centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1410

Procedimiento de Empleo Seguro
OMNISWITCH AOS

Octubre 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:05:33 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-020-5.
Fecha de Edición: octubre de 2023

Alcatel-Lucent ha participado en la realización y modificación del presente documento.

ÍNDICE

1. INTRODUCCIÓN

1. La familia **OmniSwitch de Alcatel-Lucent Enterprise** se compone de conmutadores de capa 2 y capa 3 diseñados para ofrecer baja latencia, alto rendimiento, disponibilidad y robustez.
2. Los conmutadores de la familia OmniSwitch ejecutan el sistema operativo AOS (*Alcatel-Lucent Operating System*), común para todos los equipos de la familia y que utilizan un mismo juego de comandos de línea para su configuración.
3. Los conmutadores disponen herramientas y aplicaciones de seguridad estándar integrada y automatiza para rechazar activamente las amenazas, tanto internas como externas.
4. En el presente documento se describen las recomendaciones para la configuración de los equipos de la forma más segura posible, activando o desactivando diferentes servicios o protocolos de los conmutadores.
5. 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 *OmniSwitch* de Alcatel-Lucent Enterprise, la mayoría de las recomendaciones descritas sobre seguridad son aplicables a otros equipos de red.

2. OBJETO Y ALCANCE

6. En la presente guía se recoge el procedimiento de empleo seguro para equipos OmniSwitch de **Alcatel-Lucent Enterprise**. A lo largo de los diferentes apartados, 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.
7. Los ejemplos y comandos de configuración incluidos en este documento se corresponden con la versión 8.x de AOS (*ALE Operating System*).
8. Para un mayor detalle acerca de las funcionalidades descritas se recomienda la lectura de las guías de uso y configuración de OmniSwitch:
    - OmniSwitch AOS Release 8 Switch Management Guide
    - OmniSwitch AOS Release 8 CLI Reference Guide
    - OmniSwitch AOS Release 8 Network Configuration Guide
    - OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
9. Los algoritmos criptológicos utilizados en esta guía cumplen con los requisitos estipulados en la *CCN-STIC-807 Criptología de empleo en el ENS* para la Categoría Alta.
10. **Los equipos OmniSwitch han sido cualificados e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional.** Se debe consultar dicho catálogo con el objetivo de saber qué modelos y versiones están cualificados en cada momento.

3. ORGANIZACIÓN DEL DOCUMENTO

11. El presente documento se divide en tres partes fundamentales, de acuerdo a distintas fases que componen el ciclo de vida del producto:

    a) Apartado **4**. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación** física del producto.

    b) Apartado **5**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

    c) Apartado **6**. En este apartado se recogen requisitos o recomendaciones relativas a las tareas de mantenimiento durante la fase de **operación y mantenimiento** del producto.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente:

    a) Etiqueta de envío. Deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del usuario, su dirección y el dispositivo.

    b) Embalaje externo. Deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

    c) Embalaje interno. Deberá inspeccionarse la bolsa de plástico y el sistema de sellado. La bolsa no deberá presentar cortes ni haber sido extraída. El sistema de sellado deberá estar intacto.

13. En caso de identificarse algún problema durante la inspección, el usuario deberá ponerse en contacto inmediatamente con el distribuidor autorizado o integrador, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

4.2 INSTALACIÓN SEGURA

14. Los dispositivos deberán instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

15. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control que asegure que únicamente dichas personas pueden acceder al dispositivo (incluido fuera del horario laboral).

5. FASE DE CONFIGURACIÓN

5.1 ADMINISTRACIÓN DEL PRODUCTO

16. El equipo se configurará de acuerdo con los principios de mínima funcionalidad y mínimo privilegio, es decir, se tratará de que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios en general no disponga de más privilegios que los que necesita.
17. Las actualizaciones de firmware del dispositivo, así como la configuración de funciones de seguridad importantes del sistema operativo, solo podrán ser realizadas por un número reducido de administradores/administradores de seguridad.
18. La administración del dispositivo podrá realizarse de manera local o remota, aunque la primera opción siempre será preferible a la segunda, especialmente en el caso en que el dispositivo esté integrado en un SPP (Sistema de Protección de Perímetro):
    a) Administración local: Podrá realizarse mediante un terminal utilizando comandos de línea CLI a través del puerto de consola del que disponen todos los equipos (RJ-45 o USB en algunos casos).
    b) Administración remota: En caso de que se opte por la administración remota, ésta deberá realizarse siempre desde la LAN a la que pertenece el dispositivo. Podrá realizarse a través de cualquier puerto *ethernet* del *switch* o a través de puertos de gestión fuera de banda en los modelos que disponen de ellos. Por defecto la gestión remota está desactivada y hay que habilitarla inicialmente mediante gestión local. Se recomienda el uso de SSHv2. Únicamente se habilita SSH de forma automática en el caso en que se despliega el *switch* de forma automática como cliente DHCP.
19. Para la administración del dispositivo deberá utilizarse una interfaz dedicada de solo gestión. Esta interfaz solamente podrá aceptar o responder tráfico cuyo destino sea el propio dispositivo. Los dispositivos que disponen de puertos fuera de banda son los de las familias OS6860E, OS6860N, OS6900 y OS9900.

5.2 CONTROL DE ACCESO, AUTENTICACIÓN Y NO-REPUDIO

20. Aunque es necesario desplegar los medios necesarios para que los administradores de la red puedan acceder a los equipos que la componen, también es necesario prevenir que usuarios no autorizados puedan acceder a los equipos y visualizar la información de configuración almacenada en ellos.
21. Para ello, hay que llevar a cabo una serie de medidas de seguridad para evitar accesos no deseados, tanto de aquellos usuarios que quieren acceder a los equipos desde fuera de nuestra red, como los que tratan de hacerlo por medio de

un puerto serie, o que se conectan usando un terminal o una estación de trabajo desde dentro de la red.

22. El control de acceso se ocupa de proporcionar acceso autorizado a los recursos de la red. La autenticación se refiere a confirmar la identidad de las partes que se comunican.

23. El no-repudio se refiere al mantenimiento de una vía para la auditoría, de modo que no se pueda negar el origen de los datos o la causa de un evento o acción.

5.2.1 AUTENTICACIÓN Y AUTORIZACIÓN

24. La creación de cuentas de usuario es fundamental. Cada administrador del equipo le debe ser asignado un par usuario-contraseña único para poder identificar inequívocamente a los usuarios que han accedido al equipo.

25. Se pueden utilizar mecanismos de autenticación que soporten los protocolos RADIOS o TACACS+.

5.2.1.1 UTILIZACIÓN DE UN SERVIDOR RADIUS

26. RADIUS es un protocolo estandarizado que define un sistema distribuido con topología cliente/servidor que protege a las redes de accesos no autorizados (RFC 2865 y RFC 2866.). El cliente de RADIUS es ejecutado en los *switches* o *routers* que envían peticiones de autenticación a un servidor central, el cual contiene toda la información de usuario (*Authentication, Authoritation* y *Accounting* de ese usuario).

27. Diferentes normas, como la T1.276-2003, recomiendan usar un servidor RADIUS remoto para el control de las cuentas de usuario. Esto permite un mejor control de las cuentas de usuario en la red y un menor riesgo de que haya cuentas que inadvertidamente queden sin cumplir los requisitos establecidos. La única cuenta local debe ser la de administrador, que se utilizará solo para la reconfiguración de emergencia.

28. Cuando un usuario quiere autenticarse en un sistema protegido por RADIUS se suceden los siguientes pasos:

    a) Se le pide al usuario que introduzca su *login* y *password*

    b) El *login* y el *password* cifrado son enviados al servidor de RADIUS.

    c) El usuario recibe uno de los siguientes mensajes del servidor:

    - **ACCEPT**: El usuario ha sido autenticado.
    - **REJECT**: El usuario no ha podido ser autenticado y, o bien se le solicita que introduzca sus datos de nuevo o se le niega el acceso.
    - **CHALLENGE**: Se le solicita más información al usuario.
    - **CHALLENGE PASSWORD**: Se le pide al usuario que introduzca un nuevo *password*.

29. Los *switches* disponen de un cliente RADIUS incorporado. Se requiere un servidor RADIUS que admita atributos específicos del proveedor (VSA). Los atributos de Alcatel-Lucent pueden incluir información de VLAN, hora del día o restricciones de slot/puerto.

30. Para poder configurar el *switch* como cliente RADIUS se usa el comando ***aaa radius-server.*** Este comando permite configurar los parámetros del servidor RADIUS en el *switch*. Al dar de alta un nuevo servidor RADIUS, se requiere, al menos, el nombre del *host* o una dirección IP (especificada mediante la palabra clave *host*) y la clave compartida (especificada mediante la palabra clave *key*).

31. En este ejemplo, el nombre del servidor es '*rad*', la dirección del *host* es 10.10.2.1, la dirección del servidor secundario es 10.10.3.5 y la clave es '*switch*'. La clave secreta compartida debe configurarse exactamente igual que en el servidor:

    -> aaa radius-server rad host 10.10.2.1 10.10.3.5 key switch

32. Se usa el comando **aaa authentication** para especificar la interfaz de gestión a través de la cual se permite el acceso al *switch* (consola, http o ssh). Se debe especificar los servidores principal y de *backup* que se utilizarán para verificar el inicio de sesión del usuario y la información de sus privilegios. Se pueden especificar varios servidores de diferentes tipos. Por ejemplo:

    -> aaa authentication console rad

    -> aaa authentication ssh rad

    -> aaa authentication snmp rad

    -> aaa authentication http rad

33. Se recomienda la siguiente configuración segura:

    aaa radius-server radius_server host ip_address

    aaa authentication default radius_server local

34. Los privilegios de gestión de un usuario autenticado por RADIUS se pueden controlar mediante los siguientes atributos específicos del vendedor (VSA):

    Alcatel-Acce-Priv-F-R1

    Alcatel-Acce-Priv-F-R2

    Alcatel-Acce-Priv-F-W1

    Alcatel-Acce-Priv-F-W2

35. Estos atributos se deben cargar en el servidor RADIUS que se use para la autenticación de usuarios de gestión. El servidor RADIUS devuelve la información de los privilegios de lectura y escritura del usuario sobre las diferentes funcionalidades del *switch*. El valor devuelto por estos VSA ha de ser definido en 32 bits con formato hexadecimal.

36. Los VSA Alcatel-Acce-Priv-F-R1 y Alcatel-Acce-Priv-F-R2 definen los permisos de lectura de los usuarios.

37. Los VSA Alcatel-Acce-Priv-F-W1 y Alcatel-Acce-Priv-F-W2 definen los permisos de escritura de los usuarios.

38. El comando ***show aaa priv hexa*** muestra en hexadecimal los valores para cada uno de los dominios o familias de comandos de gestión del switch:

-> show aaa priv hexa

```
file           = 0x00000001 0x00000000,
telnet         = 0x00000008 0x00000000,
dshell         = 0x00000020 0x00000000,
debug          = 0x00000040 0x00000000,
domain-admin   = 0x00000069 0x00000000,
system         = 0x00000080 0x00000000,
aip            = 0x00000100 0x00000000,
snmp           = 0x00000200 0x00000000,
rmon           = 0x00000400 0x00000000,
webmgt         = 0x00000800 0x00000000,
config         = 0x00001000 0x00000000,
domain-system  = 0x00001F80 0x00000000,
chassis        = 0x00002000 0x00000000,
module         = 0x00004000 0x00000000,
interface      = 0x00008000 0x00000000,
pmm            = 0x00010000 0x00000000,
health         = 0x00040000 0x00000000,
domain-physical = 0x0005E000 0x00000000,
ip             = 0x00080000 0x00000000,
rip            = 0x00100000 0x00000000,
ospf           = 0x00200000 0x00000000,
bgp            = 0x00400000 0x00000000,
vrrp           = 0x00800000 0x00000000,
ip-routing     = 0x01000000 0x00000000,
ipx            = 0x02000000 0x00000000,
ipmr           = 0x04000000 0x00000000,
ipms           = 0x08000000 0x00000000,
domain-network = 0x0FF80000 0x00000000,
vlan           = 0x10000000 0x00000000,
bridge         = 0x20000000 0x00000000,
stp            = 0x40000000 0x00000000,
802.1q         = 0x80000000 0x00000000,
linkagg        = 0x00000000 0x00000001,
ip-helper      = 0x00000000 0x00000002,
```

```
domain-layer2  = 0xF0000000 0x00000003,
dns            = 0x00000000 0x00000010,
domain-service = 0x00000000 0x00000010,
qos            = 0x00000000 0x00000020,
policy         = 0x00000000 0x00000040,
slb            = 0x00000000 0x00000080,
domain-policy  = 0x00000000 0x000000E0,
session        = 0x00000000 0x00000100,
avlan          = 0x00000000 0x00000400,
aaa            = 0x00000000 0x00000800,
domain-security= 0x00000000 0x00000D00
```

5.2.1.2 UTILIZACIÓN DE TACACS+

39. *Terminal Access Controller Access Control System* (TACACS +) es un protocolo estándar de autenticación y auditoría en la RFC 1321 que emplea TCP para transporte. Los *switches* disponen de un cliente TACACS + incorporado. Un servidor TACACS + permite el control de acceso a *routers*, servidores de acceso y otros dispositivos de red a través de uno o más servidores centralizados. El protocolo también permite servicios de autenticación, autorización y auditoría por separado.

40. Se utilizará el comando **aaa tacacs+-server** para configurar los parámetros TACACS+ en el *switch*.

41. Al crear un nuevo servidor, se requiere al menos un nombre de *host* o dirección IP (especificada por la palabra clave *host*), así como una clave secreta compartida (especificada por la palabra clave '*key*'). En este ejemplo, el nombre del servidor es tac1, la dirección IP del host es 10.10.5.2, la dirección de respaldo es 10.10.5.5 y la clave compartida es '*switch*'. La clave secreta compartida debe configurarse exactamente igual en el servidor.

    -> aaa tacacs+-server tac1 host 10.10.5.2 10.10.5.5 key switch

42. Existe la opción *prompt-key*, que se puede usar para introducir la clave secreta en un formato oculto en lugar de texto claro. Cuando se selecciona esta opción, se debe presionar la tecla Intro. Aparece una solicitud de contraseña que solicita que se introduzca la clave secreta. La clave secreta ha de escribirse dos veces y se acepta el comando solo si ambas entradas coinciden. La clave proporcionada en este modo no se muestra en la CLI como texto. Por ejemplo:

    -> aaa tacacs+-server tac1 prompt-key host 10.10.2.2

    Enter Key: ****

    Confirm Key: ****

43. Se utilizará el comando de **aaa authentication** para especificar la interfaz de gestión a través de la cual se permite el acceso al *switch* (como consola, http o

SSH). Se especificarán los servidores principal y de respaldo que se utilizarán para verificar el inicio de sesión del usuario y la información de privilegios. Estos servidores podrán ser de diferentes tipos. Por ejemplo:

-> aaa authentication console tac1

-> aaa authentication ssh tac1

-> aaa authentication snmp tac1

-> aaa authentication http tac1

5.2.1.2.1 Limitaciones del cliente TACACS+

44. Las limitaciones son:

- TACACS+ soporta únicamente el acceso autenticado al *switch* y no se puede utilizar para la autenticación de usuarios.
- La autenticación y la autorización se combinan juntas y no se pueden realizar de forma independiente.
- No se soporta la autorización de comandos sobre la marcha. La autorización es similar a las familias de gestión de particiones AOS.
- Solo se admiten inicios de sesión ASCII entrantes.
- Se soportan hasta un máximo de 50 sesiones simultáneas de TACACS+ cuando no se activa ningún otro mecanismo de autenticación.
- La auditoría de los comandos introducidos por el usuario en el proceso de TACACS+ remoto no se soporta en el archivo boot.cfg en el momento del arranque del *switch*.

5.2.1.3 CONFIGURACIÓN DE CONTRASEÑAS

45. A la hora de seleccionar contraseñas para las cuentas, deberán seguirse las siguientes directrices y opciones de configuración:

a) Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.

b) Deberán ser privadas y no compartirse con nadie.

c) Deberán ser de 12 caracteres como mínimo.

Descripción	Comando	Valor recomendado
Longitud mínima de contraseña	***user password-size min***	12 caracteres

Tabla 1. Longitud de contraseña de administrador.

La longitud por defecto de las contraseñas es de 8 caracteres, lo que se considera insuficiente para un usuario administrador.

-> ***user password-size min 12***

d) Deberán incluir caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", al menos 3 juegos de estos caracteres: letras en mayúscula, letras en minúscula, números , y caracteres especiales.

Descripción	Comando	Valor recomendado
Número mínimo de mayúsculas en la contraseña	***user password-policy min-uppercase***	1
Número mínimo de minúsculas en la contraseña	***user password-policy min-lowercase***	1
Número mínimo de dígitos decimales en la contraseña	***user password-policy min-digit***	1
Número mínimo de caracteres especiales en la contraseña	***user password-policy min-nonalpha***	1

Tabla 2. Contenidos mínimos de la contraseña de administrador.

La configuración por defecto para dichos parámetros de configuración es "0". Es decir, no se cumpliría ninguno de los requisitos mínimos definidos en este punto. Para poder cumplir, sería necesario utilizar al menos 3 de los siguientes comandos.

-> user password-policy min-uppercase 1

-> user password-policy min-lowercase 1

-> user password-policy min-digit 1

-> user password-policy min-nonalpha 1

e) El algoritmo de autenticación para las contraseñas de texto sin formato se debe configurar como SHA-256. Para ello, al crear un usuario se especificará el tipo de cifrado usado para almacenar la contraseña en el *switch*:

-> user alcatel password <password> read-write all sha256

f) Se debe establecer el periodo de caducidad de la contraseña, y obligar a los usuarios a cambiarla tras el número de días especificado.

Descripción	Comando	Valor recomendado
Tiempo de caducidad de la contraseña para todos los usuarios	***user password-expiration***	180

Tabla 3. Caducidad de las contraseñas de administrador

El valor por defecto de este parámetro es de "0", lo que significa que no se aplicaría control sobre la frecuencia mínima en la que se cambian las contraseñas.

Una vez que una contraseña caduca, se pedirá al usuario que cambie la contraseña en el siguiente inicio de sesión. El siguiente ejemplo establece el cambio de contraseña en 180 días

-> user password-expiration 180

g) Las contraseñas no deberán cambiarse con demasiada frecuencia. Para ello, se debe configurar el periodo mínimo durante el cual el administrador no puede cambiar la contraseña.

Descripción	Comando	Valor recomendado
Periodo mínimo en el que un usuario no puede volver a cambiar la contraseña	***user password-min-age***	4

Tabla 4. Frecuencia de cambio de la contraseña de administrador

Este comando es utilizado para evitar que un usuario cambie la contraseña en un breve periodo de tiempo para volver a su contraseña original.

El valor por defecto de este parámetro es de "0", lo que significa que no se aplicaría control sobre la frecuencia mínima en la que se cambian las contraseñas. El siguiente ejemplo establece que el usuario no puede cambia la contraseña en los siguientes 4 días tras un cambio:

-> user password-min-age 4

h) No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas. Para ello, se debe configurar el número mínimo de contraseñas a retener en el historial y que no se pueden repetir a la hora de cambiar la contraseña.

Descripción	Comando	Valor recomendado
Mínimo número de contraseñas a retener en el historial	***user password-history***	10

Tabla 5. Configuración del historial de contraseñas de administrador

-> user password-history 5

Este ejemplo establece que el usuario no puede cambiar la contraseña a otra que sea igual a las cinco últimas. El valor por defecto de esta configuración es de "4".

46. Son contraseñas poco seguras palabras comúnmente utilizadas o cadenas de caracteres consecutivos (Ej.: "1234"). A continuación, se establecen una serie de contraseñas prohibidas:

    a) Palabras de diccionario.

    b) Caracteres repetitivos o secuenciales (Ej.: "aaaaaaa" o "1234abcd").

    c) Patrones de teclado (Ej.: 'zaq12wsx' or 'qwertyuiop').

    d) Nombres propios específicos de contexto, nombres de usuario, nombre del host del sistema, etc.

47. Las contraseñas nunca deben almacenarse en claro. Alcatel-Lucent AOS guarda los hashes de las contraseñas de usuario, mediante SHA.

48. Las cuentas creadas y no utilizadas deben eliminarse o inhabilitarse.

5.2.1.4 CONFIGURACIÓN DE UN ADMINISTRADOR AUTORIZADO

49. Las cuentas raíz se encuentran siempre pre-configuradas de fábrica. Su uso debe restringirse a la instalación y configuración inicial del dispositivo. Nunca deberán utilizarse en la operación normal del equipo.

50. El administrador autorizado deberá tener todos los permisos, incluido el de cambiar la configuración del dispositivo.

51. Para configurar un administrador autorizado se deberá:

    a) Crear un usuario con un nombre y contraseña inicial mediante el comando ***user***. El ejemplo siguiente crea un usuario *administrador1* con contraseña inicial C*ontraseña1*:

    -> user administrador1 password Contraseña1

    b) Configurar los privilegios de lectura, escritura o lectura-escritura que ese usuario tendrá sobre los diferentes dominios o familias de comandos del conmutador y por lo tanto sobre las funcionalidades del mismo. En el siguiente ejemplo se configura el usuario creado anteriormente con permisos de lectura-escritura para las funcionalidades de nivel 2, de la capa física y de calidad de servicio del *switch*:

    -> user administrador1 read-write domain-layer2 domain-physical qos

    c) Si no se especifica ningún permiso, los usuarios creados toman por defecto los valores del usuario por defecto. Se pueden modificar los parámetros del usuario por defecto.

d) En caso de acceso autenticado al *switch* mediante RADIUS los privilegios de gestión sobre los diferentes dominios o familias se han de pasar sobre los VSAs tal como se indica en los párrafos 34 a 38.

5.2.1.5 MODO FIPS

52. El modo FIPS se usa para asegurar que se usan únicamente algoritmos de cifrado fuertes en el acceso al *switch*.

53. *Federal Information Processing Standards* (FIPS) es un modo de operación que satisface los requisitos de seguridad de los módulos criptográficos. Según el estándar FIPS 140-2 del Instituto Nacional de Estándares y Tecnología (NIST) de EEUU, se requiere el soporte de algoritmos criptográficos fuertes para lograr el cumplimiento de FIPS. Cuando el modo FIPS está habilitado en OmniSwitch, los dispositivos OmniSwitch utilizan el cifrado compatible con FIPS 140-2 en las diversas interfaces de gestión, como SFTP, HTTP, SSH y SSL.

54. Estos algoritmos criptográficos fuertes garantizan una comunicación segura con el dispositivo para proporcionar seguridad basada en criptografía para redes IP mediante el uso de los protocolos de seguridad apropiados, algoritmos criptográficos y claves, evitando cualquier forma de secuestro, piratería o ataque en el dispositivo a través del modo seguro de comunicación.

55. A continuación, se describen las funcionalidades del modo FIPS:

    - FIPS opera en modo OpenSSL permitiendo solo algoritmos criptográficos fuertes y altamente seguros.
    - OpenSSH y *Web Server* que usan OpenSSL como la capa subyacente para comunicaciones seguras también funcionan en el modo FIPS.
    - SNMPv3 admite SHA + AES seguro. MD5 o DES no están permitidos.
    - El modo FIPS se habilita / deshabilita solo con un reinicio del *switch*.

56. El módulo SNMPv3, así como todos los protocolos de administración de los *switches* como SFTP, HTTP, SSH y SSL utilizan los algoritmos de cifrado compatibles con FIPS 140-2.

5.2.1.5.1 Configuración del Modo FIPS en AOS

57. Antes de habilitar el modo FIPS en el *switch*, se deben tener en cuenta los siguientes requisitos previos:

    - Los clientes SSH/SFTP/SSL/SNMPv3 deben soportar los algoritmos criptográficos seguros estándar de FIPS para comunicarse con un dispositivo OmniSwitch en modo FIPS.
    - Las comunicaciones SNMPv3 en el modo FIPS admiten SHA+AES. El establecimiento de sesión con MD5 o DES debe ser rechazado.

- Los certificados o claves específicos del usuario deben generarse utilizando algoritmos criptográficos compatibles con FIPS. El módulo OpenSSL no tiene controles para verificar el cumplimiento de FIPS del certificado o claves en la memoria flash.

58. El siguiente procedimiento se utiliza para configurar el modo FIPS en el conmutador:

    - Habilitar FIPS en el switch

      -> system fips admin-state enable
      WARNING: FIPS Admin State only becomes Operational after write memory and reload

    - Reiniciar el switch y confirmar.

      -> reload from working no rollback-timeout
      Confirm Activate (Y/N): y

    - Verificar el estado de FIPS

      -> show system fips
      Admin State: Enabled
      Oper State: Enabled

    - Deshabilitar cualquier protocolo inseguro en el *switch*, tales como Telnet o FTP.

      -> ip service telnet admin-state disable

      -> ip service ftp admin-state disable

59. A continuación se pueden crear usuarios con contraseñas seguras compatibles con FIPS

    -> user snmpadmin password trustsha+aes sha+aes

60. Este usuario y contraseña pueden ser usados para iniciar sesión en un *switch* en modo FIPS. Se puede verificar la configuración de este usuario mediante el siguiente comando:

    -> show user = snmpadmin

    User name = snmpadmin,

    Password expiration = 12/22/2019 11:01 (30 days from now),

    Password allow to be modified date = 10/25/2019 10:59 (3 days from now),

    Account lockout = Yes (Automatically unlocked after 19 minute(s) from now),

    Password bad attempts = 3,

    Read Only for domains = None,

    Read/Write for domains = Admin System Physical Layer2 Services policy Security,

    Read/Write for families = ip rip ospf bgp vrrp ip-routing ipx ipmr ipms ,

    Snmp allowed = YES,

    Snmp authentication = SHA,

    Snmp encryption = AES

Console-Only = Disabled

5.2.2 CONTROL DE ACCESO

5.2.2.1 ACLS CON DESTINO AL GRUPO DE RED SWITCH

61. Las listas de acceso son una herramienta fundamental, dado que nos permiten seleccionar qué direcciones IP son permitidas en cada puerto. Las ACLs se evalúan línea a línea, hasta que se encuentra una coincidencia, por lo que hay que definir primero los casos más específicos y avanzar hasta llegar a los casos más generales. Por defecto, se deniega todo el tráfico.

62. Se pueden usar grupos de políticas de red basadas en direcciones IP de origen o de destino.

63. El *switch* contiene un grupo de red predefinido llamado "*switch"* (incluye direcciones IPv4 configuradas para el *switch*) y un grupo de red predeterminado denominado *"switch6"* (incluye direcciones IPv6 configuradas para el conmutador). Ambos grupos de red también se pueden usar como condición de una política.

64. El grupo predefinido "*switch*" permite crear ACLs que únicamente permitan conexiones desde una lista predeterminada de direcciones IP.

65. En el siguiente ejemplo de configuración se define un grupo de red "*management*" con las direcciones IP de gestión conocidas y de confianza. Se define una condición de la política con el tráfico originado en el grupo "*management*" y destino al grupo predefinido "*switch*". Se crean las acciones *drop* y *accept*, una regla *trusted* que permite el tráfico desde un grupo a otro y otra *untrusted* que descarta el tráfico no permitido:

    -> policy network group management <ip_address> mask <mask> <ip_address> mask <mask> <ip_address> mask <mask> ...
    -> policy condition trusted source network group management destination network group Switch
    -> policy condition untrusted destination network group Switch
    -> policy action accept
    -> policy action drop disposition drop
    -> policy rule trusted precedence 65010 condition trusted action accept
    -> policy rule untrusted precedence 65000 condition untrusted action drop
    -> qos apply

66. En protocolos como BGP (*Border Gateway Protocol*) o BFD (*Bidirectional Forwarding Detection*) puede ser necesario incluir las direcciones IP de todos los *routers* vecinos en el grupo de red "*management*".

67. Este tipo de configuración de QoS puede consumir muchas entradas TCAM (*Ternary Content Addressable Memory*) en caso de que haya muchos rangos de red de gestión definidos y muchas direcciones IP locales activas (el número de rangos de red de administración predefinidos multiplicado por el número de

direcciones IP locales activas da el número de entradas TCAM consumidas). Se recomienda utilizar rangos de red en lugar de direcciones IP con máscara de 32 bits para reducir la cantidad de entradas de TCAM reservadas.

68. En AOS 8 hay una opción para reducir la cantidad de recursos TCAM consumidos usando "***qos switch-group compact***". A continuación se puede ver un ejemplo de configuración en OS6900, que consume 16 (4 × 4) entradas TCAM en el modo expanded y 4 (4 × 1) en el modo compact.

69. Es necesario reiniciar el *switch* para aplicar los cambios.

```
-> show configuration snapshot qos ip
! IP:
ip interface "vlan100" address 192.168.100.1 vlan 100
ip interface "vlan101" address 192.168.101.1 vlan 101
ip interface "vlan102" address 192.168.102.1 vlan 102
ip interface "vlan103" address 192.168.103.1 vlan 103

! QOS:
qos switch-group compact
policy network group management 192.168.100.1192.168.101.1
policy network group management 192.168.102.1192.168.103.1
policy condition trusted source network group management destination network
group Switch
policy action accept
qos apply
```

70. Con la configuración inicial se consumen 16 entradas, mientras que con la segunda, tras el reinicio del *switch* se usan solo 4 entradas.

5.2.3 CONFIGURACIÓN DE LOGON BANNER

71. El mensaje de inicio de sesión (*Logon Banner*) es un mensaje que se muestra a los usuarios, antes de que realicen el *login*. En el sistema no aparece por defecto ningún mensaje, por lo que deberá configurarse.

72. Este mensaje deberá advertir que solo los usuarios autorizados pueden acceder al Sistema y que toda la actividad será supervisada para verificar el cumplimiento de la política de seguridad. Además, en dicho mensaje no se facilitará información del Sistema que pueda identificarlo o caracterizarlo ante un atacante.

73. Tras el primer arranque del conmutador, el sistema crea un fichero llamado de texto *"**pre_banner.txt**"* que inicialmente está vacío.

74. El administrador puede editar dicho fichero en el propio *switch* mediante el editor de texto **vi**, o bien puede crear el fichero en un editor de texto externo y copiar el fichero con el mismo nombre en el directorio ***/flash/switch*** del conmutador.

75. El fichero *"pre_banner.txt"* no se copia a los diferentes equipos de una pila cuando se lanza el comando ***copy running certified***. El administrador debe copiar dicho fichero en todos los conmutadores de la pila de forma manual.

5.2.4 REGISTRO DE EVENTOS

76. A la hora de gestionar una red, es fundamental mantener un registro de los eventos que en ella suceden, de forma que el administrador pueda revisar esta información y saber qué es exactamente lo que ha pasado. Para ello los registros de eventos han de ser configurados de forma adecuada.

77. Un registro configurado para que recoja demasiada información puede llegar a ser demasiado complejo de leer, ocultando información de importancia bajo varias capas de datos insustanciales. A su vez, un registro demasiado sencillo puede no recoger datos de vital importancia a la hora de analizar el estado de la red.

5.2.4.1 REGISTRO DE COMANDOS

78. El *switch* permite el registro de comandos a través del comando ***command-log***.

79. Esta funcionalidad permite a los usuarios registrar los comandos más recientes introducidos vía Secure Shell y sesiones de consola. Además de la lista de comandos, se registran los resultados de cada entrada de comando. Los resultados incluyen información de si un comando se ejecutó correctamente o si se produjo un error de sintaxis o configuración.

80. Por defecto, el registro de comandos está deshabilitado. Para habilitar el registro de comandos en el switch, se introduce el siguiente comando:

```
-> command-log enable
```

81. Cuando el registro de comandos se habilita, se crea automáticamente un archivo llamado ***command.log*** en el directorio *flash* del switch. Una vez habilitado, los comandos de configuración introducidos por línea de comandos se grabarán en este archivo hasta que se desactive el registro de comandos.

82. Para ver el estado del registro de comandos:

```
-> show command-log status
 CLI command logging: Enable
```

83. Para ver una lista de comandos registrados junto con la información correspondiente (incluidos los resultados), se introduce el comando ***show command-log***. Por ejemplo:

```
-> show command-log
Command: ip interface vlan-68 address 168.14.12.120 vlan 68
    UserName: admin
    Date: MON APR 28 01:42:24
    Ip Addr: 128.251.19.240
    Result: SUCCESS
Command: ip interface vlan-68 address 172.22.2.13 vlan 68
    UserName : admin
    Date: MON APR 28 01:41:51
    Ip Addr: 128.251.19.240
    Result: ERROR: Ip Address must not belong to IP VLAN 67 subnet
Command: ip interface vlan-67 address 172.22.2.12 vlan 67
    UserName : admin
```

Date: MON APR 28 01:41:35
Ip Addr: 128.251.19.240
Result: SUCCESS
Command: command-log enable
UserName: admin
Date: MON APR 28 01:40:55
Ip Addr: 128.251.19.240
Result: SUCCESS

84. Los comandos más recientes aparecen en primer lugar. Se indica también el usuario que introdujo el comando, la fecha y hora, la dirección del sistema desde el que se hizo, y el resultado de la operación, con comentarios en caso de error.

85. Se puede hacer registro remoto de comandos mediante el comando:

-> swlog output remote command-log

5.2.4.2 RADIUS Y TACACS+

86. Los servidores de auditoría (*accounting*) rastrean los recursos de la red, como el tiempo, los paquetes, los bytes, etc., y la actividad del usuario (cuando un usuario inicia y cierra sesión, cuántos intentos de inicio de sesión se realizaron, duración de la sesión, etc.). Los servidores de auditoría pueden estar ubicados en cualquier lugar de la red y pueden ser de diferentes tipos.

87. La palabra clave ***local*** debe especificarse si desea que la auditoría se realice a través de la función "***Switch Logging***" del switch. Si se especifica ***local***, debe ser el último servidor de la lista.

88. Los servidores de auditoría externos se configuran a través de los comandos **aaa radius-server** y **aaa tacacs + -server**, tal como se indicó en el punto 5.2.1 de este documento.

89. Para habilitar la auditoría (registrar una sesión de usuario) para **el Acceso Autenticado al Switch (ASA)** se usa el comando ***aaa accounting session*** con los nombres de servidor configurados previamente. En el siguiente ejemplo, los servidores RADIUS y LDAP ya se han configurado a través de los comandos aaa radius-server y aaa ldap-server:

-> aaa accounting session rad1 ldap2 local

90. Después de introducir este comando, la auditoría se realizará a través del servidor RADIUS **rad1**. Si ese servidor no está disponible, se usará el servidor LDAP, **ldap2**. Por último, si tampoco ese servidor está disponible, el registro se realizará localmente en el switch a través de la función de "***Switch Logging"***.

91. Este comando se usa de la siguiente manera:

- Use la forma ***no*** del comando para deshabilitar la contabilidad del Acceso Autenticado al Switch. Ejemplo:

-> no aaa accounting session

- Se pueden especificar hasta 4 servidores de auditoría (total). Se requiere al menos un servidor. Cada nombre de servidor debe estar separado por un espacio.
- Los servidores pueden ser RADIUS, TACACS +, servidores LDAP y/o la funcionalidad de *Switch Logging* **local**.
- Si se especifica **local** como servidor1, el conmutador solo utilizará la función Switch Logging **local** para la auditoría.
- Si **local** se especifica como opción de respaldo, debe ponerse en último lugar en la lista de servidores incluidos en el comando. La función *Switch Logging* siempre está disponible si el *switch* está activo.
- El *switch* usa solo el primer servidor disponible en la lista para la auditoría. Por ejemplo, si el servidor1 no está disponible, el *switch* usa el servidor2.
- Los servidores RADIUS, TACACS + y LDAP pueden tener un servidor de respaldo adicional especificado a través de los comandos ***aaa radius-server, aaa tacacs+-server*** *y* ***aaa ldap-server****.*

5.2.4.3 REGISTRO CENTRALIZADO DE ACTIVIDAD

92. OmniSwitch está configurado para ayudar a monitorizar la actividad en el *switch* por medio de *traps* SNMP, registros (*logs*) locales del *switch* y registro remoto (vía *syslog*).
93. El equipo soporta la versión SNMPv3, que es la recomendada ya que proporciona mecanismos de seguridad y control de la información accedida.
94. Se recomienda la siguiente configuración segura:

    -> snmp station ip_address username v3 enable
    -> no swlog output
    -> swlog output flash **(predeterminado)**
    -> swlog output ip_address
    -> swlog appid all level info **(predeterminado)**
    -> swlog **(predeterminado)**

95. ***snmp station ip_address username v3 enable*** se usa para configurar una interfaz para enviar los *traps* a una estación SNMP. Se recomienda OmniVista 2500 NMS como estación de monitorización y registro de *traps* de los switches OmniSwitch. Los *traps* que puedan indicar la manipulación de una red deben enviarse al administrador de la red para su atención inmediata. Los *traps* que pueden requerir una acción de seguridad inmediata son:
    - ***coldStart***, ***warmStart***: detecta la manipulación física del switch.
    - ***alaStackMgrRoleChangeTrap***: detecta la modificación del switch primario o secundario de una pila. Esto también podría indicar manipulación física.

- ***httpServerDoSAttackTrap***: el servidor HTTP está bajo un posible ataque DoS.
- ***alaDoSTrap***: se ha identificado un posible ataque DoS en el switch.
- ***stpRootPortChange***: el puerto root de *Spanning Tree* ha cambiado. Un cambio de root puede indicar una posible manipulación de la configuración de Spanning Tree. Este *trap* puede ser difícil de monitorizar en redes que cambian su configuración de *Spanning Tree* a menudo.
- Dependiendo de la configuración de su red, estos *traps* pueden proporcionar información de seguridad importante.
- ***chassisTrapsPossibleDuplicateMac*** - Posible falsificación de un dispositivo.
- ***lpsViolationTrap***: se ha producido una infracción en las reglas de LPS (*Learned Port Security*).

96. ***swlog output flash*** hace que los log de salida del switch se almacenen en la memoria flash del propio switch. Así se mantiene una copia en caso de que el servidor syslog no esté accesible.
97. ***swlog output <ip_address>*** hace que los log del switch se envíen a un servidor syslog remoto. Es importante disponer de un servidor remoto para copia de seguridad, por protección contra el borrado o llenado del archivo 'swlog' en la memoria flash del switch.
98. ***swlog appid all level info*** restablece el nivel de registro a “info”. El nivel "warn" y superior siempre debe registrarse por razones de seguridad. El nivel "info" proporciona información adicional que puede ayudar en las auditorías de seguridad. Los niveles de depuración “debug” no se deben usar excepto cuando se rastrean problemas específicos, ya que pueden causar un llenado prematuro del archivo 'swlog' y sobrescritura de información de seguridad importante.
99. ***swlog*** habilita el registo “*swlog*” en los destinos de salida configurados. Nunca debe ser apagado.
100. Se recomienda que el archivo *'swlog'* se borre (***swlog clear***) cuando se configura el switch por primera vez para eliminar eventos no aplicables.
101. El comando ***swlog output flash file-size <****kilobytes****>*** permite ajustar en kilobytes el tamaño del fichero de logs del conmutador en su memoria flash.
102. El tamaño del fichero de logs en la memoria flash del conmutador no debe reducirse por debajo del valor por defecto. El valor por defecto está determinado específicamente para cada familia de productos para permitir el registro máximo.

5.2.5 SINCRONIZACIÓN HORARIA

103. Se recomienda configurar el dispositivo para el uso de servidores NTP, de forma que todos los dispositivos desplegados puedan llevar a cabo el registro de eventos de forma precisa.

104. Los pasos para llevar a cabo la configuración NTP son los siguientes:

a) Configurar el servidor NTP desde el que el conmutador recibirá la información de tiempo. Se puede hacer mediante una dirección IP o *hostname*/FQDN.

-> ntp server 198.206.181.139
-> ntp server clock3.ovcirrus.com

b) Habilitar el cliente NTP del conmutador. Por defecto el cliente NTP está deshabilitado.

-> ntp client admin-state enable

c) Para comprobar el estado del servidor NTP en el conmutador se utilizará el siguiente comando:

-> show ntp server status

5.3 CONFIDENCIALIDAD DE LOS DATOS Y SEGURIDAD DE LA COMUNICACIÓN

105. La confidencialidad de los datos hace referencia a la protección de dichos datos ante una divulgación no autorizada. La seguridad de la comunicación se encarga de garantizar que la información solo fluya entre los puntos finales autorizados sin ser desviada o interceptada.

5.3.1 PERMITIR ÚNICAMENTE LOS PROTOCOLOS SEGUROS

106. AOS proporciona protocolos no seguros por compatibilidad con equipos antiguos. Estos protocolos no deben ser utilizados. Hay protocolos seguros disponibles que proporcionan el mismo tipo de funcionalidad.

107. Todos los servicios que no se utilizan deben desactivarse para reducir aún más la exposición. Por ejemplo, si no se utiliza SNMP, deberán eliminarse los comandos para habilitar SNMP.

Protocolo desactivado	Alternativa	Razón
TELNET	SSH	Telnet no usa cifrado ni certificados.
FTP	SFTP SCP	FTP no usa cifrado ni certificados.
TFTP	SFTP SCP	TFTP no requiere autenticación de usuario ni usa cifrado.

HTTP	HTTPS	HTTP no usa cifrado ni certificados
SNMP V1	SNMP V3	SNMP v1 no requiere autenticación de usuario. V3 además proporciona cifrado.
SNMP V2	SNMP V3	SNMP v2 no proporciona cifrado.
UDP-RELAY		Desactivar salvo que se use el servicio.
NTP		Desactivar salvo que se use NTP.

108.Según lo anterior la configuración segura sugerida podría ser la siguiente:

-> ip service all admin-state disable

-> ip service ssh admin-state enable

-> ssh enforce-pubkey-auth enable

-> ip service snmp admin-state enable

-> ip service http admin-state enable

-> webview force-ssl enable

-> snmp security privacy all

109.A continuación, se describen algunas consideraciones:

- SSH requiere "***ssh enforce-pubkey-auth enable***" para trabajar con certificados de clave pública. La clave de usuario debe cargarse en el conmutador en */flash/network/pub.*
- "***snmp security privacy all***" requiere accesos SNMP para usar v3.
- ***"ip service http admin-state enable/disable***" habilita o deshabilita tanto **http** como https. Incluso si el puerto http está abierto, un usuario siempre se redirige al puerto https y no supone una amenaza para la seguridad. Es el comportamiento esperado.

110.Los servicios habilitados se pueden ver con el comando ***show ip Service***

```
-> show ip service
 Name                    Port              Status
-------------------------+-----------------+-----------------
 ftp                              21    disabled
 ssh                              22    enabled
 telnet                           23    disabled
 http                             80    enabled
 ntp                             123    enabled
 snmp                            161    enabled
 https                           443    enabled
```

5.3.2 CONFIGURACIÓN DE SNMPV3

111. La configuración de SNMPv3 requiere de configuración adicional.

112. De manera predeterminada, el switch está configurado como "***privacy all***", lo que significa que el *switch* solo acepta *Sets, Gets y Get-Nexts v3* autenticados y cifrados. Se pueden configurar diferentes niveles de seguridad SNMP mediante el comando ***snmp security***, seguido del parámetro que indica el nivel de seguridad deseado.

113. Por ejemplo, la siguiente sintaxis establece el nivel de seguridad SNMP como "***authentication all***" como se define a continuación:

    -> snmp security authentication all

114. Se debe crear un usuario y la correspondiente autenticación:

    -> user snmp3 password 4G76qpjQqBtsY69g sha+aes read-write all

    -> aaa authentication snmp local

115. El soporte de los *traps* requiere además la configuración de una estación SNMP para el envío de los *traps*:

    -> snmp station 1.1.1.1 snmp3 v3 enable

116. Se recomienda igualmente la autenticación de los *traps*:

    -> snmp authentication-trap enable

5.3.3 REEMPLAZAR EL CERTIFICADO SSL POR DEFECTO

117. Por defecto los switches vienen con un certificado auto-firmado en el directorio */flash/switch* del sistema de archivos del equipo. Se recomienda reemplazar estos certificados por otros certificados y clave RSA.

118. Para ello hay que conectarse al *switch* vía consola/SSH y cambiar el nombre de los archivos "*wv-cert.pem*" y "*wv-key.pem*" en el directorio */flash/switch* por ej. "*Wv-cert.bak*" y "*wv-key.bak*".

119. Una vez hecho esto hay que conectarse al *switch* a través de FTP para copiar los nuevos certificados. Hay que copiar los archivos en el directorio */flash/switch* del *switch*.

120. Una vez cargados los nuevos certificados hay que reiniciar el *switch* para que estos certificados se carguen. Tras el reinicio, cuando se conecta al *switch* mediante https, se presentarán los nuevos certificados cargados.

5.4 DISPONIBILIDAD

121. La disponibilidad hace referencia a garantizar que no hay una denegación de acceso autorizado a los recursos de la red, la información almacenada, los dispositivos o las aplicaciones.

122. A continuación, se describen diferentes modos de ataques y las herramientas propuestas para solventar este tipo de ataques o mitigar su efecto.

5.4.1 VLAN HOPPING

123. Un atacante en un acceso puede crear paquetes especiales con etiquetas 802.1q falsificadas para inyectarlos en otras VLAN sin pasar por un enrutador. De esta forma, un atacante puede, por ejemplo, evitar las ACL con una condición de VLAN de origen.

5.4.1.1 SWITCH SPOOFING

124. OmniSwitch soporta MVRP (*Multiple VLAN Registration Protocol*). Un atacante podría hacerse pasar por un switch y negociar el registro de una VLAN como un puerto de enlace para tener acceso a una VLAN no autorizada.

125. Por defecto, MVRP está deshabilitado en OmniSwitch. Se recomienda habilitar MVRP únicamente en los puertos que se vayan a usar como enlaces por los que propagar las VLAN requeridas, y nunca en los puertos de usuario.

126. Para que un equipo pueda empezar a conmutar tramas MVRP, se debe habilitar globalmente en el switch. Esto se hace mediante el siguiente comando:

-> mvrp enable

127. Además, hay que habilitar MVRP en el puerto o agregado de enlaces para que éstos puedan ser participantes activos en MVRP:

-> mvrp port 1/1/2 enable

-> mvrp linkagg 10 enable

5.4.1.2 DOBLE ETIQUETADO

128. En otro tipo de ataques, el atacante hace un doble etiquetado de la trama, siendo la primera etiqueta la de la VLAN por defecto del puerto de acceso, de forma que cuando sale por un enlace, al ser la de la VLAN por defecto, esa primera etiqueta se elimina y llega al segundo *switch* por una VLAN a la que no se debe tener acceso sin pasar primero por un *router*.

129. Un OmniSwitch viene con la *VLAN* 1 configurada por defecto para todos los puertos.

130. Para mitigar un posible ataque de este tipo, se recomiendan los siguientes pasos:

- Asignar una VLAN por defecto distinta de la VLAN 1 a los puertos del switch:

  -> vlan 10 members port 2/5 untagged

- Manteniendo la VLAN 1 por defecto en los puertos de enlace entre switches, deshabilitar esta VLAN:

  -> vlan 1 admin-state disable

5.4.2 ATAQUES DoS EN RANGOS DE RED RESERVADOS

131. En AOS, todos los paquetes de protocolos multicast con dirección IPv6 de destino ff02::/32 y con dirección IPv4 de destino 224.0.0.0/24 siempre se copian por defecto a la CPU. El uso intensivo de CPU puede afectar las operaciones normales de los protocolos de OmniSwitch tales como LACP, ERP, IGMP.

132. Para proteger los switches AOS contra la alta utilización de la CPU debido al tráfico no deseado que se copia en esta, se utilizan reglas QoS de calidad de servicio usando la prioridad 17 de CPU.

133. La CPU descarta los paquetes que se clasifican en la cola 17, pero aun así se reenvían. De esta manera, la CPU está protegida y la red es transparente para este tipo de tráfico.

134. A continuación, se puede ver un ejemplo de configuración de regla con prioridad de CPU 17:

```
! QOS:
policy condition mdc-dvmrp destination ip 224.0.0.4
policy condition mdc-ipv4mc-reserved destination ip 224.0.0.0  mask 255.255.255.0
policy condition mdc-ipv6mc-reserved destination ipv6 ff02::  mask ff:ff:ff:ff::
policy condition mdc-ospf-5 destination ip 224.0.0.5 ip-protocol 89
policy condition mdc-ospf-6 destination ip 224.0.0.6 ip-protocol 89
policy condition mdc-pim destination ip 224.0.0.13
policy condition mdc-ripv2 destination ip 224.0.0.9 destination udp-port 520
policy condition mdc-vrrp destination ip 224.0.0.18 ip-protocol 112
policy action accept
policy action q17 cpu priority 17
policy rule mdc-vrrp precedence 65070 condition mdc-vrrp action accept
policy rule mdc-ripv2 precedence 65060 condition mdc-ripv2 action accept
policy rule mdc-pim precedence 65050 condition mdc-pim action accept
policy rule mdc-ospf-6 precedence 65040 condition mdc-ospf-6 action accept
policy rule mdc-ospf-5 precedence 65030 condition mdc-ospf-5 action accept
policy rule mdc-dvmrp precedence 65020 condition mdc-dvmrp action accept
policy rule mdc-ipv6mc-reserved precedence 65010 condition mdc-ipv6mc-reserved
65000
condition mdc-ipv4mc-reserved action q17

qos apply
```

5.4.3 IGMP FLOODING

135. En AOS 8.x, el caudal de paquetes IGMP que se copia a la CPU está limitado por defecto, por lo que no es necesario hacer ninguna configuración específica al respecto.

5.4.4 DHCP FLOODING

136. Los paquetes DHCP se copian en la CPU de forma predeterminada, independientemente del conjunto de funcionalidades habilitadas. Para proteger la CPU contra la inundación de paquetes DHCP, se puede utilizar la prioridad 17 de la

CPU. El tráfico destinado a la CPU por la cola 17 se sigue cursando por la red, pero es descartado por la CPU. De esta manera, la CPU está protegida contra ataques de *flooding,* a la vez que la red es transparente para este tipo de tráfico.

137. La siguiente configuración se puede usar en el caso en que el *ip-helper* y DHCP *Snooping* estén deshabilitados:

```
! QOS:
policy condition dhcp-67 destination udp-port 67
policy condition dhcp-68 destination udp-port 68
policy action q17 cpu priority 17
policy rule dhcp-67 precedence 65100 condition dhcp-67 action q17
policy rule dhcp-68 precedence 65110 condition dhcp-68 action q17
qos apply
```

5.4.5 CONTROL DE TORMENTAS DE TRÁFICO

138. OmniSwitch AOS dispone de mecanismos para controlar el tráfico BUM (*Broadcast, Unknown unicast y Multicast*). Para ello se puede configurar, por puerto, el límite de tráfico de cada tipo permitido en dicho puerto.

139. El límite máximo de tráfico de cada tipo (*bcast, uucast, mcast*) se puede especificar mediante un caudal fijo (*mbps*) o en paquetes por segundo (*pps*) o como un porcentaje de la velocidad del puerto (*cap%*) como podemos ver en los siguientes ejemplos:

```
-> interfaces 2/1/1 flood-limit bcast rate mbps 100
-> interfaces 2/1/2-5 flood-limit uucast rate pps 500
-> interfaces slot 3/1 flood-limit mcast rate cap% 20
```

140. Se pueden configurar igualmente dos (2) acciones cuando se llega al límite especificado, lo que permite monitorizar las tormentas de tráfico:

- **Desactivación del puerto**. El puerto se pasa a un estado de violación de política por tormenta de tráfico y se envía un *trap*.
- **Envío de *trap***. La tormenta de tráfico se controla mediante los límites especificados y se envía un *trap*. El puerto sigue activo.

141. En el siguiente ejemplo se puede ver cómo configurar las diferentes acciones:

```
-> interfaces 1/1/1 flood-limit bcast action shutdown
-> interfaces 1/1/4 flood-limit uucast action trap
-> interfaces 1/1/11 flood-limit all action shutdown
```

142. Además, cuando un puerto pasa a un estado de violación del control de tormentas, el administrador ha de limpiar dicho estado. Sin embargo, este proceso se puede automatizar estableciendo un umbral inferior de forma que cuando el tráfico que ha provocado la tormenta baje de dicho umbral, el estado de violación por tormenta de tráfico se limpia. Por ejemplo:

-> interfaces 1/1/1 flood-limit bcast rate mbps 60 low-threshold 40

-> interfaces 1/1/4 flood-limit uucast rate mbps 100 low-threshold 40

-> interfaces 1/1/5 flood-limit mcast rate pps 2000 low-threshold 1000

5.4.6 LEARNED PORT SECURITY - ATAQUES POR CAM OVERFLOW

143. La memoria CAM (*Conditional Access Memory*) de un switch es la que almacena la tabla de direcciones MAC aprendidas por el switch. Si un atacante introduce tramas con direcciones MAC de origen aleatorias puede llenar la tabla de direcciones MAC, que tiene una capacidad limitada. Cuando esto sucede, el switch deja de conmutar tráfico y empieza a inundar todos los puertos, convirtiéndose en un hub.

144. Para evitarlo, AOS soporta la funcionalidad *Learned Port Security (LPS)*, que proporciona un mecanismo para autorizar el aprendizaje de origen de las direcciones MAC en los puertos Ethernet.

145. El uso de LPS para controlar el aprendizaje de la dirección MAC de origen proporciona los siguientes beneficios:

- Un límite de tiempo configurable para el aprendizaje de MACs de origen que se aplica a todos los puertos LPS.
- Un límite configurable del número de direcciones MAC permitidas en un puerto LPS.
- Configuración dinámica de una lista de direcciones MAC de origen autorizadas.
- Configuración estática de una lista de direcciones MAC de origen autorizadas.
- Tres (3) métodos para gestionar el tráfico no autorizado: deshabilitar administrativamente el puerto LPS, detener todo el tráfico en el puerto (el puerto permanece habilitado) o solo bloquear el tráfico que viole los criterios de LPS.

146. LPS se soporta en puertos fijos, en puertos 802.1Q (*tagged*) o puertos UNP. En cambio, no se soporta en agregados de enlaces, ni en agregados de enlaces etiquetados (troncales), ni en miembros de los agregados.

147. De manera predeterminada, LPS está deshabilitado en todos los puertos del conmutador. Para habilitar LPS en un puerto, deberá utilizarse el comando ***port-security***. Por ejemplo, el siguiente comando habilita LPS en el puerto 1 de la ranura 4:

-> port-security 1/1 admin-status enable

148. Se puede habilitar LPS en rangos de puertos o puertos en diferentes slots:

-> port-security 1/1-5 admin-status enable

-> port-security 1/1-5 1/10-15 admin-status enable

149. Cuando LPS está habilitado en un puerto activo, todas las direcciones MAC aprendidas en ese puerto antes de habilitar LPS se borran de la tabla de direcciones MAC de origen.

150. Para deshabilitar LPS en un puerto, se utilizará el comando ***port-security*** con el parámetro deshabilitar. Por ejemplo, el siguiente comando deshabilita LPS en un rango de puertos:

-> port-security 1/1-5 1/10-15 admin-status disable

151. Para convertir todas las direcciones MAC aprendidas por el switch en un puerto LPS en direcciones MAC estáticas, se puede usar el comando ***port-security chassis*** con el parámetro ***convert-to-static***. Por ejemplo:

-> port-security chassis convert-to-static

-> port-security port 1/8 convert-to-static

152. Para deshabilitar LPS en un switch se usa el siguiente comando:

-> port-security chassis admin-state disable

153. Se puede configurar la ventana de aprendizaje de direcciones MAC. El valor de la ventana de aprendizaje se especifica en minutos. Si se configura con un valor 0, el tiempo de aprendizaje es infinito:

-> port-security learning-window 2

154. Se puede especificar que las direcciones MAC aprendidas tras el tiempo de la ventana de aprendizaje se conviertan en estáticas:

-> port-security learning-window 2 convert-to-static enable

155. Para configurar el máximo número de direcciones MAC que se pueden aprender en un puerto o rango de puertos se usan los comandos siguientes:

-> port-security port 2/14 maximum 5

-> port-security port 2/10-15 maximum 10

156. Por defecto, cada vez que se aprende una MAC en un puerto se envía un *trap SNMP* al administrador. Se puede especificar un umbral por debajo del cual no se envían traps. Una vez que se alcanza el umbral, se envía un *trap* por cada nueva MAC con información sobre la MAC, el switch y el puerto por el que se ha aprendido.

-> port-security port learn-trap-threshold 10

157. Con LPS se puede configurar el modo en que se quiere que el puerto se comporte cuando hay una violación de la política LPS. Cuando esto sucede, el puerto se puede configurar en uno de los siguientes modos:

- ***Restrict***: el puerto sigue habilitado, pero se bloquean la direcciones MAC no autorizadas. Todas las direcciones MAC aprendidas y autorizadas pueden seguir cursando tráfico normalmente

- ***Discard***: el puerto continúa habilitado administrativamente, pero todo el tráfico que se cursa por este puerto se descarta. Las direcciones MAC aprendidas dinámicamente en el puerto se eliminan de la tabla de direcciones.
- ***Shutdown***: el puerto se deshabilita administrativamente y no se cursa tráfico por él.

158. Por defecto, el modo de funcionamiento de LPS es ***Restrict***. Para cambiarlo se puede usar los siguientes comandos:

```
-> port-security port 4/1-10 violation shutdown
-> port-security port 1/10-15 violation restrict
```

5.4.7 FUNCIONALIDADES DE SEGURIDAD DE DHCP

159. Un atacante puede utilizar un ataque por servidor DHCP no confiable para configurar un servidor DNS y/o una puerta de enlace falsos. El atacante puede usar su propia dirección IP como puerta de enlace en las ofertas de DHCP para poder rastrear el tráfico.

160. En AOS hay dos funciones de seguridad DHCP disponibles: la opción de información del agente DHCP *relay* (*Option-82*) y DHCP *Snooping*.

- La función DHCP Option-82 permite que el agente *dhcp-relay* inserte información de identificación en los paquetes DHCP originados por el cliente antes de que se envíen al servidor DHCP.
- La función DHCP *Snooping* filtra los paquetes DHCP entre fuentes no confiables y un servidor DHCP de confianza y crea una base de datos de vínculos para registrar la información del cliente DHCP.

161. Aunque DHCP *Option-82* es un subcomponente de DHCP *Snooping*, estas dos funcionalidades son mutuamente excluyentes. Si la función DHCP *Option-82* está habilitada en el switch, entonces DHCP *Snooping* no está disponible. Lo contrario también es cierto; si DHCP *Snooping* está habilitado, entonces DHCP *Option-82* no está disponible. Además, existen las siguientes diferencias entre estas dos características:

- DHCP *Snooping* requiere y utiliza la capacidad de inserción de datos de la *Option-82*, pero no implementa ningún otro comportamiento definido en RFC 3046.
- DHCP *Snooping* es configurable a nivel de conmutador y por VLAN, pero DHCP *Option-82* solo es configurable a nivel de conmutador.

5.4.7.1 RELAY AGENT INFORMATION OPTION (OPTION-82)

162. Cuando esta función está habilitada, el *relay agent* autentica las comunicaciones entre un cliente DHCP y un servidor DHCP. Para realizar esta tarea, el agente

agrega datos de la *Option-82* al final del campo de opciones de los paquetes DHCP enviados desde un cliente a un servidor DHCP.

163. La *Option-82* consta de dos subopciones: ID de circuito e ID remota. El agente completa la siguiente información para cada una de estas sub-opciones:

- **ID de circuito**: la ID de VLAN y slot/puerto desde donde se originó el paquete DHCP.
- **ID remota**: la dirección MAC de la interfaz del *router* asociada con la ID de VLAN especificada en la subopción ID de circuito.

164. El comando ***ip dhcp relay insert-agent-information format*** se usa para configurar el tipo de datos (dirección MAC base, nombre del sistema, alias de interfaz o definido por el usuario) que se inserta en las anteriores subopciones de la *Option-82*. Por ejemplo:

-> ip dhcp relay insert-agent-information format system-name

-> ip dhcp relay insert-agent-information format base-mac

165. Por defecto, el *relay-agent* descarta los paquetes DHCP del cliente que recibe que ya contienen datos en la *Option-82*. Sin embargo, es posible configurar una política de *Option-82* para especificar cómo se tratan dichos paquetes mediante el comando ***ip dhcp relay insert-agent-information policy***. Las opciones son:

- ***drop***: se eliminan los datos de la *Option-82* de DHCP (valor predeterminado).
- ***keep***: la información de campo de la *Option-82* existente en el paquete DHCP se retiene y el paquete se transmite al servidor DHCP.
- ***replace***: los datos existentes de la *Option-82* en el paquete DHCP se reemplazan con la ID de VLAN y la dirección MAC del *switch* DHCP relay.

-> ip dhcp relay insert-agent-information policy drop

-> ip dhcp relay insert-agent-information policy keep

-> ip dhcp relay insert-agent-information policy replace

- Para habilitar DHCP *Option-82*, se usa el siguiente comando:

-> ip dhcp relay insert-agent-information

5.4.7.2 DHCP SNOOPING

166. El uso de DHCP *Snooping* mejora la seguridad de la red al filtrar los mensajes DHCP recibidos de dispositivos de fuera de la red y crear y mantener una tabla de vínculos (base de datos) para rastrear la información de acceso para dichos dispositivos.

167. Para identificar el tráfico DHCP que se origina desde fuera de la red, DHCP *Snooping* clasifica los puertos como de confianza (*trusted*) o no confiables (*untrusted*).

168. Un puerto es confiable si está conectado a un dispositivo dentro de la red, como un servidor DHCP. Reenvía mensajes DHCP para garantizar que los clientes DHCP puedan obtener direcciones IP válidas.

169. Un puerto no es de confianza si está conectado a un dispositivo fuera de la red, como *switches* o estaciones de trabajo de cliente. Los paquetes DHCP recibidos se rechazan, evitando que los clientes DHCP reciban direcciones IP no válidas.

170. DHCP *Snooping* añade además la siguiente funcionalidad:

- **DHCP Snooping de capa 2**: aplica la funcionalidad DHCP *Snooping* al tráfico *broadcast* DHCP cliente/servidor en una VLAN sin usar el *relay-agent* o que no requiere una interfaz IP en la VLAN.
- **Filtrado por IP de origen (*Dynamic ARP Inspection* – (DAI)):** restringe el tráfico del puerto DHCP Snooping solo a los paquetes que contienen la información adecuada de origen del cliente. La tabla de vínculos (bindign table) de DHCP Snooping se usa para verificar la información del cliente en el puerto para el que está habilitado el filtrado IP de origen.
- **Limitación de velocidad**: limita la velocidad de los paquetes DHCP en el puerto. Esta funcionalidad se logra utilizando la aplicación QoS para configurar las ACL para el puerto.

171. La funcionalidad DHCP Snooping se puede configurar a nivel de *switch* o a nivel de VLAN. Ambos modos son excluyentes y no pueden operar en el *switch* al mismo tiempo. Los siguientes comandos habilitan la funcionalidad a nivel de *switch* y a nivel de VLAN respectivamente:

```
-> dhcp-snooping admin-state enable

-> dhcp-snooping vlan 200 admin-state enable
```

172. Filtrado por IP de origen está habilitado por defecto a nivel de *switch*. Además, se puede configurar también por VLAN o por puerto/agregado:

```
-> dhcp-snooping ip-source-filter vlan 10 admin-state enable

-> dhcp-snooping ip-source-filter port 1/1/1 admin-state enable

-> dhcp-snooping ip-source-filter linkagg 2 admin-state enable
```

173. La tabla de vínculos (*binding table*) de DHCP *Snooping* se habilita por defecto cuando se configura DHCP *Snooping* en el *switch* o VLAN. Esta tabla se usa para filtrar el tráfico DHCP que se recibe pro los puertos no confiables. Se pueden además introducir entradas estáticas en la tabla de vínculos. Para habilitar, deshabilitar o incluir entradas en la tabla de vínculos se pueden usar los comandos siguientes:

```
-> dhcp-snooping binding admin-state enable

-> dhcp-snooping binding admin-state disable

-> dhcp-snooping binding 00:2a:95:51:6c:10 port 1/1/15 address 17.15.3.10
vlan 200
```

174. Un ejemplo de configuración de DHCP *Snooping* podría ser el siguiente:

! DHCP Snooping:

dhcp-snooping admin-state enable

dhcp-snooping binding admin-state enable

dhcp-snooping ip-source-filter port 1/1/1-24 admin-state enable dhcp-snooping port 1/1/25-26 trust

5.4.8 ATAQUE POR STP RECLAMANDO EL ROL DE ROOT

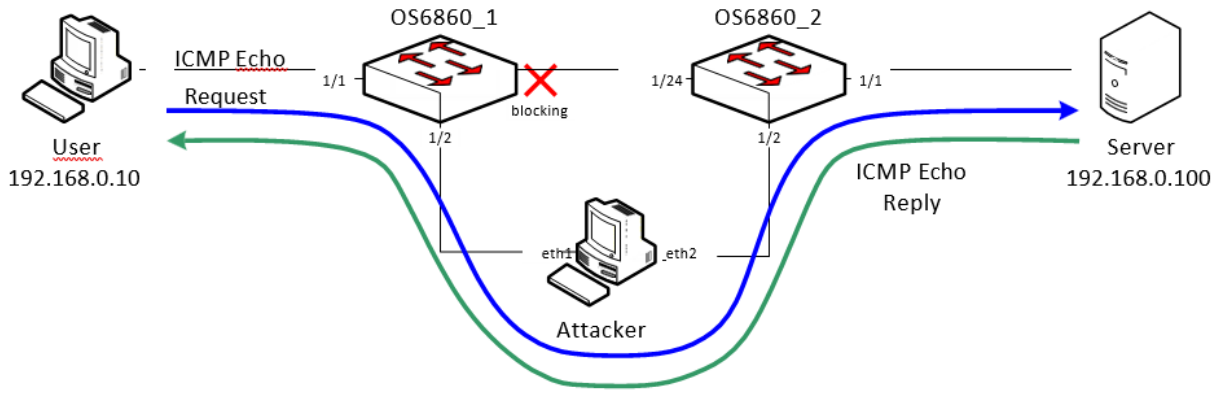
175. Los ataques por STP están orientados a desestabilizar la operación de STP (*Spanning Tree Protocol*) en la red.

176. Si un atacante tiene acceso a puertos de los *switches* de la red que pueden convertirse en puertos troncales, puede insertar un *switch* no autorizado en la red. De esta forma tiene la posibilidad de formar otra conexión con un segundo conmutador de esa red y manipular la prioridad del árbol. Si configura el *switch* atacante para que tenga una prioridad que sea menor que en cualquier otro conmutador de la empresa, la mayor parte del tráfico pasará teóricamente a través de ese conmutador.

177. El *switch* atacante con, por ejemplo, prioridad 0, anuncia sus "BPDU superiores" y la topología STP converge. El *switch* atacante se convertirá en el *root* y todo el tráfico pasará por este conmutador. Esto le da la posibilidad de ver todo el tráfico de la empresa.

178. También puede redirigir el tráfico desde enlaces de gran ancho de banda entre otros conmutadores a por ejemplo un enlace de 100 Mbps en el conmutador atacante. Esto reducirá significativamente la velocidad de la red.

179. El siguiente diagrama refleja la problemática presentada. Un atacante con dos tarjetas de red puede simular un conmutador que intercambia BPDUs con los dos conmutadores existentes en la red, reconfigurando la topología de STP y haciéndose pasar por el root de la red STP. De esta forma el switch 1 pondría en estado *blocking* el puerto que conecta con el 2 y todo el tráfico se enviaría a través del atacante, con lo que éste tendría visibilidad de todo el tráfico intercambiado entre el usuario y el servidor.



180. Para evitar esto, AOS dispone de varios mecanismos: *QoS User Port* y STP *Root Guard.*

5.4.8.1 QOS USER PORT

181. *QoS User Port* se puede usar para proteger la infraestructura de red contra ataques L2 y L3 (no solo contra ataques STP). El principio es bloquear el tráfico o desactivar un puerto en el que la función está habilitada al recibir un tipo de tráfico predefinido.

La sintaxis del comando es la siguiente:

qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}

182. Cuando se configura esta funcionalidad, el tipo de tráfico y el comportamiento del puerto se aplica a los puertos asignados al grupo ***UserPorts*** y hay que tener en cuenta lo siguiente:

- El comando ***qos user-port*** se usa para configurar un perfil para ***UserPorts*** que especifica los tipos de tráfico a buscar y selecciona cómo gestionarán dicho tráfico los puertos.
- No es necesario especificar un puerto con el comando ***qos user-port,*** ya que el comando se aplica a todos los puertos que son miembros del grupo ***UserPorts***.
- El tráfico de entrada se filtra en los puertos que son miembros del grupo ***UserPorts***.
- Se envía un *trap* SNMP cada vez que se produce un bloqueo del puerto del usuario. Para habilitar un puerto deshabilitado por una operación de bloqueo del puerto de usuario, hay que usar el comando ***interfaces*** para habilitar administrativamente el puerto o desconectar y reconectar el cable del puerto.
- Cualquier cambio en el perfil de ***UserPorts*** (por ejemplo, agregar o eliminar un tipo de tráfico) no se realiza hasta que se ejecuta el comando ***qos apply***.

183. La configuración que previene el ataque en el ejemplo de la figura anterior sería:

OS6860_1-> policy port group UserPorts 1/1-23

OS6860_1-> qos user-port shutdown bpdu

OS6860_1-> qos apply

OS6860_2-> policy port group UserPorts 1/1-23

OS6860_2-> qos user-port shutdown bpdu

OS6860_2-> qos apply

5.4.8.2 STP ROOT GUARD

184. Los administradores de red habilitan el estado restringido del rol de un puerto para evitar que *switches* externos al núcleo central de la red influyan en la

topología de *Spanning Tree*. A tener en cuenta que si se habilita el estado restringido de rol en un puerto puede afectar a la conectividad dentro de la red.

185. Por defecto, todos los puertos son elegibles para su elección como puerto *root*. Se puede evitar que un puerto en una instancia CIST / MSTI o en una instancia per-VLAN se convierta en el puerto *root* restringiendo el rol del puerto (también conocido como habilitar *root guard*). Esto se hace mediante el comando "***spantree cist restricted-rol***" o el comando ***"spantree vlan restricted-rol***", independientemente del modo STP (*per-VLAN* o *flat*) que esté activo en el *switch*. Por ejemplo:

-> spantree cist port 1/2 restricted-role enable

-> spantree cist linkagg 10 restricted-role enable

-> spantree vlan 100 port 8/1 restricted-role enable

-> spantree vlan 20 linkagg 1 restricted-role enable

186. Cuando ***root guard*** está habilitado para un puerto, este no puede convertirse en el puerto *root*, incluso si es el candidato más probable para convertirse en el puerto *root*. Sin embargo, este mismo puerto se designa como el puerto ***alternate*** una vez seleccionado el puerto *root*.

187. Por defecto, en AOS esta función no está habilitada.

5.4.9 ATAQUES EN LOS PROTOCOLOS DE ROUTING

188. Es necesario proteger los protocolos de *routing* para evitar que se inyecten rutas de forma no autorizada.

5.4.9.1 AUTENTICACIÓN DE LOS PROTOCOLOS DE ROUTING

189. RIP, OSPF, ISIS, BGP permiten el uso de autenticación en las interfaces configuradas. Cuando la autenticación está habilitada, solo pueden comunicarse los vecinos que usan el mismo tipo de autenticación y usan las mismas contraseñas o claves.

190. En OSPF hay dos tipos de autenticación: simple y HMAC-SHA La autenticación simple requiere solo una cadena de texto como contraseña, mientras que HMAC-SHA (método recomendado desde el punto de vista de la seguridad) es una forma de autenticación cifrada que requiere una clave y una contraseña. Ambos tipos de autenticación requieren el uso de más de un comando.

Autenticación simple

191. Para habilitar la autenticación simple en un interfaz OSPF, introducir el comando ***ip ospf interface auth-type*** con el nombre de interfaz:

-> ip ospf interface vlan100 auth-type simple

192. A continuación se introduce el comando ***ip ospf interface auth-key*** para establecer la clave:

-> ip ospf interface vlan100 auth-key switch

193. De esta forma únicamente los interfaces OSPF con autenticación simple y clave *switch* podrán utilizar el interfaz configurado.

Autenticación SHA

194. Para configurar el mismo interfaz con autenticación SHA, se define la clave de seguridad mediante el comando *security key:*

-> security key 5 algorithm sha256 "securitykey1234"

195. A continuación, se usa la clave definida anteriormente para la autenticación del interfaz OSPF. Esto se hace mediante el parámetro *auth-type key-chain* del comando ip ospv interface:

-> ip ospf interfaz vlan100 auth-type key-chain 5

196. Una vez se ha hecho esto, el interfaz está habilitado con autenticación SHA.

197. Para deshabilitar la autenticación OSPF en un interfaz se hace mediante el siguiente comando:

-> ip ospf interface vlan100 auth-type none

198. A continuación se puede ver un ejemplo de configuración con OSPF autenticado:

```
! OSPF:
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "vlan100"
ip ospf interface "vlan100" area 0.0.0.0
security key 5 algorithm sha256 "securitykey1234"
ip ospf interface "vlan100" status enable
ip ospf interface vlan100 auth-type key-chain 5
```

199. Donde "SecurityKey1234" es un ejemplo de contraseña que deberá modificarse en la configuración establecida, de acuerdo a las políticas definidas en el apartado 5.2.1.3

5.4.9.2 INTERFAZ PASIVO OSPF

200. Para evitar anuncios de paquetes *hello* en una VLAN que no tiene vecinos OSPF, se configura el *hello interval* a 0 en el interfaz correspondiente.

201. Se puede ver en el siguiente ejemplo:

```
! OSPF:
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "vlan1"
ip ospf interface "vlan1" area 0.0.0.0
```

ip ospf interface "vlan1" hello-interval 0

ip ospf interface "vlan1" admin-state enable

ip ospf interface "vlan100"

ip ospf interface "vlan100" area 0.0.0.0

ip ospf interface "vlan100" admin-state enable ip ospf admin-state enable

5.4.9.3 DESHABILITAR LA FUNCIÓN *AUTO-FABRIC*

202. *Auto-Fabric* es una funcionalidad que permite descubrir y configurar dinámicamente los protocolos LACP, SPB y MVRP en un *switch*. Se soporta tanto en un chasis independiente como en un chasis virtual. Si el descubrimiento automático de LACP está habilitado, el sistema intentará el descubrimiento de LACP y la configuración automática en una ventana de descubrimiento establecida. Después de que expire la ventana de descubrimiento LACP, se producirá el descubrimiento automático de SPB si está habilitado. Por último, el descubrimiento automático MVRP si está habilitado.

203. Algunos de los beneficios proporcionados por *Auto-Fabric* son:

- El descubrimiento automático reduce la sobrecarga administrativa.
- El descubrimiento automático permite el descubrimiento de los protocolos LACP, SPB y MVRP.
- La configuración LACP y SPB (no MVRP) descubierta automáticamente se puede guardar permanentemente en el archivo de configuración del conmutador para que se mantenga después de un reinicio.

204. Por razones de seguridad, **se recomienda deshabilitar esta funcionalidad** en entornos en los que se pueda producir accesos no autorizados a la red.

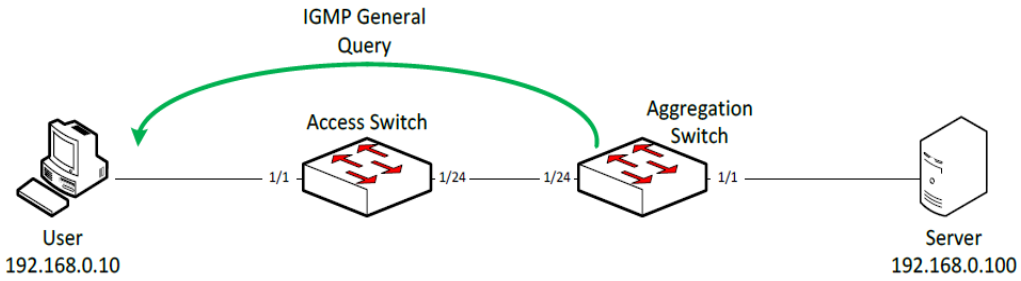
205. Para ello se usa el siguiente comando:

-> auto-fabric admin-state disable remove-global-config

5.4.10 ATAQUE POR IGMP *QUERIER* NO CONFIABLE

206. En caso de que IPMS Querying esté habilitado en una red multicast L2, solo habrá uno elegido (el de dirección IP más baja) como *querier* activo y solo este *querier* podrá enviar consultas generales IGMP. Todos los dispositivos con IPMS habilitado en la red *multicast* L2 mantienen una tabla con los *queriers* activos y envían informes de pertenencia IGMP al *querier* activo. Un atacante puede usar una dirección IP más baja para inyectar un IGMP *General Query* en un puerto no confiable.

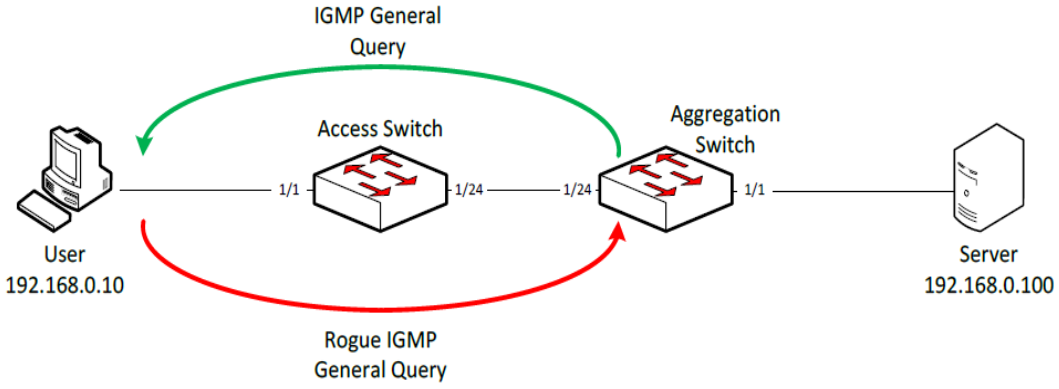
207. Antes del ataque tenemos que el *switch* de agregación es el *Querier* activo. Si miramos desde el *switch* de acceso (*Access switch*).



-> show ip multicast querier

```
Total 1 Queriers
Host Address     VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
192.168.0.254    1     1/24  no      1      252
```

208. Tras el ataque, el atacante se convierte en el *Querier* activo. Si volvemos a mirar desde el *switch* de acceso (*Access Switch*):



-> show ip multicast querier

```
Total 1 Queriers
Host Address     VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
192.168.0.10     1     1/1   no      1      167
```

209. Este tipo de ataque se puede prevenir usando políticas QoS de calidad de servicio.

! QOS :
policy port group untrusted 1/1-23
policy condition general-query-sw destination port group untrusted multicast ip 224.0.0.1
policy action drop disposition deny
policy rule deny-general-query-sw condition general-query-sw action drop qos apply

210. Esta política no descarta el IGMP *General Query* malintencionado sino que previene que éste se aprenda en el *switch* donde esta política se configura.

5.4.11 MECANISMO DE SEGURIDAD DE AGENTE LLDP NO CONFIABLE

211. El protocolo LLDP (protocolo de descubrimiento de la capa de enlace) tiene como objeto ayudar a la administración de las redes. Este protocolo proporciona información de plataformas vecinas, así como datos del enlace que los une.

212. En general, se recomienda desactivar LLDP si no es estrictamente necesario ya que puede ser empleado de manera malintencionada para influir en algunos servicios de red.

213. El mecanismo de seguridad de agente LLDP de OmniSwitch proporciona una solución para el acceso seguro a la red al detectar dispositivos no autorizados y evitar que accedan a la red interna. La seguridad del agente LLDP se consigue permitiendo un único agente LLDP remoto de confianza en un puerto de red.

214. Se puede configurar el subtipo de *Chassis* ID que se puede usar para su validación la LLDP PDU entrante. Si es *Chassis* ID no está configurado, por defecto se aprende el primer agente LLDP remoto con es *Chassis* ID recibido. Cuando se aprende más de un agente LLDP en un puerto, el puerto se mueve a un estado de violación.

215. El mecanismo de seguridad LLDP se puede habilitar o deshabilitar globalmente en el chasis, a en un slot o en un puerto individual. Cuando la seguridad del agente LLDP está habilitada, los puertos configurados son monitorizados para la recepción de cualquier LLDPDU. Cuando se recibe una LLDPDU, se aprende la ID del agente remoto y el puerto se considera como un puerto confiable si el puerto no tiene ningún otro agente remoto LLDP asignado. Si la ID del chasis del agente remoto y las ID del puerto recibidas ya están presentes en la base de datos del agente remoto de confianza en el mismo puerto, entonces el puerto permanece en un estado de confianza.

216. Por ejemplo, cuando alguien intenta tomar el control de la red conectando dispositivos no registrados a un puerto NNI, se activa el mecanismo de seguridad LLDP. Las siguientes acciones se realizan de acuerdo con la configuración de seguridad:

- Cuando se detecta el dispositivo no autorizado, se informa de una violación en el puerto.
- El puerto NNI que está conectado al dispositivo no autorizado es bloqueado. Por lo tanto, se impide que el dispositivo no autorizado acceda a la red interna.
- Sólo un Agente LLDP Remoto aprendido y validado es declarado como válido.
- Si el puerto con seguridad LLDP habilitada no recibe una LLDPDU después de un período de tres veces el del intervalo de transmisión LLDP (30 segundos) desde que el enlace se levanta, el puerto pasa a un estado de violación.

- Si existe un agente remoto de confianza, y si no se aprende ningún agente remoto LLDP, incluso después de un período de tres veces el del intervalo del temporizador LLDP (30 segundos).
- Si el mismo ID de *chasis ID* de puerto existen en la base de datos de un agente remoto de confianza, pero en un puerto diferente, entonces el agente remoto del puerto se aprende y el puerto se mueve a un estado de violación.
- Si se descubre un nuevo agente remoto LLDP en un puerto que ya tiene un agente remoto LLDP de confianza.

217. En el siguiente ejemplo se puede ver cómo configurar el mecanismo de seguridad de agente LLDP:

218. Se configura LLDP:

-> lldp chassis notification enable

-> lldp chassis tlv management port-description enable

-> lldp chassis tlv system-name enable system-description enable

-> lldp chassis tlv management management-address enable

-> lldp chassis tlv dot1 vlan-name enable port-vlan enable

-> lldp chassis tlv dot3 mac-phy enable

219. Se habilita la seguridad de agente LLDP:

-> lldp 1/1 trust-agent enable

220. Se indica la acción a realizar en caso de violación:

-> lldp 1/1 trust-agent violation-action trap

-> lldp 1/1 trust-agent violation-action trap-and-shutdown

221. Configurar el suptipo de *chassis* ID:

-> lldp 1/1 trust-agent chassis-id-subtype chassis-component

222. Para visualizar la configuración de configuración de seguridad de agente LLDP se puede hacer mediante el siguiente comando:

-> show lldp trust-agent

```
Slot/Port  Admin Status  Violation Action  Violation Status   Chassis Subtype

---------+--------------+-----------------+------------------+-----------------
1/1        Enabled        Trap Only         Trusted            1(Chassis Component)
1/2        Enabled        Trap Only         Trusted            1(Chassis Component)
1/3        Enabled        Trap Only         Trusted            1(Chassis Component)
1/4        Disabled       Shutdown          Violated           1(Chassis Component)
1/5        Enabled        Shutdown          Trusted            1(Chassis Component)
1/6        Enabled        Trap-and-Shutdown Trusted            1(Chassis Component)
1/7        Disabled       Trap-and-Shutdown Violated           1(Chassis Component)
1/8        Enabled        Trap Only         Trusted            1(Chassis Component)
1/9        Enabled        Trap Only         Trusted            1(Chassis Component)
```

5.4.12 FILTRADO DE ATAQUES DOS EN INTERFACES DEL ROUTER

223. El *switch* filtra los ataques de denegación de servicio (DoS), que son ataques de seguridad dirigidos a dispositivos disponibles en una red privada o en Internet. Determinados ataques apuntan a fallos del sistema o vulnerabilidades (por ejemplo, ataques *teardrop*), mientras que otros tipos de ataques implican generar grandes volúmenes de tráfico para que el servicio de red sea denegado a los usuarios legítimos de la red (como los ataques *pepsi*). Por defecto está habilitado en los conmutadores OmniSwitch el filtrado de los siguientes tipos de ataques de denegación de servicio excepto el de Sobrecarga de ping que hay que activarlo explícitamente:

- **Ping de la muerte ICMP:** se envían a un host paquetes *ping* que exceden el tamaño máximo de un datagrama IP (65535 bytes) y bloquean el sistema.
- **SYN Attack**: se inunda un sistema con una serie de paquetes TCP SYN, a los que el host responde con SYN-ACK. Las conexiones TCP a medio abrir pueden agotar los recursos TCP, de modo que no se aceptan otras conexiones TCP.
- **Land Attack**: se envían paquetes falsificados con el indicador SYN establecido a un host en cualquier puerto abierto que esté escuchando. La máquina puede bloquearse o reiniciarse para responder.
- **Pepsi Attack:** es la forma más común de inundación UDP dirigida a dañar las redes. Un ataque *pepsi* es un ataque que consiste en muchos paquetes UDP falsificados destinados a puertos de diagnóstico en dispositivos de red. Un ataque *pepsi* puede hacer que los dispositivos de red usen mucho de tiempo de CPU para responder a estos paquetes.
- **ARP Flood Attack:** inunda un *switch* con muchas solicitudes ARP, lo que hace que el *switch* utilice una gran cantidad de tiempo de CPU para responder a estas solicitudes. Si el número de solicitudes ARP excede el valor predeterminado de 500 por segundo, se detecta un ataque.
- **Ataque por IP no válida**: el *switch* recibe paquetes con direcciones IP de origen o destino no válidas. Cuando se detecta un ataque por IP no válida, los paquetes se descartan y se generan *traps* SNMP. Los siguientes son algunos ejemplos de direcciones IP de origen y destino no válidas:

  Dirección IP de origen no válida

  - *0.x.x.x*
  - *255.255.255.255*
  - *broadcast de subred, es decir, 172.28.255.255, para una interfaz IP 172.28.0.0/16*
  - *en el rango 224.x.x.x - 255.255.255.254*
  - *La dirección IP de origen es igual a una de las direcciones de interfaz IP del Switch*

Dirección IP de destino no válida

- *127.x.x.x*
- *en el rango 240.x.x.x - 255.255.255.254*
- *0.0.0.0 (excepciones válidas: ciertos paquetes DHCP)*
- *172.28.0.0 para una red de routers 172.28.4.11/16*
- *0.x.x.x*

- **No coinciden las direcciones IP y MAC de *multicast***. Este ataque se detecta cuando:
  - La dirección MAC de origen de un paquete recibido por un *switch* es una dirección MAC *multicast*.
  - Las direcciones IP y MAC de destino de un paquete recibido por un *switch* son las mismas que las direcciones IP y MAC de *multicast*, pero las direcciones IP y MAC *multicast* no coinciden.

  Nota. En las dos condiciones descritas anteriormente en "No coinciden las direcciones IP y MAC *multicast*", los paquetes se descartan y se generan *traps* SNMP.

- **La IP de destino es una IP unicast y la dirección MAC de destino es una dirección broadcast o multicast.** En dicha condición, se registra un evento en las estadísticas DoS. No se generan *traps* SNMP, ya que los paquetes válidos también pueden incluirse en esta categoría.

- **Sobrecarga de ping**: se inunda un *switch* con muchos paquetes ICMP, lo que hace que el *switch* utilice una gran cantidad de tiempo de CPU para responder a estos paquetes. Si el número de paquetes ICMP excede 100 por segundo, se detecta un ataque DoS. Por defecto, la detección de ataque está deshabilitada. Para habilitar la detección de este tipo de ataque se usa el comando:

  -> ip dos type ping-overload admin-state enable

- **Paquetes con la IP de loopback como dirección IP de origen**. Se reciben en el *switch* paquetes con una dirección IP de origen 127.0.0.0/8 (*loopback* de red) no válida. Cuando se detectan estos paquetes se descartan y se generan *traps* SNMP.

224. El *switch* se puede configurar para detectar varios tipos de escaneo de puertos monitorizando los paquetes TCP o UDP enviados a puertos abiertos o cerrados. La monitorización se realiza de la siguiente manera:

- *Establecer valores de penalización de paquetes*. A los paquetes TCP y UDP destinados a puertos abiertos o cerrados se les asigna un valor de penalización. Cada vez que se recibe un paquete de este tipo, su valor de penalización asignado se agrega a un total acumulado. Este total es acumulativo e incluye todos los paquetes TCP y UDP destinados a puertos abiertos o cerrados. Los valores de penalización por defecto son 10 para paquetes TCP o UDP destinados a puertos cerrados, y 0

para paquetes destinados a puertos abiertos. Estos valores se pueden asignar mediante los siguientes comandos:

-> ip dos scan close-port-penalty 25

-> ip dos scan tcp open-port-penalty 10

-> ip dos scan udp open-port-penalty 15

- *Establecer un umbral para el valor de penalización acumulado de escaneo de puertos*. Se asigna al *switch* un umbral para el valor de penalización de escaneo de puertos. Este umbral es el valor máximo que puede alcanzar el total acumulado de penalizaciones antes de enviar un *trap* SNMP. El valor por defecto es 1000 y se puede configurar mediante el siguiente comando:

  -> ip dos scan threshold 2000

- Valor de disminución (*decay value*). Estableciendo este valor de disminución, la penalización total del puerto se divide por este valor cada minuto para evitar que se llegue al umbral debido al tráfico normal. El valor por defecto es 2 y se modifica mediante el siguiente comando:

  -> ip dos scan decay 10

- Generación de *traps*. Si el valor de penalización total excede el umbral establecido para escaneo de puertos, se genera un *trap* para alertar al administrador de que puede estar produciendo un escaneo de puerto. Esta funcionalidad está habilitada por defecto. Se puede modificar mediante los siguientes comandos:

  -> ip dos trap enable

  -> ip dos trap disable

5.4.13 EJEMPLO DE CONFIGURACIÓN

225. A continuación se recoge un ejemplo de configuración segura de un dispositivo. El escenario planteado es el siguiente:

- Se trata de un equipo OS6860E de 24 puertos.
- Es un equipo de acceso.
- Los puertos 1 a 24 son puertos de acceso para PCs o teléfonos IP.
- Los puertos 25 y 26 son enlaces de red hacia el núcleo o agregación.
- Los PCs y teléfonos usan DHCP para asignación de la dirección IP.
- Se ha habilitado *routing* con OSPF.
- Las funciones de seguridad se han configurado en modo bloqueo de puerto en caso de violar alguna regla.

- LLDP sólo se habilita en los enlaces de red.
- La dirección IP para NTP, NMS y *Syslog* es la 192.168.100.253.

226. La configuración asociada es la siguiente:

```
! Chassis:
system name "OS6860"
system fips admin-state enable
! Capability Manager:
hash-control extended
! VLAN:
vlan 1 admin-state enable
vlan 100 admin-state enable
vlan 100 members port 1/1/25-26 untagged
! Spanning Tree:
spantree vlan 1 admin-state enable
spantree vlan 100 admin-state enable
! IP:
ip service port 21 admin-state disable
ip service port 23 admin-state disable
ip service port 80 admin-state disable
ip service port 123 admin-state disable
ip service port 443 admin-state disable
ip service port 3799 admin-state disable
ip interface emp address 192.168.254.1
ip interface "vlan1" address 192.168.1.254 mask 255.255.255.0 vlan 1
ip interface "vlan100" address 192.168.100.1 mask 255.255.255.0 vlan 100
ip dos type ping-overload admin-state enable
telnet admin-state disable
ftp admin-state disable
! AAA:
aaa authentication console "local"
aaa authentication snmp "local"
aaa authentication ssh "local"
user password-size min 9
user password-expiration 180
user password-policy min-uppercase 1
user password-policy min-lowercase 1
user password-policy min-digit 1
user password-policy min-nonalpha 1
! NTP:
ntp server 192.168.100.253 key 1
ntp client admin-state enable
! QOS:
qos user-port shutdown bpdu bgp ospf rip vrrp dhcp-server dvmrp isis dns-reply policy port
group UserPorts 1/1/1-24
policy condition mdc-dvmrp destination ip 224.0.0.4
policy condition mdc-ipv4mc-reserved destination ip 224.0.0.0 mask 255.255.255.0
policy condition mdc-ipv6mc-reserved destination ipv6 ff02:: mask ff:ff:ff:ff::
policy condition mdc-ospf-5 destination ip 224.0.0.5 ip-protocol 89
policy condition mdc-ospf-6 destination ip 224.0.0.6 ip-protocol 89
policy condition mdc-pim destination ip 224.0.0.13
```

policy condition mdc-ripv2 destination ip 224.0.0.9 destination udp-port 520 policy condition mdc-vrrp destination ip 224.0.0.18 ip-protocol 112
policy action accept
policy action q17 cpu priority 17
policy rule mdc-vrrp precedence 65070 condition mdc-vrrp action q17
policy rule mdc-ripv2 precedence 65060 condition mdc-ripv2 action q17
policy rule mdc-pim precedence 65050 condition mdc-pim action q17
policy rule mdc-ospf-6 precedence 65040 condition mdc-ospf-6 action accept policy rule mdc-ospf-5 precedence 65030 condition mdc-ospf-5 action accept policy rule mdc-dvmrp precedence 65020 condition mdc-dvmrp action q17
policy rule mdc-ipv6mc-reserved precedence 65010 condition mdc-ipv6mc-reserved -action q17
policy rule mdc-ipv4mc-reserved precedence 65000 condition mdc-ipv4mc-reserved action q17
qos apply
! LLDP:
lldp all chassis tlv management port-description enable system-name enable system-description enable
lldp all chassis tlv management management-address enable
lldp all port 1/1/1-24 lldpdu disable
! Session manager :
session prompt default "OS6860E->" command-log enable
! SNMP :
snmp security authentication all
snmp authentication-trap enable
snmp station 192.168.100.253 162 "snmp3" v3 enable
! Web:
webview server disable
webview access disable
! System Service:
swlog output socket 192.168.100.253
! VRRP:
ip load vrrp
! OSPF:
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "vlan1"
ip ospf interface "vlan1" area 0.0.0.0
ip ospf interface "vlan1" hello-interval 0
ip ospf interface "vlan1" admin-state enable
ip ospf interface "vlan100"
ip ospf interface "vlan100" area 0.0.0.0
ip ospf interface "vlan100" auth-type md5
ip ospf interface "vlan100" admin-state enable
ip ospf interface "vlan100" md5 1
ip ospf interface "vlan100" md5 1 key switch
ip ospf admin-state enable
! DA-UNP:
port-security port 1/1/1-24 maximum 2
port-security port 1/1/1-24 learn-trap-threshold 2
port-security port 1/1/1-24 admin-state enable
! DHCP Snooping:
dhcp-snooping admin-state enable
dhcp-snooping binding admin-state enable
dhcp-snooping ip-source-filter port 1/1/1-24 admin-state enable

dhcp-snooping port 1/1/25-26 trust

6. FASE DE OPERACIÓN Y MANTENIMIENTO

227. Durante la fase de operación de los dispositivos, los administradores de seguridad deberán llevar a cabo las siguientes tareas de mantenimiento:

a) Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.

b) Aplicación regular de parches de seguridad y actualizaciones del firmware del sistema, de cara a mantener su configuración segura.

c) Mantenimiento de registros de auditoria incluyendo los eventos del sistema. Estos registros estarán protegidos de borrado y modificación no autorizada y solamente el personal de seguridad autorizado podrá acceder a ella. La información de auditoría se guardará en las condiciones establecidas en la normativa de seguridad.

d) Auditoría de al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

e) Comprobación de que los ficheros de auditoria están protegidos del borrado y modificación no autorizada, incluso accidentales.

f) Control de acceso a la información de auditoria de forma que únicamente el personal de seguridad designado pueda acceder a ella.

g) Almacenamiento de la información de auditoria en las condiciones establecidas en la normativa de seguridad y por el período establecido.

6.1 ACTUALIZACIÓN Y PARCHES

228. Para la actualización de un conmutador Alcatel-Lucent OmniSwitch con AOS 8 a una determinada versión del sistema operativo, se recomienda la lectura detallada de las notas de la versión a la que se quiere actualizar. En este documento se indican los requisitos que debe cumplir el *switch* a actualizar.

229. En las notas de la versión se indican igualmente las versiones de *uboot/miniboot* y de FPGA que deben estar instaladas en el *switch* para poder soportar la versión del sistema operativo a la que se quiere actualizar.

230. En AOS 8 se soportan dos modos de actualización de los conmutadores:

a) Actualización estándar. Es el procedimiento indicado para conmutadores individuales, o para chasis virtual (pila) con actualización de todos los equipos a la vez. En el caso de un chasis virtual, antes de reiniciar el equipo, se copia la imagen cargada al resto de los equipos de la pila y se reinician todos a la vez.

b) Actualización ISSU (*In Service Software Upgrade*) en servicio, indicado para equipos en chasis o virtual chasis (pila), que minimiza o elimina los cortes de servicio. Con esta actualización se copia la imagen de software en todos los equipos de la pila o controladoras del chasis y se reinician secuencialmente en lugar de todos al mismo tiempo.

231. Se describen en los siguientes apartados los dos modos de actualización.

6.1.1 ACTUALIZACIÓN ESTÁNDAR

232. Para la actualización estándar de AOS se han de seguir los pasos indicados a continuación y en el orden indicados:

a) Descargar los ficheros de actualización correspondientes al modelo de conmutador que se quiere actualizar de la web de soporte de Alcatel-Lucent Enterprise.

b) Cargar los ficheros de actualización en el directorio "*Running*" del switch que se quiere actualizar. Para ello se usa SFTP. El nombre del directorio Running y los ficheros pueden variar dependiendo de la configuración y el modelo de switch.

c) Actualizar la imagen de software. Para ello se introduce el comando de reinicio del switch y se confirma, según se indica a continuación:

```
-> reload from working no rollback-timeout
Confirm Activate (Y/N) : y
This operation will verify and copy images before reloading.
It may take several minutes to complete....
```

Si se actualiza un chasis virtual (una pila), la imagen se copia en todos los switches tipo *slave* del virtual chasis y todos ellos se reinician al mismo tiempo.

d) Verificar que la actualización se ha hecho correctamente. Se hace mediante los siguientes comandos:

```
-> show microcode
/flash/working
Package          Release     Size          Description
---------+--------------+------------+--------------
Tos.img          8.6.189.R02          210697424          Alcatel-Lucent OS
-> show running-directory
CONFIGURATION STATUS
Running CMM : MASTER-PRIMARY,
CMM Mode : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot : CHASSIS-1 A,
Running configuration : WORKING,
Certify/Restore Status : CERTIFY NEEDED
SYNCHRONIZATION STATUS
```

Running Configuration : SYNCHRONIZED

e) En caso de encontrar problemas tras la actualización del switch o chasis virtual, se puede volver a la versión anterior mediante el comando:

-> reload from certified no rollback-timeout

f) Certificar el software cargado. Una vez que se ha verificado que la nueva imagen funciona correctamente, se copia dicha imagen al directorio *"Certified"*. Esto se hace mediante el siguiente comando:

-> copy running certified

-> show running-directory

CONFIGURATION STATUS

Running CMM : MASTER-PRIMARY,

CMM Mode : VIRTUAL-CHASSIS MONO CMM,

Current CMM Slot : CHASSIS-1 A,

Running configuration : WORKING,

Certify/Restore Status : ***CERTIFIED***

SYNCHRONIZATION STATUS

Running Configuration : SYNCHRONIZED

6.1.2 ACTUALIZACIÓN ISSU

233. La actualización en servicio de software (ISSU o In Service Software *Upgrade* por sus siglas en inglés) de AOS es aplicable a un chasis virtual de OmniSwitch o a los equipos chasis modulares.

234. Este modo de actualización permite la actualización del software de los equipos de forma que no se vean afectados los servicios que están soportando los *switches*. Para que realmente no haya impacto en el servicio se requiere que los elementos de red que agregan tráfico sobre la pila tengan igualmente agregados de enlaces de red redundados con los puertos de los agregados en los diferentes *switches* del chasis virtual.

235. En las notas de la versión a la que se va a actualizar se indican las versiones de software instaladas que permiten actualización ISSU. Si la versión instalada no soporta ISSU, hay que hacer la actualización estándar.

236. Para la actualización ISSU de AOS se han de seguir los pasos indicados a continuación y en el orden indicados:

a) Descargar los ficheros de actualización correspondientes al modelo de conmutador que se quiere actualizar de la web de soporte de Alcatel-Lucent Enterprise. Existe un paquete específico para la actualización ISSU.

b) Crear un nuevo directorio en el switch master del chasis virtual para la actualización ISSU:

-> mkdir /flash/issu_dir

c) Borrar cualquier otro directorio ISSU que se pudiera haber creado con anterioridad en los equipos del chasis virtual. Para ello hay que conectarse a cada uno de los equipos del chasis virtual y borrar los directorios en caso de que hubiera:

-> rm –r /flash/issu_dir

d) Copiar todos los ficheros de configuración (.cfg) existentes en el directorio "*Running*" en el nuevo directorio *issu_dir*:

-> cp /flash/working/*.cfg /flash/issu_dir

e) Cargar los ficheros de actualización en el directorio "*issu_dir"* del *switch* que se quiere actualizar. Para ello se usa SFTP. El nombre del directorio *Running* y los ficheros pueden variar dependiendo de la configuración y el modelo de *switch*.

f) Actualizar la imagen de software. Para ello se introduce el comando de ISSU del *switch* y se confirma, según se indica a continuación:

-> issu from issu_dir

Are you sure you want an In Service System Upgrade? (Y/N) : y

Como se puede ver, el comando permite lanzar el proceso ISSU desde cualquier directorio creado en la flash del equipo master del chasis virtual.

Durante el proceso ISSU se van copiando los ficheros a los equipos slave del chasis virtual. Estos equipos se van reiniciando uno a uno. Mientras no se ha actualizado uno no empieza el siguiente. Por último, se reinicia el que actúa como master del chasis virtual.

Durante la actualización se puede ver el estado del proceso mediante el siguiente comando:

-> show issu status

Issu pending

Cuando el proceso ha finalizado se indica de la siguiente manera:

-> show issu status

Issu not active

g) Verificar que la actualización se ha hecho correctamente. Se hace mediante los siguientes comandos:

-> show microcode

/flash/working

Package	*Release*	*Size*	*Description*
Tos.img	*8.6.189.R02*	*210697424*	*Alcatel-Lucent OS*

-> show running-directory

CONFIGURATION STATUS

Running CMM : MASTER-PRIMARY,

CMM Mode : VIRTUAL-CHASSIS MONO CMM,

Current CMM Slot : CHASSIS-1 A,

Running configuration : WORKING,

Certify/Restore Status : ***CERTIFY NEEDED***

SYNCHRONIZATION STATUS

Running Configuration : SYNCHRONIZED

h) Certificar el software cargado. Una vez que se ha verificado que la nueva imagen funciona correctamente, se copia dicha imagen al directorio *"Certified"*. Esto se hace mediante el siguiente comando:

-> copy running certified

-> show running-directory

CONFIGURATION STATUS

Running CMM : MASTER-PRIMARY,

CMM Mode : VIRTUAL-CHASSIS MONO CMM,

Current CMM Slot : CHASSIS-1 A,

Running configuration : WORKING,

Certify/Restore Status : ***CERTIFIED***

SYNCHRONIZATION STATUS

Running Configuration : SYNCHRONIZED

7. REFERENCIAS

STIC.1 CCN-STIC-807 Criptología de empleo en el ENS.

STIC.2 Manual configuración segura en OMNISWITCH AOS v0.1

STIC.3 OmniSwitch AOS *Release 8 Switch Management Guide*

STIC.4 OmniSwitch AOS *Release 8 CLI Reference Guide*

STIC.5 OmniSwitch AOS *Release 8 Network Configuration Guide*

STIC.6 OmniSwitch AOS *Release 8 Advanced Routing Configuration Guide*

8. ABREVIATURAS

AES	*Advanced Encription Standard*
AOS	*ALE Operating System*
ARP	*Address Resolution Protocol*
ASA	*Acceso Autenticado al Switch*
BFD	*Bidirectional Forwarding Detection*
BGP	*Border Gateway Protocol*
BUM	*Broadcast, Unknown unicast y Multicast*
CAM	Conditional Access Memory
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación*
DAI	*Dynamic ARP Inspection*
DPP	*Dispositivo de Protección de Perímetro*
ENS	*Esquema Nacional de Seguridad*
FTP	*File Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
ISSU	*In Service Software Upgrade*
LPS	*Learned Port Security*
LLDP	*Link Layer Discovery Protocol*
MVRP	*Multiple VLAN Registration Protocol*
OSPF	*Open Shortest Path First*
RSA	*Rivest, Shamir y Adleman*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
STP	*Spanning Tree Protocol*
TCAM	*Ternary Content Addressable Memory*
VSA	*Vendor Specific Atributes*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL