albentia
systems

AerDocsis System Software Software Release Notes

HoneybeeM2 19.6.6353

December 13, 2021

Contents

1. Compatible devices and minimum versions

Product family	Devices	Minimum versions
Base Stations		
BS400 and BS800	AXS-BS-450-N AXS-BS-850-N	Honeybee M1 19.6.6172
BS100	AXS-BS-150-N	Honeybee M1 19.6.6172
User Terminals		
CPE100	AXS-CPE150-15 AXS-CPE150-RS	Honeybee M1 19.6.6172
CPE200 and CPE300	AXS-CPE250-15 AXS-CPE250-RS AXS-CPE350-15 AXS-CPE350-RS	Honeybee M1 19.6.6172
Radio Links		
LNK100	LNK-LU1150-N LNK-LU1150-23	Honeybee M1 19.6.6172

2. What's new in this release?

2.1 New features

2.1.2 Common to all Base Stations

New RADIUS attributes

Two new RADIUS attributes Primary-BSID-Allow and Secondary-BSID-Allowed have been added. These attributes define which BSIDs the CPE can connect to. In case the CPE connects to a secondary BSID, the BS will disconnect the CPE after a configurable time and the CPE will execute an AFS to try to connect to a primary BS.

On the other hand, the RADIUS attributes Sector-Allowed and Zone-Allowed are no longer supported. For more details, see **Appendix 4.1**.

Remote commands

Four new remote commands have been added:

- PPPoE test mode. Configures the CPE in Routed NAT mode with PPPoE with the username **albtest** and password **albtest**. The LAN IP of the CPE is set to 192.168.0.128/24.

- Bridge test mode. Configures the CPE in bridge mode with static IP 10.11.12.3/8.

- Enable SMC. Enables the secondary management channel (SMC) on the CPE in DHCP mode and with fallback IP 176.0.0.1/24. The CPE will reconnect after receiving this command in order to apply the new configuration.

- Disable SMC. Disables the secondary management channel (SMC) on the CPE. The CPE will reconnect after receiving this command in order to apply the new configuration.

2.2 Enhanced features

2.2.1 Common to all devices

Provision

The DHCP Injection option now works also in case the traffic is encapsulated over VLAN.

System

The *Health Monitor* log file, *gather data*, now displays device information, such as its name, location, owner, MAC address, and firmware version.

Monitorization

The system now monitors if the radios are correctly calibrated. If not, an alarm is displayed on the web. If you detect this situation on your equipment, please contact Albentia engineering team to fix it. Meanwhile, the equipment will be fully funcional, however reported signal level accuracy could be affected. See **Appendix 4.2**.

Configuration

Until now, if the configuration was saved when the radios were not ready, the configuration associated with the radios, such as frequencies, frame duration or Target RSSI, would be lost.

This behavior has been fixed. If the radios are not ready and the configuration is saved, the last configuration of the radios (or the default one if the configuration had never saved) will be maintained.

Service queue management

Different optimizations have been done in the queues of the services. On the one hand, in case the queue is full, the packet that is discarded is the oldest rather than the new one. This allows TCP to detect congestion earlier.

On the other hand, the sizes of the queues associated with each service have been adjusted.

Web

Used RAM is shown in a more suitable format.

2.2.2 Common to all Base Stations

RADIUS

<u>CPE alias update</u>

If the CPE alias is updated on the RADIUS server, the BS will automatically update this information in its Signal Stats when the configured session timeout is fulfilled, without reconnecting the user.

<u>Accounting</u>

Previously, when the base station sent an accounting message to the RADIUS server, it waited for the server's response before continuing to process more accounting or authentication requests. This was a problem when the RADIUS server took too long to answer to requests or was not responding at all. And it could lead to situations where the authentication mechanism in the cell was completely blocked.

Now the base station sends the accounting messages without waiting for the response from the RADIUS server, thus avoiding the problems previously described.

<u>RADIUS authentication cache</u>

The base station has a RADIUS authentication cache, so that if a CPE is not authorized in the RADIUS server or the server does not reply, the base station will not question the RADIUS server again until the cache expires.

This functionality has been improved and this cache is only generated if the RADIUS server replies. If the server does not reply, no cache will be generated. This allows users, who are authorized in RADIUS, to enter as quickly as possible when the server is up again.

Polling

Polling, which allows users to be asked if they have needs in UL, has been improved. Now at least one UL slot per frame is dedicated for polling.

Furthermore, the base station takes into account different parameters in order to compute the minimum number of polling slots per frame, such as the frame division, the number of CPEs or the selected optimization mode.

Additionally, the automatic frame division algorithm takes into account the number of polling slots.

Automatic frame division

In case the total needs can be satisfied, the automatic frame division algorithm distributes the surplus symbols taking into account the ratio of needs between DL and UL.

REST API

New functions have been added to the REST API which allow performing certain operations in the provision of CPEs, as well as downloading the CSV file with the signal stats of a single CPE. See **Appendix 4.3** for more details.

Web

Network Setup presets now also allow to configure a default gateway.

The radio indicator master [M] / slave [S] of the CPEs has been removed from the Signal Stats page.

