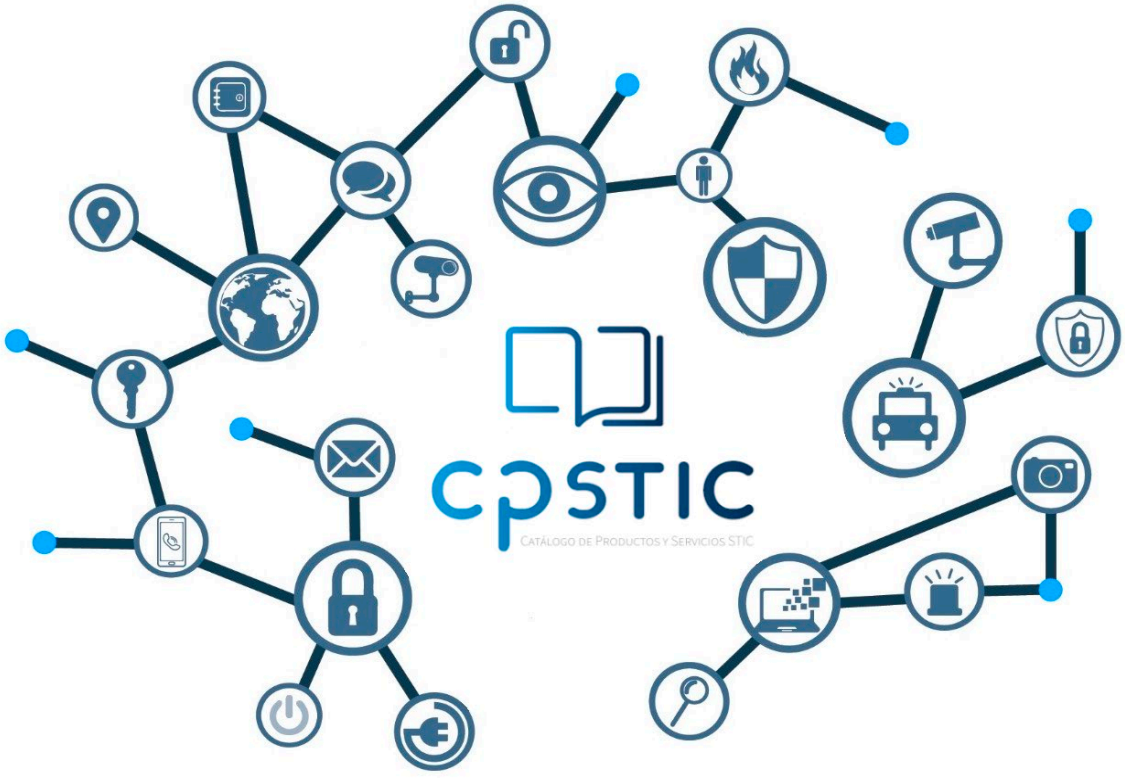
Guía de Seguridad de las TIC
CCN-STIC 1426

Procedimiento de empleo seguro
Huawei Wireless LAN AirEngine Series



Enero 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-041-4.
Fecha de Edición: Enero de 2024

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.01 12:32:51 +01'00'

ÍNDICE

1. INTRODUCCIÓN

1. Los equipos **Huawei Wireless LAN** combinan plataformas específicas de Controlador (*Access Controller*) y Punto de Acceso (*Access Points*) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas *Wi-Fi*, proporcionando acceso seguro a la red a usuarios inalámbricos.
2. Los Puntos de Acceso usan el denominado modo *FIT*. De esta manera son dependientes de un Controlador, el cual es capaz de gestionar una gran cantidad de Puntos de Acceso en modo *FIT* a la vez. El número de Puntos de Acceso que es capaz de gestionar depende del modelo del producto.
3. Los Controladores cuentan con la funcionalidad de un conmutador, a la vez que cuentan con funcionalidad específica para la gestión de Puntos de Acceso. Cuentan con varios puertos *GigabitEthernet*, cuyo número y disposición depende del modelo *hardware*.
4. Los *Huawei Wireless LAN* disponen de tres (3) interfaces de administración:
    - SSH: Interfaz de línea de comandos.
    - Serial: Interfaz de línea de comandos.
    - Web (HTTPS): Interfaz gráfica. Solo debe utilizarse durante la instalación del producto.

2. OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad de los Controladores y Puntos de Acceso Huawei con el ***firmware V200R020C00SPC300*** (con parche ***V200R020C00SPH301T) y*** V200R022C00SPC100, (con parche V200R022C00SPH301T), de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.

6. Las configuraciones indicadas aplican a los siguientes modelos *hardware*:

Tipo	Familia	Modelos
Punto de Acceso	AP	AP6050DN, AP6150DN, AP4050DE-M, AP7060DN.
Punto de Acceso	AirEngine	AirEngine5760-51, AirEngine5760-22W, AirEngine5760-22WD, AirEngine5760-X1, AirEngine5760-X1E, AirEngine5760-51, AirEngine5760-51E, AirEngine5760-X1, AirEngine5760-X1-PRO, AirEngine5760-X1E, AirEngine 6760R-51E, AirEngine 8760R-X1E AirEngine 6761-21T, AirEngine 5762-12 AirEngine 5762-12SW, AirEngine 5762-13W AirEngine 5762-15HW, AirEngine 6761-22T AirEngine 5761-12, AirEngine 5762-16W AirEngine 8760-X1-PRO, AirEngine 8760R-X1 AirEngine 6760-X1, AirEngine 6760-X1E AirEngine 6760R-51, AirEngine 6760-51EI AirEngine 6761S-21T, AirEngine 6761-21 AirEngine 6761S-21, AirEngine 6761-21E AirEngine 5760-22W, AirEngine 5761-21 AirEngine 5761S-21, AirEngine 5761-11 AirEngine 5761S-11, AirEngine 5761-12W AirEngine 5761-11W, AirEngine 5761S-11W AirEngine 5761R-11, AirEngine 5761RS-11 AirEngine 5761R-11E, AirEngine 5761S-12 AirEngine 5761S-13, AirEngine 5761-10W AirEngine 5761S-10W, AirEngine 5761-10WD AirEngine 5762S-11SW, AirEngine 5762S-12SW AirEngine 5762S-13W, AirEngine 5762S-11 AirEngine 5762S-12, AirEngine 5761-11EI
Controlador	AC	AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S.
Controlador	AirEngine	AirEngine-9700-M, AirEngine-9700-M1, AirEngine-9700-S-S

7. Dicha versión y los modelos de la tabla anterior son los **cualificados e incluidos en el Catálogo de Productos y Servicios STIC (CPSTIC)**, en la familia '***Dispositivos Inalámbricos'***.

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se estructura en las secciones indicadas a continuación:

- **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- **Apartado 6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 7**. En este apartado se incluye una lista de tareas a revisar para verificar que se han llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.
- **Apartado 8**. En este apartado se recogen las referencias utilizadas en la presente guía de empleo seguro.
- **Apartado 9**. En este apartado se recogen las abreviaturas utilizadas en la presente guía de empleo seguro.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Al tratarse de una combinación *hardware/software*, los *Huawei Wireless LAN* se entregan por correo ordinario. El producto incluye tanto un Controlador de Acceso como un Punto de Acceso. Por ello, se debe comprobar:

    - **Información de envío**. Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Huawei.
    - **Embalaje externo**. Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Huawei. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
    - **Embalaje interno**. Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de dispositivo adquirido.
    - **Sello de garantía**. Se deberá verificar que la placa de identificación del producto, alojada en el chasis, es consistente con la etiqueta del embalaje del producto.

10. En caso de que exista algún desperfecto o alguna inconsistencia será necesario contactar con el soporte de Huawei de manera inmediata para recibir instrucciones. No se recomienda realizar la instalación en este caso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. Los componentes del producto deben instalarse en un entorno en el cual solo el personal técnico dispone de autorización para la configuración, despliegue y mantenimiento del producto.
12. Se deberá tener especial cuidado con la instalación de los Puntos de Acceso, los cuales no deberán estar a la vista o al alcance de usuarios estándar. Pueden ser instalados tanto en muros como en raíles T.

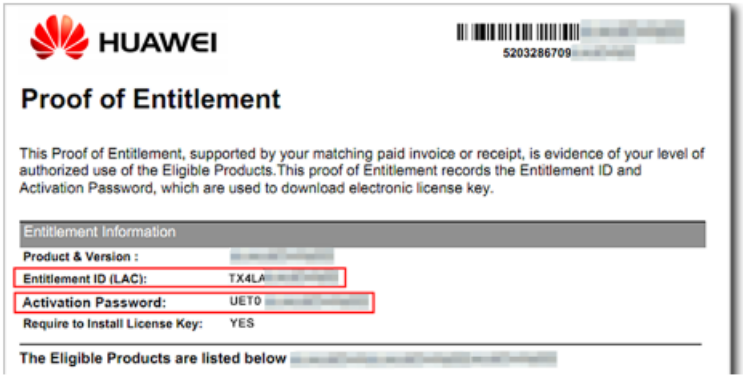
4.3 REGISTRO Y LICENCIAS

13. Existen dos (2) tipos de licencias para los dispositivos *Huawei Wireless LAN*:

    - **Licencia COMM**: la mayoría de las licencias adquiridas por contrato tienen una validez permanente, aunque puede darse el caso de que algunas tienen un periodo de validez hasta una fecha determinada.

- **Licencia DEMO**: son licencias usadas para casos especiales como pruebas o evaluaciones.

14. Para registrar la licencia se necesita contar con el archivo de licencia. Para obtener el archivo de licencia, se debe obtener la contraseña de activación en el *"Proof of Entitlement"* que se recibe al adquirir el producto.


HUAWEI

5203286709

Proof of Entitlement

This Proof of Entitlement, supported by your matching paid invoice or receipt, is evidence of your level of authorized use of the Eligible Products.This proof of Entitlement records the Entitlement ID and Activation Password, which are used to download electronic license key.

Entitlement Information	
Product & Version :	
Entitlement ID (LAC):	TX4LA
Activation Password:	UET0
Require to Install License Key:	YES

The Eligible Products are listed below

Ilustración 1. Obtención de licencias.

- Hacer *login* en el dispositivo y ejecutar el comando ***display esn*** para obtener el ESN del dispositivo.
- Hacer login en el ESDP de Huawei en *http://app.huawei.com/isdp*.
- Acceder a "*License Activation*" → "*Password Activation*"
- Introducir la contraseña de activación obtenida del "*Proof of Entitlement*", seleccionar "*I have read the above carefully*" y después pulsar "*Next*".
- Introducir el ESN obtenido anteriormente y hacer clic en "*Next*".
- Confirmar la activación haciendo clic en "*Activate License*".
- Finalmente, para descargar el archivo hacer clic en "*Download*".

15. Una vez obtenido el archivo de licencia, se debe iniciar sesión en el Controlador y transferir el archivo de licencia mediante SFTP. Usar el comando *license active <filename>* para activar la licencia. Si la licencia se instala correctamente, se mostrará el siguiente mensaje:

```
Info: The license is being activated. Please wait for a moment.
Info: Succeeded in activating the license file on the master board.
```

Ilustración 2: Mensaje de éxito al activar la licencia.

4.4 CONSIDERACIONES PREVIAS

16. Este producto consta de dos (2) dispositivos *hardware*, el Controlador de Acceso (AC) y el Punto de Acceso (AP). Ambos se suelen entregar juntos. Un Controlador de Acceso es capaz de controlar una gran cantidad de Puntos de Acceso a la vez y coordinarse con otros Controladores de Acceso.

17. A la hora de instalar el producto, se debe asegurar que se tiene acceso físico tanto al Punto de Acceso como al Controlador de Acceso, aunque se deben situar en sitios seguros lo más restringidos posibles.
18. Se debe asegurar que se cuentan con las herramientas de conectividad necesarias, tales como conectores RJ45 o cables serie necesarios para la administración del dispositivo.
19. El Controlador debe contar con el firmware y el parche instalados. En caso de no contar con el parche instalado, se deberá instalar. Para ello, el parche se deberá transferir al mediante SFTP al Controlador. Para ello se debe activar el servidor SFTP, el cual está desactivado por defecto.

```
$ sftp server enable
```

20. El Punto de Acceso debe contar con el firmware y el parche instalados. En caso de no contar con el parche instalado, se deberá instalar. Para ello, el parche se deberá transferir al mediante SFTP al Controlador de Acceso e instalarse como se detalla al final de la sección 4.5 INSTALACIÓN.

4.5 INSTALACIÓN

21. La instalación física de los Controladores de Acceso (ya sea en un *rack*, en un escritorio o en una pared), así como las medidas de precaución a tomar para cada uno de los diferentes casos se puede encontrar en la [REF1] en los módulos bajo *"Installation" → "Hardware Installation and Maintenance Guide" → "Access Controllers*". No obstante, se puntualiza que el lugar de instalación debe consistir en un lugar aislado y con buena ventilación, al que solo tenga acceso el personal autorizado.
22. La instalación física de los Puntos de Acceso (ya sea en pared o raíles), así como las medidas de precaución a tomar en cada uno de los diferentes casos se puede encontrar en la [REF1] en los módulos bajo "*Installation" → "Hardware Installation and Maintenance Guide" → "Indoor/Outdoor Access Points".*
23. El Controlador de Acceso se instalará en una ubicación apropiada y se conectará a la corriente. El Punto de Acceso se conectará a la corriente y a algún puerto del *GigabitEthernet* del Controlador de Acceso, bien sea punto a punto o mediante dispositivos de red. En caso de que el Punto de Acceso use alimentación mediante PoE, el Punto de Acceso se conectará únicamente mediante un cable RJ45 al inyector PoE, mientras que el inyector se conectará a la corriente y al Controlador de Acceso.
24. Se conectará un PC mediante puerto serie al Controlador de Acceso. A su vez, se conectará también el PC a la interfaz de gestión Ethernet (puerto ETH). Cuya IP por defecto es 169.254.1.1.

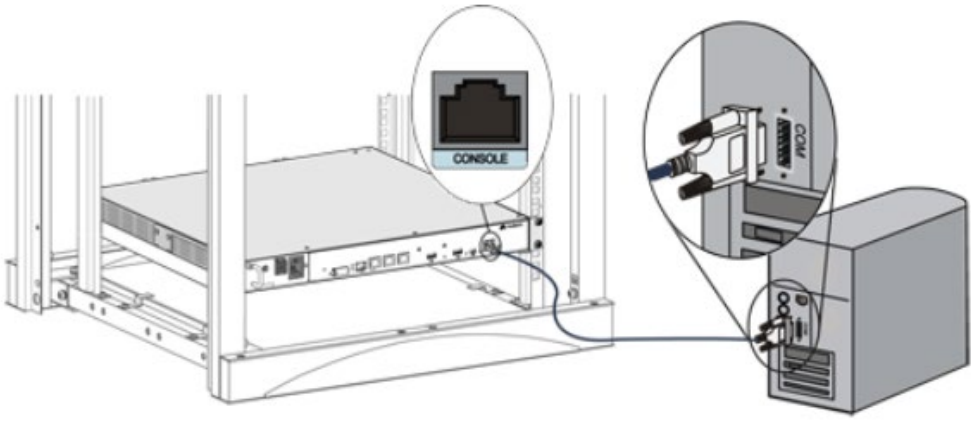


Ilustración 3: Conexión mediante puerto serie al Controlador

25. Una vez todo esté debidamente conectado, se procederá a iniciar sesión mediante el puerto serie. En el PC se hará uso del *software Putty* con los siguientes parámetros para iniciar sesión en el dispositivo. Es importante destacar que el parámetro "*Serial Line*" dependerá del número de puertos de cada PC.

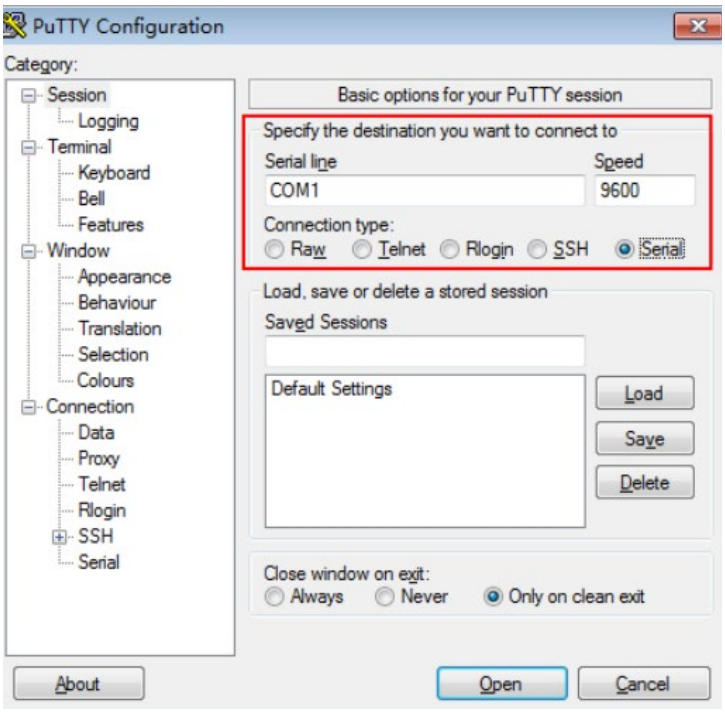


Ilustración 4: Conexión mediante puerto serie al Controlador haciendo uso de Putty

26. Al conectarse por primera vez, se requerirá introducir el nombre de usuario y la contraseña por defecto, los cuales son "*admin:admin@huawei.com*". Se deberá cambiar la contraseña del dispositivo.

27. De esta forma, ya estaría operativa la interfaz de comandos a través de la conexión *serial*.

28. Para establecer la conexión entre el Punto de Acceso y El controlador de Acceso mediante la CLI es necesario seguir las secciones "*Configuring a DHCP Server*",

"*Configuring Network Interconnections*", "*Configuring Country Codes*", "*Configuring a Source Interface or a Source Address*" y "*Adding APs*" de la guía [REF1], en el orden mencionado. Dichas secciones se encuentran bajo el módulo "*Configuration*" → "*CLI-based Configuration*" → "*WLAN Service Configuration Guide*" → "*Configuring APs to Go Online*".

29. En caso de que se desee realizar la instalación mediante la interfaz web, se debe acceder mediante el PC conectado al puerto de gestión a la dirección web https://169.254.1.1/. Se hará *login* con el usuario *admin* y la contraseña establecida previamente en el puerto serie. De esta manera la interfaz HTTPS quedará habilitada.

30. Para proceder a la instalación del producto mediante interfaz web, se deben seguir los siguientes pasos:

    a) Acceder a la sección "*Configuration*" y la sección "*Config Wizard*". Clic en "*AC*".

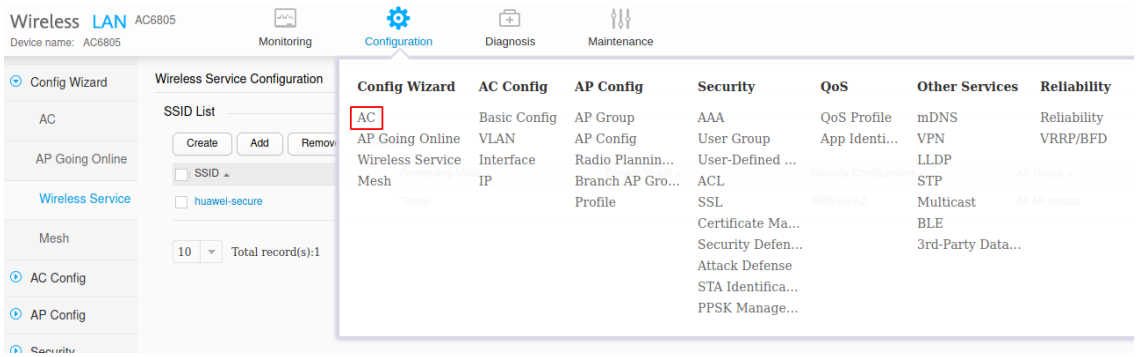


Ilustración 5: Menú de configuración del Controlador

    b) Establecer el nombre del Controlador de Acceso, la región, la hora y carga la licencia si no se ha hecho previamente.

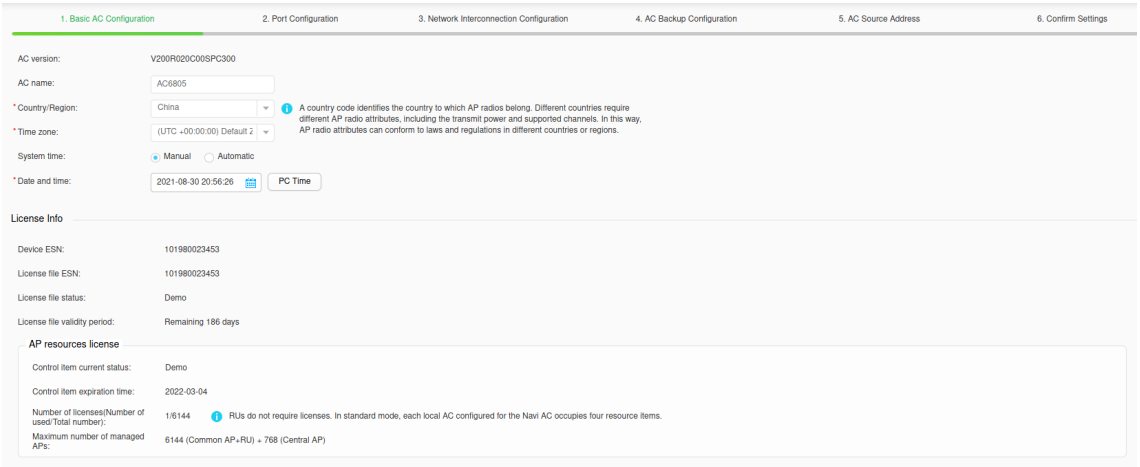


Ilustración 6: Sección de configuración básica del Controlador

    c) Hacer clic en "*Next*".

    d) Comprobar que el puerto en el que el AP está conectada es de color verde y que su VLAN por defecto es la VLAN 1. En esta instalación se usa la VLAN 1 como VLAN por defecto, aunque no es obligatorio usar exactamente dicha VLAN.

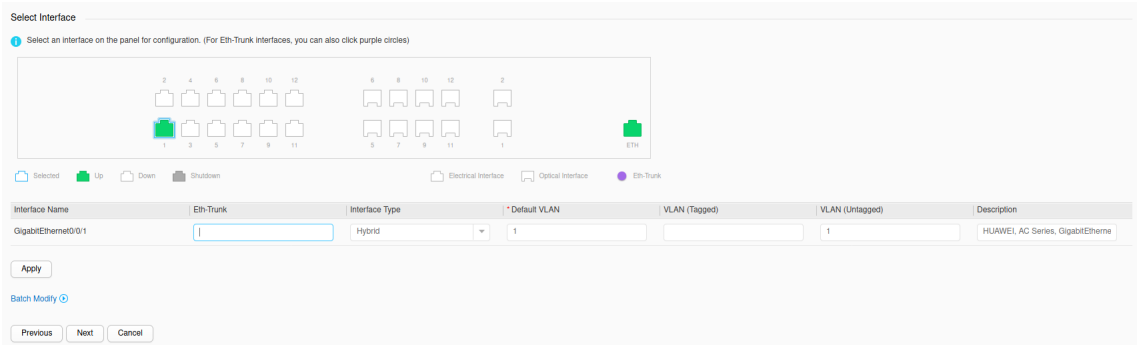


Ilustración 7: Sección de configuración de puertos del Controlador

e) Hacer clic en "*Next*".

f) Asegurar que el estado de DHCP se encuentra "*ON*".

Ilustración 8: Estado del servidor DHCP ON

g) En la sección "Interface Configuration", hacer clic en la VLAN establecida como VLAN por defecto para el puerto del Punto de Acceso.

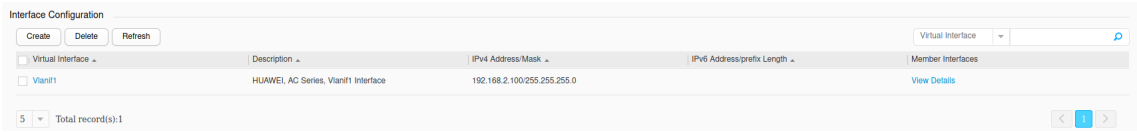


Ilustración 9: Sección de configuración de interfaces del Controlador.

h) Establecer una dirección IP para la VLAN por defecto y clic "OK".

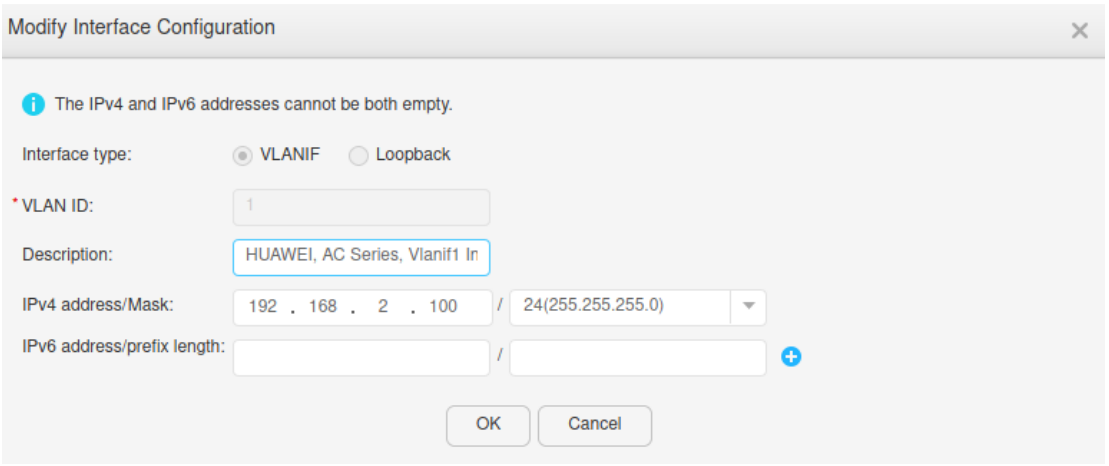


Ilustración 10: Configuración de interfaz del Controlador

i) En la sección "*DHCPv4 Address Pool List*", hacer clic en "*Create*"

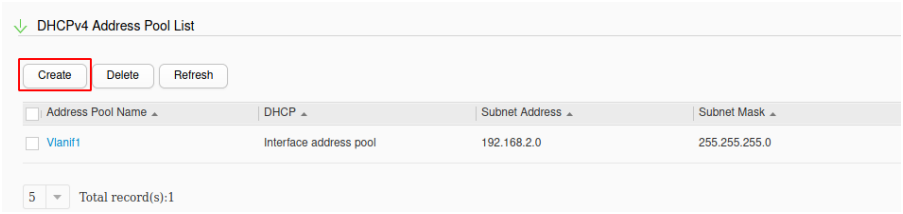


Ilustración 11: Configuración del conjunto de direcciones DHCP (I/II)

j) Seleccionar "*Interface Address Pool*" y seleccionar la interfaz por defecto usada en el puerto conectado al Punto de Acceso.

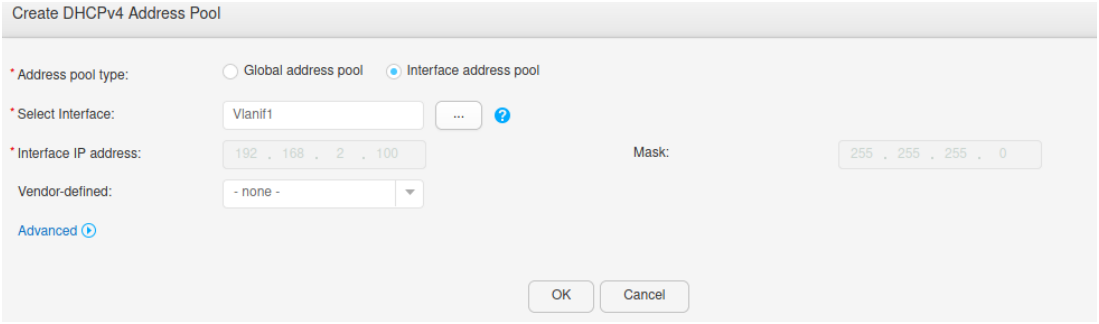


Ilustración 12: Configuración del conjunto de direcciones DHCP (II/II)

k) Hacer clic en "*OK*".

l) Hacer clic en "*Next*" de nuevo.

m) Configurar la dirección de la interfaz virtual recién creada. Seleccionar la VLAN recién creada en el campo "*Select interface*". Seleccionar el tipo de dirección IP (IPv4 en este caso) e introducir la dirección deseada.

n) Hacer clic en "*Next*".

o) Hacer clic en "*Next*" de nuevo en la sección de "*AC Backup Configuration*". El detalle de configuración de alta disponibilidad se encuentra en el apartado 5.12 ALTA DISPONIBILIDAD.

Ilustración 13: Sección de configuración de *Backups*

p) Establecer la VLAN de servicio, la cual será la establecida en el puerto conectado al Punto de Acceso. Para ello, seleccionarla en la sección de "*AC Source Address*"

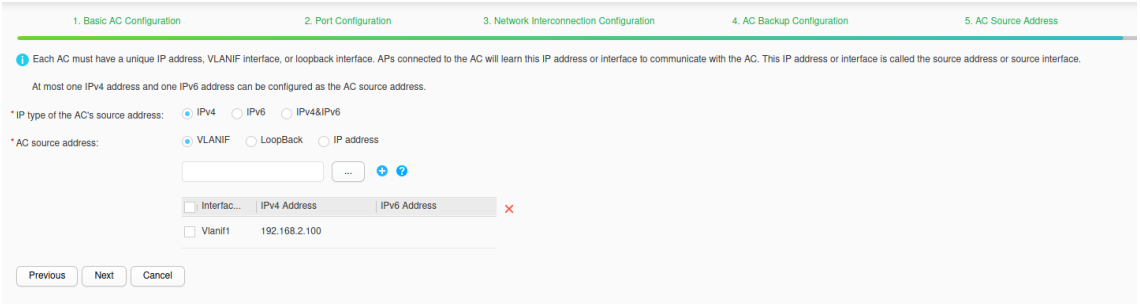


Ilustración 14: Sección de configuración de VLAN de servicio del Controlador

q) Hacer clic en "*Next*".

r) Revisar la configuración y hacer clic en "*Continue With AP Online*".

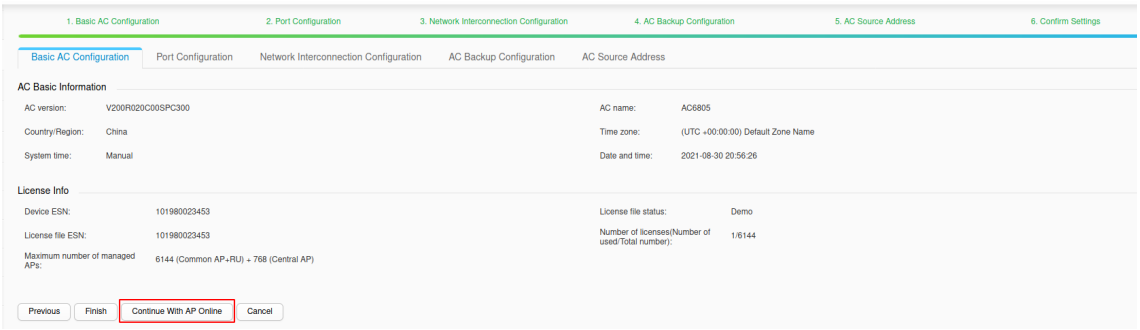


Ilustración 15: Sección de revisión de configuración del Controlador

s) Verificar que aparece el Punto de Acceso sin autenticar.

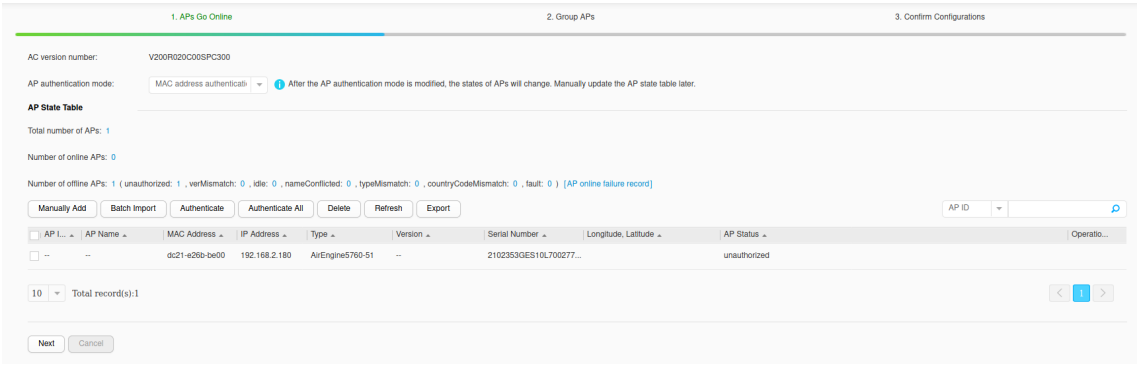


Ilustración 16: Sección de autenticación de Puntos de Acceso en el Controlador.

t) Seleccionar el AP y autenticarlo pulsando en "*Authenticate*". Una vez autenticado se debe añadir un valor al campo "*AP Name*"

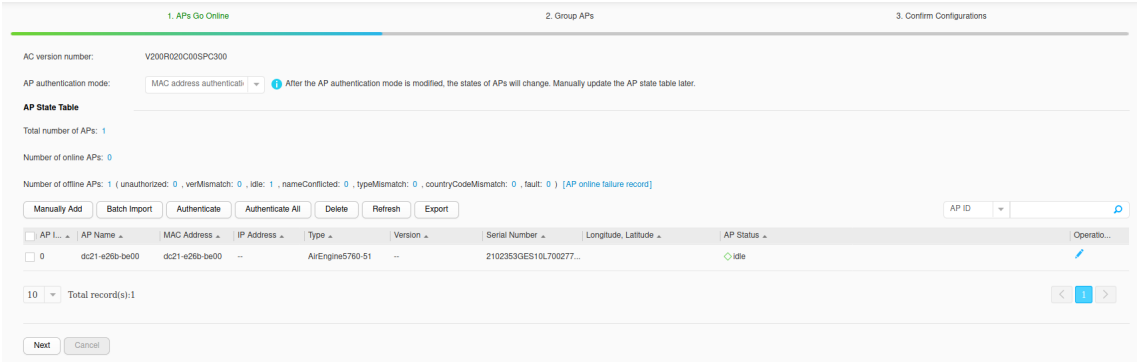


Ilustración 17: Punto de Acceso autenticado en el Controlador.

u) Hacer clic en "*Next*".

v) En este caso se incluirá el Punto de Acceso en el grupo *default*. Pulsar "*Next*".

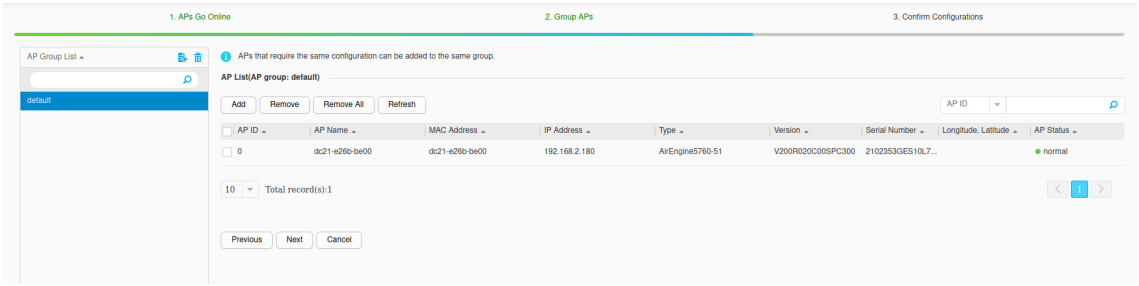


Ilustración 18: Enlace de Punto de Acceso a grupo en el Controlador

w) Comprobar que se ha añadido el Punto de Acceso al grupo default y pulsar "*Continue With Wireless Service Configuration*".

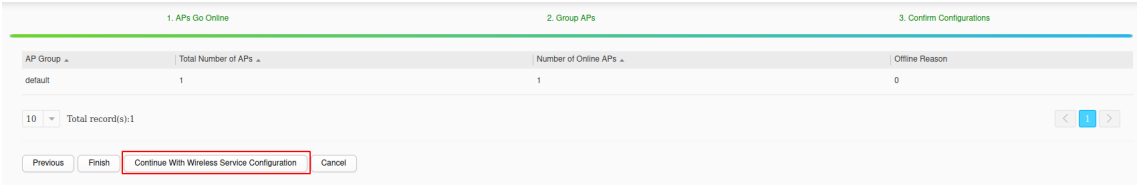


Ilustración 19: Revisión de puntos de acceso autorizados en el Controlador

x) En la sección "*Wireless Service Configuration*", crear un SSID. Para ello hacer clic en "*Create*".

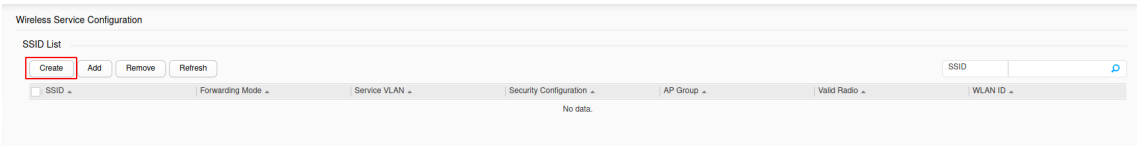


Ilustración 20: Creación de SSID

y) Establecer el nombre del SSID, la VLAN de servicio (en este caso corresponde a la VLAN la cual corresponde al puerto conectado al Punto de Acceso) y el modo de redireccionamiento (en este caso se usará modo túnel para encapsular todos los paquetes entre el Controlador de Acceso y el Punto de Acceso).

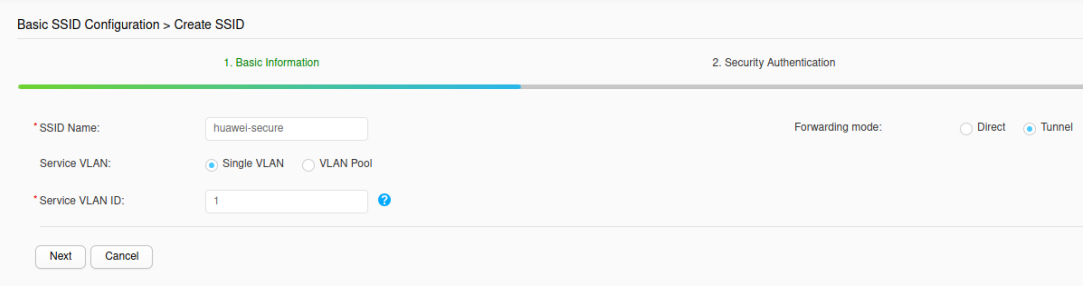


Ilustración 21: Configuración del nombre de SSID, VLAN de servicio y modo de redirección

z) Hacer clic en "*Next*".

aa) Establecer la seguridad del Punto de Acceso. En caso de escoger una clave, verificar que se utiliza únicamente AES y junto con una contraseña de longitud y complejidad considerable.

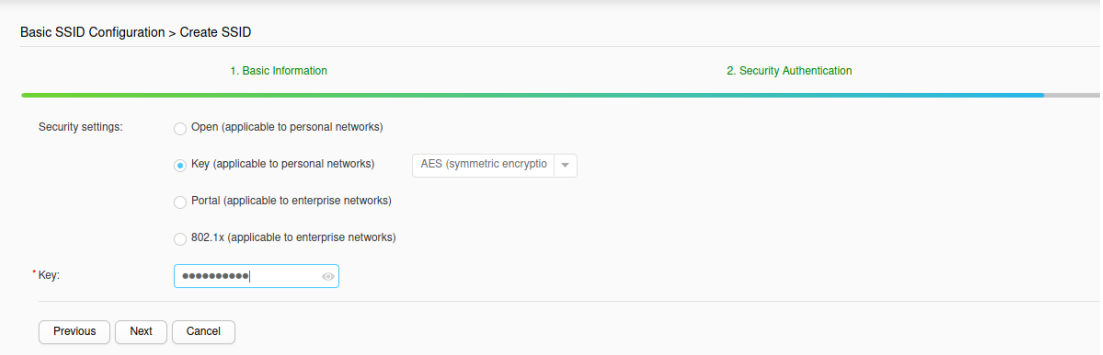


Ilustración 22: Configuración de seguridad del Punto de Acceso

bb) Hacer clic en "*Next*".

cc) Enlazar el grupo de Punto de Acceso que se haya configurado. En este caso se usará el grupo "*default*". Seleccionar la tasa de *uplink* y *downlink*.

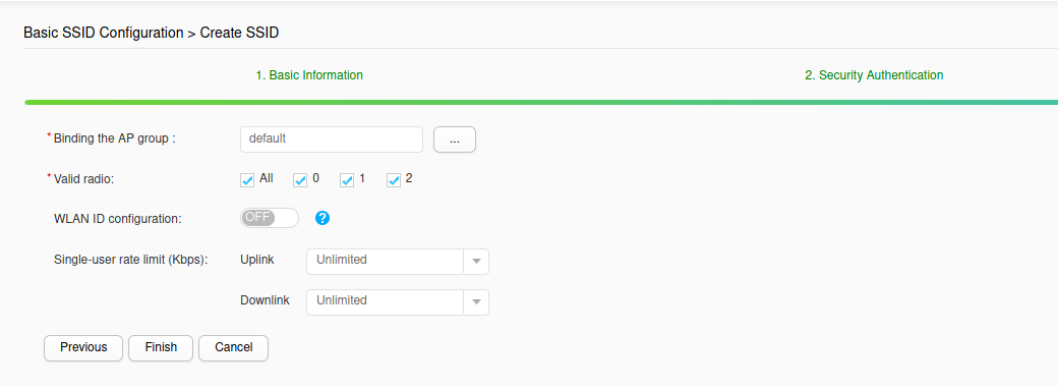


Ilustración 23: Enlace del grupo al Punto de Acceso y selección de radio y tasa de transferencia en el Punto de Acceso

dd) Hacer clic en "*Finish*". En este punto, tanto el Punto de Acceso como el Controlador de Acceso están instalados.

ee) En caso de no contar con el parche instalado, se deberá instalar. Para ello, el parche se deberá transferir al Controlador de Acceso mediante SFTP. La

instalación del parche se debe hacer después de que el Punto de Acceso esté enlazado al Controlador de Acceso, ya que de otra manera no es posible realizar la instalación del parche.

ff) El parche se instalará en los Puntos de Acceso que se especifiquen. Para instalarlo en un Punto de Acceso concreto se deberán ejecutar los siguientes comandos por la CLI del Controlador de Acceso.

$ system-view

$ wlan

$ ap-patch update load ap-mac <MAC-AP> update-filename <Archivo_Parche>

gg) En caso de que se quiera instalar el parche para varios Puntos de Acceso a la vez, podrá hacerse especificando el grupo ejecutando los siguientes comandos en la CLI del Controlador de Acceso.

$ system-view

$ wlan

$ ap-patch update multi-load ap-group <Grupo_AP> update-filename <Archivo_Parche>

31. Para actualizar los Puntos de Acceso en función de otras características como su tipo o su MAC, se puede consultar la sección "*Configuration*" → "*CLI-based Configuration*" → "*AP Management Configuration Guide*" → "*Performing an In-Service Upgrade and Patch Loading for APs*".

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

32. La configuración necesaria para que el producto opere de forma segura consiste en **aplicar una configuración segura de varias políticas a través de la interfaz de línea de comandos**. Esta interfaz es accesible a través del puerto SERIAL o a través de SSH por el puerto ETH de gestión.

33. Para acceder a la interfaz de línea de comandos y autenticarse:

    $ system-view

34. Para la protección de las comunicaciones entre el Controlador y los Puntos de Acceso, se debe habilitar el cifrado de las comunicaciones CAPWAP mediante DTLS:

    $ capwap dtls control-link encrypt

    $ capwap dtls data-link encrypt

35. Para la protección de las comunicaciones de gestión remota, se deben establecer los algoritmos seguros de intercambio de claves del servidor y cliente SSH y establecer los intervalos de regeneración de claves para el servidor SSH:

    $ ssh server key-exchange dh_group16_sha512

    $ ssh client key-exchange dh_group16-sha512

36. Para establecer los intervalos de *rekey* para el servidor SSH:

    $ ssh server rekey time <Minutos>

37. Para habilitar la primera autenticación en el cliente SSH

    $ ssh client first-time enable

5.2 AUTENTICACIÓN

38. Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario son los siguientes:

    - **Credenciales locales**, mediante usuario y contraseña de acceso. La gestión de usuarios locales se puede consultar en el apartado 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES.
    - Autenticación mediante servidor externo **RADIUS**, ver apartado 5.7 SERVIDORES DE AUTENTICACIÓN.
    - **Clave RSA** para autenticación del servicio SSH , ver apartado 5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA, párrafo 45.

39. Los mecanismos de autenticación que utiliza el producto para autenticar a otros sistemas o dispositivos son los siguientes:

- **Certificado TLS** para comunicarse con el servidor ***syslog* externo** y con el **Punto de Acceso**, ver apartado 5.6 GESTIÓN DE CERTIFICADOS.
- Clave pre-compartida para las comunicaciones con un servidor NTP externo. Su configuración se indica en el apartado 5.8 SINCRONIZACIÓN HORARIA.
- Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto. Su configuración se indica en el apartado 5.7 SERVIDORES DE AUTENTICACIÓN.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

40. La administración local del producto siempre se realiza a través de la interfaz *serial* del Controlador de Acceso, para ello es necesario conectarse al puerto serie del producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con la contraseña de usuario *admin* establecida en la fase de instalación en la sección *4.5* INSTALACIÓN, o hacer uso de un usuario con permisos de administración (ver apartado 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES).
41. La administración remota del Controlador de Acceso se realiza a través de SSH. Para ello, es necesario conectarse al producto con un cable de Ethernet en una interfaz física habilitada para tal propósito. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con las credenciales de un usuario autorizado por SSH al Controlador de Acceso.
42. La administración remota del Punto de Acceso se realizará, en la mayoría de los casos, a través del Controlador de Acceso, al cual se accede mediante SSH, como se indica en el punto anterior. El Punto de Acceso cuenta con una interfaz SSH y es posible conectarse a ella con las credenciales establecidas a través del Controlador de Acceso. Sin embargo, no es recomendable ya que prácticamente la totalidad de su funcionalidad es gestionada a través del Controlador de Acceso.
43. **No se recomienda usar la interfaz HTTPS del Controlador de Acceso para la gestión del producto, sino que será usada únicamente para la fase de instalación para facilitar el proceso**. En su lugar, se usará interfaz de línea de comandos, bien sea localmente mediante el puerto serie o remotamente mediante la interfaz SSH. Para deshabilitar la interfaz web, se deben ejecutar los siguientes comandos:

    $ system-view

    $ undo http server enable

44. Para definir el tipo de acceso de cada usuario, se deben seguir los siguientes pasos:

    - Acceder a la interfaz de línea de comandos del producto con un usuario con "*user privilege*" 15 y acceder a la vista *aaa*:

      $ system-view

$ aaa

- Ejecutar el siguiente comando para definir el tipo de acceso:

  $ local-user <user-name> service-type <ssh/terminal>

45. En caso de usar el servicio SSH, **se recomienda el uso de clave pública/privada** para la autenticación en lugar de contraseña. Es posible crear las siguientes claves, pero se recomienda el uso de claves ECC:

    - **RSA** (se debe utilizar una longitud de **clave siempre igual o superior a 3072**):

      $ system-view

      $ ssh user <Usuario> authentication-type <rsa>

      $ rsa peer-public-key <nombre_clave> enconding-type { der | openssh | pem }

      $ public-key-code begin

      $ <pegar_clave_pública>

      $ public-key-code end

      $ peer-public-key end

    - **ECC** (se debe utilizar una longitud de **clave siempre igual o superior a 256**):

      $ system-view

      $ ssh user <usuario> authentication-type <ecc>

      $ ecc peer-public-key <nombre_clave> enconding-type { der | openssh | pem }

      $ public-key-code begin

      $ <pegar_clave_pública>

      $ public-key-code end

      $ peer-public-key end

46. Es necesario enlazar la clave pública importada, bien sea ECC o RSA, al usuario en cuestión que vaya a usarla. Para ello se debe ejecutar:

    $ ssh user <Usuario> assign { rsa-key | ecc-key } <Nombre_Clave>

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

47. El producto no define roles de administración, sino que asocia un número entero entre 1 y 15 a cada usuario, denominado "*user privilege*", que corresponde al nivel de permisos del usuario. En la siguiente tabla se muestran los *user privileges* y los permisos que representan.

"User Privilege"	Permisos	Descripción

0	Visitante	Comandos de diagnóstico, como los comandos ping y *tracert*.
1	Seguimiento	Comandos de mantenimiento del sistema, como los comandos de *display*. No obstante, los comandos de *display* respecto a la configuración actual o la configuración guardada solo están disponible en niveles de "*user privilege*" de 3 o más.
2	Configuración	Comandos de configuración de los servicios.
3-15	Administración	Comandos de operación básica del sistema que se utilizan para dar soporte a los servicios, incluyendo el sistema de archivos, SFTP, comandos de gestión de usuarios, comandos de configuración a nivel de comandos y comandos de depuración.

Tabla 1: Permisos de usuario

48. No se recomienda modificar los niveles de acceso necesarios para acceder a los distintos comandos. Sin embargo, en caso de ser necesario, se pueden modificar los permisos necesarios para poder acceder a un comando mediante el comando *command-privilege level <nivel> view <vista> <comando>*.

49. Para crear un usuario se deben ejecutar los siguientes comandos:

    $ local-user <Nombre_Usuario> password irreversible-cipher <contraseña>

50. Por defecto, un usuario recién creado tiene un privilegio de nivel 0. Para asignar un nivel específico de "*user privilege*" a un usuario:

    - Acceder a la interfaz de línea de comandos del producto con un usuario con "*user privilege*" 3-15 y acceder a la vista *aaa*:

      $ system-view

      $ aaa

    - Luego, se puede asignar a un usuario un nivel de 0 a 15 de privilegios:

      $ local-user <Nombre_Usuario> privilege level <Nivel>

51. Por defecto, la política de contraseñas consiste en un valor entre 8 y 128 caracteres que debe contener, al menos, una combinación de un número, un símbolo, una mayúscula o una minúscula. El usuario administrador puede modificar los siguientes parámetros:

    - Longitud: La longitud de la contraseña mínima es 8, aunque se puede ampliar hasta a 16. **Se recomienda un valor mínimo de 12 caracteres.**

      $ system-view

      $ set password min-length <Longitud>

- Complejidad: Se puede ampliar la complejidad de la contraseña de forma que se exija la combinación de tres de los elementos mencionados anteriormente:

  $ system-view

  $ aaa

  $ user-password complexity-check three-of-kinds

- Historial: Se puede ajustar el historial de contraseñas de forma que no se puedan establecer de nuevo contraseñas que ya se hubieran establecido antes. **Se recomienda un valor de, al menos, 5 contraseñas.**

  $ system-view

  $ aaa

  $ local-aaa-user password policy administrator

  $ password history record number 5

  $ local-aaa-user password policy access-user

  $ password history record number 5

52. El usuario administrador puede establecer las políticas seguras de sesión como:

    - Tiempo de inactividad para SSH, **se recomienda un valor de 5 minutos** (300 segundos):

      $ system-view

      $ ssh server timeout <Tiempo_Segundos>

    - Tiempo de inactividad para la interfaz serie, **se recomienda un valor de 5 minutos.**

      $ system-view

      $ user-interface console 0

      $ idle-timeout <Tiempo_Minutos> <Tiempo_Segundos>

    - Número de intentos fallidos de autenticación (*retry-time*) y tiempo de espera al superar el umbral (*retry-interval*). **Se recomienda configurar un máximo de 3 intentos fallidos y un bloqueo de 5 minutos.**

      $ system-view

      $ local-aaa-user wrong-password retry-interval retry-time

53. Se debe también configurar un mensaje de aviso y consentimiento en el inicio de sesión.

    $ system-view

    $ header shell information &<Texto>&

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

54. Configurar una ACL en la interfaz VTY del Controlador de Acceso, de forma que solo se permita gestionar el dispositivo desde una IP en concreto.

    $ system-view

    $ acl number 3001

    $ rule 5 permit ip source <IP_Gestion> <Máscara>

    $ rule 10 deny ip

    $ user-interface vty 0

    $ acl 3001 inbound

55. Configurar el servicio SSH para que **solo se pueda usar desde la interfaz de gestión**.

    $ ssh server permit interface meth 0/0/1

56. Crear ACLs para que **solo** se permita la salida de tráfico SSH por la interfaz de gestión.

    $ acl number 3002

    $ rule 5 permit tcp source <IP_Interfaz_Gestión> < Máscara > destination <Red_Gestión> < Máscara > source-port eq 22

    $ rule 10 deny ip

    $ interface meth 0/0/1

    $ traffic-filter outbound acl 3002

    $ traffic-filter inbound acl 3001

57. El resto de interfaces que no se usen **deben ser deshabilitadas**.

    $ system-view

    $ interface GigabitEthernet 0/0/1

    $ shutdown

    $ quit

    $ interface GigabitEthernet 0/0/2

    $ shutdown

    $ quit

    . . .

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

58. El Controlador de Acceso utiliza SSH para la administración remota, TLS como cliente para la transmisión de auditoría a un servidor externo y DTLS para la gestión de los Puntos de Acceso.

59. El producto usa *suites* de cifrado TLS 1.2 para el cifrado del cliente TLS a la hora de enviar auditoría (*ECDHE_RSA_AES128_GCM_SHA256* y *ECDHE_RSA_AES256_GCM_SHA384*). Se recomienda mantener dichas *suites* de cifrado.

60. En el caso del protocolo SSH para la gestión del Controlador de Acceso, para que las suites criptográficas sean conformes a la guía [CCN-STIC-807], se debe configurar el Controlador de Acceso para que se permitan únicamente algoritmos de intercambio de claves superiores a *group15*. Para ello basta con ejecutar en el Controlador de Acceso:

    $ system-view

    $ ssh server key-exchange dh_group16_sha512

61. Tras la configuración, las suites criptográficas de los diferentes servicios se pueden observar en la tabla.

Tipo	Descripción suite de cifrado
SSH	Establecimiento de clave: *dh_group16_sha512* Firma criptográfica: *ecdsa-sha2-nistp256* Algoritmo de cifrado: *AES256_CTR, AES128_CTR* Autenticación de mensajes: *HMAC-SHA2-256*
Cliente TLS (AC)	Suite de Cifrado: *ECDHE_RSA_AES128_GCM_SHA256* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado y autenticación: AES 128 GCM Integridad de mensajes: SHA256 Suite de Cifrado: *ECDHE_RSA_AES256_GCM_SHA384* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado y autenticación: AES 256 GCM Integridad de mensajes: SHA384
Servidor DTLS (AC)	Suite de Cifrado: *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado y autenticación: AES 256 GCM

	Integridad de mensajes: SHA384
Cliente DTLS (AP)	Suite de Cifrado: *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado y autenticación: AES 256 GCM Integridad de mensajes: SHA384 Suite de Cifrado: *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado y autenticación: AES 128 GCM Integridad de mensajes: SHA256 Suite de Cifrado: *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA* Establecimiento de clave: *Elliptic Curve Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado: AES 256 CBC Integridad y autenticación de mensajes: HMAC-SHA1 Suite de Cifrado: *TLS_RSA_WITH_AES_128_CBC_SHA* Establecimiento de clave: RSA Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 128 CBC Integridad y autenticación de mensajes: HMAC-SHA1 Suite de Cifrado: *TLS_RSA_WITH_AES_256_CBC_SHA* Establecimiento de clave: RSA Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 256 CBC Integridad y autenticación de mensajes: HMAC-SHA1 Suite de Cifrado: *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*

	Establecimiento de clave: *Diffie-Hellman Ephemeral* Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 128 CBC Integridad y autenticación de mensajes: HMAC-SHA1 Suite de Cifrado: *TLS_DHE_RSA_WITH_AES_256_CBC_SHA* Establecimiento de clave: *Diffie-Hellman Ephemeral* Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 256 CBC Integridad y autenticación de mensajes: HMAC-SHA1 Suite de Cifrado: *TLS_RSA_WITH_AES_128_CBC_SHA256* Establecimiento de clave: RSA Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 128 CBC Integridad y autenticación de mensajes: HMAC-SHA256 Suite de Cifrado: *TLS_RSA_WITH_AES_256_CBC_SHA256* Establecimiento de clave: RSA Firma criptográfica: RSA-SHA Algoritmo de cifrado: AES 256 CBC Integridad y autenticación de mensajes: HMAC-SHA256

Tabla 2: Suites criptográficas de los servicios del producto

5.6 GESTIÓN DE CERTIFICADOS

62. El Controlador de Acceso permite importar certificados de CA, lo cual es necesario para verificar el certificado del servidor TLS externo encargado de recibir auditoría del Controlador de Acceso y del Punto de Acceso. Para ello es necesario crear un *realm* e importar la CA en dicho *realm*. Un *realm* es un identificador en el cual es posible inscribir certificados, tanto CA, como intermedios como finales. El fichero de la CA se deberá subir en formato PEM al Controlador de Acceso mediante SFTP.

    $ system-view

    $ pki realm <Nombre_Realm>

$ pki import-certificate ca realm <Nombre_Realm> pem filename <Certificado_PEM>

63. También es posible importar certificados intermediarios y certificados finales.

    $ system-view

    $ pki realm <Nombre_Realm>

    $ quit

    $ pki import-certificate local realm <Nombre_Realm> pem filename <Certificado_PEM>

64. El producto verifica que los certificados son válidos comprobando sus *flags*, su vigencia o incluso su existencia en una CRL. Dicha CRL es subida al dispositivo mediante SFTP e importada en un *realm*.

    $ system-view

    $ pki realm <Nombre_Realm>

    $ quit

    $ pki import-crl realm test filename <Archivo_CRL>

65. El *realm* creado anteriormente puede ser enlazado a una política SSL, de forma que el certificado CA importado sea usado posteriormente para autenticar el servidor *syslog* remoto. Para ello, se deben ejecutar los siguientes comandos:

    $ system-view

    $ ssl policy <Politica_SSL> type client

    $ pki realm <Nombre_Realm>

66. Es posible verificar el *Common Name*, la firma y la vigencia del certificado del servidor TLS al que se le envía auditoría:

    $ system-view

    $ info-center loghost <IP_Servidor> port <Puerto_Servidor> channel <Canal> transport tcp ssl-policy <Politica_SSL> verify-dns-name <Common_Name>

5.7 SERVIDORES DE AUTENTICACIÓN

67. Para realizar la configuración de RADIUS se debe crear un *authorization-scheme*, un *accoutning-scheme* y una *RADIUS template*. A continuación, se detallan los pasos para crear los dos (2) primeros:

    $ system-view

    $ aaa

    $ authentication-scheme radius

    $ authentication-mode radius

    $ quit

$ accounting-scheme radius

$ quit

68. Se debe configurar la función de bloqueo de cuentas fallidas ante los fallos de inicio de sesión para RADIUS.

    $ access-user remote authen-fail retry-interval <tiempo_espera> retry-time <numero_intentos>

69. Es posible desbloquear manualmente una cuenta de usuario con el comando:

    remote-user authen-fail unblock <nombre_usuario>.

70. Para configurar también el *Accounting* mediante RADIUS, ejecutar el comando aaa seguido de *accounting-scheme radius*.

71. Además, se debe configurar una RADIUS temkplate para especificar cuál será la dirección IP del servidor RADIUS y la clave compartida del mismo. Para ello, se deben ejecutar los siguientes comandos:

    $ system-view

    $ radius-server template <Nombre_Template>

    $ radius-server authentication <Direccion_RADIUS> <Puerto_RADIUS>

    $ radius-server accounting <Direccion_RADIUS> <Puerto_RADIUS>

    $ radius-server shared-key cipher <contraseña>

72. Para finalizar la configuración de RADIUS es necesario asignar el *authentication-scheme, accounting-scheme* y *radius-template* a un *authentication-profile*. Para ello se debe crear y asignar ejecutando los siguientes comandos:

    $ system-view

    $ authentication-profile name <Nombre_Perfil>

    $ authentication-scheme radius

    $ accounting-scheme radius

    $ radius-server <Nombre_Template>

73. El detalle de configuración de RADIUS se puede consultar en el apartado *Configuration → CLI-based configuration → User Access and authentication configuration guide → AAA configuration → Configuring local authentication and authorization → using RADIUS to perform Authentication, Authorization and Accounting*, de la guía [REF1].

5.8 SINCRONIZACIÓN HORARIA

74. El Controlador de Acceso permite el uso de NTP para la sincronización horaria. El Punto de Acceso siempre sincronizará su tiempo al valor del Controlador de Acceso (siempre y cuando se hayan emparejado previamente).

75. En lugar de establecer el tiempo manualmente, **se recomienda el uso de un servidor NTP para la sincronización horaria.** Se deben ejecutar las siguientes instrucciones en el Controlador de Acceso para establecer un servidor externo NTP:

    $ system-view

    $ ntp-service unicast-server <IP_NTP> version <número_versión>

76. Por defecto, se utiliza a versión 3 del protocolo NTP, la cual es considerada segura. **Se debe hacer uso de la versión 3 o la 4.**

77. Es posible autenticar la conexión estableciendo una clave predefinida entre el servidor NTP y el Controlador de Acceso, se debe hacer uso de HMAC-SHA-256. Para ello, una vez configurada la clave en el servidor NTP, se deben ejecutar las siguientes instrucciones en el producto;

    $ system-view

    $ ntp-service authentication enable

    $ ntp-service authentication-keyid <ID_Clave> authentication-mode hmac-sha256 cipher <Clave>

    $ ntp-service reliable authentication-keyid <ID_clave>

5.9 ACTUALIZACIONES

78. Tanto el Controlador de Acceso, como el Punto de Acceso, contemplan dos (2) tipos de actualizaciones:

    - **Parches**: Actúan sobre una versión del *software* del sistema. El producto comprueba la validez del parche antes de cargarlo en el sistema. Su extensión es (.pat).
    - ***Software/firmware* del sistema**: Se puede definir como el sistema operativo del producto. Al igual que los paquetes de parches, el producto comprueba la validez e integridad del *software* del sistema. Su extensión es (.cc).

79. Ambos tipos de actualizaciones puede descargarse de la web oficial de Huawei (*https://support.huawei.com*) y deben de subirse al directorio raíz del Controlador de Acceso mediante SFTP.

80. Para realizar la descarga, seleccionar el *firmware* o parche deseado desde la página de descargas, se mostrará la siguiente información:

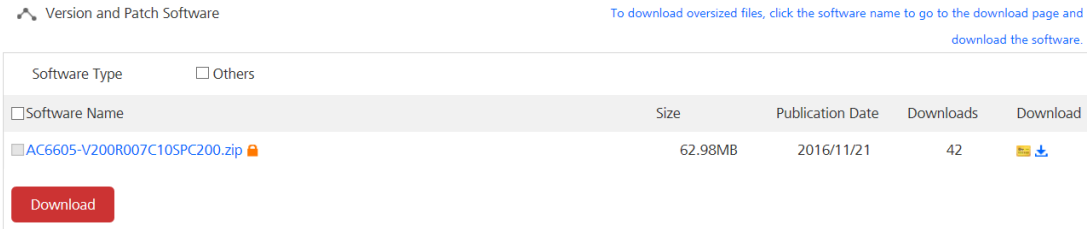


Ilustración 24. Descarga de actualizaciones

81. Desde dicha página, se puede obtener el fichero de firma del *software*, con la extensión *asc*, para verificar la autenticidad de la descarga. Esta firma se puede obtener haciendo clic sobre el icono  , el cual se muestra bajo el apartado *Download*.
82. Se debe verificar dicha firma haciendo uso de PGP. Se puede descargar *PGPVerify* desde la página de herramientas de Huawei. La clave pública se encuentra en el mismo paquete de instalación que la herramienta.
83. Para realizar la verificación se deben seguir los siguientes pasos:
    - Ejecutar el siguiente comando:

      $ "C:\PGPVerify.exe" –k "C:\KEYS" –f "C:\PGP\<software.zip.asc>
    - Se mostrará el siguiente mensaje por pantalla:

      [PASS]:Good Signature. File path: C:\PGP\<software.zip.asc>, Public key fingerprint: B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824

      [INFO]: Verify Complete.
    - Se deberá obtener el resultado "*Good Signature*".
84. Para establecer un parche en el Controlador de Acceso es necesario ejecutar la siguiente instrucción:

    $ startup patch <Parche>
85. Para instalar un *firmware* en el Controlador de Acceso es necesario ejecutar la siguiente instrucción:

    $ startup system-software <Firmware>
86. En el caso de que se quiera instalar un parche en el Punto de Acceso, es necesario subir el archivo al directorio raíz del Controlador de Acceso y ejecutar en el mismo las siguientes órdenes:

    $ system-view

    $ wlan

    $ ap-patch update load ap-name <Nombre_AP> update-filename <Parche>
87. En el caso de querer establecer un *firmware* nuevo en el Punto de Acceso, también es necesario hacerlo desde el Controlador de Acceso, como en el caso anterior. Se debe subir el archivo al Controlador de Acceso y ejecutar:

    $ system-view

    $ wlan

    $ ap update load ap-name <Nombre_AP> update-filename <Firmware>
88. Para listar el *firmware* del sistema y el paquete de parches configurados en el producto se debe ejecutar la siguiente instrucción en el Controlador de Acceso:

    $ display startup

89. Para listar el *firmware* de los puntos de acceso debe ejecutar la siguiente instrucción en el Controlador de Acceso:

    $ display ap version all

5.10 AUTO-CHEQUEOS

90. Cuando el producto se enciende o se reinicia, realiza los siguientes autochequeos:
    - Autochequeo de la integridad del *software* del sistema.
    - Autochequeo de los algoritmos de cifrado.
91. En caso de fallar algún chequeo, el sistema no finalizará el arranque y se reiniciará.

5.11 SNMP

92. El Punto de Acceso y el Controlador de Acceso son capaces de usar SNMP para transmitir información a servidores NMS o a *software* del fabricante como *iMaster NCE-CampusInsigh*t. El detalle de configuración de los diferentes servicios SNMP se puede consultar en la sección "*Configuration*" → *"CLI-based Configuration"* → "*Network Management and Monitoring Configuration Guide*" → "*Configuring SNMP*" → "*Configuring Basic SNMPv3 Functions*" de la guía [REF1].
93. **Se debe usar exclusivamente SNMPv3**, ya que las versiones anteriores del protocolo se consideran inseguras.

5.12 ALTA DISPONIBILIDAD

94. El producto cuenta con la funcionalidad VRRP HSB, la cual permite que los Puntos de Acceso no pierdan conectividad en caso de que el Controlador de Acceso o los enlaces entre ellos se caigan.

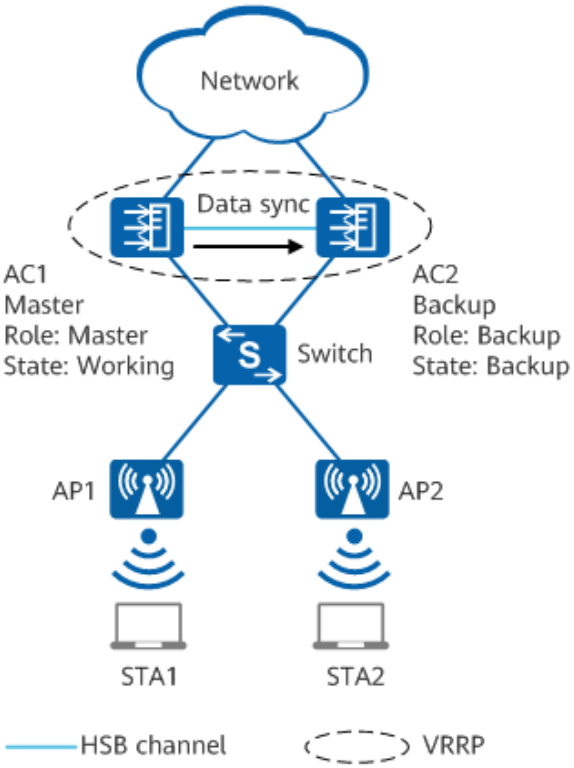


Ilustración 25: Escenario VRRP HSB

95. Como se puede observar en la imagen, el AC1 actúa como maestro, de forma que el AC2 se dedica a realizar copias de seguridad de la configuración del AC1.

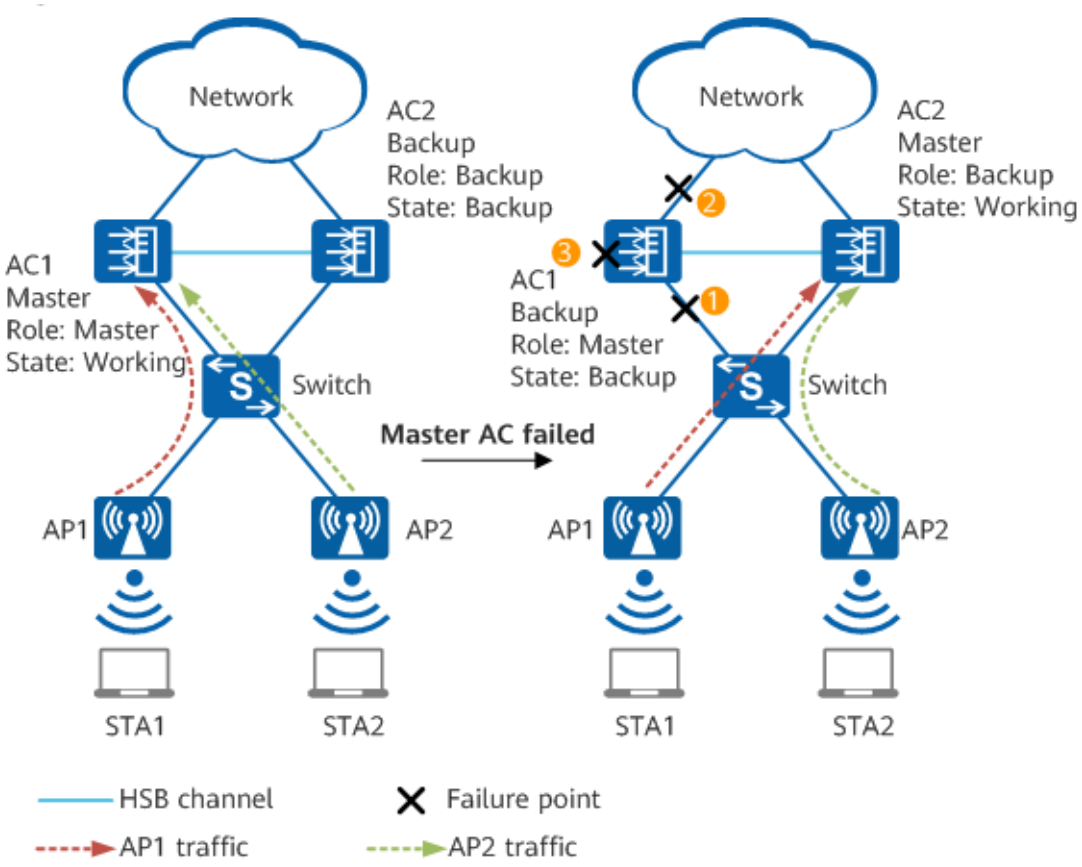


Ilustración 26: Escenario VRRB HSB en caso de que el AC maestro falle

96. Como se puede observar en la imagen, al producirse un error en AC1, en el switch o en el enlace a la red, la conexión se deriva a AC2 y por tanto los APs no pierden conexión.

97. El detalle de configuración del servicio VRRP HSB se puede consultar en la sección "*Configuration*" → *"CLI-based Configuration"* → "Reliability Configuration Guide" → *"AC Backup Configuration"* → *"VRRP HSB Configuration"* → *"Configuring an HSB Service"* de la guía [REF1].

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

98. El producto almacena los siguientes eventos de seguridad en sus registros de auditoría:

    - *Login* y *logout* de usuarios tanto del Punto de Acceso como del Controlador de Acceso.
    - Inicio de las acciones de auditoría.
    - Cambios en la configuración del producto.
    - Comandos ejecutados vía CLI.

- Fallos al intentar establecer una sesión SSH
- Conexiones 802.1X y la identificación del dispositivo/usuario que realiza dicha conexión.
- Cambios en el tiempo del Controlador de Acceso.
- Inicio y terminación de las sesiones locales.
- Conexiones inalámbricas en los Puntos de Acceso.

99. El producto guarda la siguiente información de los eventos:

Campo	Descripción
Fecha y hora	Fecha y hora en la que se produce el evento.
Tipo de evento	Clase de evento que se produce (ej.: *login*, reseteo de clave…).
Fuente del evento	Interfaz desde la que se produce el evento (ej.: SSH, Serial, Web…)
Sujeto que produce el evento	Usuario y/o IP (si corresponde).
Resultado	Resultado del evento, si aplica.

Tabla 3: Información que se guarda en los registros de auditoría

100. Es posible configurar el mínimo nivel de gravedad de los logs, de manera que solo se registrarían aquellos que superen el valor mínimo establecido. Hay tres (3) tipos de logs: *log, trap* y *debug*, los cuales a su vez tienen 8 niveles de gravedad:

- *Emergencies*
- *Alert*
- *Critical*
- *Error*
- *Warning*
- *Notification*
- *Informational*
- *Debugging*

101. Para configurar el nivel de gravedad mínimo de un canal y cada tipo de log es necesario ejecutar el siguiente comando:

$ info-center source channel <Canal> log level <nivel_mínimo> trap level <nivel_mínimo> debug level <nivel_mínimo>

102. Se puede consultar esta configuración que más detalle en la guía [REF1] en la sección *Configuration → Device Management Configuration Guide → Information Center Configuration → Configuring Information Center*.

5.13.2 ALMACENAMIENTO LOCAL

103. El producto almacena localmente los registros de auditoría en el directorio *logfile* (alojado en el directorio raíz). En dicho directorio se puede encontrar el archivo *<Nombre_AC>-log.log*, el cual almacena los logs actuales en texto plano y el archivo *<Nombre_AC>-log.dblg*, el cual almacena los logs actuales en formato binario.

104. En caso de que el archivo *.log o .dblg* sobrepasen un límite de tamaño establecido (8 MB por defecto), son comprimidos y almacenados como archivos con formato ZIP con nombre *<Nombre_AC>-<Fecha>.<Hora>.log.zip* o *<Nombre_AC>-<Fecha>.<Hora>.dblg.zip*, a la vez que los archivos *.log* y *.dblg* se quedan vacíos.

105. En caso de que se alcance el espacio de almacenamiento máximo, se borrarán archivos con formato ZIP antiguos. Es por esto que se recomienda realizar la configuración de un servidor de auditoría externo, tal como se indica a continuación.

5.13.3 ALMACENAMIENTO REMOTO

106. El Controlador de Acceso se puede configurar para enviar sus registros de auditoría a un servidor *syslog* externo**. Se debe configurar la comunicación con dicho servidor para el uso de TLS 1.2**, cifrando toda comunicación, tal como se ve a continuación.

107. Es recomendable generar certificados propios y subir la CA al Controlador de Acceso. De esta manera se puede importar la CA como se indica en el punto 5.6 GESTIÓN DE CERTIFICADOS y validar la firma del certificado TLS cuando se establezca la conexión. Para ello, se debe crear una política SSL en la cual se añada el *realm* en el que se ha importado la CA.

$ system-view

$ ssl policy <Nombre_Política-SSL> type client

$ pki-realm <Nombre_Realm>

108. Una vez creada la política, se debe crear un canal que recoja todos los eventos posibles que se produzcan en el dispositivo. Para ello, se debe ejecutar los siguientes comandos:

$ system-view

$ info-center channel 6 name <Nombre_Canal>

$ info-center source default channel <Nombre_Canal> log level debugging trap level debugging debug level debugging

109. Por último, se debe configurar el Controlador de Acceso para transmitir los logs al servidor *Syslog* mediante TLS. Por defecto, el producto siempre usará TLSv1.2.

$ info-center loghost <IP_Servidor_Syslog> channel <Nombre-Canal> port <Puerto_Servidor_Syslog> transport tcp ssl-policy <Nombre_Política_SSL> verify-dns-name <Dominio_Servidor_Syslog>

110. A su vez, si se desea mayor control sobre la información de auditoría del Punto de Acceso, es posible configurarlo para que transmita información con mayor detalle al software propietario del fabricante *iMaster NCE-CampusInsight*.

    Para ello, debe acceder al Controlador de Acceso y ejecutar:

    $ system-view

    $ mgmt isolate disable

    $ snmp-agent sys-info version v3

    $ snmp-agent mib-view iso-view include iso

    $ snmp-agent group v3 snmpv3group privacy write-view iso-view notify-view iso-view

    $ snmp-agent usm-user version v3 snmpv3user group snmpv3group

111. Debe establecer una contraseña de autenticación y cifrado, preferentemente diferentes entre sí, ejecutando las siguientes órdenes:

    $ snmp-agent usm-user version v3 snmpv3user authentication-mode sha

    $ snmp-agent usm-user version v3 snmpv3user privacy-mode aes128

112. Por último, habilitar el envío de logs al servidor externo ejecutando:

    $ wlan

    $ wmi-server name insight

    $ server ip-address <IP_NCE> port <Puerto_NCE>

    $ ap log module mid FF2B0000

    $ ap log module mid FF040000

    $ ap log module mid FF600000 name PORTAL

    $ ap log module mid D0410000 name SHELL

    $ ap log module mid FF620000 name DHCP

    $ ap log module mid FFED0000 name SEA

    $ ap log module mid FFEF0000 name WSRV

    $ ap log module mid FFF30000 name WLAN

    $ quit

    $ ap-system-profile name default

    $ wmi-server insight index 1

    $ quit

113. El Punto de Acceso ya estaría configurado para transmitir toda su información al servidor *iMaster NCE-CampusInsight*. A su vez, el servidor debe ser configurado

para recibir la información transmitida. Dicha configuración se puede consultar en la guía [REF2].

5.14 *BACKUP*

114. El producto almacena la configuración inicial (vacía) en el fichero "*vrpcfg.zip*", que se encuentra en el directorio raíz. Para guardar la configuración actual del producto (políticas implementadas, interfaces creadas, configuraciones de seguridad…) en el fichero "*config.cfg*" se debe de ejecutar el siguiente comando:

$ save all

115. No obstante, se recomienda **guardar la configuración del producto de forma automática cada cierto periodo de tiempo**. Esto se consigue mediante las siguientes instrucciones:

$ autosave interval on

$ autosave interval <Minutos>

116. El archivo de configuración **debe almacenarse en un dispositivo diferente del producto**, a través de una descarga manual por medio de SFTP. Para ello, se debe habilitar el servidor SFTP en el Controlador de Acceso mediante el comando *sftp server enable*. Después, descargar desde el producto al dispositivo que almacenará la copia de la configuración. Una vez conectado mediante SFTP, para descargar el archivo de configuración, basta con ejecutar:

$ get vrpcfg.zip

5.15 SERVICIOS DE SEGURIDAD

117. **Se debe configurar el bloqueo de paquetes malformados o fragmentados**: *SYN flood, UDP flood* y *ICMP flood*.

$ system-view

$ anti-attack abnormal enable

$ anti-attack fragment enable

$ anti-attack tcp-syn enable

$ anti-attack udp-flood enable

$ anti-attack icmp-flood enable

118. El Controlador de Acceso permite evitar ataques de *ARP spoofing,* a través del establecimiento de un ratio máximo de paquetes ARP por dirección MAC o por interfaz, entre otros. Se recomienda ejecutar las siguientes instrucciones:

$ system-view

$ cpu-defend policy antiatk

$ auto-defend enable

$ auto-defend threshold 30

$ undo auto-defend trace-type source-portvlan

$ undo auto-defend protocol tcp telnet ttl-expired igmp icmp dhcpv6 mld nd

$ auto-defend action deny timer 300

119. También se pueden **evitar ataques de tipo *ARP flood*** limitando el número de entradas ARP que el Controlador de Acceso puede aprender:

$ system-view

$ interface vlan <Vlan_ID>

$ arp-limit maximum 20

$ quit

$ arp speed-limit source-ip maximum 50

120. De la misma forma, existe la posibilidad de defenderse de ataques de tipo *DHCP Flood* limitando el número de paquetes DHCP que llegan al Control de Acceso por un puerto en concreto:

$ system-view

$ dhcp enable

$ dhcp snooping enable

$ interface gigabitethernet 0/0/<Numero_Interfaz>

$ dhcp snooping enable

$ dhcp snooping check dhcp-rate enable

$ dhcp snooping check dhcp-rate 30

121. Se debe configurar el Controlador de Acceso **para habilitar la protección *DHCP snooping*** de forma que se filtren posibles servidores DHCP que intenten suplantar al original.

$ system-view

$ dhcp enable

$ dhcp snooping enable

$ interface gigabitethernet 0/0/<Numero_Interfaz>

$ dhcp snooping enable

$ dhcp snooping trusted

122. **Se debe configurar el Controlador de Acceso para que detecte posibles Puntos de Acceso o Clientes Wireless maliciosos**. Para ello debe ejecutar:

$ system-view

$ wlan

$ ap-group name <Nombre_Grupo_AP>

$ radio 0

$ work-mode normal

$ wids device detect enable

$ wids contain enable

$ quit

$ wids-profile name wlan-wids

$ contain-mode open-ap

$ contain-mode spoof-ssid-ap

$ contain-mode client

$ contain-mode adhoc

$ quit

$ ap-group name <Nombre_Grupo_AP>

$ wids-profile wlan-wids

123. Ya que se permite gran flexibilidad a la hora de configurar el servicio, es posible consultar una configuración más detallada en la sección "*Configuration*" → "*Security Hardening Guide and Security Maintenance*" → "*(Optional) Level-2 Security Hardening Policies*" → "*Control Plane*" → "*Wireless Attack Detection and Containment"* de la guía [REF1]

124. **Se deben crear listas blancas de URLs de forma que se limiten los sitios web** a los que los usuarios *Wireless* puedan acceder. Ya que la flexibilidad de las posibles configuraciones es notable, se puede consultar un ejemplo de bloqueo en la sección "*Configuration*" → "*Security Hardening Guide and Security Maintenance*" → "*(Optional) Level-2 Security Hardening Policies*" → "*Control Plane*" → "*URL filtering*" de la guía [REF1].

125. **Se debe configurar la funcionalidad de antivirus**, de forma que se bloqueen posibles virus que se descarguen o suban a través de los Puntos de Acceso. Para activar el sistema basta con ejecutar:

$ system-view

$ defence engine enable

126. Sin embargo, es necesario aplicar la configuración del sistema para el filtrado del tráfico según el protocolo o el sentido de la comunicación. Una configuración más detallada se puede observar en la sección sección "*Configuration*" → "*Security Hardening Guide and Security Maintenance*" → "*(Optional) Level-2 Security Hardening Policies*" → "*Control Plane*" → "*Antivirus*" de la guía [REF1].

6. FASE DE OPERACIÓN

127. Durante la fase de operación del producto, los administradores de seguridad deberán llevar a cabo, al menos, las siguientes tareas de mantenimiento:

- Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado. El *firmware* activo y su integridad deberán verificarse periódicamente para comprobar que está libre de *software* malicioso.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura.
- Realización de *back-ups* periódicos y restauración de estos. Además, de almacenarlos en localizaciones seguras y planificar el proceso de automatización.
- Mantenimiento de los registros de auditoría por el periodo establecido en la normativa de seguridad. Estos registros estarán protegidos de borrado y modificación no autorizadas. Solamente el personal de seguridad autorizado podrá acceder a ellos.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro y aplicación de licencias	☐	☐	
Instalación segura del producto	☐	☐	
Verificación de la versión del *firmware*	☐	☐	
CONFIGURACIÓN			
CONFIGURACIÓN DEL MODO DE OPERACIÓN SEGURO			
Configuración de comunicaciones seguras	☐	☐	
CONFIGURACIÓN DE AUTENTICACIÓN			
Configuración de autenticación de usuarios	☐	☐	
Creación de claves SSH	☐	☐	
CONFIGURACIÓN DE USUARIOS DE ADMINISTRACIÓN			
Creación de cuentas de usuario	☐	☐	
Creación del usuario administrador	☐	☐	
Configuración de la política de contraseñas	☐	☐	
CONFIGURACIÓN DE LOS PARÁMETROS DE SESIÓN			
Configuración de tiempos de sesión e intentos de *login*	☐	☐	
Configuración del *Login Banner*	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de *cipher suites*	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
CONFIGURACIÓN DE CERTIFICADOS			
Configuración de certificados para *syslog*	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Configuración de servidores externos de autenticación	☐	☐	
CONFIGURACIÓN DE LA SINCRONIZACIÓN HORARIA			
Configuración del servidor NTP con autenticación	☐	☐	
CONFIGURACIÓN DE ACTUALIZACIONES			
Comprobación de las actualizaciones disponibles	☐	☐	
CONFIGURACIÓN DE ALTA DISPONIBILIDAD			
Configuración de alta disponibilidad	☐	☐	
CONFIGURACIÓN DE AUDITORÍA			
Configuración de eventos en el almacenamiento local	☐	☐	
Configuración del envío de eventos al servidor remoto (*syslog*)	☐	☐	
COPIAS DE SEGURIDAD			
Realización del *backup* de configuración	☐	☐	

8. REFERENCIAS

[REF1] *WLAN AC and Fit AP Product Documentation Issue 06*

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100169994&lang=en

Wireless Access Controller (AC and Fit AP) V200R022C00 CLI-based Configuration Guide

[REF2] *iMaster NCE-CampusInsight V100R019C10 Product Documentation*

https://support.huawei.com/enterprise/en/network-management-control-analysis/imaster-nce-campusinsight-pid-250872285?category=product-documentation-sets

9. ABREVIATURAS

AC	*Access Controller* (Controlador de Acceso)
ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AP	*Access Point* (Punto de Acceso)
ARP	*Address Resolution Protocol*
DHCP	*Dynamic Host Configuration Protocol*
ENS	Esquema Nacional de Seguridad
ESN	*Equipment Serial Number*
GE	*Gigabit Ethernet*
HTTPS	*Hypertext Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
PC	*Personal Computer*
RADIUS	*Remote Authentication Dial-In User Service*
RSA	*Rivest, Shamir, & Adleman (public key encryption technology)*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SYN	*Synchronization*
TLS	*Transport Layer Security*
VLAN	*Virtual Large Area Network*
VRRP	*Virtual Router Redundancy Protocol*

PUBLICACIONES DE DEFENSA

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