GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-647)

SEGURIDAD EN SWITCHES HP COMWARE

ENERO 2016

Edita:

NIPO: 002-16-005-0
Fecha de edición: enero 2016

El Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid ha participado en la elaboración del presente documento.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

enero 2016

Félix Sanz Roldán

Secretario de Estado

Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura de los switches HP pertenecientes a la familia HP 5500 EI. A lo largo de los diferentes capítulos se ofrecen consejos y recomendaciones sobre la activación o desactivación de servicios y determinadas funcionalidades de esta familia de switches con el fin de poder establecer una configuración lo más segura posible.
2. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo, sino que se recomienda al lector utilizar el índice de contenidos para localizar aquél capítulo que trate aquél aspecto sobre el que desea mejorar la seguridad. Así mismo, aunque estas páginas han sido escritas pensando en la familia de switches HP 5500EI, la mayoría de las recomendaciones descritas sobre seguridad son aplicables a otros equipos de red.

2. OBJETO

3. Analizar los mecanismos de seguridad disponibles para proteger los entornos de sistemas de información y comunicaciones que emplean switches HP. Como consecuencia, se establece un marco de referencia que contemple las recomendaciones STIC en la implantación y utilización de switches HP.
4. En líneas generales, en este documento no se valora la idoneidad de utilizar ciertos protocolos o no, sino que se describen como deben ser securizados cada uno de ellos.
5. Queda fuera del alcance de este documento la configuración de calidad de servicio necesaria para la correcta explotación del dispositivo. Se entiende que la configuración en producción garantiza que el equipo puede ser gestionado adecuadamente y que el tráfico de gestión y explotación no pone en riesgo el servicio del mismo ni queda desplazado por el tráfico de servicio o producción.
6. En el ámbito de este documento se asume que existirá un usuario de nivel administrador que podrá configurar todas las funcionalidades requeridas, incluidas las definiciones de usuarios locales.

3. ALCANCE

7. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los switches HP bajo su responsabilidad.

4. INFORMACIÓN PREVIA A LA CONFIGURACIÓN DEL EQUIPO

8. Los equipos de la familia HP 5500 EI son completamente gestionables, es decir, permiten al administrador de red configurar el equipo. En el caso particular de esta familia el sistema operativo es COMWARE v5.
9. En COMWARE v5 se trabaja con dos entornos: entorno de usuario (*User View*) y entorno de sistema (*System View*).
    1. El entorno de usuario permite trabajar con el sistema de ficheros, realizar *debugs* y pruebas básicas de conectividad.

2. El entorno de sistema permite la configuración completa del equipo, incluida la definición de usuarios locales. Desde este nivel, se accede a otras vistas particulares o contextos específicos de configuración.

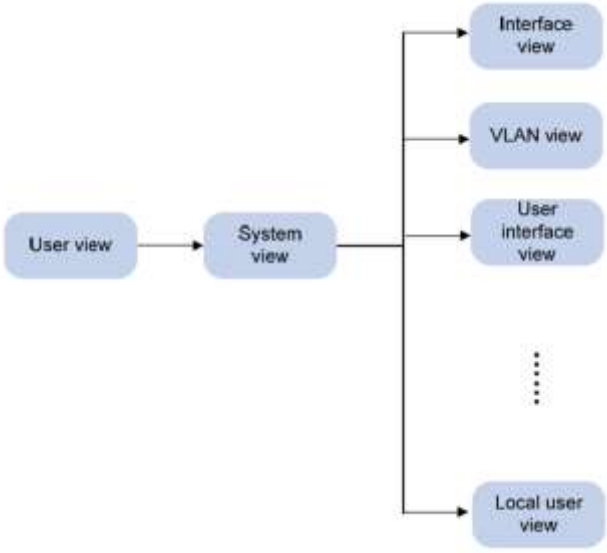

Figura 1. Jerarquía de vistas en CLI

10. Al conectarse al equipo, normalmente se entra en entorno de usuario. Se puede configurar los permisos para que usuarios autorizados entren directamente en el de sistema. Para acceder al entorno de sistema haremos uso del comando:

```
<hostname> system-view
```

Nota: Tras ejecutar el comando, pueden ser solicitadas credenciales al usuario.

11. Para salir del entorno del sistema ejecutamos lo siguiente:

```
[hostname] quit
```

Nota: Tras ejecutar el comando, se baja al entorno de usuario, aun cuando se haya entrado directamente en el entorno del sistema.

12. El equipo presenta *prompts* diferentes en distintas vistas.

Tipo de vistas	Prompt
Entorno de usuario – User view	`<hostname>`
Entorno de sistema – System view	`[hostname]`
Entorno de interfaz – Ejemplo GigabitEthernet 1/0	`[hostname-GigabitEthernet1/0]`
Entorno de interfaz – Ejemplo vlan 100	`[hostname-vlan100]`
Entorno de usuario local – Ejemplo admin	`[hostname-luser-manage-admin]`

13. Todos los cambios de configuración realizados en el equipo se almacenan en la ***current-config***, almacenándose en memoria volátil, que en caso de corte de alimentación se pierde.
14. Para no perder estos cambios es necesario salvarlos en la configuración de arranque o

startup-config que se almacena en la memoria no volátil. Se debe copiar la configuración en uso a la de arranque mediante el siguiente comando (ejecutable tanto en entorno de usuario o de sistema):

```
save safely force
```

Nota: Graba la configuración de forma robusta (mediante copia a fichero y renombrado). El modificador force evita la confirmación.

15. Se deben realizar *backups* periódicos de las configuraciones a un repositorio centralizado de manera que disminuya el tiempo de recuperación en caso de desastre. En los equipos se permite tener una configuración de arranque ***main*** o principal y otra de ***backup*** de uso en caso de que la configuración *main* falle.
16. Para recuperar una configuración anterior, se debe utilizar el comando:

```
reset saved-configuration <backup>
```

Nota: La configuración de fábrica se llama *main*

17. El *hostname* del equipo puede establecerse de la siguiente manera:

```
sysname <nombre>
```

18. Se verifica la funcionalidad al mostrarse el nombre en el *prompt*.

```
[nombre]
```

19. Es necesario por motivos legales mostrar un mensaje al intentar acceder al equipo después de la información de inicio de sesión y antes de la autenticación. Para ello se debe configurar un mensaje legal que aparezca antes de introducir las credenciales en el sistema. A modo de ejemplo se muestra la siguiente configuración en la que se utiliza el carácter "#" como elemento indicativo de fin de mensaje para entradas de más de una línea.

```
header legal #

Mensaje a mostrar cada vez se establece sesión. #
```

20. Se verifica la funcionalidad intentando establecer una sesión contra el equipo.

Nota: El carácter usado al principio en la secuencia, es usado como delimitador y puede ser usado otro.

21. Por último, se muestra una tabla con los principales símbolos de sintaxis de los comandos y su respectivo significado.

Símbolo	Significado
[…]	Parámetros opcionales, se puede elegir uno o ninguno
{…}	Se debe elegir uno entre los diferentes parámetros obligatorios
<…>	Argumento que hay que reemplazar por el valor deseado
a | b	Se debe elegir entre los parámetros a y b, y seleccionar uno
[…]*	Parámetros opcionales, se pueden elegir uno, múltiples o ninguno
{…}*	Se debe elegir al menos uno entre los diferentes parámetros obligatorios

22. Para conocer todas las opciones que ofrece un comando se utiliza el comodín "?".

5. PLANO DE GESTIÓN (MANAGEMENT PLANE)

5.1. MÉTODOS DE ACCESO AL EQUIPO Y SECURIZACIÓN **DE LOS MISMOS**

23. La configuración de los equipos se puede realizar de varias maneras: mediante interfaz de línea de comandos, interfaz web, SNMP y OpenFlow.

5.1.1. ACCESO A LA INTERFAZ DE LÍNEA DE COMANDOS (CLI)

24. La interfaz de línea de comandos, o CLI, permite la configuración completa de los equipos para regular la funcionalidad y comportamiento de los mismos. Para ello es necesario conocer el conjunto de comandos de configuración soportado para un determinado modelo, y para una versión de software concreta. En nuestro caso es necesario conocer COMWARE v5.
25. COMWAREv5 define cuatro niveles de usuarios que tendrán acceso a ciertos comandos del sistema operativo.
    1. Visitor (0): Diagnóstico de red y acceso a equipos externos. Trabaja en entorno de usuario con comandos como ping, traceroute, telnet, ssh, etc.
    2. Monitor (1): Mantenimiento del sistema y diagnóstico de fallos. Trabaja en entorno de usuario y además de los comandos anteriores puede utilizar comandos como debugging, terminal, reset, etc.
    3. System (2): Configuración del sistema, servicios, enrutamiento, etc. Trabaja tanto en entorno de usuario como de sistema. Puede utilizar todos los comandos anteriores y los de configuración excepto los de usuario.
    4. Administrator (3). Permite la configuración completa de los equipos incluida la definición de usuarios y la gestión de ficheros (manejo de configuraciones y *firmware* del equipo).
26. De los tipos de acceso a la línea de comando, diferenciamos dos posibles:
    1. Conexión física directa al equipo – Conexión fuera de banda, mediante conexión al puerto de consola. Este equipo no dispone de puerto USB.
    2. Conexión lógica y remota al equipo – Conexión en banda, mediante conexión remota al equipo utilizando interfaces de red.

5.1.1.1. CLI – CONEXIÓN DIRECTA AL EQUIPO – PUERTO DE CONSOLA (Out of Band)

27. Los equipos disponen de un puerto de consola (conexión serie) a través del cual se pueden administrar completamente todas las funciones que este proporciona. El uso del puerto de consola implica tener conexión física al equipo.
28. El puerto auxiliar (AUX0 en COMWAREv5) y el puerto de consola son el mismo puerto (en la siguiente sección nos referiremos a él como puerto de consola).
29. Cuando iniciamos una conexión a este puerto, se trata de la interfaz de usuario AUX y se activa por defecto el modo de autenticación.

30. El puerto de consola permite configurar todas las funcionalidades, sin excepción. Algunas funciones, como la recuperación de las credenciales del equipo (conocido como procedimiento de *password recovery*) son operativas únicamente desde el puerto de consola.
31. La configuración por defecto del puerto de consola es la siguiente, siendo estos parámetros modificables:

```
9600bps
Sin control de flujo
Sin paridad
1 bit de parada
8 bits de datos
```

32. Inicialmente el acceso por consola se permite a todo el mundo sin solicitar ni usuario ni contraseña.
33. En apartados posteriores se mostrará cómo proteger el acceso por consola y la definición de usuarios.

5.1.1.2. CLI – CONEXIÓN REMOTA AL EQUIPO – TELNET/SSH (In band)

34. La gestión en banda permite la conexión al dispositivo utilizando la misma red que emplea el flujo normal de tráfico. Utilizar el enfoque de red de gestión en banda tiene sus desventajas. Los datos de administración deben compartir el ancho de banda de red y los fallos en la red y los recursos pueden provocar que la infraestructura se vuelva imposible de gestionar.
35. Potencialmente, y una vez configurado correctamente, se puede acceder a la interfaz de comandos de manera remota desde un equipo con el que haya conectividad IP.
36. Los protocolos soportados son TELNET y SSH. En ambos casos el equipo se comporta como servidor, siendo necesario, para la conexión remota, una aplicación que se comporte como cliente.
37. No se debe utilizar el protocolo TELNET pues toda la información intercambiada por la sesión remota es enviada en texto plano. En su lugar hay que utilizar el protocolo SSH pues toda la información intercambiada por la sesión remota está cifrada.
38. En la configuración inicial, o en ausencia de la misma, no están habilitados ni el servidor TELNET ni el servidor SSH. En apartados posteriores se mostrará como configurar dichos servidores de manera segura.
39. El equipo por defecto tiene definidas 16 sesiones remotas simultáneas. La interfaz de acceso en este caso se denomina `vty`, y se numeran de 0 a 15.

5.1.2. GESTIÓN VIA WEB: HTTP Y HTTPS

40. Es posible configurar y administrar el equipo mediante interfaz web. De nuevo el equipo se comportará como servidor y será necesario el uso de un cliente web.
41. Se debe, en el caso de querer configurar y administrar el equipo vía web, deshabilitar el uso de HTTP, deshabilitado por defecto y habilitar el uso de HTTPS, deshabilitado por defecto.

5.1.3. SNMP

42. SNMP es el protocolo de intercambio de información de gestión entre la plataforma de gestión y los equipos gestionados.
43. Este protocolo tiene dos facetas, que se diferencian principalmente en qué motiva el intercambio de información, así como la naturaleza del mismo:
    1. Generación de alarmas o eventos, llamados *traps*. Iniciado por el dispositivo, a una o varias estaciones gestoras de la red. Notifican eventos o situaciones sufridas en el seno o en el entorno del equipo (por ejemplo, caída de un enlace o de un exceso de temperatura).
    2. Dialogo o interrogación. La estación gestora, con las correspondientes credenciales, interroga o manda información al equipo (por ejemplo, la consulta de los paquetes transmitidos por una interfaz)
44. El método utilizado, tanto en los *traps* como en el modo diálogo, es mediante el uso de MIBs (Management Information Base). Estas definiciones de información pueden tener un carácter público o propietario.
45. Actualmente existen tres versiones del protocolo SNMP. El equipo soporta la versión SNMP v3, que es la recomendada pues proporciona mecanismos de seguridad y control de la información accedida. En apartados posteriores se mostrará la configuración mas recomendable de este servicio.

5.1.4. OPENFLOW

46. OpenFlow es un protocolo de reciente creación. Sin ser el único, es uno de los que ha sido desarrollado con miras a la implementación de soluciones tipo SDN (Software Defined Networks).
47. En las arquitecturas SDN, existen tres capas o niveles funcionales:
    1. Capa de Aplicaciones.
    2. Capa de Control.
    3. Capa Infraestructura de red.
48. Este protocolo está diseñado para que la Capa de Aplicación pueda obtener un estado de la red, así como poder dar instrucciones a la misma. Esto se realiza a través de APIs.
49. La relación de un dispositivo de red con la Capa de Control, también denominada controladora, puede ser entre otros, mediante protocolos como OpenFlow.
50. Openflow es un protocolo orientado a que la Capa de Control interactúe, conociendo y pudiendo programar flujos de tráfico que el equipo maneja.

Nota: Openflow, en su diseño, no está pensado para configurar equipos, ni activar funcionalidades, si bien pueda haber implementaciones desnaturalizadas que puedan hacer ese uso, no siendo este el caso de HP.

5.2. POLÍTICA DE PASSWORDS

51. En el equipo, es posible definir una la política de contraseñas estricta que minimice el riesgo de fallos en la gestión de las mismas. En esta secuencia se describen las opciones recomendadas.

