centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1422

Procedimiento de Empleo Seguro
Allied Ware Plus (AW+) versión 5.5.0-0.6

Noviembre de 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.27 13:09:00 +01'00'

P.º de la Castellana 109, 28046 Madrid

NIPO: 083-21-209-3

Fecha de Edición: noviembre de 2021

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura en los *switches* de Allied Telesis International con sistema operativo ***Allied Ware Plus (AW+) versión 5.5.0-0.6***.
2. A lo largo de los diferentes capítulos se ofrecen consejos y recomendaciones sobre la activación o desactivación de servicios y determinadas funcionalidades de estas familias de *switches* con el fin de poder establecer una configuración lo más segura posible.
3. 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 una manera más rápida y cómoda. Así mismo, aunque para la elaboración de esta guía se ha tomado como referencia la familia de *switches* AT-x930, las recomendaciones descritas sobre seguridad son aplicables a cualquier otro equipo de red que utilice AW+. En el momento de la elaboración de esta guía, existen las siguientes familias de equipamiento con sistema operativo AW+:
    - *x930*
    - *x950*
    - *x510*
    - *x550*
    - *x530-530L*
    - *x230*
    - *x200*
    - *SBX81CFC960*
    - *SBX908*
    - *SBX908 GEN2*

2. OBJETO Y ALCANCE

4. El objeto de esta guía es analizar los mecanismos de seguridad disponibles para proteger los entornos de sistemas de información y comunicaciones que emplean *switches* Allied Telesis. Como consecuencia, se establece un marco de referencia que contemple las recomendaciones STIC en la implantación y utilización de *switches* Allied Telesis con sistema operativo AW+, versión 5.5.0-0.6.
5. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los *switches Allied Telesis* bajo su responsabilidad.
6. Es recomendable aplicar los consejos 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 para incrementar la seguridad del equipo, en primer lugar, con el fin de evitar accesos no deseados a su configuración y a los datos almacenados en él, y posteriormente se analizan 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 o desactivadas.

3. ORGANIZACIÓN DEL DOCUMENTO

7. El documento se organiza de la siguiente forma:

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

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

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

   d) **Apartado 7.** En este apartado se incluye una *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

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

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

4. FASE DE DESPLEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Para asegurar una correcta entrega del producto será necesario revisar que no ha sido manipulado durante su transporte. Para ello, se deberán llevar a cabo los siguientes pasos:

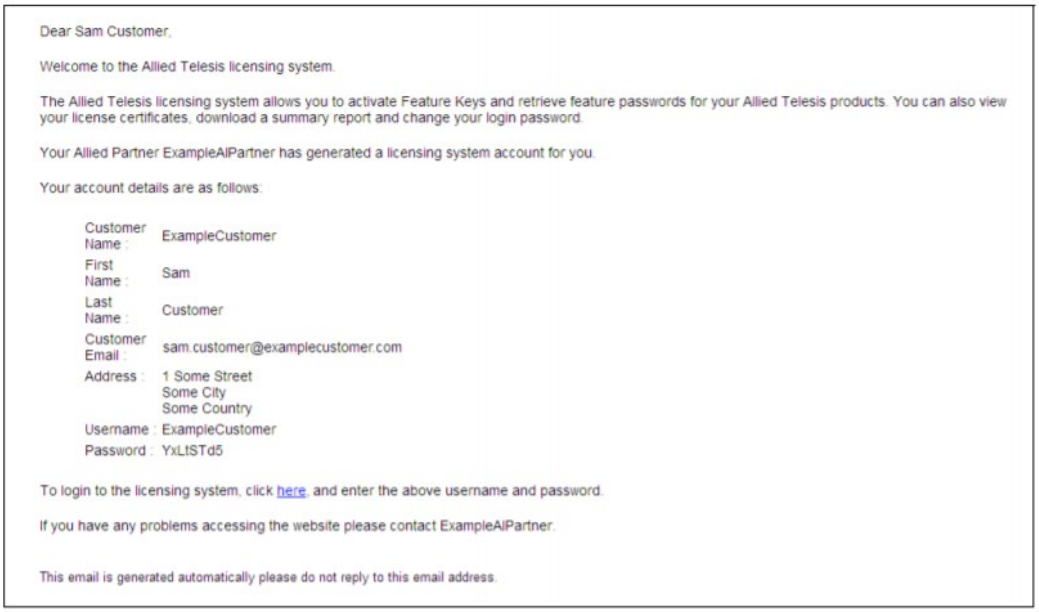
    - Comprobar que el paquete no ha sido abierto y vuelto a sellar. Esto se puede verificar examinando los sellos del empaquetado. En caso de que parezca que el paquete ha sido sellado más de una vez, contactar con el proveedor del producto.
    - Comprobar que la información de la caja, en concreto, el número de pedido, coincide con la información de compra.
    - Verificar que el producto en el interior del paquete no ha sido dañado.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Se debe desplegar el producto en un entorno físico protegido, donde solo pueda acceder el personal expresamente autorizado por la organización y que disponga de las medidas de seguridad adecuadas.

4.3 REGISTRO Y LICENCIAS

10. Se deberá utilizar la cuenta de usuario de *Allied Telesis Licensing System*, creada por el proveedor y facilitada a la organización mediante correo electrónico. Una vez adquirida la clave de licencia, se recibirá otro correo electrónico indicando que la clave se encuentra disponible.



Dear Sam Customer,

Welcome to the Allied Telesis licensing system.

The Allied Telesis licensing system allows you to activate Feature Keys and retrieve feature passwords for your Allied Telesis products. You can also view your license certificates, download a summary report and change your login password.

Your Allied Partner ExampleAlPartner has generated a licensing system account for you.

Your account details are as follows:

Customer Name :	ExampleCustomer
First Name :	Sam
Last Name :	Customer
Customer Email :	sam.customer@examplecustomer.com
Address :	1 Some Street Some City Some Country
Username :	ExampleCustomer
Password :	YxLtSTd5

To login to the licensing system, click here, and enter the above username and password.

If you have any problems accessing the website please contact ExampleAlPartner.

This email is generated automatically please do not reply to this email address.

Ilustración 1. Obtención de licencias

11. En dicho correo se incluirá la información de la clave y un enlace para su activación. Se debe acceder al enlace, registrarse con las credenciales anteriormente mencionadas e introducir, en el apartado *Activate Feature Key,* el número de licencia y pulsar *Activate*.

12. A continuación, hacer clic en la casilla para indicar que se aceptan las *condiciones de uso* y pulsar en *Activate Feature Key*. Se mostrará la siguiente información:

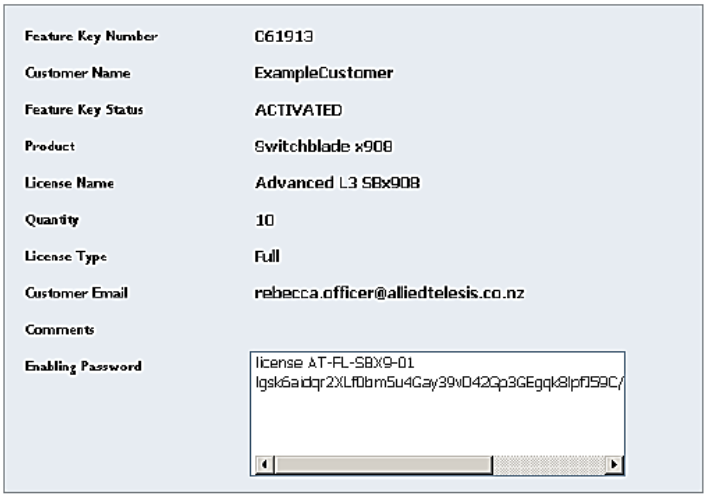


Ilustración 2. Activación de licencias

13. En el apartado *Enabling Password*, se muestra un comando que debe copiarse e introducirse en el producto para finalizar la activación de la licencia.

14. Finalmente, mediante el comando *show license*, se pueden consultar las licencias activadas en el producto, así como su fecha de expiración o de emisión.

15. El detalle sobre la gestión de licencias se puede consultar en la guía *Licensing – Feature overview and Configuration Guide – REF3.*

4.4 CONSIDERACIONES PREVIAS

16. Los *switches* de Allied Telesis con sistema operativo AW+ no tienen asignada ninguna dirección IP por defecto, por tanto, según se extrae de la caja la única manera de conectar al CLI (*Command Line Interface*) del *switch* será por medio del puerto de consola. Para esto, será necesario un programa de emulación tipo VT100, *Hyperterminal*, CRT, Putty, etc… y configurar los siguientes parámetros:

Parámetro	Valor
Velocidad	9600
Bits de datos	8
Bits de stop	1
Paridad	NO
Control de flujo	NO

Tabla 1: Parámetros puerto de consola

4.5 ESTRUCTURA DE LA LÍNEA DE COMANDOS

17. A continuación, se muestra una tabla en la que se resumen las distintas modalidades de la línea de comandos para familiarizarse con el CLI, mediante el cual se configurará el *switch*:

Modo	Método de acceso	*Prompt*	Comando para salir Comando para ir al siguiente modo
User EXEC	Este es el primer nivel de configuración. Permite cambiar propiedades del terminal y mostrar información del sistema	*awplus>*	**logout** **enable**
Privileged EXEC	Desde el modo User EXEC introducir el comando: ***enable***	*awplus#*	**disable** **configure terminal**
Configuración global	Desde el modo Privileged EXEC introducir el comando: ***conf t***	*awplus(conf)#*	***exit*** Para entrar en *conf* de interfaz: ***interface <int_name>***
Configuración de interfaz	Desde el modo de configuración global introducir el comando: ***interfaz <int_name>***	*awplus(conf-if)#*	Para salir a modo de conf: ***exit*** Para salir a modo *Privileged*: ***end (Ctrl+Z)***
Configuración de vlans	Desde el modo de configuración global introducir el comando: ***vlan database***	*awplus(config-vlan)#*	Para salir a modo de *conf*: ***exit*** Para salir a modo *Privileged*: ***end (Ctrl+Z)***

Tabla 2: Estructura línea de comandos

5. FASE DE CONFIGURACIÓN

5.1 CONFIGURACIÓN DE ARRANQUE

18. Los cambios que se realicen en la configuración del equipo se almacenarán automáticamente en una configuración denominada '*running-config*', que es la empleada por el *switch* para determinar cómo actuar con cada paquete (vlans, STP, etc). Sin embargo, esta configuración se pierde al reiniciar el equipo, de modo que para que los cambios realizados se mantengan tras un reinicio, es necesario salvar una copia de esta configuración ('*running-config*') en la '*startup-config*'. Esta última, es la configuración que, de manera predeterminada, el *switch* vuelca en la '*running-config*' durante el arranque. Esta copia se lleva a cabo mediante el uso la siguiente instrucción:

    awplus# copy running-config startup-config

5.2 USUARIO Y CONTRASEÑA POR DEFECTO

19. Por defecto todos los equipos con AW+ vienen con un usuario por defecto de tipo '*manager*' que tiene máximos privilegios (nivel 15, ver apartado 5.8 PERMISOS Y CREACIÓN DE USUARIOS). Al hacer *login* con este usuario es posible llevar a cabo cualquier operación en la gestión de ese equipo: cambio de versión de *software*, configuración de cualquier protocolo, apagado de puertos, etc. El usuario por defecto en equipos con AW+ es '*Manager*' y contraseña '*friend*'.

20. Es por esto que el primer paso para configurar el dispositivo de forma segura será el cambio de la contraseña del usuario por defecto, *manager*, ya que esta es fácil de encontrar en numerosos sitios *web*. Para ello, se debe introducir el comando:

    awplus(config)#username manager password <nuevopassword>

21. Esta nueva contraseña forma parte de la configuración activa del equipo, esto quiere decir que si se quieren mantener los cambios ante un reinicio (deseado o no) del *switch* a gestionar, se debe utilizar el comando visto anteriormente para salvar la configuración, *copy running-config startup-config*.

22. Esta contraseña deberá cumplir con lo indicado en el apartado 5.3 POLÍTICA DE CONTRASEÑAS.

5.3 POLÍTICA DE CONTRASEÑAS

23. Se recomienda hacer uso de distintas contraseñas, no sólo entre los distintos tipos de accesos a los equipos, sino entre los propios equipos, ya que comprometer uno puede provocar que todos los demás sean vulnerables.

24. Igualmente, es recomendable que las contraseñas sean 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 (,./<>;':"[]\{}|~!@#$%^&*()_+`-=).

25. El producto, mediante el comando *security-password*, permite configurar los siguientes parámetros:

    - *security-password history*. Especifica el número de contraseñas anteriores que no se permite utilizar. Se puede configurar un valor entre cero (0) y quince (15) contraseñas. **Se recomienda un valor de, al menos, cinco (5).**
    - *security-password forced-change*. Obliga a los usuarios a cambiar la contraseña tras iniciar sesión una vez esta caduque. **Este parámetro debe ser activado.**
    - *security-password lifetime*. Especifica el tiempo de validez en días de las contraseñas tras el cual expiran. Se puede configurar entre cero (0) y mil (1000) días. **Se recomienda un valor de dos meses (60 días aproximadamente).**
    - *security-password min-lifetime-enforce*. Especifica el número de días que debe pasar tras el cambio de una contraseña antes de poder modificarla de nuevo. Se puede configurar entre cero (0) y mil (1000) días. **Se recomienda un valor de una semana (7 días).**
    - *security-password minimum-categories*. Indica el número de categorías de caracteres que debe tener la contraseña para ser válida. Se entiende, en este caso, como categorías a: letras mayúsculas, letras minúsculas, números y símbolos especiales. Se recomienda configurar un valor de cuatro (4) en este comando para así obligar el uso de todas las categorías.
    - *security-password minimum-length*. Especifica la longitud mínima permitida para las contraseñas. El rango es de uno (1) a veintitrés (23) caracteres. **Se recomienda un valor de, al menos, doce (12) caracteres.**
    - *security-password reject-expired-pwd*. Indica si se puede acceder o no al sistema con una contraseña expirada. Se recomienda permitir el acceso (utilizando el comando con *no* delante), haciendo uso del comando *security-password forced-change*, indicado anteriormente. De esta forma, tras caducar una contraseña, el usuario podrá acceder, pero deberá modificarla.
    - *security-password warning*. Indica el momento en días en el cual se enviará un aviso a los usuarios cuando las contraseñas van a expirar. Se puede configurar entre cero (0) y mil (1000) días. Se recomienda un valor de una semana (7 días).

5.4 LIMITACIÓN DEL ACCESO A LA CONFIGURACIÓN DE LOS EQUIPOS

26. Si las conexiones a la gestión del *switch*, tanto por consola como por SSH no tienen un *time-out* establecido o este es demasiado largo (más de 10 minutos), entonces serán más vulnerables ante posibles ataques. Los *switches* con sistema operativo AW+, tienen configurado un *time-out* por defecto de 10 minutos para consola y SSH.

27. Se puede utilizar el comando *exec-timeout minutos segundos* para configurar la duración máxima de las conexiones mediante Consola o VTY (SSH). **Se recomienda un valor máximo de treinta (30) minutos: *exec-timeout 30 0*.**

28. De igual manera, el comando *gui-timeout minutos segundos* permite configurar la duración máxima de las conexiones mediante GUI. Se recomienda un valor de treinta (30) minutos: *gui-timeout 30 0*.

5.5 MODO DE OPERACIÓN SEGURO

29. El producto permite activar el modo de operación seguro mediante el comando ***crypto secure-mode***. Tras su activación, se deshabilitarán las siguientes opciones:

    - *Telnet.*
    - *SSHv1.*
    - *SNMPv1* y *SNMPv2*.
    - Todos los niveles de privilegio excepto 1 y 15.
    - Todos los algoritmos no FIPS, incluyendo MD5, RSA-1 y DSA.
    - La capacidad de almacenar las contraseñas en texto claro.

30. Adicionalmente el acceso a GUI solo aceptará *cipher suites* con AES128-SHA.

31. **Se deberá hacer uso del producto en modo seguro.**

5.6 ADMINISTRACIÓN DEL PRODUCTO

5.7 ADMINISTRACIÓN LOCAL Y REMOTA

32. El producto permite los siguientes métodos de administración:

    - Administración local mediante CLI.
    - Administración remota mediante CLI, realizando la conexión con SSH.
    - Administración remota mediante GUI, con HTTP/HTTPS.

33. Se recomienda administrar el producto únicamente mediante CLI, de forma local o a través de SSH. En el apartado 5.13 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS se indican los pasos necesarios para la desactivación de la administración mediante HTTP/HTTPS, así como los pasos necesarios para realizar una configuración segura de SSH.

5.8 PERMISOS Y CREACIÓN DE USUARIOS

34. A la hora de crear usuarios (y sus contraseñas) nos puede ser útil definir distintos niveles de acceso según el usuario utilizado para hacer *login* en el interfaz CLI del *switch*. En el momento de la elaboración de esta guía, AW+ soporta tres (3) niveles de acceso, tal como se refleja en la siguiente tabla. Sin embargo, tras activar el

modo de operación seguro (ver apartado 5.5 MODO DE OPERACIÓN SEGURO) tan solo se permitirá el uso de los niveles 1 y 15.

Nivel de acceso	Comandos disponibles
1	Todos los comandos del modo *user EXEC*.
7	Todos los comandos del modo *User EXEC* y algunos del *Privileged EXEC* que permiten consultar el estado y configuración del *switch* pero no el funcionamiento del *switch*: cambio de *firmware*, *reload*, etc. *'Show running-config'* NO está permitido.
15	Todos los comandos

Tabla 3: Comandos disponibles por nivel de acceso

35. Si se hace *login* con usuario de tipo *advanced user* (nivel 7), se entrará (como siempre) en el modo de '*User EXEC*' donde se puede ejecutar todos los comandos de este modo, si se necesita ejecutar comandos del modo *Privileged EXEC*, se debe habilitar el nivel 7 de dicho modo. Se usa la siguiente instrucción:

    awplus>enable 7

    Si se intenta hacer esto con un usuario de nivel 1 o se intentara acceder al nivel 15 con alguna de las siguientes instrucciones:

    awplus>enable

    awplus>enable 15

    El *switch* presentará un *prompt* como este:

    Password:

    Para que se introduzca la contraseña que da acceso al nivel indicado (7 o 15).

36. Se pueden crear contraseñas que dan acceso a niveles superiores para poder dar acceso temporal y monitorizado a usuarios de niveles inferiores que por circunstancias necesiten ejecutar determinados comandos. Así luego no será necesario cambiar la contraseña del usuario de tipo manager si no simplemente eliminar o cambiar la contraseña que se ha proporcionado para alcanzar un determinado nivel de privilegios. La instrucción para crear estas contraseñas de acceso a niveles superiores es:

    awplus(config)#enable password <level> <contraseña>

    Donde *<level>* será 15 o 7 dependiendo si se quiere dar acceso a todos los comandos del modo *Privileged EXEC* o solo a aquellos permitidos en el nivel 7.

37. Por defecto, tras configurar el Modo Seguro (5.5 MODO DE OPERACIÓN SEGURO), tanto las contraseñas de los usuarios que se han creado para hacer *login* en el equipo, como aquellas que sirven para acceder a niveles superiores de la estructura de CLI del *switch*, no se muestran en texto plano mediante el comando show *running-config*, sino que se mostrará su hash SHA-256.

38. Para la creación o modificación de usuarios, se debe utilizar el comando:

    awplus(config)# username <nombre> privilege <1-15> [password [8] <contraseña>

    Donde <nombre> es el nombre de usuario deseado. El nivel de privilegios del que dispondrá el usuario en *privilege*. En el parámetro *password*, además de la contraseña del usuario, se puede añadir el valor *8*, indicando que, en lugar de introducir la contraseña en texto plano, se introducirá cifrada (el usuario a la hora de acceder seguirá introduciendo su contraseña en texto plano). **Se debe configurar el valor 8 para evitar el almacenamiento de texto plano de las contraseñas.**

5.9 RECUPERACIÓN TRAS PÉRDIDA DE LA CONTRASEÑA DE ACCESO

39. En caso de olvidar la contraseña de los usuarios que permiten acceso completo a la gestión del equipo, existe un procedimiento denominado '*password recovery*' que permite hacer *login* en el equipo con el usuario y contraseña por defecto (*manager* y *friend*), incluso sin perder la configuración existente.

40. Para poder realizar este procedimiento es necesario estar conectado al puerto de consola del equipo, una vez establecida la conexión (aunque no se sepa el usuario para hacer *login*) se procede a interrumpir temporalmente la alimentación del equipo para forzar el reinicio de este. Habrá que estar muy atento para, en cuanto se vea el mensaje en la pantalla, pulsar: *<CTRL+B>*.

    Initialising ECC Memory... Done

    Bootloader 1.1.6 loaded

    Press <Ctrl+B> for the Boot Menu

41. Si se ha pulsado *<Ctrl+B>* antes de que desaparezca el mensaje de la pantalla, se accederá al menú de arranque del equipo, que será similar a este (según versiones):

```
Boot Menu:

 ---------------------------------------------------
 B. Boot backup software
 ---------------------------------------------------
 0. Restart
 1. Perform one-off boot from alternate source
 2. Change the default boot source (for advanced users)
 3. Update Bootloader
 4. Adjust the console baud rate
 5. Special boot options
 6. System information
 7. Restore Bootloader factory settings
 ---------------------------------------------------
 9. Quit and continue booting

Enter selection ==>
```

42. Se debe seleccionar la opción 5 '*Special boot options*' y se llegará al siguiente menú:

```
Special boot options menu:

 0. Return to previous menu
 ---------------------------------------------------
 1. Skip startup script (Use system defaults)

Enter selection ==>
```

43. En el menú, se selecciona la opción 1 para saltar la secuencia de arranque y por tanto, utilizar los valores por defecto, el mensaje en pantalla será el que se ve en la **¡Error! No se encuentra el origen de la referencia.**.

```
Option successfully set. Press 0 then 9 to boot with the default configuration
Or boot the system from an alternate source.

Special boot options menu:

 0. Return to previous menu
 ---------------------------------------------------
 1. Skip startup script (Use system defaults)

Enter selection ==> 0
```

44. Tal y como se indica en la anterior imagen, se pulsa '0' para volver al menú anterior, donde se selecciona '9' (Salir y continuar el arranque). El *switch*

reanudará el arranque y una vez completado, pedirá el usuario y contraseña para hacer *login*.

```
(LINEAS OMITIDAS POR TAMAÑO DEL DOCUMENTO)
….

Received event network.initialized

Assigning Active Workload to HA processes:
hsl, nsm, lacpd, mstpd, rmond, sflowd, irdpd
lldpd, loopprotd, ripd, vrrpd, authd, epsrd, ospfd
imi, imiproxyd

Received event network.activated

Loading default configuration
.

done!

Received event network.configured

awplus login:
```

45. Se puede utilizar el *login / password* por defecto (*manager / friend*) para acceder a la gestión del *switch*.

5.10 CONSEJOS DE SEGURIDAD EN EL ENTORNO AL ACCESO A LA CONSOLA

46. Una vez realizado este procedimiento de interrupción del arranque del *switch*, según la versión del *boot* que tenga instalada el *switch*, cuando se haga *login* en el equipo con el usuario y contraseña por defecto, este mantendrá toda la configuración excepto la parte relativa a los usuarios (versiones de *boot* 2.X.X) o no tendrá configuración alguna (versiones de *boot* 1.X.X) pero toda la configuración puede recuperarse ya que la *startup-config* no ha sido borrada (solo omitida por completo en el arranque).
47. Según el entorno esto puede suponer una brecha de seguridad ya que por medio de este procedimiento se puede extraer toda la información contenida en el archivo de configuración del *switch* (Vlans, direccionamiento IP, SNMP, etc). Por tanto, si se quiere proteger este tipo de vulnerabilidades, será necesario dotar al armario o emplazamiento donde el equipo esté instalado de cierta seguridad física que controle el acceso no deseado.
48. Es posible también activar ciertas opciones de seguridad del *bootloader* para proteger el dispositivo en caso de accesos físicos no autorizados. Para ello,

durante el arranque del dispositivo, pulsar *<Ctrl+B>* para acceder al menú del *bootloader*.

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

49. Después seleccionar la opción *S. Security Level*. Esta opción permite determinar el acceso al *boot* por parte de los usuarios. Existen tres (3) niveles de seguridad:

    - Nivel 1. Nivel de seguridad por defecto. No aporta ninguna protección, permitiendo todo acceso al mismo.
    - Nivel 2 – *Password Protected*. El segundo nivel de seguridad permite configurar una contraseña de acceso, de tal forma que, tras pulsar *<Ctrl+b>*, se deberá introducir dicha contraseña antes de poder realizar ninguna acción.
    - Nivel 3 – *Locked Down*. El tercer nivel es similar al segundo, con la diferencia de que las acciones de saltar la configuración de arranque y las opciones especiales no se podrán utilizar, aunque se conozca la contraseña. En su lugar se ofrecerá la opción de borrar de forma completa la memoria *flash* del equipo, perdiendo así toda la información y configuraciones contenidas en él.

50. Se recomienda configurar, al menos, el segundo nivel de seguridad, de tal forma que para poder acceder a las opciones del *bootloader* sea necesario conocer la contraseña.

51. El detalle de configuración del *bootloader* se puede consultar en la guía *Bootloader and Startup Feature Overview and Configuration Guide – REF2*.

5.11 CONFIGURACIÓN DE *BANNER* INFORMATIVO

52. También es recomendable crear un mensaje informativo para definir el marco legal dentro del cual se realiza la sesión con el *switch*. Este *banner* aparecerá en pantalla, justo antes de introducir el usuario y contraseña, al realizar conexiones al

CLI de los equipos. Los comandos a introducir para configurar un banner informativo, comprobar la configuración y salvarla son:

awplus# configure terminal
awplus(config)# banner motd mensaje_de_aviso
awplus(config)# exit
awplus# show running-config
awplus# copy running-config startup-config

53. Este es un ejemplo de cómo debe crearse un *banner* informativo:

awplus(config)# banner motd AVISO:El uso de este dispositivo está restringido a los usuarios expresamente autorizados. Todos los usuarios estarán monitorizados constantemente y podrán ser perseguidos en el caso de un uso fraudulento de este dispositivo.
awplus(config)#

5.12 CONFIGURACIÓN PARA GESTIÓN REMOTA

54. Para poder hacer uso de cualquiera de los interfaces de gestión remota (SSH, Web, SNMP, etc...) es necesario asignar una dirección IP al *switch* ya que los *switches* con sistema operativo AW+ no traen ninguna dirección IP configurada. Por defecto, todos los puertos del *switch* pertenecen a la vlan1 de manera que dando dirección IP a esta *vlan* cualquiera de los puertos del *switch* responderán a las peticiones TCP/IP con destino dicha dirección. Se usan los siguientes comandos:

awplus(config)# interface vlan1

awplus(config-if)#ip address X.X.X.X/MM

Donde X.X.X.X es la dirección IP (por ejemplo 192.168.1.1) y MM la máscara en notación decimal indicando el número de bits que son igual a 1. (Por ejemplo /24 = 255.255.255.0)

55. Esta misma configuración se puede aplicarla para dar direccionamiento IP a cualquiera de las *vlans* que se creen según se ve recoge en el apartado 5.31 VLANS de este documento. Únicamente se debe sustituir el '*vlan1*' por '*vlanX*' donde *X* es el identificador numeral de la *vlan* a la cual se quiere asignar direccionamiento IP.

56. Como medida básica de seguridad, si es posible prescindir de la gestión remota de los equipos, se puede evitar configurar una dirección IP para así impedir accesos no deseados a la interfaz de gestión del equipo, limitándose así la administración a la conexión física al puerto de consola de cada uno de los equipos.

5.13 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

57. Una medida de seguridad básica es limitar los servicios activos para acceder a los menús de configuración solo a través de aquellos métodos que garanticen unos niveles de seguridad aceptables. Esto limitará la posibilidad de que agentes externos se hagan con el control del equipo, o accedan a la información.

58. A continuación, se enumeran una serie de servicios ofrecidos por el equipo y si su uso es considerado recomendable desde el punto de vista de la seguridad, o es mejor usar otros medios.

59. Algunos de estos servicios se desactivarán de forma automática durante la activación del modo seguro, ver apartado 5.5 MODO DE OPERACIÓN SEGURO. Sin embargo, pueden utilizarse los pasos listados a continuación para verificar el correcto uso de los distintos servicios.

5.14 TELNET

60. Dado que TELNET es un protocolo no seguro, debe deshabilitarse. Para ello, se debe utilizar el comando:

    awplus(config)#no service telnet

5.15 SSH

61. Como norma general, el único medio de gestión debería ser a través de la consola local, ya que esto asegura controlar de manera física los accesos al *switch*. En caso de necesitar un terminal de gestión remoto, es recomendable configurar SSH, ya que, a diferencia de Telnet, SSH sí garantiza unas medidas de seguridad básicas. **Se recomienda la utilización de SSHv2 para realizar accesos a la configuración del *switch* de forma remota.**

62. Configurar el servicio de SSH requiere realizar una serie de pasos. El primero es configurar una clave de autenticación con el comando:

    awplus(config)# crypto key generate hostkey rsa [<768-32768>]

    el valor entre 768 y 32768 en la longitud en bits de la clave a generar. Para más seguridad se recomienda utilizar una clave de la mayor longitud posible. Si no se especifica un valor la clave generada tendrá una longitud de 1024 bits, por lo tanto, **se deberá especificarse un valor igual o superior a 3072 bits.**

63. También es posible hacer uso de curvas elípticas para la autenticación SSH, para ello utilizar el comando:

    awplus(config)# crypto key generate hostkey ecdsa [<256|384>]

64. A continuación, se debe habilitar el servicio de SSH, con el comando:

    awplus(config)# service ssh
    WARNING: SSHv1 host key does not exist. SSH will not be available for version 1.

    Como se observa en el mensaje, SSHv1 no estará disponible. Como se ha indicado antes, esta es la configuración recomendada, ya que SSHv2 aporta mayor seguridad.

65. Por último, se debe indicar a cuáles de los usuarios previamente definidos les estará permitido el acceso por medio de una conexión SSH:

    awplus(config)# ssh server allow-users <username>

66. Por ejemplo, para permitir la conexión por medio de SSH al usuario por defecto '*manager*', se introduce:

    awplus(config)# ssh server allow-users manager

67. Con los siguientes comandos, se puede configurar el servidor de SSH para aceptar únicamente conexiones SSHv2, rechazar la conexión si no se produce autenticación en menos de 30 segundos (por defecto son 60) y limitar el máximo el número de conexiones SSH aún sin autenticar a 5 (por defecto son 10).

    awplus(config)# ssh server v2only

    awplus(config)# ssh server login-timeout 30

    awplus(config)# ssh server max-startups 5

5.16 INTERFACE HTTP/HTTPS

68. Los interfaces de configuración basados en HTTP que incorporan los *switches* con sistemas operativos AW+ pueden suponer un problema desde el punto de vista de seguridad ya que el tráfico intercambiado durante su utilización no va cifrado y puede ser fácilmente capturado. Se puede incrementar la seguridad, en este tipo de servicios, implementando la posibilidad de que el interfaz gráfico sea ofrecido a través de HTTPS.

69. Se debe desactivar HTTP. Para ello, se debe introducir la siguiente instrucción:

    awplus(config)#no service http

70. Con este comando, el *switch* deja de atender tanto a peticiones HTTP como HTTPS. Si lo deseado es permitir el uso de https pero no así de http, será necesario mantener el servicio activo y limitar el acceso al puerto 80 de la IP gestión del *switch* por medio de una lista de control de acceso (ACL).

5.17 SNMP

71. SNMP es un servicio utilizado para realizar funciones de gestión y monitorización de red, basado en el uso de unas estructuras de datos conocidas como *Management Information Base* (MIB). Los equipos de Allied Telesis con AW+ implementan las siguientes versiones de SNMP:

    - SNMPv1. *Simple Network Management Protocol*, definido en la RFC 1157. Protocolo donde el intercambio de información de un dispositivo de red viaja en texto plano.
    - SNMPv2. Definida en las RFC 1902 hasta la 1907. Sustituye a la versión anterior y proporciona mejoras en cuanto a variedad de operaciones e implementa autenticación básica basada en comunidades.
    - SNMPv3. Tercera versión de este protocolo definido en las RFC 2273 hasta la 2275. Ofrece el más alto grado en cuanto a seguridad en el acceso a dispositivos mediante el uso de autenticación y cifrado de paquetes en la red.

72. Por defecto, los switches de Allied Telesis con AW+ no atenderán a las peticiones de SNMP. En caso de necesitar utilizar este protocolo **se debe usar SNMPv3 por las características anteriormente descritas.**

73. Se debe configurar el agente SNMP para enviar los *traps* a la dirección indicada con el usuario '*secure-user*':

    awplus(config)# snmp-server host 172.28.76.128 version 3 priv secure-user

74. Se crea el grupo de usuarios SNMP '*secure*':

    awplus(config)# snmp-server group secure priv

75. Se crea el usuario '*secure-user*' perteneciente al grupo '*secure*' y se indican los métodos de autenticación (opciones MD5 y SHA2, **se debe hacer solo uso de SHA2**) y cifrado (opciones DES y AES, **se debe hacer uso solo de AES**) así como sus correspondientes contraseñas:

    awplus(config)# snmp-server user secure-user secure auth sha

    <hash-password> priv aes <encrypt-password>

76. Nótese que en los comandos: *snmp-server host* y *snmp-server group* se utiliza siempre el parámetro '*priv*' en cuanto al nivel de seguridad ya que representa el máximo nivel de seguridad y por tanto es el recomendado.

77. Ahora se configuran los *traps* (notificaciones) que se quiere que el *switch* envíe al gestor SNMP. Para ello, se seleccionan de la siguiente lista los protocolos cuyos cambios se desean recibir.

    awplus(config)# snmp-server enable trap {[auth] [bgp] [dhcpsnooping] [epsr] [lldp] [loopprot] [mstp] [nsm] [ospf] [pim] [power-inline] [rmon][thrash-limit] [vcs] [vrrp]}

78. Una notificación que puede ser muy interesante consiste en que el equipo envíe un *trap* cuando un puerto pasa de *Link-up* a *Link-down* o viceversa. Esto permitirá recibir una alerta en el gestor cuando un equipo nuevo se conecte al *switch* o uno ya conectado pierda el enlace. El comando para que se envíen *traps* cuando esto suceda en el puerto 'port1.0.1' es: (se puede aplicar a uno o varios puertos, o incluso a una vlan)

    awplus(config)# interface port1.0.1

    awplus(config-if)# snmp trap link-status

79. Como medida de seguridad adicional, se puede restringir el rango de OIDs que un determinado grupo de usuarios de SNMPv3 puede ver y modificar, creando diferentes vistas. Por ejemplo, para crear una vista denominada 'local' que permite ver todos los OIDs desde el 1.3.6.1.2.1, pero excluye específicamente los del subárbol 1.3.6.1.2.1.4, se usaría el comando:

    awplus(config)# snmp-server view local 1.3.6.1.2.1 included

    awplus(config)# snmp-server view local 1.3.6.1.2.1.4 excluded

80. Estas vistas son aplicadas a los grupos de SNMPv3. Para que a todos los usuarios del grupo '*secure*' se les permita únicamente visualizar los OIDs permitidos por la vista '*local*', hay que configurar esa vista como vista de lectura para ese grupo:

    awplus(config)# snmp-server group secure priv read local

81. Si lo que se quiere es limitar a que a los usuarios del grupo '*secure*' puedan únicamente escribir los OIDs permitidos en la vista '*local*', hay que configurar esa vista como vista de escritura para ese grupo:

    awplus(config)# snmp-server group secure priv read local

82. Por las medidas de seguridad que ofrece SNMPv3 podría admitirse no hacer uso de ACL para limitar que únicamente el gestor de SNMP puede intercambiar mensajes de SNMP con el equipo. Sin embargo, el uso de ACL es imprescindible si por limitaciones de la plataforma de gestión se debe utilizar otra versión de SNMP.

5.18 LLDP

83. Con LLDP (*Link Layer Discovery Protocol*) se puede compartir información del sistema con otros dispositivos directamente conectados a los puertos del *switch*, ya sean otros *switches*, *routers* o incluso algunos servidores. Parte de esta información, como las direcciones IP de gestión, vlans configuradas, etc, puede ser utilizada de manera maliciosa, de modo que **la recomendación general es no hacer uso de este protocolo**. Si fuese necesario, se recomienda hacerlo únicamente en los enlaces entre *switchs* sobre los que se tenga control, nunca en los puertos donde se conectarán dispositivos de usuario final. Todos los equipos con sistema operativo AW+ tienen LLDP desactivado por defecto, en cualquier caso, el comando para desactivarlo es:

    awplus(config)#no lldp run

84. En un equipo con AW+, una vez se activa el servicio de LLDP (con el comando '*lldp run*'), por defecto, por todos los puertos se envía únicamente la información definida como obligatoria en el estándar de LLDP (IEEE 802.1AB), es decir, se envían únicamente las siguientes *TLVs (Type-Length-Values): 'Chassis ID', 'Port ID', 'Time To Live'* y *'End of LLDPDU*'. Al activar LLDP también se habilita el procesado de la información recibida mediante paquetes LLDP (LLDPDU) por cada uno de los puertos para poder rellenar la tabla de vecinos (equipos directamente conectados al *switch*).

85. Opcionalmente se puede ampliar la información que se envía por cualquiera de los puertos añadiendo al envío de las TLV obligatorias otras TLVs que comprenden información adicional como: descripción del sistema, descripción del puerto, nombre del sistema, capacidades del sistema, dirección IP de gestión, etc. En cualquier caso, como se ha indicado previamente, debido al uso malintencionado que podría hacerse de esta información se recomienda no utilizar LLDP, en caso de no ser estrictamente necesario.

5.19 MEDIDAS DE SEGURIDAD EN LOS PUERTOS FÍSICOS

86. No implementar medidas de seguridad en los interfaces de red o puertos supone habilitar puntos débiles por los que poder sufrir un ataque, o través de los cuales se podría obtener información de la red. Pero, como toda acción orientada a incrementar la seguridad puede convertirse también en un inconveniente.

5.19.1.1 SEGURIDAD FÍSICA. APAGADO DE PUERTOS

87. La medida más drástica que se puede llevar a cabo es apagar todos los puertos no utilizados. De este modo, nadie puede conectarse a la red utilizando cualquiera de los puertos libres. Conectarse a una 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 de momento no se vayan a utilizar, con los comandos:

    awplus(config)# interface interface-id o rango

    awplus(config-if)# shutdown

5.19.1.2 CONTROL DE TORMENTAS

88. Los *switches* de Allied Telesis con sistema operativo AW+ 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 DLF (*Destination Lookup Failure*) recibida por uno de los interfaces físicos. Estas tormentas en la red tienen lugar cuando un nivel excesivo de este tipo de tráfico inunda la red, colapsando los '*uplinks*' y 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).

89. Al activar esta funcionalidad los equipos comienzan a monitorizar todos los paquetes que pasan por un interfaz, y determinan si el paquete es *unicast*, *multicast* o DLF. Entonces el *switch* 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 tanto por ciento de paquetes de un determinado tipo es superior al límite establecido por el administrador para ese tipo de tráfico, el *switch* comienza a descartar paquetes de este tipo, de manera que el tanto por ciento del ancho de banda máximo de un determinado puerto, consumido por ese tipo de tráfico, no sea superior al marcado por el administrador de la red.

90. Por defecto, el control de tormentas está desactivado en todos los puertos, por tanto, cualquier tipo de tráfico puede llegar a ocupar incluso el 100% del ancho de banda disponible en el puerto. Para configurar el máximo nivel que un determinado tráfico puede alcanzar en un puerto se utilizan los siguientes comandos:

awplus(config)# interface interface-id

awplus(config-if)# storm-control {broadcast|multicast|dlf} level <level>

91. Por ejemplo, para configurar en el Puerto 1.0.23 que el máximo nivel de tráfico *broadcast* sea del 65%, los comandos son:

    awplus(config)# interface port1.0.23

    awplus(config-if)# storm-control broadcast level 65

92. Se pueden ver los niveles máximos configurados para un determinado puerto utilizando el comando:

    awplus# show storm-control interface-id

93. Para deshabilitar esta funcionalidad en un determinado puerto (o rango de ellos) y que por tanto los niveles máximos admitidos vuelvan a ser de hasta el 100%:

    awplus(config)# interface interface-id

    awplus(config-if)#no storm-control {broadcast | multicast | dlf} level

94. Por ejemplo, para desactivar el control de tormentas *broadcast* en el puerto 1.0.23, fuera cual fuera el nivel configurado, se usan los siguientes comandos:

    awplus(config)# interface port1.0.23

    awplus(config-if)# no storm-control broadcast level

5.19.1.3 LÍMITE DE DIRECCIONES MAC APRENDIDAS POR PUERTO

95. Esta funcionalidad nos permite configurar la seguridad a nivel de puerto de una forma más precisa y a su vez compleja. Permite definir qué equipos van a poder conectarse en cada puerto, o cuántas conexiones máximas se van a permitir en cada puerto y qué hacer en caso de que se alcance el número máximo de conexiones.

96. Lo primero que se debe conocer es el número de dispositivos que se van a necesitar conectar en cada uno de los puertos para poder configurar cuántas direcciones MAC el equipo va a aprender por ese puerto concreto. Se puede definir el máximo número de direcciones, en un puerto determinado, con el siguiente comando:

    awplus(config)# interface interface-id

    awplus(config-if)# switchport port-security maximum <0-256>

    Es importante considerar que el valor por defecto es 0. Por tanto, si no se configura un valor distinto, y se activa la seguridad por puerto, tan pronto como se aprenda la primera '*MAC Address*' se considera violada la seguridad y se ejecuta la acción definida según se explica en el siguiente párrafo.

97. Se puede definir qué medida se ha de tomar cuando en un puerto del *switch* se 'ven' más direcciones MAC de origen de las que en ese puerto se le permite

aprender. Esto es considerado una violación de la seguridad y se ejecuta la acción que se indique con el siguiente comando:

awplus(config-if)# switchport port-security violation {shutdown|restrict|protect}

Acción	Comportamiento
shutdown	Se apaga el puerto al detectarse la violación
restrict	Se descartan los paquetes de las nuevas MAC y se envía trap SNMP
protect	Se descartan los paquetes de la nueva MAC. *Opción por defecto*

Tabla 4: Acciones posibles tras violación de seguridad

98. Es importante indicar que, si un puerto es desactivado o apagado por la detección de una violación habiendo sido configurado para apagarse ante esta, el comando '*no shutdown*' NO vuelve a activar el puerto. Será necesario desactivar la seguridad por puerto, como se indica más adelante, para que este vuelva a estar activo.

99. También se puede indicar al equipo si las MAC que se le permite aprender en un determinado puerto lo hace "*de por vida*", de manera que las introduce como entradas estáticas de la tabla de direcciones MAC y las muestra como líneas de la '*running-config*'. Por tanto, si en ese momento se hace un salvado de configuración (copiar la *running* en la *startup*) las direcciones MAC aprendidas pasan a ser parte de la configuración de arranque del *switch* como entradas estáticas de la tabla de direcciones MAC.

100. Esto último tiene algunas consecuencias ya que, si el *switch* tiene una dirección MAC como entrada estática en un determinado puerto de su tabla de direcciones MAC, esa dirección no la aprenderá en ningún otro puerto (debido a que una misma dirección MAC no puede aprenderse en dos puertos distintos) y por tanto el dispositivo con esa dirección MAC solo podrá comunicarse con la red conectándose al puerto donde se ha creado esa entrada estática en la tabla de direcciones.

101. Del mismo modo si se ha limitado el número de direcciones MAC que se pueden aprender un puerto, y ya hay una entrada estática en la tabla de direcciones para ese puerto, en ese puerto no podrá tener comunicación con el resto de la red ningún dispositivo salvo el que cuya MAC sea la misma que está como entrada estática en la tabla de direcciones MAC.

102. Por defecto el *switch* creará las entradas estáticas en la tabla de direcciones MAC con las direcciones que vea en un determinado puerto, pero se puede hacer que este aprendizaje tenga carácter temporal con una caducidad igual al valor configurado como '*mac address-table aging-time*' (por defecto 300 seg) con el siguiente comando:

awplus(config-if)# switchport port-security aging

Una vez configurado esto, en cada arranque del *switch*, perdida de '*link*' en ese puerto, o transcurridos los segundos configurados como caducidad de la tabla de MAC del *switch*, este aprenderá el número máximo de direcciones MAC que se haya configurado y ejecutará la acción indicada como violación si se supera el número de MAC que se '*ven'* en ese puerto.

103. Una vez se ha configurado el número máximo de direcciones MAC que se pueden aprender en un determinado puerto, si se quiere que estas sean permanentes o volátiles, así como la acción a llevar a cabo si se detecta una violación de la seguridad para cada puerto, se puede habilitar la funcionalidad de seguridad por puerto en todos los interfaces. Esto se puede hacer con el comando:

    awplus(config-if)# switchport port-security

104. Del mismo modo, si se quiere desactivar esta característica en un puerto determinado, se utiliza el comando:

    awplus(config-if)# no switchport port-security

105. Para comprobar el estado de la seguridad por puerto en un determinado interfaz o grupo de interfaces, así como las intrusiones que se han detectado en el mismo, se puede utilizar los comandos:

    awplus# show port-security interface interface-id

    awplus# show port-security intrusion interface interface-id

106. Los *switches* de Allied Telesis con sistema operativo AW+ permiten la introducción de las direcciones MAC de manera manual (entrada estática), de manera que los equipos con una determinada MAC solo pueden conectarse que en el puerto en el que se realice dicha entrada.

107. Además, si se limita el número de direcciones MAC que se pueden aprender en un puerto (*port security*) y se realiza una entrada estática en la tabla de direcciones MAC para ese puerto, entonces en ese puerto solo se podrán aprender el número máximo de direcciones MAC configuradas menos el número de entradas estáticas realizadas para ese puerto. Para realizar entradas estáticas en la tabla de direcciones MAC, se utiliza el siguiente comando:

    awplus(config)# mac address-table static <AABB.CCDD.EEFF> forward interface <portID> vlan <VlanID>

108. Así para hacer una entrada estática en la tabla de direcciones para la dirección MAC: 00:16:7D:F9:EA:5F en el puerto 1.0.12 y para la vlan 5, se utiliza:

    awplus(config)# mac address-table static 00:16:7D:F9:EA:5F forward interface port1.0.12 vlan 5

5.20 NTP (*NETWORK TIME PROTOCOL*) Y *LOGGING*

5.21 *NTP FILTERING*

109. NTP, como cualquier otro servicio es vulnerable a ataques. *NTP filtering* permite la creación de reglas para especificar las direcciones IP con las cuales el proceso NTP interactuará. Existen diferentes formas de controlar el tipo de comunicación que se permite. Las reglas NTP pueden ser de los siguientes tipos:

Tipo	Descripción
-	Peticiones de tiempo y consultas de control de NTP se aceptarán de los dispositivos cuyas direcciones estén permitidas en esta lista de acceso. El proceso de NTP del *switch* es capaz de sincronizarse con un dispositivo cuya dirección está permitida en la lista de acceso.
query	Las consultas de control de NTP se aceptan desde los dispositivos cuyas direcciones estén permitidas en esta lista de acceso.
serve-only	Únicamente son aceptadas las solicitudes de tiempo que vienen desde los dispositivos cuyas direcciones están permitidas en esta lista de acceso.

Tabla 5: Tipos de reglas NTP

110. Las listas de acceso se aplican utilizando los siguientes comandos:

awplus(config)# ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>} {allow|deny}

awplus(config)# ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>} query {allow|deny}

awplus(config)# ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>} serve {allow|deny}

5.22 AUTENTICACIÓN NTP

111. El propósito de la autenticación de NTP es permitir que el cliente pueda autenticar el servidor, y no viceversa, para evitar la suplantación de un servidor NTP válido. La autenticación se realiza mediante el uso de una clave. El servidor y el cliente deben ser configurados ambos para realizar autenticación y usar la misma clave. Se recomienda el uso de SHA-1 (frente a MD5), ya que aporta un mayor nivel de seguridad.

112. Para configurar autenticación en el proceso durante el cual un *switch* sincroniza su reloj contra un servidor NTP, tres (3) pasos son necesarios:

- Habilitar autenticación para NTP[1]:

[1] En las versiones posteriores del producto (AW+ v5.5.0-1.x en adelante), el comando *ntp authenticate* no es necesario, ya que la autenticación NTP se encuentra activada por defecto y no se puede desactivar. Siendo necesario sólo configurar la clave que utilizará dicha autenticación y el servidor NTP.

awplus(config)# ntp authenticate

- Crear al menos una clave de tipo SHA-1 para que sea utilizada por la autenticación de NTP, incluir el parámetro *trusted* al final del comando para incluir dicha clave entre las claves de confianza del dispositivo. Para crear la clave con índice '1' y palabra clave 'our_secret':

  awplus(config)# ntp authentication-key 1 sha-1 our_secret trusted

- Por último, definir el servidor NTP desde el que se desea que el *switch* reciba la información. El servidor NTP debe estar configurado utilizar la misma clave SHA-1 para autenticación. Para definir un servidor NTP con dirección 10.20.30.35, usar la clave con índice 1 y la versión 4 de NTP (última disponible), se teclea:

  awplus(config)# ntp server 10.20.30.35 key 1 version 4

5.23 GESTIÓN DE CERTIFICADOS

113. Para el correcto funcionamiento de *Syslog* sobre TLS en el reenvío de logs (ver apartado 5.28 AUDITORÍA), es necesario configurar los certificados utilizados en dicha comunicación. Para ello, primero debe crearse un *Trustpoint*, el cual contendrá el certificado de la CA (*Certification Authority*) de confianza, así como los certificados del dispositivo. Posteriormente debe configurarse Syslog para hacer uso de dichos certificados.

114. El detalle sobre la gestión de certificados en el dispositivo se puede consultar en la guía *Public Key Infrastructure (PKI) Feature Overview and Configuration Guide – REF4.*

5.24 CREACIÓN DE UN TRUSTPOINT

115. Para la creación de un *Trustpoint* se deben seguir los siguientes pasos:

- Primero, crear el *Trustpoint* utilizando el siguiente comando:

  awplus(config)# crypto pki trustpoint <nombre>

- Dicho comando lo creará con el nombre indicado y situará al usuario en el modo de configuración del mismo. A continuación, mediante el comando *enrollment terminal*, se declara que utilizará certificados que se introducirán en el sistema posteriormente.

- Después, se debe introducir el certificado raíz de la CA de confianza, ejecutando el siguiente comando e introduciendo el certificado en el parámetro que aparecerá en pantalla:

  awplus(config)# crypto pki authenticate <nombre>

- Ahora es momento de crear el certificado de servidor. Mediante el comando *crypto pki enroll <nombre>*, se creará un CSR (*Certificate Signing Request*), el cual se mostrará en pantalla en formato PEM. Este debe copiarse y transmitirse a la CA correspondiente para su creación.

- En caso de disponer también de certificados intermedios, se deben importar. Para ello utilizar el siguiente comando:

  awplus(config)# crypto pki import <nombre> pem

- Una vez importados los certificados de CA, debe importarse el certificado de servidor que utilizará el dispositivo, el cual se debe recibir por parte de la CA tras el envío del CSR. Para ello se utilizará el mismo comando:

  awplus(config)# crypto pki import <nombre> pem

116. Tras la ejecución de estos comandos, el dispositivo dispondrá de:

- Certificado raíz de la CA externa.
- Certificado intermedio de la CA externa.
- Certificado de servidor propio del dispositivo firmado por la CA.
- Par de claves propio.

5.25 CONFIGURACIÓN DE *SYSLOG* SOBRE TLS

117. Para el correcto funcionamiento de la comunicación, se debe crear un *Trustpoint* siguiendo los pasos indicados en el anterior apartado. Una vez creado, se debe configurar el proceso *Syslog* para realizar una conexión segura mediante TLS. Para ello:

- Indicar al proceso *Syslog* que debe utilizar el *Trustpoint* creado:

  awplus(config)#log trustpoint <NombreTrustpoint>

- Configurar el dispositivo para enviar los log cifrados a un servidor remoto *Syslog* mediante TLS:

  awplus(config)#log host <syslog-server-IP-address> secure

- Configurar la severidad de los logs.

118. El detalle de configuración del envío de logs se puede consultar en el apartado 5.29 *LOGGING*.

5.26 ACTUALIZACIÓN DEL *SOFTWARE* DEL DISPOSITIVO

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

120. Existen varios métodos para actualizar el *software/firmware* de un *switch* de Allied Telesis. En este guía se recoge la actualización por medio de SFTP. Para realizar esta actualización, se necesita:

- Haber configurado al menos una dirección IP al *switch* para poder hacer la transferencia del archivo que contiene el nuevo *firmware.*

- Habilitar un servidor SFTP alcanzable por el *switch* (debe haber comunicación IP entre el *switch* y el servidor).
- Disponer del ultimo *firmware* disponible para el *switch* en cuestión, para ello puede ponerse en contacto con: preventa_ib@alliedtelesis.com

121. Lo primero es copiar a la memoria interna del equipo el nuevo *firmware* a ejecutar, se hace uso del comando '*copy sftp flash*', y el equipo irá pidiendo los datos necesarios según se ve en la siguiente figura:

```
awplus#copy sftp flash
Enter source host name []:192.168.1.70
Enter username [manager]:
Enter source path with file name []:x930-5.5.0-0.6.rel
Enter destination file name[x930-5.5.0-0.6.rel]:
Copying...
The authenticity of host '192.168.12.222 (192.168.12.222)' can't be established.
RSA key fingerprint is
SHA256:jtjIwvRKHjE3Bpd4is42anNOkJ2lR6vMgbVbuR1UUZ8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
manager@192.168.12.222's password:

Successful operation
awplus#
```

122. Donde '*hostname*' es la dirección IP del servidor SFTP en cuya carpeta raíz está almacenado el fichero de *firmware* que se quiere copiar a la memoria *flash* del equipo. '*File name*' es el nombre del *firmware* a copiar, en este caso *x930-5.5.0-0.6.rel*. Nótese que este nombre cambiará según la versión de *software*. El equipo nos propone como '*destination file name*' el nombre original del *firmware*, de manera que si se pulsa la tecla '*intro*' el archivo se grabará en la memoria *flash* con ese nombre. Se recomienda no cambiar el nombre del archivo ya que así se identifica fácilmente a qué versión corresponde cada archivo. A la pregunta sobre la clave RSA hay que contestar '*yes*' y a continuación escribir la clave del usuario del servidor SFTP.

123. Después, se verifica la integridad del fichero realizando el hash SHA256. Para ello utilizar el comando *crypto verify <nombre del fichero> <valor hash>*. El valor hash se obtendrá junto con el firmware tras contactar con preventa_ib@alliedtelesis.com.

124. Una vez copiado el archivo, se verifica que ya está disponible en la memoria *flash* con el siguiente comando:

```
awplus#dir
        47079454 -rwx Nov 02 2021 18:51:31  x930-5.5.0-0.6.rel
        0 drwx Oct 13 2021 15:01:00  log/
        4873 -rw- Oct 05 2021 19:11:47  default.cfg
        2719744 -rw- Sep 30 2021 17:50:32  awplus-gui_551_24.gui
        24057 -rw- Jun 19 2020 18:11:26  ssh.pcap
        214 -rw- Jun 19 2020 17:28:30  manager-rsa.pub
        0 drwx Aug 19 2019 18:03:58  gui-userdata/
awplus#
```

125. Si durante el proceso de copia diese algún error por falta de espacio en la memoria, se puede liberar espacio borrando cualquiera de los ficheros que se muestran a la salida del comando '*dir*' utilizando:

```
awplus#delete archivo.extension

Delete flash:/archivo.extension?  (y/n)[n]:y

Deleting...

Successful operation
```

126. Esto solo es necesario si se encuentran problemas de espacio en la operación realizada.

127. Cuando se tenga el nuevo *firmware* en la memoria del equipo, hay que configurar el producto para que lo utilice la próxima vez que sea reiniciado. La instrucción a utilizar es:

```
awplus(config)#boot system Nombre_Firmware.rel
```

128. En el ejemplo, para configurar el equipo para que arranque con el *software* que se acaba de cargar y reiniciar, se utilizan los comandos:

```
awplus(config)#boot system x930-5.5.0-0.6.rel
awplus(config)#exit
awplus#reload
reboot system? (y/n):y
```

129. Una vez el equipo termine de arrancar, hacer *login* y verificar que se está ejecutando el nuevo *firmware* con la instrucción:

```
awplus#show version

AlliedWare Plus (TM) 5.5.0 10/01/21 05:51:08

Build name : x930-5.5.0-0.6.rel
```

130. También podrá verificarse la información mediante el comando *show system*. Este comando mostrará información relativa al *hardware* del dispositivo, el uso de memoria y la versión del *software*.

```
awplus#show system

System Status                                    Mon Nov 16 08:42:16 2015

Board          ID      Bay     Board  Name              Rev     Serial  number
-------------------------------------------------------------------------------------------------
Base           389             AT-x930-28GSTX           A-0 000181A151300053
Expansion      417     Bay1    AT-FAN09ADP              A-0     N/A
PSU            337     PSU1    PWR250                   A-0     A212F506Z
PSU            337     PSU2    PWR250                   A-0     A212F506D
-------------------------------------------------------------------------------------------------
RAM: Total: 2007632 kB Free: 1786472 kB
Flash: 253.8MB Used: 35.8MB Available: 218.0MB
-----------------------------------------------------------------------
Environment Status   : Normal
Uptime               : 3 days 22:20:06
Bootloader version   : 3.1.3
?
Current software : x930-5.5.0-0.6.rel
Software version : 5.5.0-0.6
Build date : Thu Nov 12 12:11:29 NZDT 2015

Current boot config: flash:/backup.cfg (file exists)

System Name
awplus
System Contact
System Location
```

131. Por último, se puede utilizar el comando *show boot*, para obtener la configuración actual del *boot*.

```
awplus#show boot
Boot configuration
-----------------------------------------------------------
Current software     : x930-5.5.0-0.6.rel
Current boot image   : usb:/x930-5.5.0-0.6.rel
Backup boot image    : flash:/x930-5.4.9-2.1.rel
Default boot config  : flash:/default.cfg
Current boot config  : usb:/my.cfg (file exists)
Backup boot config   : flash:/backup.cfg (file not found)
Autoboot status      : enabled
```

5.27 ALTA DISPONIBILIDAD

132. El producto permite realizar un despliegue de Alta Disponibilidad siguiendo una de las siguientes opciones:

- Desplegando varios dispositivos redundantes en la red, de tal forma que, si uno falla, alguno de los otros dispositivos puede retomar sus labores y continuar ofreciendo el servicio. Esto requiere el uso de VRRP.
- Desplegando enlaces redundantes en la red, de tal forma que, si un enlace falla, otro pueda continuar con el servicio, como redundancia WAN.

133. El producto permite alcanzar Alta Disponibilidad combinando VRRP con un *Bypass Relay,* que crea una conexión física directa entre el puerto WAN de un dispositivo principal y el puerto *bypass* de un dispositivo de respaldo. De tal forma que, si el dispositivo principal falla, el dispositivo secundario retoma su servicio.

134. Debido a la extensión de la configuración de Alta Disponibilidad, se recomienda consultar el detalla en la guía *High Availabilityb Feature Overview and Configuration Guide – REF5*.

5.28 AUDITORÍA

5.29 *LOGGING*

135. Los *switches* con sistema operativo AW+ registran toda su actividad generando diferentes mensajes que son almacenados en fichero interno (log). Estos logs se almacenan por defecto en la memoria RAM del dispositivo como *Buffered log*. Este almacenamiento es limitado, por lo que borra los registros antiguos, cuando la memoria se llena, para almacenar los más recientes. Se eliminan en caso de reiniciar el dispositivo.

136. Los mensajes generados contienen la siguiente información:

Elemento	Descripción
<date><time>	Fecha y hora en la que se generó el mensaje.
<facility>	Nivel de *Facility* asignado al mensaje.
<severity>	Índice de importancia asignado al mensaje.
<hostname>	Nombre del dispositivo.
<program>	Programa particular que generó el mensaje (por ejemplo, kernel, ESPR, etc).
<pid>	El ID del proceso del programa en el momento que se generó el mensaje.
<message>	Contenido específico del mensaje. Puede incluir el nombre de interfaces u otra información.

Tabla 6: Tipos de mensajes generados

137. Por tanto, es muy recomendable configurar el *switch* para enviar todos estos mensajes a un '*syslog server*', un servidor externo que permitirá guardar una copia de todos los mensajes generados por el *switch*, sin temor a que, por falta de espacio o reinicios inesperados de este, se pierdan los logs del dispositivo.

138. Para que todos los mensajes generados por el *switch* sean enviados un servidor externo con dirección IP: 10.32.16.21, se puede utilizar el siguiente comando:

awplus(config)# log host 10.32.16.21 secure

139. Para filtrar el nivel de los mensajes que serán enviados a ese servidor, se utiliza:

awplus(config)# log host 10.32.16.21 level <nivel>

De manera que únicamente los mensajes con índice de importancia menor o igual que el parámetro *<nivel>,* serán enviados a al *syslog* con esa dirección IP. En la siguiente tabla se observa el tipo de mensajes correspondientes a cada índice de importancia.

Nivel	Descripción
0	Emergencia: El sistema no es funcional
1	Alerta: Se requiere una acción de manera inmediata
2	Crítica: Condiciones criticas
3	Error: Se ha producido un error.
4	Avisos: Se produce un aviso ante un evento
5	Noticias: Condiciones normales pero reseñables
6	Informaciones: Mensajes de información
7	*Debugging*: Mensajes de depuración

Tabla 7: Índices de importancia asignados a los logs

140. El detalle de configuración de los registros de auditoría se puede consultar en la guía *Logging and Debug Feature Overview and Configuration Guide – REF6*.

5.30 *BACKUP*

141. El producto permite crear una copia de seguridad del fichero de configuración mediante el comando *boot config-file backup <NombreDeFichero.cfg>*. El fichero se debe encontrar en el sistema de ficheros *flash* del dispositivo y debe tener extensión *.cfg*. Tras su creación se puede exportar a una localización externa.

142. Para cargar una copia de seguridad, importarla al dispositivo se puede utilizar el comando *boot config-file <ubicación-nombreDeFichero>*. De esta forma, tras reiniciar el dispositivo se cargará dicho fichero de configuración.

5.31 VLANS

143. Se puede definir una VLAN (*Virtual Local Area Network*) como un dominio de difusión, de manera que 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 VLANs.

5.32 VLANS COMO MEDIDA DE AISLAMIENTO

144. A nivel de seguridad, las VLAN permiten crear distintos dominios de difusión sin que influya la localización física del equipo, sino el grupo al que se quiere que pertenezca. Por lo tanto, se va a poder definir qué dispositivos podrán comunicarse con otros y cuáles no, constituyendo una capa de seguridad alrededor de equipos que contengan información crítica.

145. En la configuración por defecto que tienen los equipos de Allied Telesis, existe con una VLAN creada por defecto y denominada '*default*' y con *vlanID*: 1. En esta VLAN están asignados en un principio todos los puertos del *switch*. Como recomendación de seguridad se puede establecer una VLAN en la cual se agrupen todos los puertos inactivos y aislar éstos de cualquier VLAN que contenga puertos que estén en uso. De inicio, se puede asignar todos los puertos a una VLAN distinta a la creada por defecto por el *switch*, para después ir sacándolos de ese grupo y asignándolos a las VLAN a las que pertenecerán, de esta forma se evitará utilizar la VLAN por defecto.

146. Para crear una VLAN, entrar desde el modo global de configuración en la base de datos de VLAN y crear la VLAN utilizando los siguientes comandos:

awplus(config)#vlan database

awplus(config-vlan)#vlan <VLAN-ID>

147. Por ejemplo, para crear una VLAN con VID 22 se usan los comandos:

awplus(config)#vlan database

awplus(config-vlan)#vlan 22

148. Se pueden crear varias VLAN a la vez separando los VIDs por comas (por ejemplo: 22,23,24) o incluso con un guion de manera que se crean todas las vlan comprendidas entre los números indicados (por ejemplo: 22-24)

149. Con los comandos indicados las VLAN se crearán con el nombre VLANxxxx, donde 'xxxx' es el VID utilizado. Para crear una VLAN con un nombre determinado o cambiarle el nombre por defecto a una VLAN previamente creada:

awplus(config-vlan)#vlan <VLAN-ID> name <vlanname>

150. Por ejemplo, para crear una VLAN con VID 22 y nombre '*telefonía':*

awplus(config-vlan)#vlan 22 name telefonia

151. Se puede usar este mismo comando si se ha creado la vlan 22 y no se ha dado un nombre a la VLAN, para ponerle el nombre '*telefonía*'.

152. Con estas instrucciones, se pueden crear las VLAN necesarias, pero todos los puertos siguen perteneciendo a la VLAN por defecto (VID 1). Para configurar uno o varios puertos para que pertenezcan a una determinada VLAN la instrucción es:

awplus(config)# interface <port-list>

awplus(config-if)#switchport access vlan <VLAN-ID>

153. Por ejemplo, para que el puerto 'port1.0.24' pertenezca ahora a la VLAN 22, se utilizan los siguientes comandos:

awplus(config)# interface port1.0.24

awplus(config-if)#switchport access vlan 22

154. Por último, también es posible crear una VLAN destinada solo a las labores de gestión. Esta VLAN tendrá las siguientes características:

- Solo tendrá un puerto de acceso.
- No dirigirá tráfico de otras interfaces.
- Procesa los paquetes en la CPU, en lugar de en el hardware.
- No se puede convertir una VLAN normal en una de gestión y viceversa. Para ello sería necesario eliminar la VLAN y crearla de nuevo.
- Para crear la VLAN de gestión con nombre *VLANgestion*, utilizar el siguiente comando:

  awplus(config-vlan)#vlan <VLAN-ID> name VLANgestion state management-only

5.33 DESPLIEGUE DE VLANS A LO LARGO DE LA RED

155. Si se necesita que una VLAN contenga puertos de más de un único *switch*, será necesario asignar a esa VLAN dos puertos en cada uno de los *switches* que se atraviesen para realizar el enlace, de manera que los mensajes de *broadcast* puedan propagarse a través de ellos. Por lo tanto, los *switches* intermedios van a tener que dedicar dos puertos para poder interconectar VLAN en las cuales quizás ni siquiera tienen puertos que pertenezcan a ellas. Por ejemplo, si hay 10 VLAN, se necesitarían 20 puertos por *switch* solo para interconexiones, lo cual puede generar una situación insostenible en caso de que se disponga de un alto número de VLAN ya que no quedarían puertos disponibles.

156. En el ejemplo, el switch intermedio tiene que dedicar cuatro puertos para interconexión de las VLAN roja y verde que existen en los dos switches que interconecta sin que el mismo tenga puertos en ninguna de estas vlan.

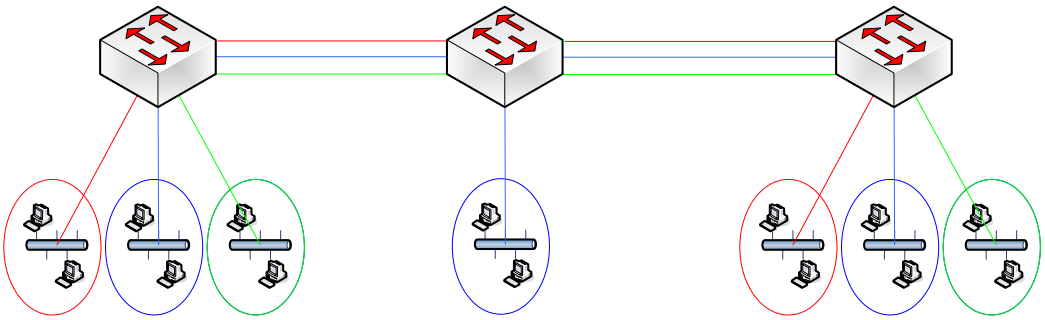


Ilustración 3. Ejemplo dedicación de puertos

157. Para evitar esto, se pueden utilizar puertos en modo *Trunk*. Un puerto en modo *trunk* permiten interconectar varias VLAN sin necesidad de emplear un puerto para cada VLAN. Esto es posible gracias al uso de etiquetas (802.1Q) en los paquetes enviados. Estas etiquetas sirven para identificar a qué VLAN pertenecen los paquetes, de manera que es posible compartir un único enlace entre *switches* manteniendo las propiedades de aislamiento de las VLAN.

158. Por defecto, todos los puertos están configurados en modo '*access*'. Están, por tanto, preparados para conectar dispositivos de usuario: PC, portátiles, impresoras, etc. Si se va a utilizar uno o más puertos para transportar más de una VLAN en un enlace entre *switches* o para conectar dispositivos capaces de atender más de una VLAN como: puntos de acceso, teléfonos IP, sevidores, etc. Es necesario configurarlos en modo *trunk* con la siguiente instrucción:

awplus(config)# interface <port-list>

awplus(config-if)# switchport mode trunk

159. Una vez que se ha configurado el modo *trunk,* es necesario indicar qué VLAN se quiere propagar por este puerto con el comando:

awplus(config-if)#switchport trunk allowed vlan add <VLAN-LIST>

160. Como se ha explicado, en estos puertos el tráfico de cada VLAN irá identificado mediante el uso de etiquetas. Esto es necesario para poder distinguir a que VLAN pertenece cada uno de los paquetes y así no mezclar tráfico entre ellas. Para que esto sea posible los paquetes de todas las VLAN, menos una de las que se trasportan en el puerto, han de llevar etiquetas. Esta VLAN cuyos paquetes no van etiquetados se la conoce como '*native*' del enlace *trunk*. Para configurar qué VLAN se envía sin etiquetar sus paquetes en un puerto (o rango de ellos) se utiliza el comando:

awplus(config-if)#switchport trunk native vlan <VLAN-ID>

161. Cuando se configura un puerto en modo *trunk*, por defecto, la VLAN 1 se envía como nativa por ese puerto. Esta VLAN es en la que todos los puertos de la mayoría de los *switches* vienen configurados. Por tanto, es muy recomendable configurar una VLAN distinta de la por defecto como nativa para ese puerto o configurar el puerto para que ninguna VLAN se envíe como nativa en los puertos

que interconectan *switches* para evitar que se establezcan comunicaciones a través de la VLAN por defecto.

162. Para configurar un puerto en modo *trunk* para que no trasmita ninguna VLAN como nativa, se utiliza el comando:

awplus(config-if)#switchport trunk native vlan none

163. A modo de ejemplo, si se quiere configurar el puerto 'port1.0.10' para transmitir las VLAN con VID: 5,6,7 y 9 etiquetadas (se entiende que dichas VLANS han sido creadas previamente) y que no se trasmita ninguna VLAN sin etiquetar, la secuencia de comandos sería:

awplus(config)# interface port1.0.10

awplus(config-if)# switchport mode trunk

awplus(config-if)#switchport trunk allowed vlan add 5-7,9

awplus(config-if)#switchport trunk native vlan none

5.34 PREVENCIÓN DE CAIDAS DEL SISTEMA

5.35 USO DE ACLS PARA PROTEGER LA CPU DE ATAQUES

164. Las listas de control de acceso (ACL) son una herramienta que los *switches* con sistema operativo AW+ disponen para decidir el tráfico que se desea permitir y/o denegar, controlando que equipos de la red tendrán comunicación entre sí (o no).

165. Es por tanto una herramienta de seguridad cuya aplicación depende del tipo de tráfico de cada red. Este apartado se ha enfocado en el uso de ACL para la protección de la CPU del equipo de los ataques más frecuentes.

166. En los siguientes párrafos se crean 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, se considera la dirección IP de gestión la 172.28.78.23 y la 172.28.0.0/16 como red de gestión.

167. Se crea la ACL con nombre '*protect-management*' y se permite el tráfico SNMP, con puerto de destino 161 y de tipo UDP, desde la red de gestión (por ejemplo: 172.28.0.0/16):

awplus(config)# access-list hardware protect-management

awplus(config-ip-hw-acl)# 10 permit udp 172.28.0.0/16

172.28.78.23/32 eq 161

168. Se añade la entrada para permitir el tráfico HTTP, con puerto de destino 80 y de tipo TCP, desde la red de gestión:

awplus(config-ip-hw-acl)# 20 permit tcp 172.28.0.0/16

172.28.78.23/32 eq 80

169. Para permitir el tráfico SSH, de tipo TCP y con puerto de destino 22, desde la red de gestión:

awplus(config-ip-hw-acl # 30 permit tcp 172.28.0.0/16 172.28.78.23/32 eq 22

170. Si se quiere que el equipo responda a los *pings* que reciba desde la red de gestión, hay que permitir el trafico ICMP desde esa red hacia la IP de gestión:

awplus(config-ip-hw-acl)# 40 permit icmp 172.28.0.0/16

172.28.78.23/32

171. Se crea una entrada que bloquea cualquier otro tráfico que vaya destinado a la dirección IP de gestión del equipo y que por tanto pueda sobrecargar la CPU de esta.

awplus(config-ip-hw-acl)# 50 deny ip any 172.28.78.23/32

172. Por último, es necesario aplicar esta ACL con nombre '*protect-management*' a todos los puertos por los cuales se necesitará acceder a la gestión del equipo, pero, al mismo tiempo, se quiere proteger de accesos a la misma desde redes distintas a la de gestión para evitar una sobrecarga en la CPU del equipo. Así, si se sabe que la gestión del equipo se alcanza por los puertos 1.0.25 y/o 1.0.26, se aplicaría la ACL según el siguiente comando:

awplus(config)# interface port1.0.25,port1.0.26

awplus(config-if)# access-group protect-management

173. Para el resto de los puertos para los que no se necesita acceso a la gestión, se puede crear y aplicar una ACL que restrinja todo el tráfico con destino la IP de gestión del equipo.

awplus(config)# access-list hardware block-management

awplus(config-ip-hw-acl)# 10 deny ip any 172.28.78.23/32

awplus(config-ip-hw-acl)# interface port1.0.1-1.0.24

awplus(config-if)# access-group block-management

5.36 PREVENCIÓN DE *MAC FLODDING*

174. Este ataque consiste en la inundación de la red con multitud de paquetes cuya dirección MAC de origen es distinta. El *switch,* de acuerdo a su manera de trabajar, irá apuntando cada una de las direcciones MAC de origen como entradas de su tabla de direcciones en los puertos donde haya visto entrar los paquetes. Si el número de direcciones MAC que el *switch* tiene que aprender supera el máximo que es capaz de almacenar, comenzará a hacer *broadcast* de todo el tráfico con objeto de no interrumpir la comunicación entre estaciones base. Este '*flooding*' de paquetes puede ser aprovechado con objeto de capturar información y, por tanto, suponer una vulnerabilidad del sistema.

175. La manera más sencilla de evitar dicha vulnerabilidad consiste en implementar la funcionalidad de seguridad por puerto, que puede limitar el máximo de

direcciones MAC aprendidas en un determinado interfaz, impidiendo que la tabla de direcciones del equipo se vea desbordada. Para más información sobre seguridad por puerto, consultar el apartado 5.13 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.

5.37 MECANISMOS FRENTE A ATAQUES DE DENEGACIÓN DE SERVICIO

176. Para mantener el servicio, se requiere un acceso a la red fiable y siempre disponible, pero existen ataques de denegación de servicio que pueden impedirlo. Algunos de estos ataques tienen como objetivo dispositivos finales y pueden reducir su rendimiento, enviar una tormenta de datos a una víctima específica o consumir recursos en línea.

177. Los *switches* de Allied Telesis incorporan defensa ante muchos de estos ataques DoS, y además la mayor parte de estas están implementadas en *hardware* por lo que no afectan al rendimiento de la red.

178. La defensa ante los distintos tipos de ataques de DoS puede ser activada para uno o varios puertos introduciendo los siguientes comandos:

awplus(config)# interface <port-list>

awplus(config-if)# dos {ipoptions|land|ping-of-death|smurf broadcast <local-ip-broadcast-addr>|synflood|teardrop}

action {shutdown|trap|mirror}

179. En la siguiente tabla se explica brevemente en qué consiste cada uno de los ataques DoS para los que los *switches* con AW+:

Tipo de ataque DoS	Descripción
ipoptions	Este tipo de ataque se produce cuando un atacante envía paquetes que contienen opciones IP en mal estado a un nodo víctima. Hay diferentes tipos de ataque '*ipoptions*' que AW+ no trata de distinguir entre ellos. Más bien, si esta protección está activada, el número de paquetes IP de entrada que contienen opciones IP son limitados. Si el número es superior a 20 paquetes por segundo, el equipo considera que se encuentra ante un posible ataque '*ipoptions*'. Esta protección no requiere la CPU para supervisar los paquetes, por lo no supone una carga adicional en la CPU del *switch*.
land	Este tipo de ataque se produce cuando la dirección IP de origen y destino es la misma. Dado que paquetes con las mismas direcciones fuente y destino nunca deben ocurrir, estos paquetes son descartados cuando este tipo de defensa está activada. Esta defensa no necesita la CPU para supervisar los paquetes, por lo no supone una carga adicional en la CPU.

Tipo de ataque DoS	Descripción
ping-of-death	Este tipo de ataque resulta de un paquete fragmentado que, cuando es re-ensamblado, superara el tamaño máximo de un datagrama IP. Para detectar este ataque, el fragmento final de los paquetes ICMP tiene que ser enviado a la CPU para su inspección. Esta defensa, por lo tanto, puede cargar la CPU. Hay que tener en cuenta que la carga extra de CPU no afectará el tráfico normal de conmutación entre puertos, pero otros protocolos tales como IGMP o RSTP sí pueden verse afectados. Esta defensa no se recomienda en entornos donde se espera que gran número de paquetes fragmentados.
smurf	Este tipo de ataque consiste en un *paquete* ping a una dirección de *broadcast*. Aunque los *routers* ya no deben reenviar paquetes a las direcciones locales de *broadcast* (ver RFC2644), el ataque *Smurf* todavía puede ser desechado de forma explícita con este comando. Para que el ataque *Smurf* obtenga resultados, se requiere la dirección IP de *broadcast*. Cualquier paquete ICMP *ping* con esta dirección de destino es considerado como un de ataque. Esta defensa no requiere la CPU para supervisar los paquetes, por lo que no supone una carga adicional en la CPU del *switch*.
synflood	En este tipo de ataque, el atacante trata de sobrecargar a la víctima con peticiones de conexión TCP, enviándole un gran número de paquetes *TCP SYN* con direcciones de origen falsas. La víctima responde con paquetes *ACK SYN*, pero debido a que las direcciones de origen son falsas, el nodo víctima no recibe ninguna respuesta. Si el atacante envía la demanda suficiente, en un período suficientemente corto, la víctima puede sufrir un bloqueo en su funcionamiento una vez que las solicitudes excedan la capacidad de su cola de conexiones. Para defenderse de este tipo de ataque, se vigila el número de paquetes *TCP-SYN* que se recibe en un puerto del *switch*. Se considera que en un puerto se está produciendo un ataque de este tipo si se reciben más de 60 paquetes *TCP-SYN* por segundo.
teardrop	En este ataque DoS, un atacante envía a la víctima, un paquete dividido en varios fragmentos, uno de ellos con un valor de desplazamiento falso (parámetro utilizado para reconstruir el paquete). Esto produce que el nodo atacado no es capaz de volver a re-ensamblar el paquete, causando probablemente un bloqueo en su funcionamiento.

Tabla 8: Tipos de ataques DoS

180. Se puede configurar el *switch* para que ejecute una acción determinada en caso de que la detección de ataque DoS sea positiva:

Acción	Comportamiento
shutdown	Se apaga el puerto al detectarse el ataque
trap	Se envía un trap SNMP informando del ataque
mirror	Se envían los paquetes al puerto de *mirroring*

Tabla 9: Tipos de acción tras detectar ataque DoS

5.38 *DHCP SNOOPING*

181. La asignación dinámica de direcciones IP por medio del uso de un servicio de DHCP supone exponer la red a una serie de vulnerabilidades conocidas relacionadas con el uso de este y por tanto **su uso no está recomendado**, a menos que se habilite *DHCP snooping* en todos los equipos de la red. Para ello:

- Primero es necesario activar *DHCP Snooping* en el dispositivo, a través del comando *service dhcp-snooping*.
- Una vez activado en el sistema, se deberá activar para una VLAN particular. Se recomienda activarlo para todas. Para ello, acceder a la configuración de la VLAN y ejecutar el comando *ip dhcp snooping*.

182. *DHCP snooping* es el proceso por el cual un *switch* observa todos los paquetes de DCHP que pasan por cualquiera de sus puertos. *DHCP snooping* envía todos los paquetes a la CPU del *switch* antes de ser transmitidos. Gracias a esto, es capaz de estudiar los paquetes de DHCP y ver qué direcciones IP están siendo asignadas a qué clientes. Con esta información, el *switch* elabora y mantiene una base de datos de las direcciones IP que están actualmente asignadas a los clientes y en qué puerto están conectados cada uno de estos clientes.

183. Cuando *DHCP snooping* está activado y se ha completado de manera correcta la concesión de una dirección IP a un cliente, crea una entrada en la base de datos. Cada entrada contiene la siguiente información:

Campo	Descripción
Client IP	La dirección IP que se ha asignado al cliente DHCP observado
MAC Address	La dirección MAC del cliente DHCP observado
Server IP	La dirección IP del servidor DHCP
Vlan	La VLAN a la que está conectado el cliente DHCP observado
Port	El puerto al que el cliente DHCP observado está conectado

Campo	Descripción
Expires	El tiempo, en segundos, hasta que la entrada de cliente DHCP expirará

Tabla 10: Entradas de la base de datos *DHCP Snooping*

184. El comando para mostrar el contenido de esta base de datos es:

awplus# show ip dhcp snooping binding

185. El propósito principal de esta base de datos es que el *switch* pueda bloquear la suplantación de direcciones IP ya que sabe qué clientes están conectados a qué puertos y con qué dirección IP, y puede, por tanto, bloquear los paquetes que llegan a un puerto X con una dirección IP de origen que sabe se ha asignado a un cliente en el puerto Y. De manera similar, si un paquete de una estación de trabajo llega con una dirección IP de origen que no aparece en ninguna parte en la base de datos de *DHCP snooping*, se determina que es un paquete que no está utilizando la dirección IP que le ha sido asignada y es descartado.

186. La protección contra la suplantación de direcciones IP es únicamente eficaz cuando las estaciones de trabajo cliente están directamente conectadas al *switch* con *DHCP snooping* activo. Si hay otro *switch* (sin DHCP *Snooping*) conectado al *switch* que está haciendo *DHCP snooping*, las estaciones de trabajo cliente conectadas en cualquier puerto del *switch* sin *DHCP snooping* podrían suplantar la dirección IP de cualquier equipo conectado en ese mismo *switch*.

187. Para admitir el escenario donde uno o más PCs de cliente hayan sido configurados con direcciones IP estáticas de manera deliberada, es posible añadir entradas estáticas en la base de datos de *DHCP snooping.*

188. Los dos (2) ataques más típicos a los que la red está expuesta con el uso de asignación dinámica de direcciones por DHCP, son:

- *Rogue DHCP server attack* (ataque por suplantación del servidor DHCP): una estación de trabajo malintencionada puede actuar como un servidor DHCP, y responder a las peticiones de dirección IP de otras estaciones de trabajo. Así, puede asignarles direcciones IP incorrectas, incompatibles con las tablas de rutas en la red, de manera que no podrán hacer uso de esta o peor aún, podría proporcionar como dirección del servidor DNS un servidor malicioso que dirija a los usuarios a sitios impostores.
- *DHCP server exhaustion attack* (ataque por agotamiento del rango de direcciones IP a asignar por el servidor): una sola estación de trabajo malintencionada puede solicitar innumerables concesiones de direcciones IP a un servidor DHCP haciéndose pasar por diferentes dispositivos cliente. Si se va modificando el ID de cliente en sus peticiones, el servidor seguirá asignando direcciones IP diferentes. Este proceso puede consumir rápidamente la totalidad del rango de direcciones IP disponibles en el

servidor, negando así a otras estaciones de trabajo en la red la oportunidad de obtener las direcciones IP cuando la soliciten

189. La funcionalidad de *DHCP Snooping* de los *switches* con sistema operativo AW+ proporciona mecanismos de seguridad frente a ambos ataques.

190. Para defenderse de los '*rogue DHCP server attacks*', *DHCP snooping* introduce el concepto de puertos de confianza y no seguros. Puertos de confianza son típicamente los puertos conectados hacia el núcleo de la red. Un puerto no seguro es aquel donde están conectadas las estaciones de trabajo. *DHCP Snooping* aplica una regla simple: los paquetes DHCP que vengan de un servidor DHCP (*OFFER, ACKs*) solo se aceptan si llegan a través de un puerto de confianza. Los paquetes DHCP de tipo Servidor recibidos en un puerto no seguro se descartan.

191. En AW+ todos los puertos están definidos como no seguros de forma predeterminada, y los puertos de confianza deben ser configurados explícitamente como '*trusted ports*'. Así para configurar la interface port1.0.24 como puerto seguro para recibir paquetes del servidor DHCP, se utiliza el comando:

awplus(config)# int port1.0.24

awplus(config-if)# ip dhcp snooping trust

192. Hay dos (2) formas en que *DHCP snooping* puede defender la red contra ataques por agotamiento del rango de direcciones IP a asignar por el servidor. La primera es la limitación de concesiones posibles en cada uno de los puertos, simplemente poniendo un límite en el número concesiones de direcciones IP que *DHCP snooping* permite asignar a estaciones conectadas en cada uno de los puertos definidos como no seguros. Por defecto, *DHCP snooping* permite una única concesión de dirección IP por puerto definido como no seguro. Este límite puede ser reconfigurado en función de cada puerto con el comando:

awplus (config) # int port1.0.12

awplus (config-if) # ip dhcp snooping max-bindings < number of leases >

Una vez alcanzado el número máximo de concesiones de direcciones IP en un determinado puerto, las siguientes solicitudes de los clientes en ese puerto son descartadas.

193. Como se indica en el párrafo anterior, limitar el número de concesiones por puerto puede limitar el daño causado por un ataque de agotamiento de las direcciones IP, pero si un puerto es configurado para conceder un número máximo de direcciones IP, un atacante conectado en ese puerto seguirá siendo capaz de adueñarse de todas estas.

194. Por lo general, en un ataque de agotamiento de direcciones IP, la dirección MAC del ID de cliente dentro de un paquete de solicitud de DHCP suele ser diferente a la dirección MAC de origen del paquete. Esto es debido a que el ID de cliente es el parámetro que el servidor utiliza para decidir si la solicitud es desde un nuevo cliente o de una que ya tiene una concesión de dirección IP. Esto obliga al atacante

por agotamiento de concesiones a utilizar una serie de diferentes IDs de cliente en sus peticiones. Pero si, del mismo modo, va cambiando la dirección MAC de origen de sus peticiones, es probable que sea bloqueado por la seguridad del puerto, que limita el número de MAC que se pueden aprender en un puerto determinado.

195. A menos de que haya pasado a través de un servicio de *DHCP relay*, una solicitud de DHCP válida siempre debe tener la dirección MAC del ID de cliente igual a la dirección MAC origen del paquete. No hay ninguna razón para que estas sean distintas. Como parte del bloqueo de ataques de agotamiento de direcciones IP disponibles para asignar en el servidor DHCP, *DHCP snooping* puede ser configurado para comprobar la consistencia de las MACs, descartando las solicitudes en las que dirección MAC de origen difiere de la dirección MAC del ID de cliente.

196. Esta verificación está activada de forma predeterminada y se puede desactivar con el comando:

awplus(config)# no ip dhcp snooping verify mac-address

197. Es importante resaltar que es necesario desactivar esta función (al menos en los puertos necesarios) cuando el *switch* con *DHCP snooping* se encuentra en camino hacia el servidor de DHCP de un servicio de *DHCP relay*, ya que la dirección MAC de origen del paquete no coincidirá con el ID de cliente en los paquetes DHCP una vez que estos hayan atravesado el servicio de *DHCP relay*.

5.39 SUPLANTACIÓN DE INDENTIDAD EN PAQUETES ARP

198. La inspección dinámica de paquetes ARP, denominada en AW+ *ARP Security*, permite en combinación con *DHCP snooping*, prevenir la suplantación de identidad en paquetes ARP. Al habilitar *ARP Security*, todos los paquetes ARP recibidos en interfaces configurados como no seguros son solo permitidos si su dirección IP y MAC están recogidas en la base de datos de *DHCP snooping*. Los comandos para activar esta funcionalidad son:

awplus(config)# interface <port-list>

awplus(config-if)# arp security

199. Por defecto, si se detecta un intento de suplantación en uno de los interfaces donde '*ARP security*' está activado, simplemente se hace una entrada en los log del equipo, pero se puede configurar para que si se detecta un paquete de este tipo se envíe un *trap SNMP* al gestor o incluso apagar el puerto:

awplus(config)# interface <port-list>

awplus(config-if)# arp security violation trap

awplus(config-if)# arp security violation link-down

5.40 CONFIGURACIÓN DE *RAPID SPANNING TREE* (802.1W)

200. 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 la red. Para evitar esta situación se produce un intercambio constante de información entre *switches*. La información se envía en tramas *Ethernet* conocidas como *Bridge Protocol Data Units* (BPDUs).

201. El funcionamiento de RSTP se basa en la elección del *root*. Esta se realiza mediante el intercambio en las BPDUs 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 *switch* que tiene el valor más bajo de toda la red se elige como '*root*'.

202. El *switch* 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 bloqueara de manera que esos enlaces puedan permanecer abiertos). Por tanto, es importante que el *root* de una red con RSTP sea el punto hacia o desde donde más tráfico se origine.

203. 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, es necesario utilizar otras herramientas para evitar que alguien pueda modificar a voluntad la topología de STP. Dichas herramientas son detalladas a continuación.

5.41 *SPANNING-TREE PORTFAST*

204. 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 *switch* 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 se conecta el nuevo equipo y se habilita la comunicación con el resto de la red, se pueden configurar como *portfast* aquellos puertos en los que no se van a conectar más *switches* que formen parten de la topología de RSTP, solo estaciones de trabajo o dispositivos de usuarios finales. Los comandos a utilizar son:

awplus(config)# interface <port-list>

awplus(config-if)# spanning-tree portfast

205. El uso de esta funcionalidad no supone que el *switch* deje de ser capaz de detectar un bucle, ya que un puerto configurado como *portfast* envía BPDUs y, tan pronto recibe una BPDU deshabilita *portfast,* pasa a comportarse como un puerto de RSTP que no tiene *portfast* configurado. 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.

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

5.42 SPANNING TREE ROOT GUARD

207. Cuando se configura un puerto como '*root guard',* hay que asegurarse 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 y altere la topología deseada. Para configurar un puerto como *Root guard,* se usan los comandos:

awplus(config)# interface <port-list>

awplus(config-if)# spanning-tree guard root

5.43 SPANNING-TREE PORTFAST BDPU-GUARD

208. Otra opción para proteger la topología deseada es utilizar '*bpdu-guard*'. Si un puerto configurado como '*bpdu-guard*' recibe una BPDU cualquiera, el puerto es automáticamente apagado. Para configurar un puerto para que sea apagado tan pronto como reciba una BPDU, se pueden utilizar los siguientes comandos:

awplus(config)# interface <port-list>

awplus(config-if)# spanning-tree portfast bpdu-guard enable

209. Una vez que un puerto ha sido apagado al recibir una BPDU, por defecto, permanece en ese estado durante 300 segundos. Si se necesita recuperarlo antes, se puede utilizar el comando '*no shutdown*' para volver a tener este puerto operativo y si se quiere modificar el tiempo que el puerto permanece apagado una vez que recibe una BPDU, se utiliza el comando:

awplus(config)# spanning-tree errdisable-timeout interval <10-1000000>

5.44 SEGURIDAD 802.1X

210. El estándar 802.1x proporciona un método de restringir el acceso a redes basado en la información de autenticación. 802.1x proporciona control de acceso a la red basado en puerto para los dispositivos conectados a una red Ethernet. Esto permite que un dispositivo controlador (el *switch*) restrinja qué dispositivos externos podrán acceder a la red conectándose en un puerto controlado mediante 802.1x. Los dispositivos externos que deseen acceder a los servicios a través de un puerto bajo control de 802.1x deben, en primer lugar, autenticarse y obtener la autorización antes de que el puerto controlado por 802.1x envíe cualquier paquete procedente de, o con destino al dispositivo externo.

5.45 COMPONENTES DE UN SISTEMA 802.1X

211. Los tres (3) componentes principales de un sistema de control de autenticación por puerto 802.1x se recogen en la siguiente tabla e imagen:

Componente	Función
Authenticator	El dispositivo que permite el acceso a los servicios que tiene accesibles detrás de él. En este ejemplo, un *switch* que tiene el control de autenticación 802.1x por puerto habilitado.
Supplicants	El cliente que desea acceder a los servicios ofrecidos por el sistema autenticador.
Authentication server	El dispositivo que utiliza las credenciales de autenticación suministrados por el solicitante, para determinar si el autenticador debe permitir el acceso a los servicios disponibles

Tabla 11: Descripción de los componentes de un sistema 802.1X

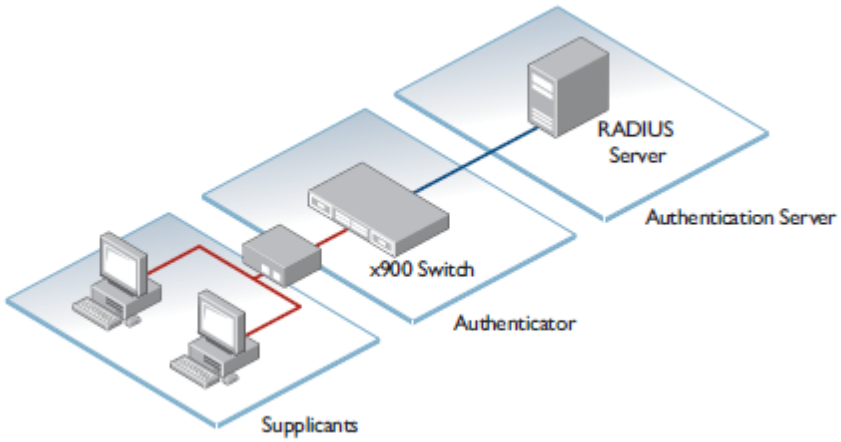


Ilustración 4. Componentes de un sistema 802.1X

5.46 CONFIGURACIÓN DEL *SWITCH* COMO AUTENTICADOR

212. Primeramente, se configura el servidor RADIUS al que se envíen las peticiones de autenticación que se reciban de los distintos clientes. Por ejemplo, para configurar un servidor RADIUS con dirección IP: 192.168.1.250 y utilizar como contraseña '*clave-radius*', se introduce el siguiente comando:

awplus(config)# radius-server host 192.168.1.250 key clave-radius

213. A continuación, se indica al módulo de 802.1x (dot1x) que utilice el servidor RADIUS configurado:

awplus(config)# aaa authentication dot1x default group radius

214. Por último, se configuran aquellos puertos donde se quiere habilitar el control de autenticación 802.1x por puerto. Si RSTP está habilitado en esos puertos se recomienda habilitar portfast para evitar los problemas que se describen en el párrafo 200 y que estos nos provoquen incidencias durante el proceso de autenticación

awplus(config)# interface <port-list>

awplus(config-if)# dot1x port-control auto

awplus(config-if)# spanning-tree portfast

5.47 CONFIGURACIÓN DEL *SWITCH* COMO RADIUS SERVER

215. Además de su uso como autenticador en una red que implementa seguridad 802.1x, para controlar el acceso a los recursos de la red, los *switches* con sistema operativo AW+ incorporan también la funcionalidad de RADIUS server interno, lo que les permite actuar también como servidores RADIUS de una red con seguridad 802.1x

216. Para habilitar el servidor RADIUS local, se utilizan los comandos:

awplus(config)# radius-server local

awplus(config-radsrv)# server enable

217. Después, se deben definir los *switches* que van a acceder a este servidor RADIUS para hacer consultas sobre las peticiones de autenticación que reciban de los clientes. Por ejemplo, para definir un *switch* cuya IP es 192.168.1.45 como autenticador (NAS) y que utilice como palabra clave '*clave-radius*', se utilizará el comando:

awplus(config-radsrv)# nas 192.168.1.45 key <radius-secret>

218. Y por último, es necesario definir los usuarios (y sus contraseñas) para los que se permitirá el acceso a la red, con el comando:

awplus(config-radsrv)# user <name1> password <password1>

awplus(config-radsrv)# user <name2> password <password2>

5.48 MULTIPLES CLIENTES POR PUERTO

219. Por defecto, los *switches* con AW+ solo permiten a un único cliente autenticarse en cada puerto, sin embargo, se puede modificar este comportamiento para uno o varios puertos, con el siguiente comando:

awplus(config)# interface <port-list>

awplus(config-if)# auth host-mode {single - supplicant | multihost| multi-supplicant}

220. Los distintos modos y su significado se recogen en la siguiente tabla:

Host-Mode	Descripción
Single-supplicant	Con esta opción, solo un cliente puede ser autenticado por puerto. Una vez que el cliente ha sido autenticado, ningún otro cliente puede ser autenticado hasta que la sesión del primer cliente se ha cerrado.
Multihost	Con este modo, una vez que el primer cliente ha sido autenticado en ese puerto todos los demás clientes o nodos conectados a través de ese puerto tienen permitido el acceso sin necesidad de ser autenticados. Este modo a veces se conoce como *piggy-back*.
Multi-Supplicant	Con este modo, múltiples clientes pueden y deben ser autenticados en cada uno de los puertos para obtener acceso a los recursos de la red.

Tabla 12: Distintos modos de acceso de clientes a puertos

5.49 AUTENTICACIÓN POR DIRECCIÓN MAC

221. La autenticación mediante 802.1x requiere como se ha visto en párrafos anteriores la acción de un cliente que envíe las credenciales de acceso al autenticador, que a su vez las enviará al servidor RADIUS para comprobar si ese usuario está definido y por tanto debe darle acceso o no.

222. Por desgracia, aunque cada vez es más habitual ver que van incorporando clientes 802.1x en sus últimas versiones, hay muchos dispositivos que no disponen de clientes de 802.1x como pueden ser: impresoras, teléfonos, cámaras IP, etc, y por tanto para permitirles el acceso a la red habría que conectarlos a puertos que no tuviesen 802.1x activo, lo que supone un agujero de seguridad importante.

223. Para evitarlo, los *switches* con sistema operativo AW+ permiten habilitar la autenticación por MAC en esos puertos donde se necesita conectar dispositivos que no dispongan de cliente 802.1x.

224. La idea es que cuando en un puerto se habilita autenticación por puerto, el *switch* manda una consulta de autenticación cuyo nombre de usuario y contraseña son la dirección MAC del dispositivo que se ha conectado en ese puerto. Por tanto, si en

el servidor RADIUS definido se ha definido un usuario/contraseña correspondiente a la MAC del dispositivo al que se quiere dar acceso a la red este quedará autenticado y podrá comunicarse por tanto con el resto de la red.

225. Del mismo modo que al configurar autenticación por 802.1x, si RSTP está habilitado en los puertos donde se quiere configurar autenticación por MAC, se recomienda habilitar *portfast* para evitar los problemas descritos en 5.41 *SPANNING-TREE PORTFAST* y que estos nos provoquen incidencias durante el proceso de autenticación. Para habilitar autenticación por MAC, lo primero es definir el método de autenticación que se utiliza para esta autenticación, con el siguiente comando se indica que use el servidor RADIUS creado anteriormente:

awplus(config)# aaa authentication auth-mac default group radius

226. Para habilitar autenticación por MAC en uno o varios puertos, se usan los siguientes comandos:

awplus(config)# interface <port-list>

awplus(config-if)# auth-mac enable

awplus(config-if)# spanning-tree portfast

227. Además, esta configuración para autenticación por MAC puede convivir en un mismo puerto con la autenticación por 802.1x. Esto da la flexibilidad de poder conectar en esos puertos equipos que soportan 802.1x o no, indistintamente. Cuando un equipo se conecta en un puerto que tiene configurados ambos métodos de autenticación, el *switch* intentará primero hacer la autenticación por MAC y, si no existe usuario definido con esa MAC en el RADIUS configurado para hacer la consulta, iniciará el intento de autenticación 802.1x con las credenciales aportadas por el cliente, si el dispositivo conectado a ese puerto las aporta. En caso de que ambos procesos fallen, el puerto permanecerá como no autorizado y, por tanto, sin conectividad a la red.

6. FASE DE OPERACIÓN

228. El correcto funcionamiento del producto requiere de aspectos que deben tenerse en cuenta. Es responsabilidad del administrador asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

- Los administradores deben estar correctamente formados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías y recomendaciones de seguridad.
- Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de *firmware* y *software* para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
- Se deberán realizar copias de seguridad periódicas para asegurar que no se pierde información.
- Se deberán revisar periódicamente los *logs* del dispositivo para verificar su correcto funcionamiento y uso.

7. CHECKLIST

229. La siguiente *checklist* contiene el listado de los aspectos de seguridad que se deben tener en cuenta para hacer un uso seguro del producto.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto.	☐	☐	
CONFIGURACIÓN			
Configuración usuario por defecto	☐	☐	
Creación política de contraseñas	☐	☐	
Deshabilitar puertos no utilizados	☐	☐	
Habilitar el modo de operación seguro	☐	☐	
Configuración del nivel de seguridad del BOOT	☐	☐	
Configuración segura de interfaces y servicios.	☐	☐	
Habilitar y configurar NTP	☐	☐	
Configuración de certificados para TLS	☐	☐	
Seleccionar y configurar SNMPv3	☐	☐	
Añadir servidor externo Syslog	☐	☐	
Creación de VLANS	☐	☐	
OPERACIÓN			
Monitorizar los registros de auditoría.	☐	☐	
Chequear con regularidad la disponibilidad de nuevas actualizaciones de seguridad. Instalar en caso de que existan.	☐	☐	

8. REFERENCIAS

REF1 Command Reference: x930 Series Switches Running AlliedWare Plus Version 5.5.0
https://www.alliedtelesis.com/sites/default/files/documents/manuals/x930_command_ref_550-0.pdf

REF2 *Bootloader and Startup Feature Overview and Configuration Guide*
https://www.alliedtelesis.com/sites/default/files/documents/feature-guides/bootloader_feature_config_guide_reva.pdf

REF3 *Licensing – Feature overview and Configuration Guide*
https://www.alliedtelesis.com/es/documents/licensing-feature-overview-and-configuration-guide

REF4 *Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.*
https://www.alliedtelesis.com/es-es/documents/public-key-infrastructure-feature-overview-and-configuration-guide

REF5 *High Availability Feature Overview and Configuration Guide.*
https://www.alliedtelesis.com/es/documents/high-availability-feature-overview-and-configuration-guide

REF6 *Logging and Debug Feature Overview and Configuration Guide.*
http://www.alliedtelesis.com/documents/logging-feature-overview-and-configuration-guide

9. ABREVIATURAS

ACL	*Access Control List*
ARP	*Address Resolution Protocol*
BDPU	*Bridge Protocol Data Units*
CA	*Certification Authority*
CLI	*Command Line Interface*
CPU	*Central Processing Unit*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denial off Service*
ENS	Esquema Nacional de Seguridad.
GUI	*Graphical User Interface*
HTTP/S	*Hypertext Trasfer Protocol/Secure*
ICMP	*Internet Control Message Protocol*
LLDP	*Link Layer Discovery Protocol*
NTP	*Network Time Protocol*
PKI	*Public Key Infraestructure*
RAM	*Random Access Memory*
SNMP	*Simple Network Management Protocol*
SSH	*Secure SHell*
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transfer Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
VTY	*Virtual TeletYpe*

PUBLICACIONES DE DEFENSA

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