centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1402

Procedimiento de Empleo Seguro
DELL EMC OS 9.14

Junio de 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.06.15 14:12:22 +02'00'

NIPO: 083-21-117-6

Fecha de Edición: junio de 2021

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

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura para la familia de equipos Dell EMC con sistema operativo **Dell EMC Networking OS 9.14**.
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 una lectura del documento completo para conocer de todas las funcionalidades descritas.

2. OBJETO Y ALCANCE

4. El objeto de este documento es analizar los mecanismos de seguridad disponibles para proteger los entornos de sistemas de información y comunicaciones que emplean los *switches Dell EMC* con sistema operativo **Dell EMC Networking OS 9.14**. Como consecuencia, se establece un marco de referencia que contempla las recomendaciones STIC en la implantación y utilización de los switches.
5. En líneas generales, en este documento no se valora la idoneidad de utilizar o no determinados protocolos, sino que busca describir cómo deben ser securizados.
6. Queda fuera del alcance de este documento la configuración de los mecanismos para garantizar la calidad de servicio necesaria para la explotación del dispositivo ya que se entiende que la calidad del servicio no afecta a la seguridad de este.
7. 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

8. 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, antes de proceder a la instalación del producto.

   b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   e) **Apartado 8.** En este apartado se incluye un breve *checklist* de acciones de configuración del producto.

   f) **Apartado 9.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

   g) **Apartado 10.** Incluye un listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Al recibir el equipo, deben verificarse los siguientes aspectos:
    - El embalaje es el original y no ha sido manipulado su sellado.
    - El equipo no debe presentar señales de haber sido manipulado o abierto.
    - 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.
10. 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.
11. 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"*, el cual mostrará la versión del sistema operativo instalado (ver apartado 6.6.1 Versión del software instalada).
12. En caso de cualquier duda al respecto puede descargarse el mismo y validarse su integridad.

4.2 CONSIDERACIONES PREVIAS

13. El objetivo de la guía es establecer un marco que permita incrementar la seguridad de un equipo. Por un lado, describe los mecanismos que evitan accesos no deseados a la administración del equipo y a los datos almacenados en él. Por otro lado, analiza los servicios y sus interacciones con la red en la que será integrado, con el objeto de diferenciar las acciones seguras y necesarias en el equipo de las acciones que no lo son y deben ser sustituidas por otras.
14. Es necesario aplicar los consejos de seguridad que contiene esta guía, al menos los relativos a proteger el acceso a la gestión del equipo y la deshabilitación de los servicios no necesarios, antes de desplegar el equipo en la red, con el objeto de evitar posibles incidentes antes de que las protecciones estén activas.
15. Asimismo, antes de desplegar el equipo es imprescindible realizar una actualización del mismo con las últimas versiones estables del sistema operativo, con el objeto de protegerlo de los problemas de seguridad detectados en versiones anteriores.
16. Esta guía no pretende ser un manual de configuración de los conmutadores Dell EMC sino un conjunto de recomendaciones y normas para efectuar su configuración de forma segura. Es importante, sin embargo, repasar algunos conceptos básicos relativos a la configuración mediante la línea de comandos, la gestión de usuarios o la actualización del *software*.

5. FASE DE INSTALACIÓN

17. Es muy importante tener en cuenta que la configuración inicial del equipo cuando procede de fábrica o después de haberse reseteado **es insegura**. Cabe decir que cuando se reinstala de fábrica, se elimina la configuración de NVRAM, *startup-config* y el resto de los atributos configurados. Sin embargo, no se elimina ni el *filesystem* ni los certificados de confianza.
18. A nivel general, una versión de Dell EMC Networking OS 9.14 está precargada en el sistema. De igual forma, el sistema viene con una configuración por defecto cuando se enciende por primera vez (excepto el *hostname* por defecto que es Dell). Es por ello que es necesario configurar el sistema mediante la CLI de acuerdo a los requerimientos necesarios.
19. A través del puerto de consola serie se puede acceder a esta 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.
20. 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 apartados posteriores de esta guía.
21. 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.

6. FASE DE CONFIGURACIÓN

6.1 GESTIÓN DEL PRODUCTO

22. Los equipos Dell EMC con sistema Dell EMC Networking OS 9.14 son equipos completamente gestionables, que permiten al administrador de red configurar el equipo mediante línea de comandos e interfaz gráfico.
23. 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**.
24. 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.
25. La CLI está estructurada en diferentes modos de acuerdo a propósitos de seguridad y gestión. Así pues, Dell Networking OS CLI está dividido principalmente en tres (3) niveles con su *prompt* específico de la línea de comandos:

    - **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 "**>**".
    - **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***".
    - **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	*Dell>*	Acceso por consola o terminal line
EXEC Privilege	*Dell#*	Acesso desde modo EXEC con el comando *enable*. Desde otro modo, usando comando *end*
Configuración	*Dell(conf)#*	Acesso desde modo EXEC Privilege con el comando *configure*. Desde otro modo (excepto EXEC y EXEC Privilege), usando comando *exit*

26. Para cerrar una sesión CLI, ya sea por consola o remotamente (SSH o Telnet), usar el comando "*exit*" desde modo *EXEC* o *EXEC Privilege*.

27. 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:

    ```
    Dell(conf)# no username sistemas
    ```

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

    ```
    Dell# copy running-config startup config
    ```

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

    ```
    Dell# show logging
    ```

6.2 AUTENTICACIÓN

30. El producto permite la autenticación de usuarios de forma local y 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+. En general, es conveniente desde el punto de vista de la seguridad y la gestión utilizar la segunda opción, ya que facilita la gestión de usuarios y la protección de la información al estar esta centralizada. En cualquier modo, en redes de pequeño tamaño la autenticación local es una opción válida.

31. 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 debe ser 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.

6.2.1 MÉTODOS DE AUTENTICACIÓN

6.2.1.1 AUTENTICACIÓN LOCAL (MODO CLÁSICO)

32. En este caso los usuarios y sus credenciales son definidos y almacenados localmente en el conmutador. Dentro de la autenticación local, el modo más simple es el modo clásico (ver adicionalmente modo RBAC en apartado 6.3.1), en el que sólo existe un usuario para cada uno de los dos (2) modos de administración: *EXEC* y *EXEC Privilege*, descritos en el apartado 6.3 Gestión de permisos de usuarios. El único usuario inicialmente existente es *admin* con privilegios máximos para poder ejecutar comandos en los dos (2) modos de privilegios definidos. Inicialmente carece de contraseña, por lo que una de las primeras tareas a realizar debe ser la protección de esas cuentas con una contraseña.

33. Para asignar una contraseña y modificar el nombre de usuario, se puede utilizar el comando:

```
Dell(conf)# username name [access-class access-list-name] [nopassword | {password | secret
| sha256-password} [encryption-type] password] [privilege level] [role role-name]
```

34. Se recomienda el uso de sha256 (*sha256-password*) y evitar el uso de texto plano.

35. Asimismo, el tipo de cifrado (*encryption-type*) es 0 por defecto si se usa texto plano, y 7 si la contraseña ya está cifrada usando un código hash.

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

```
Dell(conf)# enable sha256-password {0 cleartext-password | 8 encrypted-password}
```

37. El tipo de cifrado es 0 por defecto si se usa texto plano, 5 si la contraseña ya está cifrada usando un código hash MD5, 7 si la contraseña ya está cifrada usando un código hash DES, y 8 si la contraseña está cifrada usando *sha256*. **Se debe utilizar, como en el ejemplo, sha256.**

38. 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 (2) 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:

```
no aaa authentication login default local
```

39. Se pueden crear nuevos usuarios y asignarles niveles de privilegio mediante el comando:

```
Dell(conf)# username name [access-class access-list-name] [nopassword | {password | secret
| sha256-password} [encryption-type] password] [privilege level] [role role-name]
```

40. Los niveles de privilegio son fijos en el sistema y pueden definirse para cada tipo de acción entre los niveles 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 es 1, si no se especifica ningún valor, y para todos los comandos de configuración es 15. Por tanto, un usuario debe tener nivel de privilegio 15 para poder modificar configuraciones del sistema, bajo la configuración por defecto del dispositivo.

