Redes y comunicación de Datos 2

Sesión 13

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Dinámica: Lluvia de ideas sobre Control de acceso.
- Control de acceso
- Amenazas de seguridad de capa 2
- **Actividad:**
  - **Integración de conocimientos**

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la unidad, el estudiante explica cómo las vulnerabilidades ponen en riesgo la seguridad LAN, para mitigar algunos ataques informáticos, a través de ejemplos desarrollados en clase.

Buenas Prácticas

Buenas Prácticas

Con respecto a la Sesión 12

- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

Análisis de puertos

- **¿Qué información puede obtener un atacante?**

El análisis de puertos se utiliza para comprobar qué puertos de la red están abiertos y pueden recibir o enviar datos. También se utiliza para enviar paquetes a puertos concretos de un anfitrión y analizar respuestas para identificar vulnerabilidades.

Explotación de vulnerabilidades

¿Qué es un exploit?

- Es un fragmento/parte de código especialmente preparado para explotar una vulnerabilidad para la cual:
  - Puede existir un parche que soluciona la vulnerabilidad.
  - No existe un parche para solucionar la vulnerabilidad, en cuyo caso se denomina 0-day.

- Normalmente, son pequeños programas en los que el atacante únicamente tiene que especificar:
  - IP destino.
  - Puerto destino.
  - Otros parámetros propios de la vulnerabilidad.
  - El payload.

Buenas Prácticas

Sesión 13

Lluvia de ideas sobre el control de acceso

- ¿Qué es el control de acceso?
- ¿Qué son los componentes AAA en redes?

Control de acceso

Control de acceso

Autenticación con una contraseña local

Muchas formas de autenticación pueden ser llevadas a cabo en dispositivos de red, y cada método ofrece diferentes niveles de seguridad.

El simple método de autenticación por acceso remoto es para configurar un inicio de sesión y contraseña combinación en consola, lineas vty, y puertos auxiliares, como se muestra en las lineas vty en el siguiente ejemplo.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH es un tipo de acceso remoto más seguro:

- Requiere un nombre de usuario y una contraseña.
- El nombre de usuario y la contraseña se pueden autenticar localmente.

El método de base de datos local tiene algunas limitaciones:

- Las cuentas de usuario deben configurarse localmente en cada dispositivo que no sea escalable.
- El método no proporciona ningún método de autenticación alternativa.

