GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 648

Seguridad en conmutadores Netgear Prosafe

Noviembre 2017

Edita:
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
CCN Centro Criptológico Nacional
CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.29 14:56:38 +01'00'

NIPO: 785-17-080-3

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

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Este documento pretende servir de guía en la configuración de los conmutadores Netgear pertenecientes a la familia Prosafe y series M4100, M4200, M4300, M5300 y M6100 de la categoría Fully Managed. A lo largo de los diferentes capítulos se ofrecen recomendaciones sobre la activación o desactivación de servicios y determinadas funcionalidades de esta familia de conmutadores con el fin de poder establecer una configuración lo más segura posible.

La estructura del documento y sus contenidos no exigen una lectura lineal del mismo, se recomienda al lector utilizar el índice de contenidos para localizar la información deseada de manera más rápida y cómoda. Así mismo, aunque para la elaboración de esta guía se ha tomado como referencia la familia de conmutadores M6100, las recomendaciones descritas sobre seguridad son aplicables a cualquier otro modelo de conmutador Netgear Prosafe de las series mencionadas anteriormente.

2. OBJETO

Analizar los mecanismos de seguridad disponibles para proteger los entornos de sistemas de información y comunicaciones que emplean conmutadores Netgear Prosafe. Como consecuencia, se establece un marco de referencia que contemple las recomendaciones en la implantación y utilización de conmutadores Netgear Prosafe.

3. ALCANCE

Las autoridades responsables de la aplicación de la política de seguridad de las TIC determinarán el análisis y aplicación de este documento a los conmutadores Netgear bajo su responsabilidad.

4. ACCIONES PREVIAS A LA CONFIGURACIÓN DEL EQUIPO

Se deben aplicar las acciones de seguridad que contiene esta guía antes de que el equipo entre en contacto con la red en la que se integrará. La guía ha sido estructurada en primer lugar, indicando las medidas para evitar accesos no deseados a su configuración y a los datos almacenados en él, y posteriormente analizando los servicios que definirán sus interacciones con la red en la que esté integrado, para diferenciar aquellas acciones seguras y necesarias en el equipo, de aquellas que son poco seguras y que deben ser sustituidas por otras.

4.1. ACCESOS ACTIVADOS POR DEFECTO AL EQUIPO

Por defecto todo conmutador Prosafe Netgear Fully Managed dispone de acceso CLI, Telnet y HTTP/HTTPS activo por defecto. Además, todos los conmutadores de las familias M4200, M4300, M6100 disponen de puerto de gestión fuera de banda para un acceso remoto a la CPU del conmutador sin pasar por los puertos de conmutación. En la siguiente tabla se indican los parámetros por defecto de cada método de acceso.

Método de acceso	Puerto	Configuración por defecto
CONSOLA	USB / RJ45 RS232	Velocidad 115200 Bits de datos 8 Bits de stop 1 Paridad NO Control de flujo XON/XOFF
TELNET/HTTP/ HTTPS	Puerto de servicio o Puerto fuera de banda (OoB)	IP 192.168.0.239/16 o mediante DHCP
TELNET/HTTP/ HTTPS	Puertos de acceso	IP 169.254.100.100/16 o mediante DHCP

4.2. USUARIO POR DEFECTO

Por defecto los conmutadores disponen de un usuario con privilegios para el acceso mediante cualquier método, tanto CLI o Web GUI. Este usuario permite realizar cualquier gestión y configuración del conmutador sin ninguna restricción de forma que es imprescindible cambiar este usuario y contraseña.

Usuario por defecto	contraseña	Privilegios
admin		Gestión total (nivel 15)

4.3. PERMISOS DE USUARIO

Todo el equipamiento Netgear Prosafe Fully Managed dispone de distintos niveles de usuario. Por defecto, en los equipos encontraremos configurados dos niveles de privilegios: el nivel 0, o *User EXEC*, el cual es el nivel básico y el nivel 15, o *Privileged EXEC*, aunque posteriormente podemos especificar distintos niveles intermedios.

En los distintos niveles debemos configurar qué tipo de acciones se pueden realizar. Los niveles más altos permiten la realización de un mayor número de acciones, por ejemplo, el nivel *Privileged EXEC* podría considerarse como un “super usuario” en un entorno Unix. De este modo es posible comprender la importancia de proteger con una contraseña suficientemente fuerte, el acceso al nivel *Privileged EXEC*, ya que desde él se pueden modificar la configuración del equipo.

4.4. ESTRUCTURA DE LÍNEA DE COMANDOS

A continuación, se muestra una tabla en la que se resumen las distintas modalidades de la línea de comandos que nos ayudarán a familiarizarnos con el CLI, mediante el cual configuraremos el conmutador Netgear.

Modo	Método de acceso	Prompt
User EXEC	Este es el primer nivel de configuración. Permite cambiar propiedades del terminal, realizar funciones básicas y mostrar información del sistema	(Netgear Switch) >
Privileged EXEC	Desde el modo *User EXEC* introducir el comando ***enable***	(Netgear Switch) #
Configuración global	Desde el modo *Privileged EXEC* introducir el comando ***configure***	(Netgear Switch) (config)#
Configuración interfaz	Desde el modo de configuración global introducir el comando ***interface*** seguido de un identificador de interfaz. Si se quiere configurar un rango se puede introducir el inicio seguido de un guion y el puerto final	(Netgear Switch) (Interface #/N/#)#
Config-vlan	Desde el modo Privileged EXEC introducir el comando ***vlan database***	(Netgear Switch) (Vlan)#
Line configuration	Desde el modo de configuración global especificamos una línea de gestión que puede ser consola, telnet o ssh usando el comando ***line***	(Netgear Switch) (Config-line)#

4.5. SALVADO DE LA CONFIGURACIÓN

Es fundamental advertir que los cambios que realicemos en la configuración del equipo se almacenarán en una configuración denominada *running-config*, que es la empleada en ejecución. Esta configuración está almacenada en memoria volátil de forma que se elimina al reiniciar el equipo. Para que los cambios se mantengan una vez reiniciemos el equipo, es necesario copiar los cambios realizados de la *running-config* a la *startup-config*, que es el fichero que utiliza el conmutador para aplicar la configuración durante el arranque. Esta copia se lleva a cabo mediante el uso de una de las siguientes instrucciones.

```
(Netgear Switch) # copy system:running-config nvram:startup-config
(Netgear Switch) # save
```

4.6. MENSAJE INFORMATIVO

Por otro lado, es recomendable crear un mensaje informativo para definir el marco legal dentro del cual se realiza la sesión con el conmutador. Este banner aparecerá cuando se realicen conexiones a las diferentes líneas de comandos, consola o SSH.

```
(Netgear Switch) (config)# set clibanner
(Netgear Switch) (config)# exit
(Netgear Switch) # show clibanner
(Netgear Switch) # save
```

Se deben utilizar las dobles comillas (“) para delimitar el mensaje. Este mensaje deberá tener un máximo 2000 caracteres y puede contener caracteres especiales como tabulaciones y espacios. A continuación, un ejemplo.

```
(Netgear Switch) (config)# set clibanner "ADVERTENCIA A USUARIOS /
NOTICE TO USERS
================================================================
Esta maquina solo es para usuarios autorizados.
Si usted no esta autorizado, por favor, no intente acceder.
Todos los accesos son monitorizados y comprobados.
================================================================
This machine is only for authorized users.
If you are not authorized, please, do not try to access.
All the accesses are logged and are verified.
================================================================"
```

4.7. CONFIGURACIÓN PARA GESTIÓN REMOTA

Para poder hacer uso de cualquiera de los interfaces de gestión remota (SSH, Web, SNMP, etc…) es necesario configurar una dirección IP al conmutador. Por defecto todos los puertos pertenecen a la VLAN 1 (default). Esto es, están configurados como acceso para la VLAN 1 pero no es recomendable su uso. Se deben asignar todos los puertos a las VLAN que les corresponda y lo más segregado que se pueda.

Para dar una dirección IP a una VLAN de manera que cualquiera de los puertos del conmutador pertenecientes a dicha VLAN respondan a las peticiones TCP/IP con destino dicha dirección usaremos los siguientes comandos.

```
(Netgear switch)(config)# interface vlan 2
(Netgear switch) (config-if)# ip address X.X.X.X /MM
```

Donde X.X.X.X es la dirección IP y MM la máscara en notación decimal. Como medida básica de seguridad, se recomienda la aplicación de listas de acceso (ACL) para proteger el acceso a la gestión del conmutador de forma que solo un dispositivo o grupo de ellos pueda acceder a la configuración y administración, evitando así posibles accesos no deseados.

Por tanto, con el uso de ACL podemos decidir qué tráfico queremos permitir y/o denegar, controlando qué equipos de la red tendrán comunicación entre sí (o no). Es

por tanto una herramienta de seguridad cuya aplicación depende del tipo de tráfico de cada red que necesitemos denegar o aceptar.

Nos centramos aquí en el uso de ACL para la protección de la gestión del equipo de los ataques más frecuentes. En las reglas ACL de gestión se permitirá el acceso a los protocolos de acceso y gestión como SSH, HTTPS, SFTP y SNMP.

En los siguientes párrafos crearemos las ACL que permiten acceso a la dirección IP de gestión del dispositivo únicamente para los protocolos de gestión y deniegan cualquier otro tráfico con destino esa dirección IP. Para este ejemplo consideramos el direccionamiento 10.10.10.0/24 como red de gestión. Creamos la ACL y permitimos el tráfico SSH, desde la red de gestión.

```
(Netgear switch) (Config)# management access-list gestion
(Netgear switch) (config-macal)# permit ip-source 10.10.10.0 mask
255.255.255.0 service ssh priority 1
```

Por último tenemos que aplicar esta ACL con nombre “gestion” a la gestión del conmutador.

```
(Netgear switch) (Config)# management access-class gestion
```

Por defecto las políticas se aplican según el orden de prioridad configurado, como última regla implícita se deniegan todas conexiones que no hayan entrado en una regla de *permit* definida anteriormente.

4.8. ACTUALIZACIÓN DEL SOFTWARE DEL DISPOSITIVO

Se deben mantener los equipos actualizados con las últimas versiones estables del sistema operativo (*firmware*) para estar protegidos frente a *bugs* de seguridad que se van corrigiendo en las nuevas versiones.

Existen varios métodos para actualizar el software de un conmutador de Netgear Prosafe Fully Managed, en este guía se recoge la actualización por medio de SFTP ya que es un método cifrado de comunicación y más seguro que utilizar el método tradicional TFTP. Para realizar esta actualización necesitaremos:

- Haber configurado una dirección IP al conmutador para poder hacer la transferencia del archivo que contiene el nuevo *firmware*.
- Habilitar un servidor SFTP con el que el conmutador debe tener comunicación IP.
- Disponer del último *firmware* disponible para el conmutador en cuestión, para ello se puede descargar la última versión desde https://support.netgear.com.

Los conmutadores Netgear Prosafe disponen de dos imágenes sobre las que cargar nuevo *firmware*, con ello se facilita la operación de *rollback* de forma rápida.

Con tal de mantener dos imágenes siempre disponibles en esta guía se recomienda que la imagen 1 sea el *firmware* activo y la imagen 2 el *firmware* anterior o de *backup*. Por tanto, antes de realizar la actualización debe copiarse el *firmware* de la imagen 1 a la imagen 2.

```
(Netgear switch)# copy image1 image2
```

Para actualizar el conmutador a una nueva versión de software lo primero será copiar a la memoria interna del equipo el nuevo *firmware* a ejecutar, para esto haremos uso del comando.

```
(Netgear switch)# copy sftp://<ipaddress|hostname>/
<filepath>/<nombre fichero> image1
```

Es importante comprobar que la imagen 1 se ha actualizado correctamente y que será la siguiente imagen a ejecutar en caso de reinicio del conmutador. Para esto podemos hacer uso del siguiente comando.

```
(Netgear switch)# show bootvar
Image Descriptions
image1 :
image2 :
Images currently available on Flash
----  ------------  ------------  -----------------  ----------------
unit    image1        image2       current-active      next-active
----  ------------  ------------  -----------------  ----------------
1     11.0.0.28     11.0.0.33            image1          image1
2     11.0.0.28     11.0.0.33            image1          image1
```

5. LIMITACIÓN DE ACCESO A LA ADMINISTRACION DE EQUIPOS

El primer paso para obtener una infraestructura segura, es el cambio de la contraseña del usuario por defecto, ya que es fácil de encontrar en numerosos sitios web y documentación pública, para ello introducimos el comando, posteriormente nos pide introducir el *password* y su confirmación.

```
(Netgear switch) (Config)# username PepePerez password sFaGsFa!23$%
level 15 encrypted
```

Se deben utilizar distintas contraseñas, no sólo entre los distintos tipos de accesos a los equipos que configuremos y de acceso a los diversos niveles de ejecución, sino entre los propios equipos, ya que comprometer uno supondría una amenaza para el resto.

Igualmente, las contraseñas deben ser de al menos 12 caracteres, que no se basen en palabras de diccionario, y que contengan números y letras, además de alguno de los siguientes caracteres especiales (,./<>;':"[]\{}|~!@#$%^&*()_+`-=).

Deben cambiarse por lo menos una vez cada 90 días.

La opción *level* indica el nivel de administración de usuario, nivel 1 es un usuario de lectura mientras que el nivel 15 tiene permisos de gestión completos. Se recomienda tener todos los usuarios en nivel 1 para necesitar una segunda contraseña de gestión.

Adicionalmente se deben configurar políticas de uso de contraseñas, de forma que se obligue a cambiar la contraseña cada cierto tiempo, introducir un mínimo de caracteres especiales, mayúsculas, números, histórico de contraseñas, bloqueo de

usuario después de reintentos. Todas estas funciones se introducen mediante el comando *passwords* en modo *Global Config*. Estos son los posibles parámetros.

Comando	Descripción	Por defecto
min-length	Mínima longitud del *password*.	8
history	Retención de *password* usados por un usuario. Se puede escoger del 0 al 10.	0
lock-out	Máximo número de reintentos antes de bloquear un usuario. Del 1 al 5	0
strength maximum consecutive-characters	Máximo número de veces que puede haber un carácter consecutivo en un *password*. 0-15	0
strength maximum repeated-characters	Máximo número de caracteres repetidos. 0-15	0
strength minimum uppercase-letters	Mínimo de letras mayúsculas en el *password*. 0-15	2
strength minimum lowercase-letters	Mínimo de letras minúsculas en el *password*. 0-15	2
strength minimum numeric-characters	Mínimo número de caracteres numéricos. 0-16	2
strength minimum character-classes	Mínimo número de clases de caracteres. 0-4	4
strength exclude-keyword	Palabras excluidas como *password*	

Para comprobar la configurar introducir el comando *show password configuration*.

```
(Netgear switch) # show passwords configuration
Passwords Configuration
-----------------------
Minimum Password Length..................... 12
Password Aging (days)....................... 90
Password History............................ 10
Lockout Attempts............................ 5
Password Strength Check..................... Enable
Minimum Password Uppercase Letters.......... 2
Minimum Password Lowercase Letters.......... 2
Minimum Password Numeric Characters......... 2
Minimum Password Special Characters......... 2
Maximum Password Repeated Characters........ 4
Maximum Password Consecutive Characters..... 4
Minimum Password Character Classes.......... 4
Password Exclude Keywords................... <none>
```

5.1. ACCESO A MODO PRIVILEGIADO

Como se detalla en el punto anterior, en caso de que el administrador que se haya identificado correctamente en el equipo, y que haya accedido al *Privileged level* 1, necesite subir a un nivel superior, puede hacerlo usando el comando *enable*, y por defecto le llevará al *Privileged level* 15.