52. Para activar el control de passwords:

```
[] password-control enable
```

53. Para fijar la longitud mínima en 12 caracteres:

```
[] password-control length 12
```

54. Para fijar el número de reintentos en 2, bloqueando el usuario en caso de fallo adicional:

```
[] password-control login-attempt 2 exceed lock
```

55. Para fijar el periodo de vida a cada password a 30 días:

```
[] password-control aging 30
```

56. Para fijar el periodo mínimo de actualización a 36 horas:

```
[] password-control password update interval 36
```

57. Para que el usuario solo pueda entrar hasta 5 veces en 60 días antes de que la password expire:

```
[] password-control expired-user-login delay 60 times 5
```

58. Para fijar el tiempo máximo de inactividad a 30 días:

```
[] password-control login idle-time 30
```

59. Para rechazar contraseñas donde se incluya el usuario o su reverso:

```
[] password-control complexity user-name check
```

60. Para limitar el uso de un carácter repetido 3 veces:

```
[] password-control complexity same-character check
```

5.3. CONFIGURACIÓN DE USUARIOS LOCALES EN EL EQUIPO

61. Con la configuración de fábrica cualquier persona con acceso físico a la consola puede acceder al sistema.
62. Por lo tanto, será necesario definir usuarios de acceso al sistema y configurar el acceso a la consola para solicitar credenciales de acceso.
63. Por ejemplo, para definir un usuario *alfredo*, con la password *clave*, con permisos de *ssh* y acceso *terminal* (puerto consola):

```
[] local-user alfredo

[] password simple clave

[] authorization-attribute level 3

[] service-type ssh terminal

[] state active
```

Nota: Por defecto el estado es *active*

64. Para verificar la funcionalidad en operación se pueden establecer sesiones y utilizar el

comando:

```
[] display local-user
```

65. Para eliminar un usuario local:

```
[] undo local-user alfredo
```

66. Para bloquearlo sin su eliminación:

```
[] local-user Alfredo

[] state block
```

67. En apartados posteriores mostraremos la configuración de usuarios de autenticación local en el equipo o en servidores remotos. En los usuarios locales será necesario definir que pueden acceder por la consola (terminal).

5.4. RECOMENDACIONES DE CONFIGURACIÓN DE SERVICIOS DEL EQUIPO

5.4.1. CONSOLA

68. Para proteger el acceso por consola se debe configurar el puerto de consola para solicitar usuario y password en dicho acceso:

```
[] user-interface aux 0

[] authentication-mode password

[] set authentication password cipher <password>

[] idle-timeout 2 0

[] user privilege level 3
```

Nota: El indicador 0 puede cambiar. Cuando el equipo dispone de más de un puerto de consola, la configuración debe hacerse para cada uno de ellos.
Se debe limitar la máxima duración de la sesión sin actividad a 2 minutos. Por defecto son 10 minutos.

69. Para verificar la configuración:

```
[] display user-interface aux 0
```

70. También son posibles configuraciones más complejas donde, por ejemplo, el puerto de consola autentique al usuario contra un sistema centralizado. Esto se tratará en apartados posteriores.

5.4.2. SERVICIO DE CONFIGURACIÓN VÍA HTTP/SSL

71. En la configuración inicial del equipo el servicio web está desactivado. HTTP no es seguro al no estar cifrada la comunicación.

72. Se debe por lo tanto asegurarse de que esté desactivado. Para ello es necesario el siguiente comando:

```
[] undo ip http enable
```

73. Para ver el estado:

```
[] display ip http
```

74. Por otro lado, para configurar HTTPS es necesario contar con una entidad certificadora (CA). De la cual el equipo importará los certificados que sean necesarios.
75. En el caso que se desee hacer uso de HTTPS, son necesarios como mínimo los siguientes pasos:
    1. Configurar una entidad PKI en el equipo.
    2. Crear un dominio PKI, especificando la CA, la URL de donde se descargará el certificado y otros detalles.
    3. Crear las claves RSA locales (si no existen ya).
    4. Obtener el certificado de la CA.
    5. Solicitar un certificado para el dispositivo.
    6. Configurar una política de SSL Server.
    7. Configurar un grupo de atributos de certificados.
    8. Configurar una política de control de acceso basada en atributos.
    9. Asociar la política SSL con el servidor HTTPS.
    10. Asociar la política de control de acceso basada en atributos con el servidor HTTPS.
    11. Habilitar el servicio HTTPS.
    12. Limitar los equipos que pueden conectarse, mediante ACL.
76. En caso de que no se vaya a usar HTTPS es mejor asegurarse de que esté deshabilitado:

```
[] undo ip https enable

[] display ip https
```

5.4.3. TELNET

77. En la configuración inicial del equipo el servicio telnet está desactivado. Para asegurarnos, desactivaremos el servicio telnet por si alguien lo hubiera habilitado:

```
[] undo telnet server enable
```

5.4.4. SSH

78. En la configuración inicial del equipo el servicio ssh está desactivado. Para activarlo son necesarios los siguientes pasos:
    1. Generar la clave RSA.
    2. Activar SSH en las líneas remotas.
    3. Habilitar el servicio SSH.
79. Para generar la clave RSA que se almacenará en el dispositivo:

```
public-key local create rsa
```

80. Para activar SSH en las conexiones remotas son necesarios los siguientes comandos:

```
[] user-interface vty 0 15
[user-interface] protocol inbound ssh
[user-interface] idle-timeout 2 0
```

81. Para verificar la funcionalidad:

```
[] display users all
```

Nota: Esta secuencia habilita las conexiones remotas ssh, en las líneas virtuales de la 0 a la 15 (estos valores pueden cambiar por plataforma). Limita la sesión a 2 minutos en caso de inactividad. La autenticación *authentication-mode* debe ser de tipo *scheme*, con tipo *password* no funciona.

82. Por último, habilitamos el servicio ssh con el comando:

```
[] ssh server enable
```

Nota: Por defecto, se habilita ssh versión 2.

83. Para mayor seguridad, se debe limitar los equipos que conectan por SSH a través de listas de acceso (ACL). Para ello, se debe seguir la configuración siguiente:

```
[] acl number 2000 name ACL-GESTION
[acl_2000] rule 0 permit source 10.1.0.0 0.0.0.255
[acl_2000] rule 10 deny
[acl_2000] quit

[] user-interface vty 0 15
[user-interface] acl 2000 inbound
[user-interface] quit
```

Nota: Con este comando restringimos las direcciones IPs que pueden conectar vía SSH, a las que pasen el filtro que establece la lista de acceso 2000.
En este ejemplo, se permite únicamente la red de origen 10.1.0.0/24

5.4.5. SNMP

84. Los equipos de HP soportan las tres versiones de SNMP existentes. Se debe utilizar el protocolo SNMPv3 en modo privacidad (autenticación o privacidad son modos distintos, en los que van los datos en claro o cifrados respectivamente aunque ambos autentican).

85. Se debe limitar con ACLs desde qué direcciones IP pueden hacerse consultas SNMP. En el ejemplo siguiente se definen dos listas de acceso diferentes:

```
[] acl number 2001
[acl_2001] rule 1 permit source 192.168.100.0 0.0.0.255
[acl_2001] quit

[] acl number 2002
[acl_2002] rule 1 permit source 192.168.100.1 0
[acl_2002] quit
```

86. A continuación, fijamos la versión 3 y definimos comunidades o grupos referenciando la ACL que deseamos (la 2001 creada anteriormente):

```
[] snmp-agent sys-info version v3

[] snmp-agent group v3 AUTHGROUP authentication acl 2001

[] snmp-agent group v3 PRIVGROUP privacy acl 2001

[] snmp-agent calculate-password <password> mode sha local-engineid

[] snmp-agent usm-user v3 <snmpv3user> PRIVGROUP authentication-mode sha
<authpassword> privacy-mode aes128 <privpassword>

[] snmp-agent target-host trap address udp-domain <IP_plataforma_gestion>
params securityname <snmpv3user> v3 privacy
```

Nota: El primer comando sirve para habilitar el agente SNMP y configurarlo para versión 3. De forma opcional se puede calcular el hash (se debe utilizar sha) de una palabra para ser usado como contraseña, tal y como aparece en el cuarto comando.

5.4.6. NTP

87. En una red es necesario tener el reloj de todos los equipos sincronizados para que al resolver una incidencia, o realizar un análisis de un problema, toda la información obtenida pueda ser procesada correctamente. Para ellos se utiliza el protocolo Network Time Protocol (NTP).

88. Existen dos modos de funcionamiento, cliente o servidor, pudiendo ser ambos simultáneos.

89. Por otra parte, debemos garantizar la autenticación entre equipos que intercambian información de tiempo.

90. Para activar la autenticación de NTP hay que seguir la siguiente secuencia de comandos:

```
[] ntp-service authentication enable

[] ntp-service authentication-keyid <id> authentication-mode md5
<claveNTP>

[] ntp-service reliable authentication-keyid <id>
```

91. Para verificar la funcionalidad:

```
[] display ntp-service status

[] display ntp-service sessions
```

92. Para configurar el equipo como servidor NTP:

```
[] interface <interface-type> <interface-number>
[interface] ntp-service broadcast-server authentication-keyid <id>
```

o bien:

```
[interface] ntp-service multicast-server authentication-keyid <id>
```

Nota: Puede activarse en modo *broadcast* o multicast.

93. Finalmente hay que configurar el cliente NTP:

```
[] ntp-service unicast-server 10.1.0.1
```

Nota: Se ha configurado el equipo para que tome la hora del equipo 10.1.0.1

94. Se debe deshabilitar la recepción de mensajes NTP en una interfaz en la que no se esté usando:

```
[] interface <interface-type> <interface-number>
[interface] ntp-service in-interface disable
```

5.4.7. MENSAJES DE ACCESO

95. Suele ser necesario configurar mensajes informando de la limitación de acceso a los equipos. Para ello se utiliza el comando siguiente:

```
header login @
* Ejemplo de mensaje *@
```

96. Se puede comprobar que se muestra el mensaje al realizar un acceso al equipo.

5.4.8. TRANSFERENCIA DE FICHEROS SEGURA

97. Los equipos inicialmente permiten la transferencia de ficheros necesarios para el sistema (configuración/firmware) utilizando el protocolo tftp (cliente tftp). Este protocolo transmite la información sin cifrar, por lo que se deben emplear otros protocolos más seguros tales como sftp o scp.

98. Para configurar el cliente SFTP hay que especificar primero una IP o interfaz origen exclusiva para el cliente SFTP. Y hay que asegurar que la interfaz tiene una IP asignada.

```
[] sftp client source ip <ip> | interface <interfaz>
```

99. A continuación, hace falta conectarse al servidor mediante una clave RSA.

```
[] sftp <ip> identity-key rsa
```

Nota: Es necesario tener el servidor remoto SFTP accesible y usuario con permisos de acceso necesarios. Se utilizan los comandos habituales de SFTP (cd cambia de directorio, get recibe ficheros, put envia, help,etc…).

100. Para generar certificados para el servidor SFTP son necesarios los comandos:

```
[] public-key local create rsa

[] public-key local export rsa ssh2 pubkey
```

101. Por otra parte, SCP se basa en SSHv2.0 y ofrece también la transferencia segura de ficheros. Para su uso es necesario que se generen las claves SSH.

102. Al igual que antes, es necesario configurar el cliente SCP.

```
[] scp 192.168.0.1 get remotoR.bin localR.bin

[] scp 192.168.0.1 put localT.bin remotoT.bin
```

Nota: Es necesario tener el servidor remoto SCP accesible, teniendo el usuario los permisos de acceso necesarios. En primer ejemplo recibe el fichero *remoteR.bin* y el segundo transmite el fichero *local.bin*.

103.Por último, hay que generar los certificados y habilitar SSH.

```
[] public-key local create rsa

[] ssh server enable
```

5.5. ACTUALIZACIÓN DE FIRMWARE

104.Los switches HP 5500EI permiten almacenar en la flash del equipo más de una versión de *firmware* siempre que exista espacio libre en la memoria flash.

105.Para actualizar el *firmware* del equipo es necesario descargar el *firmware* siguiendo el procedimiento del punto anterior, indicar al switch las versiones de *firmware* a utilizar y reiniciar el equipo.

5.5.1. FIJAR SISTEMA OPERATIVO A UTILIZAR

106.Los comandos para indicar al equipo que utilice la nueva versión de *firmware* son los siguientes:

```
boot-loader file flash:/FIRMWAREPRINCIPAL.bin slot all main

boot-loader file flash:/FIRMWARESECUNDARIO.bin slot all backup

reboot
```

Nota: El primer ejemplo indica el *firmware* de arranque y en caso de fallo se utilizaría el segundo. Estos comandos se hacen desde el acceso inicial <equipo> y no desde el entorno de configuración [equipo].

107.Para verificar que se ha configurado de forma adecuada se pueden utilizar los dos comandos siguientes:

```
display flash

display boot-loader
```

5.5.2. COPIA DE SOFTWARE AL EQUIPO DESDE UBICACIÓN REMOTA

108.Para copiar un nuevo fichero de sistema operativo en la flash desde una ubicación remota:

```
scp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin

 Username: manager

 Trying 10.0.100.111 ...

 Press CTRL+K to abort

 Connected to 10.0.100.111 ...

 Enter password:
```

Nota: Este comando se ejecuta desde el acceso inicial <equipo> y no desde el entorno de configuración [equipo].

5.5.3. COPIA DE SOFTWARE DEL EQUIPO A UNA UBICACIÓN REMOTA

109.Para copiar un fichero de sistema operativo desde la memoria del equipo a una ubicación

remota:

```
scp 10.0.100.111 put A5500EI-CMW520-R2221P07.bin

Username: manager

Trying 10.0.100.111 ...

Press CTRL+K to abort

Connected to 10.0.100.111 ...

Enter password:
```

5.5.4. FIJAR FICHERO DE CONFIGURACIÓN A UTILIZAR

110. Para recuperar una configuración almacenada del equipo se utilizará el procedimiento de descarga indicado en apartados anteriores. La configuración debe estar almacenada en un servidor externo. Después es necesario indicarle al equipo que utilice la nueva configuración y reiniciar al equipo.

111. Para actualizar la configuración de inicio se utilizan los comandos siguientes:

```
startup saved-configuration flash:/PRINCIPAL.cfg main

startup saved-configuration flash:/SECUNDARIA.cfg backup

reboot
```

112. Para verificar que se ha actualizado correctamente:

```
display startup
```

Nota: El primer ejemplo indica el fichero de arranque y en caso de fallo se utilizaría el segundo.

5.5.5. COPIA DE FICHERO DE CONFIGURACIÓN DESDE UBICACIÓN REMOTA

113. Para copiar un nuevo fichero de configuración en memoria desde una ubicación remota:

```
scp 10.0.100.111 get configNueva.cfg config.cfg

Username: manager

Trying 10.0.100.111 ...

Press CTRL+K to abort

Connected to 10.0.100.111 ...

Enter password:
```

5.5.6. COPIAR FICHERO DE CONFIGURACIÓN A UNA UBICACIÓN REMOTA

114. Para copiar un fichero de configuración desde la memoria del equipo a una ubicación remota y de este modo tener un *backup* del fichero de configuración:

```
scp 10.0.100.111 put configVieja.cfg respaldo.cfg

Username: manager
```

```
Trying 10.0.100.111 ...

Press CTRL+K to abort

Connected to 10.0.100.111 ...

Enter password:
```

6. PLANO DE CONTROL (CONTROL PLANE)

6.1. SERVICIOS NIVEL 2

115. En esta sección, recogemos las recomendaciones de configuración asociadas a servicios de nivel 2, o nivel de enlace.

6.1.1. CONTROL DE BROADCAST

116. Para prevenir problemas es necesario limitar el volumen de paquetes de *broadcast* que circulan por la red. Para protegerse contra tormentas de *broadcast* se utiliza el comando siguiente:

```
[] interface GigabitEthernet x/y/z

[interface] broadcast-suppression 20
```

117. Se puede utilizar la siguiente secuencia para la verificación de la funcionalidad:

```
##GigabitEthernet1/0/1 current state: DOWN

##IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: […]

##Description: GigabitEthernet1/0/1 Interface

##Broadcast MAX-ratio: 20%
```

Nota: La configuración se realiza en cada interfaz del equipo en la que sea necesaria esta funcionalidad. Se pueden configurar los límites en porcentaje de la capacidad del equipo, en kbps o en pps.

6.1.2. VLAN

118. La mayoría de conmutadores de Nivel 2 asignan todos los puertos a un VLAN especial, normalmente VLAN 1. Además, muchos protocolos de Nivel 2 como Protocolo de árbol de expansión (STP/RSTP), Protocolo de registro GARP VLAN (GVRP) y el Protocolo de descubrimiento de la capa de enlace (LLDP), requieren una VLAN específica para enviar mensajes periódicos con el fin de controlar la red, utilizan también la VLAN 1.

119. Por todo esto, hay que configurar cuidadosamente la VLAN 1 para minimizar la inestabilidad de la red y también para evitar cualquier riesgo de seguridad en dispositivos que no sean de confianza que estén intentando explotar una vulnerabilidad en esta VLAN. A continuación, se dan algunas recomendaciones:

1. Eliminar todos los puertos de acceso desde VLAN 1.
2. Eliminar VLAN 1 de la configuración de los puertos trunk.

3. No utilizar VLAN 1 para gestión en banda, dedique un VLAN específico para la gestión en banda con el fin de separar el usuario y el tráfico de control de red.

6.1.2.1. CONTROL DE ACCESO DEL TRÁFICO

120. Es posible realizar un control de acceso del tráfico entre VLAN mediante políticas de QoS de la VLAN. Para ello, se crea una regla ACL que coincida con el tráfico y en las políticas de QoS de la VLAN se aplica una acción.

```
[] acl number <numero_ACL> name <nombre_ACL>
[acl] rule permit <protocol> <destination-port> <source-address> <source-port> <destination-address>
[acl]quit

[] traffic behavior <nombre_behavior>
[behavior] <permit|deny>
[behavior] quit

[] traffic classifier <nombre_classifier>
[classifier] if-match <nombre_ACL>
[classifier] quit

[] qos policy <nombre_QoS>
[policy] classifier <nombre_classifier> behavior <nombre_behavior>
[policy] quit

[] qos vlan-policy <nombre_policy> vlan <vlan_id> inbound
```

6.1.2.2. VLANs PRIVADAS (PVLAN)

121. Al usar VLAN Privadas (PVLAN) se puede limitar la conectividad entre máquinas dentro de una VLAN. Hay tres tipos:

1. Una VLAN aislada bloquea totalmente las comunicaciones entre dispositivos de la VLAN (que se comunicarán con el exterior a través de puertos promiscuos):

```
[] vlan <VLAN-aislada_id>
[vlan-aislada] isolated-vlan enable
[vlan-aislada] quit

[] vlan <VLAN-primaria_id>
[vlan-primaria] isolate-user-vlan enable
[vlan-primaria] quit

[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] port isolate-user-vlan {host | <VLAN-primaria_id> promiscuous}
[GigabitEthernet-x/y/z] port access vlan <VLAN-aislada_id>
[GigabitEthernet-x/y/z] quit
```

```
[] isolate-user-vlan <VLAN-primaria_id> secondary <VLAN-aislada_id>
```

2. Una *community* VLAN permite comunicaciones internas y con puertos promiscuos, aunque no se permiten comunicaciones entre dos *communities* distintas o con VLAN aisladas (una VLAN secundaria se considera *community* por defecto).

```
[] vlan <VLAN-primaria_id>
[vlan] isolate-user-vlan enable
[vlan] quit

[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] port isolate-user-vlan host
[GigabitEthernet-x/y/z] port access vlan <community-VLAN_id>
[GigabitEthernet-x/y/z] quit

[] isolate-user-vlan <VLAN-primaria_id> secondary <community-
VLAN_id>
```

3. Los puertos promiscuos pueden comunicarse con cualquier puerto de las VLAN primaria y secundaria.

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] port link-mode bridge
[GigabitEthernet-x/y/z] port isolate-user-vlan promiscuous
[GigabitEthernet-x/y/z] port link-type hybrid
[GigabitEthernet-x/y/z] port hybrid vlan <VLAN-aislada_id> to
<VLANs-communities&primaria_ids> tagged
[GigabitEthernet-x/y/z] quit

[] isolate-user-vlan <VLAN-primaria_id> secondary
<VLAN_secundarias_ids>
```

Nota: Debe prevenirse la subversión de la configuración de las PVLAN mediante el uso de firewalls o ACLs.

6.1.3. SPANNING TREE

122. Este es un protocolo cuyo propósito es evitar bucles en la red. Si bien no se trata de un protocolo que presente vulnerabilidades al propio sistema, sí que es necesario una configuración optimizada para evitar que pueda ser alterada y, por tanto, utilizado para alterar la topología de modo que se encamine tráfico de manera malintencionada.

6.1.3.1. BPDU GUARD

123. Los usuarios maliciosos pueden atacar un dispositivo de red enviando BPDUs de forma deliberada a puertos de extremo de red que pueden provocar un recalculo y problemas de topología de red.

124. Se puede evitar este tipo de ataques utilizando la función de *BPDU guard* tal y como se muestra:

```
[] stp bpdu-protection
```

125.Se pueden verificar los cambios de configuración que se han hecho.

```
[] display stp

[] display stp bpdu-statistics
```

Nota: Esta funcionalidad estará activada en todos los puertos configurados como *stp edge-port enable.*

6.1.3.2. TC-BPDU ATTACK GUARD

126.Al recibir un TC-BPDU (un PDU utilizado como notificación de cambio de topología dentro de los tipos de mensajes de STP), el dispositivo borrará la entrada de la dirección de reenvío correspondiente. Si un usuario malicioso envía una gran cantidad de TC-BPDUs a un dispositivo en un breve periodo de tiempo, el dispositivo puede saturarse eliminando la dirección Media Access Control (MAC), la tabla de dirección y las entradas de Protocolo de resolución de dirección (ARP), que puede afectar al cálculo del árbol de topología, ocupar una gran cantidad de ancho de banda e incrementar el uso de la CPU del dispositivo.

127.Con la función de *TC-BPDU attack guard* habilitada, el dispositivo realiza una operación de eliminación al recibir un TC-BPDU e inicia al mismo tiempo un temporizador (establecido en 10 segundos por defecto). Antes de que termine el temporizador, el dispositivo solo realiza la operación de eliminación durante un número de veces limitado (hasta seis veces por defecto) sin tener en cuenta el número de TC-BPDU que reciba. Esto evita la eliminación frecuente de entradas de direcciones de reenvío.

128.Los comandos siguientes sirven para habilitar esta funcionalidad.

```
[] stp bpdu-protection

[] stp tc-protection threshold <segundos>
```

6.1.3.3. ROOT GUARD

129.Hay una configuración de seguridad que proporciona el equipo para el protocolo SPT llamada Root guard cuya función es proteger el nodo raíz (root bridge) de ataques maliciosos o errores de configuración. Root guard no permite que un puerto *STP-designated* se convierta en un puerto *STP-root*. De manera que, si un paquete BPDU superior llega a ese puerto, root guard no lo tiene en cuenta y no elige entonces un nuevo nodo raíz. En vez de eso, pone el puerto en un estado de espera llamado *root-inconsistent STP state*, bloqueando el paso de las BPDUs superiores. Al cabo de un tiempo el puerto vuelve a su estado inicial de forma automática.

130.Para habilitar la funcionalidad Root Guard en un Puerto:

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] stp root-protection
```

Nota: Hay que habilitar Root Guard en los puertos donde no debe aparecer el nodo raíz, es decir en los puertos designados.

6.1.3.4. PUERTOS DEDICADOS A ACCESO DE RED

131.En aquellos puertos que vayan a ser destinados a acceso de usuarios y sistemas finales, debemos evitar que el equipo no establezca relaciones de vecindad con potenciales

equipos que se conecten. El establecimiento de una adyacencia de SPT podría alterar la topología de red y por tanto, reencaminar el curso del tráfico.

132. Con la siguiente secuencia de configuración, además de proporcionar estabilidad a la red, se ignoran BPDUs de estaciones finales.

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] stp edged-port enable
```

6.1.4. LLDP

133. Este protocolo tiene en su definición inicial, una intencionalidad de ayudar a la administración de las redes. Este protocolo proporciona información de plataformas vecinas, así como datos del enlace que los une.

134. Su funcionalidad también es usada para aplicaciones en la red. Un ejemplo de esta es la utilización que hacen algunos teléfonos IP.

135. Se debe desactivar LLDP si no es estrictamente necesario ya que puede ser empleado de manera malintencionada.

```
[] undo lldp enable

[] display lldp status
```

Nota: Mediante la manipulación de LLDP se puede influir en algunos servicios de red.

6.2. SERVICIOS NIVEL 3

136. En esta sección se recogen recomendaciones de configuración asociadas a servicios de nivel 3, o nivel de red.

6.2.1. ENRUTAMIENTO

137. Cada uno de los protocolos de enrutamiento deben ser configurados para evitar adyacencias e información aprendida no deseadas.

6.2.1.1. ENRUTAMIENTO ESTÁTICO

138. La manera más sencilla de configurar enrutamiento es realizarlo de manera manual si el número de equipos no es alto.

139. Se puede configurar una ruta estática de la siguiente manera:

```
[] ip route-static 0.0.0.0 0.0.0.0 172.16.11.1
```

140. Para verificar la funcionalidad hay que mirar en la tabla de enrutamiento IP, donde aparece una entrada con protocolo *static*.

```
[] display ip routing-table
```

6.2.1.2. RIP

141. El protocolo de enrutamiento RIP, en su modalidad RIPv2 permite autenticar los anuncios de enrutamiento.

6.2.1.2.1. SELECCIÓN DE LOS VECINOS RIP

142. En este protocolo se deben configurar los vecinos RIP con los cuales queremos que se realice intercambio de información de enrutamiento. Para ellos se utiliza la siguiente secuencia de comandos:

```
[] rip <process-id>
[rip-id] peer <ip-address>
[peer-id] undo validate-source-address
[peer-id] quit
[rip-id] quit

[] display rip <process-id>
```

6.2.1.2.2. ESTABLECIMIENTO DE VENCIDAD RIP: AUTENTICACIÓN

143. En este protocolo se puede garantizar que un equipo no establezca adyacencia si el equipo vecino no pertenece al mismo dominio de administración. Para ello hacemos uso de la autenticación en los mensajes de RIP.

```
[] rip <process-id>
[rip] version 2
[rip] undo summary
 [rip] quit

[] interface <interface-type> <interface-number>
[interface] rip authentication-mode {md5 {rfc2082 [cipher] key-string
key-id | rfc2453 [cipher] key-string}
```

Nota: El último comando debe ejecutarse dentro del ámbito de la interfaz por la que se ejecuta RIP.

6.2.1.2.3. DESHABILITAR ENVÍO DE ACTUALIZACIONES DE ENRUTAMIENTO

144. Se debe deshabilitar el envío de actualizaciones RIP en las interfaces conectadas a redes externas para evitar la fuga de información.

```
[] rip <process-id>
[rip] silent interface all
[rip] undo silent interface <interface-type> <interface-number>
```

6.2.1.2.4. CONFIGURACIÓN DEL FILTRADO DE RUTAS EN RIP

145. Se deben utilizar políticas de filtrado de rutas para evitar que se introduzca información de enrutamiento falsa en la red. Se deben configurar políticas de filtrado de rutas entrantes y salientes (*inbound/outbound*) con ACL o listas de prefijos IP.

146. Para filtrar las rutas entrantes/recibidas:

```
[] rip [<process-id>] [vpn-instance <vpn-instance-name>]
[rip] filter-policy {<acl-number> | gateway <ip-prefix-name> | ip-prefix
<ip-prefix-name> [gateway <ip-prefix-name>]} import [<interface-type>
<interface-number>]
```

Nota: El parámetro *gateway* sirve para aceptar solo las rutas recibidas desde el nodo vecino que se especifica.

147. Para filtrar las rutas salientes/redistribuidas:

```
[] rip [<process-id>] [vpn-instance <vpn-instance-name>]
[rip] filter-policy {<acl-number> | ip-prefix <ip-prefix-name>} export
[<protocol> [<process-id>] | <interface-type> <interface-number>]
```

6.2.1.3. OSPF

148. Este protocolo de enrutamiento debe ser configurado para que únicamente establezca adyacencias con vecinos autorizados.

149. Para securizar este protocolo es necesario realizar dos acciones: configurar el modo de intercambio de la clave (MD5), y activar la funcionalidad y clave en cada uno de los interfaces que ejecutarán el protocolo.

6.2.1.3.1. ESTABLECIMIENTO DE ADYACENCIA OSPF: AUTENTICACIÓN EN ÁREA OSPF

150. Se debe configurar la autenticación en áreas OSPF. Para ello, se debe utilizar la siguiente secuencia en el ámbito de definición de cada una de las áreas.

```
[] ospf <process-id>
[ospf] area <area-id>
[area] authentication-mode {md5 | simple}
[area] quit
[orpf] quit

[] display ospf
```

6.2.1.3.2. ESTABLECIMIENTO DE ADYACENCIA OSPF: CONFIGURACIÓN DE INTERFAZ

151. También se debe configurar la autenticación en interfaces OSPF, en el ámbito de definición de cada una de las interfaces.

```
[] interface <interface-type> <interface-number>
[interface] ospf authentication-mode {hmac-md5|md5} key-id
[cipher|plain] password
[interface] quit

[] display ospf peer
```

6.2.1.3.3. DESHABILITAR ENVÍO Y RECEPCIÓN DE PAQUETES OSPF

152. Se debe deshabilitar el envío de paquetes OSPF en las interfaces conectadas a redes externas para evitar la fuga de información o la recepción de información falsa.

153. Hay que ejecutar los siguientes comandos para deshabilitar el envío y recepción de OSPF:

```
[] ospf <process-id>
[ospf] silent interface all
```

```
[ospf] undo silent interface <interface-type> <interface-number>
[ospf] quit

[] display ospf interface <interface-type> <interface-number>
```

6.2.1.3.4. CONFIGURACIÓN DEL FILTRADO DE RUTAS EN OSPF

154. Se debe filtrar las rutas calculadas a través de LSAs (Link State Advertisements) antes de que se instalen en las tablas de enrutamiento de OSPF.

155. Para filtrar las rutas entrantes/recibidas:

```
[] ospf [<process-id> | router-id <router-id> | vpn-instance <vpn-instance-name>]
[ospf] filter-policy {<acl-number> [ gateway <ip-prefix-name>] | gateway <ip-prefix-name> | ip-prefix <ip-prefix-name> [gateway <ip-prefix-name>] | route-policy <route-policy-name>} import
```

Nota: El parámetro *gateway* sirve para aceptar solo las rutas recibidas desde el nodo vecino que se especifica.

156. Para filtrar las rutas salientes/redistribuidas:

```
[] ospf [<process-id> | router-id <router-id> | vpn-instance <vpn-instance-name>]
[ospf] area <area-id>
[area] filter {<acl-number> | ip-prefix <ip-prefix-name>} {import | export}
```

Nota: Para filtrar Type-3 LSAs anunciadas a un área.

6.2.1.4. BGP

157. En el caso de hacer uso de este protocolo, se debe emplear autenticación en las adyacencias BGP.

6.2.1.4.1. ESTABLECIMIENTO DE CONEXIÓN BGP: AUTENTICACIÓN

158. La siguiente secuencia sirve para configurar la autenticación de peer BGP.