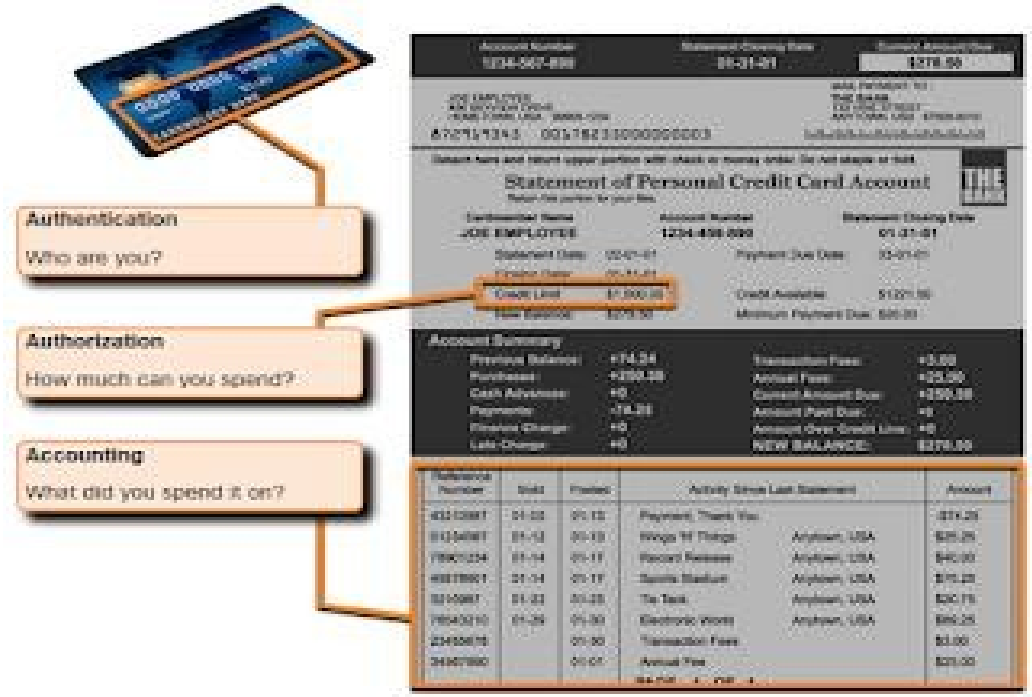
```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Control de acceso

Componentes AAA

AAA significa **Autenticación, Autorización y Contabilidad,** y proporciona el marco principal para configurar el control de acceso en un dispositivo de red.

AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).



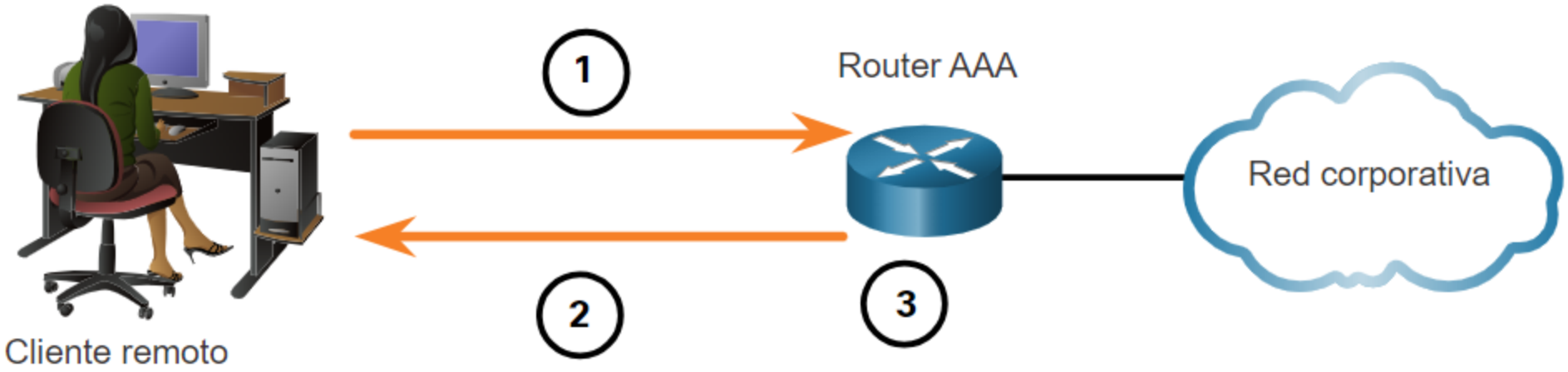
Control de acceso

Autenticación

Existen dos métodos de implementación de **autenticación AAA** son Local y basada en el servidor (server-based).

Autenticación AAA local:

- El método almacena nombres de usuario y contraseñas localmente en un dispositivo de red (por ejemplo, router Cisco).
- Los usuarios se autentican contra la base de datos local.
- **AAA local** es ideal para las redes pequeñas.

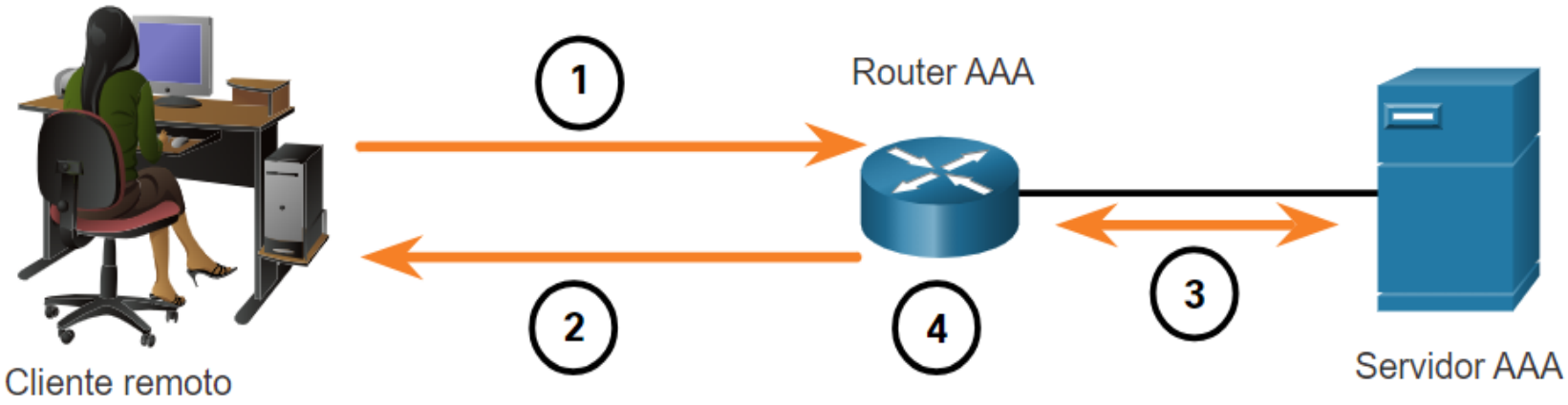


1. El cliente establece una conexión con el router.
2. El router AAA solicita al usuario un nombre de usuario y una contraseña.
3. El router autentica el nombre de usuario y la contraseña mediante la base de datos local y el usuario obtiene acceso a la red en función de la información de esta base de datos.

Autenticación

Autenticación AAA basada en el servidor:

- Con el método basado en el servidor, el enrutador accede a un servidor central AAA.
- El servidor AAA contiene los nombres de usuario y contraseñas de todos los usuarios.
- El router AAA usa el protocolo de sistema de control de acceso del controlador de acceso a terminales (TACACS+) o el protocolo de servicio de autenticación remota para usuarios de entrada telefónica (RADIUS) para comunicarse con el servidor de AAA.
- Cuando hay múltiples enrutadores y switches basado en el servidor es más apropiado.

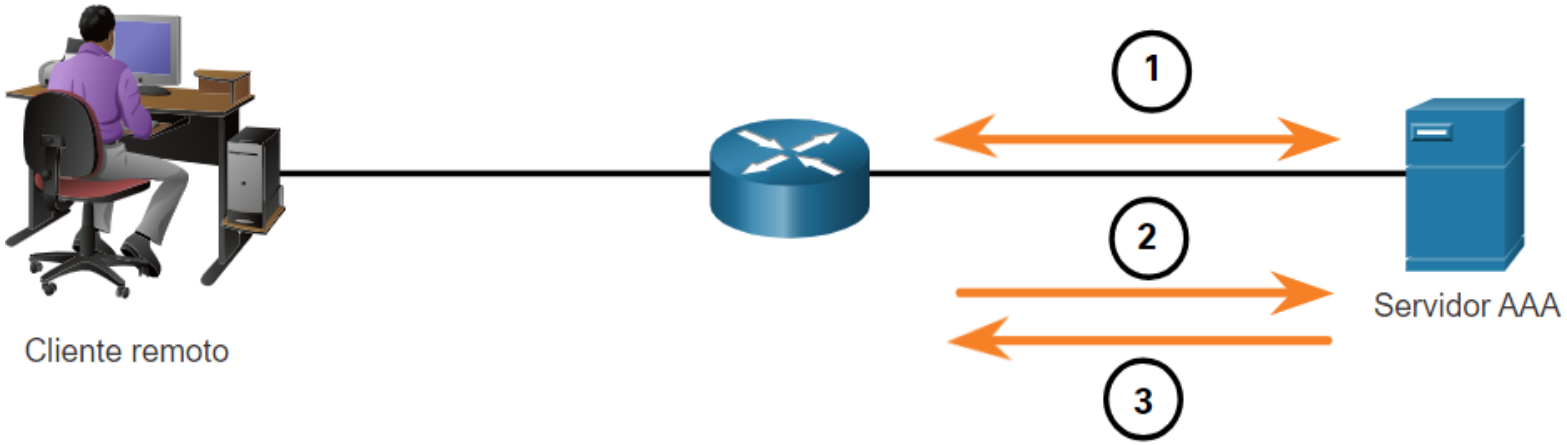


1. El cliente establece una conexión con el router.
2. El router AAA solicita al usuario un nombre de usuario y una contraseña.
3. El router autentica el nombre de usuario y la contraseña mediante un servidor de AAA remoto.
4. El usuario obtiene acceso a la red en función de la información en el servidor AAA remoto.

Control de acceso

Autorización

- La autorización es automática y no requiere que los usuarios tomen medidas adicionales después de la autenticación.
- La autorización controla lo que el usuario puede hacer o no en la red después de una autenticación satisfactoria:
- La autorización utiliza un conjunto de atributos que describe el acceso del usuario a la red. El servidor AAA utiliza estos atributos para determinar los privilegios y restricciones para ese usuario.



1. Cuando un usuario ha sido autenticado, una sesión es establecida entre el router y el servidor AAA.
2. El router pide autorización al servidor AAA para la solicitud de servicio del cliente.
3. El servidor AAA responde con un PASS/FAIL a la solicitud.

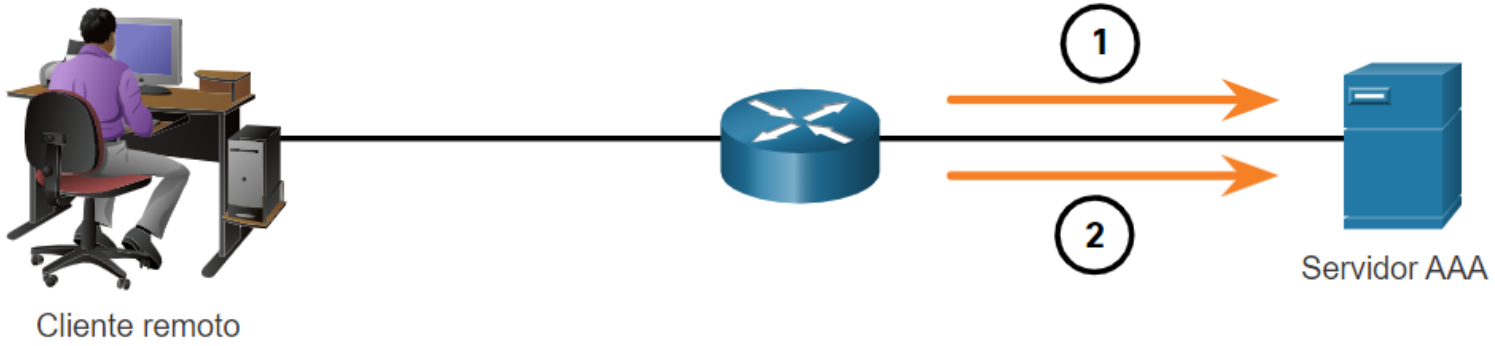
Control de acceso

Contabilidad (Auditoria)

La auditoría de AAA recopila datos de uso en los registros de AAA y los informa. La organización puede utilizar estos datos para fines como auditorías o facturación. Los datos recopilados pueden incluir la hora de inicio y finalización de la conexión, los comandos ejecutados, la cantidad de paquetes y el número de bytes.

Un uso muy implementado de la contabilidad es combinarlo con la autenticación AAA.

- Los servidores AAA mantienen un registro detallado de lo que el usuario autenticado hace exactamente en el dispositivo, como se muestra en la imagen Esto incluye todos los comandos EXEC y de configuración que emite el usuario.
- El registro contiene varios campos de datos, incluidos el nombre de usuario, la fecha y hora, y el comando real que introdujo el usuario. Esta información resulta útil para solucionar problemas de dispositivos También proporciona evidencia de cuándo las personas realizan actos maliciosos.



1. Cuando se autentica a un usuario, el proceso de registro AAA genera un mensaje para comenzar el proceso de contabilidad.
2. Cuando el usuario termina, se registra un mensaje de finalización y se da por terminado el proceso de contabilidad.

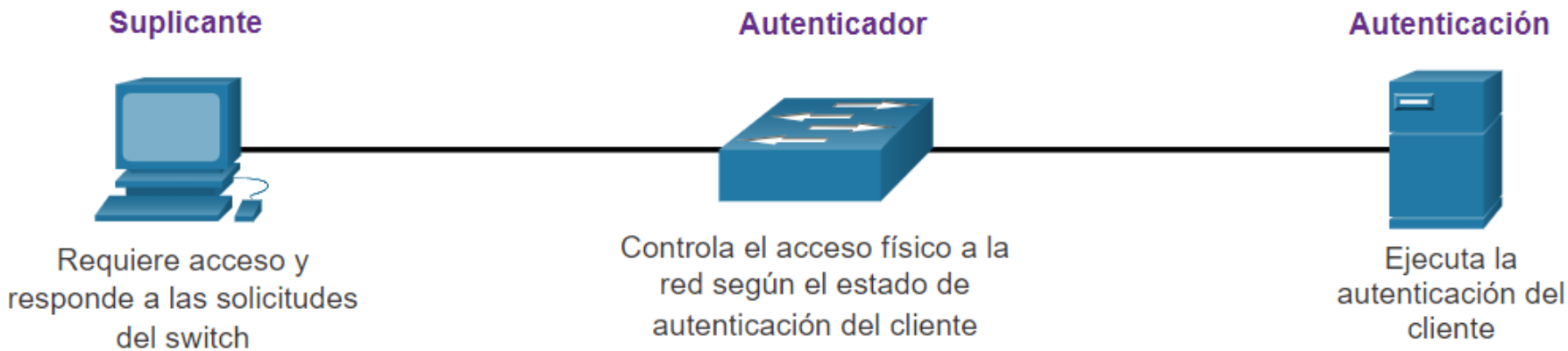
Control de acceso

802.1X

El **estándar IEEE 802.1X** define un control de acceso y un protocolo de autenticación basados en puertos. Evita que las estaciones de trabajo no autorizadas se conecten a una LAN a través de puertos de switch de acceso público. El servidor de autenticación autentica cada estación de trabajo que está conectada a un puerto del switch antes habilitar cualquier servicio ofrecido por el switch o la LAN.

Con la autenticación basada en el puerto 802.1X, los dispositivos en la red tienen roles específicos:

- ✓ **Cliente (Suplicante)**
- ✓ **Switch (Autenticador)**
- ✓ **Servidor de autenticación**



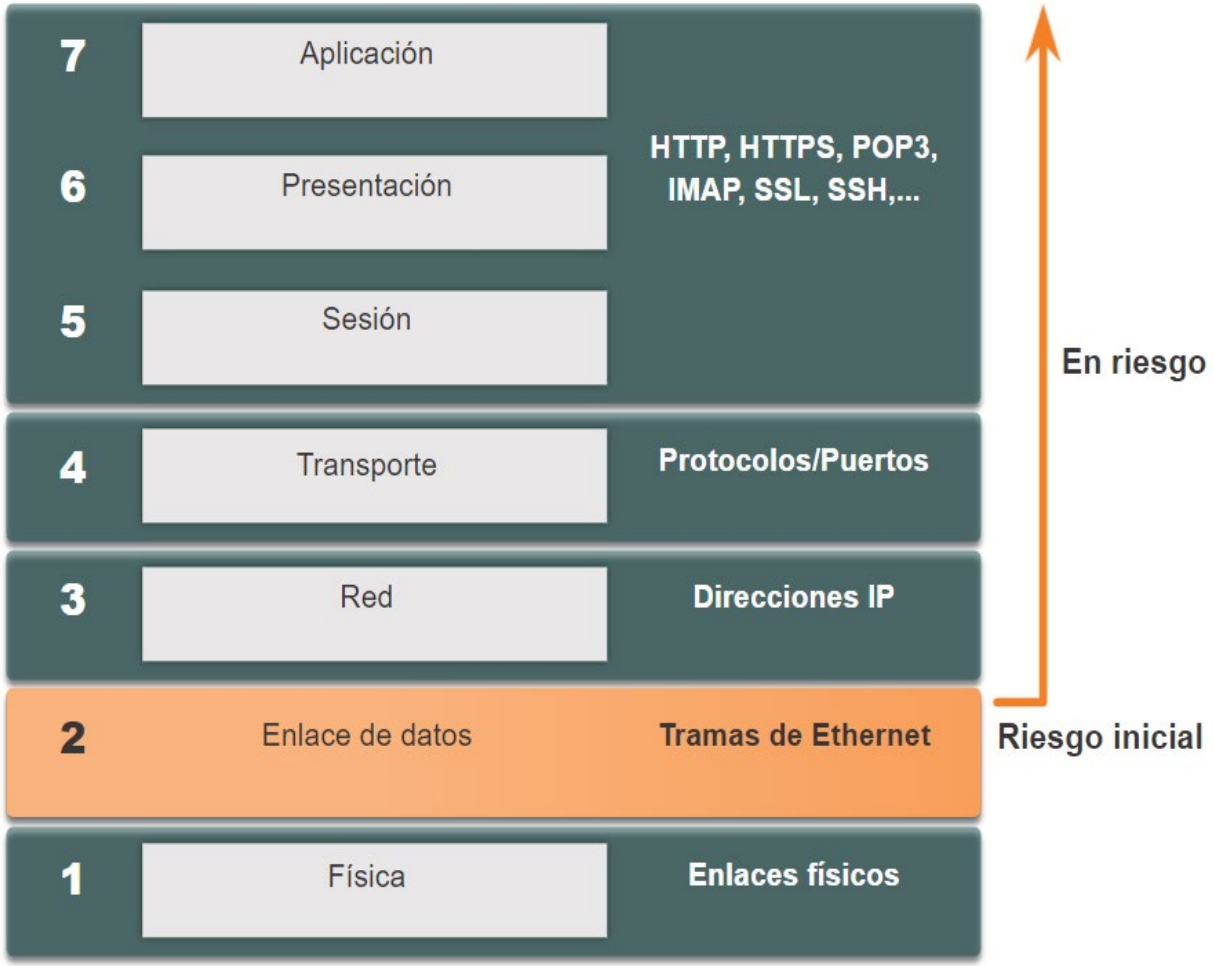
Amenazas de seguridad de capa 2

Amenazas de seguridad de capa 2

Vulnerabilidades de capa 2

Recuerde que el modelo de referencia OSI está dividido en siete capaz, las cuales trabajan de manera independiente una de otra. La figura muestra la función de cada capa los elementos de núcleo que pueden ser explotados.

Los administradores de red implementan habitualmente soluciones de seguridad para proteger los elementos en la capa 3 hasta la capa 7. Ellos usan VPNs, cortafuegos, y dispositivos IPS para proteger estos elementos Si la capa 2 se ve comprometida, todas las capas superiores también se ven afectadas.



Amenazas de seguridad de capa 2

categorías de ataque en el Switch

El primer paso para mitigar los ataques a la infraestructura de Capa 2 es comprender el funcionamiento de la Capa 2 y las amenazas de la infraestructura de Capa 2.

Categoría	Ejemplos
Ataques de tabla MAC	Incluye ataques de inundación de direcciones MAC.
Ataques de VLAN	Incluye ataques VLAN hopping y VLAN double-tagging. También incluye ataques entre dispositivos en una VLAN común.
Ataques de DHCP	Incluye ataques DHCP starvation y DHCP spoofing.
Ataques ARP	Incluye la suplantación de ARP y los ataques de envenenamiento de ARP.
Ataques de suplantación de direcciones	Incluye los ataques de suplantación de direcciones MAC e IP.
Ataques STP	Incluye ataques de manipulación al Protocolo de árbol de extensión

Técnicas de mitigación de ataques en el switch

La tabla provee una visión general de soluciones Cisco para mitigar ataques en Capa 2.

Solución	Descripción
Seguridad de puertos	Previene muchos tipos de ataques, incluidos los ataques de inundación de direcciones MAC y los ataques de hambre DHCP.
Detección DHCP	Previene ataques de suplantación de identidad y de agotamiento de DHCP.
Inspección ARP dinámica (DAI)	Previene la suplantación de ARP y los ataques de envenenamiento de ARP.
Protección de IP de origen (IPSG)	Impide los ataques de suplantación de direcciones MAC e IP.

Ataques a la tabla de direcciones MAC

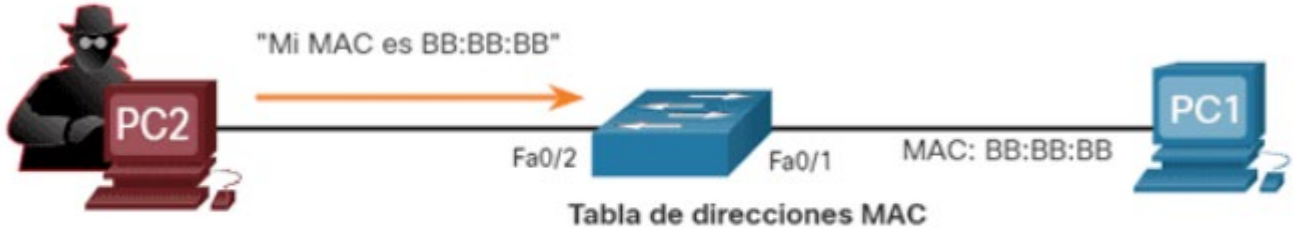


Tabla de direcciones MAC

Puerto	Dirección MAC
Fa0/1	
Fa0/2	BB:BB:BB

Ataque a la tabla de direcciones MAC

Revisión de la operación del switch

Recuerde que para tomar decisiones de reenvío, un Switch LAN de capa 2 crea una tabla basada en las direcciones MAC de origen en las tramas recibidas.

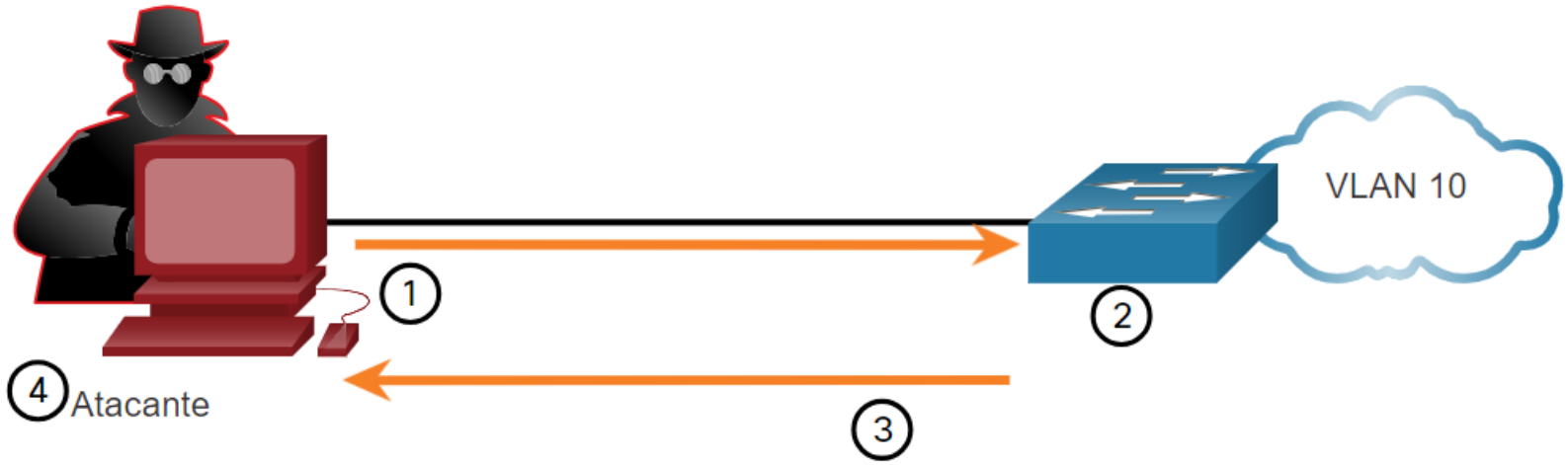
Esto se llama una tabla de direcciones MAC. Las tablas de direcciones MAC se almacenan en la memoria y se usan para cambiar switch frames más eficientemente.

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

Ataque a la tabla de direcciones MAC

Inundación de la tabla de direcciones MAC

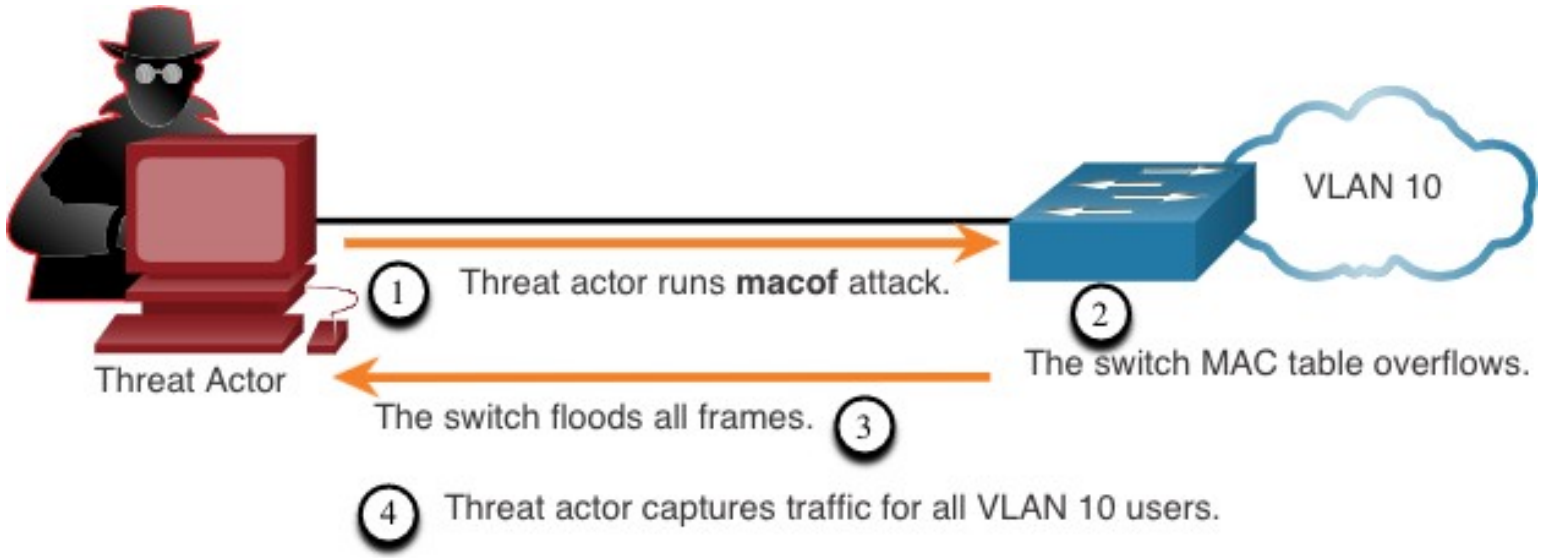
Todas las tablas MAC tiene un tamaño fijo por lo que un switch quedarse sin espacio para guardar direcciones MAC. Los ataques de inundación de direcciones MAC aprovechan esta limitación al bombardear el switch con direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch esté llena.



1. El atacante esta conectado a VLAN 10 y usa **macof** para rápidamente generar de manera aleatoria muchas direcciones MAC y IP de origen y destino.
2. En un corto periodo de tiempo la tabla MAC del switch se llena.
3. Cuando la tabla MAC esta llena, el switch empieza a reenviar todas las tramas que recibe. Mientras que **macof** continúe ejecutándose, la tabla MAC se mantiene llena y el switch continua reenviando todas las tramas que ingresan hacia cada puerto asociado a la VLAN 10.
4. Luego, el atacante usa el software de analizador de paquetes para capturar frames desde cualquier dispositivo conectado en la VLAN 10.

Inundación de la tabla de direcciones MAC

La figura muestra un actor de amenazas usando fácilmente la herramienta de ataque de red **macof** para desbordar una tabla de direcciones MAC.



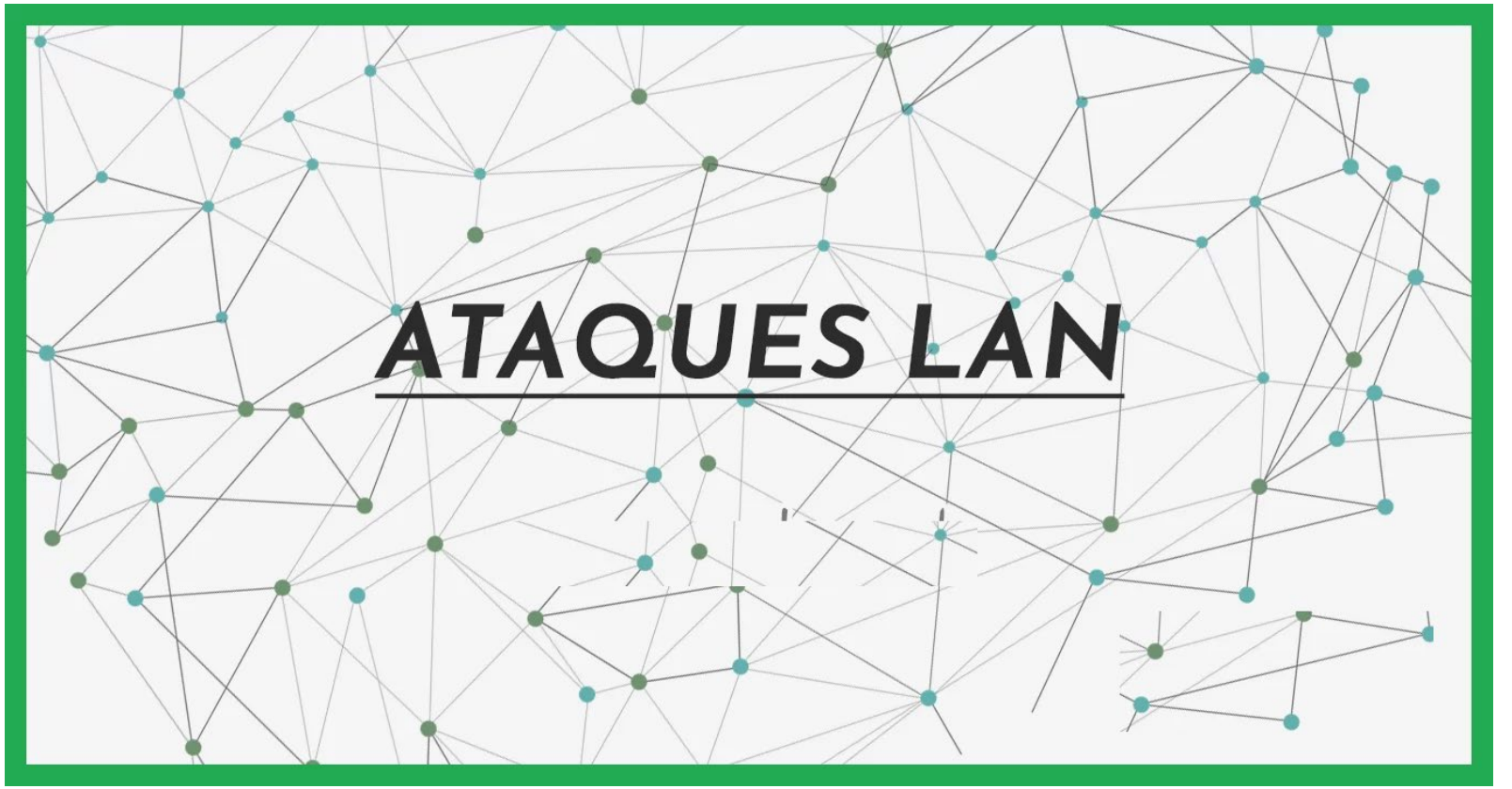
Si el actor de la amenaza detiene la ejecución de **macof** o se descubre y se detiene, el switch finalmente elimina las entradas de direcciones MAC anteriores de la tabla y comienza a actuar normalmente.

Mitigación de ataques de tabla de direcciones MAC

Lo que hace que herramientas como **macof** sean peligrosas, es que un atacante puede crear un ataque de desbordamiento de tabla MAC muy rápidamente.

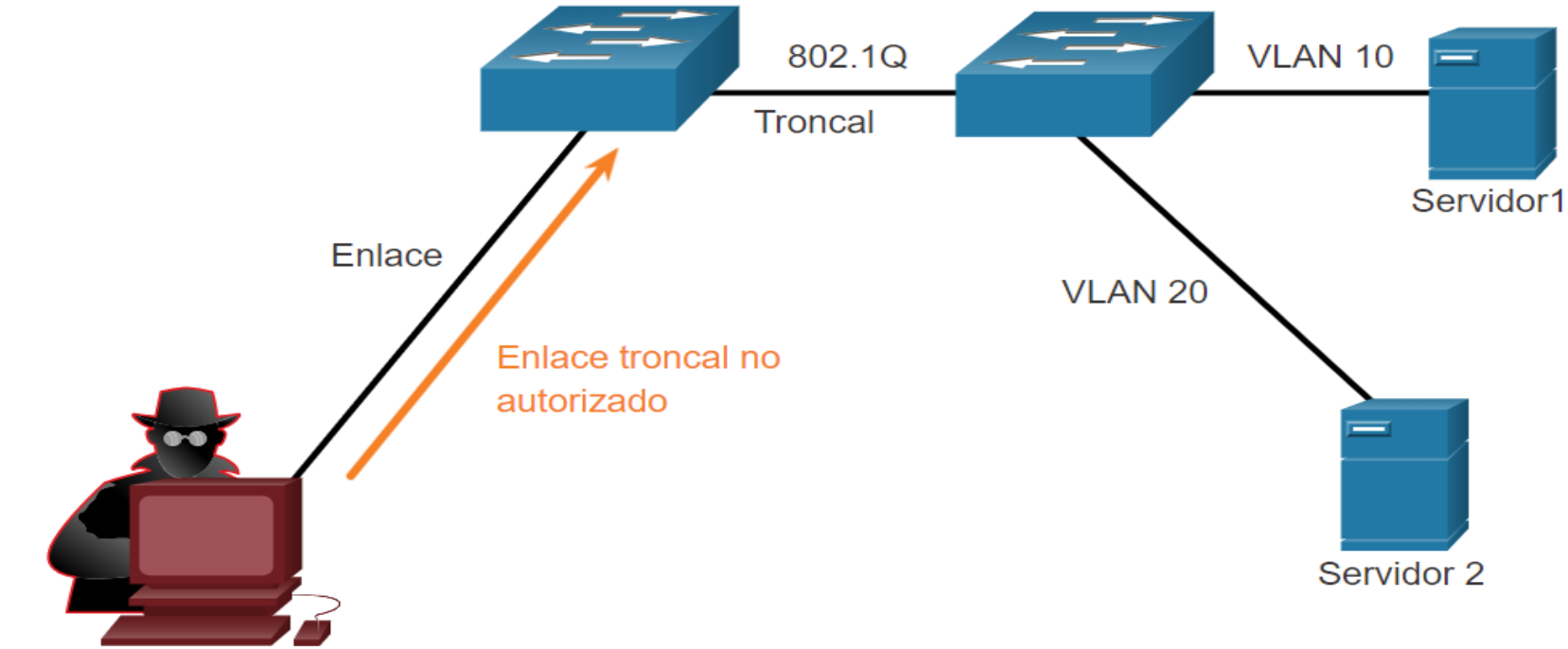
Una herramienta como **macof** puede saturar un switch con hasta 8,000 tramas falsas por segundo; creando un ataque de saturación de la tabla de direcciones MAC en cuestión de segundos

