# UD3. Seguridad en switches

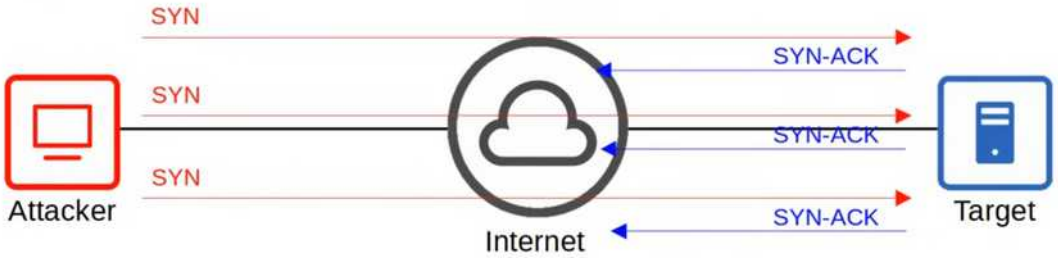
## Índice

# Tipos de Ataques

## DoS

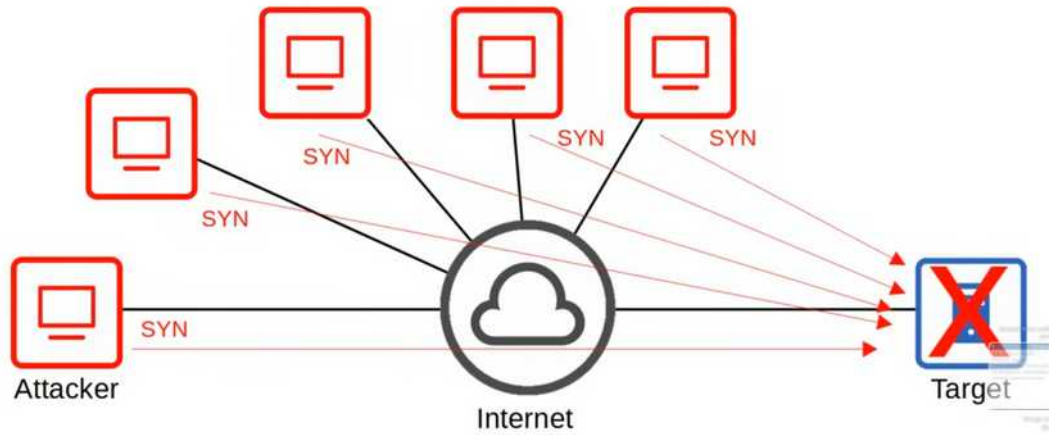
Denegación de servicio. Ejemplo TCP SYN flood

→ TCP three-way handshake: SYN | SYN-ACK | ACK
→ The attacker sends countless TCP SYN messages to the target.
→ The target sends a SYN-ACK message in response to each SYN it receives.
→ The attacker never replies with the final ACK of the TCP three-way handshake.
→ The incomplete connections fill up the target's TCP connection table.
→ The attacker continues sending SYN messages.
→ The target is no longer able to make legitimate TCP connections.



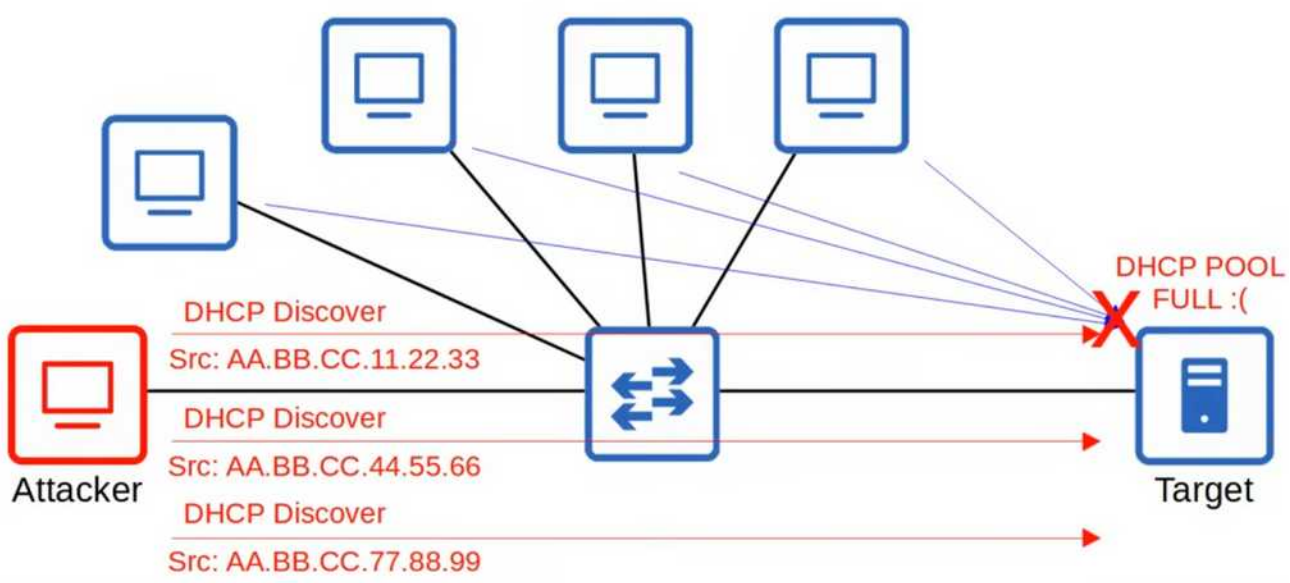

## DDoS

Denegación de servicio distribuido. Lo  mismo pero usando un conjunto de PC's como atacantes. Normalmente PC's zombies que contienen un malware que hace este ataque. El conjunto de PC's atancantes se denomina **botnet**



