centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1480

Procedimiento de Empleo Seguro
ArubaOS 16.11 (HPE 2930F, 2930M, 3810M, 5400R Series)

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.26 08:51:02 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. AOS-S Switch es una familia de equipos Aruba, para conmutación y enrutamiento de redes Ethernet, comúnmente conocidos como switches (aun cuando sean equipos que presten funciones de L2, L3 y capas superiores en algunos aspectos).
2. Esta familia de equipos cubre necesidades desde acceso, equipos de agregación y equipos Datacenter.
3. La plataforma de conmutación AOS-S Switch, impulsada por el sistema operativo de red AOS-S, simplifica las operaciones de red ofreciendo automatización, seguridad y alta disponibilidad a las redes de campus y centros de datos.
4. Los equipos de AOS-S Switch se han dotado de sólidos elementos de seguridad.
5. También han sido diseñados para poder ser explotados desde entornos locales (on-premise) y desde la cloud pública (Aruba Central, modalidad SaaS).

2 OBJETO Y ALCANCE

6. El propósito de este documento es proporcionar directrices de seguridad y mejores prácticas para las características y protocolos de gestión proporcionados por el software AOS-S, y presentar configuraciones de ejemplo para ilustrar estas mejores prácticas en acción.

7. Este documento, por tanto, pone foco en las funcionalidades que pueden ser relevantes para una configuración segura del equipo, y que este no sea un vector de ataque. No pretende ser una guía de referencia completa de las características y comandos enumerados. Por lo que se recomienda que, para ampliar el conocimiento y otras opciones de configuración, así como otra información adicional obtenga el último conjunto de manuales del software en el Portal de Soporte de Aruba [REF2].

8. Este documento describe mecanismos y funcionalidades relacionadas con los siguientes equipos de la familia de switches/routers AOS-S Switch.

   - Equipos Datacenter
     - Aruba HPE 5400R Switch Series
   - Equipos Campus
     - Aruba HPE 2930F Switch Series
     - Aruba HPE 2930M Switch Series
     - Aruba HPE 3810M Switch Series

9. Los equipos mencionados han sido incluidos en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte [REF13].

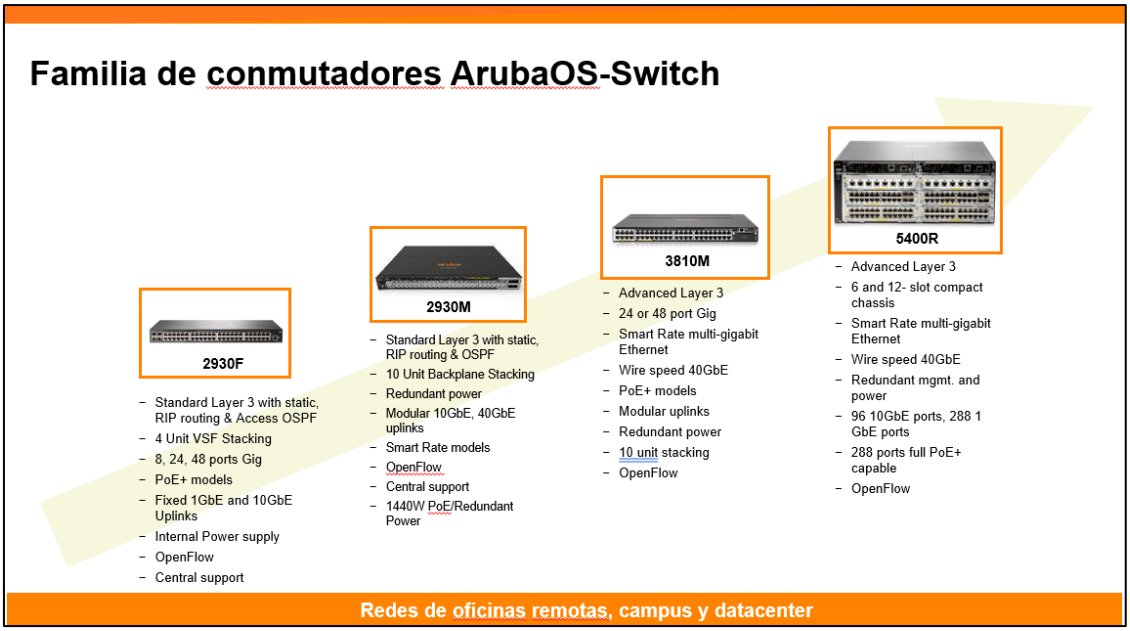

Ilustración 1. Familia de Equipos Aruba-CX

10. Como se verá en el documento, el equipo puede ser configurado de diferentes maneras. En este documento se describen los comandos y funcionalidades que proporcionan la configuración segura del mismo.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4 En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Los equipos AOS-S Switch son dispositivos físicos que deben llegar al lugar de recepción perfectamente embalados y cerrados. Deben ir acompañados de un albarán de entrega que identifique los componentes contenidos en el envío. Debe comprobarse que las cajas vengan cerradas y sin ningún tipo de daño.
12. Hay que tener en cuenta que algunos componentes del equipo pueden llegar en cajas separadas. Es necesario verificar que todos los componentes recibidos corresponden con el equipamiento pedido, para ello se verificarán los números de serie y MACs de los equipos entregados con los indicados en el documento “packing list” adjuntado con la entrega de material y con la factura electrónica (en la que se detallan los números de serie) enviada por el mayorista.
13. Todos los equipos, así como sus componentes que puedan venir embalados en cajas separadas, son perfectamente identificables mediante una etiqueta donde aparecen, entre otra información, el código del equipo o componente y el número de serie del equipo o componente.
14. En el caso en que los equipos vayan a ser administrados desde la nube, el cliente recibirá o habrá recibido en previas adquisiciones una licencia electrónica con los códigos de licencia de dispositivos en Aruba Central. Para asignar los equipos recibidos a su tenant de Aruba Central debe añadir el número de serie y la dirección MAC de cada uno de ellos en el inventario de dispositivos de HPE Greenlake [REF12]. Una vez añadidos al inventario es necesario asignar una licencia de dispositivo a cada uno de ellos.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. Los equipos AOS-S Switch cubren una amplia gama de escenarios de trabajo, desde equipos de acceso para usuarios o equipos de acceso para servidores en Centros de Proceso de Datos (CPD). El acceso físico al dispositivo debe cumplir con las medidas físicas, control de acceso, etc, exigidas por la normativa correspondiente del ENS.
16. El lugar de instalación de la mayor parte de equipos objeto del PES será típicamente un rack aunque hay un modelo de equipo 2930F de 12 puertos que puede instalarse en una superficie plana. El detalle de los entornos de montaje soportados se describe en la guía de instalación específica de cada equipo [REF7][REF8][REF9][REF10].

4.3 REGISTRO Y LICENCIAS

17. Los equipos de HPE Aruba de la gama AOS-S Switch no necesitan ser registrados para disponer de su funcionalidad. No obstante, se recomienda registrar los productos para disfrutar de todas las ventajas y facilidades que le brinda la posesión de un equipo (notificaciones de seguridad, acceso a recursos como cliente, formaciones específicas para clientes registrados, etc).
18. Si se ha contratado el soporte del equipo, es necesario registrar ese soporte y los equipos bajo soporte en la plataforma **Portal de soporte de Aruba** [REF2].

19. Como parte del contrato de soporte, se requiere que el partner de Aruba a través del cual se ha realizado la venta registre los números de serie del producto y que la ubicación de instalación se proporcione a Aruba.
20. El acceso a **Networking Support HPE** (NSP) requiere disponer de una cuenta. Para crear una cuenta en NSP, hay que navegar a: Portal de soporte de Aruba [REF2] : Account Login -> Create an Account
21. Es conveniente que los miembros de la organización con responsabilidad en la operación de los equipos dispongan de una cuenta en NSP para poder disponer de información relativa a parches, versiones de firmware así como para la apertura de casos de soporte.
22. Para obtener una demostración detallada sobre cómo crear una cuenta NSP, se puede consultar el siguiente enlace: Portal de soporte de Aruba [REF2] . La creación de una cuenta en NSP puede tardar hasta un día laboral por motivos de chequeo de la información.
23. **Networking Support HPE** proporciona las siguientes capacidades.

- Gestión de casos en línea
- Solicitar autorizaciones de devolución de materiales (RMA)
- Acceso a software, corrección de errores
- Acceso a la documentación del producto
- Acceso a base de conocimientos y Airheads en línea
- Aruba Solution Exchange para asistencia en la configuración
- Información sobre licencias
- Fechas de End of Support de los productos y software.

4.4 CONSIDERACIONES PREVIAS

24. Antes de la instalación del equipo conviene tener en cuenta las siguientes consideraciones.

- Respecto de la alimentación del equipo, es conveniente que, en el caso de disponer de más de una fuente de alimentación, estas se conecten a líneas de alimentación diferentes dentro del rack. Si las fuentes de alimentación están conectadas a diferentes líneas de alimentación de CA, se puede suministrar energía redundante en caso de pérdida de una de las líneas de alimentación de CA. Ver: HP 5400R zl2 Switches Installation and Getting Started Guide Power over Ethernet [REF10] pag 2-12
- Conviene también tener en cuenta si el equipo se va a montar en modo chasis virtual o stack VSF. En estos casos hay que prever la distancia máxima a la que se podrán instalar los equipos que dependerá del tipo de interfaz utilizado para la comunicación entre ambos equipos (interfaz RJ-45, interfaz óptico, cables DAC, …).
- Es importante también conocer el método elegido para la configuración inicial del equipo de cara a preparar las conexiones de consola o fuera de banda. En la sección 6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA se describen los diferentes métodos de configuración posibles.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

25. Los equipos pueden ser gestionados por dos formas:

- Gestión Local o *On-premise*. Se trata de gestionar el equipo de forma tradicional, mediante acceso al equipo por consola, sesión remota CLI, o por interfaz gráfico HTTPS. También pueden usarse aplicaciones con protocolos de gestión como SNMP o SSH.
- Gestión Nube o *Cloud.* Esta gestión se realiza mediante la aplicación *Aruba Central*, en modalidad Software-as-a-Service (SaaS).

4.5.1 ARUBA CENTRAL

26. Aruba Central es una plataforma que permite muchas funcionalidades, destacando entre ellas:

    - Configuración
    - Monitorización
    - Perfilado de clientes finales
    - Actualización de Firmware
    - Monitorización proactiva con motor basado en Inteligencia Artificial

27. Para el funcionamiento de Aruba Central es necesaria una licencia por equipo AOS-S Switch que se vaya a monitorizar.

28. El funcionamiento se basa en que el equipo intenta conectar con Aruba Central. En el caso que exista una licencia para el equipo, se establecerá una sesión segura SSL. Dicha sesión es iniciada siempre por el dispositivo.

29. Los puertos con los que el equipo se comunica con Aruba Central se detallan en [REF11] “Opening Firewall ports for Device Communication”.

5 FASE DE INSTALACIÓN

30. Los equipos se proporcionan con sistema operativo. La configuración inicial y actualización de firmware se cubre en la sección 6 FASE DE CONFIGURACIÓN.

31. Respecto a la instalación física del equipo, siga los manuales correspondientes de cada modelo [REF7][REF8][REF9][REF10]

5.1 PRECAUCIONES DE INSTALACIÓN

32. Para evitar lesiones personales o daños al producto al instalar el equipo, es necesario leer las precauciones y pautas de instalación [REF7][REF8][REF9][REF10]

- No montar el equipo en una pared, sobre o debajo de una mesa, o sobre o debajo de cualquier otra superficie horizontal.
- Instalar los dispositivos en un bastidor o armario lo más bajo posible. Colocar los dispositivos más pesados en la parte inferior y los dispositivos progresivamente más livianos instalados arriba.
- Para evitar que el bastidor o armario se vuelva inestable y / o se caiga, verificar que esté adecuadamente asegurado.
- Verificar que los circuitos de la fuente de alimentación estén debidamente conectados a tierra. Conectar el equipo a la fuente de alimentación utilizando el cable de alimentación suministrado con el interruptor.
- Si la instalación requiere un cable de alimentación diferente al suministrado con el equipo y la fuente de alimentación, verificar que el cable tenga el tamaño adecuado para los requisitos de corriente del equipo. Además, utilizar un cable de alimentación con la marca de la agencia de seguridad que define las regulaciones para cables de alimentación. La marca es la garantía de que el cable de alimentación se puede utilizar de forma segura con el equipo y la fuente de alimentación.
- Al instalar el equipo, la toma de CA debe estar cerca del interruptor y ser fácilmente accesible en caso de que el equipo deba estar apagado.
- No instalar el equipo en un entorno donde la temperatura ambiente de funcionamiento exceda la especificación del equipo.
- Verificar que el equipo no sobrecargue los circuitos de alimentación, el cableado y la protección contra sobrecorriente. Para determinar la posibilidad de sobrecargar los circuitos de suministro, sumar los amperios nominales de todos los dispositivos instalados en el mismo circuito que el interruptor. Comparar el total con el límite de clasificación del circuito. Las clasificaciones máximas de amperios generalmente están impresas en los dispositivos cerca de los conectores de alimentación de CA
- Verificar que el flujo de aire alrededor del equipo no esté restringido. Dejar al menos 7,6 cm (3 pulgadas) para que se enfríe. Para la dirección del flujo de aire, determinar si el equipo tiene ventiladores de adelante hacia atrás o de atrás hacia adelante y unidades de fuente de alimentación.
- Todas las fuentes de alimentación y conjuntos de ventiladores instalados en un equipo deben tener la misma dirección de flujo de aire de refrigeración (FB o BF).
- Nunca insertar ni retirar una fuente de alimentación mientras el cable de alimentación esté conectado. Verificar que el cable se haya desconectado de la fuente de alimentación antes de la instalación o desinstalación. Si se debe quitar una fuente de alimentación y luego reinstalarla, esperar al menos 5 segundos antes de la reinstalación.

De lo contrario, se pueden producir daños en el equipo. La fuente de alimentación necesita este tiempo para liberar cualquier energía acumulada.

33. Previamente a la instalación, es necesario chequear que todos los componentes del equipo han llegado correctamente embalados y etiquetados. Una vez abierta la caja del equipo, verificar que junto con el equipo se encuentran:

- Kit de documentación
- Cable de alimentación

34. Es necesario tener en cuenta que, dependiendo del modelo de equipo y del tipo de instalación, se requiere de accesorios de montaje específicos que deben venir bien con el equipo o bien en un embalaje separado.

35. Para proceder a instalar el equipo, se debe seguir el siguiente procedimiento de instalación de manera general. Para la instalación de un modelo específico se dispone de su correspondiente manual de instalación de detalle [REF7][REF8][REF9][REF10].

    a) Preparar el lugar de instalación y asegurar que el entorno físico en el que instalará el equipo esté preparado correctamente, lo que incluye tener el cableado de red correcto listo para conectarse al equipo y tener una ubicación adecuada para el equipo.

    b) Instalar las fuentes de alimentación si aún no están instaladas.

    c) Instalar los conjuntos de ventiladores si aún no están instalados.

    d) Encender el equipo y verificar que los LED’s funcionen correctamente.

    e) Apagar el equipo. Quitar la energía del equipo.

    f) Montar el equipo. El equipo se puede montar en un bastidor de telecomunicaciones de 19 pulgadas o en una cabina de equipos.

    g) Instalar los transceptores si son necesarios. El equipo tiene ranuras para instalar transceptores de tipo SFP/SFP+/QSFP+ dependiendo del modelo de equipo. Dependiendo de dónde instale el equipo, puede ser más fácil instalar los transceptores primero. Los transceptores se pueden intercambiar en caliente; se pueden instalar o quitar mientras el equipo está encendido.

    h) Conectar la alimentación al equipo. Una vez que el equipo esté montado, conectarlo a la fuente de alimentación principal.

    i) Conectar una consola de administración al equipo. Es posible que se desee modificar la configuración del equipo para que pueda administrarse mediante un navegador web o mediante una sesión SSH. Los cambios de configuración se pueden realizar usando un cable de consola para conectar un PC al puerto de consola del conmutador.

    j) Conectar los dispositivos de red. Con los cables de red adecuados, conectar los dispositivos de red a los puertos del conmutador.

36. En este punto, el equipo está completamente instalado.

5.2 PANEL FRONTAL DEL EQUIPO

37. En el panel frontal del equipo existen entre otros, dos botones particulares que, para evitar una pulsación fortuita, estos han de ser pulsados con un elemento metálico (clip o

alambre). Botón etiquetado como "*Reset*" y botón etiquetado como "*Clear*". Ver [REF7][REF8][REF9][REF10] apartado "Reset and Clear Buttons"

- *Clear.* La pulsación de este botón durante al menos un segundo, elimina las contraseñas configuradas en el equipo. A partir de este momento el acceso al equipo se realiza sin contraseña (párrafo 50) hasta que se vuelva a configurar una nueva.
- *Reset.* La pulsación de este botón durante al menos un segundo, resetea el equipo.

38. Es posible realizar otras acciones mediante combinaciones de pulsación de estos botones que se pueden consultar en [REF7][REF8][REF9][REF10] apartado "Reset and Clear Buttons"

5.2.1 BOTON CLEAR FRONTAL

39. Es posible configurar el equipo para que la pulsación de ese botón no elimine las contraseñas. Se recomienda desactivar el botón si no es posible controlar el acceso físico al equipo.

SECUENCIA DE CONFIGURACIÓN	(DES)ACTIVAR LA FUNCIONALIDAD DEL BOTÓN CLEAR
Comandos necesarios	`[no] front-panel-security password-clear [reset-on-clear]`
Verificación de la funcionalidad en operación	`Show front-panel-security`
Comentarios adicionales	Activa o desactiva la funcionalidad del botón clear. El modificador reset-on-clear permite forzar además que tras la eliminación de las credenciales, se reinicie el equipo.

Tabla 1. Configuración botón clear

5.2.2 RESTAURAR LA CONFIGURACIÓN DE FABRICA

40. El procedimiento de configuración a fábrica hace uso de los botones Clear y Reset frontales [REF7][REF8][REF9][REF10] apartado "Reset and Clear Buttons".

41. Inhabilite este mecanismo si lo desea para evitar que, al acceder físicamente al equipo, se obtenga el control del mismo.

SECUENCIA DE CONFIGURACIÓN	(DES)ACTIVAR LA FUNCIONALIDAD DE CONFIGURACIÓN A VALORES DE FÁBRICA
Comandos necesarios	`[no] front-panel-security factory-reset`
Verificación de la funcionalidad en operación	`Show front-panel-security`
Comentarios adicionales	(Des)Configura la posibilidad de llevar el equipo a estado de fábrica.

Tabla 2. Configuración botón clear

5.2.3 RECUPERACIÓN DE LA CONTRASEÑA

42. En el caso que se hayan perdido las credenciales del equipo, es posible obtener una contraseña de un solo uso (one-time contraseña) contactando con el soporte de *Hewlett Packard Enterprise Aruba*.
43. Este método incluso puede bloquearse si se desea por configuración. En tal caso, la pérdida de credenciales únicamente podría recuperarse restaurando el equipo a fábrica.
44. El procedimiento para evitar el uso de las claves de un solo uso, obtenidas mediante el soporte de HPE Aruba es el siguiente
    a) Pulsar *Clear*
    b) Dentro de los 60 segundos tras pulsar Clear, ejecute el comando "`no front-panel-security password-recovery`"
    c) Pulse Y para verificar
45. Tras ese punto, el equipo no permite la recuperación de contraseñas.
46. En los equipos Aruba 3810M, además es posible seleccionar si esta funcionalidad se incluye o no en la configuración

SECUENCIA DE CONFIGURACIÓN	BLOQUEO DE CONTRASEÑA RECOVERY
Comandos necesarios	`[no] front-panel-security display-in-config`
Verificación de la funcionalidad en operación	`Show front-panel-security`

Tabla 3. Bloqueo de recuperación de la contraseña

5.2.4 PUERTO USB

47. Los modelos que proporcionan un puerto USB pueden ser usados como medio de almacenamiento para desplegar, analizar o copiar configuraciones, o versiones de software.
48. El uso de este puerto puede deshabilitarse vía comandos, activándolo cuando sea necesario y desactivándolo a posteriori.

SECUENCIA DE CONFIGURACIÓN	(Des)Activación puerto USB frontal
Comandos necesarios	`[no] usb-port`
Verificación de la funcionalidad en operación	No disponible.

Tabla 4. Desactivación de puerto USB frontal

5.3 ACCESO AL EQUIPO CON CONFIGURACIÓN DE FABRICA

49. La configuración de los equipos se puede realizar de varias maneras: mediante interfaz de línea de comandos, mediante interfaz web, mediante SNMP y OpenFlow para programaciones de flujos dinámicas.

50. Es importante tener en cuenta cuál es la configuración inicial de un equipo en estado de fábrica:

- ACCESO SIN RESTRICCIONES
- No existe usuario predefinido
- Todos los puertos en modo acceso asociados a la VLAN 1
- VLAN 1 con cliente DHCP activo
- Servicios activos
    - Gestión web
    - Telnet
    - SSH
    - SNMP con community ***public***
    - LLDP

6 FASE DE CONFIGURACIÓN

6.1 INFORMACION PREVIA A LA CONFIGURACION DEL EQUIPO

6.1.1 CONTEXTOS Y LINEA DE COMANDOS

51. Los equipos HPE Aruba con sistema AOS-S Switch son equipos completamente gestionables, es decir, permiten al administrador de red configurar al equipo mediante línea de comandos, así como, por interfaz gráfico.

52. El interfaz gráfico permite solo un conjunto reducido de opciones de configuración dado que tiene más por objeto la monitorización y resolución de incidencias, y algunas funciones básicas de configuración de puertos y enlaces. Por esta razón esta guía se centra en la configuración segura del equipo vía línea de comandos.

53. El acceso a la línea de comandos (CLI) es posible mediante la conexión a la consola, o bien mediante conexión remota vía SSH o telnet (protocolo que no se recomienda utilizar).

54. En AOS-S Switch en la línea de comandos, existen diferentes contextos de configuración. Cada contexto se identifica con un *prompt* específico de la línea de comandos. [REF5] apartado “Switch prompts used in this guide”

55. Nivel Operador:

- Permite esencialmente comandos de troubleshooting e inspección.
- Desde aquí se puede acceder al nivel Manager, mediante el comando “`enable`”.
- El prompt está formado por el nombre del equipo seguido de “`>`”.

56. Nivel Manager:

- Permite control del equipo y todas las acciones administrativas. También permite las acciones de actualización de software.
- Permite el acceso al modo de configuración mediante el comando “`configure`”. Se acepta también, por retrocompatibilidad, el comando “`configure terminal`”.
- El prompt está formado por el nombre del equipo seguido de “#”.

57. Modo de Configuración.

- Permite la alteración de la configuración del equipo.
- La pulsación del carácter “?” ofrece al administrador la lista de opciones posibles de configuración.
- Algunas opciones de configuración suponen entrar en diferentes contextos.
- El prompt está formado por el nombre del equipo seguido de “`(config) #`”. También permite las acciones de actualización de software.

58. Modo de Contexto.

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

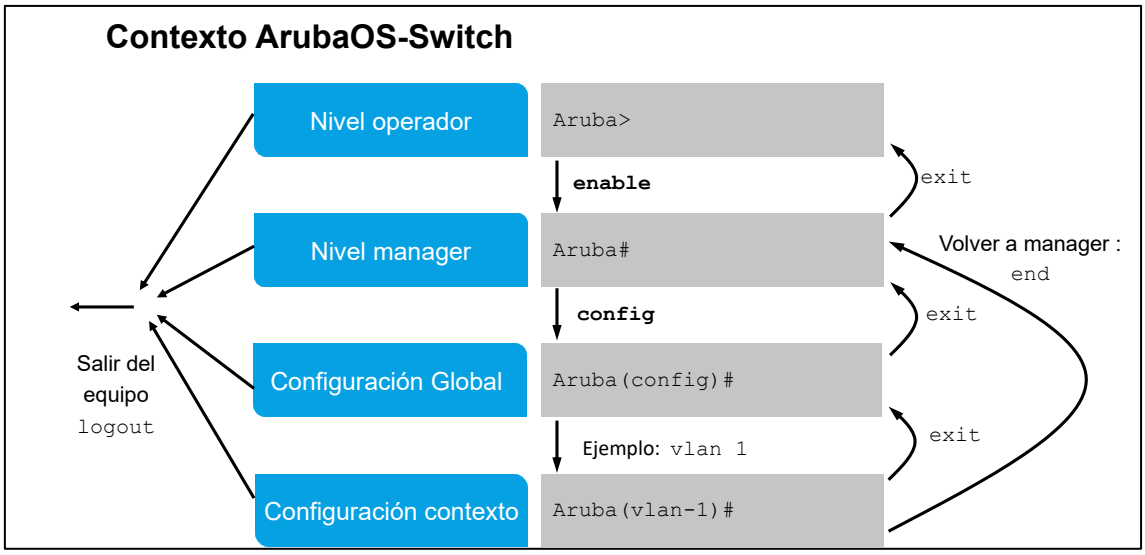

Ilustración 2. Contextos en la línea de comandos en AOS-S Switch

6.1.2 COMANDO MENU

59. Existe el comando "menu" que permite configurar los aspectos más básicos del equipo sin la necesidad de uso de comandos de línea. Es interesante para una configuración inicial.

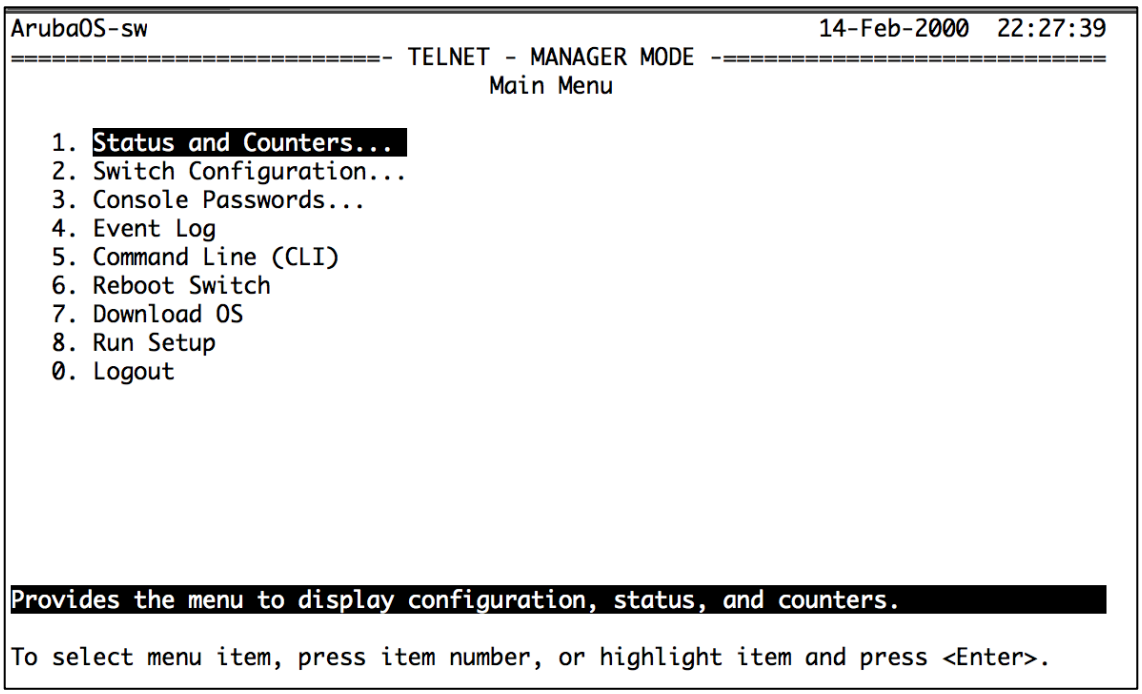

Ilustración 3. Comando menú en AOS-S Switch

60. Es importante destacar que los comandos de inspección "show" pueden ejecutarse en modo configuración.

6.2 MODO DE OPERACIÓN SEGURO

61. La interfaz de línea de comandos o CLI permite la configuración completa de los equipos para regular la funcionalidad y comportamiento de los mismos.

62. De los accesos a la línea de comando, diferenciamos dos tipos de acceso:

- Conexión física directa al equipo – Conexión fuera de banda, mediante conexión al puerto de consola. Este equipo no dispone de puerto USB de consola.
- Conexión lógica y remota al equipo – Esta conexión puede ser en banda mediante conexión remota al equipo utilizando los interfaces de red de servicio, o fuera de banda cuando se conecte al equipo a través del puerto de red de Gestión disponible a tal efecto.

63. En el apartado 6.3 AUTENTICACIÓN se describe cómo administrar el equipo de forma segura.

64. En el apartado 6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS se incluyen las recomendaciones para configurar el plano de datos de forma segura.

6.3 AUTENTICACIÓN

65. Por defecto, y para facilitar la configuración inicial, no hay ninguna autenticación configurada en el equipo.

66. Con la configuración de fábrica cualquier persona con acceso físico a la consola puede acceder al sistema. Por lo tanto, será necesario definir usuarios de acceso al sistema y configurar el acceso de consola para solicitar las credenciales de acceso, acordes a las políticas de seguridad definidas en el apartado 6.4.3.2 POLITICAS DE CONTRASEÑAS.

67. Para los servicios *Console , WebUI y SSH* es posible configurar métodos de autenticación diferentes para el modo login (operator) como para el modo enable (manager)

68. Los métodos de autenticación pueden ser: local (ver apartado 6.4.3.1 AUTENTICACIÓN LOCAL) o remoto (ver apartado 6.6.1 IDENTIDAD DEL EQUIPO: SWITCH IDENTITY PROFILE).

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

6.4.1.1 CLI - CONEXIÓN DIRECTA AL EQUIPO - PUERTO DE CONSOLA (OUT OF BAND)

69. El puerto de consola permite el acceso a todas las funcionalidades del Sistema Operativo funcional, así como a las funcionalidades BootRom del equipo durante la secuencia de arranque.

70. El equipo dispone de puerto de consola en formato RJ45 y en formato mini USB tipo B. Ambos puertos pueden usarse indistintamente. Son dos puertos de la misma conexión lógica.

71. El uso del puerto de consola implica tener conexión con proximidad física al equipo, bien sea de un terminal o de un servidor de terminales.

72. El puerto de consola permite configurar todas las funcionalidades sin excepción.

73. Algunas funciones, como la recuperación de las credenciales del equipo (conocido como procedimiento de *contraseña recovery*) son operativas únicamente desde el puerto de consola.

74. La configuración por defecto del puerto de consola es la siguiente, siendo estos parámetros modificables:

    - Velocidad: auto-sense.
    - Sin control de flujo.
    - Sin paridad.
    - 1 bit de parada.
    - 8 bits de datos.

75. Este puerto con el equipo en estado inicial de fábrica permite el acceso total. Debe configurarse el control de acceso a este puerto.

6.4.1.2 CONEXIÓN REMOTA AL EQUIPO: SSH

76. La gestión en banda permite la conexión al dispositivo utilizando la ruta en la que el control y la gestión de datos comparten la misma red con el flujo normal de tráfico. Utilizar el enfoque de red de gestión en banda tiene sus desventajas. Los datos de administración deben compartir el ancho de banda de red, pese a que los fallos en la red y los recursos pueden provocar que la infraestructura se vuelva imposible de gestionar.

77. Potencialmente, y correctamente configurado, se puede acceder a la interfaz de comandos de manera remota desde un equipo que tenga acceso a la conectividad IP con el equipo.

78. Los protocolos soportados son TELNET y SSH. En ambos casos el equipo se comporta como servidor, siendo necesario para la conexión remota, una aplicación que se comporte como cliente. Es obligatorio:

    - **Desactivar el protocolo TELNET** pues toda la información intercambiada por la sesión remota es enviada en texto plano.
    - Utilizar el protocolo SSH pues toda la información intercambiada por la sesión remota es enviada cifrada.

    IMPORTANTE: En la configuración inicial, o en su ausencia, ambos servicios, Telnet y SSH están habilitados. Es obligatorio realizar la siguiente configuración para desactivar Telnet y configurar SSH para que use una clave RSA de al menos 2048 bits (el tamaño de clave se ajustará a la política criptográfica vigente y a la CCN-STIC 807):

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN SSH Y DESACTIVACIÓN DE TELNET

Comandos necesarios	`crypto key generate ssh rsa bits 2048ip ssh`
	`no telnet-server`
	`idle-timeout 5`

Verificación de la funcionalidad en operación	`show running-config`

Comentarios adicionales	En el comando idle-timeout se propone un tiempo de referencia como 5 minutos para cerrar la sesión por inactivada

Tabla 5. Configuración de SSH y telnet

6.4.1.3 GESTIÓN VIA WEB: HTTPS

79. Es posible configurar y administrar el equipo mediante interfaz web. De nuevo el equipo se comportará como servidor y será necesario el uso de un cliente web.

80. Es obligatorio, en el caso de querer configurar y administrar el equipo vía web:

- **Deshabilitar** el uso de HTTP, habilitado por defecto.
- Securizar el uso de HTTPS, habilitado por defecto.

81. Una vez que el equipo dispone de certificado (ver apartado 6.6 GESTIÓN DE CERTIFICADOS), podemos proceder a configurar el servicio HTTPS:

SECUENCIA DE CONFIGURACIÓN	CONFIGURAR HTTPS Y DESHABILITAR HTTP

Comandos necesarios	`web-management ssl`
	`no web-management plaintext`
	`web-management idle-timeout 300`

Verificación de la funcionalidad en operación	`show snmp-server`
Comentarios adicionales	Se ha propuesto un timeout de 5 minutos a modo de ejemplo. Se recomienda configurar algun valor.

Tabla 6. Configuración Web

6.4.1.4 OPENFLOW

82. OpenFlow es un protocolo de reciente creación. Sin ser el único, es uno de los que ha sido desarrollado con miras a la implementación de soluciones tipo SDN, Redes Definidas por Software (SDN).

83. En las arquitecturas SDN, existen tres capas o niveles funcionales

- Capa de Aplicaciones
- Capa de Control
- Capa Infraestructura de red

84. Este protocolo está diseñado para que la Capa de Aplicación pueda obtener un estado de la red así como poder dar instrucciones a la misma. Esto se realiza a través de APIs.

85. La relación de un dispositivo de red con la Capa de Control, también denominada controladora, puede ser entre otros, por protocolos como OpenFlow.

86. OpenFlow es un protocolo orientado a que la Capa de Control interactúe, conociendo y pudiendo programar flujos de tráfico que el equipo maneja.

87. OpenFlow en su diseño no está pensado para configurar equipos, ni activar funcionalidades, si bien pueda haber implementaciones desnaturalizadas que puedan hacer ese uso, no siendo este el caso de los equipos HPE Aruba.

88. Mediante OpenFlow es posible la configuración de nuevos flujos de comunicaciones o modificar los ya existentes por el funcionamiento normal del switch. Por lo tanto, un acceso no permitido vía este protocolo podría alterar el comportamiento de las comunicaciones.

89. En estado de fábrica del equipo OpenFlow está deshabilitado.

6.4.1.5 ACCESO MEDIANTE API (RESTFULL)

90. Los switches Aruba proporcionan acceso vía una API RESTfull. Esto permite la gestión del equipo, a través de las primitivas que cada versión proporciona.

91. La API utiliza el protocolo HTTP o HTTPS. Por tanto, se configura con los mismos comandos que se regula el acceso HTTP/HTTPS de usuarios. Ver párrafo 81.

92. De la misma forma que el acceso web de usuario, es obligatorio deshabilitar HTTP como método de acceso, y usar HTTPS.

93. La forma de activar/desactivar el acceso API es con este comando:

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE LA REST FULL API
Comandos necesarios	`[no] rest-interface`
Verificación de la funcionalidad en operación	`show rest interface`

Comentarios adicionales	Ejemplo de
	`2930F-mesa# show rest-interface`
	`REST Interface - Server Configuration`
	`REST Interface : Enabled`
	`REST Operational Status : Up`
	`REST Session Idle Timeout : 600 seconds`
	`HTTP Access : Enabled`
	`HTTPS Access : Enabled`
	`SSL Port : 443`

Tabla 7. Configuración de la REST full API

94. El acceso API se debe realizar cumpliendo los siguientes requisitos:

- Utilizar HTTPS. Deshabilitar el uso de HTTP
- Usuario dedicado para API. Dado que la API se recomienda usar HTTPS, el procedimiento de acceso requiere autenticación (usuario y contraseña). Se requiere que estas credenciales sólo sean usadas por la aplicación, para un mejor control del acceso.
- Generar una entrada de conexión en el comando “ip authorized-manager” para el acceso de la máquina que use la API (ver apartado 6.4.1.7 ORIGENES PERMITIDOS DE CONEXIÓN REMOTA).

6.4.1.6 VLAN DE GESTION SEGURA

95. La VLAN de gestión segura está diseñada para restringir el acceso a la gestión desde aquellos equipos que están conectados a esa VLAN. Esto es, sólo los clientes que estén conectados a puertos que son miembros de la VLAN de gestión podrán tener acceso al equipo para gestión. Esto restringe el acceso a la gestión significativamente.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE VLAN
Comandos necesarios	`management-vlan < vid | vlan-name >`
Verificación de la funcionalidad en operación	`show config`
Comentarios adicionales	Solo una VLAN por equipo puede ser configurada. La dirección IP de gestión ha de ser estática. IGMP no puede ser asignado. Routing a la management VLAN no puede ser activado. Esto hace que se comporte como un puerto fuera de banda.

Tabla 8. Configuración de la VLAN

6.4.1.7 ORIGENES PERMITIDOS DE CONEXIÓN REMOTA

96. En los casos en los que la configuración de la VLAN segura de Gestión requiera ser muy restrictiva, podemos restringir hasta 10 IP o rangos de IPS desde los cuales el equipo atenderá las peticiones de conexión.

97. Es posible filtrar los siguientes métodos de conexión: ssh, telnet, web, snmp y tftp. No se deben habilitar aquellos asociados a protocolos inseguros, como Telnet o TFTP.

98. El acceso tipo web también incluye el acceso mediante la API REST.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE VLAN SEGURA DE GESTIÓN
Comandos necesarios	`ip authorized-manager <IP address> mask <mask bits> <operator|manager> method [all|ssh|telnet|web|snmp|tftp]`
Verificación de la funcionalidad en operación	`show config`
Comentarios adicionales	Además del origen No protege contra IP-spoofing. Se recomienda activar protecciones de contraseñas. Para un origen dado, es posible configurar el nivel máximo de acceso que se le permite, *operator* o *manager*.

Tabla 9. Configuración de la VLAN segura de gestión

6.4.1.8 FILTRADO MEDIANTE ACL

99. También es posible filtrar las conexiones remotas al equipo mediante el uso de las listas de acceso tradicionales. Ver apartado 6.5.2.4 PROTECCIÓN DEL PLANO DE CONTROL.

100. Es importante recordar que las listas de acceso tienen una denegación implícita final, por eso en el caso de que apliquemos una con el fin de restringir el tráfico de gestión nos aseguremos de permitir el tráfico de usuario final.

6.4.2 GESTIÓN DEL EQUIPO POR SNMP

101. SNMP es el protocolo de intercambio de información de gestión entre la plataforma de gestión y los equipos gestionados.

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

- Generación de alarmas o eventos, llamados traps. Iniciado por el dispositivo, a una o varias estaciones gestoras de la red. Notifican eventos o situaciones sufridas en el seno o en el entorno del equipo (por ejemplo, caída de un enlace o de un exceso de temperatura).
- Diálogo o interrogación. La estación gestora, con las correspondientes credenciales, interroga o manda información al equipo (por ejemplo, al consultar el valor de paquetes transmitidos por una interfaz).

103. El método utilizado, tanto en los traps como en el modo diálogo, es mediante el uso de MIBs (Management Information Base). Estas definiciones de información pueden tener un carácter público o propietario.

104. Actualmente existen tres versiones del protocolo SNMP. El equipo soporta la versión SNMP v3, que es la requerida pues proporciona mecanismos de seguridad y control de la información accedida.

105. Se requiere deshabilitar la comunidad SNMP por defecto, así como desactivar la funcionalidad SNMPv2:

SECUENCIA DE CONFIGURACIÓN	DESACTIVAR LA COMUNIDAD SNMPv2
Comandos necesarios	`no snmp-server enable` `no snmp-server community public`
Verificación de la funcionalidad en operación	`show snmp-server`
Comentarios adicionales	

Tabla 10. Desactivar la comunidad SNMPv2

106. En el caso que el gestor de la red sólo trabaje con SNMPv2, recomendamos el modo restringido el cual sólo puede hacer lecturas, pero no escrituras.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE SNMPv2 EN MODO RESTRINGIDO
Comandos necesarios	`snmp-server enable` `snmp-server community public operator restricted`
Verificación de la funcionalidad en operación	`show snmp-server`
Comentarios adicionales	

Tabla 11. Configuración de SNMPv2 en modo restringido

107. La configuración de SNMPv3 se hace en 4 pasos

a) Habilitar SNMPv3

b) Configurar los usuarios permitidos

c) Configurar las comunidades SNMPv3

d) Configurar los receptores de traps SNMP

108. En esta sección se presentan los comandos más básicos. La configuración SNMPv3 puede ser compleja. Se recomienda consultar la guía [REF5] "HPE Aruba Networking 2930M/F Management and Configuration Guide 16.11" apartado "Using SNMP tools to manage the switch" del Capítulo 7 para ampliar detalles.

109. Habilitar SNMPv3. Cuando se configura por primera vez, genera un menú interactivo.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE SNMPv3
Comandos necesarios	`snmpv3 enable`
Verificación de la funcionalidad en operación	`show snmpv3 enable`

Paso 1	Cuando se activa por primera vez genera interacción y se crea un usuario "initial" con Auth MD5 y Cifrado DES que debe ser borrado tras realizar la configuración:
	
	`switch(config)# **snmpv3 enable**`
	`SNMPv3 Initialization process.`
	`Creating user 'initial'`
	`Authentication Protocol: MD5`
	`Enter authentication contraseña: ********`
	`Privacy protocol is DES`
	`Enter privacy contraseña: ********`
	`User 'initial' has been created`
	`Would you like to create a user that uses SHA? [y/n] n`
	
	`User creation is done. SNMPv3 is now functional.`
	
	`switch(config)# **no snmpv3 user initial**`

Paso 2	Crear usuario SNMPv3 que utilizando protocolos seguros: `switch(config)# snmpv3 user snmpv3user auth sha xxxxx priv aes xxxxxxx`

Tabla 12. Configuración de SNMPv3

110. Para configurar los usuarios permitidos, es necesario primero crearlos y luego asignarlos a grupos. Existen 8 grupos predefinidos en los equipos con diferentes niveles de privilegio. Al asignar un usuario a un grupo se le asignan los permisos del grupo. Para consultar el listado de grupos con sus permisos mirar Tabla 19 de [REF5] "HPE Aruba Networking 2930M/F Management and Configuration Guide 16.11":

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE USUARIOS EN SNMPv3
Comandos necesarios	`[no] snmpv3 user <user_name> auth sha <auth_pass> priv aes <priv_pass>`
Verificación de la funcionalidad en operación	`show snmpv3 user`
Comentarios adicionales	

Tabla 13. Configuración de usuarios en SNMPv3

SECUENCIA DE CONFIGURACIÓN	CREACIÓN DE GRUPOS EN SNMPv3
Comandos necesarios	`[no] snmpv3 group <group_name > user <user_name > sec-model {<ver1 | ver2c | ver3>`
Verificación de la funcionalidad en operación	`show snmpv3 user`
Comentarios adicionales	Ejemplo: `snmpv3 group grupo1 user usuario2 sec-model ver3`

Tabla 14. Creación de grupos en SNMPv3

111. Configurar las comunidades SNMPv3. Estas son necesarias para proporcionar acceso en modo v2c o v1. Recomendamos que si es posible se configuren SNMPv3 y por tanto estas comunidades no se configuren.

SECUENCIA DE CONFIGURACIÓN	CREACIÓN DE COMUNIDADES EN SNMPv3
Comandos necesarios	`[no] snmpv3 community index <index_name> name <community_name> sec-name <security_name> tag <tag_value >`
Verificación de la funcionalidad en operación	`show snmpv3 community`
Comentarios adicionales	Ejemplo:

	snmpv3 community index 30 name gestor sec-name CommunityManagerReadWrite tag MgrStation1

Tabla 15. Creación de las comunidades SNMPv3

112. Configurar los receptores de traps SNMPv3

SECUENCIA DE CONFIGURACIÓN	CREACIÓN DE RECEPTORES TRAPS EN SNMPv3
Comandos necesarios	[no] snmpv3 notify <notify_name > tagvalue <tag_name > [no] snmpv3 targetaddress {< ipv4-addr | ipv6-addr >} <name > [no] snmpv3 params <params_name> user <user_name>
Verificación de la funcionalidad en operación	show snmpv3 community
Comentarios adicionales	

Tabla 16. Creación de receptores traps en SNMPv3

113. Finalmente, es interesante configurar notificaciones de Seguridad para eventos SNMP

SECUENCIA DE CONFIGURACIÓN	CREACIÓN DE RECEPTORES TRAPS A ENVIAR EN SNMPv3
Comandos necesarios	[no] snmp-server enable traps [snmp-auth | contraseña-change-mgr | login-failure-mgr | port-security | auth-server-fail | dhcp-snooping | arp-protect | running-configchange]
Verificación de la funcionalidad en operación	show snmpv3 community
Comentarios adicionales	

Tabla 17. Creación de receptores traps a enviar en SNMPv3

6.4.3 CONFIGURACIÓN DE ADMINISTRADORES

6.4.3.1 AUTENTICACIÓN LOCAL

114. Por defecto hay dos tipos de usuarios de acceso a la administración del equipo:, *manager y operator.* En la sección 6.4.3.1.2 Modelo RBAC (Role Based Access Control): se indica como crear más roles de usuarios con accesos más particularizados.

115. Nivel Manager – Acceso total

- Cambios de configuraciones
- Acceso a todos los contextos de configuración del modo enable
- Acceso de lectura y escritura

116. Nivel Operador – Acceso parcial

- Visibilidad de contadores y status, eventos y comandos *show.*
- Acceso a todos los contextos de configuración del modo login
- Acceso de lectura

117. Cada método de acceso al equipo (consola, SSH, telnet, HTTPS, etc) puede ser configurado con dos métodos de autenticación de usuarios. Se muestran los valores de fábrica.

```
Aruba Switch # show authentication
 Status and Counters - Authentication Information
  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Disabled
  Bypass Username For Operator and Manager Access : Disabled
                  | Login       Login         Login
  Access Task     | Primary     Server Group  Secondary
  --------------- + ----------- ------------  ----------
  Console         | Local                     None
  Telnet          | Local                     None
  Port-Access     | Local                     None
  Webui           | Local                     None
  SSH             | Local                     None
  Web-Auth        | ChapRadius  radius        None
  MAC-Auth        | ChapRadius  radius        None
  SNMP            | Local                     None
  Local-MAC-Auth  | Local                     None
                  | Enable      Enable        Enable
  Access Task     | Primary     Server Group  Secondary
  --------------- + ----------- ------------  ----------
  Console         | Local                     None
  Telnet          | Local                     None
  Webui           | Local                     None
  SSH             | Local                     None
```

118. Es importante destacar que, en el comando anterior, las menciones a Port-access (802.1x), Web-Auth y MAC-Auth son funcionalidades de acceso de usuarios a la red, y no al equipo para su administración.

119. En el comando (salida “Login Attempts : 3”) se puede ver que el número por defecto de intentos por sesión es 3.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DEL NÚMERO DE INTENTOS PERMITIDOS PARA LA AUTENTICACIÓN DEL USUARIO
Comandos necesarios	`aaa authentication num-attempts < 1-10 >`
Verificación de la funcionalidad en operación	`show authentication`
Comentarios adicionales	

Tabla 18. Configuración del número de intentos permitidos para la autenticación del usuario

120. Una vez configurados los dos métodos de autenticación, únicamente se usará el segundo en caso de indisponibilidad del primero, no en caso de no estar presente un usuario o denegarse su acceso.

121. Casi todos los tipos de acceso tienen tres métodos de autenticación posibles. Se recomienda el uso de RADIUS o TACACS+ como método de autenticación principal y dejar la autenticación local solo como método de respaldo:

- Local – Usuarios definidos en la configuración del propio equipo
- RADIUS – Utilizando un servidor RADIUS externo
- TACACS+ - Utilizando un servidor TACACS externo

122. Existen dos formas a la hora de definir usuarios:

6.4.3.1.1 Modo Clásico:

123. Este es el modo existente hasta las versiones 15.XX y se sigue manteniendo en las versiones 16.XX (en caso de no activar el otro modo).

124. En este modo, existen dos niveles de usuario: *manager* y *operator.*

125. El usuario tipo *manager* tiene acceso total al sistema, mientras que el usuario tipo *operator* únicamente tiene permisos de lectura.

126. Este modo puede ser usado tanto en autenticación local como externa.

127. En la definición de los usuarios, y en particular de las contraseñas, es relevante considerar la sección relativa al registro de las contraseñas en la configuración, tratado posteriormente en este documento.

SECUENCIA DE CONFIGURACIÓN	CONFIGURACIÓN DE USUARIO LOCAL TIPO MANAGER
Comandos necesarios	`password manager user-name <nombre_usuario> [plaintext|sha1|sha256]`
Verificación de la funcionalidad en operación	`show configuration`
Comentarios adicionales	Es posible introducir la contraseña tanto en texto plano o mediante firma sha1 o sha256. Ejemplo: `password manager user-name admin plaintext aruba123`

Tabla 19. Configuración de usuario local tipo manager

SECUENCIA DE CONFIGURACIÓN	Configuración de usuario local tipo operator
Comandos necesarios	`password operator user-name <nombre_usuario> [plaintext|sha1|sha256]`
Verificación de la funcionalidad en operación	`show configuration`
Comentarios adicionales	Es posible introducir la contraseña tanto en texto plano o mediante firma sha1 o sha256. Ejemplo: password operator user-name operador plaintext aruba123

Tabla 20. Configuración de usuario local tipo operador

6.4.3.1.2 Modelo RBAC (Role Based Access Control):

128. Este modo ha sido introducido en la versión 16.01 y sólo es funcional si se activa.

129. En este modo, se pueden crear perfiles (*roles)* a los cuales se le asignan diversas capacidades para la configuración, inspección y ejecución de comandos relativos a las diversas funcionalidades que ofrece el equipo.

130. Este modo solo funciona con servidores externos de autenticación.

131. Para más detalle de configuración del modelo RBAC consultar [REF3] capítulo RBAC.

6.4.3.2 POLITICAS DE CONTRASEÑAS

132. Tanto los nombres de usuario como las contraseñas son campos sensibles a las mayúsculas y minúsculas.

133. Existen diversos comandos para el control de la calidad de las contraseñas.

- Longitud mínima de la contraseña

SECUENCIA DE CONFIGURACIÓN	Longitud de la contraseña
Comandos necesarios	`password minimum-length <0-64>`
Verificación de la funcionalidad en operación	Estableciendo contraseñas Comando `show password-configuration`
Comentarios adicionales	Establece la longitud mínima de la contraseña, siendo obligatorio un mínimo de 12 caracteres como cumplimiento del ENS. Es necesario una contraseña de manager establecida para activar la funcionalidad Ha de concordar con otros comandos relacionados con las políticas de CONTRASEÑAS.

Tabla 21. Longitud de la contraseña

- Complejidad de la contraseña

SECUENCIA DE CONFIGURACIÓN	Complejidad de la contraseña

Comandos necesarios	`password complexity repeat-char-check`
	`password complexity repeat-password-check`
	`password complexity user-name-check`
	`password complexity all`

Verificación de la funcionalidad en operación	Estableciendo contraseñas Comando `show password-configuration`
Comentarios adicionales	La secuencia anterior configura la verificación cuando se ingresa una contraseña que no cumple unas determinadas condiciones:

	Que la passwod no contenga tres caracteres seguidos repetidos Que la contraseña no coincida con una anterior Que la contraseña no contenga el nombre del usuario Los tres controles anteriores.

Tabla 22. Complejidad de la contraseña

- Composición de la contraseña. De acuerdo con los requisitos de robustez de contraseñas aplicables en el marco del ENS y desarrollados en la CCN-STIC-807, la contraseña deberá combinar al menos 3 de los 4 tipos de caracteres siguientes: letras mayúsculas, letras minúsculas, dígitos numéricos y caracteres especiales.

SECUENCIA DE CONFIGURACIÓN	Composición de la contraseña

Comandos necesarios	`password composition lowercase <2-15>`
	`password composition uppercase <2-15>`
	`password composition specialcharacters <2-15>`
	`password composition number <2-15>`

Verificación de la funcionalidad en operación	Estableciendo contraseñas Comando `show password-configuration`
Comentarios adicionales	La secuencia anterior configura la verificación cuando se ingresa una contraseña respectivamente: • Que la contraseña debe contener un numero entre 2 y 15 letras minúsculas • Que la contraseña debe contener un numero entre 2 y 15 letras mayúsculas • Que la contraseña debe contener un numero entre 2 y 15 caracteres especiales • Que la contraseña debe contener un numero entre 2 y 15 cifras numéricas El valor por defecto para cada uno de los comandos anteriores es 2. Es necesario utilizar al menos 3 de los 4 comandos para cumplir con los requisitos de robustex de contraseñas marcados por el ENS (guía 807).

Tabla 23. Composición de la contraseña

134. El comportamiento del equipo respecto al uso de las contraseñas puede quedar regulado por estos comandos

SECUENCIA DE CONFIGURACIÓN	Configuración del comportamiento de la política de contraseña

Comandos necesarios	`password configuration aging`
	`password configuration aging-period`
	`password configuration alert-before-expiry`
	`password configuration expired-user-login`
	`password configuration history`
	`password configuration history-record`
	`password configuration log-on-details`
	`password configuration update-interval-time`
	`password` **`configuration-control`**

Verificación de la funcionalidad en operación	Estableciendo contraseñas Comando `show password-configuration`
Comentarios adicionales	La secuencia anterior configura la verificación cuando se ingresa una contraseña respectivamente: • `aging` – Habilita la comprobación de expiración de la contraseña • `aging-period` – Configura el periodo de expiración de la contraseña • `alert-before-expiry` – Configura número de dias para aviso de expiración • `expired-user-login` – Configura cuantos logins adicionales son permitidos tras la expiracion • `history` – Habilita la comprobación de la contraseña respecto a anteriores. • `history-record` – Configura el número de contraseña anteriores registradas • `log-on-details` – Configura el mostrar o no el resultado del commando "`show authentication last-login`" • `update-interval-time` – tiempo minimo de espera, que debe aguardarse antes de permitir un cambio de contraseña "contraseña configuration-control" activa o desactiva la funcionalidad.

Tabla 24. Configuración del comportamiento de la política de contraseña

135. ALMACENAMIENTO Y PROTECCIÓN DE CONTRASEÑAS Las contraseñas pueden almacenarse en el fichero de configuración, o bien excluirse del mismo. Esto lo regula el comando "`include-credentials`".
136. En caso de almacenarse en el fichero de configuración, se requiere el cifrado de las mismas, con el comando "`encrypt-credentials`".
137. Además, se requiere la opción de almacenaje en SHA256 que no permite la obtención inversa.
138. La gestión de contraseñas puede consultarse en [REF3] HPE Aruba Networking 2930M/F Access Security Guide 16.11, capítulo 3, Configuring Username and Password

SECUENCIA DE CONFIGURACIÓN	Almacenaje de la contraseñas

Comandos necesarios	`include-credentials`
	`encrypt-credentials`
	`password non-plaintext-sha256`

Verificación de la funcionalidad en operación	Estableciendo contraseñas
	Comandos:
	`show encrypt-credentials`
	`show include-credentials`

Comentarios adicionales	

Tabla 25. Almacenaje de las contraseñas

6.4.3.3 MENSAJE DE ACCESO A LA CONSOLA – BANNER

139. Se recomienda configurar un texto informativo que indique que el acceso no autorizado a este equipo está prohibido. Recomendamos no dar demasiada información en el banner acerca del sistema accedido

SECUENCIA DE CONFIGURACIÓN	Configuración de banner
Comandos necesarios	`banner motd <character delimitador> TEXTO <character delimitador>`
Verificación de la funcionalidad en operación	`Show running-config` Acceso al equipo

Comentarios adicionales	El carácter delimitador no puede ser usado en el texto introducido.
	Los saltos de línea aparecen como Se trata de un comando interactivo cuando se introduce via CLI.
	Ejemplo usando el carácter % como delimitador
	`switch(config)# banner motd %`
	`Enter TEXT message. End with the character '%'`
	`Este es un Sistema privado.`
	`Abandone la conexión si no tiene autorizacion.`
	`%`
	Aparece así en la configuración.
	`banner motd "Este es un Sistema privado.\nAbandone la conexin si no tiene autorizacion\n\n"`

Tabla 26. Configuración de banner

6.4.3.4 TEMPORIZADOR DE INACTIVIDAD EN LA CONSOLA

140. Se requiere liberar la consola en caso de inactividad para facilitar la reconexión y evitar accesos no permitidos

SECUENCIA DE CONFIGURACIÓN	Temporizador de inactividad en la consola
Comandos necesarios	`console inactivity-timer` *`0-120`*
Verificación de la funcionalidad en operación	`Show running-config`
Comentarios adicionales	Un tiempo de 0 cancela la funcionalidad por lo que es necesario utilizar un valor entre 1 y 120.

Tabla 27. Temporizador de inactividad en la consola

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.5.1 ACCESO A LA RED: 802.1X, WEB AND MAC AUTHENTICATION

141. Para controlar el acceso a la red es necesario planificar y diseñar una política de control de acceso al medio (NAC).

142. Esta puede estar basada en diferentes técnicas como 802.1X, autenticación web y autenticación MAC.

143. Asimismo, es necesaria la configuración de políticas en el servidor RADIUS que establezcan los permisos y políticas a cada usuario o dispositivo.

6.5.1.1 CONFIGURACIÓN DE SERVIDORES RADIUS

144. El equipo permite la definición de varios servidores RADIUS. También permite agruparlos para asignarlos en grupo y proporcionar un mecanismo de redundancia en caso de fallo de alguno de ellos.

SECUENCIA DE CONFIGURACIÓN	Configuración de un servidor RADIUS

Comandos necesarios	`[no] radius-server host <IP> key clave`
	`[no] radius-server host <IP> dyn-authorization`
	`[no] radius-server host <IP> time-window 0`

Verificación de la funcionalidad en operación	`Show radius`

Comentarios adicionales	Ejemplo de configuración de dos servidores:
	`radius-server host 192.168.255.10 key xxxxxxxxx`
	`radius-server host 192.168.255.10 dyn-authorization`
	`radius-server host 192.168.255.10 time-window 0`
	`radius-server host 192.168.255.11 key xxxxxxxxx`
	`radius-server host 192.168.255.11 dyn-authorization`
	`radius-server host 192.168.255.11 time-window 0`

Tabla 28. Configuración de un servidor RADIUS

145. Una vez definidos los servidores RADIUS se procede a configurar los grupos de servidores

SECUENCIA DE CONFIGURACIÓN	Configuración de grupo de servidores RADIUS

Comandos necesarios	`[no] aaa server-group radius <NombreGrupo> host <IP_ServidorRadius1>`
	`[no] aaa server-group radius <NombreGrupo> host <IP_ServidorRadius2>`
	…

Verificación de la funcionalidad en operación	`show server-group radius` `show radius`

Comentarios adicionales	Ejemplo de configuración:
	`aaa server-group radius "RAD-TEST" host 192.168.255.10`
	`aaa server-group radius "RAD-TEST" host 192.168.255.11`

Tabla 29. Configuración de grupo de servidores RADIUS

6.5.1.2 802.1X

146. Una vez definidos los servidores y grupos de servidores, es posible configurar autenticación de puertos de usuarios.

147. La configuración de la funcionalidad de autenticación 802.1X se realiza con esta secuencia:

SECUENCIA DE CONFIGURACIÓN	Configuración de 802.1X: Autenticación
Comandos necesarios	`[no] aaa authentication port-access eap-radius server-group <NombreGrupo>`
Verificación de la funcionalidad en operación	`show authentication`
Comentarios adicionales	Ejemplo de configuración: `aaa authentication port-access eap-radius server-group "RAD-TEST`

Tabla 30. Configuración de 802.1X: Autenticación

- Se deberá configurar registro de accesos:

SECUENCIA DE CONFIGURACIÓN	Configuración de 802.1X: Accounting
Comandos necesarios	`[no] aaa accounting update periodic <time>` `[no] aaa accounting network start-stop radius server-group <NombreGrupo>`
Verificación de la funcionalidad en operación	`show running-config`

Comentarios adicionales	Ejemplo de configuración:
	`aaa accounting update periodic 10`
	`aaa accounting network start-stop radius server-group "RAD-TEST"`

Tabla 31. Configuración de 802.1X: Accounting

148. Para configurar la autenticación 802.1X en el puerto:

SECUENCIA DE CONFIGURACIÓN	Configuración de 802.1X: Configuración en un puerto
Comandos necesarios	`[no] aaa port-access authenticator <Puerto(s)>` `[no] aaa port-access authenticator <Puerto(s)> client-limit <numMACs>`
Verificación de la funcionalidad en operación	`show port-access config`

Comentarios adicionales	En el puerto se configura la funcionalidad.
	También se puede configurar el número de MACs máximo por puerto. Si no se configura el límite es 1
	Ejemplo de configuración:
	`aaa port-access authenticator 3-4`
	`aaa port-access authenticator 3 client-limit 2`
	`aaa port-access authenticator 4 client-limit 2`

Tabla 32. Configuración de 802.1X: Configuración en un puerto

- La activación de 802.1X de forma global

SECUENCIA DE CONFIGURACIÓN	Configuración de 802.1X: Activación de la funcionalidad
Comandos necesarios	`[no] aaa port-access authenticator active`
Verificación de la funcionalidad en operación	`show port-access config`
Comentarios adicionales	

Tabla 33. Configuración de 802.1X: Activación de la funcionalidad

6.5.1.3 AUTENTICACIÓN MAC

149. Recomendable, configurar registro de accesos:

SECUENCIA DE CONFIGURACIÓN	Configuración de MAC: Accounting
Comandos necesarios	`[no] aaa accounting update periodic <time>` `[no] aaa accounting network start-stop radius server-group <NombreGrupo>`
Verificación de la funcionalidad en operación	`show running-config`

Comentarios adicionales	Ejemplo de configuración:
	`aaa accounting update periodic 10`
	`aaa accounting network start-stop radius server-group "RAD-TEST"`

Tabla 34. Configuración de MAC: Accounting

150. Se configura RADIUS para autenticar MAC

SECUENCIA DE CONFIGURACIÓN	Configuración de MAC: Configurar RADIUS
Comandos necesarios	`[no] aaa authentication mac-based chap-radius server-group <NombreGrupo>`
Verificación de la funcionalidad en operación	`show running-config`
Comentarios adicionales	Ejemplo de configuración: `aaa authentication mac-based chap-radius server-group "RAD-TEST"`

Tabla 35. Configuración de MAC: Configurar RADIUS

151. Para configurar la autenticación MAC en el puerto:

SECUENCIA DE CONFIGURACIÓN	Configuración de MAC: Configuración en un puerto

Comandos necesarios	`[no] aaa port-access mac-based <Puerto(s)>`
	`[no] aaa port-access mac-based <Puerto(s)> addr-limit <numMACs>`
	`[no] aaa port-access mac-based <Puerto(s)> unauth-vid <vlan>`

Verificación de la funcionalidad en operación	`show port-access config`

Comentarios adicionales	En el puerto se configura la funcionalidad.
	También se puede configurar el número de MACs máximo por puerto. Si no se configura el limite es 1.
	Se puede configurar a que VLAN se manda el equipo no autorizado
	Ejemplo de configuración de autorización MAC en el puerto 3:
	`aaa port-access mac-based 3`
	`aaa port-access mac-based 3 client-limit 2`
	`aaa port-access mac-based 3 unauth-vid 205`

Tabla 36. Configuración de MAC: Configuración en un puerto

6.5.1.4 AUTENTICACIÓN WEB

152. En este modo, el switch presenta una página web para autenticar los usuarios.

153. Recomendable, configurar registro de accesos:

SECUENCIA DE CONFIGURACIÓN	Configuración de WEB: Accounting
Comandos necesarios	`[no] aaa accounting update periodic <time>` `[no] aaa accounting network start-stop radius server-group <NombreGrupo>`
Verificación de la funcionalidad en operación	`show running-config`

Comentarios adicionales	Ejemplo de configuración:
	`aaa accounting update periodic 10`
	`aaa accounting network start-stop radius server-group "RAD-TEST"`

Tabla 37. Configuración de WEB: Accounting

154. Para configurar la autenticación WEB en el puerto:

SECUENCIA DE CONFIGURACIÓN	Configuración de WEB: Configuración en un puerto

Comandos necesarios	`[no] aaa port-access web-based <Puerto(s)>`
	`[no] aaa port-access web-based <Puerto(s)> client-limit <numMACs>`
	`[no] aaa port-access web-based <Puerto(s)> unauth-vid <vlan>`
	`[no] aaa port-access web-based <Puerto(s)> auth-vid <vlan>`

Verificación de la funcionalidad en operación	`show port-access config`

Comentarios adicionales	En el puerto se configura la funcionalidad.
	También se puede configurar el número de MACs máximo por puerto. Si no se configura el límite es 1.
	Se puede configurar a que VLAN se manda el equipo no autorizado.
	Se puede configurar a que VLAN se manda el equipo autorizado.
	Si no se configura alguna de las VLANs anteriores, se considera que se usa la asignada al puerto.
	Ejemplo de configuración de autorización MAC en el puerto 3:
	`aaa port-access web-based 3`
	`aaa port-access web-based 3 client-limit 2`
	`aaa port-access web-based 3 unauth-vid 205`
	`aaa port-access web-based 3 auth-vid 200`

Tabla 38. Configuración de WEB: Configuración en un puerto

6.5.1.5 PORTAL CAUTIVO EXTERNO

155. Es posible configurar el uso de portal cautivo externo como método de autenticación. Típicamente para solicitar o introducir credenciales.

156. Cuando se está usando mecanismos de autenticación externa, es posible que el RADIUS proporcione instrucciones al equipo para que redirija al usuario a un portal cautivo.

157. Si no se va a hacer uso del portal cautivo externo, se recomienda que se desactive esta funcionalidad.

SECUENCIA DE CONFIGURACIÓN	Deshabilitar la funcionalidad de portal cautivo Externo

Comandos necesarios	`aaa authentication captive-portal disable`
	o
	`no aaa authentication captive-portal enable`

Verificación de la funcionalidad en operación	`show captive-portal`
Comentarios adicionales	

Tabla 39. Deshabilitar la funcionalidad de portal cautivo Externo

158. En el caso que el acceso de usuarios requiera portal cautivo externo, se recomienda activar la autenticación entre el switch y el portal. La activación de esta autenticación, evita usos no autorizados.

159. Se requiere el uso de portal sobre HTTPS cuya autenticación entre el switch y el portal cautivo requiere certificado.

160. Secuencia de configuración para portales basados en HTTPS

SECUENCIA DE CONFIGURACIÓN	Configuración del portal cautivo externo con certificado

Comandos necesarios	`Requiere la`
	`aaa authentication captive-portal enable`
	`aaa authentication captive-portal profile <perfil> url <URL>`

Verificación de la funcionalidad en operación	`show captive-portal`

Comentarios adicionales	Ejemplo
	`aaa authentication captive-portal enable`
	`aaa authentication captive-portal profile demo url https://portal.cautivo/portalseguro`
	Se requiere obtener certificado de una PKI externa válida en la organización. Para generar la CSR
	`crypto pki create-csr certificate-name <nombre_certificado> ta-profile <perfil_CA> usage captive-portal`

Tabla 40. Configuración del portal cautivo externo con certificado

6.5.2 PREVENCIÓN DE ATAQUES

6.5.2.1 DYNAMIC ARP PROTECTION

161. Para configurar los mecanismos de protección ante ataques de ARP es necesario:

SECUENCIA DE CONFIGURACIÓN	Configuración Protección ARP
Comandos necesarios	`arp-protect`
Verificación de la funcionalidad en operación	`show arp-protect`
Comentarios adicionales	

Tabla 41. Configuración Protección ARP

- Para que el mecanismo sea operativo es necesario activarlo en una VLAN.

SECUENCIA DE CONFIGURACIÓN	Configuración Protección ARP para una VLAN
Comandos necesarios	`[no] arp-protect vlan [vlan-range]`
Verificación de la funcionalidad en operación	`show arp-protect`
Comentarios adicionales	Selecciona que esas VLANs estén protegidas

Tabla 42. Configuración Protección ARP para una VLAN

- Podemos determinar que puertos son fiables:

SECUENCIA DE CONFIGURACIÓN	Configuración de un puerto como trust para ARP Protection
Comandos necesarios	`[no] arp-protect trust <port-list >`
Verificación de la funcionalidad en operación	`show arp-protect`
Comentarios adicionales	Selecciona esos puertos como puertos fiables.

Tabla 43. Configuración de un puerto como trust para ARP Protection

- Es posible configurar asignaciones estáticas de IP-MAC para los casos que sea necesario.

SECUENCIA DE CONFIGURACIÓN	Configuración de una asignación estática
Comandos necesarios	`[no] ip source-binding <mac-address > vlan <vlan-id > <ip-address > interface <portnumber >`
Verificación de la funcionalidad en operación	`show arp-protect`
Comentarios adicionales	Configura una asiganación estática.

Tabla 44. Configuración de una asignación estática

- Adicionalmente podemos establecer restricciones adicionales. Podemos forzar validaciones adicionales, sobre el correcto origen y destino de las peticiones y respuestas de paquetes ARP, así como restringir el uso de IPs no permitidas.

SECUENCIA DE CONFIGURACIÓN	Configuración de validaciones adicionales en ARP Protection
Comandos necesarios	`[no] arp-protect validate <[src-mac]|[dest-mac]|[ip]>`
Verificación de la funcionalidad en operación	`show arp-protect`
Comentarios adicionales	Ejemplo: `arp-protect validate` *`src-mac dest-mac ip`*

Tabla 45. Configuración de validaciones adicionales en ARP Protection

6.5.2.2 VIRUS TRHOWLING

162. Esta funcionalidad está pensada para detectar y mitigar el impacto en la red de ataques de gusano o bien de escaneo de puertos.

163. Cuando un puerto es detectado, puede generarse notificación únicamente o bien bloquearse el puerto, bloqueo que requiere que el administrador re-habilite el puerto manualmente.

164. Dependiendo de la sensibilidad elegida para la funcionalidad, se puede determinar que el comportamiento sea:

- Notify-only: Únicamente se genera la notificación en log o SNMP.
- Throttle: El puerto es bloqueado durante un periodo de tiempo y genera la correspondiente notificación.
- Block: El puerto se bloquea. El administrador debe posteriormente rehabilitar el puerto.

165. Sensibilidad:

- low – hasta 54 destinos en menos de 0.1 segundos y una penalización de 30 segundos en modo Throttle.

- medium - hasta 37 destinos en menos de 1 segundo y una penalización de 30 a 60 segundos en modo Throttle.
- high - hasta 22 destinos en menos de 1 segundo y una penalización de 60 a 90 segundos en modo Throttle.
- aggresive - hasta 15 destinos en menos de 1 segundo y una penalización de 90 a 120 segundos en modo Throttle.

166. En los comandos se denomina la funcionalidad *connection-rate-filter.*

167. Se configura de forma global y después en los puertos en concreto.

168. Esta funcionalidad se recomienda sea activada en puertos de acceso y no tanto en los uplinks.

169. Configuración de la funcionalidad Virus Trhowling o connection-rate-filtering global.

SECUENCIA DE CONFIGURACIÓN	Configuración de Virus Trhowling o connection-rate-filtering.
Comandos necesarios	`connection-rate-filter sensitivity < low | medium | high | aggressive >` `[no] connection-rate-filter`
Verificación de la funcionalidad en operación	`show connection-rate-filter`
Comentarios adicionales	

Tabla 46. Configuración de Virus Trhowling o connection-rate-filtering

170. Configuración de la funcionalidad Virus Trhowling o connection-rate-filtering por puerto

SECUENCIA DE CONFIGURACIÓN	Configuración de Virus Trhowling o connection-rate-filtering por puerto
Comandos necesarios	`filter connection-rate <port-list> {notify-only | throttle | block}` `no filter connection-rate <port-list>`
Verificación de la funcionalidad en operación	`show connection-rate-filter`
Comentarios adicionales	

Tabla 47. Configuración de Virus Trhowling o connection-rate-filtering por puerto

171. Adicionalmente se puede mejorar la funcionalidad mediante el uso de ACLs específicas de esta funcionalidad. Estas ACLs hacen que el cómputo de las tasas esté basado en criterios más precisos. Para conocer más detalles, recomendamos acceder a la guía "Access Security Guide", sección "Virus Trhowling" [REF3].

6.5.2.3 DHCP SNOOPING

172. Para evitar ataques DHCP, en los que se suplanta la funcionalidad del servidor DHCP es posible configurar DHCP snooping en el switch.

SECUENCIA DE CONFIGURACIÓN	DHCP Snooping
Comandos necesarios	`dhcp-snooping`
Verificación de la funcionalidad en operación	`show dhcp-snooping`
Comentarios adicionales	

Tabla 48. DHCP Snooping

173. Para configurar un servidor autorizado en el switch debe configurarse la dirección IP así como el puerto donde está conectado.

SECUENCIA DE CONFIGURACIÓN	DHCP Snooping – Configuración de fuente DHCP autorizada
Comandos necesarios	`dhcp-snooping authorized-server <IP>` `switch(config)# dhcp-snooping trust <Puerto>`
Verificación de la funcionalidad en operación	`Show dhcp-snooping` `Show running-config`

Comentarios adicionales	Ejemplo, servidor en el puerto 8 con la IP 10.1.4.24
	`dhcp-snooping authorized-server 10.1.5.24`
	`dhcp-snooping trust 8`

Tabla 49. DHCP Snooping – Configuración de fuente DHCP autorizada

174. Finalmente configure las VLANs donde se quiere monitorizar la función DHCP.

SECUENCIA DE CONFIGURACIÓN	DHCP Snooping – Activación por VLAN
Comandos necesarios	`dhcp-snooping vlan <vlan-list>`
Verificación de la funcionalidad en operación	`Show dhcp-snooping` `Show running-config`
Comentarios adicionales	

Tabla 50. DHCP DHCP Snooping – Activación por VLAN

6.5.2.4 PROTECCIÓN DEL PLANO DE CONTROL

175. La Vigilancia del Plano de Control (CoPP) evita que ciertos tipos de paquetes sobrecarguen la CPU del conmutador o del módulo, ya sea limitando la velocidad o descartando

paquetes. El firmware de los equipos proporciona políticas de limitación de tráfico por defecto para los principales protocolos ejecutados por el plano de control, como, por ejemplo: BGP, OSPF, RIP, MSTP, PVST, ARP, etc.

176. La política de vigilancia del plano de control puede ser configurada por el usuario. Para más detalle ver [REF4].

177. A continuación, se muestra la política de protección del plano de control por defecto:

```
Aruba-2930F-VSF(config)# copp traffic-class all limit default
Aruba-2930F-VSF(config)# show copp config
 Traffic-Class                  CoPP Status    Rate-Limit
 ------------------------------ -------------------------
 station-arp                    Enabled        512
 station-icmp                   Enabled        128
 station-ip                     Enabled        512
 ip-gateway-control             Enabled        128
 ospf                           Enabled        512
 bgp                            Enabled        512
 rip                            Enabled        512
 multicast-route-control        Enabled        256
 loop-ctrl-mstp                 Enabled        256
 loop-ctrl-pvst                 Enabled        256
 loop-ctrl-loop-protect         Enabled        256
 loop-ctrl-smart-links          Enabled        256
 layer2-control-others          Enabled        512
 udld-control                   Enabled        256
 sampling                       Enabled        256
 icmp-redirect                  Enabled        64
 unicast-sw-forward             Enabled        512
 multicast-sw-forward           Enabled        512
 mac-notification               Enabled        512
 exception-notification         Enabled        256
 broadcast                      Enabled        512
 unclassified                   Enabled        64
```

6.5.3 LISTAS DE ACCESO (ACL) IPV4

178. Las listas de acceso son un método que nos permite filtrar flujos de datos. Pueden ser usadas para restringir el acceso a estas dos funcionalidades:

- Acceso a la gestión del equipo.
- Filtrado de tráfico.

6.5.3.1 DEFINICION DE LAS ACL(S)

179. Desde el punto de vista de cómo se define la ACL se clasifican en ***estáticas*** o ***dinámicas***.

180. Las ACLs estáticas son configuradas con comandos en el equipo. Pueden ser usadas para asignarse a puertos o a VLANs para restringir el tráfico entrante o saliente.

181. Una VLAN ACL o VACL, es una ACL que se aplica a un interfaz VLAN y que tiene destino la propia VLAN.

182. Una ACL estática asignada a un puerto filtra el tráfico en ese puerto, independientemente de si es filtrado, enrutado o tienen como destino el propio switch.

183. Una ACL dinámica es una ACL que no está definida en el propio switch, sino que ha sido proporcionada por un RADIUS como resultado de la autenticación. Una vez el cliente cesa la sesión se libera esa ACL.

6.5.3.2 TIPOS DE ACL(S)

184. ***ACL standard***. Filtran tráfico basado en las direcciones de origen. Se les asigna un nombre o un número en el rango 1-99.

185. ***ACL extendida***. Permiten filtrar tráfico basado en las direcciones IP de origen, destino y protocolos involucrados. Se les asigna un nombre o un número en el rango 100-199.

186. Las ACLs extendidas permiten filtrar atendiendo a opciones de los siguientes protocolos:

- Tráfico IPv4.
- Protocolos específicos IPv4.
- Tráfico TCP, rango de puertos, bits de control y seleccionar sesiones establecidas.
- Tráfico TCP y rango de puertos.
- Tráfico ICMP y códigos específicos.
- Tráfico IGMP y tipos específicos.

6.5.3.3 USOS DE LAS ACL(S)

187. Filtrado de tráfico. Es posible filtrar tráfico en el equipo mediante uno de estos tres métodos:

- Filtrado en el puerto mediante la asignación de una ACL estática.
- Filtrado en el puerto con la autenticación activada, mediante la asignación por parte del RADIUS de una ACL estática o bien dinámica (descargada como un atributo RADIUS).
- VLAN ACL aplicada a la VLAN.

188. Es posible que varias ACLs puedan estar aplicándose simultáneamente, si se da alguno de estos casos:

- ACL aplicada en el puerto.
- VLAN ACL aplicada en la VLAN a la que ese tráfico pertenece.
- ACL asignada por el RADIUS a un cliente concreto.

6.5.3.4 CARACTERISTICAS DE LAS ACLS

189. Una ACL consiste en la definición de varias reglas (identidad ACE, ACL Entry). Estas entradas están numeradas de forma que determina su orden de ejecución y permite por tanto la edición de la misma.

190. Cuando un tráfico es evaluado se confronta a las ACEs definidas por orden. La primera entrada que cumpla se aplica la acción asociada.

191. En caso de no cumplir ninguna se entiende que el tráfico no está permitido. Es lo que se conoce con la regla de denegación implícita. En el caso que se quiera el efecto contrario debe ser programado adecuadamente.

6.5.3.5 DEFINICIÓN DE LAS ACL(S)

192. En el caso concreto de esta sección, y dada su amplitud, se recomienda complementar este resumen funcional con las guías de configuración del producto [REF1].

193. Cada tipo de ACL permite filtrar tráfico atendiendo a diferentes campos del paquete de datos.

194. ACL ESTÁNDAR: Permite filtrar por dirección IP origen del paquete. Para detalles concretos de su uso y configuración consultar Chapter 12 IPv4 Access Control Lists (ACLs) [REF3].

195. ACL EXTENDIDA: Permite filtrar por protocolo, opciones del protocolo, IP origen y IP destino. Para detalles concretos de su uso y configuración consultar Chapter 12 IPv4 Access Control Lists (ACLs) [REF3].

6.5.4 MACSEC

196. *Media Access Control security* (MACsec) es un standard IEEE 802 que describe como securizar un enlace entre dos equipos al nivel de la capa de enlace. Los equipos que soportan MACSEC deben hacerlo manteniendo el rendimiento y prestaciones de las altas tasas de transferencia de los puertos implicados.

197. MACsec está pensado para entornos cableados, los entornos WLAN tienen su propia solución de encriptación.

198. Es un protocolo con demanda en auge para garantizar la confidencialidad de las comunicaciones cableadas.

199. El protocolo MACSEC proporciona:

- Integridad de datos *connectionless.* Cada trama MAC transporta un campo separado de verificación de integridad (de ahí el término *connectionless)*
- Autenticidad del origen de la trama. Se garantiza que cada trama MAC ha sido enviada por una estación autorizada MACSEC.
- Confidencialidad. Cada trama es encriptada.
- Protección contra la redifusión. Las tramas capturadas, no pueden ser insertadas de nuevo al medio, sin ser detectadas.

200. Se mejora la seguridad en las comunicaciones switch-to-switch con el protocolo *MACsec Key Agreement (MKA)* y el modo Static Connectivity Association Key (CAK).

201. En los equipos de Aruba se soporta:

- El modo *Switch-to-Switch Pairwise Pre-Shared CAK* con Single-User CAK por puerto.
- Nuevos components para un procesado más rápido de tráfico MACsec.
- *MACsec Key Agreement protocol (MKA)* para el descubrimiento automático de vecinos MACSEC, peer-participant liveliness, elección de Key-Server y distribución de SAKs.
- AES-GCM-128 bit key length (CAKs/ICKs/KEKs/SAKs).
- Configuración de los modos "Integrity Check Only" y "Integrity Check with Confidentiality at offset 0".
- Configuración MACsec via CLI, SNMP y sobre SSH.
- Configuración MACsec via HTTPS no se soporta actualmente.

202. Los pasos para la activación de la funcionalidad MACSEC son:

a) Creación y configuración de una política MACsec.

b) Aplicación de una política MACSEC a los puertos.

c) Configuración de los parámetros MKA en los puertos.

6.5.4.1 CREACION DE POLITICA MACSEC

SECUENCIA DE CONFIGURACIÓN	Creación de política MACSEC

Comandos necesarios	`macsec policy <policy-name>`
	`mode pre-shared-key ckn <CKN> [cak|encrypted-cak] <CAK-value>`
	`[no] confidentiality`
	`[no] replay-protection <replaywindowsize>`
	`[no] include-sci-tag`

Verificación de la funcionalidad en operación	`show macsec policy`
	`show macsec policy <policy-name>`
	`show macsec status`

Comentarios adicionales	En la introducción de la clave, puede optarse por introducirse en texto plano o ya encriptada. Para introducirla encriptada debe haberse obtenido desde un dispositivo compatible. El comando `confidentiality` proporciona encriptación de la trama MAC. Si se desactiva, no se cifra pero se valida integridad. El comando `replay-protection` verifica el campo *IP number,* y asegura que el paquete no haya llegado retrasado un número de paquetes mayor que el valor `<replaywindowsize>`. En tal caso descarta la trama. Con el valor 0 aseguramos que todas las tramas lleguen en orden estricto, evitando, reinserciones de tramas. El comando `include-sci-tag` incluye la etiqueta Secure Channel Identifier (SCI) en el campo Secure Tag.

Tabla 51. Creación de política MACSEC

SECUENCIA DE CONFIGURACIÓN	Eliminición de política MACSEC
Comandos necesarios	`no macsec policy <policy-name>`
Verificación de la funcionalidad en operación	`show macsec policy` `show macsec policy <policy-name>`
Comentarios adicionales	No debe estar en uso para poder ser eliminada

Tabla 52 Eliminación de política MACSEC

6.5.4.2 APLICACIÓN DE POLITICA MACSEC

203. Una vez definida la política es necesario aplicarla a un puerto para que tenga funcionalidad.

SECUENCIA DE CONFIGURACIÓN	Aplicar política MACSEC
Comandos necesarios	`[no] macsec apply policy <policy-name> ethernet PORT-LIST`

Verificación de la funcionalidad en operación	`show macsec status <port-num>`
	`show macsec statistics <port-num>`
	`show macsec policy <policy-name>`
	`show macsec statistics <port-num> detail`

Comentarios adicionales	

Tabla 53 Aplicar política MACSEC

6.5.4.3 CONFIGURACION DE PARAMETROS MKA EN LOS PUERTOS

204. Es posible configurar el comportamiento del protocolo *MACsec Key Agreement (MKA)*

SECUENCIA DE CONFIGURACIÓN	Configuración de parámetros MKA en los puertos
Comandos necesarios	`aaa port-access mka <key-server-priority> [transmit-interval <INTERVAL>] [ethernet]PORT-LIST`

Verificación de la funcionalidad en operación	`show macsec status <port-num>`
	`show macsec statistics <port-num>`
	`show macsec policy <policy-name>`
	`show macsec statistics <port-num> detail`

Comentarios adicionales	Es posible configurar únicamente la prioridad de server.

Tabla 54 Configuración de parámetros MKA en los puertos

6.6 GESTIÓN DE CERTIFICADOS

6.6.1 IDENTIDAD DEL EQUIPO: SWITCH IDENTITY PROFILE

205. Se recomienda crear un perfil de identidad del equipo, para facilitar las tareas de creación y solicitud de certificados.

206. En caso contrario, hay que completar los datos en cada certificado solicitado.

SECUENCIA DE CONFIGURACIÓN	Configuración del Switch Identity Profile
Comandos necesarios	`crypto pki identity-profile`
Verificación de la funcionalidad en operación	`show running-config`
Comentarios adicionales	Ejemplo: `crypto pki identity-profile switch-id-profile subject common-name switch country es state Madrid locality LasRozas org HPE org-unit Aruba`

Tabla 55 Configuración del Switch Identity Profile

6.6.2 PROCESO DE CREACIÓN DE CERTIFICADO HTTPS DEL EQUIPO

207. Se recomienda esta secuencia de configuración:

a) RECOMENDABLE: Tener una identidad de switch configurada, Switch Identity Profile.

b) Configurar un perfil de Trust Anchor (TA).

c) Copiar el certificado raíz al switch y adjuntar al perfil de Trust Anchor (TA).

d) Generar una CSR en el switch vinculado al perfil de Trust Anchor (TA). El algoritmo y tamaño de clave se ajustarán a la política criptográfica vigente y a la CCN-STIC 807.

e) Generar el certificado en la CA, con el CSR generado.

f) El certificado resultante se debe instalar en el equipo vía CLI

208. PASO 1. Configuración del Switch Identity Profile

```
switch(config)# crypto pki identity-profile
```

209. PASO 2. Configurar un perfil de Trust Anchor (TA).

```
switch(config)# crypto pki ta-profile webprofile
```

210. PASO 3. Copiar el certificado raíz al switch y admuntar al perfil de Trust Anchor (TA).

```
switch(config)# copy sftp ta-certificate webprofile sftpuser@10.10.10.1
cacert.pem
```

211. PASO 4. Generar una CSR en el switch vinculado al perfil de Trust Anchor (TA). el algoritmo y tamaño de clave se ajustarán a la política criptográfica vigente y a la CCN-STIC 807. En el caso del ejemplo se utiliza RSA de 2048 bits.

```
switch(config)# crypto pki create-csr certificate-name webcert ta-
profile webprofile usage web key-type rsa key-size 2048
-----BEGIN CERTIFICATE REQUEST-----
< CadenaCSR >
-----END CERTIFICATE REQUEST-----
```

212. PASO 5. Generar el certificado en la CA, con el CSR generado.

213. PASO 6. El certificado resultante se debe instalar en el equipo

```
switch(config)# copy sftp local-certificate sftpuser@10.10.10.1
webcert.pem
000M Transfer is successful
```

6.7 SERVIDORES DE AUTENTICACIÓN PARA AUTENTICACIÓN REMOTA DE ADMINISTRADORES

6.7.1 RADIUS SERVER COMO METODO PRIMARIO

214. El uso de un servidor RADIUS permite una forma de administrar los accesos a la configuración de los equipos de forma centralizada. De esta forma, las altas y bajas de usuarios, así como los cambios de credenciales, se pueden realizar sin necesidad de cambios en la configuración.

215. La autenticación RADIUS está soportada en Aruba ClearPass Policy Manager.

216. Es posible configurar más de un servidor RADIUS para proporcionar mayor disponibilidad.

217. Es frecuente y en muchos casos recomendable, seleccionar el método local como segundo método. De esta forma, si el equipo no tiene conectividad con los servidores de autenticación puede aún ser gestionado.

SECUENCIA DE CONFIGURACIÓN	Configuración de RADIUS como método primario de autenticación y local como tipo secundario
Comandos necesarios	`[no] aaa authentication <console|ssh|web> <enable|login > radius [servergroup <group-name>|local`
Verificación de la funcionalidad en operación	`show server-group radius`
Comentarios adicionales	Para cada método (ssh, console, …) es necesario introducer un commando. SSH incluye los protocolos SCP y SFTP Si no hay usuarios locales introducidos, y no se conecta con el RADIUS, se accede directamente al CLI Se puede especifigar un grupo de servidores radius definido. Puede haber varios grupos, para ser usado en diferentes entornos.

Tabla 56 Configuración de RADIUS como método primario de autenticación y local como tipo secundario

SECUENCIA DE CONFIGURACIÓN	Configuración servidores RADIUS
Comandos necesarios	`[no] aaa server-group radius <nombre_grupo> host <srv_radius>`
Verificación de la funcionalidad en operación	`show server-group radius`
Comentarios adicionales	Pueden definirse tres servidores dentro de un grupo Ejemplo: `aaa server-group radius "RAD-TEST" host 10.150.0.43` Se puede eliminar un servidor de un grupo. Si se elimina el ultimo servidor se elimina el grupo

Tabla 57 Configuración servidores RADIUS

218. Para proporcionar el nivel correcto de privilegios es necesario especificar el atributo "Service-Type" en las credenciales del usuario

- Service-Type = 6 proporciona acceso manager
- Service-Type = 7 proporciona acceso operator

219. Un usuario con otro nivel de servicio se le deniega el acceso.

220. Un usuario sin ese atributo se le deniega el acceso cuando el modo *privilege* está activado en el comando *ip Access manager (*descrito posteriormente)

6.7.2 TACACS SERVER COMO METODO PRIMARIO

221. El uso de un servidor TACACS permite una forma de administrar los accesos a la configuración de los equipos de forma centralizada. De esta forma, las altas y bajas de usuarios, así como los cambios de credenciales, se pueden realizar sin necesidad de cambios en la configuración.
222. La autenticación TACACS está soportada en Aruba ClearPass Policy Manager.
223. Es posible configurar más de un servidor TACACS para proporcionar mayor disponibilidad.
224. Es frecuente y en muchos casos recomendable, seleccionar el método local como segundo método. De esta forma, si el equipo no tiene conectividad con los servidores de autenticación aún puede ser gestionado.

SECUENCIA DE CONFIGURACIÓN	Configuración de TACACS como método primario de autenticación y local como tipo secundario
Comandos necesarios	`[no] aaa authentication <console|ssh|web> <enable|login > tacacs [servergroup <group-name>|local`
Verificación de la funcionalidad en operación	show server-group radius
Comentarios adicionales	Para cada método (ssh, console, …) es necesario introducer un commando. SSH incluye los protocolos SCP y SFTP Si no hay usuarios locales introducidos, y no se conecta con el RADIUS, se accede directamente al CLI Se puede especificar un grupo de servidores radius definido. Puede haber varios grupos, para ser usado en diferentes entornos.

Tabla 58 Configuración de TACACS como método primario de autenticación y local como tipo secundario

SECUENCIA DE CONFIGURACIÓN	Configuración servidores TACACS
Comandos necesarios	`[no] tacacs-server host IP-ADDR key KEY-STR`
Verificación de la funcionalidad en operación	`show tacacs`
Comentarios adicionales	Ejemplo: `tacacs-server host 1.2.3.4 key clave` Se puede eliminar un servidor de un grupo. Si se elimina el ultimo servidor se elimina el grupo

Tabla 59 Configuración servidores TACACS

225. Para proporcionar el nivel correcto de privilegios, es necesario especificar el atributo "Max-privilege" en las credenciales del usuario

226. Service-Type = 15 proporciona acceso manager

227. Service-Type = 14 o menor, proporciona acceso operator.

6.8 SINCRONIZACIÓN

228. El equipo soporta sincronizarse mediante TimeP, NTP y SNTP.

229. Se recomienda usar NTP porque es más preciso y permite configurar más de una fuente de sincronización.

6.8.1 CONFIGURAR EL EQUIPO PARA QUE FORME PARTE DE UNA RED NTP

230. La secuencia de configuración para que el equipo forme parte del servicio NTP de la red es:

a) Configurar el modo de trabajo: broadcast o unicast

b) Configurar las claves de autenticación. Se recomienda SHA1.

c) Configurar el número máximo de asociaciones de terceros equipos

d) Configurar los servidores NTP desde los cuales sincronizarse

e) Habilitar NTP.

SECUENCIA DE CONFIGURACIÓN	Sicronizar el reloj del equipo con la hora NTP

Comandos necesarios	`[no] ntp [broadcast|unicast]`
	`[no] ntp authentication key-id <KEY-ID> [authentication-mode [md5|sha1] key-value <KEYSTRING>] [trusted]`
	`[no] ntp max-association`
	`[no] ntp server <IP-ADDR|IPv6-ADDR> [key <key-id>] [oobm] [max-poll <max-poll-val>][minpoll] <min-poll-val>][burst | iburst] [version <1-4>]`

	`[no] ntp enable`
Verificación de la funcionalidad en operación	Comandos: `show running-config`

Comentarios adicionales	Un ejemplo típico de configuración puede ser:
	`ntp unicast`
	`ntp authentication key-id 1 authentication-mode sha1 key-value secret`
	`ntp server 150.214.94.5`
	`ntp server 150.214.94.10`
	`ntp enable`
	Adicionalmente
	`timesync ntp`

Tabla 60 Sicronizar el reloj del equipo con la hora NTP

6.8.2 SINCRONIZAR EL RELOJ DEL EQUIPO CON NTP

231. Para que el equipo adquiera la hora por NTP se configura con este comando.

SECUENCIA DE CONFIGURACIÓN	Sicronizar el reloj del equipo con la hora NTP
Comandos necesarios	`[no] timesync { timep | sntp | timep-or-sntp | ntp }`
Verificación de la funcionalidad en operación	Comandos: `show running-config`
Comentarios adicionales	

Tabla 61 Sincronizar el reloj del equipo con la hora NTP

6.9 ACTUALIZACIONES

232. El equipo tiene capacidad para dos versiones de software.

- Cada una de ellas conlleva su propia versión de software *Boot ROM.*
- Cada imagen puede ser actualizada independientemente. La actualización de cada versión lleva implícita la actualización del Boot ROM correspondiente.

233. La actualización puede realizarse mediante CLI, GUI.

6.9.1 INSPECCIÓN DE LAS VERSIONES DE SOFTWARE INSTALADAS

234. Para verificar la versión en ejecución ejecute el comando *show version*.

```
Aruba-2930F-VSF# show version
```

```
Image                                                          stamp:
/ws/swbuildm/rel_washington_qaoff/code/build/lvm(swbuildm_rel_washing
ton_qaoff_rel_washington)
                Jun 22 2018 12:55:58
                WC.16.06.0006
                607
Boot Image:     Primary
Boot ROM Version:    WC.16.01.0004
Active Boot ROM:     Primary
Aruba-2930F-VSF#
```

235. Podemos ver la versión en ejecución, así como el slot que está usando. También la versión de Boot ROM asociada.

236. Para verificar las versiones instaladas ejecute el comando *show versión*

```
Aruba-2930F-VSF# show flash
Image              Size (bytes) Date     Version
------------------ ------------ -------- --------------
Primary Image    :    29072623 06/22/18 WC.16.06.0006
Secondary Image  :    15642343 04/27/16 WC.16.02.0003
Boot ROM Version
----------------
Primary Boot ROM Version   : WC.16.01.0004
Secondary Boot ROM Version : WC.16.01.0004
Default Boot Image   : Primary
Default Boot ROM     : Primary
Aruba-2930F-VSF#
```

237. Es posible verificar las versiones de cada uno de los slots disponibles para versiones de software. También podemos ver el slot por defecto para el arranque.

6.9.2 POSIBILIDADES DE ACTUALIZACIÓN

238. La actualización puede realizarse mediante CLI o GUI.

239. Antes de actualizar se recomienda hacer una copia de respaldo de la configuración. En ocasiones, entre versiones diferentes los comandos pueden cambiar y por tanto pueden parecer que desaparece algún elemento configurado.

240. Usando el CLI, es posible usar TFTP y SFTP para actualizar el equipo vía red y XMODEM usando el puerto de consola para transferirlo. Recomendamos el uso de SFTP, al ser un protocolo seguro. XMODEM debe usarse si no se dispone de ninguna versión en el equipo y por tanto no puede usarse la red.

241. Un ejemplo de actualización usando CLI sería

```
copy sftp flash usuario@10.1.1.1 K_15_10_0001.swi secondary
The secondary image will be deleted.
Continue (y/n)?
Validating and Writing System Software to FLASH...
```

242. Además de TFTP y SFTP, es posible usando el interfaz gráfico es posible subir la imagen usando un fichero local al navegador que se esté usando. Esta es una opción muy cómoda. La seguridad de esta opción reside en la seguridad del protocolo usado en el navegador. Recomendamos HTTPS.

6.10 AUTO-CHEQUEOS

243. Cada vez que el switch arranca el equipo pasa un proceso de self-test durante el que se verifica el software de arranque y los diferentes componentes hardware del equipo.

```
I 01/01/90 01:00:17 03803 chassis: System Self test completed on  Mgmt
module
I 01/01/90 01:00:17 03802 chassis: System Self test started on  Mgmt
module
I 01/01/90 01:00:16 03803 chassis: System Self test completed on  Mgmt
module
I 01/01/90 01:00:16 03802 chassis: System Self test started on  Mgmt
module
----  Top of Log : Events Listed = 118  ----
```

244. El resultado del auto chequeo puede verificarse en el LED “Global Status” del equipo:

- Verde: El resultado del test ha sido satisfactorio y el equipo está operando normalmente.
- Parpadeando en Verde: El test se está realizando y el equipo aún no está operativo
- Parpadeando en Naranja: Se ha encontrado un fallo en algún componente. Si el componente dispone de led (puerto o ventilador) su led de estado parpadea de forma simultánea.
- Naranja: El fallo no ha podido ser restablecido y el self-test ha fallado. El switch no está operativo.

245. Un firmware es válido si tiene una firma digital válida, generada por el Servicio de Firma de Código de HPE (HPECSS). Los switches generarán un mensaje de error si intenta descargar una imagen que no esté firmada digitalmente.

246. Es posible verificar manualmente la firma digital del firmware

```
Aruba-2930F-VSF# verify signature flash primary
Signature is valid
Aruba-2930F-VSF# verify signature flash secondary
Signature is valid
Aruba-2930F-VSF#
```

247. Cuando se realiza una carga de firmware el equipo verifica que el firmware dispone de la firma correcta que verifica su autenticidad. Si se trata de subir un firmware que no dispone de la firma correcta el equipo genera un error y no carga el fichero en la flash.

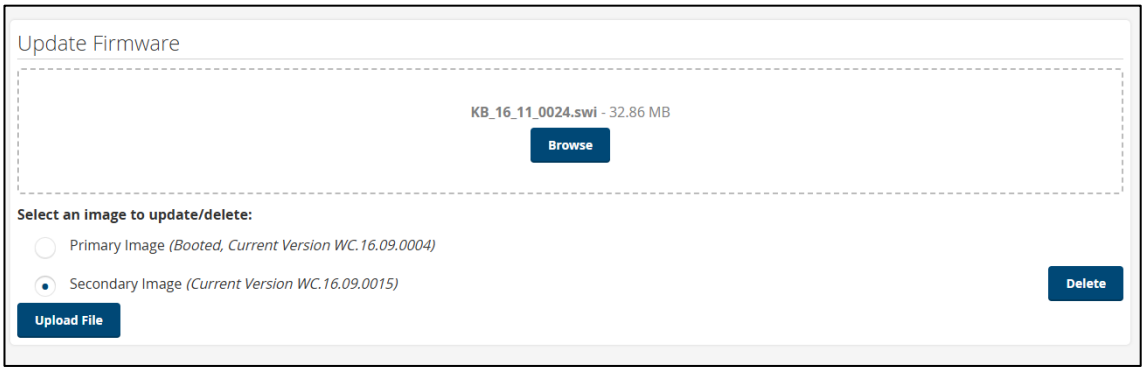

Ilustración 4. Se trata de subir un firmware de 3810 a un 2930

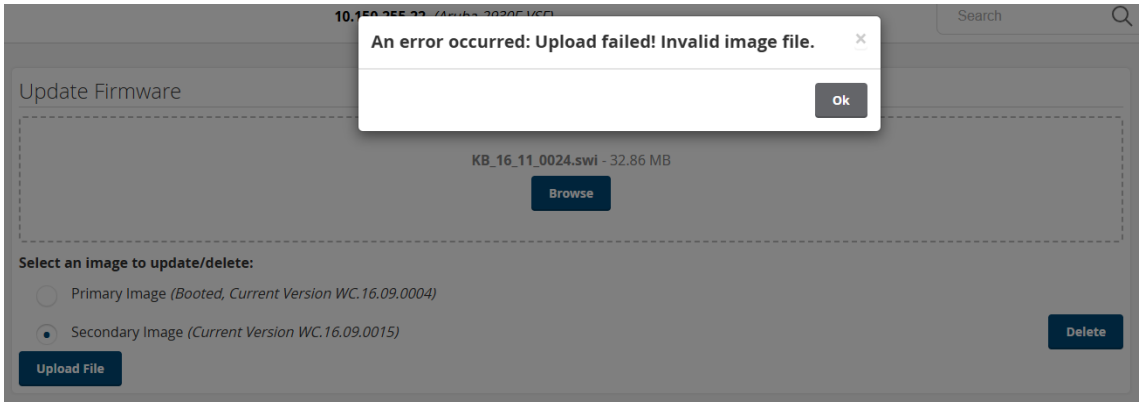

Ilustración 5. El equipo detecta la imagen como inválida

6.11 ALTA DISPONIBILIDAD

248. Diferentes equipos de la familia de conmutadores AOS-S Switch proporcionan diferentes funcionalidades de redundancia hardware:

- 2930M, 3810M y 5400R ofrecen la posibilidad de fuentes redundantes reemplazables en caliente.
- 5400R es un equipo tipo chasis que permite:
  - La instalación de controladoras redundantes.
  - Reemplazar en caliente la bandeja de ventiladores
  - Utilizar puertos alojados en diferentes tarjetas para proporcionar alta disponibilidad de conexión en caso de fallo de una tarjeta de puertos.

249. Todos los equipos de la familia permiten realizar configuraciones de red con alta disponibilidad. Cada funcionalidad de red utiliza sus mecanismos para proporcionar alta disponibilidad y redundancia. Para información detallada de esta configuración se recomienda consultar las guías de configuración de los equipos [REF1].

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

250. AOS-S Switch proporciona registros de eventos y seguridad que pueden ser almacenados localmente, además de utilizar el protocolo syslog para reenviar eventos a un servidor remoto con fines de auditoría. Los eventos registrados se pueden filtrar por nivel de gravedad, módulos del sistema de origen o mediante expresiones regulares para compararlos con el texto del mensaje.

251. El cliente de los equipos syslog puede conectarse a un servidor mediante los protocolos UDP (predeterminado), TCP o TLS. TLS es el protocolo preferido, ya que proporciona una conexión cifrada al receptor syslog. Esto requiere que el switch posea un certificado de cliente TLS firmado y que el receptor posea un certificado de servidor TLS firmado. (Los certificados autofirmados no se pueden utilizar para conexiones a un receptor syslog). UDP/TCP sin protección solo se admiten si está justificado y en red de gestión segregada.

252. El proceso para solicitar e instalar un certificado de cliente TLS firmado para syslog es similar al de solicitar e instalar un certificado SSL/TLS para la administración web. Ver apartado 6.6.2 PROCESO DE CREACIÓN DE CERTIFICADO HTTPS DEL EQUIPO.

253. Una vez instalados los certificados necesarios, es necesario configurar el equipo para que reenvíe todos los eventos con una gravedad de advertencia o superior a un servidor syslog en 10.100.1.250 mediante TLS:

```
switch(config)# logging 10.100.1.250 tls
switch(config)# logging severity warning
```

254. Para más detalle se debe consultar el apartado “Degug/syslog operation” en el capítulo “Troubleshooting” de la guía [REF5] HPE Aruba Networking 2930M/F Management and Configuration Guide 16.11.

255. En el documento “HPE Aruba Networking Event Log Messages ArubaOS-Switch for AOS-S Switch 16.11” se pueden consultar todos los eventos potencialmente generados por el equipo .

6.12.2 ALMACENAMIENTO LOCAL

256. Los logs se almacenan en el equipo en un buffer cíclico. Es posible consultarlos mediante el siguiente comando:

```
Aruba-2930F-VSF# show log
 -a                        Display all log events, including those from
previous boot cycles.
 -b                       Display log events as time since boot instead
of date/time format.
 -r                     Display log events in reverse order (most recent
first).
 -s                         Display commander and standby commander log
events.
 -t                            Display log events in granularity in 10
milliseconds.
 command                 Display command logs.
 -m                      Major event class.
 -e                      Error event class.
 -p                      Performance event class.
 -w                      Warning event class.
 -i                      Information event class.
 -d                      Debug event class.
 filter                     Display log filter configuration and status
information.
 OPTION-STR              Filter events shown.
 <cr>
```

6.13 BACKUP

6.13.1 ALMACENAMIENTO LOCAL DE CONFIGURACIONES

257. El equipo permite almacenar hasta 5 ficheros de configuración que pueden utilizarse como backup o como diferentes configuraciones para diferentes escenarios.

```
2930F-8G# show config files
Configuration files:
 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *   *  | config1
  2 |             | config2
```

```
  3 |             | backup-maquetaAOS10
  4 |             |
  5 |             |
```

258. Es posible hacer backup de la configuración actual del equipo en uno de los almacenes de configuración.

```
2930F-8G# write memory
2930F-8G# copy config config1 config backup
2930F-8G# show config files
Configuration files:
 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *   *  | config1
  2 |             | config2
  3 |             | backup-maquetaAOS10
  4 |             | backup
  5 |             |
2930F-8G#
```

6.13.2 SELECCIÓN DE LA VERSIÓN Y CONFIGURACIÓN A EJECUTAR

259. La selección de la versión de firmware (partición de arranque) a ejecutar puede hacerse además seleccionando la versión de configuración a ejecutar. Es decir, además de forzar cual es la versión en el próximo reset, seleccionamos una configuración de memoria.

```
boot system flash secondary config config-otra
```

260. Podemos determinar cuál es la configuración de arranque *startup* para una partición en concreta. El equipo puede almacenará diferentes versiones de ficheros de configuración

```
Aruba-Stack-3810M# show config files
Configuration files:
 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *   *  | config1
  2 |             | config-otra
  3 |             | config2
  4 |             |
  5 |             |
Aruba-Stack-3810M#
```

261. Para determinar cuál es la configuración de arranque *startup* para una partición en concreta se ejecuta el comando *startup-default*

```
Aruba-Stack-3810M # startup-default secondary config config-otra
Aruba-Stack-3810M # show config files
Configuration files:
id | act pri sec | name
---+-------------+----------------------------
  1 |  *   *      | config1
  2 |          *  | config-otra
  3 |             | config2
  4 |             |
  5 |             |
```

6.13.3 TRANSFERENCIA DE FICHEROS: TFTP VS. SFTP Y SCP

262. TFTP deberá permanecer deshabilitado. De forma análoga al protocolo *telnet,* se trata de un protocolo inseguro y que no debe configurarse en una instalación en producción.

263. Se requiere el uso de SFTP (Secure File Transfer Protocol) y SCP (Secure Copy Protocol) para el intercambio de ficheros.

SECUENCIA DE CONFIGURACIÓN	Configuración de SCP y SFTP

Comandos necesarios	`crypto key generate ssh rsa 2048` (ver apartado 6.4.1.2 CONEXIÓN REMOTA AL EQUIPO: SSH)
	`ip ssh filetransfer`
	`TFTP and auto-TFTP are now disabled because they cannot be secured with SSH. TFTP can be re-enabled with the 'tftp' command.`

Verificación de la funcionalidad en operación	`Show running-config`
Comentarios adicionales	Es necesario generar una clave para SSH.

Tabla 62 Configuración de SCP y SFTP

264. La activación de la suite SSH desactiva por defecto el protocolo TFTP como cliente y servidor.

265. Se puede deshabilitar explícitamente TFTP

SECUENCIA DE CONFIGURACIÓN	Configuración de SCP y SFTP
Comandos necesarios	`no tftp server` `no tftp client`
Verificación de la funcionalidad en operación	`Show running-config`
Comentarios adicionales	

Tabla 63 Configuración de SCP y SFTP

266. Es posible copiar un fichero de configuración desde el equipo a un servidor de backup.

```
2930F-8G# copy config backup sftp usuario1@10.1.1.1 backup-configuracion.txt
```

7 REFERENCIAS

267. Las referencias utilizadas en la guía son:

[REF1] AOS-S Switch Software Documentation Portal (https://arubanetworking.hpe.com/techdocs/AOS-S/DocPortal/Content/home.htm)

[REF2] Portal de soporte de Aruba
https://networkingsupport.hpe.com/home

[REF3] HPE Aruba Networking 2930M/F Access Security Guide 16.11
https://arubanetworking.hpe.com/techdocs/AOS-Switch/16.11/Aruba%202930MF%20Access%20Security%20Guide%20for%20AOS-S%2016.11.pdf

[REF4] HPE Aruba Networking 2930M/F Advanced Traffic and Monitoring Guide 16.11
https://arubanetworking.hpe.com/techdocs/AOS-S/16.11/ATMG/WC/content/pdfs.htm

[REF5] HPE Aruba Networking 2930M/F Management and Configuration Guide 16.11
https://support.hpe.com/hpesc/public/docDisplay?docId=a00107096en_us

[REF6] HPE Aruba Networking Event Log Messages ArubaOS-Switch for AOS-S Switch 16.11 https://arubanetworking.hpe.com/techdocs/AOS-Switch/16.11/Event%20Log%20Message%20Reference%20Guide%20for%20AOS-S%20Switch%2016.11.pdf

[REF7] Aruba 2930F Switch Series Installation and Getting Started Guide
https://support.hpe.com/hpesc/public/docDisplay?docId=c05163011

[REF8] Aruba 2930M Switches Installation and Getting Started Guide
https://support.hpe.com/hpesc/public/docDisplay?docId=a00015161en_us

[REF9] Aruba 3810M Switches Installation and Getting Started Guide
https://support.hpe.com/hpesc/public/docDisplay?docId=c04948676

[REF10] HP 5400R zl2 Switches Installation and Getting Started Guide Power over Ethernet
https://support.hpe.com/hpesc/public/docDisplay?docId=c04344557&docLocale=en_US

[REF11] Opening Firewall ports for Device Communication
https://arubanetworking.hpe.com/techdocs/central/2.5.8/content/nms/device-mgmt/communication_ports.htm?Highlight=open%20ports

[REF12] HPE GreenLake
https://common.cloud.hpe.com/

[REF13] CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

802.1X	IEEE Standard for Port-Based Network Access Control
AAA	Authentication Authorization Accounting
ACE	Access Control Entry
ACL	Access Control List
ACLs	Access Control Lists
AES	Advanced Encryption Standard
AH	Authentication Header
AOS	Aruba Operating System
AOS-S	Aruba Operating System Switch
API	Application Programming Interface
API REST	Application Programming Interface Representational State Transfer
ARP	Address Resolution Protocol
ASP	Aruba Support Portal
BCP	Best Current Practice
BF	Back-to-Front (flujo de aire de atrás hacia adelante)
BGP	Border Gateway Protocol
BootRom	Boot Read Only Memory
BPDUs	Bridge Protocol Data Units
CA	Corriente Alterna
CAK	Connectivity Association Key
CDP	Cisco Discovery Protocol
CLI	Command Line Interface
CN	Common Name
CoPP	Control Plane Policing
CPD	Centro de Proceso de Datos

CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones
CPU	Central Processing Unit
CSR	Certificate Signing Request
DAC	Direct Attach Copper
DHCP	Dynamic Host Configuration Protocol
DLDP	Device Link Detection Protocol
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
ESP	Encapsulating Security Payload
EST	Enrollment over Secure Transport
FB	Front-to-Back (flujo de aire de adelante hacia atrás)
GCM	Galois Counter Mode
GUI	Graphical User Interface
GVRP	GARP VLAN Registration Protocol
HPE	Hewlett Packard Enterprise
HPECSS	Hewlett Packard Enterprise Code Signing Service
HSC	Hardware Switch Controller
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICK	Integrity Check Key
ICMP	Internet Control Message Protocol
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPS	Internet Protocols
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPV4	Internet Protocol Version 4
IPv6	Internet Protocol version 6
JSON	JavaScript Object Notation
KEK	Key Encryption Key
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LED	Light-Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MAC-Auth	Media Access Control Authentication
MACSEC	Media Access Control Security
MD5	Message Digest Algorithm 5
MIB	Management Information Base
MKA	MACsec Key Agreement
MSTP	Multiple Spanning Tree Protocol
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAE	Network Analytics Engine
NMS	Network Management System
NSP	Networking Support Portal

NTP	Network Time Protocol
OOBM	Out-of-Band Management
OS	Operating System
OS-CX	Operating System-CX
OSPF	Open Shortest Path First
PC	Personal Computer
PEM	Privacy-Enhanced Mail
PHY	Physical Layer
PKI	Public Key Infrastructure
PPS	Packets Per Second
PVST	Per VLAN Spanning Tree
Python	High-level Programming Language
QoS	Quality of Service
QSFP+	Quad Small Form-factor Pluggable Plus
QSFP28	Quad Small Form-factor Pluggable 28
Radius	Remote Authentication Dial-In User Service
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
REF	Reference
REST	Representational State Transfer
RFC	Request for Comments
RIP	Routing Information Protocol
RJ-45	Registered Jack 45
RMA	Return Merchandise Authorization
RMON	Remote Network Monitoring
ROM	Read Only Memory

RSA	Rivest-Shamir-Adleman
SaaS	Software-as-a-Service
SAK	Secure Association Key
SAN	Subject Alternative Name
SCP	Secure Copy Protocol
SDN	Software Defined Network
SFP	Small Form-factor Pluggable
SFP+	Small Form-factor Pluggable Plus
SFP28	Small Form-factor Pluggable 28
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm 256-bit
SHA-512	Secure Hash Algorithm 512-bit
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2
SHA256	Secure Hash Algorithm 256
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
syslog	System Log
Syslog	System Logging Protocol
SYSLOG	System Log
TA	Trust Anchor
TACACS	Terminal Access Controller Access-Control System

TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunications Network
TELNET	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTL	Time-To-Live
UDLD	Unidirectional Link Detection
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VACL	VLAN Access Control List
VLAN	Virtual Local Area Network
VLANs	Virtual Local Area Networks
VRF	Virtual Routing and Forwarding
VSF	Virtual Switching Framework
VSX	Virtual Switching Extension
WEB	Web
WebUI	Web User Interface
WLAN	Wireless Local Area Network
X.509	ITU-T Standard for Public Key Infrastructure Certificates
XMODEM	X Modem
ZTP	Zero Touch Provisioning