Zebra Wireless Insights

Analysis Use Cases for Aruba UXI

White Paper

MN-005054-01 Rev A

Copyright

2024/07/08

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Introduction

This White Paper presents analysis use cases of Wireless Insights data from Zebra's Enterprise Mobile Computing devices, integrated in the HPE Aruba User Experience Insight (UXI) system and cloud dashboard.

These scenarios depict device deployments serving enterprise user applications within the Wi-Fi ecosystem. Each case describes thorough monitoring and analysis of device Wi-Fi connectivity health and data visibility, and offers root causes of issues and action items for solutions.

Zebra's underlying Wireless Insights features analyze Wi-Fi data in real-time directly on the devices and report the outcome to the integrated system (HPE Aruba UXI in this case), which provides system administrators with insights about the Wi-Fi ecosystem.

For detailed Wireless Insights features go to https://www.zebra.com/us/en/support-downloads/software/productivity-apps/wireless-insights.html, and for HPE Aruba UXI enablement described in this paper go to https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/%20user-experience-insight-agent-for-zebra/

For a broader scope of Zebra Wireless Software Solutions go to https://www.zebra.com/us/en/software/mobile-computer-software/mobility-dna-wireless.html

Voice Performance Assessment

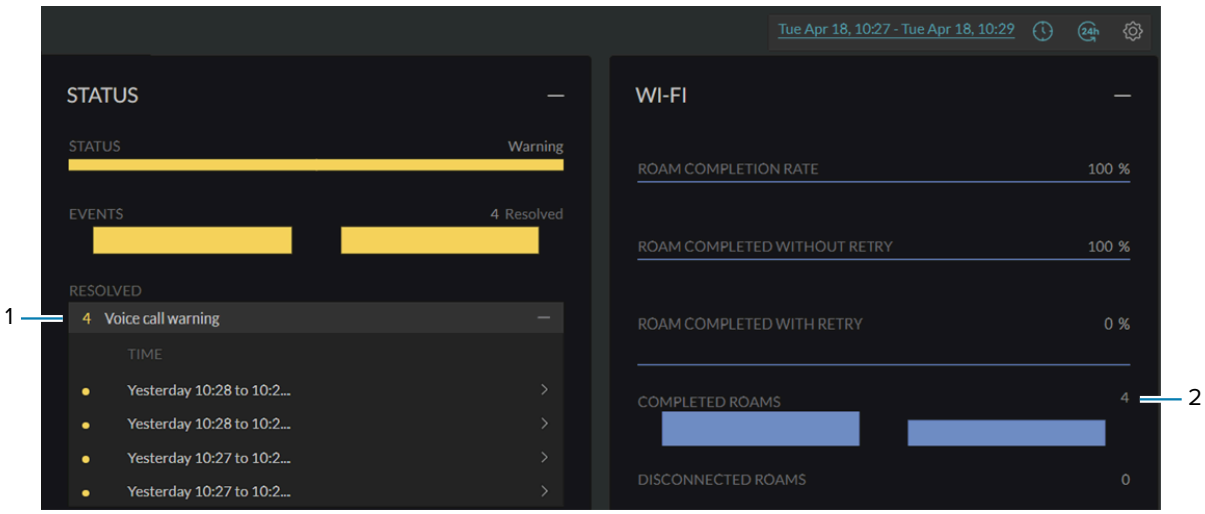
This use case deploys a voice application on Zebra devices in a Wi-Fi network. The deployment is experiencing persistent voice quality issues.

The UXI system administrator is either monitoring specific voice metrics, or end-users are experiencing voice quality issues such as glitchy audio, choppiness, and missing syllables/words. Because these issues are persistent, the entire Wi-Fi environment must be reassessed for voice quality readiness.

Analyzing Voice Quality Issues

The administrator discovers that in the given period, while a particular device user is moving, all Wi-Fi roams are completed successfully with no reported **Roam Failed** or **Retry** event. However, a **Voice call warning** event occurs at the exact time of the roam instance.

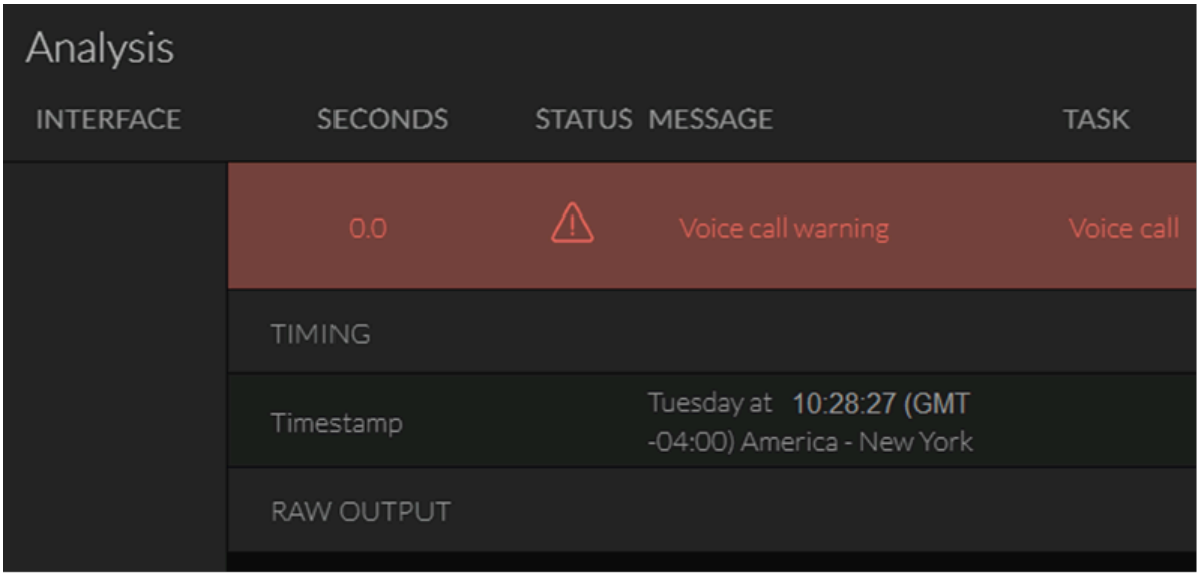
The following screen depicts a 3-minute call (10:27 to 10:29) resulting in four perfect roams, all with indications of **Voice call warning**.



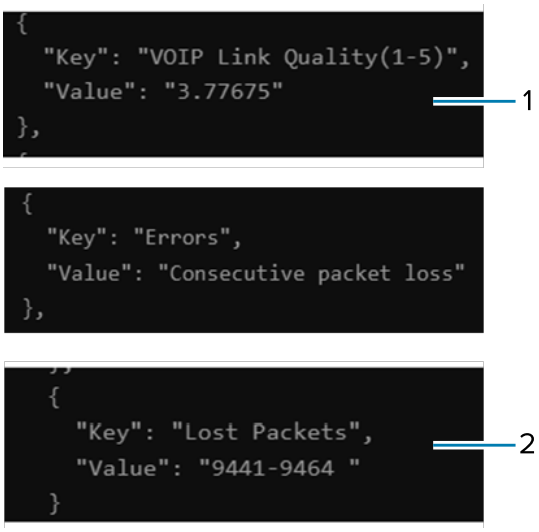
1	4 voice call warnings with event times listed. Expand to view details.
2	4 roams, 100% completed without retry.

Expand each **Voice call warning** to note specific characteristics of the voice quality problems.

- **VOIP Link Quality** (Voice over IP link quality), a standard scale of audio Mean Opinion Score (MOS) of 1 to 5, is less than 4. Wireless Insights calculates this value for small slices of the voice call, with focus on short periods over roam events. An MOS value less than 4 is concerning.
- Consecutive packet loss is more than 20, and in other instances it is similar or larger (worse). 20+ consecutive packets missing in short roaming periods is concerning.



Select the warning to view the RAW OUTPUT.



1	MOS = 3.77, less than 4
2	23 consecutive packets lost

In this example, the issue is affecting the overall user experience of audio quality, loss of syllables/words, and choppiness. Users may not have noticed this yet, or not reported it, or reported it only on a small scale.

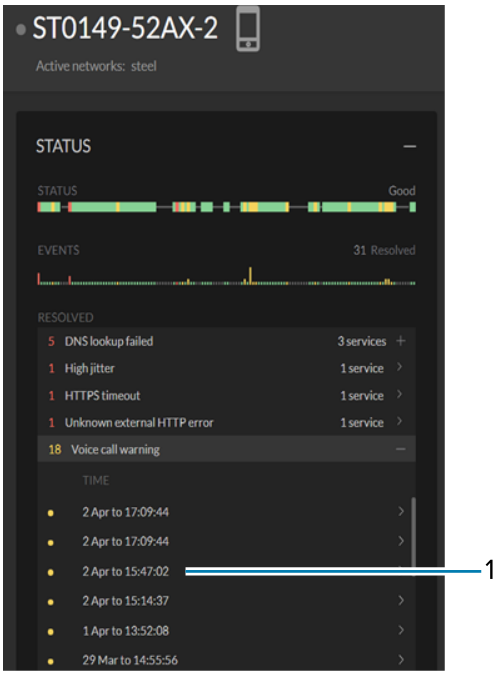
Diagnosis and Corrective Action

The administrator must immediately evaluate the scale and severity of this issue in regard to pervasiveness throughout the organization, via addressing questions such as:

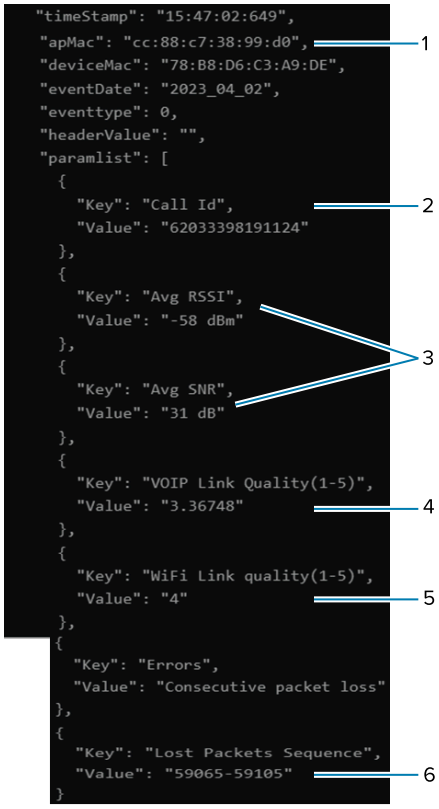
- How many other devices have similar quality issues?
- Which device types are experiencing the issues, and what software version are they running?
- In how many stores or regions do the issues occur?
- Do the issues occur within a specific characteristic of WLAN RF environment, or independent of the environment?
- Do the issues occur during a specific time of the day (rush hour)?

The quality issues here occur in environmental conditions not specific to certain areas inside stores, to certain AP(s) or other RF variables, or to type of call (within the store or via cell phone outdoors).

For the device in sample **Store #149**, select timestamp **2 Apr to 15:47:02** (1).

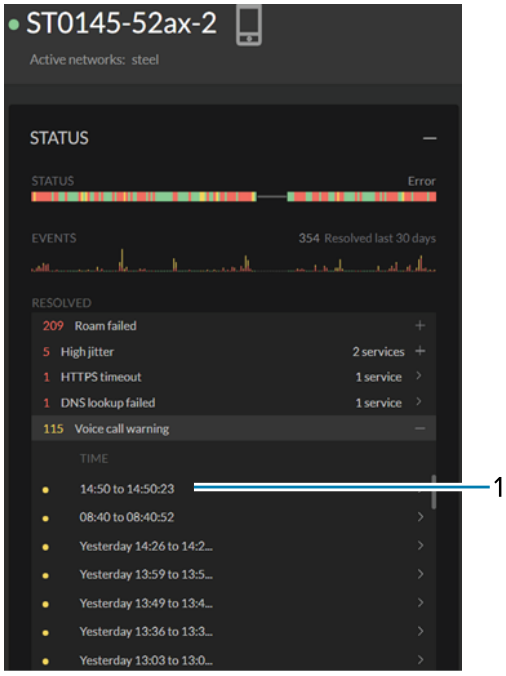


The following screen depicts device performance at that specific time.

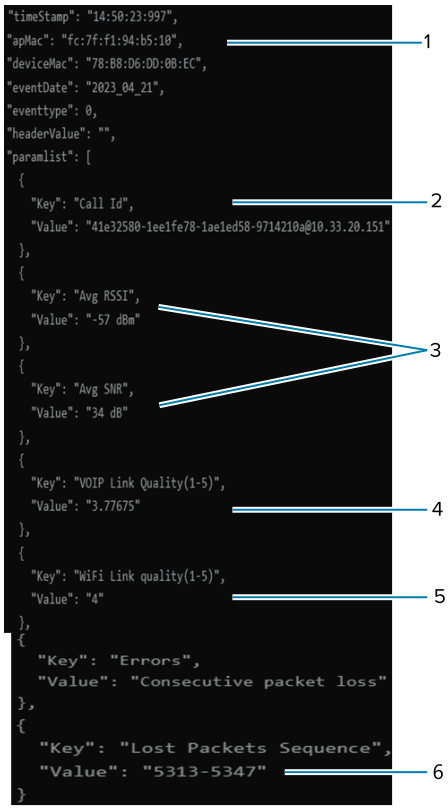


1	AP (any in store)
2	Any Call ID
3	Reasonable RSSI and SNR
4	MOS = 3.36
5	Good Wi-Fi link quality
6	40 consecutive packets lost

For the device in sample **Store #145**, select timestamp **14:50 to 14:50:23** (1).



The following screen depicts device performance at that specific time.



1	AP (any in store)
2	Any Call ID

3	Reasonable RSSI and SNR
4	MOS = 3.77
5	Good Wi-Fi link quality
6	34 consecutive packets lost

The analysis characteristics and metrics indicate a larger network problem not related to device roaming performance or WLAN AP functionality, but rather to the wired network distributed system, such as switches and routers. Investigation and isolation of such issues are typically less complex than the effort for wireless.

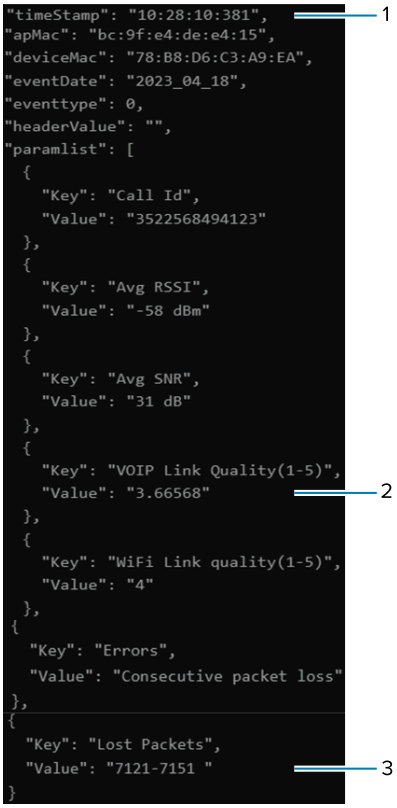
In this use case, the switch vendor quickly diagnosed and corrected the issue using vendor-proprietary debugging procedures and tools.

Validating the Solution

The administrator must now validate this solution logically and efficiently and can do this remotely.

In the following example, the administrator remotely monitors local end-user associates using devices in production or tech support personnel to obtain test results for steps 1 and 3 in the following procedure.

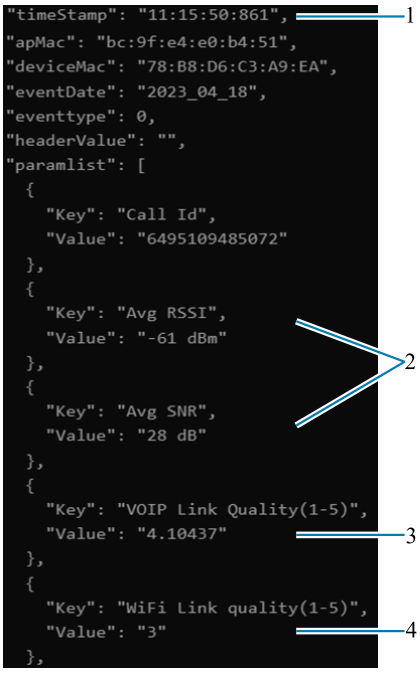
1. If possible, reproduce the issue before applying the network correction to obtain fresh data.



1	Time before fix is applied
2	MOS is 3.66

3	30 consecutive packets lost

2. Apply the network correction.
3. Re-test the network.



1	Time after fix is applied
2	Worse RSSI and SNR
3	MOS is 4.1
4	Worse Wi-Fi link quality, no error of consecutive packets lost

Step 3 results confirm the network correction resolved the issue. For a few more days, the administrator can continue to monitor the issue in more end-user devices and stores where the correction is applied.

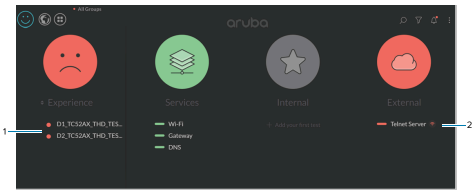
Because of the logical characteristics of the issue (each roam had intrusive packet loss shown in the metrics and leading to audio interruption), the administrator can quickly validate the correction remotely.

Poor Application Performance in Specific Areas

In this use case, UXI system monitoring reports bad signals (RSSI) for devices in specific areas, and/or end-users are experiencing application sluggishness and disconnections in a few specific locations.

The application in this example, Telnet, is sensitive to packet loss and delays, meaning the Telnet session is easily impacted by traffic impairment. The UXI system administrator has automated a pre-configured Service & App Test of an external service to monitor the real Telnet Server livelihood, or is establishing a new test due to user complaints of Telnet disconnection errors.

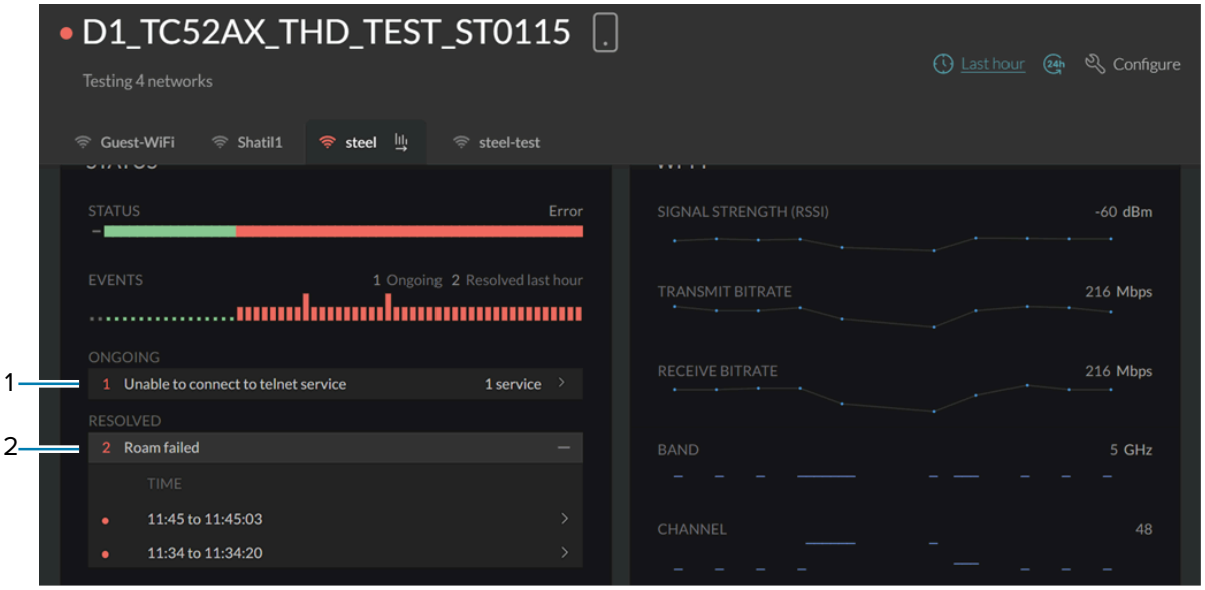
The following UXI screen illustrates this test failing for two devices.



1	Two devices with red indications
2	Telnet Server test fails

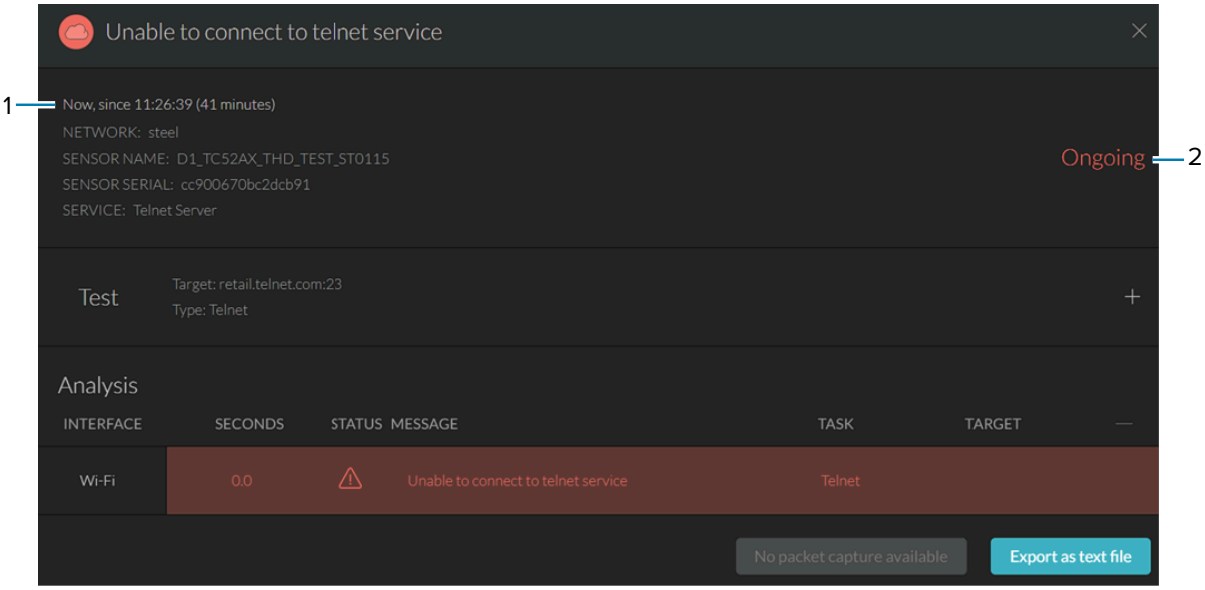
Diagnosis

Select one of the failed devices. The following screen indicates the cause of the issue is **Unable to connect to telnet service**. Note that this coincides with **Roam failed** events around the same time.



1	**Unable to connect to telnet service** issue is ongoing
2	**Roam failed** events during that time

Select the event under **ONGOING** to view the Telnet failure details.



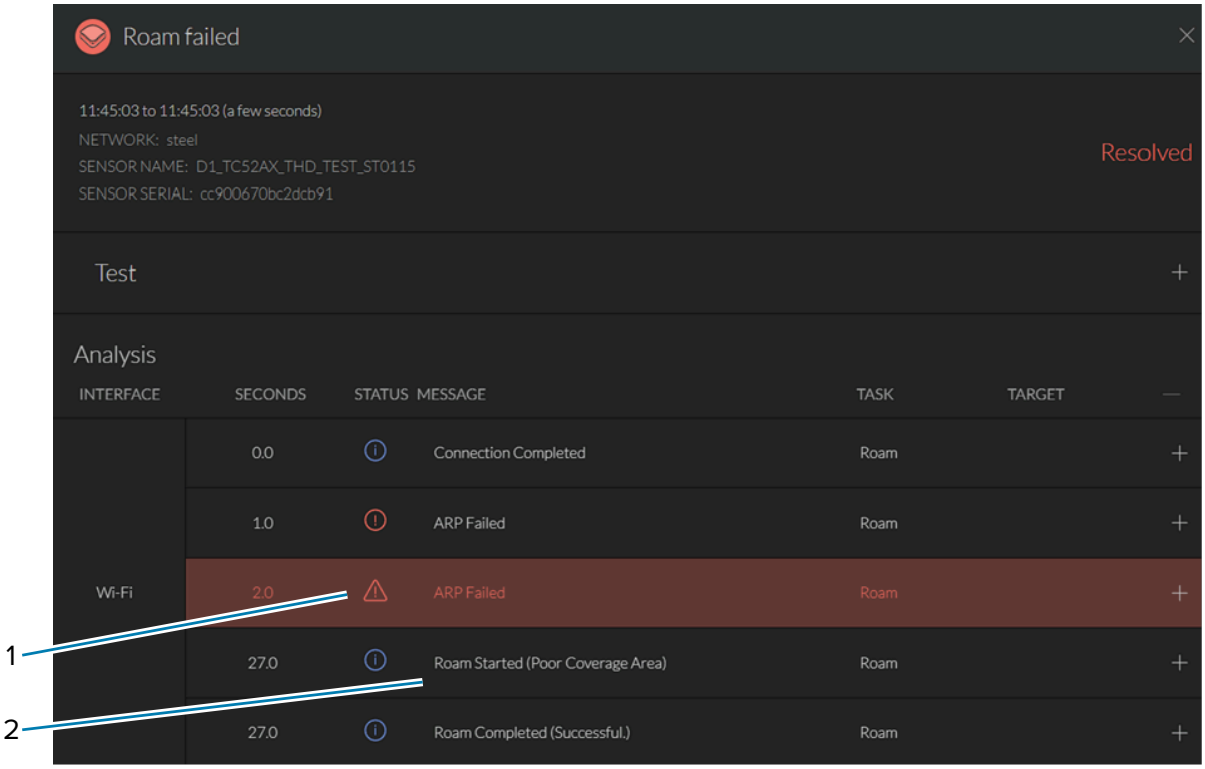
1	Time when problem was detected
2	Still ongoing

Return to the listed events and select one of the **Roam failed** instances.

The following screen shows that within the period of this instance, the device attempts to roam (to a better AP) due to a **Poor Coverage Area** caused by a poor signal combined with poor traffic (packets) performance, which can occur even during a period of successful connection.

Note that shortly prior to the roam, a **Connection Completed** event was followed by **ARP Failed**. This is another indication that in the same area, while the Wi-Fi connection is maintained, the ARP packet exchange with the network fails, corresponding to Telnet failing to send or receive data packets during very poor coverage.

Lastly, there is no evidence of a problem with the roam's 802.11 management packets between the device and the AP, indicating that the roam occurred due to poor coverage, but was able to complete successfully with no issues. The problem is due to Layer 3 data packets.

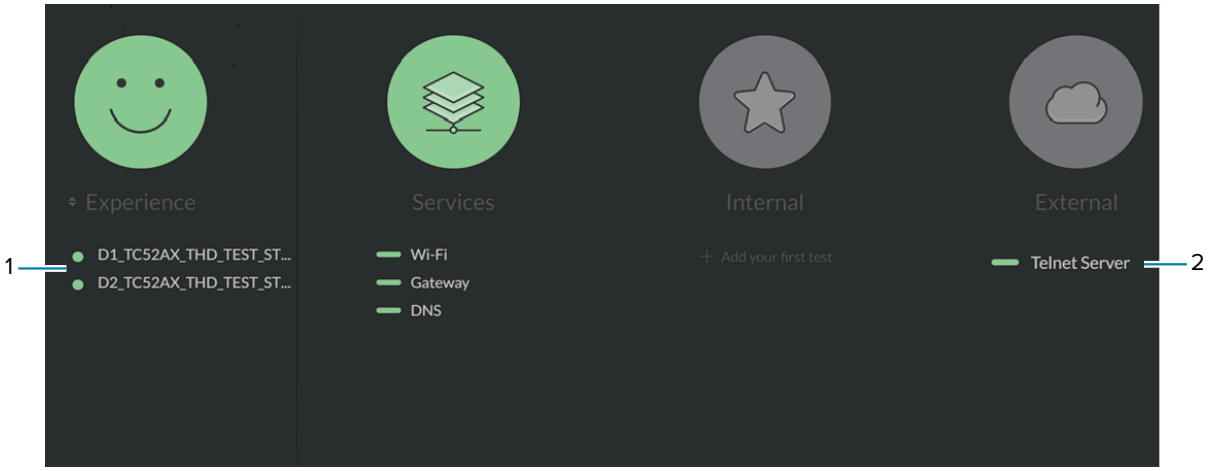


1	**ARP Failed** while the device is connected.
2	The device tries to roam again to another AP due to the **Poor Coverage Area**. The device shows **Roam Completed (Successful)** but the new AP also creates a **Poor Coverage Area** condition (not shown), indicating the problem is recurring.

Corrective Action

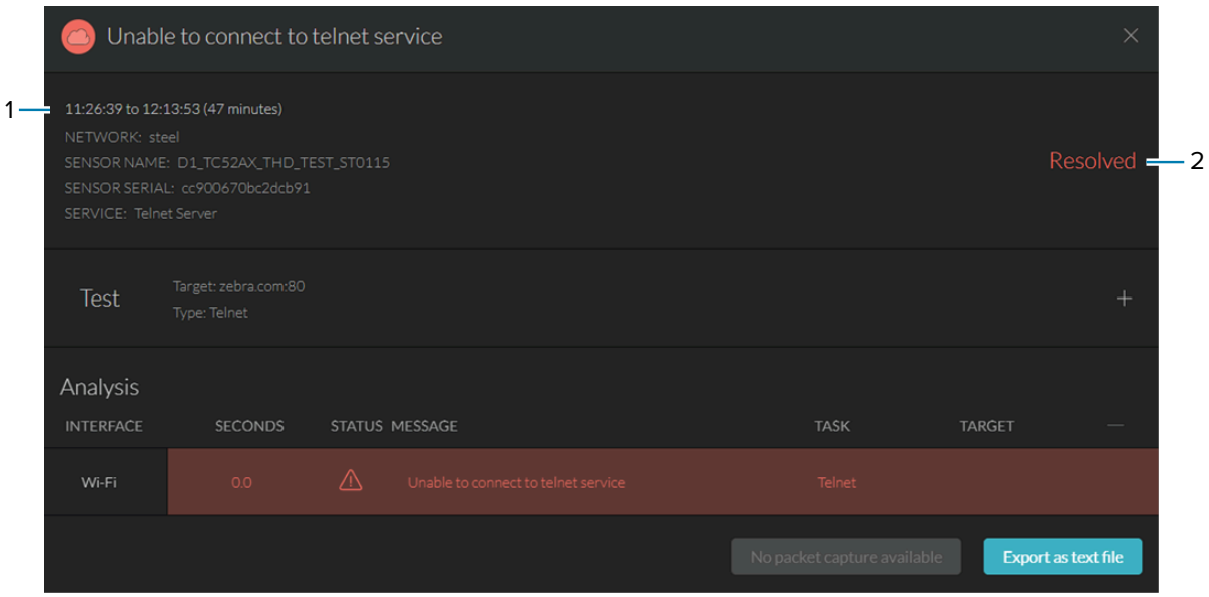
The root cause of this issue is a large Wi-Fi coverage gap in that location. The WLAN administrator should address this deficiency by deploying additional AP(s) in poor coverage areas, and/or correct the AP beaconing transmit power to increase AP RF cell sizes.

After mitigation, the administrator monitors the UXI to verify user devices roaming in that location no longer experience Telnet server test issues or roam failures, as in the following screen.



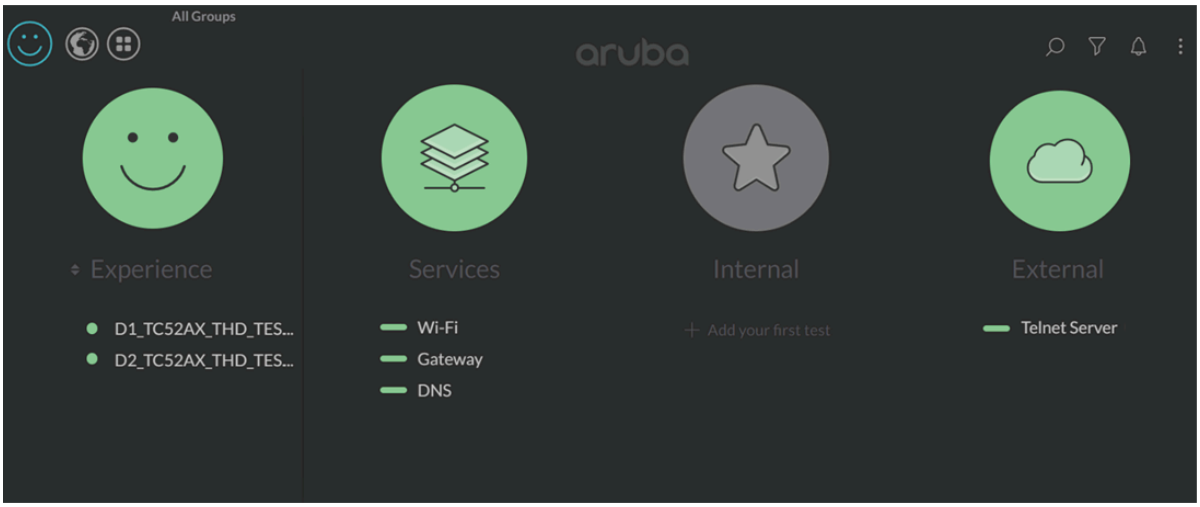
1	Same devices are both green
2	Telnet Server test passes

Select one of the devices previously showing ongoing failure to view the current Telnet test status.



1	Time original issue began, and after mitigation
2	Moved to **Resolved**

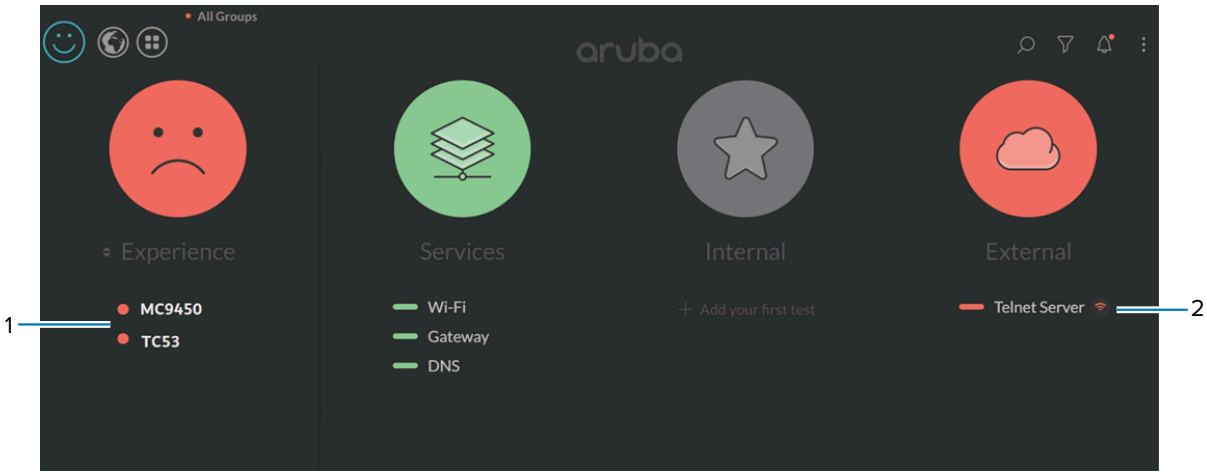
The main screen validates that the overall state over time remains stable.


All Groups
aruba
Experience
D1_TC52AX_THD_TES...
D2_TC52AX_THD_TES...
Services
Wi-Fi
Gateway
DNS
Internal
Add your first test
External
Telnet Server

Application Disconnections During Good Wi-Fi Coverage

In this use case there is good RF coverage throughout the WLAN deployment, as indicated by current surveys of external RF tools or observation of device applications such as the Wireless Analyzer. However, the UXI administrator is alerted of pre-configured UXI Service & App Tests failing to reach the network, and/or end-user reports of **network not reachable** by other applications.

The following screen depicts a UXI system alert that a pre-configured Service & App Tests Telnet Server is failing, a similar concern as discussed in Poor Application Performance in Specific Areas.



1	Two devices with red indications
2	Telnet Server test fails

Diagnosis

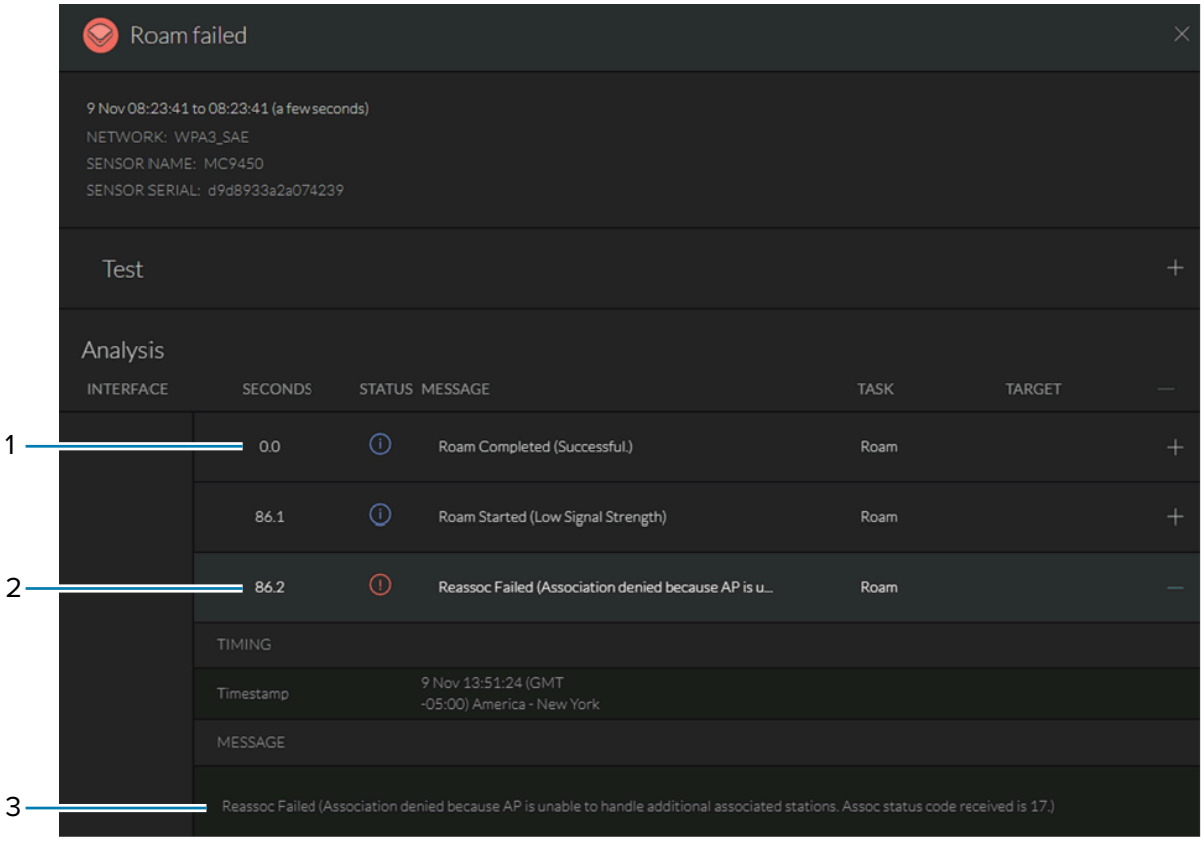
Select one of the devices. The following screen indicates the Telnet problem is **Unable to connect to telnet service**. Note that this coincides with **Roam failed** events around the same time.

1	The problem persists for long periods, but not all the time or everywhere
2	Ongoing issue of **Unable to connect to telnet service**
3	Roam failed events during that time

Note that in this scenario the administrator has already determined Wi-Fi coverage aspects don't contribute to the problem.

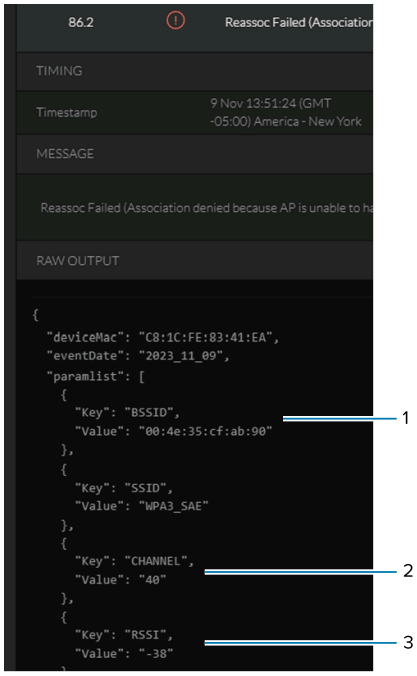
Select one of the **Roam failed** events. The following screen shows a **Roam Completed** message with an AP at a relative time of **0.0** indicating the device was connected in that area prior to the problem.

86 seconds later, when the device moves to a different area, the message **Reassoc Failed** indicates the device failed to connect to the new AP. The specific message **(Association denied because AP is unable to handle additional associated stations. Assoc status code received is 17.)** indicates that the AP reached its limit of associated clients of any kind, using a standard 802.11 reason code to convey its denial to the device.



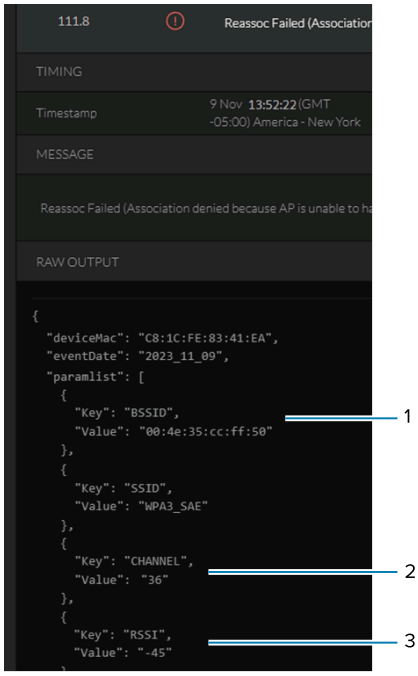
1	The device was roaming successfully in another area
2	The device attempts to roam to another AP and fails
3	Reason the AP denied the device

Scroll down in this screen to **RAW OUTPUT** to observe the specific AP information.



1	The AP's BSSID is 00:4e:35:cf:ab:90
2	The AP is on channel 40
3	Very strong RSSI

Exit this **Roam failed** instance and open another one. Scroll down to observe **RAW OUTPUT** parameters, noting this instance shows a different AP than the previous one.



1	The AP's BSSID is 00:4e:35:cc:ff:50

2	The AP is on channel 36
3	Very strong RSSI

Repeat this with a few more **Roam failed** instances. Multiple APs in the same area respond to the device with the same denial reason code, supporting the conclusion that this area of the deployment is reaching the maximum capacity of allowed connected devices. This is most likely due to user mobility dynamics in which many users congregate in specific areas at specific times.

Corrective Action

To address this, the administrator should increase the Max Stations value in the WLAN infrastructure (or adjust the configuration per AP-vendor recommendation) to accommodate the use case dynamics.

After the WLAN configuration mitigation, the administrator monitors the UXI for a duration of time (depending on the expected user mobility dynamics) to validate that devices no longer experience Telnet Server issues in any area, as shown in the following screen.