```
# macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```



Ataques de salto de VLAN

El salto de VLAN permite que otra VLAN pueda ver el tráfico de una VLAN sin cruzar primero un router. En un ataque de salto de VLAN básico, el atacante configura un host para que actúe como un switch, para aprovechar la función de puerto de enlace automático habilitada de forma predeterminada en la mayoría de los puertos del switch.

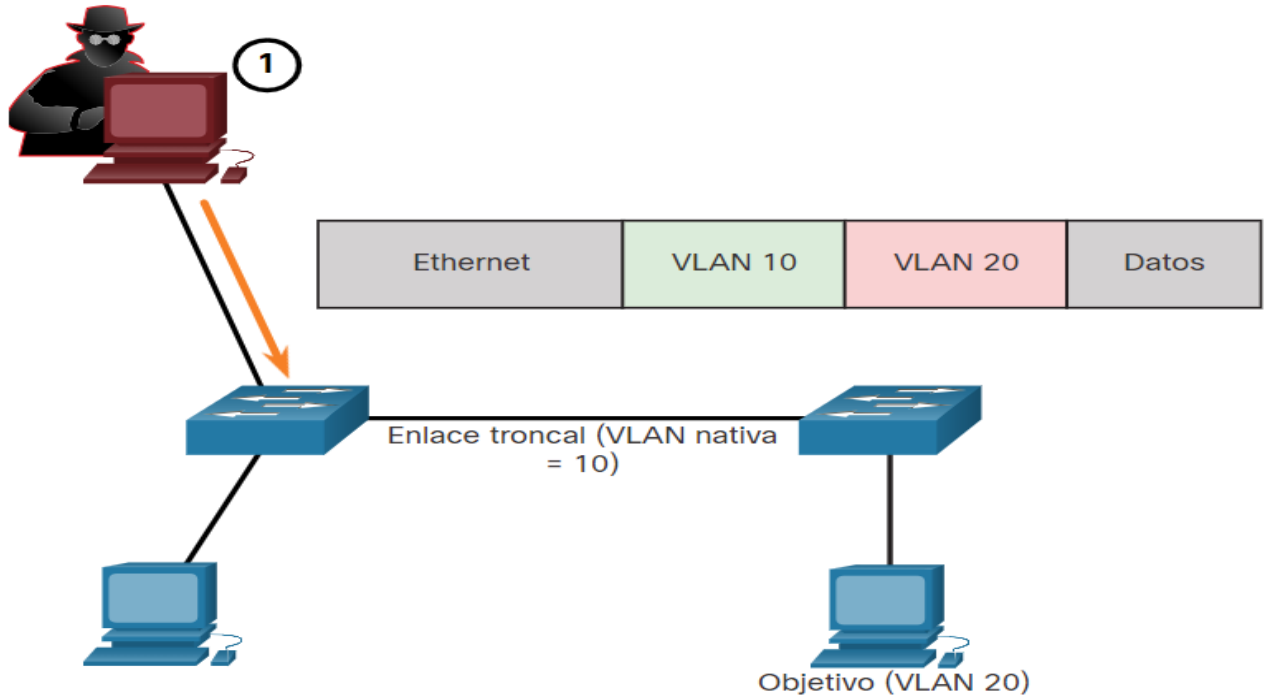


El atacante obtiene acceso a la VLAN del servidor.