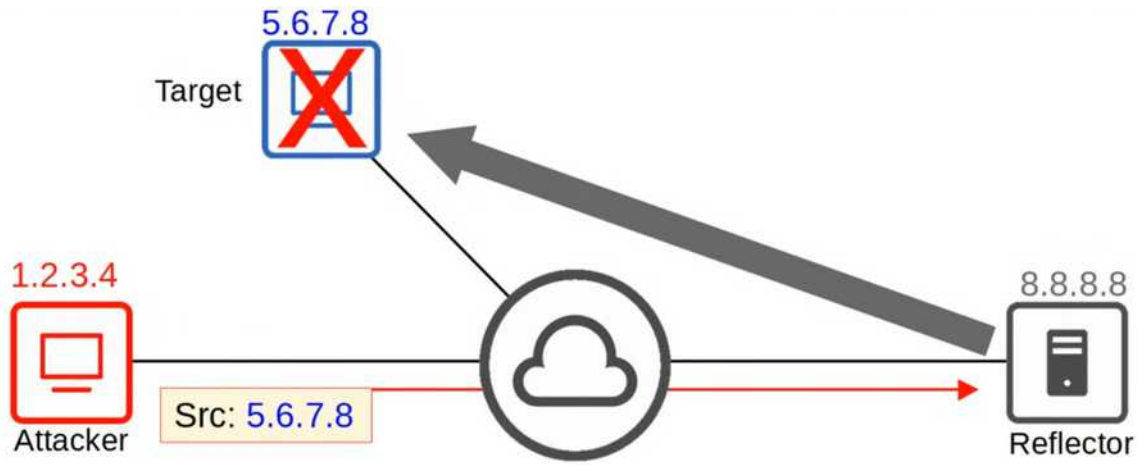
## Spoofing Atack. DHCP Starvation

Spoof significa usar una dirección falsa (una dirección MAC o IP)
No es un ataque simple sinó un tipo de ataque. Por ejemplo puede ser usado para un DHCP starvation en el que un atacante falsea una dirección MAC de origen para inundar un servidor DHCP con paquetes Discover, cuando el DHCP se queda sin direcciones IP ya no contesta a los PC's legítimos y por tanto se produce un DoS




## Refection/Amplication Attack

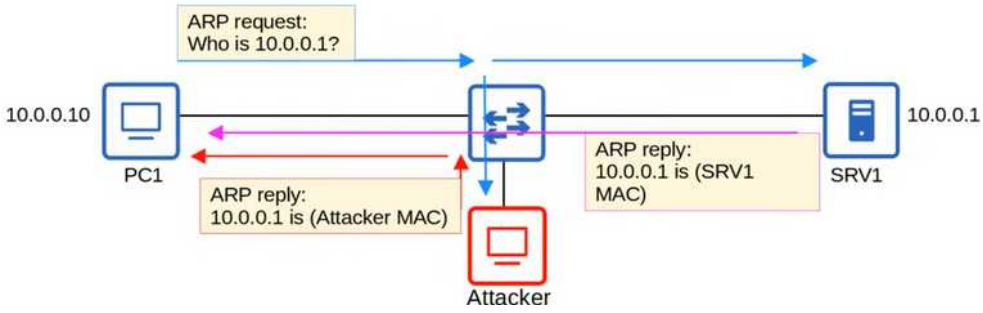
El atacante envía tráfico a un reflector con dirección de origen falseada con la dirección del target por lo que si el tráfico es lo suficientemente grande se produce un DoS en el target. En este ataque digamos que el reflector hace el trabajo por nosotros. El ataque será amplificado si pequeñas cantidades de tráfico del atacante producen grandes cantidades de tráfico en el target



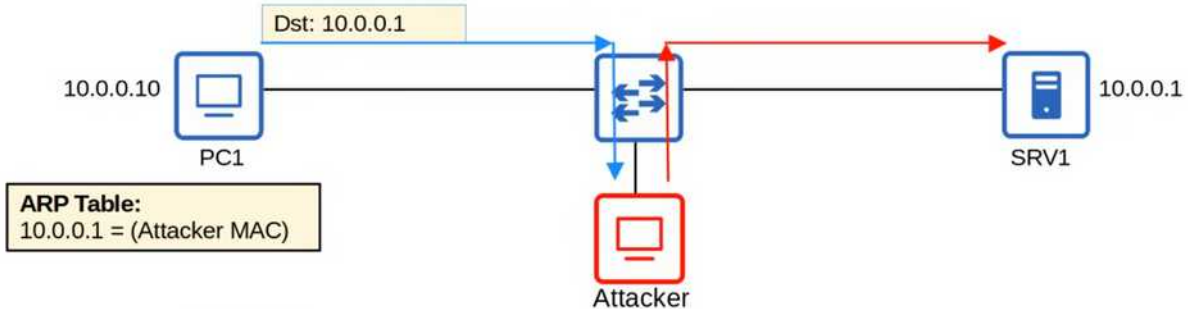
## Man-in-middle

El atacante se sitúa a sí mismo entre la fuente y el destino para curiosear o incluso modificar el tráfico antes de que llegue a su destino. Se da en todas las capas del modelo TCP/IP, un ejemplo en las capas bajas es el ARP Spoofing o también llamado ARP poisoning (envenenamiento ARP)

En el envenenamiento ARP el host manda una solicitud ARP preguntando la IP de un servidor, como es broadcast, el atacante también la recibe.
El servidor responde con su propia MAC
El atacante espera un momento y construye un paquete con su propia MAC en respuesta a la solicitud del PC lo que produce que el PC actualice su tabla MAC son la IP del atacante. Esto hace que todas las solicitudes las envíe al atacante que se pone en medio.




Así, el atacante recibe las peticiones, las mira, las cambia si quiere y luego las envía al servidor y reenvía de vuelta las respuestas haciendo que el PC no se entere




## Ataque de reconocimiento

No son ataques en si mismos sinó que buscan recopilar información sobre un target para ser usado un un ataque futuro. En las capas bajas se trata normalmente de información pública obtenida con nslookup, Whois, nmap, etc
Un whois web lo tenemos en https://lookup.icann.org/lookup
una vez obtenida la información un ingeniero social puede vender los datos, o pasarlos a un atacante.

## Malware

Malicious Software. Software que infecta un computador
Virus. Infecta un programa que está en el PC
Worms. No requiere un programa que infectar, puede infectar y expandirse por otros PC's sin el concurso del usuario. Expandir gusanos puede congestionar la red.
Troyanos. Son software disfrazado de legítimo que infecta al abrir adjuntos de emails o bajarse ficheros de internet.

# Ingeniería social

Ataca el punto más vulnerable del sistema: la gente. Implica manipulación psicológica para revelar información confidencial o que el usuario haga algo que le interese al atacante.

### Phishing

involucra emails fraudulentos que parecen de un negocio legítimo como Amazon, un banco, etc. Contiene links a un website fraudulento para por ejemplo haciendose pasar por el login del banco conseguir tus claves.
el spear phising es un tipo en el que los target son individuos específicos, por ejemplo el personal de cierta empresa, en lugar de mandar un email a una lista de gente cualquiera, lo hacemos específico a una lista concreta con lo que nuestro email parecerá más real pues contendrá información que esa lista de gente considera que le dá al mail visos de realidad. El Whaling es lo mismo pero cuando se manda a una persona concreta de gran interés como un CEO, una celebridad, periodista, político/a etc.

### Vishing

Voice Phising es el phising hecho por teléfono, por ejemplo para que nos cambiemos de compañía telefónica, de luz, etc. También puede ser spear vishing haciendose pasar por el servicio técnico de la compañía para resetear el password, etc.

### Smishing

Lo mismo por SMS

### Watering hole

El atacante pone un link malicioso en un website en el que el target confía y por tanto no duda en clicar.