41. El nivel de privilegio necesario para cada comando puede alterarse con el comando:

```
privilege mode {level level command | reset command}
```

6.2.1.2 AUTENTICACIÓN MEDIANTE SERVIDOR RADIUS

42. En este caso, los usuarios y sus credenciales se definen y almacenan en un servidor RADIUS 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.
43. RADIUS es un protocolo estandarizado que define un sistema distribuido con topología cliente/servidor que protege a las redes de accesos no autorizados. El cliente de RADIUS es ejecutado en los conmutadores o enrutadores, los cuales envían peticiones de autenticación a un servidor central, el cual contiene toda la información de usuario (*Authentication*, *Authoritation* y *Accounting* de ese usuario).
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. *Dell Networking OS 9.14* permite configurar un método de autenticación en el *login* mediante el comando "*aaa authentication login*". Para ello, es necesario crear una lista de métodos de tipo AAA con el siguiente comando.
46. Primero se crea cadena de texto de máximo 16 caracteres como el nombre de la lista de métodos que se quiere usar con método de autenticación de RADIUS.

```
Dell(conf)# aaa authentication login method-list-name name
```

47. Después se crea una lista de métodos con RADIUS y TACACS+ como métodos de autorización. El típico orden de los métodos es: RADIUS, TACACS+, Local (para hacer uso de la autenticación local como respaldo), *None* (si no se define método secundario). Si RADIUS deniega la autorización, la sesión termina.

```
Dell(conf)# aaa authorization exec {method-list-name | default} radius tacacs+ local
```

48. Además, para habilitar la autenticación de RADIUS AAA en el *login* para una determinada lista de métodos, hay que aplicarlo a la línea terminal. Para ello se entra en el modo line:

```
Dell(conf)# line {aux 0 | console 0 | vty number [end-number]}
```

49. A continuación, se habilita la autenticación de login AAA con el comando "*login authentication {method-list-name | default}*" para usar la lista de métodos ("*authorization exec methodlist*").

50. Para consultar la configuración de los métodos de autenticación utilizados se puede utilizar el comando:

```
Dell# show authentication methods
```

51. Para mostrar los intentos de autenticación de RADIUS, fallos y estadísticas básicas, se puede usar el comando:

```
Dell# show radius statisctics
```

52. Para visualizar la información en las transacciones de RADIUS para la resolución de problemas, se puede utilizar el comando:

```
Dell# debug radius
```

53. Dell EMC Networking OS 9.14 permite la configuración de múltiples servidores RADIUS, así como agruparlos para proporcionar un mecanismo de redundancia en caso de fallo de alguno de ellos.

54. Para definir un servidor RADIUS y, opcionalmente, la clave de sesión a usar se utiliza el comando:

```
Dell(conf)# radius-server host {hostname | ip-address} [auth-port port-number] [retransmit retries] [timeout seconds] [key [encryption-type] key]
```

    - auth-*port port-number*: el rango es de 0 a 65535. Hay que especificar un Puerto UDP. Por defecto es el 1812.
    - *retransmit retries*: el rango es de 0 a 100. Por defecto el valor es 3.
    - *timeout seconds*: el rango es de 0 a 1000. Por defecto el valor es 5 segundos.
    - *key [encryption-type] key*: 0 para texto plano o bien 7 para texto cifrado, 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.

55. Para especificar múltiples servidores RADIUS, se debe ejecutar el comando "***radius-server host***" múltiples veces. Cuando *Dell EMC Networking OS 9.14* intenta autenticar a un usuario, el *software* conecta con los servidores RADIUS de uno en uno, hasta que estos responden con una aceptación o rechazo.

56. La configuración RADIUS se puede visualizar con el comando:

```
Dell# show running-config radius
```

57. Y para eliminar un servidor RADIUS, puede realizarse con el comando:

```
Dell# no radius-server host {hostname | ip-address}
```

58. Adicionalmente, se pueden establecer parámetros de comunicación global para todos los servidores RADIUS. Por ejemplo, fijar el intervalo de tiempo en el que un servidor es declarado inactivo:

```
Dell(conf)# radius-server deadtime seconds
```

- *seconds: el* rango *es de 0 a 2147483647. Por defecto el valor es 0 segundos.*

59. Al igual que se ha mencionado antes para un único servidor, también se puede configurar de manera global una clave para todas las comunicaciones RADIUS entre el sistema y los servidores RADIUS, el número de peticiones de retransmisión y el intervalo de tiempo que el sistema espera una respuesta de un servidor RADIUS:

```
Dell(conf)# radius-server [encryption-type] key]
Dell(conf)# radius-server retransmit retries
Dell(conf)# radius-server timeout seconds
```

60. Para más información sobre RADIUS puede consultarse el capítulo "*Security*" de la guía "*Dell Networking OS Command Reference Guide 9.14" – REF1.*

6.2.1.3 AUTENTICACIÓN MEDIANTE SERVIDOR TACACS+

61. En Dell EMC Networking OS 9.14 es posible también gestionar el acceso a la configuración de los equipos de forma centralizada mediante servidores TACACS+.

62. Para usar TACACS+ en la autenticación de usuarios, hay que especificar el menos un servidor TACACS+ con el que el sistema puede comunicarse y configurar TACACS+ como uno de los métodos de autenticación. Se puede usar este comando múltiple veces para configurar múltiples servidores TACACS+:

```
Dell(conf)# tacacs-server host {ip-address | host}
```

63. A continuación, hay que introducir una cadena de caracteres (máximo 16 caracteres) como el nombre de la lista de métodos que se quiere usar con el método de autenticación de TACACS. Reseñar que el método TACACS+ no puede ser el último especificado:

```
Dell(conf)# aaa authentication login {method-list-name | default} tacacs+ […method3]
```

64. Además, para habilitar la autenticación de TACACS+, hay que aplicarlo a la línea terminal. Para ello se entra en el modo line:

```
Dell(conf)# line {aux 0 | console 0 | vty number [end-number]}
```

65. A continuación, se habilita la autenticación de *login AAA* con el comando:

```
login authentication {method-list-name | default}
```

66. Para consultar la configuración de los métodos de autenticación utilizados se puede utilizar el comando:

```
Dell# show authentication methods
```

67. Para visualizar la información en las transacciones de TACACS+ para la resolución de problemas, se puede utilizar el comando:

```
Dell# debug tacacs+
```

68. Para definir un servidor TACACS+ y, opcionalmente, la clave de sesión a usar se utiliza el comando:

```
Dell(conf)# tacacs-server host {hostname | ip-address} [port port-number] [timeout seconds]
[key key]
```

- *port port-number:* el rango es de 0 a 65535. Hay que especificar un Puerto TCP. Por defecto es el 49.
- *timeout seconds*: el rango es de 0 a 1000. Por defecto el valor es 10 segundos.
- *key key*: Esta clave puede tener como máximo 42 caracteres de largo y debe coincidir con la clave configurada en el servidor TACACS+.

69. Para más información sobre TACACS+ puede consultarse el capítulo "*Security*" de la guía "*Dell Networking OS Command Reference Guide 9.14" – REF1.*

6.3 GESTIÓN DE PERMISOS DE USUARIOS

70. En el producto existen dos (2) formas de controlar los permisos asignados a los usuarios que acceden al equipo para gestionarlo:

    - **Modo Clásico**. Es el modo por defecto y en él existen, como ya se ha mencionado previamente, dos (2) modos con niveles de permisos preasignados: *EXEC* y *EXEC Privilege*. Este modo se describe en el apartado 6.2.1.1 Autenticación local (modo clásico).
        - **Modo *EXEC***, con acceso parcial a la gestión del conmutador, que le permite únicamente inspeccionar el estado del equipo y los eventos que en él se producen.
        - **Modo *EXEC Privilege***, con acceso total al conmutador y a todos los contextos de configuración con permisos de lectura y escritura, posibilitando con ello la realización de todo tipo de cambios en la configuración.
    - **Modo RBAC (Role Based Access Control).** Este nuevo modo permite definir usuarios adicionales a los modos por defecto, así como especificar de forma precisa los permisos asignados a cada usuario.

71. Tal como se describe en la siguiente sección, mediante la creación de perfiles (roles), este modo permite crear nuevos usuarios definiendo sus capacidades para la configuración, inspección y ejecución de comandos relativos a las diversas funcionalidades que ofrece el equipo. La definición de los roles es local al equipo y la autenticación de los usuarios se puede realizar localmente o mediante servidores RADIUS o TACACS+. Además, cada usuario sólo puede tener un role, mientras que varios usuarios pueden tener el mismo role.

