Escuela Politécnica Superior de Jaén

Grado en Ingeniería Informática

UNIVERSIDAD DE JAÉN
Nombre del Centro

Trabajo Fin de Grado

IMPLEMENTACIÓN DE TECNOLOGÍAS DE SEGURIDAD EN REDES DE ÁREA LOCAL

Alumno: **Andrés Narváez Ortiz**

Tutor: Prof. D. Joaquín Cañada Bago
Dpto: Ingeniería de Telecomunicación

Junio, 2021

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don Joaquín Cañada Bago, tutor del Proyecto Fin de Carrera titulado: Implementación de tecnologías de seguridad en redes de área local, que presenta Andrés Narváez Ortiz, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Junio de 2021

El alumno:

Andrés Narváez Ortiz

Los tutores:

CAÑADA BAGO JOAQUIN - 25969508R

Firmado digitalmente por CAÑADA BAGO JOAQUIN - 25969508R
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-25969508R, givenName=JOAQUIN, sn=CAÑADA BAGO, cn=CAÑADA BAGO JOAQUIN - 25969508R
Fecha: 2021.06.14 12:26:31 +02'00'

Joaquín Cañada Bago

Tabla de contenidos

Capítulo 1

Introducción

Hoy en día vivimos en un mundo conectado, ya sea en el hogar, en el trabajo o en algún establecimiento público, siempre disponemos de un dispositivo conectado a una red LAN. De la misma forma, ya sea para comprar productos por internet o postear información en las redes sociales, no paramos de generar tráfico que puede ser a veces sensible y funcionar como incentivo para que una persona malintencionada intente interceptarlo.

Todo esto se agrava si hablamos de una empresa que posee información sensible de miles si no millones de usuarios. Según el periódico El Pais, cada compañía recibe en España una media de 66 ataques al año, lo que nos hace plantearnos la necesidad de mantener nuestras redes lo mas seguras posibles.

En la actualidad, existen una gran cantidad de ataques dirigidos a redes LAN que pueden poner en riesgo la seguridad de nuestra red y una gran cantidad de dichos ataques se pueden llevar a cabo sin poseer un conocimiento profundo en este ámbito que son las redes. Esto debido a que existen herramientas a las que se les puede dar un mal uso y apenas con un par de clicks, pueden llevar a cabo un ataque DoS (Denegación de Servicio) y dejar una red inutilizada. Esta manera tan sencilla de llevar a cabo ataques a nuestra red es un motivo mas por el que debemos de preocuparnos por la seguridad de las mismas.

Al igual que existen una gran cantidad de ataques a las redes LAN, también existen una gran variedad de mecanismos que nos permiten defendernos. En este documento se va a llevar a cabo un estudio de algunos de dichos mecanismos, así como su implementación y comprobación de su correcto funcionamiento. Para ello se va a diseñar una red LAN de una empresa de tamaño mediano y se va a implementar una porción de dicha red, sobre la que se van a llevar a cabo las diferentes pruebas.

Alguno de los mecanismos que se van a estudiar son por ejemplo el estándar IEEE 802.1X, que permite a nuestra red autentificar a los dispositivos que deseen conectarse a la misma, o el mecanismo Indagación de DHCP que nos permite defendernos de ataques DoS y MITM(Man in The Middle) que aprovechan vulnerabilidades del protocolo DHCP.

Capítulo 2

Objetivos

Los objetivos que se pretender alcanzar una vez finalizado el proyecto son los siguientes:

- **Diseñar una red de área local destinada a una empresa.**
- **Estudiar tecnologías de seguridad en redes LAN, como por ejemplo: VLAN, Radius, seguridad basada en puerto, seguridad en protocolos como ARP, DHCP, etc:** Se realiza el estudio de las tecnologías usadas actualmente en la seguridad en redes LAN las cuales son: Seguridad de puertos, el estándar IEEE 802.1X, PVLAN, indagación de DHCP e inspección ARP.
- **Implementar una parte de la red en los conmutadores Cisco SG300 disponibles en el departamento:** Se lleva a cabo el montaje y configuración necesarios de una red LAN haciendo uso de un conmutador de nivel 2, switch Cisco SG 300-10 y un conmutador de nivel 3, router Cisco RV 120W
- **Medir las prestaciones de la red:** Utilizando herramientas como wireshark o tcpdump se monitoriza la red y se verifica su correcto funcionamiento.
- **Verificar que la red soporta ataques típicos en redes LAN:** Tras realizar la configuración necesaria en los conmutadores de nivel 2 y 3, se llevarán a cabo distintos ataques típicos en redes LAN, como Man in the Middle (MITM) o envenenamiento ARP y se comprobará que la red soporta este tipo de ataques.

Capítulo 3

Estado del Arte

Estudio de las diferentes tecnologías relacionadas con la seguridad en redes LAN que serán implementadas y puestas a prueba en los apartados siguientes:

3.1. Seguridad de Puertos

La seguridad de puertos consiste en crear políticas de Seguridad en la capa 2, es decir, utilizando las direcciones MAC de los dispositivos para evitar conexiones no autorizadas a los equipos o puertos en cuestión llevando a cabo una acción en el momento en que se produzca dicha violación de seguridad. Las direcciones MAC utilizadas pueden aprenderse dinámicamente o configurarse de manera estática.

Cuando se asigna una dirección MAC segura a un puerto seguro, el puerto no reenvía el tráfico de ingreso para aquellos puertos que tienen direcciones MAC de origen que no son similares a las direcciones definidas. La seguridad de puertos se puede configurar de cuatro modos:

1. **Bloqueo clásico:** todas las direcciones MAC aprendidas en el puerto se bloquean y no se puede aprender direcciones MAC nuevas. Las direcciones aprendidas en el puerto no están sujetas a vencimiento ni reaprendizaje.
2. **Bloqueo dinámico limitado:** se eliminan las direcciones MAC dinámicas actuales aprendidas en el puerto y el puerto comienza a aprender direcciones MAC hasta alcanzar el número máximo de direcciones permitidas.En bloqueo dinámico limitado las direcciones están sujetas a vencimiento y reaprendizaje.
3. **Seguro permanente:** igual que bloqueo dinámico limitado, pero las direcciones MAC dinámicas actuales aprendidas se mantienen en vez de eliminarse y el puerto aprende direcciones MAC nuevas hasta llegar al límite. El reaprendizaje y el vencimiento están habilitados
4. **Eliminar en reinicio seguro:** las direcciones MAC dinámicas actuales asociadas al puerto se eliminan después de reiniciar el puerto y el puerto aprende

direcciones MAC en función del numero de direcciones permitidas en el puerto. El reaprendizaje y el vencimiento están deshabilitados.

Cuando se detecta en un puerto una trama cuya dirección MAC de origen no está autorizada, se hace uso del mecanismo de protección y se lleva a cabo una de las siguientes acciones:

- **Discard:** la trama se descarta.
- **Forward:** la trama se reenvía.
- **Shutdown:** el puerto se cierra, permaneciendo cerrado hasta que se reactive o hasta que se reinicie el switch.

La seguridad de puertos además nos permite evitar la sobrecarga de los dispositivos mediante “trampas”, limitando la frecuencia y el número de accesos.

3.2. IEEE 802.1X

3.2.1. Protoloco EAP

El estándar IEEE 802.1X se basa en el protocolo EAP (Protocolo de auntenticación extensible), cuya función es transportar la información de identificación de usuario. La forma en la que el protocolo EAP funciona es haciendo uso de un controlador de acceso, al que llamaremos autenticador, que permite o deniega el acceso a un usuario a la red.

3.2.2. Descripción general IEEE 802.1X

El estándar IEEE 802.1X, control de acceso basado en puertos, nos permite proteger las redes LAN contra el acceso de dispositivos no autorizados. El tráfico proveniente de un dispositivo no autorizado se bloquea en la interfaz hasta que dicho dispositivo se autentifica en un servidor RADIUS externo, que realiza la autenticación del solicitante a través del autenticador. Podemos distinguir tres participante en el proceso de autenticación, observar 10.2:

1. **Suplicante o cliente:** dispositivo que desea conectarse con la red.
2. **El servidor de autenticación:** contiene la información necesaria para conocer qué dispositivos y/o usuarios están autorizados para acceder a la red. Como servidor de autenticación puede utilizarse un servidor RADIUS, véase 3.2.3.

3. **El autenticador:** equipo de red (switch, punto de acceso) que recibe la conexión del suplicante o cliente. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, permitiendo el acceso a la red solo cuando el servidor de autenticación lo autorice. Existen tres metodos de autenticación:
   - **Basado en 802.1X:** compatible con todos los modos de autenticación. En este modo de autenticación, el autenticador extrae los mensajes EAP de los mensajes 802.1X y los envia al servidor de autentición mediante el protocolo RADIUS
   - **Basado en MAC:** compatible con todos los métodos de autenticación. A diferencia del método anterior, el autenticador es quien ejecuta la parte cliente EAP del software.
   - **Basado en la Web:** compatible unicamente con modos de sesión múltiple. El autenticador es quien ejecuta la parte cliente EAP del software.

En caso de que un dispositivo no autorizado envíe tráfico a un puerto, dicho tráfico puede ser bloqueado o enviados a una VLAN invitada o VLANs no autenticadas. Según la norma 802.1X, un dispositivo puede ser solicitante y autenticador simultáneamente en un puerto, y solicitar acceso al puerto y otorgarlo.

3.2.3. Servidor RADIUS

El protocolo RADIUS(Remote Access Dial in User Service) es un protocolo que sigue el esquema cliente-servidor y que nos permite gestionar el acceso de los clientes a nuestra red. Los servidores RADIUS pueden proporcionar los siguientes servicios:

- **Autenticación:** proporciona un método de autenticación haciendo uso de un nombre de usuario y contraseña definidos por el usuario.
- **Autorización:** proporciona privilegios de usuario una vez se ha iniciado sesión, mediante un proceso de autorización con el nombre de usuario autenticado.
- **Contabilidad:** permite al administrador del sistema generar informes de contabilidad desde el servidor RADIUS.

3.2.4. Open Access

La función Open Access ayuda a los administradores de sistemas a facilitar la resolución de problemas separando los errores de autenticación reales de aquellos errores producidos por errores de configuración o falta de recursos en un entorno 802.1X

Cuando se habilita esta función en una interfaz, el switch trata como éxito los errores que recibe de un servidor RADIUS y habilita el acceso a la red de las estaciones

conectadas a interfaces, independientemente de los resultados de la autenticación. Sin embargo, Open Access cambia el comportamiento habitual de bloqueo de tráfico en un puerto habilitado por la autenticación hasta que se realicen con éxito la autenticación y la autorización. Dicho comportamiento sigue siendo bloquear todo el tráfico, salvo el tráfico del Protocolo de autenticación extensible sobre LAN (EAPoL),

3.2.5. VLAN no autenticadas y la VLAN invitada

Las VLAN no autenticadas y la VLAN invitada permite a los dispositivos o puertos no autenticados mediante 802.1X acceder a determinados servicios. Mientras que la VLAN invitada es aquella que se asigna a un cliente no autorizado, las VLAN no autenticadas permiten el acceso de dispositivos autorizados y no autorizados.

3.2.6. Modos de host del puerto

Los puertos pueden configurarse en los siguientes modos de host

- **Modo de host único:** el puerto se considera autorizado si hay un cliente autorizado en el mismo. Solo puede configurarse un host por puerto.
- **Modo de host múltiple:** un puerto se considera autorizado cuando al menos hay un cliente autorizado.
- **Modo de sesión múltiple:** los puertos que se encuentren en modo de sesión múltiple no tienen estado de autenticación, de forma que el estado de autenticación se asigna a cada cliente conectado al puerto.

3.2.7. Asignación dinámica de VLAN

La asignación dinámica de VLAN consiste en asignar a un cliente no autorizado una VLAN mediante el servidor RADIUS. Cuando un puerto se encuentra en modo sesión múltiple y tiene la opción de asignación dinámica de VLAN habilitada, el cliente se añade automáticamente como miembro sin etiquetar de la VLAN especificada por el servidor RADIUS.

3.3. PVLAN

Las PVLAN, o VLAN privadas, nos permiten segmentar una VLAN primaria en varias VLANs que llamamos privadas, donde cada puerto de una VLAN privada puede comunicarse únicamente con un único puerto troncal y no con el resto de PVLANs. De

esta forma,las PVLANs proporcionan aislamiento de capa 2 entre los puertos de una red VLAN, la división de un dominio de difusión en varios subdominios de difusión discretos mediante la creación de VLAN secundarias en una VLAN principal.

Lo que se espera del uso de PVLANs es que los dispositivos que pertenezcan a una PVLANs, observar 10.3, en este caso los servidores 1,2 y 3, puedan tener acceso a internet pero no puedan comunicarse entre sí a nivel de capa 2. El proceso consiste en crear una VLAN a la que llamamos primaria, VLAN5 en el ejemplo 10.3, que contiene los puertos de los servidores y el puerto troncal que conecta con el router, asignando a cada uno de los puertos que conectan con los servidores una VLAN privada. De esta forma, la única manera de que los servidores se comuniquen entre sí es llegar hasta el router, quedando aislados en la capa 2 del resto de servidores.

En una PVLAN podemos configurar tres tipos de puertos:

- **Puertos promiscuos:** es el puerto que comunica los servidores y el router. Por este tipo de puertos circulan tramas de todas las PVLANs.
- **Puertos comunitarios:** definen grupos de puertos que pertenecen a un mismo dominio de capa 2, quedando aislados en capa 2 del resto de puertos comunitarios y puertos aislados. Pueden comunicarse con puertos promiscuos y otros puertos comunitarios pertenecientes a la misma PVLAN.
- **Puertos aislados:** puertos aislados completamente en capa 2 del resto de puertos comunitarios y puertos aislados, pudiendo enviar y recibir paquetes únicamente desde puertos promiscuos. Se conecta a un host.

Análogamente a los puertos, distinguimos tres tipos de VLANs dentro de una PVLAN que llamaremos secundarias, observar 10.4:

- **VLAN primaria:** VLAN originar que contiene al resto de PVLAN.
- **VLAN aislada:** la VLAN aislada es un tipo de VLAN secundaria que solo admite puertos aislados. Incluso en una misma VLAN aislada, los puertos aislados no pueden comunicarse entre sí, pero si con los puertos de la VLAN primaria (puerto promiscuo).
- **VLAN comunitaria:** otro tipo de VLAN secundaria que admite solamente puertos comunitarios, los cuales pueden comunicarse entre sí y con los puertos de la VLAN primaria (puerto promiscuo). Las VLANs comunitarias no pueden comunicarse con otras VLAN secundarias (aisladas o comunitarias).

3.4. Indagación de DHCP

La indagación DHCP es un mecanismo de seguridad que nos ayuda a prevenir la respuesta a paquetes falsos de DHCP y que nos permite registrar direcciones DHCP.

Dicho mecanismo se basa principalmente en separar los puertos del switch en dos tipos: puertos confiables y puertos no confiables.

Un puerto confiable es un puerto conectado a un servidor DHCP y al cual se le permite tanto enviar como recibir mensajes DHCP. Por el contrario, un puerto no confiable es aquel al que no se le permite enviar ciertos mensajes DHCP. Por defecto, todos los puertos están configurados como no confiables. Observar 10.5.

Durante el proceso de asignación de direcciones DHCP, se crea una tabla (base de datos de vinculación de indagación de DHCP) basada en los mensaje acknowledge entrantes en el switch mediante puertos confiables, en la que se registra: puerto de entrada, VLAN de entrada, dirección MAC del cliente y dirección IP del cliente, si existe. El proceso de construcción de la base de datos de vinculación de indagación de DHCP sigue los siguientes pasos, siempre que tanto el cliente DHCP como el servidor DHCP sean confiables:

1. El cliente envía DHCPDISCOVER para solicitar una dirección IP, o DHCPREQUEST para aceptar una dirección IP y una concesión.

2. El switch indaga el paquete y añade información de IP-MAC a la base de datos de vinculación de indagación de DHCP.

3. El switch envía los paquetes DHCPDISCOVER o DHCPREQUEST

4. El servidor DHCP envía el paquete DHCPOFFER para ofrecer una dirección IP, DHCPACK para asignarla o DHCPNAK para denegar la solicitud de la dirección.

5. El switch indaga el paquete. Si existe una entrada en la tabla de vinculación de indagación de DHCP que coincida con el paquete, el switch la reemplaza con una vinculación IP-MAC al recibir DHCPACK.

6. El switch reenvía DHCPOFFER, DHCPACK o DHCPNAK

Si se reciben paquetes DHCP posteriores desde hosts no confiables, es decir, si el host no coincide con la información, se descartan. Por otro lado, si el switch intenta escribir demasiadas entradas en la base de datos, las entradas excedentes se mantienen en un estado inactivo, evitando así ataques de denegación de servicio.

A continuación se presenta el tratamiento que reciben los paquetes DHCP provenientes tanto de puertos confiables como no confiables:

Tipo de paquete	Interfaz no confiable	Interfaz confiable
DHCPDISCOVER	Reenvío solo a interfaces confiables	Reenvío solo a interfaces confiables.
DHCPOFFER	Filtro	Reenvía el paquete según la información de DHCP. Si la dirección de destino es desconocida, el paquete se filtra
DHCPREQUEST	Reenvío solo a interfaces confiables	Reenvío solo a interfaces confiables.
DHCPACK	Filtro	Igual que DHCPOFFER, se añade una entrada a la base de datos de vinculación de indagación de DHCP
DHCPNAK	Filtro	Igual que DHCPOFFER. Elimina la entrada si existe
DHCPDECLINE	Verifica si hay información en la base de datos. Si hay información y no coincide con la interfaz en la cual se recibió el mensaje, el paquete se filtra. De lo contrario, el paquete se reenvía únicamente a interfaces confiables y la entrada se elimina de la base de datos.	Reenvío solo a interfaces confiables.

Tabla. 3.1: Tratamiento de paquetes DHCP

Tipo de paquete	Interfaz no confiable	Interfaz confiable
DHCPRELEASE	Igual que DHCPDECLINE.	Igual que DHCPDECLINE.
DHCPINFORM	Reenvío solo a interfaces confiables.	Reenvío solo a interfaces confiables
DHCPLEASE-QUERY	Filtrado	Filtrado

Tabla. 3.2: Tratamiento de paquetes DHCP

3.4.1. Opción 82

La opción 82, también conocida como información de agente de retransmisión DHCP, es útil en entornos donde los clientes y los servidores no se encuentran en la misma red. Este procedimiento consiste en que el conmutador, en este caso el switch, añade información adicional al encabezado de las solicitudes que los clientes hacen al servidor DHCP. Dicha información consiste en información del puerto y del agente que realiza la solicitud e indica al servidor DHCP dónde se conecta físicamente una dirección IP asignada a la red.

El objetivo principal de la opción 82 es ayudar al servidor DHCP a seleccionar la mejor subred IP de la cual obtener una dirección IP.

El switch Cisco SG 300-10 dispone de las siguientes opciones para la Opción 82:

- **Inserción DHCP:** añade información de la Opción 82 a los paquetes que no tienen información remota de la opción 82.
- **Envío de DHCP:** reenvía o rechaza los paquetes DHCP que contengan la información de la opción que provengan de puertos no confiables. En puertos confiables, los paquetes DHCP que contienen información de la Opción 82 siempre se reenvían

3.4.2. Retransmisión DHCP

La retransmisión DHCP retransmite los paquetes DHCP al servidor DHCP en caso de que dicho servidor se encuentre fuera de la red.

En el modo de capa 2 del sistema, el switch reenvía los mensajes que provienen de las VLAN en las cuales se ha habilitado la Retransmisión DHCP.

En el modo de capa 3 del sistema, el switch también puede retransmitir los mensajes DHCP recibidos desde las VLAN que no tienen direcciones IP. Siempre que la

Retransmisión DHCP esté habilitada en una VLAN sin dirección IP, se insertará la opción 82 automáticamente. Esta inserción se efectúa en la VLAN específica y no influencia el estado global de administración de la inserción de Opción 82.

3.5. Inspección ARP

La inspección ARP es un mecanismo que nos permite proteger una red contra ataques ARP, como por ejemplo el ataque conocido como “Envenenamiento ARP” que consiste en lo siguiente:

Un usuario malintencionado, el atacante, puede atacar a los host, switches y routers conectados a una red de capa 2 envenenando las memorias caché ARP de los sistemas conectado a la subred y al interceptar el tráfico que se dirige a otros hosts de la subred. Este ataque es posible debido a que el protocolo ARP permite la respuesta gratuita por parte de un host incluso si no se recibió una solicitud ARP. De esta manera, el atacante puede enviar paquetes ARP al resto de host vinculando una dirección IP de otro host, a la dirección MAC del atacante, interceptando así todo el tráfico proveniente del dispositivo que recibió el ataque.

La Inspección ARP utiliza los mismo conceptos de puertos confiables y puertos no confiables utilizados en la Indagación de DHCP además de utilizar también la base de datos de vinculación de indagación de DHCP. Por otro lado, la Inspección de ARP hace uso de “Reglas de control de acceso ARP”, tabla donde se almacenan pares IP-MAC que se consideran confiables.

Ante la llegada de un paquete ARP a una interfaz no confiable, la Inspección ARP realiza los siguientes pasos:

1. Se comparan las direcciones IP-MAC del paquete con los pares definidos en las reglas de control de acceso ARP. Si la direcciones IP-MAC del paquete coinciden con las definidas en la lista, entonces el paquete es válido; de lo contrario, no lo es.
2. Este paso solo se realiza en caso de que la Indagación DHCP se encuentre habilitada. Se compara el par IP-VLAN del paquete con la base de datos de vinculación de indagación DHCP, de forma que si no se encuentra el par VLAN-IP y la dirección MAC y la interfaz que figuran en la base de datos coinciden con la dirección MAC y la interfaz de ingreso, el paquete es válido.
3. Si la dirección IP no se encuentra ni en las reglas de control de acceso ARP ni en la base de datos de vinculación de indagación de DHCP, entonces el paquete no es válido y se descarta.
4. Si el paquete es válido se reenvía y se actualiza la memoria caché ARP.

Capítulo 4

Configuración de seguridad LAN

Exponer las vulnerabilidades que presentan las redes LAN mediante distintos ataques típicos y el proceso de configuración llevado a cabo para solventar dichas vulnerabilidades. Dicho proceso se va a llevar a cabo montando una parte de la red descrita a continuación, formada por un conmutador de nivel 2, switch Cisco SG 300-10 y un conmutador de nivel 3, router Cisco RV 120W siguiendo el siguiente esquema:

4.1. Diseño de red de área local

Para realizar el diseño de la red, se ha seguido el modelo de red jerárquico propuesto por Cisco para una red confiable, escalable y rentable. En la ilustración 10.1 se muestra el diseño propuesto para la red LAN.

En primer lugar, para asegurar la redundancia de la red se proporcionan rutas de datos alternativas entre los distintos equipos de comunicaciones, para asegurar así la supervivencia de la red ante fallos de enlace o sobrecarga de determinadas rutas.

Para dotar de mayor seguridad a la red LAN, se ha añadido una zona desmilitarizada donde se situarán los servidores públicos correspondientes, quedando estos aislados del resto de la red. En cuanto a los servidores privados, se sitúan conectados a un switch Core para una mayor velocidad de conexión.

Los equipos de trabajo conectados a la red LAN se distribuirán en tres VLAN, por ejemplo agrupándolos por departamentos, aislando posibles brechas de seguridad que puedan producirse e impidiendo el acceso de los equipos de una VLAN al resto de VLANs.

En cuanto a la redundancia en las conexiones a internet, se ha optado por contratar dos ISPs, utilizando un único router con dos interfaces WAN.

4.1.1. Red LAN implementada

Para llevar a cabo la implementación de los mecanismos de seguridad vistos en 3 se va a implementar una porción de la red LAN descrita anteriormente siguiendo el siguiente esquema:

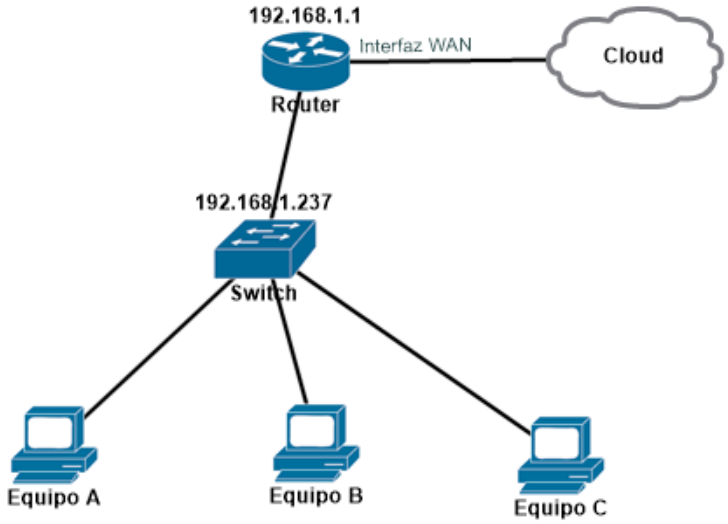

Figura 4.1: Red LAN implementada

Se ha utilizado un conmutador de nivel 2, switch Cisco SG 300-10 y un conmutador de nivel 3, router Cisco RV 120W, así como tres equipos que cumplirán distintas funciones dependiendo del mecanismo de seguridad que se esté implementando en cada momento.

4.2. Configuración de Seguridad de Puertos y acceso de equipos no reconocidos a puertos del switch

Como se ha comentado en la sección 3.1, mediante la Seguridad de Puertos se puede restringir el acceso a los puertos del Switch mediante las direcciones MAC de los dispositivos. Previo a llevar a cabo el proceso de configuración, es trivial comprobar que cualquier dispositivo que conecte con un puerto del switch es aceptado en la red, recibiendo una dirección IP automáticamente si el protocolo DHCP se encuentra activo. Solo hay que conectar un dispositivo cualquiera a un puerto del switch y observar que no se lleva a cabo ningún proceso de autorización y automáticamente estamos dentro de la red.

Dicha problemática se puede solucionar configurando la Seguridad de Puertos en el Switch. El proceso de configurar las direcciones MAC aceptadas en cada puerto se puede llevar a cabo de forma manual añadiendo dichas direcciones a la tabla “Direcciones MAC Estáticas” accediendo a la pestaña del Switch MAC Address Table >Static Addresses:

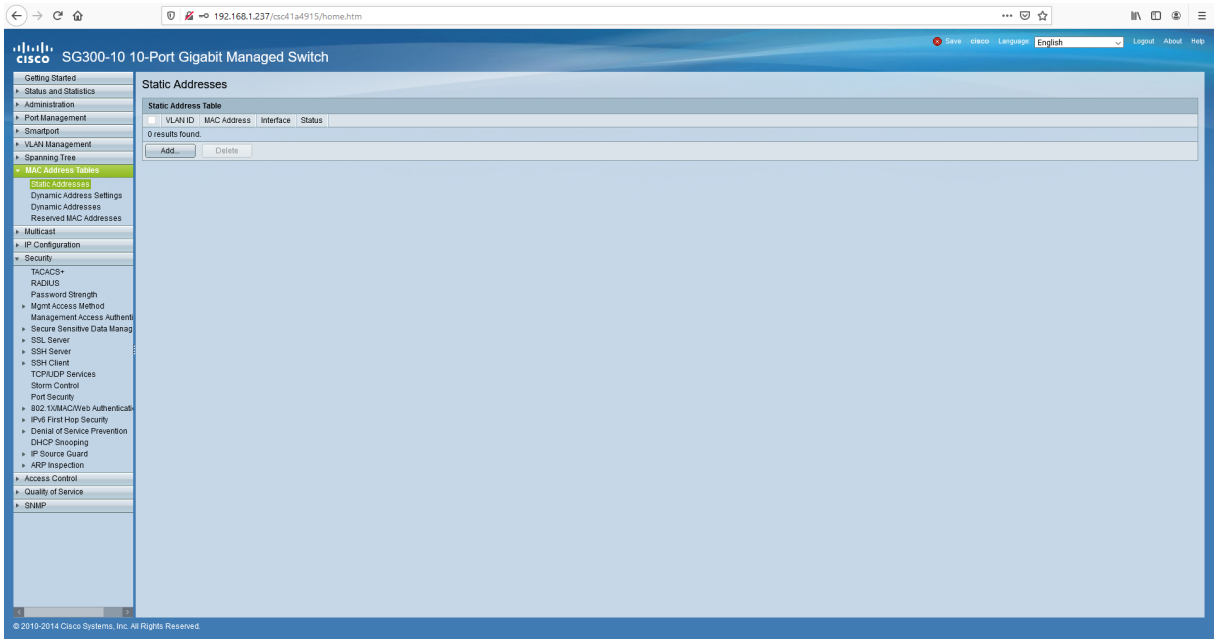

Figura 4.2: Ventana Static Addresses

Observamos que la tabla se encuentra vacía. Haciendo click en ’Add’ se pueden añadir las direcciones MAC deseadas, configurando el Puerto, la VLAN a la que pertenece, la dirección MAC y por último seleccionar uno de los cuatro estados explicados en la sección 3.1.

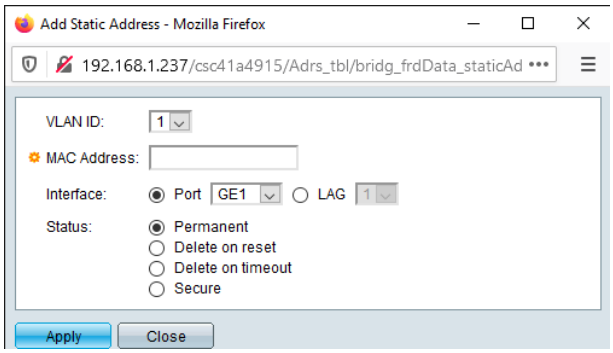

Figura 4.3: Configuración MAC estáticas

Es obvio que configurar de manera manual todas las direcciones MAC de una red LAN puede funcionar en un entorno pequeño en el que se disponga de muy pocos dispositivos, pero en una red donde el número de dispositivos sea elevado, añadir las direcciones MAC una a una es un proceso tedioso e ineficiente. Por ello se va a proceder a configurarlo de forma automática.

En primer lugar se conectan los dispositivos cuyas direcciones MAC se quieren almacenar en los puertos del Switch correspondientes. En este caso:

Equipo	Puerto	Dirección MAC
A	GE1	40:8d:5c:b1:26:33
B	GE3	70:4d:7b:a5:3c:a6
Switch	GE8	00:08:30:29:1c6:13

Tabla. 4.1: Direcciónes MAC asociadas a puertos

Una vez conectados, se accede a la interfaz basada en Web del switch utilizando la dirección IP del mismo, 192.168.1.237, y se accede a la pestaña Security/Port Security:

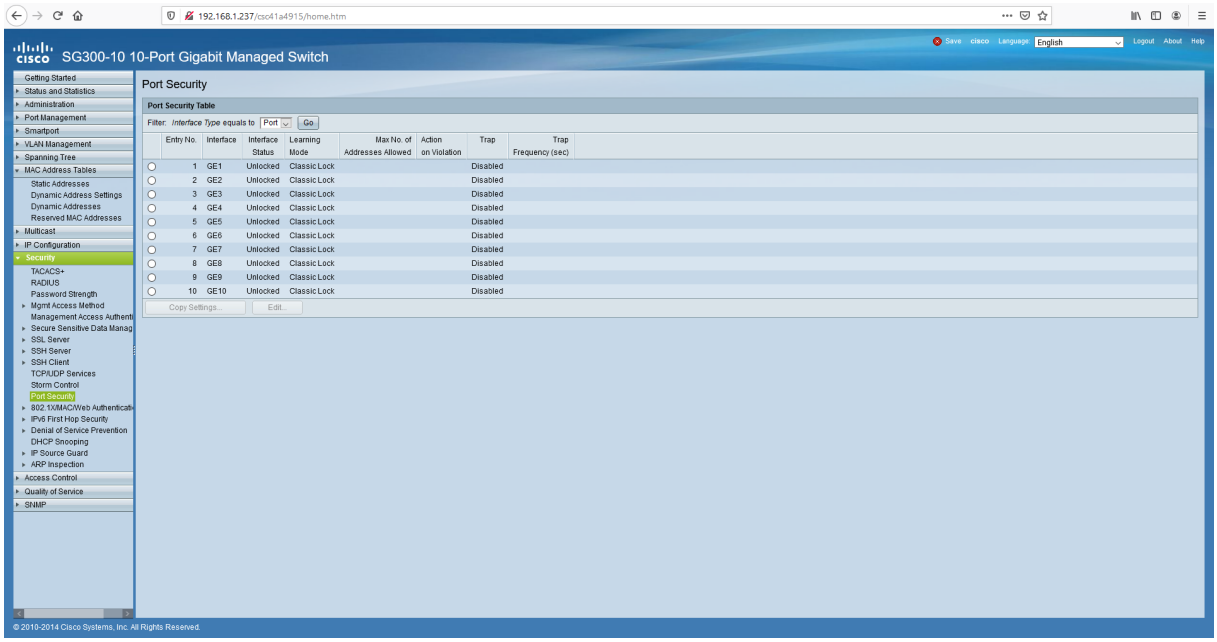

Figura 4.4: Ventana Port Security

En esta ventana se observa que todos los puertos del Switch se encuentran desbloqueados. En nuestro caso queremos bloquear los puertos 1,3 y 8, por lo que se selecciona cada uno de los puertos y se repite el siguiente proceso:

1. se selecciona el puerto correspondiente.
2. se hace click en 'Edit'.
3. se procede a configurar el puerto:
   - **Interface:** puerto seleccionado
   - **Interface Status:** habilita o deshabilita el bloqueo del puerto

- **Learning Mode:** modo en el que el switch aprende las direcciones MAC de los dispositivos. La funcionalidad de cada modo se explica en la sección 3.1.
- **Action on Violation:** acción que se lleva a cabo cuando se detecta un acceso no autorizado
- **Trap:** nos permite evitar la sobrecarga del Switch producida por accesos no autorizados
- **Trap Frequency:** tiempo mínimo que debe transcurrir entre trampas

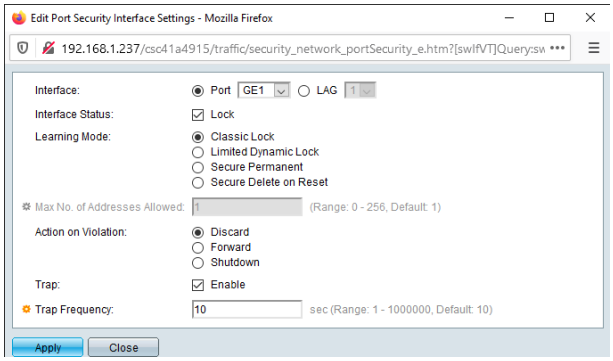

Figura 4.5: Configuración de puertos

Una vez se han configurado los puertos 1,3 y 8, se puede acceder a la tabla de direcciones MAC estáticas y observar que se han almacenado correctamente las direcciones MAC de los dispositivos conectados a dichos puertos.

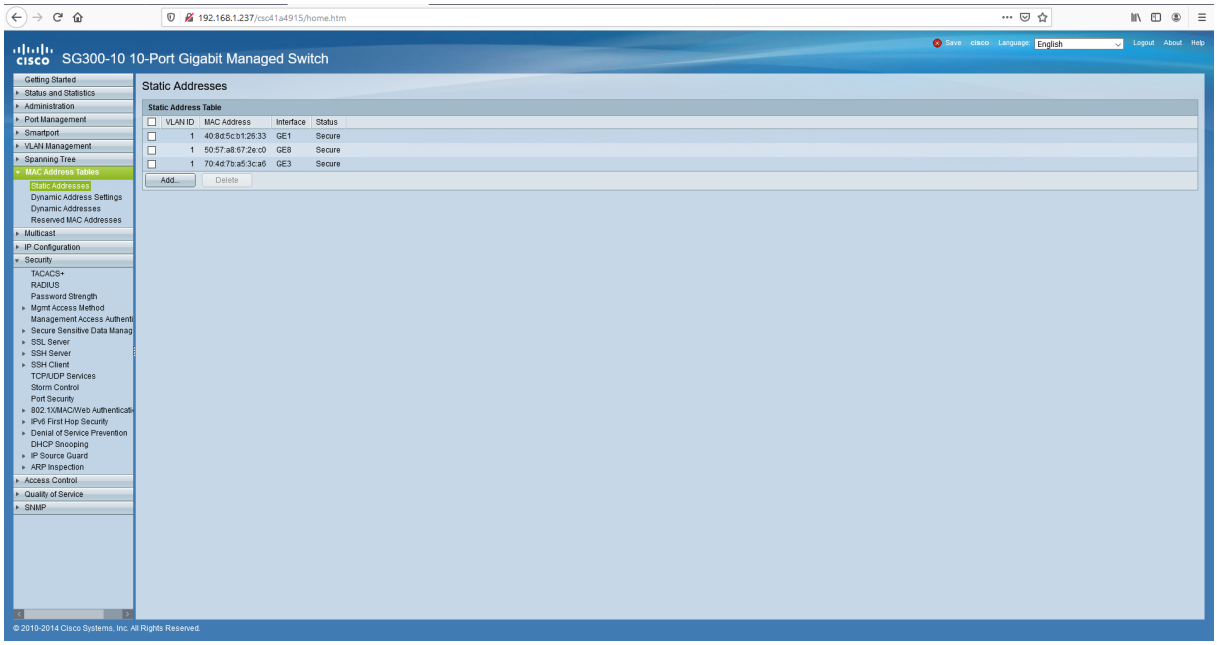

Figura 4.6: Direcciones MAC almacenadas

De esta forma, cualquier dispositivo que conecte con los puertos configurados y cuya dirección MAC no se encuentre almacenada en la tabla de direcciones MAC

estática no tendrá acceso a la red y cualquier trama enviada por dicho puerto será descartada.

4.3. Configuración del estándar IEEE 802.1X y accesos no autorizados a la red

Igual que en el apartado anterior 4.2, si nuestros equipos de comunicaciones no tienen configurado el estándar IEEE 802.1X, cualquier dispositivo que conecte con un puerto del Switch será aceptado automáticamente en la red. Implementar el estándar IEEE 802.1X nos permitirá que los equipos tengan que llevar a cabo un proceso de autenticación utilizando un nombre de usuario y contraseña antes de recibir una IP privada y poder acceder a la red.

Los dispositivos que participan en el proceso son los siguientes:

Equipo	Función	Dirección IP
Switch	Autenticador	192.168.1.237
A	Gestión	192.168.1.1
B	RADIUS	192.168.1.104
C	Cliente	—

Tabla. 4.2: Entidades

El equipo C como cliente, no dispondrá de dirección IP hasta que se autentifique correctamente mediante el estandar IEEE 802.1X.

Como se ha visto en la sección 3.2, en el proceso de autenticación intervienen tres entidades: el cliente o suplicante, el autenticador y el servidor de autenticación. En primer lugar se va a proceder a configurar el servidor de autenticación, en este caso un servidor RADIUS, utilizando FreeRadius, sobre una distribución Kali GNU/Linux.

4.3.1. Configurar el servidor RADIUS

Para configurar FreeRadius, primero se tienen que añadir los dispositivos que van a desempeñar la función de autenticadores, en nuestro caso el Switch. Para ello, se edita el fichero /etc/freeradius/3.0/clients.conf, y se añaden las siguientes líneas al final de dicho fichero:

```
client SWITCH-01{
    ipaddr = 192.168.1.237
    secret = rEdes2021
}
```

De esta forma, se ha añadido el dispositivo cliente SWITCH-01, cuya dirección IP es 192.168.1.237 y contraseña: rEdes2021. Para terminar con la configuración del servidor RADIUS, se tienen que añadir las cuentas ha usar por los clientes o suplicantes a la hora de autenticarse en la red. Para ello se edita el fichero /etc/freeradius/3.0/users y se añaden, al final de dicho fichero, tantos usuarios como deseemos, indicando un nombre de usuario y contraseña:

```
1 andres Cleartext-Password := "tfG2021"
```

Una vez realizada la configuración, se reinicia el servidor para que se apliquen los cambios realizados y se comprueba su correcto funcionamiento haciendo uso del siguiente comando: “radtest andres tfG201 localhost 0 testing 123”. Si se ha configurado correctamente el servidor RADIUS, se obtiene una salida parecida a esta:

```
┌──(root💀kali)-[/home/kali]
└─# radtest andres tfG2021 localhost 0 testing123
Sent Access-Request Id 64 from 0.0.0.0:51092 to 127.0.0.1:1812 length 76
        User-Name = "andres"
        User-Password = "tfG2021"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "tfG2021"
Received Access-Accept Id 64 from 127.0.0.1:1812 to 127.0.0.1:51092 length 20
```

Figura 4.7: Prueba servidor RADIUS

Teniendo el servidor de autenticación en funcionamiento, procedemos a configurar el Switch que cumple la función de autenticador. Previo a comenzar con la configuración del estándar IEEE 802.1X, se ha de definir una VLAN la cual será asignada posteriormente como VLAN invitada.

4.3.2. Configurar el estandar IEEE 802.1X

Primeramente, se accede al Switch utilizando un navegador web y se accede a la pestaña Seguridad >Autenticación 802.1X/MAC/Web >Propiedades. En esta ventana se procede a configurar las propiedades del protocolo de Autenticación 802.1X:

- **Port-Bashed Authentication:** activar o desactivar la autenticación basada en puertos.
- **Método de autenticación:** seleccionar el método de autenticación del usuario:
  - **RADIUS, none**: se intenta llevar a cabo la autenticación del puerto a través del servidor RADIUS. Si no se recibe respuesta por parte del servidor RADIUS, debido al mal funcionamiento del mismo por ejemplo, la autenticación

no se lleva a cabo y se permite acceder a la red. Si se lleva a cabo la autenticación a travez del servidor RADIUS pero las credenciales son incorrectas, el acceso se rechaza.

- **RADIUS:** solo se permite el acceso a la red si el usuario se autentica a través del servidor radius.
- **None:** se permite al acceso al usuario sin necesidad de autenticación.

- **Guest VLAN:** activar esta opción permite usar una VLAN invitada para los puertos no autorizados.
- **Guest VLAN ID:** si se pretende usar VLAN invitada, seleccionar el ID de dicha VLAN:
- **Guest VLAN timeout:** si el proceso de autenticación no se resuelve correctamente, el puerto se añade a la VLAN invitada despues del tiempo indicado.
- **Trap Settings:** nos permite seleccionar que eventos queremos que generen trampas(avisos).

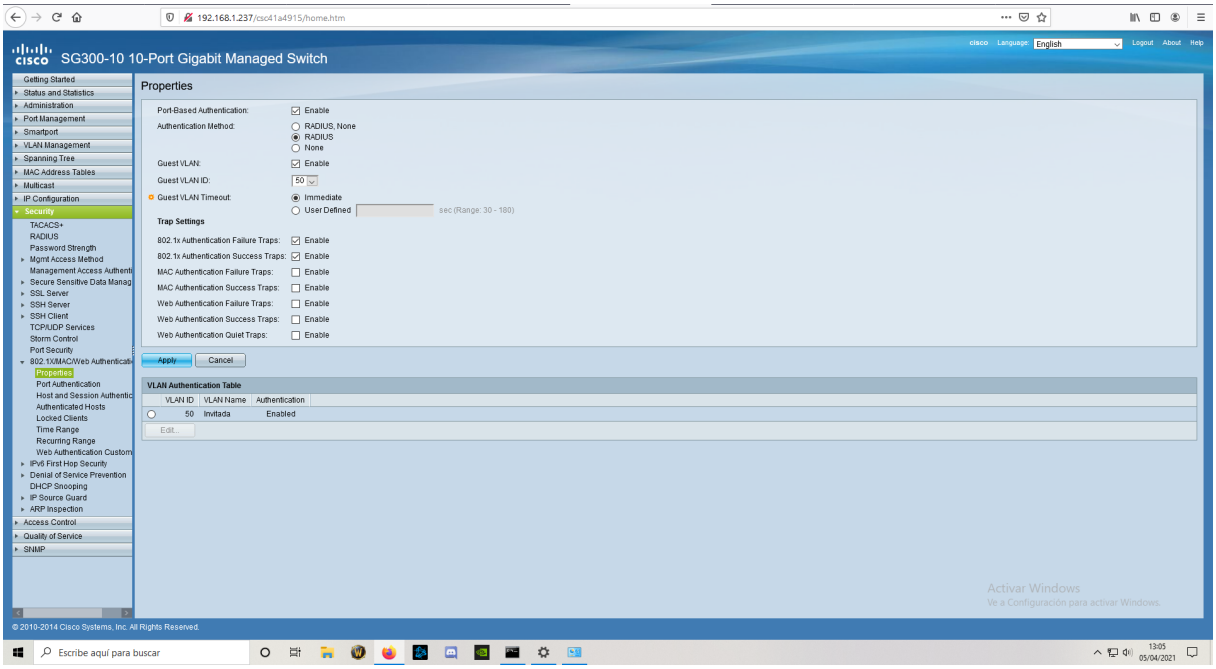

Figura 4.8: Propiedades

Seguidamente, se accede a la pestaña Seguridad >Autenticación 802.1X/MAC/web >Autenticación de puertos, donde se procede a configurar aquellos puertos en los que se quiere que se lleve a cabo la autenticación 802.1X. Para ello, se selecciona un puerto, en nuestro caso el GE5, y se hace click en el botón Edit. En la ventana de configuración, se seleccionan los parámetros deseados:

- **Interface:** puerto que se desea configurar.

- **Current Port Control:** muestra el estado actual del puerto.
- **Administrative Port Control:** estado de autorización administrativa del puerto.
  - **Forze Unauthorized:** el estado actual del puerto se coloca en estado no autorizado, lo que impide el acceso al mismo.
  - **Auto:** se habilita la autenticación basadas en el puerto en el dispositivo, cambiando de estado entre autorizado y no autorizado según si el proceso de autenticación es correcto o no.
  - **Forze Authorized:** se permite el acceso al puerto sin autenticación
- **Radius VLAN Assignment:** habilita la asignación dinámica de VLAN en el puerto seleccionado
- **Guest VLAN:** se habilita el uso de VLAN invitada
- **Open Access:** habilita la función Open Access. Consultar 3.2.4
- **802.1X/MAC/Web based Authentication:** habilita el tipo de autenticación seleccionado.
- **Periodic Reauthentication:** activa la reautenticación del puerto pasado un periodo de reautenticación especificado.
- **Reauthentication period:** periodo de tiempo tras el cual se realiza la reautenticación.
- **Reauthentication now:** seleccione esta opción para activar la reautenticación inmediata del puerto
- **Authenticator State:** muestra el estado de autorización del puerto seleccionado.
  - **Initialize:** en proceso de activación.
  - **Forze Unauthorized**
  - **Forze Authorized**
- **Maximum WBA Login Attempts:** intentos maximos de inicio de sesión en el puerto.
- **Maximum WBA Silence period:** periodo de silencio máximo permitido en la interfaz
- **Max Hosts:** cantidad máxima de host autorizados permitidos en la interfaz.
- **Quiet Period:** cantidad de segundos que el dispositivo permacene en estado de silencio(inactivo) después de una autenticación erronea
- **Resending EAP:** ingrese la cantidad de segundos que el dispositivo espera una respuesta para una trama de identidad/solicitud EAP del solicitante antes de reenviar la solicitud.

- **Max EAP Request:** ingrese el número máximo de solicitudes EAP que se pueden enviar. Si no se recibe una respuesta después del período definido (tiempo de espera para solicitantes), se reinicia el proceso de autenticación.

- **Supplicant Timeout:** cantidad de segundos que deben transcurrir antes de que se reenvíen las solicitudes EAP al solicitante

- **Server Timeout:** cantidad de segundos que deben transcurrir antes de que el dispositivo reenvíe una solicitud al servidor de autenticación

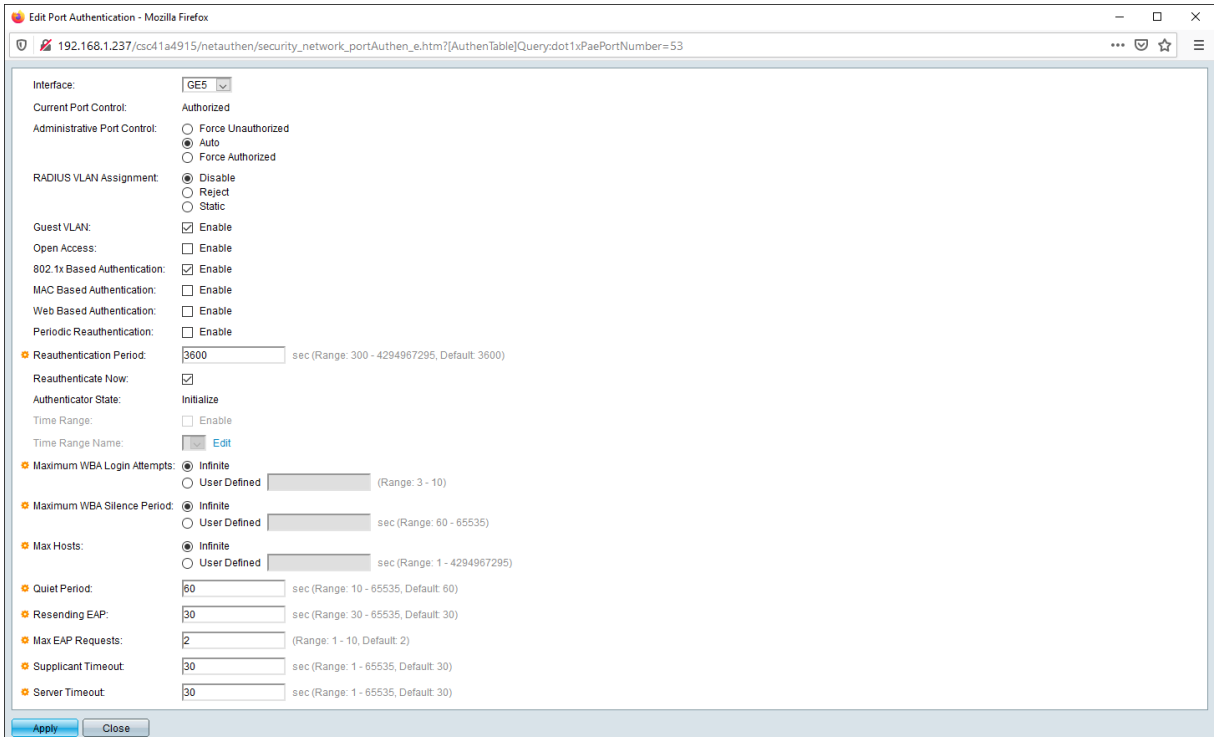

Figura 4.9: Editar autenticación de puertos

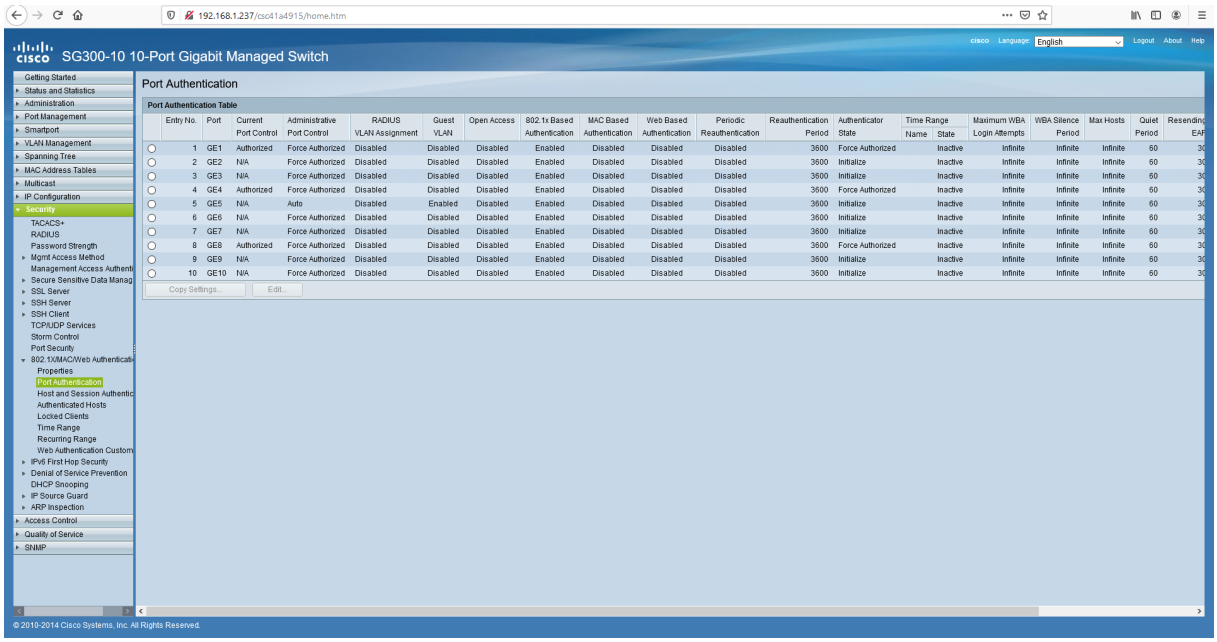

Figura 4.10: Autenticación de puertos

A continuación, en la pestaña Seguridad >Autenticación 802.1X/MAC/web >Autenticación de host y sesión, se selecciona para cada puerto el modo de host del puerto. Por defecto, se encuentra seleccionado el modo host múltiple, consultar 3.2.6.

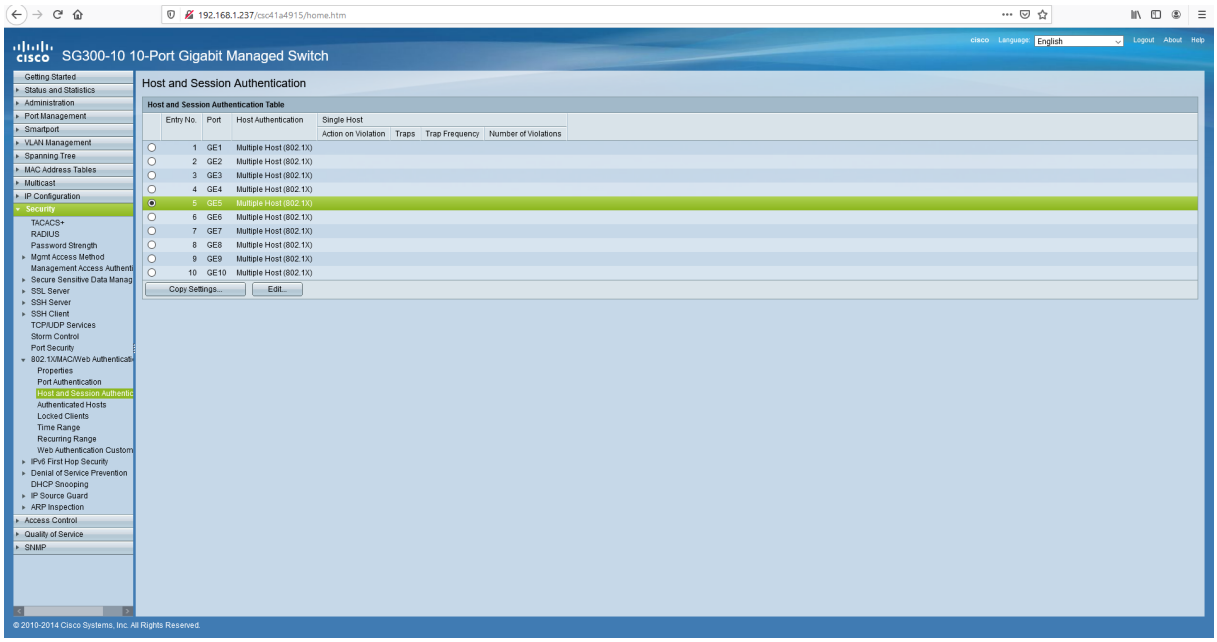

Figura 4.11: Modo de host del puerto

4.3.3. Configurar el servidor RADIUS en el switch

Para añadir el servidor RADIUS a la configuración del switch se tiene que acceder a la ventana Security >RADIUS, que nos permite modificar los siguientes parámetros:

- **RADIUS Accounting:** modo de funcionamiento del servidor RADIUS.
  - **Port Based Access Control:** especifica que el servidor RADIUS se usa para la contabilidad del puerto 802.1x.
  - **Management Access:** indica que el servidor RADIUS se usa para la contabilidad de inicio de sesión del usuario
  - **Both Port Based Access Control And Management Access:** especifica que el servidor RADIUS se usa tanto para la contabilidad de inicio de sesión del usuario como para la contabilidad del puerto 802.1X.
  - **None:** el servidor RADIUS no se utiliza.
- **Retries:** número de solicitudes transmitidas al servidor RADIUS antes de que se considere que ocurrió un error.
- **Timeout for Replay:** tiempo en segundos que el dispositivo espera una respuesta del servidor RADIUS antes de reintentar la consulta o cambiar al siguiente servidor.
- **Dead Time:** tiempo en minutos de espera antes de que se desvíen las solicitudes de servicio de un servidor RADIUS que no responde. Si el valor es 0, no se desvía del servidor.
- **key String:** clave de autenticación y cifrado entre el dispositivo y el servidor RADIUS. Debe de coincidir con la clave configurada en el servidor RADIUS.
- **Source IPv4 interface:** interfaz de origen IPv4 del dispositivo que se usará en los mensajes para la comunicación con el servidor RADIUS.
- **Source IPv6 interface:**interfaz de origen IPv6 del dispositivo que se usará en los mensajes para la comunicación con el servidor RADIUS.

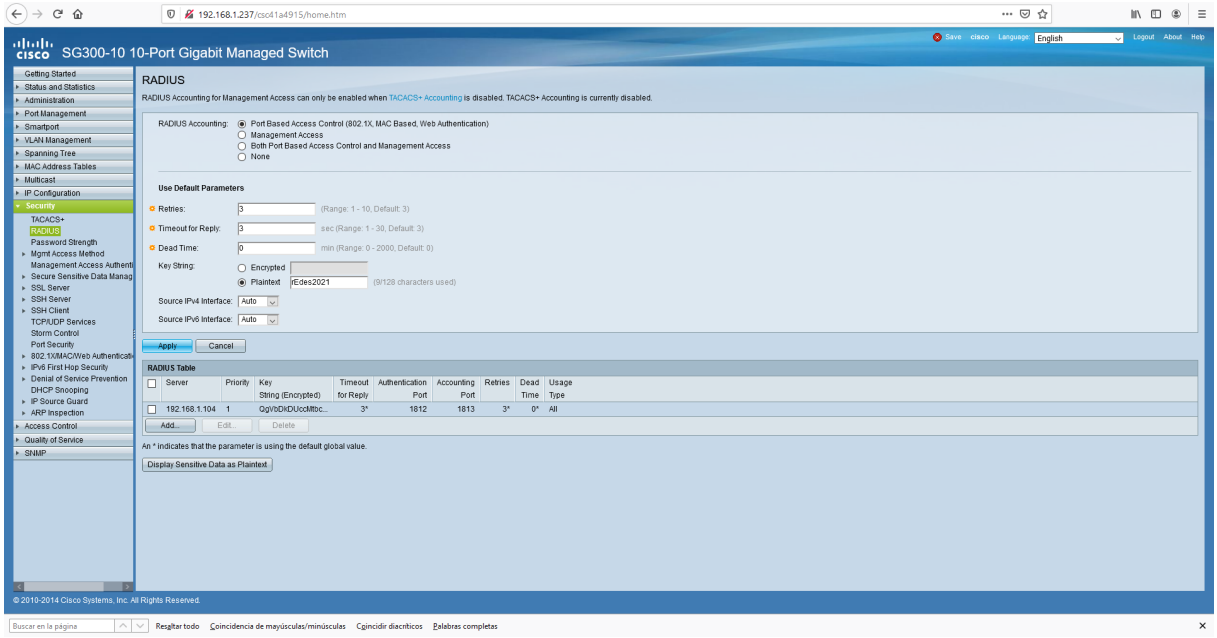

Figura 4.12: Valores por defecto

Estos valores se utilizan como valores por defecto en caso de que no se configuren valores especifícos para un servidor RADIUS. A continuación se hace click en 'Add' y se completan los valores que definen nuestro servidor:

- **Server Definition:** indica si el servidor se indentifica mediante dirección IP o nombre.
- **IP Version:** versión IP de la dirección IP del servidor RADIUS.
- **Server IP Address/Name:** dirección IP o nombre del servidor RADIUS.
- **Priority:** prioridad del servidor, la cual determina el orden en que el dispositivo intenta comunicarse con los servidores para autenticar a un usuario.
- **Key String:** clave de autenticación y cifrado entre el dispositivo y el servidor RADIUS. Debe de coincidir con la clave configurada en el servidor RADIUS.
- **Timeout for Reply:** tiempo en segundos que el dispositivo espera una respuesta del servidor RADIUS antes de reintentar la consulta o cambiar al siguiente servidor.
- **Authentication Port:** número del puerto UDP del servidor RADIUS para las solicitudes de autenticación.
- **Accounting Port:** número del puerto UDP del servidor RADIUS para las solicitudes de cuentas.
- **Retries:** número de solicitudes transmitidas al servidor RADIUS antes de que se considere que ocurrió un error.

- **Dead Time:** tiempo en minutos de espera antes de que se desvíen las solicitudes de servicio de un servidor RADIUS que no responde. Si el valor es 0, no se desvía del servidor.
- **Usage Type:** selecciona el tipo de autenticación del servidor RADIUS:
  - **Login:** se utiliza para aunteticar a un usuario que solicita administrar el dispositivo.
  - **802.1X:** se usa para la autenticación 802.1X.
  - **All:** combina las dos opciones anteriores.

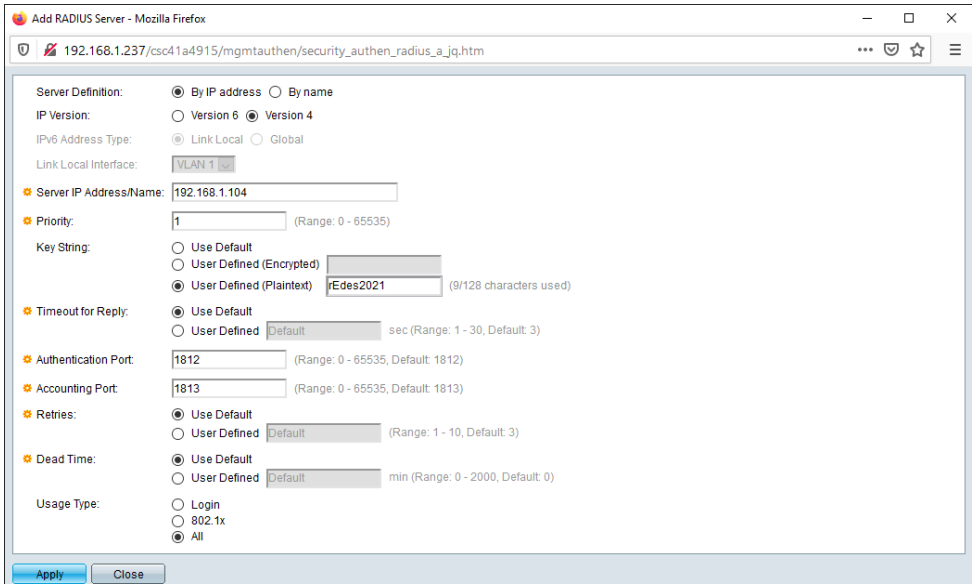

Figura 4.13: Añadir servidor RADIUS

Una vez añadido el servidor RADIUS, se ha terminado con la configuración del estándar IEEE 802.1X de forma que los dispositivos que intenten acceder a la red deberán de superar un proceso de autenticación previamente. En la sección 5.1 se lleva a cabo el proceso de autenticación desde un dispositivo cliente.

4.4. Configuración de VLAN y PVLAN y comunicación entre VLAN

4.4.1. Configuración previa

Previo a comenzar con el proceso de configuración de PVLAN, se ha de crear en el router la VLAN que cumple la función de VLAN primaria. Para ello simplemente se accede a la interfaz web del router y en la pestaña Networking >LAN >VLAN membership se añade una VLAN indicando el VLAN ID, en este caso se va a utilizar el VLAN ID 2, un nombre y dejando el resto de parámetros por defecto.

Por otro lado, tenemos que crear la misma VLAN definida en el router en el switch, siguiendo el procedimiento habitual para definir VLANs.

Para comenzar, los equipos B y C se incluyen ambos en la VLAN creada previamente con las direcciones 192.168.2.10 y 192.168.2.11 respectivamente. Como es de esperar ambos dispositivos pueden comunicarse entre si ya que forman parte de la misma VLAN. Para comprobarlo se utiliza la herramienta Ping, de esta forma podemos ver que se produce la comunicación entre ambos equipos.

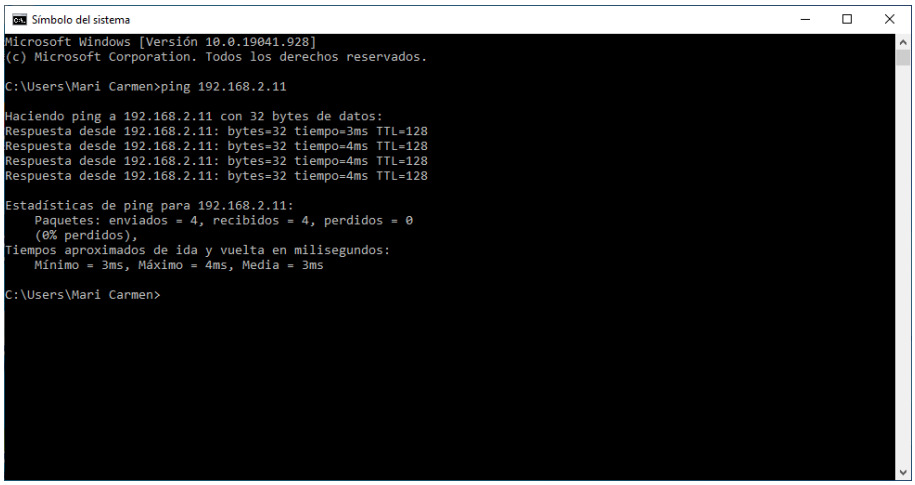

Figura 4.14: Ping desde misma VLAN

4.4.2. Configuración de PVLAN

El primer paso para crear una PVLAN es definir las VLAN que realizan la función de VLANs secundarias, puesto que la VLAN que cumple la función de VLAN primaria ya se ha definido en 4.4.1. Como se ha visto en la sección 3.3, las PVLANs actúan a nivel de puerto en la capa 2, por lo que las VLANs secundarias se han de definir en el switch y no en el router. De la misma forma que se ha definido la VLAN primaria en el switch, accedemos a la interfaz web del switch y en la ventana VlAN Management >VLAN Settings añadimos dos nuevas VLAN, con VLAN ID 21 y 22 respectivamente. El nombre no tiene ninguna función concreta, pero para que sirva de guía, vamos a utilizar los nombres ‘Isolated’ y ’Comunidad’

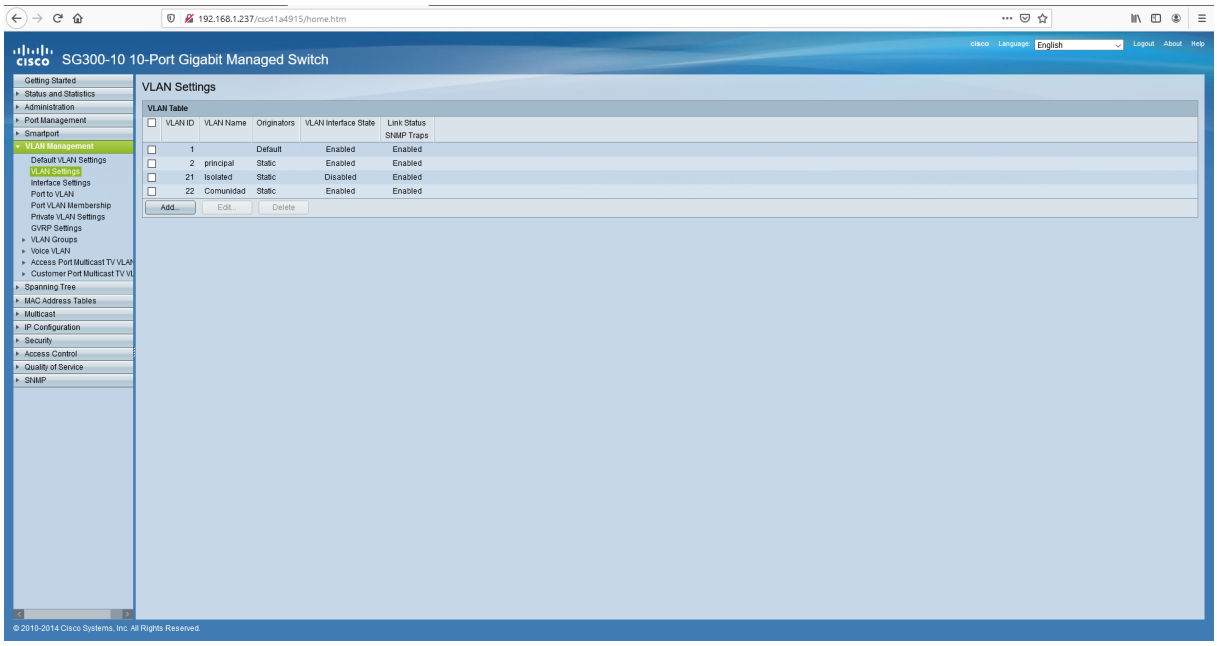

Figura 4.15: VLAN Settings

Una vez definidas en el switch las VLANs necesarias, se ha de indicar la función de cada una de ellas. Para ello se accede a la pestaña VLAN Management >Private VLAN Settings y se hace click en 'Add'. Se abre la ventana de configuración de PVLAN, donde se han de indicar los siguientes parámetros:

- **Primary VLAN ID:** se indica el VLAN ID de la VLAN primaria dentro de la PVLAN.
- **Isolated VLAN ID:** se indica el VLAN ID de la VLAN aislada dentro la PVLAN. Unicamente puede haber una VLAN aislada por PVLAN.
- **Available Community VLANs:** se indica las VLANs de comunidad que se quieren añadir a la PVLAN

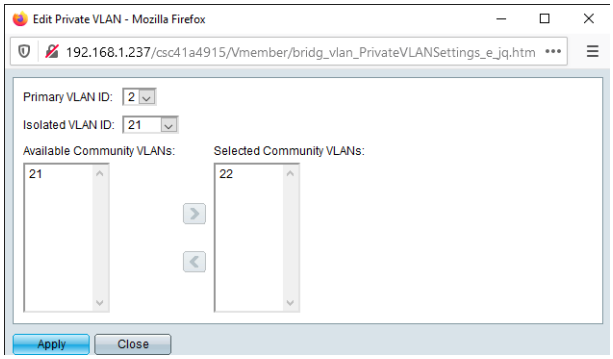

Figura 4.16: Editar PVLAN

Configurados todos los parámetros se hace clic en 'Apply' y se habrá creado la PVLAN. Se puede observar la configuración de la PVLAN creada, la cual tiene definida

como VLAN primaria la VLAN 2, como VLAN aislada la VLAN 21 y como VLAN de comunidad la VLAN 22.