### Tailgating

Se trata de entrar en áreas seguras simplemente andando detrás de una persona autorizada en el momento en que entra. Por ejemplo una persona por ser educada puede mantener abierta la puerta a una persona mayor que vaya detrás pensando que también está autorizada.

### Conseguir Passwords

pueden adivinarse las passwords por ataque de diccionario o fuerza bruta, por eso se usa autenticación multi-factor o en varios pasos pidiendo dos de estas:
algo que sabes: user/password, pin...
algo que tienes: un movil en el que presionas en una notificación, un pin enviado por sms...
algo que eres: tu huella digital, tu cara...
También se usan certificados digitales que se ven el año que viene

# AAA

Autenticación, Authorization, Accounting, o sea autenticación, autorización y logging de los cambios.
Esto se hace con servidores AAA (por ejemplo ISE de Cisco Identity Services Engine).
Los servidores AAA usan uno de estos protocolos:
RADIUS: Protocolo estándar abierto que usa los puertos UDP 1812 y 1813
TACACS+ que es unprotocolo propietario de Cisco que usa el puerto TCP 49

# Ataques a Switches

## ataque por desbordamiento de MACs

Cuando un host envía una trama en una LAN no hay nada que le impida poner la dirección MAC de origen que desee Incluso puede poner una dirección diferente en cada trama.

Con un sencillo programa un host puede enviar miles de tramas por segundo con direcciones MAC diferentes, todas falsas, de ese modo rápidamente desbordará la tabla CAM de cualquier conmutador

A partir de ese momento el conmutador difundirá todo el tráfico por inundación, actuando como si fuera un hub.

Con un programa de análisis de tráfico (sniffer o similar) el ordenador atacante, o cualquier otro de la red, podrá a partir de ese momento capturar el tráfico de otros ordenadores, incluidas las combinaciones usuario/contraseña utilizadas por los usuarios para acceder a los servicios (por ejemplo para leer el correo)

### Soluciones al ataque por desbordamiento

Algunos conmutadores permiten limitar por configuración el número de direcciones MAC asociadas a cada puerto. En ese caso cuando el conmutador recibe por un puerto mas MACs diferentes que las permitidas deshabilita el puerto (lo pone en modo shutdown)

En una LAN en estrella, los conmutadores del final deberían limitar los puertos de usuario a 1 MAC por puerto ya que contendrán solamente ordenadores conectados a ellos y no otros conmutadores.

```
switch(config)# interface f0/2
switch(config-if)# switchport port-security maximum 1
```

También se pueden configurar en el conmutador las MACs que se permiten en cada puerto, es decir construir de forma estática la tabla CAM. Esto es lo más seguro, pero impide la movilidad de equipos por lo que no suele hacerse.

## ataque por envenenamiento

Si las tramas ‘envenenadas’ (con direcciones de origen falsas) llevan como destino la dirección broadcast o cualquier dirección inexistente se distribuyen por toda la LAN, con lo que un solo host puede desbordar las tablas CAM de todos los conmutadores. El envenamineto ARP se puede producir por responder a peticiones o por mandar ARP gratuitous.

El host atacante puede husmear el tráfico de cualquier otro host en la LAN ya que los hosts de la red van a actualizar sus tablas MAC y van a enviarle el tráfico en lugar de a los destinos legítimos. Por ejemplo un atacante puede mandar un GARP con la dirección ip del router y su propia MAC con lo cual recibirá todo el tráfico de la red con destino fuera.

Además el rendimiento de la red disminuye considerablemente, pues todos los puertos reciben todo el tráfico. La red funciona como un medio compartido.

# Deshabilitar puertos en desuso

Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Por ejemplo, si un switch Catalyst 2960 tiene 24 puertos y hay tres conexiones Fast Ethernet en uso, es aconsejable inhabilitar los 21 puertos que no se utilizan. Navegue hasta todos los puertos que no se utilizan y emita el comando **shutdown** de Cisco IOS. Si más adelante se debe reactivar un puerto, este se puede habilitar con el comando **no shutdown**. La figura muestra el resultado parcial para esta configuración.

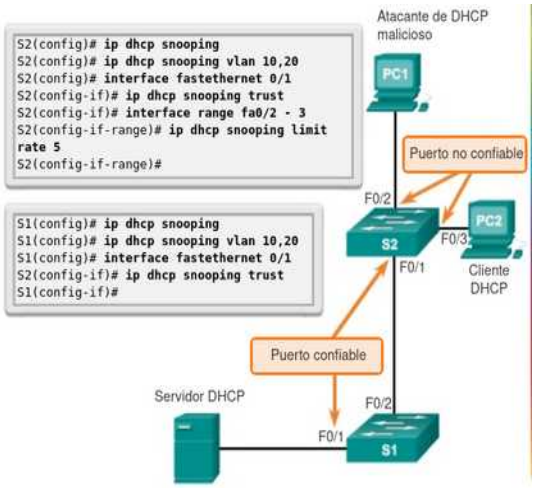
Realizar cambios de configuración a varios puertos de un switch es sencillo. Si se debe configurar un rango de puertos, use el comando **interface range**.

Switch(config)# **interface range *primer-número – último-número***

El proceso de habilitación e inhabilitación de puertos puede llevar mucho tiempo, pero mejora la seguridad de la red y vale la pena el esfuerzo.

# Snooping DHCP

El snooping DHCP es una función que determina cuáles son los puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, incluidos los paquetes de oferta de DHCP y de acuse de recibo de DHCP; los puertos no confiables solo pueden recibir solicitudes. Los puertos confiables de los hosts se alojan en el servidor de DHCP o pueden ser **un enlace hacia dicho servidor**. Si un dispositivo no autorizado en un puerto no confiable intenta enviar un paquete de oferta de DHCP a la red, el puerto se desactiva. Esta función puede unirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP.




**Ponemos confiables las interfaces de los switches que apuntan al servidor DHCP**

Los puertos no confiables son aquellos que no están configurados explícitamente como confiables.

## DHCP Starvation (DoS atack)

Un atacante envía tramas de DHCP Discover con CHADDR MAC's aleatorias consiguiendo que se le asignen IP's hasta acabar con el pool de direcciones del servidor DHCP lo que lleva a una denegación de servicio a los clientes legítimos. El CHADDR (Client Host Address) es necesario por si la trama viene de un relay, por eso el servidor DHCP no se fija en la MAC de la trama sinó en la que va dentro del paquete.

## DHCP Poisoning (M-i-t-M)

Similar al ARP poisoning, un servidor DHCP espúreo responde a los mensajes de discover de los clientes asignándoles ip's y de paso hace que los clientes lo usen a él como default gateway. El atacante puede examinar entonces todos sus paquetes o incluso modificarlos.

## Funcionamiento

DHCP Snooping diferencia entre mensajes DHCP Server (Offer, ACK y NACK) y mensajes DHCP Cliente (DISCOVER y REQUEST, Release, Decline)

Los mensajes de Servidor son prohibidos en los puertos untrust y los cliente son investigados para ver si son legítimos o no.