En este paso debemos asignar una contraseña al comando *enable*. Para asignarle una contraseña a este comando debemos realizar los siguientes pasos desde el nivel *Privileged EXEC mode*.

```
(Netgear switch)# enable password <password> encrypted
(Netgear switch)# save
```

5.2. CIFRADO DE CONTRASEÑAS

Por defecto las contraseñas se guardan en texto claro en los ficheros de configuración. Se debe utilizar la opción *encrypted* para cifrar las contraseñas de modo que en el fichero *show running* aparezcan cifradas.

5.3. TIEMPO DE INACTIVIDAD

Además de la protección de usuario se debe configurar un *timeout* para que no queden abiertas las conexiones. Estas conexiones son una amenaza frente a accesos no autorizados al conmutador.

Por defecto la línea consola tiene 5 minutos de *timeout* mientras que el acceso SSH dispone de 120 minutos. Se recomienda en medida del posible un *timeout* inferior a 10 minutos.

```
(Netgear switch)# configure
(Netgear switch)(Config)# line console
(Netgear switch)(Config-line)# serial timeout <0-160 minutes>
(Netgear switch)(Config-line)# exit
(Netgear switch)(Config)# exit
(Netgear switch)#sshcon timeout <0-160 minutes>
```

5.4. RECUPERACION DE CONTRASEÑA DE ACCESO

Es posible poder recuperar la contraseña de un usuario mediante el menú *boot* del conmutador. Para ello se debe disponer de acceso físico al equipo y tener acceso a la consola del mismo para acceder al menú de arranque.

Una vez conectados mediante el cable de consola al conmutador, para poder acceder al menú *boot,* se debe reiniciar el conmutador. En el proceso de arranque se debe pulsar la tecla "***q***" cuando aparezca el mensaje:

Starting program at 0xXXXXXXXX

Hecho esto, se puede seleccionar la opción 13:

Password Recovery Procedure

```
Boot Menu Options available
1 - Start operational code
2 - Change baud rate
5 - Load new operational code using USB
6 - Display operational code Vital Product Data
7 - File system directory listing
8 - Update boot code
9 - Delete backup image
10 - Reset the system
11 - Restore configuration to factory defaults (delete config files)
12 - Activate Backup Image
13 - Password Recovery Procedure
14 - Reformat the file system
15 - Upload a file through XMODEM
16 - Download a file through XMODEM
17 - Start Diagnostics Application
Q - Quit from operational code
Startup Select option :
```

Seleccionada la opción 13 el conmutador iniciará en modo *Privileged EXEC* sobre el que se puede modificar la contraseña del usuario mediante los comandos del punto anterior. Finalizado la configuración se debe guardar para sobrescribir el fichero *start-up* almacenado en la memoria no volátil (*nvram*).

6. SERVICIOS DE RED DEL EQUIPO

Una medida de seguridad básica a seguir es limitar los servicios activos para acceder a la gestión del conmutador, permitiendo acceder solo a aquellos que sean necesarios y dispongan de métodos que nos garanticen unos niveles de seguridad aceptables, y evitar acceso a medios que puedas ser explotados para la denegación de servicio del equipo afectado.

A continuación, se enumera una serie de servicios ofrecidos por el equipo y los comandos para configurarlos correctamente o deshabilitarlos si no es necesario, o no es recomendable su uso.

6.1. TELNET

Este servicio nos permite configurar el conmutador de forma remota una vez configurada una dirección IP de gestión. Pero este servicio debe de ser deshabilitado por la falta de cifrado, ya que permitiría, en caso de interceptar el intercambio de comunicación entre el cliente Telnet y el conmutador, detectar configuraciones, usuarios y contraseñas, así como cualquier dato escrito sobre el terminal.
Para desactivar el servicio de telnet se debe escribir el siguiente comando.

```
(Netgear switch)# no ip telnet server enable
```

Una vez introducido este comando el único medio de acceso al CLI del equipo será mediante la conexión física al puerto de consola de este, en caso de necesitar acceso remoto al interfaz CLI del conmutador se debe utilizar el protocolo SSH como se ve en la sección siguiente.

6.2. SSH

Como norma general, el único medio de gestión debería ser a través de la consola, ya que esto nos asegura controlar de una manera física los accesos a nuestro conmutador. Para deshabilitar ssh se debe ejecutar el siguiente comando.

```
(Netgear switch)# no ip ssh server enable
```

En caso de necesitar un terminal de gestión remoto solo se debe emplear SSH, ya que, a diferencia de Telnet, SSH sí garantiza unas medidas de seguridad básicas. Por lo tanto, se recomienda la utilización de SSHv2 para realizar accesos a la configuración del conmutador de forma remota.

Configurar el servicio de SSH requiere primero configurar una clave de autenticación con el siguiente comando.

```
(Netgear switch)(Config )# crypto key generate rsa
(Netgear switch)(Config )# crypto key generate dsa
```

Las claves pueden ser autogeneradas con una longitud de 1024 bits o bien descargadas de claves ya generadas previamente mediante el comando *copy,* utilizado en la actualización de *firmware*. En este caso un comando de ejemplo sería el siguiente.

```
(Netgear switch)# copy sftp://<ipaddress|
hostname>/<filepath>/<nombre fichero> nvram:sshkey-rsa2
(Netgear switch)# copy sftp://<ipaddress|
hostname>/<filepath>/<nombre fichero> nvram: sshkey-dsa
```

Una vez generadas o descargadas las claves se debe activar el protocolo SSH v2 y el servidor SSH mediante los siguientes comandos.

```
(Netgear switch)# ip ssh protocol 2
(Netgear switch)# ip ssh server enable
```

Ahora ya podemos iniciar la conexión desde un cliente que soporte SSHv2. Una vez autenticados tendremos acceso al CLI con todo el tráfico intercambiado entre el conmutador y el cliente utilizado para la gestión cifrada.

Para ver el estado del protocolo ssh se puede ejecutar el siguiente comando.

```
(Netgear switch)# show ip ssh
SSH Configuration
Administrative Mode: ..... Enable
SSH Port: ..... 22
Protocol Levels: ..... Version 2
SSH Sessions Currently Active: ..... 1
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA RSA
Key Generation In Progress: ..... None
```

6.3. INTERFACE HTTP/HTTPS

Los conmutadores Netgear Prosafe permiten acceder a una gestión completa mediante comandos y mediante una interfaz web tanto HTTPS como HTTP. Los métodos de configuración basados en HTTP pueden ser una posible vulnerabilidad o puerta de entrada para denegaciones de servicios. Por este motivo en esta guía se recomienda la desactivación de los servicios de gestión web tanto mediante HTTP como HTTPS.

Para poder desactivar los servicios de gestión web se deben ejecutar los siguientes comandos para los servicios HTTP y HTTPS.

```
(Netgear switch)# no ip http server
(Netgear switch)# no ip http secure-server
```

6.4. SNMP

SNMP es un servicio de gestión de red, que utiliza unas estructuras de datos conocidas como Management Information Base (MIB). En estos conmutadores se implementan las siguientes versiones de SNMP:

- **SNMPv1**. definido en la RFC 1157. Protocolo donde el intercambio de información de un dispositivo de red viaja en texto claro.
- **SNMPv2**. Definida en las RFC 1902 hasta la 1907. Sustituye a la versión anterior y proporciona mejoras en cuanto a operación y tipos de datos.
- **SNMPv3**. Tercera versión de este protocolo definido en las RFC 2273 hasta la 2275. Ofrece seguridad en el acceso a dispositivos mediante autenticación y cifrado de paquetes en la red.

Por lo tanto, y en caso de que sea necesaria la utilización de este protocolo, es absolutamente imperativo el implementar la tercera versión del mismo, ya que es el único capaz de garantizarnos unas medidas mínimas de seguridad.

En caso de decidir deshabilitar este protocolo es necesario seguir las siguientes instrucciones.

```
(Netgear switch)# configure
(Netgear switch) (config)# no snmp-server community mode
(Netgear switch) (config)# no snmp-server enable traps
(Netgear switch) (config)# end
```

Para configurar la autenticación y cifrado de SNMPv3 es necesario en primer lugar crear el usuario que accederá a los datos mediante SNMP y por otro configurar la autenticación (con método SHA recomendado) y cifrado con la clave DES. Los comandos a ejecutar serían los siguientes.

```
(Netgear Switch) (Config)# username [name] password [password]
(Netgear Switch) (Config)# username snmpv3 authentication [name] md5
| sha
(Netgear Switch) (Config)# users snmpv3 encryption [name] des <key>
```

Una vez creado el usuario se debe establecer los permisos de acceso mediante SNMP, las dos opciones son *readonly* y *readwrite* otorgando accesos de solo lectura y lectura/escritura respectivamente. Este comando por defecto aplica los permisos de lectura/escritura al usuario *admin* y solo lectura al resto de usuarios.

```
(Netgear Switch) (Config)# username snmpv3 accessmode [nombre]
readonly | readwrite
```

Con estos pasos seremos capaces de poder acceder a la lectura y/o escrituras de parámetros MIB del conmutador. Otra de las funciones disponibles mediante SNMP es la alerta a dispositivos de monitorización SNMP. Este servicio hace que el conmutador envíe información a otros equipos, generalmente equipos con acceso restringido y usados para gestionar la red, con información sobre eventos sucedidos. Para configurar este servicio se deben de realizar los siguientes pasos.

```
(Netgear Switch) (config)# snmptrap source-interface <unit/slot/port>
| vlan | loopback | serviceport
(Netgear Switch) (config)# snmptrap mode <community> ipaddr
(Netgear Switch) (config)# snmptrap ipaddr <community> <ipaddr>
```

Finalmente, para poder visualizar la configuración final de *traps* SNMP se pueden utilizar los siguientes comandos en modo *Privileged EXEC*.

```
(Netgear Switch) # show snmptrap
```

6.5. LLDP

LLDP (Link Layer Discovery Protocol) es un protocolo de nivel 2 que permite compartir información del sistema con otros dispositivos directamente conectados a los puertos del conmutador. Parte de esta información, como las direcciones IP de gestión, VLAN configuradas, servicios activos, versión del *firmware,* puede ser utilizada por un atacante.

No se debe hacer uso de este protocolo si no está justificado su uso. Y si fuese necesario hacerlo únicamente en los enlaces entre conmutadores sobre los que tengamos control, nunca en los puertos donde se conectarán dispositivos de usuario final. Todos los equipos Netgear Prosafe tienen LLDP activado por defecto en todas las interfaces. Para desactivarlo se debe aplicar el siguiente comando en todo el rango de interfaces.

En primer lugar para aplicar comandos de forma masiva se puede introducir el comando interface con un rango de interfaces continuo mediante el guion “-“.

```
(Netgear Switch) (config)# interface unit/slot/port-unit/slot/port
(Netgear Switch) (Interface unit/slot/port-unit/slot/port)# no lldp
transmit
(Netgear Switch) (Interface unit/slot/port-unit/slot/port)# no lldp
receive
```

En el caso de activar LLDP en un puerto determinado hay que introducir los comandos negados anteriormente.

Al activar LLD-MED se activa la extensión de LLDP que permite el intercambio de TLV adicionales que permite compartir información como servicios activos, QoS y funcionalidades específicas del dispositivo.

Este suele ser un medio de autodescubrimiento muy utilizado para las redes de Telefonía IP y la autoconfiguración de la VLAN de Voz sin necesidad de configurar los puertos de forma estática allí donde se conecte un teléfono IP.

6.6. ICMP

ICMP es un método de red básico que puede ser utilizado por atacantes para el descubrimiento de información de red como para realizar ataques de denegación de servicio. Para minimizar el uso de recursos es aconsejable desactivar los servicios ICMP disponibles. Algunos de estos están habilitados, pero por seguridad se recomienda desactivarlos globalmente si no está justificado su uso.

```
(Netgear Switch) (Interface unit/slot/port)# no ip unreachables
(Netgear Switch) (config)# no ip redirects
(Netgear Switch) (config)# no ip icmp echo-reply
```

6.7. ARP

De forma general los mensajes ARP se restringen a un único dominio de *broadcast*. Pero un conmutador puede hacer de proxy ARP desde un dominio a otro si queremos explícitamente que realice esta función.

Esta función se encuentra activa por defecto en todas las interfaces del conmutador de forma que se recomienda su desactivación en aquellas interfaces de nivel 3.

```
(Netgear Switch) (Interface unit/slot/port | Vlan X) # no ip proxy-
arp
```

7. SEGURIDAD EN LOS PUERTOS DE RED

Los interfaces de red de nivel de enlace se conocen como puertos. Y también se deben desplegar medidas de seguridad en torno a ellos ya que pueden ser objetivo de ataques o fugas de información.

En ocasiones, estas medidas de seguridad limitan la flexibilidad de los usuarios. Por ejemplo, el método empleado a continuación basado en el filtrado de direcciones físicas, limitando el paso por los puertos a las direcciones MAC autorizadas, ocasiona la pérdida de dinamismo en la configuración de nuestras redes a costa de tener mayor seguridad.

7.1. APAGADO DE PUERTOS

Una medida a llevar a cabo es apagar todos los puertos que no estemos utilizando. De este modo nos aseguramos que nadie puede conectarse a la red utilizando

cualquiera de los puertos que están libres. Desafortunadamente, conectarse a la red sería tan fácil como desconectar alguno de los dispositivos en uso y conectarse en ese puerto que ha quedado libre.

En cualquier caso, se deben apagar los puertos que no vamos a utilizar, con los siguientes comandos.

```
(Netgear Switch) (Interface unit/slot/port)# interface interface-id o
rango
(Netgear Switch) (Interface unit/slot/port)# shutdown
```

7.2. CONTROL DE TORMENTAS

Los conmutadores de Netgear Prosafe incorporan la 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.

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).

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 1 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.

Por defecto el control de tormentas está activado en *broadcast* y desactivado en *multicast* y *unicast* desconocido, en todos los puertos. El nivel de tráfico *broadcast* definido por defecto es un 5% del ancho de banda del puerto. Para realizar la configuración lo podemos hacer o bien de forma global en modo *Global Config* o bien por interfaz en *Interface Config*. Por simplicidad, vamos a aplicarlo de forma global.

```
(Netgear Switch) (config)# storm-control
{broadcast|multicast|unicast}
(Netgear Switch) (config)# storm-control
{broadcast|multicast|unicast} level <level>
```

Una vez configurado, cuando el número de tramas *broadcast, multicast o unicast* traspasan la tasa definida en el porcentaje, el puerto bloquea todos los paquetes. Hasta que no baja el nivel de paquetes por debajo de este límite este no vuelve a aceptar tramas de este tipo. Si en cambio, en esta situación de saturación queremos mantener el puerto activo, pero limitando el número de paquetes podemos utilizar la

opción *rate-limit*. Esta opción limita el número de paquetes por segundo recibidos desde 0 hasta 33554431. Por defecto este valor de tasa es 0. Para determinar la tasa de transferencia mínima se utiliza el siguiente comando.

```
(Netgear Switch) (config)# storm-control
{broadcast|multicast|unicast} rate <rate>
```

7.3. PROTECCIÓN CONMUTACIÓN ENTRE PUERTOS

Otra opción que nos ofrece Netgear Prosafe es crear *Protected Ports* (Puertos Protegidos), cuya peculiaridad es que no se realiza *forwarding* de tráfico entre dos puertos protegidos, cualquier otra combinación entre puertos protegidos y no protegidos continúan funcionando de manera normal.

Esto nos permite limitar la interacción entre equipos en una misma subred que deseemos no se comuniquen entre ellos. Esta funcionalidad permite la creación de hasta 3 grupos de *Protected Ports*. Para poder configurar un puerto como protegido debemos seguir los siguientes pasos.

```
 (Netgear Switch) (config)# interface interface-id
(Netgear Switch) (Interface interface-id)# switchport protected
<group id>
```

Esta funcionalidad solo es operativa cuando *vlan routing* y la interfaz de nivel 3 no están activas en las VLAN asociadas a los puertos que se quieren proteger.

Para poder realizar una separación más flexible y escalable se recomienda el método de *Private VLAN* (VLAN privadas) que se explicará a continuación.

La función de VLAN privadas separa un dominio VLAN regular en dos o más subdominios. Cada subdominio está definido (representado) por una VLAN primaria y una VLAN secundaria. El ID de VLAN principal es el mismo para todos los subdominios que pertenecen a una VLAN privada. El ID de VLAN secundaria distingue subdominios entre sí y proporciona aislamiento de capa 2 entre puertos de la misma VLAN privada.

Hay tres tipos de VLAN dentro de una VLAN privada:

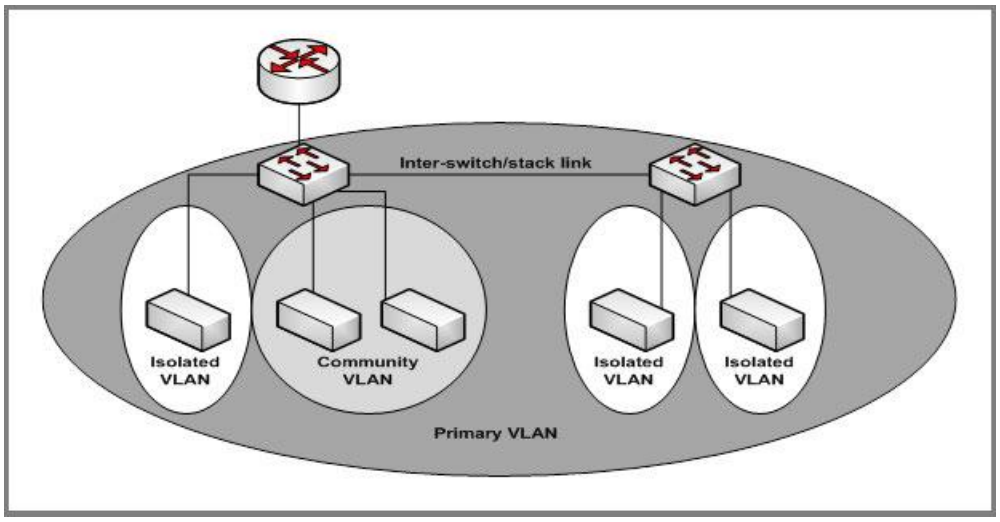
- VLAN primaria. Reenvía el tráfico de los puertos promiscuos a puertos aislados, puertos comunitarios y otros puertos promiscuos en la misma VLAN privada. Sólo se puede configurar una VLAN primaria por VLAN privada. Todos los puertos de una VLAN privada comparten la misma VLAN primaria.
- VLAN de la comunidad. Es una VLAN secundaria. Transmite el tráfico entre los puertos que pertenecen a la misma comunidad y los puertos promiscuos. Puede haber varias VLAN de la comunidad por VLAN privada.
- VLAN aislada. Es una VLAN secundaria. Transporta tráfico de puertos aislados a puertos promiscuos. Sólo se puede configurar una VLAN aislada por VLAN privada.

Hay tres tipos de designación de puerto dentro de una VLAN privada:

- Puerto Promiscuo. Pertenece a una VLAN primaria y puede comunicarse con todas las interfaces de la VLAN privada, incluidos otros puertos promiscuos, puertos comunitarios y puertos aislados.

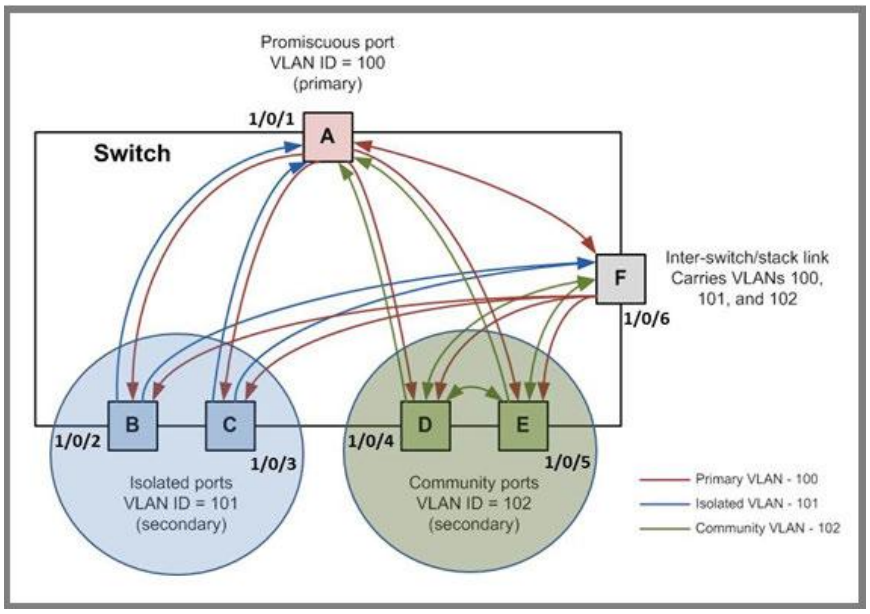
- Puertos comunitarios. Estos puertos pueden comunicarse con otros puertos comunitarios y puertos promiscuos.
- Puertos aislados. Éstos sólo pueden comunicarse con puertos promiscuos.

La siguiente figura muestra cómo las VLAN privadas se pueden extender a través de múltiples conmutadores empleando enlaces *inter-switch/stack* que transportan VLAN primarias, comunitarias y aisladas entre dispositivos.



Enlace Inter-switch/stack

La siguiente figura ilustra el flujo de tráfico de la VLAN privada. Cinco puertos A, B, C, D y E forman una VLAN privada. El puerto A es un puerto promiscuo que está asociado con la VLAN principal 100. Los puertos B y C son los puertos anfitriones que pertenecen a la VLAN aislada 101. Los puertos D y E son los puertos de comunidad que están asociados con la comunidad VLAN 102. El puerto F es el enlace *inter-switch/stack*. Está configurado para transmitir las VLAN 100, 101 y 102. Las flechas coloreadas representan posibles rutas de flujo de paquetes en el dominio VLAN privado.



Ejemplo de VLAN privada

Para la configuración de *Private* VLAN en primer lugar se deben crear las VLAN y definir su rol. Para simplificar vamos a ver el siguiente ejemplo con la VLAN 100 como primaria, VLAN 101 como aislada y VLAN 102 como comunitaria.

```
(Netgear Switch) (Config)# vlan 100
(Netgear Switch) (Config)(Vlan) # private-vlan primary
(Netgear Switch) (Config)(Vlan) # exit
(Netgear Switch) (Config)# vlan 101
(Netgear Switch) (Config)(Vlan) # private-vlan isolated
(Netgear Switch) (Config)(Vlan) # exit
(Netgear Switch) (Config)# vlan 102
(Netgear Switch) (Config)(Vlan) # private-vlan community
(Netgear Switch) (Config)(Vlan) # end
```

Una vez definido el rol de cada VLAN se debe asociar las VLAN secundarias (101-102) a la VLAN primaria 100.

```
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan association 101-102
(Netgear Switch) (Config)(Vlan) #end
```

A continuación para el ejemplo el puerto 1/0/1 actuará en promiscuo y del 1/0/1-1/0/5 serán puertos en modo host.

```
 (Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# switchport mode private-vlan
promiscuous
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)#interface 1/0/2-1/0/5
(Netgear Switch) (Interface 1/0/2-1/0/5)# switchport mode private-
vlan host
(Netgear Switch) (Interface 1/0/2-1/0/5)# end
```

Una vez definidos los puertos, hay que asignar las VLAN secundarias en cada puerto host. En el ejemplo asignaremos la VLAN aislada 101 a los puertos 1/0/2 y 1/0/3 mientras que en la VLAN comunitaria 102 la asignaremos al 1/0/4 y 1/0/5.

```
(Netgear Switch) (Config)# interface 1/0/2-1/0/3
(Netgear Switch) (Interface 1/0/2-1/0/3)# switchport private-vlan
host-association 100 101
(Netgear Switch) (Interface 1/0/2-1/0/3)# exit
(Netgear Switch) (Config)#interface 1/0/4-1/0/5
(Netgear Switch) (Interface 1/0/4-1/0/5)# switchport private-vlan
host-association 100 102
(Netgear Switch) (Interface 1/0/4-1/0/5)# end
```

Finalmente definimos todas las VLAN que podrán comunicarse con el puerto promiscuo, la 100,101 y 102.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# switchport private-vlan mapping
100 101-102
(Netgear Switch) (Interface 1/0/1)# end
```

7.4. PROTECCIÓN DE DIRECCIONES MAC POR PUERTO

La funcionalidad *port security* impide que dispositivos desconocidos envíen tráfico por cualquier puerto. La seguridad de puertos implementa dos métodos de filtración de tráfico, bloqueo dinámico y bloqueo estático. Estos métodos se pueden utilizar simultáneamente.

- Bloqueo dinámico. Se especifica el número máximo de direcciones MAC que se pueden aprender en un puerto. Una vez alcanzado el límite, no se aprenden más direcciones MAC adicionales. Sólo se reenvían las tramas con direcciones MAC de origen admisible.
- Las direcciones MAC bloqueadas dinámicamente tienen un tiempo de caducidad que puede ser configurado. Cuando un puerto se desconecta, se liberan todas las direcciones bloqueadas dinámicamente. Las direcciones MAC bloqueadas dinámicamente pueden ser aprendidas por otro puerto.
- Bloqueo estático. Puede especificar manualmente una lista de direcciones MAC estáticas para un puerto. Las direcciones MAC estáticas son permanentes y nunca son borradas.

Las direcciones bloqueadas dinámicamente se pueden convertir en direcciones bloqueadas estáticamente. Si se desea establecer una dirección MAC específica para un puerto, establezca las entradas dinámicas en 0 y, a continuación, permita sólo paquetes con una dirección MAC que coincida con la dirección MAC en la lista estática.

En caso de violación de política de seguridad o bien por una trama con una dirección MAC no fijada o bien por sobrepasar el límite de máximo número de direcciones MAC el conmutador bloqueará la trama y generará un mensaje *trap* SNMP para informar de la violación del puerto.

Es importante saber que la configuración por defecto del conmutador vendrá con la seguridad a nivel de puertos desactivada. Por lo tanto y una vez definidas estas terminologías, podemos proceder a explicar cómo llevar a cabo esta configuración. En primer lugar, hay que activar el *port-security* en cada puerto. Hay que anotar que este comando se puede configurar de forma global, pero para hacerlo así antes se deberán configurar todos los puertos para evitar bloqueo en aquellos puertos que no los deseemos. Para realizarlo en modo configuración de interfaz hay que introducir el siguiente comando.

```
(Netgear Switch) (configure)# interface interface-id
(Netgear Switch) (Interface interface-id)# port-security
```

Una vez hecho esto se podrá activar de forma global la funcionalidad de *port-security*.

```
(Netgear Switch) (configure)# port-security
```

Para configurar de forma estática las direcciones MAC que queramos permitir en un puerto del conmutador introduciremos el siguiente comando en cada puerto.

```
(Netgear Switch) (configure)# interface interface-id
(Netgear Switch) (Interface interface-id)# port-security mac-address
mac vlan-id
```

Utilizamos esta instrucción por cada dirección que queramos añadir a las tablas estáticas. Solo se puede introducir un número de entradas igual o inferior al máximo establecido en el límite máximo de direcciones MAC estáticas por puerto. Con los siguientes comandos podremos definir el máximo de direcciones MAC aprendidas de forma dinámica y el máximo número de direcciones MAC configuradas de forma estática. Dentro del modo configuración interface escribimos lo siguiente:

- Máximo de direcciones MAC dinámicas.

```
(Netgear Switch) (Interface interface-id)#port-security max-dynamic #
```

- Máximo de direcciones MAC estáticas.

```
(Netgear Switch) (Interface interface-id)#port-security max-static #
```

Si queremos limitar a una dirección MAC por cada puerto de forma estática debemos introducir el valor 0 en el comando *port-security max-dynamic.*

Puede ser interesante configurar puertos para que las direcciones aprendidas de forma dinámica se conviertan en estáticas de forma automática. Estas tendrán validez mientras el equipo no se reinicie ya que se mantienen en el fichero de configuración *running-config* que se encuentra en memoria volátil. Para habilitar este modo, llamado *sticky*, se puede realizar de forma global o bien por interfaz o rango de interfaz.

Adicionalmente, en el modo interfaz se puede acompañar el comando de una dirección MAC y un ID de VLAN para agregar una dirección *sticky* a la lista de direcciones estáticas. Estas direcciones se convierten en dinámicas si la función de *sticky* se deshabilita. Para activar la función de direcciones *sticky* se deben seguir los siguientes pasos.

- Activar direcciones *sticky* de forma global.

```
(Netgear Switch) (Config)# port-security mac-address sticky
```

- Activar direcciones *sticky* por interfaz.

```
(Netgear Switch) (Config)# interface interface-id
(Netgear Switch) (Interface interface-id)# port-security mac-address
sticky
(Netgear Switch) (Interface interface-id)# port-security mac-address
sticky [mac-address vid]
```

En el caso de querer convertir de forma definitiva direcciones aprendidas de forma dinámica a direcciones estáticas podremos introducir el siguiente comando por cada interfaz. Una vez realizado el comando para borrar las direcciones MAC se deberán borrar como si se hubiesen introducido de forma estática.

```
(Netgear Switch) (Config)# interface interface-id
(Netgear Switch) (Interface interface-id)# port-security mac-address
move
```

Una vez configurado el *port-security* podremos notificar las violaciones de políticas mediante mensajes *traps* SNMP o bien se pueden visualizar mediante el CLI. Para esto introduciremos el siguiente comando.

```
(Netgear Switch)# show port-security violation {unit/slot/port | lag
lag-intf-num}
```

Para activar el envío de *traps* SNMP se debe configurar el siguiente comando por interfaz.

```
(Netgear Switch) (Config)# interface interface-id
(Netgear Switch) (Interface interface-id)# snmp-server enable traps
violation
```

Una vez acabada la configuración podemos ver los resultados de la configuración y estado de los puertos o direcciones estáticas, dinámicas o *sticky* mediante los siguientes comandos:

- Configuración de *port-security* de un puerto.

```
(Netgear Switch)# show port-security [unit/slot/port | all]
```

- Configuración de direcciones MAC estáticas de un puerto o enlace agregado.

```
(Netgear Switch)# show port-security static {unit/slot/port | lag
lag-intf-num})
```

- Direcciones MAC dinámicas aprendidas en un puerto o enlace agregado.

```
(Netgear Switch)# show port-security dinamic {unit/slot/port | lag
lag-intf-num})
```

- Violación de políticas de *port-security* de un puerto o enlace agregado.

```
(Netgear Switch)# show port-security violation {unit/slot/port | lag
lag-intf-num}
```

8. CREACIÓN DE LISTAS DE ACCESO

Las listas de acceso (ACL) son una herramienta fundamental, la cual nos permite seleccionar qué direcciones IP vamos a permitir acceder por el puerto al que esté asociada dicha lista de acceso. Las ACL se evalúan línea a línea, hasta que se encuentra una coincidencia, por lo que hay que ser definir primero los casos más específicos y avanzar hasta llegar a los casos más generales. Por defecto se deniega todo el tráfico.

Para el tráfico IP hay dos tipos de ACL, estándar y extendidas:

- Las ACL estándar permiten o bloquean paquetes sólo en base a la dirección IP origen.
- Las ACL extendidas pueden permitir o bloquear paquetes basándose en protocolos, dirección IP origen o destino, puertos TCP/UDP origen o destino y también tipos de mensaje ICMP/IGMP.

Las recomendaciones generales a la hora de hacer una ACL son las siguientes:

- Para evitar el bloqueo total del tráfico, en cada ACL hace falta al menos una regla tipo *permit.*
- Una ACL se aplica sólo en un sentido, por tanto, solo se aplicará a los paquetes entrantes o salientes que pasen por el interfaz al que ha sido aplicada. Se debe minimizar el número de reglas.
- Al final de una regla tipo *deny*, se debe poner el parámetro *log* si se quieren registrar los paquetes denegados y poder analizar si se trata de algún tipo de ataque.
- Aunque todas las ACL tienen implícita una regla final, que deniega todo tipo de tráfico que no cumpla con ninguna de las reglas anteriores, se aconseja poner una última regla *deny any log*, con objeto de registrar en el *log* todo el tráfico descartado.

Para definir una ACL extendida, es necesario utilizar la siguiente instrucción.

```
(Netgear Switch) (Config)# access-list access-list-number {deny |
permit} protocol source source-wildcard destination destination-
wildcard [log]
```

Donde:

- *access-list-number*: número que identifica la lista de acceso extendida. Se utilizan los números del 101 al 199.
- *deny|permit*: define si la dirección que se introducirá a continuación en el campo source, debe ser admitida o rechazada.
- *source source-wildcard*: define la dirección origen a la que se está dando o denegando acceso, IP del host y su máscara en formato *wildcard*. El valor 255.255.255.255 puede sustituirse por *any*. Y la *wildcard* 0.0.0.0 por *host* seguido de la dirección IP correspondiente.
- *destination destination-wildcard*: Define el objetivo del paquete recibido. Sus campos se someten a las mismas condiciones de los de *source* y *source-wildcard*.
- *log*: De usarse este parámetro, se crea un informe cuando ésta lista niega un acceso.

Un ejemplo de modificación de una lista puede ser el siguiente.

```
(Netgear Switch) (Config)# access-list 101 permit tcp host 10.1.1.2
any
(Netgear Switch) (Config)# access-list 101 deny ip host 10.1.1.2 any
(Netgear Switch) (Config)# access-list 101 permit ip 10.1.1.0
0.0.0.255 host 10.1.1.2
```

9. MEDIDAS CONTRA LA DENEGACIÓN DE SERVICIO

Muchos de los ataques que sufren los equipos que ocupan posiciones estratégicas en una red tienen como objetivo provocar que el equipo en cuestión no pueda seguir ofreciendo sus servicios hacia la red. Son los denominados ataques de denegación de servicio (DoS).

Los ataques de tipo *fast flooding*, pueden causar que el procesador se sobrecargue, tanto que no pueda gestionar la política de accesos y se bloquee ese servicio.

El control de flujo 802.3X permite a los puertos que están recibiendo tráfico, pausar la transmisión de paquetes en su origen durante momentos de congestión. Si se activa esta posibilidad, se corre el riesgo de recibir una instrucción de pausa deteniendo la transmisión de paquetes de datos. Por tanto, los mensajes de pausa utilizados por este sistema de control de flujo pueden ser utilizados en un ataque de denegación de servicio.

Algunos tipos de ataques y ciertos errores también pueden provocar sobrecarga de paquetes (*packet floods*) en los puertos de un conmutador.

El servicio Unidirectional Link Detection (UDLD) se utiliza para determinar si existe un link unidireccional entre dos conmutadores, y en ese caso el puerto se desconecta hasta que sea restaurado manualmente. Por lo tanto, los mensajes de UDLD pueden ser usados en ataques de denegación de servicio.

Otro tipo de ataque más simple es el conocido como *SYN Flood Attack*, que consiste en el envío masivo de peticiones de conexión sin terminar de completar el intercambio de mensajes para establecer la misma. Este ataque puede saturar el buffer de conexiones incompletas del conmutador y provocar que este deje de funcionar.

El software Netgear Managed Switch proporciona soporte para clasificar y bloquear tipos específicos de ataques de denegación de servicio. Puede configurar el equipo para supervisar y bloquear los siguientes tipos de ataques:

- "SIP = DIP": dirección IP de origen = dirección IP de destino.
- *First fragment*: Tamaño del encabezado TCP menor que el valor configurado.
- *TCP fragment*: permite al dispositivo eliminar paquetes que tienen una carga útil TCP en la que la longitud de la carga útil IP menos el tamaño del encabezado IP es menor que el tamaño de encabezado TCP mínimo permitido.
- *Flag TCP*: el *flag* de TCP SYN set y puerto de origen <1024 o *flags* de control TCP = 0 y número de secuencia TCP = 0 o *flags* TCP FIN, URG y set PSH y número de secuencia TCP = 0 o *flag* TCP SYN y FIN.
- *L4 Port*: Puerto TCP / UDP de origen = Puerto TCP / UDP de destino.
- ICMP: Limitación del tamaño de los paquetes de ping ICMP.

- "SMAC = DMAC": dirección MAC de origen = dirección MAC de destino.
- Puerto TCP: Puerto TCP de origen = Puerto TCP de destino.
- Puerto UDP: Puerto UDP de origen = Puerto UDP de destino.
- *TCP Flag & Sequence*: Conjunto de TCP *flag* SYN y Puerto origen < 1024 o *flags* de Control TCP = 0 y numero de secuencia TCP = 0 o conjunto de *flags* TCP FIN, URG, y PSH y numero de secuencia TCP = 0 o conjunto de *flag* TCP SYN y FIN.
- *TCP Offset*: Permite al dispositivo descartar paquetes que tienen un *offset* en cabecera TCP = 1.
- TCP SYN: TCP *flag* SYN.
- TCP SYN & FIN: combinación de TCP *flags* SYN y FIN.
- TCP FIN & URG & PSH: Combinación de *flags* TCP FIN, URG y PSH conjuntamente con *TCP Sequence Number* = 0.
- ICMP V6: Limita el tamaño de paquetes ICMPv6 Ping.
- *ICMP Fragment*: Comprueba paquetes fragmentados ICMP.

Se pueden activar o bien todos los ataques o ataques de forma individual con los siguientes comandos:

- Activar todo los controles de DoS definidos anteriormente.

```
(Netgear Switch) (Config)#dos-control all
```

- Activar controles DoS de forma individual.

```
(Netgear Switch) (Config)#dos-control [sipdip | firstfrag [size] |
tcpfrag | tcpflag |l4port | smacdmac | tcpport | udpport | tcpflagseq
| tcpoffset | tcpsyn | tcpsynfin |tcpfinurgpsh| icmpv4 [size] |
icmpv6 [size] | icmpfrag ]
```

- Para comprobar la configuración se puede observar con el siguiente comando:

```
(Netgear Switch) # show dos-control
```

Además de los ataques predefinidos es una recomendación deshabilitar protocolos de nivel dos como *flow control* o UDLD ya que pueden ser una posible fuente de ataques de denegación de servicio.

Mediante el siguiente comando podemos desactivar el control de flujo de Ethernet para evitar que sea susceptible de un ataque. Este está desactivado por defecto.

```
(Netgear Switch) (Config)# no flowcontrol
```

Otro servicio que se recomienda desactivar es UDLD, el cual puede ser deshabilitado globalmente o en cada interfaz donde no es necesario. Para desactivarlo de forma global es necesario usar la siguiente instrucción:

```
(Netgear Switch) (Config)# no udld enable
```

Para realizar esta desactivación en cada interfaz, se puede utilizar la siguiente instrucción dentro del menú de configuración de ese interfaz.

```
(Netgear Switch) (Interface interface-id)# no udld port
```

10. DHCP SNOOPING

La asignación dinámica de direcciones IP por medio del uso de un servicio de DHCP supone exponer nuestra red a una serie de vulnerabilidades bien conocidas relacionadas con el uso de éste y por tanto no está recomendada, a menos que habilitemos DHCP Snooping en todos los equipos de la red.

DHCP Snooping es una función de seguridad que monitoriza los mensajes DHCP entre un cliente DHCP y un servidor DHCP para filtrar mensajes dañinos de DHCP y para construir una base de datos de enlaces (dirección MAC, dirección IP, ID de VLAN, puerto) que se consideran autorizadas. El administrador de red habilita DHCP Snooping globalmente y en VLAN específicas y configura los puertos dentro de la VLAN para que sean confiables o no sean de confianza. Los servidores DHCP deben ser alcanzados a través de puertos de confianza. DHCP Snooping está desactivado por defecto, para habilitarlo introducimos el comando.

```
Netgear Switch (Config)# ip dhcp snooping
```

Una vez activado de forma global, este se debe activar por cada VLAN donde queramos que DHCP Snooping este monitorizando el tráfico de asignación de direccionamiento IP dinámico.

```
Netgear Switch (Config)# ip dhcp snooping vlan vlan-id
```

Para finalizar es necesario configurar el puerto confiable donde se encuentra el servidor DHCP o desde donde se alcanza el servidor DHCP mediante otro conmutador. Todo el resto de paquetes de DHCP de servidor que no entren por un puerto confiable será descartado.

```
(Netgear Switch) (Config)# interface interface-id
(Netgear Switch) (Interface interface-id)# ip dhcp snooping trust
```

Para poder ver la tabla de asignación de IP, MAC, VLAN y puerto podemos utilizar el siguiente comando desde el modo *Privileged EXEC.*

```
(Netgear Switch) # show ip dhcp snooping binding
```

Para poder encontrar un servidor de DHCP no fiable se puede ver o bien mediante las estadísticas del servicio de DHCP Snooping la columna de *MAC Verify Failures* con el siguiente comando.

```
(Netgear Switch) # show ip dhcp snooping statistics
```

O bien con el registro de *logs*, pudiendo ser estos analizados de forma local en el conmutador o bien enviados mediante a un servidor *syslog*. Este comando se debe introducir en cada puerto.

```
(Netgear Switch) (Interface interfaceid)# ip dhcp snooping log-
invalid
```

Otra función de DHCP Snooping es evitar la suplantación de direccionamiento IP, para esto el conmutador valida que los paquetes IP enviados en cada puerto y VLAN coinciden según se ha registrado en su tabla de concesión de direccionamiento IP asignadas de forma dinámica por el servidor de DHCP conectado en un puerto confiable, esta función se llama IP Source Guard. Todos los paquetes que no coincidan con la información de la tabla serán bloqueados. Para evitar que los paquetes de dispositivos con dirección IP estática sean bloqueados es posible el completar la tabla de DHCP Binding con el siguiente comando.

```
(Netgear Switch) (Config)# ip dhcp snooping binding mac-address vlan
vlan-id ipaddress interface interface-id
```

Para activar IP Source Guard por puerto se debe introducir el siguiente comando. Este puede permitir el tráfico basado en la dirección IP de la tabla de DHCP Snooping Binding o bien con la opción port-security se filtrará según la dupla MAC y dirección IP origen.

```
(Netgear Switch) (Interface interfaceid)# ip verify source [port-
security]
```

Las entradas de la tabla de concesiones DHCP se actualizan cada vez que hay una nueva entrada o modificación, se puede retrasar la actualización de la base de datos para que esta no sea tan frecuente y realice los cambios en bloque. Por defecto este tiempo es de 300 segundos y su valor pude ser de 15 a 86400 segundos.

```
(Netgear Switch) (Config)# ip dhcp snooping database write-delay
seconds
```

Adicionalmente es posible controlar la velocidad a la que los mensajes DHCP Snooping entran en una interfaz o rango de interfaces. De forma predeterminada, la limitación de la velocidad está desactivada. Cuando está activada, la velocidad puede variar de 0 a 300 paquetes por segundo (pps). El rango del nivel de ráfaga es de 1 a 15 segundos.

```
(Netgear Switch) (Interface interfaceid)# ip dhcp snooping limit
{rate pps [burst interval seconds]}
```

Para verificar el estado de IP Source Guard y su configuración por puerto se puede utilizar el siguiente comando.

```
(Netgear Switch)# show ip verify source
```

El siguiente comando permite mostrar la tabla de IP Source Guard completa.

```
(Netgear Switch)# show ip source binding
```

10.1 ARP SNOOPING

La inspección dinámica ARP (DAI) es una característica de seguridad que rechaza paquetes ARP no válidos y maliciosos. DAI previene una clase de ataques *man in the middle*, donde una estación hostil intercepta tráfico para otras estaciones envenenando las cachés de ARP de sus vecinos. El atacante envía peticiones ARP o respuestas que asignan la dirección IP de otra estación a su propia dirección MAC.

DAI se basa en la función de DHCP Snooping. DHCP Snooping escucha los intercambios de mensajes DHCP y genera una base de datos vinculante de direcciones MAC válidas, direcciones IP, VLAN e interfaces.

Cuando se habilita DAI, el conmutador omite paquetes ARP cuya dirección MAC remitente y la dirección IP del remitente no coinciden con una entrada en la base de datos de concesiones de DHCP. Opcionalmente puede configurar la validación adicional de paquetes ARP.

Para activar la función de DAI por VLAN introducir el siguiente comando.

```
(Netgear Switch) (Config)# ip arp inspection vlan vlan-list
```

Si se quiere activar la validación adicional para comprobar la dirección MAC origen (src-mac), dirección MAC destino (dst-mac) o validación de la dirección IP de los paquetes ARP recibidos.

```
Netgear Switch) (Config)# ip arp inspection validate {[src-mac] [dst-
mac] [ip]}
```

En caso de no querer validar paquetes ARP mediante DAI es posible la configuración de un puerto confiable con el siguiente comando.

```
(Netgear Switch) (Interface interfaceid)# ip arp inspection trust
```

Para poder visualizar y alertar cuando hay paquetes de ARP inválidos o que no cumplen con las características de la base de datos se puede registrar en modo *log* tanto en local como en un servidor *syslog*.

```
(Netgear Switch) (Config)# ip arp inspection vlan vlan-list logging
```

Es posible configurar los valores de límite de velocidad (rate-limiting) y de intervalo de ráfaga (burst) para una interfaz o rango de interfaces. Al configurar la opción *none*, significa que la interfaz no está limitada en las tasas para las inspecciones ARP dinámicas. El valor máximo de *pps* mostrado en el rango de la opción *rate* puede ser mayor que el límite permitido por hardware. Por lo tanto, es necesario comprender el rendimiento del conmutador y configurar la tasa máxima de *pps* en consecuencia.

La interfaz de usuario acepta un límite de velocidad para una interfaz de confianza o *trusted*, pero el límite no se aplica a menos que la interfaz esté configurada como no confiable. El comando se puede aplicar por interfaz o grupo de interfaces.

```
(Netgear Switch) (Interface interfaceid)# ip arp inspection limit
{rate pps [burst interval seconds] | none}
```

Una vez aplicado la configuración podemos ver el estado, configuración y estadísticas por puerto con los siguientes comandos.

- Ver las estadísticas DAI por puerto y por VLAN.

```
(Netgear Switch) # show ip arp inspection statistics vlan vlan-list
```

- Ver la configuración de DAI por VLAN.

```
(Netgear Switch) # show ip arp inspection vlan vlan-id
```

- Ver la configuración de DAI por cada puerto o de todos los puertos.

```
(Netgear Switch) #show ip arp inspection interfaces [unit/slot/port]
```

11. VLAN

Podemos definir una VLAN o Virtual Local Area Network como un dominio de difusión, o lo que es lo mismo, todos los miembros pertenecientes a una VLAN reciben los paquetes de *broadcast* de los otros miembros de su VLAN, pero no de los pertenecientes a otras VLAN.

A diferencia con las LAN tradicionales es que las agrupaciones de equipos y la creación de subredes se va a implementar de forma lógica y, por lo tanto, la pertenencia a una VLAN no depende de la ubicación física del equipo. Es por esto que las labores de administración de las LAN se facilitan enormemente gracias a las VLAN, ya que para modificar la pertenencia de equipos a las distintas subredes no se va a necesitar de un desplazamiento físico de los mismos.

11.1 CREACIÓN DE VLAN COMO MEDIDAS DE AISLAMIENTO

El soporte de VLAN en un conmutador de capa 2 ofrece beneficios tanto a nivel de enlace como de red. Al igual que un *bridge*, un conmutador VLAN reenvía el tráfico basado en el encabezado de la capa 2. Al igual que un enrutador, divide la red en segmentos lógicos, lo que proporciona una mejor administración, seguridad y administración del tráfico de multidifusión.

Una VLAN es un conjunto de estaciones finales y puertos de conmutación que las conectan. Puede haber diferentes razones para la división lógica, como la pertenencia a un departamento o diferentes niveles de seguridad. El único requerimiento físico es que la estación final y el puerto al que está conectado pertenezcan a la misma VLAN.

Cada VLAN en una red tiene una ID de VLAN asociada, que aparece en la etiqueta IEEE 802.1Q en la cabecera de la capa 2 de paquetes transmitidos. Una estación final puede omitir la etiqueta o la parte VLAN de la etiqueta, en cuyo caso el primer puerto de conmutación en recibir el paquete puede rechazarlo o insertar una etiqueta usando su ID de VLAN predeterminada. Un puerto determinado puede manejar el tráfico de más de una VLAN, pero sólo puede admitir una ID de VLAN predeterminada.

La función *Private Edge VLAN* añade una capa más de seguridad permitiendo establecer la protección entre los puertos ubicados en el conmutador. Esto significa que un puerto protegido no puede reenviar tráfico a otro puerto protegido en el mismo conmutador y VLAN, o bien que un grupo de puertos pueda comunicarse entre ellos, pero no con el resto de puertos de la misma VLAN. Esta característica no proporciona protección entre puertos ubicados en diferentes conmutadores.

Los conmutadores Netgear Prosafe Managed por defecto tienen creada la VLAN 1 y en la cual están asignados todos los puertos incluidos los puertos de gestión, por lo cual la primera acción recomendable sería la creación de una nueva VLAN que mantenga los puertos de configuración fuera de las subredes a las que accedan los usuarios no administradores.

```
(Netgear Switch)# network mgmt_vlan vlan-id
```

Otra recomendación de seguridad es la de establecer una VLAN en la cual agrupemos todos los puertos inactivos y aislar éstos de cualquier VLAN que contenga puertos activos. Por tanto, es una buena práctica asignar de inicio todos los puertos a una VLAN distinta a la creada por defecto por el conmutador, para después ir sacándolos de ese grupo y asignándolos a las VLAN a las que pertenecerán, de esta forma nunca utilizaremos la VLAN por defecto lo que nos garantiza una mejora en la seguridad.

A la hora de configurar VLAN y asignarlas a puertos, en primer lugar debemos crear y definir la VLAN en cada conmutador. Para esto accedemos al modo *Config VLAN* desde *Privileged EXEC mode*:

```
(Netgear Switch) # vlan database
(Netgear Switch) (Vlan)# vlan vlan-id
(Netgear Switch) (Vlan)# exit
```

Donde *vlan-id* puede ser un id no usado hasta el momento para definir una nueva VLAN o bien el id de una VLAN ya definida para poder modificarla. El identificador se compone de un número entre los valores 1 a 4094, siendo desde la 1006 a la 4094 consideradas *Extended Range VLAN* cuyo funcionamiento es ligeramente distinto al de las VLAN habituales. Es recomendable analizar esas diferencias antes de implementar una Extended VLAN, por ejemplo, no se guardan en la base de datos de las VLAN, y tienen un conjunto de opciones de configuración más limitado que el de las VLAN normales.

Por otro lado, es recomendable añadir un nombre descriptivo a la VLAN para saber su función. Si no se introduce un nombre el conmutador crea uno por defecto identificado como VLAN <numero vlan>. Donde <numero vlan> es el valor introducido en la creación de la VLAN en 4 dígitos. Por ejemplo, si creamos la VLAN 4 el nombre por defecto será VLAN0004.

```
(Netgear Switch) (Vlan)# vlan name vlan-id “name”
```

11.2 ASIGNACIÓN DE VLANS A PUERTOS

Antes de indicar cómo configurar o asignar una VLAN a un puerto vamos a describir las diferentes características o conceptos de VLAN asociados a puertos en un conmutador Netgear Prosafe Managed. Estos son los siguientes:

- *port PVID*: Es la VLAN predeterminada en un puerto del conmutador. Todas las tramas recibidas por un puerto sin identificación de VLAN en la cabecera 802.1Q, el conmutador la identificará con la VLAN configurada en PVID.
- *vlan tagging*: Las VLAN son identificadas como *tagged* en un puerto permitiendo que todas las tramas que se envían desde el puerto hacia el dispositivo conectado vayan con la cabecera 802.1Q y el campo VLAN con el identificador de VLAN. Las tramas de VLAN no especificada como *tagged* irán sin cabecera 802.1Q.
- *vlan participation*: incluye las VLAN a las que forma parte un puerto, esta puede ser una, varias o todas. Por defecto está incluida la VLAN 1 con lo que si se quiere evitar enviar tráfico de la VLAN 1 se debe excluir específicamente.
- *vlan acceptframe*: establece que tipo de tramas son aceptadas por un puerto, hay tres tipos de tramas diferenciadas:
  - *untagged*: solo las tramas sin cabecera 802.1Q son aceptadas.
  - *vlanonly*: solo las tramas con cabecera 802.1Q son aceptadas.
  - *all*: todas las tramas son aceptadas.
  - *ingress filter*: solo las VLAN incluidas en *vlan participation* son aceptadas por el puerto, el resto son descartadas.

Una vez se han descrito los principales conceptos de asignación de VLAN vamos a mostrar como configurar un puerto con dos perfiles típicos. Puerto donde se conecta un PC o dispositivo final que no dispone de configuración de 802.1Q y solo pertenece a una VLAN y un puerto donde circulan varias VLAN identificadas como 802.1Q por ejemplo un puerto de enlace con un conmutador.

- Cuando configuramos un puerto de usuario o *edge port* hay que tener en cuenta en qué VLAN queremos que participe este dispositivo final para poder asignar a la VLAN predeterminada en el puerto. Por otro lado, aplicaremos *vlan accept frame* para que solo el tráfico sin etiqueta circule por el puerto y filtraremos todas las tramas que no pertenezcan a la VLAN configurada.

```
(Netgear Switch)(Interface interfaceid)# vlan participation exclude 1
(Netgear Switch)(Interface interfaceid)# vlan participation include
vlanid
(Netgear Switch)(Interface interfaceid)# vlan pvid vlanid
(Netgear Switch)(Interface interfaceid)# vlan acceptframe
admituntaggedonly
(Netgear Switch)(Interface interfaceid)# vlan ingressfilter
```

- Cuando configuramos un puerto donde queremos que circulen varias VLAN como por ejemplo un puerto UPLINK, puerto de conexión a host que gestione varias VLAN o bien puerto de conexión a un enrutador o cortafuegos. En este caso

debemos configurar que las tramas que se conmuten por dicho puerto tengan la cabecera 802.1Q con el identificador de VLAN. En este tipo de puertos también se define una VLAN predefinida o VLAN nativa, por defecto es la VLAN 1. Como se ha explicado anteriormente es una recomendación de seguridad evitar esta VLAN por defecto con lo que se debe cambiar a otra VLAN que debe estar configurada en los dos extremos. Por esta VLAN nativa circulará el tráfico de gestión de nivel 2 como UDLD, LLDP, STP, etc. La configuración de un puerto de este tipo se hará de la siguiente forma.

```
(Netgear Switch)(Interface interfaceid)# vlan participation exclude 1
(Netgear Switch)(Interface interfaceid)# vlan participation include
vlanid [separado por coma o guion en rangos consecutivos incluido
vlan nativa]
(Netgear Switch)(Interface interfaceid)# vlan pvid vlanid [vlan
nativa]
(Netgear Switch)(Interface interfaceid)# vlan tagging vlanid range
[separado por coma o guion en rangos consecutivos excluido vlan
nativa]
(Netgear Switch)(Interface interfaceid)# vlan ingressfilter
(Netgear Switch)(Interface interfaceid)# vlan acceptframe all
```

12. CONFIGURACIÓN DE SPANNING TREE

El propósito del Spanning Tree Protocol (STP) es eliminar los bucles en el sistema de conmutación. Existen cuatro versiones de STP: STP clásico (802.1d), Rapid STP (RSTP, 802.1w), Multiple STP (MSTP, 802.1s) y una versión no estandarizada de STP el RPVSTP+ desarrollador por Cisco.

Mientras STP puede tomar 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.

En MSTP *(*Multiple Spanning Tree Protocol*)*, cada instancia Spanning Tree puede contener varias VLAN. Cada instancia de Spanning Tree 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.

El protocolo Per VLAN Rapid Spanning Tree (PVRSTP) es similar al protocolo Rapid Spanning Tree (RSTP) según lo definido por IEEE 802.1w, pero con una diferencia principal: PVRSTP ejecuta una instancia por VLAN. Es decir, cada VLAN configurada ejecuta una instancia independiente de PVRSTP y cada instancia elige un *root bridge* independiente de otra instancia. Una región puede incluir tantos *root bridge* como VLAN que están configuradas para PVRSTP. PVRSTP es equivalente al RPVST + de Cisco y puede interactuar con él.

La diferencia entre MSTP y PVSTP o PVRSTP radica principalmente en la forma en que el protocolo mapea las instancias de STP a VLAN: PVSTP o PVRSTP crea una instancia de STP para cada VLAN, mientras que MSTP asigna una o más VLAN a cada instancia, múltiple árbol de expansión (MST).

12.1. RAPID SPANNING TREE

RSTP (Rapid Spanning Tree Protocol), definido en el estándar IEEE 802.1W, es un protocolo de encaminamiento de nivel 2 que evita bucles en la red, al tiempo que ofrece redundancia en los caminos que dispone la red para el envío de paquetes. Los bucles pueden ocurrir cuando han sido configurados caminos redundantes para incrementar la resistencia de la red ante la caída de algún enlace. En caso de establecerse un bucle es posible que las estaciones comiencen a recibir mensajes duplicados, y crear situaciones que vuelvan inestable y mermen el rendimiento de nuestra red. Para evitar esta situación se produce un intercambio constante de información entre conmutadores. La información se envía en tramas Ethernet conocidas como Bridge Protocol Data Units (BPDU).

El funcionamiento de RSTP se basa en la elección del *root*. Esta se realiza mediante el intercambio en las BPDU de un parámetro llamado *Bridge ID* que se compone de 8 bytes. Los dos primeros se utilizan para mandar la prioridad de STP y los seis bytes restantes la dirección MAC del equipo. Una vez se analizan todos los *Bridge ID* el conmutador que tiene el valor más bajo de toda la red se elige como *root*.

El conmutador que se elige como *root* tiene la peculiaridad de que va a mantener todos los caminos disponibles (ninguno de sus enlaces se cerrará para evitar un posible bucle, si no que el resto de la red se bloqueará de manera que esos enlaces puedan permanecer abiertos). Por tanto, es importante que el *root* de una red con RSTP sea el punto hacia/desde donde más tráfico se origine.

Si un dispositivo con menor *Bridge ID* se introduce en la red, se convertirá de manera automática en el nuevo *root*, mermando el rendimiento de las comunicaciones en esta. Como en este protocolo no se ha definido ningún tipo de identificación que permita averiguar la validez de la información recibida, tendremos que utilizar otras herramientas para evitar que alguien pueda modificar a voluntad la topología de STP que se verán a continuación.

12.1 SPANNING-TREE EDGE PORT

Cuando un puerto tiene configurado RSTP, al detectar que un dispositivo se conecta físicamente en ese puerto, no se empieza a transmitir o recibir información del dispositivo conectado de una manera inmediata, ya que el conmutador comienza a enviar y escuchar tramas BPDU con objeto de determinar si el dispositivo que se ha conectado supone un bucle en la red (y en tal caso bloquear la trasmisión/recepción de datos por este puerto) o en caso contrario, tras un tiempo en el que se estudia la posibilidad de la existencia de bucle en la red, comenzar la comunicación con el dispositivo conectado en el puerto. Para evitar este tiempo de retardo entre que conectamos el nuevo equipo y se habilita la comunicación con el resto de la red, se pueden configurar como *edge port* aquellos puertos en los que no vamos a conectar más conmutadores que formen parten de la topología de RSTP, sino simplemente estaciones de trabajo o dispositivos de usuarios finales. Los comandos a utilizar son los siguientes a nivel de interfaz.

```
(Netgear Switch)(Interface interfaceid)# spanning-tree auto-edge
```

El uso de esta funcionalidad no supone que conmutador deje de ser capaz de detectar un bucle, ya que un puerto configurado como *auto-edge* envía BPDU y tan pronto recibe una BPDU deshabilita la función *edge port* y pasa a comportarse como un puerto de RSTP normal. Además, es muy recomendable configurarlo en todos los puertos que vayan a tener *link down* y *link up* de manera periódica (como ocurre con los ordenadores al apagarlos al abandonar el puesto de trabajo) para evitar que el exceso de trafico de RSTP perjudique el rendimiento de la red.

Edge port mejora el tiempo de conexión de un nuevo dispositivo a una red en la que esta RSTP configurado, pero no nos protege de que un puerto de los que se supone que solo va a dar acceso a estaciones de trabajo se conecte un dispositivo que tenga RSTP activo y pueda alterar la topología de nuestra o incluso hacerse el *root* de la red, para evitar esto podemos utilizar las funcionalidades que se indican a continuación.

12.2 SPANNING-TREE ROOT GUARD

Al configurar un puerto como *root guard* nos aseguramos que este siempre será un puerto designado (Designated Role). Cuando un puerto que tiene configurado *root guard* recibe un BPDU con un *Bridge ID* inferior al *root* existente, pasa automáticamente al estado *discarding* dejando de trasmitir cualquier tipo de paquete que por él se reciba. De este modo se impide que el dispositivo aquí conectado se convierta en el nuevo *root* de la red, alterando la topología deseada. Para configurar un puerto como *root guard* usamos el comando en modo interfaz.

```
(Netgear Switch)(Interface interfaceid)# spanning-tree guard root
```

12.3 SPANNING-TREE PORTFAST BPDU-GUARD

Otra opción para proteger la topología deseada es utilizar *bpduguard*. Si un puerto configurado como *bpduguard* recibe una BPDU cualquiera, el puerto es automáticamente apagado. Para configurar un puerto para que sea apagado tan pronto como reciba una BPDU podemos utilizar los comandos.

```
Netgear Switch (config)# spanning-tree bpduguard
```

Una vez que un puerto ha sido apagado al recibir una BPDU, por defecto permanece en estado *D-Disable* 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 resto configuraremos *auto recovery* mediante los siguientes comandos en el modo *Global Config*.

```
Netgear Switch (config)# errdisable recovery cause bpduguard
Netgear Switch (config)# errdisable recovery interval <30-86400>
```

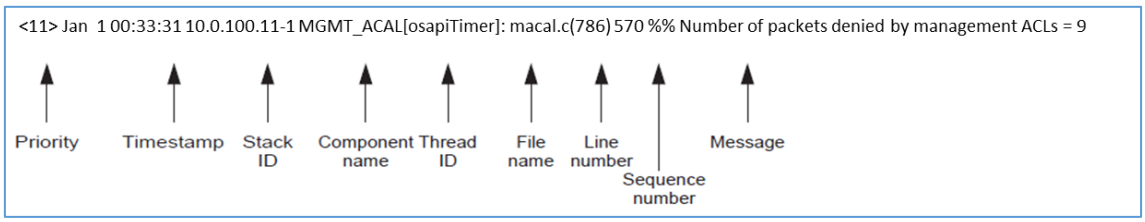
13. MANTENIMIENTO DE REGISTROS Y DEPURACIÓN: LOGS Y NTP

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

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

Los conmutadores NETGEAR Prosafe generan mensajes en respuesta a eventos, fallos o errores que ocurren en la plataforma, así como cambios en la configuración u otras ocurrencias. Estos mensajes se almacenan localmente y pueden ser reenviados a uno o más puntos de colección centralizados para fines de monitorización o almacenamiento de archivos a largo plazo. La configuración local y remota de la capacidad de registro incluye el filtrado de mensajes registrados o reenviados según la gravedad y el componente generador.

En el siguiente diagrama se muestra cómo interpretar un mensaje de *log*.



La prioridad (es decir, el número que se indica entre corchetes angulares antes de cada mensaje de registro, por ejemplo, <11> en el ejemplo anterior) se calcula sumando 8 al valor de severidad, en este caso 3 (Error). Si conoce la prioridad, puede determinar la facilidad y la gravedad de las siguientes maneras:

- *facility* = Prioridad dividida por 8. El número entero es la facilidad. Por ejemplo, si la prioridad es 11, divida 11 por 8. El resultado es 1,375. El número entero es 1, que es la instalación.
- *severity* = Prioridad menos 8. Por ejemplo, si la prioridad es 11, resta 8 de 11. El resultado es 3, que es Error.
- Los valores de *severity* son los siguientes:
  - Emergencia (0). El sistema es inutilizable.
  - Alerta (1). La acción debe ser tomada inmediatamente.
  - Crítico (2). Condiciones críticas.
  - Error (3). Condiciones de error.
  - Advertencia (4). Condiciones de advertencia.
  - Aviso (5). Condiciones normales pero significativas.
  - Información (6). Mensajes informativos.
  - Debug (7). Mensajes de nivel de depuración

Si se quiere ver los mensajes en consola se puede configurar para que todos los *logs* generados en tiempo real se envíen a la consola de línea CLI o bien se almacena en memoria volátil por defecto. Estos comandos se introducen en modo *Global Config*:

- Guardado de *logs* en local:

```
(Netgear switch) (Config)# logging buffered
```

- Salida de *logs* en pantalla de línea de comandos:

```
(Netgear switch) (Config)# logging console [severitylevel]
```

Los mensajes registrados en una la línea de comandos o servidor de *syslog* utilizan un formato idéntico, por ejemplo, el siguiente mensaje:

```
<15> Ago 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %%
Interface 12 transitioned to root state on message age timer expiry.
```

Este ejemplo indica un mensaje con gravedad 7 (15 mod 8) (depuración) en un chasis y generado por el componente MSTP que se ejecuta en el ID de subproceso 2110 el 24 de agosto de 05:34:05 por la línea 318 del archivo mstp_api.c. Este es el 237º mensaje registrado con el sistema IP 0.0.0.0 y el ID de tarea 1.

```
<15> Ago 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %%
Interface 12 transitioned to root state on message age timer expiry.
```

Este ejemplo indica un mensaje de nivel de usuario (1) con gravedad 7 (depuración) en un sistema que no es un chasis y generado por el componente MSTP ejecutándose en el ID de subproceso 2110 el 24 de agosto de 05:34:05 por la línea 318 del archivo *mstp_api.c*. Este es el 237o mensaje registrado.

En los *logs* almacenados en el sistema, sólo se muestran las últimas 200 entradas en la pantalla. Por seguridad y escalabilidad se recomienda que los mensajes se envíen a un servidor *syslog*. Este tráfico es enviado en texto claro de forma que debemos asegurarnos que el camino que sigue este tráfico sea un camino seguro y aislado del resto de la red.

Para configurar un servidor de *syslog* podemos determinar un filtro de severidad para enviar *logs*. Este podrá variar según cada situación, pero se recomienda mantener como mínimo la severidad de *notice* (5). Por defecto el puerto es el 514 y la severidad es *critical* (2).

```
(Netgear Switch) (Config)# logging host <hostaddress | hostname>
addresstype [port-number [<severitylevel>]]
```

Para poder establecer una interfaz origen para el envío de tramas *logs* y mantener filtro de seguridad en el servidor *syslog* o servidores se debe configurar el siguiente comando.

```
(Netgear Switch) (Config)# logging syslog source-interface
{unit/slot/port | {loopback loopback-id} | {vlan vlan-id} {tunnel
tunnel-id | serviceport}}
```

Finalmente, para poder ver la configuración de *syslog* del sistema podemos utilizar los siguientes comandos en modo *Privileged EXEC*:

- Ver configuración de servicios *logs:*

```
(Netgear Switch) # show logging
```

- Ver *logs* almacenados en local en el conmutador:

```
(Netgear Switch) (Config)# show logging buffered
```

- Ver servidores de *syslog* configurados:

```
(Netgear Switch) (Config)#show logging host
```

13.1 SINCRONIZACIÓN DE TIEMPO Y HORA

A la hora de analizar *logs* y poder correlar eventos, es de vital importancia una sincronización de tiempo de todos los elementos de la red que intervienen en el análisis. Para esto la configuración de un protocolo de sincronización con un reloj único nos permite poder tener una misma referencia en todos los equipos de red. Los conmutadores Netgear Prosafe utilizan el protocolo SNTP como protocolo de sincronización de tiempo. Las características de SNTP son las siguientes:

- SNTP proporciona sincronización de fecha y hora de la red.
- Puede utilizarse en modo *broadcast* o *unicast*.
- Soporta SNTP cliente implementado a través de UDP, que escucha en el puerto 123.

Los pasos para configurar un servidor de tiempos son los siguientes:

- Configurar la dirección IP del servidor SNTP.

```
(Netgear Switch) (Config)# sntp server ipaddress
```

- Activar el modo de cliente SNTP. El modo de cliente puede ser el modo de difusión o el modo *unicast*. Si el servidor NTP no es suyo, debe utilizar el modo *unicast*:
  - **Unicast.** SNTP opera de una manera punto a punto. Un cliente de *unicast* envía una solicitud a un servidor designado en su dirección de *unicast* y espera una respuesta desde la que puede determinar el tiempo y, opcionalmente, el retardo de ida y vuelta y el desplazamiento del reloj local en relación con el servidor.
  - **Broadcast.** SNTP funciona de la misma manera que el modo de multidifusión, pero utiliza una dirección de difusión local en lugar de una dirección de multidifusión. La dirección de difusión tiene un único alcance de subred mientras que una dirección de multidifusión tiene un amplio alcance de Internet.

```
(Netgear Switch) (Config)# sntp client mode [broadcast | unicast]
```

Cuando el modo de cliente SNTP está habilitado, el cliente espera el intervalo de sondeo para enviar la consulta al servidor. El valor predeterminado es de aproximadamente 1 minuto. Si se quiere modificar este intervalo de sondeo o *polling* se puede ejecutar el comando siguiente.

```
(Netgear Switch) (Config)# sntp [unicast | broadcast] client poll-
interval
```

En el caso de configurar una IP origen para el envío de peticiones NTP como en el caso de los *syslog* se puede definir con el siguiente comando.

```
(Netgear Switch) (Config)# sntp source-interface {unit/slot/port |
loopback loopback-id | vlan vlan-id}
```

Una vez hemos configurado la sincronización de reloj, si ésta se hace sobre un NTP atómico o de horario estándar, es importante sincronizar la zona horaria y los desfases horarios de verano e invierno. El comando será el siguiente.

```
(Netgear Switch) (Config)# clock summer-time recurring EU offset 60
(Netgear Switch) (Config)# clock timezone 1 minutes 0
```

Una vez realizada la configuración podemos ver la sincronización NTP con los servidores de tiempos y su estado con el siguiente comando en el modo Privileged EXEC.

```
(Netgear Switch)# show sntp server
```

Si queremos ver la hora que tiene el conmutador utilizaremos el siguiente comando y su opción *detail* para ver la configuración de horario de verano y zona horaria.

```
(Netgear Switch)# show clock [detail]
```

14. AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO

Esta sección está relacionada con el apartado 5 de esta guía, ya que trata las posibilidades que disponemos a la hora de incrementar la seguridad en el acceso a nuestros equipos.

Un posible problema con los procedimientos vistos hasta el momento, es que hasta ahora siempre se ha realizado la autenticación de forma local en el conmutador. Y es 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 nuestra red exactamente igual. Además de los problemas que supone el tener que crear/modificar los perfiles de los administradores en todos los equipos uno a uno.

Para solucionar estos problemas disponemos de varios mecanismos de autenticación y de creación de cuentas de forma centralizada. Esto nos 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 sólo sea

necesario realizarlo en un único equipo. A estos métodos se los denomina *Authentication, Authorization and Accounting* (AAA).

El concepto de *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. Por último, el *Accounting* el cual ofrece un servicio de registro de los servicios accedidos por un usuario al igual que el ancho de banda utilizado por este usuario. Netgear implementa AAA utilizando dos protocolos para poder acceder a los servidores de seguridad: RADIUS y TACACS+.

14.1 RADIUS

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). El servidor RADIUS normalmente se trata de un sistema multiusuario ejecutando el software de servidor de RADIUS.

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

- Se le pide al usuario que introduzca su *login* y *password*.
- El *login* y el *password* cifrado son enviados al servidor de RADIUS.
- El usuario recibe uno de los siguientes mensajes del servidor:
  - ACCEPT: El usuario ha sido autenticado.
  - REJECT: El usuario no ha podido ser autenticado y, o bien se le solicita que introduzca sus datos de nuevo o se le niega el acceso.
  - CHALLENGE: Se le solicita más información al usuario.
  - CHALLENGE PASSWORD: Se le pide al usuario que introduzca un nuevo *password*.

14.2 802.1X

En la autenticación basada en puertos, cuando 802.1X está habilitado globalmente y en el puerto, la autenticación correcta de cualquier solicitante conectado al puerto da como resultado que todos los usuarios puedan utilizar el puerto sin restricciones. En un momento dado, sólo un suplicante puede intentar la autenticación en un puerto en este modo. Los puertos en este modo están bajo control bidireccional. Este es el modo de autenticación predeterminado.

La red 802.1X tiene tres componentes:

- **Autenticadores:** El puerto que se autentica antes de permitir el acceso al sistema.

• **Suplicantes:** El host está conectado al puerto autenticado que solicita acceso a los servicios del sistema.

• **Servidor de autenticación:** El servidor externo, por ejemplo, el servidor RADIUS que realiza la autenticación en nombre del autenticador e indica si el usuario está autorizado para acceder a los servicios del sistema.

En primer lugar, para la configuración de autenticación de usuarios debemos configurar los servidores RADIUS que van a realizar la función de validación, es recomendable que se configuren varios servidores por redundancia e indicar el servidor primario. Finalmente, en la asociación autenticador y servidor de autenticación hay un intercambio de un *secret*, este debe ser asociado a cada host. Para esto hay que introducir los siguientes comandos en modo *Global Config*.

```
(Netgear Switch) (config)# radius server host [auth | acct] {hostname
| ip-address} [name] [port port-number] [name]
(Netgear Switch) (config)# radius server primary {hostname | ip-
address}
(Netgear Switch) (config)# radius server key auth {hostname | ip-
address}
Enter secret (64 characters max):****
Re-enter secret:****
```

Donde:

- *hostname | ip-address:* Especificamos la dirección IP o el nombre de host del servidor de RADIUS.
- *port port-number:* Puerto UDP destino al que enviar las peticiones de autenticación, si no se especifica se utilizar el puerto por defecto de autenticación RADIUS 1812.
- *secret string:* Especifica la clave de cifrado/descifrado que se usará en las comunicaciones entre el conmutador y el servidor de RADIUS.

Una vez que hemos definido qué servidor realizará las comprobaciones, debemos proceder a especificar cómo llevar a cabo el proceso de autenticación y que tipo de autenticación 802.1X se va a utilizar.

```
(Netgear Switch)# configure terminal
(Netgear Switch) (config)# aaa authentication dot1x default radius
```

Una vez definido el servicio de autenticación y activado el servicio 802.1x todos los puertos requerirán de autenticación de un suplicante para poder activar el tráfico de datos del puerto. En el caso de que un puerto no tenga un cliente con suplicante debemos forzar la autorización para evitar que este puerto esté bloqueado. Esta configuración será en el caso de puertos donde hay equipos conectados tipo impresoras, equipos de red, conmutadores, enrutadores, teléfonos, etc. que no tienen suplicante instalado. Para evitar este bloqueo debemos forzar la autenticación de la siguiente manera.

```
(Netgear Switch)(Interface interfaceid)# 2)# dot1x port-control
force-authorized
```

Por el contrario, si queremos bloquear un puerto y que siempre este desautorizado podemos introducir el siguiente comando. Con este, aunque se conecte un equipo con suplicante y con un usuario autorizado este equipo no se podrá conectar a la red.

```
(Netgear Switch)(Interface interfaceid)# 2)# dot1x port-control
force-unauthorized
```

Otra opción es el de disponer una VLAN de invitados de forma que si después de un *timeout* el puerto no recibe ningún mensaje EAPOL de suplicante auto-configura una VLAN predefinida que puede estar restringida a un determinado uso, por ejemplo, acceso a ciertos servicios restringidos. Para esto en cada puerto específico debemos configurar un *timeout* y la VLAN de invitados.

```
(Netgear Switch)(Interface interfaceid)# dot1x timeout guest-vlan-
period <1-300 segundos>
(Netgear Switch)(Interface interfaceid)# dot1x guest-vlan vlanid
```

Para activar la función de protección 802.1x en el conmutador se debe activar de forma global mediante el siguiente comando.

```
(Netgear Switch)  (config)# dot1x system-auth-control
```

14.3 AUTORIZACION Y ACCOUNTING

Por otro lado, la autorización en la administración del conmutador aporta capilaridad a los comandos y accesos disponibles por el usuario. Cuando la autorización AAA está activada, el conmutador obtiene información del perfil del usuario, la cual se encuentra, bien en la base de datos local del conmutador, o en un servidor de seguridad, y mediante esa información se configura la sesión del usuario.

Los servidores TACACS + admiten la autorización de comandos. El protocolo RADIUS no admite la autorización de comandos, pero puede utilizar un atributo específico del proveedor (VSA) con par de valores de atributo 26 (AV) para descargar una lista de comandos permitidos o denegados para un usuario. Esta lista de comandos se descarga desde el servidor RADIUS.

Cuando un usuario ejecuta un comando, el comando se valida contra la lista de comandos descargados para el usuario. Cualquier cambio en una lista de acceso de autorización de comandos de usuario surte efecto después de que un usuario haya iniciado de nuevo una sesión.

```
(Netgear Switch)(Config)# aaa authorization commands [listname]
[radius | tacacs]
 (Netgear Switch)(Config)# line [ssh | telnet | console]
(Netgear Switch)(Config-line)# authorization commands <listname>
```

Al principio del documento se ha hablado de los 15 niveles de privilegios que un usuario del conmutador puede tener. Para poder asignar los privilegios de forma automática por RADIUS o TACACS que se debe configurar la autorización en modo ejecución (EXEC).

Si el método de autorización EXEC utiliza un servidor de autorización TACACS+, se establece una sesión independiente con el servidor TACACS+ para devolver los atributos de autorización.

Si el método de autorización EXEC utiliza un servidor de autorización RADIUS, se utiliza el atributo de tipo de servicio 6 o el atributo específico de proveedor de Cisco (VSA) *shell: priv-lvl*. Si el valor del atributo del tipo de servicio se devuelve como administrador o el *shell: priv-lvl* de Cisco VSA es al menos FD_USER_MGR_ADMIN_ACCESS_LEVEL (15), el usuario recibe acceso al modo EXEC privilegiado.

Dado que el protocolo RADIUS no admite autorización, el atributo de nivel de privilegios debe devolverse con la respuesta de autenticación. Si el atributo de tipo de servicio ya está presente en el paquete de respuesta RADIUS como administrador, se omite el *shell* de Cisco VSA *priv-lvl*. Los siguientes comandos activan la autorización por TACACS y RADIUS al acceso al CLI.

```
(Netgear Switch)(Config)# aaa authorization exec [listname] [radius |
tacacs]
(Netgear Switch)(Config)# line [ssh | telnet | console]
(Netgear Switch)(Config-line)# authorization exec <listname>
```

El proceso de auditoría registra lo que un usuario hace o ha hecho en el conmutador. Puede configurar un servidor de contabilidad TACACS+ o un servidor de *accounting* RADIUS para que tenga registro de las siguientes acciones:

- Registro de los servicios que se utilizaron. Puede utilizar este tipo de registro como una herramienta de auditoría para servicios de seguridad.
- Registro cuando un usuario inicia sesión y se desconecta de una sesión EXEC de su usuario.

En este caso vamos a ver un ejemplo de configuración de autorización con un servidor TACACS+ con *accounting* de comandos y de acceso EXEC. TACACS+ soporta el *accounting* de comandos y acceso EXEC.

```
(Netgear Switch)(Config)# tacacs-server host 10.100.5.13
(Netgear Switch)(Tacacs)# key 12345678
(Netgear Switch)(Tacacs)# exit
(Netgear Switch)(Config)# aaa authorization commands [listame] tacacs
(Netgear Switch)(Config)# aaa authorization exec [listame] tacacs
(Netgear Switch)(Config)# aaa accounting commands [listame] stop-only
tacacs
(Netgear Switch)(Config)# aaa accounting exec [listame] stop-only
tacacs
(Netgear Switch)(Config)# line [ssh | telnet | console]
(Netgear Switch)(Config-telnet)# accounting commands [listame]
(Netgear Switch)(Config-telnet)# login authentication tacacs
(Netgear Switch)(Config-telnet)# authorization commands tacacs
(Netgear Switch)(Config-telnet)# exit
```

ANEXO A: ACRÓNIMOS Y ABREVIACIONES

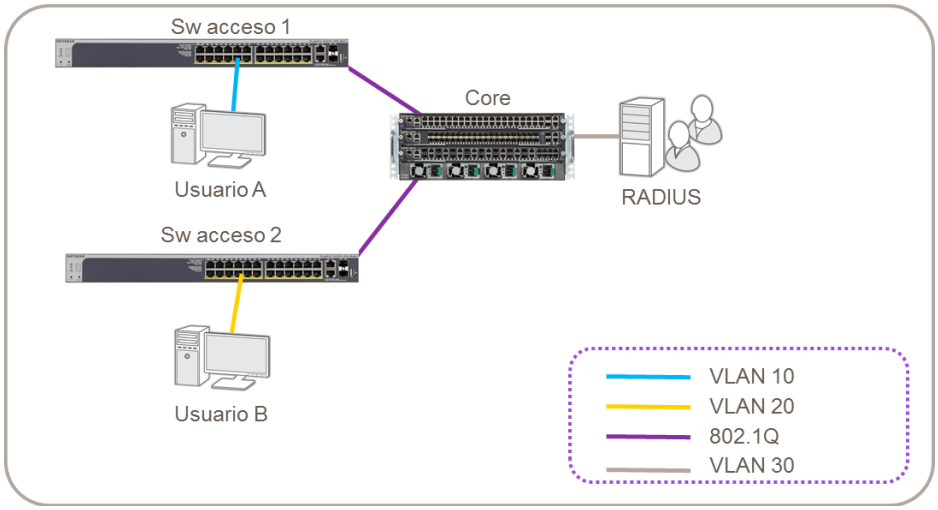
- Authentication, Authorization and Accounting (AAA): es el marco de servicios de seguridad que ofrece un sistema de identificación de usuarios (authentication), para control de acceso remoto (authorization), y para obtener y enviar información de seguridad para facturación, auditorias e informes (accounting).
- Address Resolution Protocol (ARP): es un protocolo TCP/IP empleado para obtener la dirección física de un nodo. Una estación cliente realiza un broadcast de peticiones ARP en una red con la IP del nodo del cual quiere comunicarse, y el nodo con esa dirección le responde enviando de vuelta su dirección física. Así pueden empezar una comunicación entre ambos.
- Bridge Protocol Data Unit (BPDU): es un mensaje de datos que es intercambiado entre los conmutadores pertenecientes a una extended LAN que usa una topología STP.
- Domain Name System (DNS): es un protocolo que traduce nombres de dominio en direcciones IP usando servidores DNS. Cada servidor DNS contiene una base de datos de nombres de dominio (nombres de equipos) y sus correspondientes direcciones IP.
- Dynamic Host Configuration Protocol (DHCP): es un protocolo que asigna automáticamente direcciones IP a estaciones clientes que se están conectando a una red TCP/IP.
- File Transfer Protocol (FTP): es un medio de transferencia de ficheros entre equipos conectados a una red. Usa TCP como protocolo de transporte, el puerto 21 para el control de conexiones, y el puerto 20 para conexiones de datos, todos ellos son los valores por defecto. Puede ser configurado con nombres de usuario y passwords para identificación y autenticación.
- Hyper Text Transfer Protocol (HTTP): es el protocolo usado por los navegadores y servidores web para la transferencia de archivos. Usa TCP como mecanismo de transporte y el puerto 80 por defecto. Puede ser configurado para identificación y autenticación mediante nombres de usuario y contraseñas.
- Internet Control Message Protocol (ICMP): es un protocolo TCP/IP usado para enviar mensajes de control y de error.
- Internet Protocol (IP): es uno de los principales protocolos usados por los equipos de red a nivel 3 de la tabla OSI. Es un protocolo no orientado a conexión, por lo que depende de otros mecanismos (por ejemplo, TCP) para ponerlos en el orden correcto cuando lleguen a su destino.
- Local Area Network (LAN): es una red que abarca un área relativamente pequeña. La mayoría de las LAN están limitadas a un edificio o conjunto de edificios.
- Link Layer Discovery Protocol (LLDP): es un protocolo de la capa de enlace, de proveedor neutral, perteneciente a la suite de protocolos de Internet, utilizado por los dispositivos de red para informar de su identidad, capacidades y los vecinos en una red de área local IEEE 802, principalmente cableada.
- Media Access Control (MAC): es la dirección física (de nivel 2) de un equipo de red, que lo identifica de forma unívoca.

- Management Information Base (MIB): es una estructura de datos usada por SNMP que define que es posible obtener de un sistema y que puede ser controlado.
- Network Time Protocol (NTP): es un protocolo empleado para sincronizar el reloj de un equipo con un servidor. Usa UDP como protocolo de transporte y el puerto 123 como puerto por defecto.
- Private VLAN: Ofrece aislar a nivel 2, equipos de la misma subred.
- Remote Authentication Dial-in User Service (RADIUS): es un sistema distribuido de tipo cliente/servidor, que asegura redes contra accesos no autorizados. Los clientes de RADIUS se ejecutan en los equipos de red (por ejemplo, enrutadores o conmutadores), los cuales envían peticiones de autenticación a un servidor central de RADIUS, que contiene la información de autenticación y acceso a servicios de todos los usuarios de la red.
- Simple Network Management Protocol (SNMP): es un protocolo de monitorización y gestión de redes. Los datos son enviados desde agentes SNMP, que son procesos hardware y/o software informando de la actividad en cada equipo de red (por ejemplo, enrutadores o conmutadores), hasta una estación de trabajo encargada de monitorizar y /o gestionar la red. Los agentes envían la información contenida en una MIB. Utiliza UDP como protocolo de transporte y el puerto 161 (SNMP polls) y el puerto 162(SNMP traps) por defecto.
- Secure Shell (SSH): es un protocolo e interfaz de comandos basado en Unix, empleado para obtener acceso en un equipo remoto de forma segura. Usa TCP como protocolo de transporte y el puerto 22 por defecto. Emplea criptografía basada en claves públicas tanto para la conexión como para la autenticación, y usa algoritmos de cifrado para proteger las conexiones a equipos remotos.
- Spanning Tree Protocol (STP): es un protocolo de nivel 2 utilizado para evitar bucles indeseados, a la vez que permite la existencia de caminos redundados entre dos puntos de la red favoreciendo la consistencia de la red ante caídas de enlaces.
- Transmisión Control Protocol (TCP): es uno de los principales protocolos usados en redes de ordenadores a nivel 4 de la tabla OSI. TCP es un protocolo orientado a conexión, y permite a dos hosts establecer una conexión e intercambiar flujos de datos. A diferencia de UDP, TCP garantiza la entrega de la información.
- Trivial File Transfer Protocol (TFTP): es una manera sencilla de envío de ficheros. Utiliza UDP como protocolo de transporte y por defecto utiliza el puerto 69. No ofrece ninguna opción de seguridad.
- Type-length-value (TLV): la información LLDP es enviada por los dispositivos por cada uno de sus interfaces en intervalos fijo, en forma de tramas de Ethernet. Cada trama contiene una unidad de datos de LLDP (LLDPDU) y cada LLDPDU es una secuencia de estructuras de tipo-longitud-valor (TLV).
- User Datagram Protocol (UDP): es uno de los principales protocolos usados en redes de ordenadores a nivel 4 de la tabla OSI. UDP es un protocolo no orientado a conexión, que ofrece muy pocos servicios de recuperación ante errores.
- Virtual Local Area Network (VLAN): es un grupo de sistemas pertenecientes a una o más LAN, que están configurados para comunicarse entre ellos como si estuviesen conectados al mismo medio (por ejemplo, Ethernet).

ANEXO B: EJEMPLOS DE CONFIGURACIÓN

Con tal de poder plasmar los conceptos que se han visto en el documento a continuación mostraremos un conjunto de ejemplos de configuración según un escenario hipotético. Este escenario es una red simplificada que pretender aglutinar las principales funcionalidades más complejas como la configuración de STP, 802.1x, ACL o STP.

Partimos de un escenario de dos niveles, acceso y *core*, donde los usuarios son conectados a conmutador de acceso y los conmutadores de acceso son agregados en un nodo de *core* que también dispone de las conexiones de los servidores y distintos servicios. Para este ejemplo en el Core también se encuentra un servidor RADIUS. La red usuarios esta segmentada mediante 2 VLAN para diferencia el tráfico y permisos de dos grupos de usuarios y existe otra VLAN de servicios. Las VLAN creadas son la 10, 20 para usuarios y la 30 para servicios (RADIUS). Los enlaces UPLINK de los conmutadores de acceso gestionarán tráfico de la VLAN 10 y 20 con lo que deben ser capaces enviar tramas 802.1Q con la identificación de VLAN.



Por otro lado, el conmutador de *core* realizará también funciones de *inter-VLAN routing*, esta función nos permitirá mostrar la configuración de ACL en la que se denegará el tráfico entre VLAN pero se permitirá el resto de tráfico hacia otros destinos.

Los PC de usuarios todos dispondrán de suplicante 802.1x de forma que todos los puertos de usuario dispondrán de autenticación 802.1x y el usuario será validado con el servidor RADIUS.

Finalmente, STP nos permitirá poder tener un entorno redundante y seguro contra bucles, para esto se configurará RSTP de forma que el *core* sea el *root* de la topología y se proteja su posición a la vez que los puertos de usuarios estarán protegidos para evitar que no se conecte un conmutador con 802.1w activado.

1. CONFIGURACIÓN DE VLAN

Para poder configurar las VLAN del escenario es necesario en primer lugar crear las VLAN y posteriormente configurar los puertos como es debido tanto como puerto de usuario como los puertos de UPLINK.

1- Configurar las VLAN (se debe realizar los mismos comandos en los 3 conmutadores), por simplificar se muestra solo la configuración del Core.

```
(SW Core) #vlan database
(SW Core) (Vlan-Config)#vlan 10,20,30,99
(SW Core) (Vlan-Config)#vlan name 10 usuario-A
(SW Core) (Vlan-Config)#vlan name 20 usuario-B
(SW Core) (Vlan-Config)#vlan name 30 RADIUS
(SW Core) (Vlan-Config)#vlan name 99 nativa
(SW Core) (Vlan-Config)#exit
```

2- Configurar los puertos de usuario A y B en los conmutadores de acceso:

```
(SW 1) #configure
(SW 1) (Config)#interface 1/0/1
(SW 1) (Interface 1/0/1)#vlan pvid 10
(SW 1) (Interface 1/0/1)#vlan participation exclude 1
(SW 1) (Interface 1/0/1)#vlan participation include 10
(SW 1) (Interface 1/0/1)#vlan ingressfilter
(SW 1) (Interface 1/0/1)#vlan acceptframe admituntaggedonly
(SW 2) #configure
(SW 2) (Config)#interface 1/0/1
(SW 2) (Interface 1/0/1)#vlan pvid 20
(SW 2) (Interface 1/0/1)#vlan participation exclude 1
(SW 2) (Interface 1/0/1)#vlan participation include 20
(SW 2) (Interface 1/0/1)#vlan ingressfilter
(SW 2) (Interface 1/0/1)#vlan acceptframe admituntaggedonly
```

3- Configurar los puertos UPLINK de los conmutadores de acceso y *core*. Para estos enlaces de UPLINK la VLAN nativa será la VLAN 99:

```
(SW 1) #configure
(SW 1) (Config)#interface 1/0/24
(SW 1) (Interface 1/0/24)#vlan pvid 99
(SW 1) (Interface 1/0/24)#vlan participation exclude 1
(SW 1) (Interface 1/0/24)#vlan participation include 10,20,30,99
(SW 1) (Interface 1/0/24)#vlan ingressfilter
(SW 2) #configure
(SW 2) (Config)#interface 1/0/24
(SW 2) (Interface 1/0/24)#vlan pvid 99
(SW 2) (Interface 1/0/24)#vlan participation exclude 1
(SW 2) (Interface 1/0/24)#vlan participation include 10,20,30,99
(SW 2) (Interface 1/0/24)#vlan ingressfilter
(SW Core) #configure
(SW Core) (Config)#interface 1/0/43-1/0/44
(SW Core) (Interface 1/0/43-1/0/44)#vlan pvid 99
(SW Core) (Interface 1/0/43-1/0/44)#vlan participation exclude 1
(SW Core) (Interface 1/0/43-1/0/44)#vlan participation include
10,20,30,99
(SW Core) (Interface 1/0/43-1/0/44)#vlan ingressfilter
```

4- Configurar la VLAN del servidor RADIUS:

```
(SW CORE) #configure
(SW CORE) (Config)#interface 1/0/24
(SW CORE) (Interface 1/0/24)#vlan pvid 30
(SW CORE) (Interface 1/0/24)#vlan participation exclude 1
(SW CORE) (Interface 1/0/24)#vlan participation include 30
(SW CORE) (Interface 1/0/24)#vlan ingressfilter
(SW CORE) (Interface 1/0/24)#vlan acceptframe admituntaggedonly
```

5- Configurar *inter-VLAN routing* en Core:

```
(SW Core) #vlan database
(SW Core) (Vlan-Config)#vlan routing 10
(SW Core) (Vlan-Config)#vlan routing 20
(SW Core) (Vlan-Config)#vlan routing 30
(SW Core) (Vlan-Config)#exit
(SW Core) #configure
(SW CORE) (Config)#interface vlan 10
(SW CORE) (Interface Vlan 10)#ip address 10.10.10.1 255.255.255.0
(SW CORE) (Interface Vlan 10)#exit
(SW CORE) (Config)#interface vlan 20
(SW CORE) (Interface Vlan 20)#ip address 10.10.20.1 255.255.255.0
(SW CORE) (Interface Vlan 20)#exit
(SW CORE) (Config)#interface vlan 30
(SW CORE) (Interface Vlan 30)#ip address 10.10.30.1 255.255.255.0
(SW CORE) (Interface Vlan 30)#exit
(SW CORE) (Config)#routig
```

2. CONFIGURACIÓN 802.1X

Para que usuario A y usuario B puedan acceder a la red deben autenticarse con su cliente suplicante instalado en el PC. Los conmutadores de acceso realizarán las funciones de autenticadores y enviarán las peticiones de autenticación al RADIUS de forma que en el servidor RADIUS deberán estar dadas de alta las IP de gestión de los conmutadores de acceso como clientes RADIUS y los usuarios en la base de datos de usuarios. Para este ejemplo vamos a suponer que los conmutadores de acceso tienen una IP en la VLAN de servidores VLAN 30. Con las IP 10.10.30.1 para el conmutador 1 y 10.10.30.2 para el conmutador 2. El RADIUS con la IP 10.10.30.10.

1- Dar de alta el servidor RADIUS con la clave *secret* netgear1234:

```
(SW 1) (Config)#radius server host auth 10.10.30.10 name RADIUS1
(SW 1) (Config)#radius server key auth 10.10.30.10
Enter secret (16 characters max):netgear1234
Re-enter secret:netgear1234
(SW 1) (Config)#radius server msgauth 10.10.30.10
(SW 1) (Config)#radius server primary 10.10.30.10
(SW 2) (Config)#radius server host auth 10.10.30.10 name RADIUS1
(SW 2) (Config)#radius server key auth 10.10.30.10
Enter secret (16 characters max):netgear1234
Re-enter secret:netgear1234
(SW 2) (Config)#radius server msgauth 10.10.30.10
```

```
(SW 2) (Config)#radius server primary 10.10.30.10
```

2- Forzamos los puertos UPLINK a modo autorizado para no perder el acceso con el *core*:

```
(SW 1) #configure
(SW 1) (Config)#interface 1/0/24
(SW 1) (Interface 1/0/24)#dot1x port-control force-authorized
(SW 2) #configure
(SW 2) (Config)#interface 1/0/24
(SW 2) (Interface 1/0/24)#dot1x port-control force-authorized
```

3- Activar la autenticación 802.1x en el conmutador:

```
(SW 1) (Config)#dot1x system-auth-control
(SW 1) (Config)#aaa authentication dot1x default radius
(SW 2) (Config)#dot1x system-auth-control
(SW 2) (Config)#aaa authentication dot1x default radius
```

3. Configuración de ACL

La configuración de ACL nos permite el filtrado de tráfico basado en los capos de cabeceras de nivel 3 y nivel 4. Para poder representar la configuración de este ejemplo vamos a configurar ACL en el conmutador principal para proteger el acceso entre las VLAN de usuario. Para esto aplicaremos ACL de entrada en la interfaz de nivel 3 VLAN 10 y VLAN 20. El resto de tráfico será permitido para permitir la navegación y acceso a recursos compartidos excepto al servidor RADIUS. A la hora de configurar las ACL debemos tener en cuenta las siguientes claves:

- Las reglas de ACL se aplican en orden, si no se aplica ninguna regla se aplica la regla por defecto que es la denegación.
- Las reglas pueden ser estándar o extendidas. Las estándar, se numeran del 1-99 y solo tiene como campos de coincidencia el campo de IP origen. Las ACL extendidas se numeran de la 100 a 199 y permiten configurar parámetros de coincidencia de los campos de cabecera de nivel 3 y 4 tanto de origen como de destino
- Las reglas se pueden aplicar a puertos físicos o puertos lógicos como VLAN. Las reglas ACL se aplican de entrada.

1. Configurar reglas para aplicar en la interfaz VLAN 10 donde se debe denegar el tráfico hacia la red 10.10.20.0/24 y hacia el host 10.10.30.10/32. Para esto creamos las ACL 101:

```
(SW CORE) (Config)#access-list 101 deny ip any 10.10.20.0 0.0.0.255
log
(SW CORE) (Config)#access-list 101 deny ip any host 10.10.30.10 log
(SW CORE) (Config)#access-list 101 permit ip any any
```

2. Configurar reglas para aplicar en la interfaz VLAN 20 donde se debe denegar el tráfico hacia la red 10.10.10.0/24 y hacia el host 10.10.30.10/32. Para esto creamos las ACL 102:

```
(SW CORE) (Config)#access-list 102 deny ip any 10.10.20.0 0.0.0.255
log
(SW CORE) (Config)#access-list 102 deny ip any host 10.10.30.10 log
(SW CORE) (Config)#access-list 102 permit ip any any
```

3. Aplicamos las ACL a las respectivas VLAN, 101 en VLAN 10 de entrada y 102 en VLAN 20 de entrada:

```
(SW CORE) (Interface Vlan 10)#ip access-group 101 in
(SW CORE) (Interface Vlan 10)#ip access-group 102 in
```

4. CONFIGURACIÓN DE STP SEGURO

Para asegurar la disponibilidad de la red y evitar el recalculo de topologías por un cambio del *root* de STP y evitar que se conecte cualquier conmutador que envíe tráfico BPDU a ningún conmutador de usuario, vamos a realizar dos acciones:

- Configurar la prioridad en el conmutador Core para que esta sea el *root* de la red.
- Configurar la funcionalidad de *edge-port* con *bpduguard*.

Con esta configuración creamos una topología consistente y evitamos posibles recálculos de la topología, así como envío de cambios de topología cada vez que se encienda y apague un PC:

1- Prioridad en el conmutador Core. La prioridad en STP viene dada por los últimos 4 bits del campo de 16 bits que en caso de PVSTP o RPVSTP contiene el VLAN ID. Por este motivo el campo de prioridad irá en saltos de 4096. Para asegurar que el conmutador de Core sea el root le configuraremos la prioridad de 0:

```
(SW CORE) (Config)#spanning-tree mode rstp
(SW CORE) (Config)#spanning-tree mst priority 0 0
```

2- Teniendo en cuenta que los puertos de 1 a 23 forman parte de puertos de usuarios vamos a configurar *auto-edge* y *bpdu guard* para que el puerto converja de forma rápida, pero a la vez se eviten bucles o la conexión de conmutador en dichos puertos:

```
(SW 1) #configure
(SW 1) (Config)#interface 1/0/1-1/0/23
(SW 1) (Interface 1/0/24-1/0/23)#spanning-tree auto-edge
(SW 1) (Interface 1/0/24-1/0/23)#exit
(SW 1) (Config)#spanning-tree bpduguard
(SW 2) #configure
(SW 2) (Config)#interface 1/0/1-1/0/23
(SW 2) (Interface 1/0/24-1/0/23)#spanning-tree auto-edge
(SW 2) (Interface 1/0/24-1/0/23)#exit
(SW 2) (Config)#spanning-tree bpduguard
```

ANEXO C: CONFIGURACIONES POR DEFECTO

En este anexo se resumen los parámetros por defecto de un conmutador tal como viene de fábrica. Esta información nos servirá de referencia para la configuración y securización del dispositivo.

Feature	Default
IP address	169.254.100.100
Subnet mask	255.255.0.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management Mode	None
SNTP client	Enabled
SNTP server	Not configured
Global logging	Enabled
CLI command logging	Disabled
Console logging	Enabled (Severity level: debug and above)
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP	Enabled (SNMPv1/SNMPv2, SNMPv3)
SNMP Traps	Enabled
Auto Install	Enabled
Auto Save	Disabled

Feature	Default
sFlow	Enabled
ISDP	Enabled (Versions 1 and 2)
RMON	Enabled
TACACS	Not configured
RADIUS	Not configured
SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Captive Portal	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	None configured
IP source guard (IPSG)	Disabled
DHCP snooping	Disabled
Dynamic ARP inspection	Disabled
Protected ports	None
Private groups	None
Flow control support (IEEE 802.3x)	Disabled
Head of line blocking prevention	Disabled
Maximum frame size	1518 bytes
Auto-MDI/MDIX support	Enabled
Auto-negotiation	Enabled
Advertised port speed	Maximum Capacity
Broadcast storm control	Enabled
Port mirroring	Disabled
LLDP	Enabled
LLDP-MED	Enabled
MAC table address aging	300 seconds (dynamic addresses)

Feature	Default
DHCP Layer 2 relay	Disabled
Default VLAN ID	1
Default VLAN name	Default
GVRP	Disabled
GARP timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP operation mode	IEEE 802.1s RSTP
Optional STP features	Disabled
STP bridge priority	32768
Multiple Spanning Tree	Disabled
Link aggregation	No Link Aggregation Groups (LAGs) configured
LACP system priority	1
Routing mode	Disabled
IP helper and UDP relay	Disabled
Tunnel and loopback interfaces	None
DiffServ	Enabled
Auto VoIP	Disabled
Auto VoIP traffic class	6
MLD snooping	Disabled
IGMP snooping	Disabled
IGMP snooping querier	Disabled
GMRP	Disabled

ANEXO D: REFERENCIAS

Para la descarga de los manuales completos de referencia, guía CLI y ejemplos se puede acceder desde el área de descargas de la página web de Netgear https://support.netgear.com indicando en el buscador el modelo sobre el que se quiere realizar la descarga. Una vez en el sitio web del modelo elegido, seleccionando *Documentation,* se permite la descarga de documentación para cada versión. Como ejemplo del modelo M6100 versión de firmware 11 tenemos los siguientes manuales

- Guía de comando CLI:
http://www.downloads.netgear.com/files/GDC/M5300/M5300-M6100-M7100_CLI_v11_20Apr2015.pdf
- Guía de referencia de configuración:
http://www.downloads.netgear.com/files/GDC/M5300/M5300-M6100-M7100_SWA_v11_30Oct2015.pdf
- Guía de configuración vía web:
http://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf