VALTORIS TECHNICAL WHITE PAPER

Analyzing AGV Roaming Delays with Wireshark

Industrial WiFi Troubleshooting Guide

1. The Challenge of Roaming in OT Networks

In standard IT environments, a Wi-Fi roaming delay of 300-500 milliseconds is completely invisible to end-users due to application buffering. However, in Operational Technology (OT) environments, Automated Guided Vehicles (AGVs) rely on highly deterministic protocols like Profinet, Ethernet/IP, or Modbus TCP.

A delay of just 50ms can trigger a PLC watchdog timeout, resulting in a sudden, hard stop of the vehicle. This guide will show you exactly how to capture and identify these "Phantom Disconnects" using Wireshark.

2. Capture Setup & Preparation

To accurately capture the 802.11 handover process, you cannot rely on standard wired packet captures from the switch. You must capture the traffic **over the air**.

- **Hardware Requirements:** A laptop with a Wi-Fi adapter that supports *Monitor Mode* (promiscuous mode for wireless).
- **Positioning:** Place the capture device physically near the "overlap zone" where the AGVs typically experience the fault.
- **Configuration:** Tune your Wi-Fi adapter to the specific channel(s) used by the Access Points (APs) in that overlap zone.

3. The Wireshark Filters

Once you have a raw packet capture (PCAP) of the fault event, finding the specific roaming delay among millions of packets requires precise filtering.

> **Step 1: Isolate Authentication Frames**
> Use the EAPOL (Extensible Authentication Protocol over LAN) filter to find the WPA2 4-Way Handshake.

```
Display Filter: eapol
```

4. Analyzing the 4-Way Handshake

In a standard non-802.11r environment, the AGV must complete a full 4-way cryptographic handshake with the new AP before data can flow. Look for these four specific packets in your filtered view:

1. **Message 1:** AP sends ANonce to AGV.
2. **Message 2:** AGV sends SNonce and MIC to AP.
3. **Message 3:** AP sends GTK and MIC to AGV.
4. **Message 4:** AGV sends ACK to AP.

5. Identifying the "Phantom Disconnect" (The Delta Time)

The key metric is the time it takes to complete the handshake. In Wireshark, ensure you have the **Time Delta from previous captured frame** column enabled (Go to Edit > Preferences > Columns).

```
No. Time Source Destination Protocol Info
105 12.001000 AP_1 AGV_MAC EAPOL Key (Message 1 of 4)
106 12.152000 AGV_MAC AP_1 EAPOL Key (Message 2 of 4)
107 12.405000 AP_1 AGV_MAC EAPOL Key (Message 3 of 4)
108 12.450000 AGV_MAC AP_1 EAPOL Key (Message 4 of 4)
```

In the real-world example above, the entire process takes ~450ms. During this massive gap, if you clear the EAPOL filter, you will see a spike in TCP Retransmissions and Profinet alarms as the PLC panics.

6. Validating the 802.11r Solution

Once you upgrade to hardware like the Valtoris VT-LTE400 and enable **802.11r Fast BSS Transition (FT)**, the Wireshark capture will look entirely different.

- You will **no longer see the 4-Way EAPOL Handshake** during the roam.
- Instead, you will see **Authentication (Fast BSS Transition)** frames.
- The Delta Time for these frames will drop from ~450ms to typically **12-18ms**.

> **Conclusion:** If your EAPOL handshake takes longer than your PLC's watchdog timer, your hardware is physically incapable of maintaining the connection. Upgrading your AGV's wireless bridge to support 802.11r FT is the only definitive fix.