```
[] bgp <asn>
 [bgp] peer <ip-address> as-number <remote-asn>
 [bgp] peer <ip-address> password cipher <clave>
```

Nota: En ejemplo anterior, quedan como variables: el sistema autónomo propio <asn>, la IP remota del peer BGP y la clave compartida <clave>.

159. Para verificar la funcionalidad en operación:

```
[] display bgp
```

6.2.1.4.2. GTSM: MECANISMO DE SEGURIDAD TTL

160. GTSM (Generalized TTL Security Mechanism, RFC 3682) se utiliza para evitar ataques DoS a BGP. Por defecto, se aceptan paquetes entrantes con un TTL de 0 o superior. Esto significa que si un atacante utiliza un TTL de hasta 255 podría enviar paquetes al puerto

BGP, pudiendo causar una inundación, si está a menos de 256 saltos, y el nodo externo los aceptaría. Por seguridad, se puede configurar para que solo se acepten los paquetes entrantes del nodo vecino (se puede especificar el número de saltos máximo para lo que se considera un nodo como vecino).

161. Para configurarlo, se necesitan los siguientes comandos:

```
[] bgp <asn>
 [bgp] peer <ip-address> as-number <remote-asn>
 [bgp] peer <ip-address> ttl-security hops <hop-count>
```

Nota: Se aceptan únicamente los paquetes que llegan con un TTL mayor a 255 menos el número de saltos (*hop-count)* especificado. Habría que asegurarse de que los nodos vecinos envían sus paquetes con un TTL de 255.

6.2.1.4.3. FILTRAR LOS PREFIJOS BGP CON UNA LISTA DE PREFIJOS

162. Otra medida importante de seguridad en BGP, además de la autenticación, es filtrar los prefijos que se envían o reciben via BGP. Se debe configurar una lista de prefijos que se permiten y/o rechazan en ambas direcciones (*inbound y outbound*), es decir los que se aprenden y se anuncian. Un ejemplo de prefijos que se deben rechazar son aquellos reservados para testeo o uso local descritos en RFC 3330 o aquellos que pertenecen a espacios de direcciones IP sin asignar (*bogons*).

163. Primero hay que definir las listas de prefijos:

```
[] ip ip-prefix BGP-PL-INBOUND index <num> deny | permit 192.168.2.0 24

[] ip ip-prefix BGP-PL-OUTBOUND index <num> deny | permit 192.168.2.0 24
```

164. Se puede verificar con el comando siguiente que se han añadido correctamente:

```
[] display ip ip-prefix
```

Nota: Hay que elegir si se desea denegar o permitir el prefijo de la red que se especifica a continuación (por ejemplo la ruta 192.168.2.0/24). El *número* de índice sirve para fijar un orden a las reglas: la que tenga un índice más bajo es la primera que se comprueba.

165. A continuación, se deben configurar las políticas de filtrado de rutas de distribución de BGP:

```
[] bgp <asn>
[bgp] peer <ip-address> ip-prefix BGP-PL-INBOUND import
[bgp] peer <ip-address> ip-prefix BGP-PL-OUTBOUND export
```

Nota: El filtrado de rutas también se podría hacer con AS-path ACL (*Autonomous System path Access*).

6.2.1.5. IS-IS

166. En el protocolo ISIS es posible establecer diferentes niveles de seguridad: por interfaz, por área y por dominio.

6.2.1.5.1. ESTABLECIMIENTO DE ADYACENCIA IS-IS: AUTENTICACIÓN PEER

167. Para configurar la autenticación con un vecino, es decir por la interfaz que conecta con el vecino, se utilizan los comandos siguientes:

```
[] interface <interface-type> <interface-number>
[interface] isis authentication-mode md5 <password> [level-1 | level-2]
[ip | osi]
```

168. Para verificar la funcionalidad se pueden utilizar varios comandos:

```
[] display isis brief

[] display isis interface

[] display isis peer
```

6.2.1.5.2. ESTABLECIMIENTO DE ADYACENCIA IS-IS: AUTENTICACIÓN ÁREA

169. Para configurar la autenticación en área:

```
[] isis [<process-id>]
[isis] area-authentication-mode md5 <password> [level-1 | level-2] [ip |
osi]
```

6.2.1.5.3. ESTABLECIMIENTO DE ADYACENCIA IS-IS: AUTENTICACIÓN DOMINIO

170. La configuración de la autenticación en dominio es similar a las anteriores:

```
[] isis [<process-id>]
[isis] domain-authentication-mode md5 <password> [level-1 | level-2] [ip
| osi]
```

6.2.1.5.4. DESHABILITAR ENVÍO Y RECEPCIÓN DE PAQUETES IS-IS

171. Se debe deshabilitar el envío y recepción de paquetes IS-IS en las interfaces conectadas a redes externas para evitar la fuga de información o recepción de información falsa.

```
[] interface <interface-type> <interface-number>
[interface] isis silent
```

6.2.1.5.5. CONFIGURACIÓN DEL FILTRADO DE RUTAS EN IS-IS

172. Los paquetes LSP (*Link State PDUs*) son los encargados de distribuir la información de enrutamiento entre los nodos IS-IS. Estos los guardan en la LSDB (*Link State Database*), utilizan el algoritmo SPF para calcular la ruta más corta, y finalmente la instalan en su tabla de enrutamiento. Por seguridad, se debe filtrar con ACL, con una lista de prefijos IP o una política de enrutamiento las rutas calculadas antes de ser añadidas en la tabla.

173. Los nodos IS-IS también pueden enviar paquetes LSP a sus vecinos informando de las rutas para que las añadan en sus tablas. Se debe configurar para que solo se distribuyan a los vecinos las rutas que pasen el filtro.

174. Para filtrar las rutas calculadas de LSP recibidos:

```
[] isis [<process-id>] [vpn-instance <vpn-instance-name>]
[isis] filter-policy {<acl-number> | ip-prefix <ip-prefix-name> | route-
policy <route-policy-name>} import
```

175. Para filtrar las rutas redistribuidas:

```
[] isis [<process-id>] [vpn-instance <vpn-instance-name>]
[isis] filter-policy {<acl-number> | ip-prefix <ip-prefix-name> | route-
policy <route-policy-name>} export [<protocol> [<process-id>]]
```

176. Se pueden utilizar los comandos siguientes para verificar la funcionalidad:

```
[] display isis route

[] display isis lsdb
```

6.2.2. PROTECCIONES CONTRA LA SUPLANTACIÓN DE IDENTIDAD

177. Muchos ataques utilizan la falsificación de direcciones IP de origen para ser efectivos, como algunos ataques DoS o DDoS, o para ocultar el verdadero origen de un ataque y dificultar el rastreo de tráfico. Comware ofrece *Unicast Reverse Path Forwarding* (URPF) así como *IP Source Guard* (IPSG) para impedir ataques que se basen en la suplantación de dirección IP de origen. Además, a menudo se despliegan ACL y *null routing* como medios manuales de prevención de suplantación de identidad.

178. *IP Source Guard* es efectivo para reducir la suplantación de las redes que están bajo control directo administrativo, utilizando puerto del conmutador, dirección MAC y verificación de dirección de origen.

179. URPF ofrece verificación de red de origen y puede reducir los ataques de suplantación de las redes que no estén bajo control directo administrativo.

180. La seguridad del puerto se puede utilizar para validar direcciones MAC en el nivel de acceso.

181. La detección ARP mitiga los vectores de ataque que utilizan envenenamiento ARP en segmentos locales.

6.2.2.1. PROTECCIÓN BÁSICA ANTI-SPOOFING MEDIANTE ACL

182. Una configuración manual de los ACL puede ofrecer una protección anti-spoofing cuando en un ataque se usan direcciones desconocidas o sin confianza.

```
[] acl number <numero_ACL> name <nombre_ACL>
[acl] rule deny ip source <ip> <netmask>
[acl] quit

[] interface <interface-type> <interface-number>
[interface] packet-filter name <nombre_ACL> inbound
```

6.2.2.2. URPF

183. URPF permite a un dispositivo verificar que la dirección de origen de un paquete reenviado se puede alcanzar a través de la interfaz que recibió el paquete.

184. No debe emplearse URPF como la única protección contra la suplantación de identidad. Los paquetes falseados podrían introducirse en la red a través de una interfaz habilitada con URPF si hubiera una ruta adecuada de retorno a la dirección IP de origen.

185. URPF se puede configurar de dos modos: flexible (*loose*) o estricto (*strict*). En los casos en los que haya un enrutamiento asimétrico es preferible la configuración de modo

flexible porque el modo estricto desecha paquetes en estas situaciones.

```
[] ip urpf loose | strict
```

Nota: Se configura URPF de forma global. Para prevenir la pérdida de paquetes y rutas válidas, no se permite habilitar URPF si el número de rutas de entrada que mantiene el switch excede la mitad del tamaño de la tabla de enrutamiento.

6.2.2.3. PROTECCIÓN IP SOURCE GUARD

186. Después de recibir un paquete, un puerto con *IP source guard* habilitado obtiene los atributos clave (dirección IP de origen, dirección MAC de origen y etiqueta VLAN) del paquete y después busca una coincidencia entre las entradas vinculantes del *IP source guard*. Si existe coincidencia, el puerto reenvía el paquete; si no, lo desecha. Se puede habilitar esta propiedad en un puerto conectado a terminales para bloquear el acceso ilegal (como *IP spoofing*) y mejorar la seguridad del puerto.

187. *IP source guard* soporta entradas estáticas y dinámicas. Puede configurar las entradas estáticas en escenarios en los que haya sólo algunos hosts en un LAN y sus direcciones IP estén configuradas manualmente. Por ejemplo, puede configurar una entrada estática de un puerto que se conecta a un servidor de manera que el puerto reciba y envíe paquetes solamente desde/al servidor.

188. Configuración de *IP Source Guard* estático:

```
[] interface <interface-type> <interface-number>
[interface] ip source binding {ip-address <ip> | mac-address <mac (xxxx-xxxx-xxxx>}*
```

189. Para configurarlo de una forma dinámica (habiendo activado previamente DHCP snooping, que se explica cómo en el apartado siguiente):

```
[] interface <interface-type> <interface-number>
[interface] ip verify source {ip-address | mac-address}*
```

190. Para verificar la funcionalidad se utiliza el siguiente comando:

```
[] display ip source binding
```

6.2.2.4. PROTECCIÓN DHCP SNOOPING

191. Hay dos acciones básicas asociadas a esta funcionalidad:

1. Asociaciones IP-a-MAC de clientes DHCP: DHCP snooping guarda las direcciones MAC e IP leyendo sus mensajes DHCP-REQUEST y DHCP-ACK de los puertos de confianza.
2. Asegurar que los clientes DHCP obtengan direcciones IP de servidores DHCP válidos: Cuando hay en la red un servidor DHCP no autorizado, un cliente DHCP puede obtener una dirección IP ilegal. Para asegurar que los clientes DHCP obtienen direcciones IP de servidores DHCP válidos, puede especificar que un puerto sea de confianza o sin confianza, mediante la función DHCP snooping.
    i. Puertos de confianza: Un puerto de confianza está conectado a un servidor DHCP autorizado directa o indirectamente. Reenvía mensajes DHCP para garantizar que los clientes DHCP puedan obtener direcciones IP válidas.

ii. Puertos sin confianza: Un puerto sin confianza está conectado a un servidor DHCP no autorizado. Los paquetes DHCP-ACK o DHCP-OFFER recibidos del puerto se rechazan, evitando que los clientes DHCP reciban direcciones IP no válidas.

192. La configuración de estas protecciones puede contener muchas variables. Se establecen en este documento una configuración ejemplo de protección, existiendo más opciones de las aquí mostradas.

193. Para habilitar DHCP snooping de forma global se utiliza el comando siguiente:

```
[] dhcp-snooping
```

194. Para habilitarlo en un puerto donde se conecta un servidor DHCP autorizado:

```
[] interface <interface-type> <interface-number>
[interface] description Puerto de servidor DHCP
[interface] dhcp-snooping trust
```

Nota: El comando *description* únicamente da una descripción a la interfaz, no es un comando necesario para configurar DHCP snooping.

195. Para habilitarlo en un puerto de acceso con opción 82 standard:

```
[] interface <interface-type> <interface-number>
[interface] description Puerto de acceso
[interface] dhcp-snooping information enable
[interface] dhcp-snooping information format verbose node-identifier sysname dhcp-snooping trust
```

196. Si se quiere comprobar la funcionalidad se utilizan los comandos:

```
[] display dhcp-snooping binding

[] display dhcp-snooping trust

[] display dhcp-snooping packet statistics
```

6.2.2.5. PROTECCIÓN ARP DETECTION

197. Sirve para mitigar ataques de envenenamiento (*poisoning*) ARP donde al atacante envía paquetes ARP falsos con el objetivo de corromper la caché de ARP o realizar un ataque de hombre en el medio. Su objetivo es bloquear los paquetes ARP provenientes de clientes no autorizados para prevenir ataques de suplantación (*spoofing*).

198. *ARP Detection* funciona validando la IP y la MAC de los paquetes ARP que circulan, utilizando los datos generados por *IP Source Guard* o DHCP snooping. Si no se han habilitado ninguno de estos dos mecanismos de seguridad hay que configurar manualmente la comprobación de la validez de usuario creando una serie de reglas.

199. Primero se debe comprobar la validez de usuario:

```
[] arp detection <id-number> {permit | deny} ip {any | <ip-address> [<mask>]} mac {any | <mac-address> [<mask>]} [vlan <vlan-id>]
```

Nota: Se verifica siempre, aunque se tenga habilitado DHCP snooping o IP Source Guard.

200. A continuación, se habilita la funcionalidad ARP Detection:

```
[] vlan <vlan-id>
[vlan] arp detection enable
```

201. Por defecto, todos los puertos se consideran inseguros y se aplica ARP Detection. Si se quiere especificar que un puerto es seguro:

```
[] interface <interface-type> <interface-number>
[interface] arp detection trust
```

202. También se pueden configurar otra serie de reglas acerca de la MAC origen, de la MAC destino y de la IP, de forma que se verificarán primero estas reglas generales y luego se comprobará la validez de usuario. Para ello se utiliza el siguiente comando:

```
[] arp detection validate {dst-mac | ip | src-mac}
```

Nota: Se pueden elegir los parámetros que se quieren verificar al habilitar la funcionalidad:

src-mac: verifica si la MAC en el cuerpo del mensaje es la misma que la de la cabecera Ethernet.

dst-mac: verifica si la MAC destino de los paquetes ARP de respuesta es todo ceros, todo unos o no se corresponde con la de la cabecera Ethernet. Si es así, se descartan.

Ip: verifica las direcciones IP origen y destino de los paquetes ARP de respuesta. Se consideran inválidas direcciones "todo ceros", "todo unos" y multicast.

203. Para comprobar que se ha configurado correctamente:

```
[] display arp detection

[] display arp detection statistics
```

6.2.2.6. PROTECCIÓN ARP CONTRA IP FLOOD ATTACKS

204. Si el dispositivo recibe un número elevado de paquetes IP desde un host con destinos inalcanzables, el dispositivo envía muchos ARP *request*, inundando las subredes vecinas, y por otro lado sigue intentando resolver la dirección destino de los paquetes IP, incrementando la CPU.

205. Para protegerlo de estos ataques, se debe habilitar la función *ARP source suppression* o *ARP black hole routing*.

206. *ARP source* suppression sirve cuando los paquetes tienen la misma dirección de origen. Funciona estableciendo un umbral para el número de ARP *requests* que se envían durante 5 segundos para paquetes con una dirección destino que no se puede resolver. Si se sobrepasa el umbral, se suprime el envío de ARP *requests* en los siguientes 5 segundos.

207. Se habilita y configura *ARP source suppression* de la forma siguiente:

```
[] arp source-suppression enable

[] arp source-suppression limit <limit-value>
```

Nota: *limit-value* es el valor umbral, es decir el máximo número de paquetes que se aceptan durante 5 segundos. Si no se especifica, el valor por defecto es 10.

208. Para verificar la funcionalidad:

```
[] display arp source-suppression
```

209. Por otra parte, *ARP black hole routing* sirve cuando los paquetes tienen diferentes direcciones de origen. Si se reciben paquetes cuya dirección de destino no se puede resolver con ARP, se crea una ruta nula (*black hole route*) donde se envían todos los paquetes.

210. Se habilita *ARP black hole routing* de la forma siguiente:

```
[] arp resolving-route enable
```

6.2.2.7. LIMITAR TASA DE PAQUETES ARP

211. Sirve para limitar la tasa de paquetes ARP procesados en la CPU del switch. Es muy útil si se habilita la función *ARP Detection* ya que todos los paquetes ARP se redireccionan a la CPU para examinarlos, y si un atacante envía muchos podría causar una ralentización del sistema por la sobrecarga. Se debe habilitar esta opción después de *ARP Detection* o para evitar ataques *ARP flood*.

212. Para habilitar esta funcionalidad se deben utilizar los comandos siguientes:

```
[] snmp-agent trap enable arp rate-limit

[] arp rate-limit information interval <seconds>

[] interface <interface-type> <interface-number>
[interface] arp rate-limit {disable | rate <pps> drop}
```

Nota: Los dos primeros comandos sirven para habilitar y especificar el intervalo (*seconds*) en el que se envían los mensajes de captura y logs para informar de que la tasa de ARP se ha excedido. De esta manera, también se limita el número de mensajes de señalización para evitar que se sobrecargue el sistema. El parámetro *pps* es la tasa límite en paquetes por segundo.

6.2.2.8. DETECCIÓN DE ATAQUES ARP BASADOS EN DIRECCIÓN MAC ORIGEN

213. Se debe utilizar esta configuración para limitar el número de paquetes ARP que envía una misma dirección MAC. Se detecta un ataque cuando la tasa de paquetes ARP sobrepasa durante 5 segundos un cierto umbral. La dirección MAC se añade entonces a la tabla de detección de ataques.

214. Para habilitar y configurar *ARP source suppression*:

```
[] arp anti-attack source-mac {filter | monitor}

[] arp anti-attack source-mac threshold <threshold-value>

[] arp anti-attack source-mac aging-time <time>

[] arp anti-attack source-mac exclude-mac <mac-address>
```

Nota: Se debe elegir entre el modo **filter**, donde se genera un log y filtra los paquetes ARP provenientes de la MAC atacante (recomendado), o modo **monitor** que simplemente genera un log. El parámetro *threshold-value* es el valor umbral y *time* es el tiempo que se desea que permanezca la MAC detectada en la tabla de atacantes. El último comando sirve para especificar una MAC que se sabe que es segura, por lo que no hace falta que se filtre.

215. Para verificar la funcionalidad en operación:

```
[] display arp anti-attack source-mac {slot <slot-number> | interface
<interface-type> <interface-number>}
```

6.2.2.9. PROTECCIÓN ICMP

216. Para mejorar el rendimiento del equipo se debe quitarle visibilidad, así como proteger la CPU, para ello se propone considerar la inclusión de estos comandos.

```
[] undo ip unreachables

[] undo ip redirects

[] undo ip ttl-expires
```

6.2.2.10. LIMITACIÓN DE ENCAMINAMIENTO DE BROADCAST DIRIGIDOS

217. Se debe limitar el ámbito de los *broadcast* que pueden recibirse en una determinada red. Deshabilitado por defecto, puede activarse y filtrar quien puede hacer llegar *broadcast* a una red.

218. Para deshabilitar *broadcast* externos a nivel global:

```
[] (undo) ip forward-broadcast
```

219. Para deshabilitar *broadcast* externos, en una interfaz particular o limitar quien puede mandarlos:

```
[] interface <interface-type> <interface-number>
[interface] (undo) ip forward-broadcast [acl <numeroACL>]
```

6.3. LIMITACIÓN DEL TRÁFICO EN EL PLANO DE CONTROL

220. La funcionalidad de protección del plano de control, permite configurar una política de calidad de servicio (QoS) para manejar que tasa de paquetes y de qué tipo pueden llegar al equipo, evitando así ataques DoS. En este sentido, el plano de control puede ayudar a proteger el equipo.

221. Para aplicar una política QoS hay que seguir una serie de procedimientos previos, tal y como se muestra en la siguiente figura.

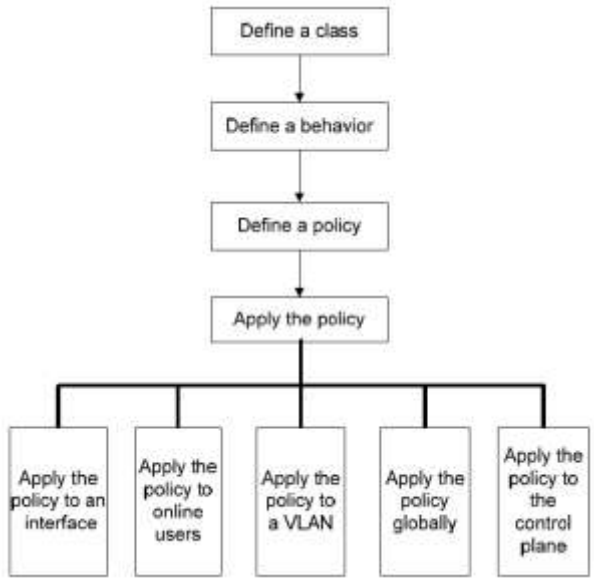

Figura 2. Procedimiento para la configuración de una política QoS

222. En el apartado 6.1.2.1 "Control de acceso del tráfico", se definieron la clase (*class*) y el comportamiento (*behavior*) de la política. Aquí se explicará únicamente como aplicar la política QoS al plano de control.

223. Se aplica una política QoS de la forma siguiente:

```
[] control-plane slot <slot-number>
[control-plane] qos apply policy <policy-name> [inbound|outbound]
```

224. Para verificar que se ha creado correctamente:

```
[] display qos policy control-plane slot <slot-number>
[] display qos policy control-plane pre-defined
```

Nota: En el caso de una pila o chasis virtual, se puede definir una política por CPU o miembro del stack.

7. PROTECCIÓN PARA IPV6

7.1. DETECCIÓN ND (NEIGHBOR DISCOVERY)

225. Es posible explotar el protocolo de descubrimiento de vecinos de IPv6 enviando paquetes construidos (ya que el protocolo no posee ningún mecanismo de seguridad). De esta forma, un atacante puede suplantar la identidad de un host o desconfigurar IPv6 en todos los equipos de la red al suplantar el *gateway*. Para detectar estos paquetes comprueba la consistencia de la MAC de la trama Ethernet (activado con el comando "ipv6 nd mac-check enable") y la detección ND, donde se comprueba que el origen del paquete sea válido:

```
[] vlan <vlan_id>
[vlan] ipv6 nd detection enable
[vlan] quit
```

```
[] interface <interface-type> <interface-number>
[interface] ipv6 nd detection trust
[interface] quit
```

226.Para comprobar la funcionalidad se utiliza el comando:

```
[] display ipv6 nd detection
```

7.2. CONFIGURACIÓN DE IPSEC

227.El switch permite utilizar IPsec. Para configurar correctamente esta funcionalidad, debe definirse un conjunto de parámetros de seguridad para la negociación IPsec SA. Pese a que existe la posibilidad de usar AH para autenticar, es preferible usar ESP ya que cifra la información.

228.Para configurar IPsec proposal:

```
[] ipsec proposal <nombre>

[] esp encryption-algorithm aes [longitud_clave]

[] esp authentication-algorithm sha1

[] encapsulation mode {transport | tunnel}
```

Nota: El parámetro *longitud_clave* es un entero que fija la longitud de la clave AES. Cuanto mayor sea más segura será, pero el rendimiento puede verse afectado.

229.Para configurar la política IPsec:

```
[] ipsec policy <nombre_pol> <numero_secuencia> manual

[] proposal <nombre_prop>

[] tunnel local <ip_local>

[] tunnel remote <ip_remota>

[] sa spi {inbound | outbound} esp <numero_spi>

[] sa {string-key|authentication-hex|encription-hex} {inbound|outbound}
esp <clave>
```

230.Para aplicar la política:

```
[] enable ipsec-policy <nombre_pol>
```

231.Finalmente, para ver estadísticas e información acerca de la funcionalidad:

```
[] display ipsec [policy|proposal|sa|statistics]
```

8. CONTROL DE TRÁFICO Y SEGURIDAD EN LOS PUERTOS

8.1. CREACIÓN DE LISTAS DE ACCESO (ACLS)

232.Este modelo soporta tres tipos de lista de acceso: básicas, avanzadas y de nivel 2. Las

listas de acceso básicas se basan en direcciones de origen, IPv4 o IPv6. Las listas de acceso avanzadas, permiten seleccionar entre más valores tanto si son de IPv4 como si son de IPv6: *Source address, destination address, packet priority, protocols over IP*, y otros campos de las cabeceras de Nivel 3 y Nivel 4.

233. Las listas de acceso permiten ser programadas en el tiempo.

234. Pueden analizar tramas de nivel 2, permiten filtrar basado en valores de la cabecera de nivel 2, direcciones origen y destino MAC, 802.1p, y protocolo de capa de red (*link layer protocol type*).

235. Las listas de acceso permiten la edición de una entrada, ya que estas se encuentran numeradas.

236. Existen 3 tipos de listas de acceso:

- Listas de acceso básicas (en las que se emplea los números 2000 al 2999) y que solo comprueban la dirección origen de los paquetes de IPv4 e IPv6.
- Listas de acceso avanzadas (emplean los números 3000 al 3999) que verifican las direcciones origen y destino, prioridad, protocolos de capas superiores y otros campos de las cabeceras de IPv4 e IPv6.
- Listas de acceso de cabeceras de tramas Ethernet (emplean del 4000 al 4999) y comprueban campos de la cabecera de las tramas, prioridad de 802.1p y tipo de protocolo de nivel de enlace.

8.1.1. EJEMPLO: LISTA DE ACCESO BÁSICA

237. Ejemplo de lista de acceso básica numerada:

```
[] acl number 2000
[acl] rule permit source 10.0.100.111 0.0.0.0
[acl] rule permit source 20.0.0.0 0.255.255.255
```

238. Ejemplo de lista de acceso básica con nombre:

```
[] acl number 2001 name listabasica
[acl] rule permit source 10.0.100.111 0
```

8.1.2. EJEMPLO: LISTA DE ACCESO AVANZADA

239. Ejemplo de lista de acceso avanzada numerada:

```
[] acl number 2000
[acl] rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100.111
0.0.0.0
```

240. Ejemplo de lista avanzada con nombre:

```
[] acl number 3001 name listaavanzada
[acl] rule deny ip source 10.1.100.0 0.0.0.255 destination 10.0.100.111 0
```

8.1.3. EJEMPLO: LISTA DE ACCESO TRAMAS

241. Ejemplo de lista de acceso de tramas de nivel 2:

```
[] acl number 4000
[acl] rule deny dest-mac 00aa-bb00-0000 00aa-bbff-ffff
```

Nota Este comando filtra las MACs de destino que empiezan por `00aa-bb`.

8.2. CREACIÓN DE LISTAS NEGRAS

242. Una alternativa al filtrado mediante ACL es la configuración de listas negras (más eficientes y fáciles de configurar).

243. Esta funcionalidad añade y elimina entradas de forma automática a partir de los fallos en el *login* de los usuarios y permite añadir también entradas de forma manual, las cuales pueden ser permanentes o no.

```
[] blacklist enable

[] blacklist ip <ip> [timeout <minutos>]
```

244. Para observar el estado de las listas negras se usa el comando:

```
[] display blacklist all
```

8.3. CONTROL DE TRÁFICO

245. El switch dispone del servicio **NetStream**, que se encarga de identificar anomalías y actividad relacionada con seguridad de red mediante el seguimiento de flujos de tráfico. La forma más sencilla de habilitar NetStream es en una interfaz:

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] ip netstream {inbound | outbound}
```

246. Con el siguiente comando se puede obtener información para el seguimiento de direcciones IP:

```
[] display ip netstream cache
```

247. En If(Direc) se puede ver la interfaz por la que llega el tráfico de una IP determinada:

```
Type DstIP(Port)          SrcIP(Port)          Pro ToS If(Direc)    Pkts
    DstMAC(VLAN)          SrcMAC(VLAN)
    TopLblType(IP/MASK)   Lbl-Exp-S-List

IP 11.1.1.1(1024)         11.1.1.2(21)          6  128 ET1/0(I)    42996
L2 0012-3f86-e94c(10)     0012-3f86-e86a(0)             ET1/4/0(I)  1253
MPLS LDP(3.3.3.3/24)      1:18-6-0                      ET1/1(O)     291
                            2:24-6-0
                            3:30-6-1
IP& 192.168.123.1(2048)   192.168.1.1(0)          1    0 ET1/1(O)      10
L2 0012-3f86-e95d(0)      0012-3f86-e116(1008)

IP& 172.16.1.1(68)        172.16.2.1(67)         17   64 ET1/2(I)    1848
MPLS LDP(4.4.4.4/24)      1:55-6-0
                            2:16-6-1
```

Figura 3. Información que proporciona la funcionalidad NetStream

248. El servicio **sFlow** es un monitor de tráfico que se utiliza para analizar estadísticas de tráfico. Para configurar el switch para conectar con un colector sFlow utilizamos los siguientes comandos:

```
[] sflow collector <colector-id> ip <ip>
[collector] sflow agent ip <ip>
[collector] quit

[] interface GigabitEthernet x/y/z [# Flow Sampling]
[GigabitEthernet-x/y/z] sflow sampling-mode {determine | random}
[GigabitEthernet-x/y/z] sflow sampling-rate <ratio>
[GigabitEthernet-x/y/z] sflow flow max-header <longitud>
[GigabitEthernet-x/y/z] sflow flow collector <colector-id>
[GigabitEthernet-x/y/z] quit

[] interface GigabitEthernet x/y/z [# Counter Sampling]
[GigabitEthernet-x/y/z] sflow counter interval <segundos>
[GigabitEthernet-x/y/z] sflow counter collector <colector-id>
```

8.4. LIMITACIÓN APRENDIZAJE DE PUERTOS

249. Se debe limitar el número de MACs que el equipo aprende en un determinado puerto a únicamente las estrictamente necesarias.

