

APPLICATION NOTE

How to configure CBB Roaming

July 2025

Content

1.	Introduction.....	3
2.	Requirements	4
3.	Roaming Limitation	4
4.	Connect Before Break Concept	5
5.	Connect Before Break Details.....	6
5.1	Improvements.....	6
5.2	Time Chart	6
5.3	Connect Before Break Process	7
5.3.1	Initial state	7
5.3.2	Scanning.....	7
5.3.3	Association of client 2	8
5.3.4	Switch between radio cards.....	8
5.3.5	Network convergence.....	9
5.3.6	Final state.....	9
6.	Roaming basic parameters	10
7.	Roaming advanced parameters.....	10
8.	Wi-Fi Client settings.....	11
9.	Connect Before Break configuration	11
9.1	CBB in Bridged Mode.....	13
9.2	CBB in Router Mode	16
10.	Logs	18
11.	CBB Connectivity Troubleshooting	20
	Verify Interface Status	20
	Analyze Wireless Activity	20
	Run a Site Survey	22
	Additional recommendations.....	22

1. Introduction

The purpose of this document is to explain the concept of the ACKSYS *Connect Before Break* (CBB) functionality and guide you in configuring your ACKSYS product in client mode with CBB.

Roaming occurs when a wireless client device moves out of the usable range of one wireless access point (AP) and connects to another AP typically one with a stronger signal.

Roaming happens in three main steps:

Scanning

The Wi-Fi client sends a probe request for a specific SSID, and nearby access points respond with probe replies. The client builds a list of APs along with their signal strengths. The selection of the best AP is based on:

- SSID match
- Security compatibility
- Signal strength

The AP with the highest signal strength that meets SSID and security criteria is selected.

Authentication & Association

The client sends an authentication request to the selected AP and waits for a response. Upon successful authentication, it sends an association request. Once associated, the new AP informs the old AP with a disassociation packet to update routing tables.

Convergence

The client finalizes the handoff by re-associating with the new AP. The network updates are triggered, completing the handover process.

Note: Even with two radio cards, conventional roaming causes a brief disconnection while switching APs. This can result in packet loss, especially during high-throughput data transfers.

To address this, ACKSYS developed a proprietary roaming mode, **Connect Before Break** that minimizes packet loss, even in high-speed environments.

2. Requirements

To illustrate **CBB** we will take the example of train-to-ground communication, but it can be used in many other environments (cable car, shuttle, AGV...).

Requirements for this use case:

- RailBox dual radio cards or any ACKSYS Dual Radio
- 2 antennas pointing to the same direction (1 antenna per radio card)
- The TX signal power must be the same for each antenna and radio-frequency cable
- No discontinuity in Wi-Fi coverage on ground, and the minimum power must be sufficient to transfer data

To ensure 0.1% packet loss error ratio, you must also verify:

- No ACI (adjacent channel interference)
- No CCI (co-channel interference)

All APs on the trackside must be bridged (Layer 2) together.

3. Roaming Limitation

There are different types of roaming:

- Reactive roaming,
- Proactive roaming in mono radio mode,
- Proactive roaming in dual radio mode.

Reactive roaming is the default roaming in WiFi, as per the standard. It starts scanning only upon the current AP is lost.

Limitation: This is not efficient and causes high packet loss.

Application: WiFi clients roaming rarely from AP to AP

Proactive roaming in mono radio mode allows channel scanning while the client is associated to an AP. It's not waiting for the AP loss to start the scanning process. So, this is an improvement in comparison to the standard.

Limitation: the data flow is still regularly interrupted by the scan process and the change of AP.

Application: This roaming type is suited for not critical mobility applications and low packets loss for urban mobility.

Proactive roaming in dual radio mode allows to start the scan process on a separate WiFi radio. This will free up the first WiFi radio which only processes user data. Scanning card collects information in regards to the best surrounding AP's. Data card switches to the elected AP when suited.

Limitation: the data flow is still regularly interrupted by the change of AP.

Application: This roaming type is suited for not critical mobility applications with very low packets loss ratio.

None of these roaming types is suitable for high speed mobility and critical applications.

Objective: establish a reliable train to ground communication, with a bandwidth of 500Mb/s at 350km/h

4. Connect Before Break Concept

Proprietary type of roaming developed by ACKSYS:

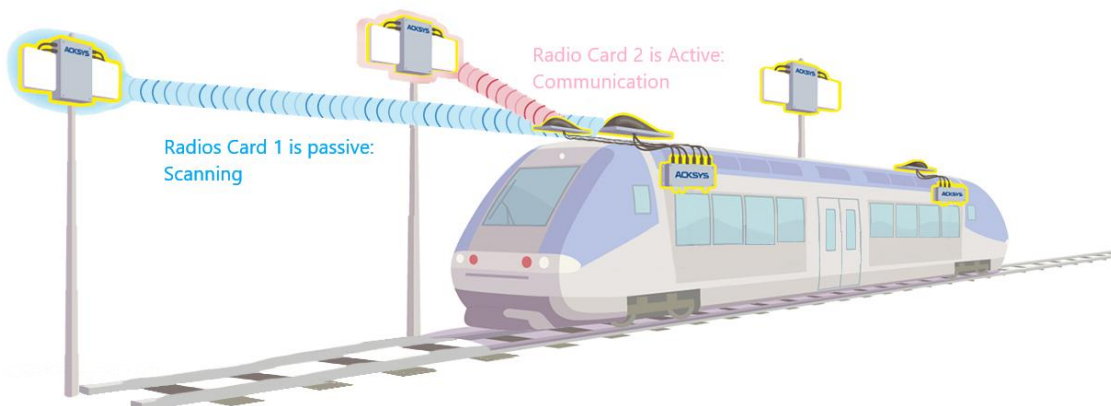
- Requires 2 radios, one radio scans while the other one transfers data
- The 2 Wi-Fi clients alternatively transfer data and scan (switches role from 'scan' to 'data transfer').

To reach 0 packet loss, we ensure there is always 1 radio connected to the new AP, while the other card is disconnecting from the old AP.

The card transferring data is called "active radio" and is connected to the best AP. The other card is scanning and is called "passive" radio and is connected to the next best AP.



1. On the active radio, the signal level of the current AP drops below the roaming threshold, and enter in 'need roam' status
2. If the passive radio has a better signal level meeting the roaming criteria,
 - ⇒ The passive radio moves to active
 - ⇒ The active card
 - moves to passive mode
 - is still associated to the old AP
 - keeps sending and receiving packets from the ground until convergence of the network to the new AP
3. The new active card sends Gratuitous ARP (GARP) frames to converge the network
4. Then the active card leaves the current AP and starts scanning (as passive card)



5. Connect Before Break Details

5.1 Improvements

Connect Before Break (CBB) is an improved dual client proactive roaming. The 2 clients execute alternatively data communication or scan.

Those 2 clients can be either on the same radio or on 2 separate radios. In case of 2 separate radios, multi-channel roaming can be supported.

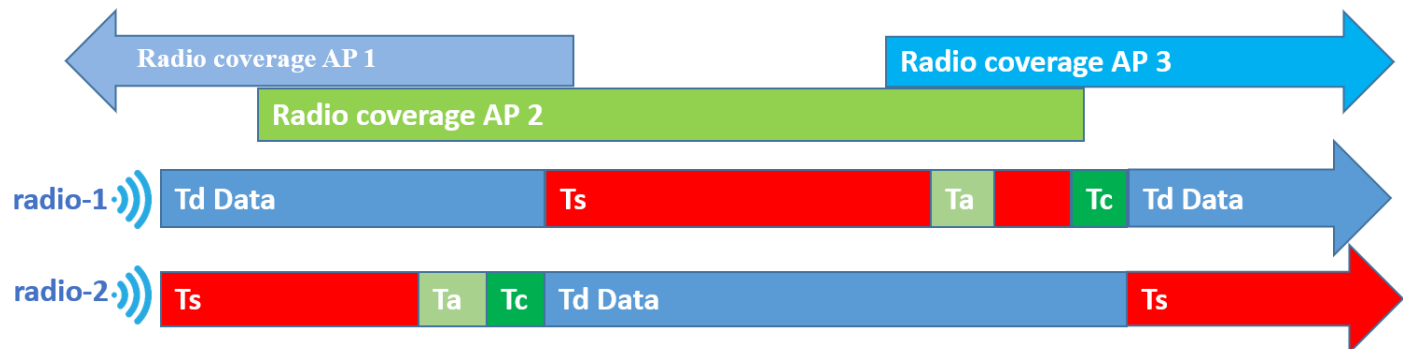
The AP change has minimal impact on data flow (and packet loss) as it is not anymore handled by the client owning the data session but by the one doing the scanning.

When thresholds are met, the scanning client stops scanning and associates to the newly elected AP. Data flow is switched between the 2 clients: scanning client becomes data handling client and data handling client starts scanning and associating to the next best AP.

This roaming type is suited for high to very high mobility use-cases.

5.2 Time Chart

Alternatively, Client 1 and Client 2 are sending data or are scanning:



Where:

- **Td:** sending data period
- **Ts:** scanning period
- **Ta:** association period (depends on security algorithms used)
- **Tc:** convergence time (depends on ground network)
- **Th:** handover duration = **Tc**

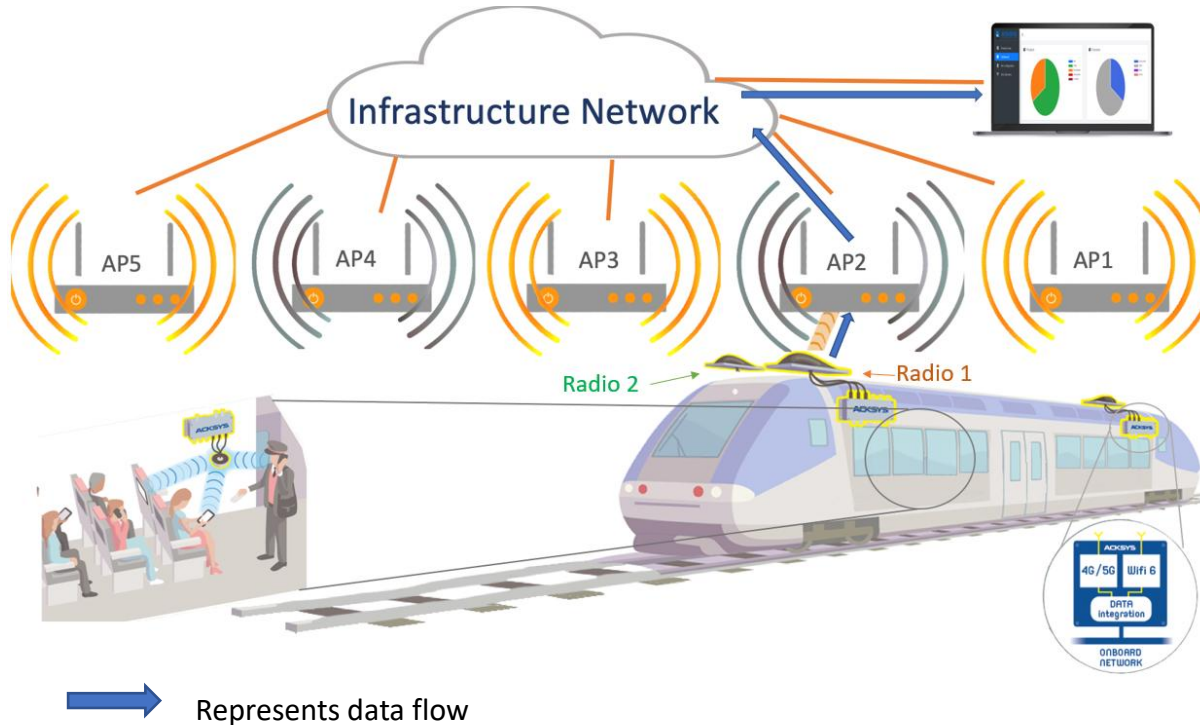
Roaming (and convergence) is triggered by the gratuitous ARP sent from the device to the new AP (and underlying switch).

In case of CBB, association and roaming (convergence) are not following each other, unlike in previous roaming types. This allows to remove Ta time from Th, and is the improvement brought by the Connect Before Break solution.

5.3 Connect Before Break Process

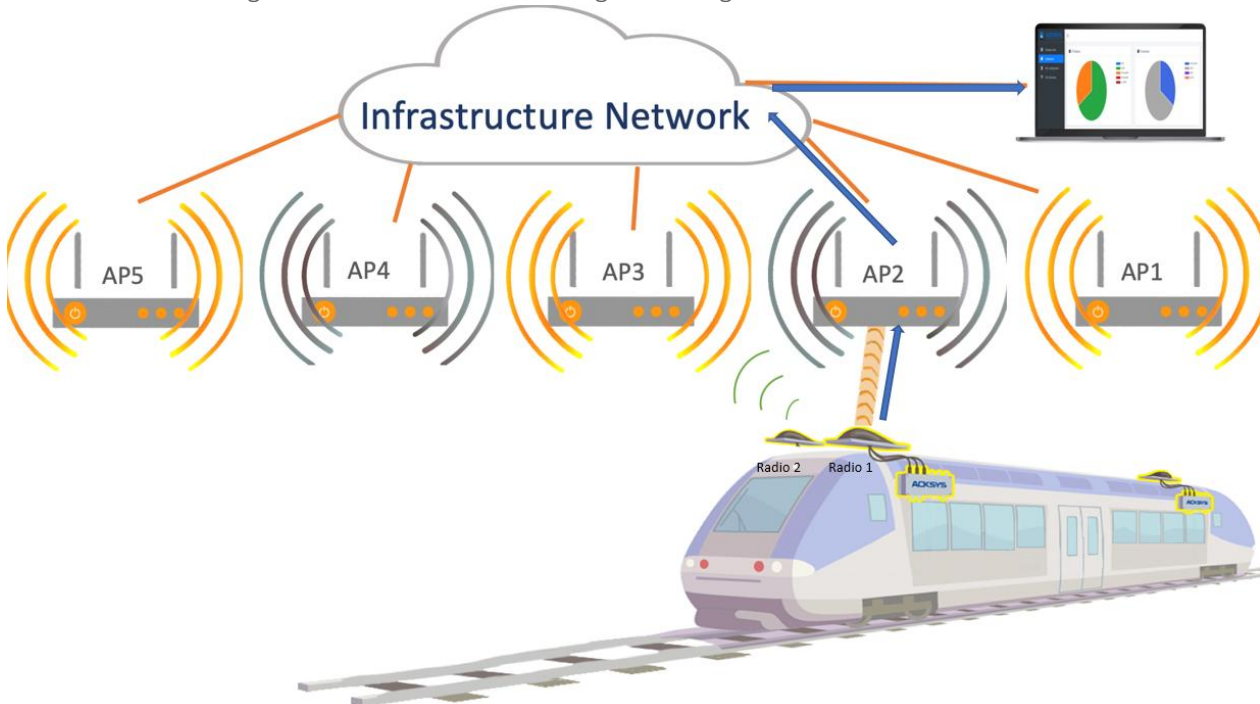
5.3.1 Initial state

All the data are sent by the first radio card.



5.3.2 Scanning

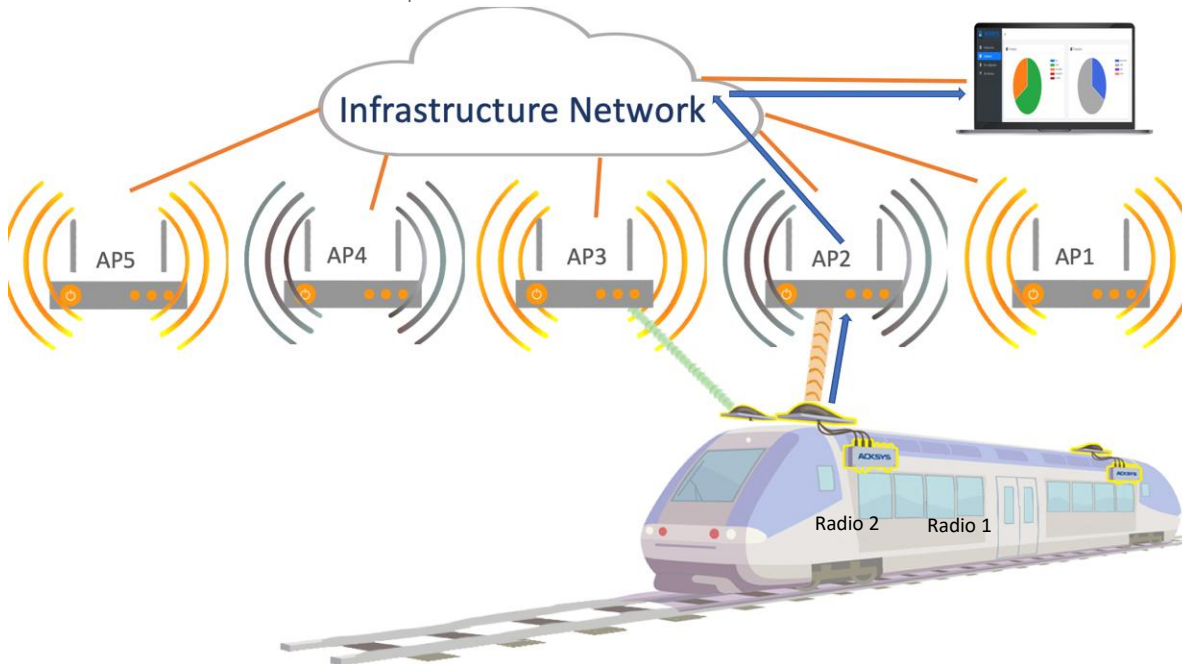
As the train is moving the 2nd radio card is scanning for an eligible AP.



5.3.3 Association of client 2

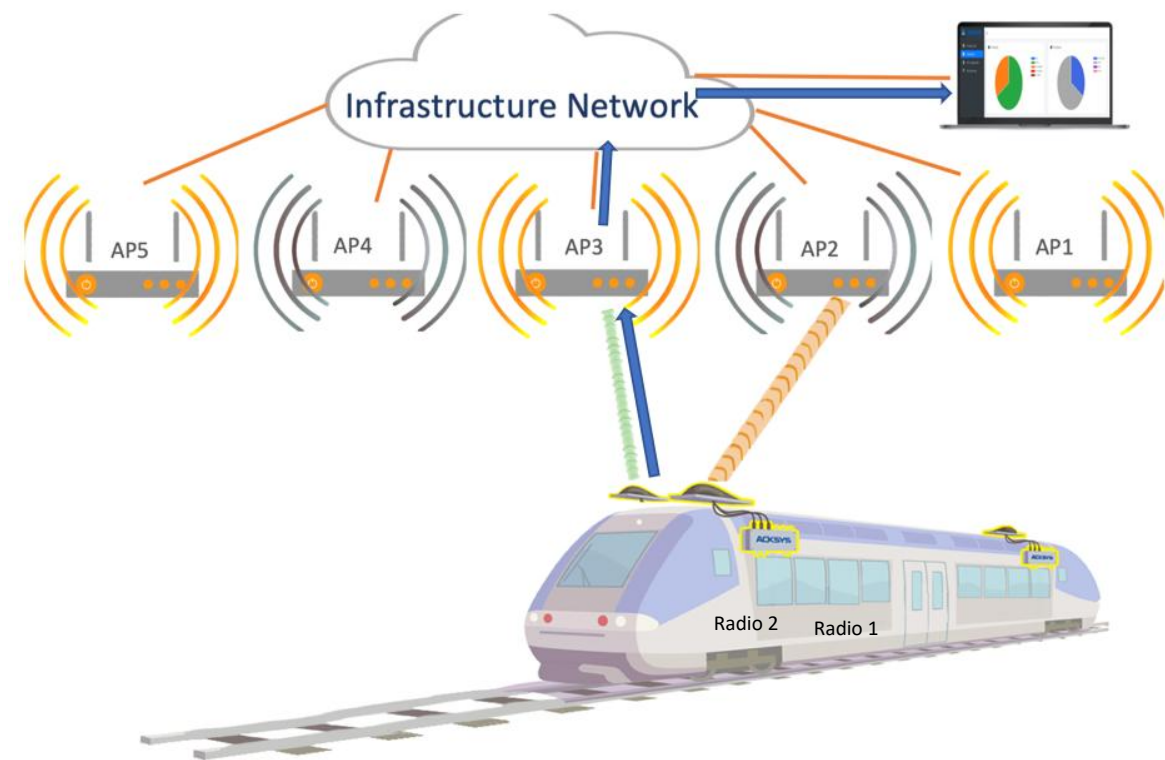
The 2nd radio card associates to the next available AP. Scanning on radio 2 results in election of AP3, and association to AP3.

Data flow on radio 1 is not interrupted.

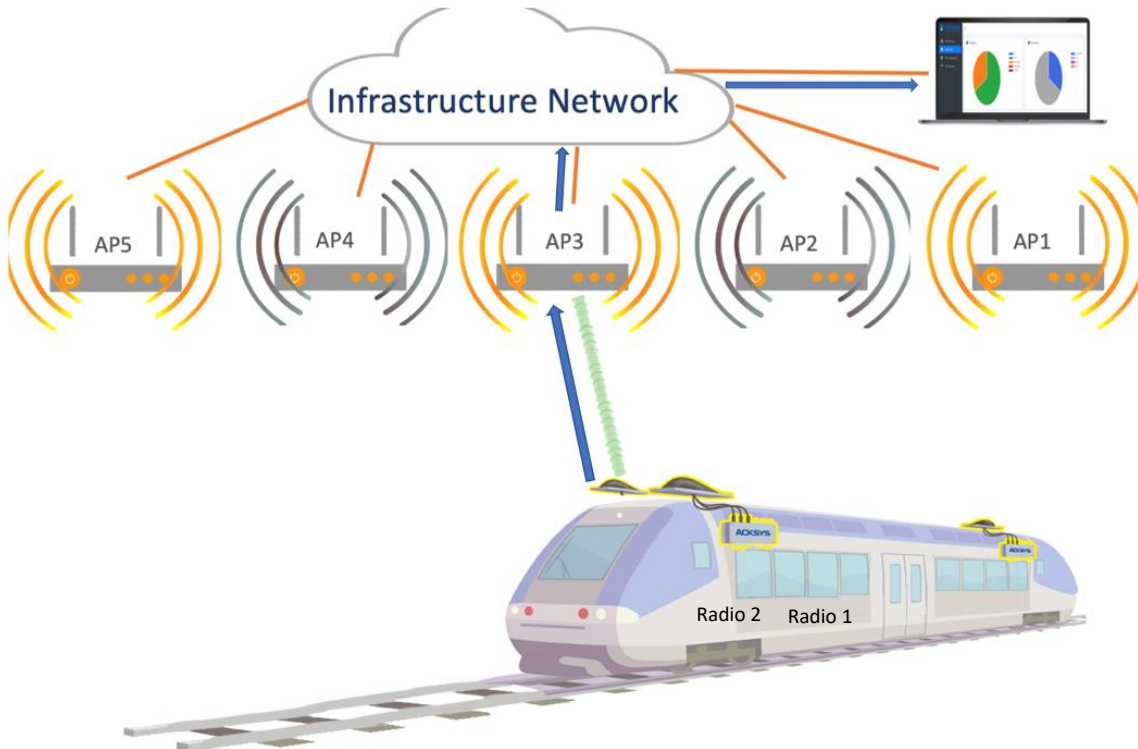


5.3.4 Switch between radio cards

Data are sent via the radio 2.

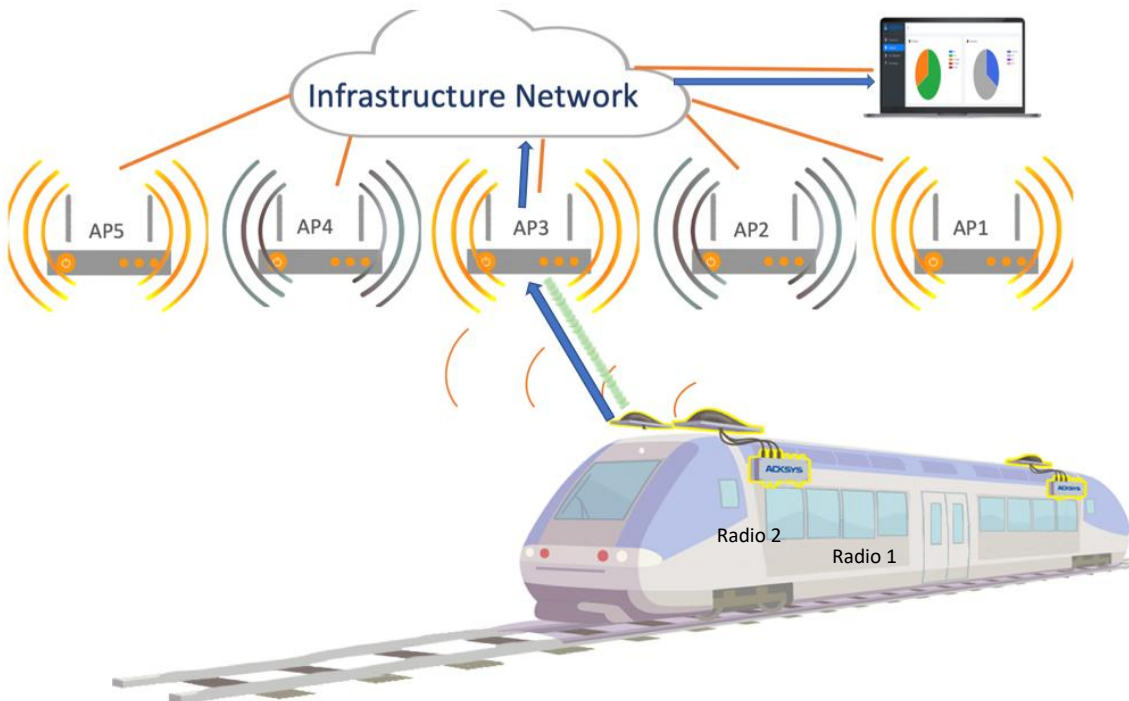


5.3.5 Network convergence



Convergence is terminated. Gratuitous ARP are sent to infrastructure network to update the MAC tables.

5.3.6 Final state



Scanning is done now by Radio 1 with no impact on radio 2 data flow.

6. Roaming basic parameters

Scan parameters:

- List of channels to scan,
- Time between two scans (parameter C),
- Level of current AP above which no scanning needed.

Conditions to select the candidate AP:

- Minimum: minimum signal level to analyze candidate,
- Boost: signal improvement to be brought by candidate AP.

Conditions to leave current AP for candidate AP:

- Leave threshold: signal below which current AP will be left.

7. Roaming advanced parameters

Stability parameter:

- Hysteresis: threshold measurement tolerance.

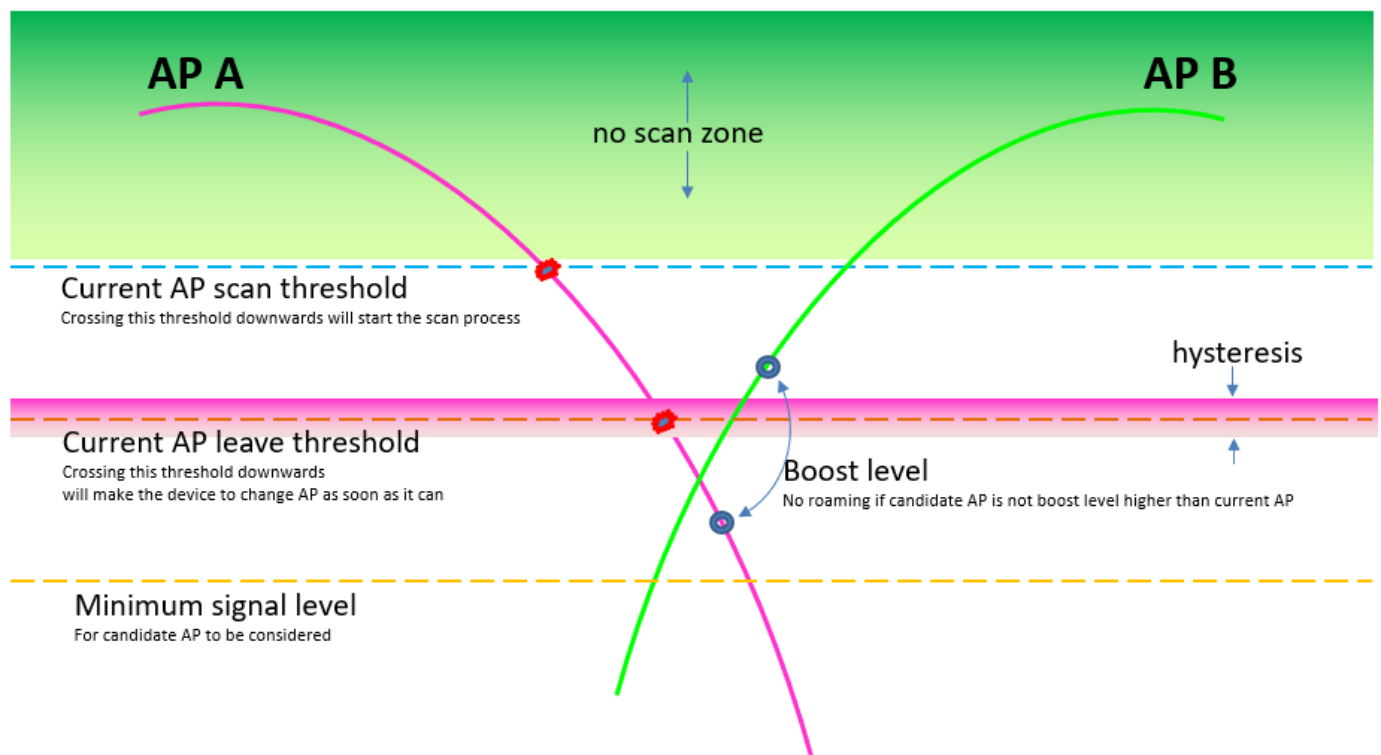
Candidate AP parameters:

- Maximum: maximum signal level to analyze candidate AP,
- No-return delay: minimum delay before returning to an already used AP.

Conditions to leave current AP for the candidate AP:

- Minimum delay between two roamings,
- Signal thresholds,
- RSSI smoothing factor (weighing importance of latest beacons vs older ones),
- Number of lost beacons.

Roaming sequence:



⇒ **Performances achieved:**

- Packet loss magnitude order: < 0,1% at 350km/h
- not dependent of speed
- not dependent of throughput

8. Wi-Fi Client settings

For this example, we will use the following parameters:

- Bridge client mode (no routing)
- 802.11ac using channels 36, 40 & 44
- SSID: AcksysRBB
- No security
- Roaming delay between scans = 2 seconds
- Roaming leave threshold = -75 dB
- Interface Wi-Fi 1 used for data



NOTE: Please note that when the Wi-Fi client is in bridge mode, the **Connect Before Break** can be used only with Acksys WaveOS products as Access points. To use Access Points from other brands, your client must be configured as a NAT router.

9. Connect Before Break configuration

In SETUP/PHYSICAL INTERFACES, set the RADIO CLUSTER to *Group for connect before break* and press



PHYSICAL INTERFACES

WIFI 1

WIFI 2

LAN 1

LAN 2

VIRTUAL INTERFACES

NETWORK

VPN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

SETUP

TOOLS

STATUS

WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

Combination	Channel selection		Max number of interfaces			
	Multiplicity	Can use DFS	Access point	Infrastructure client	Mesh point	Ad-hoc
Multiple access points	single, auto, multiple	yes	8			
Client / bridge	single, auto, multiple, roaming*	yes		1		
SRCC	single	yes	auto	auto		
Other / Ad-hoc	single	no			unsupported	unsupported

When using several roles, they all use the same shared channel; in this case, the client role must not be set to multichannel roaming.
Repeater mode is a combination of two roles: access point + client.

* The roaming feature is not yet available for IEEE802.11ac cards.

WI-FI INTERFACE

Wifi 1: Wi-Fi 5 (Dual band)

CHANNEL

802.11 MODE

SSID

ROLE

SECURITY

ACTIONS

36 40 44

802.11ac+n

acksys

Client (infrastructure)

none

Wifi 2: Wi-Fi 5 (Dual band)

CHANNEL

802.11 MODE

SSID

ROLE

SECURITY

ACTIONS

Automatic

802.11ac+n

acksys

Access Point (infrastructure)

none

Interface disabled

GLOBAL PARAMETERS

RADIO REGULATION AREA

Country

United States

RADIO CLUSTER

Cluster mode

Do not group

Group for scanning

Group for connect before break

Do not group

Save & Apply

Save

Copyright © 2025 ACKSYS Communications & Systems. All rights reserved.

11

The choice of the initial primary interface has, in most cases, no effect on the operation since it's a temporary state. The WiFi 1 interface is selected by default as the primary card. **This is the configuration we will use for this example.**

RADIO CLUSTER	
Cluster mode	Group for connect before break ▼
Primary data card	<input checked="" type="radio"/> WiFi 1 <input type="radio"/> WiFi 2
Secondary data card	<input type="radio"/> WiFi 1 <input checked="" type="radio"/> WiFi 2




For your information, please note that you can also choose to use only one radio card for both functions. In the following example, the Connect before break client is defined only on WiFi1, and WiFi2 can be used for another purpose. **Beware: this implies that you can use only one radio channel!**

RADIO CLUSTER	
Cluster mode	Group for connect before break ▼
Primary data card	<input checked="" type="radio"/> WiFi 1 <input type="radio"/> WiFi 2
Secondary data card	<input checked="" type="radio"/> WiFi 1 <input type="radio"/> WiFi 2

If your product only has one radio card, of course you have no choice: both functions, scanning and data exchange, are handled by the same radio interface, **and you can scan only one channel**

RADIO CLUSTER	
Cluster mode	Group for connect before break ▼
Primary data card	<input checked="" type="radio"/> WiFi
Secondary data card	<input checked="" type="radio"/> WiFi

After saving this page, edit the Wi-Fi interface

WI-FI INTERFACE						
	WiFi 1: Wi-Fi 5 (Dual band)					<input checked="" type="checkbox"/>
	CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
	36 40 44	802.11ac+n	Acksys	Client (infrastructure)	none	 

[Edit this network](#)

Give a name to the *bond interface* (here we choose *Roaming*), and change the Wi-Fi settings according to your needs.

SETUP

TOOLS

STATUS

WIRELESS SETTINGS : WIFI 1

The *Device Configuration* section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the *Interface Configuration*.

If *SRCC* role is selected, most of the *Device Configuration* is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION

General Setup

a/b/g Data Rates

Advanced Settings

802.11 mode

802.11ac+n (5 GHz)

Changing the mode may affect the list in the 'a/b/g data rates' tab

HT mode

20MHz for 802.11ac

Automatic 40MHz HT mode is not compatible with AP, Ad-hoc, Mesh and multi-interfaces

Automatic channel select

☐

Automatic channel select is not compatible with Ad-hoc, Mesh and multi-interfaces

Channel

BEWARE : Multi-channel selection is possible only with double-radio products

36 (5.180 GHz) - Max Tx power 23 dBm

40 (5.200 GHz) - Max Tx power 23 dBm

44 (5.220 GHz) - Max Tx power 23 dBm

48 (5.240 GHz) - Max Tx power 23 dBm

52 (5.260 GHz) - Max Tx power 23 dBm (DFS)

56 (5.280 GHz) - Max Tx power 23 dBm (DFS)

The Max Tx Power mentioned is the legal limit for the selected country, it may be higher than the effective maximum power that can be provided by the radio card

This field is ignored in client proactive roaming mode; see 'Roaming' tab instead

INTERFACE CONFIGURATION

General Setup

Wireless Security

Advanced Settings

Roaming

Advanced Roaming

Frame filters

Role

Client (infrastructure)

Multiple ESSIDs

☐

ESSID

AcksysRBB

bond interface

create bond interface: Roaming

The cluster mode "roaming before break" require a bonding to work

Back to Overview

Reset

Save

Save & Apply

9.1 CBB in Bridged Mode

In the advanced settings, select *4 addresses format (WDS)*. Caution: this implies the exclusive use of WaveOS Acksys access points.

INTERFACE CONFIGURATION

General Setup

Wireless Security

Advanced Settings

Roaming

Frame filters

Bridging mode

ARP NAT (pseudo L2 NAT)

ARP NAT (pseudo L2 NAT)

4 addresses format (WDS)

Wired device cloning (only one)

Profinet device cloning (only one)

Deauthenticate before roaming to next AP

Do not cache old scan results

Back to Overview

Reset

Save

Save & Apply

In the Roaming tab, select *Enable proactive roaming*

INTERFACE CONFIGURATION

General Setup
Wireless Security
Advanced Settings
Roaming
Frame filters

When Proactive Roaming is disabled, the device will scan the general channels selection configured above.

When Proactive Roaming is enabled, its suboption 'list of channels scanned' will supersede the general channels selection above.

DFS channels are subject to passive scans.

Enable proactive roaming
☐

If unchecked, the device will not roam until it loses its current AP

Back to Overview
Reset
Save
Save & Apply

Set your roaming parameters, then

Save & Apply

INTERFACE CONFIGURATION

General Setup
Wireless Security
Advanced Settings
Roaming
Advanced Roaming
Frame filters

When Proactive Roaming is disabled, the device will scan the general channels selection configured above.

When Proactive Roaming is enabled, its suboption 'list of channels scanned' will supersede the general channels selection above.

DFS channels are subject to passive scans.

Enable proactive roaming
☒

If unchecked, the device will not roam until it loses its current AP

List of channels scanned for the next AP discovery

BEWARE : Multi-channel selection is possible only with double-radio products

36 (5.180 GHz)
40 (5.200 GHz)
44 (5.220 GHz)
48 (5.240 GHz)
52 (5.260 GHz) (DFS)
56 (5.280 GHz) (DFS)

If no channel is selected, the scan list is the complete list of available channels

In 802.11n HT mode 40MHz, if the primary channel of the AP is not fixed, you will have to select both the primary and secondary channels

Delay between two successive scan cycles
2000

Value in milliseconds, e.g. "10000". Must be greater than 0

Current AP leave threshold
-75

Value in dBm, e.g. "-80". Below (worse than) this value, the device will try to use another AP

Required level boost
6

Roaming occurs only if the candidate signal level is above the current AP's plus this value

Current AP scan threshold
0

Value in dBm, e.g. "-40". Above (better than) this value, the device will stop scanning. Set to 0 to scan unconditionally. Incompatible with the Maximum signal level option

Minimum signal level
0

In dBm, e.g. "-75". 0 to disable. Roaming won't occur if the candidate signal is below this level. Association is still possible if no other AP is available

Back to Overview
Reset
Save
Save & Apply

Edit your main Network (default name is [LAN](#))

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

LAN

VPN

BRIDGING

ROUTING / FIREWALL

QOS


SERVICES


SETUP

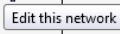
TOOLS

STATUS

NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	<input checked="" type="checkbox"/>	192.168.15.116	255.255.255.0		Default	

 Add network

 Edit this network

Include the [Roaming](#) bond interface into the bridge, then

 Save & Apply

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

LAN

ROAMING

VPN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

SETUP

TOOLS

STATUS

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

General Setup

Interfaces Settings

Advanced Settings

Bridge interfaces

☒ creates a bridge over specified interface(s)

Enable STP/RSTP

☐ Enables the Spanning Tree Protocol on this bridge

WARNING: Some cautions must be taken with wireless interfaces, please see user guide

Enable LLDP forwarding

☐ Enables the LLDP frame forwarding.

bridge VLAN

☐ Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)

Interface

☐ WiFi adapter: WiFi 2 - AcksysRBB (bond: Roaming)
 ☐ WiFi adapter: WiFi 1 - AcksysRBB (bond: Roaming)
 ☒ Bond virtual interface: Roaming
 ☒ Ethernet adapter: LAN 1 (network: lan)
 ☒ Ethernet adapter: LAN 2 (network: lan)

MTU


1500


IP ALIASES


NATed VRRP networks warning
The following applies to NATed networks which use the VRRP protocol:


- Public-side NAT MUST NOT define IP aliases; else the NAT might use the alias IP as public address instead of the VRRP IP
- Conversely, Private-side NAT SHOULD define a private IP alias to allow connection tracking replication

This section contains no values yet

 Add

 Reset

 Save

 Save & Apply

9.2 CBB in Router Mode

In router mode, we will configure two distinct network zones, one dedicated to the LAN interface and another for the WiFi interface.

In the advanced settings, select *4 addresses format (WDS) in case of AP are ACKSYS or ArpNet for any other AP Vendor.*

INTERFACE CONFIGURATION

General Setup
Wireless Security
Advanced Settings
Roaming
Advanced Roaming
Frame filters

Bridging mode
ARP NAT (pseudo L2 NAT)
Allows to set the bridging method. Applied only if this interface is added in a bridge

Deauthenticate before roaming to next AP
Optional. When ON, the previous AP stops transmission immediately, saving up bandwidth. When OFF, let more time for the AP controller to manager handover.

Do not cache old scan results
When scanning for APs, ignore those APs found prior to the last scan pass.

Multiple connection failures watchdog
0
Delay (seconds) before sanitary reboot after repeated failed connection attempts to all legitimate APs around. Leave empty or zero to disable.

Edit your main Network (default name is *LAN*)

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES
VIRTUAL INTERFACES
NETWORK
LAN
VPN
BRIDGING
ROUTING / FIREWALL
QOS
SERVICES

NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	<input checked="" type="checkbox"/>	192.168.15.116	255.255.255.0		Default	Edit this network

Add network

Exclude the *Roaming* bond interface into the bridge, then save

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Bridge interfaces
creates a bridge over specified interface(s)

Enable STP/RSTP
Enables the Spanning Tree Protocol on this bridge
WARNING: Some cautions must be taken with wireless interfaces, please see user guide

Enable LLDP forwarding
Enables the LLDP frame forwarding.

bridge VLAN
Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)

Interface
WiFi adapter: WiFi 2 - AcksysRBB (bond: Roaming)
WiFi adapter: WiFi 1 - AcksysRBB (bond: Roaming)
Bond virtual interface: Roaming (network: lan)
Ethernet adapter: LAN1 (network: LAN)
Ethernet adapter: LAN2 (network: LAN)

MTU
1500

We will create another Network, WAN and associate its to the Bond Interface not in the Bridge

NETWORK - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Bridge interfaces
☐ ? creates a bridge over specified interface(s)





Interface


☐ WiFi adapter: WiFi 2 - AcksysRBB (bond: Roaming)
☐ WiFi adapter: WiFi 1 - AcksysRBB (bond: Roaming)
☒ Bond virtual interface: Roaming (network: net1)
☐ Ethernet adapter: LAN1 (network: LAN)
☐ Ethernet adapter: LAN2 (network: LAN)

MTU

2 Network OverView





NETWORK OVERVIEW


NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LAN	<input checked="" type="checkbox"/>			192.168.16.116	255.255.255.0		Default	 
WAN	<input checked="" type="checkbox"/>			192.168.15.116	255.255.255.0		Default	 

 Add network

2 Network Zones OverView

NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
zone_LAN	"LAN"	zone_WAN	<input type="checkbox"/>	All enabled	 
zone_WAN	"WAN"	-	<input checked="" type="checkbox"/>	All enabled	 

 Add zone


Your product is now ready for a fast and efficient roaming, without loss of packets during the handover


SETUP
TOOLS
STATUS

DEVICE INFO
NETWORK
WIRELESS
ASSOC STATIONS
CHANNEL STATUS
MESH SURVEY
SERVICES STATUS
SITE SURVEY
SRCC STATUS
SERVICES
LOGS

ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WiFi 1	AcksysRBB	Infrastructure	C4:93:00:0C:50:20	40	-36 dBm	-103 dBm	67 dB

 Reset

10. Logs

Specific logs are raised during the roaming process.

First enable these logs in TOOLS / LOGS SETTINGS, and in WIRELESS CLIENT LOG SETTINGS, select Roaming level:

SETUP

TOOLS

STATUS

FIRMWARE UPGRADE

PASSWORD SETTINGS

SYSTEM

NETWORK

SAVE CONFIG / RESET

LOG SETTINGS

LOG SETTINGS

You can configure the log parameters on this page.

General settings:
This section is about configuring the system log, which filters and and dispatches the log messages to the user.
The "System Log Output Level" acts as a final filter for the log messages from various components. Set it to the highest level you want to see from any component. So, please make sure the system log output level is high enough to display all required messages.

Wireless log settings:
These sections configure wireless logging for access points and clients. The messages are sent to the system log.

VRRP service log settings:
This section configures logging of VRRP activities. Messages are sent to the system log.

GENERAL SETTINGS

System Log Output Level	Notice
System Log Buffer Size	16 <small>kiB</small>
External System Log Server	192.168.1.130
External System Log Server Port	514

WIRELESS CLIENT LOG SETTINGS (ALL INTERFACES)

Wireless Log Level	Roaming (System log \geq Notice)
--------------------	------------------------------------

The corresponding required System Log Output Level is shown in parenthesis.
Furthermore, the roaming level requires extra configuration in Advanced Roaming parameters.

Then in SETUP / PHYSICAL INTERFACE / WIFI / Advanced Roaming, select which information you want to log:

Roaming log info

☒ Display scan process while associated
☒ Display scan process while un-associated
☒ Display best bssid selection comparison
☒ Display roaming parameters
☒ Log filtered table of APs used to select the best AP (limited to line buffer available space)
☒ Include unfiltered APs in the above table (show all APs seen)
☒ Display reasons for filtering out APs at INFO level instead of DEBUG
☒ Display roaming state changes

Select the roaming log info will show in product log.

To show the log you must set the wireless client log level to roaming or more and general log level to notice or more in 'log settings' section.

When a wireless client transitions (roams) from one access point (AP) to another within the same network, the system automatically records this event in the roaming logs. Each roaming instance generates corresponding log entries that capture relevant details such as the timestamp, source and destination APs, client MAC address, and signal strength metrics.

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

SERVICES

LOGS

SYSTEM LOG

KERNEL LOG

ROAMING LOG

CONFIG LOG

CLIENT ROAMING LOG

For meaningful logs, please enable the following:

- General log at "Notice" level with sufficient buffer size,
- Wireless client log at "Roaming" level,
- For the relevant Wireless client, set Roaming log info to "Dump AP table..."

Warning:

- Take care to enable only one client log at a time. Else all client logs will be mixed up here.
- Remember that log files are not preserved over reboots.

Download as plain log file

Download as tabbed file

Mon	Jan	10	12:23:11	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-101	1	[00:09:90:01:4f:dc]	-30-101	1	/
Mon	Jan	10	12:23:21	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	/00:09:90:01:4f:dc/	-21-102	1	/
Mon	Jan	10	12:23:31	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	[00:09:90:01:4f:dc]	-30-102	1	/
Mon	Jan	10	12:23:41	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	/00:09:90:01:4f:dc/	-21-102	1	/
Mon	Jan	10	12:23:51	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-30-101	1	*
Mon	Jan	10	12:24:02	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	[00:09:90:01:4f:dc]	-30-102	1	*
Mon	Jan	10	12:24:12	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	[00:09:90:01:4f:dc]	-29-102	1	/
Mon	Jan	10	12:24:22	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-30-101	1	/
Mon	Jan	10	12:24:32	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-102	1	/00:09:90:01:4f:dc/	-30-102	1	/
Mon	Jan	10	12:24:42	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-31-101	1	*
Mon	Jan	10	12:24:52	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-102	1	[00:09:90:01:4f:dc]	-29-102	1	/
Mon	Jan	10	12:25:02	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	/00:09:90:01:4f:dc/	-29-102	1	/
Mon	Jan	10	12:25:13	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	[00:09:90:01:4f:dc]	-30-102	1	*
Mon	Jan	10	12:25:23	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-30-101	1	/
Mon	Jan	10	12:25:33	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-102	1	/00:09:90:01:4f:dc/	-29-102	1	/
Mon	Jan	10	12:25:43	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-30-101	1	*
Mon	Jan	10	12:25:53	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-30-102	1	[00:09:90:01:4f:dc]	-30-102	1	/
Mon	Jan	10	12:26:03	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-31-101	1	*
Mon	Jan	10	12:26:13	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-29-102	1	[00:09:90:01:4f:dc]	-22-102	1	*
Mon	Jan	10	12:26:24	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-101	1	[00:09:90:01:4f:dc]	-29-101	1	/
Mon	Jan	10	12:26:34	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-102	1	[00:09:90:01:4f:dc]	-22-102	1	*
Mon	Jan	10	12:26:44	2022	daemon.notice	wpa_supplicant[7573]:	BG wlan0	/00:09:90:01:4f:dc/	-31-102	1	/00:09:90:01:4f:dc/	-29-102	1	*

These logs are useful for monitoring client mobility, troubleshooting connectivity issues, and optimizing wireless coverage in System Logs:

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

SERVICES

LOGS

SYSTEM LOG

KERNEL LOG

ROAMING LOG

CONFIG LOG

SYSTEM LOG

Save logs to file

```

j): send NTP request (timeout 10s, try 0/5)
j): Set date to Mon Jan 10 15:21:08 2022 CET
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-14 qual=0 noise=-101
BG wlan0 [00:09:90:01:4f:dc] -28-102 1 |00:09:90:01:4f:dc/ -27-102 1 |*04:f0:21:1b:77:77* -14-101 6 |/20:9a:7d:88:01:86/ -85-102
wlan0: bgscan acksys_notify_scan: last:-26 current:00:09:90:01:4f:dc[-28] best:04:f0:21:1b:77:77[-14]
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-14 qual=0 noise=-101
BG wlan0 [00:09:90:01:4f:dc] -19-102 1 |00:09:90:01:4f:dc/ -18-102 1 |*04:f0:21:1b:77:77* -14-101 6 |/04:f0:21:22:9b:26/ -76-101
wlan0: bgscan acksys_notify_scan: last:-25 current:00:09:90:01:4f:dc[-19] best:04:f0:21:1b:77:77[-14]
telemetry: New connection saved in position [0].
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-23 qual=0 noise=-101
BG wlan0 /00:09:90:01:4f:dc/ -28-101 1 |00:09:90:01:4f:dc/ -27-101 1 |*04:f0:21:1b:77:77* -23-101 6 |
wlan0: bgscan acksys_notify_scan: last:-27 current:00:09:90:01:4f:dc[-28] best:04:f0:21:1b:77:77[-23]
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-14 qual=0 noise=-101
BG wlan0 [00:09:90:01:4f:dc] -29-101 1 |00:09:90:01:4f:dc/ -28-101 1 |*04:f0:21:1b:77:77* -14-101 6 |
wlan0: bgscan acksys_notify_scan: last:-26 current:00:09:90:01:4f:dc[-29] best:04:f0:21:1b:77:77[-14]
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-14 qual=0 noise=-101
BG wlan0 [00:09:90:01:4f:dc] -30-103 1 |00:09:90:01:4f:dc/ -19-103 1 |*04:f0:21:1b:77:77* -14-101 6 |/04:f0:21:22:9b:26/ -76-101
wlan0: bgscan acksys_notify_scan: last:-26 current:00:09:90:01:4f:dc[-30] best:04:f0:21:1b:77:77[-14]
# 9594 cmd /usr/sbin/ack_service/ack_service_check
# 9595 cmd /usr/sbin/acksys_telemetry_check
wlan0: bgscan acksys: scan result notification, state=SCANNING
wlan0: wlan0: scan_acksys_is_best: compare best & bssid=04:f0:21:1b:77:77 level=-14 qual=0 noise=-101

```

11. CBB Connectivity Troubleshooting

Verify Interface Status

In the event of a malfunction, begin by checking the [STATUS / Network](#) page to ensure that all network interfaces are properly mounted and recognized.

SETUP TOOLS STATUS						
DEVICE INFO						
NETWORK						
BRIDGES						
MULTICAST ROUTES						
ROUTES						
WIRELESS						
SERVICES						
LOGS						

INTERFACES						
BOND1						
BOND VIRTUAL DEVICE						
IP CONFIGURATION						
not configured						
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	WiFi 2	04:f0:21:28:ad:dc	0	0	Role: Transparent client (infrastructure) SSID: AcksysRBB Channel: Automatic	1500
	WiFi 1	04:f0:21:28:ad:db	556023	588491	Role: Transparent client (infrastructure) SSID: AcksysRBB Channel: 40	1500

LAN						
IP CONFIGURATION						
IPv4: 192.168.15.16 Netmask: 24 MTU: 1500						
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	bond1	0a:8b:7a:32:07:01	556023	588491	N/A	1500
	LAN 1	00:09:90:00:71:32	5776630	3197548	Negotiated 1000 baseTX FD, link ok	1500
	LAN 2	00:09:90:00:71:33	0	0	no link	1500

Analyze Wireless Activity

In the event of a malfunction, begin by checking the [STATUS / Network](#) page to ensure that all network interfaces are properly mounted and recognized.

The [STATUS / WIRELESS / ASSOCIATED STATIONS](#) and the [STATUS / WIRELESS / SERVICES STATUS](#) pages provide valuable insights, particularly an instant overview of the radio interfaces' status, allowing you to determine which interface is active and which is passive.

For example:

- If **no station is associated** and both radio interfaces are in **scanning** mode, it indicates that the client has not yet discovered any access point. In such cases, we recommend performing a **site survey** to verify the presence of access points configured with the expected parameters (SSID, radio channel, security mode, etc.).

SETUP TOOLS STATUS								
DEVICE INFO								
NETWORK								
WIRELESS								
ASSOC STATIONS								
CHANNEL STATUS								
MESH SURVEY								
SERVICES STATUS								
SITE SURVEY								
SRCC STATUS								
SERVICES								
LOGS								

ASSOCIATED STATIONS								
ASSOCIATED STATIONS RESULTS : 0								
GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	-	-	-	-	-	-	-	-

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

SERVICES STATUS

WIFI 1

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	N.A	04:f0:21:28:ad:db	SCANNING	N.A	N.A	N.A	N.A

WIFI 2

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	N.A	04:f0:21:28:ad:dc	SCANNING	N.A	N.A	N.A	N.A

- If **WiFi1** is connected while **WiFi2** is still scanning, it means the first interface has established a connection, while the second is still searching for a secondary access point.

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WiFi 1	AcksysRBB	Infrastructure	C4:93:00:0C:50:20	40	-36 dBm	-103 dBm	67 dB

Reset

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

SERVICES STATUS

WIFI 1

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	AcksysRBB	04:f0:21:28:ad:db	COMPLETED	40	5200 MHz	20 MHz	HT20

WIFI 2

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	N.A	04:f0:21:28:ad:dc	SCANNING	N.A	N.A	N.A	N.A

- When **WiFi2** successfully connects, both interfaces are associated, ensuring optimal redundancy or load balancing.

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

SERVICES STATUS

WIFI 1

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	AcksysRBB	04:f0:21:28:ad:db	COMPLETED	40	5200 MHz	20 MHz	HT20

WIFI 2

SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Client	AcksysRBB	04:f0:21:28:ad:dc	COMPLETED	44	5220 MHz	20 MHz	HT20

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 2

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WiFi 1	AcksysRBB	Infrastructure	C4:93:00:0C:50:20	40	-39 dBm	-103 dBm	64 dB
	WiFi 2	AcksysRBB	Infrastructure	C4:93:00:08:A0:76	44	-64 dBm	-105 dBm	41 dB

Run a Site Survey

If the product fails to detect any access point, you can initiate a **site survey** to identify which APs are visible to the device. If no Access Points are detected, this may indicate an issue with the **antennas** or the **radio module**. If access points are detected, verify that the **SSID**, **frequency**, and **security settings** are correctly aligned with the client's configuration:

SETUP

TOOLS

STATUS

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

CHANNEL STATUS

MESH SURVEY

SERVICES STATUS

SITE SURVEY

SRCC STATUS

SERVICES

LOGS

SITE SURVEY

Wireless Environment Survey

Radio under test

WiFi 1

Scan Radio

- When the radio card is in *client mode*, and a list of channels is selected, the survey includes **these channels only**.
- When the radio card is in *access point mode*, the scan will **disconnect** associated clients. On DFS channels, CAC will be re-performed if required.
- When the radio card is in *802.11s mesh mode*, peers seldom appear because their beacon interval is large per the protocol definition.

WiFi 1 : SCAN RESULTS PER BAND

2.4 GHz

5 GHz

Access Point Scan Result

WiFi 1 : SCAN RESULTS DETAILS

2.4 GHz - 5 GHz

NAME	CHANNEL	BANDWIDTH	ROLE	BSSID	ENCRYPTION	SIGNAL	
hidden	36	40 MHz	Access Point	04:F0:21:42:02:29	WPA2 PSK	-87 dBm	
AcksysRBB	44	20 MHz	Access Point	C4:93:00:08:A0:76	None	-38 dBm	Join

Additional recommendations

For better WIFI connectivity troubleshooting, please :

- Ensure APs are broadcasting the correct SSID.
- Check signal strength and noise levels using a spectrum analysis tool if needed.
- Make sure firmware and configuration are up to date on both the client and AP.

Support : <https://support.acksys.fr>