centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1429

Procedimiento de empleo seguro
DELL EMC Networking

Marzo 2022

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA 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
2022.03.25 09:24:23 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-113-9

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 4
2. OBJETO Y ALCANCE 5
3. ORGANIZACIÓN DEL DOCUMENTO 6
4. FASE PREVIA A LA INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.2 DESCARGA DE SOFTWARE E INSTALACIÓN DE LICENCIA 7
4.3 CONSIDERACIONES PREVIAS 8
5. FASE DE CONFIGURACIÓN 9
5.1 ORGANIZACIÓN DE LA INTERFAZ DE COMANDOS 9
5.2 MODO DE OPERACIÓN SEGURO 10
5.2.1 HABILITACIÓN MODO FIPS 10
5.2.2 HABILITACIÓN MODO SECURE-CLI 11
5.3 AUTENTICACIÓN 11
5.3.1 MÉTODOS DE AUTENTICACIÓN 11
5.4 GESTIÓN DE USUARIOS 13
5.4.1 REGLAS PARA LA DEFINICIÓN DE ROLES 15
5.5 SEGURIDAD EN EL ACCESO A LA ADMINISTRACIÓN 16
5.5.1 GESTIÓN LOCAL DEL EQUIPO 16
5.5.2 GESTIÓN REMOTA DEL EQUIPO 18
5.6 GESTIÓN DE CERTIFICADOS 24
5.6.1 CREACIÓN DE UN CSR 24
5.6.2 INSTALACIÓN DE CERTIFICADOS 24
5.6.3 CREACIÓN DE SECURITY PROFILES 24
5.7 ACTUALIZACIÓN DEL SOFTWARE DEL DISPOSITIVO 25
5.7.1 VERSIÓN DE SOFTWARE INSTALADA 25
5.7.2 GUARDAR CONFIGURACIÓN ACTUAL 26
5.7.3 ACTUALIZACIÓN DEL SISTEMA 26
5.8 AUDITORIA 27
5.8.1 SYSLOG 28
5.9 POLÍTICAS DE CALIDAD DE CONTRASEÑAS 28
5.9.1 ALMACENAMIENTO DE CONTRASEÑAS 29
5.9.2 CONFIGURACIÓN DE FÁBRICA Y RECUPERACIÓN DE CONTRASEÑAS 30
5.10 AUTO CHEQUEOS 31
5.11 SERVICIOS DE RED DEL EQUIPO 31
5.11.1 LLDP 31
5.11.2 ICMP 32
5.11.3 TRANSFERENCIA DE FICHEROS 33
5.11.4 SINCRONIZACIÓN DE TIEMPO 33
5.12 CONTROL DE TRÁFICO Y SEGURIDAD EN LOS PUERTOS DE RED 34
5.12.1 APAGADO DE PUERTOS 35
5.12.2 MEDIDAS DE PROTECCIÓN DE PUERTOS 35

5.12.3 CONTROL DEL TRÁFICO 36
5.12.4 USO DE VLAN COMO MEDIDA DE AISLAMIENTO 37
5.12.5 VLAN PRIVADAS 39
5.12.6 PROTECCIÓN FRENTE A ENVÍO DE MENSAJES DE CONTROL STP 41
5.12.7 LISTAS DE ACCESO IP 43
5.12.8 LISTAS DE ACCESO MAC 47
5.13 PROTECCIÓN FRENTE ATAQUES 48
5.13.1 DHCP SNOOPING 48
5.13.2 ARP SNOOPING 49
5.13.3 INUNDACIÓN MAC 50
6. FASE DE OPERACIÓN 53
7. CHECKLIST 54
8. REFERENCIAS 56
9. ABREVIATURAS 57

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura de la familia de equipos Dell EMC con sistema operativo **Dell EMC Networking SmartFabric OS 10.5**.
2. A lo largo de los diferentes capítulos, se ofrecen consejos y recomendaciones sobre la activación o desactivación de servicios y funcionalidades de los equipos de red con el fin de establecer una configuración lo más segura posible.
3. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. El lector puede utilizar el índice de contenidos para localizar y acceder al capítulo que trate el aspecto sobre el que desea mejorar la seguridad. Sin embargo, se recomienda realizar lectura rápida del documento completo para hacerse una idea de todas las funcionalidades descritas.

2. OBJETO Y ALCANCE

4. El presente documento tiene como objetivo detallar las configuraciones de seguridad de los Switches con el sistema operativo **Dell EMC Networking SmartFabric OS 10.5**, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.
5. Las configuraciones indicadas aplican a los siguientes modelos *hardware*: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128FON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON.
6. En el ámbito de este documento, se asume que existirá un usuario de nivel administrador que podrá configurar todas las funcionalidades requeridas, incluidas las definiciones de usuarios locales.

3. ORGANIZACIÓN DEL DOCUMENTO

7. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

   a) **Apartado 4**. En este apartado se recogen aspectos y recomendaciones a considerar durante el despliegue e instalación del producto.

   b) **Apartado 5.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) **Apartado 7.** En este apartado se incluye un breve *checklist* de acciones de configuración del producto.

   e) **Apartado 8.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

   f) **Apartado 9.** Incluye un listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El producto se recibirá en forma de *appliance* físico. Al recibir el equipo deben verificarse los siguientes aspectos:
   a) El embalaje es original y no ha sido manipulado su sellado.
   b) El equipo no debe presentar señales de haber sido manipulado o abierto.
   c) Debe validarse que el número de matrícula del equipo (*Service tag*) se corresponde con el que se encuentra en el albarán de recepción del equipo y en la factura del mismo.
9. Ante cualquier duda se recomienda ponerse en contacto con el servicio de soporte *Dell Pro Support* a través de los datos de contacto proporcionados junto con el equipo.
10. Se debe verificar que el sistema operativo instalado, en caso de haberse solicitado el equipo con el sistema preinstalado, se corresponde con el solicitado y es el original proporcionado por *Dell Technologies*. Para ello, se debe ejecutar el comando "*show version*", que mostrará la versión del sistema operativo instalado (ver apartado 5.7.1 VERSIÓN DE SOFTWARE INSTALADA).
11. En caso de solicitar el producto con el sistema operativo instalado, este dispondrá también de la licencia de uso pre-cargada.

4.2 DESCARGA DE SOFTWARE E INSTALACIÓN DE LICENCIA

12. En caso de que el *appliance* se reciba sin el software instalado, o la versión no corresponda con Dell EMC Networking SmartFabric OS 10.5, se deberá descargar e instalar el sistema operativo.
13. Para ello, se deberán seguir los siguientes pasos:
   a) Acceder al repositorio *Dell Digital Locker*.
   b) Localizar el pedido, enviado por correo electrónico, y seleccionar el nombre de producto.
   c) En la página *Product*, el campo *Assigned to* se encontrará vacío. Hacer clic en *Key Available for Download*.
   d) Introducir la etiqueta de dispositivo en los campos *Bind to* y *Re-Enter ID*. De esta forma el software quedará asignado al dispositivo físico.
   e) Seleccionar cómo se desea recibir la licencia: por correo o descargándola localmente. Hacer clic en *Submit*.
   f) En la pestaña *Available Downloads*, seleccionar la versión del software y hacer clic en *Download*.
   g) Leer el acuerdo y hacer clic en *Yes, I agree*.

h) Hacer clic en *Download Now* para obtener el software. Almacenarlo en un servidor local.

14. Tras la descarga, para verificar la autenticidad e integridad del fichero, se debe realizar su hash SHA-256 y verificar que coincide con el indicado en la página de descarga.

15. Una vez verificado el fichero, importarlo al *appliance* desde el servidor local haciendo uso de SCP. Para llevar a cabo la instalación, seguir los siguientes pasos:

    a) Arrancar el dispositivo, acceder al menú de arranque y seleccionar *ONIE Rescue*.

    b) Parar el descubrimiento DHCP: *onie-discovery-stop*.

    c) Configurar la dirección IP del dispositivo: *ifconfig eth0 X.X.X.X netmask 255.255.0.0 up*.

    d) Instalar el software: *onie-nos-install scp://a.b.c.d/ficero_instalación.bin*

16. Por último, deberá importarse la licencia de uso. Tal como se ha visto, durante la descarga del sistema operativo se obtiene también la licencia, esta se recibe en formato .zip. Abrir el fichero y extraer la licencia, después utilizar el siguiente comando para instalarla utilizando SCP: *license install scp://userid:password@hostip/filepath*.

4.3 CONSIDERACIONES PREVIAS

17. A través del puerto de consola serie se puede acceder a la configuración. Asimismo, en cuanto uno de los puertos de datos se conecte a una red que le proporcione una dirección IP por DHCP, la gestión del conmutador estará también accesible por telnet o SSH sin ningún control de acceso.

18. Por ello, **es imprescindible asegurar la configuración del equipo en un entorno seguro y aislado antes de desplegarlo en la red**. Como mínimo, se deberán asignar claves de acceso a los usuarios de administración, desactivar todos los servicios que no se vayan a utilizar o que no presenten la seguridad adecuada, asegurar los servicios que queden activos y deshabilitar todos los interfaces de red que no se vayan a utilizar, todo ello siguiendo las recomendaciones que aparecen en los subapartados posteriores de esta guía.

19. Es muy importante mantener el software del equipo actualizado a las últimas versiones publicadas, con el fin de incorporar todas las correcciones de seguridad incorporadas al software por el fabricante

5. FASE DE CONFIGURACIÓN

5.1 ORGANIZACIÓN DE LA INTERFAZ DE COMANDOS

20. Los equipos Dell EMC con sistema Dell SmartFabric OS 10.5 son equipos completamente gestionables, permitiendo al administrador de red configurar el equipo mediante la línea de comandos e interfaz gráfico.
21. El interfaz gráfico (GUI) ofrece sólo un conjunto reducido de opciones básicas de configuración de puertos y enlaces, dado que tiene por objeto la monitorización y resolución de incidencias. Por esta razón esta guía se centra en la configuración segura del equipo **vía el interfaz de línea de comandos**.
22. El acceso a la línea de comandos (CLI) es posible mediante la conexión directa a la consola (puerto serie), o bien mediante el acceso remoto vía red IP utilizando SSH.
23. El CLI está estructurado en diferentes modos de acuerdo con propósitos de seguridad y gestión. Así pues, la línea de comandos está dividida principalmente en tres niveles con su *prompt* específico de la línea de comandos:

    a) **Modo EXEC**: es el modo por defecto. Tan sólo permite una selección limitada de comandos, en concreto comandos *show* para visualizar información del sistema. El *prompt* está formado por el nombre del equipo seguido de "**>**".

    b) **Modo EXEC Privilege**: permite el control del equipo y todas las acciones administrativas, así como las acciones de actualización de software, tareas de diagnóstico o habilitar/deshabilitar operaciones de *debug*. El *prompt* está formado por el nombre del equipo seguido de "**#**". Desde el modo EXEC se puede acceder a este modo ejecutando el comando "**enable**". Desde otro modo, se puede acceder a través del comando "**end**".

    c) **Modo Configuración**: Permite la modificación de la configuración del equipo. Se accede a este modo mediante la ejecución del comando "**configure**". Es imprescindible acceder desde el modo EXEC Privilege. El prompt está formado por el nombre del equipo seguido de "**(conf)#**". La pulsación del carácter "?" ofrece al administrador la lista de opciones posibles de configuración. Desde otro modo se puede acceder con el comando "**exit**".

        - **Sub-modos de Configuración específica**. Permite la configuración particular de un aspecto específico. Algunos ejemplos son la configuración de interfaces de red, VLANs, ACL, OSPF, etc. El prompt está formado por el nombre del equipo seguido de "**(xxxxx) #**", donde xxxx adopta un literal que describe el contexto en concreto en el que se encuentra el usuario. La pulsación del carácter "?" ofrece al administrador la lista de opciones posibles de configuración específicas de este contexto, junto con algunos comandos generales.

Modo	Prompt	Acceso
EXEC	OS10>	Acceso por consola o terminal line

EXEC Privilege	OS10#	Acceso desde modo EXEC con el comando *enable*. Desde otro modo, usando comando *end*
Configuración	OS10(conf)#	Acceso desde modo EXEC Privilege con el comando *configure*. Desde otro modo (excepto EXEC y EXEC Privilege), usando comando *exit*

24. Para cerrar una sesión CLI, ya sea por consola o remotamente, usar el comando "exit" desde modo *EXEC* o *EXEC Privilege*.

25. Casi todos los comandos de configuración tienen una forma "*no*", que se utiliza normalmente para desactivar esa función. En ocasiones, desactivar una función requiere especificar además los parámetros originales que la activaban. Por ejemplo:

```
OS10# no username NombreUsuario
```

26. El comando "*copy running-config startup config*" guarda la configuración del equipo en el fichero de configuración de arranque.

```
OS10# copy running-configuration startup configuration
```

27. El comando "*show*" se utiliza para obtener información de configuración y estado del conmutador. Por ejemplo, para ver los *logs* de seguridad.

```
OS10# show logging log-file
```

5.2 MODO DE OPERACIÓN SEGURO

5.2.1 HABILITACIÓN MODO FIPS

28. El modo seguro del producto permite establecer una serie de configuraciones seguras predeterminadas. Para poder activar este modo en el equipo es necesario adquirir una licencia. Una vez activada la licencia FIPS en el equipo (ver apartado 4.2 DESCARGA DE SOFTWARE E INSTALACIÓN DE LICENCIA) se puede activar el modo seguro con el comando: ***crypto fips enable***

29. Una vez aplicado el cambio los comandos del sistema estarán restringidos a valores de configuración seguros, bloqueando cualquier configuración considerada insegura. Los detalles de esta modalidad se pueden consultar en la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

30. En este modo, el producto solo hará uso de:

    a) TLSv1.2 en todas las comunicaciones que hagan uso de TLS. Más concretamente, en el envío de log a un servidor externo de auditoría y las comunicaciones RADIUS.

    b) SSHv2 en todas las comunicaciones que hagan uso de SSH. Más concretamente, en la gestión remota del dispositivo.

31. **Se debe utilizar el producto en modo seguro.** Se puede verificar que el producto opera en modo seguro mediante el comando *show fips status*, se deberá obtener el mensaje *FIPS Mode: Enabled*.

5.2.2 HABILITACIÓN MODO SECURE-CLI

32. La habilitación del modo *secure-cli* evita que un usuario pueda elevar su nivel de privilegio dentro del contexto de la CLI. Es decir, un usuario nunca podrá realizar un comando de tipo "*enable*" para subir su nivel de privilegio, aunque este esté protegido por una contraseña. Así mismo aplicar la configuración *secure-cli* inhabilita a los usuarios cambiar la contraseña de *admin* del sistema, incluso aunque tengan nivel de privilegio suficiente para hacerlo.
33. La forma de habilitar este modo se realiza con el comando: ***secure-cli enable***
34. Se recomienda activar el modo *secure-cli*. En caso necesario, es posible deshabilitarlo con el comando: ***secure-cli disable***.

5.3 AUTENTICACIÓN

35. En los conmutadores Dell EMC la autenticación de usuarios puede ser local o remota. En el primer caso, los usuarios y sus credenciales de acceso se definen localmente en cada conmutador; en el segundo, la autenticación se realiza en servidores de autenticación externos de tipo RADIUS o TACACS.
36. El producto hace uso, por defecto, únicamente de la autenticación local. Se recomienda el uso de autenticación local para la gestión de los dispositivos.
37. Por defecto, y con el objeto de facilitar su puesta en marcha inicial, la configuración de fábrica de los conmutadores no incluye ninguna autenticación activa: cualquier persona con acceso físico a la consola puede acceder al sistema. Por ello, una de las primeras tareas será la definición de los usuarios con permisos de acceso al sistema y la configuración del acceso de consola para que solicite las credenciales de acceso.

5.3.1 MÉTODOS DE AUTENTICACIÓN

5.3.1.1 AUTENTICACIÓN LOCAL

38. En este caso los usuarios y sus credenciales son definidos y almacenados localmente en el conmutador. El único usuario inicialmente existente es *admin* con privilegios máximos para poder ejecutar comandos en los dos modos de privilegios definidos. Inicialmente dispone de la contraseña *admin* por defecto, por lo que una de las primeras tareas a realizar debe ser la protección de esas cuentas con una contraseña.
39. Para asignar una contraseña, se puede utilizar el comando:

```
OS10(conf)# username name password [role role-name] [privilege level level]
```

40. El modo EXEC Privilege no está restringido por defecto, así pues, también se aconseja configurar una contraseña para acceder desde el modo EXEC.

```
OS10(conf)# enable password encryption-type {0 cleartext-password | sha-256 | sha-512} contraseña
priv-lvl nivel
```

41. El tipo de cifrado es 0 por defecto si se usa texto plano, sha-256 si la contraseña está cifrada usando *sha256* y sha-512 si la contraseña está cifrada utilizando *sha512*. **Se debe utilizar sha256 o sha512**.

42. La autenticación local se puede utilizar también como método secundario o de respaldo a la autenticación remota. Por ejemplo, en el caso de que la autenticación se realice mediante un servidor RADIUS externo y el equipo no alcance ninguno de los servidores RADIUS configurados, si la autenticación local se ha configurado como método de respaldo, se haría uso de los dos usuarios para controlar el acceso a la administración del equipo. La autenticación local está disponible por defecto, salvo que se deshabilite explícitamente con el comando:

```
OS10(conf)# no aaa authentication login default local
```

5.3.1.2 AUTENTICACIÓN MEDIANTE SERVIDORES EXTERNOS

43. En este caso los usuarios y sus credenciales se definen y almacenan en un servidor RADIUS o TACACS+ externo, que permite centralizar la administración de los usuarios que acceden a la configuración de los equipos. De esta forma, las altas y bajas de usuarios, así como los cambios de credenciales, se pueden realizar sin necesidad de cambios en la configuración del producto.

44. Como se ha mencionado, es frecuente y en muchos casos recomendable seleccionar el método de autenticación local como método de respaldo, incluyéndolo en la lista de métodos de autenticación, tal como se verá posteriormente. De esta forma, si el equipo no tiene conectividad con los servidores de autenticación puede aún ser gestionado.

45. Se puede configurar un método de autenticación en el *login* mediante el comando "*aaa authentication login*". Para ello utilizar el siguiente comando:

```
OS10(conf)# aaa authentication login {console | default} {local | group radius | group tacacs+}
```

    a) *Console*. Configura los métodos de autenticación para los accesos locales por consola.

    b) *Default*. Configura los métodos de autenticación para los accesos remotos mediante SSH y Telnet.

46. En caso de configurar más de un método, se utilizará el segundo método como respaldo. Por ejemplo, si no se puede conectar con un servidor RADIUS, se realiza la autenticación local. Si el servidor RADIUS deniega el acceso, la sesión termina. Por ejemplo:

```
OS10(conf)# aaa authentication login default radius local
```

47. Una vez configurado el tipo de autenticación, el producto hará uso del servidor o servidores configurados. En caso de configurar más de un servidor del mismo tipo, se tratará de conectar con el primer servidor configurado y en caso de no lograr la conexión, se pasará al siguiente.

48. Para configurar un servidor RADIUS, haciendo uso de TLSv1.2:

```
OS10(conf)# radius-server host {hostname | ip-address} tls security-profile key {0
authentication-key | 9 authentication-key | authentication-key} [auth-port port-number]
```

a) auth-*port port-number*: el rango es de 0 a 65535. Se debe especificar un Puerto UDP. Por defecto es el 1812.

b) *key [encryption-type] key*: 0 para texto plano o bien 9 para texto cifrado con sha-256, y una cadena de caracteres para la clave. Dicha clave puede tener como máximo 42 caracteres de largo y debe coincidir con la clave configurada en el servidor RADIUS. Se debe hacer uso de claves cifradas.

c) *Security-profile*. Define el certificado utilizado por el producto para la autenticación TLS con el servidor RADIUS. Ver apartado 5.6.3 CREACIÓN DE SECURITY PROFILES.

49. Para configurar los parámetros de conexión de RADIUS:

a) En caso de no recibir respuesta del servidor, se puede configurar el número de veces que se reenviará la petición: *radius-server retransmit num_retries.*

b) Para configurar el tiempo de espera a una respuesta, el valor por defecto es 5 segundos: *redius-server timeout seconds*.

50. Para configurar un servidor TACACS+:

```
OS10(conf)# tacacs-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
```

a) *Auth-port port-number:* el rango es de 0 a 65535. Hay que especificar un Puerto TCP. Por defecto es el 49.

b) *key [encryption-type] key*: 0 para texto plano o bien 9 para texto cifrado con sha-256, y una cadena de caracteres para la clave. Dicha clave puede tener como máximo 42 caracteres de largo y debe coincidir con la clave configurada en el servidor TACACS+. Se debe hacer uso de claves cifradas.

51. Para más información sobre RADIUS puede consultarse el capítulo "*AAA*" de la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

5.4 GESTIÓN DE USUARIOS

52. El producto dispone por defecto del usuario *admin* únicamente. Se pueden crear nuevos usuarios y asignarles roles mediante el comando:

```
OS10(conf)# username name password password role role [priv-lvl privilege-level]
```

53. Por defecto, se incluyen definidos 4 roles de usuario de sistema. Hay que destacar que estos roles no se pueden eliminar:

a) ***Operador de Red* (*netoperator*)**: Tiene acceso para ver la configuración del dispositivo, pero no puede realizar cambios. Tiene un nivel de privilegio por defecto de 1.

b) **Administrador de Red (*netadmin*)**: tiene acceso completo a los comandos de configuración del tráfico del switch, como las interfaces o ACLs. Tiene un nivel de privilegio por defecto de 15.

c) **Administrador de Seguridad (*secadmin*)**: Tiene acceso completo a los comandos de configuración de las políticas de seguridad y acceso al sistema, como la política de contraseñas, AAA o claves criptográficas. Puede ver información de seguridad, como logs de auditoría o estadísticas de acceso al sistema. Tiene un nivel de privilegio por defecto de 15.

d) **Administrador de Sistema (*sysadmin*)**: este rol tiene acceso exclusivo a los comandos utilizados para manipular el sistema de ficheros y acceder al Shell. Puede crear usuarios y roles. Tiene un nivel de privilegio por defecto de 15.

54. El producto consta de los niveles de privilegio entre 0 y 15. De forma que un usuario puede ejecutar comandos que están en su nivel de privilegio o inferior. Por defecto el nivel de privilegio al crear usuarios depende del rol, tal como se indica anteriormente.

55. Por defecto, para todos los comandos de configuración el nivel necesario es 15 y para los comandos de tipo *show* es 1. Por tanto, un usuario debe tener nivel de privilegio 15 para poder modificar configuraciones del sistema, bajo la configuración por defecto del dispositivo.

56. Los permisos de los usuarios vienen determinados por la combinación de dos parámetros:

    a) Rol de usuario. El rol determina el conjunto total de tareas que puede realizar el usuario.

    b) Nivel de privilegios. El nivel de privilegio restringe, dentro de dicho conjunto, qué comandos puede utilizar el usuario.

57. De tal forma que el nivel de privilegios puede limitar de forma adicional los permisos de un usuario, pero son los roles quienes indican las tareas que pueden realizar. Por ejemplo, un usuario con rol *netadmin*, aunque tenga nivel de privilegios 15, no podrá crear políticas de seguridad (correspondiente a *secadmin*). Por otra parte, un usuario *netadmin*, al que se reduzca el nivel de privilegios, podrá ver la configuración de ACLs pero no modificarlas.

58. Se puede modificar el nivel de privilegio necesario para poder ejecutar un comando mediante:

```
OS10(conf)# privilege mode {level Level command | reset command}
```

59. Los roles definidos en un equipo pueden consultarse con el comando. En el siguiente apartado se india como crear y modificar los roles.

```
OS10# show users
```

60. Los permisos asignados a un comando pueden consultarse con el siguiente comando, cuya salida muestra el rol de usuario y el nivel de permiso:

```
OS10# show role mode ?
configure              Global configuration mode
exec                   Exec mode
interface              Interface configuration mode
line                   Line configuration mode
route-map              Route map configuration mode
```

5.4.1 REGLAS PARA LA DEFINICIÓN DE ROLES

61. Para crear un nuevo rol de usuario y verificar que éste ha heredado los permisos de seguridad de administrador, usamos los siguientes comandos:

```
OS10(conf)# userrole {default | name} inherit existing-role-name
```

```
OS10# show users
Index Line    User    Role     Application Idle Login-Time            Location          Privilege
----- ------ ------ ------  ----------- ---- --------------------- -------------     ---------
1      pts/0 admin  sysadmin bash        >24h 2018-05-23 T23:05:03Z 10.14.1.91 [ssh] 15
2      pts/1 netad  netadmin bash        >24h 2018-05-30 T20:04:27Z 10.14.1.214[ssh] 10
```

a) *existing-role-name*: es uno de los 4 roles predefinidos.

62. Los permisos de un rol pueden ser modificados usando el comando “role mode mode { { { addrole | deleterole } role-name } | reset } command”.

63. Los parámetros a introducir son:

a) *mode*: debe elegirse entre categorías de comandos configure, exec, interface, line, route-map y router.

b) *addrole/deleterole*: para indicar si estamos añadiendo o quitando permisos a un rol sobre cierto comando.

c) *role-name*: el rol sobre el que estamos actuando.

d) *reset*: nos permite poner los permisos de roles de un comando a su valor por defecto

e) *command*: el comando concreto sobre el que actuamos para asignar privilegios de ejecución a un rol.

64. Vemos un ejemplo a continuación: ***role mode configure addrole netoperator command username***

65. Este comando otorga privilegios de ejecución del comando de configuración *username* al rol *netoperator*. Por defecto, este comando *username* solo está disponible para el rol *sysadmin*.

66. Es importante resaltar que la asignación de roles se debe hacer durante el proceso de creación del usuario, si se desea modificar a posteriori debe primero eliminarse el usuario y volverse a crear con el rol adecuado.

67. También es posible crear roles nuevos en el sistema a partir de los roles existentes mediante el comando: ***userrole name inherit existing-role-name***

68. Teniendo en cuenta los roles básicos definidos por defecto en el sistema, es posible crear hasta 4 roles adicionales.

69. Para eliminarlos, basta con escribir "*no*" delante del comando "*userrole*".

5.5 SEGURIDAD EN EL ACCESO A LA ADMINISTRACIÓN

70. Es imprescindible prevenir que usuarios no autorizados puedan acceder a los equipos y visualizar o cambiar la información de configuración almacenada en ellos. Es necesario, por lo tanto, implementar medidas de seguridad que impidan esos accesos no deseados, tanto de aquellos usuarios que intenten acceder a nuestros equipos desde dentro o fuera de nuestra red a través de los interfaces de datos, como de los que traten de hacerlo por medio del acceso físico al equipo y la conexión a los puertos de consola.

5.5.1 GESTIÓN LOCAL DEL EQUIPO

5.5.1.1 PUERTO DE CONSOLA

71. Los equipos están dotados de un puerto de consola serie con conector RJ45 que permite el acceso a todas las funcionalidades de gestión del Sistema Operativo (otras formas de acceso como el interfaz web sólo permiten el acceso parcial), así como a las funcionalidades ofrecidas por el *software* de arranque del equipo.

72. Algunas funciones, como la recuperación de las credenciales del equipo (procedimiento de *password recovery*) sólo están disponibles desde el puerto de consola.

73. El uso del puerto de consola requiere proximidad física al equipo, con el objeto de conectar un terminal serie al mismo, aunque también es posible acceder remotamente a la consola si se utiliza un servidor de terminales (equipo que permite el acceso remoto a una o varias líneas serie a través de redes IP).

74. Como se ha mencionado, en el estado inicial de fábrica del equipo, la consola permite el acceso total a la gestión. Por tanto, la primera tarea a realizar debe ser la de configurar un usuario del sistema y protegerlo con contraseña:

```
OS10(conf)# username name password password role role [priv-lvl privilege-level]
```

75. Desde el momento en que se ejecuta este comando, el conmutador activa el control de acceso a la gestión del equipo y sólo se permite el acceso con las credenciales.

76. Igualmente es necesario configurar una contraseña de *enable* como una medida básica de control de seguridad para el modo *EXEC Privilege* desde el modo *EXEC*. Por defecto el modo *EXEC Privilege* se encuentra sin restringir.

77. El comando para crear esta contraseña de *enable* es el siguiente:

```
OS10(conf)# enable password encryption-type password-string priv-lvl privilege-level
```

a) *encryption-type*: especifica el modo de introducir la contraseña. Por defecto el valor es 0 para indicar que es texto plano. Si el valor es sha-256, se indica que está cifrada con un algoritmo de SHA-256. Y si el valor es de sha-512, se indica que se usa un algoritmo de cifrado SHA-512. Se debe usar SHA-256 o SHA-512.

b) *Priv-lvl.* Determina el nivel de privilegio al cual afecta la contraseña. Se recomienda utilizar el nivel 15 para restringir el uso de todos los comandos del sistema.

78. Por otro lado, es importante evitar que las sesiones establecidas, ya sea por consola o por SSH o Telnet se queden abiertas y puedan ser utilizadas con fines espurios. Por ello, es importante cerrar siempre las sesiones de gestión utilizando el comando "*exit*", así como fijar un periodo máximo de inactividad para las sesiones, de forma que éstas se cierren automáticamente transcurrido ese periodo de inactividad.

79. Para fijar el periodo de inactividad en segundos se utiliza el comando, se recomienda un valor de 5 minutos:

```
OS10(conf)# exec-timeout timeout-value
```

80. El valor de timeout-value expresará un valor en segundos durante la que la sesión estará activa. Para cancelar se usará:

```
OS10(conf)# no exec-timeout timeout-value
```

81. El comando anterior no solo afecta a las sesiones de consola, sino también a las sesiones SSH y TELNET. Se puede especificar también un periodo de inactividad para los terminales de línea virtuales (vty) a los que se puede acceder remotamente a través de SSH. En el ejemplo, las líneas vty de 0 a 9 con un periodo de 5 minutos y 0 segundos.

```
OS10(conf)# line vty 0 9
OS10(config-line-vty)# exec-timeout 5 0
```

82. Adicionalmente, se recomienda configurar un mensaje de bienvenida (*banner*) que indique que el acceso no autorizado a este equipo está prohibido. Dicho texto no debe proporcionar ninguna información acerca del sistema accedido que pueda ser utilizada por un atacante.

83. Para configurar el banner se utiliza el comando:

```
OS10(conf)# banner motd <delimitador> TEXTO <caracter-delimitador>
```

84. El carácter delimitador se utiliza para permitir introducir mensajes compuestos por múltiples líneas. No puede ser usado en el texto introducido. Una vez introducido el mensaje, los saltos de línea aparecen como "\n" al mostrar la configuración (*show running-config*).

85. Por ejemplo, usando el carácter % como delimitador:

```
OS10(conf)# banner motd %
Este es un sistema privado. Abandone la conexión si no tiene autorización
```

```
%
```

86. En la configuración aparecerá como:

```
banner motd "Este es un sistema privado. \n Abandone la conexión si no tiene
autorización\n\n"
```

87. Al igual que el valor del tiempo de inactividad, el mensaje de bienvenida aplica también a las sesiones establecidas por TELNET y SSH descritas más adelante.

88. Asimismo, conviene asignar un nombre al equipo mediante el comando "*hostname*".

89. Por ejemplo:

```
OS10(conf)#   hostname   dellsw
dellsw(conf)#
```

5.5.1.2 PUERTO USB

90. En los modelos que tienen un puerto USB tipo A (distinto de los puertos USB micro-B de consola), este puede ser usado como medio de almacenamiento para desplegar, analizar y copiar configuraciones o versiones del software.

91. Como regla general, se recomienda mantener deshabilitado el puerto USB, activándolo cuando su uso sea necesario y desactivándolo a posteriori una vez usado. Para deshabilitarlo utilizar el siguiente comando:

```
OS10(conf)# unmount usb
```

5.5.2 GESTIÓN REMOTA DEL EQUIPO

92. El equipo puede ser gestionado mediante una conexión remota a través de los puertos Ethernet que dispone. A través de protocolos basados en la arquitectura TCP/IP como Telnet, SSH y a través de una API se puede acceder a la configuración del equipo y a la obtención de información de configuración y rendimiento de éste. Solo se recomienda la gestión remota mediante SSH, el resto de protocolos se deshabilitarán, tal como se ve posteriormente.

93. En los siguientes apartados se verán más en detalle los requisitos para el acceso remoto a la gestión, así como los distintos servicios disponibles y las recomendaciones a seguir para no poner en riesgo la seguridad del equipo.

5.5.2.1 REQUISITOS Y RECOMENDACIONES INICIALES

94. Para acceder remotamente al sistema, hay que asignar una dirección IP a los puertos de gestión. Para ello se seguirán los siguientes pasos:

```
OS10(conf)# interface ManagementEthernet slot/port
OS10(config-if)# ip address ip-address/mask
OS10(config-ip)# exit
```

95. Si además queremos asignar esa dirección IP en alguna de las VLAN, el comando será como en el siguiente ejemplo, donde se asigna la dirección 10.1.9.2/24 en la VLAN 100:

```
OS10(conf)# interface vlan 100
OS10(config-if)# ip address 10.1.9.2 255.255.255.0
OS10(config-ip)# exit
```

96. Esta dirección permitirá a los sistemas con acceso a dicha VLAN acceder a la gestión del conmutador a través de alguno de los mecanismos descritos en las siguientes subsecciones basados en TCP/IP (SSH, SNMP, etc.).

97. Si el equipo tiene asignadas direcciones IP en otras VLAN, el acceso a la gestión será posible desde cualquiera de los equipos que tengan acceso a esas VLAN con dirección IP. Este hecho, muy habitual en el caso de que el equipo se configure a nivel 3 como router entre VLANs, puede plantear problemas de seguridad, ya que expone la gestión del equipo a múltiples equipos locales o incluso remotos.

98. Con el objeto de solventar este problema, el producto ofrece la posibilidad de definir una VLAN de gestión segura, diseñada para restringir el acceso a la gestión del equipo únicamente a aquellos equipos que estén conectados a esa VLAN. Esto es, sólo los clientes que estén conectados a puertos que son miembros de la VLAN de gestión podrán tener acceso al equipo para gestión. El resto de direcciones IP asignadas a otras VLANs no servirán para acceder a la gestión.

99. **Se debe configurar el equipo desde una VLAN específica para ello.**

100. Para crear una crear una VLAN se usa el siguiente comando:

```
interface vlan vlan-id [of-instance{of-id}]
```

a) *vlan-id*: es el identificador de la VLAN. El rango es de 1 a 4094.

b) *of-instance{of-id}*: es el identificador de la instancia de OpenFlow. El rango es de 1 a 8.

101. Y para especificar la interfaz de gestión a través de la red de gestión fuera de banda (out-of-band), se usa el siguiente comando:

```
interface managementethernet slot/port
```

102. Existen algunas restricciones a tener en cuenta:

a) Sólo una VLAN por equipo puede ser configurada como VLAN de gestión.

b) La dirección IP de gestión ha de ser estática.

c) No puede ser configurado en la VLAN de gestión nada relacionado con protocolos de encaminamiento o IGMP.

d) Se recomienda no hacer uso de la VLAN creada por defecto (VLAN 1) para esta configuración, para evitar que durante la configuración de nuevos equipos se pueda dar acceso por error a la VLAN de gestión.

103. Además, es muy recomendable que la red de gestión se utilice exclusivamente para la gestión de equipos y ningún sistema ajeno a la gestión tenga conectividad con

ella. Con este modelo (denominado gestión fuera de banda) mejoramos sensiblemente la seguridad del conmutador mediante la separación del tráfico de gestión del resto de tráficos de nuestras redes.

104. El siguiente paso es definir el camino desde el switch a la red desde la que se accede remotamente. Las rutas de gestión están separadas de las rutas del resto de IPs y éstas sólo se gestionan a través de los puertos de gestión. Así pues, se debe configurar el acceso a esta red de gestión de la siguiente manera:

```
OS10(conf)# management route {{ip-address mask | {ipv6-address prefix-length}}{forwarding-
router-address | managementetehernet}

OS10(conf)#management route 192.100.0.0/24 100.3.73.235
```

5.5.2.2 TELNET

105. El acceso a la gestión mediante el protocolo **TELNET se considera inseguro**, ya que toda la información intercambiada en la sesión de gestión remota se envía sin cifrar. Por lo tanto, no deberá utilizarse, ni siquiera en los casos en los que se utilice una red de gestión aislada, dada la facilidad de obtener información sensible (usuarios y claves, por ejemplo) si alguien consigue capturar el tráfico de gestión.

106. Dado que este servicio viene activado de fábrica, deberá ser desactivado mediante el comando siguiente:

```
OS10(conf)# no ip telnet server enable
```

5.5.2.3 SSH

107. El protocolo recomendado para el acceso remoto a la gestión de un equipo en entornos sensibles es SSH, dado que toda la información enviada es cifrada mediante algoritmos modernos considerados fiables. De tal forma que permite un acceso a CLI seguro.

108. Para configurar el acceso por SSH se debe ejecutar el siguiente comando:

```
OS10(conf)# ip ssh server enable
```

109. **Se debe establecer un tiempo límite de inactividad en la sesión**, tras el cual la sesión se cerrará. El comando "*exec-timeout*" introducido en el apartado 5.5.1.1 PUERTO DE CONSOLA, permite configurar ese tiempo límite.

110. Las claves RSA utilizadas por el protocolo se generan automáticamente al arrancar el equipo por primera vez. Se recomienda regenerar estas claves durante la configuración del dispositivo, para ello, ejecutar el comando: ***crypto key generate rsa keysize***.

111. El valor de tamaño de clave puede definirse entre 1024 y 4096 bits. Deben utilizarse claves de longitud 3072 bits o superiores. Las claves deben ser generadas por un usuario con rol *sysadmin* y nivel de privilegio 15.

112. Cuando el producto opera en modo FIPS, la generación de claves solo permite longitudes de 2048 o mayores. Adicionalmente, en dicho modo solo se hace uso de la versión SSHv2 del protocolo.

113. Deben definirse también los algoritmos utilizados por el protocolo para asegurar el uso de aquellos que aportan una mayor seguridad. Para ello ejecutar los siguientes comandos:

```
OS10# ip ssh server cipher aes128-ctr aes256-ctr
OS10# ip ssh server mac hmac-sha1 hmac-sha2-256 hmac-sha2-512
```

5.5.2.4 SNMP

114. SNMP es el protocolo de intercambio de información de gestión entre plataformas de gestión y los equipos gestionados.

115. Este protocolo tiene dos (2) facetas principales, que se diferencian principalmente en qué motiva el intercambio de información, así como la naturaleza del mismo:

a) Generación de alarmas o eventos, llamados *traps*, que se envían desde los dispositivos hacia una o varias estaciones gestoras de la red. Notifican eventos o cambios de estado producidos en un equipo o en su entorno (por ejemplo, la caída de un enlace o un exceso de temperatura)

b) Dialogo o interrogación, que permite a las estaciones gestoras, con las correspondientes credenciales, interrogar o mandar órdenes al equipo (por ejemplo, configurar la dirección IP o consultar estadísticas sobre el valor de paquetes transmitidos por una interfaz).

116. Actualmente existen tres (3) versiones del protocolo SNMP. Los equipos con Dell EMC soportan las tres versiones, aunque la única que proporciona mecanismos de seguridad y control adecuados es **SNMPv3**, por lo que es **la versión que se debe utilizar** en caso de necesitar el uso de SNMP en un sistema.

117. Para configurar una política de SNMPv3 en modo de sólo lectura, en el cual sólo se pueden hacer lecturas de información, pero no modificaciones de la configuración, se ejecuta el siguiente comando:

```
OS10(conf)# no snmp-server community public ro
```

118. Al aplicar este comando deshabilitaremos SNMP v1 y v2. Dejando solo funcional SNMP v3, que es el modo recomendado.

119. A continuación, se crean las traps de SNMPv3 con el siguiente comando:

```
OS10(conf)# snmp-server enable traps [notification-type] [notification-option]
```

120. Un ejemplo con los diferentes atributos puede ser:

```
OS10(conf)# snmp-server enable traps bgp
OS10(conf)# snmp-server enable traps config
OS10(conf)# snmp-server enable traps ecfm
OS10(conf)# snmp-server enable traps ecmp
OS10(conf)# snmp-server enable traps ets
OS10(conf)# snmp-server enable traps entity
OS10(conf)# snmp-server enable traps fips
OS10(conf)# snmp-server enable traps isis
OS10(conf)# snmp-server enable traps lacp
OS10(conf)# snmp-server enable traps pfc
OS10(conf)# snmp-server enable traps stack
OS10(conf)# snmp-server enable traps stp
OS10(conf)# snmp-server enable traps vlt
OS10(conf)# snmp-server enable traps vrrp
OS10(conf)# snmp-server enable traps xstp
OS10(conf)# snmp-server enable traps envmon cam-utilization fan supply temperature
OS10(conf)# snmp-server enable traps snmp authentication coldstart linkdown linkup
```

121. Si no se configura este comando, no se enviará ninguna trap. Si por el contrario no se especifica el "*notification-type*", todas las traps se habilitan automáticamente.

122. A continuación, se indica la descripción detallada de las traps:

Tipo	Descripción
bgp	Trap para los cambios en BGP
config	Traps para cambios en la configuración de startup o running
ecfm	Traps para cambios de ECMP
ecmp	Traps para desbalanceo de tráfico ECMP
entity	Traps para cambios de MIB
envmon	Traps para cuando se excede un umbral ambiental
ets	Traps de ETS
fips	Traps para cambios de estado en FIPS snooping
isis	Traps para cambios de estado de adyacencia IS-IS
lacp	Traps para cambios de estado de LACP
pfc	Traps para cambios de estado de PFC
snmp	Traps definidas en RFC-1157: authentication, coldstart, linkdown, linkup, syslog-reachable, syslog-unrecheable
stack	Traps para cambios de stacking role
stp	Traps para cambios de estado en Spanning Tree Protocol (STP) RFC 1493
vlt	Traps para cambios de estado de VLT
vrrp	Traps para cambios de estado en un grupo VRRP

Tipo	Descripción
xstp	Traps para cambios de estado en STP (802.1s), RSTP (802.1w), and PVST+

123. También se puede crear un grupo de SNMP3 que mapee los usuarios de SNMP con las vistas de SNMP. Para más información, revisar el apartado de "*Simple Network Management Protocol (SNMP)"* en la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

```
 OS10(conf)# snmp-server group group_name 3 priv snmpv3-password [read name] [write name]
[notify name]

 OS10(conf)# snmp-server group ccGroup 3 priv read ccReadView write ccWriteView notify
ccNotifyView
```

124. Para configurar los receptores de *traps* SNMPv3 se usa el comando "*snmp-server host*" con los siguientes atributos:

```
OS10(conf)# snmp-server host 10.16.150.203 traps version 3 priv mySNMPv3Password udp-port 162
```

a) *ip-address*: la dirección IP del host. El máximo número permitido de hosts es 16.

b) *traps*: indica que se van a enviar notificaciones de tipo trap a un host determinado. Por defecto es traps.

c) *version*: especifica el modelo de seguridad y su versión 3 (que es la más segura de los tres métodos). Se debe utilizar la versión 3.

d) *priv snmpv3-password*: especifica la autenticación y la contraseña de SNMPv3.

e) *udp-port* (opcional): indica el puerto del host remoto. El rango es de 0 a 65535. El valor por defecto es 162.

125. Para configurar los usuarios permitidos, es necesario primero crearlos y luego asignarlos a grupos. Los grupos son los que tienen los permisos. El comando para la creación de usuarios es:

```
OS10(conf)# snmp-server user name group_name 3 [auth sha auth-password] [priv aes128 priv
password]
```

a) *name*: indica el nombre del usuario en el host que conecta con el agente. No puede exceder de 20 caracteres.

b) *group-name*: es una cadena de caracteres que indica el nombre del grupo. No puede exceder de 20 caracteres. El número 3 posterior, indica que se está usando SNMPv3.

c) *auth sha*: designan el nivel de autenticación y la contraseña tipo *sha*.

d) *priv aes128*: indica el algoritmo de cifrado AES CFB 128-bit.

126. Un ejemplo del uso de este comando es:

```
OS10(conf)# snmp-server user ccUser ccGroup 3 auth sha myShaPassword priv aes128 myAesPasswd
```

5.6 GESTIÓN DE CERTIFICADOS

127. Deben configurarse los certificados utilizados en las distintas comunicaciones del producto. Estos certificados son presentados a clientes SSH, además de implementaciones con servidor TLS que requieren autenticación del cliente (como es el caso de Syslog y Radius). Así mismo están firmados digitalmente con una clave privada por un servidor con autoridad de certificación.

128. Se pueden ver los certificados instalados en el sistema con el comando "*show crypto ca-certs*".

5.6.1 CREACIÓN DE UN CSR

129. El producto permite la creación de CSRs (*Certificate Signing Request*). Para ello utilizar el comando:

```
OS10(conf)# crypto cert generate {self-signed | request} [cert-file cert-path key-file
{private | keypath}] [country 2-letter code] [state state] [locality city] [organization
organizationname] [orgunit unit-name] [cname common-name] [email email-address] [validity
days] [length length] [altname alt-name]
```

130. Introducir la información concreta de la organización en los parámetros del comando. El parámetro *Lenght* admite valores entre 2048 y 4096, **se deben utilizar longitudes de clave iguales o superiores a 3072 bits**.

5.6.2 INSTALACIÓN DE CERTIFICADOS

131. Para cargar los certificados en el producto, se deberá utilizar *flash, usbflash, tftp, ftp*, o *scp* para descargarlos al sistema. Se recomienda utilizar SCP para esta acción.

132. Se pueden ver los certificados del sistema con el comando "*show crypto ca-certs*", al igual que se puede instalar uno nuevo con:

    a) El comando "*crypto ca-cert install {path}*". Permite la instalación de *certificados* de CA (*Certificate Authority*) de confianza.

    b) El comando "*crypto cert install cert-file cert-path key-file {key-path | private} [password passphrase]*" permite la instalación de certificados en el dispositivo. Estos pueden ser los creados previamente mediante un CSR.

133. Los certificados instalados se emplearán automáticamente para la autenticación de clientes SSH. Los certificados instalados se emplearán también en las conexiones que utilicen mecanismos de comunicaciones cifradas basadas en protocolo TLS para validación de las mismas, como *Syslog* seguro.

5.6.3 CREACIÓN DE SECURITY PROFILES

134. Una vez instalados los certificados, para poder hacer uso de ellos en las comunicaciones con un servidor de autenticación RADIUS (ver apartado 5.3.1.2 AUTENTICACIÓN MEDIANTE SERVIDORES EXTERNOS) y con el servidor de auditoría externo (ver apartado 5.8.1 SYSLOG), se debe crear un perfil de seguridad, para ello:

a) Crear un perfil con el nombre deseado utilizando *crypto security-profile nombre_perfil*.

b) Asignar el certificado deseado, previamente importado, utilizando *certificate nobre_cert*.

5.7 ACTUALIZACIÓN DEL SOFTWARE DEL DISPOSITIVO

135. Esta sección describe cómo instalar y actualizar el software necesario para operar el producto.

5.7.1 VERSIÓN DE SOFTWARE INSTALADA

136. Para verificar la versión de software instalada en el equipo se utiliza el comando "*show version*":

```
OS10#show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2021 by Dell Inc. All Rights Reserved.
OS Version: 10.5.2.3
Build Version: 10.5.2.3.316
Build Time: 2021-02-26T20:03:25+0000
System Type: S5248F-ON
Architecture: x86_64
Up Time: 08:04:25
```

137. Una vez descargado el nuevo software desde la web https://www.dell.com/support/, hay que verificar la integridad con el comando "*verify sha256 [flash://]img-file [hash-value]*" en modo *EXEC Privilege*, cuyos atributos son:

```
OS10# verify sha256 flash://FTOS-SE-9.14.1.bin
e6328c06faf814e6899ceead219afbf9360e986d692988023b749e6b2093e933
SHA256 hash VERIFIED for FTOS-SE-9.14.1.bin
```

a) *sha256:* Algoritmo de seguridad HashSHA256 Secure Hash Algorithm.

b) flash (opcional): especifica el disco flash, aunque también se puede indicar el nombre de la imagen del fichero.

c) hash-value (opcional): especifica el hash publicado en la web de soporte.

d) *img-file:* indica el nombre del archivo con la imagen del software a validar.

138. Después de tener validada la imagen, habrá que seguir las instrucciones de las *release notes* de la versión específica de código para actualizar (*upgrade/downgrade*).

139. Las *release notes* de cada versión se pueden consultar en el repositorio Dell Digital locker con el usuario de soporte de cliente.

140. Puede que sea necesario reiniciar el sistema inmediatamente después de la actualización o bien se puede posponer. En este sentido, se puede comprobar las versiones de ambas particiones (A y B) usando el comando "*show boot system*":

```
dv-fedgov-s3100-5>show boot system stack-unit 1
Current system image information in the system:
================================================
Type           Boot Type    A           B
------------------------------------------------------------
stack-unit 1   FLASH BOOT   9.14(1.0)   9.14(1.9)[boot]
```

5.7.2 GUARDAR CONFIGURACIÓN ACTUAL

141. La llamada *running-config* contiene la configuración actual del sistema. Se recomienda copiarla a la configuración de arranque *startup-config*. En los siguientes pasos se detalla este proceso, asumiendo que el directorio actual es la memoria flash interna.

   a) Guardar la configuración *running-config* a la configuración de arranque *startup-config* en la memoria interna flash de la partición primaria*:*

   ```
   OS10# copy running-config startup-config
   ```

   b) Guardar la configuración *running-config* a un servidor SCP*:*

   ```
   OS10# copy running-config scp://{userid:passwd@hostip}/filepath
   ```

5.7.3 ACTUALIZACIÓN DEL SISTEMA

142. **Se debe mantener el software del equipo actualizado a las últimas versiones publicadas**, con el fin de incorporar todas las correcciones de seguridad incorporadas al software por el fabricante.

143. La actualización del sistema operativo puede realizarse desde la línea de comandos (CLI) o a través de autodescubrimiento ONIE si se ha adquirido un switch tipo ONIE. Este último proceso es conocido como instalación automática *zero-touch*. Antes de actualizar es muy recomendable hacer una copia de respaldo de la configuración (al menos dentro del propio conmutador o, para más seguridad, a un servidor externo). Para ello se debe seguir el proceso indicado en el apartado anterior.

144. Esta copia nos permitirá recuperar la configuración original en caso de tener que volver atrás en una actualización de versiones, ya que en ocasiones el formato de los comandos puede variar entre distintas versiones y la actualización provoca cambios no deseados en la configuración.

145. El proceso de descubrimiento automático de ONIE localiza la imagen de software almacenada, la descarga e instala y reinicia el dispositivo con la nueva imagen. El descubrimiento automático se repite hasta que ocurre una instalación satisfactoria de la imagen del software y reinicia el switch.

146. Para una instalación manual mediante el CLI es posible usar FTP, TFTP y SCP para actualizar el equipo vía interfaces de red IP, se recomienda utilizar SCP. También se puede hacer usando un dispositivo USB.

147. Los pasos a seguir en una actualización mediante línea de comandos, son los siguientes:

a) Actualizar el código en la partición A con el comando "upgrade system [flash]. Se debe hacer uso de SCP: | ftp: stack-unit <1-6> | tftp: | scp: | usbflash:] [A:]":

```
OS10# upgrade system scp: a:
```

b) Verificar que se ha actualizado correctamente con el comando "*show boot system stack-unit [1-6] | all]*".

c) Cambiar el parámetro de "*primary boot"* a la partición actualizada:

```
OS10(conf)# boot system stack-unit 1 primary system:a
```

d) Salvar la configuración con el comando "*write memory*".

e) Actualizar el código en la partición B con el comando "*upgrade system [flash: | ftp: stack-unit <1-6> | tftp: | scp: | usbflash:] [B:]*". Se debe hacer uso de SCP:

```
OS10# upgrade system scp: b:
```

f) Verificar que se ha actualizado correctamente con el comando "*show boot system stack-unit [1-6] | all]*".

g) Salvar la configuración con el comando "*write memory*".

h) Reiniciar el producto con el comando "*reload*" y verificar la nueva versión con "*show version*".

148. Para actualizar el *Boot Flash* y la *BIOS*, los pasos a seguir son:

a) Actualizar la imagen de *Boot Flash*:

```
OS10# upgrade boot bootflash-image stack-unit 1 booted
```

b) Actualizar la imagen de *Boot Selector*:

```
OS10# upgrade boot bootselector-image stack-unit 1 booted
```

c) Reiniciar el switch con el comando "*reload*" y verificar la imagen del *Boot Selector* con el comando "*show system stack-unit 1*".

149. Los pasos a seguir en una actualización manual es seleccionar la opción ONIE: Rescue del menú anterior y seguir con el procedimiento que se indica en el capítulo "*Getting Started*" de la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

150. Posteriormente para actualizar el firmware, los pasos a seguir son:

a) Actualizar la imagen:

```
OS10#    image    install    image://onie-firmaware-x86_64-dellemc_s5200_c3538-
r0.3.40.5.1-9.bin
```

b) Reiniciamos el switch con el comando "*reload*".

```
OS10# reload
```

5.8 AUDITORIA

151. El producto permite almacenar registros de auditoría, incluyendo:

a) Accesos exitosos y fallidos de usuarios al sistema.

b) Cambios en la configuración.

c) Establecimiento de conexiones.

152. Para activar el registro de eventos de seguridad, se debe ejecutar el comando *logging audit enable*.

153. Estos registros se almacenan por defecto localmente. Se recomienda configurar el envío a un servidor externo de auditoría mediante *syslog*, permitiendo así una mejor gestión de los registros.

5.8.1 SYSLOG

154. El producto permite configurar el envío de registros de auditoría a un servidor de *Syslog*. Para ello se puede configurar soporte TLSv1.0, v1.1 y v1.2. La configuración es automática, intentando negociar por defecto TLSv1.2 y solo negociando versiones anteriores en base a las capacidades del otro extremo. Deberá configurarse el modo de operación segura (ver 5.2.1 HABILITACIÓN MODO FIPS), para que solo se soporte TLSv1.2, rechazando la conexión con cualquier otra versión anterior.

155. A continuación, se describen los pasos a seguir:

a) Primero debe crearse un perfil de seguridad, tal como se indica en el apartado 5.6.3 CREACIÓN DE SECURITY PROFILES.

b) Para configurar el servidor de auditoría externo, utilizar el siguiente comando:

```
OS10(conf)# logging security-profile nombre_perfil
OS10(conf)# logging server IP tls
```

156. Para más información al respecto, se puede consultar el apartado "*Audit log*" de la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

5.9 POLÍTICAS DE CALIDAD DE CONTRASEÑAS

157. Cuando la autenticación de un sistema se basa principalmente en nombres de usuarios y claves, la seguridad depende en gran medida de la calidad de las contraseñas utilizadas. El producto permite configurar diversos atributos para el control de la calidad de las contraseñas que se usan para la gestión del switch y otras funciones de control de acceso de usuarios.

158. Para definir la política de seguridad en la creación de contraseñas, se usa el siguiente comando:

```
OS10(conf)# password-attributes [min-length number] [max-retry number] [lockout-period
minutes]][character-restriction [upper number] [lower number] [numeric number] [special-
char number]]
```

a) *min-length number*: indica el número de caracteres. El rango es de 0 a 32. **Se debe utilizar una longitud de, al menos, 12 caracteres.**

b) *max-retry number* (opcional): indica el máximo número de intentos. El rango es de 1 a 16. **Se debe configurar con un valor bajo, por ejemplo, 3 intentos.**

c) *lockout-period minutes* (opcional): este parámetro mejora la seguridad del switch bloqueando las sesiones Telnet o SSH cuando existen varios intentos fallidos de login. El rango es de 1 a 1440 minutos. El valor por defecto es 0 minutos y no habilitado. **Se debe configurar un valor de 5 minutos.**

d) *character-restriction* (opcional): indica los caracteres permitidos. Para todos los tipos de caracteres se debe configurar un valor de, al menos, uno:

- *upper number* (opcional): indica el número de mayúsculas permitido. El rango es de 0 a 31.
- *lower number* (opcional): indica el número de minúsculas permitido. El rango es de 0 a 31.
- *numeric number* (opcional): indica cuántas cifras numéricas están permitidos. El rango es de 0 a 31.
- *special-char number* (opcional): indica el número de caracteres especiales permitido. El rango es de 0 a 31.

159. Un ejemplo de cómo construir una contraseña robusta es el siguiente:

```
OS10(conf)# password-attributes min-length 15
OS10(conf)# password-attributes character-restriction lower 1
OS10(conf)# password-attributes character-restriction upper 1
OS10(conf)# password-attributes character-restriction numeric 1
OS10(conf)# password-attributes character-restriction special-char 1
OS10(conf)#password-attributes max-retry 5 lockout-period 5
```

160. Adicionalmente, las contraseñas y claves son almacenadas en el fichero de configuración y se muestran de forma cifrada.

161. El comando "*service obscure-passwords*" las oculta, pero no cambia el fichero de configuración. Cuando se usa RBAC, tan sólo los roles de administrador del sistema y administrador de seguridad pueden usar este comando.

162. Para verificar que se han ocultado satisfactoriamente, mostrar la configuración de *startup* o *running*.

```
OS10(conf)# service obscure-passwords
OS10(conf)# show running-config
OS10(conf)# show startup-config
```

5.9.1 ALMACENAMIENTO DE CONTRASEÑAS

163. Tal como se ha mencionado antes, las claves de usuario se almacenan en el fichero de configuración de *running y startup config*. Para que las contraseñas sean protegidas, se recomienda configurar su almacenamiento de forma que no se almacene la contraseña sin cifrar, sino un valor cifrado de la misma mediante un algoritmo hash a través de "*enable password sha-256*" o "*enable password sha-512*".

164. De esta forma, el producto almacenará únicamente el valor hash sha-256 o sha-512 de dichas contraseñas.

5.9.2 CONFIGURACIÓN DE FÁBRICA Y RECUPERACIÓN DE CONTRASEÑAS

165. A continuación, se indica cómo restaurar la configuración de fábrica y recuperar la contraseña del producto en caso necesario.

166. El procedimiento de **restauración a la configuración de fábrica** del equipo elimina los parámetros existentes de la NVRAM, la configuración de arranque y demás parámetros configurados como *stacking* y *fanout*.

167. Para ello, en modo EXEC Privilege se usa el comando "restore factory-defaults stack-unit {stack—unit—number | all} {clear-all | nvram | bootvar}":

168. El siguiente ejemplo ilustra cómo restaurar la configuración de fábrica:

```
OS10# restore factory-defaults stack-unit 1 nvram
    ********************************************************************
    * Warning - Restoring factory defaults will delete the existing *
    * persistent settings (stacking, fanout, etc.) *
    * After restoration the unit(s) will be powercycled immediately. *
    * Proceed with caution ! *
    ********************************************************************

Proceed with factory settings? Confirm [yes/no]:yes

-- Restore status --
Unit   Nvram     Config
-----------------------
1      Success
Power-cycling the unit(s).
....
```

169. También es posible realizarlo desde el menú de reinicio del switch, estando conectado por consola.

170. El siguiente proceso indica cómo recuperar la contraseña:

a) Abrir una conexión serie al switch y realizar un *power cycle*. A continuación, presionar *Esc* cuando aparezca uno de los siguientes mensajes: **"Hit** Esc **key to interrupt autoboot:"** o **"Hit any key to stop autoboot:".** Seguidamente se verá el prompt de U-Boot: **"=>"**

b) Una vez dentro de este menú, ignorar la configuración de arranque:

```
=> setenv stconfigignore true
=> saveenv
=> reset
```

c) Cuando el switch se haya reiniciado completamente, aplicar la configuración de arranque a la running-config:

```
OS10> enable
OS10# copy startup-config running-config
```

d) Eliminar cualquier contraseña y secreto del modo *enable*, y volvemos a crear un secreto o contraseña:

```
OS10# config
OS10(config)# no enable password
OS10(config)# no enable secret
OS10(config)# enable secret <enter password here>
OS10(config)# enable password <enter password here>
```

e) Buscar usuarios configurados y eliminarlos. Seguidamente crear un nuevo usuario con permisos de lectura y escritura:

```
OS10(config)# do show run | grep username
username Delluser password 7 66a88a701a5b6b80 privilege 15

OS10(config)# no username Delluser
OS10(config)# username Delluser password P@$$w0rd123 privilege 15
```

f) Se guarda la configuración y se reinicia el *switch*:

```
OS10(config)# do write memory
OS10(config)# do reload
```

5.10 AUTO CHEQUEOS

171. El producto realiza una serie de auto chequeos de forma automática durante el arranque:

a) BIOS POST. Si se detecta algún problema en la BIOS del sistema, se detiene el arranque.

b) *System Software Self-tests*. Si durante el arranque se detecta algún error grave en el software, el producto se reinicia automáticamente. En caso de detectar errores menores, se muestra una alerta.

c) *Secure Boot*. Se verifica la integridad del *kernel* del producto. Para activar esta verificación, ejecutar el comando *secure-boot enable*.

d) *FIPS Self-tests*. Se verifican las funciones criptográficas del producto. Si algún test falla, el sistema mostrará una alerta y generará un evento de auditoría.

5.11 SERVICIOS DE RED DEL EQUIPO

172. **Para garantizar la seguridad de un equipo es imprescindible ser consciente de qué servicios de red tiene activados y tomar las medidas adecuadas para asegurarlos.** Asimismo, es importante destacar que mantener activo un servicio que no se utiliza puede convertirse en un problema de seguridad importante, ya que puede exponer vulnerabilidades que sean aprovechadas por atacantes.

173. Por ello, **se deben desactivar todos aquellos servicios que no sean necesarios**, sobre todo teniendo en cuenta que algunos de ellos suelen venir activados en las configuraciones por defecto.

5.11.1 LLDP

174. El protocolo LLDP (*Link Layer Discovery Protocol*) estandarizado por el IEEE es un protocolo de nivel 2 que permite compartir información entre equipos red (*routers*, conmutadores y otros) directamente conectados. Permiten a un equipo informar a

sus vecinos de, por ejemplo, el nombre del equipo, el tipo o la versión del sistema operativo utilizada, así como proporcionar información sobre la configuración de las VLAN.

175. En general dicho protocolo consiste básicamente en el envío periódico de paquetes con la información mencionada hacia direcciones *multicast* que escuchan el resto de equipos. De esta forma, se proporciona información útil para la configuración y gestión de la red. Además, diversas herramientas y plataformas de gestión de red requieren su uso. Sin embargo, la información que proporcionan puede ser utilizada maliciosamente para conocer detalles sobre la red por parte de atacantes.

176. Por ello, si este protocolo no es estrictamente necesario para el funcionamiento de la red, se recomienda deshabilitarlo de forma global. En caso de que sean necesario, se deben deshabilitar en los interfaces donde no se utilicen (p. ej., en los puertos de acceso a los que se conectan los equipos finales).

177. Para desactivar LLDP de forma global, hay que usar el comando:

```
OS10(config)#no     lldp
enable
```

178. Para desactivarlo selectivamente en los puertos de gestión, basta con desde el menú de interface (del puerto en concreto) lanzar los anteriores comandos, por ejemplo:

```
OS10(conf-if-eth1/1/1:1)# no lldp {[med | tlv-select | vlan-name-tlv | transmit | receive
| management-addr-tlv
OS10(conf-lldp)# show config
```

179. Finalmente, se puede obtener información sobre la configuración de LLDP de la siguiente forma:

```
OS10(conf)# show lldp neighbors
Loc PortID          Rem Host Name        Rem Port Id                  Rem Chassis Id
-------------------------------------------------------------------------------------
ethernet1/1/53      DELL-02              ethernet1/1/53              c0:3e:ba:dc:85:00
ethernet1/1/55      DELL-01              ethernet1/1/55              c0:3e:ba:dc:81:00
OS10(conf)# show lldp ?
dcbx         Show DCBX information
errors       Show lldp errors
interface    Select an interface
med          Show lldp med
neighbors    Show lldp neighbor info
timers       Show lldp timers
tlv-select   Enabled tlvs in LLDP
traffic      Show lldp traffic info
```

5.11.2 ICMP

180. ICMP es el protocolo que define los mensajes de control de las redes IP como, por ejemplo, las solicitudes/respuestas de eco utilizadas en ping o los mensajes de error enviados cuando se descarta un datagrama IP.

181. Dichos mensajes pueden ser utilizados por los atacantes para descubrir información de la red o para realizar ataques de denegación de servicio. Por ello, **se deben desactivar todas aquellas opciones de uso de ICMP que no sean necesarias**, tales como los mensajes de redirección (pensados, por ejemplo, para escenarios con varios *routers* en una misma subred IP) y los mensajes de error de tipo "***Destination unreachable***" generados cuando el conmutador tiene activadas funciones de nivel 3 y descarta un paquete IP, por ejemplo, debido a que el TTL ha llegado a cero o no existe una ruta para encaminarlo.

182. Para desactivar las funciones de ICMP mencionadas, dentro del menú interface, hay que crear una lista de acceso y aplicarla posteriormente. La sintaxis del comando sería:

```
permit icmp [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any |
host ip-address] [capture | count | dscp value | fragment | log]
```

183. De tal forma, que se permitirá el uso de aquellos mensajes necesarios. Declarar de forma expresa una condición como *permit* implica que, si no se añade ninguna condición más, cualquier otro tráfico será implícitamente denegado.

5.11.3 TRANSFERENCIA DE FICHEROS

184. Para transferir archivos a/o desde el conmutador existen tres protocolos diferentes: TFTP, FTP y SCP. El protocolo TFTP (*Trivial File Transfer Protocol*) se considera inseguro, por no incluir capacidades de autenticación o cifrado, por ello es mejor no usarlo. Así pues, se recomienda el uso SCP (*Secure Copy Protocol*) para el intercambio de ficheros.

185. La copia de ficheros se realiza mediante el comando "*copy*". Por ejemplo, para copiar un fichero a servidor SCP:

```
OS10# copy config://Dell-EF-8.2.1.0.bin scp://myusername:mypassword@10.10.10.10/Dell/Dell-EF-
8.2.1.0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
27952672 bytes successfully copied
```

5.11.4 SINCRONIZACIÓN DE TIEMPO

186. Los equipos Dell EMC soportan la sincronización del reloj interno con servidores de hora externos mediante el protocolo NTP (*Network Time Protocol*). **Se recomienda utilizar NTP por su mayor precisión y su capacidad de gestionar más de una fuente de sincronización.**

187. Para evitar posibles ataques relacionados con el protocolo NTP (por ejemplo, aquellos que buscan cambiar la hora de los equipos para realizar ataques del tipo *reply* o simples ataques *DoS*), es muy recomendable que los servidores de NTP utilizados en la organización tengan activada la opción de autenticación. De esta forma se pueden autenticar los mensajes intercambiados entre clientes y servidores, dificultando con ello la mayoría de los ataques.

188. Para configurar que el equipo forme parte del servicio NTP de la red es necesario: configurar el modo de trabajo, *broadcast* o *unicast*; configurar las claves de autenticación; configurar el número máximo de asociaciones de terceros equipos; configurar los servidores NTP desde los cuales sincronizarse; y, por último, habilitar NTP.

189. Por defecto en los equipos de Dell EMC, el NTP está deshabilitado. Basta simplemente especificar un servidor de NTP para así habilitarlo.

190. Los pasos que seguir para configurar que el reloj del equipo se sincronice con uno o varios servidores NTP externos son los siguientes:

a) Se puede configurar los interfaces para recibir la información de NTP a través de *broadcast*, aunque no se recomienda. Dentro del menú *interface*:

```
ntp broadcast client
```

b) Habilitar la autenticación para el tráfico de NTP entre el *switch* y los servidores de tiempo de NTP. Seguidamente hay que configurar la clave de autenticación, así como su identificador y el tipo de cifrado:

```
OS10(conf)# ntp authenticate
OS10(conf)# ntp authentication-key <number> {md5 | sha1} {0|7]} <key value>
```

- *number*: este valor debe coincidir con el comando ntp trusted-key.
- *key value*: 0 para texto plano y otro número para clave cifrada.
- Deberá utilizarse SHA1 frente a MD5.

c) Configurar la dirección IP del servidor NTP (repetir para cada servidor), por ejemplo:

```
OS10(conf)# ntp server 192.100.0.16 key 1000
```

d) Autenticar el sistema del NTP del que sincroniza:

```
OS10(conf)#ntp trusted-key 1000
```

191. Finalmente, se puede comprobar la configuración en el conmutador de NTP mediante:

```
OS10# show running-configuration ntp
!
ntp authenticate
ntp authentication-key 345 md5 5A60910F3D211F02
ntp server 11.1.1.1 version 3
ntp trusted-key 345
```

5.12 CONTROL DE TRÁFICO Y SEGURIDAD EN LOS PUERTOS DE RED

192. En este capítulo se describirán una serie de medidas de seguridad que pueden aplicarse en el producto para mejorar la seguridad de los puertos de red de los *switches*, así como controlar el tráfico que gestiona el equipo.

5.12.1 APAGADO DE PUERTOS

193. Una medida de seguridad básica consiste en **deshabilitar todos aquellos puertos del conmutador que no se estén utilizando**, con el objeto de evitar que alguien pueda conectar equipos no autorizados a esos puertos.

194. Para bloquear o cerrar los puertos no utilizados, se usa el comando "*shutdown*". Y para consultar su estado, los comandos "*show interfaces*" (en modo EXEC *Privilege*) o "*show config*" (en menú interface):

```
OS10(conf)# interface ethernet1/4/17
OS10(conf-if-eth-1/4/17)# shutdown
```

5.12.2 MEDIDAS DE PROTECCIÓN DE PUERTOS

195. Se proporcionan medidas específicas para poder configurar la seguridad a nivel de puerto de una forma precisa, definiendo qué equipos (direcciones MAC) pueden conectarse o limitando el número máximo de equipos que se conectan a cada puerto. Permite, además, configurar la generación de alarmas o incluso el bloqueo de los puertos en caso de que se detecten accesos no permitidos.

196. Para poder configurar estas funcionalidades es necesario tener un inventario de las direcciones físicas de los equipos que se van a conectar o una estimación de cuantos equipos se conectan en cada puerto. Asimismo, es necesario introducir algunos conceptos previos para conocer qué configuración de las posibles se adapta mejor a nuestras necesidades.

197. Cuando se activa el control de seguridad en un puerto, se puede configurar:

a) El número máximo de direcciones MAC permitidas en un interfaz. El rango permitido es de 1 a 100.000:

```
OS10(conf)# mac learning-limit address-limit [vlan vlan-id] [station-move-violation
[dynamic]] [dynamic [no-station-move| station-move]]
```

b) El modo en el que el puerto conoce las direcciones permitidas:

- *No-station-move*: proporciona seguridad adicional en el puerto al prevenir un "*station-move*". Es el modo por defecto.
- *Station-move*: permite que una dirección MAC de la tabla sea aprendida por otra *interface*.
- *Dynamic*: las direcciones se aprenden de forma dinámica, incluso en el caso de existir un límite.

198. La opción *station-move-violation* define las acciones a tomar cuando se alcanza el límite de direcciones MAC aprendidas en una interfaz y se recibe una nueva:

a) *learn-limit-violation log*: Generar un log cuando se alcanza el límite.

b) *learn-limit-violation shutdown*: Cerrar el interfaz y generar un log cuando se alcanza el límite.

199. Tan sólo está disponible una *trap* para la opción "*station-move*". El resto de opciones no disponen de *traps* de SNMP.

200. Por otro lado, las direcciones MAC aprendidas dinámicamente en un puerto se pueden convertir en "*sticky*" MAC de la siguiente forma:

```
OS10(conf)# mac learning-limit mac-address-sticky
```

201. Es importante tener en cuenta que las direcciones MAC aprendidas de forma dinámica se almacenan en la tabla de filtrado del *switch* durante un tiempo máximo (unos minutos típicamente) siguiendo el algoritmo estándar de los conmutadores Ethernet. Además, si el conmutador se reinicia se eliminan. Por el contrario, las direcciones configuradas de forma estática se añaden a la configuración del conmutador, por lo que se conservan en la tabla de filtrado tras un rearranque del equipo.

202. Asimismo, es necesario remarcar que existe un número máximo de direcciones MAC seguras que podemos configurar, y que viene fijado por el número máximo de direcciones MAC que sistema es capaz de gestionar.

203. Una vez activada la seguridad en un puerto del conmutador pueden producirse situaciones que violen los límites de seguridad definidos, bien porque el número máximo de direcciones MAC seguras en un puerto se ha alcanzado, o bien porque una dirección aprendida en un interfaz se ha detectado en otro interfaz de la misma VLAN.

5.12.3 CONTROL DEL TRÁFICO

204. Los *switches* incorporan una funcionalidad de control de tormentas, que permite prevenir que el tráfico en la red se vea alterado (o incluso interrumpido) por culpa de una tormenta de *broadcast*, *multicast* o tráfico *unicast* desconocido recibido por uno de los interfaces físicos.

205. Estas tormentas tienen lugar cuando un nivel excesivo de este tipo de tráfico inunda la red, colapsando recursos de los equipos involucrados en la transmisión, disminuyendo por tanto la efectividad de la red. Las tormentas más típicas son las provocadas por la aparición de un bucle en la red o cuando se produce un ataque de denegación de servicio (DoS).

206. Al activar esta funcionalidad los equipos comienzan a monitorizar todos los paquetes que pasan por las interfaces donde se habilite, y determinan si el paquete es *unicast*, *multicast* o *unicast* desconocido. Entonces el conmutador compara el número de paquetes de cada tipo recibidos en un intervalo de un segundo, con el total de paquetes recibidos en ese mismo segundo. Si el número de paquetes de un determinado tipo es superior al límite establecido por el administrador para ese tipo de tráfico, el conmutador comienza a descartar paquetes de este tipo, de manera que el ancho de banda consumido por ese tipo de tráfico no colapse el resto de tráfico que atraviesa ese puerto.

207. Para realizar la configuración lo podemos hacer o bien de forma global en modo EXEC *Privilege* o bien por puerto.

208. Para configurarlo en un puerto, desde el modo *interface* configuramos los paquetes por segundo permitidos para el tipo de tráfico. El último comando cierra el puerto si recibe más paquetes PFC/LLFC (*Priority Flow Control / Link Level Flow Control*) del ratio configurado:

```
storm-control { broadcast | multicast | unknown-unicast } rate-in-pps
```

209. Para configurarlo en el modo EXEC *Privilege*, los comandos son:

```
OS10(conf-if-eth1/1/1)# storm-control broadcast 1000
```

210. Para visualizar la configuración del control de tormentas se usa el comando "*show storm-control broadcast | multicast | unknown-unicast [interface]*". Un ejemplo sería:

```
OS10# show storm-control multicast interface ethernet 1/1/1:1
 Interface         Direction       Packets/Second
 ------------------------------------------------
 ethernet1/1/1:1     Ingress       5
```

5.12.4 USO DE VLAN COMO MEDIDA DE AISLAMIENTO

211. Las LAN virtuales o VLAN constituyen la funcionalidad básica de los conmutadores actuales para crear redes separadas dentro del mismo conmutador. A grandes rasgos, una VLAN es una forma de virtualizar un conmutador, creando múltiples redes lógicas sobre un mismo conmutador físico.

212. Cada puerto de un conmutador debe pertenecer a al menos una VLAN. El tráfico enviado por los sistemas conectados a cada VLAN queda confinado en esa VLAN: cada VLAN constituye un dominio de *broadcast* diferente. En este sentido, el uso de VLAN permite reducir el tráfico de difusión en las redes, confinando a cada VLAN los efectos de los problemas tales como las tormentas de *broadcast*.

213. Un puerto puede pertenecer a varias VLAN distintas, en cuyo caso se debe configurar en modo etiquetado. Es el caso habitual de los enlaces entre conmutadores o de los puertos conectados a servidores. Los puertos conectados a sistemas de usuarios suelen pertenecer a una única VLAN y estar configurados en modo no etiquetado.

214. Las VLAN pueden expandirse a varios conmutadores, de forma que sistemas conectados a conmutadores distintos pueden pertenecer a la misma VLAN.

215. En Dell EMC, el sistema soporta hasta 4093 VLANs creadas según puerto y una única por defecto, de acuerdo a la especificación de IEEE 802.1Q. De esta forma, la VLAN 1 es la de por defecto, y a ella pertenecen todos los interfaces no etiquetados. Para evitar posibles problemas en la red cuando se interconectan *switches*, es recomendable no utilizar dicha VLAN y crear una nueva VLAN en la que se agrupen todos los puertos inactivos.

216. Para crear una VLAN basta con realizar:

```
OS10(conf)# interface vlan vlan-id
```

217. Donde *vlan-id* debe ser un valor no usado del rango de VLAN permitido (2- 4094). Para que un puerto pertenezca a una VLAN en el modo etiquetado (*tagged*) o no etiquetado (untagged) se utilizan los comandos siguientes en función de cada caso:

```
OS10(conf)# interface vlan vlan-id
OS10(conf-if-vl-1)# tagged interface
OS10(conf-if-vl-1)# access interface
```

218. Cuando se configuran las VLANs y los puertos que pertenecen a ella hay que tener especial cuidado en introducir estrictamente los puertos que se hayan considerado de uso necesario.

219. Para conocer las VLAN definidas en un conmutador y sus características se puede utilizar el comando:

```
OS10# show vlan
Codes: * - Default VLAN, G - GVRP VLANs
  NUM  Status   Q  Ports
* 1    Inactive U  So 9/4-11
  2    Active   U  Te 1/1,18/1
  3    Active   U  Te 1/2,19/1
  4    Active   T  Te 1/3,20/1
  5    Active   U  Po 1
  6    Active   U  Te 1/12/1
                U  So 9/0
```

220. Existen soluciones que permiten automatizar la distribución de la información sobre las VLAN creadas en cada conmutador y evitar la configuración manual de la pertenencia a las VLAN creadas en los enlaces troncales entre conmutadores.

221. El protocolo GVRP (GARP VLAN *Registration Protocol*) se utiliza para esta función. Su funcionamiento se basa en el intercambio de información entre conmutadores a través de los enlaces en los que están activados.

222. A continuación, se muestra cómo habilitar GVRP de manera global y también a nivel de puerto:

```
OS10(conf)# grvp enable
```

```
…
OS10(conf-if-te-1/21/1)#switchport
OS10(conf-if-te-1/21/1)#gvr enable
OS10(conf-if-te-1/21/1)#no shutdown
OS10(conf-if-te-1/21/1)#show config
!
interface TenGigabitEthernet 1/21/1
no ip address
switchport
gvrp enable
no shutdown
```

223. Este hecho puede constituir un problema de seguridad, ya que el conmutador propaga la información sobre sus VLAN a través de todos sus puertos y esa información podría ser utilizada para conocer los identificadores de VLAN

utilizados. Por ello, es importante deshabilitar el funcionamiento de GVRP en todos los puertos que no sean troncales o en los que no se necesite su uso.

224. Para deshabilitar GVRP, basta con usar el comando "disable". A continuación, se muestra un ejemplo a nivel global:

```
Dell(conf)# protocol gvrp
Dell(config-gvrp)# disable
```

5.12.5 VLAN PRIVADAS

225. Las VLAN privadas o PVLAN constituyen una manera de limitar la conectividad entre los sistemas pertenecientes a una VLAN, segregándolos en varios conjuntos de puertos o puertos aislados y definiendo qué tráficos están permitidos entre ellos.

226. En una PVLAN existen los siguientes tipos de puertos:

a) **Puertos promiscuos (*promiscuous*)**, que pueden comunicarse con cualquier otro puerto de la VLAN. Son los puertos asignados típicamente a los servidores o routers.

b) **Puertos aislados (*isolated*)**, que solo pueden comunicarse con puertos promiscuos que están en la misma PVLAN.

c) **Puertos de comunidad (*community*)**, que pueden comunicarse con los puertos promiscuos y con los puertos de su misma comunidad (se pueden crear múltiples comunidades de puertos).

d) **Puertos de trunk**, que transportan el tráfico de VLAN entre switches.

227. Para crear una VLAN privada se utilizan varias VLAN de dos tipos distintos:

a) **VLAN primaria**, que es la responsable de distribuir el tráfico desde los puertos promiscuos a las VLAN secundarias en las que residen los puertos aislados o de comunidad. Los puertos promiscuos deben pertenecer a esta VLAN.

b) **VLAN secundarias (de comunidad o aislada),** que son aquellas a las que pertenecen los puertos o conjuntos de puertos que no deben tener conectividad entre ellos. Típicamente se crea una VLAN secundaria para los puertos aislados y otra por cada comunidad que se utilice. Para poder usar una VLAN secundaria es necesario asociarla a una VLAN primaria.

228. Los pasos a seguir en la creación de una PVLAN, son los siguientes:

a) **Paso 1**: crear los puertos que se asignarán a la PVLAN con el comando "*mode switchport mode private-vlan {host | promiscuous | trunk}*", siendo host un puerto aislado o de comunidad:

```
OS10#conf
OS10(conf)#interface Ethernet 2/1/1
OS10(conf-if-eth-2/1/1)#switchport mode private-vlan promiscuous
OS10(conf)#interface Ethernet 2/2/1
OS10(conf-if-eth-2/2/1)#switchport mode private-vlan host
OS10(conf)#interface Ethernet 2/3/1
OS10(conf-if-eth-2/3/1)#switchport mode private-vlan trunk
OS10(conf)#interface Ethernet 2/2/1
OS10(conf-if-eth-2/2/1)#switchport mode private-vlan host
OS10(conf)#interface port-channel 10
OS10(conf-if-po-10)#switchport mode private-vlan promiscuous
```

b) **Paso 2**: crear una VLAN primaria siguiendo los siguientes pasos:

- Acceder al modo de *interface VLAN* en la VLAN en la que se quiere asignar interfaces PVLAN, con el comando "*interface vlan vlan-id*".
- Habilitar la VLAN desde el modo *interface VLAN*, con el comando "*no shutdown*".
- Establecer el modo PVLAN primario a la VLAN seleccionada, con el comando "*private-vlan mode primary*".
- Mapear las VLAN secundarias a la primaria seleccionada anteriormente, con el comando "*private-vlan mapping secondary-vlan vlan-list*" siendo *vlan-list* un rango o bien VLAN separadas por comas.
- Añadir los puertos promiscuos como interfaces etiquetados o no, con el comando "*tagged interface*" o "*untagged interface*".
- Opcional: asignar una IP a la VLAN, con el comando "*ip address ip_address*".
- Opcional: Habilitar/deshabilitar las comunicaciones a nivel 3 entre VLAN secundarias, con el comando "*ip local-proxy-arp*".

c) **Paso 3**: crear una VLAN de comunidad, que es una VLAN secundaria en una PVLAN:

- Acceder al modo de *interface VLAN* en la VLAN en la que se quiere asignar interfaces PVLAN, con el comando "*interface vlan vlan-id*".
- Habilitar la VLAN desde el modo *interface VLAN*, con el comando "*no shutdown*".
- Establecer el modo PVLAN de comunidad a la VLAN seleccionada, con el comando "*private-vlan mode community*".
- Añadir uno o más puertos de tipo host a la VLAN, con el comando "*tagged interface*" o "*untagged interface*".

d) **Paso 4**: crear una VLAN aislada, que es una VLAN secundaria en VLAN primaria:

- Acceder al modo de *interface VLAN* en la VLAN en la que se quiere asignar interfaces PVLAN, con el comando "*interface vlan vlan-id*".

- Habilitar la VLAN desde el modo *interface VLAN*, con el comando "*no shutdown*".
- Establecer el modo PVLAN aislado a la VLAN seleccionada, con el comando "*private-vlan mode isolated*".
- Añadir uno o más puertos de tipo host a la VLAN, con el comando "*tagged interface*" o "*untagged interface*".

229. Un ejemplo de configuración sería el siguiente:

```
OS10#conf
OS10(conf)# interface vlan 10
OS10(conf-vlan-10)# private-vlan mode primary
OS10(conf-vlan-10)# private-vlan mapping secondary-vlan 100-101
OS10(conf-vlan-10)# untagged eth 2/1/1
OS10(conf-vlan-10)# tagged eth 2/3/1

OS10(conf)# interface vlan 101
OS10(conf-vlan-101)# private-vlan mode community
OS10(conf-vlan-101)# untagged eth 2/10/1

OS10(conf)# interface vlan 100
OS10(conf-vlan-100)# private-vlan mode isolated
OS10(conf-vlan-100)# untagged eth 2/2/1
```

5.12.6 PROTECCIÓN FRENTE A ENVÍO DE MENSAJES DE CONTROL STP

230. Cuando se utiliza el protocolo *Spanning Tree* (STP) en una red compuesta por varios conmutadores es muy importante protegerse frente al posible envío de mensajes de control (BPDU) falsos generados desde los puertos de acceso a la red.

231. Estos mensajes BPDU (*Bridge Protocol Data Unit*) son mensaje de datos que se intercambian entre los conmutadores pertenecientes a una LAN extendida que usa una topología STP.

232. Existen múltiples ataques documentados que mediante el envío de estas BPDU falsas permiten redirigir la información hacia sistemas fraudulentos (ataques *man-in-the-middle*) o simplemente interrumpir el servicio (ataques de denegación de servicio).

233. Es por ello imprescindible proteger los conmutadores para que solo acepten BPDUs procedentes de los puertos que los conectan con otros conmutadores y descartar todas aquellas BPDUs recibidas a través de puertos de acceso.

234. Existen varias versiones de STP: STP clásico (802.1d), *Rapid STP* (RSTP, 802.1w) y *Multiple STP* (MSTP, 802.1s). Mientras STP puede tardar de 30 a 50 segundos para responder a un cambio de topología, RSTP es típicamente capaz de responder a los cambios en unos pocos segundos.

235. RSTP es esencialmente lo mismo que STP, pero proporciona una convergencia e interoperabilidad más rápida entre *switches* que STP o MSTP.

236. En MSTP cada instancia *Spanning Tree* puede contener varias VLAN y cada una es independiente de otras instancias. Este enfoque proporciona varias rutas de

reenvío para el tráfico de datos, habilita el equilibrio de carga y reduce el número de instancias de Spanning Tree necesarias para soportar un gran número de VLAN.

237. En OS10 soporta las siguientes extensiones de BPDU y así descartar el tráfico de la interface cuando se produce una violación de BPDU:

```
OS10(conf-if-eth1/1/1:1)# spanning-tree {bpdufilter | bpduguard } | [enable | disable}
OS10(conf-if-eth1/1/1:1)# spanning-tree guard {loop | root | none}
```

a) *BPDU filtering*. Detiene el envío o la recepción de BPDU de un dispositivo defectuoso, protegiendo la red de imprevistos inundación de BPDU. Habilitar el filtrado BPDU en una interfaz hace que el sistema deje de enviar o recibir BPDU.

b) *BPDU guard*. Bloquea los puertos con puente L2 y los puertos LAG conectados a los hosts y servidores finales para que no reciban ningún BPDU. Cuando habilita la protección BPDU y cuando las tramas BPDU se reciben en la interfaz, el puente o LAG se coloca en estado de bloqueo. En caso de un LAG, los puertos se bloquean STP o apagado basado en la acción del comando de desactivación de error. El tráfico de datos se cae, pero el puerto continúa para reenviar BPDU a la CPU que luego se descartan. Para evitar una mayor recepción de BPDU, deberá configurarse un puerto para apagar con el comando *error disable*.

c) *Root guard.* Conserva la posición del puente raíz durante las transiciones de red. STP selecciona el puente raíz con el más bajo valor de prioridad. Durante las transiciones de red, otro puente con una prioridad más baja puede intentar convertirse en el puente raíz y provocar un comportamiento de red impredecible. Para evitar tal intento y preservar la posición del puente raíz, configurar el comando raíz de protección del árbol de expansión. Esta configuración coloca el puerto en un estado inconsistente si el puerto recibe BPDU superior. La protección contra la raíz está habilitada solo en puertos designados. La configuración de *root guard* se aplica a todas las VLAN configuradas en el puerto.

d) *Loop guard*. Evita bucles de reenvío L2 causados por un cable o una falla del hardware de la interfaz. Cuando una falla de hardware ocurre, un enlace de árbol de expansión participante se vuelve unidireccional y el puerto deja de recibir BPDU. Cuando el puerto bloqueado deja de recibir BPDU, pasa a un estado de reenvío que causa el árbol de expansión bucles en la red. Habilitar la protección de bucle mediante el comando de bucle de protección de árbol de expansión en un interfaz para que pase al estado *Loop-Inconsistent* hasta que reciba BPDU. Después de que las BPDU recibido, el puerto sale del estado *Loop-Inconsistent* o *Blocking* y pasa a un estado apropiado estado determinado por STP. Habilitar la protección de bucle por puerto lo habilita en todas las VLAN configuradas en el puerto.

238. Una vez activado el comando, si se recibe una BPDU por alguno de los puertos especificados, se descartará la BPDU y se deshabilitará el puerto.

```
OS10(conf-if-eth1/7/1:1)# do show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32769, Address c03e.bada.e780
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32769, Address c03e.bada.e780
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Flush Interval 200 centi-sec, Flush Invocations 2
Flush Indication threshold 5

OS10(conf-if-eth1/7/1:1)#do show ip interface brief
Interface Name            IP-Address          OK       Method       Status      Protocol
================================================================================================
Ethernet 1/1/1:1          unassigned          NO       unset        up          down
```

239. Una vez que un puerto ha sido apagado al recibir una BPDU, por defecto permanece deshabilitado hasta que se realice el comando "*no shutdown*" en el puerto. Es posible configurar una recuperación del puerto en el caso que se quiera dar una opción automática de recuperación. Para esto, se puede configurar el *auto recovery* mediante el comando:

```
OS10# errdisable recovery cause {bpduguard | mac-move-violation | mac-learn-limit-violation}
```

240. Y, por último, para visualizar el tipo de guarda, se usa el comando:

```
OS10# show spanning-tree guard
Interface
Name             Instance  Sts        Guard type
-----------------------------------------------
Ethernet1/1/1:1  VLAN 1    BLK        Rootguard
```

5.12.7 LISTAS DE ACCESO IP

241. Las listas de acceso (Access Control List o ACL) son un método de filtrado de flujos de datos. Pueden ser usadas para restringir el acceso a la gestión del equipo de una forma más precisa y para realizar el filtrado de tráfico que atraviesa el equipo. Aplicadas a los conmutadores, las ACL se basan en un conjunto de filtros que determinan la autorización (reglas de tipo *permit*) o denegación (reglas de tipo *deny*) del tráfico en función de campos de las cabeceras de los paquetes tales como las direcciones IP y puertos, tanto origen como destino, o el protocolo.

242. Por cada paquete recibido, las reglas que componen una ACL se evalúan línea a línea hasta que se encuentra una coincidencia. Por esta razón, **hay que definir primero las reglas más específicas y posteriormente las más generales**. Es importante recordar que las listas de acceso tienen una denegación implícita al final (**todo el tráfico se filtra por defecto salvo que se permita explícitamente**). Por ello, en el caso en que queramos restringir un determinado tráfico, debemos asegurarnos de permitir el resto de tráfico en una regla final. De ahí la importancia de escribir in orden las reglas de ACL.

243. Las ACL pueden aplicarse, entre otros, a puertos específicos o a VLAN completas. También es posible definir ACL asociadas a usuarios o grupos de usuarios concretos

que se cargan dinámicamente desde servidores RADIUS tras el proceso de autenticación. Por ello, es importante tener en cuenta que varias ACL pueden estar aplicándose simultáneamente a un determinado tráfico.

244. Se permite crear listas de acceso tanto para IPv4 como IPv6. Aunque sólo se muestran en este apartado los principales comandos para crear listas para IPv4, su utilización para IPv6 es inmediata, sin más que cambiar el formato de las direcciones.

5.12.7.1 TIPOS DE ACLS

245. Existen dos tipos de ACL según el procedimiento usado para definirlas:

a) Las **ACLs estáticas** se configuran mediante comandos en el propio equipo. Pueden ser usadas para asignarlas a puertos o a VLAN con el objeto de restringir el tráfico entrante o saliente.

b) Por el contrario, una **ACL dinámica** no se define en el propio equipo, sino que se configura en un servidor RADIUS y se carga dinámicamente en el conmutador como resultado de un proceso de autenticación. La existencia de las ACL dinámicas está ligada a la sesión de autenticación: una vez el cliente cierra la sesión, se libera la ACL.

246. En este apartado nos centramos únicamente en las ACL estáticas.

247. Según su aplicación, podemos distinguir también varios tipos: ACL para VLAN o grupo de VLAN, ACL para conjunto de puertos, *Ingress* ACL (aplicada a interfaces y tráfico de entrada en el sistema), *Egress* ACL (aplicada a *line cards* y tráfico de salida del sistema) y ACL comunes de IP.

248. Según cómo se especifica el tráfico a filtrar, existen dos tipos de listas de acceso:

a) ***ACL standard***, que filtran el tráfico únicamente en función de las direcciones IP origen. Se identifican mediante un nombre o un número en el rango 1-99.

b) ***ACL extendida***, que permiten filtrar el tráfico basándose en un número de campos mucho más amplio, principalmente las direcciones IP y los puertos, tanto origen como destino, así como los protocolos y puertos utilizados. También se identifican mediante un nombre o un número en el rango 100-199.

249. Dada su mayor expresividad y potencial se recomienda siempre utilizar listas de acceso extendidas.

5.12.7.2 CREACION DE ACLS

250. Para crear una nueva lista de acceso se debe usar el comando:

```
OS10(conf)# ip access-list [standard | extended] acces-listname
```

a) [*standard | extended]*: se selecciona el tipo de lista, estándar o extendida.

b) *access-listname*: define el identificador de la lista de acceso. El rango es 1-99 para lista estándar y 100- 199 para listas extendidas.

251. A continuación, se configura el filtro dentro del modo *config-std-nacl*:

```
{deny | permit} {source [mask] | any | host ip-address} [count [byte] [dscp] [order] [monitor
[session-id]] [fragments]
```

a) *source*: determina el origen.

b) *mask*: identifica una máscara.

c) *any*: representa cualquier dirección.

d) *host*: especifica una determinada dirección IP.

e) *monitor*: permite monitorizar la sesión con un determinado identificador.

252. El comando completo para una lista estándar es el siguiente:

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [byte]
[dscp] [order] [monitor [session-id]] [fragments]
```

253. Cabe mencionar que cuando se asignan números de secuencia a estas listas, puede que haya que insertar un nuevo filtro. Para evitar reconfigurar múltiples filtros, la opción óptima es asignar números de secuencia en múltiplos de cinco. De tal forma en caso de necesitar añadir nuevas reglas, se dispone de huecos.

254. A continuación, se muestra un ejemplo de configuración de **lista estándar:**

```
OS10(config-route-map)#ip access standard acl1
OS10(config-std-nacl)#permit 10.1.0.0/16 monitor 177
OS10(config-std-nacl)#show config
!
ip access-list standard acl1
 seq 5 permit 10.1.0.0/16 monitor 177
Dell(config-std-nacl)#
```

255. El comando completo para una **lista extendida** es el siguiente:

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp | ip | tcp | udp} {source mask
| any | host ip-address} {destination mask | any | host ip-address} [operator port [port]]
[count [byte]] [order] [monitor [session-id]] [fragments]
```

256. A continuación, se muestra un ejemplo de configuración de **lista extendida:**

```
OS10(config-route-map)#ip access standard acl1
OS10(config-std-nacl)#permit 10.1.0.0/16 monitor 177
OS10(config-std-nacl)#show config
!
ip access-list standard acl1
 seq 5 permit 10.1.0.0/16 monitor 177
OS10(config-std-nacl)#

OS10(config-ext-nacl)#seq 15 deny ip host 112.45.0.0 any log monitor 501
OS10(config-ext-nacl)#seq 5 permit tcp 12.1.3.45 0.0.255.255 any
OS10(config-ext-nacl)#show config
!
ip access-list extended dilling
  seq 5 permit tcp 12.1.0.0 0.0.255.255 any
  seq 15 deny ip host 112.45.0.0 any log monitor 501
OS10(config-ext-nacl)#
```

257. Para mostrar las listas de acceso configuradas en un conmutador o los detalles de alguna de ellas se puede utilizar el comando:

```
OS10# show ip access-lists [access-list-name] [interface interface] [in | out] [vrf vrf-name]
```

258. No obstante, existen comandos adicionales para modificar las listas de acceso e introducir nuevas entradas. El detalle de configuración de ACLs se puede consultar en la guía "*Dell EMC SmartFabric OS10 User Guide*" – *REF1*.

5.12.7.3 APLICACION DE LISTAS DE ACCESO

259. Como se ha mencionado antes, las listas de acceso pueden aplicarse directamente a puertos del conmutador, definiendo si aplican al tráfico entrante o saliente (*Ingress ACL* o *Egress ACL*).

260. En el caso de configurar un *Egress ACL* en interfaces físicos, se consigue proteger el sistema de ataques maliciosos e incidentes. Por ejemplo, en un ataque de denegación de servicio en un interfaz específico, se puede bloquear el tráfico y así proteger los dispositivos.

261. Un ejemplo de crear reglas de ACL para tráfico *Egress* y comprobar la configuración, es el siguiente:

```
OS10(conf)# interface Ethernet 1/1/1
OS10 (conf-if-eth-1/1/1)# ip access-group abcd out
OS10(conf-if-eth-1/1/1)# do show running-configuration interface ethernet 1/1/12
!
Ethernet 1/1/1
  no ip address ip access-group abcd out
OS10(conf-if-eth-1/1/1)# end
OS10# configure terminal
OS10(conf)# ip access-list extended abcd
OS10(config-ext-nacl)# permit tcp any any
OS10(config-ext-nacl)# deny icmp any any
OS10(config-ext-nacl)# permit 1.1.1.2
OS10(config-ext-nacl)# end
OS10# show ip accounting access-list
!
Extended Ingress IP access list abcd on ethernet 0/0
  seq 5 permit tcp any any
  seq 10 deny icmp any any
  seq 15 permit 1.1.1.2
```

262. También es posible crear un ACL VLAN *group* de forma que la regla del ACL se aplique a todos los miembros de VLAN. Los pasos para realizarlo son:

a) Crear un ACL VLAN Group con el comando "*acl-vlan-group {group name}*" desde el modo *Privilege EXEC*.

b) Añadir una descripción a este grupo desde el modo *conf-acl-vl-grp* con el comando "description description".

c) Aplicar un *Egress* IP ACL al grupo desde el modo *conf-acl-vl-grp* con el comando "*ip access-group {group name} out implicit-permit*".

d) Añadir los miembros de las VLAN al grupo, desde el modo *conf-acl-vl-grp* con el comando "member vlan {VLAN-range}.

e) Mostrar la configuración creada, como en el siguiente ejemplo:

```
OS10# show acl-vlan-group detail
Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300
Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000
OS10#
```

5.12.8 LISTAS DE ACCESO MAC

263. De forma análoga a las listas de acceso IP descritas en el apartado anterior, se permite filtrar el tráfico en función de campos de las cabeceras de nivel 2 de las tramas Ethernet: direcciones MAC origen y destino, protocolo (Ethertype), identificador de VLAN ID y clase de servicio.

264. La configuración de las listas de acceso de nivel 2 es muy similar a las listas de acceso IP, por lo que los conceptos y pasos a seguir son prácticamente los mismos, por lo que es posible crear listas de acceso estándar y extendidas. Asimismo, las listas pueden ser identificadas por nombre o por número; y también pueden ser asignadas a un puerto o a una VLAN completa.

265. Para crear una MAC ACL se usa el comando "*mac access-list standard mac-list-name*". El formato de las entradas en las listas estándar es el siguiente:

```
seq sequence-number permit | deny {any | mac-source-address [mac-source-address-mask]}
[count [byte]] | [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

266. El formato de las entradas en las listas extendidas es el siguiente:

```
    seq sequence-number {any | host mac-address | mac-source-address mac-source-address-mas
    {any   |   host   mac-address   |   mac-destination-address   mac-destination-address-mas
    [ethertype operator] [count [byte]] | [log] [monitor]
```

267. Destacar que a la hora de especificar la dirección MAC origen o destino se puede especificar una máscara, por lo que es posible filtrar en función de prefijos. Por ejemplo, se podrían permitir o filtrar tramas procedentes de dispositivos de un determinado fabricante.

5.13 PROTECCIÓN FRENTE ATAQUES

268. Existen en la actualidad multitud de ataques posibles encaminados a comprometer la seguridad de nuestros equipos de red, con el objetivo de hacerse con el control de su gestión, obtener copias de la información que viaja por la red o simplemente paralizar el servicio que ofrecen.

269. Muchos de estos ataques clásicos a los conmutadores están documentados y los fabricantes ofrecen ya medidas efectivas que pueden mitigarlos, impidiendo que ocurran. Incluso para los ataques desconocidos, existen medidas que pueden ayudar a detectarlos de forma temprana y poder tomar medidas para paliarlos.

270. A continuación, se detallan algunos de estos ataques y las medidas que se pueden tomar para proteger al producto frente a ellos.

5.13.1 DHCP SNOOPING

271. El ataque conocido como DHCP *Spoofing* se aprovecha de la simplicidad del protocolo DHCP y de la falta de mecanismos estándar que permitan asegurar la autoconfiguración de los sistemas finales mediante DHCP.

272. El ataque se basa en el despliegue de servidores DHCP maliciosos que asignan parámetros de configuración (direcciones IP, dirección del router, etc.) falsos a los sistemas finales, con varios objetivos posibles:

    a) Comprometer la disponibilidad de la red (ataque *DoS*), asignando, por ejemplo, direcciones IP incorrectas a los equipos para que pierdan la conectividad con el resto de la red.

    b) Redirigir el tráfico de los sistemas finales para que atraviesen otros sistemas maliciosos (ataque *man-in-the-middle*) para interceptar los mensajes enviados y poder realizar acciones como el robo de datos y credenciales.

273. El principal problema que presenta DHCP se debe a la incapacidad de distinguir los servidores legítimos de los que no lo son, que permite el fácil despliegue de servidores DHCP falsos en los sistemas de usuarios conectados a la red.

274. Para evitar ataques del tipo DHCP Spoofing, el producto incluye la funcionalidad DHCP Snooping, que permite informar al conmutador de cuáles son los puertos y direcciones de los servidores DHCP legítimos, con el objetivo de filtrar todos los mensajes DHCP procedentes de servidores no autorizados.

275. Para activar la funcionalidad de DHCP Snooping se debe ejecutar lo siguiente:

    a) Activar DHCP *Snooping* a nivel global:

```
OS10(conf)# ip dhcp snooping
```

    b) Especificar los puertos conectados a los servidores DHCP como de confianza. Desde el modo *interface*, cambiar al modo *interface port extender*:

```
OS10(conf-if-eth1/1/1)# ip dhcp snooping trust
```

c) Habilitar DHCP *Snooping* en una VLAN:

```
ip dhcp snooping vlan name
```

276. Una vez activado en una VLAN, todos los puertos participantes pasan a ser no confiables y cualquier mensaje DHCP de los enviados por los servidores será filtrado. Una vez declarado un puerto como confiable, se aceptarán los mensajes DHCP de servidor procedentes de él, independientemente de la dirección IP de la que procedan.

277. Para mejorar todavía más la seguridad, se puede crear una entrada estática en la tabla de DHCP:

```
OS10(conf)# ip dhcp snooping binding mac mac-address vlan vlan-id ip ip-address interface
[ethernet slot/port/sub-port | port-channel port-channel-id | VLTi]
```

278. Para ver la configuración de DHCP Snooping se pueden usar los siguientes comandos:

```
OS10# show ip dhcp snooping binding
Codes : S - Static D – Dynamic
IPv4 Address   MAC Address              Expires(Sec)    Type    VLAN    Interface
=============================================================================
10.1.1.22      11:22:11:22:11:22        120331          S       100     ethernet1/1/4
33.1.1.44      11:22:11:22:11:23        120331          S       200     port-channel100
103.1.1.5      11:22:11:22:11:24        120331          D               300 ethernet1/1/5:4
```

5.13.2 ARP SNOOPING

279. El protocolo de resolución de direcciones ARP (*Address Resolution Protocol*) es un sencillo protocolo que permite averiguar dinámicamente la dirección MAC que corresponde a una determinada dirección IP en una LAN. Se basa en el envío de mensajes de solicitud (ARP *Request*), normalmente a la dirección de difusión de la LAN, que son contestados por los sistemas aludidos mediante respuestas (ARP *Reply*). La información obtenida mediante ARP se almacena en las tablas ARP que todo sistema IP mantiene.

280. Al igual que DHCP, la sencillez del protocolo lo hace vulnerable a los ataques de falsificación de mensajes ARP o ARP *Spoofing*. El ataque más típico consiste en enviar mensajes ARP falsificados a una LAN para conseguir atraer el tráfico de otros sistemas hacia un sistema malicioso que posteriormente los redirige hacia su destino original.

281. El ataque se realiza envenenando las tablas de ARP de los sistemas de la red, mediante el envío de paquetes ARP *Reply* en los que se asocian las direcciones IP por las que preguntan otros sistemas con la dirección MAC del sistema malicioso. De esta forma los sistemas envenenados enviarán el tráfico hacia el sistema malicioso.

282. Se proporciona una funcionalidad para proteger el funcionamiento del protocolo ARP basándose en la función de DHCP *Snooping*.

283. A grandes rasgos, el funcionamiento de esta protección consiste en que con la inspección dinámica de ARP, se reenvían sólo las tramas de ARP que han sido validadas contra la tabla de *binding* de DHCP. Es decir, el conmutador confiará y distribuirá las respuestas ARP recibidas por los puertos declarados como confiables y las recibidas por los puertos no confiables que aparezcan en la tabla de asociaciones IP-MAC. El resto de respuesta ARP se descartarán.

284. Para activar la función de inspección dinámica de ARP, hay que seguir los siguientes pasos:

    a) Habilitar DCHP *Snooping*.

    b) Validar las tramas de ARP contra la tabla de *binding* de DCHP *Snooping*, con el comando "*arp inspection*" en modo *interface*.

285. Para activar la función de inspección dinámica ARP por VLAN, introducir el siguiente comando:

```
OS10(conf)# arp inspection
```

286. En caso de no querer validar paquetes ARP mediante inspección dinámica ARP, es posible la configuración de un puerto confiable con el siguiente comando en modo interface:

```
arp inspection-trust
```

287. Se pueden visualizar las entradas de la tabla de ARP de la siguiente forma:

```
OS10# show ip arp inspection database
Number of entries : 828
Address               Hardware               Address Interface        VLAN
------------------------------------------------------------------------------
10.2.1.1       00:40:50:00:00:00       port-channel100         vlan3001
10.1.1.13      00:2a:10:01:00:00       port-channel100         vlan3001
10.1.1.62      00:2a:10:01:00:01       port-channel100         vlan3001
```

288. Y las estadísticas que muestran los paquetes ARP válidos e inválidos que han sido procesados, se pueden consultar con el siguiente comando:

```
OS10#show arp inspection statistics

Dynamic ARP Inspection (DAI) Statistics
---------------------------------------
Valid ARP Requests : 0
Valid ARP Replies : 1000
Invalid ARP Requests : 1000
Invalid ARP Replies : 0
OS10#
```

5.13.3 INUNDACIÓN MAC

289. Todo conmutador Ethernet mantiene una tabla de filtrado que utilizan para realizar la función básica de encaminamiento de las tramas que recibe. Esta tabla almacena la asociación entre las direcciones MAC de los equipos conectados a sus puertos y los identificadores de esos puertos.

290. Cuando el conmutador recibe una trama por alguno de sus puertos, extrae la dirección destino y la compara con las entradas de su tabla de filtrado (almacenada en una CAM o *Content-Addressable Memory*). Si la dirección de destino se encuentra en la tabla, reenvía el paquete a través del puerto asociado en la tabla CAM con esa dirección. En caso contrario, si la dirección no está registrada en la tabla, se envía la trama por todos los puertos (difusión).

291. Las entradas en la tabla de filtrado se autoconfiguran automáticamente mediante el algoritmo de aprendizaje hacia atrás: cada vez que llega una trama se aprende de su dirección MAC origen, registrando en la tabla CAM dicha dirección asociada al puerto por el que llegó la trama.

292. Las tablas CAM tienen una capacidad limitada, que típicamente se especifica en la hoja de datos de cada equipo. Cuando esta tabla se llena, el conmutador deja de aprender direcciones y, por tanto, para todas aquellas direcciones destino que no aparezcan en su tabla se verá obligado a hacer difusión de las tramas a través de todos los puertos de la VLAN.

293. Esta situación puede darse en casos en que el número de usuarios conectados a la red supere la capacidad de los conmutadores. Aunque es más frecuente que la causa sean los ataques de Denegación de Servicio (DoS) que tratan de explotar esta vulnerabilidad.

294. Típicamente, estos ataques consisten en enviar un número muy grande de tramas Ethernet con direcciones MAC origen aleatorias, de manera que se llenen las tablas CAM del equipo. Este hecho provocará que el conmutador realice difusión de una parte del tráfico que conmuta, provocando un aumento de la carga de la red o incluso su colapso. Además, provocará un problema añadido de confidencialidad de la información, ya que tramas que deberían enviarse por un puerto concreto se están distribuyendo a todos los puertos de la VLAN.

295. Uno de los mecanismos de prevención consiste en utilizar las medidas ya citadas en apartados anteriores y así limitar el número de direcciones MAC que el conmutador puede aprender en cada puerto.

296. Esta limitación se debe aplicar a los puertos de acceso que conectan equipos de usuario, para evitar que un posible atacante inunde la tabla de filtrado. En los puertos troncales no se suele incluir esta limitación. O si se incluye, se debe tener en cuenta que en esos puertos el número de direcciones asociadas puede ser grande.

297. El número máximo de direcciones MAC permitidas en un interface, se puede configurar con el siguiente comando:

```
OS10(conf)# mac learn {limit | no-limit}
```

298. Para visualizar la tabla de direcciones MAC (asociadas a puertos y VLAN), podemos verlo con el siguiente comando en modo EXEC y EXEC Privilege:

```
show mac-address-table [address mac-address | interface interface | vlan vlan-id] [aging-time]
dynamic | static] [count [vlan vlan-id] [interface interface-type [slot [/port[/subport]]]]]
```

a) *address mac-address* (opcional): define la dirección MAC en formato xx:xx:xx:xx:xx:xx.

b) *dynamic* (opcional): muestra las direcciones MAC aprendidas dinámicamente.

c) *static* (opcional): muestra las direcciones MAC configuradas específicamente en el switch.

d) *aging-time*: muestra la información del tiempo de *aging*.

e) *interface interface* (opcional): identifica el *interfaz*.

f) *interface interface-type* (opcional): define el tipo de *interface*, seguido del número de *slot*.

g) *vlan vlan-id* (opcional): identifica la dirección MAC asignada a una determinada VLAN. EL rango es de 1 a 4094.

h) *count* (opcional): define el total de direcciones MAC, ya sean estáticas asociadas a interfaces específicos, dinámicas o en general todas las que haya en uso.

6. FASE DE OPERACIÓN

299. Durante la fase de operación del producto se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

a) Revisar las alertas que genera en sistema, tanto en la consola CLI como en el servidor *syslog* configurado.

b) Realizar copias de la configuración actual (*running-config)* a la configuración de arranque (*startup-config*) de forma periódica.

c) Exportar las copias de seguridad de la configuración de forma periódica a un servidor externo.

d) Controlar el acceso a la información de auditoría, de tal forma que únicamente el personal designado pueda acceder a ella.

e) Comprobar si hay nuevas actualizaciones de software disponibles, con el objetivo de mantener el sistema actualizado siempre a la última versión.

f) Gestionar los usuarios, permitiendo el acceso solo a los usuarios necesarios en cada momento.

7. CHECKLIST

300. En esta sección se incluye una lista de verificación con cada una de las recomendaciones sobre configuraciones seguras que se han comentado a lo largo del documento.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Consideraciones Previas	☐	☐	
Instalación	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro/FIPS	☐	☐	
Activación del modo Secure-CLI	☐	☐	
AUTENTICACIÓN			
Configuración autenticación local	☐	☐	
Configuración RADIUS	☐	☐	
Configuración TACACS+	☐	☐	
ADMINISTRACIÓN			
Configuración de usuarios	☐	☐	
Configuración de roles y niveles de privilegio	☐	☐	
Configuración de las sesiones locales	☐	☐	
Configuración de las sesiones remotas	☐	☐	
Desactivación de Telnet	☐	☐	
Configuración SSH y SNMP	☐	☐	
CONFIGURACIÓN			
Configuración control del tráfico	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Creación de certificados	☐	☐	
Configuración del protocolo NTP	☐	☐	
Guardado de la configuración	☐	☐	
Creación de la política de contraseñas seguras	☐	☐	
Configuración de la protección contra ataques	☐	☐	
AUDITORÍA			
Registro de Eventos	☐	☐	
Configuración del almacenamiento Local	☐	☐	
Configuración del Almacenamiento Remoto	☐	☐	

8. REFERENCIAS

REF1 *Dell EMC SmartFabric OS10 User Guide. Release 10.5.1*
https://dl.dell.com/topicspdf/dell-emc-smartfabric-os10_users-guide11_en-us.pdf

9. ABREVIATURAS

AAA	*Authentication, Authorization and Accounting*
API	*Application Programming Interface*
ARP	*Address Resolution Protocol*
BPDU	*Bridge Protocol Data Unit*
CAM	*Content-Adressable Memory*
CLI	*Command Line Interface*
DNS	*Domain Name System*
DHCP	*Dynamic Host Configuration protocol*
DoS	*Denial of Service*
ENS	*Esquema Nacional de Seguridad*
FTP	*File Transfer Protocol*
GUI	*Graphical User Interface*
GVRP	*GARP VLAN Registration Protocol*
HTTP	*Hyper Text Transfer Protocol*
HTTPD	*Hyper Text Transfer Protocol Daemon*
HTTPS	*Hyper Text Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
LAN	*Local Area Network*
LLDP	*Link Layer Discovery Protocol*
MAC	*Media Access Control*
MIB	*Management Information Base*
MSTP	*Multiple Spanning Tree Protocol*
NTP	*Network Time Protocol*
PVLAN	*Private VLAN*
RADIUS	*Remote Authentication Dial-in User Service*
RBAC	*Role Based Access Control*
REST	*Represantional State Trasnfer*
RSTP	*Rapid Spanning Tree Protocol*
SCP	*Secure Copy Protocol*
SNMP	*Simple Network Management Protocol*

SNTP	*Simple Network Time Protocol*
SSH	*Secure Sehll*
STP	*Spanning Tree Protocol*
TACACS	*Terminal Access Controller Access Control System*
TCP	*Transmision Control Protocol*
TFTP	*Trivial File Transfer Protocol*
TLV	*Type-Length-Value*
UDP	*User Datagram Protocol*
USB	*Universal Serial Bus*
VLAN	*Virtual Local Area Network*

PUBLICACIONES DE DEFENSA

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