The Signal Stats CSV now includes information about the CPE antenna.

The CPEs and the BS exchange their coordinates. This information is included in the Signal Stats CSV.

The Signal Stats CSV now also indicates how the CPE configures its WAN IP address (static, dynamic, or PPPoE). This information is also shown in the *Additional Actions* selector. See **Appendix 4.4** for more details about the new fields of the CSV.

2.2.3 BS400 and BS800 Base Stations

Web

Now a single temperature is shown for each pair of combined radios. For example, only a single temperature is shown for the blue and striped blue radios.

2.2.4 Common to all User Terminals

Security

An option which allows to hide the security warning in the web permanently has been added and it is persistent between reboots. This does not affect the report that the CPE sends to the base station, so it will show the security warnings related to the CPE as usual. See **Appendix 4.5**.

Furthermore, if the CPE is in bridge mode, the security warning related to WAN Service Filtering is no longer shown, nor it is reported to the base station.

ACK suppression

A new feature has been implemented to reduce the number of ACKs and SACKs of the TCP protocol sent in UL by the CPE. This allows to reduce the bandwidth in UL used in this kind of connections. However, some special TCP implementations could exhibit unexpected behaviours in presence of these mechanisms.

See **Appendix 4.6** for more details.

Miscellaneous

A log message related to UPnP has been removed in order to avoid flooding the log file.

2.3 Fixed bugs

2.3.1 Common to all User Terminals

Monitorization

Fixed a bug related to radio temperature monitoring.

2.3.2 Common to all Base Stations

RADIUS

The *Accounting Interval* parameter accepted a maximum value of 600 seconds, but the web allowed setting higher values, without having any effect actually.

Fixed a race condition in the internal RADIUS daemon authentication lists of the base stations.

Networking

The Loop Protect subsystem could cause the base station to be stalled in some scenarios.

Provision

After changing the template and reconnecting the CPE, in some cases the configuration associated with the new template was not applied. This bug has been fixed.

Sometimes the web crashed when the BS had carriers which did not belong to the zone and the templates were modified. This bug has been fixed.

System

The factory restore might not delete the provisioning database. This bug has been fixed.

Remote commands

When the *remote command* which enables WAN Service Filtering was sent, the CPE tried to enable the BS authentication wrongly, generating a trace in the log of the CPE.

PPPoE packet classification

Special PPPoE packets such as the messages associated with the discovery stage (PADI / PADO) and the protocol messages (LCP, CHAP,...) always matched to any classifier, regardless of the action of this classifier. Thus, if the action of the highest order classifier was *drop*, the PPPoE packets were dropped and the session was never established.

This behavior has been fixed and these special packets only matched to a classifier if it is not a *discard* one.

Web

When a CPE was configured in Routed NAT mode with PPPoE and the PPPoE session could not be stablished, the base station Signal Stats page showed wrong information in the *CPE Networking Info* table.

2.3.3 BS400 and BS800 Base Stations

Signal cycle

In scenarios with high UL interference level the signal cycle stats could not be computed correctly, causing wrong modulations or CINR measurements. This could cause the BS to balance CPEs to carriers with a really bad signal, often causing the CPE disconnection.

2.3.4 Common to all User Terminals

Networking

If the CPE had ICMP WAN Service Filtering enabled, ICMP requests initiated by the CPE to the Internet were also blocked. This bug has been fixed and only incoming ICMP requests to the public CPE IP are blocked.

Fixed a bug related to port forwarding. If the external service ports were redirected and the associated internal ports were subsequently modified, the firewall rules might not be updated correctly. Thus, the equipment was not accessible on the configured external ports.

Radio

When the CPE runs a spectrum analysis, triggered through the web or by *remote command*, the CPE remembers the carrier of the base station to which it was connected before starting the spectrum analysis. This way, when the spectrum analysis finishes, the CPE will try to connect to that carrier before starting a new AFS cycle.

Web

Fixed a bug related to the permissions of the *Device* page of the CPEs. Now, the user cannot access to the *Health Monitor* configuration with the profile *user*.

2.3.5 CPE250 and CPE300 User Terminals

Networking

The size of the Ethernet reception buffers has been increased to avoid little packet losses in high traffic load scenarios.

Miscellaneous

The *Burst Mode* did not work correctly, presenting a erratic behavior related to the maximum capacity of the service, the activation and pause times.

A bug related to the accessing to certain flash memory addresses has been fixed. Additionally, a deadlock related to the kernel JFFS2 driver that could cause flash corruption has been fixed.

2.3.6 CPE100 User Terminals

Networking

Fixed a bug related to PPPoE that could cause the PPPoE session not to be established again after the CPE was disconnected from the base station.

3. Important notes

3.1 BS800 Base Stations

In order to avoid problems during the update process, it is recommended to stop the radios before updating.

3.2 REST API and RADIUS dictionary

This firmware version includes changes related to the REST API and RADIUS. Therefore, it is recommended to download the new documentation from Albentia PRO.

