Release Notes
System Software 10.1.23

Inhalt

1 New functions

A DETAILED DESCRIPTION OF THE INDIVIDUAL NEW FUNCTIONS CAN BE FOUND IN THE ONLINE HELP AND THE MANUAL OF YOUR DEVICE.

1.1 WLAN Bridge Links

System Software 10.1.23 offers WLAN Bridge Links in the **Wireless LAN -> WLAN -> Bridge Links** menu.

For a bridge link, you can select a *master* or a *slave* mode in the **Wireless LAN -> WLAN -> Bridge Links -> New** menu. To connect two devices via a bridge link, configure one device in master and the other in slave mode.

1.2 “Sticky Client”

A client in a WiFi network is called a “sticky client” if it tends to hang on to the original access point (AP) currently registered to. This is also true if the data rate is significantly decreasing and there is an AP with a stronger signal nearby which the client could join.

This behavior is caused by the fact that many clients are originally designed for home network environments where only a single AP is in use and the connection to this AP should be maintained. Roaming is not required here. In professional environments, requirements are completely different because several APs operate in a WiFi network. Here, optimal roaming increases WiFi performance considerably.

1.2.1 Roaming

Clients in a larger WiFi network should monitor the indicators for the quality of their connection to an AP. A change in these parameters should cause a roaming decision, i.e. the client should associate to another AP. The Receive Signal Strength Indicator (RSSI), the signal to noise ratio and the number of errors or retries during data transfer may be such indicators.

1.2.2 Consequences for other clients

The optimal roaming process of a client in a WiFi network does not only benefit the client itself but all other clients in this WiFi network, as well. If a client operates at a low transmission rate, the data transfer of a certain data volume take more time. and clients in the same AP cell have to wait longer than necessary to transfer their data.

1.2.3 Mitigating “sticky clients” (only for bintec W2003ac)

To mitigate the consequences of “sticky client” behavior, the AP can influence the roaming decisions of the client.

Received Signal Strength Indicator (RSSI)

For this purpose, System Software 10.1.23 supports the RSSI threshold in **bintec W2003ac** devices. The function is available if the parameter **Operation Mode** = *Access-Point / Bridge Link Master* is set under **Wireless LAN -> WLAN -> Radio Setting -> Edit**.

In the menus **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> New/Edit -> Advanced Settings** and **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> New,** you can define a threshold for the signal level using the parameter **RSSI threshold** under **Low RSSI threshold management**. If an AP recognizes that one of its clients falls below the signal level for a longer period than set under **Grace time**, it stops communicating with this client. Normally, a client tries to connect to the “old” AP for several times and then searches for a new one.

Data rate trimming

System Software 10.1.23 supports **Data Rate Trimming** for **bintec W2003ac** devices. To access this function, set **Operation Mode** = *Access-Point / Bridge Link Master* under **Wireless LAN -> WLAN -> Radio Setting -> Edit**. Using **Data Rate Trimming** increases WiFi performance by blocking low data transfer rates and enforcing the use of higher data rates.

If the distance between a client and its current AP increases, the signal level received by the client as well as the signal quality decreases. To compensate this, the client decreases its data transmission rate because using lower data rates reduces error rates. If using lower data rates is prevented (so called data rate trimming), a client is forced to connect to another AP as soon as the distance to its current AP increases. All clients are forced to use the allowed data rates only.

You can configure the supported data rates under **Data-Rate Trimming** in the **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> New/Edit -> Advanced Settings** and **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> New** menus. Depending on the selected frequency band several predefined data rate profiles are available.

1.3 WLAN Controller – Deleting a configuration

If the WLAN controller is switched off, use the 🗑 icon in the **Wireless LAN Controller -> Controller Configuration** menu to completely delete its configuration.

1.4 New MIB Variables

The MIB variable *wlanStatisticsChannelUtil* displays the channel load in percent. The MIB variable *wlcWlanIfStatChannelUtil* does the same for the WLAN controller.

2 Error corrections

2.1 Alert Service – Memory leak

(ID #191, #690)

If the Email alert service was used with an encrypted connection, a memory loss could occur.

Additionally, some texts may not be displayed correctly.

2.2 GUI – DHCP Server not deactivated

(ID #501, #298)

Occasionally, the DHCP server remained active, although it was deactivated in the **First steps** assistant.

2.3 NAT – Incorrect port forwarding

(ID #431)

If a service was deleted in the **Firewall -> Services -> Services** menu, it was deleted in the **Network -> NAT -> NAT configuration -> New** menu, too, and you could not restore it. A warning is displayed now. Restoring of a service is possible by resetting the device to factory settings.

2.4 SSHD – Key processing not possible

(ID #489)

The system could not process RSA keys of 2048 bits or longer.

2.5 WLC – Wrong values

(ID 20556)

By mistake, the signal strength 0dBm was processed as no signal (and not as maximum signal). If there was no data traffic, wrong values were used too.

2.6 WLAN – Access points malfunction

(ID #550)

Under certain circumstances access points sporadically showed an inconsistent behavior: Although an access point reached the state *managed*, the connection to the SSID was instable. Resetting the access point did not solve the problem.

2.7 WLAN – Wrong number of wireless networks (VSS)

(ID #601)

A maximum of eight available wireless networks was displayed instead of 16.

2.8 SIP - Crash and stacktrace

(ID #354)

If a SIP phone initiated an external call, the system crashed with a stacktrace.

2.9 WLC – Problems with wireless networks and pre-shared keys

(ID #469)

It could occur that after finishing the WLAN controller wizard not all wireless networks (VSS) were switched on and not all WLAN pre-shared keys were saved.

2.10 WLAN – Interference problem

(ID 20622)

If interferences with other services (Bluetooth for example) occurred in an automatically selected channel, WiFi was deactivated. Automatic channel selection continuously tried to use the same channel. A different channel will be used now.

2.11 WLAN – Beacon period parameter problems

(ID 20646)

If several radio modules were configured with different beacon period values for each one, problems occurred: the latest configured beacon period value was used for all radio modules.

2.12 WLAN – Interferences

(ID #448)

Interferences could cause problems because the system did not consider which channels are excluded per definition when choosing a new channel.

2.13 WLAN – Restart

(ID #475)

Sporadic restarts of the system could occurred if any further client registered.

3 Known Limitations

The following limitations have been identified in System Software 10.1.23:

3.1 System management – MAC address

(ID #606)

Within a bridge group, the correct MAC address for a virtual interface is displayed in the GUI, but the description in the MIB reference for this address is not correct.

3.2 WLAN Controller – Status display

(ID #802)

In several submenus of the **Wireless LAN Controller** menu, it may occur that a wrong icon is displayed for the system status or the wireless network (VSS) status during channel scan. During 5 GHz radio module initialization, a note is missing that a channel scan is active. Under certain circumstances, it may occur that a channel scan is displayed although there is no current scan.

3.3 WLAN – User-friendly GUI

(ID #1000)
If a client tries to connect to a bridge master and no master is found for three seconds, the radio module is deactivated for 20 seconds, but this is not visible to the user.

3.4 Configuration – Sporadic Panic

(ID #998, #1003)

There may be sporadic panics when configuring a radio module or deleting a bridge link.

3.5 WLAN – Bridge link

(ID #999)

Using a bridge master with two radio modules and an already connected client, the original, but no longer valid channel is displayed if the frequency band was changed later.

Moreover, the connection speed of bridge links is limited.

3.6 WLAN – Client mode not working

(ID #1025)

In client mode the device cannot connect to an AP.