6.3.1 MODO RBAC

72. Por defecto, *Dell EMC Networking OS 9.14* incluye definidos cuatro (4) roles de usuario de sistema, pudiendo llegar hasta 8. Destacar que estos roles predefinidos no se pueden eliminar:

- ***Operador de Red* (netoperator)**: no tiene privilegio para modificar la configuración del *switch*. Se puede acceder en modo *EXEC* (monitorización) para ver la configuración actual e información del estado.
- **Administrador de Red (*netadmin*)**: puede configurar, mostrar y hacer debug de las operaciones de red en el *switch*. Se puede acceder a todos los comandos disponibles desde este role. Sin embargo, desde aquí no se puede acceder a los comandos disponibles al administrador de seguridad de red para operaciones de criptografía, AAA o comandos únicamente reservados para el administrador del sistema.
- **Administrador de Seguridad (*secadmin*)**: puede controlar la política de seguridad en los sistemas de un mismo dominio o topología de red. Los comandos de este rol incluyen la habilitación del modo FIPS, políticas de contraseñas, *timeouts* de inactividad, establecimiento de *banner*, y las operaciones de clave criptográfica para el acceso seguro de caminos.
- **Administrador de Sistema (*sysadmin*)**: este role tiene acceso completo a todos los comandos del sistema, acceso exclusivo a los comandos que manipulan el formateo del fichero, y acceso a la *shell* del sistema. Asimismo, también puede crear IDs y roles de usuario.

73. La siguiente tabla detalla los modos que dichos roles predefinidos pueden acceder:

Role	Modo
netoperator	-
netadmin	*Exec Config Interface Router IP Route-map Protocol MAC*
secadmin	*Exec Config Line*
sysadmin	*Exec Config Interface Line Router IP Route-map Protocol MAC*

74. Los roles definidos en un equipo pueden consultarse con el comando:

```
Dell# show userroles
```

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

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

6.3.1.1 REGLAS PARA LA DEFINICIÓN DE ROLES

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

```
Dell(conf)# userrole name [inherit existing-role-name]
Dell(conf)# do show userroles
```

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

77. Los permisos de este nuevo rol pueden ser modificados usando el comando

```
role mode modo { { { addrole | deleterole } role-name } | reset } command
```

78. Los parámetros a introducir son:
    - *mode*: debe elegirse entre categorías de comandos *configure, exec, interface, line, route-map y router.*
    - *addrole/deleterole*: para indicar si se está añadiendo o quitando permisos a un rol sobre cierto comando.
    - *role-name*: el rol sobre el que se actúa.
    - *reset*: permite poner los permisos de roles de un comando a su valor por defecto
    - *command*: el comando concreto sobre el que se actúa para asignar privilegios de ejecución a un rol.
79. Se detalla un ejemplo a continuación: ***role mode configure addrole netoperator command username***
80. 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*.
81. Por otro lado, también se puede crear un nombre de usuario que se autentique según un rol. Para ello se usa el comando:

```
username name password encryption-type password role role-name
```

    Por ejemplo:

```
Dell(conf)# username juan password 0 password role secadmin
```

82. Para eliminarlo, basta con escribir "*no*" delante del comando "*username*".
83. Es importante resaltar que la asignación de roles se debe hacer durante el proceso de creación del usuario. Si se desea modificar a posteriori, se debe primero eliminar el usuario y volverse a crear con el rol adecuado.
84. También es posible crear roles nuevos en el sistema a partir de los roles existentes mediante el comando: ***userrole name inherit existing-role-name***
85. Teniendo en cuenta los roles básicos definidos por defecto en el sistema, es posible crear hasta 4 roles adicionales.
86. Para eliminarlos, basta con escribir "*no*" delante del comando "*userrole*".
87. Los usuarios con roles y privilegios son autorizados con el mismo mecanismo. Hay seis (6) métodos disponibles para la autorización: *radius*, *tacacs+*, *local*, *enable*, *line* y *none*. Cuando se habilita la autorización AAA basada en rol, los siguientes métodos no están disponibles: *enable*, *line* y *none*.

- Activación de autenticación en base a las definiciones de roles guardadas en el equipo:

```
Dell(conf)# aaa authentication login {method-list-name | default} method […
method4]
```

- Activación de autorización en base a las definiciones de roles guardadas en el equipo:

```
Dell(conf)# aaa authorization exec {method-list-name | default} method [… method4]
```

88. Para más información puede consultarse la guía *"Dell Networking Command Line Reference Guide 9.14" – REF1.*

6.4 SEGURIDAD EN EL ACCESO A LA ADMINISTRACIÓN

89. Es imprescindible prevenir que usuarios no autorizados puedan acceder a los equipos y visualizar o modificar 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 los 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.

6.4.1 HABILITACIÓN DE MODOS ESPECIALES SEGUROS

6.4.1.1 HABILITACIÓN MODO SEGURO/FIPS

90. El modo seguro o modo FIPS 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 se puede activar el modo FIPS con el comando: ***FIPS mode enable.***

91. Una vez aplicado el cambio, los comandos del sistema estarán restringidos a valores de configuración que atienden el estándar de seguridad FIPS, bloqueando cualquier configuración considerada insegura. Los detalles de esta modalidad se pueden consultar en la guía "Dell Networking OS Configuration Guide 9.14" – REF2.

92. **Se debe utilizar el producto en modo seguro.**

6.4.1.2 HABILITACIÓN MODO SECURE-CLI

93. 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 el *password* de admin del sistema, incluso aunque tengan nivel de privilegio suficiente para hacerlo.

94. La forma de habilitar este modo se realiza con el comando: ***secure-cli enable***

95. Se recomienda activar el modo *secure-cli*. En caso necesario, es posible deshabilitarlo con el comando: ***secure-cli disable***.

6.4.2 GESTIÓN LOCAL DEL EQUIPO

6.4.2.1 PUERTO DE CONSOLA

96. 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.
97. Algunas funciones, como la recuperación de las credenciales del equipo (procedimiento de *password recovery*) solo están disponibles desde el puerto de consola.
98. 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).
99. 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:

```
Dell(conf)# username name [access-class access-list-name] [nopassword | {password | secret
| sha256-password} [encryption-type] password] [privilege level] [role role-name]
```

    - *encryption-type*: especifica el modo de insertar la contraseña. Por defecto el valor es 0 para indicar que es texto plano. Si el valor es 7, se indica que está cifrada con un hash. **Se debe utilizar sha256.**

100. Desde el momento en que se ejecuta este comando, el conmutador activa el control de acceso a la gestión del equipo y solo se permite el acceso con las credenciales.
101. 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.
102. Hay dos (2) tipos de contraseñas de *enable*:

    - *enable password*: almacena la contraseña en la configuración *running/startup* usando un método de cifrado DES.
    - *enable secret*: almacena la contraseña usando un método de cifrado.

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

```
Dell(conf)# enable sha256-password {0 cleartext-password | 8 encrypted-password}
```

    - *sha256–password*: indica que la contraseña es de tipo sha256.

- *encryption-type*: especifica el modo de insertar la contraseña. Por defecto, el valor es 0 para indicar que es texto plano. Si el valor es 8, se indica que está cifrada con un hash tipo sha256. **Se debe utilizar sha256.**

104. Por otro lado, es importante evitar que las sesiones establecidas en la consola del equipo 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 estas se cierren automáticamente transcurrido ese periodo de inactividad.

105. Para fijar el periodo de inactividad se utiliza el comando:

```
Dell(conf)# line console 0
Dell(config-line-console)# exec-timeout minutes seconds
```

106. Un tiempo de 0 cancela la funcionalidad. **Se recomienda un valor de 10 minutos.**

107. El comando anterior no solo afecta a las sesiones de consola, sino también a las sesiones SSH. 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 10 minutos y 0 segundos.

```
Dell(conf)# line vty 0 9
Dell(config-line-vty)# exec-timeout 10 0
```

108. Adicionalmente, **se debe 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.

109. Para configurar el banner se utiliza el comando:

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

110. 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*).

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

```
Dell(conf)# banner motd %
Enter TEXT message. End with the character '%'
Este es un sistema privado. Abandone la conexión si no tiene autorización
%
```

112. En la configuración aparecerá como:

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

113. Al igual que el valor del *timer* de inactividad, el mensaje de bienvenida aplica también a las sesiones establecidas por SSH descritas más adelante.

114. Asimismo, conviene asignar un nombre al equipo mediante el comando "*hostname*". Por ejemplo:

```
Dell(conf)# hostname dellsw
dellsw(conf)#
```

6.4.2.2 PUERTO USB

115. 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*.

116. 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:

```
Dell(conf)# unmount usb
```

6.4.3 GESTIÓN REMOTA DEL EQUIPO

117. 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 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 este.

118. 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.

6.4.3.1 REQUISITOS Y RECOMENDACIONES INICIALES

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

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

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

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

121. 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, web, SNMP, etc.).

122. 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.

123. Con el objeto de solventar este problema, *Dell EMC Networking OS 9.14* 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.

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

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

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

- *vlan-id*: es el identificador de la VLAN. El rango es de 1 a 4094.
- *of-instance{of-id}*: es el identificador de la instancia de *OpenFlow*. El rango es de 1 a 8.

126. 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
```

127. Existen algunas restricciones a tener en cuenta:

- Sólo una VLAN por equipo puede ser configurada como VLAN de gestión.
- La dirección IP de gestión ha de ser estática.
- No puede ser configurado en la VLAN de gestión nada relacionado con protocolos de encaminamiento o IGMP.
- 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.

128. 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) se mejora la seguridad del conmutador mediante la separación del tráfico de gestión del resto de tráficos de nuestras redes.

129. 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 estas 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:

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

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

6.4.3.2 TELNET

130. 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. No se recomienda 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.

131. Dado que este servicio viene activado por defecto, **deberá ser desactivado** mediante el comando siguiente:

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

6.4.3.3 SSH

132. El protocolo recomendado para el acceso remoto a la gestión 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.

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

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

134. **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 6.4.2.1 Puerto de consola, permite configurar ese tiempo límite.

135. Las claves RSA utilizadas por el protocolo se generan automáticamente al arrancar el equipo por primera vez. En caso de querer regenerar las claves, se debe ejecutar el comando: ***crypto key generate rsa keysize***.

136. El valor de tamaño de clave (*keysize*) puede definirse entre 1024 y **2048 bits**, siendo este último el valor que **debe ser utilizado**. Las claves deben ser generadas por un usuario con rol *sysadmin* o nivel de privilegio 15.

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

6.4.3.4 SNMP

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

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

- 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)
- 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).

140. Actualmente existen tres (3) versiones del protocolo SNMP. El producto soporta todas ellas, 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.

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

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

142. Al aplicar este comando se deshabilita SNMP v1 y v2. Dejando solo funcional SNMP v3.

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

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

144. 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.

145. 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
xstp	Traps para cambios de estado en STP (802.1s), RSTP (802.1w), and PVST+

146. También se puede crear un grupo de SNMP3 que mapee los usuarios de SNMP con las vistas de SNMP. Para más información, se puede consultar el apartado de "*Simple Network Management Protocol (SNMP)"* en la guía "*Dell Networking Configuration Guide 9.14"* – REF2, y el apartado "*Simple Network Management Protocol (SNMP) and Syslog"* en la guía "*Dell Networking Command Line Reference Guide 9.14"* – REF1.

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

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

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

- *ip-address*: la dirección IP del host. El máximo número permitido de *hosts* es 16.
- *traps*: indica que se van a enviar notificaciones de tipo trap a un host determinado. Por defecto es traps.
- *version*: especifica el modelo de seguridad y su versión 3 (que es la más segura de los tres métodos). Por defecto es 1.
- *priv snmpv3-password*: especifica la autenticación y la contraseña de SNMPv3.
- *udp-port* (opcional): indica el puerto del host remoto. El rango es de 0 a 65535. El valor por defecto es 162.

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

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

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

- *name*: indica el nombre del usuario en el host que conecta con el agente. No puede exceder de 20 caracteres.
- *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.
- *priv sha*: designan el nivel de autenticación y la contraseña tipo *sha*.
- *aes128*: indica el algoritmo de cifrado AES CFB 128-bit.

149. Un ejemplo del uso de este comando es:

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

6.5 GESTIÓN DE CERTIFICADOS

150. Con el objeto de facilitar las tareas de creación y solicitud de certificados en caso de utilizarse en el equipo, Dell EMC Networking OS 9.14 permite instalar certificados de confianza.

151. Estos certificados son presentados a clientes SSH, además de implementaciones con servidor TLS que requieren autenticación del cliente (como es el caso de *Syslog*). Así mismo, están firmados digitalmente con una clave privada por un servidor con autoridad de certificación.

6.5.1 CREACIÓN DE UN CSR

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

```
Dell(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]
```

153. El parámetro *Lenght* admite valores entre 2048 y 4096, **se deben utilizar longitudes de clave iguales o superiores a 3072 bits.**

6.5.2 INSTALACIÓN DE CERTIFICADOS

154. Para cargar los certificados en el producto, se deberá utilizar *flash, usbflash, tftp, ftp*, o *scp* para descargarlos al sistema.

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

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

156. 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.

6.6 ACTUALIZACIÓN DEL *SOFTWARE* DEL DISPOSITIVO

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

6.6.1 VERSIÓN DE SOFTWARE INSTALADA

158. Para verificar la versión de *software* instalada en el equipo se utiliza el comando "*show version*". En este ejemplo, el *switch* tiene versión 9.5(1.0B5) y debe ser actualizado a la versión 9.14.1:

```
Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 9.5(1.0B5)
```

159. 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:

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

- *sha256:* Algoritmo de seguridad *HashSHA256 Secure Hash Algorithm*.
- *flash (opcional):* especifica el disco flash, aunque también se puede indicar el nombre de la imagen del fichero.
- *hash-value (opcional):* especifica el hash publicado en la web de soporte.
- *img-file:* indica el nombre del archivo con la imagen del *software Dell EMC Networking* a validar.

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

161. Las *release notes* de cada versión se pueden consultar en la página de soporte de Dell Networking o en el repositorio Dell Digital locker con el usuario de soporte de cliente.

162. Puede que sea necesario reiniciar el sistema inmediatamente después de la actualización o bien se puede posponer. En este sentido, se pueden 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]
```

6.6.2 GUARDAR CONFIGURACIÓN ACTUAL

163. 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.

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

  ```
  Dell# copy running-config startup-config
  ```

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

  ```
  Dell# copy running-config flash://filename
  ```

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

  ```
  Dell# copy running-config scp://{hostip | hostname}/ filepath/filename
  ```

6.6.3 ACTUALIZACIÓN DEL SISTEMA

164. **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.

165. La actualización del sistema operativo puede realizarse desde la línea de comandos (CLI) o a través del interfaz gráfico (GUI). 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.

166. 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.

167. Mediante el CLI es posible usar TFTP y SCP para actualizar el equipo vía interfaces de red IP.

168. Los pasos a seguir en una actualización de Dell EMC Networking OS mediante línea de comandos, son los siguientes:

- Actualizar el código en la partición A con el comando "*upgrade system [flash: | ftp: stack-unit <1-6> | tftp: | scp: | usbflash:] [A:]*":

  ```
  Dell# upgrade system tftp: a:
  ```

- Verificar que se ha actualizado correctamente con el comando "*show boot system stack-unit [1-6] | all]*".
- Cambiar el parámetro de primary boot a la partición actualizada:

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

- Salvar la configuración con el comando "*write memory*".
- Actualizar el código en la partición B con el comando "*upgrade system [flash: | ftp: stack-unit <1-6> | tftp: | scp: | usbflash:] [B:]*":

  ```
  Dell# upgrade system tftp: b:
  ```

- Verificar que se ha actualizado correctamente con el comando "*show boot system stack-unit [1-6] | all]*".
- Salvar la configuración con el comando "*write memory*".
- Reiniciar el producto con el comando "*reload*" y verificar la nueva versión con "*show version*".

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

- Actualizar la imagen de *Boot Flash*:

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

- Actualizar la imagen de *Boot Selector*:

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

- Reiniciar el switch con el comando "*reload*" y verificar la imagen del *Boot Selector* con el comando:

  ```
  show system stack-unit 1
  ```

6.7 AUDITORIA

6.7.1 SYSLOG

170. *Dell Networking OS 9.14* permite monitorizar los cambios en el sistema usando mensajes de errores y eventos. Por defecto estos mensajes se recogen en:

- El *buffer* interno.
- Las líneas de consola y terminal.
- Cualquier servidor *syslog* configurado.

171. Asimismo, se permite visualizar los logs de auditoría, previamente habilitando el comando "*logging extended*". Tan sólo el administrador de sistema basado en RBAC puede ver este tipo de logs. En el caso de los logs de seguridad, son los administradores de seguridad y sistema basados en RBAC los que pueden consultarlos.

172. Si *extended logging* estuviera deshabilitado, tan sólo se podrían ver eventos del sistema.

173. También es posible configurar una conexión segura desde el *switch* a un servidor de *syslog*. Por defecto, soporta 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. En caso de haber configurado el modo de operación segura (ver 6.4.1.1 Habilitación del modo seguro/FIPS), solo se soportará TLSv1.2, rechazando la conexión con cualquier otra versión anterior.