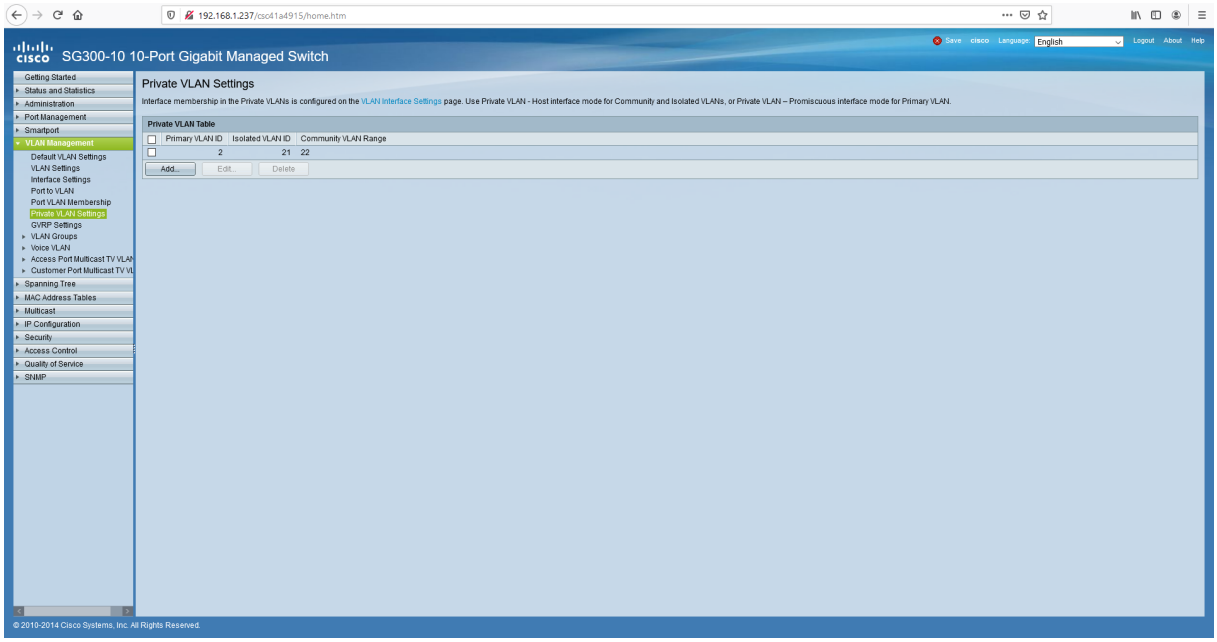

Figura 4.17: Private VLAN Settings

Por último, se han de definir a nivel de puerto las PVLANs correspondientes. Para ello, en la ventana VLAN Management >Interface Settings, se seleccionan los puertos correspondientes, en nuestro caso los puertos GE4,GE5 y GE8, y se hace click en 'Edit'. Se procede a configurar los siguientes parámetros:

- **Interface VLAN Mode:** Modo de interfaz para la VLAN.
  - **Private VLAN - Host:** la interfaz se configura como aislada o de comunidad, seleccionando la VLAN aislada o de comunidad a la que pertenece el puerto.
  - **Private VLAN - Promiscuous:** la interfaz se selecciona como promiscua.
- **Primary VLAN:** se selecciona la VLAN principal en la VLAN privada.
- **Secondary VLAN - Host** se selecciona la VLAN aislada o de comunidad a la que pertenece el puerto.
- **Available Secondary VLANs:** en los puertos promiscuos, se seleccionan todas las VLANs secundarias necesarias para el reenvío normal de paquetes desde las VLAN secundarias disponibles.

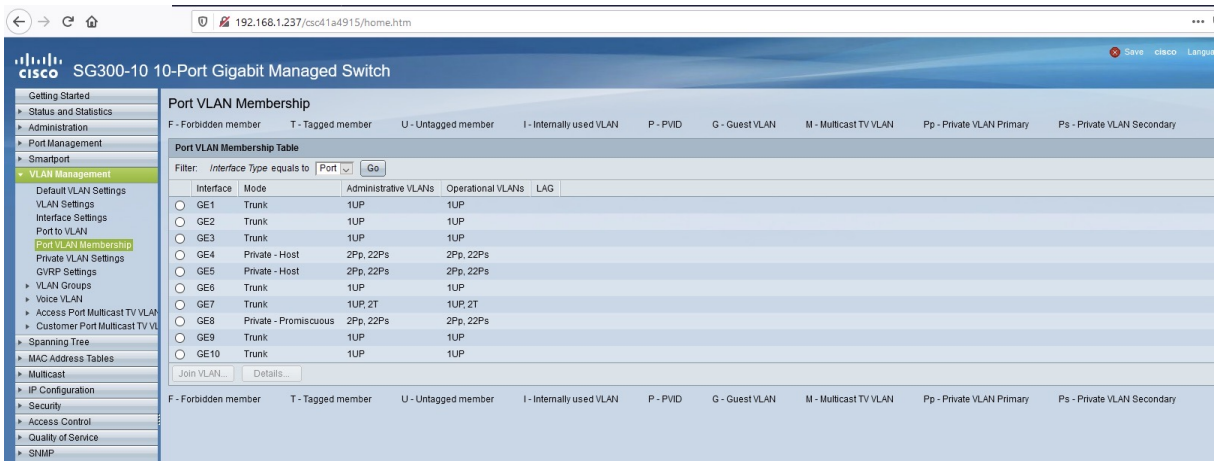

Figura 4.18: Interface Settings

Como se puede observar en 4.18, tanto el puerto GE4 como GE5 se han asignado a la PVLAN 2, que tiene como VLAN primaria la VLAN 2 y como VLAN secundaria la VLAN 22, que se ha definido previamente como VLAN de comunidad. Por otro lado, el puerto GE8 se ha asignado como puerto promiscuo por el que discurre tráfico de la VLAN 21 y 22, ya que es el puerto que conecta el switch con el router.

Puesto que los puertos GE4 y GE5 se han definido como de la misma comunidad, los equipos que conecten en dichos puertos podrán establecer conexión entre ellos y con el puerto promiscuo. En la sección 5.2 se muestra como interactuan los puertos dependiendo de si se configurar como de comunidad o aislados.

4.5. Ataque de hambre DHCP y de suplantación DHCP. Configuración de indagación DHCP

Los equipos que forman la red se van a utilizar de la siguiente manera:

Equipo	Función	Dirección IP
Switch	DHCP snooping	192.168.1.237
A	Víctima	192.168.124
B	Atacante	192.168.1.104
Router	Servidor DHCP	192.168.1.1

Tabla. 4.3: Entidades

4.5.1. DHCP spoofing

Las redes LAN son redes sensibles a ataques del tipo MITM, que permiten a un atacante interceptar la comunicación entre dos equipos. En lo referente al protocolo

DHCP, el ataque conocido como DHCP spoofing permite a un atacante realizar un MITM entre un equipo de comunicación y un dispositivo aprovechando el protocolo DHCP. Dicho ataque consiste en que un atacante responde a mensajes DHCP DISCOVER enviados por las víctimas con mensajes DHCP OFFER, nombrándose a sí mismo como Puerta de enlace predeterminada o servidor DNS. De esta forma, el equipo víctima asignará como Puerta de enlace la dirección IP del equipo atacante y todo el tráfico generado por la víctima será enviado al atacante en vez de al equipo de comunicaciones correspondiente.

Para llevar a cabo este ataque y exponer la vulnerabilidad de nuestra red LAN se va a usar una distribución Kali Linux junto con dos herramientas que incorpora dicha distribución, Wireshark y Ettercap.

Wireshark es una herramienta que nos permite analizar el tráfico de nuestra red en tiempo real. En primer lugar se va a usar dicha herramienta para analizar el intercambio de mensajes entre un dispositivo que solicita una dirección IP mediante el protocolo DHCP y el servidor DHCP, en nuestro caso el router. Para ello se abre Wireshark en el equipo atacante y se selecciona la interfaz a través de la cual se va a escuchar el tráfico.

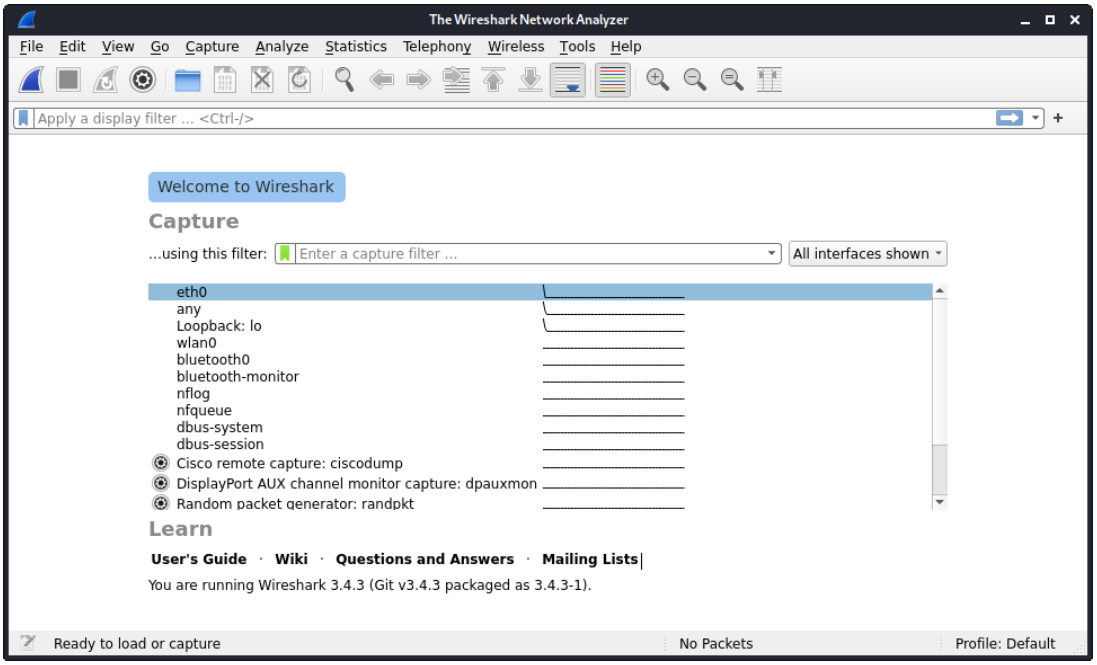

Figura 4.19: Wireshark interfaz

Una vez seleccionada la interfaz, Wireshark comienza a registrar el tráfico de la red, pero en nuestro caso solo nos interesan los paquetes DHCP por lo que se utiliza el filtro para poder visualizar los mensajes DHCP de una manera mas cómoda. Una vez Wireshark se encuentra a la escucha, se coencta el equipo que realizará la función de víctima al switch y se observa:

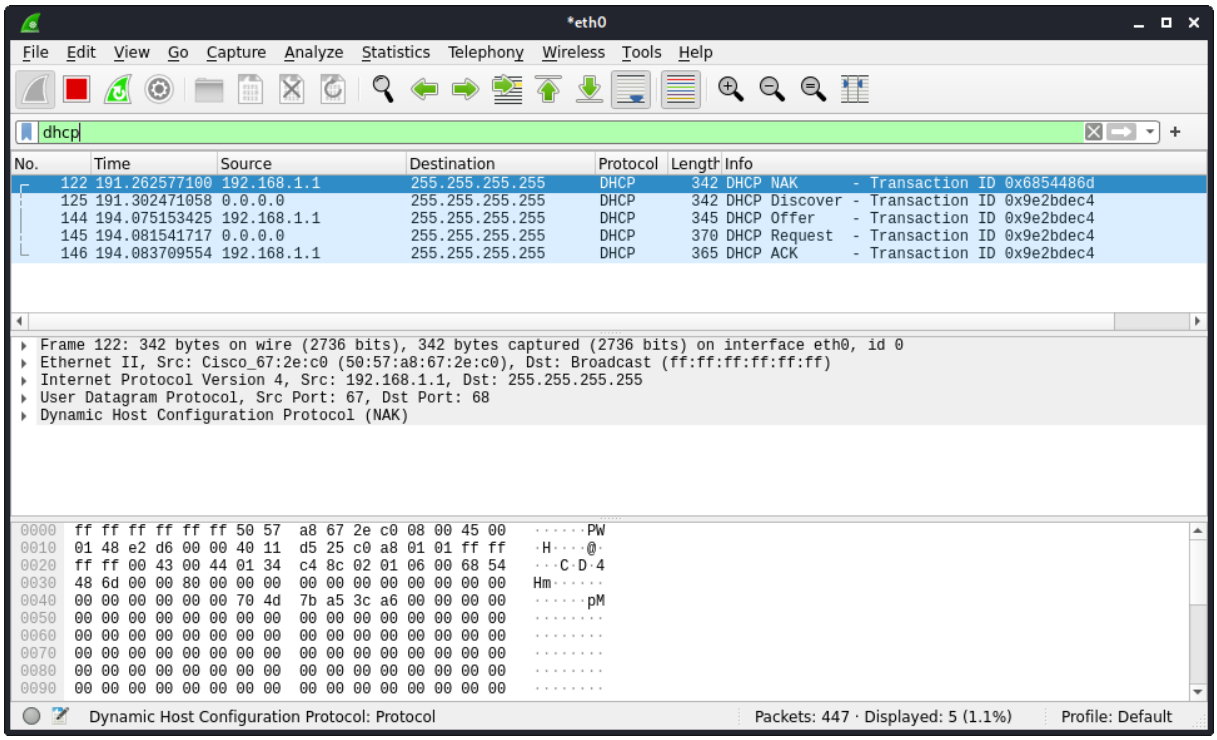

Figura 4.20: Wireshark Filtro

Como era de esperar, el equipo realiza el intercambio de mensajes del protocolo DHCP sin problemas y dispone de la información necesaria para navegar por la red. Se va a dejar Wireshark a la escucha para analizar el tráfico que va a generar el ataque DHCP spoofing.

Como se ha mencionado anteriormente, se va a llevar a cabo el ataque DHCP spoofing utilizando la herramienta Ettercap. Para comenzar con el ataque, se abre Ettercap, se hace click en el botón MITM menu y se selecciona DHCP spoofing.

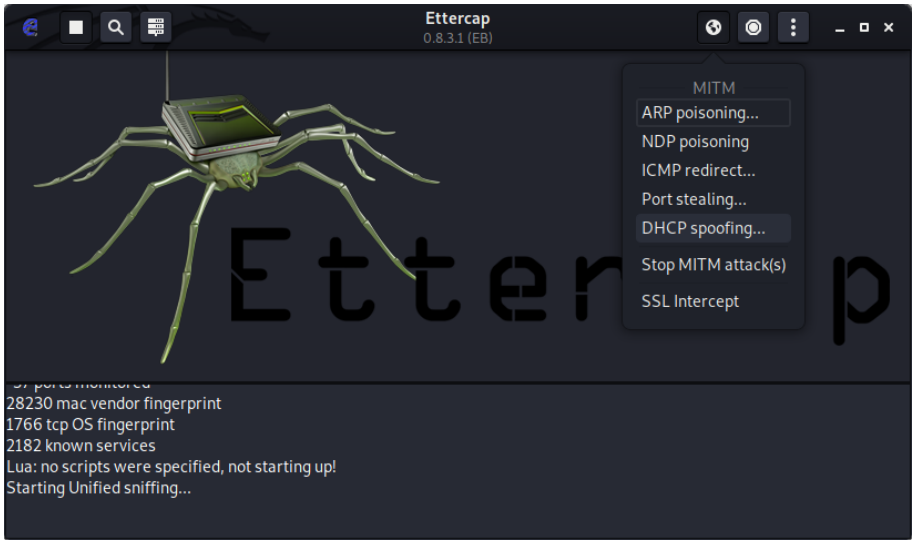

Figura 4.21: Ettercap MITM

Ettercap permite configurar tres parámetros:

- **IP Pool:** permite indicar el rango de direcciones IP que pueden ser asignadas a las víctimas. Si se deja en blanco, la dirección IP asignada a la víctima será la que indique el servidor DHCP.
- **Netmask:** máscara de la red.
- **DNS server IP:** dirección IP del servidor DNS. En nuestro caso, vamos a indicar como DNS a la misma máquina atacante.

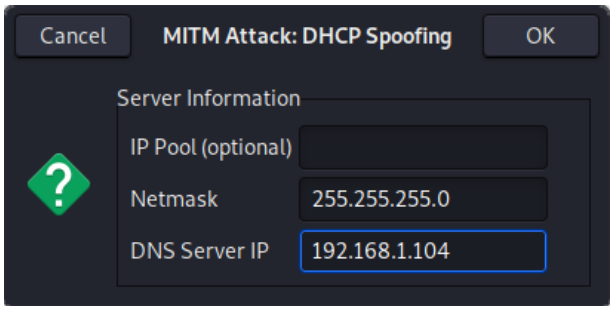

Figura 4.22: Ettercap configuración

Una vez configurado se hace click en 'OK'. De esta forma se ha iniciado el ataque, y en el momento en que un dispositivo solicite una dirección IP mediante el protocolo DHCP, tanto el servidor DHCP como el atacante van a responder a dicha solicitud y si la respuesta del atacante consigue ser más 'rápida' que la del servidor DHCP, el ataque se habrá realizado con éxito. Cabe destacar que puede ser necesario que la víctima solicite varías veces una dirección IP hasta que la respuesta del atacante sea más 'rápida' que la del servidor DHCP.

Con el ataque DHCP spoofing en marcha, se solicitan direcciones IP mediante el protocolo DHCP en el equipo víctima haciendo uso de los comandos:

```
ipconfig/release // Liberar dirección IP
ipconfig/renew // Sokicitar dirección IP
```

Una vez que el atacante responda a la petición del cliente, este último recibira la configuración de red mediante un mensaje DHCP y asignará como Puerta de enlace y servidor DNS la dirección IP del equipo atacante. se puede comprobar que el ataque se realizado con éxito de dos maneras:

1. Analizando el tráfico en Wireshark: se puede observar que el mensaje ACK del protocolo DHCP indicá como Router y Domain Name Server la dirección 192.168.1.104, que es justamente la dirección IP del atacante.

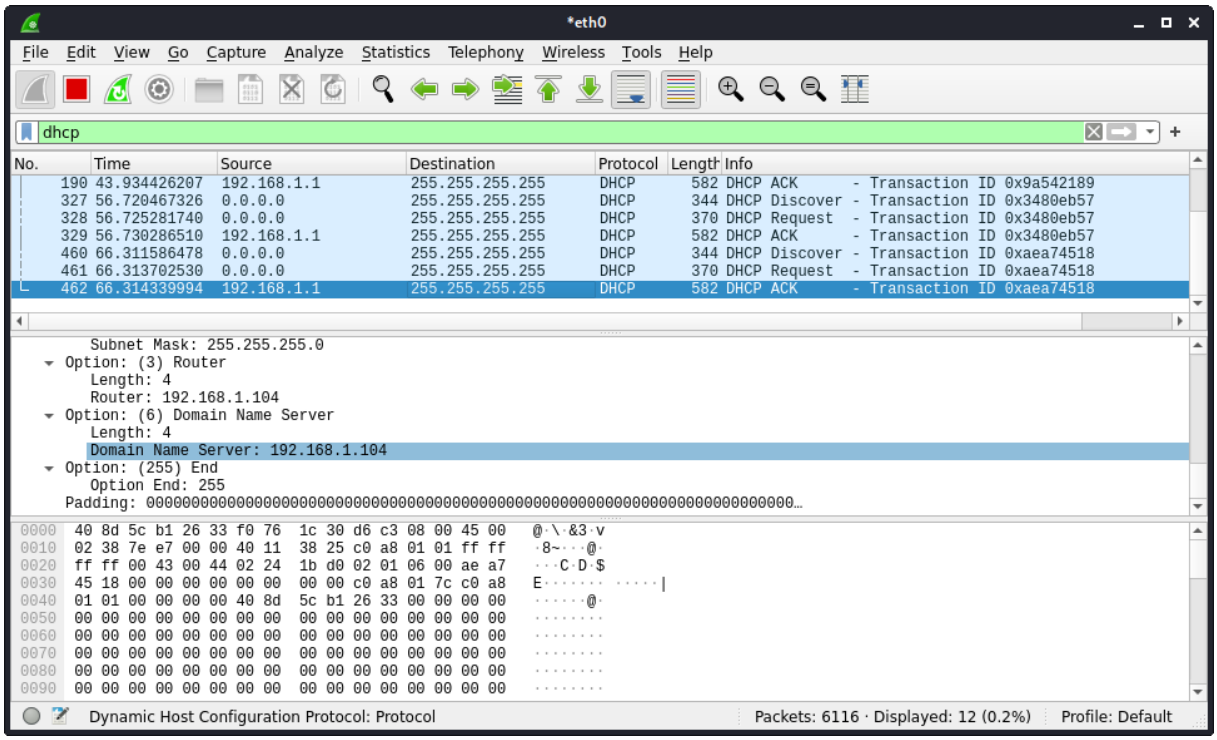

Figura 4.23: Wireshark mensaje ACK

2. Comando ipconfig/all: en la máquina víctima ejecutando el comando ipconfig/all se puede observar que tanto la Puerta de enlace predeterminada como el Servidor DNS tienen asignados la dirección IP del atacante, 192.168.1.104.

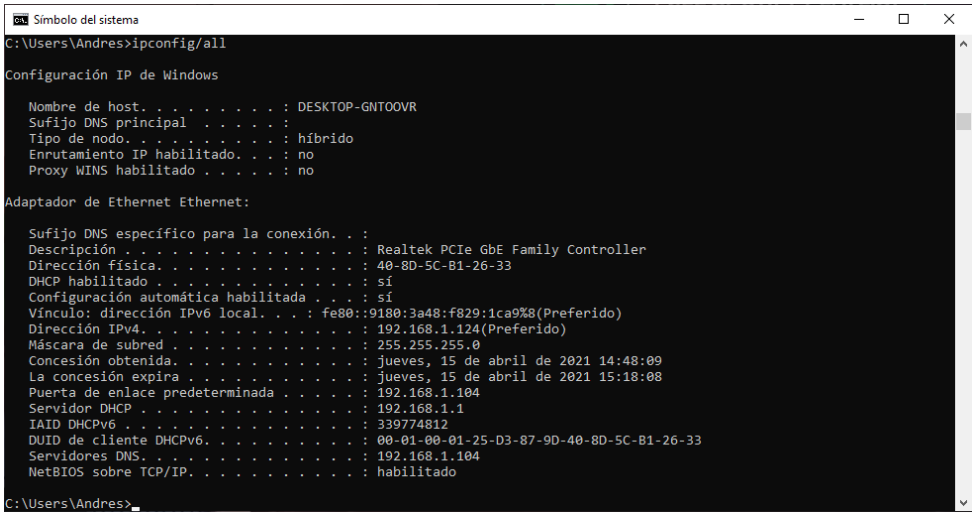

Figura 4.24: ipconfig/all

Por último, se comprueba que el tráfico generado por la víctima pasa a través del atacante antes de llegar a su destino. Para ello se usa el comando tracert -d 8.8.8.8 en el equipo víctima y en la máquina atacante, haciendo uso de Wireshark, se filtran los paquetes por el protocolo ICMP y se observa que aparece tráfico con origen 192.168.1.124 y destino 8.8.8.8, lo que significa que dicho tráfico generado por la víctima circula a través del atacante antes de llegar al destino 8.8.8.8.

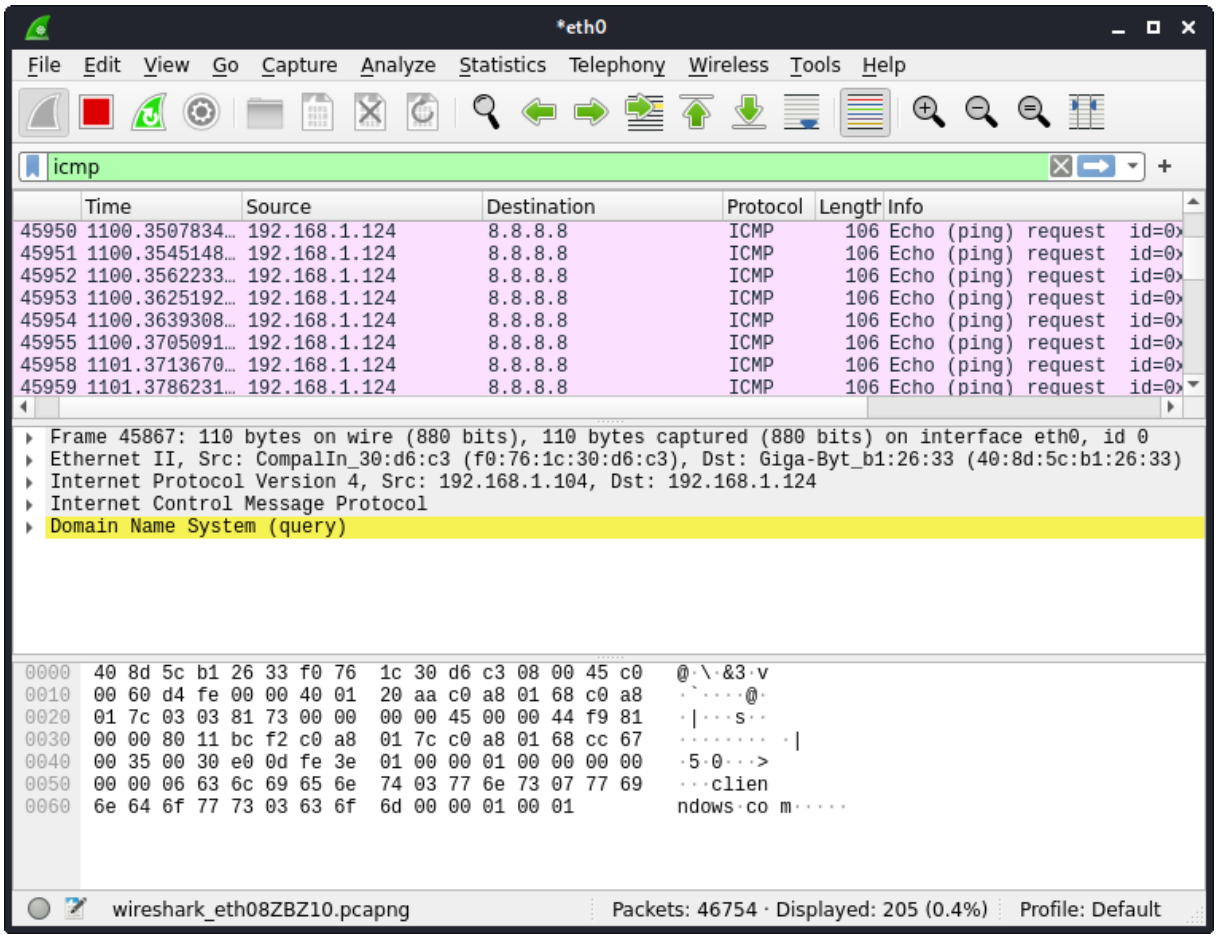

Figura 4.25: Wireshark ICMP

4.5.2. Ataque Hambre DHCP

Otro tipo de ataques que pueden afectar al correcto funcionamiento de nuestra red LAN son los ataques de denegacion de servicio (DoS). Un atacante puede sobrecargar el servidor DHCP con mensajes DHCP Discover utilizando diferentes direcciones MAC mediante software para agotar el rango de direcciones IP que el servidor DHCP tiene para ofrecer, provocando la caída del servidor y por ende que ningún dispositivo pueda recibir direcciones IP ni hacer uso de la red. Este ataque se conoce como 'Ataque de hambre DHCP' y para llevarlo a cabo se va a utilizar la herramienta Yersinia en una distribución Kali Linux.

Yersinia es una herramienta que nos permite llevar a cabo ataques de capa 2. Es posible que dicha herramienta no se encuentre instalada en las distribuciones Kali Linux, simplemente ejecutamos 'sudo apt-get install yersinia'. Cabe destacar que Yersinia se encuentra en su versión 0.8.2 por lo que es posible experimentar algún tipo de bugs durante su uso.

En primer lugar, se comprueba que nuestra máquina puede acceder al servidor DHCP, el router en nuestro caso, sin problemas:

Figura 4.26: Ping a servidor DHCP

Se abre la interfaz gráfica de la herramienta Yersinia mediante el comando 'yersinia -G' y se hace click en 'Launch attack'. En la ventana emergente, se selecciona la pestaña DHCP y se marca la opción 'Sending DISCOVER packet'. Se hace click en 'OK' y el ataque comienza automáticamente.

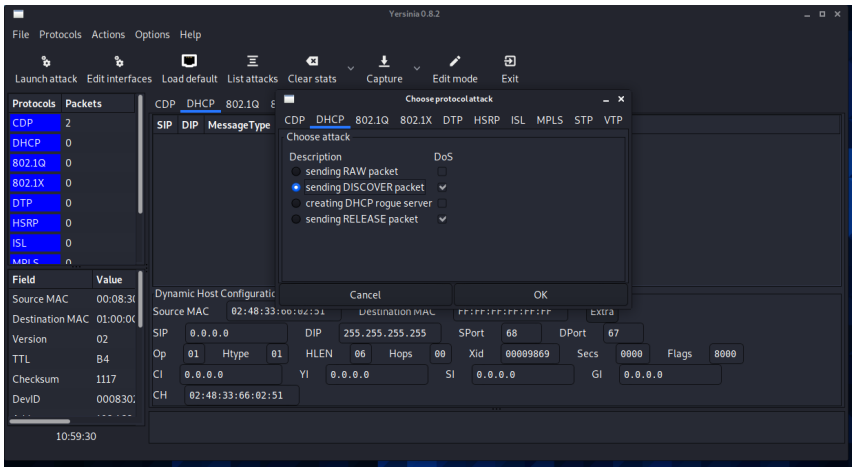

Figura 4.27: Configuración Yersinia

Se observa a la izquierda de la ventana el contador con el número de paquetes DHCP enviados, y en la parte central cada uno de los paquetes. En cuanto a la parte inferior donde se encuentran los elementos configurables, únicamente cabe destacar que los parámetros 'Source MAC' y 'Destination MAC' establecen el rango de direcciones MAC a utilizar en el envío de paquetes DISCOVER.

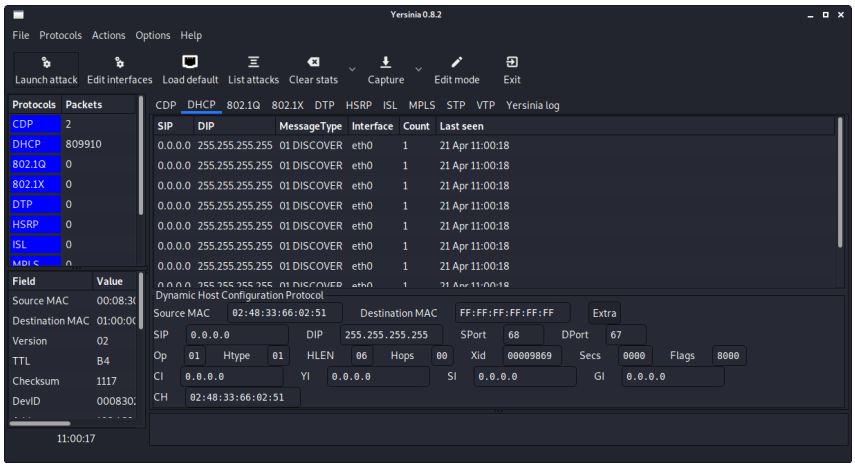

Figura 4.28: Yersinia

Para comprobar que el ataque se está llevando acabo y que está provocando una denegación de servicio en el servidor DHCP podemos volver a hacer ping observar que no se recibe respuesta.

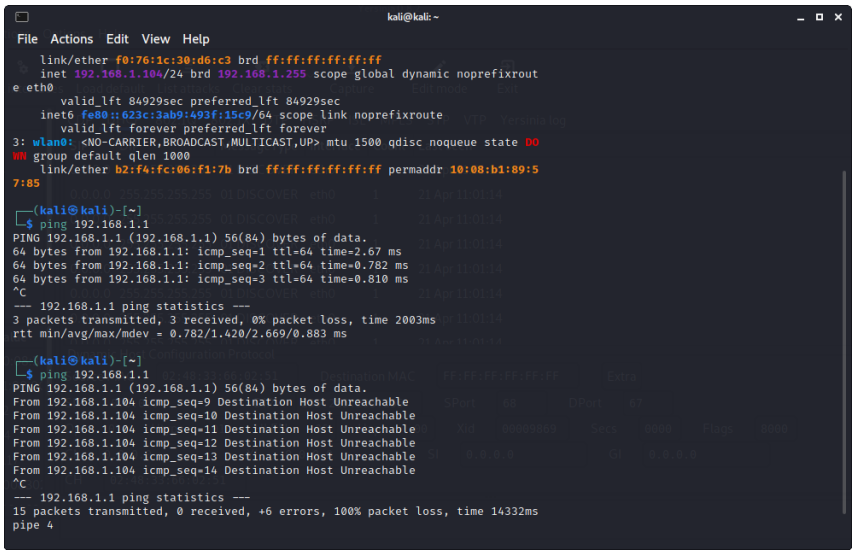

Figura 4.29: Ping a servidor DHCP

Por último, utilizando la herramienta Wireshark durante el ataque, se puede analizar el tráfico DHCP y observar que, efectivamente, el servidor DHCP reserva direcciones IP para cada uno de los paquetes DISCOVER recibidos hasta agotar el rango de direcciones disponibles, lo que provoca la denegación de servicio.

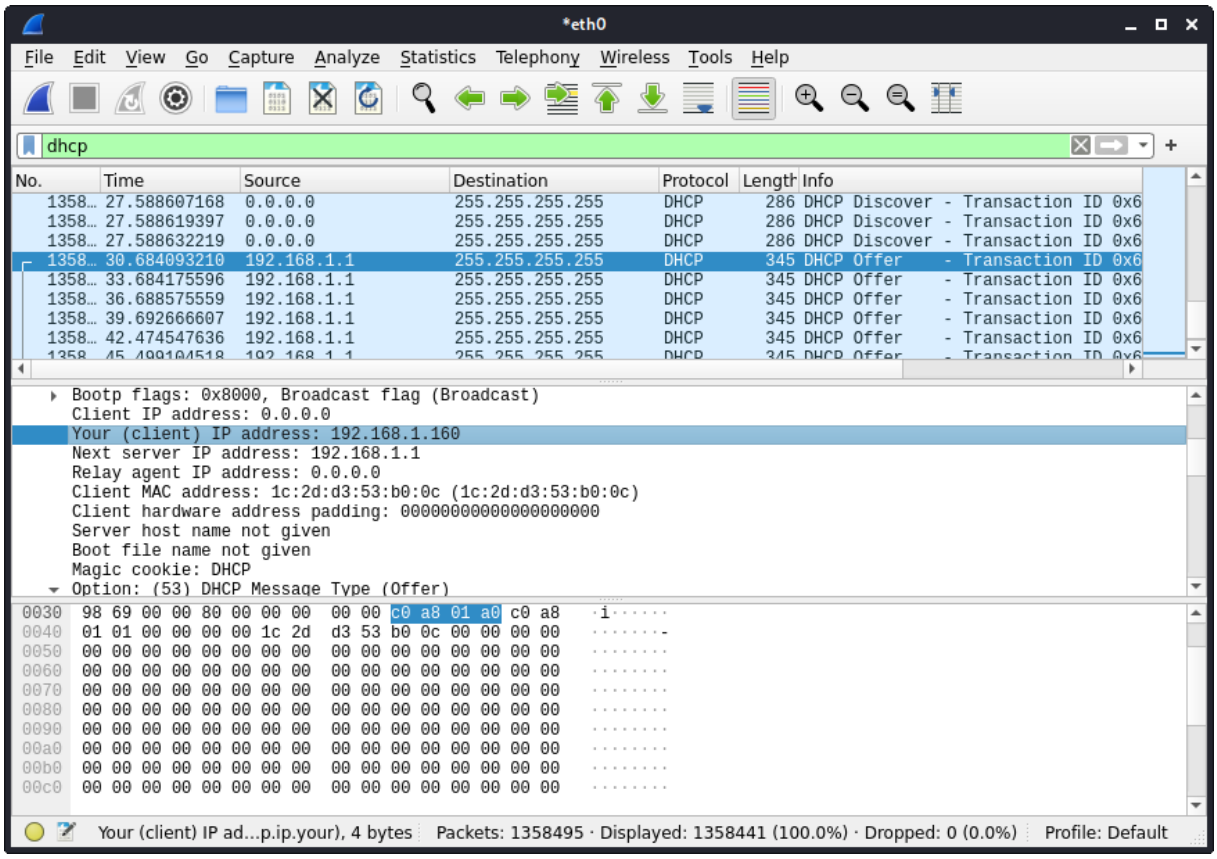

Figura 4.30: Wireshark

4.5.3. Configuracion Indagación DHCP

Una vez expuestas las vulnerabilidades de nuestra red LAN provocadas por el protocolo DHCP, se va a llevar a cabo el proceso de configuración necesario en nuestros equipos de comunicaciones para solventar dichas vulnerabilidades. El mecanismo que nos permite defendernos de los ataques expuestos anteriormente se conoce como DHCP snooping o indagación DHCP, ver sección 3.4.

El proceso de configuración de indagación DHCP se lleva a cabo en el switch, por lo que se accede a la interfaz web del mismo y se comienza con la configuración:

En primer lugar se accede a la ventana IP configuration >DHCP snooping/relay >Properties donde se pueden configurar los siguientes campos:

- **Opción 82:** habilita la Opción 82 para insertar información de la Opción 82 a los paquetes.
- **Retransmision DHCP:** habilita la retransmision DHCP.
- **Estado de undagación de DHCP:** habilita la indagación DHCP. Si se encuentra habilitada, se pueden seleccionar los siguientes campos:

- **Transferencia de la opción 82:** seleccione esta opción para dejar la información remota de Opción 82 cuando reenvía paquetes.

- **Verificar dirección MAC:** verifica que la dirección MAC de origen del encabezado de capa 2 coincida con la dirección de hardware del cliente tal como aparece en el Encabezado de DHCP (parte de la carga) en los puertos no confiables de DHCP.

- **Base de datos de respaldo:** mantiene una copia de seguridad de la base de datos de vinculación de indagación DHCP en la memoria flash del dispositivo.

- **Intervalo de actualización del respaldo de la base de datos:** frecuencia con la que se realiza el backup de la base de datos de vinculación de indagación DHCP

Para añadir un servidor DHCP, simplemente se hace click en **Añadir** y se ingresa la dirección IP del servidor DHCP.

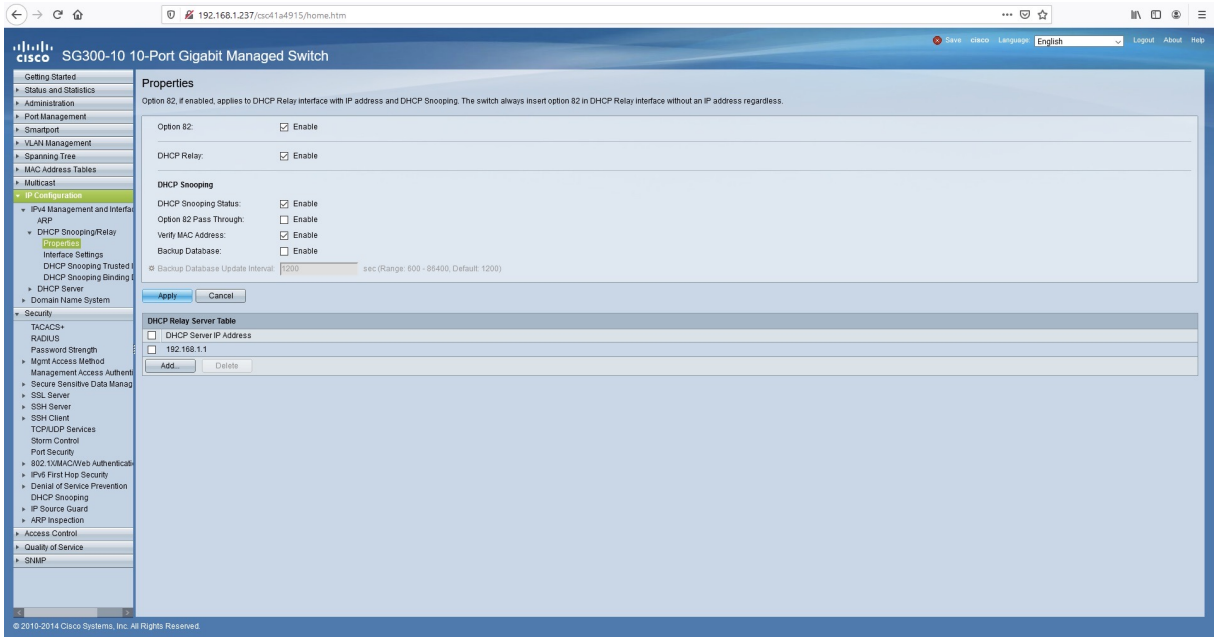

Figura 4.31: DHCP snooping propiedades

El siguiente paso consiste en indicar en que VLANs va a habilitarse la indagación y retransmisión DHCP. Para ello se abre la ventana IP configuration >DHCP snooping/relay >Interface Setting y se hace click en **Añadir**.

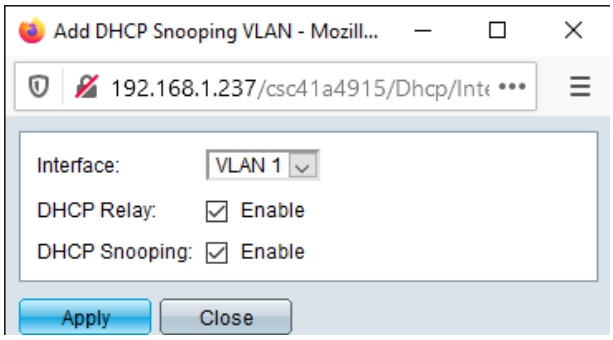

Figura 4.32: DHCP snooping VLAN

Se indica la VLAN que se quiere añadir y se seleccionan las opciones indagación DHCP y retransmision DHCP. Se hace click en **Aplicar**.

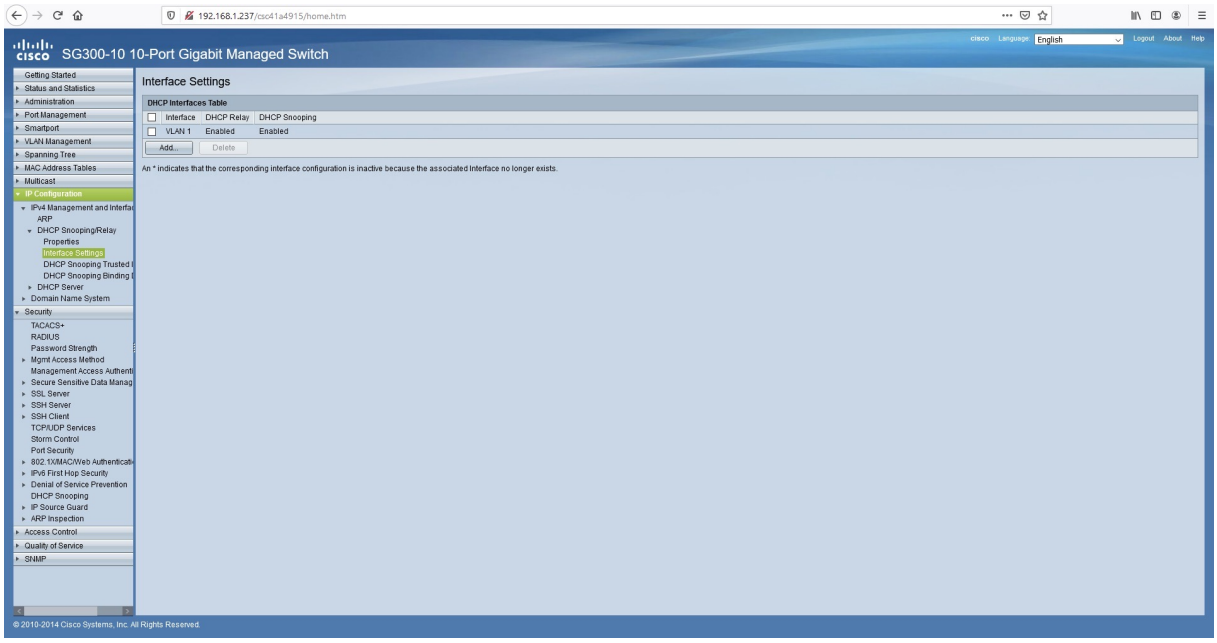

Figura 4.33: Interface Setting

Como se ha visto en la sección 3.4, con el mecanismo de indagación DHCP se distinguen puertos confiables y no confiables en el switch, y por defecto todos los puertos se encuentran configurados como no confiables. Para cambiar la configuración de los puertos se accede a la ventana IP configuration >DHCP snooping/relay >DHCP Snooping Trusted Interfaces, se selecciona un puerto y se hace click en **Edit**.

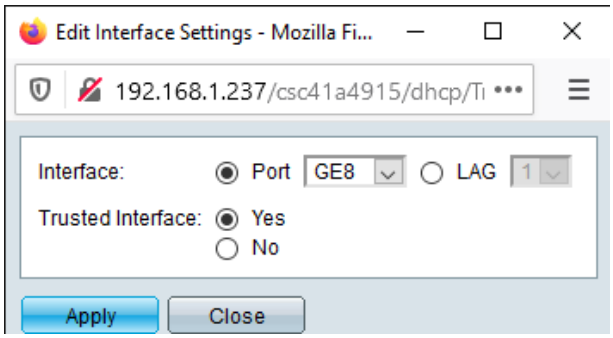

Figura 4.34: Editar puertos confiables

Se marca la opción 'yes' o 'no' dependiendo de si se quiere configurar el puerto como confiable o no confiable. Se debe marcar como confiable únicamente el puerto donde conecte el servidor DHCP, en nuestro caso el puerto GE8. Llegados a este punto, ya se encuentra activo en el switch la indagación DHCP.

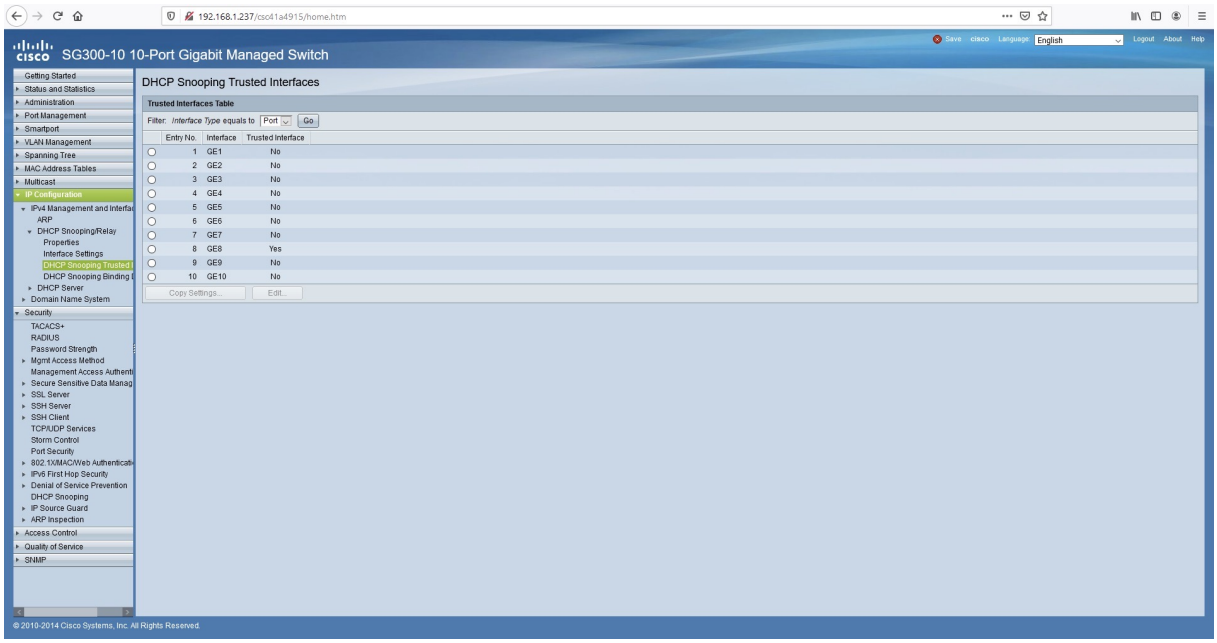

Figura 4.35: Puertos confiables

por último, se va a echar un vistazo a la base de datos de vinculación de indagación DHCP en la pestaña IP configuration >DHCP snooping/relay >DHCP Snooping Binding Database.

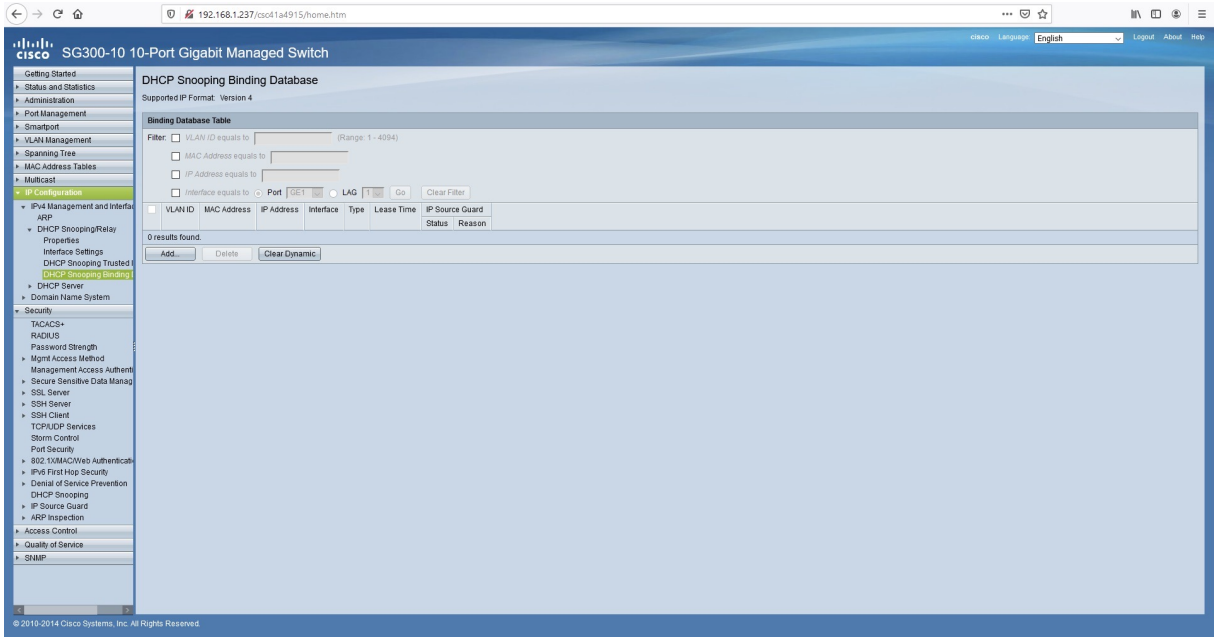

Figura 4.36: Base de datos

La base de datos de vinculación de indagación DHCP dispone de un filtro para buscar entradas en la base de datos por VLAN ID, MAC, IP o interfaz. También nos permite añadir entradas manualmente indicando:

- **ID de VLAN:** VLAN en la que se espera el paquete.
- **Dirección MAC:** dirección MAC del paquete.
- **Dirección IP:** dirección IP del paquete.
- **Interfaz:** puerto en el que se espera el paquete.
- **Tipo:**
  - **Dinámico:** la entrada tiene tiempo de concesión limitado.
  - **Estático:** la entrada se configuró de manera estática.
- **Tiempo de concesión:** en caso de que la entrada sea dinámica, indica el tiempo que la entrada permanecerá activa en la base de datos.

Las entradas se añadirán a la base de datos automáticamente tal cual se explica en la sección 3.4, de forma que en el momento en el que un equipo se conecte a la red y realice el intercambio de mensajes DHCP con el servidor DHCP, dicho equipo se añadirá automaticamente a la base de datos:

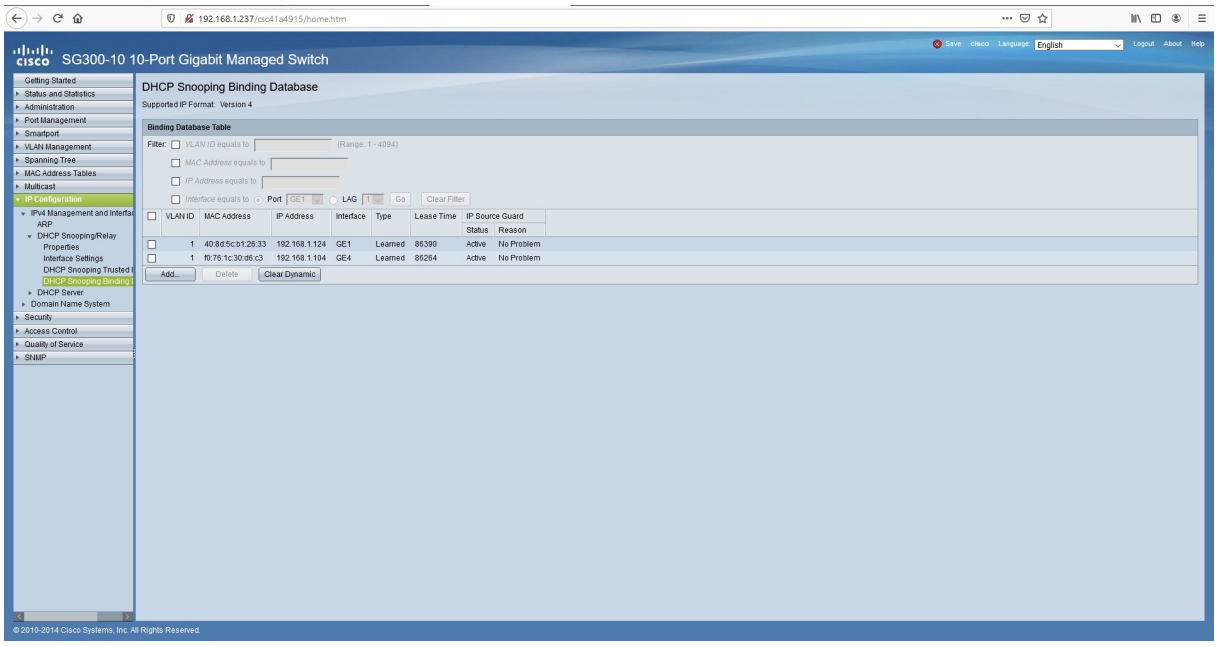

Figura 4.37: Base de datos

De esta forma, nuestra red LAN queda protegida contra ataques como los expuestos anteriormente, DHCP spoofing y Hambre DHCP, además de llevar el control de los dispositivos conectados a la red mediante las entradas de la base de datos de vinculación de DHCP, la cual será necesaria en la siguiente sección para implementar otro mecanismo de seguridad denominado Inspección ARP.

En la sección 5.3 se pone a prueba la efectividad del mecanismo indagación DHCP.

4.6. Ataque de envenenamiento ARP y configuración inspección ARP

La configuración de los equipos a utilizar va a ser la misma que la mostrada en la tabla 4.3, con la diferencia de que el switch implementará la tecnología inspección ARP.

El ataque conocido como ARP poisoning o envenenamiento ARP, explicado en la sección 3.5, es otro ataque de tipo MITM que permite a un atacante interceptar todo el tráfico proveniente de la víctima haciendo uso de vulnerabilidades presentes en el protocolo ARP.

Para llevar a cabo dicho ataque, se va a utilizar la misma herramienta que en el apartado anterior 4.5, Ettercap.

Los dispositivos almacenan los pares de direcciones IP-MAC en la caché ARP, a la que podemos acceder mediante el comando ’arp -a’.

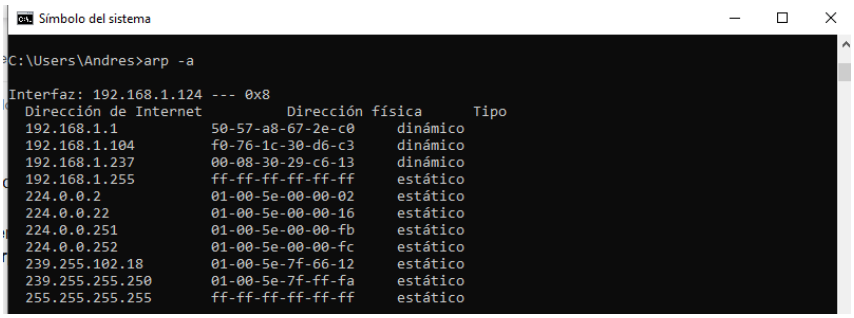

Figura 4.38: arp -a

Una vez realizado el ataque, se accedera de nuevo a la caché ARP del dispositivo y se comprobaran los resultados.

4.6.1. Envenenamiento ARP

En primer lugar, se abre la herramienta Ettercap y se hace click en 'Host list'. Ettercap realiza un escaneo de la red y muestra los dispositivos encontrados. Para llevar a cabo el ataque, se tienen que seleccionar dos objetivos (Target), el primer target será el ordenador que queremos monitorizar y el segundo target la puerta de enlace. Para asignar los objetivos se selecciona el dispositivo correspondiente y se hace click en 'Add to Target 1' y 'Add to Target 2' respectivamente.

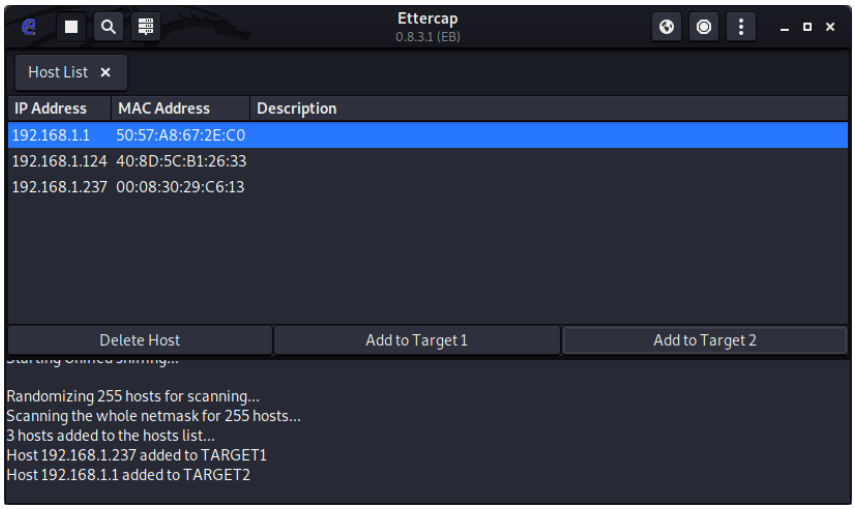

Figura 4.39: añadir objetivos

Asignados los objetivos podemos comenzar el ataque, se hace click en'MITM menu' y se selecciona ARP poisoning.

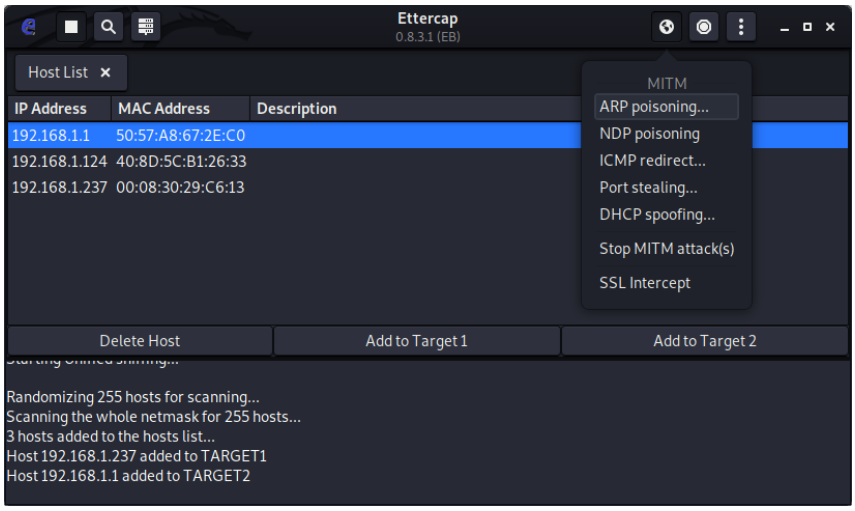

Figura 4.40: ARP poisoning

Ettercap permite seleccionar dos parámetros opcionales:

- **Sniff remote connections:** este parametro nos permite a Ettercap rastrear conexiones que pasen a traves de la puerta de enlace, a parte de la conexión entre los objetivos.

- **Only poison one-way:** Ettercap envenenará unicamente la conexion desde el objetivo 1 al objetivo 2, en una única dirección.

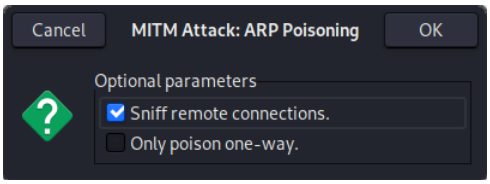

Figura 4.41: Parametros ARP

Por último se hace click en 'OK' y el ataque comenzará automaticamente. Se oyede comprobar que efectivamente se ha producido el envenenamiento ARP utilizando la herramienta Wireshark en el atacante y observando que se intercepta todo el tráfico de la víctima. Pero, como se ha mencionado anteriormente, también se puede observar la caché ARP de la víctima con el parámetro arp -a

Figura 4.42: arp -a

Y observar que tanto las direcciones 192.168.1.1 (Puerta de enlace) y 192.168.1.104 (atacante) tienen asignadas la misma dirección MAC.

4.6.2. Inspección ARP

Para evitar los ataques de envenenamiento ARP se puede configurar en el Switch el mecanismo de seguridad conocido como Inspección ARP, explicado en la sección 3.5. Para ello se accede a la interfaz web del Switch y se abre la ventana Security >ARP inspection >Properties. En esta ventana se puede configurar la Inspección ARP mediante los siguientes parámetros:

- **Estado de inspección ARP:** habilita la Inspección ARP.
- **Validación de paquete de ARP:** habilita las siguientes comprobaciones de validación:
  - **MAC de origen:** compara la dirección MAC de origen del paquete que aparece en el encabezado Ethernet con la dirección MAC del remitente que aparece en la solicitud ARP. La comprobación se realiza tanto en las solicitudes como en las respuestas ARP.
  - **MAC de destino:** compara la dirección MAC de destino del paquete que aparece en el encabezado Ethernet con la dirección MAC de la interfaz de destino. Esta comprobación se realiza para las respuestas ARP.
  - **Direcciones IP:** compara el cuerpo ARP para detectar direcciones IP no válidas o inesperadas. Las direcciones incluyen 0.0.0.0, 255.255.255.255 y todas las direcciones IP de multidifusión.
- **Intervalo de búfer de registro:**
  - **Frecuencia de reintento:** habilita el envío de mensajes SYSLOG para los paquetes descartados. Permite ingresar la frecuencia con la que se envían los mensajes.
  - **Nunca:** deshabilita el envio de mensajes SYSLOG para paquetes descartados.

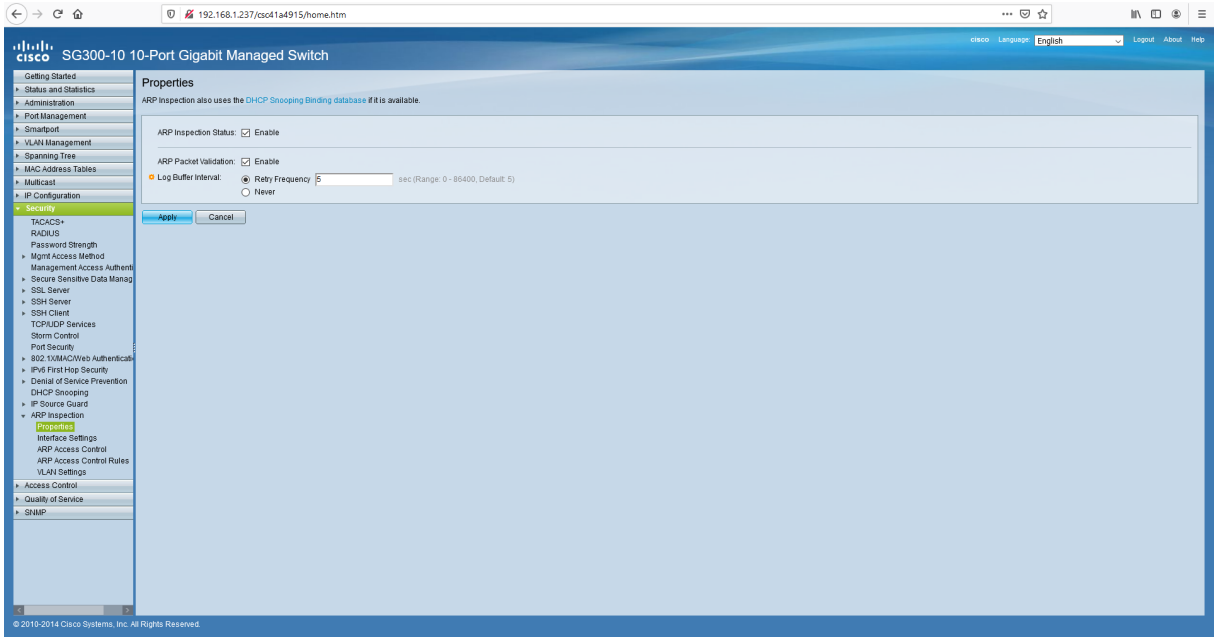

Figura 4.43: Propiedades

El siguiente paso es indicar las interfaces que se consideran confiables. El funcionamiento de interfaces confiables y no confiables es el mismo que el visto en la sección 3.4. Para ello se accede a la ventana Security >ARP inspection >Interface Settings, se seleccionan las interfaces que se quieren marcar como confiables y se hace click en 'Edit'. En la ventana emergente, se marca la casilla 'Yes' y se hace click en 'Apply'. En nuestro caso el puerto que conecta el Switch con el Router es el GE8, por ende es dicho puerto el que se tiene que marcar como confiable.

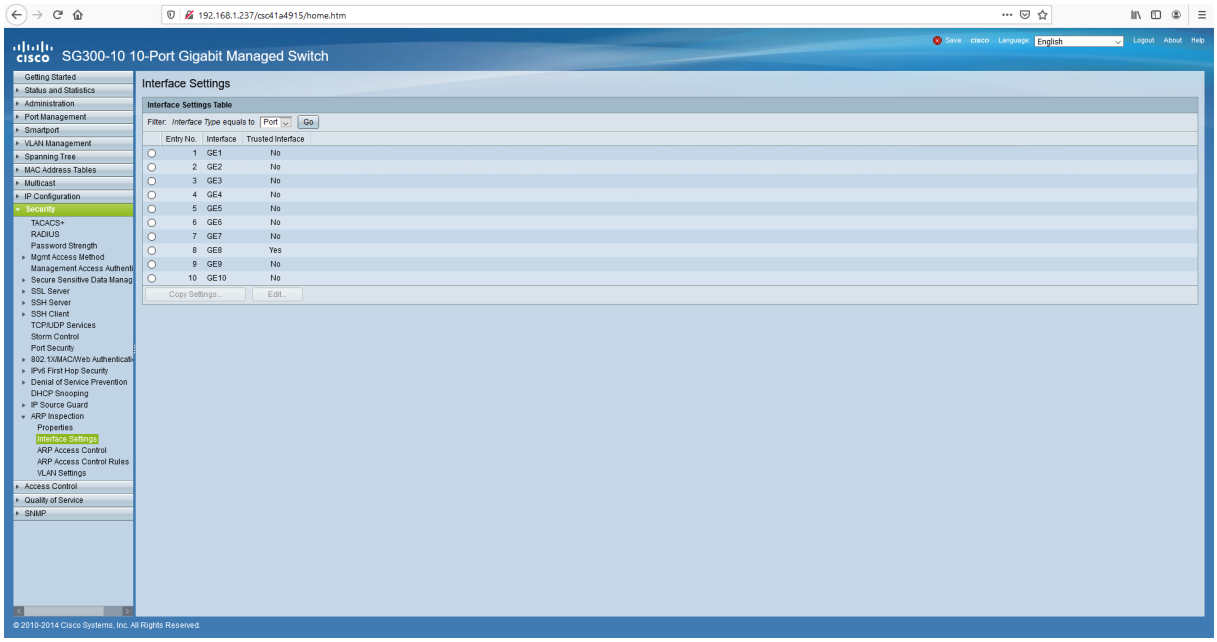

Figura 4.44: Configuración de interfaces

La Inspección ARP compara los pares de direcciones MAC-IP de los paquetes con las entradas presentes en la tabla de inspección ARP. Para añadir entradas a dicha tabla, se accede a la pestaña Security >ARP inspection >ARP Access Control y se hace click en 'Add'. Se indican el nombre de la lista de control de acceso ARP y las direcciones MAC-IP del paquete. Lógicamente, las direcciones MAC-IP deben de corresponderse con el mismo dispositivo.

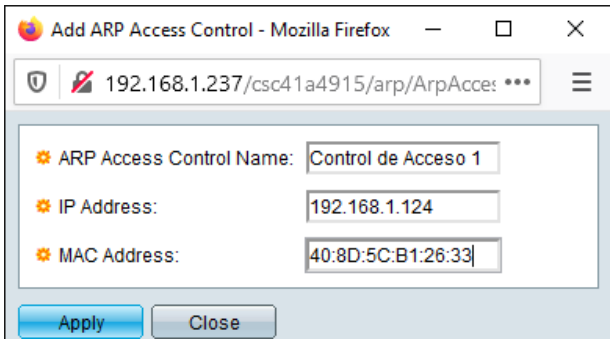

Figura 4.45: Añadir grupo reglas de acceso

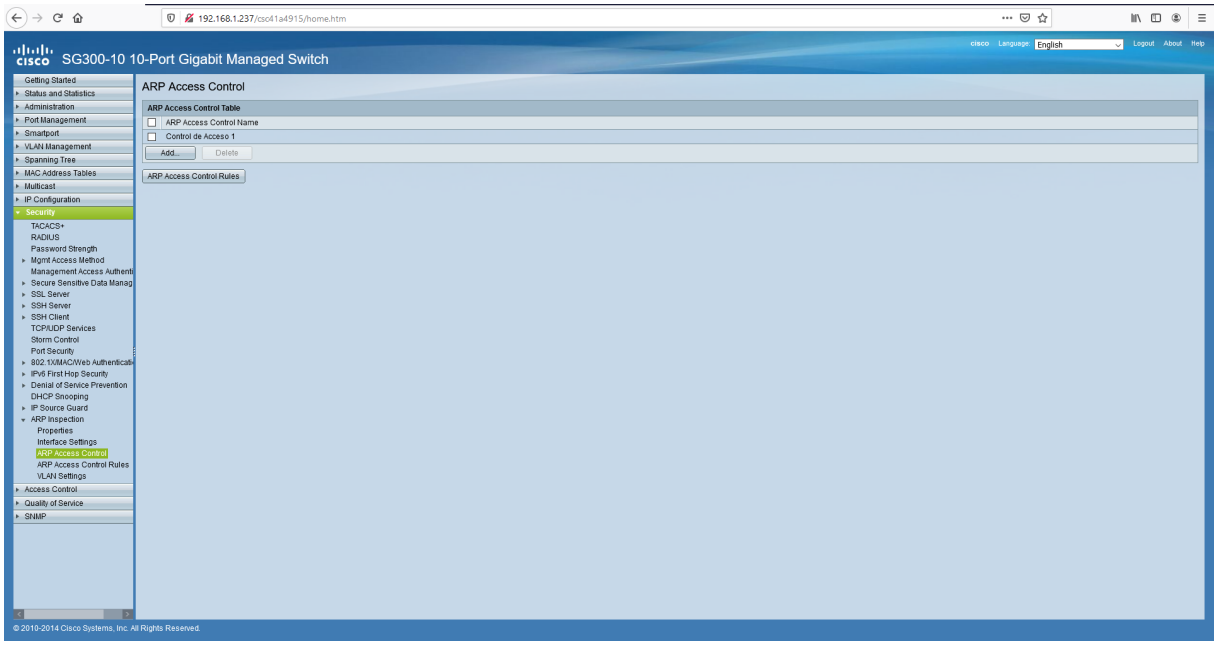

Figura 4.46: Grupos reglas de acceso

Si se quiere añadir mas reglas al grupo de control de acceso creado anteriormente, se hace click en Security >ARP inspection >ARP Access Control Rules. Se seleccuina el grupo al que se quiere añadir las nuevas reglas y se hace click en 'Add'. Se indica la dirección MAC-IP y se hace click en 'Apply', de esta forma se puede añadir todas las reglas que se necesiten. En nuestro caso, se han añadido dos reglas, una para el equipo que sufre el ataque de envenenamiento ARP, con dirección IP 192.168.1.124 y otra regla para el router.

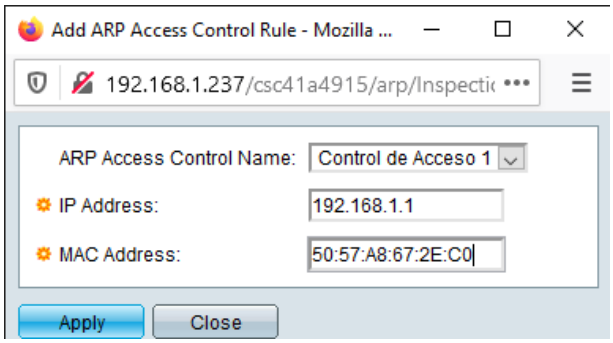

Figura 4.47: Añadir regla de acceso

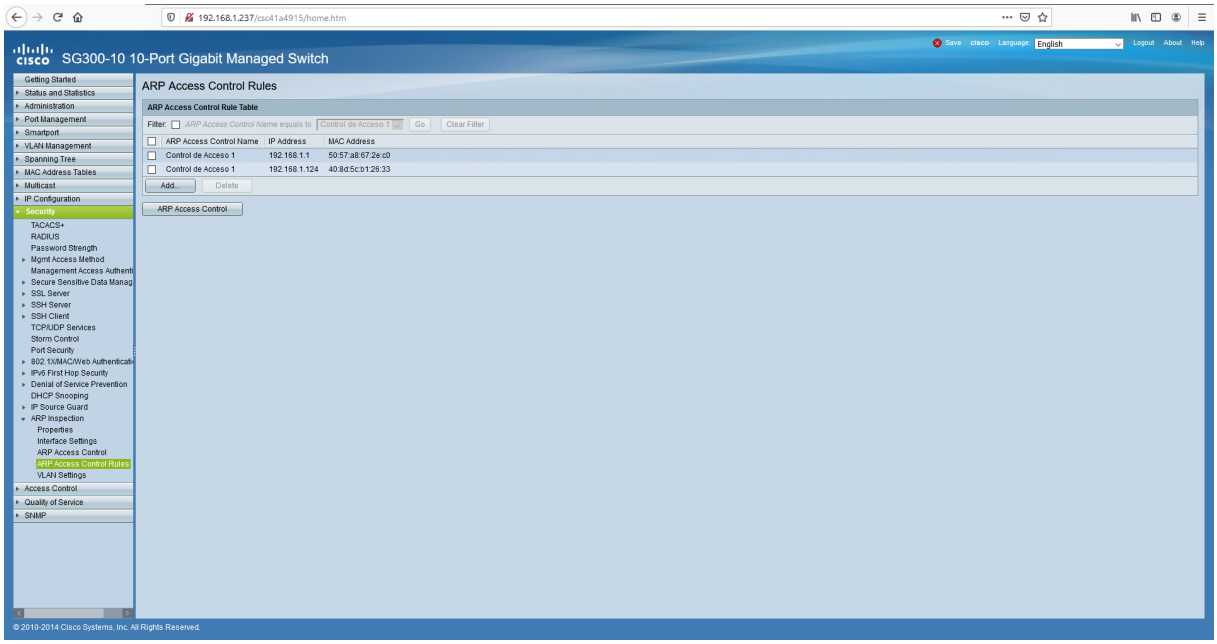

Figura 4.48: Reglas de acceso

Por útimo, se tiene que indicar en que VLANs va a llevarse a cabo la inspección ARP. Para ello se accede a Security >ARP inspection >VLAN Settings. En la parte superior se indican las VLANs que habilitan la inspección ARP y en la parte inferiores se indican que grupo de reglas de control de acceso ARP afectan a cada VLAN.

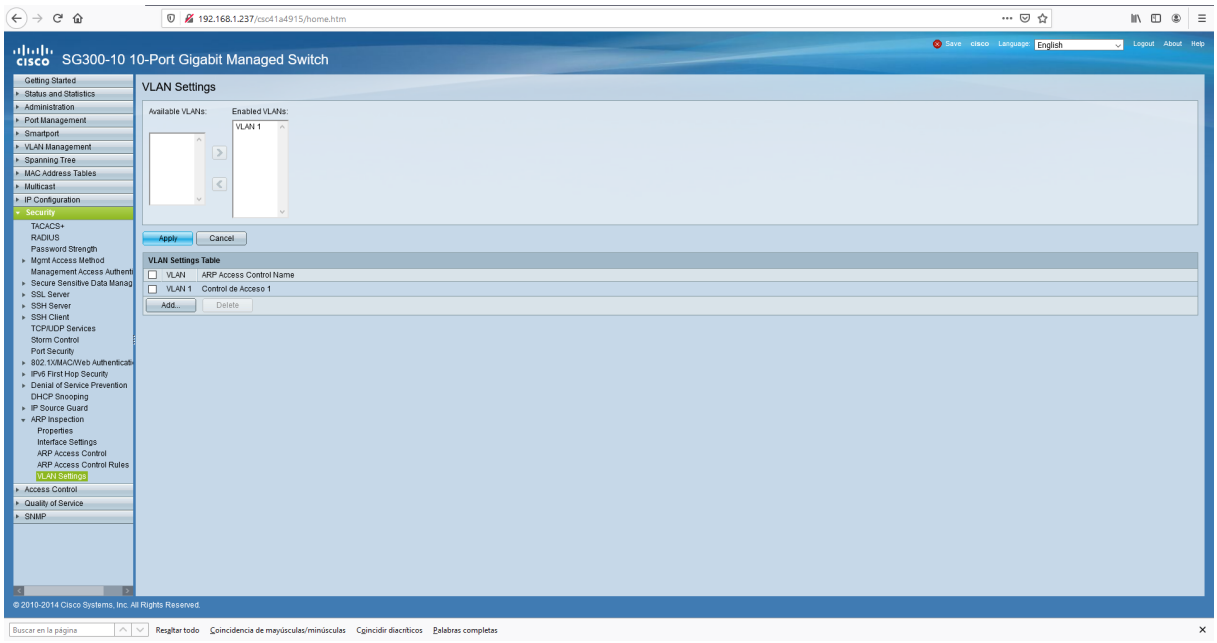

Figura 4.49: Configuración VLAN

Terminado el proceso de configuración de la inspección ARP, el ataque envenenamiento ARP no debería de tener ningún efecto puesto que el switch, al recibir un paquete con un par de direcciones MAC-IP que no esté registrado ni en la tabla de control de acceso ARP ni en la base de datos de vinculación de indagación DHCP, lo va a descartar impidiendo el envenenamiento de las cachés ARP de los dispositivos. En la sección 5.4 se comprueba la efectividad del mecanismo inspección ARP.

Capítulo 5

Resultados

5.1. Seguridad de puertos y IEEE 802.1X

Una vez configurado el estandar IEEE 802.1X, se puede comprobar su correcto funcionamiento conectando al puerto configurado (GE5) un dispositivo que haga la función de cliente. Vamos a utilizar un equipo con Window 10 que se tiene que configurar para que pueda llevar a cabo la auntenticación 802.1X. Para ello se conecta el equipo al puerto correspondiente y se observa que no se le permite el acceso a la red:

- En primer lugar, se pulsan simultáneamente las teclas 'Window + r' y se escribe 'services.msc'. Se busca el servicio denominado 'Configuración automática de redes cableadas' y se hace doble click, abriendo la ventana de propiedades de dicho servicio. en la opción 'Tipo de inicio' se selecciona 'Automática', y se hace click en el botón 'iniciar'.

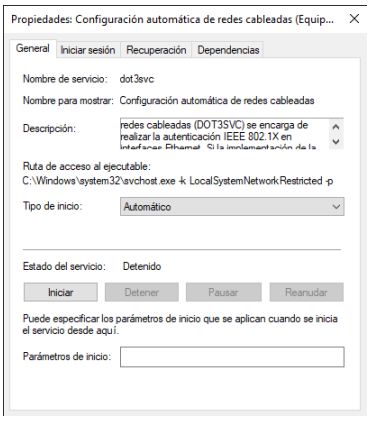

Figura 5.1: Propiedades servicio

- A continuación, se accede a Panel de control >Redes e internet >Conexiones de red >Ethernet >Propiedades y en la pestaña 'Autenticación', se habilita la autenticación IEEE 802.1X y como método de autenticación de red se selecciona PEAP.

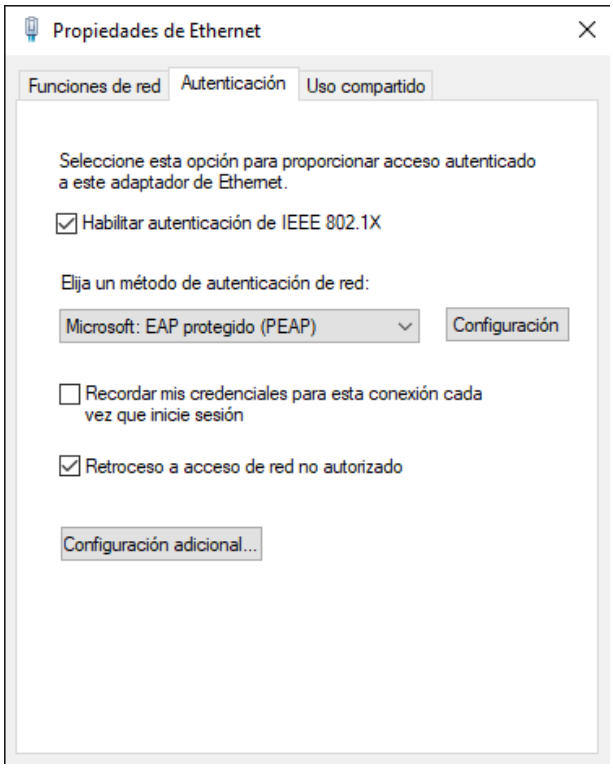

Figura 5.2: Propiedades Ethernet

Una vez configurado el cliente para utilizar IEEE 802.1X, al conectar el equipo a la red, se abre una ventana que pide introducir un nombre de usuario y contraseña. Si introducimos unas credenciales de usuario almacenadas en el servidor RADIUS, tendremos acceso a la red y podremos navegar por la misma libremente. En caso opuesto, se nos denegará el acceso a la red.

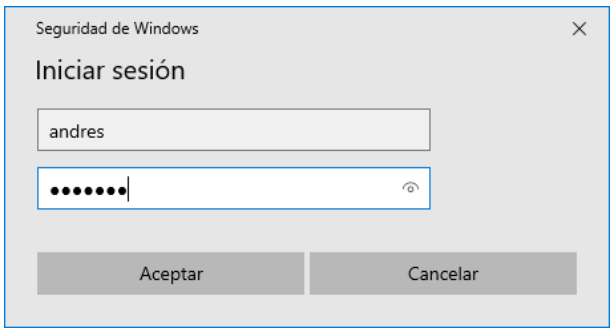

Figura 5.3: Login

Por último, se puede acceder de nuevo al Switch, y en la ventana Security >802.1X/-MAC/Web Authentication >Authenticated Hosts observar que el proceso de autenticación 802.1X del equipo conectado al puerto GE5 se ha llevado a cabo correctamente y ha sido añadida a la tabla de dispositivos autenticados.

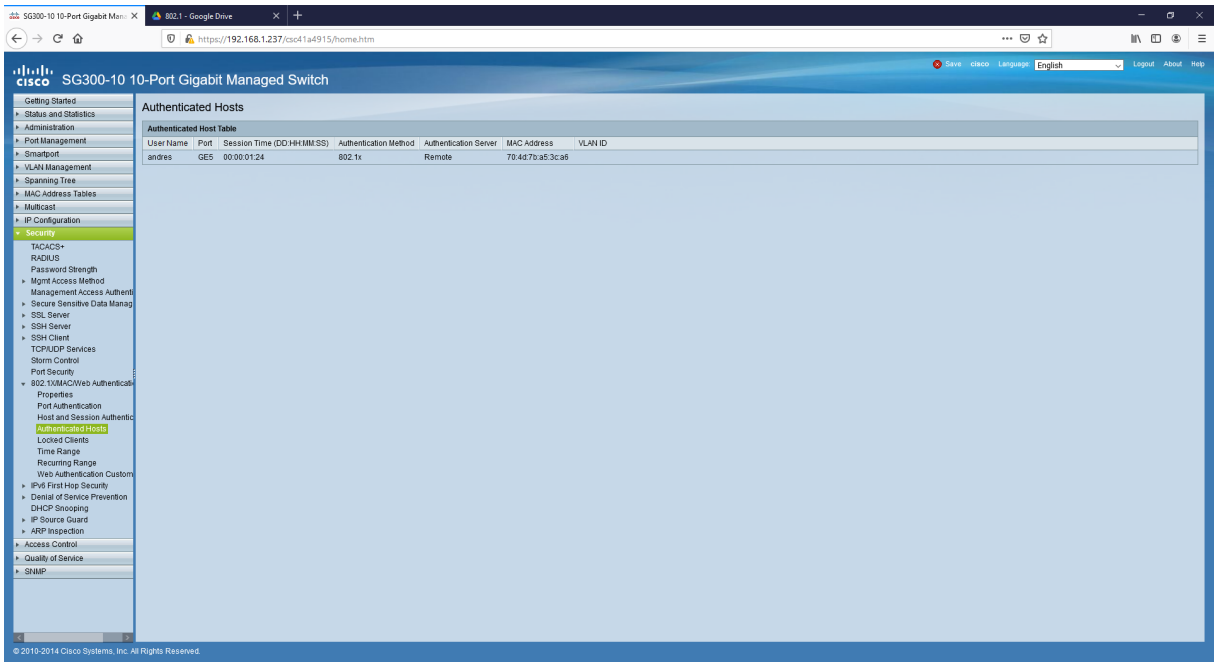

Figura 5.4: Login

5.2. Comunicación dentro de PVLAN

Como se ha visto en la sección 3.3 dependiendo de como se definan los puertos podemos gestionar la comunicación entre miembros de una PVLAN. Equipos que se encuentren en una VLAN de comunidad podrán comunicarse con el resto de equipos de la misma comunidad y con el puerto promiscuo, mientras que un puerto aislado solamente puede comunicarse con el puerto promiscuo.

De esta forma y en primer lugar, se definen los puertos GE4 y GE5 como puertos de comunidad pertenecientes a la VLAN de comunidad 22, y mediante la herramienta Ping se comprueba si pueden establecer conexión:

○	4	GE4	Private VLAN - Host	22	Admit Untagged Only	Enabled	2	22
○	5	GE5	Private VLAN - Host	22	Admit Untagged Only	Enabled	2	22

Figura 5.5: Puertos de comunidad

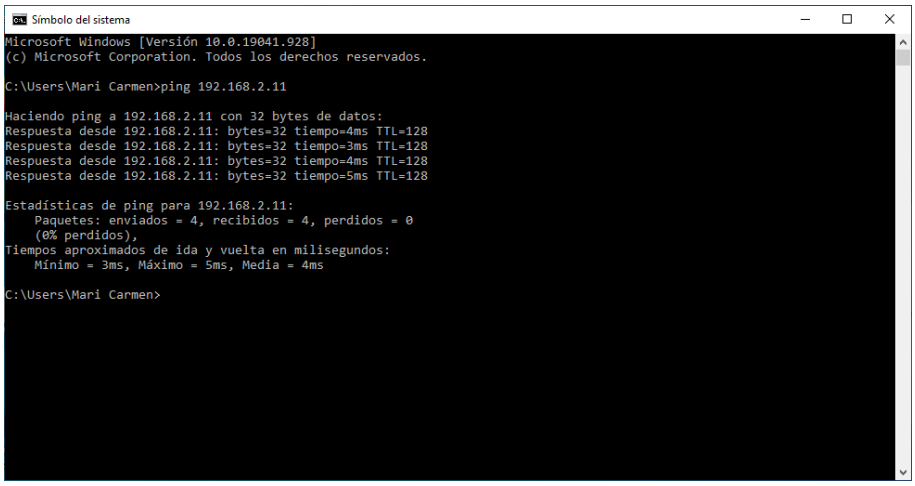

Figura 5.6: Ping entre misma comunidad

Los equipos pertenecientes a la misma VLAN de comunidad conectan entre sí como era de esperar. A continuación se va a configurar el puerto GE4 como aislado, asignándole la VLAN 21, y haciendo ping de nuevo, se comprueba que los equipos han perdido conexión puesto que uno pertenece a una VLAN aislada y otro a una VLAN de comunidad.

○	4	GE4	Private VLAN - Host	21	Admit Untagged Only	Disabled	2	21
○	5	GE5	Private VLAN - Host	22	Admit Untagged Only	Enabled	2	22

Figura 5.7: Puertos aislado y de comunidad

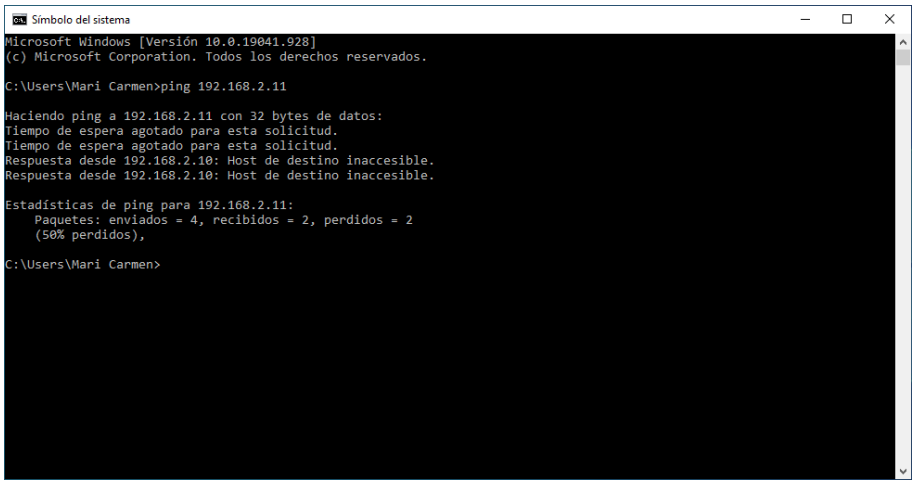

Figura 5.8: Ping entre puerto aislado y de comunidad

Debido a que el puerto GE4 está configurado como aislado, solo puede establecer comunicación con los puertos promiscuos, por lo que estando dentro de la misma VLAN que el resto de equipos, se encuentra aislado consiguiendo un nivel mas de segmentación dentro de una red LAN.

5.3. Comprobar resistencia a ataques DHCP

La configuración del mecanismo de seguridad Indagación DHCP en el switch dota a nuestra red LAN de inmunidad contra los ataques vistos en la sección 4.5. Para comprobarlo, se van a realizar de nuevo los mismo ataques y observar los resultados.

Por un lado, si repetimos el ataque de Hambre DHCP con la herramienta Yersinia, se puede comprobar que no se pierde la conexión con el servidor DHCP haciendo ping al mismo, pero es mas ilustrativo observar la base de datos de vinculación de Indagación de DHCP.

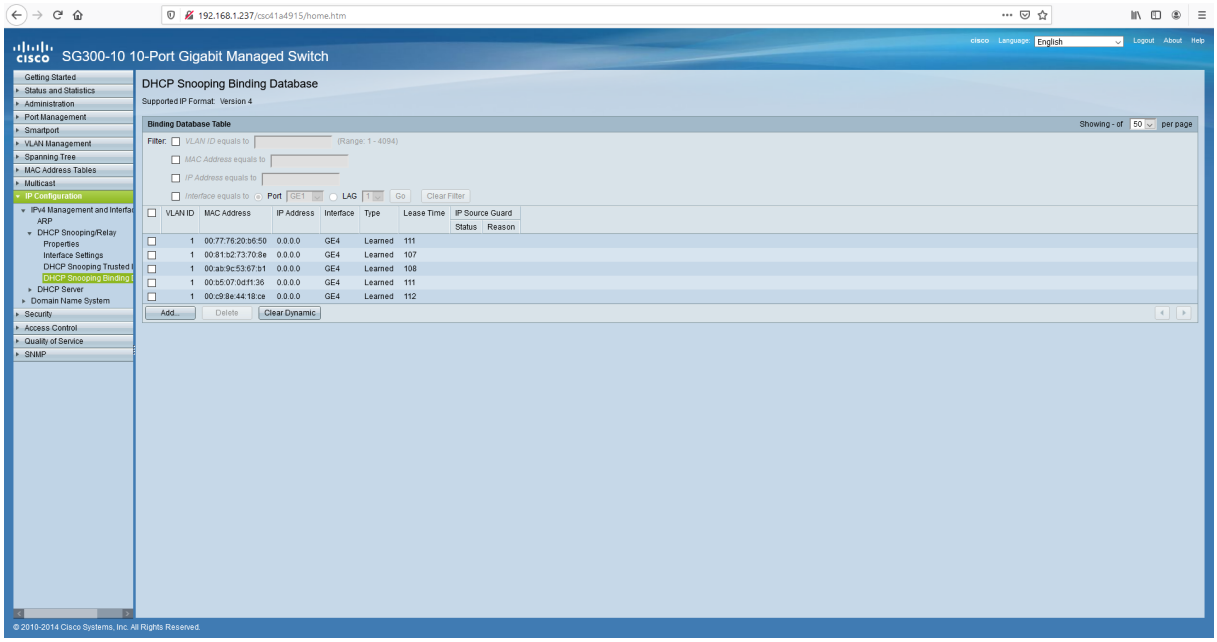

Figura 5.9: Base de datos DHCP

Se ve que se han incluido algunas entradas en la base de datos con dirección IP 0.0.0.0, esto se debe a que el switch, al recibir un exceso de mensajes DHCP DISCOVER, interpreta que se está llevando a cabo un ataque de este tipo, y mantiene las entradas en la base de datos como inactivas para no colapsar y provocar una denegación de servicio.

Por otro lado, al repetir el ataque DHCP spoofing, se observa el tráfico que captura Wireshark:

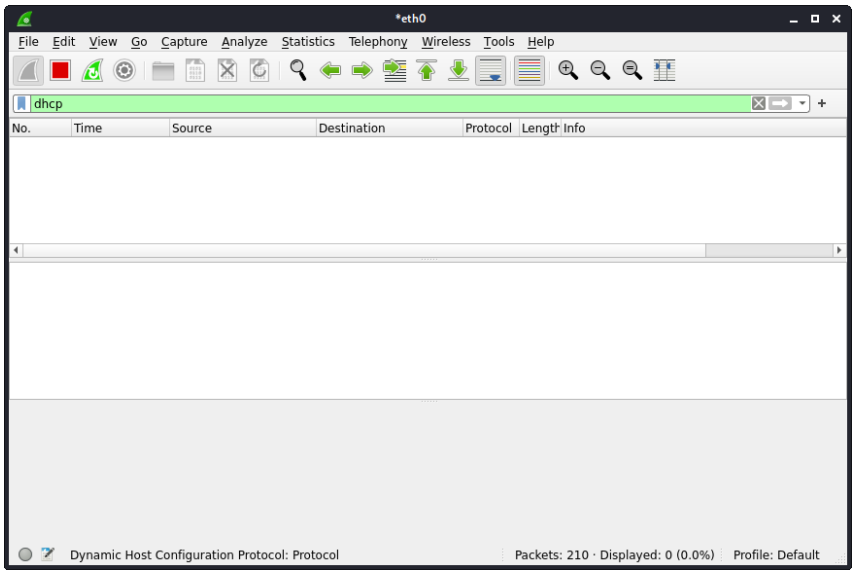

Figura 5.10: Wireshark vacío

No captura tráfico DHCP. Esto se debe a que como hemos explicado en la tabla 3.1, el switch solo reenvía mensajes DHCP DISCOVER por interfaces confiables, que en nuestro caso es la interfaz GE8, mientras que la interfaz del atacante GE4 no es confiable. Aún si el atacante consiguiera enviar mensajes DHCP OFFER, estos mismos mensajes serían filtrados por el switch siempre que no provengan de una interfaz confiable.

5.4. Comprobar resistencia a ataques ARP

Tras configurar la inspección ARP, se va a repetir el ataque de envenenamiento ARP de la misma forma que se ha llevado a cabo en el apartado 3.5 para comprobar la efectividad de dicho método.

Esta vez, se va a usar la herramienta Wireshark para asegurar que el ataque se lleva a cabo. Se configura el ataque utilizando la herramienta Ettercap y una vez se lanza, se observa el tráfico ARP capturado por Wireshark.

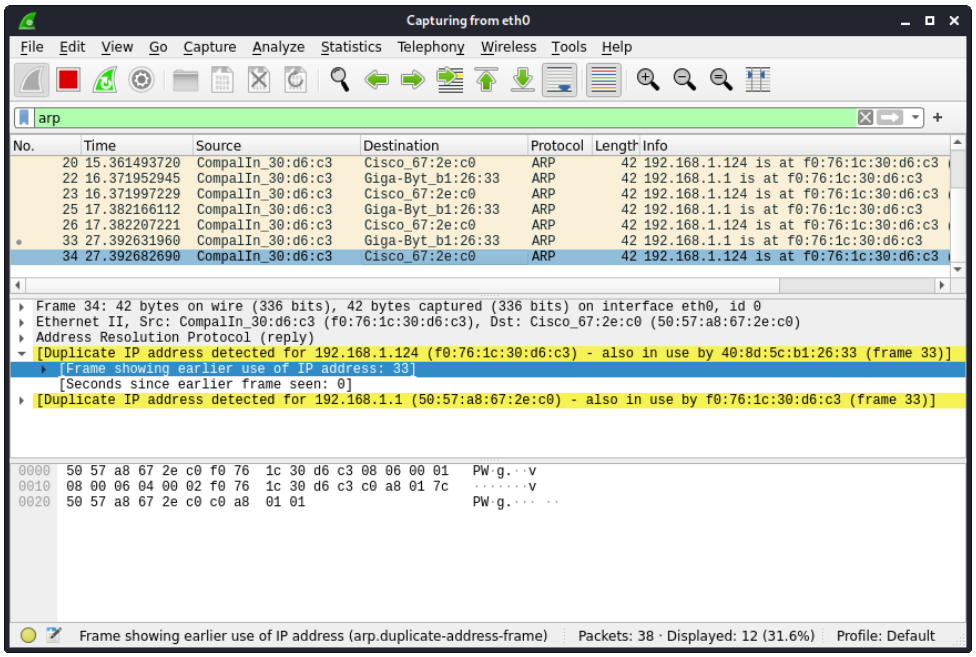

Figura 5.11: Wireshark ARP

Se puede observar que se han enviado los mensajes ARP 'envenenados', por lo tanto, desde el cliente se ejecuta el comando 'arp -a' para comprobar si la caché ARP ha sido modificada.

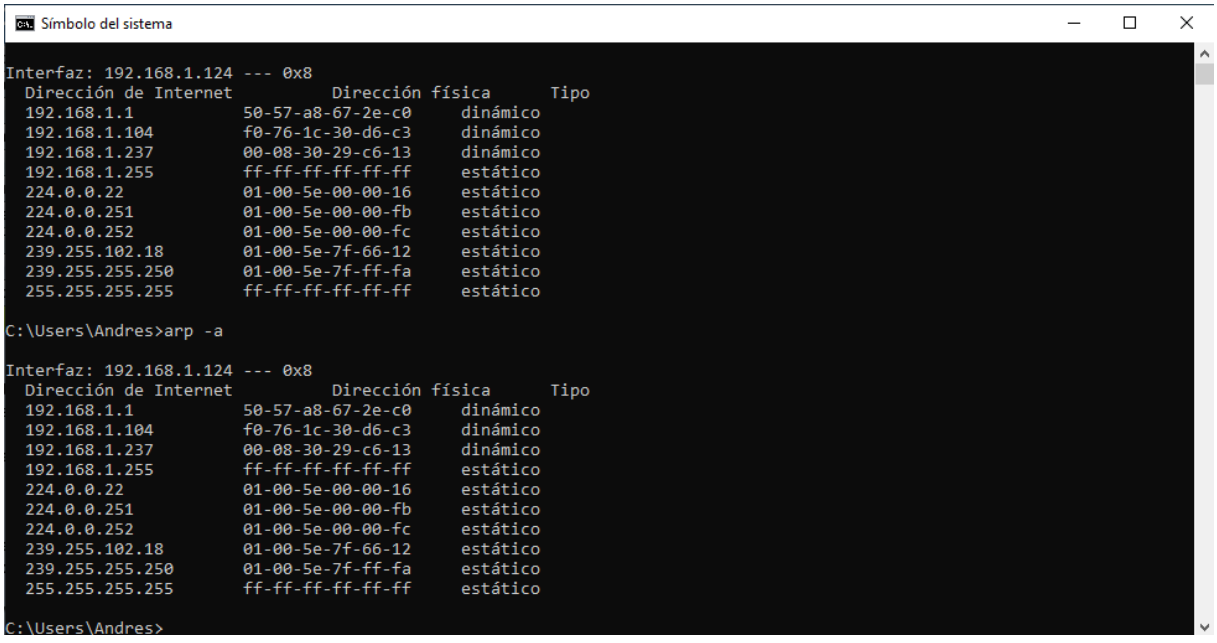

Figura 5.12: arp -a

Como era de esperar, la caché ARP de la víctima no ha sido modificada por los paquetes ARP 'envenenados' enviados por el atacante. El mecanismo de seguridad inspección ARP, al comparar el par dirección IP-MAC del mensaje ARP 'enveneda-do' con los pares IP-MAC establecidos en las reglas de acceso ARP, ha filtrado los

mensajes ARP ’envenenados’ impidiendo su reenvío al resto de la red. De esta forma, nuestra red LAN es inmune a los ataques de envenenamiento ARP.

Capítulo 6

Conclusiones

Este trabajo de fin de grado se a llevado a cabo con la intención de estudiar y conocer las principales vulnerabilidades que presentan las redes LAN, así como los mecanismos de seguridad de los que se dispone para solventar dichas vulnerabilidades. Una vez realizado el trabajo y tras conocer los principales ataques que se pueden llevar a cabo a una red LAN, sorprende la facilidad con las que dichos ataques se pueden llevar a cabo, lo que hace que preocuparnos de la seguridad de nuestras redes sea aun mas importante.

Es primordial que las empresas e instituciones en general dediquen el esfuerzo e inversión necesario en la seguridad de sus redes, puesto que cada vez son mas los datos sensibles que estos almacenan lo que pueden incentivar a usuarios malintencionados a querer atacar dichas redes con el objetivo de obtener beneficio a cambio o de utilizar la información sensible en beneficio propio.

Con la pandemia que estamos viviendo provocada por la COVID-19 el número de ciberataques sufridos por las empresas han aumentado en esta época de pandemia en la que los recursos web y el trabajo a través de internet se encuentra mas al día que nunca. El daño producido por ataques como los que han afectado al SEPE en España en este último año o la gran cantidad de ataque con Ransomware que se llevan a cabo últimamente podría verse reducido o incluso evitado si se utilizaran los mecanismos de seguridad de los que disponemos y las empresas e instituciones se mantuvieran al día en cuanto a la seguridad de sus redes.

Está claro que la seguridad en redes, en sistemas de información y la seguridad informática en general es un tema que tomará gran importancia en los años venideros y que requerirá de gran cantidad de profesionales especializados para llevar a cabo el diseño, implementación y mantenimiento de los sistemas y arquitecturas de seguridad que protegerán las cantidades ingentes de información que circula por las redes hoy en día.

Debido a lo expuesto anteriormente, este tfg pretende servir como ayuda para todos aquellos interesados en la seguridad y que pretendan hacer de sus redes el lugar mas seguro posible utilizando los mecanismos mas actuales de los que disponemos para dicho propósito.

Capítulo 7

Líneas de Futuro

Una vez se han estudiado e implementado las principales tecnologías actuales que dotan de una mayor seguridad a nuestras redes LAN, quedan dos vías abiertas en las que se puede seguir avanzando.

Por un lado, podemos estudiar estas misma tecnologías en otros dispositivos, ya que Cisco posee una gran variedad de switches, como podrían ser los modelos de la serie 500: Sx500, SG500X, SG500XG y ESW2-550X que poseen unas características bastante parecidas al modelo sobre el que se a trabajado en este documento, u otros switches como el modelo S3900-48T4S cuyos modos de configuración son diferentes a los estudiados.

Por otro lado, una vez dotado de seguridad LAN a nuestra red, se podrían estudiar métodos de seguridad WAN. Por ejemplo se podría diseñar un sistema de seguridad perimetral, utilizando Firewall que incluya:

- Sistemas de WebProxy: consiste en configurar un servidor con un sistema operativo virtual que funcione como interlocutor entre servidor y clientes de internet y que permita el uso de mecanismos para el control de acceso y autorizaciones con contraseñas.
- Sistemas de antivirus corporativos: sistemas que incluyen mecanismos para controlar la seguridad perimetral de una red, así como los correos electrónicos y sistemas de ficheros.
- Infraestructura de clave pública (PKI): infraestructura que permite al gestión de los certificados digitales de una organización y definir políticas de certificación.

En cuanto a la seguridad WAN, entramos en un ambiente extenso en el que se dispone de un gran número de mecanismos y de métodos que requieren una gran precisión en el diseño e implementación de arquitecturas de seguridad, así como de un trabajo de mantenimiento que sería muy interesante de estudiar, puesto que como sabemos, la seguridad en sistemas informáticos es un tema que ha llegado para quedarse y que requiere de una gran cantidad de profesionales.

Capítulo 8

Presupuesto de costes

Para llevar a cabo una estimación de los costes, estos se van a dividir en dos apartados. Por un lado los costes de los equipos necesarios para llevar a cabo el montaje de la red, y por otro lado los costes en personal para llevar a cabo la configuración de los diferentes equipos.

En cuanto a los equipos, como se puede ver en el diseño de red propuesto 10.1, disponemos de 7 switch, de los cuales 3 de ellos son Switch de acceso, 2 switch de Distribución y 2 switch Core. En cuanto a los equipos de comunicación de nivel 3, la red está compuesta por 2 router. Basándonos en el precio de los dispositivos utilizados en este documento para llevar a cabo el montaje de una porción de la red diseñada, switch Cisco SG300-10 y router Cisco RV 120W, podemos estimar un coste:

Equipo	**Euros/Unidad**	**Unidades**	**Coste Total**
Switch SG300-10	321,30	7	2249,10
Router RV 120W	160,65	2	321,30
			2570,40

Tabla. 8.1: Coste de equipos

El precio por unidad de cada dispositivo se ha calculado realizando una media entre el precio mas bajo y el precio mas alto encontrado en el mercado, obteniendo al final un coste total en Euros de 2570,40 Euros en equipos, de los cuales 2249,10 Euros corresponden a los switches y 321,30 Euros corresponden a los router.

La estimación de costes en lo que a personal se refiere se va a llevar a cabo basándonos en el salario medio anual propuesto por Glassdoor para un administrador de redes el cual se establece en 33.199 Euros anuales, así como el salario medio propuesto por Indeed para técnicos de red establecido en 20.603 Euros anuales. De esta forma, suponiendo un equipo formado por 5 personas, de las cuales una de ellas es administrador de redes y el resto técnicos de red, trabajando durante un periodo de tiempo de dos meses a jornada completa, podemos estimar:

Puesto	Numero de personal	Euros/mes	Coste Total
Administrador de redes	1	2766,58	2766,58
Técnico de red	4	1716,91	6867,64
			9634,22

Tabla. 8.2: Coste de personal

Uniendo ambos presupuestos, de coste y de personal obtenemos:

Personal	Equipos	Coste total
9634,22	2570,40	12204,62

Tabla. 8.3: Coste total

De esta forma obtenemos un coste total de 12204,62 Euros, de los cuales 9634,22 Euros están destinados a personal y 2570,40 Euros están destinados a los equipos necesarios.

Capítulo 9

Diagrama temporal

A continuación se presenta la planificación temporal que se ha seguido a la hora de llevar a cabo el proyecto.

La planificación se ha divido en dos partes diferenciadas. La primera de ellas llamada Estudio, es el periodo en el que se ha llevado a cabo el estudio y comprensión de los mecanismos expuestos anteriormente. La segunda parte llamada Implementación y Pruebas comprende el periodo de tiempo en el que se ha llevado a cabo el montaje de la red, así como las configuraciones y pruebas de rendimiento necesarias para comprobar el correcto funcionamiento de los diferentes mecanismos de seguridad.

Por otro lado, el proceso de documentación se ha llevado a cabo conforme se realizaban el resto de tareas.

La planificación temporal del proyecto en su totalidad queda plasmada en el siguiente diagrama de Gantt:

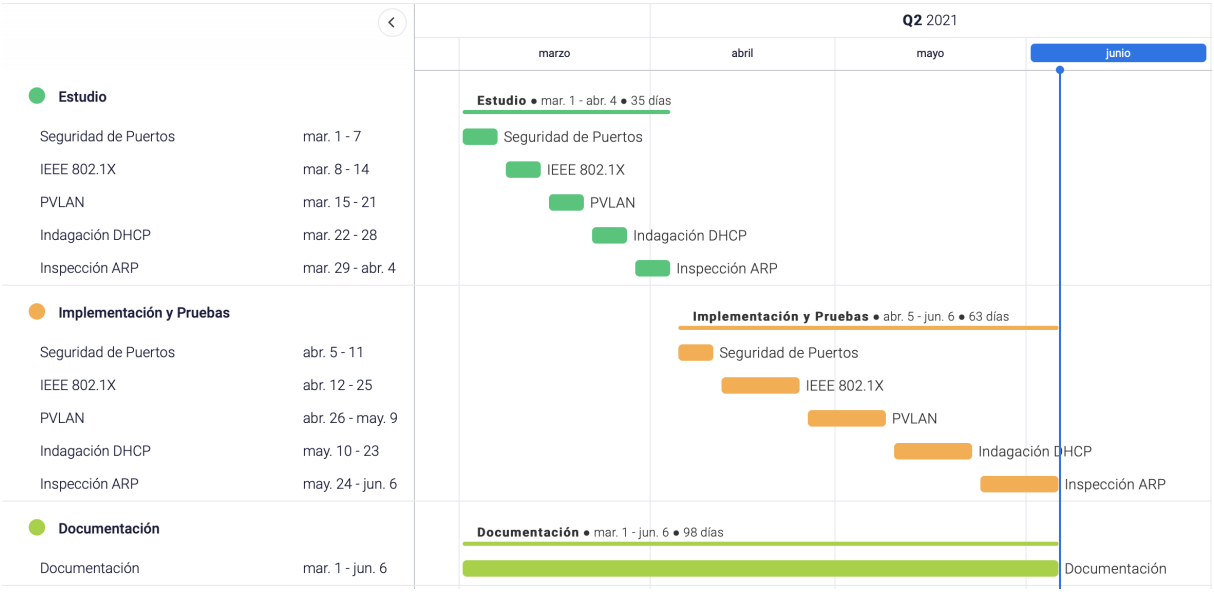

Figura 9.1: Diagrama de Gantt

Capítulo 10

Anexos

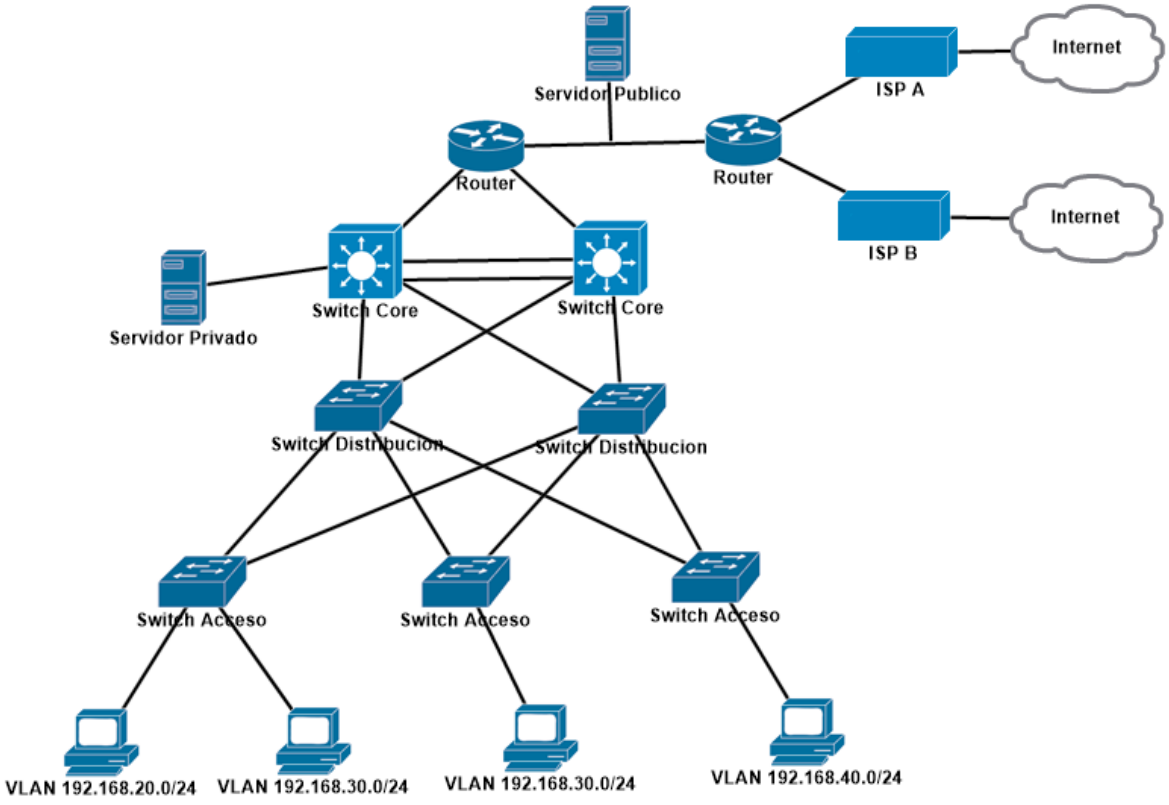

Figura 10.1: LAN

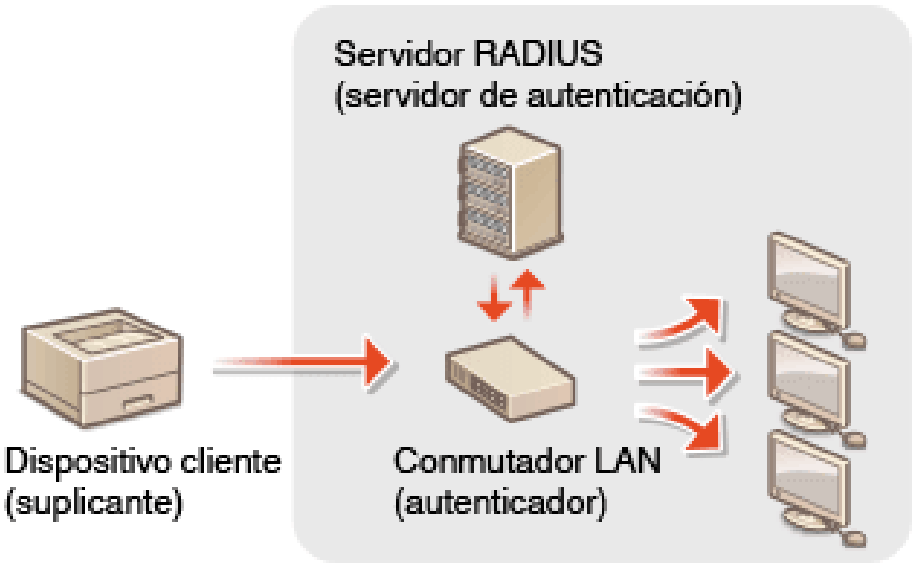

Figura 10.2: IEEE 802.1X

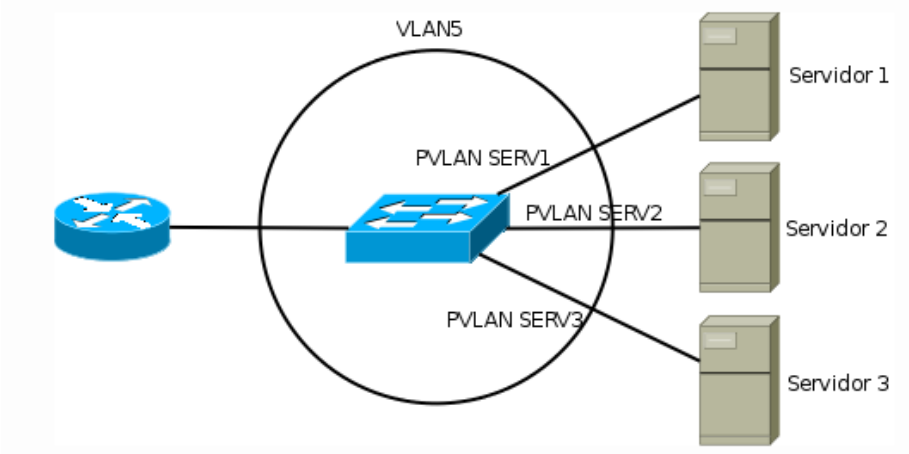

Figura 10.3: PVLAN

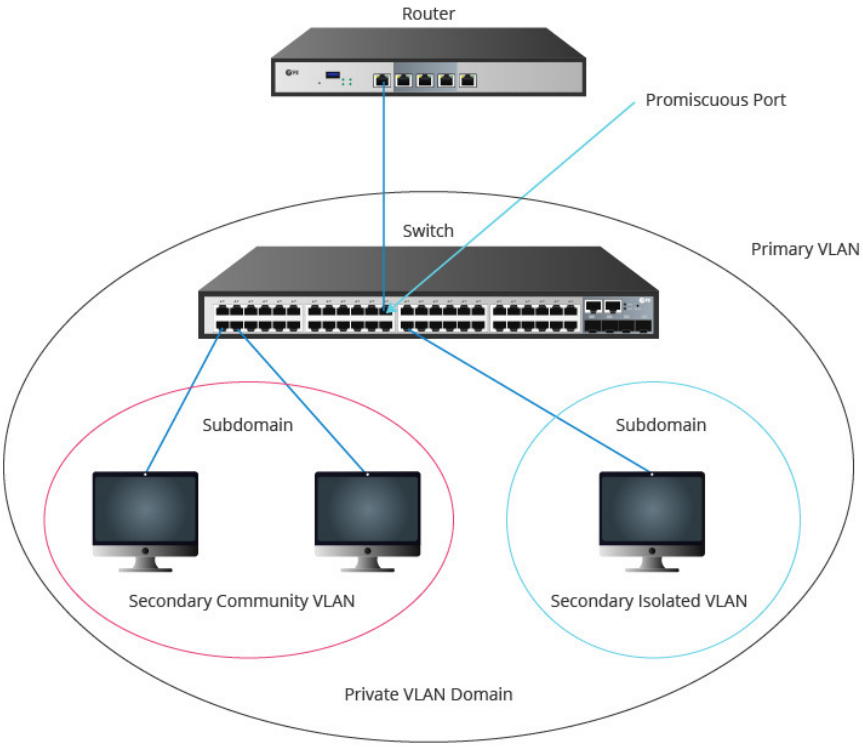

Figura 10.4: VLAN secundarias

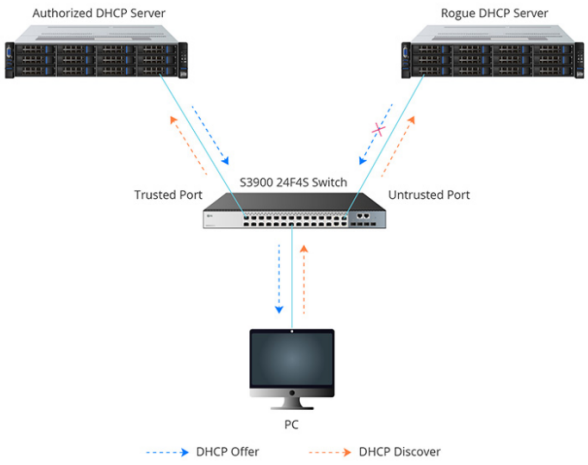

Figura 10.5: DHCP inspeccion

Capítulo 11

Bibliografia

- Cisco 300 Series Managed Switches Administration Guide 1.4.0 (Spanish) | Enhanced Reader. (n.d.). Retrieved June 7, 2021, from pdf
- Cisco RV 120W Wireless-N VPN Firewall Administration Guide | Enhanced Reader. (n.d.). Retrieved June 7, 2021, from pdf
- Chapter 1. Introduction. (n.d.). Retrieved June 7, 2021, from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
- ettercap(8) - Linux man page. (n.d.). Retrieved June 7, 2021, from https://linux.die.net/man/8/ettercap
- yersinia(8): FrameWork for layer 2 attacks - Linux man page. (n.d.). Retrieved June 7, 2021, from https://linux.die.net/man/8/yersinia
- Configure RADIUS Clients | Microsoft Docs. (n.d.). Retrieved June 7, 2021, from https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-radius-clients-configure
- Tutorial Ubuntu - Autenticación Radius usando Freeradius [Paso a paso]. (n.d.). Retrieved June 7, 2021, from https://techexpert.tips/es/ubuntu-es/autenticacion-radiu
- ¿Qué es el protocolo 802.1X / EAP y cómo funciona? - CCM. (n.d.). Retrieved June 7, 2021, from https://es.ccm.net/contents/785-802-1x-eap
- Distributed Virtual Switch: Que son las PVLAN? | Tecnologias Aplicadas. (n.d.). Retrieved June 7, 2021, from https://patriciocerda.com/distributed-virtual-switch-que
- ¿Qué es el DHCP snooping? - IONOS. (n.d.). Retrieved June 7, 2021, from https://www.ionos.es/digitalguide/servidores/seguridad/dhcp-snooping/
- CCNA Security – DHCP Starvation – NETTYNIC. (n.d.). Retrieved June 7, 2021, from https://nettynic.wordpress.com/2019/05/29/ccna-security-dhcp-starvation/
- Envenenamiento ARP - EcuRed. (n.d.). Retrieved June 7, 2021, from https://www.ecured.cu/Envenenamiento_ARP#:~:text=ElARPSpoofingoenvenenamiento,eltráfico%2Coinclusodetenerlo.

- dhcp snooping – prevención de ataques DHCP | capa3.es. (n.d.). Retrieved June 7, 2021, from https://capa3.es/dhcp-snooping-prevencion-de-ataques-dhcp.html
- Dynamic Arp Inspection – Prevención de ataques MiTM | capa3.es. (n.d.). Retrieved June 7, 2021, from https://capa3.es/dynamic-arp-inspection-prevencion-de-ataques
html