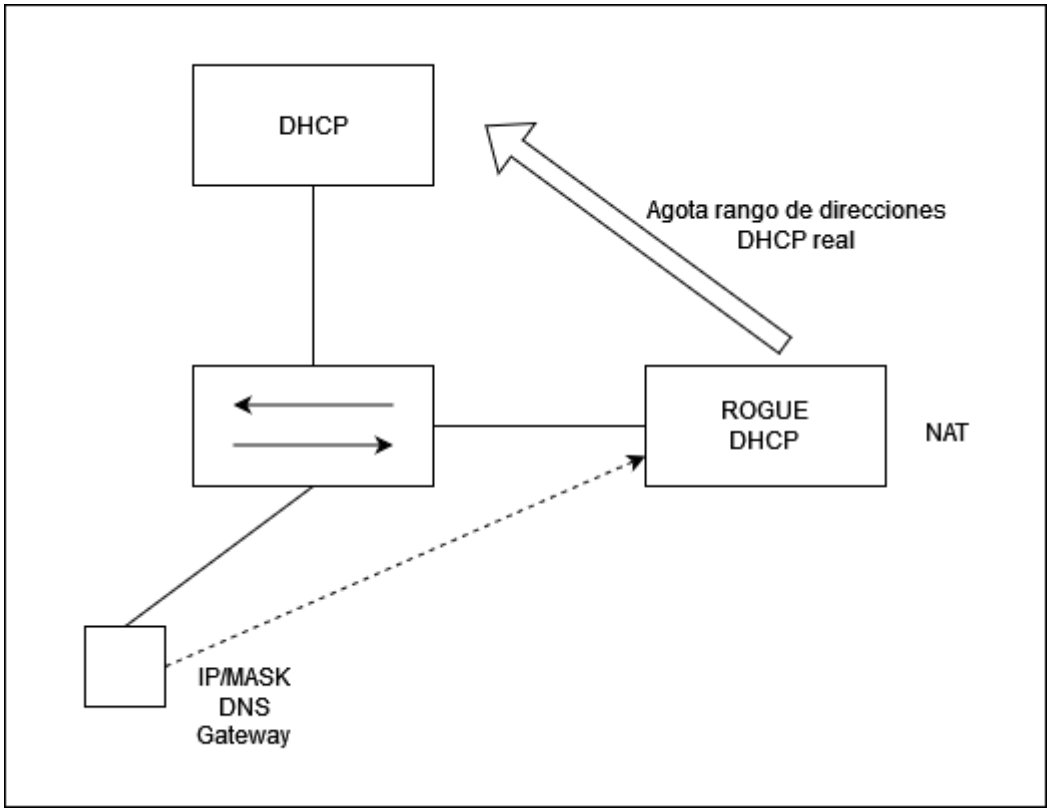
ARP Spoofing Attach

Consiste en utilizar “Gratuitous ARP” que consisten en notificar a los demás cual es la IP y Mac sin haber solicitado, están pensados para reducir el número de peticiones ARP.



DHCP Spoofing

Suplantamos un servidor DHCP.



Medidas de seguridad

Un método de prevención es la creación de VLANS anidadas o vlans privadas, lo que consiste en crear VLANs dentro de otras VLANs.

Port Security

La idea es limitar el número de mac simultáneas aprendidas por puerto, cuando se habilita, un puerto solo puede aprender una dirección MAC simultánea. El problema viene cuando se usan máquinas virtuales, ahí lo que se hace es permitir el aprendizaje de varias direcciones mac:

```
switchport port security maximum
```

Si un puerto alcanza el número máximo de MAC pasa a estado de error disable: para reactivarlo hay que entrar en el puerto, hacer un shutdown y un no-shutdown (Básicamente, tumbarlo y destumbarlo).