250. En este ejemplo se limita a 3 estaciones diferentes:

```
[] interface <interface-type> <interface-number>
[interface] mac-address max-mac-count 3
```

8.5. AISLAMIENTO DE PUERTOS: PORT-ISOLATIONS

251. Es una característica de seguridad de nivel 2 que limita la conectividad entre estaciones o servidores dentro de una VLAN. Sin el aislamiento de puertos todos los dispositivos dentro de una LAN pueden comunicarse entre sí libremente.

252. Existen situaciones en las que se debe limitar la comunicación entre dispositivos dentro de un segmento de red. El aislamiento de puertos a veces se usa para prohibir la comunicación entre servidores dentro de un segmento de red alcanzable desde el exterior. En el caso de que un servidor se hubiera comprometido la ausencia de conectividad con otros servidores debido a este aislamiento se limitaría el impacto de ese fallo de seguridad.

253. La funcionalidad incluye puertos aislados (*isolated ports*), puertos de uplink (*uplink ports*), y grupos de aislamiento (*isolated groups*). El sistema operativo de los switches permite la creación de múltiples grupos de aislamiento, cada uno de los cuales puede contener múltiples puertos aislados y un puerto de uplink.

8.5.1. PUERTOS AISLADOS (ISOLATED PORTS)

254. La configuración de algunos puertos en una VLAN como puertos aislados previene la comunicación entre los dispositivos conectados a esos puertos dentro de dicha VLAN.

255. Para configurar un puerto como *isolated port*:

```
[] interface <interface-type> <interface-number>
[interface] description *** Isolated Port ***
[interface] port access vlan <vlan-id>
[interface] port-isolate enable
```

8.5.2. PUERTOS UPLINK (UPLINK PORTS)

256. Para configurar un puerto como *uplink port*:

```
[] interface <interface-type> <interface-number>
[interface] description *** Uplink Port ***
[interface] port access vlan <vlan-id>
[interface] port-isolate uplink-port
```

8.5.3. GRUPOS DE AISLAMIENTO (ISOLATED GROUPS)

257. Para crear grupos:

```
[] interface <interface-type> <interface-number>
[interface] description *** Isolated Port of Group1 ***
[interface] port access vlan <vlan-id>
[interface] port-isolate enable group <number>

[] interface <interface-type> <interface-number>
[interface] description *** Uplink Port of Group 1 ***
[interface] port access vlan <vlan-id>
[interface] port-isolate uplink-port group <number>
```

8.6. LIMITACIÓN DE APRENDIZAJE DE PUERTOS: PORT SECURITY

258. Port security es un mecanismo de NAC (Network Access Control) basado en la dirección MAC. Es una extensión del IEEE 802.1X y la autenticación MAC. Previene del acceso no autorizado de dispositivo basándose en la verificación de la dirección MAC de origen, en el tráfico de entrada en el puerto, y de la dirección MAC de destino, en el tráfico de salida.

259. Con la seguridad de puerto activada (*port security*), las tramas cuya dirección MAC de origen no corresponde con una de las aprendidas por el equipo (con las condiciones establecidas) son consideradas ilegales. Las estaciones que no pueden ser autenticadas vía 802.1X o vía MAC son consideradas ilegales.

260. Una vez se han detectado las tramas o eventos ilegales, el dispositivo toma la acción predefinida automáticamente. Al mismo tiempo que se aumenta la seguridad se simplifica la administración del dispositivo. Los paquetes ilegales pueden ser de dos tipos:

1. Paquetes que haya fallado la autenticación
2. Paquetes cuya dirección MAC origen no haya sido aprendida

261. Los modos principales en que puede el puerto ser configurado son:

Modos	Descripción
noRestrictions	En este modo la funcionalidad está deshabilitada y no se restringe el acceso en el puerto.
autoLearn	El puerto en este modo añade las direcciones MAC aprendidas a la tabla de MAC address. Si se alcanza el límite, el puerto cambia a modo seguro.
secure	En este modo el puerto no aprende nuevas direcciones MAC y permite solo paquetes cuya dirección MAC origen coincide con una dirección MAC segura configurada para pasar.
userLogin	Un puerto en este modo ejecuta autenticación 802.1X e implementa control de acceso basado en Puerto. El puerto puede servir a diversos usuarios 802.1X. Si un usuario pasa la autenticación 802.1X todos los demás usuarios del puerto pueden acceder a la red sin autenticarse.
userLoginSecure	Un puerto en este modo ejecuta autenticación 802.1X e implementa control de acceso basado en MAC. El puerto sólo permite a un usuario pasar la autenticación 802.1X.
userLoginWithOUI	Este modo es similar al modo *userLoginSecure*. La diferencia es que un puerto en este modo también permite tramas desde una dirección MAC que contenga un identificador específico de organización (OUI).
macAddressWithRadius	Un puerto en este modo ejecuta autenticación MAC a los usuarios.
macAddressOrUserLoginSecure	Este modo es la combinación del modo *macAddressWithRadius* y del modo *userLoginSecure*. Para usuarios cableados el puerto ejecuta autenticación MAC una vez que recibe tramas non-802.1X y autenticación 802.1X si las recibe 802.1X.

Modos	Descripción
macAddressElseUserLoginSecure	Este modo es la combinación del modo *macAddressWithRadius* y del modo *userLoginSecure*. Ejecuta sólo autenticación MAC para non-802.1X. Para tramas 802.1X, ejecuta autenticación MAC y si esta falla, 802.1X.
userLoginSecureExt	Un puerto en este modo ejecuta autenticación 802.1X basada en MAC y permite que múltiples usuarios tengan acceso.
macAddressOrUserLoginSecureExt	Este modo es similar al modo *macAddressOrUserLoginSecure* excepto que un puerto en este modo permite que múltiples usuarios 802.1X y MAC tengan acceso.
macAddressElseUserLoginSecureExt	Este modo es similar al modo *macAddressElseUserLoginSecure* excepto que un puerto en este modo permite que múltiples usuarios 802.1X y Mac tengan acceso.

262. Presentamos a continuación el ejemplo de la configuración de una limitación de número de MACs en un determinado puerto. En este caso, se limita a 3 estaciones diferentes y se utiliza el modo *autolearn*.

```
[] port-security enable
[] interface Ethernet 0/4/1
 [Ethernet 0/4/1] port link-mode bridge
 [Ethernet 0/4/1] port-security max-mac-count 3
 [Ethernet 0/4/1] port-security port-mode autolearn
```

9. AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO (AAA)

263. La gestión de diversos dispositivos por varias personas diferentes puede crear importantes problemas de gestión de las cuentas de usuario. Este problema se puede resolver utilizando un servicio de autenticación central que simplifique la gestión de las cuentas. Con este mecanismo, la creación y eliminación de cuentas se realiza únicamente desde un servidor central. Esto resulta útil, por ejemplo, para habilitar o deshabilitar el acceso de un usuario a todos los dispositivos con un sencillo cambio que no requiere aplicar una configuración concreta a cada dispositivo.

264. Comware soporta dos protocolos para la autenticación central de usuarios en varios dispositivos: RADIUS y HWTACACS. El modelo de para la autenticación centralizada es fundamentalmente el mismo para RADIUS y HWTACACS.

265. A continuación, se ilustran unas configuraciones de ejemplo.

9.1. CONFIGURACIÓN RADIUS

266. Se pueden utilizar las siguientes secuencias para configurar un servidor RADIUS en el switch:

```
[] radius scheme demo
 [radius-demo] primary authentication 10.10.10.10 key simple <shared_key>
 [radius-demo] primary accounting 10.10.10.10 key simple <shared_key>
```

```
[radius-demo] secondary authentication 20.20.20.20 key simple
<shared_key>
[radius-demo] secondary accounting 20.20.20.20 key simple <shared_key>
[radius-demo] quit

[] domain system
[isp-system] authentication login radius-scheme demo local
[isp-system] accounting login radius-scheme demo local
[isp-system] quit

[] domain default enable system
```

Nota: Esta configuración autentica y registra acciones contra dos servidores, *10.10.10.10* y si falla este, contra *20.20.20.20* (se pueden configurar hasta 16 servidores secundarios).

Además, en la definición del dominio se ha especificado que, en caso de fallo, use usuarios locales como referencia.

El último comando es el que habilita las definiciones anteriores como defecto para el sistema. El nombre de usuario que envía el switch al servidor remoto está en el formato *userid@isp-name*, donde *isp-name* representa el ISP al que pertenece el usuario (por ejemplo, *system*).

9.2. CONFIGURACIÓN TACACS

267. El ejemplo siguiente es similar al anterior, pero sirve para configurar un servidor TACACS:

```
[] hwtacacs scheme demo
[hwtacacs-demo] primary authentication 10.10.10.10 key simple
<shared_key>
[hwtacacs-demo] primary accounting 10.10.10.10 key simple <shared_key>
[hwtacacs-demo] secondary authentication 20.20.20.20 key simple
<shared_key>
[hwtacacs-demo] secondary accounting 20.20.20.20 key simple <shared_key>
[hwtacacs-demo] quit

[] domain system
[isp-system] authentication login hwtacacs-scheme demo local
[isp-system] accounting login hwtacacs-scheme demo local
[isp-system] quit

[] domain default enable system
```

Nota: Esta configuración autentica y registra acciones contra dos servidores, *10.10.10.10* y si falla este, contra *20.20.20.20*. Además, en la definición del dominio se ha especificado que, en caso de fallo, use usuarios locales como referencia.

10. AUTENTICACIÓN EN RED LOCAL

10.1. AUTENTICACIÓN 802.1X

268. El switch permite la implementación de 802.1X, asignando una VLAN a un usuario que se ha autenticado. Esta funcionalidad permite asignar un estado a cada puerto (controlado – descontrolado) y dentro de los controlados, permitir o no el tráfico (por defecto, de forma automática). Esta autenticación se puede realizar en base al puerto o la MAC. Según la autenticación, se pueden asignar VLAN de invitados (para no autenticados), para quienes han fallado la autenticación (contraseña errónea), y VLAN críticas (ningún RADIUS está disponible).

269. Activación global:

```
[] dot1x
```

270. Para habilitar 802.1X en una interfaz se debe elegir el modo de control de acceso, establecer el límite máximo de usuarios por puerto y habilitar la reautenticación periódica (por defecto cada 3600s). Además, puede elegirse el tipo de trigger de autenticación (para cuando los clientes no pueden iniciar la autenticación) entre multicast (el switch envía EAP-Request por multicast para detectar clientes 802.1X) y unicast (el switch inicia la autenticación al recibir tráfico de una MAC desconocida):

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] dot1x
[GigabitEthernet-x/y/z] dot1x port-method {mac-based | portbased}
```

Nota: *mac-based* por defecto

```
[GigabitEthernet-x/y/z] dot1x max-user <numero_usuarios>
[GigabitEthernet-x/y/z] dot1x re-authenticate
[GigabitEthernet-x/y/z] dot1x {guest-vlan | auth-fail vlan | critical
vlan} <vlan_id>
[GigabitEthernet-x/y/z] dot1x {multicast-trigger|unicast-trigger}
```

Nota: Multicast por defecto

```
[GigabitEthernet-x/y/z] quit

[] display dot1x
```

10.1.1. EJEMPLO DE CONFIGURACIÓN DE ENTORNO

271. Hay que asegurarse de que está configurado el servidor RADIUS para AAA (se explica mas adelante) y de que se han creado las cuentas de usuario.

1. Primero hay que crear una VLAN y asignar los puertos:

```
[] vlan <vlan_id>
[vlan] port GigabitEthernet x/y/z
```

2. A continuación, se configura el esquema RADIUS (ya explicado anteriormente)

excluyendo el nombre de dominio del ISP del username enviado al RADIUS:

```
[Device-radius-<esquema>] user-name-format without-domain
```

3. Después, hay que configurar el dominio del ISP, aplicando el esquema RADIUS:

```
[] domain <dominio_ISP>
[isp] authentication lan-access radius-scheme <dominio_ISP>
[isp] authorization lan-access radius-scheme <dominio_ISP>
[isp] accounting lan-access radius-scheme <dominio_ISP>
```

4. El último paso es configurar 802.1X con guest VLAN:

```
[] dot1x (habilita globalmente)
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] dot1x
[GigabitEthernet-x/y/z] dot1x port-method portbased
[GigabitEthernet-x/y/z] dot1x guest-vlan <vlan_id>
```

10.1.2. HARDWARE AUTHENTICATION BYPASS PROTOCOL (HABP)

272. *HW Authentitaction Bypass Protocol* (HABP) se utiliza para que aquellos equipos que no soportan 802.1X puedan comunicarse a través de elementos de red que requieran autenticación sin realizarla.

273. Supongamos un ejemplo de escenario con tres switches (B-A-C). El switch A tiene habilitado 802.1X. Para poder realizar comunicaciones entra B y C, será necesario habilitar el servidor HABP en A y los clientes HABP en B y C, además de especificar una VLAN para los paquetes HABP. Suponiendo que el switch A tiene 802.1X configurado.

274. En el Switch A, habilitar HABP (habilitado por defecto) y configurarlo en modo servidor, usando la VLAN 1 para paquetes HABP:

```
[] habp enable
[] habp server vlan 1
```

275. En los switches B y C, habilitar HABP (habilitado por defecto), configurarlo en modo cliente (por defecto) y especificar la VLAN 2 para intercambio de paquetes HABP (un cliente HABP pertenece por defecto a VLAN 1):

```
[] habp enable
[] undo habp server
[] habp client vlan 2
```

10.2. AUTENTICACIÓN POR MAC

276. La autenticación por MAC no requiere ningún tipo de cliente. Al detectar una MAC desconocida, inicia un proceso de autenticación y, si falla, tira todos los paquetes durante un tiempo. Se puede configurar una *guest/critical* VLAN:

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] mac-authentication
[GigabitEthernet-x/y/z] mac-authentication max-user <n_max>
```

```
[GigabitEthernet-x/y/z] mac-authentication {guest-vlan | critical vlan}
<vlan_id>
```

10.2.1. AUTENTICACIÓN LOCAL

277. Se puede configurar una autenticación local o por un servidor RADIUS. Para hacerlo de manera local, hay que seguir los siguientes pasos:

1. Crear un usuario cuyo nombre y password sea su MAC en minúsculas y con guiones.
2. Configurar el dominio del ISP para realizar una autenticación local para los usuarios de la LAN:

   ```
   [] domain <dominio>

   [domain] authentication lan-access local
   ```

3. Activar la autenticación MAC globalmente y para el puerto x/y/z:

   ```
   [] mac-authentication

   [] mac-authentication interface GigabitEthernet x/y/z
   ```

4. Especificar el dominio del ISP para la autenticación MAC:

   ```
   [] mac-authentication domain <dominio>
   ```

5. Configurar la autenticación MAC para ser usada en cuentas basadas en MAC. Los nombres y passwords se expresan con guiones y en minúsculas.

