



The **Hirschmann™** BAT Operating System

Information regarding Release

HiLCOS Software Version 9.13

Copyright (c) 2002 – 2018 Hirschmann Automation and Control GmbH, Neckartenzlingen (Germany)

Hirschmann Automation and Control GmbH takes no responsibility or warranty for software not developed or manufactured by Hirschmann Automation and Control GmbH, especially with regard to shareware and other third-party software.

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Germany

Internet: <http://www.beldensolutions.com>

2018-11-14

Table of Contents

1. Preface	3
2. Known Issues	3
3. New features and improvements in Version 9.13.5500-REL	4
WLAN- Management.....	4
System	4
4. Improvements in Versions 9.12.5910-RU7, 9.12.5900-RU6, 9.12.5850-RU5, 9.12.5800-RU4, 9.12.5750-RU3,	5
WLAN	5
WLAN (Client-Mode)	5
Security / WLAN	5
5. Improvements in Version 9.12.5600-RU1	6
WLAN	6
Network connectivity	6
Security	6
System	6
6. Improvements in Version 9.12.5500-REL	7
WLAN	7
Security	7
System	7
7. Improvements in Version 9.10.5126-REL	8
WLAN	8
Network connectivity	8
Security	8
System	8
8. Improvements in Version 9.00.5112-RU1	9
WLAN	9
Network connectivity	9
Security	9
System	9
9. Comments	10



The **Hirschmann™** BAT Operating System

1. Preface

This document describes the innovations within HiLCOS software version 9.13.

The Version 9.13 supports OpenBAT, BAT450 and BAT WLAN controller devices.

2. Known Issues

The use of RSTP together with AutoWDS can lead to an unstable AutoWDS network. It is recommended to use AutoWDS with RSTP disabled.

In very rare cases when adding a new Access Point (AP) in the AutoWDS network interactions between neighboring AutoWDS APs can occur. This can cause short-term disruptions of wireless links.

If APs are added in an AutoWDS network before enabling Auto-Accept, these APs must be accepted manually after switching Auto-Accept.

The use of redundant WLAN-Controller architectures in combination with the WLC-Fast-Recovery mechanism reduces the interruption on Layer3-Data tunnels when a WLAN-Controller fails to less than one second.

In very rare cases the events of client roaming and WLC Failure might occur at the same time. When in this case and there is no network traffic transferred from the client to a destination behind the connected AP/WLC, the network topology might not be updated. This can result in packet loss of traffic directed in the opposite direction.



The **Hirschmann™** BAT Operating System

3. New features and improvements in Version 9.13.5500-REL

WLAN- Management

- Fast Recovery of CAPWAP Layer3 DATA Tunnel in case of a WLC failure

System

- Support BATOne-Wireless devices



The **Hirschmann™** BAT Operating System

4. Improvements in Versions 9.12.5910-RU7, 9.12.5900-RU6, 9.12.5850-RU5, 9.12.5800-RU4, 9.12.5750-RU3,

WLAN

- Update regulatory approvals on the BAT devices
- Regulatory update regarding 2014/53/EU - Radio Equipment Directive (RED)
- Correction of TX power limits in channel 149 for Singapore and China profiles
- Adding capability to OpenBAT-R devices to operate as „Short Range Device“ in 5.8GHz Band according to EN 300 440.
- The PoE LED, on the OpenBAT-R, OpenBAT-F and BAT450-F, now indicates operation with power supply in client mode via PoE.

WLAN (Client-Mode)

- Improved Roaming-Handover delay for client mode in an IEEE 802.1x secured WLAN network.
- Optional setting to delay roaming event after the detection of a better suited access point.

Security / WLAN

- Fix for WPA2 Vulnerability KRACK

5. Improvements in Version 9.12.5600-RU1

WLAN

- Update regulatory approvals of the BAT devices
- Configurable WLC preference option added to managed-AP configuration
- Improved client scanning behavior
- Reduction of False-Positive detections in radar detection algorithm for EN301893
- Fixed noise floor calculation
- Fixed increased packet loss due to frequent background scanning

Network connectivity

- Improved client recovery timeout during AP failure in a roaming scenario
- Improved RSTP recovery time
- Fixed address usage in CAPWAP protocol stack when VRRP is used

Security

- Improved L2-Firewall multicast forwarding

System

- Added SNMP-Traps for the following events: DFS-Radar detected, Roaming-Client handover, NTP clock sync
- Added missing SNMP Trap descriptions
- Fixed script configuration for user-defined daylight-saving-time settings
- Fixed SNMPv2 Trap enterprise OIDs



The **Hirschmann™** BAT Operating System

6. Improvements in Version 9.12.5500-REL

WLAN

- Update regulatory approvals of the BAT devices
- Fix of configuration problems when operating a 1:1 NAT on a WLAN interface in client mode
- Improved roaming handover delay by the use of Opportunistic Key Caching and several logical WLAN Networks on separate WLAN interfaces

Security

- Fix of device specific TLS certificate generation on BAT450-F devices

System

- HiLCOS 9.12 is compliant to FCC regulations U-NII, ET Docket No. 13-49 (FCC 14-30 and FCC 16-24)
- SNMP Trap for status change of the Power Supply Unit

7. Improvements in Version 9.10.5126-REL

WLAN

- C2C (WLAN Coach Coupling) for full automatic coupling of access points in trains.
- 1:1 NAT on WLAN interfaces in client mode.
- Wireless Link Status to allow the long term observation of the quality of a WLAN connection.
- It is possible to use the Public Spot web API to create 802.1x users.
- SSIDs with a space in the name are correctly handled.
- Now it is possible to use a * as a wildcard in the station table.
- Now it is possible to define a max bandwidth per client per SSID.
- Double entries of MAC addresses in the station table are now avoided.

Network connectivity

- Improved roaming times for Train-To-Trackside applications.
- Improvements for seamless handover when roaming together with PRP (Parallel Redundancy Protocol).
- Devices with a name longer than 16 characters are now correctly displayed in the web search.
- With the cli command „show script error“, it is now possible to show errors in an applied script.
- Client-Binding is supported when load balancing is used.
- For new access points the state of the certificate is now displayed in CAPWAP.
- The length of the device name is extended up to 64 characters.
- Automatic configuration synchronization between BAT-Controller.

Security

- WIDS Intruder Identification for improved identification of an intruder inside the WLAN.
- WIDS configuration rollout with BAT-Controller.
- For the TLS/SSL certificates a unique RSA key is generated after a reset of the BAT.
- SCEP is extended by the AES-192, AES-256, SHA-256, SHA-384 und SHA-512 algorithms.
- The BAT offers now the possibility to save the configuration in an encrypted format on the PC.

System

- HiLCOS 9.10 supports the brand new BAT450 hardware.

8. Improvements in Version 9.00.5112-RU1

WLAN

- Improved stability of WPA1 connections
- Improved reliability and monitoring of AP - Client connections
- Configuration of Client-Bridge support on OpenBAT-Client devices
- Improved configuration and management of Public-Spot User Accounts
- Improved stability when configuring the WLC SCEP-Client

Network connectivity

- Improved stability of PRP connections
- Improved stability of the IP-Router
- Improved stability when handling SNMP packets

Security

- Improved security of devices with default configuration by using device specific default SSL/TLS keys
- A status object is added to display the use of Default-Passwords

System

- Improved device handling with the fix of the following problem: With a firmware Up- or Downgrade to HiLCOS 9.00-Rel the device LEDs might be turned off. The LEDs can be turned back on by manually switching off and on the corresponding setting.



The **Hirschmann™** BAT Operating System

9. Comments

If you want to upgrade the firmware of your device to a new version, please install the latest LANconfig version first. **Before running the firmware-upload, you should save the OpenBAT configuration to a file.** After that, you can use LANconfig to load the latest HiLCOS-version into the device.