Ataques de doble etiquetado de VLAN

Un atacantes de situaciones específicas que podrían incrustar una etiqueta 802.1Q oculta dentro del marco que ya tiene una etiqueta 802.1Q. Esta etiqueta permite que la trama se envíe a una VLAN que la etiqueta 802.1Q externa no especificó.

- **Paso 1:** El atacante envía una trama 802.1Q de doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal.



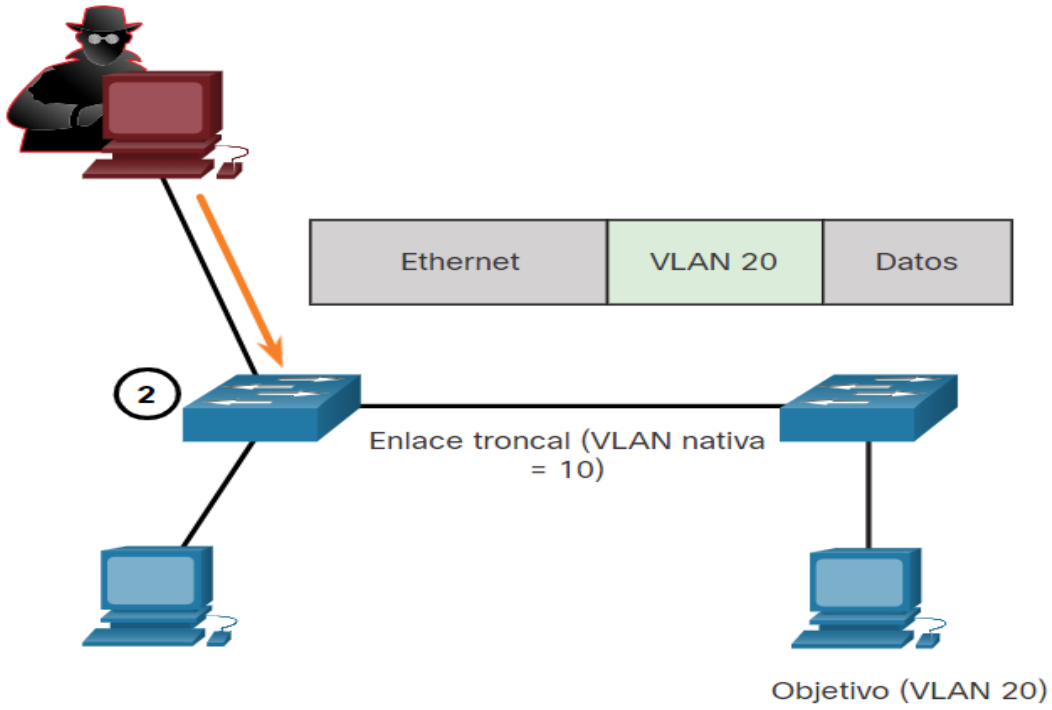
Ataques de doble etiquetado de VLAN

- **Paso 2**: El frame llega al primer switch, que mira la primera etiqueta 802.1Q de 4 bytes. El switch ve que el frame está destinado a la VLAN 10, la cual es una VLAN nativa.

El switch reenvía el paquete a todos los puertos VLAN 10 después de quitar la etiqueta VLAN 10.

La trama no es re-etiquetada porque es parte de la VLAN nativa.

En este punto, la etiqueta VLAN 20 todavía está intacta y no ha sido inspeccionada por el primer switch.

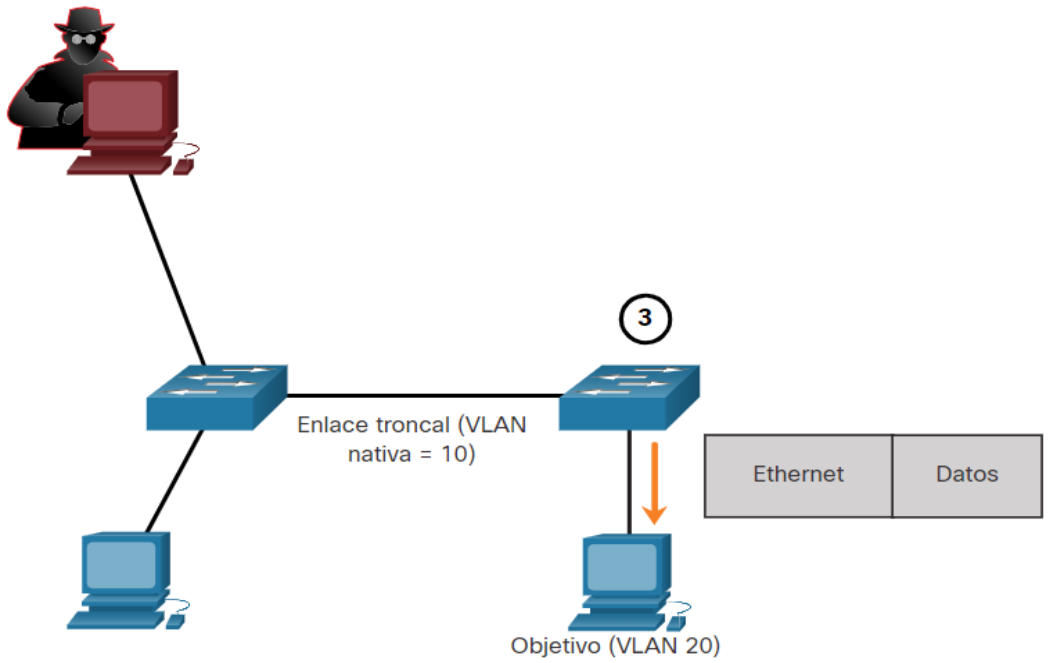


Ataques de doble etiquetado de VLAN

- **Paso 3**: La trama llega al segundo switch que no tiene conocimiento de que debía ser para la VLAN 10 (nativa). El switch emisor no etiqueta el tráfico de la VLAN nativa como se especifica en la especificación 802.1Q.

El segundo switch solo mira la etiqueta interna 802.1Q que insertó el atacante y ve que el frame está destinado a la VLAN 20 de destino.

El segundo switch envía el paquete al puerto víctima o lo satura, dependiendo de si existe una entrada en la tabla de MAC para el host víctima.



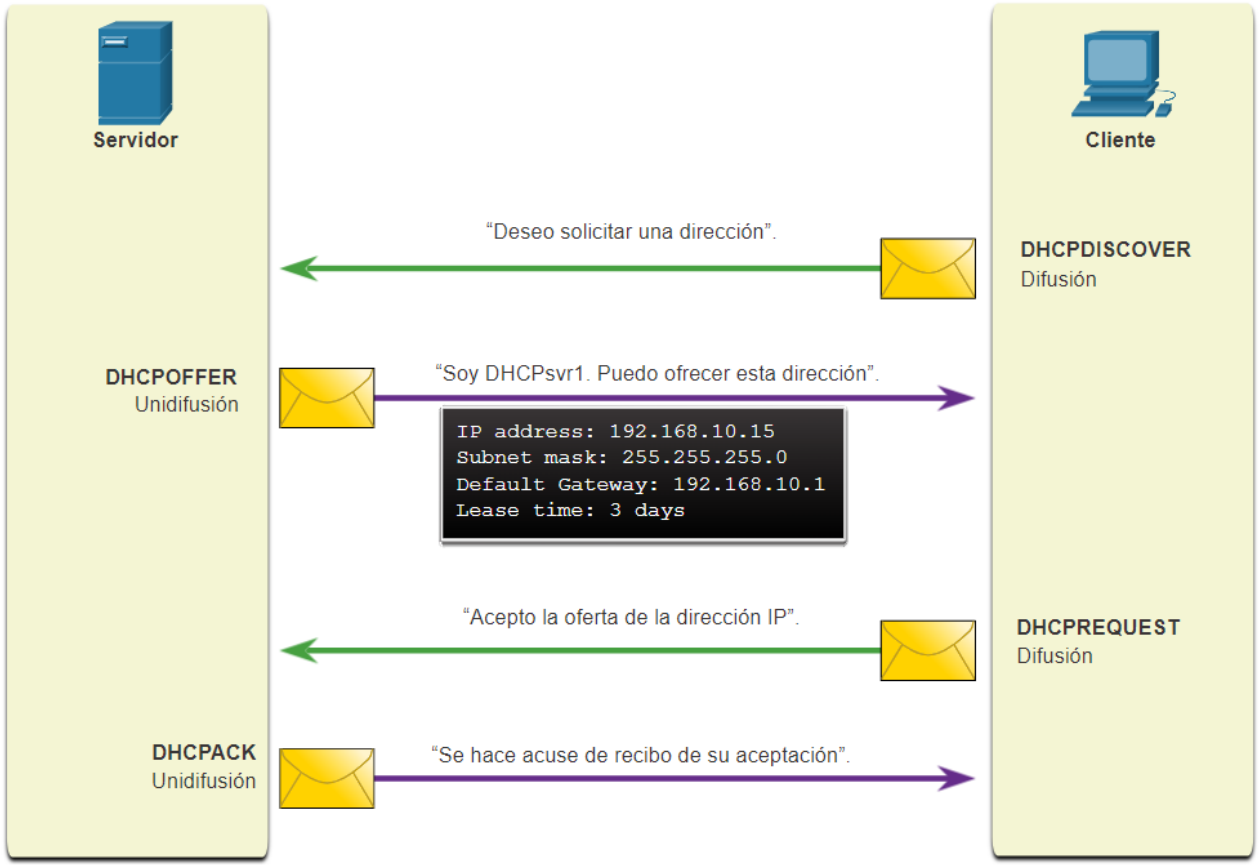
Mitigación de Ataque de VLAN

Se pueden evitar los saltos de VLAN y los ataques de doble etiquetado de VLAN mediante la implementación de las siguientes pautas de seguridad troncal, como se discutió en un módulo anterior:

- Deshabilitar troncal en todos los puertos de acceso.
- Deshabilitar troncal automático en enlaces troncales para poder habilitarlos de manera manual.
- Asegúrese de que la VLAN nativa solo se usa para los enlaces troncales.