   ```
   [] mac-authentication user-name-format mac-address with-hyphen
   lowercase
   ```

10.2.2. AUTENTICACIÓN CON RADIUS

278. Para autenticar con un servidor RADIUS se debe:

1. Crear una cuenta compartida para los usuarios autenticados en el RADIUS.
2. Configurar un esquema RADIUS añadiendo el siguiente comando:

   ```
   [Device-radius-<esquema>] user-name-format without-domain
   ```

3. Aplicar el esquema al dominio del ISP para AAA:

   ```
   [] domain <dominio>

   [dominio] authentication default radius-scheme <esquema>

   [dominio] authorization default radius-scheme <esquema>

   [dominio] accounting default radius-scheme <esquema>
   ```

4. Habilitar autenticación MAC globalmente o en un puerto x/y/z:

   ```
   [] mac-authentication

   [] mac-authentication interface GigabitEthernet x/y/z
   ```

5. Especificar el domino del ISP para autenticación MAC:

```
[] mac-authentication domain <dominio>
```

6. Especificar usuario y password de la cuenta compartida:

```
[] mac-authentication user-name-format fixed account <nombre_comun>
password simple <passwd_comun>
```

10.3. AUTENTICACIÓN MEDIANTE PORTAL WEB

279. La autenticación mediante portal (o autenticación web) permite el acceso a una red al autenticarse en un sitio web.

280. Vamos a ver un ejemplo de funcionamiento en el que los usuarios pueden acceder a una red en caso de no autenticarse, y acceder a Internet en caso de que sí. Suponiendo que todos los equipos están conectados de esta forma y configurados correctamente.

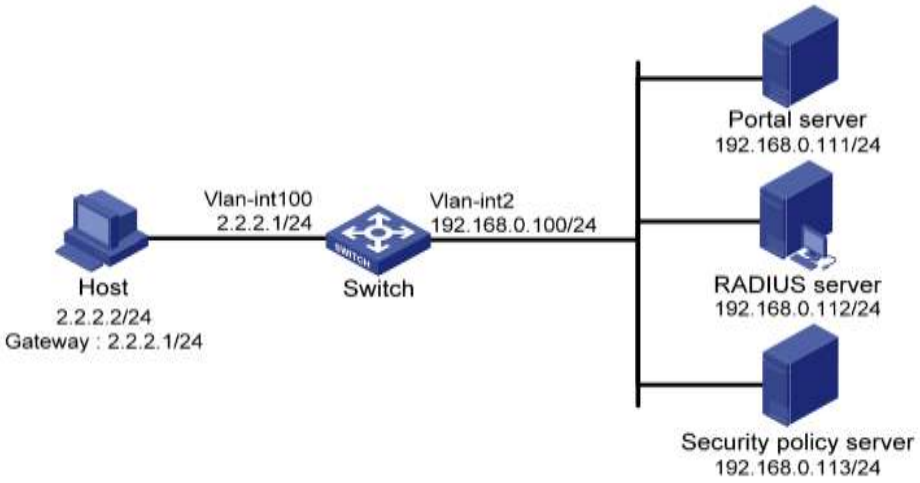

Figura 4. Esquema del escenario de autenticación por portal básico

1. Crear un esquema RADIUS (ya explicado), añadiendo los siguientes comandos:

```
[Switch-radius-<esquema>] user-name-format without-domain

[Switch-radius-<esquema>] security-policy-server
   <ip_serv_polit_segur>
```

2. Configurar un dominio de autenticación, configurando los métodos AAA:

```
[] domain <dominio>

[domain] authentication portal radius-scheme <esquema>

[domain] authorization portal radius-scheme <esquema>

[domain] accounting portal radius-scheme <esquema>
```

3. Configurar el dominio como *default* para todos los usuarios. Si uno introduce el nombre de usuario sin el dominio del ISP en el inicio de sesión, los métodos AAA del dominio se le aplican.

```
[] domain default enable <dominio>
```

4. Configurar un ACL para recursos de la subred (`rule permit ip destination <ip> <netmask>`) y otro para los recursos de Internet (`rule permit ip`). En el servidor de políticas de seguridad, especificar el primer ACL como el de aislamiento y el segundo ACL como el de seguridad.
5. Configurar el portal de autenticación y una regla *portal-free* en la interfaz que conecta con el servidor de portal.

```
[] portal server <nombre_servidor> ip <ip_portal_server> key
portal port <puerto> url <url>

[] portal free-rule 1 source interface GigabitEthernet x/y/z
destination any
```

6. Habilita la autenticación por portal en la interfaz que conecta al host.

```
[] interface vlan-interface <vlan>

[vlan] portal server <nombre_servidor> method direct
```

10.3.1. AUTENTICACIÓN MEDIANTE PORTAL WEB A NIVEL 2

281. Hay otra opción para autenticación mediante portal, hacerlo en capa 2. Vamos a ver un ejemplo de configuración, suponiendo los servidores RADIUS y DHCP, las VLAN y el dominio PKI correctamente configurados:

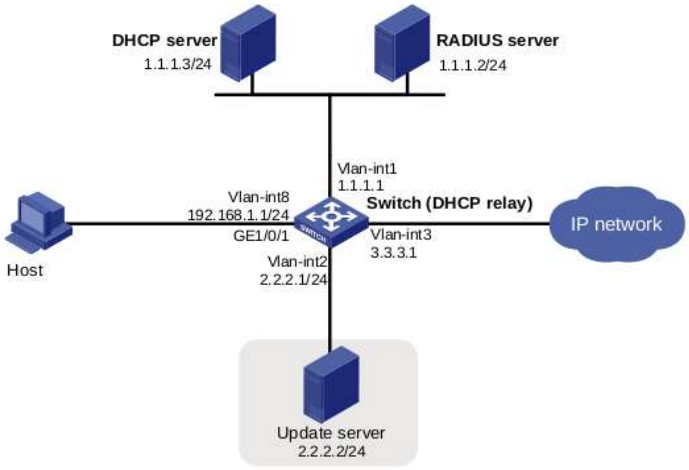

Figura 5. Esquema del escenario de autenticación por portal a nivel 2

1. Configurar el servidor de políticas SSL y especificar el dominio PKI.

```
[] ssl server-policy <serv_politica_SSL>

[ssl] pki <dominio_PKI>
```

2. Configurar el servidor de portal para soportar HTTPS y referenciar al de políticas SSL.

```
[] portal local-server https server-policy <serv_politica_SSL>
```

3. Configurar la IP de la interfaz de loopback <loop_iface> como <loop_ip> y especificarla como la IP de escucha del servidor de portal de capa 2

```
[] interface loopback <loop_iface>

[loopback] ip address <loop_ip> 32

[loopback] quit

[] portal local-server ip <loop_ip>
```

4. Habilitar autenticación por portal en el puerto GigabitEthernet y especificar la VLAN Auth-Fail.

```
[] interface GigabitEthernet x/y/z

[GigabitEthernet-x/y/z] port link-type hybrid

[GigabitEthernet-x/y/z] mac-vlan enable

[GigabitEthernet-x/y/z] portal local-server enable

[GigabitEthernet-x/y/z] portal auth-fail vlan <vlan_Auth-Fail>
```

5. Crear un esquema RADIUS (ya exlicado anteriormente). Establecer el tipo de servidor (al usar un servidor IMC, usar el tipo “extended”).

```
[Switch-radius-<esquema_RADIUS>] server-type extended
```

6. Configurar el dominio de autenticación. Crear un dominio de ISP, configurar los métodos AAA y establecer el dominio por defecto (ya explicado anteriormente).
7. Configurar el agente de relay DHCP. Crear un grupo de servidores DHCP y añadir el servidor de la red.

```
[] dhcp enable

[] dhcp relay server-group <id_grupo> ip <ip_serv_DHCP>
```

8. Habilitar el agente de relay DHCP. Correlar el grupo de servidores DHCP con la interfaz de VLAN del host.

```
[] interface vlan-interface <vlan_host>

[vlan] dhcp select relay

[vlan] dhcp relay server-select <id_grupo>
```

9. Hacer lo mismo con las VLAN Auth-Fail y la de acceso a Internet.

11. CONFIGURACIÓN PKI

282.Para configurar PKI en el switch, tenemos que configurar tres parámetros:

1. Entidad DN: Para identificar la identidad de un certificado a través de una *entity Distinguished Name*. Se crea una entidad y se entra en su vista. A continuación, se

rellenan una serie de parámetros opcionales acerca de la entidad DN:

```
[] pki entity <entity-name>

[] common-name <name>

[] country <country-code-str>

[] ip <ip-address>

[] locality <locality-name>

[] organization <org-name>
```

Nota: *country-code-str* es el código del país. Por ejemplo, US para EEUU, CN para China y ES para España.

2. A continuación, se crea el dominio PKI y se entra en su vista:

```
[] pki domain <domain-name>

[] ca identifier <name>

[] certificate request entity <entity-name>

[] certificate request from {ca | ra}

[] certificate request url <url-string>

[] root-certificate fingerprint {md5 | sha1} <string>
```

Nota: En el cuarto comando, hay que especificar el tipo de autoridad que gestiona la petición del certificado. Hay que añadir el último comando si se quiere hacer la verificación del certificado del root de forma automática. *url-string* es la URL del servidor de registro con el formato: http://host:port/Issuing Jurisdiction ID, donde Issuing Jurisdiction ID es una cadena de hexadecimales generada por el servidor de la CA. Por ejemplo: http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337

3. Para hacer la entrega de la petición del certificado PKI de forma automática:

```
[] pki domain <domain-name>

[] certificate request mode auto [ key-length <key-length> |
     password {cipher | simple} <password>]
```

283. Finalmente, para obtener el certificado de la CA o el local y guardarlo de forma local:

```
[] pki retrieval-certificate {ca | local} domain <domain-name>
```

12. AUTENTICACIÓN MEDIANTE TRIPLE PROTECTION

284. Puede realizarse un escenario en el que se combinen los tres tipos de autenticación que se han visto en este documento (802.1X, MAC y por portal).

285. Se realiza autenticación MAC al recibir paquetes ARP o DHCP *broadcast* por primera vez. Si la autenticación falla, se realiza una autenticación 802.1X o por portal.

286. Se realiza autenticación 802.1X cuando se reciben paquetes EAP de un cliente 802.1X. Si le función de *trigger unicast* está habilitada, cualquier paquete de un cliente 802.1X

puede disparar la autenticación 802.1X.

287. Se realiza autenticación por portal al recibir un paquete HTTP de un terminal.

288. Vamos a ver un ejemplo de los comandos que habría que introducir con un ejemplo concreto:

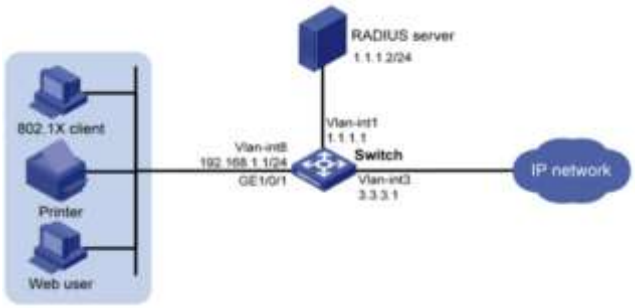

Figura 6. Esquema del escenario de autenticación mediante Triple Protection

289. Configurar el RADIUS para AAA. En este ejemplo, se añadirá un usuario 802.1X, un usuario de portal y otro de autenticación MAC; y una LAN autorizada. Configurar también las VLAN correspondientes

1. Configurar el servidor de portal local para soportar HTTP:

```
[] portal local-server http
```

2. Configurar la IP de la interfaz de loopback 0 como 4.4.4.4:

```
[] interface loopback 0
[loopback] ip address 4.4.4.4 32
[loopback] quit
```

3. Especificar la dirección IP de escucha del servidor de portal local para autenticación por portal en capa 2 como 4.4.4.4:

```
[] portal local-server ip 4.4.4.4
```

4. Habilitar autenticación por portal en capa 2 en la interfaz de red de los hosts:

```
[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] portal local-server enable
[GigabitEthernet-x/y/z] quit
```

5. Habilitar autenticación 802.1X globalmente. Además, hacerlo (control de acceso basado en MAC) en la interfaz de red de los hosts:

```
[] dot1x

[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] dot1x port-method macbased
[GigabitEthernet-x/y/z] dot1x
[GigabitEthernet-x/y/z] quit
```

6. Habilitar autenticación por MAC globalmente. Además, hacerlo en la interfaz de

red de los hosts:

```
[] mac-authentication

[] interface GigabitEthernet x/y/z
[GigabitEthernet-x/y/z] mac-authentication
[GigabitEthernet-x/y/z] quit
```

7. Crear un esquema RADIUS (como se ve en este documento). Establecer el tipo de servidor (al usar un servidor IMC, usar el tipo "extended"). Especificar los nombres de usuario enviados al servidor RADIUS para no llevar nombres de dominio:

```
[Switch-radius-<esquema_RADIUS>] server-type extended

[Switch-radius-<esquema_RADIUS>] user-name-format without-domain
```

8. Finalmente, configurar el dominio de autenticación. Crear un dominio de ISP, configurar los métodos AAA y establecer el dominio por defecto (como se ve en autenticación por portal). Si un nombre de usuario no incluye nombre de dominio del ISP, se usa el esquema por defecto:

```
[] domain default enable <dominio_ISP>
```

13. SECURIZACIÓN AUTOMATIZADA BÁSICA – MODALIDAD FIPS

290. El instituto estadounidense NIST (*National Institute od Standard adn Technology*) ha generado unas normas llamadas FIPS (*Federal Information Processing Standards*) (FIPS) especificando los requisitos para los módulos de cifrado.

291. La norma FIPS 140-2 define cuatro niveles de seguridad, simplemente llamados de "Level 1" a "Level 4", de menor a mayor seguridad. Actualmente el equipo HP 5500 EI soporta "Level 2". En el resto de este capítulo, las referencias a las siglas FIPS, se refieren a la norma FIPS 140-2.

292. Los cambios que se aplican al configurar el equipo en modo FIPS son los siguientes:

1. FTP/TFTP es deshabilitado.
2. Telnet es deshabilitado.
3. HTTP server es deshabilitado.
4. Cluster management es deshabilitado.
5. SNMPv1 y SNMPv2c son es deshabilitado. Sólo SNMPv3 es disponible.
6. SSL server solo soporta TLS1.0.
7. SSH server no acepta conexiones de clientes SSHv1.
8. SSH solo soporta RSA.
9. Las claves RSA tienen que usar una longitud de módulo de 2048 bits. La clave DSA generada al menos ha de ser de 1024 bits.
10. SSH, SNMPv3, IPsec y SSL no soportan DES, 3DES, RC4 o MD5.

11. Sólo admite usuarios con passwords de al menos 10 caracteres y debe contener mayúsculas, minúsculas, dígitos y caracteres especiales.

293. Puede utilizarse como un método rápido de securizar un dispositivo, pero hay que tener en cuenta que es un método estricto y que puede dejar el equipo inaccesible. Además no se asegura que se esté cumpliendo la normativa correspondiente que aplique en cada caso en concreto. Es decir, su utilización no garantiza ningún cumplimiento, es necesario realizar un proceso de verificación siempre.

294. El procedimiento de configuración de FIPS es el siguiente:

1. Crear un usuario:
    i. Password cumpliendo los requisitos:
        1. Al menos 10 caracteres.
        2. Debe contener mayúsculas, minúsculas, dígitos y caracteres especiales.
    ii. Habilitar acceso al terminal.
    iii. Autorizar al usuario con nivel 3 de administración.
2. Habilitar FIPS.
3. Grabar la configuración.
4. Resetear el equipo.

295. La secuencia de comandos sería:

[Sysname] password-control enable [Sysname] local-user test [Sysname-luser-test] service-type terminal [Sysname-luser-test] authorization-attribute level 3 [Sysname-luser-test] password Password:*********** Confirm :*********** Updating user(s) information, please wait..... [Sysname-luser-test] quit	Creamos el usuario test
[Sysname] fips mode enable FIPS mode change requires a device reboot. Continue?[Y/N]:y Change the configuration to meet FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter FIPS mode.	Habilitamos FIPS
[Sysname] save The current configuration will be written to the device. Are you sure? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg] (To leave the existing filename unchanged, press the enter key): flash:/startup.cfg exists, overwrite? [Y/N]:y Validating file. Please wait..... Saved the current configuration to mainboard device successfully. Configuration is saved to device successfully. [Sysname] quit	Grabamos la configuración
<Sysname> reboot ... Tras el RESET ...	Reseteamos el equipo
User interface aux0 is available. Please press ENTER. Login authentication Username:test Password: Info: First logged in. For security reasons you will need to change your	Credenciales del usuario test

password. Please enter your new password. Password:********** Confirm :********** Updating user(s) information, please wait..... <Sysname> <Sysname> display fips status FIPS mode is enabled	Es obligado a cambiar la password Las restricciones se han aplicado y puede observarse las restricciones al internar configurar servicios.

14. EJEMPLO DE ESCENARIO BÁSICO

296. A continuación, se muestra la configuración de seguridad recomendada en un escenario sencillo, con tres equipos, cada uno conectado en un puerto diferente del switch. Se diseñará de manera que los tres equipos pertenezcan a una vlan 999, pero que los equipos .204 y .205 no puedan comunicarse entre ellos, pero sí con .200. Este último puede comunicarse con cualquiera.

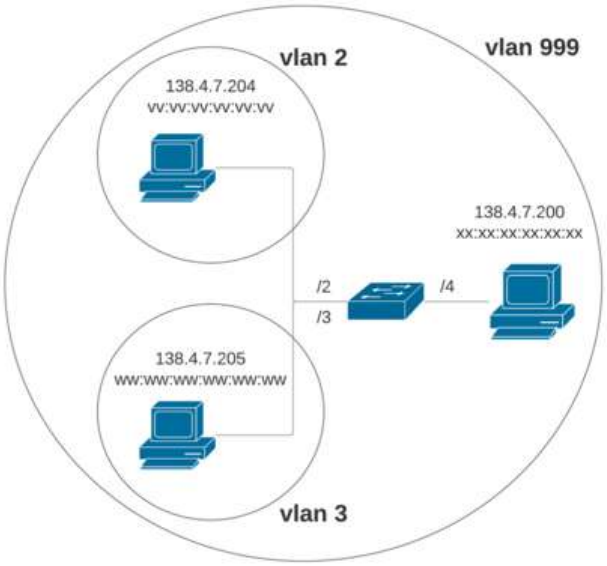

Figura 7. Esquema del escenario básico

297. Se empieza definiendo la política de contraseñas:

```
[HP]password-control enable
Info: Password control is enabled.
[HP]password-control length 12
[HP]password-control login-attempt 2 exceed lock
[HP]password-control complexity user-name check
Info: Check of password include username is enabled for all users.
```

298. A continuación, se crea un usuario local, con permisos de nivel 3 y acceso por SSH:

```
[HP]local-user admin
New local user added.
```

```
[HP-luser-admin]password simple asdfqwer1234
Updating user(s) information, please wait...
[HP-luser-admin]authorization-attribute level 3
[HP-luser-admin]service-type ssh terminal
[HP-luser-admin]state active
```

299.Se configura una contraseña para el acceso por consola:

```
[HP]user-interface aux 0
[HP-ui-aux0]authentication-mode password
[HP-ui-aux0]set authentication password cipher passwordconsola
[HP-ui-aux0]user privilege level 3
```

300.Se deshabilita el acceso remoto a través de HTTP, HTTPS y TELNET:

```
[HP]undo ip http enable
Info: HTTP server has been stopped!
[HP]undo ip https enable
Info: HTTPS server has been stopped!
[HP]undo telnet server enable
```

301.Se crea una clave RSA para la autenticación a través de SSH, y se habilita el servidor:

```
[HP]public-key local create rsa
Warning: The local key pair already exist.
Confirm to replace them? [Y/N]:Y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++
++++++++++++++++++++++++++++++++
++++++++++++
+++++++
[HP]ssh server enable
Info: Enable SSH server.
```

302.Se crean una serie de reglas ACL para permitir el acceso únicamente a los equipos de la red:

```
[HP]acl number 2000 name ACL-GESTION
[HP-acl-basic-2000-ACL-GESTION]rule 0 permit source 138.4.7.0 0.0.0.255
[HP-acl-basic-2000-ACL-GESTION]rule 10 deny
[HP-acl-basic-2000-ACL-GESTION]quit
[HP]user-interface vty 0 15
[HP-ui-vty0-15]acl 2000 inbound
```

303.Se habilita SNMP v3 y se configura un grupo privado mediante ACLs y claves de autenticación:

```
[HP]snmp-agent sys-info version v3
[HP]acl number 2001
[HP-acl-basic-2001]rule 1 permit source 138.4.7.0 0.0.0.255
[HP-acl-basic-2001]quit
[HP]acl number 2002
[HP-acl-basic-2002]quit
[HP]snmp-agent group v3 PRIVGROUP privacy acl 2001
[HP]snmp-agent calculate-password authpassword mode sha local-engineid
The secret key is: 1DD42B1E1B2D87D3CF2328B388058DCC554E6528
[HP]snmp-agent calculate-password privpassword mode sha local-engineid
The secret key is: 9D02C5CA9D06985DD58346A73E7FFFBBF97A81DA
[HP]snmp-agent usm-user v3 usuariosnmp PRIVGROUP authentication-mode sha
1DD42B1E1B2D87D3CF2328B388058DCC554E6528 privacy-mode aes128
9D02C5CA9D06985DD58346A73E7FFFBBF97A81DA
```

304.Se configura la autenticación para el servicio NTP:

```
[HP]ntp-service authentication enable
[HP]ntp-service authentication-keyid 2 authentication-mode md5
NTPpassword
[HP]ntp-service reliable authentication-keyid 2
```

305.Para protegerse contra tormentas de *broadcast*, se habilita el control de *broadcast* en los puertos activos:

```
[HP]interface gigabitethernet 1/0/2
[HP-GigabitEthernet1/0/2]broadcast-suppression 20
[HP-GigabitEthernet1/0/2]quit
[HP]interface gigabitethernet 1/0/3
[HP-GigabitEthernet1/0/3]broadcast-suppression 20
[HP-GigabitEthernet1/0/3]quit
[HP]interface gigabitethernet 1/0/4
[HP-GigabitEthernet1/0/4]broadcast-suppression 20
```

306.Se configuran las VLANs privadas:

```
[HP]vlan 999
[HP-vlan999]isolate-user-vlan enable
[HP-vlan999]quit
[HP]vlan 2 to 3
Please wait... Done.
[HP]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]port isolate-user-vlan host
[HP-GigabitEthernet1/0/2]port access vlan 2
```

```
[HP-GigabitEthernet1/0/2]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]port isolate-user-vlan host
[HP-GigabitEthernet1/0/3]port access vlan 3
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]port isolate-user-vlan 999 promiscuous
[HP-GigabitEthernet1/0/4]quit
[HP]isolate-user-vlan 999 secondary 2 to 3
```

307. A continuación, se habilitan las funcionalidades de seguridad para SPT:

```
[HP]stp bpdu-protection
[HP]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]stp edged-port enable
Warning: Edge port should only be connected to terminal. It will cause
temporary loops if port GigabitEthernet1/0/3 is connected to bridges.
Please use it carefully!
[HP-GigabitEthernet1/0/4]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]stp root-protection
[HP-GigabitEthernet1/0/3]stp edged-port enable
Warning: Edge port should only be connected to terminal. It will cause
temporary loops if port GigabitEthernet1/0/3 is connected to bridges.
Please use it carefully!
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]stp root-protection
[HP-GigabitEthernet1/0/2]stp edged-port enable
Warning: Edge port should only be connected to terminal. It will cause
temporary loops if port GigabitEthernet1/0/3 is connected to bridges.
Please use it carefully!
```

308. Se deshabilita LLDP:

```
[HP]undo lldp enable
```

309. Se registran las IP y MAC de cada una de las máquinas de la red:

```
[HP]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]ip source binding ip-address 138.4.7.204 mac-
address vvvv-vvvv-vvvv
[HP-GigabitEthernet1/0/2]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]ip source binding ip-address 138.4.7.205 mac-
address wwww-wwww-wwww
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]ip source binding ip-address 138.4.7.200 mac-
address xxxx-xxxx-xxxx
```

310. Para configurar la funcionalidad ARP Detection se debe comprobar primero la validez de los usuarios si no se ha configurado DHCP snooping:

```
[HP]arp detection 20 permit ip 138.4.7.200 mac xxxx-xxxx-xxxx vlan 999
[HP]arp detection 21 permit ip 138.4.7.204 mac vvvv-vvvv-vvvv vlan 999
[HP]arp detection 22 permit ip 138.4.7.205 mac wwww-wwww-wwww vlan 999
```

311. Se habilita ARP Detection en la VLAN 999.

```
[HP]vlan 999
[HP-vlan999]arp detection enable
```

312. Se habilita a nivel global la protección contra *IP Flood Attacks* con *ARP source suppression* y *ARP black hole routing*. Se deja el valor por defecto del umbral:

```
[HP]arp source-suppression enable
[HP]arp resolving-route enable
```

313. Se limita la tasa de paquetes ARP en cada puerto para evitar la sobrecarga del sistema:

```
[HP]snmp-agent trap enable arp rate-limit
[HP]arp rate-limit information interval 3
[HP]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]arp rate-limit rate 10 drop
[HP-GigabitEthernet1/0/2]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]arp rate-limit rate 10 drop
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]arp rate-limit rate 10 drop
```

314. Se configura la detección de ataques ARP basados en dirección MAC origen:

```
[HP]arp anti-attack source-mac filter
[HP]arp anti-attack source-mac threshold 10
[HP]arp anti-attack source-mac aging-time 200
```

315. Se desactivan ciertas características relacionadas con ICMP para aumentar la protección del equipo:

```
[HP]undo ip unreachables
[HP]undo ip redirects
[HP]undo ip ttl-expires
```

316. Se activa NetStream para detectar las interfaces por las que llegan los mensajes de cada IP:

```
[HP]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]ip netstream inbound
[HP-GigabitEthernet1/0/2]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]ip netstream inbound
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]ip netstream inbound
[HP-GigabitEthernet1/0/4]quit
```

317. Se activa Port-Security y se configura para que únicamente haya una máquina por cada interfaz. De este modo, se evita el funcionamiento de máquinas virtuales en la red:

```
[HP]port-security enable
Please wait.............................. Done.
[HP]interface GigabitEthernet 1/0/2
[HP-GigabitEthernet1/0/2]port-security max-mac-count 1
[HP-GigabitEthernet1/0/2]port-security port-mode autolearn
[HP-GigabitEthernet1/0/2]interface GigabitEthernet 1/0/3
[HP-GigabitEthernet1/0/3]port-security max-mac-count 1
[HP-GigabitEthernet1/0/3]port-security port-mode autolearn
[HP-GigabitEthernet1/0/3]interface GigabitEthernet 1/0/4
[HP-GigabitEthernet1/0/4]port-security max-mac-count 1
[HP-GigabitEthernet1/0/4]port-security port-mode autolearn
[HP-GigabitEthernet1/0/4]quit
```

15. ACRÓNIMOS

Acrónimo	Significado
AAA	Authentication, Authoritation and Accounting
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Units
CA	Certification Authority
CLI	Command Line Interface
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standards
GTSM	Generalized TTL Security Mechanism
HABP	Hardware Authentication Bypass Protocol
https	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IPSEC	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
Kbps	Kilobytes per second
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MD5	Message-Digest Algorithm 5
NAC	Network Access Control
NTP	Network Time Protocol
OSPF	Open Shortest Path First
TELNET	Telecommunication Network
PKI	Public Key Infrastructure
pps	Packets per second
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
RIP	Routing Information Protocol
RSA	Rivest, Shamir, Adleman
SCP	Secury CoPy
SDN	Software Defined Networking
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Sistema Operativo
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TFTP	Trivial File Tranfer Protocol
TTL	Time To Live
URPF	Unicast Reverse Path Forwarding
VLAN	Virtual Local Area Network
VTY	Virtual Type terminal

16. TABLA DE COMPROBACIÓN DE CUMPLIMIENTO

318. A continuación, se muestra una plantilla de comprobación de las funcionalidades necesarias

Concepto	Estado	Comentario
Software actualizado	SI ❒ NO ❒ N/A ❒	
Usuarios personales	SI ❒ NO ❒ N/A ❒	
Gestión de passwords	SI ❒ NO ❒ N/A ❒	
TELNET desactivado	SI ❒ NO ❒ N/A ❒	
SSH activado	SI ❒ NO ❒ N/A ❒	
HTTP (HTTPS) desactivado	SI ❒ NO ❒ N/A ❒	
NTP configurado con autenticación	SI ❒ NO ❒ N/A ❒	
Acceso SNMPv3 configurado	SI ❒ NO ❒ N/A ❒	
Acceso SNMPv1 SNMPv2 desactivado	SI ❒ NO ❒ N/A ❒	
Protección contra tormentas de broadcast	SI ❒ NO ❒ N/A ❒	
VLAN configuradas correctamente	SI ❒ NO ❒ N/A ❒	
Seguridad STP activada	SI ❒ NO ❒ N/A ❒	
Servicio LLDP desactivado	SI ❒ NO ❒ N/A ❒	
Enrutamiento estático	SI ❒ NO ❒ N/A ❒	
Enrutamiento dinámico	SI ❒ NO ❒ N/A ❒	
Limitación del tráfico de gestión	SI ❒ NO ❒ N/A ❒	
Detección de ARP spoofing activada	SI ❒ NO ❒ N/A ❒	
Protección contra IP Flood activada	SI ❒ NO ❒ N/A ❒	
Protecciones ICMP activadas	SI ❒ NO ❒ N/A ❒	
Servicio NetStream activado	SI ❒ NO ❒ N/A ❒	
Listas de acceso configuradas	SI ❒ NO ❒ N/A ❒	
Control de tráfico	SI ❒ NO ❒ N/A ❒	
Limitación de mac aprendidas	SI ❒ NO ❒ N/A ❒	
Puertos aislados	SI ❒ NO ❒ N/A ❒	
Port-secutity	SI ❒ NO ❒ N/A ❒	
AAA Radius/HW TACACS	SI ❒ NO ❒ N/A ❒	
802.1X	SI ❒ NO ❒ N/A ❒	
Autenticación por MAC	SI ❒ NO ❒ N/A ❒	
Autenticación mediante portal web	SI ❒ NO ❒ N/A ❒	
PKI	SI ❒ NO ❒ N/A ❒	
FIPS	SI ❒ NO ❒ N/A ❒	

17. REFERENCIAS

319. Para hacer este documento se han consultado dos guías principales de referencia:

1. “HP 5500 EI & 5500 SI Switch Series. Security Configuration Guide”
2. “HP Networking guide to hardening Comware-based devices”