4. Appendix

4.1 RADIUS

Below you can see a typical RADIUS configuration for a CPE, including the 2 new attributes incorporated in this firmware release.

```
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
```

These attributes are optional and their logic is detailed below.

- Not included in the RADIUS response: The CPE will be authorized.

- Primary-BSID-Allowed only, no Secondary-BSID-Allowed: The BS will authorize the CPE only if the BSID configured in the BS matches one of those included in this attribute.

- Secondary-BSID-Allowed only, no Primary-BSID-Allowed: The attribute will be ignored.

- Both Primary-BSID-Allowed and Secondary-BSID-Allowed are present:

  ○ If the BSID configured in the BS matches one of those included in the Primary-BSID-Allowed attribute, the CPE will be authorized.

  ○ If the BSID configured in the BS does NOT match any of those included in the Primary-BSID-Allowed attribute, but does match those included in the Secondary-BSID-Allowed attribute, the CPE will also be authorized. The difference is that the BS will disconnect the CPE after *"Secondary BSID TO"* seconds. The CPE can be disconnected for this reason up to *"Max. Secondary BSID disconnections"*. Once this number of disconnections has been reached, the CPE will be authorized and will NOT be disconnected. Once these retries have been fulfilled, if the CPE is disconnected for any reason (signal, forced from the BS, etc.), the BS will reset this counter, that is, it will be allowed but it will be disconnected after *"Secondary BSID TO"* seconds.

- If the BSID configured in the BS does NOT match any of the primary and secondary BSIDs, the CPE will NOT be authorized.

These attributes have the format specified above: list of BSIDs separated by commas.

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

It is very important to take into account 2 aspects:

1. The BSIDs have to be separated by commas without any blank space.

2. The maximum number of BSIDs that can be included in the list is 12 (12 primary + 12 secondary). This limitation is due to the size of the RADIUS attributes.

We have 2 configurable parameters on the BS web related to RADIUS BSIDs:

Remote Setup

Parameter	Active Value	New Value
AAA Mode [?]	Local	Radius ▾
Server (IP or FQDN)	10.11.12.2	10.11.12.2
Secret	testing123	testing123
Password	password	password
Realm type [?]	None	None ▾
Realm	@	@
User format [?]	Colon (:)	Colon (:) ▾
Accounting [?]	Disabled	☐
Accounting Interval [?]	600	600
Show/Hide extended options ☑		
Authentication Port (UDP)	1812	1812
Accounting Port (UDP)	1813	1813
Max. Accounting Users [?]	0	0
Session-Timeout [?]	86400	86400
Login tries [?]	1	1
Radius retries [?]	3	3
Radius TO [?]	7	7
Radius cache lease [?]	84 s	84 s
Radius dead server lease [?]	84 s	84 s
Reauth retry time [?]	0 s	0 s
Secondary BSID TO [?]	900 s	900 s
Max. Secondary BSID disconnections [?]	0	0

Modify

1. **Secondary BSID TO**. Number of seconds after which a CPE that has been authorized by Secondary-BSID-Allowed will be disconnected.

2. **Max. Secondary BSID disconnections**. Number of times that a CPE that has been authorized by Secondary-BSID-Allowed can be disconnected. After this number, the BS will check if the CPE is still

authorized each time the session timeout is fulfilled. This counter will be reset in case one of these two conditions are met:

- If the CPE has been disconnected for more than "Secondary BSID TO" seconds.

- If the CPE has already reached its maximum number of disconnections and disconnects for any reason.

If the "Max. Secondary BSID disconnections" is set to 0, the BS will disconnect every CPE that has entered through secondary BSID every "Secondary BSID TO" indefinitely.

The minimum configurable value of "Secondary BSID TO" is 300 seconds.

In order to use the new attributes, it is mandatory to update the RADIUS dictionary on the server. The new dictionary is available in Albentia PRO.

4.2 Calibration alarms

Below you can see an example of an alarm which appears when the radios are not calibrated.
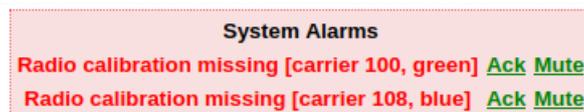
If you detect this situation on your equipment, please contact Albentia engineering team to fix it. Meanwhile, the equipment will be fully funcional, however reported signal level accuracy could be affected.

4.3 REST API

Here are some examples of the new REST API functions.

Get the list of templates

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

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

Get the list of users

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"
        }]
```

```
}
```

User modification

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

Parameters:

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

Get provision information of one user

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"
}
```

Mofidy the provision of one user

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

Parameters:

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

Remove one user from provision

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

Get CSV for one user

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 Signal Stats CSV

The new fields in the Signal Stats CSV are detailed below.

```
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 Disabling security warning

Below you can see the section where you can disable the security warnings in the CPE.

Security warnings

Security Warnings
The passwords for some users (root, wmax, xml, admin) have not been changed.

Hide Security Warnings: ☐ Set

4.6 ACK suppression

The following screenshot shows how to configure TCP ACK suppression in a UL service. It is possible to select what kind of ACKs will be suppresed: only ACKs or both, ACKs and SACKs.