

Switching, Routing, y Wireless Essentials

- 1 Configuración básica de dispositivos
- 2 Conceptos de switching
- 3 VLANs
- 4 Inter-VLAN Routing
- 5 STP Concepts
- 6 EtherChannel
- 7 DHCPv4
- 8 SLAAC y DHCPv6
- 9 Conceptos de FHRP
- 10 Conceptos de Seguridad de LAN
 - 10.0 Introducción
 - 10.1 Seguridad de Punto Terminal
 - 10.2 Control de Acceso
 - 10.3 Amenazas a la seguridad de Capa 2
 - 10.4 Ataque de Tablas de Direcciones MAC
 - 10.5 Ataques a la LAN
 - 10.6 Práctica del Módulo y Cuestionario
- 11 Configuraciones de seguridad del Switch
- 12 Conceptos WLAN
- 13 Configuraciones de redes inalámbricas WLAN
- 14 Conceptos de enrutamiento
- 15 Rutas IP estáticas
- 16 Resuelva problemas de rutas estáticas y predeterminadas

Seguridad de Punto Terminal

10.1.1

Ataques de Red Actuales



Normalmente, los medios de comunicación cubren los ataques de red externos a redes empresariales. Sencillamente busque en el internet por "Los ataques más recientes de red" y encontrará información actualizada de ataques actuales. Muy posiblemente, estos ataques envuelven una o más de las siguientes:

- **Negación de Servicio Distribuido (DDoS)** – Esto es un ataque coordinado desde muchos dispositivos, llamados zombies, con la intención de degradar o detener acceso público al sitio web y los recursos de una organización.
- **Filtración de Datos** – Este es un ataque en el que los servidores de datos o los hosts de una organización han sido comprometidos con el fin de robar información confidencial.
- **Malware** – Este es un ataque en el que los hosts de una organización son infectados con software malicioso que causa una serie de problemas. Por ejemplo, ransomware como WannaCry, mostrado en la figura, encripta los datos en un host y bloquea el acceso hasta que se le pague un rescate.



10.1.2

Dispositivos de Seguridad de Red



Se necesitan diversos dispositivos de seguridad para proteger el perímetro de la red del acceso exterior. Estos dispositivos podrían incluir un router habilitado con una Red Privada Virtual (VPN), un Firewall de Siguiente Generación (NGFW), y un Dispositivo de Acceso a la Red (NAC).



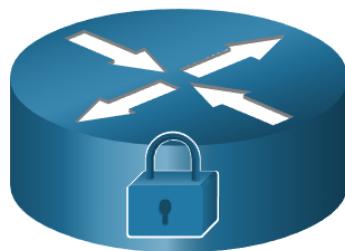
Haga clic en cada dispositivo de seguridad de red para obtener más información.

Router habilitado con VPN

NGFW

NAC

Red Privada Virtual (VPN) proporciona una conexión segura para que usuarios remotos se conecten a la red empresarial a través de una red pública. Los servicios VPN pueden ser integrados en el firewall.



10.1.3

Protección de terminales

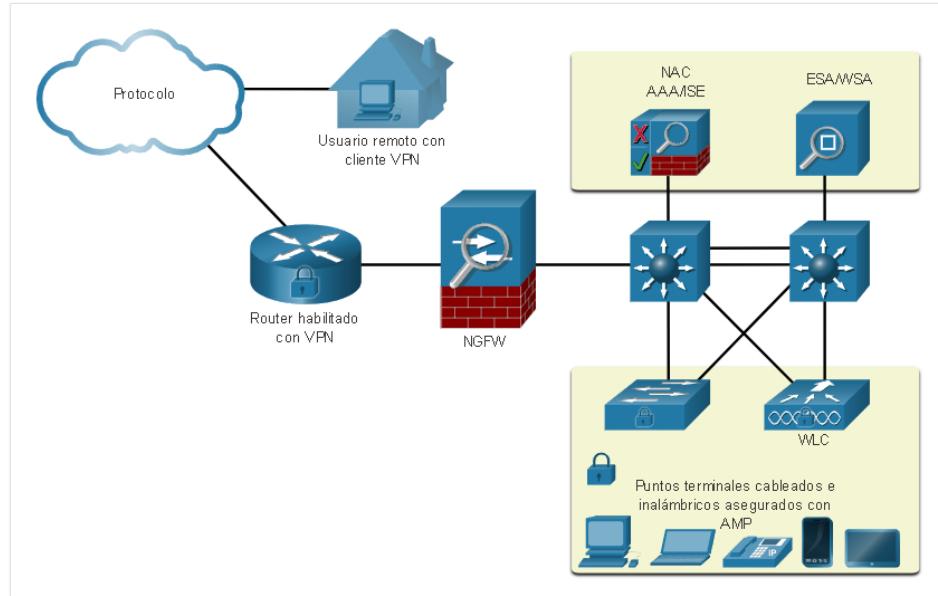


Los dispositivos LAN como los switches, los Controladores de LAN Inalámbricos (WLCs), y otros puntos de acceso (AP) interconectan puntos terminales. La mayoría de estos dispositivos son susceptibles a los ataques LAN que se cubren en este módulo.

Sin embargo, muchos ataques se originan dentro de la red. Si un atacante se infiltra en un host interno, este puede ser el punto de partida para que obtenga acceso a dispositivos esenciales del sistema, como servidores e información confidencial.

Los puntos terminales son hosts que generalmente consisten en computadoras portátiles, computadoras de escritorio, servidores y teléfonos IP, así como dispositivos propiedad de los empleados (BYOD). Los puntos terminales son particularmente susceptibles a ataques relacionados con malware que se originan a través del correo electrónico o la navegación web. Estos puntos finales suelen utilizar características de seguridad tradicionales basadas en host, como antivirus/antimalware, firewalls basados en host y sistemas de prevención de intrusiones (HIPS) basados en host. Sin embargo, actualmente los puntos finales están más protegidos por una combinación de NAC, software AMP basado en host, un Dispositivo de Seguridad de Correo Electrónico (ESA) y un Dispositivo de Seguridad Web (WSA). Los productos de Protección Avanzada de Malware (AMP) incluyen soluciones de dispositivos finales como Cisco AMP.

La figura es una topología simple que representa todos los dispositivos de seguridad de red y soluciones de dispositivos finales discutidas en este módulo.



10.1.4

Dispositivo de Seguridad de Correo Electrónico Cisco (ESA)



Los dispositivos de seguridad de contenido incluyen un control detallado sobre el correo electrónico y la navegación web para los usuarios de una organización.

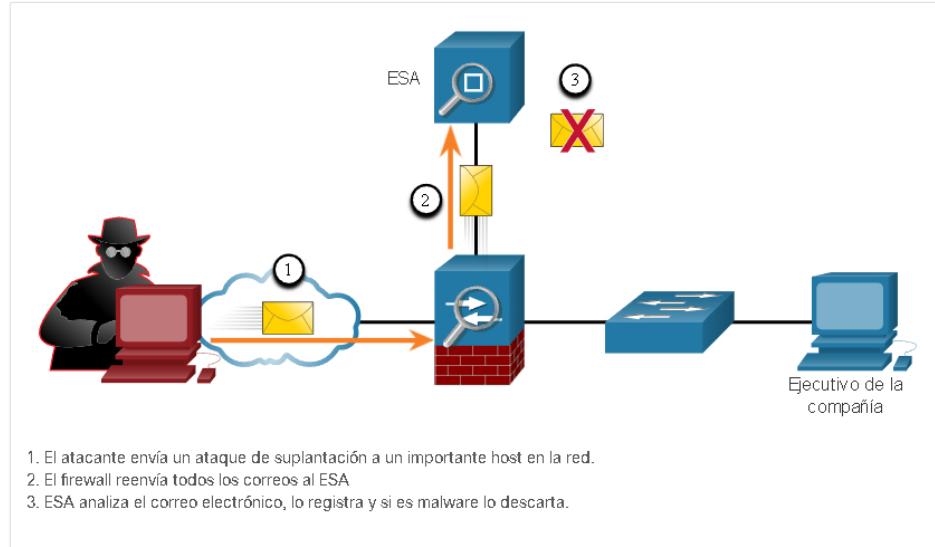
Según el Talos Intelligence Group de Cisco, en junio de 2019, el 85% de todos los correos electrónicos enviados eran spam. Los ataques de suplantación de identidad son una forma de correo electrónico no deseado particularmente virulenta. Recuerda que

ataques de suplantación de identidad son una forma de correo electrónico no deseado particularmente virulenta. Recuerda que un ataque de phishing lleva al usuario a hacer clic en un enlace o abrir un archivo adjunto. Spear phishing selecciona como objetivo a empleados o ejecutivos de alto perfil que pueden tener credenciales de inicio de sesión elevadas. Esto es particularmente crucial en el ambiente actual, donde, de acuerdo al Instituto SANS, 95% de todos los ataques en redes empresariales son del resultado de un spear phishing exitoso.

El dispositivo Cisco ESA está diseñado para monitorear el Protocolo Simple de Transferencia de Correo (SMTP). Cisco ESA se actualiza en tiempo real de Cisco Talos, quien detecta y correlaciona las amenazas con un sistema de monitoreo que utiliza una base de datos mundial. Cisco ESA extrae estos datos de inteligencia de amenazas cada tres o cinco minutos. Estas son algunas funciones de Cisco ESA:

- Bloquear las amenazas
- Remediad contra el malware invisible que evade la detección inicial
- Descartar correos con enlaces malos (como se muestra en la figura).
- Bloquear el acceso a sitios recién infectados
- Encriptar el contenido de los correos salientes para prevenir perdida de datos.

En la figura Cisco ESA descarta el correo con enlaces malos.



10.1.5

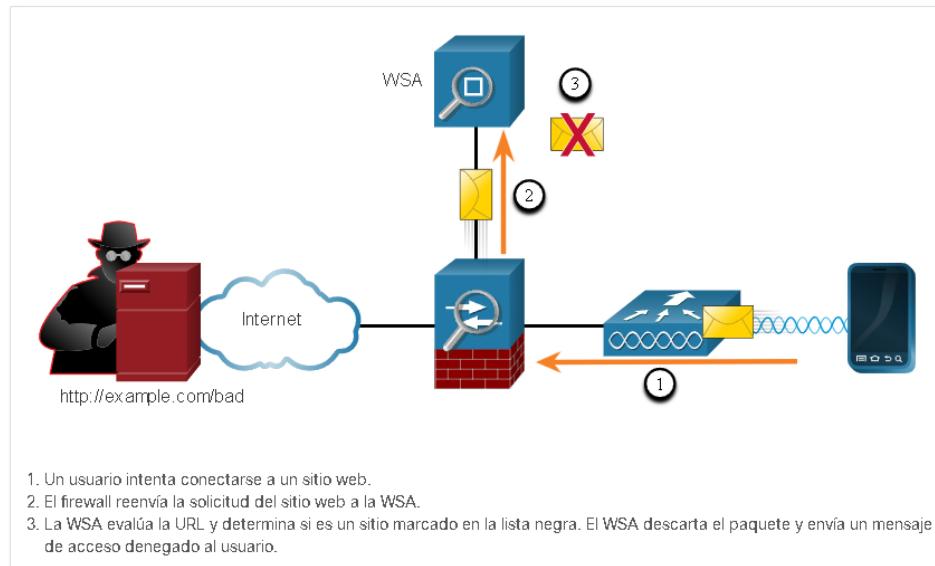
Dispositivo de Seguridad de la Red de Cisco (WSA)



Cisco Web Security Appliance (WSA) es una tecnología de mitigación para amenazas basadas en la web. Ayuda a las organizaciones a abordar los desafíos de asegurar y controlar el tráfico web. Cisco WSA combina protección avanzada contra malware, visibilidad y control de aplicaciones, controles de políticas de uso aceptable e informes.

Cisco WSA proporciona un control completo sobre cómo los usuarios acceden a Internet. Ciertas funciones y aplicaciones, como chat, mensajería, video y audio, pueden permitirse, restringirse con límites de tiempo y ancho de banda, o bloquearse, de acuerdo con los requisitos de la organización. La WSA puede realizar listas negras de URL, filtrado de URL, escaneo de malware, categorización de URL, filtrado de aplicaciones web y cifrado y descifrado del tráfico web.

En la figura, un usuario corporativo intenta conectarse a un sitio marcado en la lista negra.



10.1.6

Ponga a prueba su conocimiento – Seguridad de Punto Terminal



Elija la MEJOR respuesta para las siguientes preguntas y compruebe su conocimiento sobre seguridad de punto terminal (endpoint security)

1. ¿Cuál ataque encripta los datos en los hosts con el propósito de extraer un pago monetario de la víctima?

¡Lo tienes!

- DDoS
- Vulneración de datos
- Malware
- Ransomware

2. ¿Cuáles dispositivos han sido diseñados específicamente para proveer seguridad a la red? (Elija tres opciones)

¡Lo tienes!

- Router habilitado con VPN
- NGFW
- Switch
- WLC
- NAC

3. ¿Cuál dispositivo monitorea el tráfico SMTP para bloquear amenazas y cifrar mensajes salientes para prevenir pérdida de datos?

¡Lo tienes!

- NGFW
- ESA
- NAC
- WSA

4. ¿Cuál dispositivo monitorea el tráfico HTTP para bloquear el acceso a sitios riesgosos y cifrar mensajes salientes?

¡Lo tienes!

- NGFW
- ESA
- NAC
- WSA

[Verificar](#)

[Mostrar](#)

[Restablecer](#)

< 10.0 [Introducción](#)

[Control de Acceso](#) >



Router habilitado con VPN

NGFW

NAC

Firewall de Siguiente Generación (NGFW) - proporciona inspección de paquetes con estado, visibilidad y control de aplicaciones, un Sistema de Prevención de Intrusos de Próxima Generación (NGIPS), Protección Avanzada contra Malware (AMP) y filtrado de URL.



Router habilitado con VPN

NGFW

NAC

Un dispositivo NAC incluye autenticación, autorización y registro (AAA). En empresas más grandes, estos servicios podrían incorporarse en un dispositivo que pueda administrar políticas de acceso en una amplia variedad de usuarios y tipos de dispositivos. El Cisco Identity Services Engine (ISE) es un ejemplo de dispositivo NAC.





Switching, Routing, y Wireless Essentials

- 1 Configuración básica de dispositivos
- 2 Conceptos de switching
- 3 VLANs
- 4 Inter-VLAN Routing
- 5 STP Concepts
- 6 EtherChannel
- 7 DHCPv4
- 8 SLAAC y DHCPv6
- 9 Conceptos de FHRP
- 10 Conceptos de Seguridad de LAN
 - 10.0 Introducción
 - 10.1 Seguridad de Punto Terminal
 - 10.2 Control de Acceso
 - 10.2.1 Autenticación con una contraseña local
 - 10.2.2 Componentes AAA
 - 10.2.3 Autenticación
 - 10.2.4 Autorización
 - 10.2.5 Registro
 - 10.2.6 802.1x
 - 10.2.7 Verifique su comprensión: Control de Acceso
 - 10.3 Amenazas a la seguridad de Capa 2
 - 10.4 Ataque de Tablas de Direcciones MAC
 - 10.5 Ataques a la LAN
 - 10.6 Práctica del Módulo y Cuestionario
- 11 Configuraciones de seguridad del Switch
- 12 Conceptos WLAN
- 13 Configuraciones de redes inalámbricas WLAN

Control de Acceso

10.2.1

Autenticación con una contraseña local



En el tema anterior usted aprendió que un NAC provee servicios AAA. En este tema usted aprenderá más sobre AAA y las formas de controlar el acceso.

Muchas formas de autenticación pueden ser llevadas a cabo en dispositivos de red, y cada método ofrece diferentes niveles de seguridad. El método más simple de autenticación para acceso remoto consiste en configurar un inicio de sesión, combinando nombre de usuario y contraseña, a nivel de consola, líneas vty, y puertos auxiliares, como se muestra en el siguiente ejemplo. Este método es el más simple de implementar, pero también el más débil y menos seguro. Este método no es fiable y la contraseña es enviada en texto plano. Qualquier persona con la contraseña puede acceder al dispositivo.

```
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, que se encriptan durante la transmisión.
- El nombre de usuario y la contraseña pueden ser autenticados por el método de base de datos local.
- Proporciona más responsabilidad porque el nombre de usuario queda registrado cuando un usuario inicia sesión.

El siguiente ejemplo ilustra el SSH y métodos de acceso remoto a una base de datos local

```
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
```

El método de base de datos local tiene algunas limitaciones

- Las cuentas de usuario deben ser configuradas localmente en cada dispositivo. En una gran empresa con múltiples routers y switches que controlar, puede tomar mucho tiempo implementar y cambiar bases de datos locales en cada dispositivo.
- Además, la configuración de la base de datos local no proporciona ningún método de autenticación de respaldo. Por ejemplo, ¿qué sucede si el administrador olvida el nombre de usuario y la contraseña para ese dispositivo? Sin un método de respaldo disponible para la autenticación, la restauración se convierte en la única opción.

Una mejor solución es hacer que todos los dispositivos se refieran a la misma base de datos de nombres de usuario y contraseñas alojados en un servidor central.

10.2.2

Componentes AAA



AAA significa Autenticación, Autorización y Registro. El concepto de AAA es similar al uso de una tarjeta de crédito, como se muestra en la imagen. La tarjeta de crédito identifica quién la usa y cuánto puede gastar el usuario de esta, y mantiene un registro de cuántos elementos o servicios adquirió el usuario.

"AAA" o "triple A", estos servicios proporcionan el marco principal para ajustar 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 (registrar).

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	\$278.50
MAIL PAYMENT TO: THE BANK 1234 FAIR STREET ANYTOWN, USA 67500-0010		
672919345 001762550000000003		
Detach here and return upper portion with check or money order. Do not staple or fold.		
Statement of Personal Credit Card Account Retain this portion for your files.		
Cardmember Name JOE EMPLOYEE		Account Number 0000 0000 0000 0000
Statement Closing Date 01-31-01		

- 14 Conceptos de enrutamiento
- 15 Rutas IP estáticas
- 16 Resuelva problemas de rutas estáticas y predeterminadas

¿Quién es?

Autorización

¿Cuánto puede gastar?

Registro

¿En qué gastó el dinero?

JOE EMPLOYEE 1234-567-8900 01-31-01

Statement Date: 02-01-01 Payment Due Date: 03-01-01

Crossover Date: 01-31-01

Credit Limit: \$1500.00

New Balance: \$276.50

Credit Available: \$1221.50

Minimum Payment Due: \$20.00

Account Summary

Previous Balance: +74.24

Purchases: +250.50

Cash Advances: +0

Payments: -74.25

Finance Charge: +0

Late Charge: +0

Transaction Fees: +3.00

Annual Fees: +25.00

Current Amount Due: +250.50

Amount Past Due: +0

Amount Over Credit Line: +0

NEW BALANCE: \$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
23455678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE: 1 OF 1

10.2.3

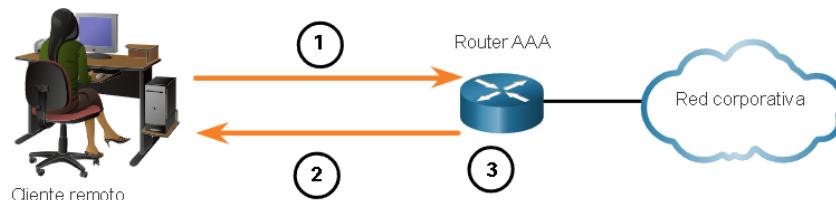
Autenticación



Dos métodos de implementación de autenticación AAA son Local y basado en servidor.

Autenticación AAA local

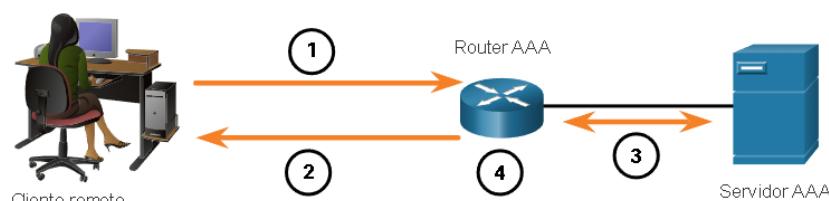
Los AAA locales guardan los nombres de usuario y contraseñas localmente en un dispositivo de red como el router de Cisco. Los usuarios se autentican contra la base de datos local, como se muestra en la figura. AAA local es ideal para las redes pequeñas.



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 AAA basada en el servidor

Con el método basado en servidor, el router accede a un servidor central de AAA, como se muestra en la imagen. 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 Terminal Mejorado (TACACS+) o el protocolo de Servicio de Autenticación Remota de Usuario de Discado (RADIUS) para comunicarse con el servidor de AAA. Cuando hay múltiples enruteadores y switches, el método 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.

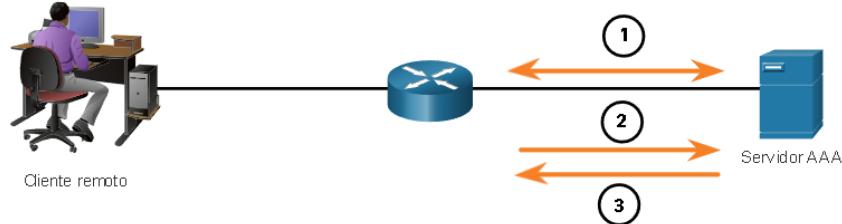
10.2.4

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. Estos atributos son usados por el servidor AAA para determinar privilegios y restricciones para ese usuario, como se muestra en la figura.



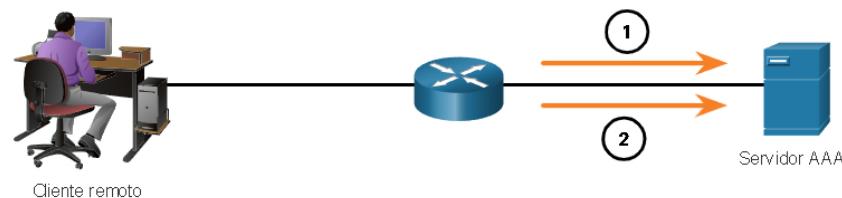
1. Cuando un usuario ha sido autenticado, una sesión es establecida entre el router y el servidor AAA.
2. El router pide autorización al servidor AAA para la solicitud de servicio del cliente.
3. El servidor AAA responde con un PASS/FAIL a la solicitud.

Registro



El registro de AAA recopila y reporta datos de uso. 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 debe registro consiste en 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. Además proporciona evidencia contra individuos que realizan actividades maliciosas.



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.

802.1x



El estándar IEEE 802.1X define un control de acceso y un protocolo de autenticación basados en puertos. Este protocolo 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 de habilitar cualquier servicio ofrecido por el switch o la LAN.

Con la autenticación 802.1X basada en puertos, los dispositivos de la red cumplen roles específicos, como se muestra en la figura:



Requiere acceso y responde a las solicitudes del switch

Controla el acceso físico a la red según el estado de autenticación del cliente

Ejecuta la autenticación del cliente

- **Cliente (suplicante)** - Este es un dispositivo ejecutando software de cliente 802.1X, el cual está disponible para dispositivos conectados por cable o inalámbricos.
- **Switch (Autenticador)** - El switch funciona como actúa intermediario (proxy) entre el cliente y el servidor de autenticación. Solicita la identificación de la información del cliente, verifica dicha información al servidor de autenticación y transmite una respuesta al cliente. Otro dispositivo que puede actuar como autenticador es un punto de acceso inalámbrico.
- **Servidor de autenticación** - El servidor valida la identidad del cliente y notifica al switch o al punto de acceso inalámbrico si el cliente está o no autorizado para acceder a la LAN y a los servicios del Switch.

10.2.7

Verifique su comprensión: Control de Acceso



Elija la MEJOR respuesta para las siguientes preguntas y compruebe su conocimiento sobre control de acceso.

1. ¿Cuál componente AAA es responsable de recolectar y reportar el uso de datos para propósitos de auditoría y facturación?

¡Lo tienes!

- Autenticación
- Autorización
- Registro

2. ¿Cuál componente AAA es responsable de controlar quien está autorizado a acceder a la red?

¡Lo tienes!

- Autenticación
- Autorización
- Registro

3. ¿Cuál componente AAA es responsable de determinar que puede acceder un usuario?

¡Lo tienes!

- Autenticación
- Autorización
- Registro

4. En una implementación 802.1X, ¿qué dispositivo es responsable de retransmitir las respuestas?

¡Lo tienes!

- Suplicante
- Autenticador
- Router
- Servidor de autenticación
- Cliente

Verificar

Mostrar

Restablecer

< 10.1 Seguridad de Punto Terminal

Amenazas a la seguridad de Capa 2 >

Switching, Routing, y Wireless Essentials

1	Configuración básica de dispositivos
2	Conceptos de switching
3	VLANs
4	Inter-VLAN Routing
5	STP Concepts
6	EtherChannel
7	DHCPv4
8	SLAAC y DHCPv6
9	Conceptos de FHRP
10	Conceptos de Seguridad de LAN
10.0	Introducción
10.1	Seguridad de Punto Terminal
10.2	Control de Acceso
10.2.1	Autenticación con una contraseña local
10.2.2	Componentes AAA
10.2.3	Autenticación
10.2.4	Autorización
10.2.5	Registro
10.2.6	802.1x
10.2.7	Verifique su comprensión: Control de Acceso
10.3	Amenazas a la seguridad de Capa 2
10.3.1	Capa 2 Vulnerabilidades
10.3.2	Categorías de Ataques a Switches
10.3.3	Técnicas de Mitigación en el Switch
10.3.4	Ponga a prueba su conocimiento: Amenazas de Seguridad de Capa 2
10.4	Ataque de Tablas de Direcciones MAC
10.5	Ataques a la LAN
	Resumen del Módulo

Amenazas a la seguridad de Capa 2

10.3.1

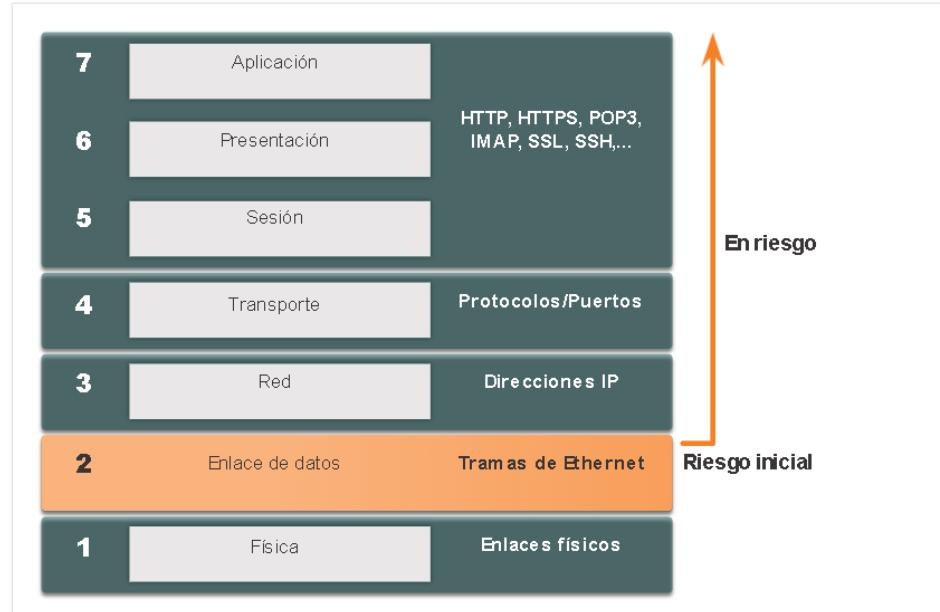
Capa 2 Vulnerabilidades



Los dos temas anteriores discutieron seguridad en puntos terminales. En este tema, usted va a seguir aprendiendo sobre formas de asegurar una LAN, enfocándose en las tramas de la Capa de Enlace (Capa 2) y el switch.

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

Los administradores de red regularmente implementan soluciones de seguridad para proteger los componentes en la Capa 3 y hasta la Capa 7. Ellos usan VPNs, firewalls, y dispositivos IPS para proteger estos elementos. Si la Capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. Por ejemplo, si un atacante con acceso a la red interna captura los marcos de la Capa 2, entonces toda la seguridad implementada en las capas anteriores sería inútil. El atacante podría causar mucho daño en la infraestructura de red LAN de Capa 2.



10.3.2

Categorías de Ataques a Switches



La seguridad es solamente tan sólida como el enlace más débil en el sistema, y la Capa 2 es considerada el enlace más débil. Esto se debe a que las LAN estaban tradicionalmente bajo el control administrativo de una sola organización. Nosotros confiábamos inherentemente en todas las personas y dispositivos conectados a nuestra LAN. Hoy, con BYOD y ataques más sofisticados, nuestras LAN se han vuelto más vulnerables a la penetración. Además de proteger de la Capa 3 a la Capa 7, los profesionales de seguridad de red también deben mitigar los ataques a la infraestructura LAN de la Capa 2.

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.

Los ataques contra la infraestructura LAN de capa 2 se describen en la tabla y se analizan con más detalle más adelante en este módulo.

Layer 2 Attacks

Categoría	Ejemplos
Ataques a la tabla MAC	Incluye ataques de saturación de direcciones MAC.
Ataques de VLAN	Incluye ataques VLAN Hopping y VLAN Double-Tagging. Esto también incluye ataques entre dispositivos en una misma VLAN.
Ataques de DHCP	Incluye ataques de agotamiento y suplantación DHCP.

10.6	Práctica del Módulo y Cuestionario
11	Configuraciones de seguridad del Switch
12	Conceptos WLAN
13	Configuraciones de redes inalámbricas WLAN
14	Conceptos de enrutamiento
15	Rutas IP estáticas
16	Resuelva problemas de rutas estáticas y predeterminadas

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.
Ataque de STP	Incluye ataques de manipulación al Protocolo de Árbol de Extensión

10.3.3

Técnicas de Mitigación en el Switch



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

Layer 2 Attack Mitigation

Solución	Descripción
Seguridad de Puertos	Previene muchos tipos de ataques incluyendo ataques MAC address flooding Ataque por agotamiento del DHCP
DHCP Snooping	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.

Estas soluciones de Capa 2 no serán efectivas si los protocolos de administración no son seguros. Por ejemplo, los protocolos administrativos Syslog, Protocolo Simple de Administración de Red (SNMP), Protocolo Trivial de Transferencia de Archivos (TFTP), Telnet, Protocolo de Transferencia de Archivos (FTP) y la mayoría de otros protocolos comunes son inseguros, por lo tanto, se recomiendan las siguientes estrategias:

- Utilice siempre variantes seguras de protocolos de administración como SSH, Protocolo de Copia Segura (SCP), FTP Seguro (SFTP) y Seguridad de capa de sockets seguros / capa de transporte (SSL / TLS).
- Considere usar una red de administración fuera de banda para administrar dispositivos.
- Usar una VLAN de administración dedicada que solo aloje el tráfico de administración.
- Use ACL para filtrar el acceso no deseado.

10.3.4

Ponga a prueba su conocimiento: Amenazas de Seguridad de Capa 2



Elija la MEJOR respuesta para las siguientes preguntas y compruebe su conocimiento sobre amenazas de seguridad.

1. ¿Cuáles de las siguientes técnicas de mitigación son usadas para proteger desde la Capa 3 hasta la Capa 7 del modelo OSI? (Elija tres opciones).

¡Lo tienes!

- DHCP Snooping
 VPN
 Firewalls
 IPSG
 Dispositivos IPS

2. ¿Cuáles de las siguientes técnicas de mitigación evita muchos tipos de ataques, incluidos los ataques de saturación de la tabla MAC y agotamiento de direcciones DHCP?

¡Lo tienes!

- IPSG
 Detección de DHCP
 DAI
 Seguridad de puertos

3. ¿Cuál de las siguientes técnicas de mitigación previene suplantación de direcciones MAC e IP?

¡Lo tienes!

- IPSG

- DHCP Snooping
- DAI
- Seguridad de puertos

4. ¿Cuál de las siguientes técnicas de mitigación previene ataques de suplantación ARP y envenenamiento ARP?

¡Lo tienes!

- IPSG
- DHCP Snooping
- DAI
- Seguridad de puertos

5. ¿Cuál de las siguientes técnicas de mitigación previene ataques el agotamiento y suplantación DHCP?

¡Lo tienes!

- IPSG
- DHCP Snooping
- DAI
- Seguridad de puertos

[Verificar](#)

[Mostrar](#)

[Restablecer](#)

[!\[\]\(98ed6f947b7758d2a448faade293496c_img.jpg\) 10.2 Control de Acceso](#)

[\[Ataque de Tablas de Direcciones MAC\]\(#\) 10.4 >](#)

Switching, Routing, y Wireless Essentials

1	Configuración básica de dispositivos
2	Conceptos de switching
3	VLANs
4	Inter-VLAN Routing
5	STP Concepts
6	EtherChannel
7	DHCPv4
8	SLAAC y DHCPv6
9	Conceptos de FHRP
10	Conceptos de Seguridad de LAN
10.0	Introducción
10.1	Seguridad de Punto Terminal
10.2	Control de Acceso
10.2.1	Autenticación con una contraseña local
10.2.2	Componentes AAA
10.2.3	Autenticación
10.2.4	Autorización
10.2.5	Registro
10.2.6	802.1x
10.2.7	Verifique su comprensión: Control de Acceso
10.3	Amenazas a la seguridad de Capa 2
10.3.1	Capa 2 Vulnerabilidades
10.3.2	Categorías de Ataques a Switches
10.3.3	Técnicas de Mitigación en el Switch
10.3.4	Ponga a prueba su conocimiento: Amenazas de Seguridad de Capa 2
10.4	Ataque de Tablas de Direcciones MAC
10.4.1	Revisar la Operación del Switch
	Saturación de Tablas de Direcciones MAC

Ataque de Tablas de Direcciones MAC

10.4.1

Revisar la Operación del Switch



En este tema el foco esta aun en los switches, específicamente en la tabla de direcciones MAC y como estas tablas son vulnerables a ataques.

Recuerde que para tomar decisiones de reenvío, un Switch LAN de Capa 2 crea una tabla basada en las direcciones MAC de origen que se encuentran en las tramas recibidas. Como se muestra en la figura, esto es llamado una tabla de direcciones MAC. Tabla de direcciones MAC se guarda en la memoria y son usadas para reenviar tramas de forma eficiente.

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.cec4	DYNAMIC	Fa0/3
1	00d0.ba07.8499	DYNAMIC	Fa0/2

S1#

10.4.2

Saturación de Tablas de Direcciones MAC

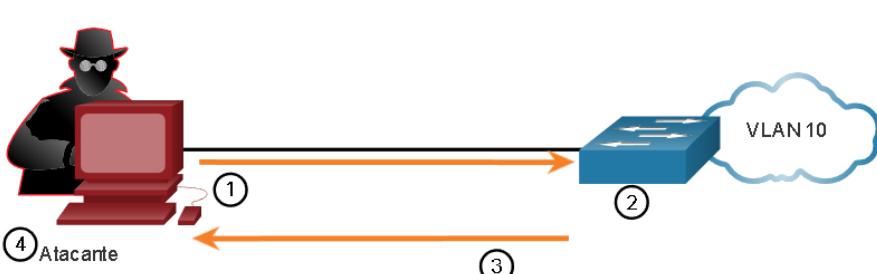


Todas las tablas MAC tiene un tamaño fijo, por lo que un switch puede quedarse sin espacio para guardar direcciones MAC. Los ataques de saturación de direcciones MAC aprovechan esta limitación al bombardear el switch con direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch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

Cuando esto ocurre, el switch trata la trama como un unicast desconocido y comienza a inundar todo el tráfico entrante por todos los puertos en la misma VLAN sin hacer referencia a la tabla MAC. Esta condición ahora permite que un atacante capture todas las tramas enviadas desde un host a otro en la LAN local o VLAN local.

Nota: El tráfico se satura solo dentro de la LAN o VLAN local. El atacante solo puede capturar el tráfico dentro de la LAN o VLAN local a la que está conectado el atacante.

La figura muestra como el atacante puede fácilmente usar la herramienta de red llamada **macof** para desbordar una tabla de direcciones MAC.



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** continúa 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.

Si el atacante detiene la ejecución de **macof** o si es descubierto y detenido, el switch eventualmente elimina las entradas mas viejas de direcciones MAC de la tabla y empieza a funcionar nuevamente como un switch.

10.4.2	Saturación de Tablas de Direcciones MAC
10.4.3	Mitigación de Ataques a la Tabla de Direcciones MAC.
10.4.4	Verifica tu entendimiento- Ataques a Tablas de Direcciones MAC.
10.5	Ataques a la LAN
10.6	Práctica del Módulo y Cuestionario
11	Configuraciones de seguridad del Switch
12	Conceptos WLAN
13	Configuraciones de redes inalámbricas WLAN
14	Conceptos de enrutamiento
15	Rutas IP estáticas
16	Resuelve problemas de rutas estáticas y predeterminadas

10.4.3

Mitigación de Ataques a la Tabla de Direcciones MAC.

Lo que hace que herramientas como **macof** sean peligrosas es que un atacante puede crear un ataque de saturación de tabla MAC muy rápidamente. Por ejemplo, un switch Catalyst 6500 puede almacenar 132,000 direcciones MAC en su tabla de direcciones MAC. 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. Este ejemplo muestra la salida del comando **macof** en un host Linux.

```
# 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 83:73:14:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 18388662028:18388662028(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 1818924173:1818924173(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
```

Otra razón por la que estas herramientas de ataque son peligrosas, es porque no solo afectan el switch local sino que también afectan switches conectados de Capa 2. Cuando la tabla de direcciones MAC de un switch está llena, comienza a desbordar todos los puertos, incluidos los conectados a otros switches de Capa 2.

Para mitigar los ataques de saturación de la tabla de direcciones MAC, los administradores de red deben implementar la seguridad del puerto. Seguridad de puertos (Port security) permitirá que el puerto aprenda sólo un número específico de direcciones MAC de origen. Seguridad de puertos (Port security) será discutido más adelante en otro módulo.

10.4.4

Verifica tu entendimiento- Ataques a Tablas de Direcciones MAC.



Elige la MEJOR respuesta para las siguientes preguntas y comprueba su conocimiento sobre ataques de tablas de direcciones MAC.

1. ¿Cuál es el comportamiento de un SWITCH como resultado de una ataque exitoso a la tabla de direcciones MAC?

- ¡Lo tienes!
- El switch se apagará.
- Las interfaces del switch pasarán al estado "error-disabled".
- El switch reenviará todas las tramas recibidas por todos los otros puertos dentro de la VLAN.
- El switch descartará todas las tramas recibidas.

2. ¿Cuál sería el motivo principal por el que un atacante podría lanzar un ataque de saturación de la dirección MAC?

- ¡Lo tienes!
- Para que el atacante pueda ver tramas que están destinados a otros dispositivos.
- Para que el atacante pueda ejecutar un código arbitrario en el switch.
- Para que el switch deje de enviar tráfico.
- Para que los hosts legítimos no puedan obtener una dirección MAC.

3. ¿Qué técnica de mitigación se debe implementar para prevenir ataques de saturación de direcciones MAC?

- ¡Lo tienes!
- IPSG
- DAI
- Seguridad de puertos (Port security)
- DHCP Snooping

[Verificar](#)

[Mostrar](#)

[Restablecer](#)

10.3

Amenazas a la seguridad de Capa 2

10.5

Ataques a la LAN

Switching, Routing, y Wireless Essentials

- 1 Configuración básica de dispositivos
- 2 Conceptos de switching
- 3 VLANs
- 4 Inter-VLAN Routing
- 5 STP Concepts
- 6 EtherChannel
- 7 DHCPv4
- 8 SLAAC y DHCPv6
- 9 Conceptos de FHRP
- 10 Conceptos de Seguridad de LAN
 - 10.0 Introducción
 - 10.1 Seguridad de Punto Terminal
 - 10.2 Control de Acceso
 - 10.2.1 Autenticación con una contraseña local
 - 10.2.2 Componentes AAA
 - 10.2.3 Autenticación
 - 10.2.4 Autorización
 - 10.2.5 Registro
 - 10.2.6 802.1x
 - 10.2.7 Verifique su comprensión: Control de Acceso
- 10.3 Amenazas a la seguridad de Capa 2
 - 10.3.1 Capa 2 Vulnerabilidades
 - 10.3.2 Categorías de Ataques a Switches
 - 10.3.3 Técnicas de Mitigación en el Switch
 - 10.3.4 Ponga a prueba su conocimiento: Amenazas de Seguridad de Capa 2
- 10.4 Ataque de Tablas de Direcciones MAC
 - 10.4.1 Revisar la Operación del Switch
- Saturación de Tablas de

Ataques a la LAN

10.5.1

Video - VLAN y Ataques DHCP



Este tema investiga los diferentes tipos de ataques LAN y las técnicas de mitigación a estos ataques. Como en temas anteriores, estos ataques tienden a ser específicamente a los switches y Capa 2.

Haga clic en reproducir en la figura para ver un video sobre ataques de denegación de servicio.

Video – VLAN and DHCP Attacks

This video will cover the following:

- VLAN Hopping Attack
- VLAN Double – Tagging Attack
- DHCP Starvation Attack
- DHCP Spoofing Attack

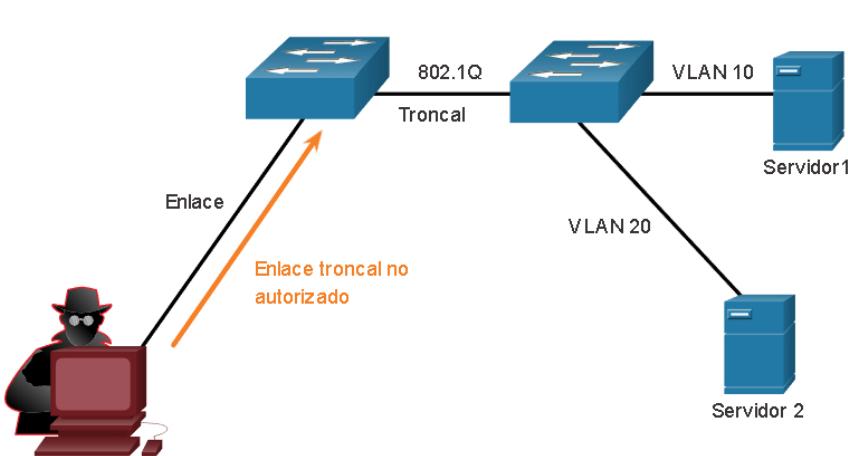


Ataque de VLAN Hopping



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

El atacante configura el host para falsificar la señalización 802.1Q y la señalización del Protocolo de enlace dinámico (DTP), propiedad de Cisco, hacia el enlace troncal con el switch de conexión. Si es exitoso, el switch establece un enlace troncal con el host, como se muestra en la figura. Ahora el atacante puede acceder todas las VLANs en el switch. El atacante puede enviar y recibir tráfico en cualquier VLAN, saltando efectivamente entre las VLAN.



El atacante obtiene acceso a la VLAN del servidor.

10.4.2	Saturación de Tablas de Direcciones MAC
10.4.3	Mitigación de Ataques a la Tabla de Direcciones MAC.
10.4.4	Verifica tu entendimiento- Ataques a Tablas de Direcciones MAC.
10.5	Ataques a la LAN
10.5.1	Video - VLAN y Ataques DHCP
10.5.2	Ataque de VLAN Hopping
10.5.3	Ataque de VLAN Double-Tagging
10.5.4	Mensajes DHCP
10.5.5	Ataques de DHCP
10.5.6	Video- Ataques ARP, Ataques STP, y Reconocimiento CDP.
10.5.7	Ataques ARP
10.5.8	Ataque de Suplantación de Dirección
10.5.9	Ataque de STP
10.5.10	Reconocimiento CDP
10.5.11	Verifique su comprensión - Ataques LAN
10.6	Práctica del Módulo y Cuestionario
11	Configuraciones de seguridad del Switch
12	Conceptos WLAN
13	Configuraciones de redes inalámbricas WLAN
14	Conceptos de enrutamiento
15	Rutas IP estáticas
16	Resuelva problemas de rutas estáticas y predeterminadas

10.5.3 Ataque de VLAN Double-Tagging

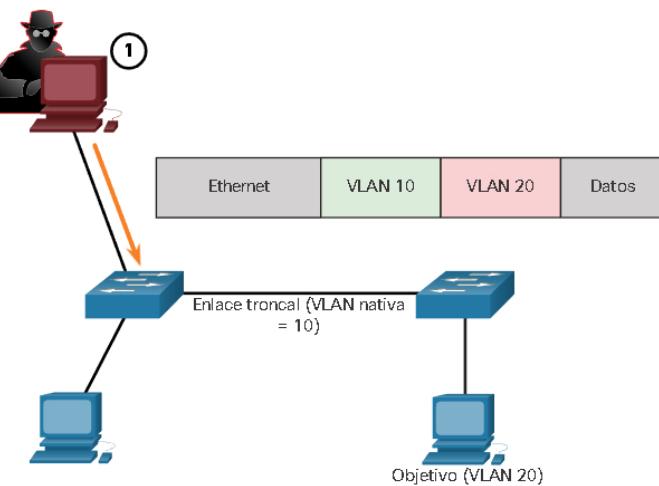
Un atacante, en situaciones específicas, podrían insertar una etiqueta 802.1Q oculta dentro de la trama que ya tiene una etiqueta 802.1Q. Esta etiqueta permite que la trama se envíe a una VLAN que la etiqueta 802.1Q externa no especificó.

 Haga clic en cada paso para ver un ejemplo y una explicación de un ataque de VLAN Double-Tagging.

Paso 1

El atacante envía una trama 802.1Q con doble etiqueta (double tag) al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal. Para fines de este ejemplo, supongamos que es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.

Paso 2



Paso 3



Un ataque de VLAN Double-tagging es unicast, y funciona unidireccional, y funciona cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal. La idea es que el doble etiquetado permite al atacante enviar datos a hosts o servidores en una VLAN que de otro modo se bloquearía por algún tipo de configuración de control de acceso. Presumiblemente, también se permitirá el tráfico de retorno, lo que le dará al atacante la capacidad de comunicarse con los dispositivos en la VLAN normalmente bloqueada.

Mitigación de Ataques a VLAN

Los ataques de VLAN hopping y VLAN Double-Tagging se pueden evitar mediante la implementación de las siguientes pautas de seguridad troncal, como se discutió previamente en este módulo:

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

10.5.4 Mensajes DHCP

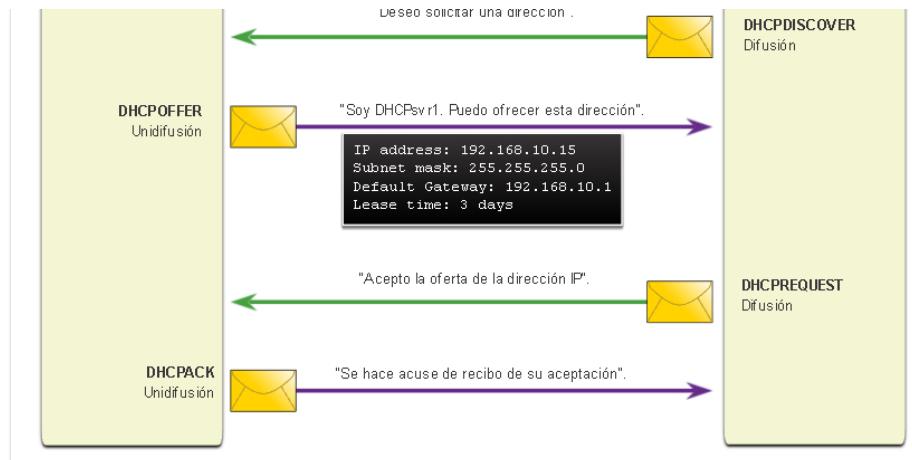
Los servidores DHCP, de manera dinámica, proporcionan información de configuración de IP a los clientes, como la dirección IP, la máscara de subred, el gateway predeterminado, los servidores DNS y más. Una revisión de la secuencia típica de un intercambio de mensajes DHCP entre el cliente y el servidor es mostrada en la figura.



Servidor



Cliente



Ataques de 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 un ataque de agotamiento DHCP es crear un DoS para la conexión de 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 DISCOVER con una dirección MAC falsa.

Ataque de Suplantación DHCP

Un ataque de suplantación DHCP se produce cuando un servidor DHCP no autorizado se conecta a la red y brinda parámetros de configuración IP falsos a los clientes legítimos. Un servidor no autorizado puede proporcionar una variedad de información engañosa:

- **Puerta de enlace predeterminada incorrecta** - el atacante proporciona una puerta de enlace no válida o la dirección IP de su host para crear un ataque de MITM. Esto puede pasar totalmente inadvertido, ya que el intruso intercepta el flujo de datos por la red.
- **Servidor DNS incorrecto** el atacante proporciona una dirección del servidor DNS incorrecta que dirige al usuario a un sitio web malicioso.
- **Dirección IP incorrecta** - El servidor no autorizado proporciona una dirección IP no válida que crea efectivamente un ataque DoS en el cliente DHCP

Haga clic en cada paso para ver un ejemplo y una explicación de un ataque de suplantación de identidad de DHCP

Paso 1

El atacante se conecta a un servidor DHCP dudoso.

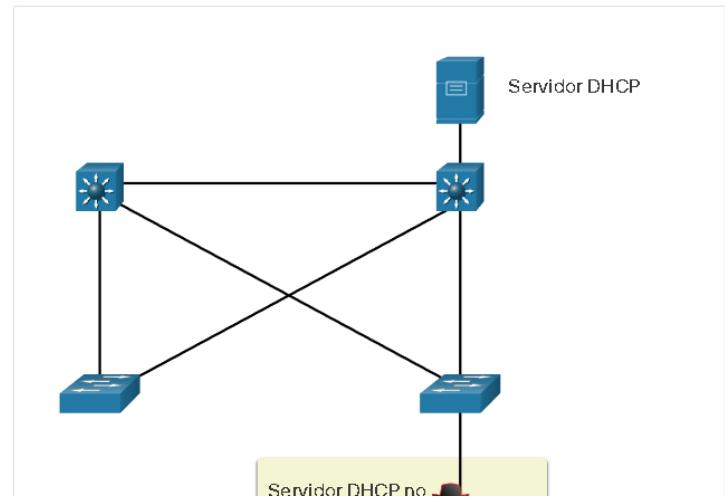
Paso 2

Supongamos que un atacante conecta con éxito un servidor DHCP no autorizado a un puerto de switch en la misma subred que los clientes. El objetivo del servidor no autorizado es proporcionar a los clientes información de configuración de IP falsa.

Paso 3

Paso 4

Paso 5





10.5.6

Video- Ataques ARP, Ataques STP, y Reconocimiento CDP.

Haga clic en reproducir en la figura para ver un video sobre ataques de denegación de servicio.

Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

This video will cover the following:

- ARP Spoofing Attack
- ARP Poisoning Attack
- STP Attack
- CDP Reconnaissance



10.5.7

Ataques ARP

Recuerde que los hosts transmiten una solicitud de ARP a otros hosts del segmento para determinar la dirección MAC de un host con una dirección IP específica. Esto es típicamente hecho para descubrir la dirección MAC de una puerta de enlace predeterminada. Todos los hosts de la subred reciben y procesan la solicitud de ARP. El host con la dirección IP que coincide con la de la solicitud de ARP envía una respuesta de ARP.

Según ARP RFC, cualquier cliente puede enviar una respuesta de ARP no solicitada llamada “ARP gratuito”. Cuando un host envía un ARP gratuito, otros hosts en la subred almacenan en sus tablas de ARP la dirección MAC y la dirección IP que contiene dicho ARP.

El problema es que un atacante puede enviar un mensaje ARP gratuito al switch y el switch podría actualizar su tabla MAC de acuerdo a esto. Por lo tanto, cualquier host puede reclamar ser el dueño de cualquier combinación de dirección IP Y MAC que ellos elijan. En un ataque típico el atacante puede enviar respuestas ARP, no solicitadas, a otros hosts en la subred con la dirección MAC del atacante y la dirección IP de la puerta de enlace predeterminada.

Hay muchas herramientas disponibles en Internet para crear ataques de MITM de ARP, como dsniff, Cain & Abel, ettercap y Yersinia. IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de Capa 2. IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de capa 2.

La suplantación de identidad ARP y el envenenamiento ARP son mitigados implementando DAI.



Haga clic en cada paso para ver un ejemplo y una explicación de un ataque de suplantación de identidad de DHCP

Paso 1

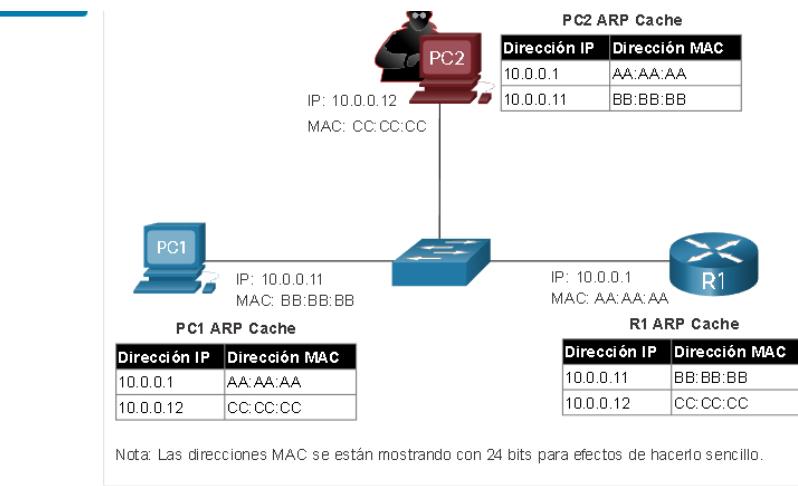
Estado normal con una tabla MAC convergida.

Paso 2

Cada dispositivo tiene una tabla MAC actualizada con la dirección IP y MAC correctas de cada dispositivo en la red.

Paso 3





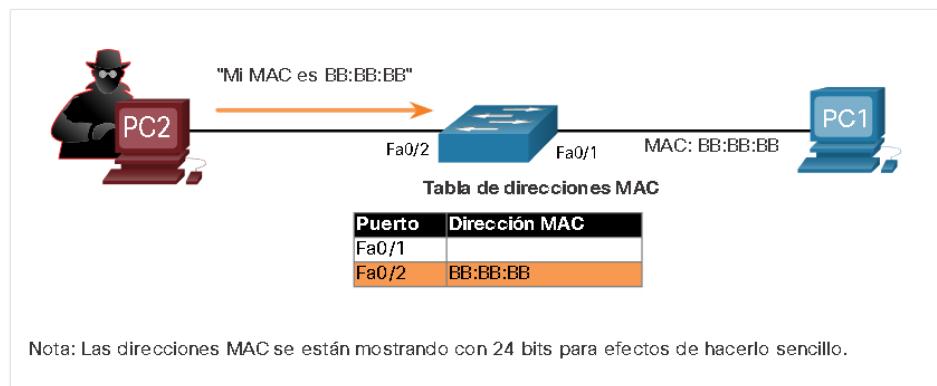
10.5.8

Ataque de Suplantación de Dirección



Las direcciones IP y las direcciones MAC pueden ser suplantadas por una cantidad de razones. El ataque de suplantación de identidad se da cuando un atacante secuestra una dirección IP válida de otro dispositivo en la subred o usa una dirección IP al azar. La suplantación de direcciones IP es difícil de mitigar, especialmente cuando se usa dentro de una subred a la que pertenece la IP.

Los atacantes cambian la dirección MAC de su host para que coincida con la dirección MAC conocida de un otro host objetivo. Luego, el host atacante envía una trama a través de la red con la dirección MAC recién configurada. Cuando el switch recibe la trama, examina la dirección MAC de origen. El switch sobrescribe la entrada actual en la tabla MAC y asigna la dirección MAC al nuevo puerto, como se ve en la figura. Luego, sin darse cuenta, reenvía las tramas host atacante.



Cuando el host de destino envía tráfico, el switch corregirá el error, re-alineando la dirección MAC al puerto original. Para evitar que el switch corrija la asignación del puerto a su estado correcto, el atacante puede crear un programa o script que constantemente enviará tramas al switch, para que el switch mantenga la información incorrecta o falsificada. No hay un mecanismo de seguridad en la Capa 2 que permita a un switch verificar la fuente de las direcciones MAC, lo que lo hace tan vulnerable a la suplantación de identidad.

La suplantación de identidad de direcciones IP y direcciones MAC puede ser mitigada implementando IPSG.

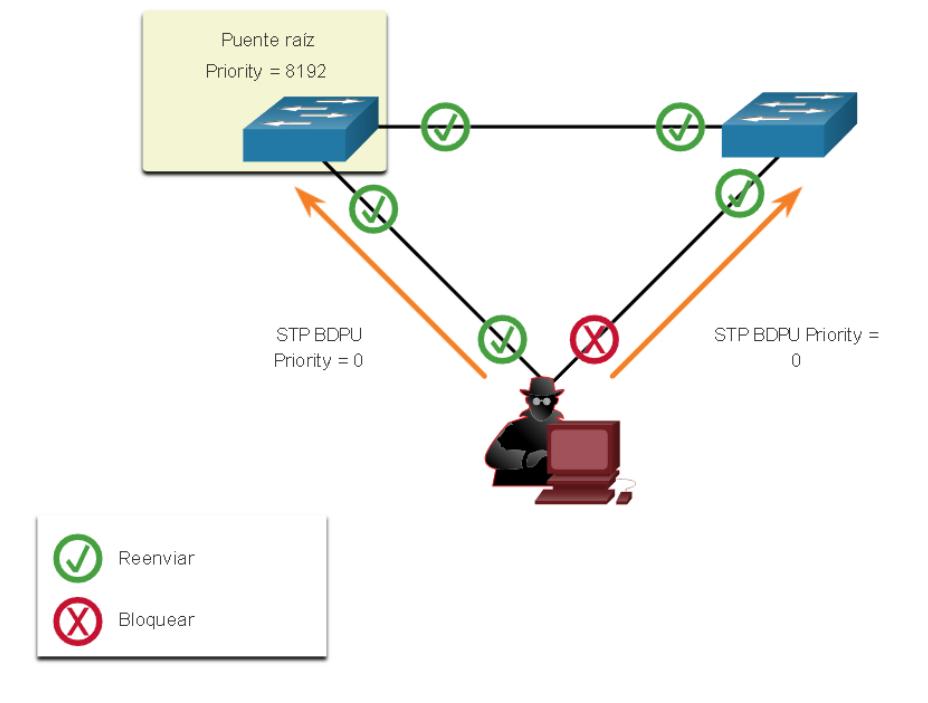
10.5.9

Ataque de STP

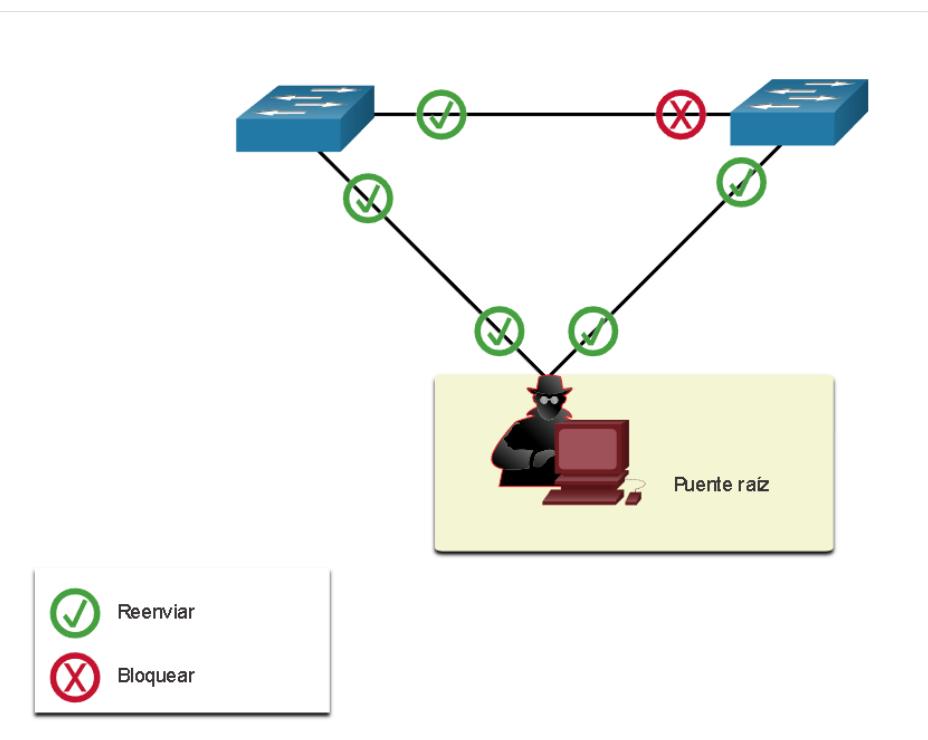


Los atacantes de red pueden manipular el Protocolo de Árbol de Expansión (STP) para realizar un ataque falsificando el root bridge y cambiando la topología de una red. Los atacantes hacen que su host parezca ser un root bridge; por lo tanto capturan todo el tráfico para el dominio del Switch inmediato.

Para realizar un ataque de manipulación de STP, el host atacante transmite Unidades de Datos de Protocolo de Puente STP (BPDU), que contienen cambios de configuración y topología que forzarán los re-cálculos de Árbol de Expansión, como se muestra en la figura. Las BPDU enviadas por el host atacante anuncian una prioridad de puente (bridge) inferior, en un intento de ser elegidas como root bridge.



Si tiene éxito, el host atacante se convierte en el puente raíz, como se muestra en la figura, y ahora puede capturar una variedad de frames, que de otro modo no serían accesibles.



Este ataque STP es mitigado implementando BPDU Guard en todos los puertos de acceso. BPDU Guard se discute con detalle más adelante en el curso.

10.5.10

Reconocimiento CDP



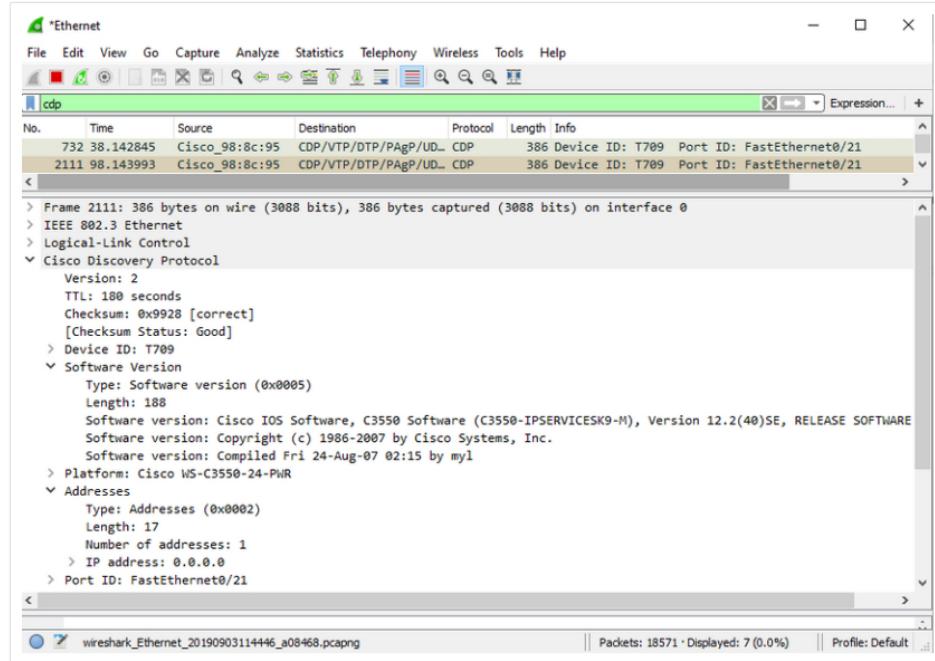
Cisco Discovery Protocol (CDP) es un protocolo de detección de enlaces de Capa 2 patentado. Está habilitado en todos los dispositivos de Cisco de manera predeterminada. CDP puede detectar automáticamente otros dispositivos con CDP habilitado y ayudar a configurar automáticamente la conexión. Los administradores de red también usan CDP para configurar dispositivos de red y solucionar problemas.

La información de CDP se envía por los puertos con CDP habilitado en transmisiones periódicas sin encriptar. La información de CDP incluye la dirección IP del dispositivo, la versión de software de IOS, la plataforma, las funcionalidades y la VLAN nativa. El dispositivo que recibe el mensaje de CDP actualiza la base de datos de CDP.

La información de CDP es muy útil para la solución de problemas de red. Por ejemplo, CDP puede usarse para verificar la conectividad de Capa 1 y 2. Si un administrador no puede hacer ping a una interfaz con conexión directa, pero aún recibe información de CDP, es probable que el problema esté en la configuración de Capa 3.

Sin embargo, un atacante puede usar la información proporcionada por CDP para detectar vulnerabilidades en la infraestructura de red.

En la figura, una captura de Wireshark de ejemplo, muestra el contenido de un paquete de CDP. El atacante puede identificar la versión del software Cisco IOS del dispositivo. Esto permite que el atacante determine si hay vulnerabilidades de seguridad específicas a esa versión determinada de IOS.



Las transmisiones de CDP se envían sin encriptación ni autenticación. Por lo tanto, un atacante puede interferir con la infraestructura de la red enviando tramas de CDP fabricadas con información falsa a dispositivos de Cisco con conexión directa.

Para mitigar la explotación de CDP, se debe limitar el uso de CDP en los dispositivos o puertos. Por ejemplo, se debe deshabilitar CDP en los puertos de extremo que se conectan a dispositivos no confiables.

Para deshabilitar CDP globalmente en un dispositivo, use el comando del modo de configuración global **no cdp run**. Para habilitar CDP globalmente, use el comando de configuración global **cdp run**.

Para deshabilitar CDP en un puerto, use el comando de configuración de interfaz **no cdp enable**. Para habilitar CDP en un puerto, use el comando de configuración de interfaz **cdp enable**.

Nota: El Protocolo de detección de capa de enlace (LLDP) también es vulnerable a los ataques de reconocimiento. Configure **no lldp run** para deshabilitar LLDP globalmente. Para deshabilitar LLDP en la interfaz, configure **no lldp transmit** y **no lldp receive**.

10.5.11

Verifique su comprensión - Ataques LAN



Elija la MEJOR respuesta para las siguientes preguntas y compruebe su conocimiento sobre ataques LAN.

1. Un atacante cambia la dirección MAC de su dispositivo por la dirección MAC de la puerta de enlace predeterminada. ¿Qué tipo de ataque es este?

¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

2. El atacante envía un mensaje de BPDU con prioridad 0. ¿Qué tipo de ataque es este?

 ¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

3. Un actor de amenaza solicita todas las direcciones IP disponibles en una subred. ¿Qué tipo de ataque es este?

 ¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

4. Un atacante envía un mensaje que causa que todos los otros dispositivos crean que la dirección MAC del atacante es la puerta de enlace predeterminada. ¿Qué tipo de ataque es este?

 ¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

5. Un atacante configura un host con el protocolo 802.1Q y forma un enlace troncal con el switch que tiene conectado. ¿Qué tipo de ataque es este?

 ¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

6. Un amenazante descubre la versión de IOS y la dirección IP de Switch local. ¿Qué tipo de ataque es este?

 ¡Lo tienes!

- Suplantación de direcciones
- Suplantación ARP
- Reconocimiento CDP
- Agotamiento DHCP
- Ataque de STP
- VLAN Hopping

Verificar

Mostrar

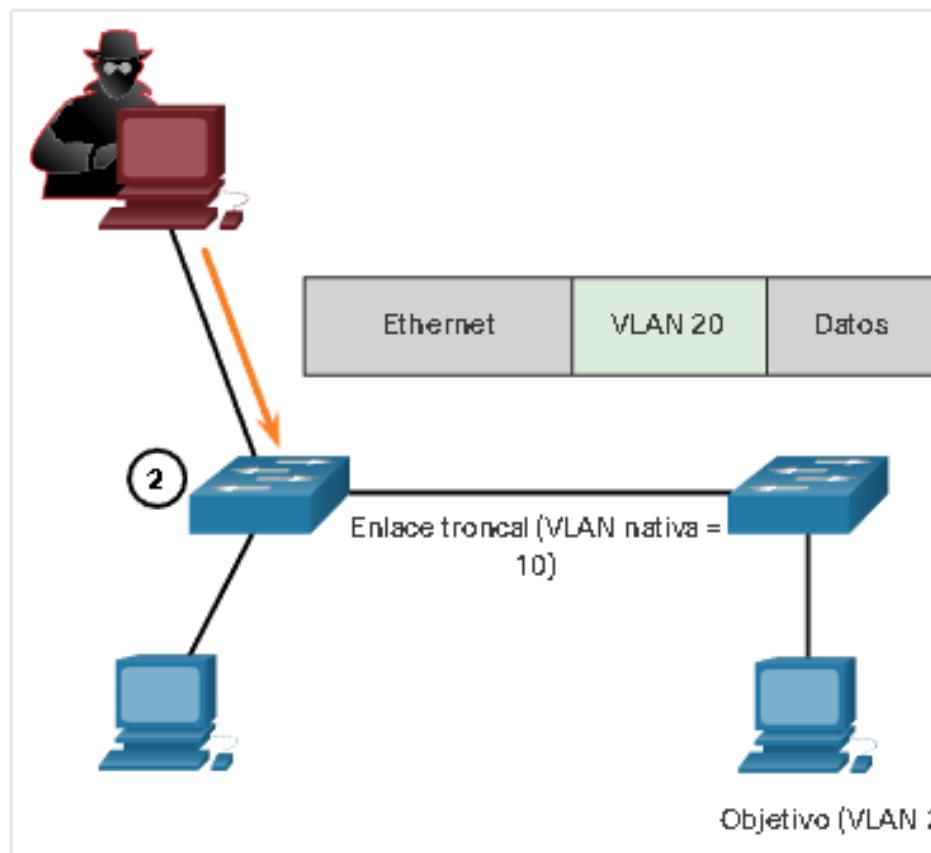
Restablecer

Paso 1

El frame llega al primer switch, que mira la primera etiqueta 802.1Q de 4 bytes. El switch ve que la trama está destinada para la VLAN 10, la cual es una VLAN nativa. El switch reenvía el paquete a todos los puertos de VLAN 10, después de quitar la etiqueta de VLAN 10. La trama no es re-etiquetada porque es parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 todavía está intacta y no ha sido inspeccionada por el primer switch.

Paso 2

Paso 3





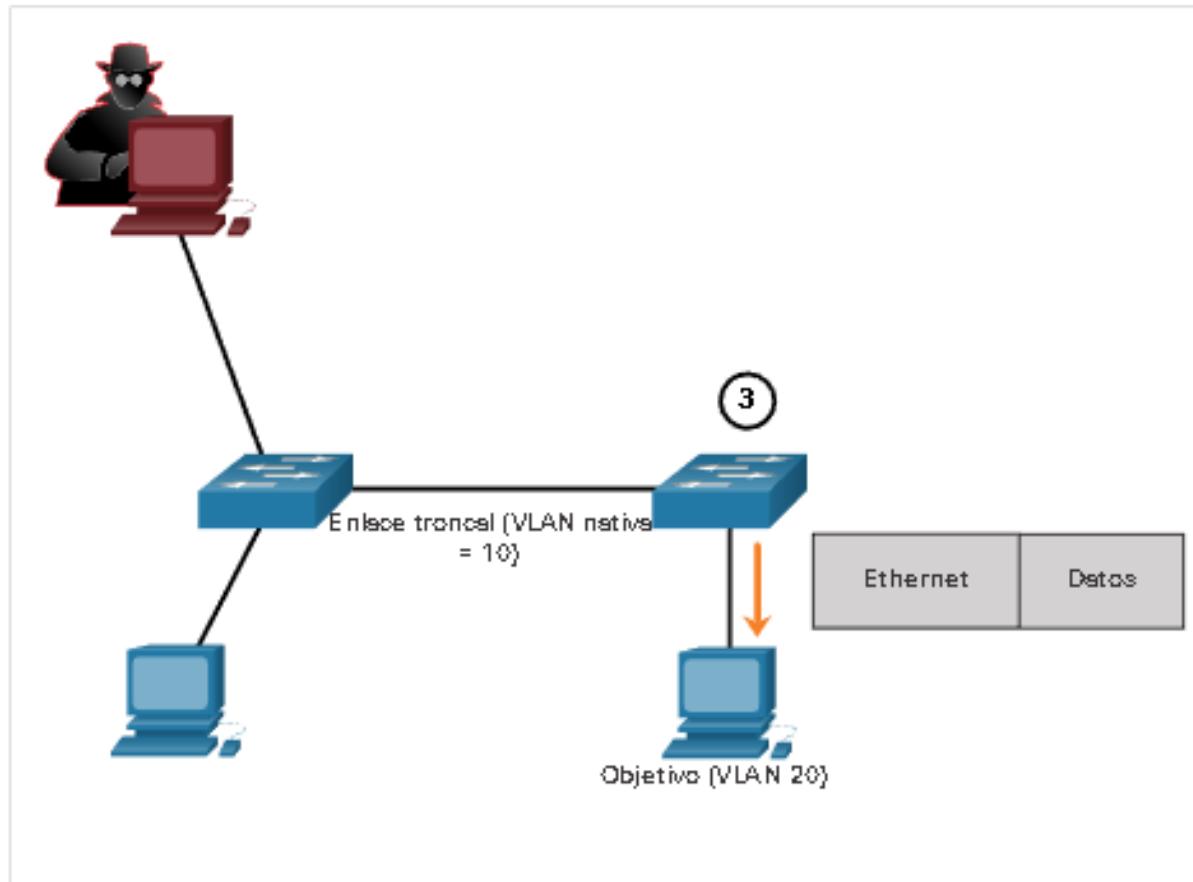
Haga clic en cada paso para ver un ejemplo y una explicación de un ataque de VLAN Double-Tagging.

Paso 1

La trama llega al segundo switch, que no tiene conocimiento de que debia ser para la VLAN 10. El switch emisor no etiqueta el tráfico de la VLAN nativa, como se especifica en la especificación 802.1Q. El segundo switch observa solo la etiqueta interna 802.1Q, que el atacante insertó, y ve que la trama está destinada a la VLAN 20 (la VLAN víctima). 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.

Paso 2

Paso 3



Paso 1

El cliente transmite mensajes DHCP DISCOVER, tipo broadcast

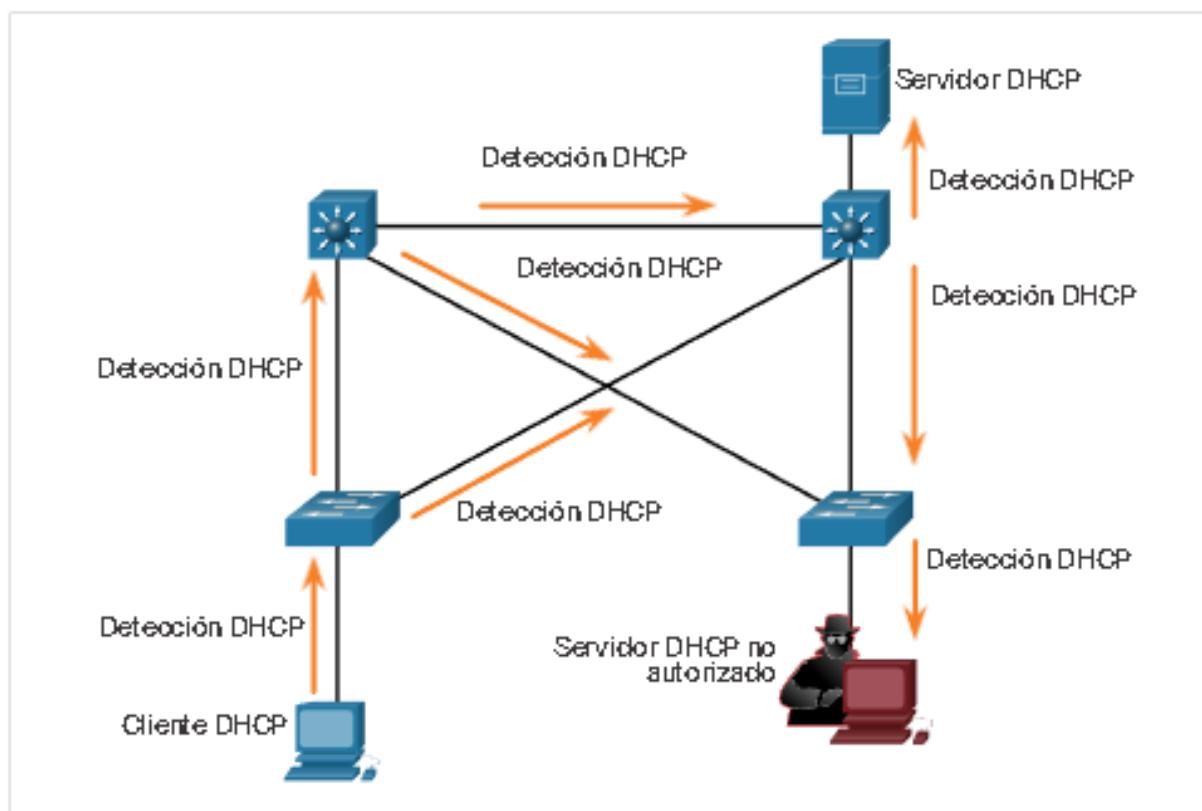
Paso 2

Un cliente legítimo se conecta a la red y requiere parámetros de configuración de IP. Por lo tanto, el cliente emite un DHCP DISCOVER, tipo broadcast, en búsqueda de una respuesta de un servidor DHCP. Ambos servidores recibirán el mensaje y responden.

Paso 3

Paso 4

Paso 5



Paso 1

Respuesta DHCP legítima y no autorizada

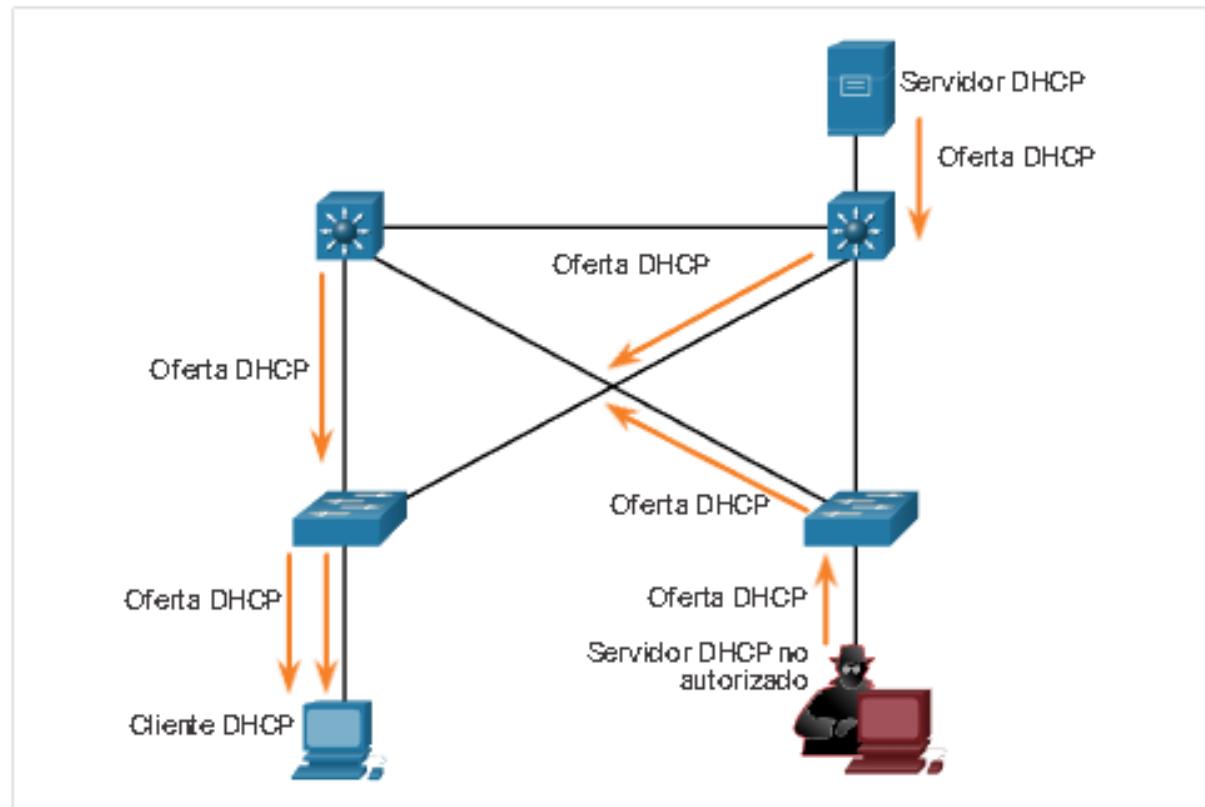
Paso 2

El servidor DHCP legítimo responde con parámetros de configuración de IP válidos. Sin embargo, el servidor no autorizado también responde con una oferta DHCP, la cual contiene parámetros de configuración IP definidos por el atacante. El cliente responderá a la primera oferta recibida.

Paso 3

Paso 4

Paso 5



Paso 1

Paso 2

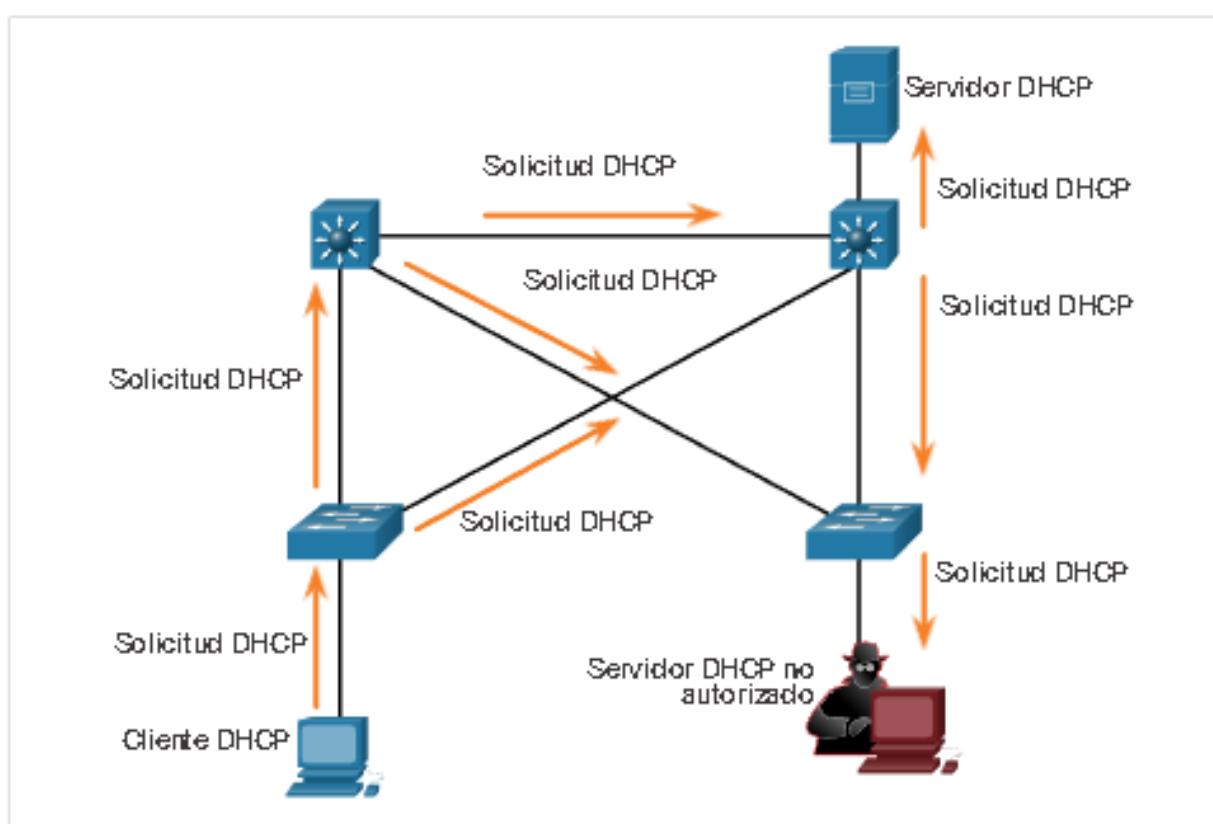
Paso 3

Paso 4

Paso 5

El cliente acepta la oferta del servidor DHCP no autorizado

La oferta maliciosa fue recibida primero, y por lo tanto, el cliente hace envía un DHCP REQUEST, tipo broadcast, aceptando los parámetros IP definidos por el atacante. El servidor legítimo y el dudoso recibirán la solicitud.



Paso 1

El servidor malicioso confirma que recibió la solicitud

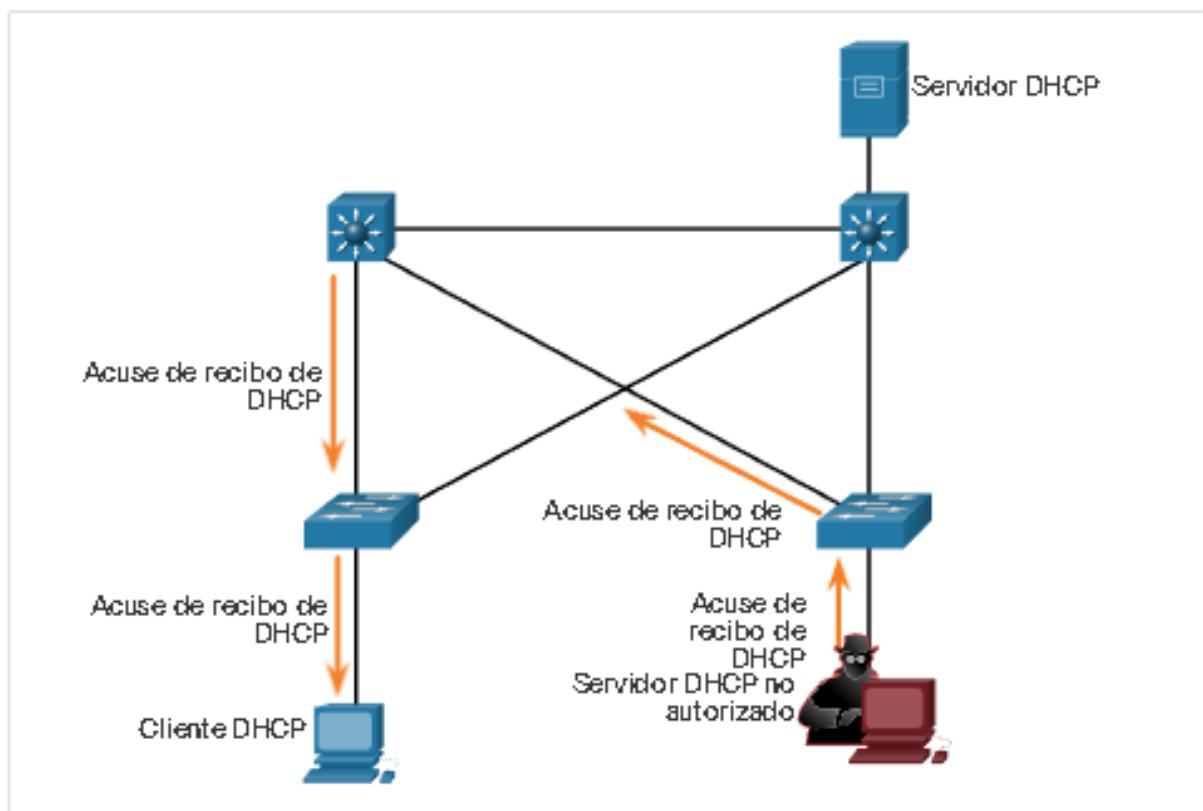
Paso 2

Solamente el servidor no autorizado emite una respuesta individual al cliente para acusar recibo de su solicitud. El servidor legítimo dejará de comunicarse con el cliente.

Paso 3

Paso 4

Paso 5



Paso 1

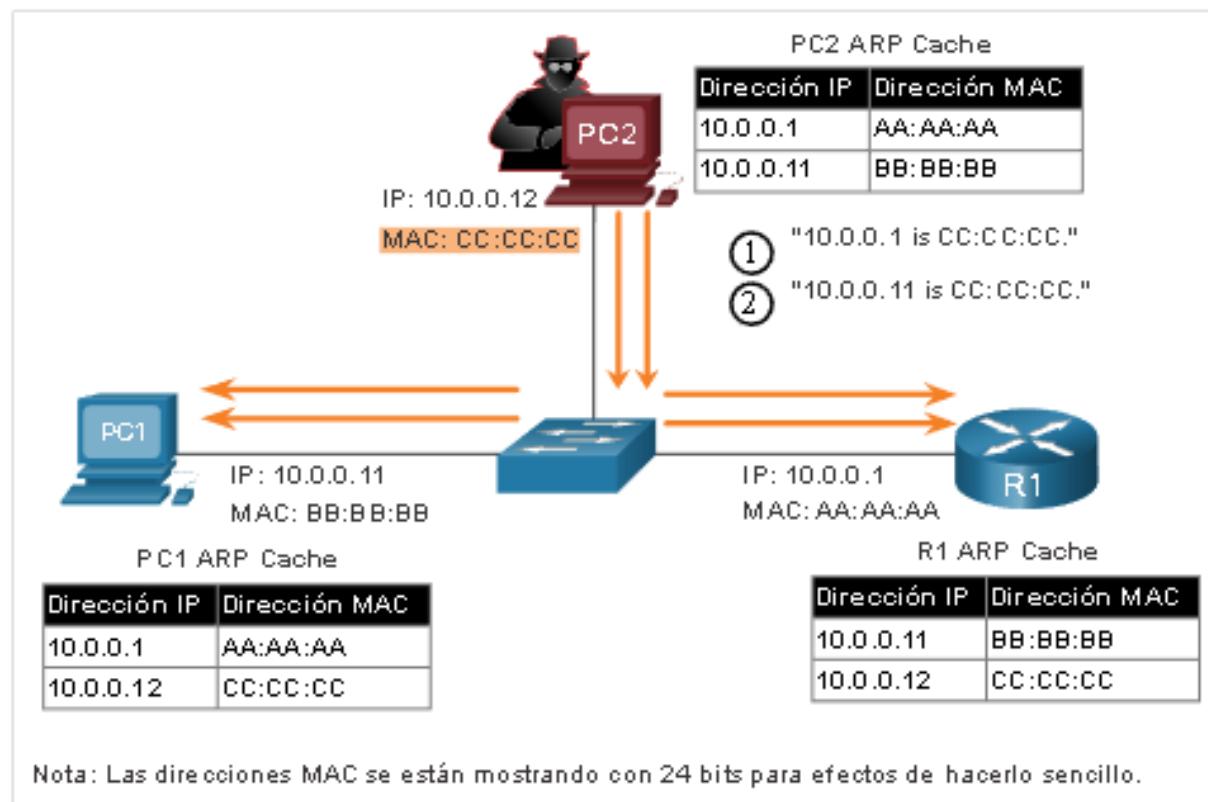
Ataque por Suplantación de ARP

Paso 2

El atacante envía dos respuestas gratuitas falsas en un intento de reemplazar R1 como la puerta de enlace predeterminada.

Paso 3

1. En el primero ARP informa todos los dispositivos en la LAN que la dirección MAC del atacante (CC:CC:CC) está mapeado a la dirección IP de la PC1, 10.0.0.11.
2. El segundo le informa a todos los dispositivos en la LAN que la dirección MAC del atacante (CC:CC:CC) está mapeado a la dirección IP de la PC1, 10.0.0.11.



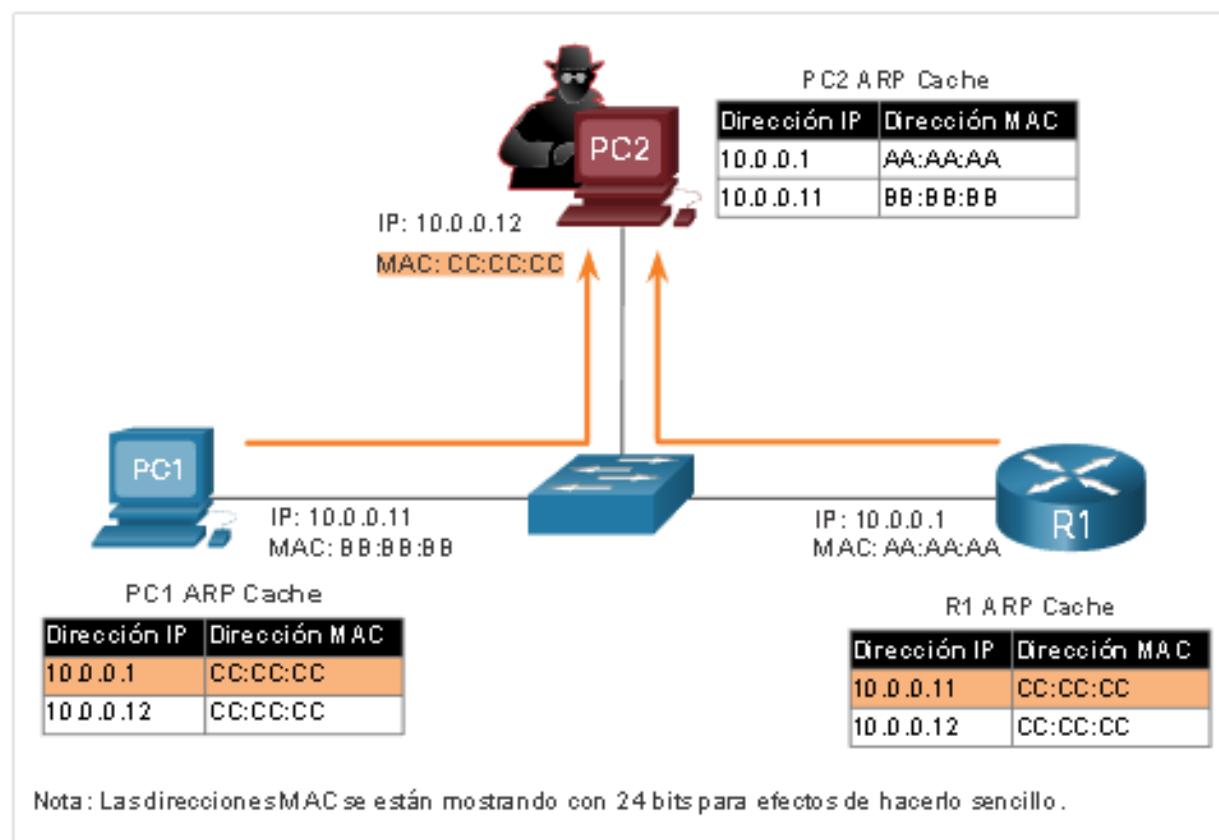
Paso 1

Ataque de envenenamiento ARP con ataque MITM.

Paso 2

R1 y PC1 remueven la entrada correcta de la dirección MAC de cada uno y la reemplaza con la dirección MAC de PC2. El atacante ha logrado envenenar la caché ARP de todos los dispositivos en la subred. El envenenamiento ARP lleva a varios ataques MITM, posando una seria amenaza de seguridad en la red.

Paso 3





Switching, Routing, y Wireless Essentials

1	Configuración básica de dispositivos
2	Conceptos de switching
3	VLANs
4	Inter-VLAN Routing
5	STP Concepts
6	EtherChannel
7	DHCPv4
8	SLAAC y DHCPv6
9	Conceptos de FHRP
10	Conceptos de Seguridad de LAN
10.0	Introducción
10.1	Seguridad de Punto Terminal
10.2	Control de Acceso
10.2.1	Autenticación con una contraseña local
10.2.2	Componentes AAA
10.2.3	Autenticación
10.2.4	Autorización
10.2.5	Registro
10.2.6	802.1x
10.2.7	Verifique su comprensión: Control de Acceso
10.3	Amenazas a la seguridad de Capa 2
10.3.1	Capa 2 Vulnerabilidades
10.3.2	Categorías de Ataques a Switches
10.3.3	Técnicas de Mitigación en el Switch
10.3.4	Ponga a prueba su conocimiento: Amenazas de Seguridad de Capa 2
10.4	Ataque de Tablas de Direcciones MAC
10.4.1	Revisar la Operación del Switch
	Saturación de Tablas de

Práctica del Módulo y Cuestionario

10.6.1

¿Qué aprendí en este módulo?



Los punto terminales son particularmente susceptibles a ataques malware que se originan a través de correo electrónico o el navegador web, como DDOS, filtración de datos y malware. Estos puntos terminales suelen utilizar características de seguridad tradicionales basadas en host, como antivirus/antimalware, firewalls basados en host y sistemas de prevención de intrusiones (HIPSs) basados en host. Los puntos terminales están mejor protegidos por una combinación de NAC, software AMP basado en host, un dispositivo de seguridad de correo electrónico (ESA) y un dispositivo de seguridad web (WSA). La WSA puede realizar listas negras de URL, filtrado de URL, escaneo de malware, categorización de URL, filtrado de aplicaciones web y cifrado y descifrado del tráfico web.

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 (registrar). La autorización utiliza un conjunto de atributos que describe el acceso del usuario a la red. Un uso muy implementado del Registro es en combinación con la Autenticación AAA. Los servidores AAA mantienen un registro detallado de lo que el usuario autenticado hace exactamente en el dispositivo. 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.

Si la Capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. 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: Port Security, DHCP snooping, DAI, y IPSG. Estos no van a funcionar a menos que los protocolos de administración sean seguros.

Los ataques por saturación de MAC, saturan la tabla de direcciones MAC del switch, con información falsa, hasta que este llena. Cuando esto ocurre, el switch trata la trama como un unic平 desconocido, y comienza a reenviar todo el tráfico entrante por todos los puertos en la misma VLAN, sin hacer referencia a la tabla MAC. El atacante puede ahora capturar todas las tramas enviadas desde un host para otro host en una LAN o VLAN local. El atacante usa **macof** para rápidamente generar, de manera aleatoria, muchas direcciones MAC y IP de origen y destino. Para mitigar los ataques de saturación de la tabla de direcciones MAC, los administradores de red deben implementar la seguridad del puerto.

El VLAN Hopping permite que una VLAN pueda ver el tráfico de otra VLAN sin cruzar primero un router. El atacante configura a un host para actuar como un Switch y tomar ventaja de la característica de puerto troncal habitabilidad por defecto en la mayoría de puertos del switch

Un ataque VLAN Double-Tagging 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 Double-Tagging permite al actor de la amenaza enviar datos a los hosts o servidores en una VLAN que de otro modo se bloquearía por algún tipo de configuración de control de acceso. El tráfico de retorno también será permitido, dejando que el atacante se comunique con otros dispositivos en la VLAN normalmente bloqueada.

Los ataques de VLAN hopping and VLAN double-tagging 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.
- Asegurarse de que la VLAN nativa solo se usa para los enlaces troncales.

Los servidores DHCP, de manera dinámica, proporcionan la información de configuración de IP a los clientes, como la dirección IP, la máscara de subred, el default gateway, los servidores DNS y más. Los dos tipos de ataques DHCP son agotamiento y suplantación de identidad. Ambos ataques pueden ser mitigados implementando DHCP snooping.

Ataque ARP: un atacante puede enviar un mensaje ARP gratuito al switch y el switch podría actualizar su tabla MAC de acuerdo a esto. Ahora el atacante envía respuestas ARP no solicitadas a otros hosts en la subred con la dirección MAC del actor amenazante y la dirección IP del default gateway. La suplantación de identidad ARP y el envenenamiento ARP son mitigados implementando DAI.

Ataque de suplantación de direcciones: la suplantación de identidad de una dirección IP es cuando un atacante secuestra una dirección IP válida de otro dispositivo en la subred o usa una dirección IP al azar. Los atacantes cambian la dirección MAC de su host para que coincida con otra dirección MAC conocida de un host de destino. La suplantación de identidad de direcciones IP y direcciones MAC puede ser mitigada implementando IPSG.

Ataque STP: el amenazante manipula STP para conducir un ataque suplantando root bridge y cambiando la topología de la red. Los atacantes hacen que su host aparezca como un root bridge; por lo tanto capturan todo el tráfico para el dominio del switch inmediato. Este ataque STP es mitigado implementando BPDU guard en todos los puertos de acceso.

La información de CDP se envía por los puertos con CDP habilitado en transmisiones periódicas sin encriptar. La información de CDP incluye la dirección IP del dispositivo, la versión de software de IOS, la plataforma, las funcionalidades y la VLAN nativa. El dispositivo que recibe el mensaje CDP actualiza su base de datos CDP, la información suministrada por el CDP puede también ser usada por un atacante para describir vulnerabilidades en la infraestructura de la red. Para mitigar la explotación de CDP, se debe limitar el uso de CDP en los dispositivos o puertos.

10.4.2	Saturación de Tablas de Direcciones MAC
10.4.3	Mitigación de Ataques a la Tabla de Direcciones MAC.
10.4.4	Verifica tu entendimiento- Ataques a Tablas de Direcciones MAC.
10.5	Ataques a la LAN
10.5.1	Video - VLAN y Ataques DHCP
10.5.2	Ataque de VLAN Hopping
10.5.3	Ataque de VLAN Double-Tagging
10.5.4	Mensajes DHCP
10.5.5	Ataques de DHCP
10.5.6	Video- Ataques ARP, Ataques STP, y Reconocimiento CDP.
10.5.7	Ataques ARP
10.5.8	Ataque de Suplantación de Dirección
10.5.9	Ataque de STP
10.5.10	Reconocimiento CDP
10.5.11	Verifique su comprensión - Ataques LAN
10.6	Práctica del Módulo y Cuestionario
10.6.1	¿Qué aprendí en este módulo?
10.6.2	Módulo Quiz: Conceptos de Seguridad de LAN
11	Configuraciones de seguridad del Switch
12	Conceptos WLAN
13	Configuraciones de redes inalámbricas WLAN
14	Conceptos de enrutamiento
15	Rutas IP estáticas
16	Resuelva problemas de rutas estáticas y predeterminadas

10.6.2

Módulo Quiz: Conceptos de Seguridad de LAN

1. ¿Cuáles son los dos protocolos que admiten los dispositivos de Cisco para comunicaciones AAA? (Elija dos opciones).

Tema 10.2.0 - Los dispositivos de Cisco admiten dos protocolos AAA: TACACS+ y RADIUS. El protocolo de router de reserva activa (HSRP) se utiliza en los routers de Cisco para permitir redundancia de gateway. El protocolo de detección de capa de enlace (LLDP) es un protocolo para la detección de vecinos. El protocolo de enlace troncal VLAN (VTP) se utiliza en switches de Cisco para administrar las redes VLAN en un switch de servidor con VTP activado.

VTP
 LLDP
 HSRP
 TACACS
 RADIUS

2. ¿Qué servicio habilitado de manera predeterminada en los routers de Cisco puede revelar información importante sobre el router y hacerlo quizás más vulnerable a los ataques?

Tema 10.5.0 - CDP es un protocolo patentado de Cisco que recopila información de otros dispositivos de Cisco conectados. Está habilitado de manera predeterminada en los dispositivos de Cisco. LLDP es un protocolo de estándar abierto que presta el mismo servicio. Puede habilitarse en un router de Cisco. HTTP y FTP son protocolos de capa de aplicaciones que no recopilan información sobre los dispositivos de red.

CDP
 HTTP
 FTP
 LLDP

3. ¿Cuándo la seguridad es una preocupación, ¿cuál capa OSI es considerada el enlace más débil en un sistema de redes?

Tema 10.3.0 - La seguridad es solamente tan sólida como el enlace más débil en el sistema, y la capa 2 es considerado el enlace más débil. Además de proteger de la capa 3 a la capa 7, los profesionales de seguridad de red también deben mitigar los ataques a la infraestructura LAN de la capa 2.

Capa 3
 Capa 2
 Capa 7
 Capa 4

4. ¿Cuál ataque de Capa 2 resultara en el switch reenviando todas las tramas hacia todos los puertos?

Tema 10.4.0 - Cuando un atacante envía rápidamente las tramas con las direcciones MAC suplantadas a un switch, la tabla de direcciones MAC del switch se llena. Una vez que la tabla de direcciones MAC del switch está llena, el switch inundará todas las nuevas tramas entrantes a todos los puertos.

Envenenamiento ARP
 Suplantación de dirección IP
 Manipulación del Protocolo Árbol de Expansión
 Saturación de direcciones MAC

5. ¿Por qué se prefiere la autenticación con AAA sobre un método de base de datos local?

Tema 10.2.0 - El método de autenticación de la base de datos local no proporciona un método de autenticación de reserva si un administrador olvida el nombre de usuario o la contraseña. La recuperación de contraseña será la única opción. Cuando se usa la autenticación con AAA, se puede configurar un método alternativo para permitir que un administrador use uno de los muchos métodos posibles de autenticación de respaldo.

- Utiliza menos ancho de banda de red.
- Especifica una contraseña diferente para cada línea o puerto.
- Proporciona un método de autenticación alternativa si el administrador olvida el nombre de usuario o la contraseña.
- Requiere una combinación de inicio de sesión y contraseña en la consola, líneas vty y puertos auxiliares.

6. Implementación basada en un servidor AAA, ¿Cuál protocolo le permitirá al router comunicarse de manera exitosa con el servidor AAA?

Tema 10.2.0 - Con un método basado en servidor, el router accede a un servidor AAA central usando el protocolo del usuario de acceso telefónico de autenticación remota (RADIUS) o del sistema de control de acceso del controlador de acceso de terminal (TACACS+). SSH es un protocolo utilizado para el inicio de sesión remoto. 802.1x es un protocolo utilizado en la autenticación basada en puerto. TACACS es un protocolo heredado y ya no se utiliza.

- RADIUS
- SSH
- Un ataque de suplantación de DHCP se produce cuando un servidor DHCP no autorizado se conecta a la red y brinda parámetros de configuración IP falsos a los clientes legítimos.
- 802.1x

7. ¿Cuál solución Cisco ayuda a prevenir ataques de suplantación de identidad de direcciones IP y MAC?

Tema 10.3.0 - CISCO proporciona soluciones para ayudar a mitigar los ataques de la capa 2 incluyendo:

- La protección de IP de origen (IPSG) - impide los ataques de suplantación de direcciones MAC e IP.
- La inspección dinámica de ARP (DAI) - evita la suplantación de ARP y los ataques de envenenamiento de ARP.
- La detección DHCP - impide el agotamiento de direcciones DHCP y los ataques de suplantación de DHCP.
- La seguridad de puertos - evita muchos tipos de ataques, incluidos los ataques de sobrecarga de la tabla CAM y agotamiento de direcciones DHCP

- Detección DHCP
- Seguridad de puertos
- Protección de la IP de origen
- Inspección dinámica de ARP

8. ¿Cuál es el propósito del Registro AAA?

Tema 10.2.0 - La auditoría AAA recopila e informa los datos de uso de la aplicación. La organización puede utilizar estos datos para fines como auditorías o facturación. La autenticación AAA es el proceso de verificar que los usuarios son quienes dicen ser. La autorización AAA es lo que los usuarios pueden y no pueden hacer en la red después de que se autentiquen.

- Determinar a qué recursos puede acceder un usuario.
- Recolectar y reportar el uso de la aplicación.
- Autorización
- Autenticación

9. ¿Cuáles ataques a Capa 2 tendrán como resultado que los usuarios legítimos no obtengan direcciones IP validas?

Tema 10.5.0 - El ataque de agotamiento DHCP causa el agotamiento del grupo de direcciones IP de un servidor DHCP antes de que los usuarios legítimos puedan obtener direcciones IP válidas.

- Saturación de direcciones MAC
- Agotamiento DHCP
- Suplantación ARP
- Suplantación de dirección IP

10. ¿Qué tres productos de Cisco se centran en soluciones de seguridad de punto terminal? (Escoja tres opciones).

Tema 10.1.0 - Los componentes principales de las soluciones

de seguridad de punto final son los dispositivos de correo electrónico y seguridad web de CISCO, y el dispositivo CISCO NAC. Los dispositivos de sensores ASA, SSL / IPsec VPN y IPS proporcionan soluciones de seguridad que se centran en la red empresarial, no en dispositivos de punto terminal.

- NAC Appliance
- Adaptive Security Appliance
- Dispositivo de Seguridad Web (WSA)
- Dispositivo Sensor IPS
- Dispositivo de seguridad de correo electrónico (ESA)
- Dispositivo VPN SSL / IPsec

11. ¿Verdadero o Falso? En el estándar 802.1X, el cliente que intenta acceder a la red se conoce como suplicante.

Tema 10.2.0 - Según la terminología de 802.1X, la estación de trabajo del cliente se conoce como suplicante.

- Falso
- Verdadero

12. ¿Qué está involucrado en un ataque de suplantación de identidad a una dirección IP?

Tema 10.5.0 - En un ataque de suplantación de dirección IP, la dirección IP de un host de red legítimo es secuestrada y utilizada por un nodo no autorizado. Esto permite que el nodo no autorizado se haga pasar por un nodo válido en la red.

- Una dirección IP legítima de una red es secuestrada por un nodo no autorizado.
- Un nodo deshonesto responde a una solicitud ARP con su propia dirección MAC indicada por la dirección IP objetivo.
- Un ataque de suplantación de DHCP se produce cuando un servidor DHCP no autorizado se conecta a la red y brinda parámetros de configuración IP falsos a los clientes legítimos.
- Un mensaje DHCP falso es enviado para consumir todas las direcciones IP disponibles en el servidor DHCP.

13. ¿Cuáles son los tres servicios proporcionados por el marco de AAA? (Elija tres opciones).

Tema 10.2.0 - El marco de autenticación, autorización y contabilidad (AAA) presta servicios de protección de acceso a dispositivos de red.

- Automatización
- Autorización
- autobalancing
- autoconfiguración
- Autenticación
- Registro

14. Debido a los controles de seguridad implementados, un usuario solo puede acceder a un servidor con FTP. ¿Qué componente de AAA logra esto?

Tema 10.2.0 - Uno de los componentes de AAA es la Autorización. Una vez que se autentica usuario a través de AAA, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones tiene permitido realizar.

- Accesibilidad
- Autenticación
- Auditoría
- Registro
- Autorización

15. ¿Qué plan de mitigación es el ideal para prevenir un ataque de DoS que genera saturación del búfer del switch?

Tema 10.3.0 - Los ataques de desbordamiento de tabla de direcciones MAC (CAM), de desbordamiento de búfer y de suplantación de dirección MAC pueden mitigarse configurando la seguridad del puerto. Por lo general, el administrador de red no deshabilita STP porque previene los bucles de Capa 2. DTP está deshabilitado para prevenir el salto de VLAN. Colocar los puertos sin usar en una VLAN sin usar mitiga la congestión ocasionada por

sin usar en una VLAN sin usar evita la conectividad cableada no autorizada.

- Habilitar la seguridad del puerto.
- Deshabilitar STP.
- Colocar los puertos sin usar en una VLAN sin usar.
- Desactivar el DTP.

[Verificar](#)

[Mostrar](#)

[Restablecer](#)

 10.5 Ataques a la LAN

11.0 Introducción 