



AirLink OS 2.1

RELEASE NOTES

About AirLink OS 2.1

This release of AirLink OS 2.1 is for the AirLink XR90 and XR80. These release notes describe new features, bug fixes and known issues that apply to this release.

New Features

WAN

Added several improvements to Multi-WAN, including DNS resolution (Resolve DNS requests using the active WAN link for the originating traffic), and local logging of Multi-WAN switching decisions.

Added a WAN Auto Detect mode for all Ethernet ports.

When enabled (the default setting), when the Ethernet interface comes up (at boot or when a cable is connected), the router attempts to obtain an IP address over IPv4 (DHCPv4) and IPv6 (SLAAC/DHCPv6—either stateful or stateless). If a DHCPv4/v6 response or Router Advertisement is received, the Ethernet interface is placed in WAN mode.

For applications where LAN-only clients are connected to Ethernet ports, WAN Auto Detect can be disabled to ensure the fastest DHCP response times, if LAN DHCP server timeout responses are observed.

Enhanced IP passthrough by:

- adding configurable subnet option
- issuing proxy-arps for any WAN IP address within the specified subnet mask, when a subnet less than /32 is configured.
- adding the ability to respond to pings for a passed-through IP address (ICMP Response For WAN IP)
- adding options for “First Host” and “MAC Address” when enabling IP passthrough.

VPN

Added VPN features, including FIPS for IPsec.

XR80/XR90: Added hardware acceleration for IPsec VPN (except IPv6 ESP-in-UDP and MOBIKE).

Wi-Fi

XR90: Enhanced in-vehicle Wi-Fi support, including a default WAN policy to give 5GHz priority over 2.4GHz.

Location and Telemetry

Added enhancements and improvements to vehicle telemetry, including optimizing time to get first GNSS fix and adding seat belt reports.

ALMS

Added items to the default status report, including location and various cellular status items. The Status Report is now enabled by default.

ALMS now shows XR cartridge information, including serial numbers.

Cellular

Added a new custom APN for ATT ECC SIM to the Auto APN feature.

NTP

Increased the update interval for NTP to reduce network traffic, and added configuration parameters to allow further tuning of time syncing of the device with external time sources.

These parameters are: min interval, max interval, and max number of NTP sources to use.

Security Enhancements

Security and CVE Vulnerabilities

Addressed potential vulnerabilities related to;

- [CVE-2020-24586](#)
- [CVE-2020-24587](#)
- [CVE-2020-24588](#)
- [CVE-2020-26139](#)
- [CVE-2020-26140](#)
- [CVE-2020-26141](#)
- [CVE-2020-26142](#)
- [CVE-2020-26143](#)
- [CVE-2020-26144](#)
- [CVE-2020-26145](#)
- [CVE-2020-26146](#)
- [CVE-2020-26147](#)
- [CVE-2012-0871](#)
- [CVE-2013-4327](#)
- [CVE-2013-4391](#)
- [CVE-2013-4392](#)
- [CVE-2013-4393](#)
- [CVE-2013-4394](#)
- [CVE-2016-3189](#)
- [CVE-2016-7795](#)
- [CVE-2017-1000082](#)
- [CVE-2017-18078](#)
- [CVE-2017-3738](#)
- [CVE-2017-9217](#)
- [CVE-2017-9445](#)
- [CVE-2018-0732](#)
- [CVE-2018-0733](#)
- [CVE-2018-0734](#)
- [CVE-2018-0735](#)
- [CVE-2018-0737](#)
- [CVE-2018-0739](#)
- [CVE-2018-1000877](#)
- [CVE-2018-1000878](#)
- [CVE-2018-1000879](#)
- [CVE-2018-1000880](#)
- [CVE-2018-1049](#)
- [CVE-2018-15686](#)
- [CVE-2018-15687](#)
- [CVE-2018-15688](#)
- [CVE-2018-16864](#)
- [CVE-2018-16888](#)
- [CVE-2018-18311](#)
- [CVE-2018-18312](#)
- [CVE-2018-19211](#)
- [CVE-2018-19217](#)
- [CVE-2018-20796](#)
- [CVE-2018-5407](#)
- [CVE-2018-6954](#)
- [CVE-2018-9251](#)
- [CVE-2019-1000019](#)
- [CVE-2019-1000020](#)
- [CVE-2019-11463](#)
- [CVE-2019-12290](#)
- [CVE-2019-12450](#)
- [CVE-2019-12749](#)
- [CVE-2019-12900](#)
- [CVE-2019-13012](#)
- [CVE-2019-14834](#)
- [CVE-2019-14889](#)
- [CVE-2019-1543](#)
- [CVE-2019-16168](#)
- [CVE-2019-18224](#)
- [CVE-2019-19126](#)
- [CVE-2019-19645](#)
- [CVE-2019-19646](#)
- [CVE-2019-20386](#)
- [CVE-2019-20810](#)
- [CVE-2019-3842](#)
- [CVE-2019-3843](#)
- [CVE-2019-3844](#)
- [CVE-2019-5094](#)
- [CVE-2019-7309](#)
- [CVE-2019-9936](#)
- [CVE-2019-9937](#)
- [CVE-2020-0556](#)
- [CVE-2020-10543](#)
- [CVE-2020-10711](#)
- [CVE-2020-10878](#)
- [CVE-2020-11494](#)
- [CVE-2020-12049](#)
- [CVE-2020-12464](#)
- [CVE-2020-12655](#)
- [CVE-2020-12657](#)
- [CVE-2020-12659](#)
- [CVE-2020-12723](#)
- [CVE-2020-12770](#)
- [CVE-2020-12771](#)
- [CVE-2020-12826](#)
- [CVE-2020-13143](#)
- [CVE-2020-13776](#)
- [CVE-2020-13974](#)
- [CVE-2020-14155](#)
- [CVE-2020-15393](#)
- [CVE-2020-15436](#)
- [CVE-2020-15780](#)
- [CVE-2020-15888](#)
- [CVE-2020-15945](#)
- [CVE-2020-1712](#)
- [CVE-2020-1751](#)
- [CVE-2020-24394](#)
- [CVE-2020-27153](#)
- [CVE-2020-29368](#)
- [CVE-2020-29374](#)
- [CVE-2021-27645](#)
- [CVE-2021-33910](#)
- [CVE-2021-3588](#)
- [CVE-2021-37600](#)

Bug Fixes

Networking and Connectivity

Resolved an issue where, after a reboot, the LPWA radio Adapter Status in AirLink OS Status/Monitoring could show “Standby” after previously showing “No Service” despite the radio being enabled.

Resolved an issue where, after the router is reset to factory defaults from AirLink OS, the LPWA radio could not reconnect to the network.

Resolved an issue where, after creating a DHCP Reservation (Fixed IPv4 or IPv6 Assignment) for a HOST-PC client with a previous IP allocation, the client persisted in using the previous IP allocation.

Resolved an issue where, with the XR90 connected via Cellular to the WAN and a host PC connected to the XR90 via Ethernet, the IPv4 Passthrough value for the WAN IPv4 interface could be reported (on Networking > General > WAN) on the Update WAN IPv4 Interface as “Value not Available” instead of the correct Ethernet interface.

Resolved an issue where a Windows 10 computer connected to XR90 via USB lost Internet connection after the XR90 was rebooted.

Wi-Fi

XR90: Resolved an issue where IPv6 Prefix Extension was not supported in Multi-WAN scenarios (that is, more than one WAN interface).

Resolved an issue where, when using XR90 Wi-Fi in Client mode, a background scan could result in reduced Wi-Fi WAN to Eth/Wi-Fi LAN throughput.

Resolved an issue where the Wi-Fi or XP cellular WAN interfaces could disconnect after a reboot.

Resolved an issue where, with XR90 as a 5GHz access point, the LED that indicates Wi-Fi traffic stopped blinking purple when more than one client device was connected.

AirLink OS

Resolved an issue where creating multiple templates from the current configuration could produce templates with invalid data.

Datasets

Resolved an issue where it was not possible to create a dataset from scratch in ALMS/AirVantage.

Hardware

Resolved an issue where unsupported link speeds 5000baseT/Full and 2500baseT/Full were shown as available for selection on the GigE Ethernet ports (Eth2 and Eth3).

Resolved an issue with the XP1 Ethernet port, which sometimes exhibited ping failures after power-cycling.

Known Issues

Wi-Fi

Windows PCs using Cisco AnyConnect Client with Network Access Manager for Wi-Fi authentication will fail to connect to the XR90 in Access Point mode when PMF (enabled in any of the WPA3 modes) is enabled on the XR90. (See cisco.com/quickview/bug/CSCvq05530.) To resolve, use WPA2 and disable PMF.

An issue exists in dual Access Point and Client mode where the XR Wi-Fi Client interface can restart unnecessarily after losing connection to the remote Access Point. This causes the XR Access Point to drop connected clients.

After upgrading to AirLink OS 2.0 from an earlier release, it may not be possible to configure the Wi-Fi B 5GHz interface. To resolve, reset the device to factory defaults.

Changing security protocols on SSID 1 and 2 (2.4GHz and 5GHz) may cause issues with password recognition on Apple devices (passwords may need to be entered multiple times).

Networking and Connectivity

It has been found that the Idle Traffic threshold under Network Watchdog > Monitoring Rules is high enough that interfaces can restart while still carrying active traffic. Because the threshold is not user configurable, Sierra Wireless recommends using one of the available ICMP Ping methods to monitor traffic for the Network Watchdog.

When creating a bandwidth profile under Quality of Service (QoS) > Bandwidth Policies, the UI converts Download and Upload settings from kilobytes and kilobytes/sec to megabytes and megabytes/sec. These conversions are inexact--40,000 KB is converted to 39.06 MB, for example.

XR90: An issue exists where the radio module adapter status may read "No Service" (with the cellular network LED flashing red), however the Cellular interface is active.

XR90: Under Cellular Configuration, the Preferred Technology setting "5G Only" is not supported by the radio module.

IPv6 DNS Propagate does not work with Windows 10 Enterprise.

XR90: An issue exists where IPv6 routes on multi-APN interfaces were not created after multiple reboots.

IPv6 DNS Propagate fails for the Ethernet WAN interface. Manually configured DNSv6 servers are not propagated from WAN to HOST-PC on the LAN.

XR90: Port forwarding may not work when more than one WAN interface is active.

Do not set the WAN Propagate feature to "auto" when two cellular WAN interfaces are configured for a LAN bridge.

In Multi-WAN scenarios where DNS needs to be always available, it is recommended to not use the WAN Propagate feature if the DNS servers being passed to clients are WAN link specific. For example, when using two SIM cards for different carriers, if Carrier 1 provides the DNS server to the client, then the client should be aware that if the Carrier 1 link is lost and the WAN link switches to Carrier 2 (with its own private DNS), the DNS does not resolve until the client renews its DNS servers. DNS renewal time depends on lease time configuration (two minutes minimum).

XR90: QoS (traffic shaping and policing) cannot be applied for traffic to/from the gateway itself, and may not be applied to some flows through the gateway.

When configuring an Ethernet or Wi-Fi WAN, the assigned address/mask can be the same as one of the LAN subnets. This causes issues with DNS queries from the LAN segment if the DNS resolver is on the WAN gateway (typically the Wi-Fi gateway provides its own address as DNS resolver to its DHCP clients). At present, AirLink OS does not show an alert when this condition exists.

VPN

IPv4 IPsec VPN (connected over cellular) does not work after IPv6 Clat is enabled.

AirVantage

After an XR90 with R2C eSIM is activated, the router must be rebooted to reattach to the network.

After a “Network Detach” operation initiated via ALMS Diagnostics, the HL7800 LPWA radio cannot recover a Network attachment.

Location and Telemetry

During drive tests, store-and-forward operation to maintain NMEA data during network outages does not start consistently after an outage is detected.

AirLink OS 2.1 does not support Dead Reckoning. As a result, [ALMS ARA Driver Behavior reports](#) are not supported in this release.

AirLink OS

Validation errors may arise when resetting the XR90 to a custom template (for instance, when the template contains settings for Multi-WAN policies).

A template containing a SIM configuration cannot be used to modify a SIM configuration on another XR90 (that is, when a SIM configuration is already present on the target XR90). A template containing a SIM configuration can only be used to create a new configuration on another XR90 (that is, no SIM configuration has been applied to the target device yet).

To use a template containing a SIM configuration, first delete the SIM configuration from the target XR90.