- Si se recibe un mensaje en un puerto trusted se reenvía sin inspección

- si se recibe un mensaje en un puerto untrusted se inspecciona:

- si es un mensaje de servidor se descarta ysi es un mensaje de cliente se inspeccionan MACs

## Para habilitar el DHCP snooping:

Paso 1. Habilita la detección de DHCP mediante el comando **ip dhcp snooping** del modo de configuración global.

Paso 2. Habilita la detección de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan número**. Es necesario el paso anterior, no llega con éste sólo

Paso 3. Definimos los puertos como confiables en el nivel de la interfaz mediante la identificación de los puertos confiables con el comando **ip dhcp snooping trust**.

Paso 4. (Optativo) Limitamos la velocidad a la que un atacante puede enviar solicitudes de DHCP falsas de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate velocidad**. Por ejemplo ip dhcp snooping limit rate 1 limita a 1 mensaje DHCP por segundo, si se supera esta ratio el puerto será puesto en err-disabled con lo que tendremos que deshabilitarlo y habilitarlo como en port-security. También se puede hacer que se recupere automaticamente con **errdisable recovery cause dhcp-rate-limit** del modo de configuración global.

Pondremos también para evitar problemas con agentes relay y la inserción de la opción 82 con el comando **no ip dhcp snooping information option**

Con **show errdisable recovery** vemos los modos que tenemos habilitados, podemos habilitar el que queramos con errdisable recovery cause *causa*. Vemos que hay un tiempo de espera hasta que se recupere que podemos cambiar con **errdisable recovery interval segundos**

Paso 5. Ver la tabla con **show ip dhcp snooping binding**

# DAI (Dynamic Arp Inspection)

La Inspección Dinámica de ARP (DAI) es una función de seguridad que valida los paquetes del Protocolo de Resolución de Direcciones (ARP) en una red. DAI permite al administrador de red interceptar, registrar y descartar paquetes ARP con enlaces de direcciones MAC a direcciones IP no válidos validando contra la tabla de dhcp snooping. Esta capacidad protege la red de ciertos ataques de M-i-M como el envenenamiento ARP. Todos los puertos son no confiables por defecto. Típicamente los puertos conectados a switches y routers serán confiables y los conectados a hosts no.

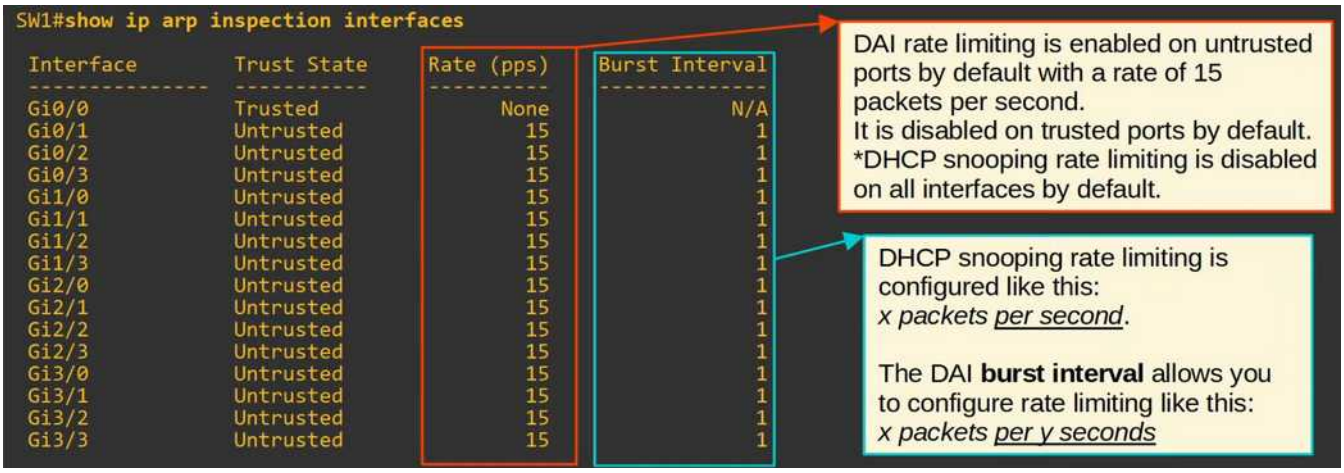
DAI inspecciona la MAC origen, IP origen de los mensajes ARP recibidos en puertos no confiables y mira si coinciden con la tabla DHCP snooping.
Hay que entender que ésto solo funciona para hosts que usan DHCP. Existen ARP ACL's que pueden ser configuradas manualmente para hosts que no usan DHCP

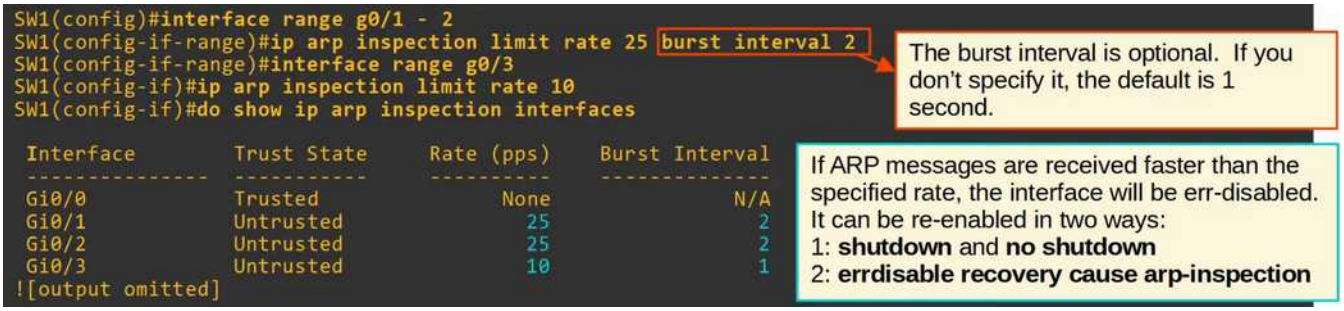
Al igual que DHCP snooping, DAI tambien tiene un rate-limit para prevenir ataques que sobrecarguen el switch con mensajes ARP. Date cuenta que ambos requieren CPU para funcionar, aunque los mensajes del atacante sean bloqueados, pueden conseguir un DoS sobrecargando la CPU enviando ARP's

Switch(config)# **ip arp inspection vlan numero**

Para confiar en puertos debemos, desde la configuración del interface o del rango poner:
Switch(config-if)# **ip arp inspection trust**

Switch# **show ip arp inspection interfaces**



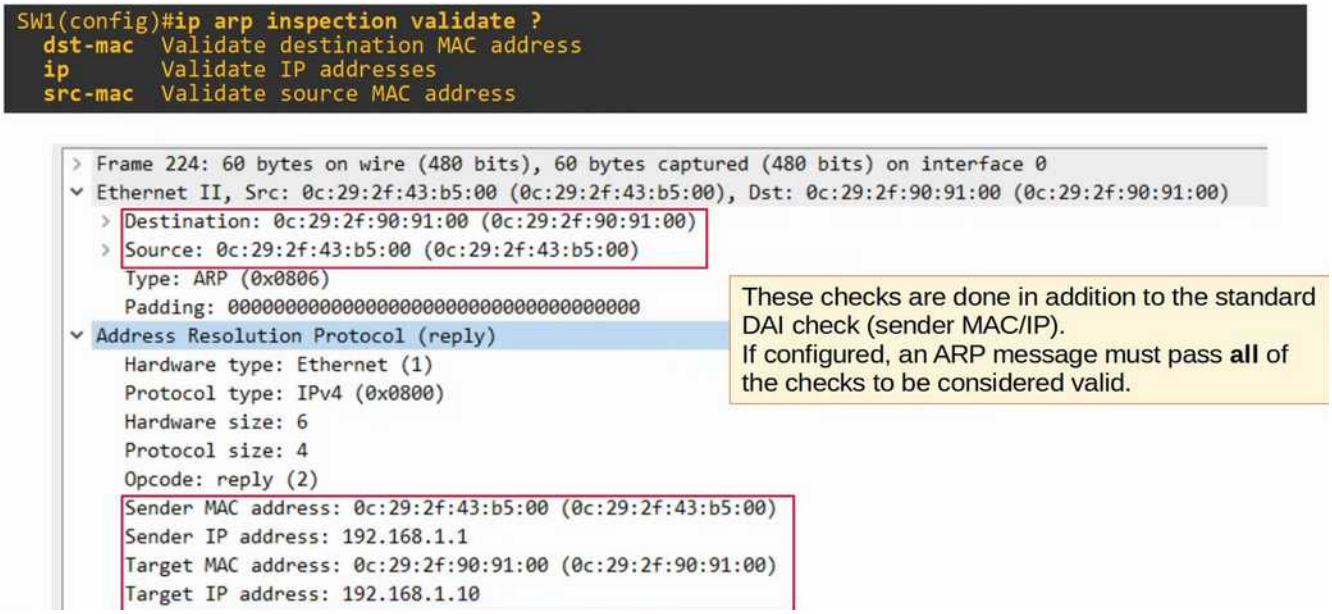
Podemos validar más profundamente todas las MAC con
Switch(config)# **ip arp inspection validate dst-mac src-mac ip**

**dest-mac** valida la MAC destino en la cabecera ethernet contra la MAC del paquete ARP para respuestas ARP

**src-mac** valida la MAC origen en la cabecera ethernet contra la MAC del paquete ARP para solicitudes y respuestas ARP

**ip** valida que la ip sea válida para un host, es decir, que no sea 0.0.0.0 o 255.255.255.255 o similar.

Estas validaciones son a mayores de la validación que hace DAI contra la tabla DHCP snooping, hay que ponerlas en el mismo comando, no en varios, si queremos validar 1, 2 o las tres




## ACL’s

Para crear una ACL para los servidores que no usan DHCP usamos

Switch(config)# **arp access-list** *nombre*

Switch(config-arp-nacl)# **permit host** *ip* **mac host** *mac*

Switch(config)# **ip arp inspection filter** *nombre* **vlan** *numero*

Lógicamente si el servidor cambia de IP tenemos que variar la ACL, también si otros equipos no usan DHCP...

con **show ip arp inspection** vemos un resumen de la configuración actual y estadísticas.

# Port Security

La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto. **switchport port-security** Habilita la seguridad **switchport port-security maximum 10**. Hablita 10 direcciones MAC

Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC, cualquier intento adicional de conexión de las direcciones MAC desconocidas genera una violación de seguridad.

## Tipos de direcciones MAC seguras

Existen varias maneras de configurar la seguridad de puerto. El tipo de dirección segura se basa en la configuración e incluye lo siguiente:

Direcciones MAC seguras **estáticas**: son direcciones MAC que se configuran manualmente en un puerto mediante el comando **switchport port-security mac-address dirección-mac** del modo de configuración de interfaz. Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch. La podemos guardar.

Direcciones MAC seguras **dinámicas**: son direcciones MAC detectadas dinámicamente y se almacenan solamente en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia. Solo hay que haber habilitado el port-security.

Direcciones MAC seguras **persistentes**: son direcciones MAC que pueden detectarse de forma dinámica o configurarse de forma manual, y que después se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución. Hay que insertarlas son la clave sticky

## Direcciones MAC seguras persistentes

Para configurar una interfaz a fin de convertir las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes y agregarlas a la configuración en ejecución, debe habilitar el aprendizaje por persistencia. El aprendizaje por persistencia se habilita en una interfaz mediante el comando **switchport port-security mac-address sticky** del modo de configuración de interfaz.

Cuando se introduce este comando, el switch convierte todas las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes, incluso las que se detectaron dinámicamente antes de que se habilitara el aprendizaje por persistencia. Todas las direcciones MAC seguras persistentes se agregan a la tabla de direcciones y a la configuración en ejecución. Nunca caducan aunque se habilite el Aging.

Las direcciones MAC seguras persistentes también se pueden definir manualmente. Cuando se configuran direcciones MAC seguras persistentes mediante el comando **switchport port-security mac-address sticky dirección-mac** del modo de configuración de interfaz, todas las direcciones especificadas se agregan a la tabla de direcciones y a la configuración en ejecución.

Si se guardan las direcciones MAC seguras persistentes en el archivo de configuración de inicio, cuando el switch se reinicia o la interfaz se desactiva, la interfaz no necesita volver a aprender las direcciones. Si no se guardan las direcciones seguras persistentes, estas se pierden.

Si se inhabilita el aprendizaje por persistencia mediante el comando **no switchport port-security mac-address sticky** del modo de configuración de interfaz, las direcciones MAC seguras persistentes siguen formando parte de la tabla de direcciones, pero se eliminan de la configuración en ejecución.

Observe que la característica de seguridad de puertos no funciona hasta que se habilita la seguridad de puertos en la interfaz mediante el comando **switchport port-security**.

## Modos de violación de seguridad

Existe una violación de seguridad cuando se produce cualquiera de estas situaciones:

Se agregó la cantidad máxima de direcciones MAC seguras a la tabla de direcciones para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.

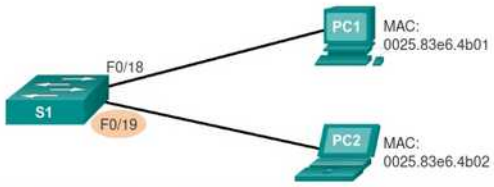
Una dirección aprendida o configurada en una interfaz segura puede verse en otra interfaz segura de la misma VLAN.

Se puede configurar una interfaz para uno de tres modos de violación, con la acción específica que se debe realizar si se produce una violación. La figura muestra los tipos de tráficos de datos que se envían cuando se configura en el puerto uno de los siguientes modos de violación de seguridad.

| | |
|---|---|
| Especifica la interfaz que se debe configurar para la seguridad de puertos. | `S1(config)# interface fastethernet 0/18` |
| Establece la interfaz en modo de acceso. | `S1(config-if)# switchport mode access` |
| Establezca la seguridad de puerto en la interfaz. | `S1(config-if)# switchport port-security` |

**Protect** (Proteger): cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. No hay ninguna notificación de que se produjo una violación de seguridad.

**Restrict** (Restringir): cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. En este modo, hay una notificación de que se produjo una violación de seguridad.




**Comandos de CLI de Cisco IOS**

| | |
|---|---|
| Especifica la interfaz que se debe configurar para la seguridad de puertos. | `S1(config)# interface fastethernet 0/19` |
| Establece la interfaz en modo de acceso. | `S1(config-if)# switchport mode access` |
| Establezca la seguridad de puerto en la interfaz. | `S1(config-if)# switchport port-security` |
| Establece la cantidad máxima de direcciones seguras permitidas en el puerto. | `S1(config-if)# switchport port-security maximum 50` |
| Habilita el aprendizaje por persistencia. | `S1(config-if)# switchport port-security mac-address sticky` |

**Shutdown** (Desactivar): en este modo de violación (predeterminado), una violación de seguridad de puerto produce que la interfaz se inhabilite de inmediato por errores y que se apague el LED del puerto. Aumenta el contador de violaciones. Cuando hay un puerto seguro en estado inhabilitado por errores, se lo puede sacar de dicho estado mediante la introducción de los comandos **shutdown** y **no shutdown** del modo de configuración de interfaz.

Para cambiar el modo de violación en un puerto de switch, use el comando del modo de configuración de interfaz **switchport port-security violation {protect | restrict | shutdown}.**

## Aging

Por defecto las MAC seguras no caducan, por eso tienen Aging Time 0. Podemos cambiar esto con **switchport port-security aging time** *minutos* El modo por defecto es absolute pero podemos elegir inactivity que cuenta el tiempo desde el último paquete recibido de esa MAC. Con **switchport port-security aging type {absolute | inactivity}** Las MAC estáticas no caducan, solo las dinámicas, a menos que lo configuremos con **switchport port-security aging static**

# Verificar la seguridad de puerto

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

## Verificar los parámetros de seguridad de puerto

Para mostrar la configuración de seguridad de puertos para el switch o la interfaz especificada, use el comando **show port-security [interface ID-de-interfaz].** El resultado de la configuración de la seguridad del puerto dinámico se muestra en la figura. De manera predeterminada, se permite una dirección MAC en este puerto.

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

El resultado que se muestra en la figura muestra los valores de la configuración de seguridad del puerto persistente. La cantidad máxima de direcciones se estableció en 50, como se configuró.

Nota: la dirección MAC se identifica como sticky MAC (MAC persistente).

Las direcciones MAC persistentes se agregan a la tabla de ejecución. Como se muestra en la figura 3, la dirección MAC persistente del PC2 se agregó a la configuración en ejecución para S1.

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 50
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

## Verificar las direcciones MAC seguras

Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz especificada con la información de vencimiento para cada una, use el comando **show port-security address**. Como se muestra en la figura las direcciones MAC seguras se indican junto con los tipos.

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan   Mac Address     Type           Ports   Remaining Age
                                                 (mins)
----   -----------     ----           -----   -------------
1      0025.83e6.4b01  SecureDynamic  Fa0/18      -
1      0025.83e6.4b02  SecureSticky   Fa0/19      -
-----------------------------------------------------------
```

Cuando se configura un puerto con seguridad de puertos, una violación puede provocar que el puerto se inhabilite por errores. Cuando un puerto se inhabilita por errores, se desactiva eficazmente, y no se envía ni se recibe tráfico en ese puerto.

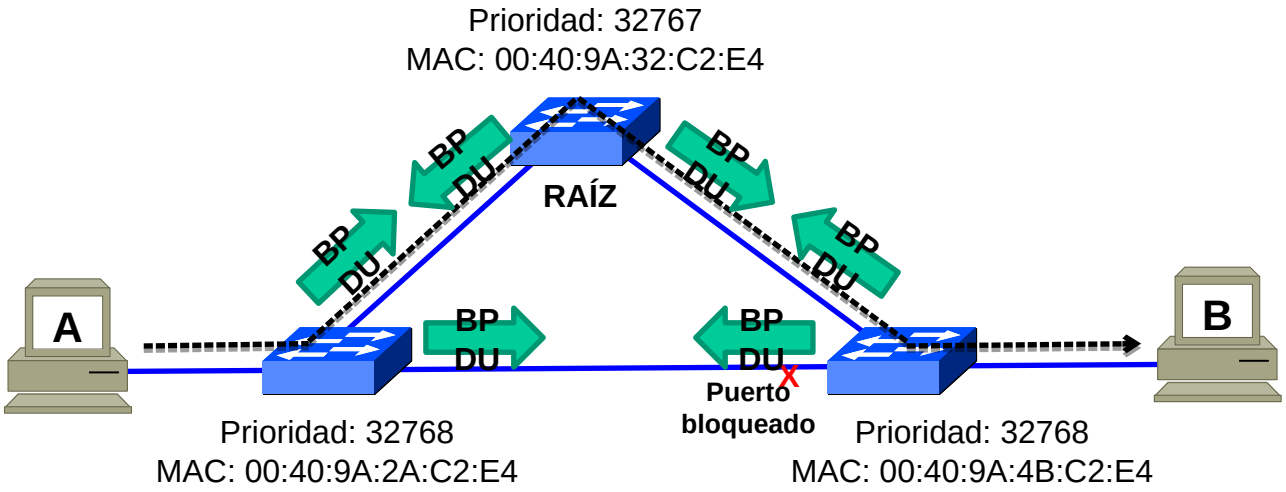
El estado del enlace y del protocolo del puerto cambia a down (inactivo). El LED del puerto cambia a color naranja. El comando show interfaces identifica el estado del puerto como err-disabled. El resultado del comando show port-security interface ahora muestra el estado del puerto como secure-shutdown. Debido a que el modo de violación de seguridad de puertos está establecido en shutdown, el puerto que experimenta la violación de seguridad pasa al estado de inhabilitación por errores.

Tambien podemos ver el running-config las estáticas y las sticky

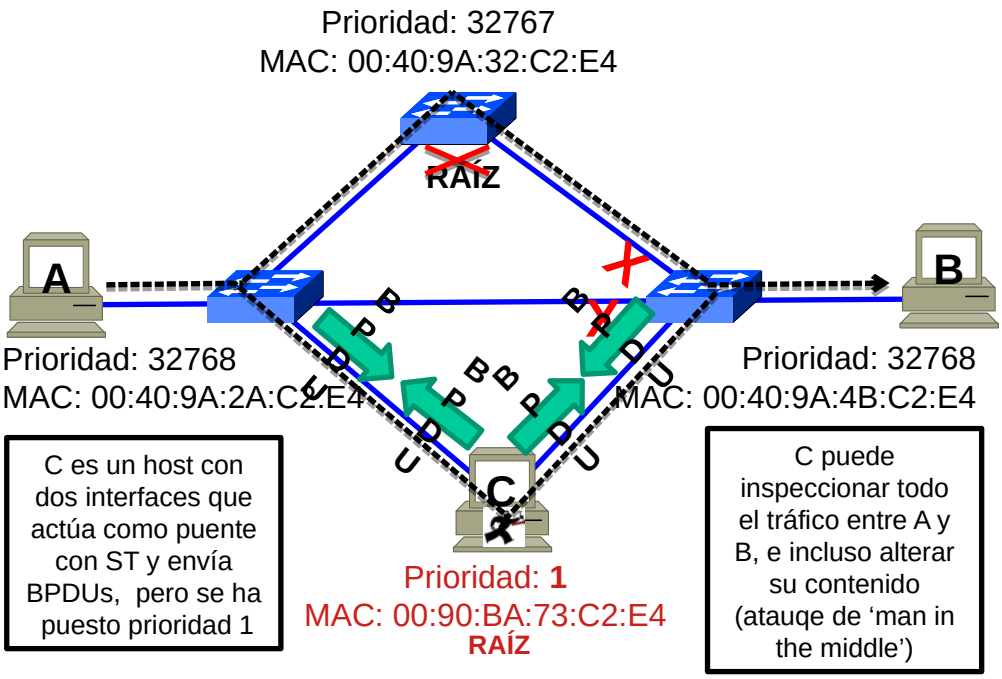
# Ataques a STP

El protocolo Spanning Tree (ST) no incorpora ningún mecanismo de protección frente a ataques. Los mensajes se envían de forma no segura, sin autentificar ni encriptar. Cualquier equipo (un host por ejemplo) puede enviar BPDUs.
ST se basa en elegir un puente raíz y fijar un único camino para llegar a él desde cualquier punto
Como ya hemos visto el puente de menor prioridad es siempre elegido como raíz.

### Situación inicial del ataque




### Ataque producido por un host (host C)



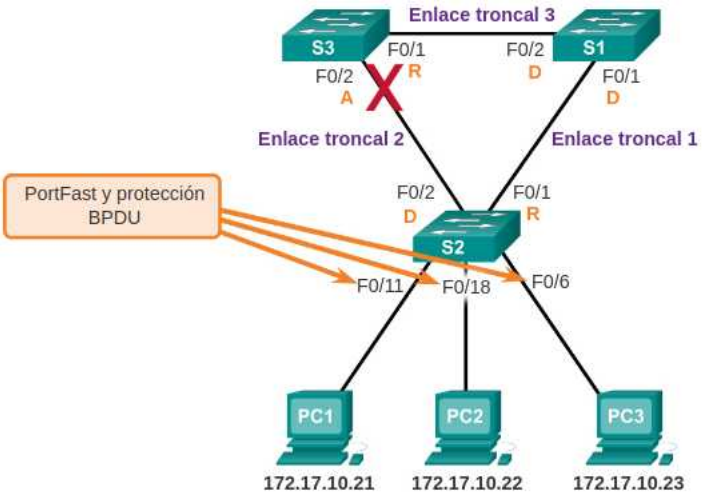

C es un host con dos interfaces que actúa como puente con ST y envía BPDUs, pero se ha puesto prioridad 1

C puede inspeccionar todo el tráfico entre A y B, e incluso alterar su contenido (atauqe de 'man in the middle')

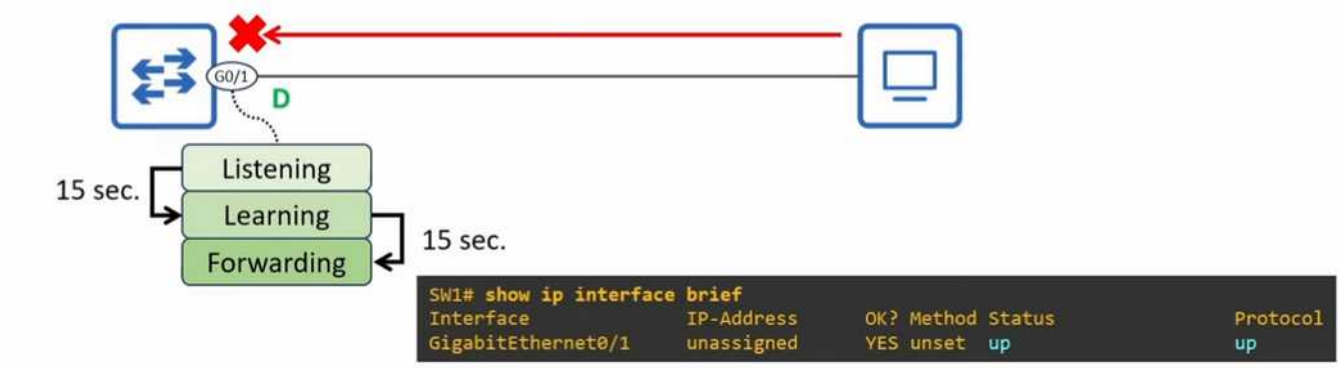
No hay ningún motivo razonable que justifique el envío de BPDUs por parte de un host
En los conmutadores podemos activar la función 'BPDU Guard' en los puertos donde se conectan hosts. Así si se recibe por ellos una BPDU el puerto se desactiva (estado shutdown)
Alternativamente se puede activar el 'Root Guard'. En este caso no se bloquean todas las BPDUs, solo las que pretendan cambiar el raíz
Lo normal sería activar estas protecciones en todos los puertos, excepto aquellos en que se vayan a conectar conmutadores

# PortFast y BPDU Guard

PortFast es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto pasa del estado de bloqueo al de reenvío de inmediato, omitiendo los estados de transición de STP 802.1D usuales (los estados de escucha y aprendizaje que tardan por defecto 15 segundos en pasar de uno a otro). Puede utilizar PortFast en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente, en lugar de esperar a que STP IEEE 802.1D converja en cada VLAN. Los puertos de acceso son puertos conectados a una única estación de trabajo o a un servidor.




Pero ojo, portfast no deshabilita STP en el puerto que sigue enviando BPDU's




La tecnología Cisco PortFast es útil para DHCP. Sin PortFast, un equipo puede enviar una solicitud de DHCP antes de que el puerto se encuentre en estado de enviar e impedirle al host la posibilidad de obtener una dirección IP utilizable y cualquier otra información. Debido a que PortFast cambia el estado a enviar de manera inmediata, el equipo siempre obtiene una dirección IP utilizable.

**Nota:** debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar a que converja el árbol de expansión, solo se debe utilizar en puertos de acceso conectados a hosts. Si habilitas PortFast en un puerto que se conecta a otro switch, corres el riesgo de crear un bucle de árbol de expansión. Sin embargo hay dos excepciones:

1. cuando el puerto está conectado mediante un enlace trunk a un equipo, normalmente un servidor de virtualización, que tiene máquinas virtuales cada una en una VLAN distinta.
2. Cuando el puerto está unido a un router formando un ROAS

En estos dos casos podemos forzar el portfast en el trunk con

switch(config-if)# **`spanning-tree portfast trunk`**

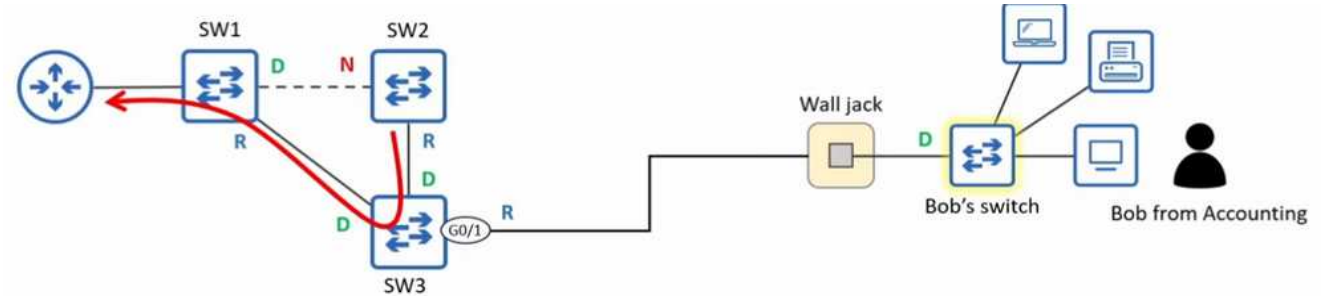
Para configurar PortFast es un puerto de switch, introducimos el comando

**`spanning-tree portfast`** del modo de configuración de interfaz en cada interfaz en la que se deba habilitar PortFast. Sólo se habilita si el puerto está en modo acceso.

El comando **`spanning-tree portfast default`** del modo de configuración global habilita PortFast en todas las interfaces no troncales.

## BPDU Guard

Protege la red de que se conecten switches no autorizados en puertos que estaban destinados a hosts. Puede ser configurado a parte de portfast pero normalmente se usan juntos pues ambos están pensados para puertos a los que se conectan hosts



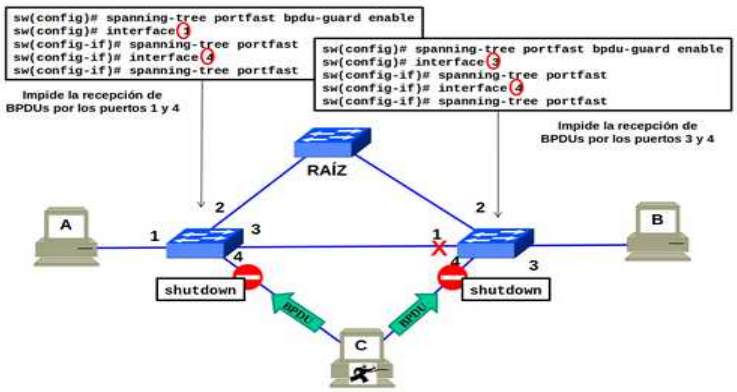

En una configuración de PortFast válida, nunca se deben recibir BPDU, ya que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switches Cisco admiten una característica denominada "protección BPDU". Cuando se habilita, la protección BPDU coloca al puerto en estado *deshabilitado por error* ***err-disabled*** al recibir una BPDU. Esto desactiva el puerto completamente y debes volver a activar la interfaz de forma manual.

Para configurar la protección BPDU en un puerto de acceso de capa 2, utilizamos el comando **`spanning-tree bpduguard enable`** del modo de configuración de interfaz.

El comando **`spanning-tree portfast bpduguard default`** del modo de configuración global habilita la protección BPDU en todos los puertos que ya tengan el PortFast habilitado.

Para verificar que se hayan habilitado PortFast y la protección BPDU para un puerto de switch, utilizamos el comando **`show running-config`**

La característica PortFast y la protección BPDU están deshabilitadas en todas las interfaces de manera predeterminada.




## BPDU Filter

Hemos visto que Portfast no deshabilita STP por lo que los puertos conectados a hosts siguen enviando BPDU's lo que lleva a estos problemas: Consumo de ancho de banda y tiempo de procesado en los hosts y publicación de información sobre la topología STP de nuestra LAN

BPDU Filter soluciona esto previniendo que un puerto envíe BPDU's pero no deshabilita el puerto, puede ser habilitado de dos formas, en cada interfaz o de manera global

SW(config-if)# spanning-tree bpdufilter enable

El puerto no enviará BPDU's e ignorará los que reciba, en efecto deshabilita STP en el puerto por lo que hay que usarlo con precaución. Por eso, es mejor no usarlo así pues si tenemos bpduGuard no le hará caso.

**SW(config)# spanning-tree portfast bpdufilter default**

Será activado en todos los puertos con portfast y usar spanning-tree bpdufilter disable en puertos específicos. El puerto no enviará BPDU's, pero si recibe uno, portfast y bpdufilter se deshabilitan y el puerto se convierte en un puerto STP normal. Si tenemos también activado BPDUGuard y recibe un BPDU el filter se deshabilita pero BPDUGuard actúa y deshabilita la interfaz

# Monitorización

## Port Mirroring

El puerto espejo es una técnica que permite copiar todo el tráfico de uno o más puertos de origen a un puerto de destino.

Esto puede resultar muy útil para analizar los flujos de red que transitan por ciertos puertos o en una VLAN, especialmente en una fase de resolución de problemas.

Para configurar Port Mirroring tenemos que usar el comando monitor poniendo un número de sesión (puedes hacer varias sesiones) la fuente (que pueden ser varios puertos) y el destino (sólo uno):

Switch(config)#**monitor session 1 source interface f0/1 both** -- admite rx, tx o both

Switch(config)#**monitor session 1 destination interface f0/2**

### Comprobar la monitorización

Switch#**show monitor session 1**

### Por Mirroring en una VLAN

Switch(config)#**monitor session 1 source vlan 10 both**

Switch(config)#**monitor session 1 destination interface f0/2**