Mensajes DHCP

Los servidores DHCP proporcionan dinámicamente la información de configuración de IP a los clientes, como la dirección IP, la máscara de subred, el gateway predeterminado, los servidores DNS y más. En la figura se muestra una revisión de la secuencia del intercambio de mensajes DHCP entre el cliente y el servidor.



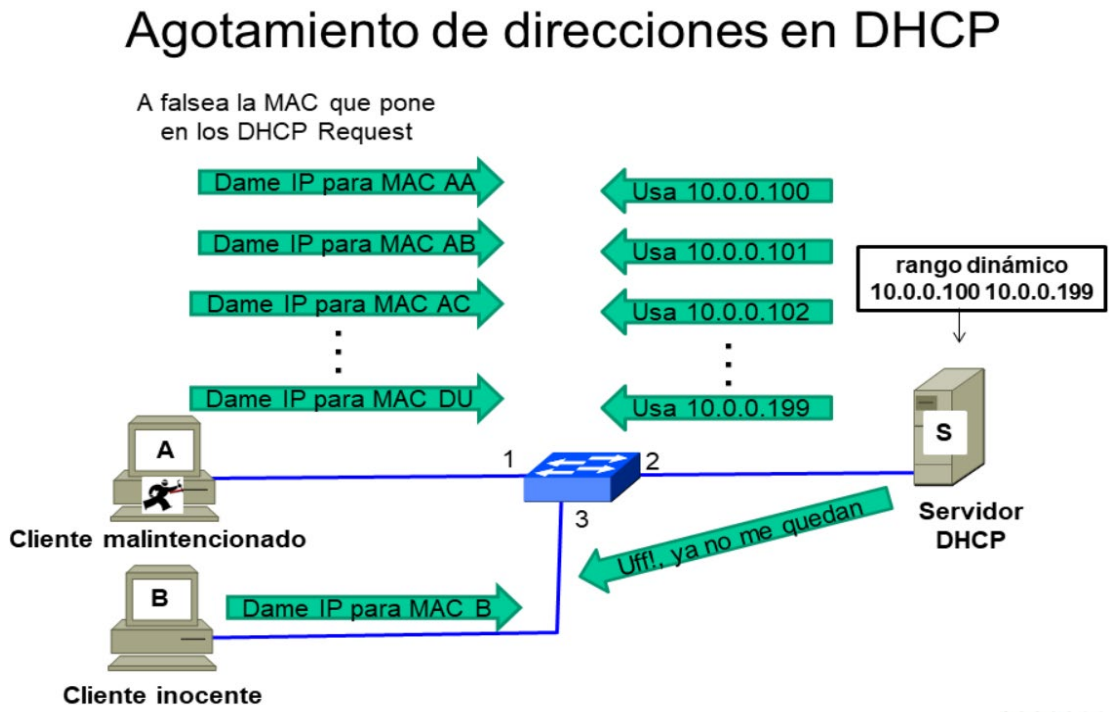
Mensajes DHCP

Los dos tipos de ataques DHCP son agotamiento y suplantación de identidad. Ambos ataques pueden ser mitigados implementando DHCP snooping.

Ataque por agotamiento DHCP - el objetivo de este ataque es crear un DoS para conectar clientes. Los ataques de agotamiento de DHCP requieren una herramienta de ataque, como Gobbler.

Gobbler tiene la capacidad de ver todo el alcance de las direcciones IP alquilables e intenta alquilarlas todas.

Específicamente, este crea un mensaje DHCP de descubrimiento con una dirección MAC falsa.



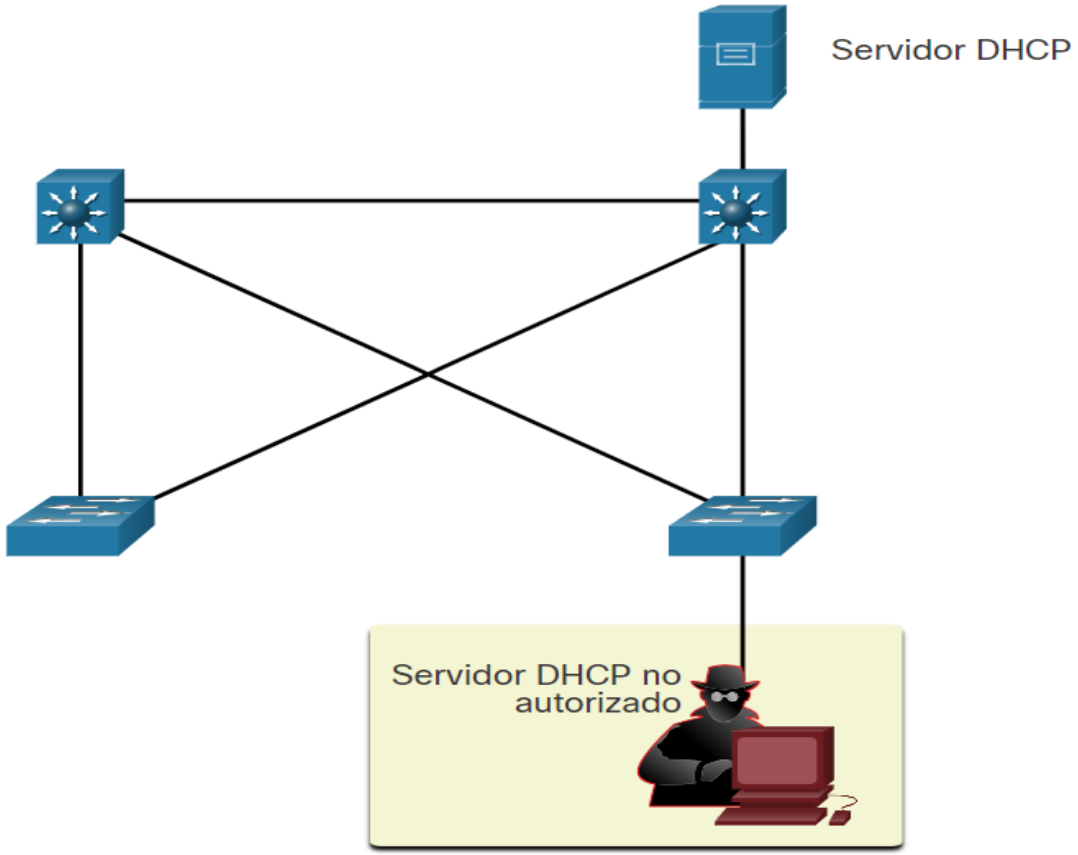
Mensajes DHCP

- **Ataque de suplantación DHCP -** Este ocurre cuando un servidor DHCP falso se conecta a la red y proporciona parámetros de configuración de IP falsos a clientes legítimos. Un servidor no autorizado puede proporcionar una variedad de información engañosa, que incluye lo siguiente:

  - **Puerta de enlace predeterminada incorrecta**.
  - **Servidor DNS incorrecto**
  - **Dirección IP incorrecta**

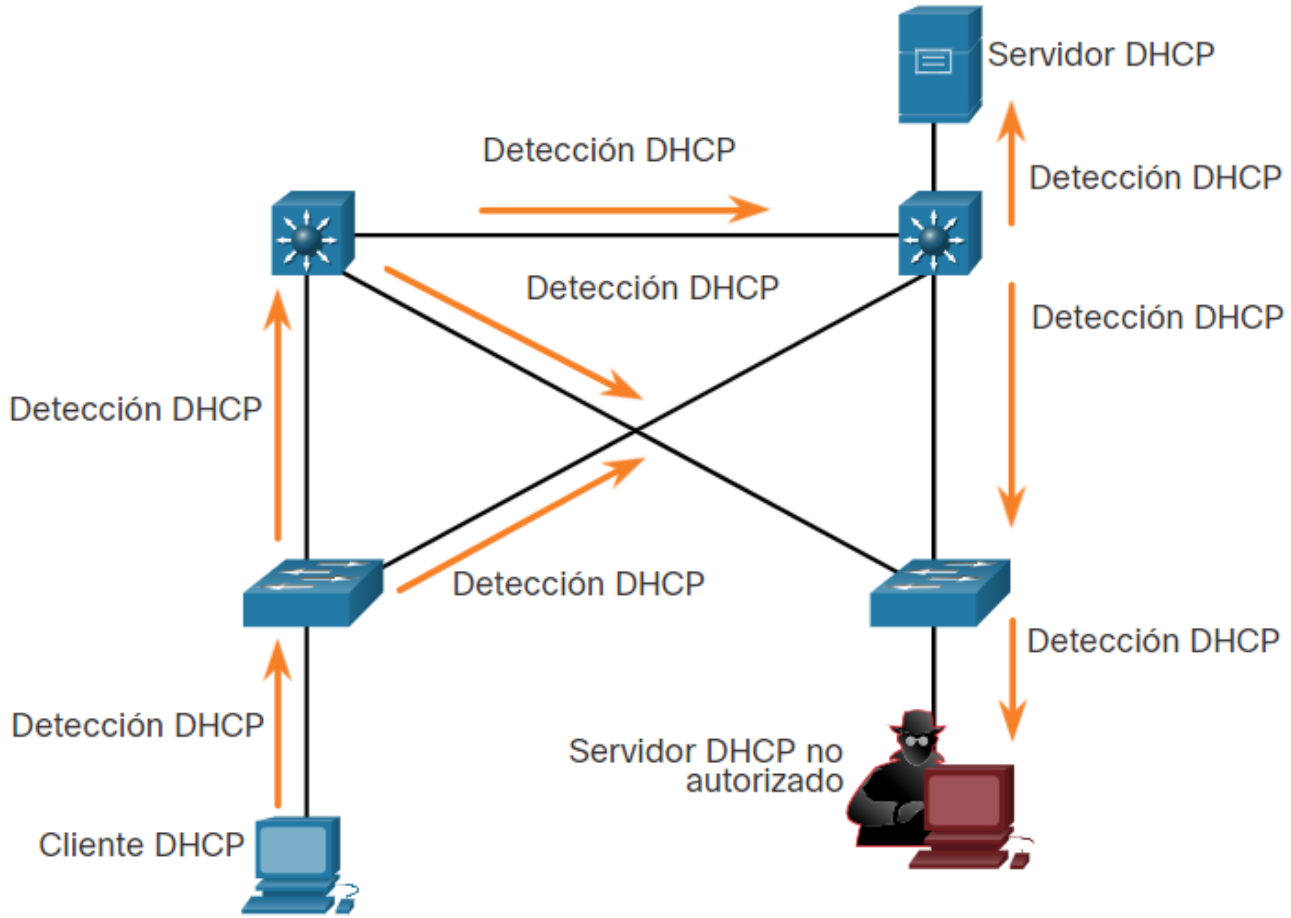
Mensajes DHCP

- **Ataque de DHCP Spoofing (Suplantación)**
  - **El actor de amenazas habilita el servidor DHCP falso**



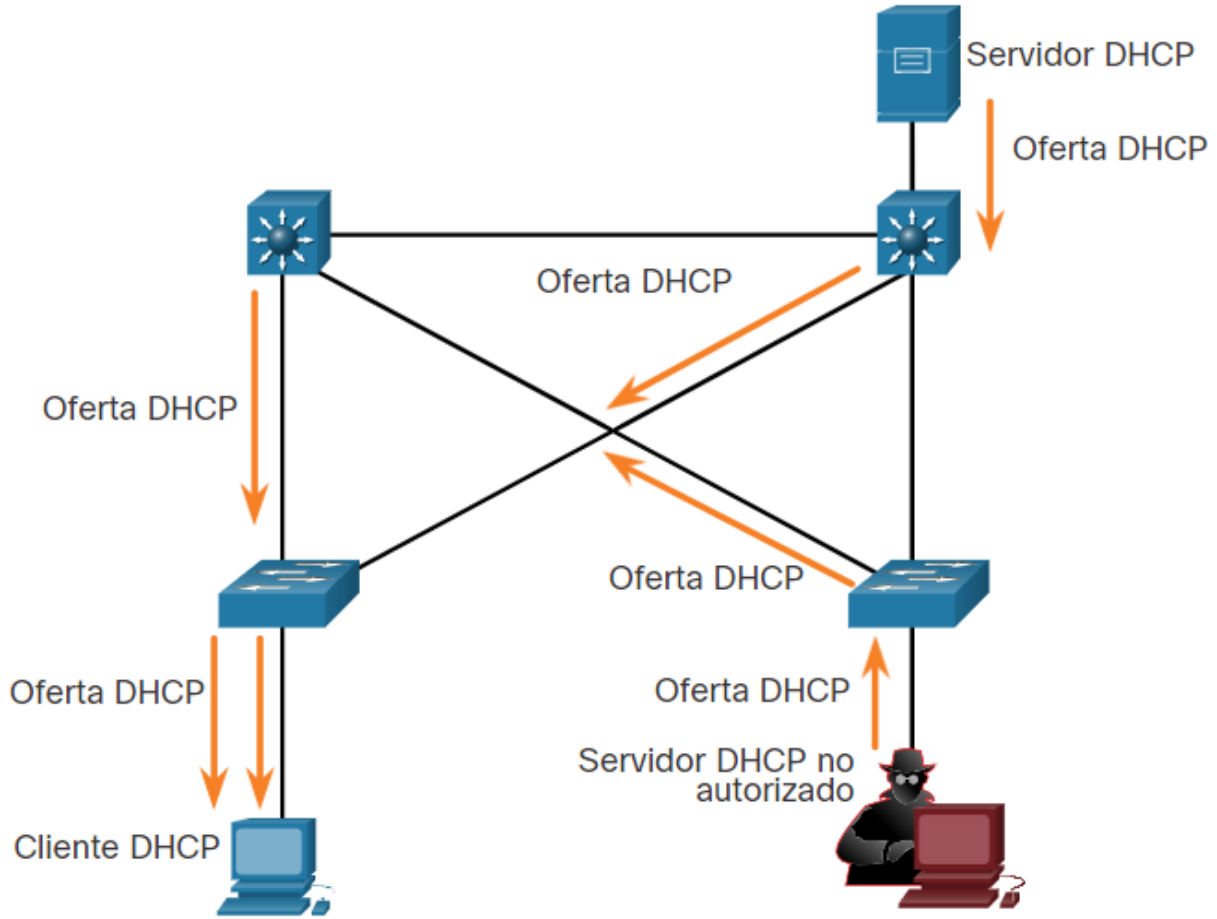
Mensajes DHCP

- **Ataque de DHCP Spoofing (Suplantación)**
  - **El cliente difunde mensajes DHCP discover, tipo broadcast**



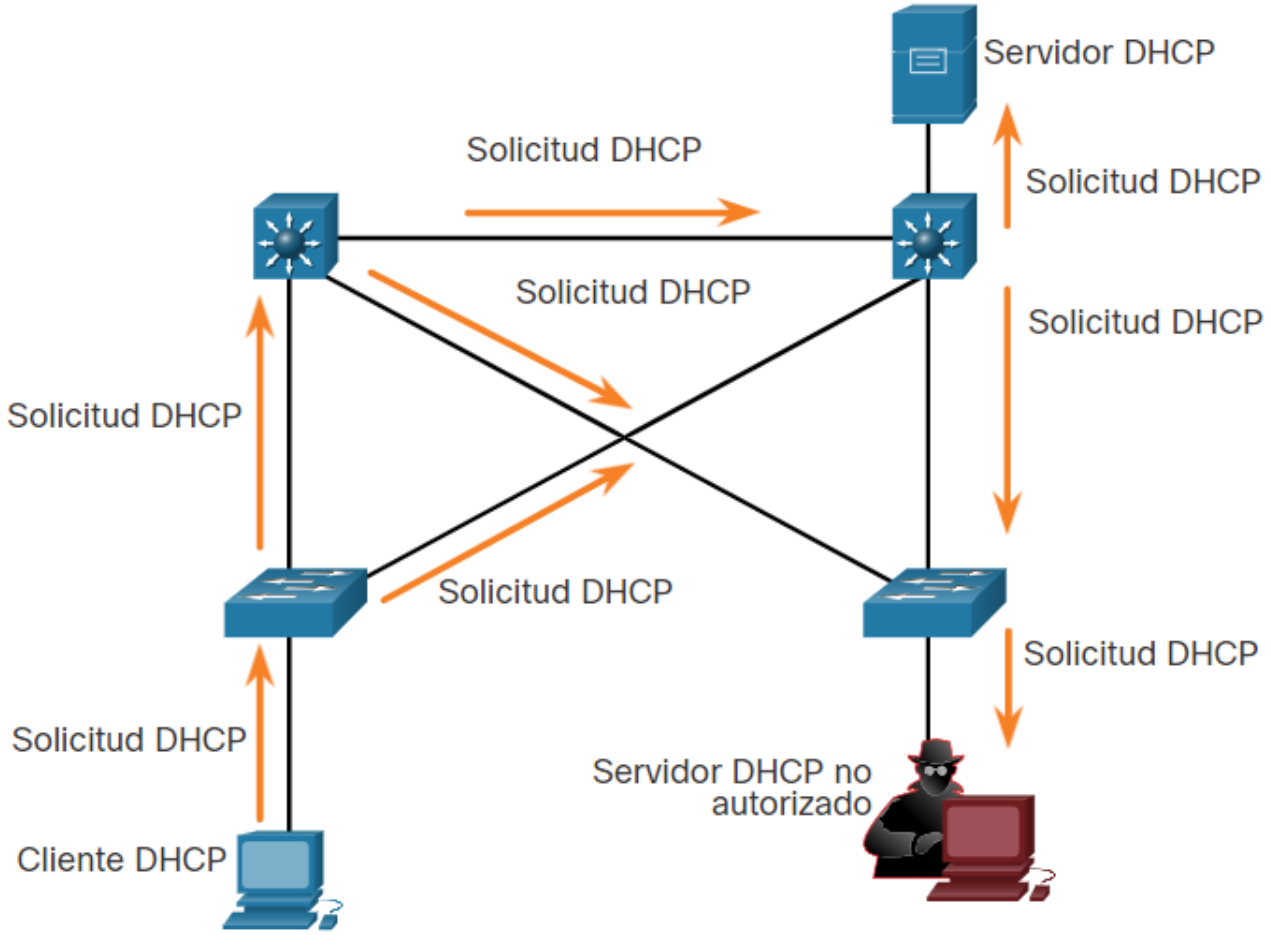
Mensajes DHCP

- **Ataque de DHCP Spoofing**
  - **Respuesta legítima y no autorizada de DHCP**



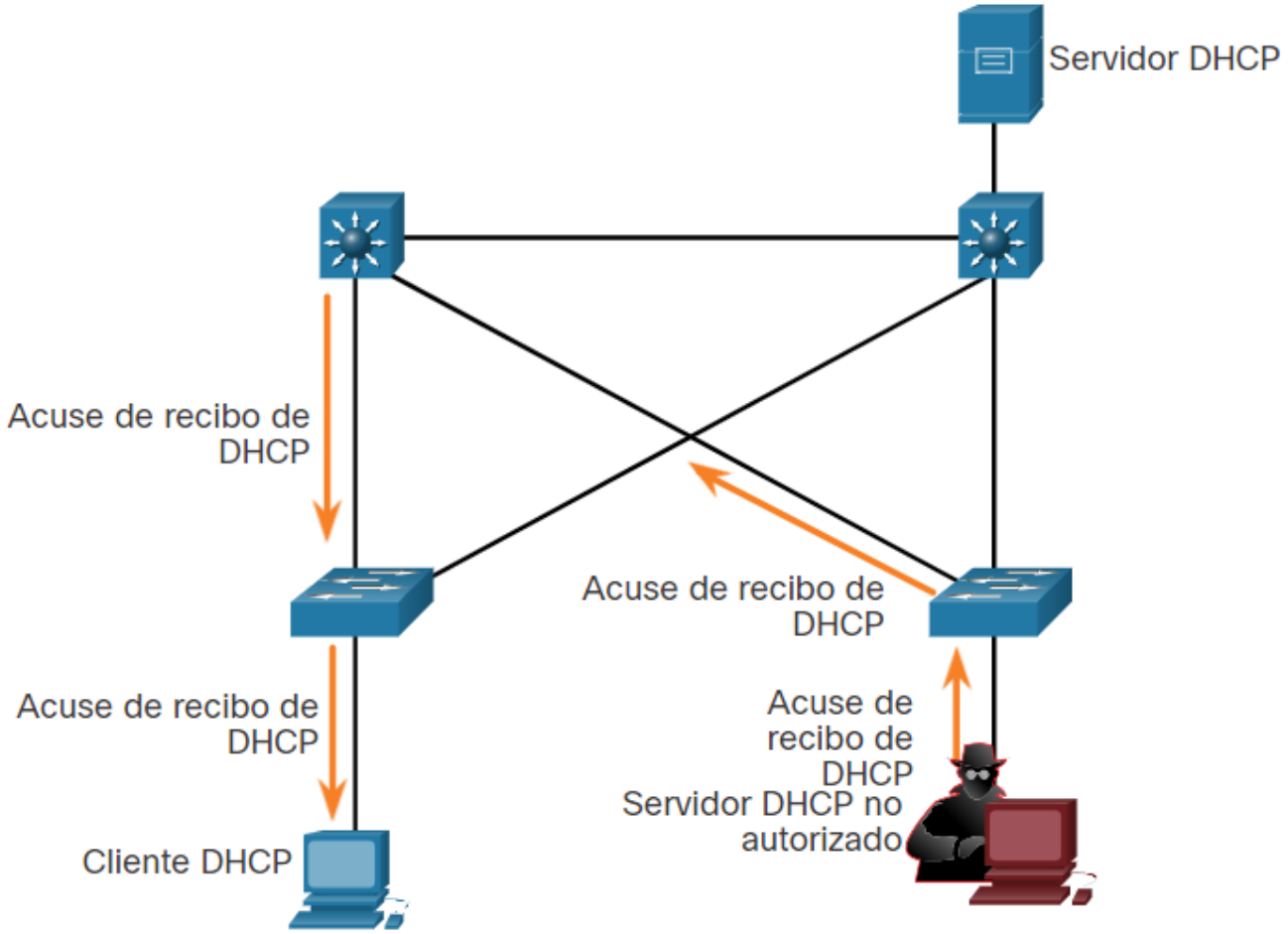
Mensajes DHCP

- **Ataque de DHCP Spoofing**
  - **El cliente acepta la oferta del servidor DHCP no autorizado**



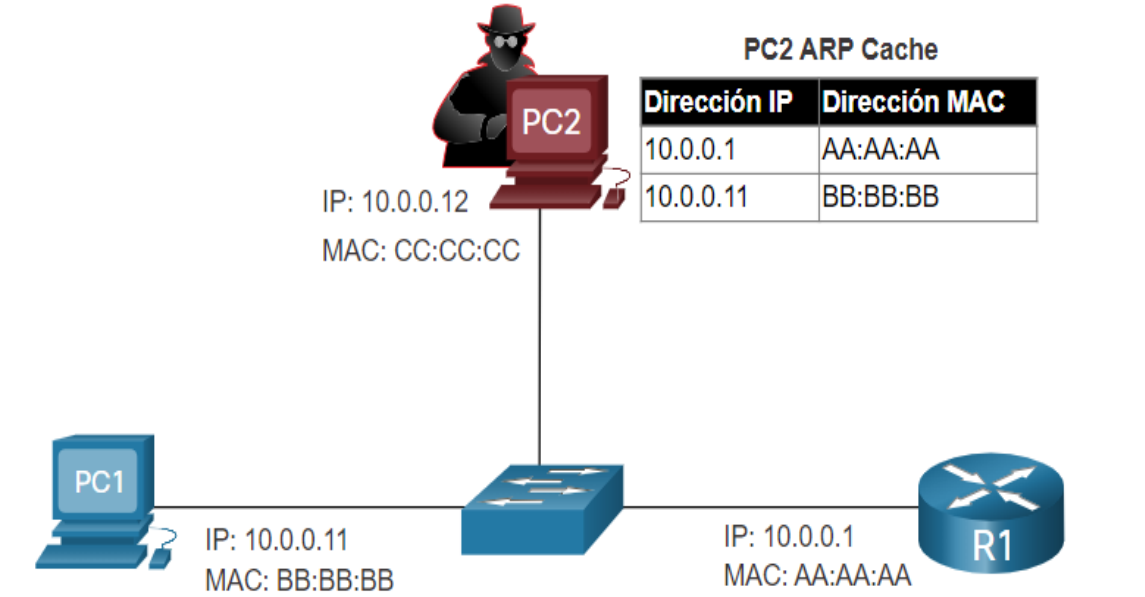
Mensajes DHCP

- **Ataque de DHCP Spoofing**
  - **Servidor falso confirma que recibió la solicitud.**



Mensajes DHCP (Ataques ARP)

Estado normal con tablas MAC convergentes



PC2 ARP Cache

Dirección IP	Dirección MAC
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

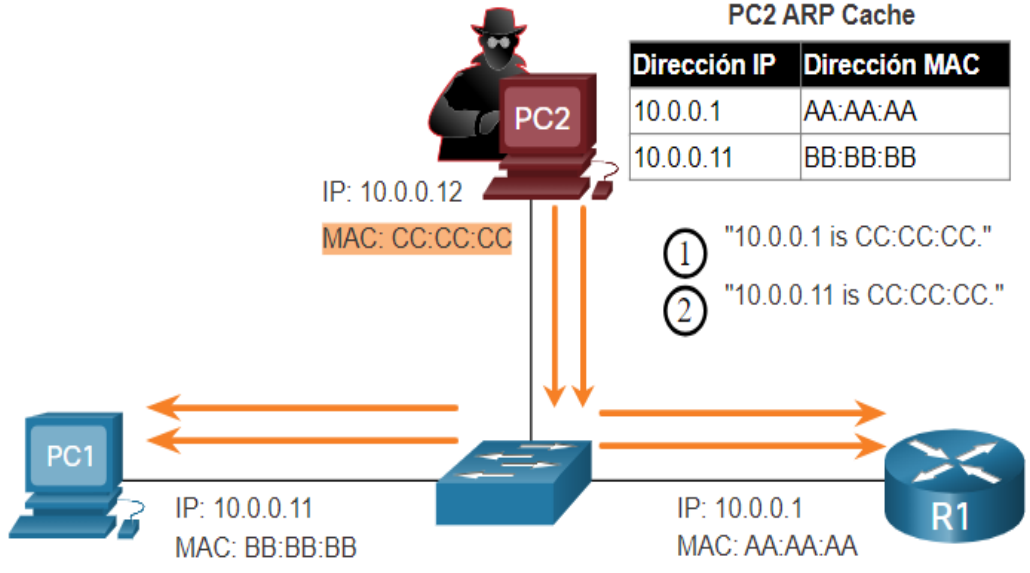
PC1 ARP Cache

Dirección IP	Dirección MAC
10.0.0.1	AA:AA:AA
10.0.0.12	CC:CC:CC

R1 ARP Cache

Dirección IP	Dirección MAC
10.0.0.11	BB:BB:BB
10.0.0.12	CC:CC:CC

Ataque ARP spoofing



PC2 ARP Cache

Dirección IP	Dirección MAC
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

PC1 ARP Cache

Dirección IP	Dirección MAC
10.0.0.1	AA:AA:AA
10.0.0.12	CC:CC:CC

R1 ARP Cache

Dirección IP	Dirección MAC
10.0.0.11	BB:BB:BB
10.0.0.12	CC:CC:CC

Actividad

Práctica de laboratorio

Packet Tracer - Configurar equipos remotos

Actividades

- ¿Por qué es tan importante la seguridad de capa 2?
- ¿Qué configuración o proceso considera que es la piedra angular de la seguridad de capa 2?
- ¿En qué casos sería demasiado engorrosa implementar una VLAN de administración dedicada?
- ¿Conoce alguna otra herramienta que pueda generar un ataque de inundación de direcciones MAC?
- ¿Cuál es el peligro en la inundación de tramas de unidifusión desconocidos?
- ¿Qué configuraciones podría implementar para evitar troncales no autorizados y, por lo tanto, ataques de salto de VLAN?
- ¿En qué parte de la red se debe habilitar un protocolo de descubrimiento de capa 2?

Conclusiones

¿Qué aprendí en esta sesión?

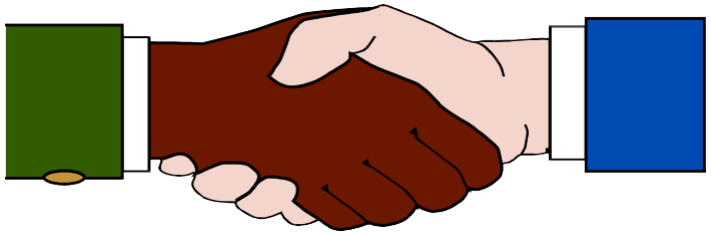
¿Qué aprendí en está sesión?

- El salto de VLAN permite que otra VLAN pueda ver el tráfico de una VLAN sin cruzar primero un router.
- Un ataque doble-etiqueta a una VLAN es unidireccional y funciona únicamente cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal.
- El salto de VLAN y los ataques de doble etiquetado de VLAN se pueden evitar mediante la implementación de las siguientes pautas de seguridad troncal:
  - Deshabilitar troncal en todos los puertos de acceso.
  - Deshabilitar troncal automático en enlaces troncales para poder habilitarlos de manera manual.
  - Asegúrese de que la VLAN nativa solo se use para los enlaces troncales.

¿Qué aprendí en este módulo?

- Los ataques por saturación de MAC se aprovechan de esta limitación con direcciones MAC de origen falsas que colman la tabla de direcciones MAC del switch y saturan el switch.
- AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).
- El estándar IEEE 802.1X define un control de acceso y un protocolo de autenticación basado en puertos que evita que las estaciones de trabajo no autorizadas se conecten a una LAN a través de los puertos de switch acceso público.

Gracias



Universidad
Tecnológica
del Perú