albentia systems

AerDocsis System Software Software Release Notes

HoneybeeM2 19.6.6353

13 de Diciembre de 2021

albentia systems

Contenidos

1. Dispositivos compatibles y versiones mínimas

Familia	Dispositivos	Versiones mínimas
Estaciones Base		
BS400 y BS800	AXS-BS-450-N AXS-BS-850-N	Honeybee M1 19.6.6172
BS100	AXS-BS-150-N	Honeybee M1 19.6.6172
Terminales de Usuario		
CPE100	AXS-CPE150-15 AXS-CPE150-RS	Honeybee M1 19.6.6172
CPE200 y CPE300	AXS-CPE250-15 AXS-CPE250-RS AXS-CPE350-15 AXS-CPE350-RS	Honeybee M1 19.6.6172
Radioenlaces		
LNK100	LNK-LU1150-N LNK-LU1150-23	Honeybee M1 19.6.6172

2. Novedades en ésta versión

2.1 Nuevas funcionalidades

2.1.2 Comunes a todas las estaciones base

Nuevos atributos RADIUS

Se han añadido dos nuevos atributos de RADIUS Primary-BSID-Allow y Secondary-BSID-Allowed. Estos atributos definen a qué BSIDs se puede conectar el CPE. En caso de que el CPE se conecte a un BSID secundario, la BS desconectará al CPE después de un tiempo configurable y el CPE ejecutará un AFS para intentar conectarse a una BS primaria.

Por otra parte, los atributos de RADIUS Sector-Allowed y Zone-Allowed dejan de estar soportados.

Para más detalle, ver el **Anexo 4.1**.

Remote commands

Se han añadido 4 nuevos remote commands:

- PPPoE test mode. Configura al CPE en modo Routed NAT con PPPoE con el usuario **albtest** y contraseña **albtest**. La IP LAN del CPE se configura en 192.168.0.128/24.
- Bridge test mode. Configura al CPE en modo bridge con IP estática 10.11.12.3/8.
- Enable SMC. Habilita el canal secundario de gestión (SMC) en el CPE en modo DHCP y con IP de *fallback* 176.0.0.1/24. El CPE se reconectará tras recibir este comando para que se aplique la nueva configuración.
- Disable SMC. Deshabilita el canal secundario de gestión (SMC) en el CPE. El CPE se reconectará tras recibir este comando para que se aplique la nueva configuración.

2.2 Mejoras

2.2.1 Comunes a todos los dispositivos

Provisión

La opción de DHCP Injection ahora funciona también en el caso de que el tráfico esté encapsulado sobre VLAN.

Sistema

El fichero de log del *Health Monitor*, el *gather data*, ahora muestra información del dispositivo, tal como su nombre, localización, propietario, dirección MAC y versión de *firmware*.

Monitorización

El sistema ahora monitoriza si las radios están correctemente calibradas. En caso de no estarlo, se muestra una alarma en la web. Si se detecta esta alerta en un equipo, póngase en contacto con el departamento de ingeniería para solucionarlo. No obstante el equipo será perfectamente funcional sin ella y sólo afecta a la precisión de los niveles reportados. Ver **Anexo 4.2**.

Configuración

Hasta ahora, si se guardaba la configuración sin que las radios estuvieran preparadas, se perdía la configuración asociada a las radios, como las frecuencias, la duración de trama o el *target RSSI*.

Se ha corregido ese comportamiento, de tal forma que si las radios no están aún preparadas, si se guarda la configuración se mantendrá la última configuración de las radios que estuviera guardada o la de por defecto si la configuración no se había guardado nunca.

Gestión de las colas de servicios

Se han realizado diferentes optimizaciones en las colas de los servicios. Por un lado, en caso de que la cola esté llena, el paquete que se descarta es el más antiguo en lugar del nuevo. Esto permite que TCP detecte antes la congestión.

Por otra parte, se han ajustado los tamaños de las colas asociadas a cada servicio.

Web

La memoria RAM usada se muestra en un formato más adecuado.

2.2.2 Comunes a todas las estaciones base

RADIUS

Actualización del alias de un CPE

Si se actualiza el alias del CPE en el servidor RADIUS, la BS automáticamente actualizará esta información en su *Signal Stats* cuando se cumpla el *session timeout* configurado, sin necesidad de reconectar al usuario.

Accounting

Anteriormente, cuando la estación base envíaba un mensaje de *accounting* al servidor RADIUS, ésta esperaba a recibir la respuesta del servidor antes de seguir procesando más peticiones de *accounting* o autenticación. Esto se convertía en un problema cuando el servidor RADIUS tardaba demasiado en responder a las peticones o directamente no respondía. Y podía conducir a situaciones en las que se bloquease completamente el mecanismo de autenticación en la celda.

Ahora la estación base envía los mensajes de *accounting* sin esperar la respuesta del servidor RADIUS, evitando así los posibles descritos con anterioridad.

Caché de autenticación RADIUS

La estación base cuenta con una caché de autenticación RADIUS, de tal forma que si un CPE no está autorizado en el servidor RADIUS o éste no responde, la estación base no volverá a consultar al servidor RADIUS hasta que venza el tiempo de permanencia en esta caché.

Este sistema se ha mejorado, de tal forma que esta caché sólo se genera en el caso de que el servidor RADIUS responda. Si el servidor no responde, no se generará dicha caché. Así se permite que los usuarios que sí están dados de

alta en el RADIUS entren lo más rápido posible cuando el servidor vuelva a estar disponible.

Sistema de polling

Se ha mejorado el sistema de *polling* a los CPEs, el cual permite preguntar a los usuarios si tienen la necesidad de cursar tráfico en UL. Ahora se garantiza al menos un slot de UL dedicado a *polling* en cada trama.

Además, en el cálculo del número mínimo de pollings por trama se tienen en cuenta diferentes parámetros, tales como la división de trama, el número de CPEs o el modo de optimización seleccionado.

Por otra parte, ahora se tiene en cuenta el número de *pollings* a la hora de calcular la división automática de trama.

División automática de trama

En caso de que las necesidades totales puedan ser satisfechas, el algoritmo de división automática de trama reparte los símbolos sobrantes teniendo en cuenta la proporción de necesidades entre DL y UL.

API REST

Se han añadido nuevas llamadas a la API REST que permiten realizar ciertas operaciones sobre la provisión de los CPEs, así como descargar el fichero CSV con las estadísticas de señal de un CPE en particular. Ver el **Anexo 4.3** para más detalle.

Web

Los *Presets* de Network Setup permiten ahora también configurar un *default gateway*.

Se ha eliminado de la página de *Signal Stats* el indicador de *radio master* [M] y *slave* [S] de los CPEs.

El CSV de Signal Stats ahora incluye información sobre la antena del CPE.

Los CPEs y la BS se intercambian sus coordenadas de posición. Esta información se incluye en el CSV de Signal Stats.

El CSV de Signal Stats ahora también indica el método para obtener la IP WAN del CPE (*static*, *dynamic* o PPPoE). También esta información se muestra en el desplegable de *Additional Actions*.

Ver **Anexo 4.4** para más detalle acerca de los nuevos campos del CSV.

2.2.3 Estaciones base BS400 y BS800

Web

Ahora se muestra una única temperatura por cada par de radios combinadas. Por ejemplo, sólo se muestra una única temperatura para las radios azul y azul rayada.

2.2.4 Comunes a todos los terminales de usuario

Seguridad

Se ha incorporado la opción de ocultar el warning de seguridad en la web de forma permanente, siendo esta configuración permanente entre reinicios. Esto no afecta al reporte que se hace a la estación base, de modo que en ella sí se seguirán mostrando los warnings de seguridad relativos al CPE. Ver **Anexo 4.5**.

Por otra parte, si el CPE está en modo *bridge* ya no se muestra el warning de seguridad relativo al WAN Service Filtering ni tampoco se reporta a la estación base.

ACK suppression

Se ha implementado un mecanismo que permite reducir el número de ACKs y SACKs del protocolo TCP enviados en UL por el CPE. Esto permite reducir el ancho de banda en UL usado en este tipo de conexiones. No obstante, algunas implementaciones especiales de TCP podrían no responder adecuadamente en presencia de este mecanismo.

Ver **Anexo 4.6** para más detalle.

Otros

Se ha eliminado una traza asociada al UPnP que podía indundar el log del CPE.

2.3 Fallos solucionados

2.3.1 Comunes a todos los dispositivos

Monitorización

Se ha corregido un bug relativo a la monitorización de la temperatura de las radios.

2.3.2 Comunes a todas las estaciones base

RADIUS

El parámetro *Accounting Interval* aceptaba como valor máximo 600 segundos, pero la web permitía configurar valores mayores, sin tener realmente efecto.

Se ha corregido una carrera en las listas internas de autenticación del demonio de RADIUS de las estaciones base.

Red

El sistema de protección ante bucles (*Loop Protect*) podía provocar en algunos casos un cuelgue de la estación base.

Provisión

Se ha corregido el bug por el cual tras cambiar la *template* y reconectar al CPE, en algunos casos no se aplicaba la configuración asociada a la nueva *template*.

Corregido un bug por el que en ocasiones la web fallaba cuando la BS tenía portadoras fuera de la zona y se manipulaban las *templates*.

Sistema

Se ha corregido el bug por el cual tras efectuar un *factory restore* en ocasiones la base de datos de provisión no se eliminaba.

Remote commands

Cuando se enviaba el remote command para habilitar el WAN Service Filtering, el CPE intentaba activar el certificado de BS authentication erróneamente, dejando una traza en el log del CPE.

Clasificación de paquetes PPPoE

Los paquetes especiales de PPPoE como los mensajes asociados a la fase de descubrimiento (PADI/PADO) y los mensajes del protocolo (LCP, CHAP, …) siempre entraban por cualquier clasificador, independientemente de la acción de dicho clasificador. De este modo, si la acción del clasificador de mayor orden era de descarte, los paquetes de PPPoE eran descartados y la sesión nunca llegaba a establecerse.

Se ha corregido este comportamiento de tal forma que estos paquetes especiales sólo entran por un clasificador en caso de que éste no sea de descarte.

Web

Cuando un CPE estaba configurado en modo Routed NAT con PPPoE y la sesión PPPoE no se podía levantar, en la web de la BS, página Signal Stats y pinchando en la MAC del CPE, se mostraba información errónea en la tabla *CPE Networking Info*.

2.3.3 Estaciones base BS400 y BS800

Ciclo de señal

En escenarios con alta interferencia en UL las estadísticas del ciclo de señal podían no calcularse correctamente, dando como resultado medidas erróneas de modulación o CINR. Esto podía provocar que la BS balancease CPEs a portadoras con muy mala señal, ocasionando en algunas ocasiones la caída del enlace radio del CPE.

2.3.4 Comunes a todos los terminales de usuario

Red

Si el CPE tenía activo el WAN Service Filtering de ICMP, también se estaban bloqueando las peticiones ICMP iniciadas por el CPE hacia Internet. Se ha corregido para que sólo se bloqueen las peticiones ICMP entrantes hacia la IP pública del CPE.

Se ha corregido un bug relativo a la redirección de puertos. Si los puertos externos de servicio se redirigían y, posteriormente, se modificaban los puertos internos asociados, las reglas de *firewall* podían no actualizarse correctemente. De este modo, no se podía acceder al equipo en los puertos externos configurados.

Radio

Ahora cuando el CPE realiza un análisis de espectro, tando desde la web como por remote command, el CPE recuerda cuál era la portadora de la estación base a la que estaba conectado antes de arrancar el análisis de espectro. De este modo, cuando el análisis de espectro finalice, el CPE intentará conectarse a dicha portadora antes de arrancar un nuevo ciclo de AFS.

Web

Se ha corregido un bug relativo a los permisos de la página *Device* de los CPEs. Ahora ya no se puede acceder a la configuración del *Health Monitor* con el perfil de usuario *user*.

2.3.5 Terminales de usuario CPE200 y CPE300

Red

Se ha incrementado el tamaño de los *buffers* de recepción ethernet para evitar perqueñas pérdidas puntuales de paquetes en escenarios de alta carga de tráfico.

Otros

El *Burst Mode* no funcionaba correctamente, presentando un comportamiento errático a la hora definir la máxima capacidad del servicio y de respetar los tiempos de activación y pausa.

Se ha corredigo un bug relativo al acceso a determinadas direcciones de la memoria flash. También se ha arreglado un *deadlock* asociado al driver de JFFS2 del kernel que podía provocar corrupciones en la flash.

2.3.6 Terminales de usuario CPE100

Red

Se ha corregido un bug relativo al PPPoE que podía provocar que la sesión PPPoE no volviera a establecerse tras una caída del enlace radio del CPE.

3. Información importante

3.1 Estaciones base BS800

Con el objetivo de evitar problemas durante el proceso de actualización, se recomienda parar las radios antes de actualizar.

3.2 API REST y diccionario RADIUS

Esta versión de firmware incluye cambios relativos a la API REST y al RADIUS. Por ello, se comienda descargar la documentación asociada desde Albentia PRO.

4. Apéndice

4.1 RADIUS

A continuación se muestra una configuración de RADIUS típica para un CPE, incluyendo los 2 nuevos atributos incorporados en esta versión de firmware.

```
00:1F:4A:00:19:7C Cleartext-Password := "password"
        Provision-Type = TEMPLATE,
        Alias-User = "cpe_prueba",
        Alias-Template = "template_prueba",
        Primary-BSID-Allowed = "00:1F:4A:00:00:AA,00:1F:4A:00:00:BB",
        Secondary-BSID-Allowed = "00:1F:4A:00:00:CC,00:1F:4A:00:00:DD",
        Session-Timeout = 60
```

Estos atributos son opcionales y su lógica de funcionamiento se detalla a continuación.

- No incluídos en la respuesta RADIUS: El CPE será autorizado.
- Sólo Primary-BSID-Allowed, sin Secondary-BSID-Allowed: La BS sólo autorizará al CPE si el BSID configurado en la BS coincide con alguno de los incluídos en este atributo.
- Sólo Secondary-BSID-Allowed, sin Primary-BSID-Allowed: El atributo se ignora.
- Ambos, Primary-BSID-Allowed y Secondary-BSID-Allowed están presentes:
    - Si el BSID configurado en la BS coincide con alguno de los incluídos en el atributo Primary-BSID-Allowed, el CPE será autorizado.
    - Si el BSID configurado en la BS NO coincide con ninguno de los incluídos en el atributo Primary-BSID-Allowed, pero sí con los incluídos en el atributo Secondary-BSID-Allowed el CPE también será autorizado. La diferencia es que la BS desconectará al CPE pasados "Secondary BSID TO" segundos. El CPE puede ser desconectado por este motivo hasta "Max. Secondary BSID disconnections". Alcanzadas este número de desconexiones, el CPE será autorizado y NO será desconectado. Cumplidos estos retries, si el CPE se cae por cualquier motivo (señal, forzado desde la BS, etc), la BS reiniciará

este contador, es decir, se le permitirá pero se le desconectará pasados "Secondary BSID TO" segundos.

- Si el BSID configurado en la BS NO coincide con ninguno de los BSIDs primarios y secundarios, el CPE NO será autorizado.

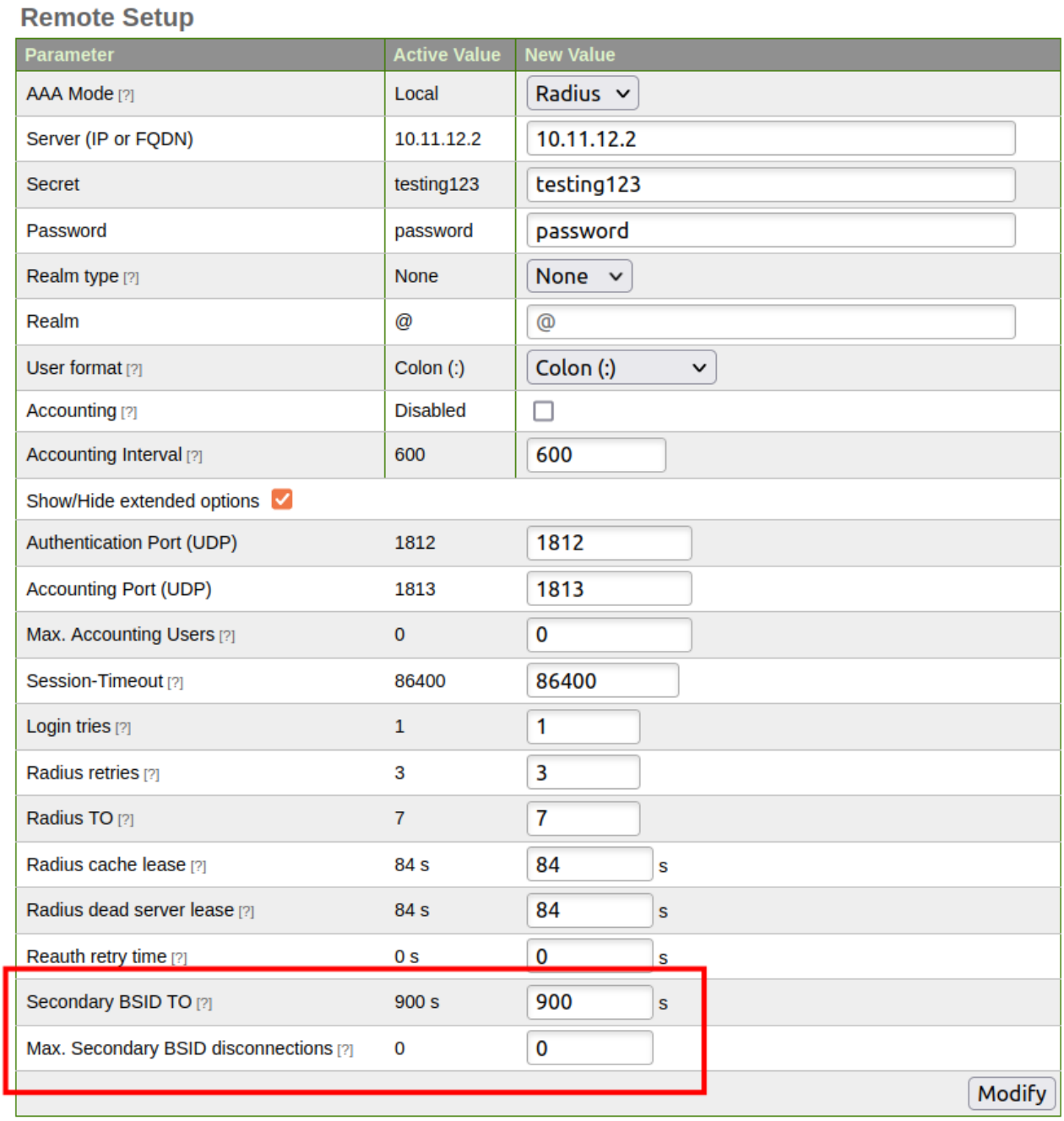
Estos atributos tienen el formato especificado más arriba: listado de BSIDs separados por coma.

```
Primary-BSID-Allowed = "00:1F:4A:00:00:AA,00:1F:4A:00:00:BB",
```

Muy importante tener en cuenta 2 cosas:

1. Los BSIDs tienen que estar separados por comas **sin ningún tipo de espacio**.
2. El número máximo de BSIDs que se pueden incluir en el listado es de **12 (12 primarios + 12 secundarios)**. Esta limitación viene dada por el tamaño de los atributos de RADIUS.

Tenemos 2 parámetros configurables en la web de la BS relativos a los BSIDs de RADIUS:



1. **Secondary BSID TO.** Número de segundos tras los cuales un CPE que ha sido autorizado por Secondary-BSID-Allowed será desconectado.
2. **Max. Secondary BSID disconnections.** Número de veces que un CPE que ha sido autorizado por Secondary-BSID-Allowed puede ser

desconectado. Pasado este número, la BS comprobará que el CPE sigue autorizado cada vez que se cumpla el *session timeout*, tal y como si hubiera sido autorizado por un BSID primario. Este contador se reinicia, es decir, se volverá a desconectar este número de veces como si fuera la primera vez que entra en la celda, si se cumplen cualquiera de estas dos condiciones:

- Si el CPE lleva desconectado más de "Secondary BSID TO" segundos.
- Si el CPE ya ha alcanzado su número máximo de desconexiones y se desconecta por cualquier motivo.

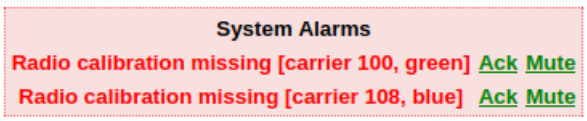
Si el "Max. Secondary BSID disconnections" se configura a 0, la BS desconectará a todo CPE que haya entrado por secondary BSID cada "Secondary BSID TO" indefinidamente.

El mínimo valor configurable de "Secondary BSID TO" es de 300 segundos.

Para poder usar los nuevos atributos, es imprescindible actualizar el diccionario de RADIUS en el servidor. El diccionario actualizado se encuentra disponible en Albentia PRO.

4.2 Alarmas de calibración

A continuación se muestra un ejemplo de alarma en un cuyas radios no están calibradas.



Si se detecta esta alerta en un equipo, póngase en contacto con el departamento de ingeniería para solucionarlo. No obstante el equipo será perfectamente funcional sin ella y sólo afecta a la precisión de los niveles reportados.

4.3 API REST

A continuación se muestran algunos ejemplos de las nuevas funciones de la API REST.

Recuperación de las *templates*

GET - /gui/local_aa.cgi/rest/templates

```
{
      "templates":      [{
                  "template_id":    "template_1"
            }, {
                  "template_id":    "template_2"
            }]
}
```

Recuperación de los usuarios

GET - /gui/local_aa.cgi/rest/users

```
{
      "users":      [{
                  "hwaddr":     "00:1F:4A:00:40:17",
                  "alias":      "CPE",
                  "provtype":   "template",
                  "template_id":        "template_1",
                  "access":     "allow"
            }, {
                  "hwaddr":     "00:1F:4A:00:37:10",
                  "alias":      "CPE",
                  "provtype":   "template",
                  "template_id":        "template_2",
                  "access":     "allow"
            }]
```

```
}
```

Modificación de un usuario

POST - /gui/local_aa.cgi/rest/users

Parámetros

```
"hwaddr=00:1F:4A:00:AA:AA&alias=mycpe&template=mytemplate&access=allow"
```

Recuperar la información de provisión de un usuario

GET - /gui/local_aa.cgi/rest/user/00:1F:4A:01:8A:3D

```
{
      "hwaddr":   "00:1F:4A:01:8A:3D",
      "alias":    "TEST RELEASE",
      "provtype": "template",
      "template_id":    "template_OTA",
      "access":   "allow"
}
```

Modificar la provisión de un usuario

PUT - /gui/local_aa.cgi/rest/user/00:1F:4A:01:8A:3D

Parámetros:

"alias=mycpe&template=mytemplate&access=allow"

Desprovisionar a un usuario

DELETE - /gui/local_aa.cgi/rest/user/00:1F:4A:01:8A:3D

Recuperar CSV para un usuario particular

GET - /gui/stats.cgi/rest/download/00:1F:4A:00:AA:AA"

```
MAC_ADDRESS,CARRIER,RADIO,ALIAS,STATUS,AUTHENTICATED,MANAGED,UPTIME(secs),TX_POW(
dBm),UL_MODULATION,DL_MODULATION,UL_RSSI(dBm),DL_RSSI(dBm),UL_CINR(dB),DL_CINR(dB
),NUM_FLOWS,APPROX_DIST(m),DIST_ERROR(m),SW_VER,IP,MNG_IP,SECURE_HTTP,UL_INTERF_L
VL,DL_INTERF_LVL,NET_MODE,WAN_CONNECTION,FREQ_MODE,UL_EXPECT_RSSI(dBm),DL_EXPECT_
RSSI(dBm),BS_AUTH,COORDINATES,ANTENNA

00:1F:4A:01:8A:3D,green,MASTER,"TEST          RELEASE",Active,NO,YES,994,23,16QAM-
3/4,64QAM-3/4,-67.75,-
71,19,24,2,0,104,6353,10.11.12.83,10.11.12.83,NO,0,0,ROUTED(NAT),DYNAMIC
IP,FIXED,-,-,NO,N/A,Unknown antenna
```

4.4 CSV de Signal Stats

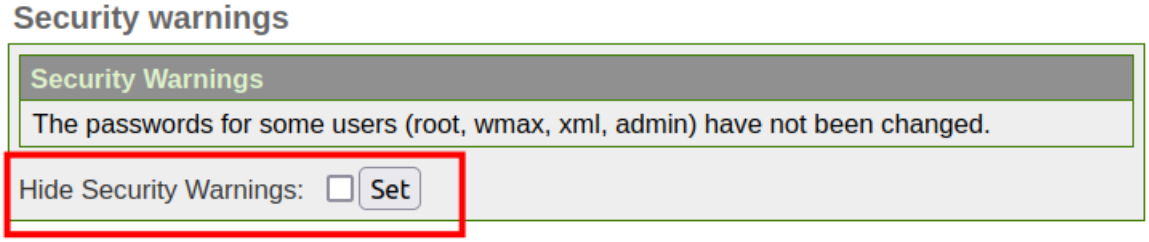
A continuación se detallan los nuevos campos en el CSV del Signal Stats.

```
MAC_ADDRESS,CARRIER,RADIO,ALIAS,STATUS,AUTHENTICATED,MANAGED,UPTIME(secs),TX_POW(
dBm),UL_MODULATION,DL_MODULATION,UL_RSSI(dBm),DL_RSSI(dBm),UL_CINR(dB),DL_CINR(dB
),NUM_FLOWS,APPROX_DIST(m),DIST_ERROR(m),SW_VER,IP,MNG_IP,SECURE_HTTP,UL_INTERF_L
VL,DL_INTERF_LVL,NET_MODE,WAN_CONNECTION,FREQ_MODE,UL_EXPECT_RSSI(dBm),DL_EXPECT_
RSSI(dBm),BS_AUTH,COORDINATES,ANTENNA

00:1F:4A:01:8A:3D,green,MASTER,"TEST          RELEASE",Active,NO,YES,2117,23,16QAM-
3/4,64QAM-3/4,-66.25,-
70,20,24,2,0,104,6353,10.11.12.83,10.11.12.83,NO,0,0,ROUTED(NAT),DYNAMIC
IP,FIXED,-,-,NO,40.3531244,-3.7453141,Unknown antenna
```

4.5 Deshabilitación de advertencias de seguridad

A continuación se muestra el menú en el que se pueden deshablitar las advertencias de seguridad en el CPE.



4.6 Supresión de ACKs

A continuación se muestra cómo configurar la supresión de ACKs de TCP en un servicio de subida. Se puede seleccionar que se supriman sólo los ACKs o también los SACKs.