

MINISTERIO DE DEFENSA



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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-192-1

Fecha de Edición: Mayo de 2025



CENTRO CRIPTOLOGICO
NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2026.01.16 07:37:42 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1 INTRODUCCIÓN	4
2 OBJETO Y ALCANCE	5
3 ORGANIZACIÓN DEL DOCUMENTO	7
4 FASE PREVIA A LA INSTALACIÓN	8
4.1 ENTREGA SEGURA DEL PRODUCTO	8
4.2 ENTORNO DE INSTALACIÓN SEGURO	8
4.3 REGISTRO Y LICENCIAS	8
4.4 CONSIDERACIONES PREVIAS	9
4.5 METODOS DE GESTION	9
4.5.1 ARUBA CENTRAL	9
5 INSTALACIÓN	11
5.1 PRECAUCIONES DE INSTALACIÓN	11
6 FASE DE CONFIGURACIÓN	14
6.1 MODO DE SEGURIDAD	14
6.1.1 MODO DE SEGURIDAD STANDARD Y MEJORADO (ENHANCED)	14
6.1.2 PASSWORD DE ACCESO A SERVICIOS	15
6.2 CONEXION INICIAL	16
6.2.1 PUERTO DE CONSOLA SERIE FUERA DE BANDA	16
6.2.2 PUERTO DE RED (FUERA DE BANDA O PRODUCCION)	16
6.2.3 CONFIGURACIÓN SIN INTERVENCIÓN HUMANA – ZERO TOUCH PROVISIONING (ZTP)	17
6.2.4 APLICACIÓN MÓVIL ARUBA CX	18
6.3 CONFIGURACION INICIAL	19
6.3.1 PRIMERA CONEXION	19
6.3.2 IDENTIFICACION DEL EQUIPO	20
6.3.3 INTERFAZ FUERA DE BANDA Y VRF MANAGEMENT	20
6.3.4 VRF DEFAULT	21
6.4 ADMINISTRACIÓN DEL PRODUCTO	21
6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA	21
6.4.2 CONFIGURACIÓN DE ADMINISTRADORES	21
6.4.3 SINCRONIZACIÓN HORARIA	26
6.4.4 ALTA DISPONIBILIDAD	28
6.5 CONFIGURACIÓN DE PUERTOS	29
6.5.1 VLAN EN PUERTOS	29
6.5.2 APAGADO DE PUERTOS	30
6.5.3 LIMITE DE MAC POR PUERTO	30
6.5.4 LIMITACION DE TRAFICO DE BROADCAST	32
6.5.5 PROTECCION FRENTE A ENVIO DE MENSAJES DE CONTROL STP	33
6.5.6 LISTAS DE ACCESO	33
6.6 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS	37
6.6.1 PROTOCOLOS DE ACCESO	37
6.6.2 TRANSFERENCIA DE ARCHIVOS	38
6.6.3 PUERTO USB	38
6.6.4 SERVIDOR SSH	38
6.6.5 SERVIDOR HTTP	40
6.6.6 SERVIDOR HTTPS	40

6.6.7	ACL PARA CONTROLAR SERVICIOS DEL EQUIPO	41
6.6.8	SNMP	42
6.7	MITIGACION DE ATAQUES	43
6.7.1	DHCP SNOOPING	43
6.7.2	DYNAMIC ARP INSPECTION	43
6.7.3	CONTROL PLANE POLICING.....	44
6.8	PROTOCOLOS DE ROUTING	45
6.8.1	BGP.....	45
6.8.2	OSPF.....	47
6.9	GESTIÓN DE CERTIFICADOS	50
6.9.1	PKI EN EL SWITCH	50
6.9.2	PKI EST.....	51
6.9.3	FORMAS DE GENERACION E IMPORTACION DE CERTIFICADOS.....	51
6.10	ACTUALIZACIONES	54
6.11	AUTO-CHEQUEOS.....	55
6.11.1	VERIFICACIÓN DE SOFTWARE CUANDO ES INSTALADO AL EQUIPO	55
6.11.2	VERIFICACIÓN DE SOFTWARE CUANDO ES EJECUTADO.....	55
6.12	AUDITORÍA	56
6.12.1	REGISTRO DE EVENTOS.....	56
6.13	BACKUP	56
6.13.1	CHECKPOINTS	56
6.13.2	ROLLBACK	58
6.13.3	MODO CHECKPOINT AUTO	58
6.14	SERVICIOS DE SEGURIDAD ADICIONALES	59
6.14.1	DESACTIVACION BLUETOOTH.....	59
6.15	CONTROL DE ACCESO A LA RED	59
6.15.1	RADIUS CONTROL DE ACCESO A RED	60
6.15.2	DEFINICION DE ROLES DE USUARIO	61
6.15.3	CONFIGURACION PUERTO	63
6.16	RESETEO A FABRICA (FACTORY DEFAULTS)	64
7	FASE DE OPERACIÓN	66
7.1	SEGURIDAD	66
7.2	COPIAS DE SEGURIDAD	66
7.3	MONITORIZACION.....	66
7.3.1	NETWORK ANALYTICS ENGINE (NAE)	66
7.4	ACTUALIZACIONES FIRMWARE	68
8	CHECKLIST	69
9	REFERENCIAS.....	72
10	ABREVIATURAS.....	73

1 INTRODUCCIÓN

1. Aruba CX es la última y más reciente familia de equipos de Aruba, para conmutación y enrutamiento de redes Ethernet, comúnmente conocidos como *switches* (aún 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 Aruba CX, impulsada por el sistema operativo de red AOS-CX, simplifica las operaciones de red ofreciendo automatización, análisis distribuidos, seguridad y alta disponibilidad a las redes de campus y centros de datos. La arquitectura de microservicios en torno a la cual se construye AOS-CX ofrece análisis en toda la red y total programabilidad para permitir una garantía de red completa.
4. Los equipos de ArubaCX, 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-CX, 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 [REF1].
8. Este documento describe mecanismos y funcionalidades relacionadas con los siguientes equipos de la familia de switches/routers Aruba CX
 - a) Equipos Datacenter
 - Aruba CX 8320 Switch Series
 - Aruba CX 8325 Switch Series
 - Aruba CX 8360 Switch Series
 - Aruba CX 8400 Switch Series
 - b) Equipos Campus
 - Aruba CX 6000 Switch Series
 - Aruba CX 6100 Switch Series
 - Aruba CX 6200 Switch Series
 - Aruba CX 6300 Switch Series
 - Aruba CX 6400 Switch Series
 - c) Equipos Acceso – Ruggedizados
 - Aruba CX 4100i Switch Series
9. Los equipos mencionados han sido cualificados en el catálogo CPSTIC para categoría ENS ALTA en las familias “Switches” y “Enrutadores”.

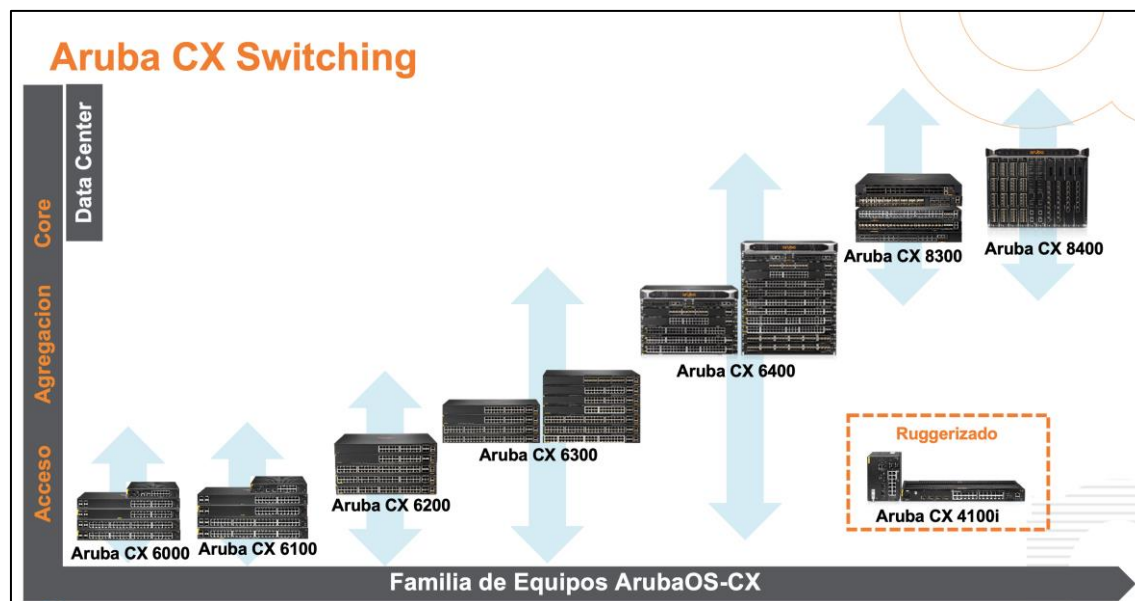


Ilustración 1 Familia de Equipos Aruba-CX

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, con independencia de cómo sea configurado.

3 ORGANIZACIÓN DEL DOCUMENTO

11. Este documento se organiza en los siguientes apartados
 - a) Apartado **4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase previa a la instalación del producto.
 - b) Apartado **5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de instalación del producto.
 - c) Apartado **6**. En este apartado se recogen las tareas recomendadas en la fase de configuración del producto, para lograr una configuración segura.
 - d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
 - e) Apartado **8**. En este apartado se recogen una checklist con las comprobaciones de las recomendaciones.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. Los equipos Aruba OS-CX 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 vengán cerradas y sin ningún tipo de daños.
13. 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.
14. Todos los equipos así como sus componentes que puedan venir embalados en cajas separadas son perfectamente identificables mediante una etiqueta donde aparecen, entre otras informaciones, el código del equipo ó componente y el número de serie del equipo ó componente.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. Los equipos Aruba OS-CX cubren una amplia gama de escenarios de trabajo, desde equipos de acceso para usuarios ó dispositivos cableados a equipos de Centros de Proceso de Datos (CPD). Desde un punto de vista de la seguridad, el equipo puede securizarse sin necesidad de ser físicamente instalado en un CPD.
16. El lugar de instalación será típicamente un rack aunque ciertos modelos pueden instalarse en una superficie plana. El detalle de los entornos de montaje soportados se describe en la guía de instalación específica del equipo.

4.3 REGISTRO Y LICENCIAS

17. Los equipos de HPE Aruba de la gama Aruba OS-CX 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 **Aruba Support Portal** [REF1].
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 **Aruba Support Portal** (ASP) requiere disponer de una cuenta. Para crear una cuenta en ASP, hay que navegar a: <https://asp.arubanetworks.com/> [REF1].
21. Es conveniente que los miembros de la organización con responsabilidad en la operación de los equipos dispongan de una cuenta en ASP 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 ASP, se puede consultar el siguiente enlace: <https://asp.arubanetworks.com/more-information>. La

creación de una cuenta en ASP puede tardar hasta un día laboral por motivos de chequeo de la información.

23. **Aruba Support Portal** proporciona las siguientes capacidades.
- a) Gestión de casos en línea
 - b) Solicitar autorizaciones de devolución de materiales (RMA)
 - c) Acceso a software, corrección de errores
 - d) Acceso a la documentación del producto
 - e) Acceso a base de conocimientos y Airheads en línea
 - f) Aruba Solution Exchange para asistencia en la configuración
 - g) Información sobre licencias

4.4 CONSIDERACIONES PREVIAS

24. Antes de la instalación del equipo conviene tener en cuenta las siguientes consideraciones.
25. 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.
26. Conviene también tener en cuenta si el equipo se va a montar con en chasis virtual o stack (VSF ó VSX). En estos casos hay que preveer 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 óptica cables DAC, ...)
27. Es importante también conocer el método elegido para la configuración inicial del equipo de cara a preparar las conexiones de consola, fuera de banda ó por el dispositivo USB bluetooth. En la sección 5.1 CONFIGURACION INICIAL se describen los diferentes métodos de configuración posibles.

4.5 METODOS DE GESTION

28. Los equipos pueden ser gestionados por dos formas:
- a) **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, SSH o API REST.
 - b) **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

29. 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
30. Para el funcionamiento de Aruba Central es necesaria una licencia por equipo Aruba-CX que se vaya a monitorizar.
31. 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.
32. Los puertos con los que el equipo se comunica se detallan en la siguiente tabla:

Fully Qualified Domain Name	Protocol and Port
activate.arubanetworks.com (used in API calls)	TCP port 443
device.arubanetworks.com	TCP port 443
devices-v2.arubanetworks.com	TCP port 443
d2vxf1j0rhr3p0.cloudfront.net	TCP port 80
common.cloud.hpe.com/ccssvc/ccs-system-firmware-registry	TCP ports 80 and 443

Tabla 1 Aruba Central: Puertos y destinos utilizados para la comunicación desde el equipo

5 INSTALACIÓN

33. Los equipos se proporcionan con sistema operativo. La configuración inicial y actualización de firmware se cubre en la sección **6 FASE DE CONFIGURACIÓN**.
34. Respecto a la instalación física del equipo, recomendamos seguir los manuales correspondientes de cada modelo.

5.1 PRECAUCIONES DE INSTALACIÓN

35. Para evitar lesiones personales o daños al producto al instalar el equipo, es necesario leer las precauciones y pautas de instalación siguientes:
 - a) No montar el equipo en una pared, sobre o debajo de una mesa, o sobre o debajo de cualquier otra superficie horizontal.
 - b) Montar los dispositivos instalados 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.
 - c) Para evitar que el bastidor o armario se vuelva inestable y / o se caiga, verificar que esté adecuadamente asegurado.
 - d) 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.
 - e) 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.
 - f) 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.
 - g) No instalar el equipo en un entorno donde la temperatura ambiente de funcionamiento exceda la especificación del equipo.
 - h) 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.
 - i) 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.
 - j) 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).

- k) 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.
36. 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:
- a) Kit de documentación
 - b) Adaptador USB Bluetooth que permite configurar el equipo desde un dispositivo móvil. Requiere la aplicación móvil Aruba CX. (El adaptador se adjunta a una tarjeta en el kit de documentación).
 - c) Cable de alimentación
37. 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 ó bien en un embalaje separado.
38. 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.
- a) Preparar el lugar de instalación. 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+/SFP28/QSFP+/QSFP28 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 o Telnet. Los cambios de configuración se pueden realizar usando un cable de consola para conectar un PC al puerto de consola del conmutador, o usar el adaptador Bluetooth incluido para configurar el equipo desde un dispositivo móvil.

- j) Conectar los dispositivos de red. Con los cables de red adecuados, conectar los dispositivos de red a los puertos del conmutador.
39. En este punto, el equipo está completamente instalado.

6 FASE DE CONFIGURACIÓN

40. El equipo se entrega con una versión de sistema operativo. Por lo tanto, puede arrancarse y es operativo.
41. El equipo arranca con una configuración básica por defecto que en esencia consiste:
 - a) Todos los puertos asignados a VLAN1
 - b) Interface IP VLAN1 con asignación de IP por DHCP
 - c) Cuenta usuario admin sin password asignada ni predeterminada (el equipo forzará a fijar una)
42. A partir de este punto por tanto se puede proceder a la configuración inicial.

6.1 MODO DE SEGURIDAD

6.1.1 MODO DE SEGURIDAD STANDARD Y MEJORADO (ENHANCED)

43. El sistema operativo AOS-CX proporciona acceso al sistema Linux subyacente, permitiendo a los administradores lanzar una sesión de shell Bash desde la línea de comandos del switch.
44. Por defecto, todas las cuentas que forman parte del grupo de administradores pueden acceder al shell utilizando el comando *start-shell*, y pueden utilizar el comando *sudo* para ejecutar comandos del shell con permisos de root. Esto permite proporcionar herramientas avanzadas de troubleshooting.
45. El uso indebido del acceso al shell podría dar lugar a la divulgación del tráfico de red sensible a un tercero no autorizado a través de la duplicación de paquetes a un dispositivo remoto, o podría causar una denegación de servicio mediante la modificación o eliminación de los archivos del sistema y hacer que el dispositivo no pueda arrancar, requiriendo la restauración del software a través de la consola de ServiceOS.
46. El acceso al shell Bash se puede deshabilitar completamente cambiando el modo de seguridad del switch. AOS-CX proporciona dos modos de seguridad que controlan el acceso a la consola del ServiceOS: *standard* y *enhanced*.
47. Otro método para limitar el acceso al shell sería utilizar un servidor de autorización TACACS+ externo y denegar el acceso al comando *start-shell* a todos los usuarios excepto a aquellos que lo requieran específicamente. Para obtener más información sobre el uso de TACACS+ para implementar la autorización de comandos, consulte la documentación de su plataforma de software TACACS+ preferida.
48. Todos los conmutadores Aruba CX funcionan en modo estándar por defecto, sin restricciones a nivel de sistema para ninguna funcionalidad. El modo de seguridad mejorado desactiva el acceso al comando *start-shell* en la CLI de AOS-CX, así como los comandos de ServiceOS *config-clear*, *password*, *sh* y *update*.
49. El cambio del modo de seguridad del conmutador se realiza desde el shell de ServiceOS, que requiere una conexión de consola al conmutador. Todos los cambios en el modo de seguridad del conmutador (de *standard* a *enhanced*, o de *enhanced* a *standard*) tienen como resultado la puesta a cero del sistema de archivos y el restablecimiento de los valores predeterminados de fábrica.

50. Para realizar el cambio de modo ejecutamos este comando para resetear el equipo en modo ServiceOS.

```
switch# boot system serviceos
One time boot to ServiceOS initiated.
Checking if the configuration needs to be saved...
This will reboot the system to ServiceOS and render
the entire switch unavailable.
Access to ServiceOS is only available through the serial console.
Continue (y/n)?
```

Secuencia 1 Reinicio del equipo en modo ServiceOS

51. Una vez que el conmutador se haya reiniciado y se muestre el indicador de inicio de sesión de ServiceOS, inicie sesión como *admin*. Utilice el siguiente comando para activar el modo de seguridad mejorado:

```
SVOS> secure-mode enhanced
#####WARNING#####
This will set the switch into enhanced secure mode. Before
enhanced secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
#####WARNING#####
Continue (y/n)?
```

Secuencia 2 Activación modo seguridad mejorado (enhanced)

52. Confirmando pulsando **y** hará que el conmutador se reinicie, ponga a cero el sistema de archivos y se reinicie una vez más.
53. Para volver al modo de seguridad estándar, reinicie el ServiceOS como se ha indicado anteriormente, inicie sesión como administrador y utilice el siguiente comando:

```
SVOS> secure-mode standard
#####WARNING#####
This will set the switch into standard secure mode. Before
standard secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
#####WARNING#####
Continue (y/n)?
```

Secuencia 3 Activación modo seguridad standard

6.1.2 PASSWORD DE ACCESO A SERVICIOS

54. Por defecto, el shell de ServiceOS (accesible sólo desde el puerto de consola del conmutador local) no requiere ninguna contraseña para iniciar sesión como *admin*; para habilitar la autenticación con contraseña para ServiceOS, utilice el siguiente comando desde el contexto de configuración:

```
switch(config)# system serviceos password-prompt
```

Secuencia 4 Activación password para ServiceOS

55. Cuando este ajuste está activado, el inicio de sesión en el shell de ServiceOS con el usuario administrador requiere la misma contraseña utilizada para autenticar al usuario administrador en la CLI o la interfaz de usuario web de AOS-CX.
56. Si este ajuste está activado, no se puede restablecer una contraseña de usuario administrador olvidada mediante ServiceOS; si no hay otras cuentas de usuario locales o RADIUS/TACACS con acceso de nivel de administrador, el conmutador debe ponerse a fábrica introduciendo el nombre de usuario zeroize en el indicador de inicio de sesión de ServiceOS para restaurar el acceso de administrador. Consulte 5.17 RESETEO A FABRICA (FACTORY DEFAULTS) a los valores predeterminados de fábrica para obtener más información.

6.2 CONEXION INICIAL

57. El equipo puede configurarse inicialmente mediante uno de estos métodos:
 - a) Puerto de Consola Serie
 - b) Puerto Ethernet Fuera de Banda
 - c) Zero Touch Provisioning (ZTP)
 - d) Aplicación Aruba CX
58. En este documento se describen los comandos que proporcionan la configuración segura del mismo, con independencia de cómo sean insertados.

6.2.1 PUERTO DE CONSOLA SERIE FUERA DE BANDA

59. Para la conexión de consola es necesario la utilización de un ordenador con un software de emulación de terminal (por ejemplo putty.exe para entornos Windows)
60. Para establecer sesión con la consola:
 - a) Conecte el puerto USB-C del conmutador al puerto USB-C del ordenador mediante un cable USB-C.
 - b) Inicie el software de emulación de terminal en el ordenador y configure una nueva sesión serie con los siguientes ajustes:
 - Velocidad: 115200 bps
 - Bits de datos: 8
 - Bits de parada: 1
 - Paridad: Ninguna
 - Control de flujo: Ninguno

6.2.2 PUERTO DE RED (FUERA DE BANDA O PRODUCCION)

61. Se puede utilizar una estación de trabajo configurada con el software de emulación de terminal VT-100 utilizando el protocolo SSH.
62. Es necesario conectar la estación de trabajo y el equipo a la misma red de gestión. En este caso se utiliza el puerto de administración fuera de banda RJ-45 del equipo. Será necesario en este caso que el equipo haya adquirido una IP por DHCP y se conozca la IP asignada.

63. El equipo puede admitir simultáneamente una sesión de consola a través del puerto de consola y varias sesiones SSH de red a través del puerto de administración.
64. Este método de conexión no se podrá usar hasta que haya credenciales de usuario definidas en el equipo.

6.2.3 CONFIGURACIÓN SIN INTERVENCIÓN HUMANA – ZERO TOUCH PROVISIONING (ZTP)

65. El término Zero Touch Provisioning (ZTP) hace referencia a la posibilidad de que el equipo se autoconfigure de forma automática con la mínima intervención humana.
66. Se utiliza ZTP para configurar un equipo automáticamente desde un servidor remoto. El equipo debe estar en la configuración predeterminada de fábrica. Si se va a utilizar ZTP, el administrador de red o el coordinador del sitio de instalación debe proporcionar un cable RJ-45 conectado a la red adecuada.
67. Se debe conectar el puerto de gestión fuera de banda o un puerto de red.
68. Es necesario conectar el equipo a la red mediante el puerto de administración fuera de banda RJ-45 y encender el equipo (o apagarlo y luego encenderlo si estaba encendido).
69. ZTP pasa al estado "Failed" si el switch recibe la IP DHCP para vlan1 y no recibe ninguna opción ZTP en los primeros minutos (de 1 a 10 en función de modelos).
70. Se pueden distinguir dos escenarios de despliegue mediante Zero Touch Provisioning (ZTP), en función del método de gestión: local o cloud.
71. En el manual *Fundamentals Guide* ([REF4]-[REF11]) del equipo a instalar se obtiene más información sobre el uso de ZTP.
72. El equipo intenta ambas formas de ZTP arrancando la primera que encuentra disponible, si alguna de las dos progresa.

6.2.3.1 ZTP CON GESTIÓN CLOUD: ARUBA CENTRAL

73. En este caso el equipo intenta establecer una sesión segura con la aplicación Aruba Central que se encuentra en Internet. Para ello el equipo intenta establecer una sesión https con alguno de los dos destinos:
 - a) device.arubanetworks.com: TCP port 443
 - b) devices-v2.arubanetworks.com: TCP port 443
74. Una vez establecida la sesión segura, el equipo será dirigido al contexto de administración correspondiente. Para ello, el administrador ha debido de dar de alta el equipo asignándole la correspondiente licencia.
75. Una vez establecida la sesión y tras verificarse las condiciones necesarias, el administrador puede proceder a la configuración del equipo desde la aplicación Aruba Central.

6.2.3.2 ZTP A SERVIDOR GESTION LOCAL

76. El conmutador envía una detección DHCP desde el puerto de gestión. En los conmutadores que admiten operaciones ZTP en los puertos de datos, también envía una detección DHCP desde todos los puertos de datos en la VLAN predeterminada.

77. El conmutador espera a recibir opciones DHCP indefinidamente o hasta que se modifique la configuración en ejecución. Si se recibe una dirección IP DHCP pero no se reciben opciones DHCP, el conmutador espera un minuto más antes de finalizar la operación ZTP.
78. Se debe configurar el servidor DHCP para proporcionar una solución de servidor ZTP basada en estándares. Las opciones y características que son específicas de las herramientas de la solución de gestión de redes (NMS), no son compatibles. Las opciones DHCP soportadas son:

Opción DHCP	Descripción
60	Vendor Class Identifier (VCI)
66	Dirección IPv4 del servidor TFTP (no se admite la especificación de un nombre de host en lugar de una dirección IP).
43 subopcion 144	Nombre del archivo de configuración
43 subopcion 144	Nombre del archivo de imagen del firmware
67	Nombre del archivo de configuración (la subopción 144 de la opción 43 tiene prioridad sobre esta opción).

Tabla 2. Opciones DHCP soportadas

79. El archivo de configuración es un archivo de texto que se convierte en la configuración de inicio y de ejecución en el conmutador después de que se complete la operación ZTP. La configuración puede estar en formato CLI o JSON.
80. El método de transferencia es mediante TFTP. Dado que este protocolo se considera no seguro, la utilización de este mecanismo debe estar complementado por verificaciones adicionales de la integridad de la configuración.
81. Se recomienda ampliar estos conceptos en los guías *Fundamentals Guide* ([REF4]-[REF11]) de cada modelo de switch.

6.2.4 APLICACIÓN MÓVIL ARUBA CX

82. Con los modelos 6200 y superiores, con cada equipo se proporciona un dongle Bluetooth USB. Conectado al puerto USB se puede hacer uso de la Aplicación móvil Aruba CX, disponible para IOS(Apple) y Android ([REF2] y [REF3])
83. La aplicación móvil Aruba CX permite configurar el equipo mediante menus y acceso a la consola mediante Bluetooth, pudiendo facilitar la operación ya instalado en su ubicación final.
84. En el manual “Fundamentals Guide” del equipo a instalar se obtiene más información sobre el uso de la aplicación móvil Aruba CX para configurar el equipo.

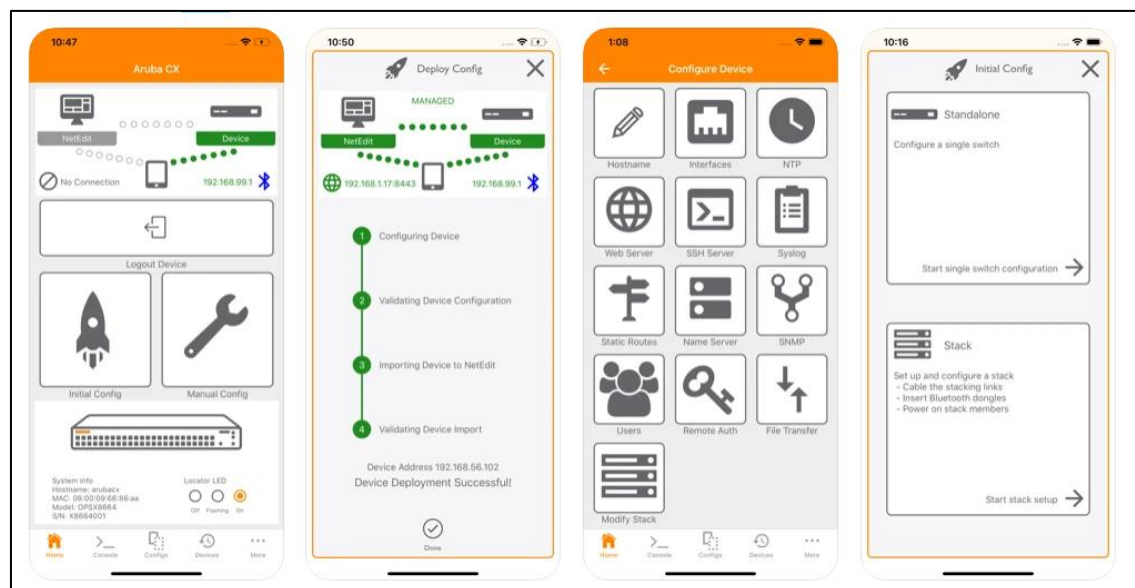


Ilustración 2 Capturas de la aplicación Aruba CX

6.3 CONFIGURACION INICIAL

6.3.1 PRIMERA CONEXION

85. En un estado predeterminado de fábrica, los dispositivos AOS-CX se configuran con el usuario predeterminado admin sin contraseña la primera vez. Inmediatamente, y sin ninguna otra opción, se pide al usuario que cree una contraseña antes de darle acceso a la CLI.
86. Se muestra una captura para un modelo 6200F.

```
(C) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.
We'd like to keep you up to date about:
* Software feature updates
* New product announcements
* Special events
Please register your products now at: https://asp.arubanetworks.com
6200 login: admin
Password:[ENTER]
Please configure the 'admin' user account password.
Enter new password: *****
Confirm new password: *****
6200#
```

Secuencia 5 Primera conexión - Asignación contraseña usuario admin

87. La interfaz de gestión integrada proporciona una forma de acceder y gestionar el conmutador que está separada del tráfico de producción. Las redes internas separadas del tráfico de producción suelen denominarse redes de gestión fuera de banda (OOBM). Limitando los clientes que pueden gestionar los dispositivos a sólo aquellos que residen en la red OOBM, limitamos drásticamente el universo de dispositivos que pueden intentar controlar el dispositivo.

88. En AOS-CX, la interfaz de gestión está lógicamente separada del resto del switch por medio de una única tabla virtual de enrutamiento y reenvío (VRF), denominada mgmt VRF.

6.3.2 IDENTIFICACION DEL EQUIPO

89. Es necesario identificar al equipo con un nombre de equipo. Para eso utilizamos el comando *hostname*

```
Hostname nombre_equipo
```

Secuencia 6 Identificación del equipo: hostname

6.3.3 INTERFAZ FUERA DE BANDA Y VRF MANAGEMENT

90. El equipo presenta como configuración al menos dos VRFs: *Default* y *Management*
91. Tenga en cuenta que el mgmt VRF es único en el sentido de que se asigna permanentemente al puerto físico de gestión y no puede asociarse a ninguna otra interfaz del switch; el propio puerto de gestión no puede asociarse a ningún otro VRF.
92. La interfaz de gestión está habilitada por defecto para aprender una dirección IP a través de DHCP.
93. Para configurar la interfaz de gestión con una dirección IP estática, puerta de enlace y DNS:

```
interface mgmt
  ip static 10.1.1.5/24
  default-gateway 10.1.1.1
  nameserver 10.0.1.10 10.0.1.11
```

Secuencia 7 Configuración interfaz Management

94. Para mostrar el estado de la interfaz de gestión fuera de banda:

```
6200# show interface mgmt

Address Mode           : static
Admin State            : up
Link State              : down
Mac Address             : b8:d4:e7:xx:xx:xx
IPv4 address/subnet-mask : 10.1.1.5/24
Default gateway IPv4    : 10.1.1.1
IPv6 address/prefix     :
IPv6 link local address/prefix:
Default gateway IPv6    :
Primary Nameserver      : 10.0.1.10
Secondary Nameserver    : 10.0.1.11
Tertiary Nameserver     :

6200#
```

Secuencia 8 Estado interfaz fuera de banda

6.3.4 VRF DEFAULT

95. El equipo presenta como configuración al menos dos VRFs: *Default* y *Management*
96. El VRF Default se asocia automáticamente con todas las interfaces que no son de gestión, incluidos los puertos enrutados de capa 3, los puertos no enrutados y las interfaces VLAN conmutadas (SVI) creadas en el conmutador, a menos que la interfaz esté explícitamente unida a otro VRF.
97. Los siguientes servicios de gestión están habilitados por defecto en un conmutador Aruba CX:
 - a) SSH en el puerto TCP 22
 - b) HTTP/HTTPS y API REST de lectura/escritura en los puertos TCP 80 y 443
98. Los conmutadores Aruba CX 8320, 8325, 8360 y 8400 se envían con estos servicios habilitados sólo en el VRF de gestión, mientras que los conmutadores 6200, 6300 y 6400 se envían con estos servicios habilitados tanto en el VRF por defecto como en el de gestión. Como la serie i4100, 6000 y 6100 no tiene un puerto de gestión dedicado o el VRF asociado, los servicios de gestión están habilitados sólo en el VRF por defecto.
99. Para una seguridad óptima, Aruba recomienda encarecidamente gestionar los switches desde una red de gestión dedicada, cuando sea posible, y deshabilitar los servicios de gestión en todas las demás VRFs.

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

100. El equipo puede ser gestionado mediante una conexión remota a través de los puertos Ethernet que dispone. A través de protocolos basados en la arquitectura TCP/IP como SSH, HTTPS y a través de una API REST se puede acceder a la configuración del equipo y a la obtención de información de configuración y rendimiento de este.
101. No se dispone de acceso a través de protocolos no seguros como telnet.
102. Ver 5.7 CONFIGURACION DE PROTOCOLOS Y SERVICIOS para su configuración y protección de acceso así como medios de acceso remoto.

6.4.2 CONFIGURACIÓN DE ADMINISTRADORES

103. ArubaOS-CX permite tres métodos de autenticación de usuarios de gestión:
 - Local: Los usuarios y sus password son almacenadas en la base de datos del propio switch
 - RADIUS: Utilizando uno o varios servidores RADIUS para autenticar usuarios
 - TACACS+: Utilizando uno o varios servidores TACACS+ para autenticar usuarios

6.4.2.1 AUTENTICACION LOCAL.

104. Las cuentas de usuario local pueden ser asignadas a unos de los dos grupos de usuarios que proporcionan diferente nivel de acceso al switch:
 - Administradores: acceso completo

- Actualización de firmware
- Cambios de configuración
- Visualización de la información de configuración del switch incluyendo información sensible como password
- Añadir o eliminar usuarios locales o cambiar sus passwords
- Todos los métodos de REST API ((GET, PUT, POST, PATCH, DELETE))
- Privilege level 15
- Operadores: acceso limitado
 - Acceso Display-Only
 - Ver información no sensible de la configuración
 - Solo método GET a través de la REST API
 - Privilege level 1

105. Ejemplo de como crear un usuario como administrador

```
switch(config)# user localadmin group administrators password
Enter password: *****
Confirm password: *****
```

Secuencia 9 Creación de un usuario local con permisos de administración

106. Configuración de usuarios con password introducida en texto en claro:

```
switch(config)# user localoperator group operators password plaintext I-h@ve-Read-0n1y-Acc3ss!
```

Secuencia 10 Creación de un usuario local con permisos de operador y clave introducida en texto plano

107. La password puede ser introducida en formato claro o encriptado (lo cual facilita el registro de configuraciones con estas definiciones incluidas), el formato del comando es:

```
switch(config)# user <USERNAME> group {administrators | operators | auditors | <USER-GROUP>}
password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
```

Secuencia 11 Formatos posibles de introducción de claves de password

108. El campo usuario tiene como máximo una longitud de 32 caracteres y no puede contener ciertos nombre Linux reservados. La longitud de la password máxima será también de 32 caracteres.

109. Para visualizar los grupos de usuarios o nombres de usuarios se utilizará:

```
show user-group [<GROUP-NAME>] [vsx-peer]
show user information
show user-list [vsx-peer]
```

Secuencia 12 Comandos para inspeccionar los usuarios y sus grupos

6.4.2.1.1 COMPLEJIDAD DE LA PASSWORD

110. Se pueden definir criterios de complejidad de la password a través del comando *password complexity*:

```
como por ejemplo:
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 3
switch(config-pwd-cplx)# minimum-length 8
switch(config-pwd-cplx)# position-changes 10
switch(config-pwd-cplx)# lowercase-count 2
switch(config-pwd-cplx)# uppercase-count 2
switch(config-pwd-cplx)# numeric-count 2
switch(config-pwd-cplx)# special-char-count 2
switch(config-pwd-cplx)# enable
switch# exit
```

Secuencia 13 Complejidad mínima de la password de los usuarios

111. De las opciones posibles:

- a) History count: Impide reutilización de passwords anteriores en esa cuantía
- b) Position-Change: Relativo a cambios de orden de palabras sobre password anteriores
- c) Siendo las demás opciones autodescriptivas.

6.4.2.1.2 LONGITUD MÍNIMA DE LA PASSWORD

112. Los administradores de sistemas pueden especificar la longitud mínima de la password mediante el siguiente comando. Por ejemplo para requerir una password mínima de longitud 12 sería:

```
switch(config)# aaa authentication minimum-password-length 12
```

Secuencia 14 Longitud mínima de la password de los usuarios locales**6.4.2.1.3 LIMITACIÓN DE LOS INTENTOS DE LOGIN FALLIDOS.**

113. Se puede limitar el número de intentos de login fallidos para autenticaciones locales mediante el siguiente comando:

```
switch(config)# aaa authentication limit-login-attempts <ATTEMPTS> lockout-time <LOCKOUT-TIME>
```

Secuencia 15 Número de intentos y bloqueo en caso de fallos de login**6.4.2.2 AUTENTICACION REMOTA RADIUS**

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

115. El servidor externo de autenticación a utilizar debe soportar el protocolo RADIUS (RFC 2865). Por ejemplo, la autenticación RADIUS está soportada en el gestor Aruba ClearPass Policy Manager de Aruba HPE. En el ámbito del software libre, se puede utilizar FreeRADIUSn(freeradius.org).

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

```
Aruba# show aaa authentication
```

Secuencia 16 Inspeccionar metodos de autentiación en uso en el equipo

117. Se permite la configuración de múltiples servidores RADIUS, así como agruparlos para proporcionar un mecanismo de redundancia en caso de fallo de alguno de ellos. Para definir un servidor RADIUS y, opcionalmente, la clave de sesión a utilizar se utiliza el comando

```
Aruba(config)# radius-server host <dir-IP> key <clave> vrf default
```

Secuencia 17 Definición de un servidor RADIUS

118. Con los servidores definidos, se puede crear un grupo de servidores, que posteriormente sea invocado.

```
radius-server host radius1.dominio.com key ciphertext XXXXXXXXXX
radius-server host radius2.dominio.com key ciphertext YYYYYYYYYY
aaa group server radius grupo_radius
    server radius1.dominio.com
    server radius2.dominio.com
!
```

Secuencia 18 Definición de servidores RADIUS y un grupo de servidores

119. Para habilitar la autenticación RADIUS como primer método y como secundario la autenticación local el comando de configuración sería:

```
switch(config)# aaa authentication login default group grupo_radius local
```

Secuencia 19 RADIUS como primer método de autenticación de usuarios locales

6.4.2.3 AUTENTICACION REMOTA TACACS

120. En ArubaOS es posible también gestionar el acceso a la configuración de los equipos de forma centralizada mediante servidores TACACS+. Al igual que RADIUS, la autenticación basada en TACACS+ está soportada en el gestor Aruba ClearPass Policy Manager.

121. La gestión de los servidores TACACS+ es muy similar a la de RADIUS: es posible configurar más de un servidor TACACS+ para proporcionar mayor disponibilidad; se pueden especificar grupos de servidores TACACS+ para asociarlos a distintos servicios; o se puede especificar la autenticación local como método de respaldo en caso de perder la conectividad con los servidores TACACS+. Los comandos que utilizar para TACACS+ son muy similares a los de RADIUS. Por ejemplo, para definir autenticación vía TACACS+ para el acceso a la gestión:

```
Aruba(config)# [no] aaa authentication login <console|default|https-server|ssh> group <GROUP_LIST>
```

Secuencia 20 Configuración de autenticación local TACACS

122. Siendo el significado de los parámetros el mismo que en el caso de RADIUS.

123. Para definir un servidor TACACS es necesario introducir el siguiente comando:

```
Aruba(config)# [no] tacacs-server host <dir-IP> key KEY-STR
```

Secuencia 21 Definición de un servidor TACACS

124. Por ejemplo

```
tacacs-server tacacs.dominio.com key ciphertext XXXXXXXXXX
tacacs-server tacacs.dominio.com key ciphertext YYYYYYYYYY
aaa group server radius grupo_tacacs
    server tacacs.dominio.com
    server tacacs.dominio.com
!
```

Secuencia 22 Ejemplo definición servidores TACACS y grupo de servidores

125. Dentro del servidor TACACS+, para proporcionar el nivel correcto de privilegios es necesario especificar el atributo “Max-privilege” en las credenciales del usuario. Si Service-Type = 15 se proporciona acceso en modo manager y si Service-Type = 14 o menor, se proporciona acceso en modo operator.

126. TACACS permite como ventaja sobre RADIUS, activar autorización y registro de accesos. Esto se configuraría así:

```
switch(config)# aaa authorization commands default group grupo_tacacs
switch(config)# aaa accounting all default start-stop group grupo_tacacs
```

Secuencia 23 Activación de registros de accesos y autorización de comandos

127. Para mas informacion sobre TACACS+ puede consultarse la guía “Access Security Guide” de cada producto.

6.4.2.4 CONFIGURACION ADICIONAL SESIONES CLI

128. Los administradores pueden establecer un número máximo de sesiones de gestión CLI concurrentes por usuario, así como un tiempo de espera de la sesión que cerrará automáticamente una sesión CLI después de un período de inactividad.

129. Por defecto, AOS-CX permite hasta 5 sesiones CLI concurrentes para cada cuenta de usuario. Este valor se puede cambiar desde el contexto cli-session con el comando *max-per-user*. Para establecer un máximo de 2 sesiones concurrentes por usuario:

```
switch(config)# cli-session
switch(config-cli-session)# max-per-user 2
```

Secuencia 24 Limitación de sesiones CLI por usuario

130. Los usuarios de la sesión CLI conectados pueden ser desconectados automáticamente después de un período de inactividad especificado. Por defecto, el tiempo de espera de la sesión CLI se establece en 30 minutos, y puede cambiarse desde el contexto cli-session utilizando el comando *timeout*. Para establecer un período de tiempo de espera de 5 minutos:

```
switch(config-cli-session)# timeout 5
```

Secuencia 25 Temporizador para desconexión de usuarios

131. El período de tiempo de espera de la sesión puede establecerse entre 0 (sin tiempo de espera) y 43.200 minutos (30 días). El temporizador sólo se aplica a las sesiones de la CLI, no a la interfaz web.

6.4.2.5 BANNER DE ACCESO

132. El período de tiempo de espera de la sesión puede establecerse entre 0 (sin tiempo de espera) y 43.200 minutos (30 días). El temporizador sólo se aplica a las sesiones de la CLI, no a la interfaz web.

133. En el relación al acceso al equipo dentro de las buenas prácticas estaría añadir en el acceso un banner notificando las condiciones de acceso al equipos, este banner se configuraría de la siguiente manera:

```
switch(config)# banner motd %
Enter a new banner. Terminate the banner with the delimiter you have chosen.
switch(config-banner-motd)# =====
switch(config-banner-motd)#           Este es un sistema privado
switch(config-banner-motd)#. Abandone la conexión si no esta autorizado.
switch(config-banner-motd)# =====
switch(config-banner-motd)# %
```

Secuencia 26 Ejemplo de definición de un banner de acceso

134. Desde un cliente SSH el acceso queda así:

```
% ssh admin@switch_arubacx
=====
Este es un sistema privado
Abandone la conexión si no esta autorizado.
=====
admin@10.218.10.132's password:
Last login: 2022-02-18 17:23:02 from 10.218.10.244
User "admin" has logged in 5 times in the past 30 days
6200#
```

Secuencia 27 Captura de acceso al equipo, con banner configurado

135. El banner también se muestra en las conexiones web al equipo.

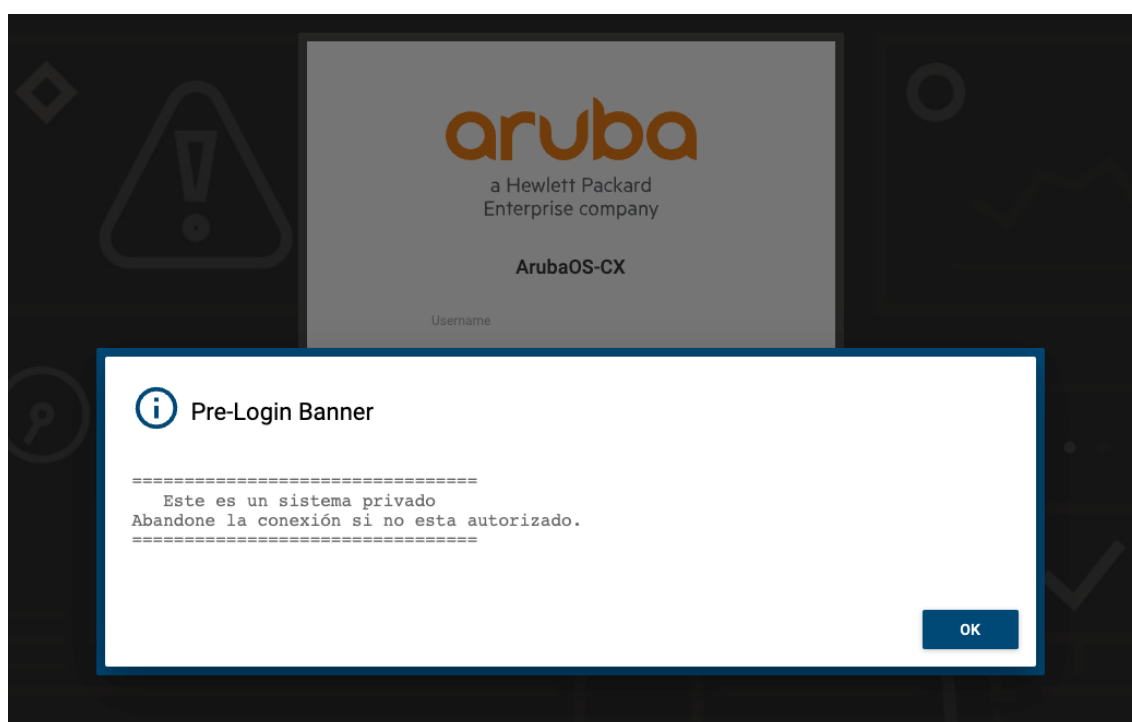


Ilustración 3 Banner presentado en acceso GUI al equipo

6.4.3 SINCRONIZACIÓN HORARIA

136. Los equipos ArubaCX soportan la sincronización del reloj interno con servidores de hora externos mediante los protocolos TimeP, NTP (Network Time Protocol).
137. Para evitar posibles ataques relacionados con el protocolo NTP (p. ej., aquellos que buscan cambiar la hora de los equipos para realizar ataques del tipo reply o simples ataques DoS), es muy recomendable que los servidores de NTP utilizados en la organización tengan activada la opción de autenticación. De esta forma se pueden autenticar los mensajes intercambiados entre clientes y servidores, dificultando con ello la mayoría de los ataques.

138. Para configurar que el equipo forme parte del servicio NTP de la red es necesario: habilitar la autenticación; configurar las claves de autenticación; configurar los servidores NTP desde los cuales sincronizarse; definir la instancia VRF desde la que se alcanzará el sincronizador y, por último, habilitar NTP si estaba previamente deshabilitado (por defecto está habilitado).

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

a) Habilitar autenticación NTP

```
Aruba-CX(config)# ntp authentication
```

Secuencia 28 Habilitar autentiación en NTP

b) Configurar las claves de autenticación, así como su identificador y el tipo de cifrado (se recomienda usar SHA1).

```
Aruba-CX(config)# ntp authentication-key <KEY-ID> {md5 | sha1} <PASSWORD> [trusted]
```

Secuencia 29 Configurar claves de autenticación en NTP

c) Definir los servidores NTP hasta un máximo de 8 servidores, por lo que se podrá repetir este comando tantas veces como se desee hasta completar los 8 y pudiendo definir alguno de ellos como preferido.

```
Aruba-CX(config)# ntp server <IP-ADDR> [key <KEY-NUM>] [prefer]
```

Secuencia 30 Definir los servidores NTP con su preferencia

d) Definir la instancia VRF que se utilizara para establecer la conexión con el servidor NTP y actualizar así el dispositivo.

```
Aruba-CX(config)# ntp vrf <VRF-NAME>
```

Secuencia 31 Configurar la VRF de trabajo para NTP

e) Habilitar NTP. Esta opción está habilitada por defecto por lo que sería necesaria en el caso de que por algún motivo se hubiese deshabilitado anteriormente.

```
Aruba-CX(config)# ntp enable
```

Secuencia 32 Habilitar NTP

140. Finalmente se puede comprobar la configuración NTP con los siguientes comando:

```
Aruba-CX(config)# show ntp status
NTP Status Information
NTP                               : Enabled
NTP Authentication                : Enabled
NTP Server Connections            : Using the default VRF
System time                       : Mon May 10 15:13:23 CEST 2021
NTP uptime                       : 1 days, 3 hours, 17 minutes, 25 seconds
NTP Synchronization Information
NTP Server                       : 192.168.2.116 at stratum 4
Poll interval                    : 1024 seconds
Time accuracy                    : Within 0.006468 seconds
Reference time                   : Mon May 10 2021 14:49:25.970 as per Europe/Madrid
```

Secuencia 33 Verificar estado NTP

141. Comando para chequear los sincronizadores de tiempo a los que está vinculado el dispositivo:

```
Aruba-CX(config)# show ntp associations
```

ID	NAME	REMOTE	REF-ID	ST	LAST	POLL	REACH
* 1	DC-01.lab.com	192.168.2.116	162.159.200.123	4	705	1024	377
+ 2	time.cloudflare.com	162.159.200.123	10.40.9.201	3	596	1024	377

Secuencia 34 Estado de asociaciones NTP

142. Para mostrar las claves de autenticación definidas:

Aruba-CX(config)# show ntp authentication-keys			
Key ID	Trusted	Type	Encrypted Key
1	No	SHA1	AQBapbhBuAX7PxpennLcFfk5xBiD9K4+wnZHKu1/mqxewNs0CgAAAJaTpzSrC9NI3yE=

Secuencia 35 Mostrar claves autenticación NTP

6.4.4 ALTA DISPONIBILIDAD

143. La alta disponibilidad de los equipos se proporciona mediante la constitución de chassis virtual o bien de stacks de equipos.

144. Los equipos de las familias 8300, 8400 y 6400 utilizan Aruba VSX. Las familias 6200 y 6300 utilizan Aruba VSF. Los equipos 6100, 6000 e i4100 no hacen stack.

6.4.4.1 ARUBA VSX

145. Aruba VSX se caracteriza por que dos equipos pasan a formar un equipo virtual. Cada miembro de los equipos mantiene su plano de control propio, y su autonomía operativa, pero sincronizan el estado de algunas de sus funciones para proporcionar una percepción que se trata de un solo equipo.

146. En Aruba VSX a modo cada equipo tiene su propio direccionamiento, y

147. En otras palabras, con Aruba VSX dos equipos se presentan en la red como un solo equipo a Nivel 2 pero como dos equipos a Nivel 3.

148. Las principales ventajas que aporta Aruba VSX son la alta disponibilidad y continuidad en el servicio, así como poder liberar de la necesidad de hacer usos de protocolos como Spanning Tree que se han demostrado problemáticos en la operación.

149. La decisión de hacer uso o no de Aruba VSX tiene por tanto un carácter de arquitectura y diseño funcional de la red. Las medidas de seguridad recomendadas son las mismas con VSX que un equipo individual.

6.4.4.2 ARUBA VSF

150. Aruba VSF es una tecnología de stack o apilamiento de equipos. Tiene la característica que se realiza por puertos de red estándar. Esto permite que los equipos agrupados puedan estar adyacentes o bien separados físicamente. Esto aporta sencillez a los diseños de red.

151. Aruba VSF hace que todos los equipos tengan se comporten como un equipo tanto a nivel 2 como a nivel 3, se ejecuta la misma versión de software en todos los equipos.

152. La decisión de hacer uso o no de Aruba VSF tiene por tanto un carácter de arquitectura y diseño funcional de la red. Las medidas de seguridad recomendadas son las mismas con VSF que un equipo individual.

6.5 CONFIGURACIÓN DE PUERTOS

6.5.1 VLAN EN PUERTOS

153. Las LAN virtuales o VLAN constituyen la funcionalidad básica de los conmutadores actuales para crear redes separadas dentro del mismo conmutador. A grandes rasgos, una VLAN es una forma de virtualizar un conmutador, creando múltiples redes lógicas sobre un mismo conmutador físico.
154. Cada puerto de un conmutador debe pertenecer a al menos una VLAN. El tráfico enviado por los sistemas conectados a cada VLAN queda confinado en esa VLAN: cada VLAN constituye un dominio de broadcast diferente. En este sentido, el uso de VLAN permite reducir el tráfico de difusión en las redes, confinando a cada VLAN los efectos de los problemas tales como las tormentas de broadcast.
155. Un puerto puede pertenecer a varias VLAN distintas, en cuyo caso se debe configurar en modo etiquetado. Es el caso habitual de los enlaces entre conmutadores o de los puertos conectados a servidores. Los puertos conectados a sistemas de usuarios suelen pertenecer a una única VLAN y estar configurados en modo no etiquetado.
156. Las VLAN pueden expandirse a varios conmutadores, de forma que sistemas conectados a conmutadores distintos pueden pertenecer a la misma VLAN.
157. La conexión entre VLAN debe realizarse a nivel 3, mediante routers externos o servicios de encaminamiento implementados en los propios conmutadores. En ArubaOS-CX, la configuración inicial del equipo consta de una única VLAN ya creada (VLAN 1), a la que pertenecen por defecto todos los interfaces. Para evitar posibles problemas en la red cuando se interconectan switches, es recomendable no utilizar dicha VLAN y crear una nueva VLAN en la que se agrupen todos los puertos inactivos.
158. Para crear una VLAN basta con realizar:

```
vlan <VLAN-LIST>
```

Secuencia 36 Creación de una VLAN en AOS-CX

159. Donde VLAN_ID debe ser un identificador no usado del rango de VLAN permitido (2-4040). Para que un puerto pertenezca a una vlan en el modo etiquetado (tagged) o no etiquetado (untagged) se utiliza el comando ejecutado desde el contexto del interfaz

```
switch(config)# interface 1/1/12
switch(config-if)# description PUERTO EN ACCESO VLAN 10
switch(config-if)# vlan access 10
switch(config)#
switch(config)# interface 1/1/2
switch(config-if)# description PUERTO EN TRUNK con VLAN 20 nativa y 2,3,4 etiquetadas
switch(config-if)# vlan trunk native 20
switch(config-if)# vlan trunk allowed 2,3,4
switch(config)#
```

Secuencia 37 Asignación de VLANs a puertos

160. Cuando se configuran las VLANs y los puertos que pertenecen a ella hay que tener especial cuidado en introducir estrictamente los puertos que se hayan considerado de uso necesario.
161. Existen soluciones que permiten automatizar la distribución de la información sobre las VLAN creadas en cada conmutador y evitar la configuración manual de la pertenencia a las VLAN creadas en los enlaces troncales entre conmutadores.
162. El protocolo GVRP (GARP VLAN Registration Protocol) o su sucesor MVRP (Multiple VLAN Registration Protocol) se utilizan para esta función. Su funcionamiento se basa en el intercambio de información entre conmutadores a través de los enlaces en los que están activados.
163. En ArubaOS-CX se dispone MVRP (recomendado frente a GVRP), cuando se activa el protocolo con el comando siguiente de modo global.
164. MVRP tiene interrelación con Spanning-Tree, por lo que es necesario conocerlo con cierto detalle, en caso que se desee utilizar.

6.5.2 APAGADO DE PUERTOS.

165. En determinados escenarios, una medida de seguridad básica consiste en deshabilitar todos aquellos puertos del conmutador que no se estén utilizando, con el objeto de evitar que alguien pueda conectar equipos no autorizados a esos puertos.
166. Para bloquear o cerrar los puertos no utilizados:

```
switch(config)# interface <interface>
switch(config-if)# [no] shutdown
```

Secuencia 38 Dehabilitación de un puerto

167. Para conocer el estado de los puertos se puede utilizar el comando:

```
show interface brief
```

Secuencia 39 Verificación del estado de los puertos

6.5.3 LIMITE DE MAC POR PUERTO

168. ArubaOS-CX proporciona medidas específicas para poder configurar la seguridad a nivel de puerto de una forma precisa, definiendo qué equipos (direcciones MAC) pueden conectarse o limitando el número máximo de equipos que se conectan a cada puerto.
169. Permite, además, configurar la generación de alarmas o incluso el bloqueo de los puertos en caso de que se detecten accesos no permitidos.
170. Para poder configurar estas funcionalidades es necesario tener un inventario de las direcciones físicas de los equipos que se van a conectar o una estimación de cuantos equipos se conectan en cada puerto. Asimismo, es necesario introducir algunos conceptos previos para conocer cuál de las configuraciones posibles se adapta mejor a nuestras necesidades.
171. Cuando se activa el control de seguridad en un puerto, se puede configurar:

- a) La funcionalidad se activa de forma global en la configuración

```
port-access port-security enable
```

Secuencia 40 Activación funcionalidad port-security

- b) El número máximo de direcciones MAC permitidas se configura con el comando *client-limit* dentro del interfaz.

```
interface 1/1/2
  no shutdown
  no routing
  vlan access 1
  port-access port-security
  client-limit 2
```

Secuencia 41 Ejemplo limitación de dispositivos por puerto

- c) Si se desean, se pueden configurar las direcciones MAC permitidas. Se configuran mediante el comando *mac-address* dentro del interfaz

```
interface 1/1/3
  no shutdown
  no routing
  vlan access 1
  port-access port-security
    mac-address aa:bb:cc:dd:ee:01
    mac-address aa:bb:cc:dd:ee:02
```

Secuencia 42 Definición de MACs concretas permitidas por puerto

172. Es importante tener en cuenta que las direcciones MAC aprendidas de forma dinámica se almacenan en la tabla de filtrado del switch durante un tiempo máximo (unos minutos típicamente) siguiendo el algoritmo estándar de los conmutadores Ethernet. Además, si el conmutador se reinicia se eliminan. Por el contrario, las direcciones configuradas de forma estática se añaden a la configuración del conmutador, por lo que se conservan en la tabla de filtrado tras un rearranque del equipo.
173. Una vez activada la seguridad en un puerto del conmutador pueden producirse situaciones que violen los límites de seguridad definidos, bien porque el número máximo de direcciones MAC seguras en un puerto se ha alcanzado, o bien porque una dirección aprendida en un interfaz se ha detectado en otro interfaz de la misma VLAN.
174. Para detectar este tipo de situaciones, denominadas intrusiones, los conmutadores Aruba permiten definir una política de reacción frente a este tipo de eventos mediante el parámetro *action* del comando *port-security*:

```
port-access security violation action [notify | shutdown]
```

Secuencia 43 Definición de la acción asociada en caso de exceso de dispositivos por puerto

175. Se define el modo de proceder cuando se detecte un evento de las características descritas:
- a) Notify: lo notifica a través de un evento o log en el servidor syslog
 - b) Shutdown: tira el puerto que ha superado el límite
176. Para este último modo existe un comando para recuperación automática:

```
port-access security violation action shutdown auto-recovery [enable | disable]
```

Secuencia 44 En caso de exceso de dispositivos, y acción programada shutdown, auto-habilitación habilitada

177. Finalmente, para conocer la configuración de seguridad de los puertos del equipo se puede usar el comando:

```
show port-access security
```

Secuencia 45 Inspección del estado de seguridad de los puertos

6.5.4 LIMITACION DE TRAFICO DE BROADCAST

178. Una tormenta de broadcast consiste en la presencia de un volumen de tráfico excesivo enviado a la dirección de difusión (broadcast) de la LAN. Dado que por definición el tráfico enviado a broadcast debe ser replicado en todos los puertos del conmutador, esto puede provocar un consumo excesivo de recursos del equipo y de ancho de banda de la red para hacer frente a este tráfico. En casos graves, incluso puede causar el colapso total del conmutador y de la red.
179. El origen de las tormentas de broadcast puede ser variado, aunque principalmente se producen por dos motivos: que existan bucles en la red y que no se tenga activado el protocolo Spanning Tree para gestionarlos; o que existan dispositivos finales que generen mucho tráfico de difusión o que retransmitan el tráfico enviado a la dirección de difusión que reciben de vuelta a la red.
180. En este último caso, el origen del tráfico puede deberse a la configuración errónea de un dispositivo o a un ataque de denegación de servicio, como, por ejemplo, los ataques conocidos como ataques Fraggie o Smurf.
181. En estos ataques, se generan paquetes de tipo UDP o ICMP suplantando la dirección de origen de la víctima y enviados a la dirección de broadcast de una subred IP. Cuando todas las máquinas conectadas a ella responden, generan una tormenta de respuestas hacia la víctima, consumiendo el ancho de banda de la red y congestionando el sistema atacado.
182. Para prevenir este tipo de ataques o los efectos de una configuración errónea, es importante implementar medidas que limiten el tráfico de tipo broadcast, de forma que nunca llegue a consumir todos los recursos de la red y quede un margen para que el equipo pueda seguir teniendo conectividad y no se quede aislado.
183. ArubaOS-CX proporciona comandos para limitar el ancho de banda consumido por el tráfico de difusión. La configuración se realiza para cada puerto del conmutador, por lo que se pueden implementar políticas de limitación distintas para cada tipo de interface (acceso, inter-switch, etc.).

184. Para limitar el ancho de banda consumido por el tráfico de difusión en un puerto:

```
rate-limit {broadcast | multicast | unknown-unicast} <RATE> { pps | kbps }
```

Secuencia 46 Definición de tasa límite de tráfico de difusión por puerto

185. Por ejemplo, para limitar 4000pps el tráfico de difusión que entra por el interfaz 3:

```
switch(config)# interface 1/3/3
switch(config-if)# rate-limit multicast 4000 pps
```

Secuencia 47 Ejemplo de definición de tasa límite de tráfico multicast por puerto

186. No existe una recomendación general sobre el valor límite de tráfico de difusión, ya que depende de cada entorno particular. Sin embargo, un valor entre el 5 y 10% puede ser razonable para la mayoría de los casos.

187. Es posible con este mismo comando controlar otros tipos de tráfico, como el tráfico multicast, etc:

```
switch# config
switch(config)# interface 1/3/3
switch(config-if)# interface lag 100
switch(config-if)# rate-limit broadcast 50 pps
```

Secuencia 48 Secuencia 46 Ejemplo de definición de tasa límite de tráfico broadcast por puerto

6.5.5 PROTECCION FRENTE A ENVIO DE MENSAJES DE CONTROL STP

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

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

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

191. Para activar la protección frente al envío de BPDUs en un conjunto de puertos, se debe utilizar el comando:

```
spanning-tree bpduguard
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpduguard
```

Secuencia 49 Protección de mensajes BPDU en puerto

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

193. Adicionalmente, es posible generar una alarma (trap) de SNMP para avisar al gestor de red del evento detectado. Para ello hay que ejecutar el comando:

```
spanning-tree trap {new-root|topology-change [instance <0-64>] | errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}
switch(config)# spanning-tree trap errant-bpdu
```

Secuencia 50 Configuración de generación de alarma en caso de BPDU

194. Para ver la configuración relativa a la protección frente a envío de BPDUs se puede ejecutar el comando:

```
show spanning-tree detail
```

Secuencia 51 Inspección del estado del Spanning-Tree

6.5.6 LISTAS DE ACCESO

195. Las listas de acceso (Access Control List o ACL) son un método de filtrado de flujos de datos. Pueden ser usadas para restringir el acceso a la gestión del equipo y para realizar

el filtrado de tráfico que atraviesa el equipo. Aplicadas a los conmutadores, las ACLs se basan en un conjunto de reglas básicas (Access Control Entries o ACE) que determinan la autorización (reglas de tipo permit) o denegación (reglas de tipo deny) del tráfico en función de campos de las cabeceras de los paquetes tales como las direcciones IP y puertos, tanto origen como destino, o el protocolo.

196. Por cada paquete recibido, las reglas que componen una ACL se evalúan línea a línea hasta que se encuentra una coincidencia. Por esta razón, hay que definir primero las reglas más específicas y posteriormente las más generales. Es importante recordar que las listas de acceso tienen una denegación implícita al final (todo el tráfico se filtra por defecto salvo que se permita explícitamente). Por ello, en el caso en que queramos restringir un determinado tráfico, debemos asegurarnos de permitir el resto de tráfico en una regla final.
197. En ArubaOS-CX las ACL pueden aplicarse, entre otros, a puertos específicos o a VLANs completas. También es posible definir ACLs asociadas a usuarios o grupos de usuarios concretos que se cargan dinámicamente desde servidores RADIUS tras el proceso de autenticación. Por ello, es importante tener en cuenta que varias ACLs pueden estar aplicándose simultáneamente a un determinado tráfico.
198. ArubaOS-CX permite crear listas de acceso tanto para IPv4 como IPv6. Aunque solo se muestran en este apartado los principales comandos para crear listas para IPv4, su utilización para IPv6 es inmediata, sin más que cambiar el formato de las direcciones.

6.5.6.1 TIPOS DE ACLS.

199. Existen dos tipos de ACL según el procedimiento usado para definirlos: estáticas o dinámicas.
 - a) Las ACLs estáticas se configuran mediante comandos en el propio equipo. Pueden ser usadas para asignarlas a puertos o a VLANs con el objeto de restringir el tráfico entrante o saliente.
 - b) Por el contrario, una ACL dinámica no se define en el propio equipo, sino que se configura en un servidor RADIUS y se carga dinámicamente en el conmutador como resultado de un proceso de autenticación. La existencia de las ACL dinámicas está ligada a la sesión de autenticación: una vez el cliente cierra la sesión, se libera la ACL.
200. En este apartado nos centramos únicamente en las ACL estáticas.
201. Según su tipo, tenemos listas de acceso de tráfico de tráfico IP o nivel 3 (IPv4 y IPv6) así como ACLs tipo MAC, de tráfico Ethernet o nivel 2.

6.5.6.2 CREACION DE ACLS

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

```
switch(config)# access-list ip <ACL-NAME>
switch(config-acl-ip)# [<SEQUENCE-NUMBER>]
{permit|deny}
{any|ip|ah|gre|esp|igmp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]}|<ADDRESS-GROUP>}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]}|<ADDRESS-GROUP>}
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count] [log]
```

Secuencia 52 Estructura de la definición de una ACL de IP

203. Se recomienda identificar las listas con nombres y que estos sean descriptivos (p.ej.:DENY-PORT-23, DENY-HOST-X, etc.). Recomendamos consultar los manuales y otros recursos didácticos para profundizar en ejemplos y detalles de configuración.

204. Veamos un ejemplo de definición de ACL:

```
switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 10 permit udp any 172.16.1.0/24
switch(config-acl-ip)# 30 permit tcp 172.26.1.0/24 any syn ack dscp 10
switch(config-acl-ip)# 40 deny any any any count
switch(config-acl-ip)# exit
```

Secuencia 53 Ejemplo de definición de una ACL

205. Para añadir una nueva línea es importante tener en cuenta la numeración ya definida. En este ejemplo se añade un comentario:

```
switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 20 comment Permit all TCP ephemeral ports
switch(config-acl-ip)# exit
```

Secuencia 54 Ejemplo ACL: nuevas líneas añadidas

206. La ACL quedaría definida así:

```
access-list ip MY_IP_ACL
  10 permit udp any 172.16.1.0/255.255.255.0
  20 comment Permit all TCP ephemeral ports
  30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
  40 deny any any any count
```

Secuencia 55 Ejemplo de ACL definida tras añadido

207. Para mostrar las listas de acceso configuradas en un conmutador o los detalles de alguna de ellas se pueden utilizar los comandos:

```
switch# show access-list

Type      Name
Sequence  Comment
          Action          L3 Protocol
          Source IP Address Source L4 Port(s)
          Destination IP Address Destination L4 Port(s)
          Additional Parameters
-----
IPv4      MY_IP_ACL
          10
          permit          udp
          any
          172.16.1.0/255.255.255.0
          20 Permit all TCP ephemeral ports
          30
          permit          tcp
          172.26.1.0/255.255.255.0
          any
```

```

dscp: AF11
ack
syn
40
deny          any
any
any
Hit-counts: enabled
switch #

```

Secuencia 56 Comando de inspección de ACL

6.5.6.3 APLICACION DE LISTAS DE ACCESO

208. En el uso de ACLs para filtrar tráfico, se pueden aplicar simultáneamente de entrada y salida, tanto ACLs de nivel 3 como de nivel 2. Esta tabla describe los usos en función del objeto donde se apliquen.

ACL type	IPv4+6	IPv4+6	MAC	MAC
Direction	In	Out	In	Out
L2 interface (port)	Yes	Yes	Yes	Yes
L2 LAG	Yes	Yes	Yes	Yes
L3 interface (port)	Yes	Yes	Yes	Yes
L3 LAG	Yes	Yes	Yes	Yes
VLAN	Yes	Yes	Yes	Yes
Interface VLAN	Yes (routed)	Yes (routed)		
Management interface	Yes			
Control plane (per VRF)	Yes			

Tabla 3 Tipos de ACL aplicables para filtrado de tráfico en cada tipo de objeto

209. Las listas de acceso pueden aplicarse directamente a puertos del conmutador para filtrar tráfico, definiendo si aplican al tráfico entrante o saliente:

```
apply access-list {ip|ipv6|mac} <ACL-NAME> {in|out}
```

Secuencia 57 Aplicación de ACL a puertos

210. También es posible aplicar las listas de acceso a un Interface VLAN o a una VLAN serían:

```
apply access-list {ip|ipv6} <ACL-NAME> {routed-in|routed-out}
```

Secuencia 58 Aplicación de ACL a interfaz VLAN

- a) routed-in: Selects the routed inbound (routed ingress) traffic direction.
- b) routed-out: Selects the routed outbound (routed egress) traffic direction.

211. Es posible conocer estadísticas sobre el número de veces que se aplican las distintas reglas de una ACL, así como otra información que puede ser relevante.

6.5.6.4 LISTAS DE ACCESO MAC

212. De forma análoga a la listas de acceso IP descritas en el apartado anterior, ArubaOS-CX permite filtrar el tráfico en función de campos de las cabeceras de nivel 2 de las tramas Ethernet: direcciones MAC origen y destino, protocolo (Ethertype), identificador de VLAN ID y clase de servicio.
213. La configuración de las listas de acceso de nivel 2 es muy similar a las listas de acceso IP, por lo que los conceptos y pasos a seguir son prácticamente los mismos: es posible crear listas de acceso estandar y extendidas; las listas pueden ser identificadas por nombre o por número; y también pueden ser asignadas a un puerto o a una VLAN completa.
214. El formato de las entradas en las ACLs es el siguiente:

```
access-list mac <ACL-NAME>
[<SEQUENCE-NUMBER>]
{permit|deny}
{any|<SRC-MAC-ADDRESS>[/<ETHERNET-MASK>]]}
{any|<DST-MAC-ADDRESS>[/<ETHERNET-MASK>]]}
{any|arp|appletalk|arp|fcoe|fcoe-init|ip|ipv6|
ipx-arp|ipx-non-arp|is-is|lldp|mpls-multicast|mpls-unicast|q-in-q|
rbridge|trill|wake-on-lan|<NUMERIC-ETHERTYPE>}
[pcp <PCP-VALUE>] [vlan <VLAN-ID>] [count] [log]
```

Secuencia 59 Estructura de la definición de una ACL de MAC

215. Vemos un ejemplo de ACLs de nivel 2, donde se filtran diversos protocolos así como un rango de MACs de origen:

```
access-list mac filtroQinQ
 10 deny any any q-in-q
 20 deny any any mpls-unicast
 30 deny any any mpls-multicast
 35 deny 0001.9700.0000/FFFF.FF00.0000 any any
 40 deny any any wake-on-lan
 50 permit any any any
```

Secuencia 60 Ejemplo de definición de una ACL de nivel 2

216. Destacar que a la hora de especificar la dirección MAC origen o destino se puede especificar una máscara, por lo que es posible filtrar en función de prefijos. Por ejemplo, se podrían permitir o filtrar tramas procedentes de dispositivos de un determinado fabricante
217. Para aplicar esa lista a un puerto o una VLAN se haría de forma similar a las de IP pero en lugar de utilizar “ip” utilizando el comodín “mac”. Por ejemplo aplicarlo a una vlan serían:

```
apply access-list mac <ACL-NAME> {in|out}
! Ejemplo
apply access-list mac filtroQinQ in
```

Secuencia 61 Ejemplo de Aplicación de ACL de nivel 2

6.6 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS

6.6.1 PROTOCOLOS DE ACCESO

218. El equipo puede ser gestionado mediante una conexión remota a través de los puertos Ethernet que dispone, así como desde el puerto fuera de banda. A través de protocolos basados en la arquitectura TCP/IP como SSH, y HTTPS. También a través de una API se

puede acceder a la configuración del equipo y a la obtención de información de configuración y rendimiento de este.

219. En relación a protocolos inseguros **no** se dispone de servicio telnet.

6.6.2 TRANSFERENCIA DE ARCHIVOS

220. En cuanto a transferencia de ficheros se recomienda el uso de SFTP. Se soporta TFTP por compatibilidad histórica con servicios de gestión. Por ejemplo para subir una imagen mediante SFTP sería:

```
switch# copy sftp://sftpuser@10.10.10.1/TL_10_01_0001.swi primary vrf mgmt
```

Secuencia 62 Ejemplo de transferencia de con sftp

6.6.3 PUERTO USB

221. En los equipo tipo chasis, se puede controlar el uso de puerto USB para almacenamiento externo. El puerto USB se (des)habilita de la siguiente manera:

```
switch(config)# [no] usb
```

Secuencia 63 (Des)Activación del puerto USB (en modelos tipo chasis)

6.6.4 SERVIDOR SSH

222. El acceso remoto mediante SSH requiere al menos versión SSH v2.0. El servidor SSH realiza un rekey para todas las sesiones SSH abiertas cada hora o cada 1GB de datos transferido, lo que ocurra primero, limitando por tanto el periodo de tiempo de datos expuestos a esa franja.

223. Por defecto el SSH tiene los siguientes valores:

Característica	Valor por defecto
Máximo de intentos de password	3 intentos
Autenticación basada en password	Habilitado
Periodo de gracia para accesos SSH con fallo de passwords	120 segundos
Autenticación SSH de clave publica	Habilitado
Temporizador de inactividad	60 segundos

Tabla 4 Valores por defecto servidor SSH

224. En relación a la configuración relativa a seguridad del servidor SSH se pueden configurar los siguientes parámetros:

a) Habilitar/Deshabilitar el servidor ssh

```
[no] ssh server vrf mgmt
```

Secuencia 64 Habilitar SSH

b) Generación de la clave del servidor. El equipo dispone de varias claves, en función del tipo de clave generada. Se puede regenerar la clave de cada tipo:

- ecdsa - Especifica ECDSA como clave de host del servidor SSH.
- ed25519 - Especifica ED25519 como clave de host del servidor SSH.
- rsa - Especifica RSA como clave de host del servidor SSH.

Ejemplos:

```
ssh host-key rsa bits 2048
```

```
ssh host-key ecdsa ecdsa-sha2-nistp256
```

Secuencia 65 Ejemplos de generación de clave para SSH

- c) Configuración de los cyphers. Se pueden seleccionar los cifradores que se desean soportar. El comando es *ssh ciphers* y los tipos soportados son:
- aes128-cbc
 - aes192-cbc
 - aes256-cbc
 - aes128-ctr
 - aes192-ctr
 - aes256-ctr
 - aes128-gcm@openssh.com
 - aes256-gcm@openssh.com
 - chacha20-poly1305@openssh.com
- d) Configuración de los algoritmos del host key. Los valores soportados son:ssh hos
- ecdsa-sha2-nistp256
 - ecdsa-sha2-nistp384
 - ecdsa-sha2-nistp521
 - rsa-sha2-256
 - rsa-sha2-512
 - ssh-ed25519
 - ssh-rsa
- e) Configuración del uso de MAC
- hmac-sha1
 - hmac-sha1-96
 - [hmac-sha1-etm@openssh.com](#)
 - hmac-sha2-256
 - hmac-sha2-512
 - hmac-sha2-256-etm@openssh.com
 - [hmac-sha2-512-etm@openssh.com](#)
- f) Configuración de los algoritmos de intercambio de claves
- curve25519-sha256
 - curve25519-sha256@libssh.org

- diffie-hellman-group-exchange-sha1
 - diffie-hellman-group-exchange-sha256
 - diffie-hellman-group14-sha1
 - diffie-hellman-group14-sha256
 - diffie-hellman-group16-sha512
 - diffie-hellman-group18-sha512
 - ecdh-sha2-nistp256
 - ecdh-sha2-nistp384
 - ecdh-sha2-nistp521
- g) Utilización de algoritmos de clave pública
- ecdsa-sha2-nistp256
 - ecdsa-sha2-nistp384
 - ecdsa-sha2-nistp521
 - ssh-ed25519
 - ssh-rsa
 - rsa-sha2-256
 - rsa-sha2-512
 - x509v3-ecdsa-sha2-nistp256
 - x509v3-ecdsa-sha2-nistp384
 - x509v3-ecdsa-sha2-nistp521
 - x509v3-rsa2048-sha256
 - x509v3-sign-rsa
 - x509v3-ssh-rsa
- h) Session Timeout

6.6.5 SERVIDOR HTTP

225. No se dispone de servidor HTTP. El puerto 80 se implementa para redireccionar al puerto HTTPS (443)

6.6.6 SERVIDOR HTTPS

226. Para habilitar o deshabilitar el servidor HTTPS se hará con el siguiente comando:

```
switch# config
switch(config)# [no] https-server vrf mgmt
```

Secuencia 66 Activar o desactivar el servidor HTTPS del equipo

227. Así mismo el equipo dispone acceso a la REST API a través de HTTPS que puede ser modificado:

```
https-server rest access-mode {read-only | read-write}
```

Secuencia 67 Activación acceso API

228. En el modo read-write habilita la llamadas del tipo POST, PUT y DELETE

229. Para cerrar todas las sesiones abiertas se puede emplear el siguiente comando:

```
https-server session close all
```

Secuencia 68 Cerrar sesiones HTTPS abiertas con el equipo

230. Para ver estado de configuración del servidor HTTPS:

```
switch# show https-server
HTTPS Server Configuration
-----
VRF : default, mgmt
REST Access Mode : read-write
Max sessions per user : 6
Session timeout : 20
```

Secuencia 69 Estado servidor HTTPS

6.6.7 ACL PARA CONTROLAR SERVICIOS DEL EQUIPO

231. Como se ha comentado, en ArubaOS-CX, la interfaz de administración se puede separar lógicamente del resto del Switch por Virtual Routing Forwarding (VRF); funcionalidad puede ser utilizadas para la interfaz de administración a la que se asigna una instancia dedicada mgmt VRF.

232. El tráfico no puede ser enrutado entre el interfaz de gestión y los puertos normales del switch protegiendo de esta manera el acceso al mismo, así mismo a la interfaz de gestión se le puede asignar una dirección dedicada de default gateway. El interfaz de gestión está habilitado por defecto.

233. Para configurar la interfaz de gestión de manera estática se haría de la siguiente manera:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip static 10.1.1.5/24
switch(config-if-mgmt)# default-gateway 10.1.1.1
switch(config-if-mgmt)# nameserver 10.0.1.10 10.0.1.11
```

Secuencia 70 Ejemplo configuración interfaz mgmt (management)

234. El interfaz de gestión fuera de banda no permite la definición de ACLs.

235. En el caso que se gestione el equipo en banda, se recomienda proteger el acceso a la dirección de gestión se pueden limitar mediante listas de control de acceso (ACLs). Así se implementa un control granular sobre que rangos de IPS o protocolos se permite acceder al switch.

236. Por ejemplo la siguiente lista de acceso restringiría los protocolos y direcciones que pueden acceder al interfaz de gestión. En este caso, se ha configurado restricciones de acceso al puerto de gestión, VLAN2 en este caso:

```
switch(config)# interface vlan 2
switch(config)# ip address 10.1.1.5/24
switch(config)# access-list ip mgmt_traffic
switch(config-acl-ip)# 10 permit tcp 10.1.1.0/24 10.1.1.5 eq 22
switch(config-acl-ip)# 20 permit tcp 10.1.1.0/24 10.1.1.5 eq 443
switch(config-acl-ip)# 30 permit tcp 10.0.1.50 10.1.1.5 eq 22
switch(config-acl-ip)# 40 permit tcp 10.0.1.50 10.1.1.5 eq 443
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
```

```
switch(config-if)# apply access-list ip mgmt-traffic in
```

Secuencia 71 Ejemplo de lista de acceso para interfaz de Gestión

237. Nota: Todas las ACLs llevan implícitas una regla “deny any” al final de la lista.

6.6.8 SNMP

238. En relación a protocolos de gestión SNMP se dispone de v1, v2 y v3 estando por defecto todas ellas deshabilitadas.

239. Para evitar que la información SNMP se transmita en texto plano se recomienda utilizar la versión 3 de SNMP.

240. Los pasos a seguir para configurar SNMP Versión 3 son los siguientes

- a) Habilitar SNMP en una instancia VRF

```
Aruba-CX(config)# snmp-server vrf <VRF-NAME>
```

Secuencia 72 SNMP - Activación en VRF

- b) Definir el contacto, localización y descripción del switch (Opcional)

```
Aruba-CX(config)# snmp-server system-contact <Contacto>
Aruba-CX(config)# snmp-server system-location <Localizacion>
Aruba-CX(config)# snmp-server system-description <Descripcion>
```

Secuencia 73 SNMP - Datos administrativos: Contacto, localización y descripción

- c) Deshabilitamos SNMP en V2 y V1

```
Aruba-CX(config)# snmp-server snmpv3-only
```

Secuencia 74 SNMP - Activación de Versión 3 en exclusiva

- d) Definir un usuario SNMP V3

```
Aruba-CX(config)# snmpv3 user admin auth sha auth-pass plaintext <SHA-TEXT> priv aes priv-pass
plaintext <AES-TEXT>
```

Secuencia 75 SNMPv3 - Definición de usuario y credenciales

- e) Crear un contexto SNMP V3. Recordar lo expuesto en el punto 3 donde se ha cambiado la comunidad por defecto por seguridad.

```
Aruba-CX(config)# snmpv3 context <Contexto> vrf <VRF-NAME> community <Comunidad>
```

Secuencia 76 SNMPv3 Creación de contexto

241. Por otro lado, si vamos a enviar traps, se definirían de esta forma.

```
Aruba-CX(config)# snmp-server host <IP> trap version v3 user <Usuario> vrf <VRF-NAME>
```

Secuencia 77 SNMP - Activación de envío de traps

242. Hay que indicar que en los switches Aruba de la gama CX, SNMP solo tiene propiedades de lectura.

6.7 MITIGACION DE ATAQUES

6.7.1 DHCP SNOOPING

243. DHCP snooping protege la red de los ataques DHCP más comunes, como la suplantación de direcciones resultante de un servidor DHCP fraudulento que opera en la red, o el agotamiento de las direcciones en un servidor DHCP causado por las solicitudes masivas de direcciones de un atacante en la red. La función funciona designando servidores DHCP de confianza y puertos en los que se aceptarán las solicitudes y respuestas DHCP.

244. Nota: DHCP snooping es compatible se soporta en 4100, 6000, 6100, 6200, 6300, 6400 y 8400.

245. Para determinar los servidores DHCP autorizados o de confianza se usan el comando *dhcpv4-snooping*. Se muestra un ejemplo, donde se muestra las posibilidad de configurarlo por VRF.

```
switch(config)# dhcpv4-snooping authorized-server 192.168.2.2
switch(config)# dhcpv4-snooping authorized-server 192.168.2.3 vrf default
switch(config)# dhcpv4-snooping authorized-server 192.168.2.10 vrf default
```

Secuencia 78 DHCP Snooping - Servidores autorizados

246. Para activar la funcionalidad, en un puerto o en una vlan se usa el comando *dhcpv4-snooping*.

```
Ejemplo de configuración por interfaz
switch(config)# interface 1/1/1
switch(config-vlan-100)# dhcpv4-snooping
switch(config-vlan-100)# exit
switch(config)#

Ejemplo de configuración por vlan
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv4-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Secuencia 79 DHCP Snooping - Activación en puertos y VLANs

247. Existen más parámetros de la funcionalidad, disponibles en el manual.

6.7.2 DYNAMIC ARP INSPECTION

248. El Protocolo de Resolución de Direcciones (ARP) permite a los hosts comunicarse a través de la red creando un mapeo de direcciones IP a MAC que se utiliza en la transmisión de paquetes. Los atacantes pueden utilizar ARP para generar mapeos falsos, lo que les permite falsificar las direcciones MAC de otros clientes e interceptar el tráfico destinado a ellos. Además, un atacante podría generar un número ilimitado de entradas ARP artificiales, llenando las cachés de otros clientes en la red y provocando una denegación de servicio (DoS).

249. El comando *arp inspection* activa la inspección dinámica de ARP en la VLAN actual, obligando a que todos los paquetes ARP procedentes de puertos no confiables sean sometidos a una comprobación de asociación MAC-IP contra una tabla de vinculación.

250. El tamaño de la tabla dinámica se puede configurar con el comando *arp cache-limit*.

251. La activación de la funcionalidad se hace por VLAN.

```
switch(config)# arp cache-limit 4097
switch(config)# vlan 1
switch(config-vlan)# arp inspection
```

Secuencia 80 ARP Inspection - Configuración

252. Nota: La inspección dinámica de ARP se soporta en 6200, 6300, 6400 y 8400.

6.7.3 CONTROL PLANE POLICING

253. Nota: La serie de conmutadores CX 6100 admite un número menor de clases de tráfico CoPP configurables y no dispone de valores de "ráfaga" configurables.

254. La vigilancia del plano de control evita que la inundación de ciertos tipos de paquetes sobrecargue la CPU del conmutador o del módulo limitando la velocidad o descartando los paquetes. El software del conmutador proporciona un número de clases configurables de paquetes que pueden ser limitados en su velocidad, incluyendo (pero no limitado a) las difusiones ARP, la multidifusión, los protocolos de enrutamiento (BGP, OSPF) y el árbol de expansión.

255. La siguiente política de CoPP por defecto aplica las siguientes definiciones de clases de tráfico y límites de velocidad (en paquetes por segundo) en un switch de la serie 6300:

6300# show copp-policy default						
class	drop	priority	rate	pps	burst	pkts
acl-logging	0		25		25	25
arp-broadcast	2		1250		1250	1250
arp-protect	2		2075		2075	2075
arp-unicast	3		825		825	825
bfd-control	5		850		850	850
bgp	5		750		750	750
captive-portal	2		2075		259	2075
client-onboard	5		1024		1024	1000
dfp-collector	0		512		512	500
dhcp	2		750		750	750
erps	6		225		225	225
icmp-broadcast-ipv4	2		325		325	325
icmp-multicast-ipv6	2		475		475	475
icmp-security-ipv6	2		325		325	325
icmp-unicast-ipv4	3		225		225	225
icmp-unicast-ipv6	3		400		400	400
ieee-8021x	2		2075		259	2075
igmp	4		1600		450	1600
ip-exceptions	0		100		100	100
ip-lockdown	0		100		100	100
ip-tracker	0		256		256	250
ipsec	5		1025		128	1025
ipv4-options	1		100		100	100
lacp	5		2050		2050	2050
lldp	5		100		100	100
loop-protect	6		225		225	225
mac-lockout	0		100		100	100
manageability	4		4218		4218	4200
mdns	2		150		150	150
mirror-to-cpu	0		100		100	100
mld	4		1600		450	1600
mvrp	5		225		225	225
nae-packet-monitor	0		100		200	100
ntp	4		100		100	100
ospf-multicast	5		1025		1025	1025
ospf-unicast	5		1025		1025	1025
pim	5		1700		1700	1700

ptp	5	1000	250	1000
secure-learn	2	2075	259	2075
sflow	1	1000	125	1000
stp	6	1500	1500	1500
udld	6	450	450	450
unknown-multicast	1	1025	128	1025
unresolved-ip-unicast	1	325	325	325
vrrp	4	400	400	400
default	2	4225	528	4225
6300#				

Secuencia 81 Política de Plano de Control por defecto

256. La política de CoPP por defecto puede ser modificada, pero no puede ser eliminada. Para revertir una política de CoPP por defecto modificada a la configuración por defecto de fábrica, utilice el siguiente comando:

```
switch(config)# copp-policy default revert
```

Secuencia 82 Recuperación de la configuración por defecto de la política de plano de control

257. Los administradores pueden crear hasta 32 políticas de CoPP personalizadas, aunque sólo una puede estar activa en un momento dado. Los siguientes comandos demuestran la creación de una política de CoPP personalizada simple, y cómo se aplica al conmutado

```
switch(config)# copp-policy copp_policy_01
switch(config-copp)# class arp-broadcast priority 2 rate 1000 burst 1000
switch(config-copp)# class unknown-multicast priority 2 rate 1000 burst 1000
switch(config-copp)# class unresolved-ip-unicast priority 2 rate 1000 burst 1000
switch(config-copp)# default-class priority 1 rate 3000 burst 3000
switch(config-copp)# exit
switch(config)# apply copp-policy copp_policy_01
```

Secuencia 83 Ejemplo de definición de política de plano de control

258. Para retirar del servicio una política de CoPP personalizada y aplicar automáticamente la política por defecto:

```
switch(config)# no apply copp-policy copp_policy_01
```

Secuencia 84 Desactivación de una política personalizada de plano de control

259. Para eliminar una política de CoPP personalizada:

```
switch(config)# no copp-policy copp_policy_01
```

Secuencia 85 Eliminación de una política personalizada de plano de control

260. Una política de CoPP personalizada activa no puede ser eliminada; primero debe ser retirada del servicio utilizando el comando anterior.

6.8 PROTOCOLOS DE ROUTING

6.8.1 BGP

261. Las mejores prácticas actuales del IETF para la seguridad de BGP (BCP194) contienen muchas sugerencias útiles. Esta guía se centrará en los tres puntos siguientes:

- Utilizar la funcionalidad ACL de control para limitar la comunicación BGP a los peers BGP configurados

- b) Asegurar las sesiones BGP entre peers con autenticación.
- c) Utilizar mecanismos de seguridad TTL para evitar ataques de spoofing de terceros.

262. Nota: BGP es soportado en las plataformas 6300, 6400, 8320, 8325, 8360 y 8400.

6.8.1.1 ACL DEL PLANO DE CONTROL PARA LAS SESIONES DE PEERING DE BGP

263. Los dispositivos que ejecutan BGP escuchan conexiones en el puerto TCP 179. Al establecer una sesión de peering BGP, un dispositivo establecerá activamente una relación con el otro peer enviando el primer paquete TCP SYN. Este dispositivo se conoce como el lado saliente de la conexión. El otro peer, al escuchar el TCP SYN, responde con un SYN/ACK, es referido como la conexión entrante. Dado que cualquiera de los dos peers puede asumir cualquiera de los dos papeles, es necesario configurar entradas ACL para BGP en ambas direcciones.

264. Basándose en el mismo ejemplo de ACL de plano de control que antes, las siguientes entradas permitirán el tráfico desde 10.20.0.10 para que pueda establecer una sesión de peering BGP con el dispositivo. Dado que cualquiera de los dos lados puede jugar el papel de salida o de entrada en la conexión, la ACL requiere dos entradas por peer:

```
switch(config)# access-list ip CONTROLPLANE
switch(config-acl-ip)# 800 comment LOCKDOWN BGP SESSIONS
switch(config-acl-ip)# 805 permit tcp 10.20.0.10 gt 1023 any eq 179
switch(config-acl-ip)# 810 permit tcp 10.20.0.10 eq 179 any gt 1023
```

Secuencia 86 BGP - ACL control - Permitir vecinos conocidos

265. Después de permitir el tráfico de todos los peers configurados, bloquee todos los demás dispositivos para que no puedan intentar establecer una sesión de peering BGP, denegando el resto del tráfico hacia o desde el puerto TCP 179.

```
switch(config-acl-ip)# 890 deny tcp any gt 1023 any eq 179
switch(config-acl-ip)# 895 deny tcp any eq 179 any gt 1023
```

Secuencia 87 BGP - ACL control - No Permitir vecinos desconocidos

6.8.1.2 AUTENTICACIÓN DE PEERS BGP MEDIANTE MD5

266. Las sesiones TCP entre los dos peers pueden asegurarse añadiendo protección MD5 a la cabecera de la sesión TCP. El compendio MD5 actúa como una contraseña entre los peers. Esta configuración se realiza dentro del contexto de configuración de BGP, y ambos peers deberán configurar la misma contraseña.

```
switch(config-bgp)# neighbor 10.20.0.10 password plaintext meatballs4me!
```

Secuencia 88 BGP - Establecer autenticación MD5

6.8.1.3 SEGURIDAD DEL TTL DE BGP

267. Asumiendo que la mayoría de los vecinos de enrutamiento están típicamente conectados directamente, un método simple para bloquear la suplantación remota desde dispositivos remotos es verificar el TTL de los paquetes del peer y descartar los paquetes cuyo TTL es menor que la cantidad esperada.

268. Aquí hay un ejemplo usando el peer BGP especificado arriba. Asumiendo que el valor máximo de TTL es 255, los paquetes del peer se comparan con el hop-count, introducido abajo como un valor de 1

```
switch(config-bgp)# neighbor 10.20.0.10 ttl-security-hops 1
```

Secuencia 89 BGP - Configuración de saltos TTL

269. Con un valor máximo de TTL de 255 y un valor configurado de hop-count de 1, los paquetes con un TTL inferior a 254 serán descartados.

6.8.1.4 OTRAS CONFIGURACIONES DE BGP

270. Para elementos adicionales relacionados con BGP, como la configuración del filtrado de rutas entrantes y salientes o la limitación del número máximo de rutas a aprender por vecino BGP, consulte la parte de BGP y Políticas de Ruta y Mapas de Ruta de la Guía de Enrutamiento IP de AOS-CX. La publicación del IETF Best Current Practice on BGP Operations and Security(<https://tools.ietf.org/rfc/bcp/bcp194.txt>) es también un recurso excelente y altamente recomendado.

6.8.2 OSPF

6.8.2.1 INTERFACES PASIVAS OSPF

271. Nota: OSPF es soportado en las plataformas 6200, 6300, 6400, 8320, 8325, 8360 y 8400.

272. A diferencia de BGP, la mayoría de los protocolos de enrutamiento tienden a descubrir vecinos mediante el envío y la recepción de paquetes *Hello*. Debido a que la construcción de estas relaciones de vecindad ocurre dinámicamente, el administrador debe tomar medidas para controlar dónde se pueden formar las relaciones de vecindad y que los vecinos potenciales sean dispositivos conocidos y de confianza.

273. Para limitar dónde puede aprender vecinos OSPF, AOS-CX soporta el concepto de interfaces OSPF pasivas. Una interfaz OSPF pasiva tiene sus subredes IP anunciadas, pero no establece relaciones de vecinos con otros dispositivos OSPF en la interfaz.

274. El método recomendado es hacer pasivas todas las interfaces OSPF habilitadas. El método recomendado es hacer que todas las interfaces OSPF habilitadas sean pasivas:

```
switch(config-ospf-10)# passive-interface default
```

Secuencia 90 OSPF - Configurar todos los interfaces en modo pasivo

275. La interfaz pasiva es entonces removida de cada interfaz específica donde las relaciones de vecinos OSPF son permitidas. Como este es un cambio de configuración a nivel de interfaz, ocurre desde el contexto de la interfaz:

```
switch(config-if)# no ip ospf passive
```

Secuencia 91 OSPF - Eliminar el modo pasivo de un interfaz

6.8.2.2 AUTENTICACIÓN DE VECINOS OSPF

276. Técnicamente hablando, todos los intercambios OSPF son autenticados. Sin embargo, la autenticación por defecto utilizada por los proveedores de red es "null", es decir, vacía o

cero. OSPF también soporta el uso de una simple contraseña de texto plano y la autenticación criptográfica.

277. AOS-CX soporta varios métodos de autenticación OSPF, incluyendo hashes criptográficos SHA de hasta 512 bits, para autenticar mensajes entre vecinos OSPF. Al configurar la autenticación entre vecinos OSPF, el método de autenticación y la clave deben ser los mismos en las interfaces conectadas en ambos dispositivos.

278. Para configurar la autenticación SHA-512, cambie el método de autenticación por defecto de null a hmac-sha-512 desde el contexto de la interfaz:

```
switch(config-if)# ip ospf authentication hmac-sha-512
```

Secuencia 92 OSPF - Autenticación con vecino SHA-512

279. A continuación, configure una clave SHA que se utilizará para la conexión; la clave puede introducirse como texto plano o como una cadena de texto cifrado con hash:

```
switch(config-if)# ip ospf sha-key 1 plaintext ospfshakestring
```

Secuencia 93 OSPF - Definición de clave SHA

280. Nota: Cualquier cadena de clave SHA o MD5 introducida en texto plano será automáticamente convertida en texto cifrado antes de ser almacenada en la configuración del switch.

281. Alternativamente, la función de llavero de AOS-CX puede ser utilizada para especificar una clave de autenticación criptográfica a nivel de sistema que puede ser utilizada por múltiples interfaces OSPF:

```
switch(config)# keychain ospf-keychain
switch(config-keychain)# clave 1
switch(config-keychain-key)# cryptographic-algorithm hmac-sha-512
switch(config-keychain-key)# key-string plaintext ospfshakestring
switch(config-keychain-key)# interfaz 1/1/49
switch(config-if)# ip ospf authentication keychain
switch(config-if)# ip ospf keychain ospf-keychain
```

Secuencia 94 OSPF – Utilización de clave del llavero

6.8.2.3 AUTENTICACIÓN Y ENCRYPTACIÓN DE ÁREA OSPFV3 CON IPSEC

282. Nota: La configuración de autenticación o encriptación de área OSPFv3 será anulada por la autenticación o encriptación a nivel de interfaz, donde esté configurada.

283. Los vecinos de OSPFv3 pueden utilizar la autenticación a nivel de interfaz, como se describe en la sección anterior. Sin embargo, se puede utilizar un método alternativo para proporcionar encriptación y/o autenticación para toda un área OSPFv3 utilizando el protocolo IPsec, que aplica automáticamente los métodos configurados a todas las interfaces miembros.

284. Hay dos tipos de encapsulación IPsec soportados en AOS-CX para asegurar áreas OSPFv3:

- a) Cabecera de autenticación IPv6 (AH), que añade una cabecera de autenticación IPv6 a los paquetes OSPFv3

- b) Encrypted Security Payload (ESP), que proporciona tanto autenticación como encriptación para los paquetes OSPFv3

285. La autenticación y el cifrado IPsec se configuran desde el contexto del proceso del router OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)#
```

Secuencia 95 OSPFv3 - Activación

286. Tanto la autenticación como la encriptación requieren un índice de política de seguridad (SPI) especificado, que es un valor entero entre 256 y 4.294.967.295; este valor se utiliza en cada router OSPFv3 en el área asegurada para coincidir con una política de autenticación y/o encriptación IPsec configurada.
287. Cada política IPsec OSPFv3 en un conmutador debe utilizar un valor SPI diferente, y el valor SPI (así como las claves de autenticación y/o encriptación) debe coincidir en todas las interfaces vecinas OSPFv3 que utilicen esa política dentro del área asegurada.
288. Para configurar la autenticación AH para el área 1 de OSPFv3, especifique el SPI, el método de autenticación (md5 o sha1), el tipo de clave (texto plano, cadena hexadecimal o texto cifrado) y la propia cadena de claves. Si no se especifica un tipo de clave y una cadena, se pedirá al usuario que introduzca una clave de texto plano de forma interactiva:

```
switch(config-ospfv3-1)# area 1 authentication ipsec spi 1024 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Secuencia 96 Configuración tunel IPSEC para relación de vecindad

289. Para configurar el cifrado ESP para el área 1, especifique el SPI, el método de autenticación, el tipo y la cadena de la clave de autenticación, el tipo de cifrado (3des, aes, des o null), el tipo de clave y la cadena de la clave de cifrado. Si no se especifican el tipo de cifrado y la cadena de claves, se pedirá al usuario que introduzca una clave en texto plano de forma interactiva.
290. Si el tipo y la cadena de clave de autenticación no se especifican, se pedirá al usuario que introduzca tanto una clave de autenticación en texto plano como el tipo de cifrado y la clave en texto plano deseados.

```
switch(config-ospfv3-1)# area 1 encryption ipsec spi 1024 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
Enter the IPsec encryption type (3des/aes/des/null)? aes
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Secuencia 97 Configuración tunel IPSEC para relación de vecindad

291. Dependiendo del tipo de cifrado seleccionado, la clave de cifrado en texto plano o hexadecimal debe tener una longitud determinada:
- a) 3DES:
- Hexadecimal: 48 dígitos

- Texto plano: 24 caracteres
 - b) DES:
 - Hexadecimal: 16 dígitos
 - Texto sin formato: 8 caracteres
 - c) AES
 - Hexadecimal: 32, 48 o 64 dígitos
 - Texto sin formato: 16, 24 o 32 caracteres
292. Para el cifrado AES, las longitudes de clave especificadas corresponden a AES128, AES192 o AES256, respectivamente. El tipo utilizado se determinará automáticamente por la longitud de la clave de cifrado introducida.

6.9 GESTIÓN DE CERTIFICADOS

293. Los certificados pueden instalarse en el conmutador para ser utilizados por funciones como el cliente syslog, la interfaz de usuario web o la API REST.
294. Si adquiere un certificado de una CA de confianza, el conmutador puede generar la solicitud de firma de certificado (CSR) que se utiliza para obtener el certificado. El conmutador también puede generar directamente certificados autofirmados.
295. Como alternativa, el certificado y la clave privada pueden generarse fuera del conmutador y luego importarse.
296. El software de gestión de certificados X509, como OpenSSL, puede utilizarse para generar la clave privada y la CSR y, a continuación, combinar el certificado y la clave privada en un archivo PEM o PKCS#12 adecuado para su importación en el conmutador.
297. Al validar los certificados de los dispositivos homólogos, el conmutador comprueba que el nombre de host configurado (**hostname**) del dispositivo homólogo coincida con el campo Subject Alternative Name (SAN) o con el Common Name (CN) dentro del campo certificateSubject. Si el campo SAN está presente y coincide con el nombre de host, la validación tiene éxito, de lo contrario falla. Si el campo SAN no está presente, y el CN coincide con el nombre de host, la validación tiene éxito, de lo contrario falla.

6.9.1 PKI EN EL SWITCH

298. Los conmutadores de la serie AOS-CX permiten la instalación de certificados de autoridad de certificación (CA) y la generación e instalación de certificados de hoja.
299. Los elementos en este caso relevantes son:
- a) Trust anchor profiles
 - b) Certificado de dispositivo (Leaf certificates)
 - c) Coincidencia obligatoria del nombre de host del dispositivo homólogo
300. **Trust anchor profiles.** El conmutador admite 64 perfiles de anclaje de confianza (TA). Cada perfil TA almacena un certificado de CA de confianza. El certificado puede ser un certificado de CA raíz, que debe ser autofirmado, o un certificado de CA intermedia emitido por otra CA.

- a) Validar los certificados que los pares remotos presentan cuando intentan establecer una conexión segura con un servicio en el conmutador, por ejemplo, el servidor SSH.
 - b) Validar los certificados de hoja instalados en el conmutador que son utilizados, por ejemplo, por el cliente syslog, la WebUI o la API REST.
301. **Certificado de dispositivo.** Los certificados de hoja pueden instalarse en el conmutador para ser utilizados por funciones como el cliente syslog, la interfaz de usuario web o la API REST. Si adquiere un certificado de una CA de confianza, el conmutador puede generar la solicitud de firma de certificado (CSR) que se utiliza para obtener el certificado. El conmutador también puede generar directamente certificados autofirmados. Como alternativa, el certificado y la clave privada pueden generarse fuera del conmutador y luego importarse. El software de gestión de certificados X509, como OpenSSL, puede utilizarse para generar la clave privada y la CSR y, a continuación, combinar el certificado y la clave privada en un archivo PEM o PKCS#12 adecuado para su importación en el conmutador.
302. **Coincidencia obligatoria del nombre de host del dispositivo homólogo.** Al validar los certificados de los dispositivos homólogos, el conmutador comprueba que el nombre de host configurado del dispositivo homólogo coincida con el campo Subject Alternative Name (SAN) o con el Common Name (CN) dentro del campo certificateSubject. Si el campo SAN está presente y coincide con el nombre de host, la validación tiene éxito, de lo contrario falla. Si el campo SAN no está presente, y el CN coincide con el nombre de host, la validación tiene éxito, de lo contrario falla.

6.9.2 PKI EST

303. EST (Enrollment over Secure Transport) (RFC 7030) define el protocolo que utilizan los dispositivos para solicitar certificados de autoridad de certificación (CA) de confianza y para inscribir/reinscribir certificados de dispositivo de los servicios de CA utilizando canales seguros, específicamente HTTP sobre TLS.
304. Los dispositivos pueden configurarse para solicitar los certificados de CA de confianza y para solicitar la inscripción y reinscripción de los certificados de dispositivo de forma automática, sin necesidad de que intervenga el administrador, manteniendo la seguridad e integridad de todo el proceso de inscripción.
305. El conmutador incluye un cliente EST implementado como parte de la infraestructura PKI.

6.9.3 FORMAS DE GENERACION E IMPORTACION DE CERTIFICADOS

306. En la documentación de los equipos ([REF4]-[REF11]) en el manual Security Guide, se encuentran descritos diferentes escenarios:
- a) Ejemplo de uso de EST para la inscripción de certificados
 - b) Ejemplo que incluye el uso de un certificado intermedio
 - c) Instalación de un certificado de autofirmado (creado dentro del switch)
 - d) Instalación de un certificado firmado por la CA (creado fuera del switch)
 - e) Instalación de un certificado de una CA raíz
 - f) Instalación de un certificado firmado por la CA (iniciado en el switch)

- g) Instalación de un certificado firmado por CA (creado fuera del switch)

307. Reproducimos dos ejemplos, que entendemos puedan de uso frecuente.

6.9.3.1 INSTALACIÓN DE UN CERTIFICADO AUTOFIRMADO (CREADO DENTRO DEL SWITCH)

308. Este procedimiento describe cómo crear (totalmente dentro del conmutador) e instalar un certificado de hoja X.509 autofirmado. Y asociarlo con una de las siguientes características del conmutador: cliente syslog, cliente RadSec, portal cautivo, servidor HTTPS o HSC (controlador de conmutador de hardware).

309. Procedimiento

- a) Cree un contexto de certificado con el comando *crypto pki certificate*. Esto cambia al contexto de configuración del certificado.
- b) Defina las propiedades del certificado leaf con el comando *subject*.
- c) Establezca el tipo de clave de cifrado para el certificado leaf con el comando *key-type*.
- d) Genere e instale el certificado autofirmado con el comando *enroll self-signed*.
- e) Salga del contexto del certificado leaf con el comando *exit*.
- f) Asocie el certificado de hoja con una función del conmutador (cliente syslog, cliente RadSec, portal cautivo, servidor HTTPS o HSC) con el comando *crypto pki application*.

310. Ejemplo

- a) Crea el contexto de certificado de hoja
- b) Define las características del certificado de hoja
- c) Crea e instala el certificado de hoja autofirmado.
- d) Asocia el certificado de hoja con el cliente syslog (ejemplo de aplicación) en el conmutador.

```
switch(config)# crypto pki cert SS_LC
switch (config-cert-SS_LC)# subject common-name SSLeaf country US
state CA locality Rocklin org Company org-unit Site
switch (config-cert-SS_LC)# key-type rsa key-size 3072
switch (config-cert-SS_LC)# enroll self-signed
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, OU=Site, O=Company,
CN=SSLeaf
Key Type: RSA (3072)
Continue (y/n)? y
Self-signed certificate is created and enrolled successfully.
switch (config-cert-SS_LC)# exit
switch(config)# crypto pki application syslog-client certificate SS_LC
```

Secuencia 98 Instalación de un certificado de hoja autofirmado (creado dentro del switch)

6.9.3.2 INSTALACIÓN DE UN CERTIFICADO FIRMADO POR LA CA (CREADO FUERA DEL SWITCH)

311. Este procedimiento describe cómo instalar un certificado leaf X.509 autofirmado (que se creó fuera del conmutador). Y luego asociar el certificado con una de las siguientes características del conmutador: cliente syslog, RadSecclient, portal cautivo, servidor HTTPS o HSC (controlador de conmutador de hardware).

312. Requisitos previos: Un certificado autofirmado (incluyendo los datos de la clave privada) debe crearse fuera del conmutador.

313. Procedimiento

- Cree el contexto de certificado con el comando *crypto pki certificate*, que a continuación conmuta al contexto de certificado de hoja creado.
- Importe los datos del certificado de hoja al conmutador con el comando *import (self-signed leaf certificate)*.
- Salga del contexto de certificado de hoja con el comando *exit*.
- Asocie el certificado de hoja con una función del conmutador (cliente syslog, cliente RadSec, portal cautivo, servidor HTTPS o HSC) con el comando *crypto pki application*.

314. Ejemplo:

- Crear el contexto de certificado.
- Importar el certificado autofirmado.
- Asociar el certificado con el cliente syslog (aplicación) en el conmutador.

```
switch(config)# switch(config)# crypto pki certificate SS_LC2
switch(config)# switch(config-cert-SS_LC)# import terminal self-signed
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAYyAwIBAgIQP8nnS2Vp15u07xXMdktDJzANBgkqhkiG9
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAwGA1UECgwFXjJ1YmxDAOGNBAMMB1Jvb3gw
switch(config-cert-import)# HhcNMTkNDEwMjIwNT1WbhcjIwMTA0MjIwNE1wBzQswQYDVQGEwJV
...
switch(config-cert-import)# 1fIYZYGQy1a0AwFuPTTxBXHYwRxTPbUYU5tumJrFwRPM40VY8S9D
switch(config-cert-import)# 1NGNm3NG03GqPScs/TF9bVyFA5B0rS51mm7kNfRY1K8D/kMTfRreS
switch(config-cert-import)# YQ1u1NqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBAGkqhkiG9wBBQ0wMzAbBgkqhkiw0QwwDQImNpJMN7sVGwC
switch(config-cert-import)# MBQGCCqGSIB3DQMHAit+2qadNAASCMg5LYJ4AFm3EfffH5p51Ggr8
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvoAWgoYaeD83PeswToAGv5VS80MFTPTtr
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c/6rPs1pcjbdXw283DiD1MW0peoS2a
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41DtH0X9Sgf6aa1LjiStg+N7cND9XfgTj/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----

switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported successfully.
switch(config-cert-SS_LC2)# exit
switch(config)# crypto pki application syslog-client certificate SS_LC2
```

Secuencia 99 Ejemplo Instalación de un certificado firmado por la CA (creado fuera del switch)

6.9.3.3 OTRAS CONSIDERACIONES

315. Los switches soportan la importación en formato PEM de certificados codificados ITU-T X.509 v3.

316. Con el siguiente comando se puede asociar el certificado con diferentes aplicaciones, como se ha visto en los ejemplos anteriores:

```
crypto pki application <APP-NAME> certificate <CERT-NAME>
```

Secuencia 100 Asociación de certificado con su uso

317. Siendo APP-NAME alguno de los siguientes:

- a) captive-portal: Captive portal
- b) hsc: Hardware switch controller.
- c) https-server: HTTPS server.
- d) radsec-client: RadSec client.
- e) syslog-client: Syslog client.

318. Los certificados pueden ser visualizados su asociación, el certificado mismo y su *ta-profile* a través de los siguientes comandos:

```
show crypto pki application
show crypto pki certificate
show crypto pki ta-profile
```

Secuencia 101 Inspección de certificados y fuentes de confianza

6.10 ACTUALIZACIONES

319. Los switches disponen de dos localizaciones para su software (firmware), una partición llamada "Primary" y otra "Secondary" por lo que habrá que especificar cual de las dos particiones se quiere actualizar en cada momento.

320. Se soportan varios modos de transmisión del software al switch de manera remota desde un servidor de ficheros, uno mediante TFTP y otro mediante SFTP, por lo que se recomienda utilizar por seguridad el modo SFTP.

321. También se dispone de la posibilidad de transmitir el software de manera local mediante el puerto USB tipo A, de tal manera que el software ya se encuentra descargado en una llave usb.

322. El comando para la actualización del software del switch mediante el uso de un servidor de ficheros es:

```
Aruba-CX(config)# copy <REMOTE-URL> {primary | secondary} [vrf <VRF-NAME>]
```

Secuencia 102 Comando para copia de software remota a partición del equipo

323. Donde <REMOTE-URL> es la dirección del servidor de ficheros en el siguiente formato para una conexión SFTP:

```
sftp://<USERNAME>@<IP-ADDR>[:<PORT-NUM>]/<FILENAME>
```

Secuencia 103 Formato de la URL para la copia de software remota

324. El comando para una actualización local del software a través de una llave usb sería:

```
Aruba-CX(config)# copy usb:/file {primary | secondary}
```

Secuencia 104 Comando para copia de software desde USB

325. Para comprobar las versiones de software que hay cargados en cada partición sería el siguiente comando:

```
Aruba-CX(config)# show images
```

Secuencia 105 Comando para verificación de imágenes instaladas en el equipo

326. Para comprobar la versión de software que hay cargada en el momento actual sería mediante el siguiente comando:

```
Aruba-CX(config)# show version
```

6.11 AUTO-CHEQUEOS

6.11.1 VERIFICACIÓN DE SOFTWARE CUANDO ES INSTALADO AL EQUIPO

327. Todos los firmware vienen firmados desde Aruba, y el equipo dispone de los certificados necesarios almacenados en el chip TPM para verificar la integridad del software.

328. Los switches realizan un chequeo del firmware cuando este es copiado desde cualquiera medio, como se describe en el punto 5.11 ACTUALIZACIONES, hacia la memoria flash del switch.

329. Si la comprobación es correcta, nos devolverá el prompt del CLI.

```
This operation will overwrite the primary firmware image which is currently
in use by Redundant Management. After the image update completes, Redundant
Management functionality will be unavailable until the system has been rebooted.
Continue (y/n)? y
Connected to 192.168.2.116.
Changing to: /C/Users/Administrator/.
sftp> get E:/Descargas/ArubaOS-CX_6200_10_06_0101.swi image.dnld.VmeRRh
Fetching /C/Users/Administrator/E:/Descargas/ArubaOS-CX_6200_10_06_0101.swi to image.dnld.VmeRRh
/C/Users/Administrator/E:/Descargas/ArubaOS-C100% 338MB 5.6MB/s 01:00
Verifying and writing system firmware...
Aruba-CX(config)#
```

Secuencia 106 Copia remota de firmware y verificación positiva

330. Si el firmware no es correcto devuelve un mensaje de error informando de su inconsistencia

```
Fetching /C/Users/Administrator/E:/Descargas/WC_16_10_0014.swi to image.dnld.4M8eMe
/C/Users/Administrator/E:/Descargas/WC_16_10_100% 29MB 6.6MB/s 00:04
Verifying and writing system firmware...
Firmware image signature is not valid
Aruba-CX(config)#
```

Secuencia 107 Copia remota de firmware y verificación negativa

6.11.2 VERIFICACIÓN DE SOFTWARE CUANDO ES EJECUTADO

331. También se realiza un chequeo durante el arranque antes de cargar el firmware

```
Looking for SVOS.
Primary SVOS: Checking...Loading...Finding...Verifying...Booting...
ServiceOS Information:
  Version:      ML.01.08.0002
  Build Date:   2021-02-19 08:02:23 UTC
```

```

Build ID:      ServiceOS:ML.01.08.0002:04af6da43747:202102190802
SHA:          04af6da43747146d6da5ab9ca4622efa65289a78
Boot Profiles:
0. Service OS Console
1. Primary Software Image [ML.10.06.0101]
2. Secondary Software Image [ML.10.07.0004]
Select profile(primary):
Booting primary software image...
Verifying Image...
Image Info:
  Name: ArubaOS-CX
  Version: ML.10.06.0101
  Build Id: ArubaOS-CX:ML.10.06.0101:f197b0b27572:202103010059
  Build Date: 2021-02-28 17:31:44 PST
Extracting Image...
Installing Rootfs...
Loading Image...
Done.
kexec_core: Starting new kernel
System is initializing

```

Secuencia 108 Captura de arranque, destacando verificación del software

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

- 332. AOS-CX crea registros locales de eventos y seguridad y puede utilizar el protocolo syslog para enviar estos registros a un servidor remoto con fines de análisis y auditoría.
- 333. El cliente syslog utiliza por defecto UDP para la comunicación syslog, aunque también se admiten TCP y TLS.
- 334. Cuando se configura AOS-CX para enviar registros a un servidor remoto, es una práctica común establecer un valor de facilidad. Este valor actúa como una etiqueta que el servidor remoto puede utilizar para determinar qué archivo debe adjuntar el mensaje syslog.
- 335. A continuación se muestra un ejemplo de cómo configurar AOS-CX para enviar mensajes de registro de eventos a través de syslog a un servidor remoto.
- 336. Se recomienda que se use protocolo TLS e idealmente, firmado con certificado.
- 337. Este ejemplo utiliza la instalación por defecto de local7 y envía mensajes de eventos marcados como informativos y superiores, desde la *VRF mgmt* así como eventos relacionados con el accounting de seguridad:

```
logging 1.1.1.1 tls vrf mgmt legacy-tls-renegotiation auth-mode certificate
```

Secuencia 109 Ejemplo de syslog remoto con cifrado basado en certificados

6.13 BACKUP

6.13.1 CHECKPOINTS

- 338. Un Checkpoint (punto de control) es una instantánea de la configuración en ejecución de un conmutador y sus metadatos relevantes durante el tiempo de creación.
- 339. Los Checkpoint se pueden utilizar para aplicar la configuración del conmutador almacenada en un punto de control siempre que sea necesario, por ejemplo, para volver a una configuración anterior y limpia.

340. Los puntos de control pueden aplicarse a otros conmutadores de la misma plataforma.

341. El conmutador admite dos tipos de puntos de control:

- a) Puntos de control generados por el sistema: El conmutador genera automáticamente un punto de control del sistema cada vez que se produce un cambio de configuración.
- b) Puntos de control generados por el usuario: El administrador puede generar manualmente un punto de control siempre que sea necesario.

342. Un conmutador puede almacenar múltiples puntos de control Checkpoint máximos: 64 (incluyendo la configuración de inicio)

- a) Checkpoints de usuario máximos: 32
- b) Checkpoints del sistema: 32

343. Checkpoint de Usuario

- a) Los puntos de control del usuario pueden crearse en cualquier momento, siempre que exista una diferencia de configuración desde que se creó el último punto de control.
- b) Los puntos de control pueden aplicarse a las configuraciones en ejecución o de inicio del conmutador.
- c) Todos los puntos de control generados por el usuario incluyen una marca de tiempo para identificar cuándo se creó el punto de control.

344. Checkpoint de sistema

- a) Los puntos de control generados por el sistema se crean automáticamente por defecto.
- b) Cada vez que se produce un cambio de configuración, el switch inicia un contador de tiempo de espera (300 segundos por defecto). Para cada cambio de configuración adicional, el contador de tiempo de espera se reinicia. Si el tiempo de espera expira sin que se realicen cambios de configuración adicionales, el conmutador genera un nuevo punto de control.
- c) Los puntos de control generados por el sistema se denominan con el prefijo CPC seguido de una marca de tiempo en el formato <AAAAMMDDHHMMSS>. Por ejemplo: CPC20170630073127.
- d) Los puntos de control del sistema se pueden aplicar utilizando la función de retroceso de puntos de control o el comando de copia. Se puede crear un máximo de 32 puntos de control del sistema.
- e) Más allá de este límite, el punto de control del sistema más reciente sustituye al punto de control del sistema más antiguo.

345. Formato de fichero soportados

- a) Puede restaurar una configuración del conmutador copiando una configuración del conmutador almacenada en una unidad USB o en un dispositivo de red remoto a través de SFTP/TFTP.
- b) Los formatos de archivos remotos que admite el conmutador dependen del lugar en el que se vaya a restaurar el punto de control.

Restaurando un checkpoint en ...	Formato de fichero
Running Configuration	CLI
	JSON
	Punto de control
Startup Configuration	JSON
	Punto de control
Checkpoint seleccionado	Checkpoint específico

Secuencia 110 Formato de fichero permitido para operaciones con Checkpoints

6.13.2 ROLLBACK

346. El término rollback se utiliza para referirse a cuando la configuración de un switch se revierte a un punto de control preexistente.

347. Por ejemplo, el siguiente comando aplica la configuración del punto de control *ckpt1*. Todas las configuraciones anteriores se pierden después de la ejecución de este comando:

```
checkpoint rollback ckpt1
```

Secuencia 111 Restauración de una configuración (checkpoint)

348. También puede especificar la reversión de la configuración en ejecución o de la configuración de inicio con un punto de control especificado, como se muestra con el siguiente comando:

```
copy checkpoint <nombre del punto de control>{running-config | startup-config}
```

Secuencia 112 Restauración de un Checkpoint a la configuración, running o startup

6.13.3 MODO CHECKPOINT AUTO

349. El modo automático de punto de control configura el conmutador con soporte de conmutación por error, haciendo que vuelva automáticamente a la configuración anterior si se vuelve inoperable o inaccesible debido a los cambios de configuración que se están realizando.

350. Después de entrar en el modo automático de punto de control, tiene una cantidad de tiempo establecida para añadir, eliminar o modificar la configuración existente del conmutador. Para guardar los cambios, debe ejecutar el comando *checkpoint auto confirm* antes de que expire el temporizador del modo automático.

351. Si no ejecuta el comando *checkpoint auto confirm* dentro del tiempo especificado, todos los cambios de configuración que haya realizado se descartarán y la configuración en ejecución volverá al estado en que se encontraba antes de entrar en el modo *checkpoint auto*.

352. Probar hacer uso de esta funcionalidad:

- a) Habilite el modo *checkpoint auto*.

```
checkpoint auto <TIME-LAPSE-INTERVAL>
```

Secuencia 113 Activación Modo Checkpoint auto

- b) Para guardar la configuración, antes del tiempo especificado en el paso 1, introduzca el comando

```
checkpoint auto confirm
```

Secuencia 114 Confirmación Modo Checkpoint

6.14 SERVICIOS DE SEGURIDAD ADICIONALES

6.14.1 DESACTIVACION BLUETOOTH

353. Es posible desactivar la funcionalidad de bluetooth

```
switch(config)# bluetooth disable
switch# show bluetooth
Enabled : No
Device name : <XXXX>-<NNNNNNNNNN>
switch(config)# show running-config
...
bluetooth disabled
...
```

Secuencia 115 Desactivación Bluetooth

6.15 CONTROL DE ACCESO A LA RED

354. Una de las funciones más relevantes que pueden realizar estos equipos es el autenticar, autorizar y registrar los accesos a la red de los usuarios y dispositivos.
355. Una buena práctica sería disponer que todos los puertos de red habilitados, autenticuen a los dispositivos que se intenten conectar. De esta forma, evitamos que usuarios que tengan acceso físico a las dependencias de nuestra organización, puedan conectar cualquier dispositivo sin autorización.
356. Esto sin duda, mejoraría la seguridad de la red y por tanto de nuestra organización. Esta funcionalidad no aporta en sí misma seguridad a la configuración del equipo, sino como se ha comentado al conjunto de sistemas y aplicaciones, y por tanto también a los equipos de red.
357. Se describe brevemente en este documento, para tener una visión de alto nivel de cómo sería configurar esta funcionalidad.
358. Para desplegar esta funcionalidad son necesarios tres pasos importantes:
- Configurar Servidores RADIUS. Estos servidores recibirán todas las peticiones de autenticación. Podrán estar integrados con diversos sistemas de identidades, como directorios, LDAPS, y BBDD.
 - Configurar políticas de usuarios. Para cada tipo de usuario, dispositivo o estado, podemos configurar su política correspondiente para que posteriormente le sea asignada .
 - Configurar los puertos para que realicen la autenticación.

359. En AOS-CX el comportamiento de los dispositivos conectados, las políticas de usuario, al equipo se puede regular con dos aproximaciones:

- a) Asignar la VLAN y filtros definidos por ACL.
- b) Asignar un role de usuario.

360. La primera opción, se trata de una aproximación clásica. El comportamiento podría venir regulado de dos formas:

- Estar predefinido en el puerto
- Se recibido como atributos radius adicionales en un proceso de autenticación RADIUS.

361. LA segunda opción, es más completa y ofrece más opciones. Un Role de Usuario es un objeto que agrupa la definición de diferentes elementos (se puede ver como un perfil o grupo de propiedades):

- a) *Ingress user policy*. Una política que regula los tráficos permitidos de entrada al puerto
- b) *VLAN Access*. VLAN de acceso asignada
- c) *VLAN Trunk*. Conjunto de VLANs con etiqueta 802.1Q
- d) *Inactivity timeout*. Tiempo de inactividad que implica automáticamente su desconexión
- e) *Reauth-periodo*. Temporizador de reautenticación.
- f) *Captive-portal-profile*. Asigna un Portal de invitados a este rol.
- g) *Auth-mode*. Configura el modo de autenticación. Se puede elegir:
 - *Client-mode*. que cada usuario/dispositivo se tenga que autenticar
 - *Device-mode*. El primer dispositivo que se autentica, abre el puerto para los demás. Este modo está indicado cuando conectamos algún dispositivo de red, como por ejemplo un punto de acceso, servidor con máquinas virtuales.

Se puede además configurar estos parámetros, no relacionados con la seguridad estrictamente

- h) *Poe-priority*. Parámetro para gestionar prioridades en consumo PoE.
- i) *Mtu*. Configura la MTU para el rol
- j) *Vlan trunk allowed*. Lista de VLANs configuradas para el interfaz.
- k) *Trust-mode*. Configura el modo de confianza de QoS.

362. Para más información sobre el control de acceso a la red, se recomienda los manuales de Security Guide de cada modelo y versión.

6.15.1 RADIUS CONTROL DE ACCESO A RED

363. Se muestra a continuación una configuración de referencia de:

- a) Configuración de servidores RADIUS
- b) Grupo de Servidores RADIUS

- c) Activación de la funcionalidad CoA
- d) Activación de métodos de autenticación

Configuración Global RADIUS	Comentarios
radius-server host radius1.dominio.com key ciphertext XXXXXXXXXX	Definición de un servidor radius, con la clave mutua
radius-server host radius2.dominio.com key ciphertext YYYYYYYYYY	Definición de un servidor radius, con la clave mutua
aaa group server radius grupo_radius	Definición de un grupo de RADIUS
server radius1.dominio.com	Inclusión de un servidor RADIUS en un grupo de servidores RADIUS
server radius2.dominio.com	Inclusión de un servidor RADIUS en un grupo de servidores RADIUS
!	Activación de la funcionalidad CoA
radius dyn-authorization enable	Seleccionamos un grupo de servidores RADIUS para 802.1X
!	Seleccionamos un grupo de servidores RADIUS para MAC-AUTH
aaa authentication port-access dot1x authenticator	Activamos la autenticación 802.1X a nivel dispositivo
radius server-group grupo_radius	Activamos la autenticación MAC-AUTH a nivel dispositivo
enable	
aaa authentication port-access mac-auth	
radius server-group grupo_radius	
enable	
aaa authentication port-access dot1x authenticator enable	
aaa authentication port-access mac-auth enable	

Secuencia 116 Ejemplo de configuración RADIUS del equipo para control de acceso a la red

6.15.2 DEFINICION DE ROLES DE USUARIO

364. Se muestra en en este ejemplo algunas definiciones de roles de usuario.

365. En primer lugar mostramos un ejemplo de algunos roles

DEFINICION DE ROLES LOCALES	Comentarios
!!! Definición ROLE ACCESO corporativo y externo	Definimos algunas clases de servicio
class ip corporativo	Clase de servicio para seleccionar accesos a entorno corporativo
10 match any any 10.20.0.0/255.255.0.0	Ejemplo: Rango Aplicativos CPD
class ip proxy	Clase de servicio para seleccionar accesos a proxy
10 match tcp any 10.1.2.3 eq 8888	Clase de servicio para seleccionar DHCP y DNS
class ip dhcp-dns	Clase de servicio para seleccionar ICMP a Rango CPD
10 match udp any any eq 67	Clase de servicio para seleccionar ICMP a proxy
20 match udp any any eq 53	Definición de Política corporativo
class ip ping-cpd	Permitimos DHCP y DNS
10 match icmp any 10.20.0.0/255.255.0.0	Permitimos accesos al CPD y proxy. Implícitamente, denegamos accesos laterales a equipos de su misma VLAN.
class ip ping-proxy	Permitimos ICMP
10 match icmp any 10.1.2.3	VLANS que serán asignadas a los roles
port-access policy p_corporativo	Definición de Política corporativo
10 class ip dhcp-dns	Permitimos DHCP y DNS
20 class ip corporativo	Permitimos accesos al proxy. Implícitamente, denegamos accesos laterales a equipos de su misma VLAN.
40 class ip proxy	Permitimos ICMP
30 class ip ping-cpd	
50 class ip ping-proxy	

<pre> port-access policy p_externo 10 class ip dhcp-dns 20 class ip proxy 30 class ip ping-cpd vlan 102 name corporativo vlan 2100 name externo port-access role corporativo associate policy p_corporativo reauth-period 14400 vlan access name corporativa port-access role externo associate policy p_externo reauth-period 3600 vlan access name externos </pre>	Definición role corporativo Asociamos la política “corporativo” con el role Indicamos que este dispositivo debe reautenticarse cada 4 horas Indicamos que la vlan asociada el vlan con nombre corporativa. Esto permite la misma definición en switches con diferente vlans
--	---

Secuencia 117 Ejemplos de roles de usuarios

DEFINICION DE ROLES LOCALES	Comentarios
<pre> !!! Definición ROLE INVITADOS PUERTO CABLEADO port-access role TelefonoIP client-inactivity timeout none vlan trunk allowed 103 poe-priority high </pre>	Definición role Definimos que no se expulse el equipo por inactividad Asociamos vlan 103 en modo trunk para un teléfono IP Indicamos PoE con prioridad crítica

Secuencia 118 Ejemplos de roles para teléfono IP

DEFINICION DE ROLES LOCALES	Comentarios
<pre> !!! Definición ROLE INVITADOS PUERTO CABLEADO class ip clearpass 10 match tcp any 192.168.255.15 eq 80 20 match tcp any 192.168.255.15 eq 443 class ip dhcp-dns 10 match udp any any eq 67 20 match udp any any eq 53 class ip http 10 match tcp any any eq 80 20 match tcp any any eq 443 class ip ping 10 match icmp any any port-access policy cp_policy 10 class ip dhcp-dns 20 class ip clearpass 30 class ip ping 40 class ip http action redirect captive-portal </pre>	Definimos algunas clases de servicio Clase de servicio para seleccionar accesos a PORTAL Clase de servicio para seleccionar DHCP y DNS, necesarios para portal de invitados Clase de servicio para seleccionar HTTP y HTTPS necesarios para portal Clase de servicio para seleccionar ICMP Definición de Política Permitimos DHCP y DNS Permitimos accesos a Portal Invitados Permitimos ICMP REDIRIGIMOS tráfico navegación a portal invitados Definición perfil portal invitados URL del portal Definición role Asociamos el portal de invitados con este role Asociamos una política con el role

<pre> aaa authentication port-access captive-portal-profile cp_guest url https://portal.dominio.com/guest/aoswitch_guest.php port-access role invitado_cable associate captive-portal-profile cp_guest associate policy cp_policy </pre>	
--	--

Secuencia 119 Ejemplo de roles para invitados conectados a puertos de cobre

6.15.3 CONFIGURACION PUERTO

366. Se presenta una configuración modelo que contempla la potencial autenticación 802.1X y MAC-AUTH en un puerto. El control de acceso recae en el RADIUS server.

367. El RADIUS server, además de mandar las respuestas ACCEPT o REJECT, puede mandar otros atributos entre los que puede

Configuración recomendada autenticación 802.1X y MAC-AUTH simultanea	Comentarios
<pre> interface 1/1/12 no shutdown no routing vlan access 10 spanning-tree bpduguard spanning-tree root-guard spanning-tree tcnguard spanning-tree port-type admin-edge port-access onboarding-method concurrent enable aaa authentication port-access allow-cdp-bpdu aaa authentication port-access allow-lldp-bpdu aaa authentication port-access client-limit 2 aaa authentication port-access preauth-role PreauthRole aaa authentication port-access reject-role RejectRole aaa authentication port-access auth-role AuthRole aaa authentication port-access dot1x authenticator cached-reauth cached-reauth-period 86400 eapol-timeout 30 max-eapol-requests 1 max-retries 1 reauth enable aaa authentication port-access mac-auth cached-reauth cached-reauth-period 86400 quiet-period 30 reauth enable client track ip enable </pre>	Puerto habilitado Puerto que hace switching Asignación inicial del puerto Comandos de spanning-tree recomendados Permite autenticación simultanea 802.1X y MAC Permite CDP con el puerto sin autenticar (para tel. IP, y similares) Permite LLDP con el puerto sin autenticar (para tel. IP) Se limita el número de MACs en el puerto Política que se asigna al equipo previo a la autenticación (MAC) Política que se asigna al equipo en caso de ser rechazado Política que se asigna al equipo en caso de ser aceptado Sección de autenticación 802.1X Utilización de credenciales cacheadas, si RADIUS caído tras la autenticación del dispositivo. Temporizador Timeout de 802.1X Peticiones máximas 802.1X Reintentos máximos Reautenticación periódica activada Activación del mecanismo de autenticación 802.1X Sección de autenticación MAC-AUTH Utilización de credenciales cacheadas, si RADIUS caído tras la autenticación del dispositivo. Temporizador Tiempo que el switch no intenta reautenticar a un cliente rechazado Reautenticación periódica activada Activación del mecanismo de autenticación MAC-AUTH Rastreo de ip asignada al dispositivo Periodo de actualización Mecanismo detección bucle

```
client track ip update-interval 60
loop-protect
exit
```

Secuencia 120 Plantilla de configuración de buenas prácticas para swtiches CX

6.16 RESETEO A FABRICA (FACTORY DEFAULTS)

368. El método recomendado para devolver un conmutador Aruba CX a la configuración predeterminada de fábrica es ponerlo a cero.

369. Cuando se inicia el proceso de puesta a cero ocurre lo siguiente:

- El conmutador se reinicia a ServiceOS
- Los archivos de imagen de software primario y secundario se respaldan en la memoria desde el almacenamiento flash
- Todo el dispositivo de almacenamiento flash se sobrescribe con ceros para borrar de forma segura todos los datos almacenados
- El dispositivo de almacenamiento flash se reformatea con un sistema de archivos predeterminado de fábrica
- Los archivos de imagen de software respaldados se escriben en flash en sus ubicaciones originales
- El conmutador se reinicia a la imagen de software primaria con una configuración predeterminada.

370. Hay cuatro métodos que se pueden utilizar para poner a cero un switch.

371. En primer lugar, un usuario administrador puede utilizar el comando *erase all zeroize* de la CLI del AOS-CX:

```
switch# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)?
```

Secuencia 121 Método zeroize para borrado de equipo

372. En segundo lugar, y para equipos 6400 o 8400 un usuario administrador puede utilizar el comando *erase zeroize* desde la CLI de ServiceOS, para borrar de forma segura cualquier dato del usuario contenido en el SSD u otros dispositivos de almacenamiento del módulo de gestión:

```
SVOS> erase zeroize
#####WARNING#####
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
#####WARNING#####
Continue (y/n)?
```

Secuencia 122 Método de borrado de equipos desde ServiceOS para equipos formato chasis (8400 y 6400)

373. En tercer lugar, un usuario con acceso físico al panel frontal del conmutador y a un dispositivo de almacenamiento USB con formato FAT32 puede poner a cero el conmutador (El USB se usa a modo de verificar el acceso físico al equipo, equivalente a un hipotético botón de reset que no existe). Desde el prompt de inicio de sesión de ServiceOS introduciendo el nombre de usuario zeroize y siguiendo las instrucciones proporcionadas:

```
ServiceOS login: zeroize
This will securely erase all customer data, including passwords, and
reset the switch to factory defaults.
This action requires proof of physical access via a USB drive.
* Create a FAT32 formatted USB drive
* Create a file in the root directory of the USB drive named zeroize.txt
* Type the following serial number into the zeroize.txt file: xxxxxxxxxx
* Insert the USB drive into the target module
* Confirm the following prompt to continue
Continue (y/n)?
```

Secuencia 123 Metodo de borrado mediante acceso físico al equipo y llave USB

374. Por último, al cambiar el modo de seguridad del conmutador, éste se pone a cero. Consulte la sección 5.3 MODO DE SEGURIDAD mejorado para obtener más información.

7 FASE DE OPERACIÓN

375. Durante la fase de operación se recomiendan algunas tareas periódicas.

7.1 SEGURIDAD

376. Seguridad y eventos de seguridad

377. puesta al día

7.2 COPIAS DE SEGURIDAD

378. Hacer copias de seguridad con regularidad, con alguno de estos métodos:

- a) Copia manual o automatizada, como se ha indicado en la sección 5.14 BACKUP
- b) Hacer uso de alguna herramienta de Gestion de Red
- c) Hacer uso de la gestión cloud, Aruba Central.

7.3 MONITORIZACION

379. Monitorización del equipo. Puede realizarse de varias formas

- a) Hacer uso de alguna herramienta de Gestion de Red
- b) Hacer uso de la gestión cloud, Aruba Central.
- c) Monitorización del agente NAE del equipo. Este agente, que se dispone en modelos 6200 y superiores, permite la monitorización

7.3.1 NETWORK ANALYTICS ENGINE (NAE)

380. Este módulo de analíticas integrado en el equipo, dispone de su propio manual *Aruba Netowrk Analytics Engine* ([REF4]-[REF11])

381. El motor de análisis de red (Network Analytics Engine, NAE) se accede desde el interfaz HTTPS del equipo.

382. El motor de análisis de red (Network Analytics Engine, NAE) de Aruba es el primer marco integrado de su clase para el aseguramiento y la corrección de la red. Combinando las capacidades de automatización completa y visibilidad profunda del sistema operativo AOS-CX, este marco único permite la supervisión, la recopilación de datos de red, la evaluación de las condiciones y la toma de acciones correctivas a través de agentes de scripting simples.

383. Este motor está integrado con la configuración del sistema AOS-CX y las bases de datos de series temporales, lo que le permite examinar las tendencias históricas y predecir los problemas futuros debido a la escala, la seguridad y los cuellos de botella de rendimiento.

384. Con esa información, puede crear módulos de software que detectan automáticamente estos problemas y tomar las acciones apropiadas.

385. Con la visión de la red más rápida y la automatización proporcionada por el motor de análisis de red de Aruba, puede reducir el tiempo dedicado a las tareas manuales

7.3.1.1 INTERFAZ GUI PARA ANALITICAS

386. La interfaz web de AOS-CX proporciona acceso a la información relacionada con los agentes, scripts y alertas de Aruba Network Analytics Engine en el conmutador, incluidos los gráficos de datos de series temporales y otra información generada por los agentes habilitados.
387. En la interfaz web de AOS-CX, seleccione Analytics en el panel de navegación para ver la información en el panel de control de Analytics.
388. Puede mostrar paneles de gráficos de series temporales para un máximo de nueve agentes en el tablero. Sin embargo, se pueden habilitar muchos más agentes en un conmutador.
389. Las páginas de detalles de análisis le permiten activar, desactivar, crear, eliminar o editar agentes, cargar scripts y ver datos detallados sobre los recursos supervisados. Se requieren derechos de administrador para las acciones que modifican un agente.

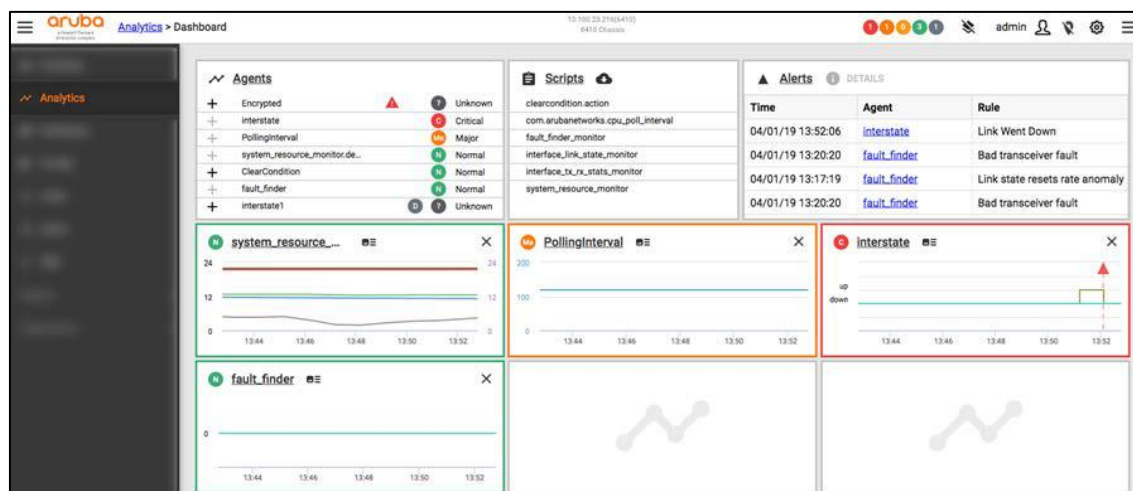


Ilustración 4 Captura interfaz NAE

7.3.1.2 SCRIPTS DE ARUBA NAE

390. Un script de Aruba Network Analytics Engine es un script de Python que define qué recursos del switch deben ser monitorizados y, opcionalmente, reglas que definen qué acciones tomar cuando ciertas condiciones son verdaderas.
391. Ejemplos de tareas que un script puede definir incluyen las siguientes:
- Monitorizar el uso medio de la CPU y enviar un mensaje de registro del sistema cuando el uso de la CPU es mayor del 70% durante 5 minutos.
 - Monitorizar el estado de la conexión de un vecino BGP particular y ejecutar un comando CLI cuando el estado de la conexión pasa de UP a DOWN.
392. Un script se utiliza para crear un agente, que es una instancia ejecutable específicamente configurada de un script en un switch. Un solo script puede ser la plantilla para muchos agentes diferentes.

7.3.1.3 AGENTES EN ARUBA NAE

393. Un agente de Aruba Network Analytics Engine es una instancia ejecutable específicamente configurada de un script NAE en un conmutador. Cuando el agente está habilitado, realiza las tareas definidas por el script. Los agentes tienen derechos de administrador.
394. Para los scripts que proporcionan parámetros de configuración, los diferentes agentes pueden ser configurados para utilizar valores de parámetros específicos al realizar las tareas definidas por el script.
395. Por ejemplo, un script que monitoriza el estado de conexión de un vecino BGP en particular puede definir un parámetro para especificar qué vecino BGP monitorizar. Desde esa secuencia de comandos, puede hacer lo siguiente:
- a) Puede crear un agente para supervisar un vecino BGP específico especificando ese vecino BGP como valor del parámetro.
 - b) Puede crear varios agentes, uno para cada vecino BGP que desee supervisar.
 - c) Cuando se añade un nuevo vecino BGP, puede crear un agente para supervisar ese vecino sin tener que cambiar la propia secuencia de comandos.
396. Algunos parámetros que son enteros, como un umbral de utilización de la CPU, pueden cambiarse para un agente determinado después de que se haya creado ese agente. Los administradores de red pueden cambiar estos parámetros fácilmente a través de la interfaz de usuario web, sin necesidad de tener conocimientos de programación.

7.4 ACTUALIZACIONES FIRMWARE

397. Se recomienda mantener el equipo actualizado, tanto desde un punto de vista de seguridad y operativo.
398. Se puede verificar las versiones en Aruba Support Portal [REF1]

8 CHECKLIST

399. Se presenta una checklist con las recomendaciones, asumiendo que se ha elegido el método de configuración inicial a través de puerto de consola.
400. En el caso que el método elegido sea configuración automática sin intervención humana (ZTP por ejemplo) se deberá crear una configuración final que contengan todos los empleados.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	—	—	No aplica. Aruba CX no requiere de licencias en los equipos
Recopilación de datos: Hostname, IP, Credenciales de administrador	☐	☐	
Conexionado de puerto fuera de banda	☐	☐	Recomendado
Primera conexión inicial al equipo. Configuración password usuario admin.	☐	☐	
Stack o chasis virtual.	☐	☐	En caso que el equipo vaya a formar parte de un stack o chasis virtual, proceda a establecerlo en este punto.
Configuración de hostname	☐	☐	Recomendado
Configuración del interfaz fuera de banda, o como alternativa, interfaz VLAN para gestión	☐	☐	
Actualización de firmware	☐	☐	Recomendado
Configurar password de acceso a ServiceOS	☐	☐	Recomendado
Autenticación local (en el equipo) de usuarios administradores. Complejidad de la password. Limitación de intentos de login fallidos y bloqueo	☐	☐	Se recomienda que la autenticación principal sea contra un servidor RADIUS o TACACS. En caso de hacer uso de usuarios locales se recomiendan esas medidas.

ACCIONES	SÍ	NO	OBSERVACIONES
Autenticación remota de usuarios administradores (RADIUS o TACACS)	☐	☐	Recomendado
Configuración CLI: Limitación de sesiones por usuario Temporizador de desconexión de sesiones	☐	☐	Recomendado
Banner de Acceso	☐	☐	Recomendado
Sincronización horaria	☐	☐	Recomendado
Instalación de certificados	☐	☐	Recomendado
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Puertos de red: Apagado de puertos no configurados	☐	☐	Recomendado en caso de no hacer uso de autenticación de acceso a la red (NAC)
Puertos de red: Limite de MAC por puerto	☐	☐	Opcional, en función del entorno
Limitación del tráfico BroadCast y Multicast	☐	☐	Recomendado
Protección paquetes Spanning Tree	☐	☐	Recomendado (en caso de
Filtros de tráfico (ACL o roles de usuario)	☐	☐	Recomendado. Se recomienda que todos los tráficos de los usuarios, sean restringidos en la medida de lo posible al uso necesario.
Restricción de accesos SSH y HTTPS	☐	☐	Recomendado. Se debe restringir cómo se pueden acceder a esos servicios
Restricción de accesos al equipo (ACL Management)	☐	☐	Recomendado. Se debe restringir cómo se pueden acceder las funcionalidades del equipo
Configuración SNMPv3	☐	☐	Recomendado
Mitigación de ataques (DHCP Snooping, ARP Inspection y Control Plane Policy)	☐	☐	Recomendado

ACCIONES	SÍ	NO	OBSERVACIONES
BGP y OSPF. Autenticación con vecinos	☐	☐	Recomendado. Esta configuración debe hacerse en coordinación con el equipo vecino.
Configuración de SYSLOG externo	☐	☐	Recomendado.
	☐	☐	
CONFIGURACIÓN			
CONTROL DE ACCESO A LA RED			
Configuración servidor(es) RADIUS	☐	☐	Recomendado
Configuración de las diferentes políticas de los dispositivos y usuarios	☐	☐	Recomendado
Configuración de los puertos para autenticar dispositivos	☐	☐	Recomendado

9 REFERENCIAS

- [REF1] Portal de soporte, documentación, licenciamiento, notificaciones de seguridad y otras funciones.
Aruba Support Portal <https://asp.arubanetworks.com>
- [REF2] Aplicación Aruba CX Apple Store
<https://apps.apple.com/us/app/aruba-cx/id1414572411>
- [REF3] Aplicación Aruba CX Google Play
https://play.google.com/store/apps/details?id=com.arubacx&hl=en_US&gl=US
- [REF4] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6300-6400.pdf
- [REF5] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6200.pdf
- [REF6] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6000-6100.pdf
- [REF7] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8400.pdf
- [REF8] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8360.pdf
- [REF9] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8325.pdf
- [REF10] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8320.pdf
- [REF11] Manuales producto
Documentation Portfolio for 10.08
https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_4100i.pdf

10 ABREVIATURAS

ACL	Access Control List
AH	Authentication Header
AOS-CX	ArubaOS-CX
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
BPDUs	Bridge Protocol Data Units
CA	Corriente Alterna
CLI	Command Line Interface
CN	Common Name
CoPP	Control Plane Policing
CPD	Centro de Proceso de Datos
CPU	Central Processing Unit
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration 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)
GUI	Graphical User Interface
HSC	Hardware Switch Controller
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security

JSON	JavaScript Object Notation
LED	Light-Emitting Diode
MAC	Media Access Control
MD5	Message Digest Algorithm 5
MVRP	Multiple VLAN Registration Protocol
NAE	Network Analytics Engine
NMS	Network Management System
NTP	Network Time Protocol
OOBM	Out-of-Band Management
OS	Operating System
OS-CX	Operating System-CX
OSPF	Open Shortest Path First
PEM	Privacy-Enhanced Mail
PKI	Public Key Infrastructure
PPS	Packets Per Second
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
REF	Reference
REST	Representational State Transfer
RFC	Request for Comments
RJ-45	Registered Jack 45
RMA	Return Merchandise Authorization
RSA	Rivest-Shamir-Adleman
SaaS	Software-as-a-Service
SAN	Subject Alternative Name
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
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2

SHA-256	Secure Hash Algorithm 256-bit
SHA-512	Secure Hash Algorithm 512-bit
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
Syslog	System Logging Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTL	Time-To-Live
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VSF	Virtual Switching Framework
VSX	Virtual Switching Extension
X.509	ITU-T Standard for Public Key Infrastructure Certificates
ZTP	Zero Touch Provisioning