174. A continuación, se describen los pasos a seguir para configurar un servidor *Syslog* externo:

```
Dell# clear logging auditlog
```

- Habilitar en el producto el servidor SSH:

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

- En el servidor de *syslog*, crear un túnel SSH inverso desde el servidor de *syslog* hasta el *switch* de Dell EMC:

```
ssh -R <remote port>:<syslog server>:<syslog server listen port> user@remote_host -nNf
```

- Configurar la recogida de *logs* en un *host* local. Si no se realiza, el sistema muestra un error cuando se intenta habilitar la autorización AAA basada en rol:

```
Dell(conf)# logging localhost tcp port
```

175. El envío de mensajes del sistema a un servidor de syslog específico, se realiza a través del siguiente comando. Destacar que se puede configurar hasta 8 servidores de *syslog*:

```
Dell(conf)# logging {ip-address | ipv6-address | hostname} {{udp {port}} | {tcp {port}}}
```

176. Para más información al respecto, se puede consultar el manual *"Dell Networking OS Configuration Guide 9.14" – REF2.*

6.8 POLÍTICAS DE CALIDAD DE CONTRASEÑAS

177. 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. En *Dell EMC Networking OS 9.14*, existen diversos atributos para el control de la calidad de las contraseñas que se usan para la gestión de conmutador y otras funciones de control de acceso de usuarios.

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

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

- *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**.
- *max-retry number* (opcional): indica el máximo número de intentos de inicio de sesión. El rango es de 1 a 16. **Se debe configurar con un valor bajo, por ejemplo, 5 intentos.**
- *lockout-period minutes* (opcional): este parámetro mejora la seguridad del producto bloqueando las sesiones 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 el menor tiempo posible**.
- *user-lockout-period minutes* (opcional): este parámetro mejora la seguridad del producto bloqueando la cuenta del usuario local si hay un número de intentos fallidos de *login* mayor que el valor configurado en el parámetro *max-retry*. El rango es de 1 a 1440 minutos. El valor por defecto es 3.
- *character-restriction* (opcional): indica los caracteres mínimos necesarios. El rango es de 0 a 31:
  - *upper number* (opcional): indica el número de mayúsculas necesario. El rango es de 0 a 31.
  - *lower number* (opcional): indica el número de minúsculas necesario. El rango es de 0 a 31.
  - *numeric number* (opcional): indica cuántas cifras numéricas son necesarias. El rango es de 0 a 31.
  - *special-char number* (opcional): indica el número de caracteres especiales necesarios. El rango es de 0 a 31.

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

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

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

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

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

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

183. Para más información de contraseñas, revisar la *guía "Dell Command Line Reference Guide 9.14" – REF1.*

6.8.1 ALMACENAMIENTO DE CONTRASEÑAS

184. 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 estén protegidas, se recomienda configurar su almacenamiento de forma que no se almacene la contraseña sino un valor resumen de la misma a través de "*enable sha256-password*".

6.8.2 CONFIGURACIÓN DE FÁBRICA Y RECUPERACIÓN DE CONTRASEÑAS

185. A continuación, se indica cómo restaurar la configuración de fábrica y recuperar la contraseña en un *switch* con *Dell EMC Networking OS 9.14.*

186. 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*.

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

```
Dell# 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).
....
```

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

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

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

190. El siguiente proceso indica cómo recuperar la contraseña:

- 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: **"=>".**
- Una vez dentro de este menú, ignorar la configuración de arranque.
- Cuando el switch se haya reiniciado completamente, se aplica la configuración de arranque a la running-config:

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

- Eliminar cualquier contraseña y secreto del modo *enable*, y volver a crear un secreto o contraseña:

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

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

```
Dell(config)# do show run | grep username
username Delluser password 7 66a88a701a5b6b80 privilege 15
Dell(config)# no username Delluser
Dell(config)# username Delluser password P@$$w0rd123 privilege 15
```

- Eliminar la autenticación por consola, en caso necesario:

```
Dell(conf)# line console 0
Dell(config-line-console)# no authentication login no password
Dell(config-line-console)# do write memory
Dell(config-line-console)# exit
```

- Guardar la configuración y reiniciar el *switch*:

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

6.9 SERVICIOS DE RED DEL EQUIPO

191. **Para garantizar la seguridad de un equipo es imprescindible ser consciente de los servicios de red activados y tomar las medidas adecuadas para asegurarlos.** 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.

192. 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.

6.9.1 LLDP

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

194. 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.

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

196. Para desactivar LLDP de forma global, hay que usar los comandos:

```
Dell(config)# protocol lldp
Dell(config)# disable
```

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

```
Dell(conf)# interface tengigabitethernet 1/3/1
Dell(conf-if-te-1/3/1)# protocol lldp
Dell(conf-if-te-1/3/1-lldp)# ?
advertise        Advertise TLVs
disable          Disable LLDP protocol on this interface
…
```

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

```
Dell(conf)# protocol lldp
Dell(conf-lldp)# show config
```

6.9.2 ICMP

199. 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.

200. 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.

201. Para desactivar las funciones de ICMP mencionadas, dentro del menú interface, hay que usar los comandos:

```
no ip unreachable
no ip redirects
```

6.9.3 TRANSFERENCIA DE FICHEROS

202. Para transferir archivos a/o desde el producto existen tres (3) 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 no se debe usar. Así pues, se recomienda el uso de FTP (*File Transfer Protocol*) y SCP (*Secure Copy Protocol)* para el intercambio de ficheros. Por defecto el servidor FTP está deshabilitado, por lo que para habilitarlo se usa el comando:

```
Dell(conf)# ftp-server enable
```

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

```
Dell# copy flash://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
```

6.9.4 SINCRONIZACIÓN DE TIEMPO

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

205. 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.

206. 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.

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

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

- 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
  ```

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

  ```
  Dell(conf)# ntp authenticate
  Dell(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.
  - Se recomienda usar SHA1 frente a MD5, pero ninguno de los dos algoritmos se considera suficiente seguro.

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

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

- Autenticar el sistema del NTP del que sincroniza:

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

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

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

6.10 CONTROL DE TRÁFICO Y SEGURIDAD EN LOS PUERTOS DE RED

210. En este apartado se describirán una serie de medidas de seguridad que pueden aplicarse a los equipos con Dell Networking OS 9.14 para mejorar la seguridad de los puertos de red de los conmutadores, así como controlar el tráfico que gestiona el equipo.

6.10.1 APAGADO DE PUERTOS

211. 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.

212. 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):

```
Dell(conf)# interface tengigabitethernet 4/17
Dell(conf-if-te-4/17)# shutdown
Dell(conf-if-te-4/17)#show config
!
  interface tenGigabitEthernet 4/17
  ip address 192.168.10.1/24
  shutdown
```

6.10.2 MEDIDAS DE PROTECCIÓN DE PUERTOS

213. *Dell Networking OS 9.14* proporciona 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.

214. 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 cuál de las configuraciones posibles se adapta mejor a nuestras necesidades.

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

- El número máximo de direcciones MAC permitidas en una *interface (address-limit)*. El rango permitido es de 1 a 100.000:

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

- 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.

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

- *learn-limit-violation log*: Generar un log cuando se alcanza el límite.
- *learn-limit-violation shutdown*: Cerrar la *interface* y generar un log cuando se alcanza el límite.

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

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

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

219. 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.

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

221. Una vez activada la seguridad en un puerto del conmutador pueden producirse situaciones que alcancen 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.

6.10.3 CONTROL DEL TRÁFICO

222. El producto incorpora 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.

223. 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).

224. 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.

225. La configuración se puede realizar, o bien de forma global en modo *EXEC Privilege*, o bien por puerto.

226. Para configurarlo en un puerto, desde el modo *interface* se configuran 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 packets_per_second in
storm-control multicast packets_per_second in
storm-control pfc-llc pps in shutdown
```

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

```
storm-control broadcast packets_per_second in
storm-control multicast packets_per_second in
storm-control unknown-unicast packets_per_second in
```

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

```
Dell# show storm-control multicast Tengigabitethernet 1/1/1
Multicast storm control configuration
Interface  Direction     Packets/Second
----------------------------------------
Te 1/1/1     Ingress       5
```

6.10.4 USO DE VLAN COMO MEDIDA DE AISLAMIENTO

229. 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.

230. 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*.

231. 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.

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

233. 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.

234. Para crear una VLAN basta con realizar:

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

235. 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:

```
Dell(conf)# interface vlan vlan-id
Dell(conf-if)# tagged interface
Dell(conf-if)# untagged interface
```

236. 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.

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

```
Dell# 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
```

238. 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.

239. 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.

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

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

241. 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, **se debe deshabilitar el funcionamiento de GVRP en todos los puertos que no sean troncales o en los que no se necesite su uso.**

242. 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
```

6.10.5 VLAN PRIVADAS

243. 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.

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

- **Puertos promiscuos (*promiscuous*)**, que pueden comunicarse con cualquier otro puerto de la VLAN. Son los puertos asignados típicamente a los servidores o routers.
- **Puertos aislados (*isolated*)**, que solo pueden comunicarse con puertos promiscuos que están en la misma PVLAN.

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

245. Para crear una VLAN privada en *Dell EMC Networking OS 9.14* se utilizan VLAN de dos (2) tipos distintos:

- **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.
- **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.

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

- **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:

```
Dell#conf
Dell(conf)#interface TenGigabitEthernet 2/1/1
Dell(conf-if-te-2/1/1)#switchport mode private-vlan promiscuous
Dell(conf)#interface TenGigabitEthernet 2/2/1
Dell(conf-if-te-2/2/1)#switchport mode private-vlan host
Dell(conf)#interface TenGigabitEthernet 2/3/1
Dell(conf-if-te-2/3/1)#switchport mode private-vlan trunk
Dell(conf)#interface TenGigabitEthernet 2/2/1
Dell(conf-if-te-2/2/1)#switchport mode private-vlan host
Dell(conf)#interface port-channel 10
Dell(conf-if-po-10)#switchport mode private-vlan promiscuous
```

- **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*".

- **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*".

- **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*".

247. Un ejemplo de configuración sería el siguiente:

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

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

6.10.6 PROTECCIÓN FRENTE A ENVÍO DE MENSAJES DE CONTROL STP

248. 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.

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

250. 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).

251. 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.

252. 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.

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

254. 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.

255. Para deshabilitar el puerto cuando se recibe una BPDU, se usa el siguiente comando:

```
Dell(conf-if)# spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast
[bpduguard [shutdown-on-violation]] | priority priority}
```

- *bpduguard*: deshabilita el puerto cuando recibe un mensaje BPDU.
- *shutdown-on-violation*: deshabilita la *interface* cuando se recibe un mensaje BPDU y el puerto está deshabilitado.

256. 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.

257. A continuación, se muestra un ejemplo de BPDU bloqueadas. Para ello se usa el comando "*show spanning-tree [stp | rstp | mstp] brief*" que muestra la configuración relativa a cada protocolo de *Spanning-tree*:

```
Dell(conf-if-te-1/7/1)# do show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e805.fb07
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e85d.0e90
Configured hello time 2, max age 20, forward delay 15

Interface                          Designated
Name     PortID  Prio Cost Sts Cost Bridge ID  PortID
------------ -------- ---- ------- --- ------- --------------------
Te 1/6/1 128.263 128 20000 FWD 20000 32768 0001.e805.fb07 128.653
Te 1/7/1 128.264 128 20000 EDS 20000 32768 0001.e85d.0e90 128.264

Interface
Name Role PortID Prio   Cost Sts  Cost Link-type Edge
------------ ------ -------- ---- ------- --- ----------------
Te 1/6/1  Root   128.263 128 20000 FWD 20000 P2P No
Te 1/7/1  ErrDis 128.264 128 20000 EDS 20000 P2P No

Dell(conf-if-te-1/7/1)#d o show ip interface brief tengigabitEthernet 1/7/1
Interface             IP-Address OK Method Status Protocol
TenGigabitEthernet 1/7/1 unassigned YES Manual up up
```

258. 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:

```
Dell# show spanning-tree 0 guard
Interface
Name       Instance  Sts         Guard type
--------   -------- ---------  ----------
Te 1/1        0    INCON(Root) Rootguard
Te 1/2        0    LIS         Loopguard
Te 1/3        0    EDS (Shut)  Bpduguard
```

259. Por último, para visualizar el tipo de guarda, se usa el comando:

```
Dell# errdisable recovery cause {bpduguard | fefd | maclearnlimit}
```

6.10.7 LISTAS DE ACCESO IP

260. 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.

261. 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 se quiera restringir un determinado tráfico, es necesario asegurarse de permitir el resto de tráfico en una regla final. De ahí la importancia de escribir in orden las reglas de ACL.

262. En Dell EMC Networking OS 9.14, 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.

263. *Dell EMC Networking OS 9.14* 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, basta con cambiar el formato de las direcciones.

6.10.7.1 TIPOS DE ACLS

264. Existen dos (2) tipos de ACL según el procedimiento usado para definirlas:

- 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.
- 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.

265. En este apartado, se detallan únicamente las ACL estáticas.

266. Según su aplicación, se pueden 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.

267. Según como se especifica el tráfico a filtrar, existen dos (2) tipos de listas de acceso:

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

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

6.10.7.2 CREACION DE ACLS

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

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

- [*standard | extended]*: se selecciona el tipo de lista, estándar o extendida.
- *access-listname*: define el identificador de la lista de acceso. El rango es 1-99 para lista estándar y 100- 199 para listas extendidas.

270. 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]
```

- *source*: determina el origen.
- *mask*: identifica una máscara.
- *any*: representa cualquier dirección.
- *host*: especifica una determinada dirección IP.
- *monitor*: permite monitorizar la sesión con un determinado identificador.

271. 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]
```

272. 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.

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

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

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

274. 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]
```

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

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

Dell(config-ext-nacl)#seq 15 deny ip host 112.45.0.0 any log monitor 501
Dell(config-ext-nacl)#seq 5 permit tcp 12.1.3.45 0.0.255.255 any
Dell(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
Dell(config-ext-nacl)#
```

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

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

277. 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 Networking Command Line Reference Guide 9.14" – REF1.*

6.10.7.3 APLICACION DE LISTAS DE ACCESO

278. 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*).

279. 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 una *interface* específica, se puede bloquear el tráfico y así proteger los dispositivos.

280. Un ejemplo de creación de reglas de ACL para tráfico entrante y comprobación de la configuración, es el siguiente:

```
Dell(conf)# interface TenGigabitEthernet 1/1/1
Dell(conf-if-te-1/1/1)# ip access-group abcd out
Dell(conf-if-te-1/1/1)# show config
!
TenGigabitEthernet 1/1/1
  no ip address ip access-group abcd out
  no shutdown
Dell(conf-if-te-1/1/1)# end
Dell# configure terminal
Dell(conf)# ip access-list extended abcd
Dell(config-ext-nacl)# permit tcp any any
Dell(config-ext-nacl)# deny icmp any any
Dell(config-ext-nacl)# permit 1.1.1.2
Dell(config-ext-nacl)# end
Dell# show ip accounting access-list
!
Extended Ingress IP access list abcd on gigethernet 0/0
  seq 5 permit tcp any any
  seq 10 deny icmp any any
  seq 15 permit 1.1.1.2
Dell# configure terminal
Dell(conf)# interface te 1/2/1
Dell(conf-if-te-1/2/1)# ip vrf forwarding blue
Dell(conf-if-te-1/2/1)# show config
!
interface TenGigabitEthernet 1/2/1
ip vrf forwarding blue
no ip address
shutdown
Dell(conf-if-te-1/2/1)# end
```

281. Un ejemplo de crear reglas de ACL para tráfico saliente y comprobar la configuración, es el siguiente:

```
Dell(conf)# interface tengigabitethernet 1/1/1
Dell(conf-if-te1/1/1)# ip access-group abcd in
Dell(conf-if-te1/1/1)# show config
!
tengigabitethernet 1/1/1
  no ip address
  ip access-group abcd in
```

```
  no shutdown
Dell(conf-if-te1/1/1)# end
Dell# configure terminal
Dell(conf)# ip access-list extended abcd
Dell(config-ext-nacl)# permit tcp any any
Dell(config-ext-nacl)# deny icmp any any
Dell(config-ext-nacl)# permit 1.1.1.2
Dell(config-ext-nacl)# end
```

282. 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:

- Crear un *ACL VLAN Group* con el comando "*acl-vlan-group {group name}*" desde el modo *Privilege EXEC*.
- Añadir una descripción a este grupo desde el modo *conf-acl-vl-grp* con el comando "*description description*".
- 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*".
- Añadir los miembros de las VLAN al grupo, desde el modo *conf-acl-vl-grp* con el comando "member vlan {VLAN-range}.
- Mostrar la configuración creada, como en el siguiente ejemplo:

```
Dell# 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
Dell#
```

6.10.8 LISTAS DE ACCESO MAC

283. De forma análoga a las listas de acceso IP descritas en el apartado anterior, *Dell EMC Networking OS 9.14* 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.

284. La configuración de las listas de acceso MAC 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.

285. 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]
```

286. 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-mask}
{any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype
operator] [count [byte]] | [log] [monitor]
```

287. 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.

288. A continuación, se muestra un ejemplo para visualizar las MAC ACL y sus contadores (si es que han sido configurados):

```
Dell# show mac accounting access-list TestMac interface tengigabitethernet 1/8 in

Ingress Standard mac access-list TestMac on TenGigabitEthernet 1/89

Total cam count 2

  seq 5 permit aa:aa:aa:aa:00:00 00:00:00:00:ff:ff count (0 packets)

  seq 10 deny any count (20072594 packets)
```

6.11 SISTEMAS DE CONTROL DE ACCESO

289. Esta sección está relacionada con la gestión de usuarios y la autenticación. Detalla las opciones disponibles para incrementar la seguridad en el acceso a los equipos.

290. Un posible problema es la autenticación de forma local en el conmutador dado que, si no hay un sistema global de autenticación que almacene las cuentas de usuario, pueden originarse inconsistencias si no se configuran todos los equipos de la red exactamente igual, además de los problemas que supone el tener que crear o modificar los perfiles de los administradores en todos los equipos uno a uno.

291. Para solucionar estos problemas, se dispone de varios mecanismos de autenticación y de creación de cuentas de forma centralizada. Esto permite que todos los equipos chequeen con este sistema, la validez de los datos de usuario

introducidos y que a la hora de realizar modificaciones en las cuentas solo sea necesario realizarlo en un único equipo.

292. A estos métodos se los denomina *Authentication, Authorization and Accounting (AAA)*:

- *Authentication*: permite identificar usuarios, ya sean remotos o locales, antes de permitirles acceder al equipo.
- *Authorization*: permite regular el acceso a servicios del equipo por parte de un usuario dependiendo del grado de acceso que tenga asignado.
- *Accounting*: ofrece un servicio de registro de los servicios accedidos por un usuario al igual que el ancho de banda utilizado por este usuario.

293. Dell EMC implementa AAA utilizando dos (2) protocolos para poder acceder a los servidores de seguridad: RADIUS y TACACS+.

294. A continuación, se van a describir las distintas formas de control de acceso soportadas. Lo primero, indicar que el registro de accesos debe estar configurado. Actualmente, la opción de *Accounting* sólo está disponible para TACACS+:

```
aaa accounting {system | exec | commands level | role role-name} {name | default}{start-stop | wait-start | stop-only} {tacacs+}
```

295. A continuación, se muestra un ejemplo de configuración:

```
DellEMC(conf)# aaa accounting exec default start-stop tacacs+
DellEMC(conf)# aaa accounting command 15 default start-stop tacacs+
DellEMC(conf)# aaa accounting command role secaadmin default start-stop tacacs+
```

6.11.1 CONTROL DE ACCESO MEDIANTE 802.1X

296. 802.1X es una norma del IEEE para el control de acceso a red utilizada tanto en redes Ethernet inalámbricas como cableadas. Permite autenticar los dispositivos que se conectan a la red con el objeto de autorizar o no el acceso a la red. La autenticación se lleva a cabo mediante un servidor RADIUS externo, aunque también puede configurarse localmente.

297. En el caso de Dell EMC Networking OS 9.14, se soporta RADIUS y *Active Directory* para la autenticación de acceso a los puertos usando 802.1X.

298. Para habilitar 802.1X:

- Dentro del modo *EXEC Privilege*, se habilita 802.1X de forma global con el comando "*dot1x authentication*".
- A continuación, entrar en el modo *interface* seleccionando una *interface* o rango de estas, con el comando "*interface [range]*".
- Habilitar 802.1X en la *interface* seleccionada, con el comando "*dot1x authentication".*

299. Para verificar que se ha habilitado correctamente:

```
Dell# show running-config | find dot1x
```

```
dot1x authentication
!
[output omitted]
!
interface TenGigabitEthernet 2/1/1
 no ip address
 dot1x authentication
no shutdown
!
Dell#
```

300. A continuación, se realiza la configuración de la conexión del servidor RADIUS:

```
Dell# show dot1x interface TenGigabitEthernet 2/1/1
802.1x information on Te 2/1/1:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Port Auth Status:       UNAUTHORIZED
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Disable
Guest VLAN id:          NONE
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Disable
Mac-Auth-Bypass Only:   Disable
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             2
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            2
Host Mode:              SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
```

- Dentro del modo de configuración, se configura la dirección IP o nombre del *host* que apunta a la ubicación del servidor RADIUS, con el comando "*radius-server host ip-address*".
- Se configura la clave del servidor RADIUS para el protocolo de enlace con el servidor RADIUS, con el comando "*radius-server key {encryption-type} key*", siendo el tipo de cifrado 0 si es una clave no cifrada, 7 si es una clave oculta, y *key* la clave como una cadena de caracteres.

- Se identifica el servidor de autenticación dot1x como un servidor RADIUS, con el comando "*dot1x auth-server radius*".
- Finalmente se verifica su correcta configuración:

```
Dell# show run | grep radius|dot1x
dot1x authentication
dot1x authentication
radius-server host 10.180.58.10 key 7 7bb92471cb453a73
```

301. Se puede evitar que una *interface* esté bloqueada, forzando la autenticación de la siguiente manera (*force-authorized*) o bien bloquearla y que nunca esté autorizada (*force-unauthorized*), con el siguiente comando desde el modo interface:

```
dot1x port-control {force-authorized | auto | force-unauthorized}
```

302. Otra opción es disponer de una VLAN de invitados para usuarios con acceso limitado o dispositivos que no soportan 802.1X. Es decir, si un dispositivo no responde en 30 segundos, se asume que no soporta 802.1X. Entonces se añade a la VLAN de invitados y se pospone su autenticación al siguiente intervalo de re-autenticación.

303. También es posible configurar el periodo de tiempo límite para intercambiar información con el servidor.

```
Dell(conf-if-interface-slot/port[/subport])# dot1x guest-vlan vlan-id
Dell(Interface interfaceid)# dot1x reauthentication [interval seconds]
Dell(Interface interfaceid)# dot1x server-timeout seconds
```

304. Para aquello casos en los que 802.1X haga un *timeout* porque el host no respondió, *Dell EMC Networking OS 9.14* permite autenticar al host en base a su dirección MAC:

```
Dell(Interface interfaceid)# dot1x mac-auth-bypass
```

305. Para más información sobre la autenticación basada en 802.1x puede consultarse la guía "*Dell Command Line Reference Guide 9.14*" – REF1.

6.11.2 POLÍTICAS DE ACCESO BASADAS EN ROLES

306. En los equipos Dell EMC es posible, además de regular el acceso a la red mediante la consulta de credenciales a un servidor externo, asignarles una política de acceso a la red. Con ello, se consigue administrar las conexiones del equipo de una manera más segura y eficiente. Es decir, cuando un usuario se autentica y se conecta correctamente a la red se le asigna automáticamente un perfil de acceso que le permitirá realizar las acciones que el administrador del equipo haya definido.

307. Este método de definición de usuarios, denominado definición de roles o perfiles, puede resultar interesante ya que permite aislar partes de la red a personas no autorizadas, creando para ello roles de invitado, de empleado, de administradores, etc.

308. En este sentido, en Dell EMC Networking OS 9.14 se puede configurar la autorización de acceso basándonos sólo en el rol del usuario. Si el usuario no

dispone de rol, entonces el acceso al sistema se deniega. Así pues, cuando se habilita la autorización AAA basada en rol, se asegura que no se bloquee al usuario y que la autenticación esté disponible por todas las líneas terminales.

309. Existen unos prerrequisitos mínimos cuando se habilita autorización AAA basada en rol:

- Deben crease y utilizarse los roles para permitir el acceso al sistema (ver apartado 6.3.1 Modo RBAC)
- Configurar la autenticación de *login* en la consola. Esto permite que todos los usuarios estén propiamente identificados a través de la autenticación, sin importar el punto de acceso.
- Especificar una lista de métodos de autenticación: RADIUS, TACACS+ o local. Por consistencia, la mejor práctica es definir la misma lista de métodos de autorización a todas las líneas.
- Verificar que la configuración ha aplicada a la línea de consola o VTY:

```
Dell (conf)# do show running-config line
!
line console 0
login authentication test
authorization exec test
exec-timeout 0 0
line vty 0
login authentication test
authorization exec test
line vty 1
login authentication test
authorization exec test
```

310. Para habilitar la autorización AAA basada en rol, se usa el siguiente comando:

```
Dell(conf)# aaa authorization role-only
```

311. Y para configurarlo se usa en modo EXEC *Privilege* el siguiente comando, determinando el modo CLI que el usuario usará en su sesión:

```
Dell(conf)# aaa authorization role-only exec {method-list-name | default} method […
method4]
```

312. Se puede restringir aún más los permisos de usuario con el siguiente comando en modo EXEC Privilege:

```
Dell(conf)# aaa authorization command {method-list-name | default} method […method4]
```

313. La siguiente configuración es un ejemplo con la lista de métodos TACACS+, RADIUS y local:

```
!
radius-server host 10.16.150.203 key <clear-text>
!
tacacs-server host 10.16.150.203 key <clear-text>
```

```
!
aaa authentication login ucraaa tacacs+ radius local
aaa authorization exec ucraaa tacacs+ radius local
aaa accounting commands role netadmin ucraaa start-stop tacacs+
!
```

314. Para conocer más en detalle los parámetros de configuración de políticas de roles, así como la configuración de AAA, consultar el manual *"Dell EMC Networking Configuration Guide 9.14" – REF1.*

6.11.2.1 CONFIGURACIÓN DE ATRIBUTOS VSA PARA RBAC EN RADIUS Y TACACS+

315. Ya sea usando el mecanismo de autorización RBAC (*Role Based Access Control*) o el basado en niveles de privilegio (clásico), las implementaciones de RADIUS y TACACS+ de Dell EMC Networking OS 9.14 soportan dos (2) opciones para su configuración: nivel de privilegio y roles. Es decir, puede recuperarse de RADIUS el role o el nivel de privilegio de un usuario que está autenticándose. De esta forma, RADIUS puede hacer de repositorio de configuración del nivel de autorización, con independencia del mecanismo usado en el *switch*.

316. Para ello, el identificador de atributo en el diccionario RADIUS para *Dell EMC Networking* es 6027 y el atributo consiste en una cadena de caracteres encabezada por "*Force10-avpair*" con el formato "*protocol: attribute sep value*" donde se almacena o bien el rol o bien el nivel de privilegio usado. El *switch* utilizará el valor recuperado y lo interpretará en función del mecanismo de autorización configurado en el propio switch, pudiendo ser este valor un número de nivel de privilegio o el nombre de un rol.

317. A continuación, se muestra un ejemplo de creación de un valor de atributo para el rol definido de sistema:

```
Force10-avpair= "shell:role=sysadmin"
```

6.12 PROTECCIÓN FRENTE ATAQUES

318. Existen en la actualidad multitud de ataques posibles que buscan comprometer la seguridad de los 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.

319. 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.

320. A continuación, se detallan algunos de estos ataques y las medidas que se pueden tomar para securizar un conmutador Dell EMC frente a ellos.

6.12.1 *DHCP SNOOPING*

321. 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.

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

    - 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.
    - 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.

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

324. Para evitar ataques del tipo *DHCP Spoofing*, *Dell EMC Networking OS 9.14* 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.

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

    - Activar *DHCP Snooping* a nivel global:

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

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

      ```
      ip dhcp snooping trust
      ```

    - Habilitar *DHCP Snooping* en una VLAN:

      ```
      ip dhcp snooping vlan name
      ```

326. 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 procedentes de él, independientemente de la dirección IP de la que procedan.

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

```
Dell# ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type
slot/port lease number
```

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

```
Dell# show ip dhcp snooping
IP DHCP Snooping : Enabled.
IP DHCP Snooping Mac Verification              : Disabled.
IP DHCP Relay Information-option               : Disabled.
IP DHCP Relay Trust Downstream                 : Disabled.
Database write-delay (In minutes)              : 0
DHCP packets information
Relay Information-option packets               : 0
Relay Trust downstream packets                 : 0
Snooping packets                               : 0
Packets received on snooping disabled L3 Ports : 0
Snooping packets processed on L2 vlans         : 142
DHCP Binding File DetailsInvalid File          : 0
Invalid Binding Entry                          : 0
Binding Entry lease expired                    : 0
List of Trust Ports                            :Te 1/4/1
List of DHCP Snooping Enabled Vlans            :Vl 10
List of DAI Trust ports                        :Te 1/4/1
```

329. Los comandos anteriores que aplican al protocolo IPv4 también tienen su versión en IPv6. Para más información sobre *DHCP Snooping*, puede consultarse el manual "*Dell Command Line Reference Guide 9.14" – REF1.*

6.12.2 *ARP SNOOPING*

330. El protocolo de resolución de direcciones ARP (*Address Resolution Protocol*) es un protocolo sencillo que permite conocer 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.

331. 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.

332. 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.

333. *Dell EMC Networking OS 9.14* proporciona una funcionalidad para proteger el funcionamiento del protocolo ARP basándose en la función de *DHCP Snooping*.

334. 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.

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

- Habilitar DCHP *Snooping*, tal como se ha visto en el apartado anterior.
- Validar las tramas de ARP contra la tabla de *binding* de DCHP *Snooping*, con el comando "*arp inspection*" en modo *interface*.

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

```
arp inspection
```

337. 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
```

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

```
Dell#show arp inspection database
Protocol Address    Age(min) Hardware Address   Interface VLAN  CPU
---------------------------------------------------------------------
Internet 10.1.1.251 -        00:00:4d:57:f2:50  Te 1/2/1  Vl 10 CP
Internet 10.1.1.252 -        00:00:4d:57:e6:f6  Te 1/1/1  Vl 10 CP
Internet 10.1.1.253 -        00:00:4d:57:f8:e8  Te 1/3/1  Vl 10 CP
Internet 10.1.1.254 -        00:00:4d:69:e8:f2  Te 1/5/1  Vl 10 CP
Dell#
```

339. Las estadísticas que muestran los paquetes ARP válidos e inválidos que han sido procesados se pueden consultar con el siguiente comando:

```
Dell#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
Dell#
```

340. Para más información sobre *ARP Protect*, puede consultarse el manual *"Dell Command Line Reference Guide 9.14" – REF1.*

6.12.3 INUNDACIÓN MAC

341. Todo conmutador Ethernet mantiene una tabla de filtrado utilizada 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.

342. 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).

343. 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.

344. 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.

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

346. 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.

347. 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.

348. 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.

349. El número máximo de direcciones MAC permitidas en una *interface*, se puede configurar con el siguiente comando:

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

350. Para visualizar la tabla de direcciones MAC (asociadas a puertos y VLAN), se debe usar 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]]]]]
```

- *address mac-address* (opcional): define la dirección MAC en formato xx:xx:xx:xx:xx:xx.
- *dynamic* (opcional): muestra las direcciones MAC aprendidas dinámicamente.
- *static* (opcional): muestra las direcciones MAC configuradas específicamente en el *switch*.
- *aging-time*: muestra la información del tiempo de *aging*.
- *interface interface* (opcional): identifica la interface.
- *interface interface-type* (opcional): define el tipo de *interface*, seguido del número de *slot*.
- *vlan vlan-id* (opcional): identifica la dirección MAC asignada a una determinada VLAN. EL rango es de 1 a 4094.
- *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.

7. FASE DE OPERACIÓN

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

- Revisar las alertas que genera en sistema, tanto en la consola CLI como en el servidor *syslog* configurado.
- Realizar copias de la configuración actual (*running-config)* a la configuración de arranque (*startup-config*) de forma periódica.
- Exportar las copias de seguridad de la configuración de forma periódica a un servidor externo.
- Controlar el acceso a la información de auditoría, de tal forma que únicamente el personal designado pueda acceder a ella.
- Comprobar si hay nuevas actualizaciones de *software* disponibles, con el objetivo de mantener el sistema actualizado siempre a la última versión.
- Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

8. CHECKLIST

352. 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			
Modo seguro/FIPS	☐	☐	
Modo Secure-CLI	☐	☐	
AUTENTICACIÓN			
Configuración autenticación Local	☐	☐	
Configuración RADIUS	☐	☐	
Configuración TACACS	☐	☐	
ADMINISTRACIÓN			
Configuración de usuarios	☐	☐	
Configuración de RBAC	☐	☐	
Configuración Gestión Remota	☐	☐	
Configuración Gestión Local	☐	☐	
CONFIGURACIÓN			
Configuración control del tráfico	☐	☐	
Certificados	☐	☐	
Servicios de Red	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Sincronización Horaria	☐	☐	
Actualizaciones del software	☐	☐	
Guardado de la configuración	☐	☐	
SNMP	☐	☐	
Política de contraseñas seguras	☐	☐	
Protección frente a ataques	☐	☐	
AUDITORÍA			
Registro de Eventos	☐	☐	
Almacenamiento Local	☐	☐	
Almacenamiento Remoto	☐	☐	

9. REFERENCIAS

REF1 *Dell Networking Command Line Reference Guide 9.14*. Específica para cada modelo de *Switch*.

REF2 *Dell Networking OS Configuration Guide 9.14.* Específica para cada modelo de *Switch*.

La documentación está disponible en la web de soporte de Dell, dentro del apartado: *Support* > *Product Support* > *Manuals*: https://www.dell.com/support/manuals

10. 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*
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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA