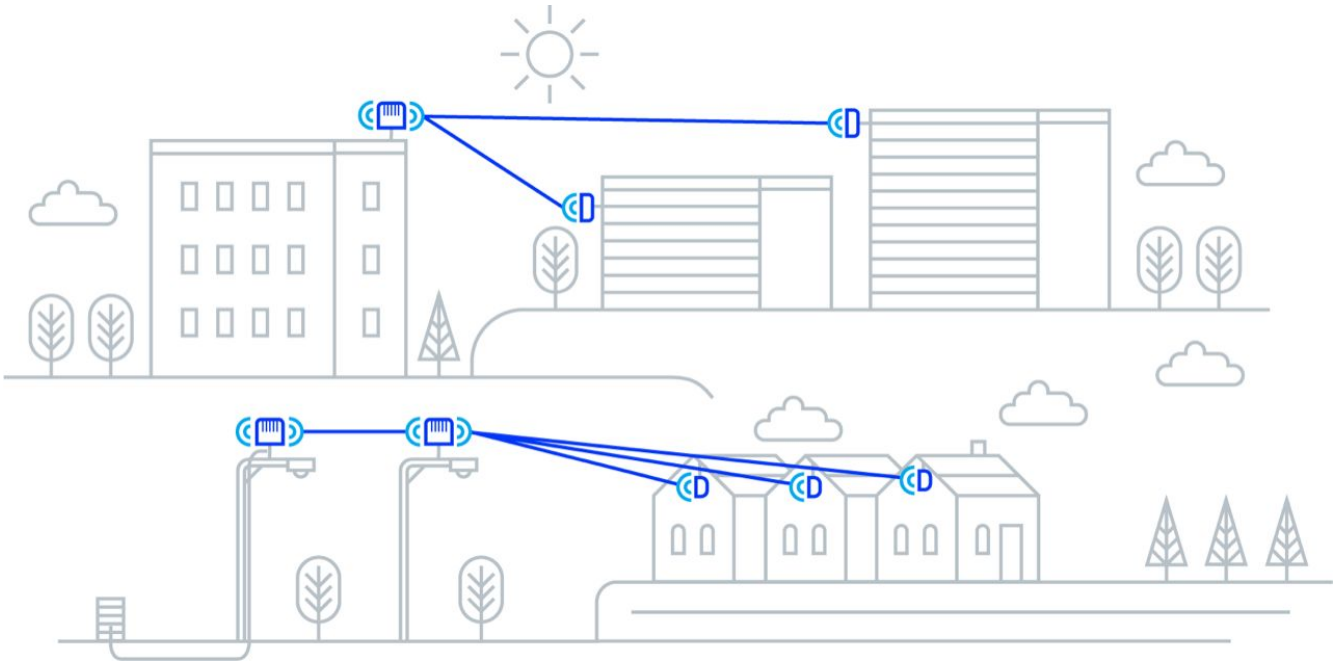


Altowav AltoPlex Series
K60DN and K60CN1 User Guide

Version 4.2.0

December 4, 2025

Copyright, trademark, and legal information

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
— Reorient or relocate the receiving antenna.
— Increase the separation between the equipment and receiver.
— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
— Consult the dealer or an experienced radio/TV technician for help.

Any modifications to this product which are not authorized by Altowav Inc. could void your authority to operate this equipment.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCT.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE ARE PROVIDED “AS IS” WITH ALL FAULTS. ALTOWAV DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL ALTOWAV OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OF DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF ALTOWAV HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Altowav would like to thank all of our staff for their efforts and expertise in development and implementation of the K60DN and K60CN1.

Regulatory statements

FCC Radiation Exposure Statement

The K60DN and K60CN1 device complies with FCC radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters (14 inches) of separation between the K60DN and K60CN1 and all persons shall be maintained.

FCC Regulatory Statement

The K60DN and K60CN1 equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. For full Regulatory notices and statements, refer to the manufacturer and product as declared on the hardware label.

ISED Industry Canada Radiation Exposure Statement

IC Radiation Exposure Statement:

The K60DN and K60CN1 device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters of separation between the K60DN and K60CN1 and all persons shall be maintained.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Un minimum de 35 centimètres de séparation entre le K60DN and K60CN1 et toutes les personnes doit être maintenu.

ISED Industry Canada Regulatory Statement

The K60DN and K60CN1 device complies with Industry Canada licence-exempt RSS standard(s). This device contains license-exempt transmitter(s)/receivers(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device is not to be operated on aircraft or satellites (ISED RSS-210 Annex J).

Cet appareil contient des émetteurs/récepteurs exempts de license qui sont conformes aux CNR exempts de license d'Innovation, Sciences et Développement économique Canada. Son fonctionnement est soumis aux deus conditions suivantes :

(1) Cet appareil ne doit pas causer d'interférences.

(2) Cet appareil doit accepter toute interférence, y compris celles qui peuvent entraîner un fonctionnement indésireable de l'appareil.

Cet appareil ne doit pas être utilisé à bord d’un avion ou de satellites (l’Annexe J de la norme ISED RSS-210).

Revision history

Revisions	Date
Updated for the 4.2.0 software release: • Added information about changing the SSID and encryption passkey for the 60 GHz airlink. • Added description of the new Link State parameter in the **Wireless** table on the **Status** tab, and the **Wireless Status** table on the **Wireless** tab, of the WebUI. • Added information about a new **Hide SSID** configuration parameter that hides the diagnostic Wi-Fi SSID.	12/04/2025
Updated for the 3.6.0 software release: • Added MAC filtering. • Added information about the factory default fallback static IP address of 192.168.0.1, new to release 3.6.0. • Added link to the Altowav enterprise MIB	05/05/2025
Updated for the 3.3.1 release: • **LL Discovery** information added to the **Status** page of the K60DN. • Updated VLAN configuration information. • Upgrading Firmware procedures updated.	02/05/2025
Release 3.2.0: • Added DN link auto-configuration. • Spanning Tree Protocol updated to include BPDU filter. • Changes made to information about logging into the WebUI to support read-only access for all pages in the WebUI.	12/18/2024
Release 2.7.3: • Spanning Tree Protocol pdated to include bridge priority and port cost. • New topic added to Enable Passwordless SSH.	9/25/24

Revisions	Date
• Updated references to the default password to reflect the new default password: **admin**.	

Contents

K60DN and K60CN1 User Guide overview

Thank you for choosing the Altowav AltoPlex series for your fixed-point networking solution. This user guide describes installation, configuration and operations of K60DN and K60CN1 devices.

This guide is intended for network and system administrators who will install, configure, and manage Altowav networks using K60DN and K60CN1 devices.

This guide includes instructions for the installation, configuration and management of K60DN and K60CN1 devices using the WebUI. Other methods of device and network management, such as the Command Line Interface (CLI), REST API and the AltoCommand network management tool, are mentioned, but detailed instructions are not provided.

It is assumed readers are familiar with:

- Basic networking concepts.
- Routing and switching in networks.
- Specific network practices, operations and settings at the installation.
- The topology of the network being installed and managed.

Additional Documents

Further information about the K60DN and K60CN1 devices:

- For general technology specifications and product datasheets, see altowav.com/technology/
- K60DN Quick Start Guide
- K60CN1 Quick Start Guide
- Altowav AltoCommand User Guide

Additional help

Altowav is committed to providing our customers with high quality technical support.

Web	support.altowav.com
E-mail	support@altowav.com

Introduction

Designed to help service providers deliver an excellent customer experience while managing costs, the AltoPlex platform utilizes carrier-grade gigabit connectivity to provide wireless network access. The platform enables highly customizable network management without the need for a centralized controller.

The AltoPlex platform delivers the superior performance and rich feature set promised by 802.11ay, with a lower cost and simplified management, as compared to our competitors in the 60 GHz solution marketplace.

With the AltoPlex platform, service providers can deploy and manage small to very large networks cost-effectively, and support many applications including:

- Gigabit fixed-wireless access (FWA).
- Surveillance camera connectivity.
- Multi-dwelling unit distribution.

The AltoPlex platform includes a REST API, providing the flexibility for network administrators to use the monitoring and management systems of their choice.

Network Design and Deployment Guidelines

Altowav offers training tailored to your specific operations. Contact us for more information.

This section offers some general information and guidelines for designing and deploying your Altowav Gen3 platform network. In addition, some guidelines refer to specific operations of the K60DN and K60CN1 devices, such as scan ranges, distances, and number of wireless links per radio interface. This section includes:

The diagram below shows a simple ring topology of K60DN units (distribution nodes) including one spur (DN-8). A few CN links are shown to demonstrate additional connections and general topology. Polarity is shown for the K60DN units. The point of presence (PoP) is the location or facility that connects to the Internet.

Note: DN-1 and DN-2 have direct SFP+ connection to the PoP but no wireless connection to each other. Both DN-1 and DN-2 are set to the same polarity. This design practice avoids the use of hybrid polarity around the ring and can offer some redundancy.

About wireless links in the AltoPlex platform

- 60GHz wireless links rely on line of sight (LOS).
- Device roles: K60DNs are distribution nodes which form the distribution network. K60CN1 are client nodes and used for client access.
- Priorities:
  - When planning, designing, and deploying your network, give priority to the K60DN units in distribution rings to benefit the entire network. Units closest to the PoP will have the heaviest traffic.
  - K60DN distribution networks are built first.
  - K60CN1 clients are added after the distribution network is up and running. Consider the distribution and density of clients during the design and planning of networks.
- K60DN units form wireless links with other units through configuration settings.
  - K60DN-K60DN links are configured on both K60DN units in the DN responder setting.

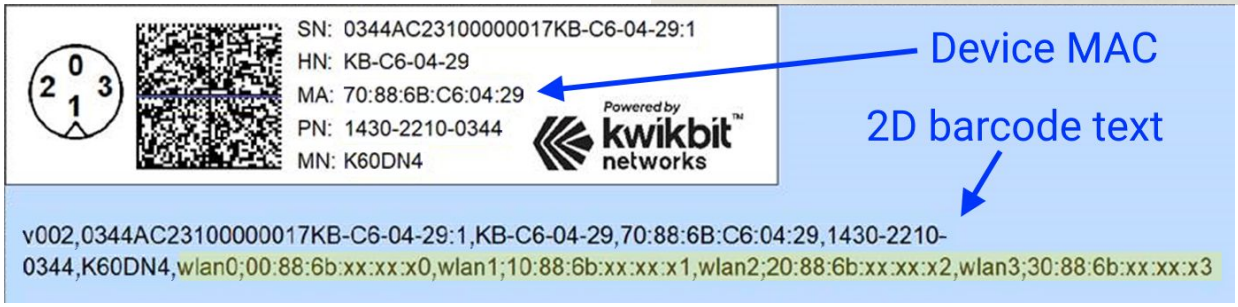
    - K60DN-K60CN1 links are configured only on the K60DN in the CN responder list setting, after the distribution network is up and running. This is typically done as clients are installed.
- Weighted MCS levels are a good performance metric for the Altowav Gen3 Platform. Power control in both the K60DN and the K60CN1 adjusts automatically to drive optimal MCS levels.

K60DN -- General Information

- The K60DN has four radio interfaces, Radio 0-3. These radio interfaces are also called wlan0-3 in device labeling, and when using the REST API or CLI for configuration. Radio 0 is the same radio as wlan0. Radio 1 is the same as wlan1, and so on.
    - **Scan range:** Each radio interface scans 90° azimuth (-45° to 45°), covering 360° total.
    - **Channel:** Each radio interface can be set to a single channel (1-4).
    - **Golay:** Each radio interface can be set to a single Golay code (1-3). Golay is a coding algorithm used to mitigate co-channel interference. K60DN's set to the same channel within range of each other can mitigate co-channel interference by using dissimilar Golay codes. See Common Design Issues for an example of this.
    - **Polarity (odd or even):** Polarity is a mechanism of TDMA used in determining when to transmit or receive during a timing cycle. It plays a critical role in TDMA operation.

      A single polarity is typically set per K60DN device to optimize throughput. However, polarity can be set per radio sector, (resulting in hybrid polarity on the K60DN), if necessary for less common network designs. Hybrid polarity results in diminished throughput and is generally avoided.
    - **Maximum DN-to-DN links:** 1 per radio interface.
    - **Maximum DN-to-CN links:** 15 per radio interface.
- The K60DN uses GPS for location and synchronization.

- **To find the K60DN device and radio interface MAC addresses,** scan the 2D barcode on the Kwikbit Networks label on the side of the K60DN or on its box. An inventory spreadsheet with MAC addresses is shipped or supplied electronically with the K60DN units. (MAC addresses for each unit are also available through the WebUI, after the K60DN is connected.) The label image below shows the radio MAC addresses (wlan0-3) in the 2D barcode text with yellow highlighting.

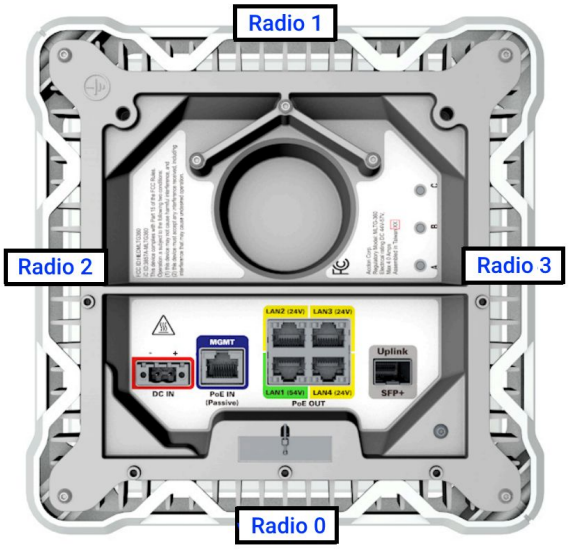
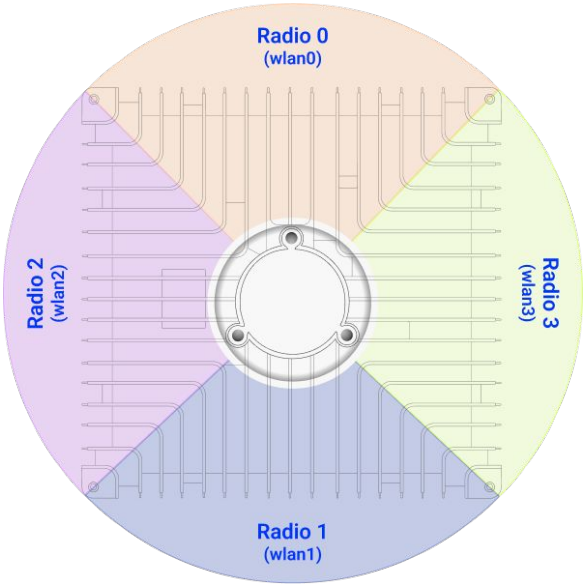


How to determine the position of Radio 0-3 (wlan0-3) in various orientations

These views may be useful for installation or maintenance.

Out of the box	Mounted on a pole in the field
 Radio 1 (wlan1) on the label sticker side.	Radio 3 (wlan3)  Radio 1 (wlan1) on the label sticker side. Radio 0 (wlan0) on the port cover (cable tray) side. Radio 2 (wlan2)

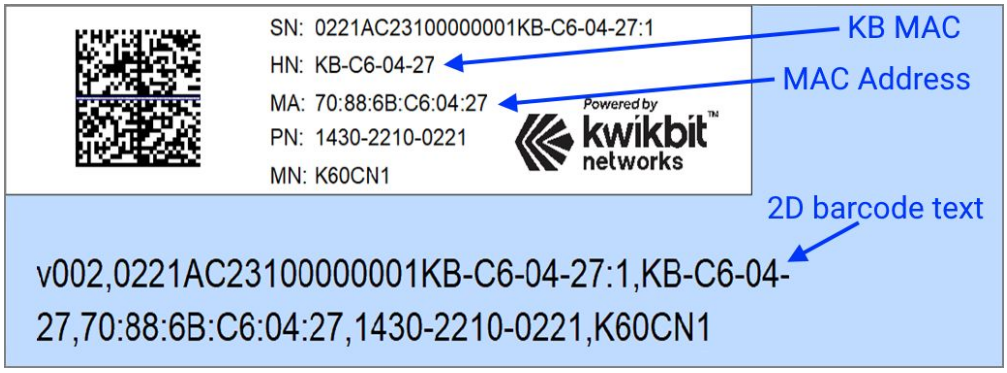
Bottom and top views may be useful for design and configuration purposes.

Bottom view of K60DN	Top view of K60DN radio sectors
	
From the bottom view, Radio 1 (wlan1) is on the same side as the pole mount bracket. Radio 0 (wlan0) is on the side nearest the ports.	From the top view, Radio 0 (wlan0) is on the side on which one of the three top screws is centered. Radio 1 (wlan1) is on the same side as two of the top three screws.

Note: Radio 0-3 interfaces are also known as wlan0 - wlan3 in configuration parameters accessed through the CLI and REST API.

K60CN1 -- General Information

- The K60CN1 has one radio interface, located on the smooth front of the device.
  - **Scan range:** -45° to 45° for a total 90° azimuth scan range.
  - The K60CN1 radio interface links to a single K60DN radio sector.
- **The K60CN1 KB MAC address** is listed on the K60CN1's back label and box label. This is used when installing a K60CN1 and configuring it to connect to the K60DN as a CN responder.



- The K60DN-K60CN1 link is formed by configuring the K60DN's CN responder list to include the KB MAC of the K60CN1. See the K60CN1 Installation section for step-by-step instructions.

Deployment Guidelines for Design

The following guidelines provide information for planning trouble-free deployment and long term operation. See the K60DN Installation section and the K60CN1 Installation section for specific deployment steps.

- Maintain an unobstructed sky view over the top of the K60DN for GPS synchronization. GPS is used for TDMA synchronization on wireless links. This is not required for K60CN1 units, because they use over-the-air (OTA) time synchronization.
- Maintain a clear LOS between units for all wireless links.
- K60DN sectors with the default beam elevation, **Narrow**, have a scan range of +/- 7.5° (total 15° elevation range). See the General Design approach below for how this may affect K60DN-K60CN1 wireless links within close proximity. See the Beam Elevation Settings - Design Considerations topic, for a description of beam elevation settings.
- Distances for K60DN-K60DN links, at default beam elevation:
  - Up to 250 m for MCS 9.
  - Up to 185 m for MCS 12.
- Distance K60DN-K60CN1 links, at default beam elevation:

    - Up to 180 m for MCS 9.
    - Up to 75 m for MCS 12.
- Stable and secure installation is required to avoid movement due to wind.
- For cases where a K60DN cannot be installed on top of a pole, or for poles up to 10” in diameter, a K60DN Mounting J Bracket, (Altowav Model AX-K60DN-JMOUNT), may be used. Unobstructed sky view is required for GPS. Sides must remain unobstructed for clear LOS between radio interfaces on both ends of the wireless link. When using J brackets, assess any possible obstructions to LOS for the mounted device.
- Connecting to power:
    - The K60DN can be powered in two ways. **Option A -** DC power enables the use of PoE output on LAN ports. **Option B -** PoE Input power must be passive and disables the PoE output for LAN ports. Do not supply both DC power and PoE power at the same time! See *Connecting_the_K60DN_to_Procet-1N* for detailed information about power options.
    - The K60CN1 is powered by an indoor PoE injector (passive). This supplies power and provides connectivity to the router or access point at the customer premise.

General Design Approach

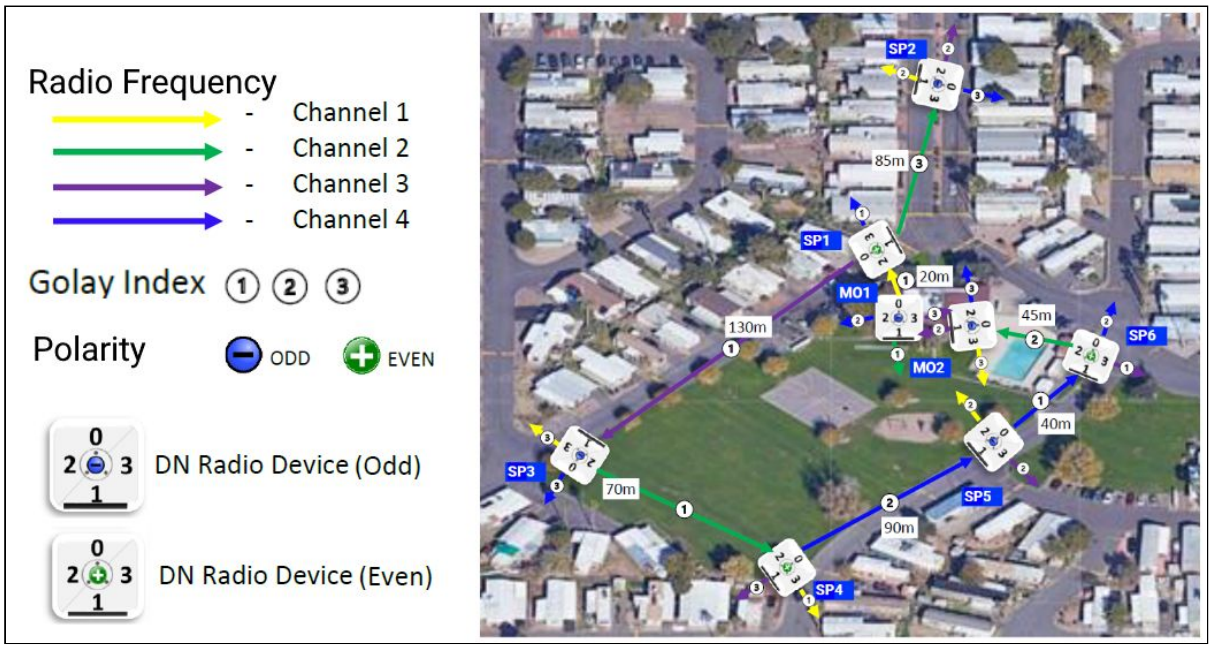
Each organization will have its own design and deployment tools and considerations for their specific site. The following outline offers a general approach. It does not include all considerations and details of design and planning. For more in-depth training contact Altowav: support@altowav.com.

General tasks for network design:

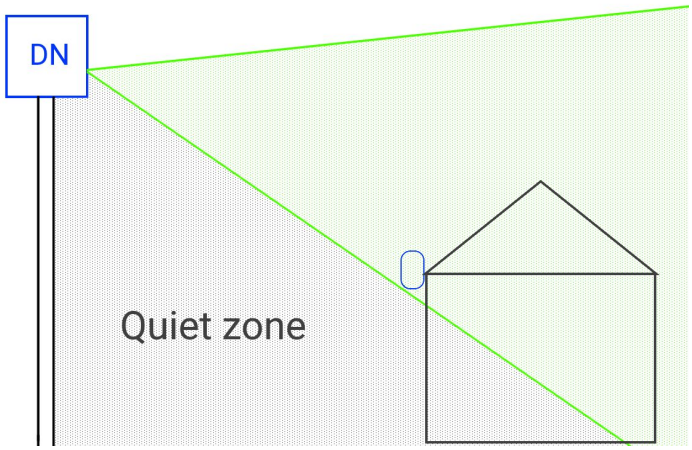
- **Survey the site** via Google Earth, onsite visits, drone survey.
    - Identify fiber/backhaul point of presence (PoP).
    - Identify access/equipment cabinet location.
    - Determine pole locations - consider LOS, distances, coverage and height.
- **Design the K60DN-K60DN links** (distribution network) -- planning the following:
    - **Polarity** -- shown with **blue (-)** for **odd** and **green (+)** for **even** in the sample map below.
    - **Channel frequency** -- shown with link color. **Ch1**, **Ch 2**, **Ch 3**, **Ch 4**.
        - Optimize frequency for distribution links first, then non-distribution links inside the ring, then non-distribution links outside the ring.
        - Use channels 2, 3 and 4 for K60DN-K60DN links for best distribution network performance. Use channel 1 for sectors with no K60DN-K60DN links.
        - Begin by using the same channel for straight line links (with different Golay codes - see Common_Design_Issues below). For example, see links **SP4-to-SP5** and **SP5-to-SP6** in the map image below. This alleviates adjacent sector

interference and enables more flexibility for other sector channels. Channels may be adjusted as the network develops.

- **Golay codes** -- shown by circled number ①②③.
- **Radio sector orientation.** The sample map image below shows general azimuth with arrows and radio sectors (0-3) on the K60DN device icons. Avoid using Radio 2 and Radio 3 for straight-line topology since they share a data bus. Using Radio 0 and Radio 1 will maximize traffic speeds because they have individual data buses.

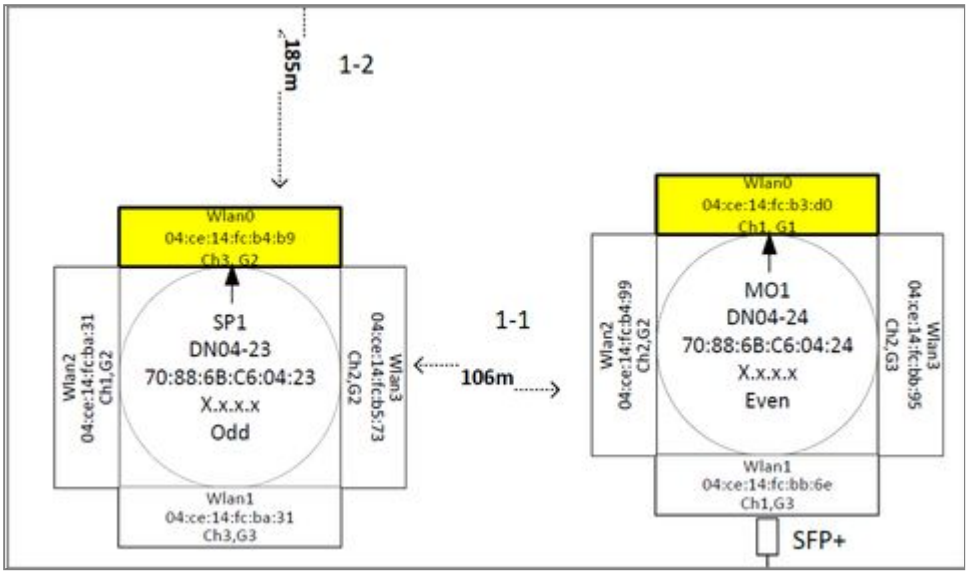


- **Design the K60DN-K60CN1 links** (client access network).
  - Keep in mind that each K60CN1 must be inside the 90° azimuth of the K60DN radio sector to which it connects.
  - When planning multiple K60CN1 links to a single K60DN radio sector, center the longest distance links to avoid path loss.
  - Height planning: Avoid the quiet zone for K60DN-K60CN1 links caused by the default beam elevation (+/- 7.5°). For example, a K60DN mounted 5 m high has a quiet zone within 38.5 m radius from the pole at ground level or a 15.4 m radius for a K60CN1 installed at a 3 m height.



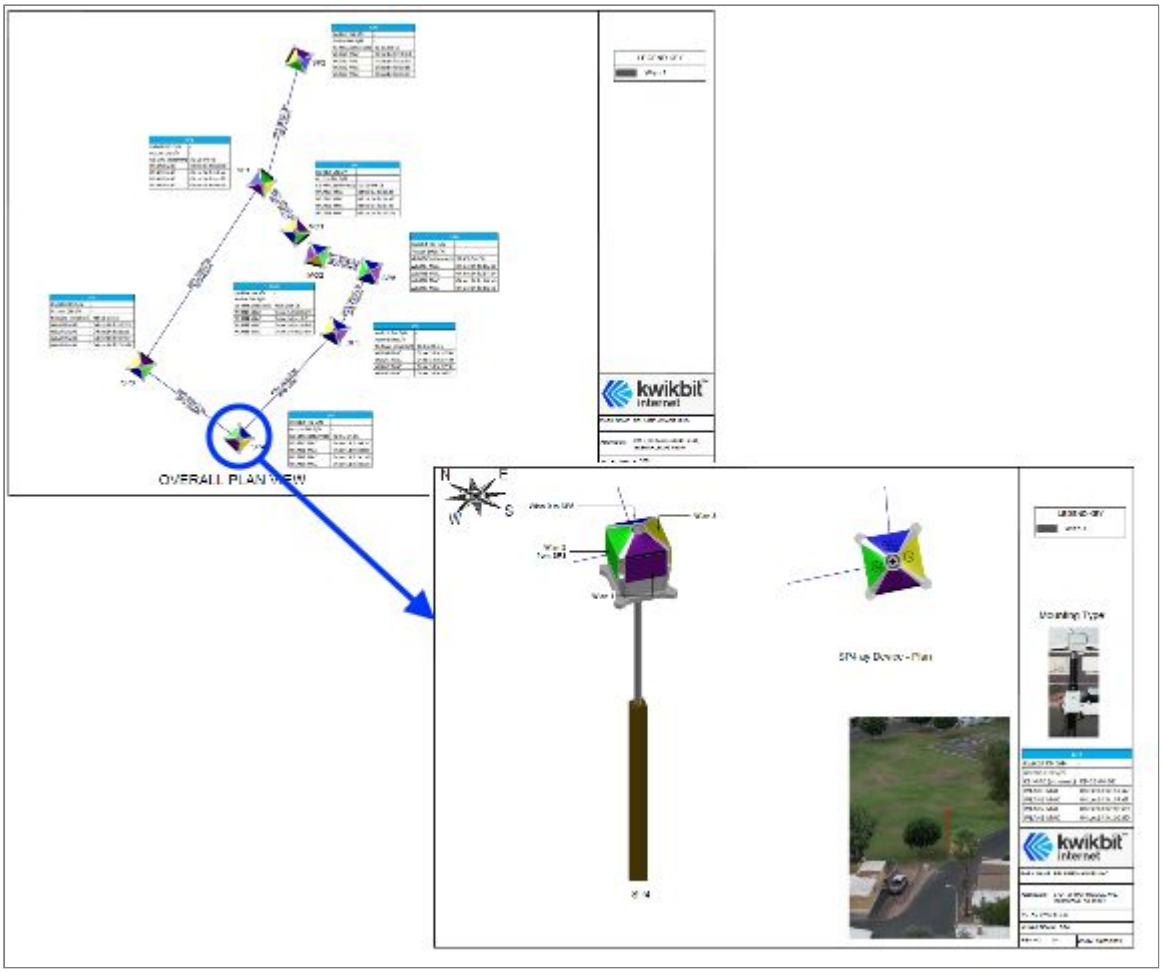
Some options to avoid the close-proximity quiet zone include raising the height of the K60CN1 or connecting it to a K60DN that is further away. Or, consider a beam elevation change after testing and evaluating the impact on current and future devices to be linked to that K60DN sector. See the topic on Beam Elevation Settings - Design Considerations.

- **Fill in specific details before deployment.** Add specific K60DN MAC addresses, radio orientations and distances to the distribution network design for all team members to use in bench configuration and installation. Having this information ready for design, support and installation teams enables more flexible configuration options. Here are two options.
  - A detailed design drawing including switch point names, device MAC address, radio sector MAC addresses, polarity, channel, Golay code, link distances and link names. The level of detail shown below is useful for bench configuration and installation.



  - Create engineering drawings of the distribution network showing radio orientation and distances. Label all switch points and K60DN units. Include tables for K60DN serial numbers, radio sector MAC addresses, channel, Golay code, and polarity to

enable bench configuration. Include photo or CAD drawings to facilitate installation as needed.



- Create an access network assessment (ANA) table showing all the K60DN's in the distribution network with viability assessed for each potential site for a K60CN1.

About Bench Configuration

K60DN units should be configured prior to installation. After the K60DN is installed, it may be difficult to access ports and see LED indicator lights. See K60DN Installation for bench configuration steps.

- Plan specific radio sectors 0-3 in the network design, using specific K60DNs for the distribution network. This information is used in configuration settings.
- WebUI settings, based on the design information:
  - **WebUI Access** -- DHCP is enabled by default, so the WebUI is accessible via direct connection to PC or switch with a DHCP server. (Power options for bench configuration: DC power from the Procet-1N, or power and connect via passive PoE (90W) connected to **MGMT Uplink** port.)
  - **Status tab:** Check firmware version, update on **Admin** tab, if needed.

- **Admin tab**: Description and Location set to be consistent with network design.
- **Wireless tab:** For each radio interface set the **Channel**, **Golay index**, **Polarity** and enter the MAC address for the **DN responders** (the radio interface on the remote end of the K60DN-K60DN link) according to the network design. **CN responders** are added later, at the time of K60CN1 installation.
- **LAN tab:** Review and enable ports as required in network design.
- **Network tab:** Adjust settings per network design.

- Beamforming and connections are verified later as K60DNs are installed.

K60CN1 units do not require bench configuration.

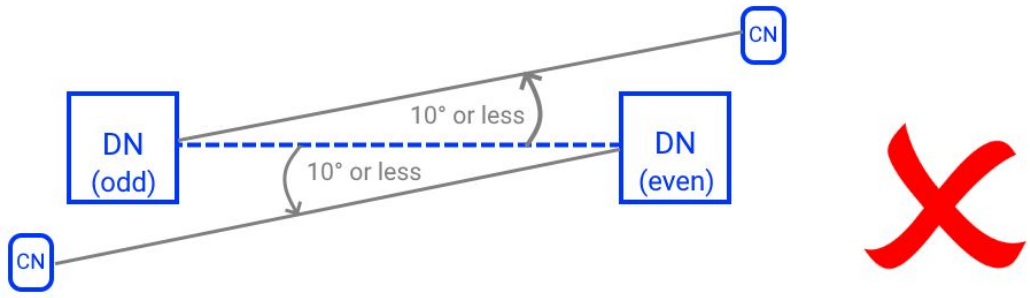
- Configuring a K60DN to link to the K60CN1 triggers the K60DN to attempt connection until it is successful. For this reason, configuring this connection setting should be done at the time of installation. See an Example of how to add a K60CN1 to the K60DN's CN responder list.
- The K60CN1 defaults to the K60DN's **Mgmt VLAN** after the link is established, enabling an operator to configure all settings (including VLAN) after the link is established.

Common Design Issues

Most design issues below have been identified generally for 60GHz networks running on 802.11ay-based technology. Here we address them specifically for the Gen3 platform devices: K60DN and K60CN1.

Issue: Tight angles between K60CN1-K60DN links and K60DN-K60DN links

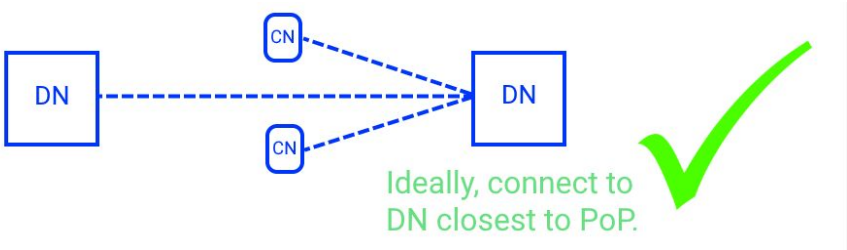
Tight angles between the K60CN1-K60DN link and the K60DN-K60DN link in the same sector, such as the butterfly topology, can result in early weak interference. This problem occurs at angles tighter than 10°. Early weak interference can be hard to detect because it does not create any signal-to-interference-plus-noise ratio (SINR) degradation, but it still blocks desired packets by locking the receiver before the arrival of the packet.



For more detail on the issues caused by the butterfly topology and a example of it, see Case Study: Butterfly Configuration Issues.

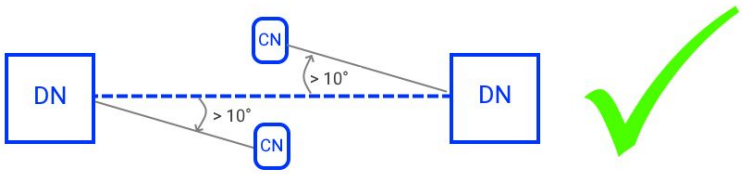
Best Practice:

If the K60CN1s cannot be positioned to avoid the tight angle, the best workaround is to link both K60CN1s to same K60DN. Ideally the K60CN1s would link to the K60DN closest to the PoP. This will minimize the number of hops from the PoP to the K60CN1. This ideal is not always practical, due to site conditions and line of sight.



Additional Solution:

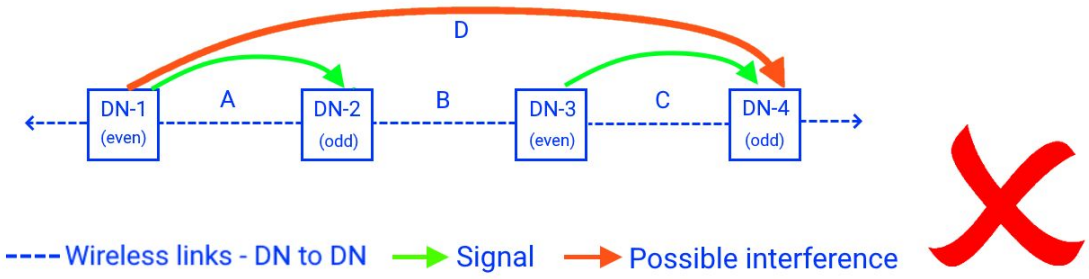
Design and deploy sites where the K60CN1-K60DN links are more than 10° away from the K60DN-K60DN links as shown in the butterfly topology diagram below.



Issue: K60DNs in a straight line and too close together

An example of this is four or more K60DNs in a line. In this configuration, a signal can be far reaching and cause interference to an unintended endpoint. Straight line interference is more impactful for short link distances.

The diagram below shows even-polarity transmission in the same channel. In this case, signal A from DN-1 to DN-2, can also cause a signal D that may interfere with an unintended endpoint such as interference on DN-4 as it receives transmissions from DN-3.

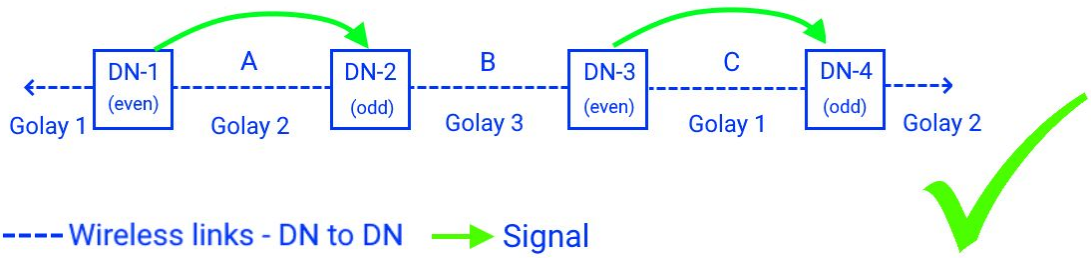


Issue: Straight line interference

Solutions:

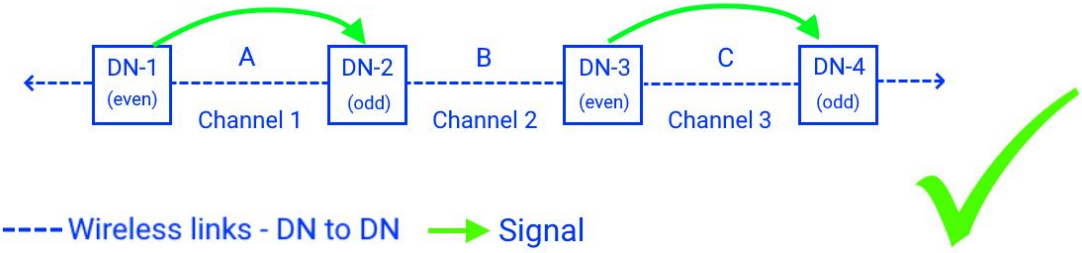
If the straight-line formation in close proximity is unavoidable, here are some solutions to consider:

- **Set the Golay code (1-3) for both ends of each link.** Make sure that the Golay code is different for the link between the two DNs with the possible signal interference (DN-1 and DN-4, in the diagram below).



Using Golay codes to address straight-line interference

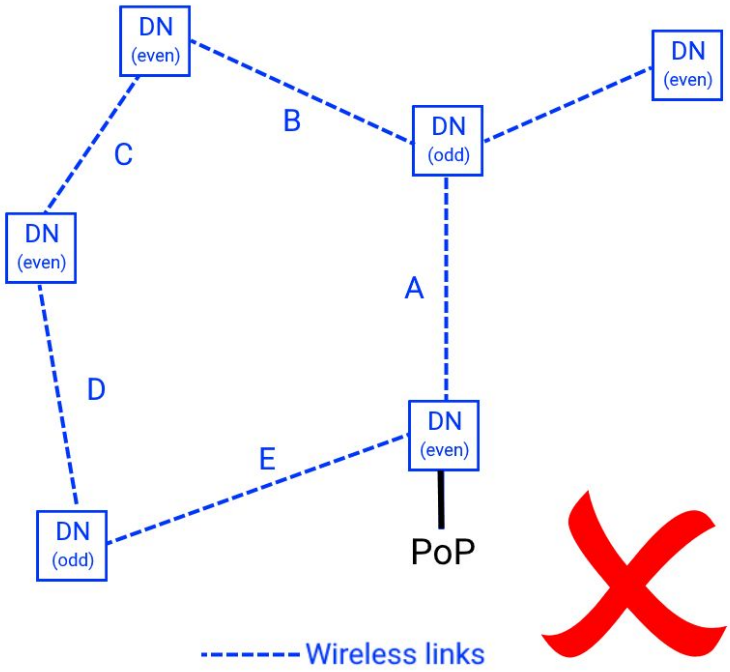
- **Less optimal solution:** If using Golay codes is not an option for some reason, using different channels (1-4) between the DNs will resolve the issue. This provides a reliable solution, if network design and short link distances require it. However, in general practice the same channel is used in straight line formation to avoid adjacent sector interference and provide more flexible options for channel selection on adjacent sectors.



Using different channels to address straight-line interference

Issue: Ring polarity issues

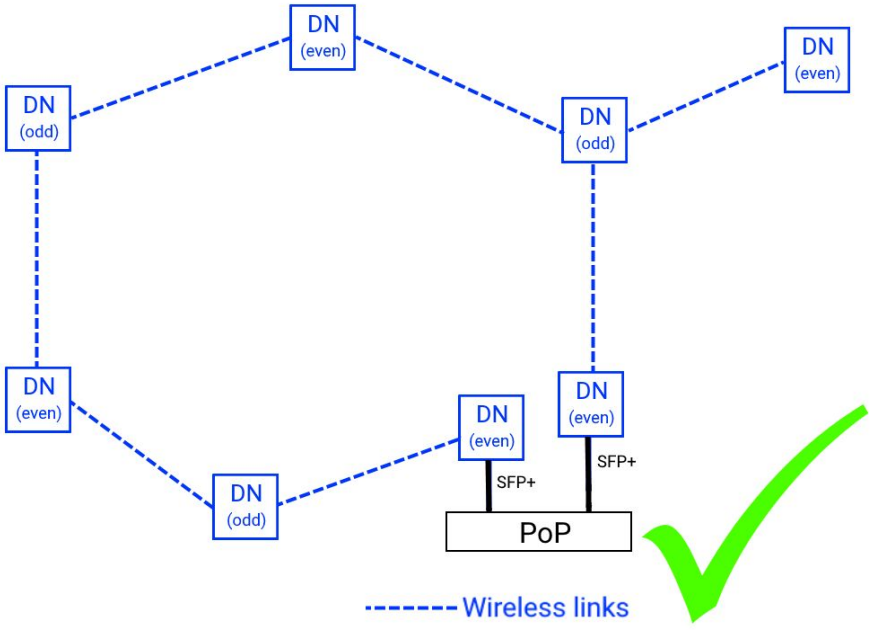
An odd number of K60DN units in a ring topology can cause performance problems because a pair of linked K60DN units will have like polarity. This is shown with link C between two K60DNs set to even polarity. Note, spurs off the ring do not contribute to this type of ring polarity issue so do not count them in the number of K60DNs in the ring.



Issue: Like polarity for an odd number of K60DNs in a ring

Best practice:

Design the distribution ring with two K60DN units connected directly to the PoP, but not wirelessly connected to each other. The units can be set to the same polarity or two different polarities, depending upon the number of K60DN units in the ring. This enables maximum throughput performance by avoiding the use of hybrid polarity.



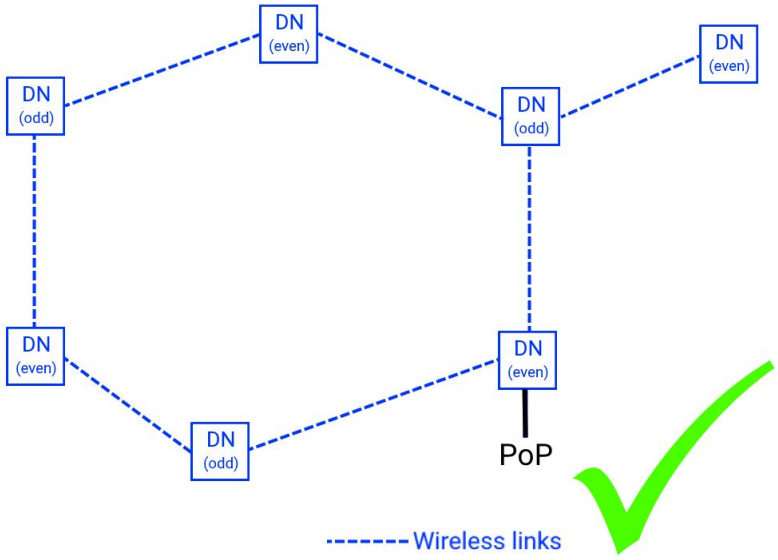
Best Practice: Design with two K60DNs at the access cabinet

The two K60DN units at the access cabinet also provide some redundancy.

Note: If the two K60DNs at the PoP are set to different polarities, potential interference could result when the same channel is used for links to these K60DNs. Careful design and planning is crucial.

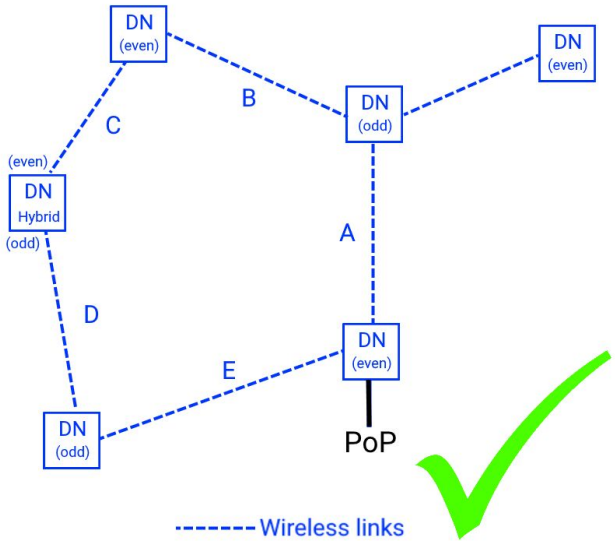
Additional Solutions:

- Design the ring topology with an even number of K60DN units. This enables maximum throughput performance.



Design with an even number of K60DN units in the ring

- If the topology must include an odd number of K60DNs in a ring, and cannot use two K60DNs at the PoP, create a hybrid node at the farthest node from the fiber point of presence. On the hybrid node, polarity is set as needed for each sector.
- **Note:** Throughput for hybrid nodes is reduced by half on that node's links, shown in the diagram as link C and D.



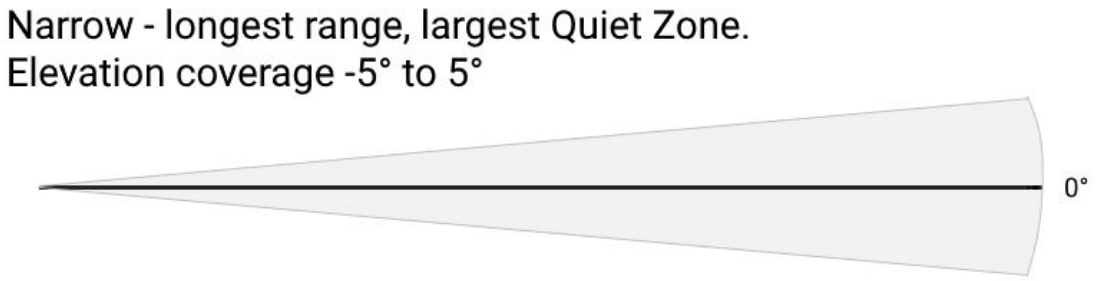
Hybrid polarity set on the node furthest from the PoP

Beam Elevation Settings - Design Considerations

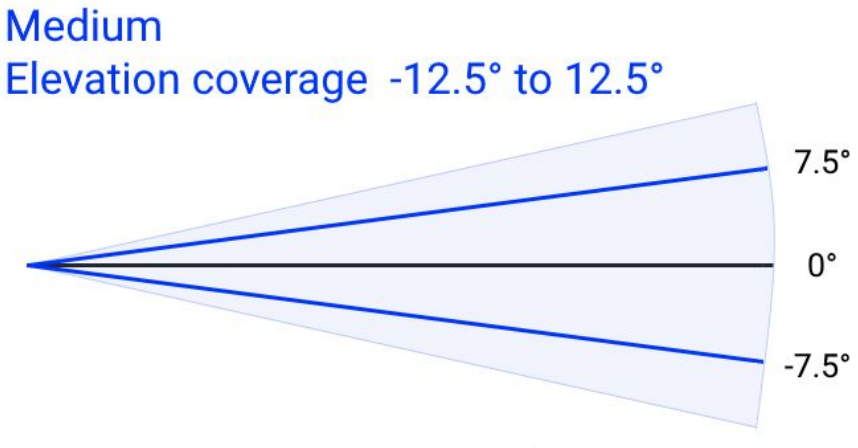
Beam elevation settings can be set to **Narrow**, **Medium** or **Tall** for each sector of a K60DN. The default is **Narrow**. All firmware versions previous to 1.7.0 use only **Narrow** elevation.

Elevation can be configured via the WebUI (Wireless tab), REST API or CLI.

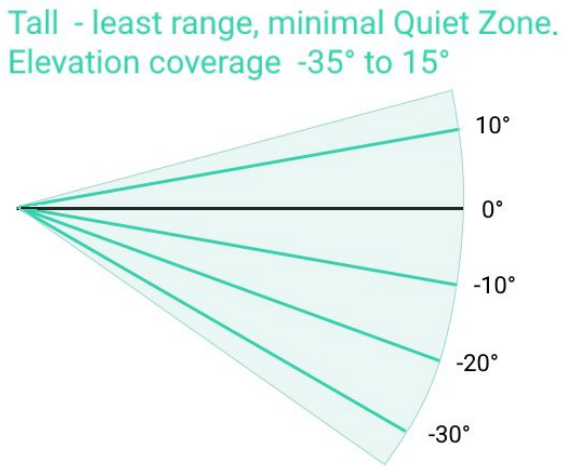
Test and consider the effects of beam elevation changes for the specific network site, before committing to the changes. Keep in mind, the changes affect all current and future links for the sector. Use the following information to help determine whether or not changes are suitable for a specific case.



Narrow primary use case: Default. Provides best performance for maximum range.



Medium primary use case: Edges or corners of network sites where range is limited.



Tall - recommended for DN-CN links only. Primary use cases: Edges or corners of network sites where range is very limited, and for cases where access within the Quiet Zone is required.

Beam elevation settings for all sectors with DN-DN links:

- When the physical elevation is similar for K60DNs, all DN-DN link sectors should use the **Narrow** setting (default).
- If elevation differences are enough to degrade performance and the distance is about 100 m or less between K60DNs, the **Medium** elevation could be used after testing. Be aware that this will decrease the range for the link.
- Do not use the **Tall** elevation for DN-DN sectors.
- Exercise Caution when changing the beam elevation for DN-DN links. The change could limit the effective range and inhibit the link. It is best to perform elevation changes when onsite presence is available or a secondary path is available for the K60DN.

Beam elevation settings for sectors with only DN-CN links:

- Begin with **Narrow** elevation (default) for maximum K60CN1 distance.
- Beam elevation changes should be tested and their impacts considered within the full scope of the design layout and potential interference for each network. Keep in mind that beam elevation changes affect all current and future DN-CN links on the sector.
- For K60CN1s that are closer than 75 m with marginal RF performance, **Medium** elevation could be tested, verified and used.
- For K60CN1s closer than 50 m, **Tall** elevation could be used, but this limits the maximum distance for optimal K60CN1 performance to 15-50 m.

K60DN Installation and Configuration

K60DN Installation

The K60DN installation instructions include:

- Tool list
- K60DN box contents and functional description.
- Network design information required.
- Bench configuration steps.
- K60DN onsite installation steps.

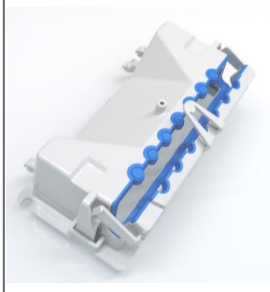
Tool List:

1/8" slotted screwdriver for DC plug

8mm nut driver or slotted screw for band clamp

#2 Phillips head screwdriver for pole-mount brackets and port covers

Box contents:

	 **Stainless steel band clamp** 		 **DC plug** 	
K60DN	**Pole-mount bracket**	**Port cover**	**Screw kit**	**Passive PoE injector*** **(for bench configuration)**

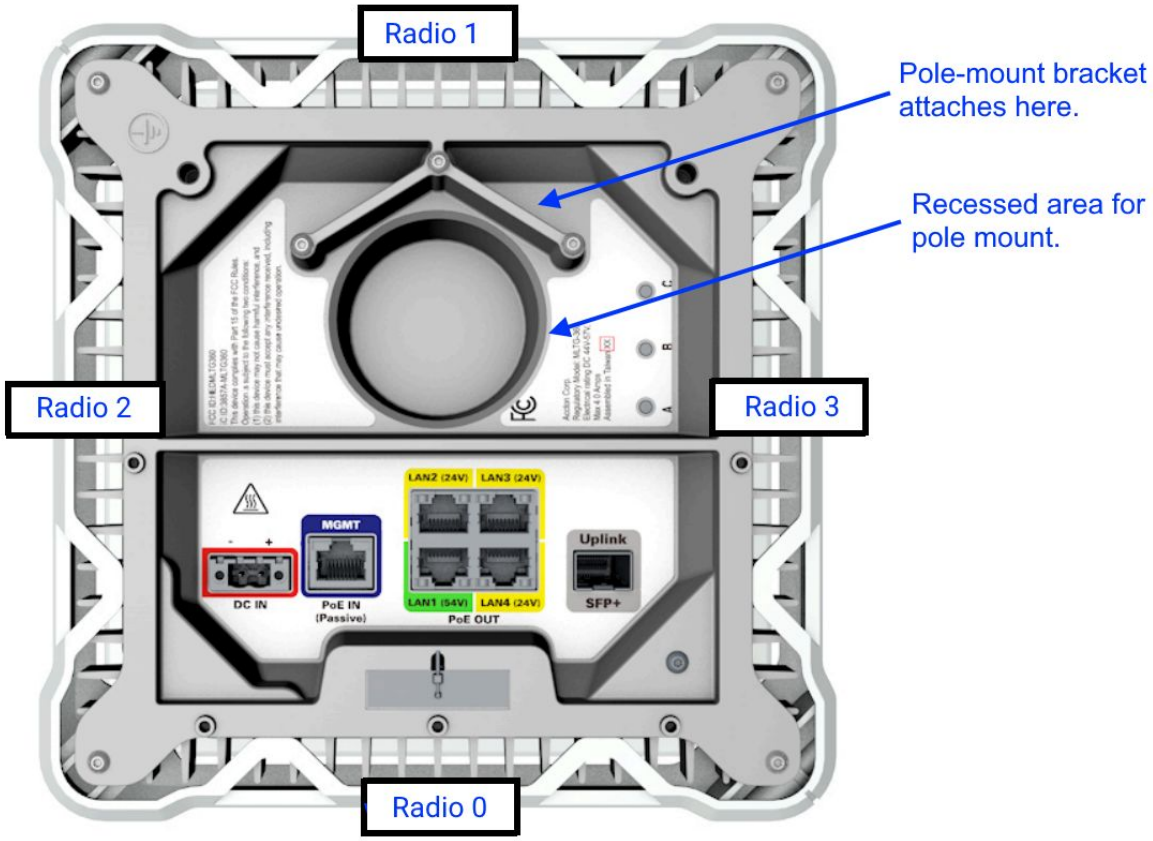
*A passive (non-IEEE) PoE injector that can provide 90 W at 56 V, such as the one supplied is required.

The K60DN is a distribution node that supports the Altowav Gen3 Platform for 60 GHz wireless. The K60DN has four radio interfaces, one per side, which form four 90° sectors to provide 360° degree coverage.

To ensure SFP 10 G transceiver performance at a fiber access site, the SFP+ port module and transceiver cable for the K60DN unit(s) to be installed for fiber access must be supplied by the network installation Engineer or Design team.

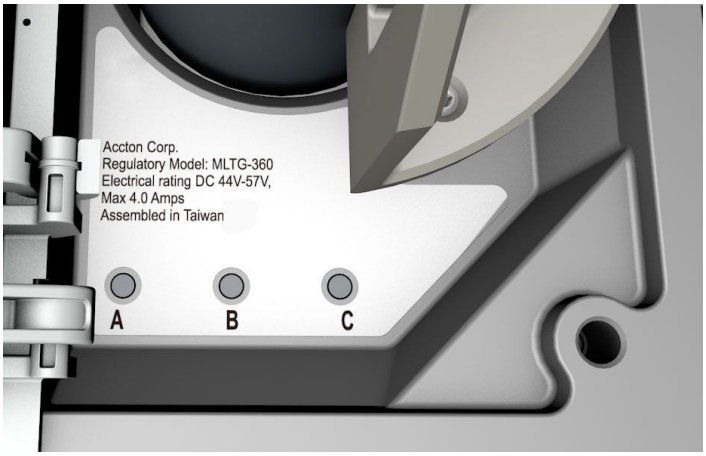
The bottom view below, shows the radio locations, the brace for the pole-mount bracket, the recessed area for pole mounting which fits a 1.57" - 2" diameter (4-5 cm) pole, and port labels.

Bottom view of K60DN



LED Indicators

LEDs on the bottom of the K60DN show connections and activity.



- **A** indicates an external Ethernet link.
- **B** is lit to show connection to power and normal operation.
- **C** indicates wireless link(s).

See LED Indicator Lights for a description of more LED sequences.

Network Design Information Required

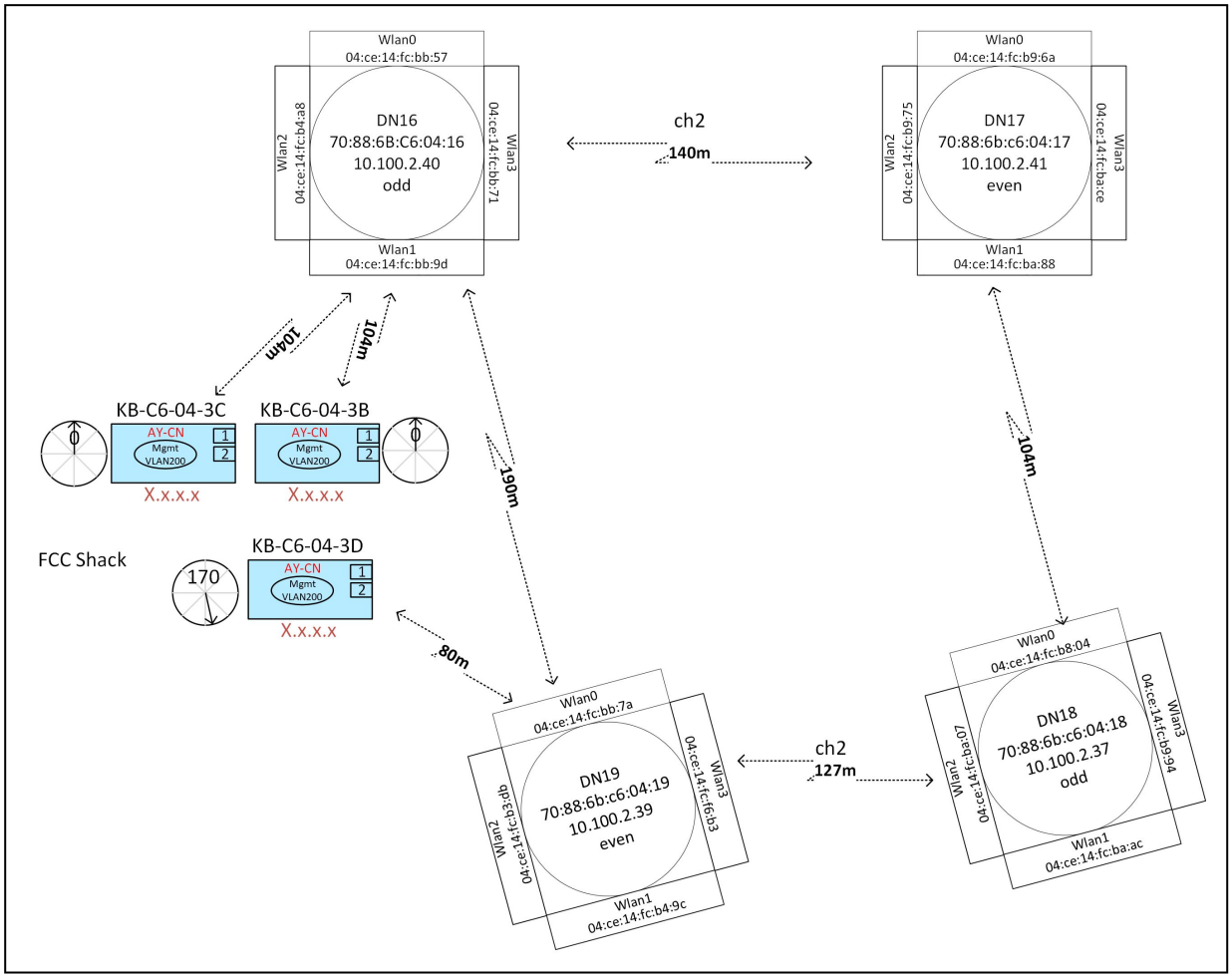
Before installation the network design should be well planned and documented. Having a detailed network diagram available during bench configuration and installation helps avoid costly, time-consuming adjustments after install. Required information for bench configuration and installation includes:

- The MAC address of the device, and the four radio interface MAC addresses for the four sectors on each K60DN. To find these, scan the 2D barcode on the Altowav label on the side of the unit or on the box. The KB MAC address (KB-C6-XX-XX) is also on the side label.

Label sticker on Radio 1 (wlan1) side of K60DN

- The planned channel, Golay index and polarity for each radio interface on this K60DN.
- The MAC address for other K60DN radio interfaces to be connected to this K60DN. This information is entered on the Wireless tab of the WebUI in the **DN responder** field.
- The KB MAC addresses for K60CN1s to be connected to this K60DN. This is entered in on the Wireless tab of the WebUI in the **CN responder** field. CN responders should be added at the time they are installed, not before.
- The Management VLAN ID and PVIDs for this network site.
- The site location for installation. This is used for configuring the device's Location/ Description information and for preparing for the physical installation.

This simple network diagram shows an example of how to communicate the required information. In this case there is no elevation adjustment noted.



Tip: Adopt standard conventions and practices to help simplify design, installation and reading detailed network diagrams.

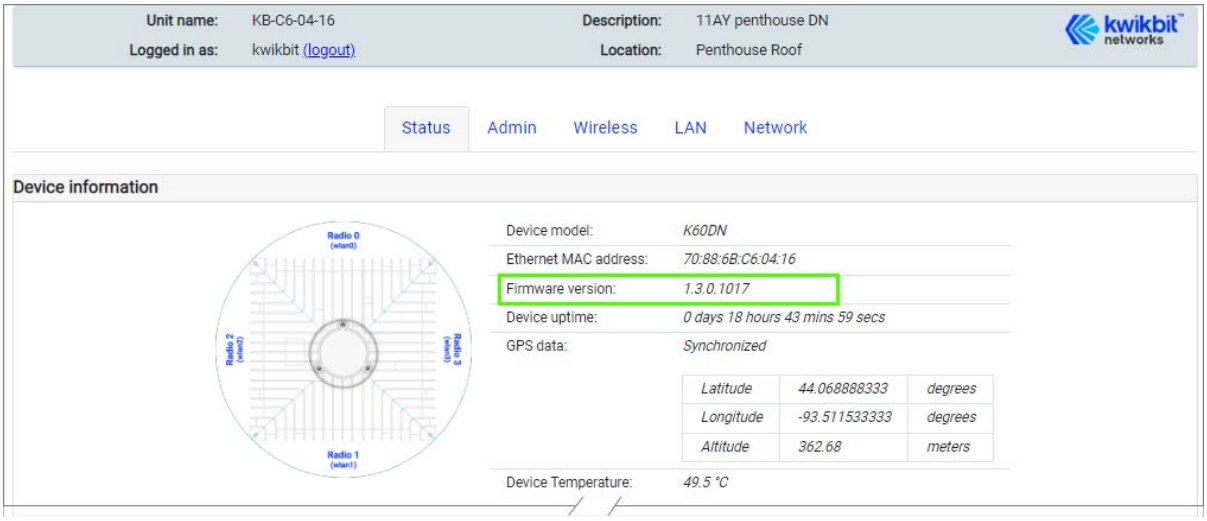
- **Boresight:** Position K60DNs to make K60DN-K60DN links as close to boresight as possible.
- **Distance:** The shorter a K60DN-K60DN link, the better the performance.
- **Straight-line topologies:** Avoid using Radio 2 and Radio 3 for straight-line topology since they share a data bus. Using Radio 0 and Radio 1 will maximize traffic speeds because they have individual data buses.

Bench configuration:

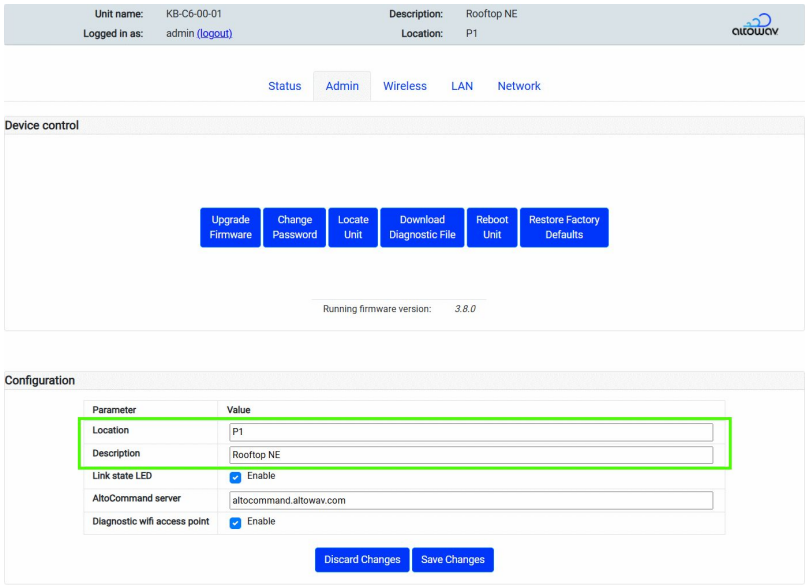
Bench configuration is strongly recommended before installing K60DNs in a distribution network. This ensures the distribution network devices are configured consistently before installation on poles or other difficult to access locations. The steps below use the WebUI for configuration.

1. Connect the **MGMT PoE In** port of the K60DN to the **OUT** port of the passive PoE injector supplied with the K60DN. A passive (non-IEEE) PoE injector that can provide 90 W at 56 V is required. Connect the Internet-connected switch or PC to the **IN** port of the PoE injector.

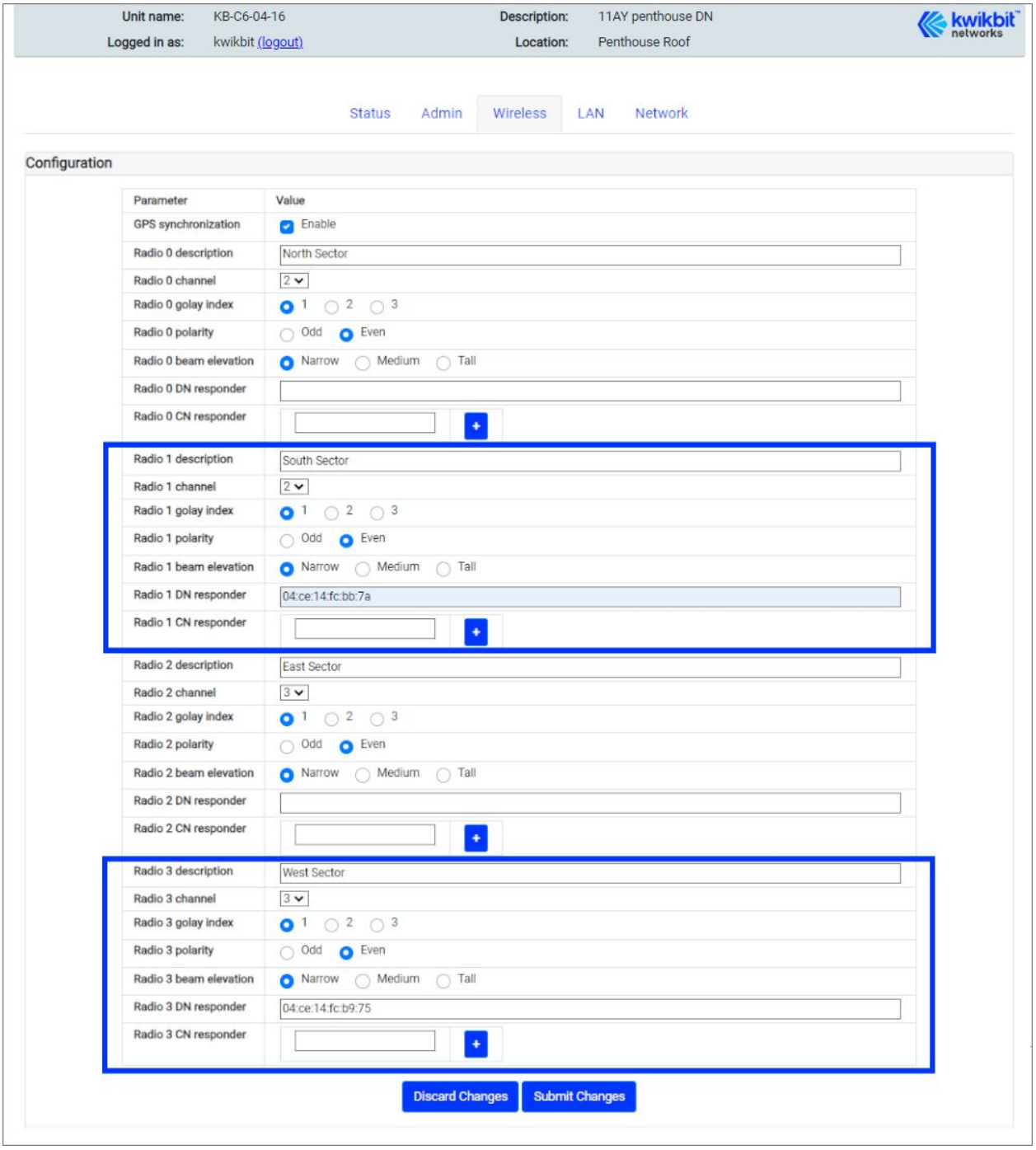
2. K60DNs default to DHCP. Access the WebUI by browsing to the IP address. For example, enter **https://<ip address>/** into the browser's address bar.
   A. A warning screen displays. Click the **Advanced** button and then **Proceed to...**
   B. The WebUI opens at the Status tab. Clicking another tab requires you to enter the password: **admin** (for release 1.8.1 and earlier, the default password is **kwikbit**).
3. On the **Status** tab or the **Admin** tab, determine the current Firmware version and note whether this K60DN needs an upgrade.



4. On the **Admin** tab, enter the **Location** and **Description** for the device and click the **Save Changes** button. If a firmware upgrade is required, use the **Upgrade Firmware** button to browse to the new firmware version and install it.



5. On the **Wireless** tab, set the **Channel**, **Golay index**, **Polarity** and enter the MAC address for the **DN responder** (the radio interface on the remote end of the K60DN-K60DN link). Refer to the detailed network diagram for this information. The following sample shows DN16 in the network diagram with **DN responder** filled out for RF connections on Radio 1 and Radio 3.



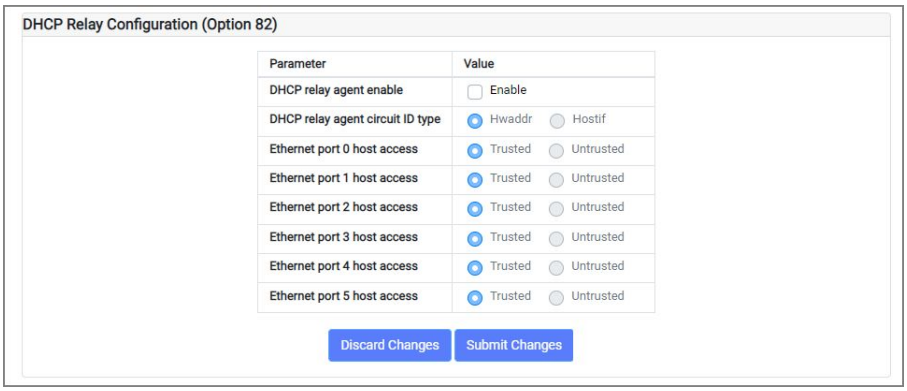
Click the **Submit Changes** button.

> **Tip:** Stay on this tab and verify links are reset and the Wireless Status table updates. This ensures that settings and links are complete before making additional changes.

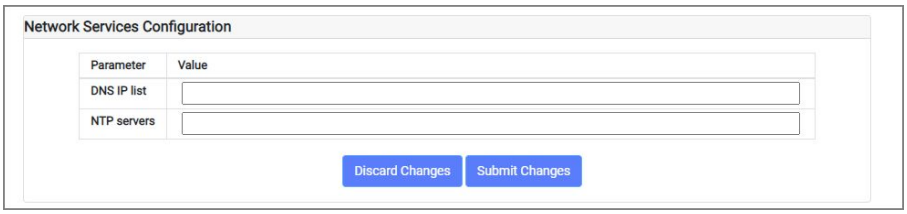
Note: It is best practice to add/remove K60CN1s to the CN responder list at the time they are installed or removed.

6. Review settings on the **LAN** tab, make sure the ports are enabled as needed for the K60DN.

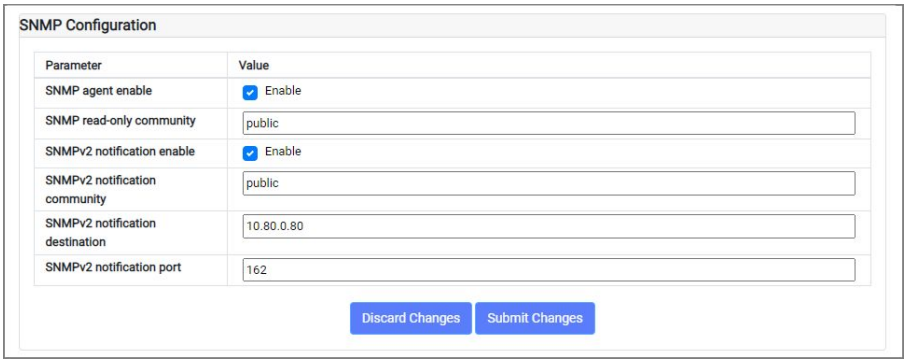
7. Adjust settings on the **Network** tab and **Submit Changes** after each section:
   A. DHCP Relay (Option 82).



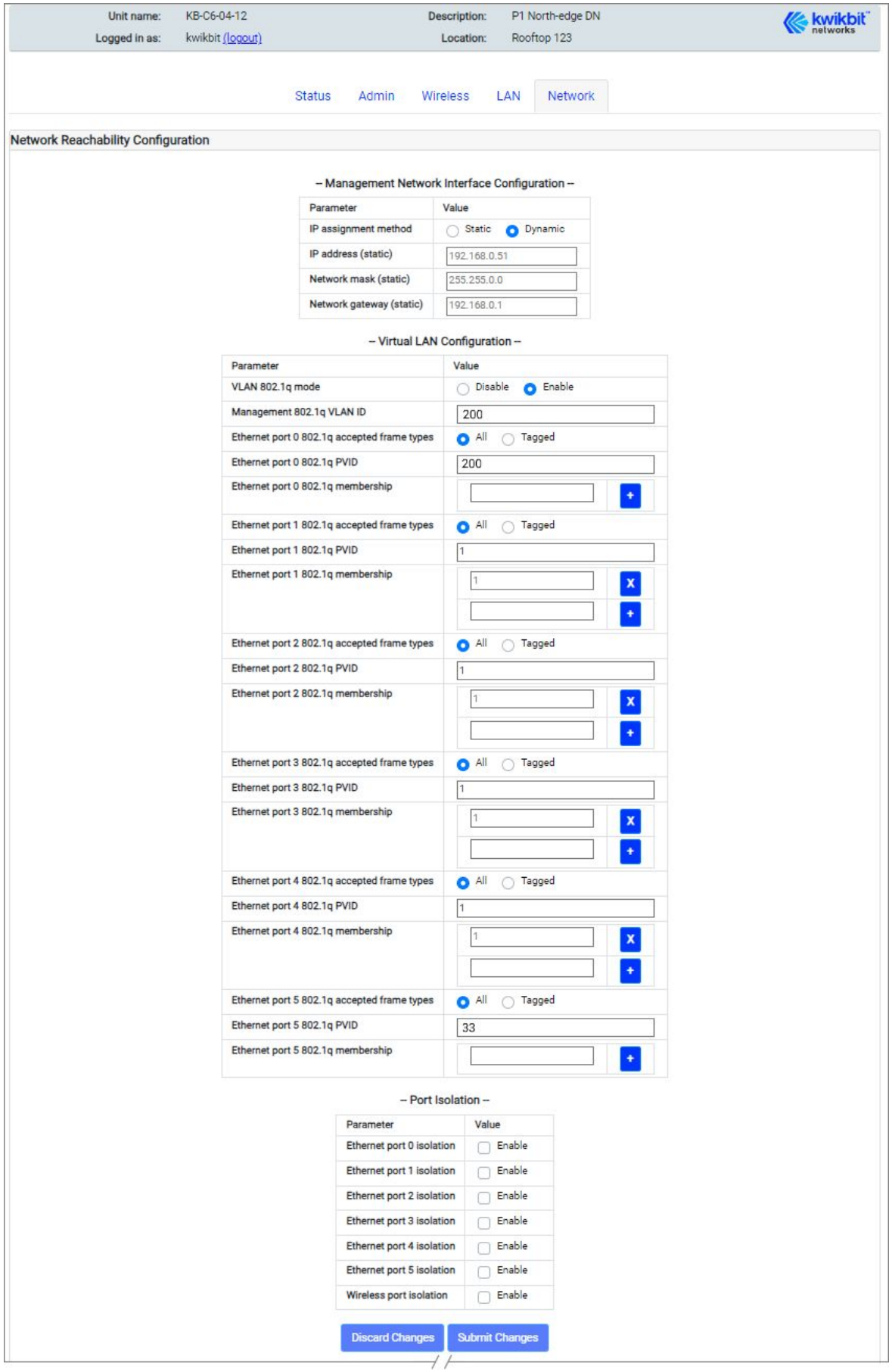
   B. Network Services DNS.



   C. SNMP Configuration.



   D. Network Reachability Configuration including Management Network Interface config, VLAN ID, frame type, PVIDs Frame type.


Unit name: KB-C6-04-12
Logged in as: kwikbit (logout)
Description: P1 North-edge DN
Location: Rooftop 123
kwikbit networks
Status
Admin
Wireless
LAN
Network
Network Reachability Configuration
-- Management Network Interface Configuration --
Parameter
Value
IP assignment method
Static
Dynamic
IP address (static)
192.168.0.51
Network mask (static)
255.255.0.0
Network gateway (static)
192.168.0.1
-- Virtual LAN Configuration --
Parameter
Value
VLAN 802.1q mode
Disable
Enable
Management 802.1q VLAN ID
200
Ethernet port 0 802.1q accepted frame types
All
Tagged
Ethernet port 0 802.1q PVID
200
Ethernet port 0 802.1q membership
Ethernet port 1 802.1q accepted frame types
All
Tagged
Ethernet port 1 802.1q PVID
1
Ethernet port 1 802.1q membership
1
Ethernet port 2 802.1q accepted frame types
All
Tagged
Ethernet port 2 802.1q PVID
1
Ethernet port 2 802.1q membership
1
Ethernet port 3 802.1q accepted frame types
All
Tagged
Ethernet port 3 802.1q PVID
1
Ethernet port 3 802.1q membership
1
Ethernet port 4 802.1q accepted frame types
All
Tagged
Ethernet port 4 802.1q PVID
1
Ethernet port 4 802.1q membership
1
Ethernet port 5 802.1q accepted frame types
All
Tagged
Ethernet port 5 802.1q PVID
33
Ethernet port 5 802.1q membership
-- Port Isolation --
Parameter
Value
Ethernet port 0 isolation
Enable
Ethernet port 1 isolation
Enable
Ethernet port 2 isolation
Enable
Ethernet port 3 isolation
Enable
Ethernet port 4 isolation
Enable
Ethernet port 5 isolation
Enable
Wireless port isolation
Enable
Discard Changes
Submit Changes

8. Close the browser window and remove the PoE cable. The K60DN is now ready for installation at the network site.

Prepare the Procet-1N for Installation

Prepare the Procet-1N power supply (Altowav Model: AX-PSW-OD-P100-4C1) for installation before going on site:

- Install the AC line for connection to power.
- Attach the DC terminal plug to an appropriate length of outdoor-rated CAT6 cable (when using preferred power Option A).

See *Connecting_the_K60DN_to_Procet-1N* for more details about power options.

K60DN Installation at Distribution Network Site

Installation tips:

- Install the K60DN on the top of a pole with no obstructions above the unit to enable the GPS synchronization.

  For cases where pole-top installation cannot be done, or for poles up to 10” in diameter, a K60DN Mounting J Bracket, (Altowav Model: AX-K60DN-JMOUNT), may be used. Keep in mind, the unobstructed sky view is required for GPS.
- Maintain clear line of sight (LOS) at the sides of the K60DN for links.
- **Power source: A DC power source is recommended** because PoE power output for the K60DN LAN ports can only be supplied when the power source is DC. The outdoor Procet-1N is recommended (Altowav Model: AX-PSW-OD-P100-4C1).

  If the PoE power option is used: The PoE injector required to power the K60DN via the MGMT PoE In port is a passive (non-IEEE) injector that can provide 90 W at 56 V. See *Connecting_the_K60DN_to_Procet-1N* for more details about power options.

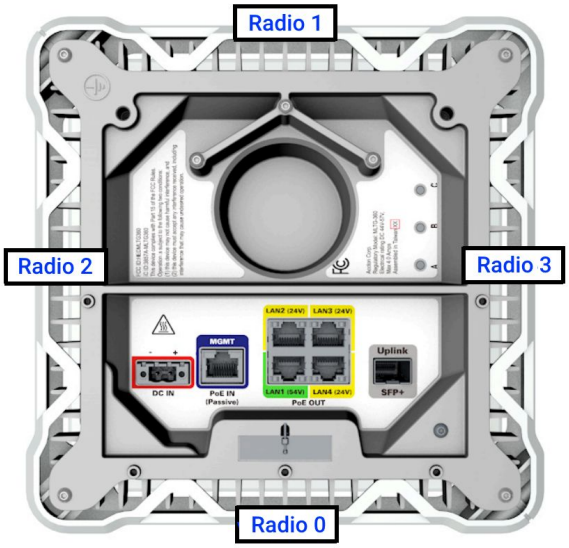
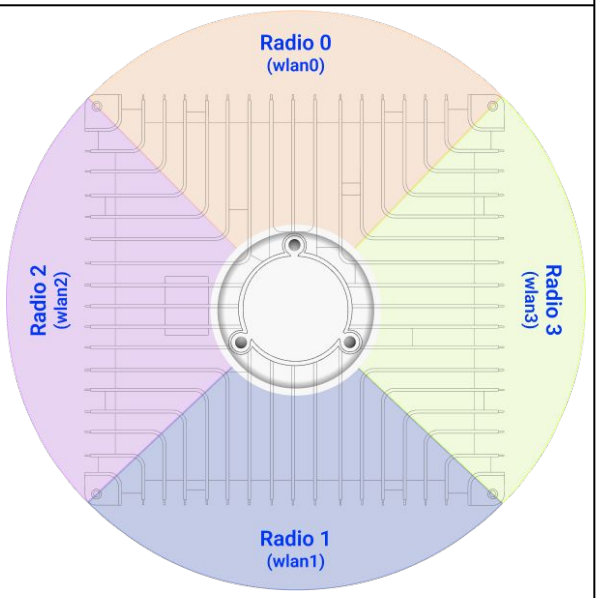
  Note: DC power and PoE power cannot be connected to the K60DN at the same time.
- Installation begins with the K60DNs at the point of presence (PoP) and proceeds outward to enable testing of connections and verifying configuration as the K60DN devices come online.
- Maximize performance for straight-line topology by running through Radio 0 (wlan0) and Radio 1 (wlan1) because they have independent data buses. Radio 2 and Radio 3 share a bus.
- When adjustments to positioning or aiming the K60DN are done after the K60DN has connected to other devices, power cycle the unit. To power cycle, simply disconnect the K60DN from power and reconnect it.

How to determine the position of Radio 0-3 (wlan0-3) in various orientations

These views may be useful for installation or maintenance.

Out of the box	Mounted on a pole in the field
 Radio 1 (wlan1) on the label sticker side.	Radio 3 (wlan3) Radio 1 (wlan1) on the label sticker side.  Radio 0 (wlan0) on the port cover (cable tray) side. Radio 2 (wlan2)

Bottom and top views may be useful for design and configuration purposes.

Bottom view of K60DN	Top view of K60DN radio sectors
	
From the bottom view, Radio 1 (wlan1) is on the same side as the pole mount bracket. Radio 0 (wlan0) is on the side nearest the ports.	From the top view, Radio 0 (wlan0) is on the side on which one of the three top screws is centered. Radio 1 (wlan1) is on the same side as two of the top three screws.

Note: Radio 0-3 interfaces are also known as wlan0 - wlan3 in configuration parameters accessed through the CLI and REST API.

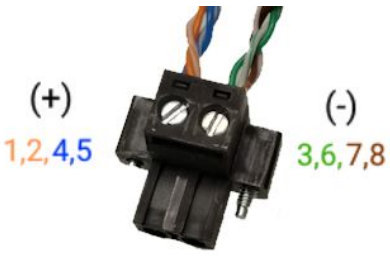
At the installation site:

1. **Attach the ground wire to the ground screw.** The other end will connect to nearby good earth. Local codes determine whether grounding is required or optional.

2. **Install connections per the network design:** Steps for the PoP node are different than other K60DNs in the network.
    - **For the PoP node:** The PoP node may be connected to fiber via the **Uplink SFP+** port. Connect the outdoor-rated transceiver cable to the K60DN **Uplink SFP+** port, according to your network design. Then connect any LAN connections per network design.

    - **For K60DN units that are not PoP nodes**: Install cable for any LAN ports on the K60DN per the network design. If there are no LAN connections go to the next step.
3. **Connect to power**. For the recommended Option A: Connect **PoE1** on the Procet-1N power supply to the **DC In** terminal on the K60DN using the custom CAT6 terminal plug. Wire the DC plug making sure the correct wires are connected to the terminals, (+) orange and blue, (-) green and brown, as shown below.

    Note: PoE out for LAN ports is only available with DC power supply. See *Connecting the K60DN to Procet-1N* for more about power options.



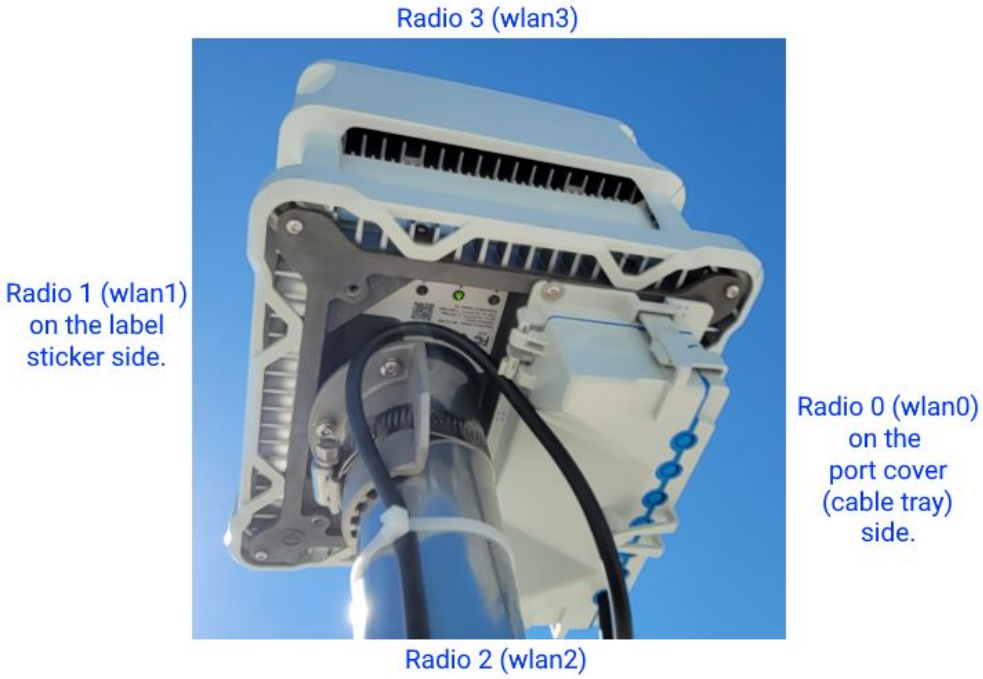
PINS	T568B Color
Pin 1	white/orange stripe
Pin 2	orange solid
Pin 3	white/green stripe
Pin 4	blue solid
Pin 5	white/blue stripe
Pin 6	green solid
Pin 7	white/brown stripe
Pin 8	brown solid

> **Tip:** Twist the wires together before inserting into the plug. This helps avoid shorts or nicks and makes insertion easier.

Verify that power is on -- LED B is lit.

4. **Attach the pole mount bracket and port cover to the K60DN**.
5. **Mount the K60DN on top of a 1.57-2 in diameter (4-5 cm) pole, with no obstructions above the unit to enable the GPS synchronization:** Attach the pole mount bracket to the K60DN. Place the indentation on the bottom of the K60DN at the top of the pole and secure

the mounting bracket to the pole with the band clamp. Make sure that Radios 0-3 on the K60DN are oriented according to the network design.



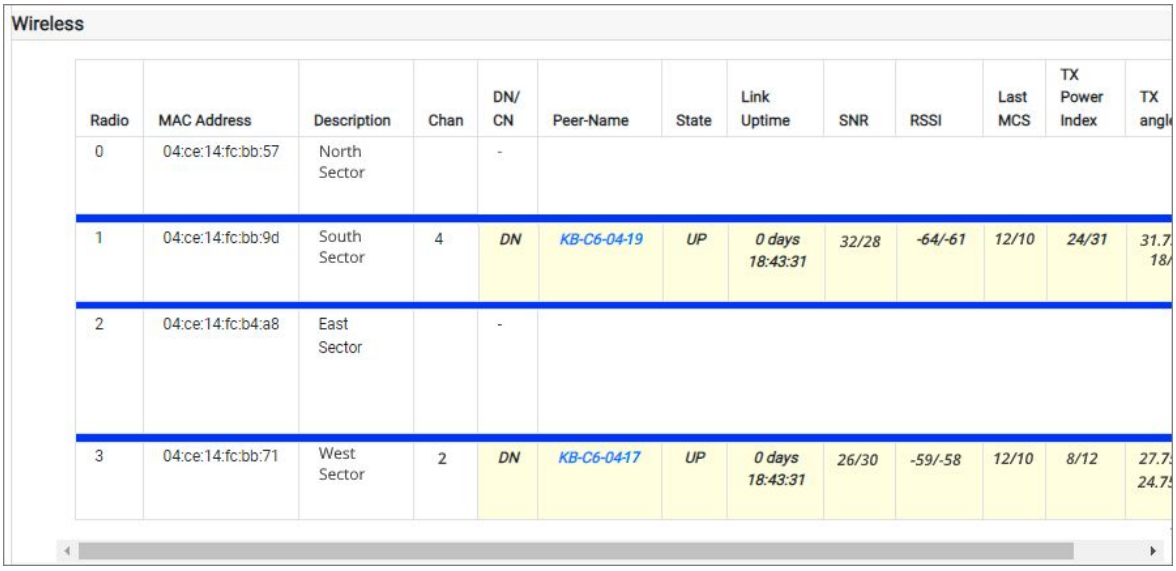
Note: The top of the K60DN must remain unobstructed to enable GPS synchronization. Sides must remain unobstructed to enable LOS with other radio interfaces.

Note: Optionally, use a K60DN Mounting J Bracket, (Altowav PN: AX-K60DN-JMOUNT), to mount the K60DN to the side of a pole, up to 10" in diameter. (J Bracket is not supplied unless requested.)

6. **Install the remaining K60DN devices according to the detailed network diagram.** Work outward from the fiber access.
7. **When all K60DN devices are installed and powered up verify connections.** Ensure that each K60DN is found and review performance, adjust and fine tune before finalizing the installation.

   Note: If the K60DN is repositioned or re-aimed after K60DN-K60DN connections are made, re-beamform the link by resetting the responder for the link, rebooting or power cycling the unit. Resetting the responder is the preferred method when the K60DN has any other wireless links.

   - **Verify through the WebUI** that each K60DN is connected to the correct K60DNs per the network design. This sample of the Wireless table the Status tab shows the K60DN connections for DN16 on Radio 1 and Radio 3, as shown in the sample design diagram above.



Wireless

Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	State	Link Uptime	SNR	RSSI	Last MCS	TX Power Index	TX angl
0	04:ce:14:fc:bb:57	North Sector		-								
1	04:ce:14:fc:bb:9d	South Sector	4	DN	KB-C6-04-19	UP	0 days 18:43:31	32/28	-64/-61	12/10	24/31	31.7 18/
2	04:ce:14:fc:b4:a8	East Sector		-								
3	04:ce:14:fc:bb:71	West Sector	2	DN	KB-C6-04-17	UP	0 days 18:43:31	26/30	-59/-58	12/10	8/12	27.7 24.7

- **Check signal quality.** For example, a K60DN-K60DN link should have an RSSI of greater than -65. For K60DN-K60DN link distances of up to 185 m, expect an MCS level of 12 with significant traffic. For K60DN-K60CN1 links expect an MCS level of 9.

Connecting to the K60DN and K60CN1

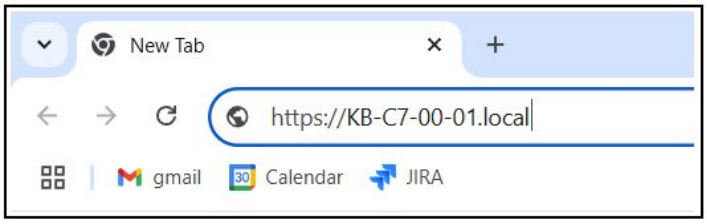
By default, AltoPlex radios use dynamic IP address assignment and, beginning with release 3.6.0, have a factory default fallback static IP address of 192.168.0.1.

Additionally:

- Radios can be configured to use a static IP address, rather than dynamic IP address assignment. This will override the fallback IP unless the radio is factory reset. After a factory reset, it will return to default behavior.
- Radios upgraded to release 3.6.0 that have not been factory reset will have a factory default fallback IP address of 192.168.0.51, unless they have a configured static IP address that overrides the default address. After a factory reset, they will have the default behavior.

Because AltoPlex radios participate in multicast DNS (mDNS), computers that support mDNS and are on the same subnet as the radio can connect to the radio by using its hostname. In general, this should work regardless of whether the radio is configured to use dynamic or static addressing, or if it is using the fallback default IP.

For example, if your radio's hostname is KB-C6-00-01 and your computer is on the same subnet as the radio, you can access the WebUI by typing **https://KB-C6-00-01** (or **https://KB-C6-00-01.local**) into your browser's URL address bar:



Use the factory default fall-back IP address to connect to the radio

This section applies to radios with firmware version 3.6.0 or newer. Radios with older firmware have a unique fallback link local IP address that was provided on a printed label when the device was manufactured. For devices originally manufactured with a software version prior to 3.6.0 and then upgraded to release 3.6.0 or newer, the default IP address will depend on whether the device has been factory reset since the upgrade:

- If the device has not been factory reset, the default IP address is 192.168.0.51.
- If the device has been factory reset, the default IP address is 192.168.0.1.

To connect to an AltoPlex radio by using its default fallback IP address:

1. Configure your computer to be a member of the 192.168.0.*x* subnet.

   For example, on Windows 11:

   A. Click the **Windows** icon.
   B. Click **Settings**.
   C. Click **Network & internet**.
   D. Click **Ethernet**.
   E. For **IP assignment**, click **Edit**.
   F. Select **Manual**.
   G. Click to toggle on **IPv4**.
   H. For **IP address**, type an address in the 192.168.0.*x* subnet (for example, **192.168.0.2**).
   I. For **Subnet mask**, type **255.255.255.0**.
   J. Click **Save**.

2. Next, either:
   - Plug your computer's Ethernet connection into the **LAN** port of a PoE injector that is connected to the radio.

     > **Tip:** The LAN port is sometimes labeled as the **Data out** port, the **Out** port, or something similar.

   - Plug both your computer and the radio into a PoE switch.

     > **Tip:** To access the radio by using the default IP address, make sure that the switch is not connected to the backhaul network or that the backhaul network does not have a DHCP server running on it.

3. Access the radio's WebUI by entering either the hostname (for example, **https://KB-C6-00-01**) or the default IP address (**https://192.168.0.1**) in the address bar of a web browser.

   Note: If a radio has a configured static IP address that is different than the default address, the configured IP address must be used to access the radio.

4. A warning message may indicate that the self-signed certificate used by the device is not recognized by the browser. Instructions to clear the message vary depending on the browser. For example, in Chrome:
   A. Click **Advanced**.
   B. Click **Proceed to...**

The WebUI will open with the **Status** tab displayed.

Determine the IP address of a radio by using mDNS

If you configure a radio to use a static IP address and subsequently do not remember the IP address, you can use mDNS commands to determine the radio's IP address.

Note: This requires that your computer supports mDNS and is on the same subnet as the radio.

- Windows Powershell:
  `Resolve-DnsName <hostname>`
- MacOS:
  `dns-sd -G v4v6 <hostname>`
- Linux:
  `avahi-resolve-host-name -4 <hostname>.local`

where <hostname> is the hostname of the AltoPlex radio (KB-XX-XX-XX).

Access the radio by using the management Wi-Fi access point

AltoPlex radios also provide a mechanism to access all radios through a management Wi-Fi access point, which is enabled by default but can be disabled. See Wi-Fi connection to a K60DN and K60CN1 for more information.

K60DN Configuration via WebUI

The K60DN can be configured through its WebUI, before or after it is connected to the distribution network.

How to access the WebUI before installation, for bench configuration: To access the WebUI before installation or connection, power the K60DN with the supplied passive PoE injector. (Note, a passive (non-IEEE) PoE injector that can provide 90 W at 56 V is required.)

1. Connect the **MGMT PoE In** port of the K60DN to the **OUT** port of the passive PoE injector supplied with the K60DN. Connect the Internet-connected switch or PC to the **IN** port of the PoE injector.
2. K60DNs default to DHCP. Access the WebUI by browsing to the IP address. For example, enter **https://<IP address>/** into the browser's address bar.
    A. A warning screen displays. Click the **Advanced** button and then **Proceed to...**
    B. The WebUI opens at the Status tab. Clicking another tab requires you to enter the password: **kwikbit**.

How to access the WebUI for K60DN units that are already part of a network: After the K60DN is connected to the distribution network, you can access the WebUI using one of the following methods.

- Enter the IP address of the K60DN into a browser address bar from a PC connected to the network. For example, **https://<IP address>/**.
- Link from the Wireless table of a connected K60DN's WebUI by clicking the name of the K60DN to configure in the **Peer Name** column of that table.
- If using the Altowav Gen3 Edge Controller (v2.4.7 or higher), access the WebUI from the Devices page. (On the row of the device to configure, click on the (**...**) in the settings column and select the **Connect to Device** option.)

Common tasks for configuration:

- View information about the device, its firmware version, its wireless connections, its LAN interfaces, and Management interfaces on the Status tab. You can also click on a **Peer-Name** to access the WebUI for a connected device.
- Click on the **Admin** tab and do one of the following: **Change Password**, set **Location** or **Description** per your network design plan, or upgrade the firmware version.
- Click on **Wireless** tab and do this in the Configuration section: set **Channels**, **Golay** codes, and **Polarity** per your network design. Set **CN responder** (KB MAC) to form connection

with installed K60CN1s. Set **DN responder** (MAC address for a radio interface on a connecting K60DN). All connections to be made per your network design.

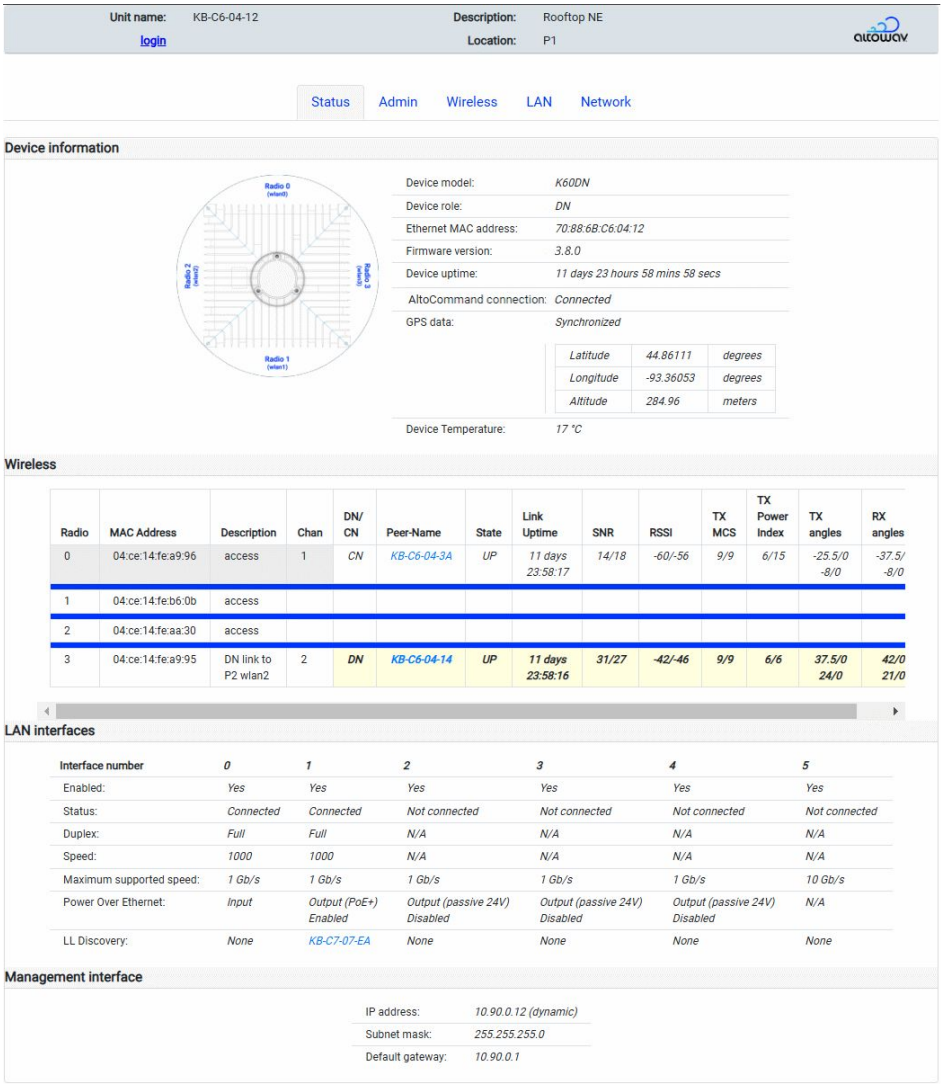
- On **Network** tab, set network config items for Management, VLAN.

The header of the WebUI shows the Unit name of the K60DN, (also called the KB MAC), Description and Location, as well as offering a **login** link. Login is not required to have read-only access to the WebUI, but is required to set configurations on any other tab of the WebUI.

Tip: The header background changes from gray to yellow when a unit is unreachable.

Status tab:

The Status tab shows a summary of information about the unit, its wireless and LAN connections, and interface information. Logging in is not required to view Status information, but clicking any tab triggers a log in prompt.



Device Information

This section shows the model name, Ethernet MAC address (MGMT PoE port MAC), firmware version, device uptime, status of the AltoCommand server, GPS data, and device temperature.

> **Tip:** The Status tab shows the current firmware version. Firmware can be updated using the **Upgrade Firmware** button on the Admin tab. It is recommended that all K60DNs in the network use the same firmware version.

Wireless

The table in this area shows Wireless link status for the K60DN. Information includes the Radio number, MAC Address, Description, Channel, model (DN or CN), Peer-Name for connected

devices, State (UP or DOWN), Link Uptime SNR, RSSI, Last MCS, TX Power Index,TX angles, RX angles. Use the horizontal scroll bar to view all values.

A light yellow background highlights the K60DN-K60DN connections.

Wireless

Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	State	Link Uptime	SNR	RSSI	Last MCS	TX Power Index	TX angles	RX angles
0	04:ce:14:fc:b5:06	toward se	2	DN	KB-C6-04-BE	UP	42 days 22:47:39	11/11	-63/-62	9/9	16/15	22.5/0 0/0	22.5/0 0/0
1	04:ce:14:fc:ba:2f	radio 1 description not set		-									
2	04:ce:14:fc:b9:92	toward fcc	3	DN	KB-C6-4C-A5	UP	14 days 20:29:42	13/11	-60/-62	9/9	16/17	-7.5/0 -4.5/0	-7.5/0 0/0
				CN	KB-C6-04-3D	UP	0 days 03:40:16	11/13	-62/-59	9/9	17/18	16.5/0 8/0	16.5/0 8/0
3	04:ce:14:fc:ba:74			-									

> **Tip:** Hover over the heading where multiple values are shown for a tool tip describing the values.

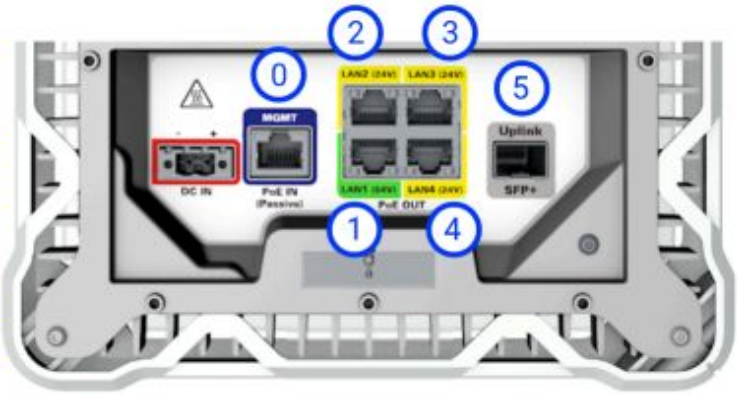
Values for **SNR, RSSI**, **Last MCS** and **TX Power Index** show values for both ends of the link – local and remote.

Values for **TX angles** and **RX angles** show local radio azimuth/elevation angles and remote radio azimuth/elevation angles. If that information is unavailable, the beam index -- a single value -- is listed.

LAN interfaces

This area shows information for all LAN interfaces, including whether a port is enabled, its Status (Connected or Not connected), Duplex mode, Speed, Maximum supported speed, and PoE mode.

LAN Interface number	Label on K60DN port
0	MGMT (PoE in)
1	LAN1 (54V) PoE out
2	LAN2 (passive 24V) PoE out
3	LAN3 (passive 24V) PoE out
4	LAN4 (passive 24V) PoE out
5	Uplink SFP+



If the Ethernet port is connected via a switch to any LAN peers that are also AltoPlex devices, they will be listed in the **LL Discovery** field.

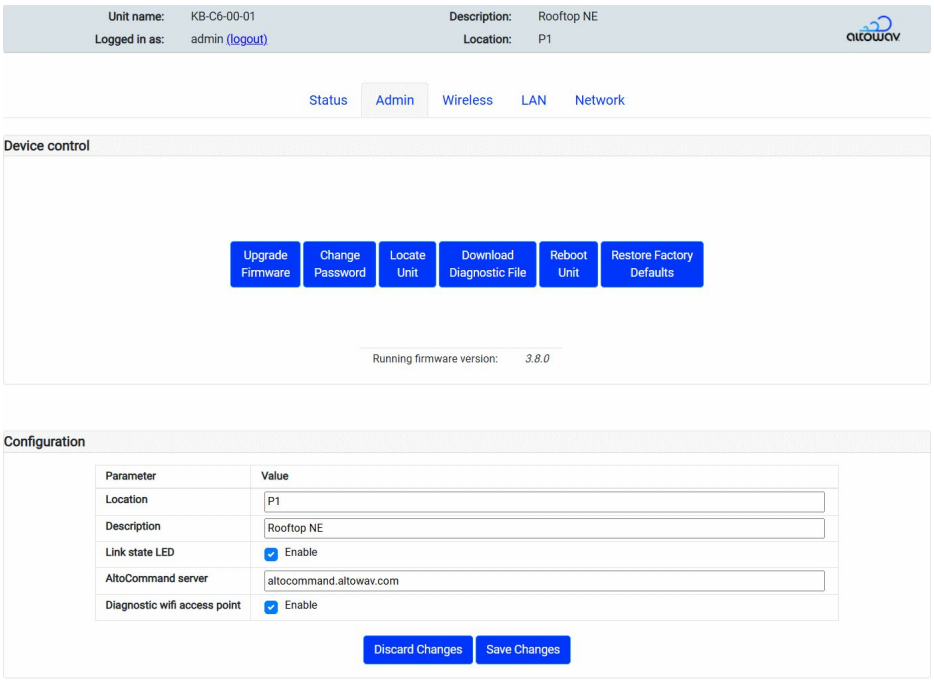
Management interface

This area lists the MGMT interface IP address, Subnet mask and Default gateway. It also shows how the IP was assigned (dynamic or static.)

Admin tab

The Admin tab has options for administrative tasks such as rebooting, restoring factory defaults, upgrading, changing the password, locating a unit, downloading a diagnostic file, as well as setting the unit's location and description.

Typical configuration tasks include entering a Location and Description for the K60DN, changing the password, and upgrading firmware.



Device Control

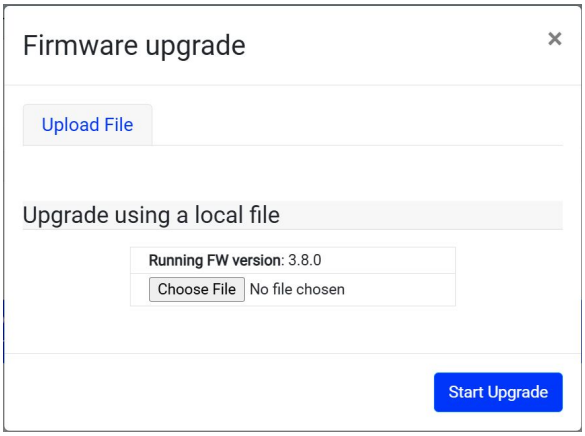
The installed version of firmware is listed here. This area also offers buttons to complete the following tasks:

Reboot – restarts the unit remotely.

Restore Factory Defaults – restores all device configuration to factory defaults. If the unit is unreachable and cannot be reset with this button, it may require a hard reset.

> **Note:** Factory reset returns the unit's password to the default: **admin** (For firmware version 1.8.1 or earlier, the default password is **kwikbit**). Since the IP assignment uses DHCP by default, the factory reset is not likely to affect the IP address of the K60DN.

Upgrade Firmware – updates the device firmware with the file you choose. Click the **Upgrade Firmware** button and upload or browse to the firmware upgrade file. Then click **Start Upgrade**. Note, the device will reboot as part of the upgrade process. See Upgrading Firmware for more detailed steps.



Change Password – Use this button to change the password, according to your organization's network policy.

Locate Unit – Click this button to put the unit into locate mode, where it flashes an LED signal for field personnel to identify the unit. For the K60DN, the LED sequence is LED **B** is on steady, while **A** and **C** are blinking.

Download Diagnostic File - Automatically downloads a detailed diagnostic text file for the device. The file contains detailed information about the device and its status at the time of the download. The file name includes the host name (KB MAC), the date and time. For example, a file named KB-C6-04-15_diag_2023-05-12-14-43-32.txt, means this is the diagnostic text file for unit KB-C6-04-15, created at 2:43:32 pm (UTC) on May 12, 2023.

Configuration

This area includes the following settings.

Location – indicates the physical location where the device will be installed.

Description – may include orientation, function, role or other information about the device.

Link state LED – enables / disables the LED for displaying the link state of the node.

AltoCommand server – enter the fully-qualified domain name or IP address of the AltoCommand server that this radio will connect to. After the connection to the AltoCommand server has been configured on the AltoPlex radio, the radio sends an approval request to the server. A user on the AltoCommand server must approve the request, which will open a reverse tunnel for communication between the server and the radio. Note that any connected CNs will inherit this setting.

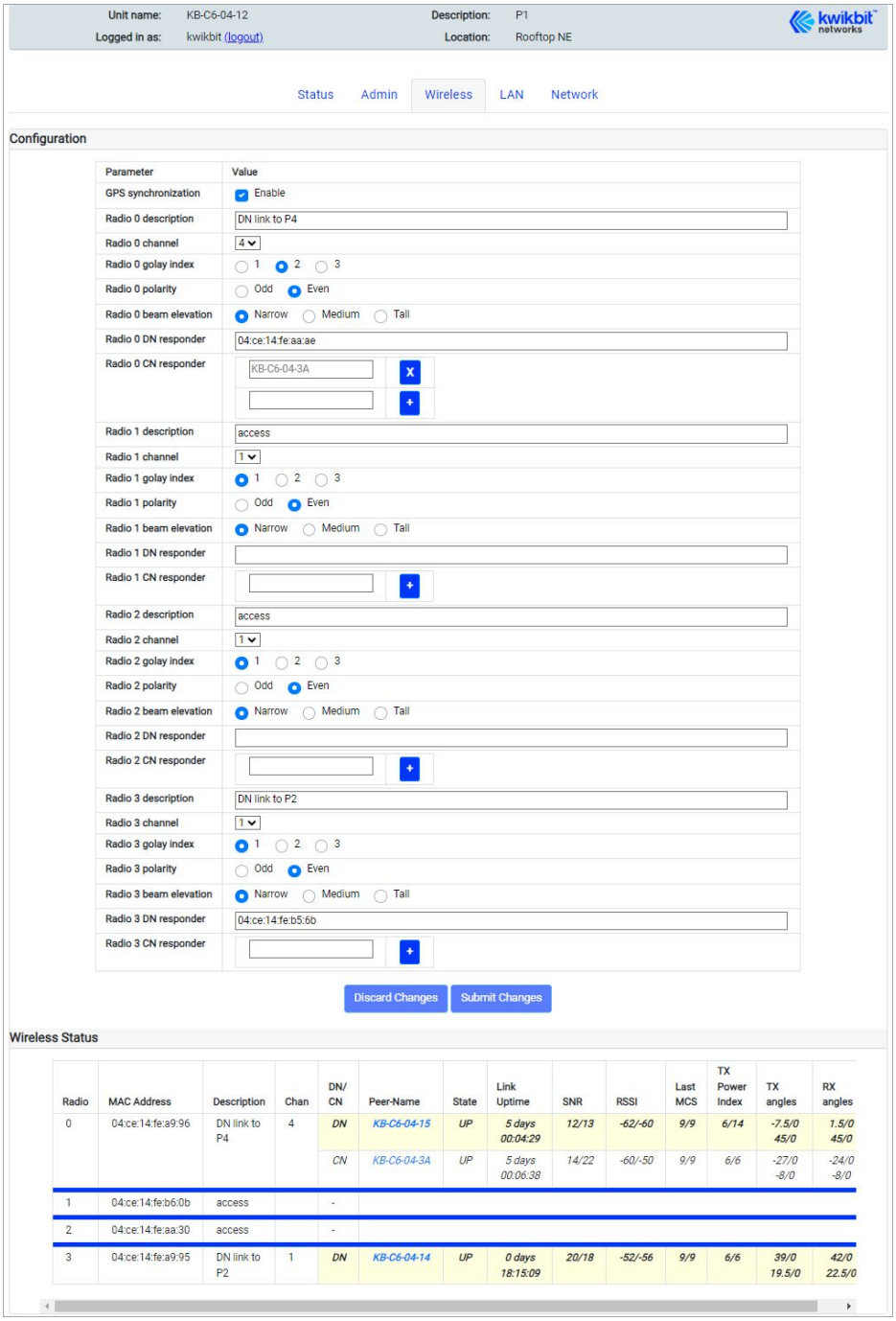
Diagnostic wifi access point – enables / disables Wi-Fi access for the unit. Default setting is enabled. See Wi-Fi Access to a K60DN for when and how to use the Diagnostic Wi-Fi access point.

Note: Disabling this setting turns off the Wi-Fi access point completely, (not just the Wi-Fi user interface). The device will not be seen by a Wi-Fi search when this setting is disabled.

Wireless tab

The Wireless tab includes a GPS synchronization checkbox, as well as settings for each radio interface including, radio description, channel, Golay index, polarity, DN responders, and CN responders. The Wireless status table is also included on this tab, enabling you to view the state of RF links, verify connections and browse to peers, as needed.

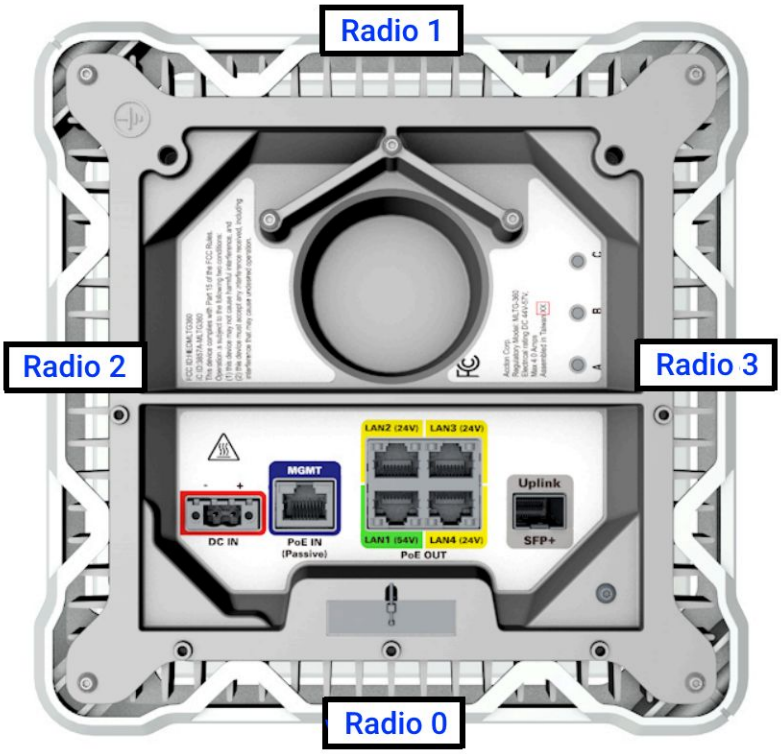
> **Tip:** After clicking **Submit Changes** stay on this tab until the links reset and the Wireless status table updates. This ensures that settings and links are complete before more changes are made.



Configuration

The Configuration section of the K60DN Wireless tab includes a setting for enabling/disabling **GPS synchronization**. The K60DN uses GPS for location and TDMA synchronization. Enabling/ disabling the GPS Synchronization cause the K60DN to reboot when the change is submitted.

The settings in this section are prefixed by the name of the wireless interface.



The following configuration settings are used to make each radio sector's links unique, in order to form and secure a wireless connection with another device.

Description enter a meaningful description to assist Field Technicians during installation or troubleshooting. For example, "East sector, directed to KB-C6-xx-xx".

Channel set the channel for radio sector, 1-4.

Golay index set the Golay index for the radio sector 1-3.

Polarity set polarity to odd or even for the radio sector.

Beam elevation set beam elevation for all wireless links on the sector, current and future. See Beam Elevation Settings - Design Considerations.

DN responder sets the MAC address for the K60DN radio interface on the remote side of the K60DN-K60DN link.

CN responder sets the list of KB MAC addresses for the connected K60CN1s. Note, it is best practice to add the CN responder KB MAC address to this list at the time of installation, not before.

The **Submit Changes** button resets the link configuration to the values selected. Configuration changes are shown in the Wireless Status table as they become complete.

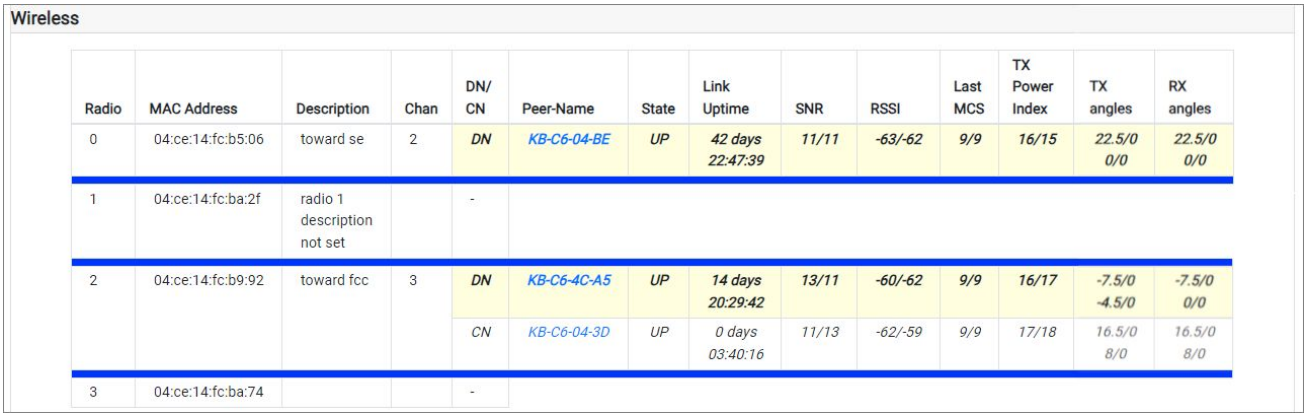
Note: Changes to **GPS Synchronization** cause a reboot of the device.

Wireless Status

The Wireless Status table is the same information shown in the Wireless table on the Status tab.

The Wireless Status area shows link status for each radio on the K60DN. Information includes the Radio number, MAC Address, Description, Channel, model (DN/CN), Peer-Name for connected devices, State (UP/DOWN), Link Uptime, SNR, RSSI, Last MCS, TX Power Index, TX angles and RX angles.

> **Tip:** During installation, the Wireless Status table makes it easy to access the WebUI for connected peers. To access the WebUI for a peer, click on the name listed under Peer-Name. A new browser tab opens for the named device's WebUI. See the K60CN1 Installation information for an example of how this is used.



Hover over column headings for brief descriptions of the values shown. Use the horizontal scroll bar to view all values in the table.

LAN tab

The LAN tab provides settings for enabling traffic and PoE on the LAN ports for the K60DN.

Note: PoE power output is available only when the K60DN is powered via **DC in**. See Connecting K60DN to the Procet-1N for more detailed information.

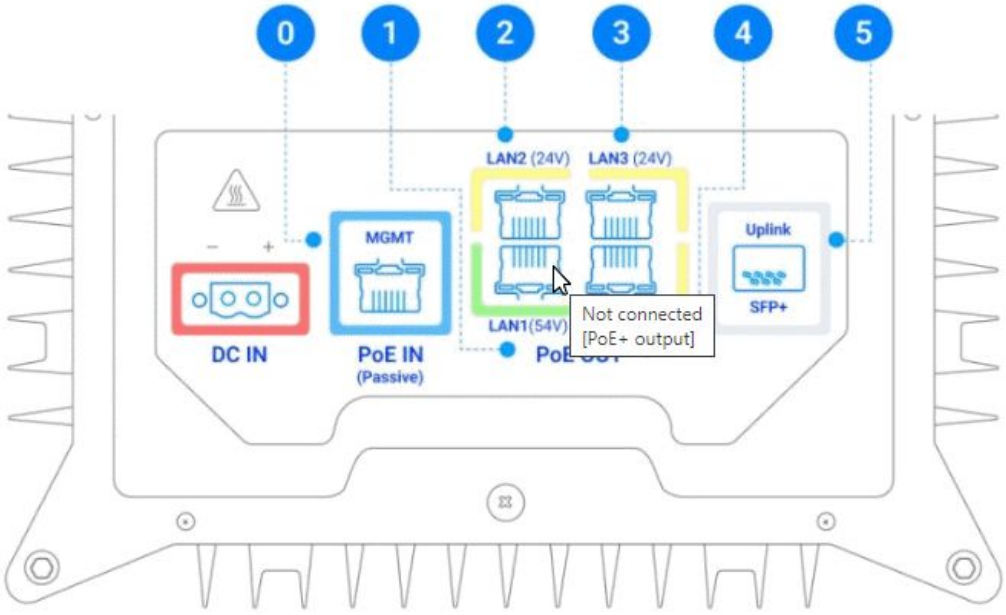
Unit name:	KB-C6-04-15	Description:	P4
Logged in as:	kwikbit (logout)	Location:	system location not set

Status | Admin | Wireless | LAN | Network

Ethernet Port Configuration

Interface number:	0	1	2	3	4	5
Port enable	☑ Enable	☑ Enable	☑ Enable	☑ Enable	☑ Enable	☑ Enable
PoE enable	N/A	☐ Enable	☐ Enable	☐ Enable	☐ Enable	N/A

Discard Changes | Submit Changes



MAC Filter Configuration

Parameter	Value
Ethernet port 0 mac limit	Unlimited
Ethernet port 0 destination mac address	
Ethernet port 0 unicast conversion	☐ Enable
Ethernet port 1 mac limit	Unlimited
Ethernet port 1 destination mac address	
Ethernet port 1 unicast conversion	☐ Enable
Ethernet port 2 mac limit	Unlimited
Ethernet port 2 destination mac address	
Ethernet port 2 unicast conversion	☐ Enable
Ethernet port 3 mac limit	Unlimited
Ethernet port 3 destination mac address	
Ethernet port 3 unicast conversion	☐ Enable
Ethernet port 4 mac limit	Unlimited
Ethernet port 4 destination mac address	
Ethernet port 4 unicast conversion	☐ Enable

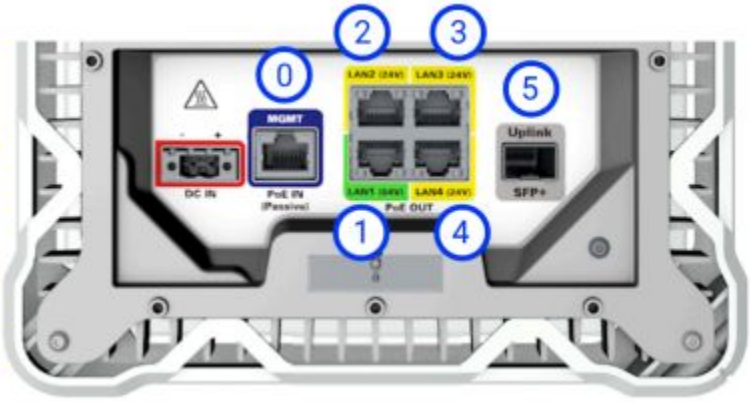
> **Tip:** Hover over the interface ports in the LAN tab diagram for tool tips with configuration and connection information about the ports.

Ethernet Port Configuration

Check or clear the **Port enable** setting to enable / disable traffic on any LAN port.

Check or clear the **PoE enable** setting to enable / disable PoE out for the ports where it is available (LAN1- LAN4).

LAN Interface number	Label on K60DN port
0	MGMT (PoE in)
1	LAN1 (54V) PoE out
2	LAN2 (passive 24V) PoE out
3	LAN3 (passive 24V) PoE out
4	LAN4 (passive 24V) PoE out
5	Uplink SFP+



MAC Filter Configuration

AltoPlex radios support both source and destination MAC filtering.

- **Source MAC filtering** — Configures the radio to forward network traffic on a specific Ethernet port only if the traffic is originating from specific MAC addresses.

  On AltoPlex radios, source MAC filtering is configured by setting the number of allowed MAC addresses (up to 10 are supported). The radio then automatically populates an allowlist that contains the first devices that connect to the Ethernet port, up to the configured limit. Traffic is not forwarded from any devices not on the allowlist.

  - You clear the allowlist by either rebooting the radio or making a change to the configuration, at which point a new allowlist will be automatically created.
- **Destination MAC filtering** — Configures the radio's individual Ethernet ports to only forward unicast network traffic to a specified destination MAC address. Network traffic with a destination MAC address that matches the configured MAC will be forwarded. All other network traffic will be dropped.

  You can also configure the radio to convert broadcast and multicast traffic into unicast and forward it to the configured destination MAC address. This may be useful for certain types of broadcast or multicast network traffic, such as DHCP requests.

Configure MAC filtering

In the **MAC Filter Configuration** section of the **LAN** tab, for each Ethernet port:

1. Configure source MAC filtering:
   A. For **Ethernet port *x* mac limit**, select the number of MAC addresses to be included in the allowlist. Allowed values are **1**-**10** and **Unlimited**. The default is **Unlimited**, which means that source MAC filtering is disabled.
   B. An allowlist is automatically generated based on the first MAC addresses that connect to the device after source MAC filtering is enabled, up to the configured limit.
      - You can repopulate the allowlist by rebooting the radio or making a configuration change.
      -
2. Configure destination MAC filtering:
   A. For **Ethernet port *x* destination mac address**, type the destination MAC address that unicast network traffic must contain for the traffic to be forwarded.
   B. For **Ethernet port *x* unicast conversion**, click **Enable** to convert broadcast and multicast network traffic to unicast and forward that traffic to the specified destination MAC address.
3. Click **Submit Changes.**

Show the current MAC filter configuration

You can show the current MAC filter configuration, including the current allowlist that the radio is using for source MAC filtering, by using either the CLI or the REST API.

- **CLI**:
  1. Log in via ssh to the K60DN and K60CN1:

     ```
     $ ssh admin@<hostname>
     admin@<hostname>'s password:
     ```

     where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.
  2. Use the **mac_filter_status** command:

     ```
     KB-C6-00-01> mac_filter_status
       kb_name: KB-C6-00-01
       ports:
         eth1:
           filter_eth1_destination_mac: 70:88:6B:C7:00:02
           filter_eth1_unicast_conversion: enable
           filter_eth1_source_mac_limit: 4
           source_mac_allowlist:
             a0:b1:c2:d3:e4:f5
             0a:1b:2c:3d:4e:5f
             ff:ee:dd:cc:bb:aa
             00:11:22:33:44:55
         eth2:
           filter_eth2_destination_mac: 70:88:6B:C7:00:02
           filter_eth2_unicast_conversion: enable
     ```

```
        filter_eth2_source_mac_limit: 4
        source_mac_allowlist:
          a1:b2:c4:d5:e5:f6
          1a:2b:3c:4d:5e:6f
          aa:bb:cc:dd:ee:ff
          55:44:33:22:11:00
      eth3:
        filter_eth3_destination_mac:
        filter_eth3_unicast_conversion: disable
        filter_eth3_source_mac_limit: unlimited
        source_mac_allowlist:
KB-C6-00-01>
```

- **REST API**:

  Use the **device/mac_filter_status** API. For example:

  1. In your browser, type the following URL in the address bar:
     `https://<hostname>/rest/v002/device/mac_filter_status?output=text`

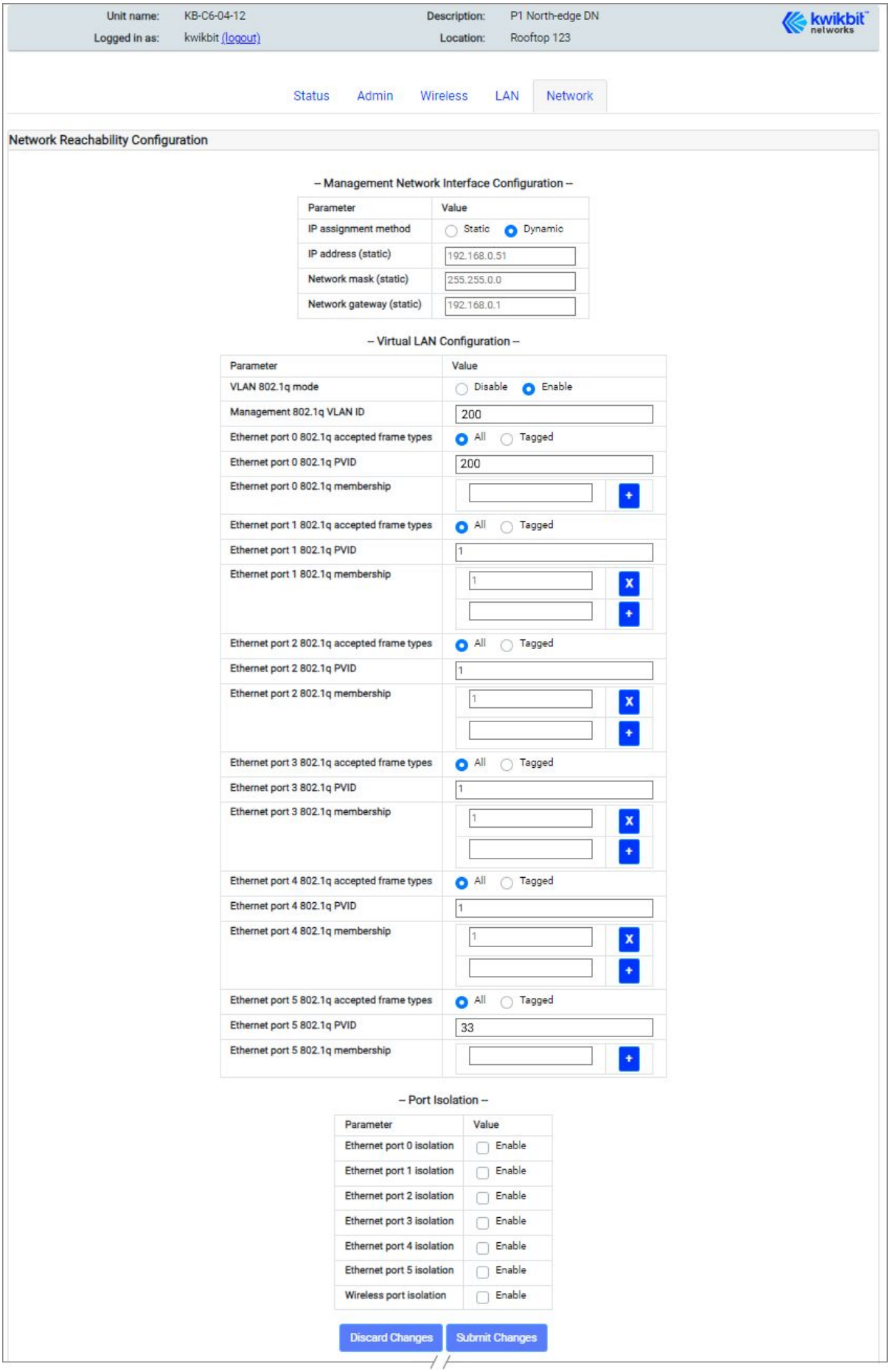
     where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio.

  2. The following output is displayed in the browser window:

```
kb_name: KB-C6-00-01
ports:
  eth1:
    filter_eth1_destination_mac: 70:88:6B:C7:00:02
    filter_eth1_unicast_conversion: enable
    filter_eth1_source_mac_limit: 4
    source_mac_allowlist:
      a0:b1:c2:d3:e4:f5
      0a:1b:2c:3d:4e:5f
      ff:ee:dd:cc:bb:aa
      00:11:22:33:44:55
  eth2:
    filter_eth2_destination_mac: 70:88:6B:C7:00:02
    filter_eth2_unicast_conversion: enable
    filter_eth2_source_mac_limit: 4
    source_mac_allowlist:
      a1:b2:c4:d5:e5:f6
      1a:2b:3c:4d:5e:6f
      aa:bb:cc:dd:ee:ff
      55:44:33:22:11:00
  eth3:
    filter_eth3_destination_mac:
    filter_eth3_unicast_conversion: disable
    filter_eth3_source_mac_limit: unlimited
    source_mac_allowlist:
```

Network tab

The Network tab has many settings and is shown in two images. The first image shows Network Reachability Configuration, which includes settings for Management Network Interfaces, VLAN Configuration and Port Isolation.


Unit name: KB-C6-04-12
Logged in as: kwikbit (logout)
Description: P1 North-edge DN
Location: Rooftop 123
kwikbit networks
Status
Admin
Wireless
LAN
Network
Network Reachability Configuration
– Management Network Interface Configuration –
Parameter
Value
IP assignment method
Static
Dynamic
IP address (static)
192.168.0.51
Network mask (static)
255.255.0.0
Network gateway (static)
192.168.0.1
– Virtual LAN Configuration –
Parameter
Value
VLAN 802.1q mode
Disable
Enable
Management 802.1q VLAN ID
200
Ethernet port 0 802.1q accepted frame types
All
Tagged
Ethernet port 0 802.1q PVID
200
Ethernet port 0 802.1q membership
Ethernet port 1 802.1q accepted frame types
All
Tagged
Ethernet port 1 802.1q PVID
1
Ethernet port 1 802.1q membership
1
Ethernet port 2 802.1q accepted frame types
All
Tagged
Ethernet port 2 802.1q PVID
1
Ethernet port 2 802.1q membership
1
Ethernet port 3 802.1q accepted frame types
All
Tagged
Ethernet port 3 802.1q PVID
1
Ethernet port 3 802.1q membership
1
Ethernet port 4 802.1q accepted frame types
All
Tagged
Ethernet port 4 802.1q PVID
1
Ethernet port 4 802.1q membership
1
Ethernet port 5 802.1q accepted frame types
All
Tagged
Ethernet port 5 802.1q PVID
33
Ethernet port 5 802.1q membership
– Port Isolation –
Parameter
Value
Ethernet port 0 isolation
Enable
Ethernet port 1 isolation
Enable
Ethernet port 2 isolation
Enable
Ethernet port 3 isolation
Enable
Ethernet port 4 isolation
Enable
Ethernet port 5 isolation
Enable
Wireless port isolation
Enable
Discard Changes
Submit Changes

Network Reachability Configuration

Note: With Altowav Gen3 technology, the K60DN establishes a wireless link with the K60CN1 when it is installed and added to the K60DN's CN responder list. Once connected, the K60CN1 remains reachable for management traffic regardless of its VLAN settings. This operation eliminates a problem seen with Altowav Gen2 (802.11ad) technology where incorrect VLAN settings could render a device unreachable via airlink.

Management Network Interface Configuration -- IP assignment method defaults to **Dynamic**. If set to **Static**, it also requires entering an **IP address**, **network mask** and **network gateway**.

Virtual LAN Configuration

VLAN 802.1q mode — Select **Enable** to enable VLAN support on this radio.

Management 802.1q VLAN ID — The identification number of the VLAN used for management purposes.

Ethernet port x 802.1q accepted frame types — For VLANs that the port is a member of, accept **All** incoming Ethernet packets, or only packets that are **Tagged**.

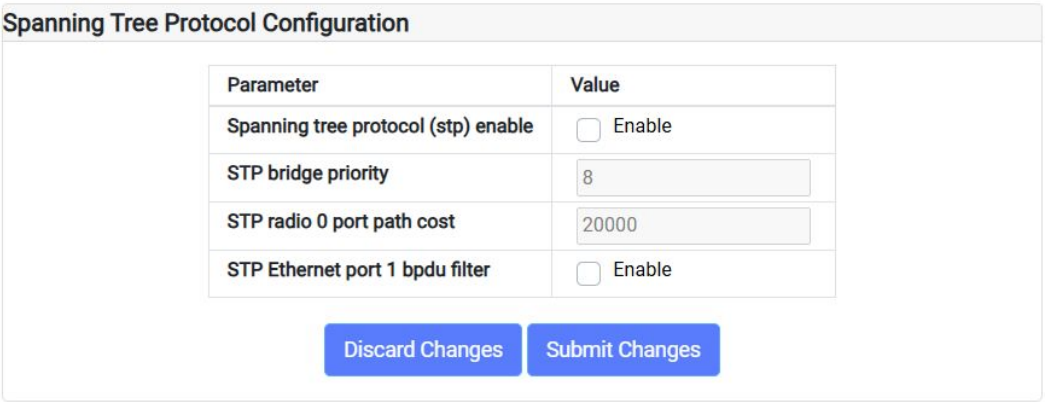
Ethernet port x 802.1q PVID — The Port VLAN ID (PVID). This determines what VLAN ID will be assigned to untagged frames.

Ethernet port x 802.1q membership — The VLANs that this Ethernet Port is a member of. Allowed values are single integers, a range of integers, or both. Values should be comma-separated without spaces. For example, 1,6,10-15. Maximum value is 4094.

Ethernet port x isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Ethernet interface.

Wireless port isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Wireless interface.

Network tab — Spanning Tree Protocol Configuration



Spanning tree protocol — Enable/disable spanning tree protocol (STP) by checking/clearing the box. If enabled, optionally set the bridge priority and port path cost for the wireless interface.

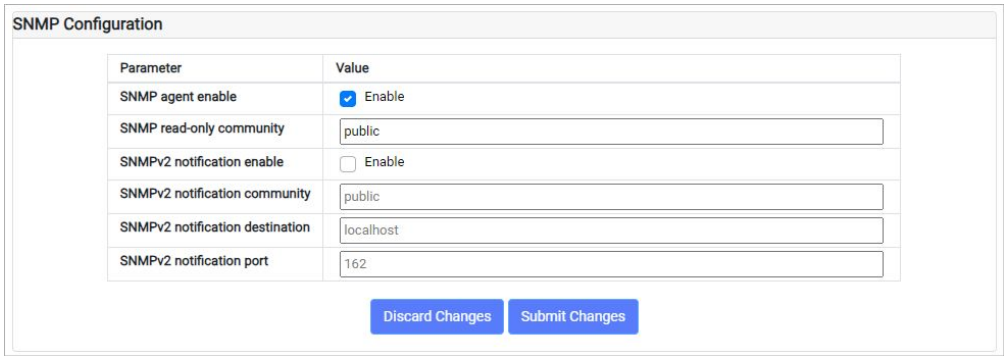
STP bridge priority is used to determine which device will serve as the root of the spanning tree. The device with the lowest priority will serve as the root. The priority configured here is a multiplier; to determine the actual STP priority, multiply by 4096.

The **STP port path cost** is used to determine the preferred path to the root. The path with the lowest cumulative cost is used.

The **STP Ethernet port 1 bpdu filter** prevents BPDU packets from being forwarded, which allows for separate networks to be isolated from participating in the same STP environment. When enabled, the filter is applied whether or not Spanning Tree Protocol is enabled.

Network tab — SNMP Configuration

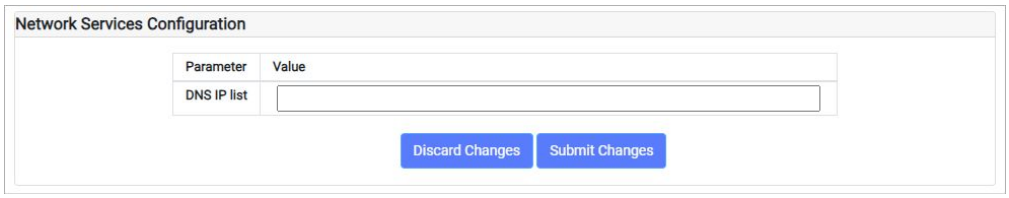
Simple Network Management Protocol (SNMP) is used to monitor devices on a network for performance and error information. The settings in this section enable/disable SNMP and configure notification and community access settings.



The Altowav enterprise MIB can be downloaded at https://www.altowav.com/technology/assets/pdf/ALTOWAV-MIB.mib.

Network tab — Network Services Configuration

DNS IP list — A list of DNS server IP addresses using commas to separate the addresses.



Network tab — DHCP Relay Configuration (Option 82)

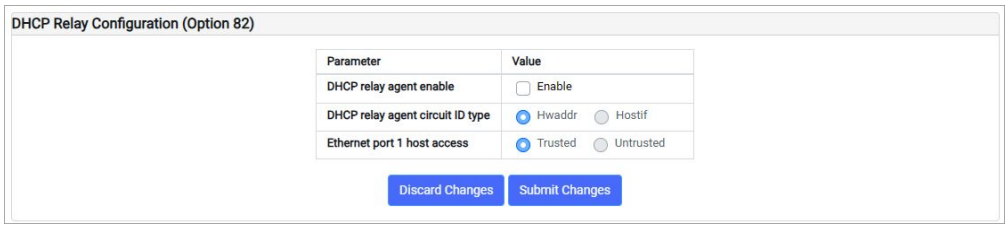
Enable the DHCP relay agent to:

- Prevent unauthorized DHCP servers from serving IP addresses to devices on your network.
- Insert a circuit ID into a DHCP message that identifies the source of the message. The **DHCP relay agent circuit ID type** can be either **HWaddr** (the MAC address of the K60DN and K60CN1's Ethernet port, in ASCII format), or the **Hostif** (the hostname:Ethernet_port of the K60DN and K60CN1 in ASCII format).

You can also select whether the Ethernet port is:

- **Trusted** — All DHCP packets coming from devices attached to the Ethernet port will be forwarded.
- **Untrusted**:
  - All DHCP server packets from attached devices will be blocked.
  - All DHCP client packets from attached devices that have option 82 information in their header will be blocked.
  - All DHCP client packets from attached devices that do not have option 82 information in their header will be fowarded, with the circuit ID appended.

  Note: All wireless links are automatically considered trusted.



K60CN1 Installation and Configuration

K60CN1 Installation

The K60CN1 installation instructions include:

- Tool list.
- K60CN1 box contents and functional description.
- Network design information required.
- Installation and configuration steps.
- Configuration example.

Tool List:

- 8mm nut driver or slotted screwdriver for band clamp.
- #2 Phillips head screwdriver for wall mount.

Box contents:

K60CN1

Stainless steel band clamps

Screw kit

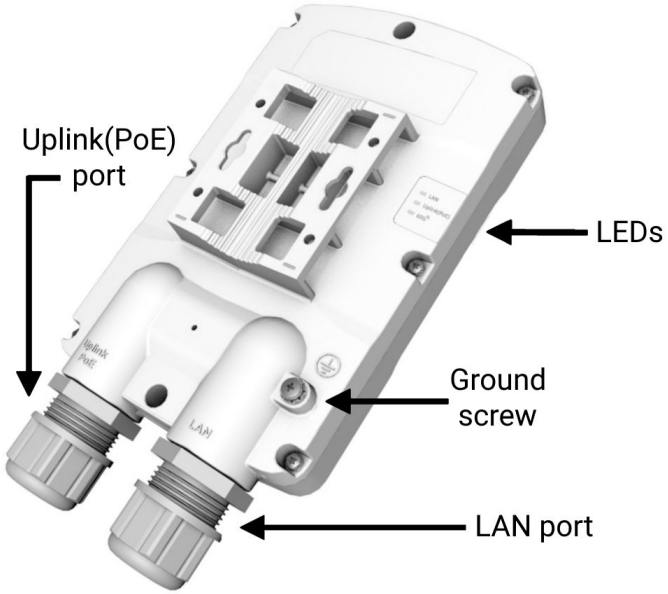
PoE injector

Cable glands

Port seal

Power cord

The K60CN1 is a client node supporting the Altowav Gen3 platform for 60GHz wireless. It has a durable and weatherproof outer case. The K60CN1 ports, LEDs and the ground screw are labeled on the back of the device.



LED Indicators

LEDs on the back of the K60CN1 show connections and activity.

Normal Operation:

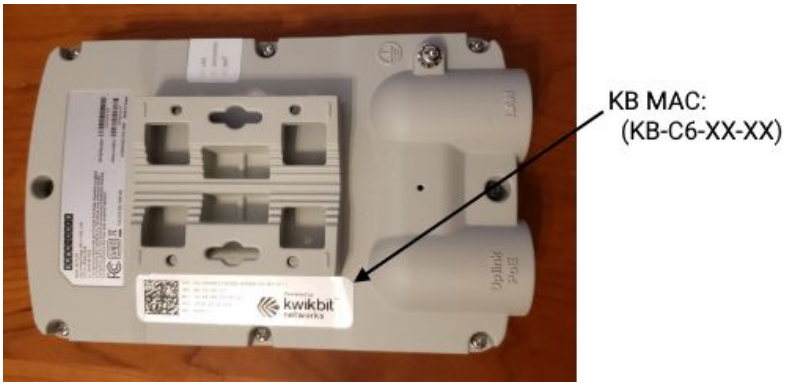
- **LAN** indicates an external Ethernet link. (Green)
- **Uplink(PoE)** shows connection to power and normal operation. (Red)
- **60G** indicates active wireless link(s). (Blue)

See LED Indicator Lights for a description of more LED sequences.

Network Design Information Required

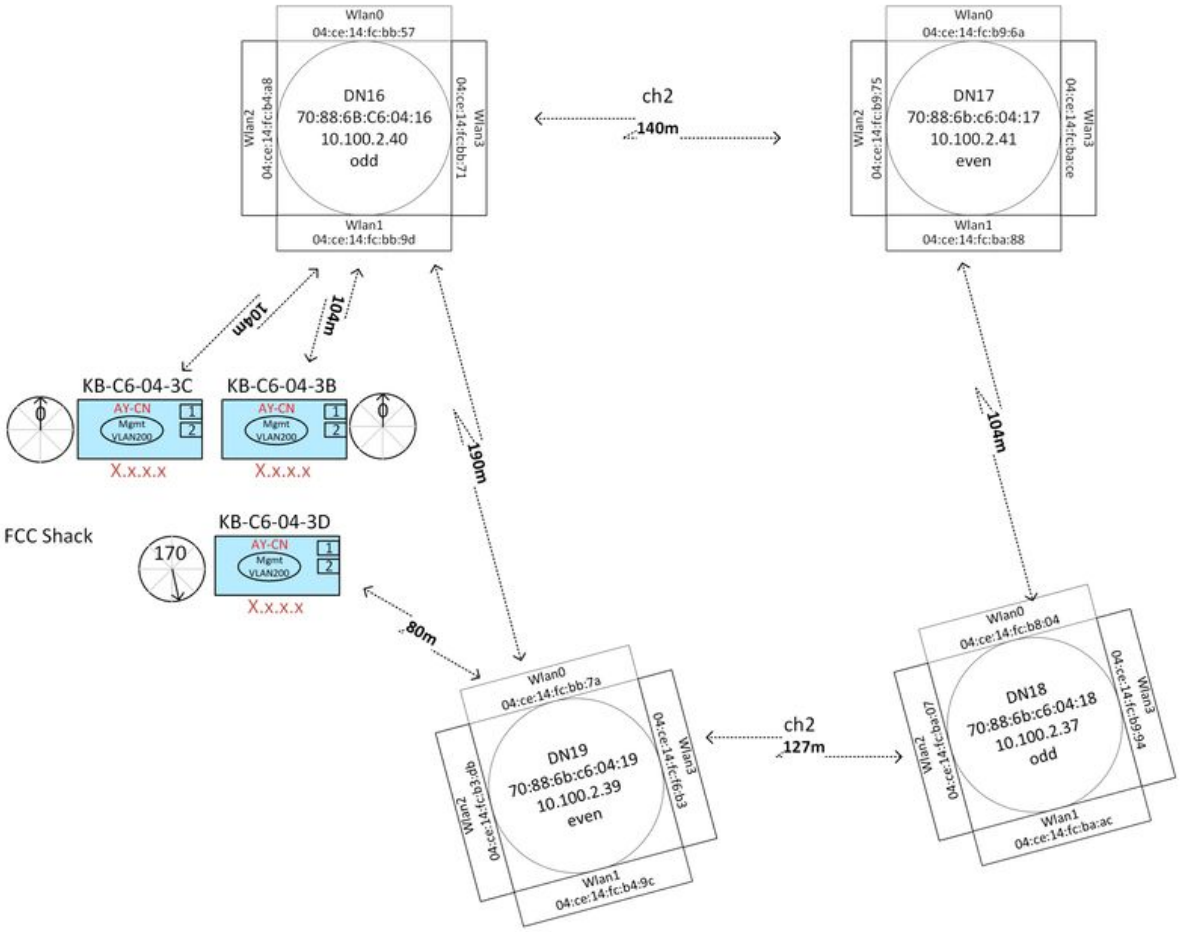
Before installation, the network design should be well planned and documented. Required information for installation and configuration:

- KB MAC for this K60CN1 - Verify the information on its back label against the network design.



- Identity (IP address) of the connected K60DN (distribution node). **The WebUI for this K60DN unit must be accessible.**
- Identity of the radio interface on the K60DN to which this K60CN1 will connect, (a specific Radio # or radio MAC address).
- Azimuth for aiming the K60CN1 toward the desired radio sector. **Clear line-of-sight (LOS) is required.**
- Any elevation angle required for optimal connection. Note, adjusting elevation angle may also require a precision mounting bracket, (not supplied).
- Site location for installation. This is used for configuring the device's Location/Description information and for preparing for the physical installation. A map of the network topology on a satellite view of the network site is often used.
- Specific network settings for the install site such as Management VLAN ID and PVID.

The network diagram below shows a good way to communicate much of the required information. The K60CN1 devices are shown in blue and the K60DNs are shown with device and radio sector information. Radios 0-3 are labeled with Wlan0-3. This sample does not show specific azimuth. In this sample no elevation adjustment is noted.



Installation tips:

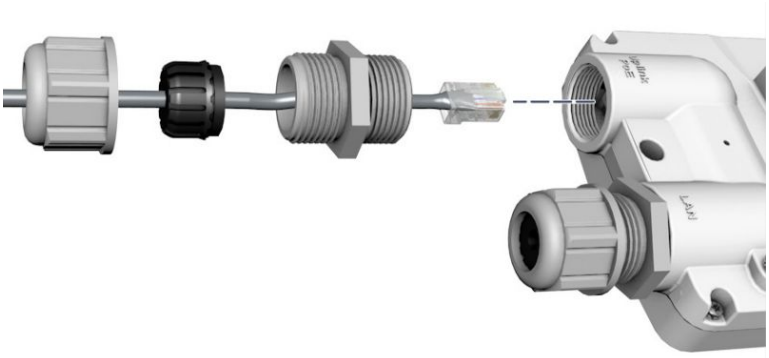
- Orient the K60CN1 to face the K60DN radio sector to which it will connect.
- Clear line-of-sight (LOS) is required.
- With the Altowav Gen3 platform, the K60DN establishes a wireless link with the K60CN1 when the K60CN1 is added to the K60DN's CN responder list. Once connected, the K60CN1 remains reachable for management traffic regardless of its VLAN settings. This operation eliminates a problem seen with Gen2 (802.11ad) technology where incorrect VLAN settings could render a device unreachable via airlink.
- If the K60CN1 is repositioned or re-aimed for adjustment after installation and connection, rebeamform the link by removing and re-adding it to the CN Responder list on the connected K60DN. Or, reboot or power-cycle the K60CN1.

K60CN1 Installation at Customer Premise

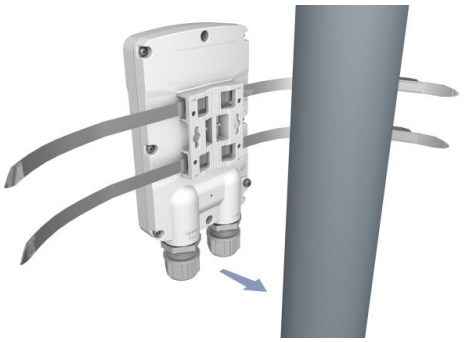
At the installation site:

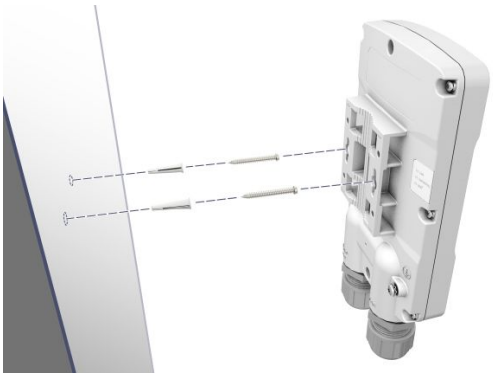
1. **Attach a ground wire to the ground screw.** (Local codes determine whether grounding is required or optional.) The other end of the ground wire should connect to nearby good earth when mounted at the install location.

2. **Install outdoor-rated Cat6 cable in the Uplink(PoE) port.** Remove the cable glands, insert the RJ45 as shown. Insert the plug securely. Then replace the cable glands and screw them in securely. Install the supplied port seal to weatherproof the LAN port.



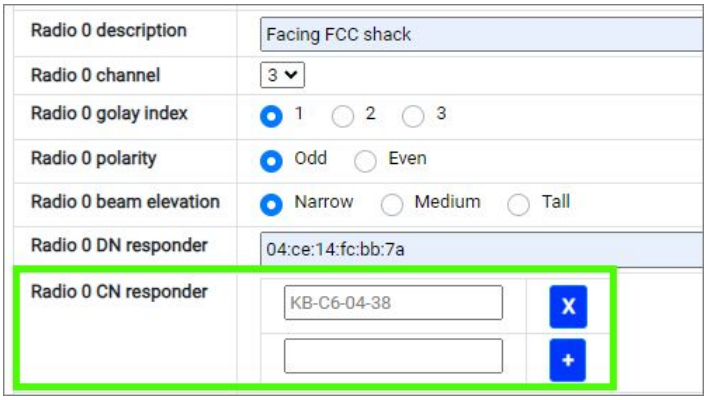
3. **Mount the K60CN1 to a pole or wall at the customer premise.** Align it to the azimuth specified by the network design for connection to the K60DN. Ensure a clear line of sight (LOS) between the K60CN1 and K60DN. For pole mounts, use the supplied stainless steel band clamps for durability.



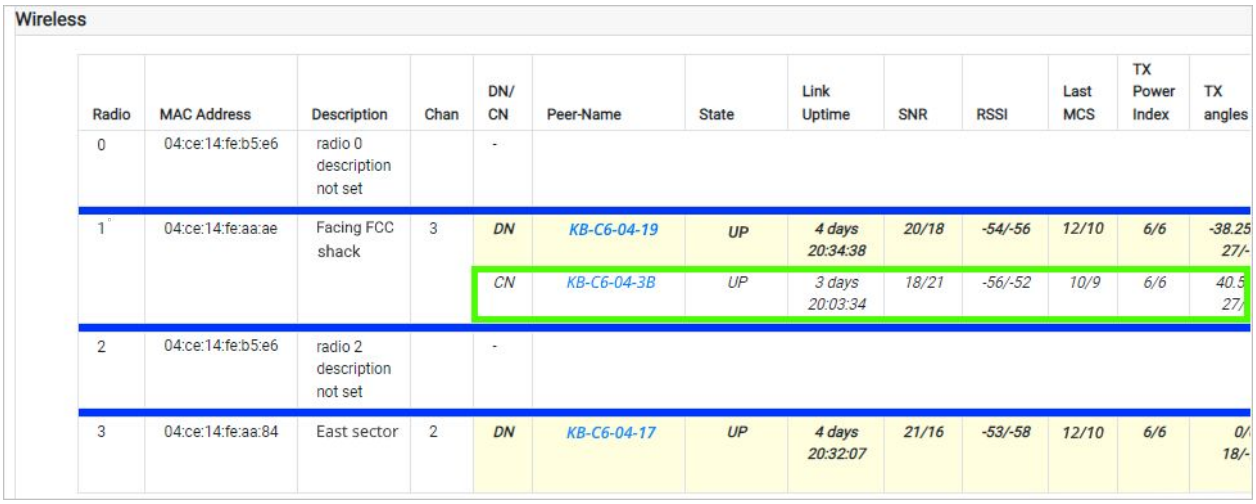


4. **Install and connect the supplied PoE injector.** Connect the Cat6 cable from the K60CN1 to the PoE port on the injector. Connect the PoE injector to AC power, usually a power strip or wall outlet. Verify that power is on. The Uplink(PoE) LED on the back of the K60CN1 will be on or blinking. Connect the LAN port of the PoE injector to customer's router or access point.
5. **Add the K60CN1 to the K60DN's CN responder** list. This enables the K60DN to connect to the K60CN1. Open the K60DN's WebUI (default password: **admin**; for release 1.8.1 and earlier, the default password is **kwikbit**). See administrator for current PW.) Go to the **Wireless** tab and add this K60CN1's KB MAC to the **CN responder** list for the K60DN radio

interface specified in the network design. Verify the K60DN Radio # (wlan#) and the K60CN1's KB MAC using the network design information. The sample image shows adding KB-C6-04-3B to the K60DN's **Radio 1 CN responder** list.



Click **Submit Changes** and wait for the K60CN1 to connect and appear under **Peer-Names** in the Wireless table.



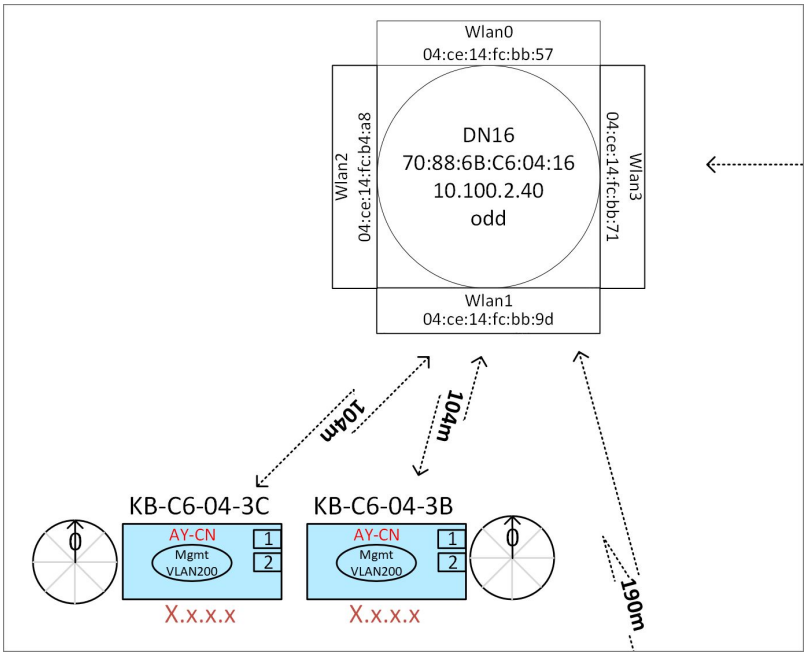
See the example following these K60CN1 installation steps.

6. **After the K60CN1 has connected, configure its settings.** Click on the K60CN1's KB MAC listed under Peer-Name. Click the **Admin** tab, enter the password as requested (default password: **admin**; for release 1.8.1 and earlier, the default password is **kwikbit**). Set the **Location** and **Description** and click the **Save Changes** button. Review and adjust settings on the LAN and Network tabs, according to the network design. **Save** the configuration and close the WebUI.
7. **Verify the unit's performance,** before moving to the next installation. Look for an RSSI value of greater than -65dBm and an MCS level of 9, with traffic. If less than that, reposition the K60CN1 for better connection and re-beamform. Check RSSI and MCS again.

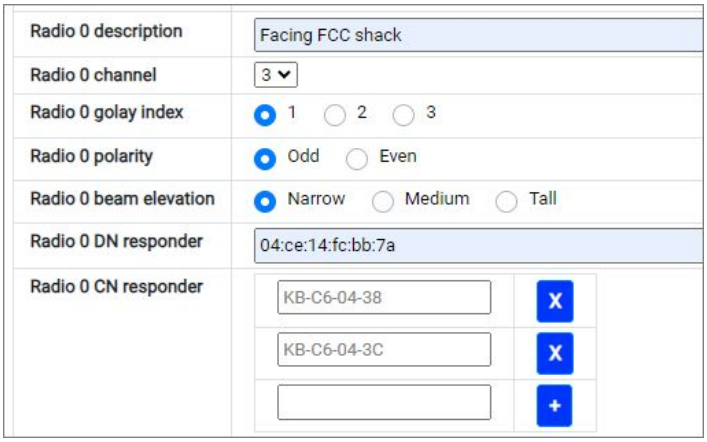
   Note: If the K60CN1 is repositioned or re-aimed after connecting to the K60DN, rebeamform the link by removing and re-adding it to the CN responder list, rebooting or power cycling the unit. This ensures an optimal refresh of the connection.

Example: Add the K60CN1 to the K60DN's CN responder list

Focusing on the area of the network diagram shown below, this example adds the K60CN1 (KB-C6-04-3C) to the **CN responder** list for the K60DN (DN16) on **Radio 1** (**wlan1)**.



1. Use the Edge Controller or browse to **https://10.100.2.40** to access the K60DN's WebUI. If issued a security warning, click the **Advanced** button and **Proceed** to the site.
2. Click the **Wireless** tab and enter the password.
3. Add **KB-C6-04-3C** to the blank **Radio 1 CN responder** field and click the **+** button.



4. Click **Submit Changes**.
5. View the Wireless table on the K60DN's WebUI and wait for the K60CN1 (KB-C6-04-3C) to appear under Peer-Name for Radio 1.

Connecting to the K60DN and K60CN1

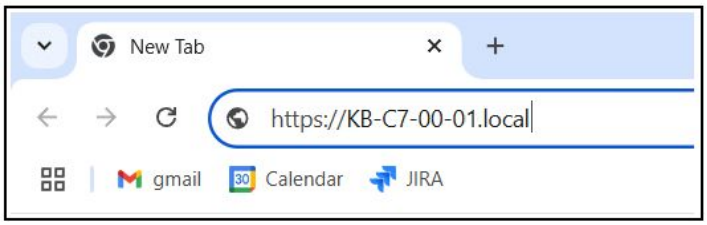
By default, AltoPlex radios use dynamic IP address assignment and, beginning with release 3.6.0, have a factory default fallback static IP address of 192.168.0.1.

Additionally:

- Radios can be configured to use a static IP address, rather than dynamic IP address assignment. This will override the fallback IP unless the radio is factory reset. After a factory reset, it will return to default behavior.
- Radios upgraded to release 3.6.0 that have not been factory reset will have a factory default fallback IP address of 192.168.0.51, unless they have a configured static IP address that overrides the default address. After a factory reset, they will have the default behavior.

Because AltoPlex radios participate in multicast DNS (mDNS), computers that support mDNS and are on the same subnet as the radio can connect to the radio by using its hostname. In general, this should work regardless of whether the radio is configured to use dynamic or static addressing, or if it is using the fallback default IP.

For example, if your radio's hostname is KB-C6-00-01 and your computer is on the same subnet as the radio, you can access the WebUI by typing **https://KB-C6-00-01** (or **https://KB-C6-00-01.local**) into your browser's URL address bar:



Use the factory default fall-back IP address to connect to the radio

This section applies to radios with firmware version 3.6.0 or newer. Radios with older firmware have a unique fallback link local IP address that was provided on a printed label when the device was manufactured. For devices originally manufactured with a software version prior to 3.6.0 and then upgraded to release 3.6.0 or newer, the default IP address will depend on whether the device has been factory reset since the upgrade:

- If the device has not been factory reset, the default IP address is 192.168.0.51.
- If the device has been factory reset, the default IP address is 192.168.0.1.

To connect to an AltoPlex radio by using its default fallback IP address:

1. Configure your computer to be a member of the 192.168.0.*x* subnet.

   For example, on Windows 11:

   A. Click the **Windows** icon.
   B. Click **Settings**.
   C. Click **Network & internet**.
   D. Click **Ethernet**.
   E. For **IP assignment**, click **Edit**.
   F. Select **Manual**.
   G. Click to toggle on **IPv4**.
   H. For **IP address**, type an address in the 192.168.0.*x* subnet (for example, **192.168.0.2**).
   I. For **Subnet mask**, type **255.255.255.0**.
   J. Click **Save**.

2. Next, either:
   - Plug your computer's Ethernet connection into the **LAN** port of a PoE injector that is connected to the radio.

     > **Tip:** The LAN port is sometimes labeled as the **Data out** port, the **Out** port, or something similar.

   - Plug both your computer and the radio into a PoE switch.

     > **Tip:** To access the radio by using the default IP address, make sure that the switch is not connected to the backhaul network or that the backhaul network does not have a DHCP server running on it.

3. Access the radio's WebUI by entering either the hostname (for example, **https://KB-C6-00-01**) or the default IP address (**https://192.168.0.1**) in the address bar of a web browser.

   Note: If a radio has a configured static IP address that is different than the default address, the configured IP address must be used to access the radio.

4. A warning message may indicate that the self-signed certificate used by the device is not recognized by the browser. Instructions to clear the message vary depending on the browser. For example, in Chrome:
   A. Click **Advanced**.
   B. Click **Proceed to...**

The WebUI will open with the **Status** tab displayed.

Determine the IP address of a radio by using mDNS

If you configure a radio to use a static IP address and subsequently do not remember the IP address, you can use mDNS commands to determine the radio's IP address.

Note: This requires that your computer supports mDNS and is on the same subnet as the radio.

- Windows Powershell:
  `Resolve-DnsName <hostname>`
- MacOS:
  `dns-sd -G v4v6 <hostname>`
- Linux:
  `avahi-resolve-host-name -4 <hostname>.local`

where <hostname> is the hostname of the AltoPlex radio (KB-XX-XX-XX).

Access the radio by using the management Wi-Fi access point

AltoPlex radios also provide a mechanism to access all radios through a management Wi-Fi access point, which is enabled by default but can be disabled. See Wi-Fi connection to a K60DN and K60CN1 for more information.

K60CN1 Configuration via WebUI

During installation, the K60CN1's KB MAC (KB-XX-XX-XX) is added to the **CN responder** list for the specific K60DN radio interface to which it connects. That configuration change for the K60DN initiates the wireless link between the K60DN and this K60CN1. See an example of how to add the K60CN1 to the CN responder list at the end of the K60CN1 Installation topic.

After the K60CN1 link to the network is active, you can access the WebUI using one of the following methods.

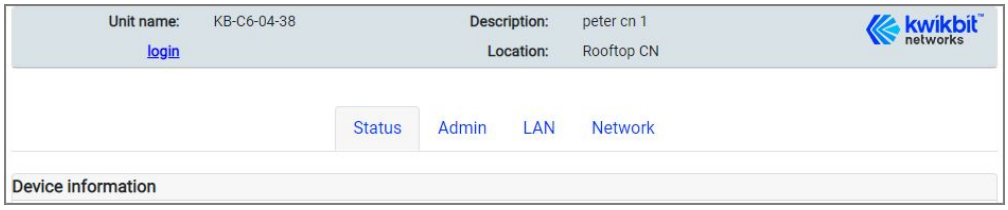
- Link from the connected K60DN's WebUI **Peer Name** list.

- Enter the IP address of the K60CN1 into a browser address bar from a PC connected to the network. For example, **https://10.100.2.45**
- If using the Altowav Gen3 Edge Controller (v2.4.7 or higher), access the WebUI from the Devices page. (On the row of the device to configure, click on the (**...**) in the settings column and select the **Connect to Device** option.)

General startup configuration steps often include:

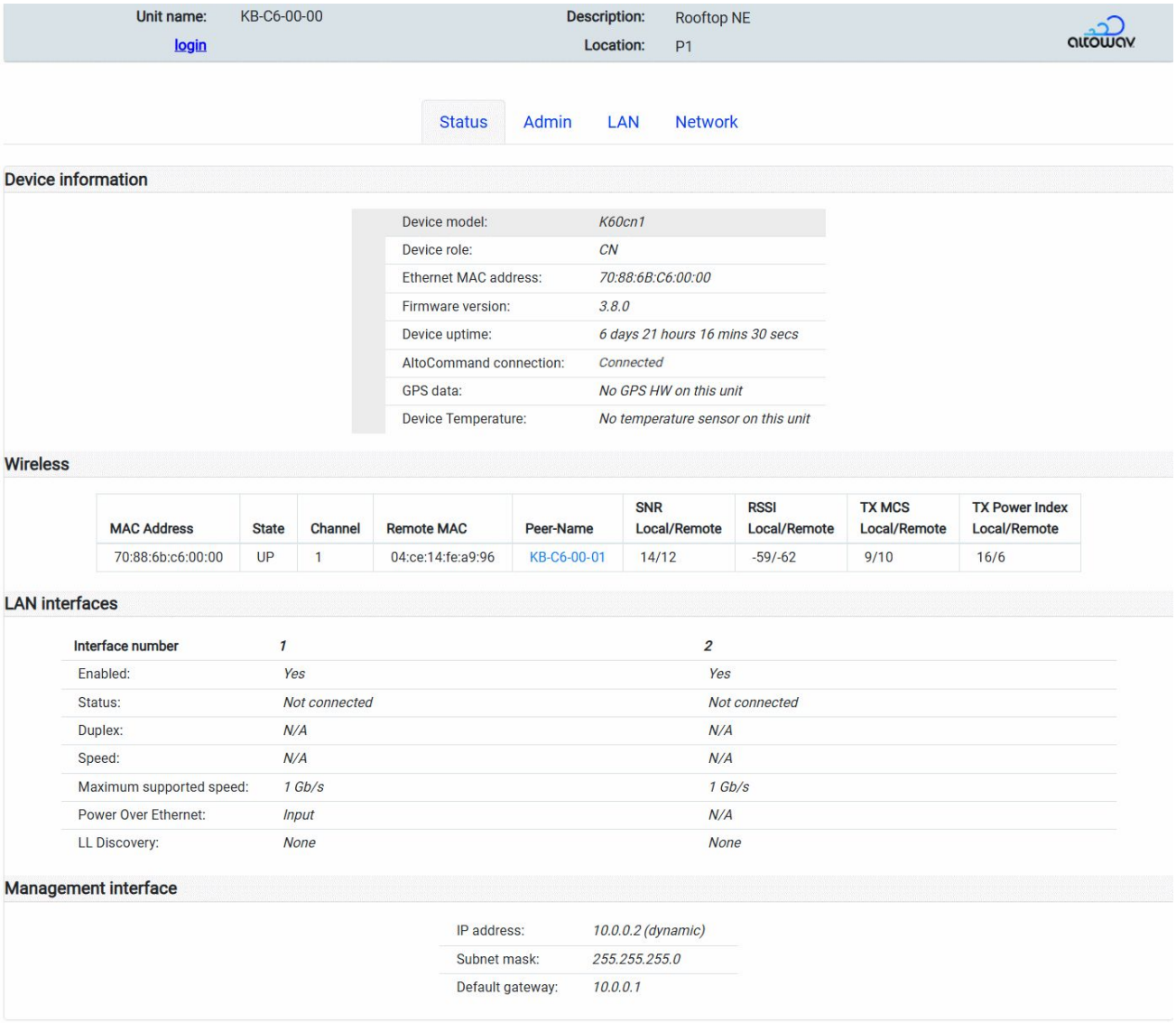
- Click on the **Admin** tab and do one or more of the following: **Change Password**, set **Location** or **Description** per your network design plan, or **Upgrade Firmware** version.
- On **Network** tab, set network config items for Management, VLAN.

The header of the WebUI shows the Unit name of the K60CN1, (also called the KB MAC), Description and Location, as well as offering a **login** link. Login is not required to have read-only access to the WebUI, but is required to set configurations on any other tab of the WebUI.



Status tab:

The Status tab shows a summary of information about the unit, its wireless and LAN connections, and interface information. Login is not required to view the Status tab. However, you will be asked to log in when clicking on any other tab.



Device information

This area describes the model of the device, Ethernet MAC address, firmware version, device uptime, and the AltoCommand server connection.

Note, K60CN1 devices do not have GPS hardware or temperature sensors.

Wireless

This area lists the MAC address as well as its current State (UP/DOWN), Channel frequency used, Remote MAC, Peer-Name (KB Name of connected K60DN), as well as local / remote measurements for SNR, RSSI, Last MCS level, and TX Power Index.

LAN interfaces

This area shows information for each LAN interface: whether it is enabled, its status, duplex mode, speed, maximum supported speed, PoE status and LAN peers.

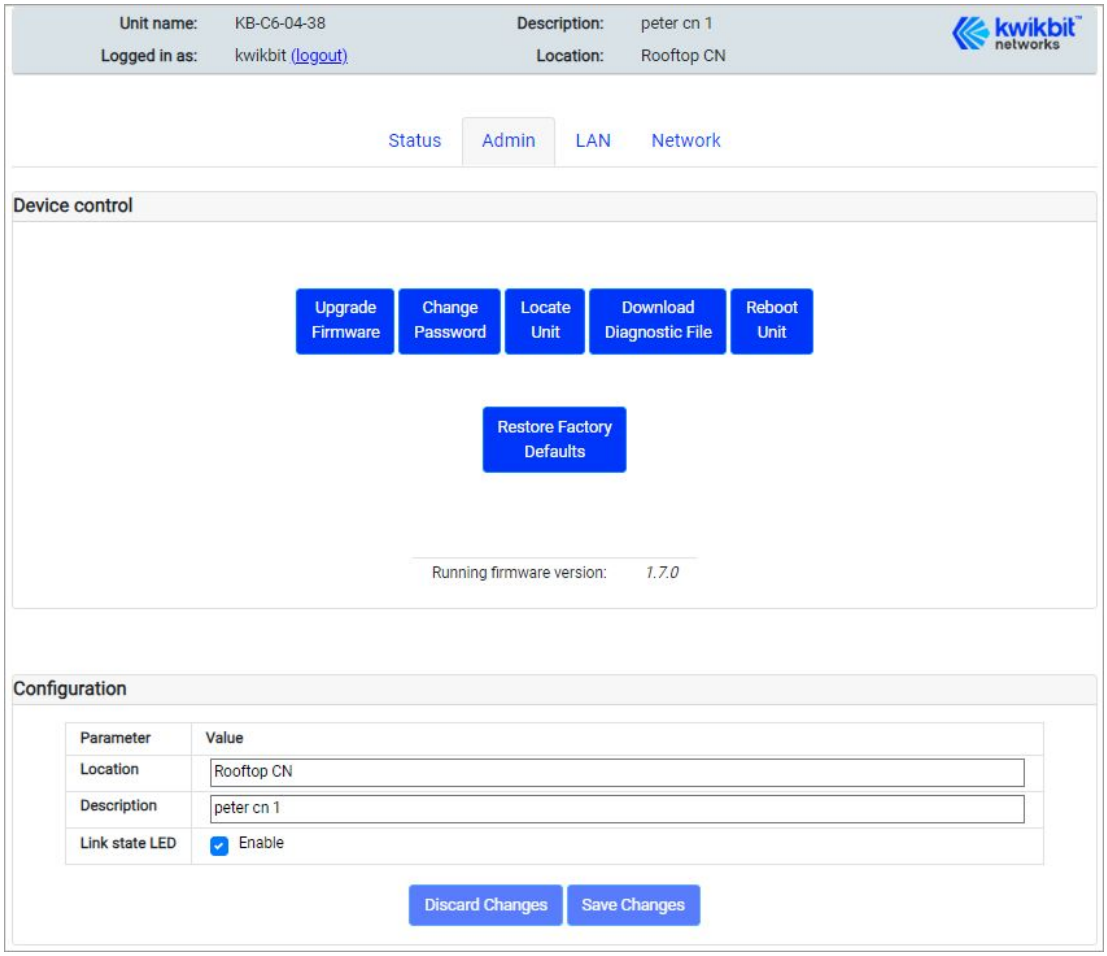
Management interface

This area lists the IP address (showing assignment as dynamic or static), subnet mask and default gateway for the Management interface on the node.

Admin tab:

During initial configuration enter a **Location** and **Description** for the node, and if required **Change Password**.

Other options for Reboot, Restore Factory Defaults, Upgrade Firmware, Locate Unit and Download Diagnostic File are more useful for K60CN1s that are currently running as part of a network.



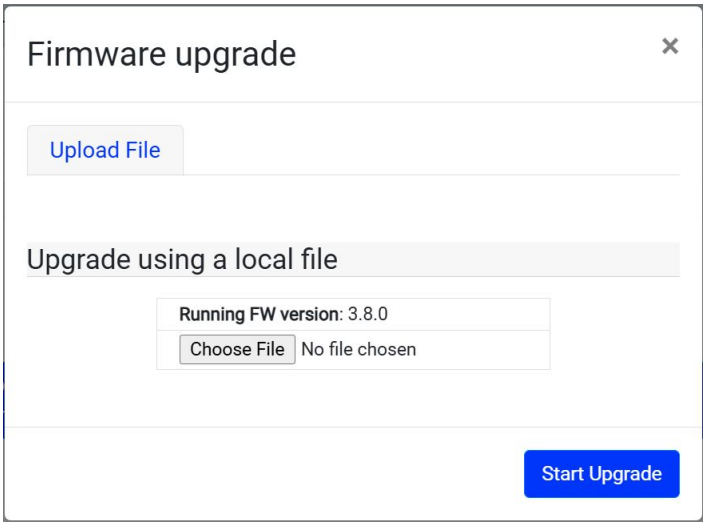
Device control

Reboot - restarts the unit remotely.

Restore Factory Defaults - restores all device configuration to factory defaults. If the unit is unreachable and cannot be reset with this button, it may require a factory reset by power cycling three times.

Note: Factory reset returns the unit's password to the default: **admin** (For firmware version 1.8.1 or earlier, the default password is **kwikbit**). Since the IP assignment uses DHCP by default, the factory reset is not likely to affect the IP address of the K60CN1.

Upgrade Firmware - updates the device firmware with the file you choose. Click the **Upgrade Firmware** button and upload or browse to the firmware upgrade file. Then click **Start Upgrade** on the resulting dialog. Note, the device will reboot as part of the upgrade process.



Change Password - enables you to change the device's password, according to your organization's network policy.

Locate Unit – Click this button to put the unit into locate mode. In locate mode, the device flashes an LED signal for field personnel to identify the unit. LED sequence: **Uplink(PoE)** is on, while **LAN** and **60G** are blinking.

Download Diagnostic File - Automatically downloads a detailed diagnostic text file for the device. The file contains detailed information about the device and its status at the time of the download. The file name includes the host name (KB MAC), the date and time. For example, a file named KB-C6-04-3A_diag_2023-05-12-14-43-32.txt, means this is the diagnostic text file for unit KB-C6-04-3A, created at 2:43:32 pm (UTC) on May 12, 2023.

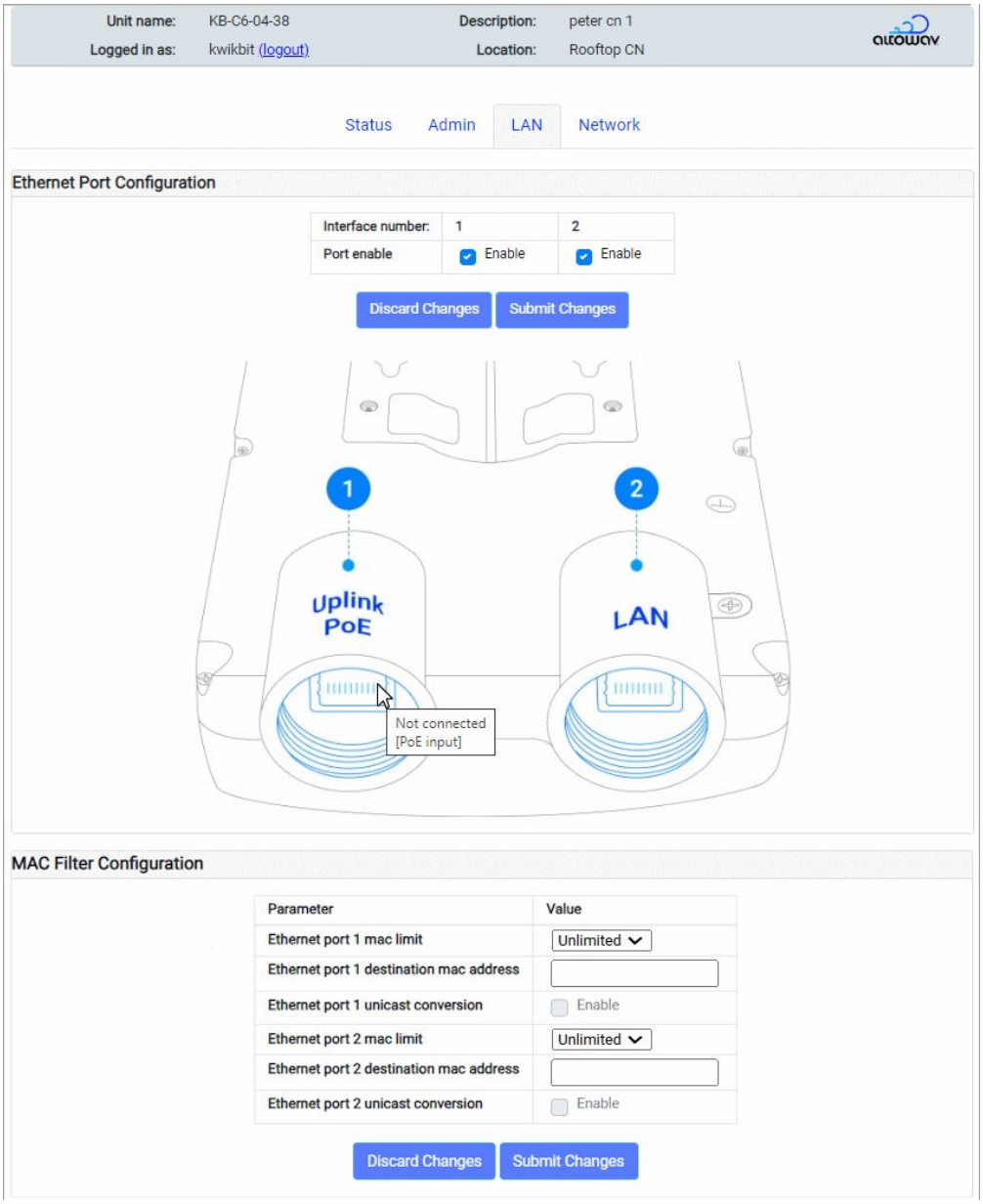
Configuration

Location - specifies the physical location of this K60CN1. Examples may be latitude and longitude, or if installed at a customer premise, it may include a lot or unit number in a Manufactured Home Park, or a street address.

Description - specifies more identifying information about the device. Often this includes the customer name.

LAN tab:

The LAN tab provides settings for enabling traffic and PoE on the LAN ports for the K60CN1.



Ethernet Port Configuration

Port enable -- check or clear boxes to enable/disable ports. Ports are enabled by default.

> **Tip:** Hover over either port in the graphic to show the current connection status of the port.

MAC Filter Configuration

AltoPlex radios support both source and destination MAC filtering.

- **Source MAC filtering** — Configures the radio to forward network traffic on a specific Ethernet port only if the traffic is originating from specific MAC addresses.

  On AltoPlex radios, source MAC filtering is configured by setting the number of allowed MAC addresses (up to 10 are supported). The radio then automatically populates an allowlist that contains the first devices that connect to the Ethernet port, up to the configured limit. Traffic is not forwarded from any devices not on the allowlist.

  - You clear the allowlist by either rebooting the radio or making a change to the configuration, at which point a new allowlist will be automatically created.
- **Destination MAC filtering** — Configures the radio's individual Ethernet ports to only forward unicast network traffic to a specified destination MAC address. Network traffic with a destination MAC address that matches the configured MAC will be forwarded. All other network traffic will be dropped.

  You can also configure the radio to convert broadcast and multicast traffic into unicast and forward it to the configured destination MAC address. This may be useful for certain types of broadcast or multicast network traffic, such as DHCP requests.

Configure MAC filtering

In the **MAC Filter Configuration** section of the **LAN** tab, for each Ethernet port:

1. Configure source MAC filtering:
   A. For **Ethernet port *x* mac limit**, select the number of MAC addresses to be included in the allowlist. Allowed values are **1**-**10** and **Unlimited**. The default is **Unlimited**, which means that source MAC filtering is disabled.
   B. An allowlist is automatically generated based on the first MAC addresses that connect to the device after source MAC filtering is enabled, up to the configured limit.
      - You can repopulate the allowlist by rebooting the radio or making a configuration change.
      -
2. Configure destination MAC filtering:
   A. For **Ethernet port *x* destination mac address**, type the destination MAC address that unicast network traffic must contain for the traffic to be forwarded.
   B. For **Ethernet port *x* unicast conversion**, click **Enable** to convert broadcast and multicast network traffic to unicast and forward that traffic to the specified destination MAC address.
3. Click **Submit Changes.**

Show the current MAC filter configuration

You can show the current MAC filter configuration, including the current allowlist that the radio is using for source MAC filtering, by using either the CLI or the REST API.

- **CLI**:
  1. Log in via ssh to the K60DN and K60CN1:

```
$ ssh admin@<hostname>
admin@<hostname>'s password:
```

where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Use the **mac_filter_status** command:

```
KB-C6-00-01> mac_filter_status
  kb_name: KB-C6-00-01
  ports:
    eth1:
      filter_eth1_destination_mac: 70:88:6B:C7:00:02
      filter_eth1_unicast_conversion: enable
      filter_eth1_source_mac_limit: 4
      source_mac_allowlist:
        a0:b1:c2:d3:e4:f5
        0a:1b:2c:3d:4e:5f
        ff:ee:dd:cc:bb:aa
        00:11:22:33:44:55
    eth2:
      filter_eth2_destination_mac: 70:88:6B:C7:00:02
      filter_eth2_unicast_conversion: enable
      filter_eth2_source_mac_limit: 4
      source_mac_allowlist:
        a1:b2:c4:d5:e5:f6
        1a:2b:3c:4d:5e:6f
        aa:bb:cc:dd:ee:ff
        55:44:33:22:11:00
    eth3:
      filter_eth3_destination_mac:
      filter_eth3_unicast_conversion: disable
      filter_eth3_source_mac_limit: unlimited
      source_mac_allowlist:
KB-C6-00-01>
```

- **REST API**:

  Use the **device/mac_filter_status** API. For example:

1. In your browser, type the following URL in the address bar:

```
https://<hostname>/rest/v002/device/mac_filter_status?output=text
```

   where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio.

2. The following output is displayed in the browser window:

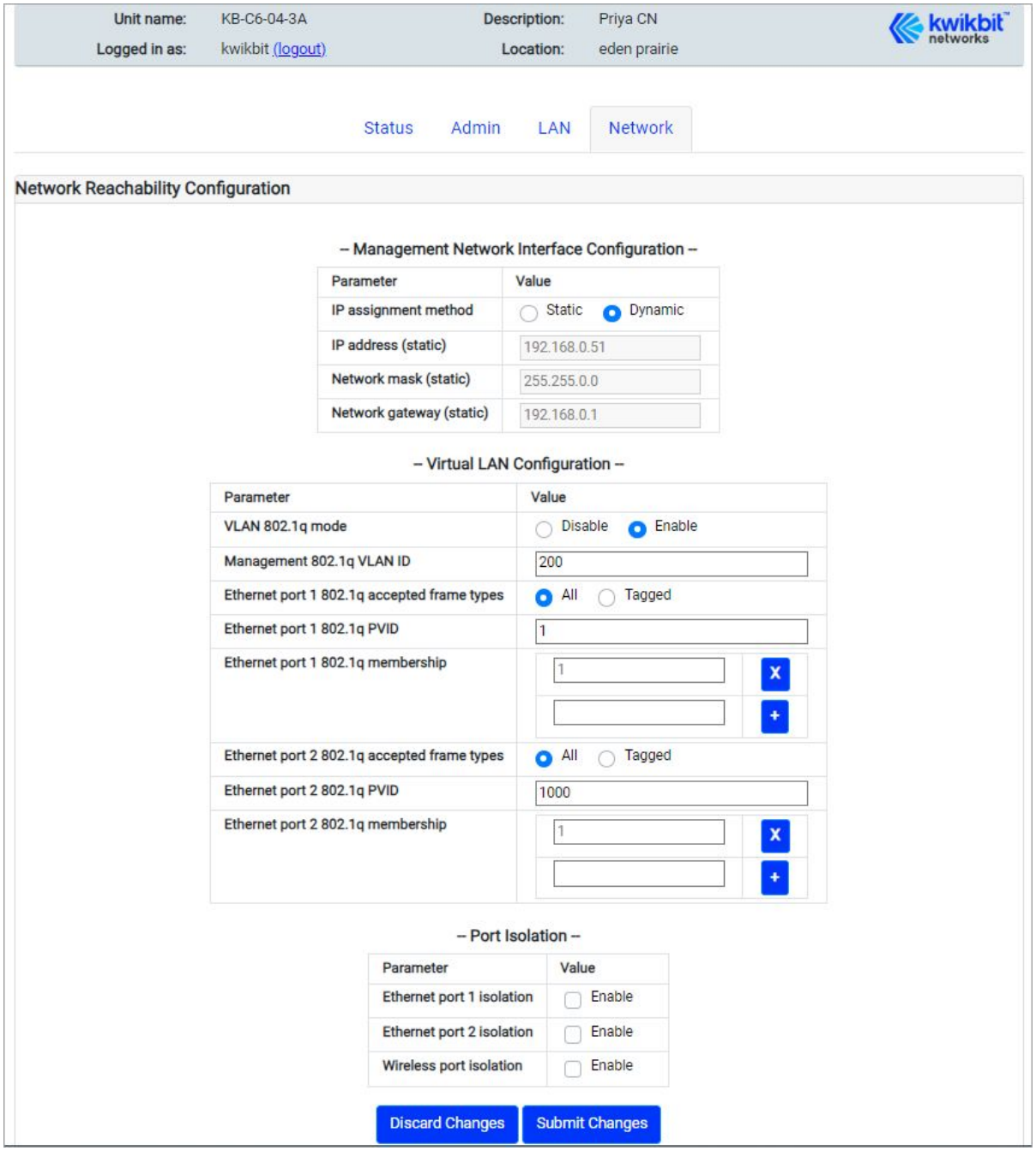
```
kb_name: KB-C6-00-01
ports:
  eth1:
    filter_eth1_destination_mac: 70:88:6B:C7:00:02
    filter_eth1_unicast_conversion: enable
    filter_eth1_source_mac_limit: 4
    source_mac_allowlist:
      a0:b1:c2:d3:e4:f5
      0a:1b:2c:3d:4e:5f
      ff:ee:dd:cc:bb:aa
```

```
    00:11:22:33:44:55
eth2:
  filter_eth2_destination_mac: 70:88:6B:C7:00:02
  filter_eth2_unicast_conversion: enable
  filter_eth2_source_mac_limit: 4
  source_mac_allowlist:
    a1:b2:c4:d5:e5:f6
    1a:2b:3c:4d:5e:6f
    aa:bb:cc:dd:ee:ff
    55:44:33:22:11:00
eth3:
  filter_eth3_destination_mac:
  filter_eth3_unicast_conversion: disable
  filter_eth3_source_mac_limit: unlimited
  source_mac_allowlist:
```

Network tab:

The Network tab offers settings for Management Network Interfaces, VLAN configuration and Port Isolation, as well as additional Layer 2, SNMP, and Network Services Configuration. The Network tab has a long list of settings, so the images below show only one section at a time with brief descriptions following.

Note: Adding a K60CN1 to a K60DN's CN responder list establishes the wireless link between a K60DN and a K60CN1. With the airlink established, the Network settings have far less impact on reachability than they did with 802.11ad-based technology. This improvement means the order of configuring Network settings is no longer critical for reachability. However, setting the IP address to Static and losing it or forgetting it will still make a device unreachable.



VLAN 802.1q mode — Select **Enable** to enable VLAN support on this radio.

Management 802.1q VLAN ID — The identification number of the VLAN used for management purposes.

Ethernet port x 802.1q accepted frame types — For VLANs that the port is a member of, accept **All** incoming Ethernet packets, or only packets that are **Tagged**.

Ethernet port x 802.1q PVID — The Port VLAN ID (PVID). This determines what VLAN ID will be assigned to untagged frames.

Ethernet port x 802.1q membership — The VLANs that this Ethernet Port is a member of. Allowed values are single integers, a range of integers, or both. Values should be comma-separated without spaces. For example, 1,6,10-15. Maximum value is 4094.

Ethernet port x isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Ethernet interface.

Wireless port isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Wireless interface.

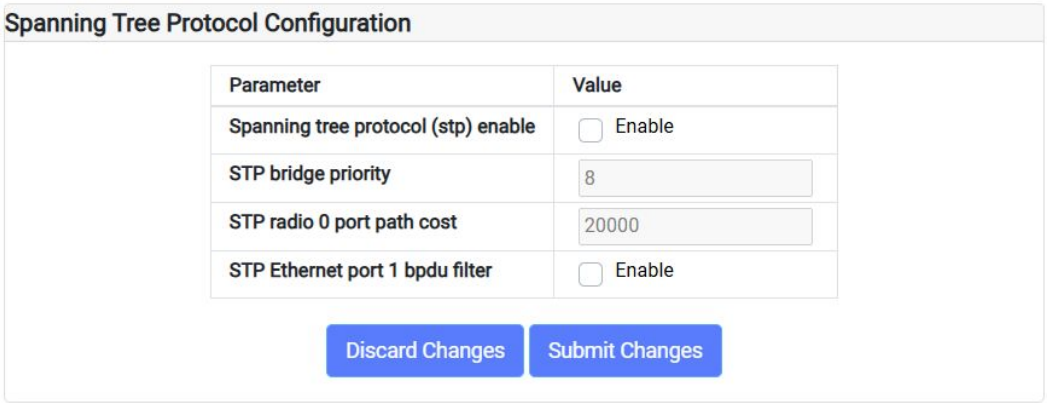
Network Reachability Configuration

Management Network Interface Configuration -- IP assignment method is Dynamic by default. If set to Static, IP address, Network mask and Network gateway must set.

Virtual LAN Configuration -- Enable/disable the 802.1q VLAN mode, setting VLAN IDs, accepted frame types, PVIDs and memberships as required for your specific network operation.

Port Isolation - Enable/disable the port isolation for each port interface on the unit by checking/clearing the box.

Network tab — Spanning Tree Protocol Configuration



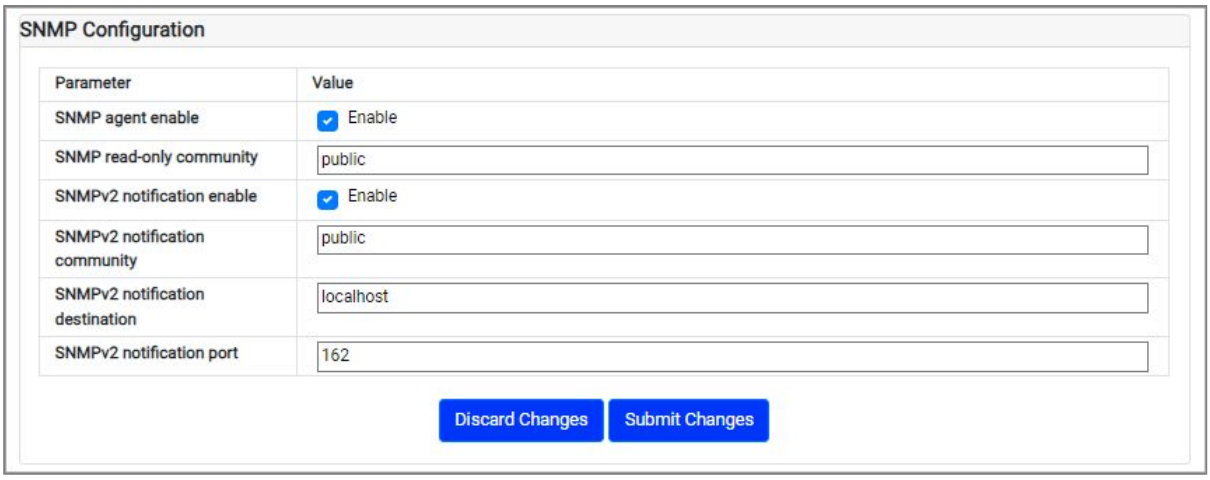
Spanning tree protocol — Enable/disable spanning tree protocol (STP) by checking/clearing the box. If enabled, optionally set the bridge priority and port path cost for the wireless interface.

STP bridge priority is used to determine which device will serve as the root of the spanning tree. The device with the lowest priority will serve as the root. The priority configured here is a multiplier; to determine the actual STP priority, multiply by 4096.

The **STP port path cost** is used to determine the preferred path to the root. The path with the lowest cumulative cost is used.

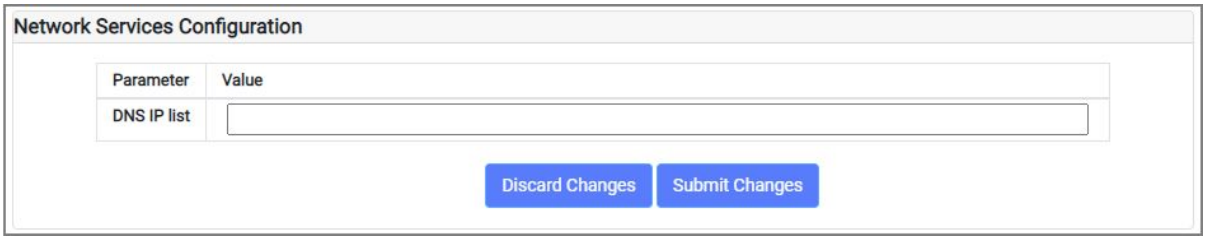
The **STP Ethernet port 1 bpdu filter** prevents BPDU packets from being forwarded, which allows for separate networks to be isolated from participating in the same STP environment. When enabled, the filter is applied whether or not Spanning Tree Protocol is enabled.

SNMP Configuration



Simple Network Management Protocol (SNMP) is used to monitor devices on a network for performance and error information. The settings in this section enable / disable SNMP and configure notification and community access settings.

Network Services Configuration



DNS IP list -- IP addresses for domain name servers (DNS) in dotted decimal format. This defaults to blank. If entering more than one IP address, separate them with commas.

DHCP Relay Configuration (Option 82)

Enable the DHCP relay agent to:

- Prevent unauthorized DHCP servers from serving IP addresses to devices on your network.
- Insert a circuit ID into a DHCP message that identifies the source of the message. The **DHCP relay agent circuit ID type** can be either **HWaddr** (the MAC address of the K60DN's Ethernet port, in ASCII format), or the **Hostif** (the hostname:Ethernet_port of the K60DN in ASCII format).

You can also select whether the Ethernet port is:

- **Trusted** — All DHCP packets coming from devices attached to the Ethernet port will be forwarded.
- **Untrusted**:
  - All DHCP server packets from attached devices will be blocked.
  - All DHCP client packets from attached devices that have option 82 information in their header will be blocked.
  - All DHCP client packets from attached devices that do not have option 82 information in their header will be fowarded, with the circuit ID appended.

Note: All wireless links are automatically considered trusted.

Maintenance and security

Wi-Fi connection to a K60DN and K60CN1

Connect to a K60DN and K60CN1 via Wi-Fi to access the WebUI for diagnostic purposes and configuration tasks, if required.

Note: The Wi-Fi connection to the K60DN and K60CN1 provides a connection to the device for management and diagnostic purposes. It does not provide a connection to the an external network, or to the internet.

Some scenarios where this may be useful:

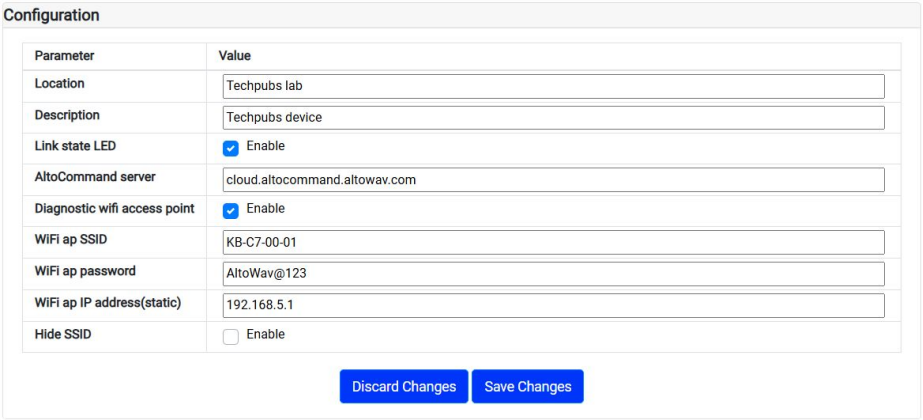
- If the device's WebUI is unreachable via standard access methods. This could happen if Network settings were inadvertently set to unworkable values, or if a direct connection is not feasible due to where the unit is mounted.
- When a device is reset to factory defaults, a Wi-Fi connection may be useful to reconfigure settings after the reset.
- After the initial install of a device, if links do not come up as expected per your design, a Wi-Fi connection could be used to verify and update configurations. This may be especially helpful in cases where the unit is rotated, resulting in sector orientation that is different from the design plan, or in cases where bench configuration was done improperly.

  Tip: To avoid this issue, make sure links come up as part of the installation process.

- In rare cases, the distribution node could become unreachable after configuration and operation in a network. If the unit cannot be reached via wireless or Ethernet link, the unit may be reachable via Wi-Fi.

Wi-Fi settings

Settings for Wi-Fi access are in the Configuration section of the **Admin** tab of the WebUI.



Default for **Diagnostic Wi-Fi access point** is enabled.

Default **Wi-Fi ap SSID** is the hostname of the device. (Listed as HN: KB-XX-XX-XX on the device label.)

Default **Wi-Fi ap password** is **AltoWav@123**.

Default **Wi-Fi ap IP address** is 192.168.5.1. This is the static IP for the device's Wi-Fi access point.

If **Hide SSID** is enabled, the Wi-Fi SSID will not be broadcast.

Prerequisites for connecting to the K60DN and K60CN1 via Wi-Fi:

- You must be in close range to the K60DN and K60CN1 in order to connect to it via Wi-Fi — generally within 10 - 20 ft.
- A K60DN and K60CN1 allows only one incoming connection to Wi-Fi at a time. If multiple technicians are on site, only one may be connected.

To access a device via Wi-Fi:

1. Scan for possible Wi-Fi connections.
2. Find the device's hostname and select **Connect**.
3. Enter the **Wi-Fi ap password**.
4. Browse to the device's **Wi-Fi ap IP address** to open the WebUI.

The WebUI opens to the **Status** tab.

Change the device password

For all AltoPlex devices, passwords can be changed using the WebUI. The process is the same for all devices.

Note: Take care when changing passwords, so that the device's WebUI is not rendered unreachable.

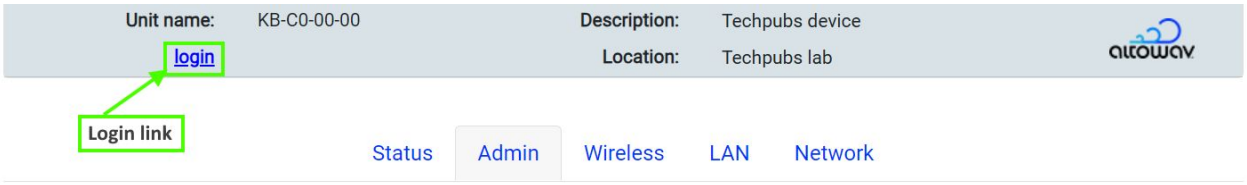
To change the device password:

1. Access the WebUI of the K60DN and K60CN1. In your browser's address bar, type:

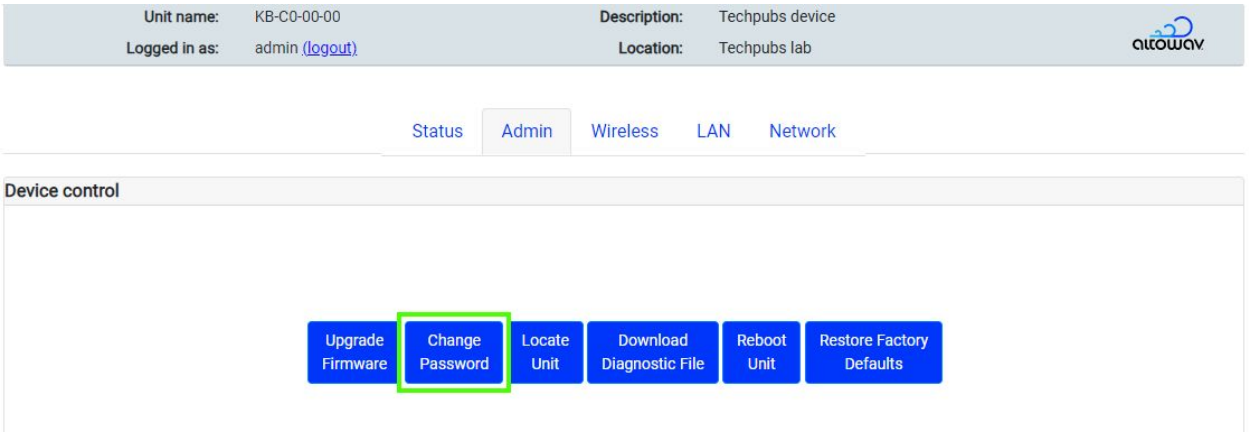
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



3. Click the **Admin** tab.
4. Click the **Change Password** button in the **Device control** section.



   The **Change user password** dialog opens.

5. Enter and re-enter the new password and click **Change Password**.

Enable Passwordless SSH

By default, the K60DN and K60CN1 requires a password to log onto the device when using SSH. You can use the **ssh_keys** CLI command to configure passwordless SSH login to the K60DN and K60CN1.

Note: This procedure describes how to upload an SSH key to the K60DN and K60CN1. You need to generate the SSH key on your local machine using a tool such as the Linux **ssh-keygen** command.

1. Log in via ssh to the K60DN and K60CN1:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Enter **control** mode:

   ```
   KB-C6-00-01> control
   KB-C6-00-01(control)>
   ```

3. Use the **ssh_keys** command:
   - Use **ssh_keys add file *user@host:/path*** to add a key that is stored on a different host, where:
     - *user* is the username to log into the host.
     - *host* is the name of the host machine.
     - *path* is the path and filename of the key file.
   - Use **ssh_keys add text *key*** to add a key by copying the contents of the key file and pasting the contents as an argument of the **ssh_keys add** command.
   - Use **ssh_keys show** to return a list of installed keys.
   - Use **ssh_keys delete *number*** to uninstall the key specified by *number*. The number of the key is determined with the **ssh_keys show** command.
   - Use **ssh_keys delete all** to uninstall all keys.

Note: All authorized keys are deleted when a factory reset is performed.

Upgrading firmware

Upgrade roadmap

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.
2. Upgrade the devices one at a time.
3. Always start with the K60DN and K60CN1 furthest from the root node.

Upgrade from the WebUI

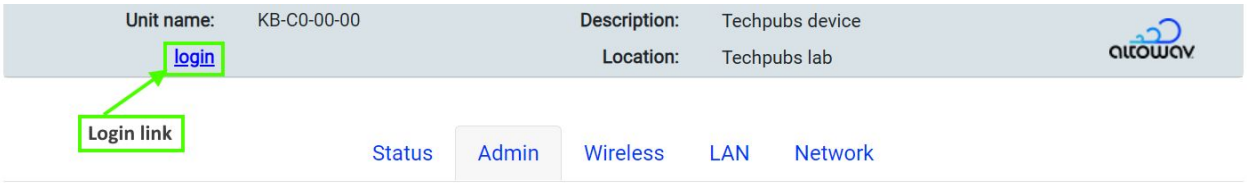
1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

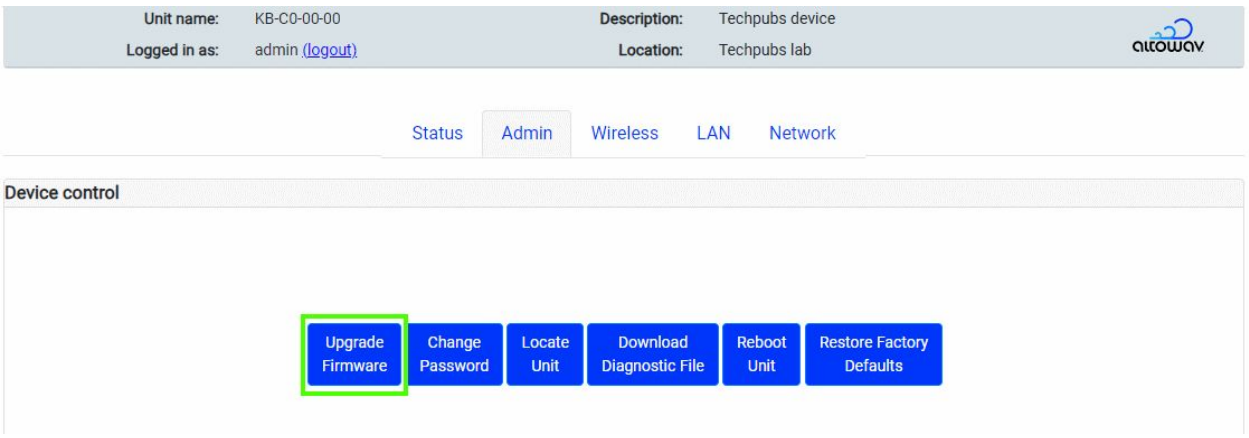
   - A digest file, not used as part of this upgrade process.
   - The firmware binary.
2. Access the WebUI of the K60DN and K60CN1. In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.
3. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.

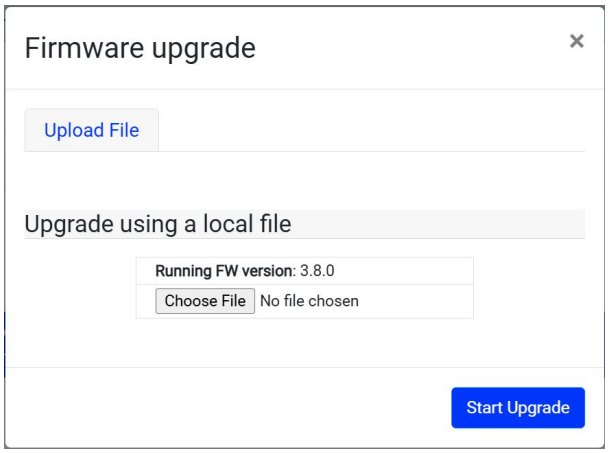


4. Click the **Admin** tab.
5. Click the **Upgrade Firmware** button.



The **Firmware upgrade** dialog opens.

6. Click **Choose File**.
7. Browse to the directory where the upgrade binary file was downloaded and select the file.
8. Click **Start Upgrade**.



Upgrade from the CLI

Upgrade from the CLI by using Secure File Copy (scp)

Use Secure File Copy (scp) to upload a file from a remote host to the K60DN and K60CN1 and install the file:

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

   - A digest file, not used as part of this upgrade process.
   - The firmware binary.

2. Log in via ssh to the K60DN and K60CN1:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

3. Enter **control** mode:

   ```
   KB-C6-00-01> control
   ```

```
KB-C6-00-01(control)>
```

4. Upload and install the software:
   ```
   KB-C6-00-01(control)> software upgrade scp://user@server/
   firmware_filename
   ```
   where:
   - *user* is the name of the user on the remote host.
   - *server* is the hostname or IP address of the remote host.
   - *firmware_filename* is the path and filename of the upgrade software.
5. When prompted, type the password to log into the remote host.

   The upgrade software will be uploaded and installed on the K60DN and K60CN1. You can monitor the status of the upgrade by using the **software status** command:

   ```
   KB-C6-00-01(control)> software status
   current-software-version: 3.9.1
   status: upgrading
   running-sw-version: 3.9.1
   new-sw-version: 4.2.0
   upgrade-running: yes
   ```

   After the software upgrade completes, the device will reboot.

Upgrade from the CLI by using a TFTP server

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:
   - A digest file, not used as part of this upgrade process.
   - The firmware binary.
2. Upload the binary file to the TFTP directory on your server. The TFTP server must be accessible from each device being upgraded.
3. Log in via ssh to the K60DN and K60CN1:
   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```
   where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.
4. Enter **control** mode:
   ```
   KB-C6-00-01> control
   KB-C6-00-01(control)>
   ```
5. Upload and install the software:
   ```
   KB-C6-00-01(control)> software upgrade tftp://server/firmware_filename
   ```
   where:

- *server* is the hostname or IP address of the TFTP server.
- *firmware_filename* is the path and filename of the upgrade software.

The upgrade software will be uploaded and installed on the K60DN and K60CN1. You can monitor the status of the upgrade by using the **software status** command:

```
KB-C6-00-01(control)> software status
current-software-version: 3.9.1
status: upgrading
running-sw-version: 3.9.1
new-sw-version: 4.2.0
upgrade-running: yes
```

After the software upgrade completes, the device will reboot.

Upgrade from the REST API

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

   - A digest file, not used as part of this upgrade process.
   - The firmware binary.
2. Upload the firmware image file to a server that can be access by all devices.
3. Use the `configuration/software_upgrade` API to install the firmware file. For example:

   ```
   curl -k -u admin:<password> \
   https://<hostname>/rest/v002/configuration/software_upgrade \
   -X POST \
   -H "Content-Type:application/octet-stream" \
   -H "X-File-Name:<filename>" \
   --data-binary@<path>/<filename>
   ```

   Where:

   - *password* is the password to log into the device. The default password is **admin**.
   - *path* is the path to the firmware file. If the command is executed from the same local directory as the firmware file, path is not necessary.
   - *filename* is the name of the firmware upgrade file, for example, kb_sw-prod-DEVO OR NOMAD-4.2.0.
   - *hostname* is the hostname or IP address of the radio being upgraded.

   The following example curl command uses the `-i` option to show the response headers, and demonstrates that the file transfer was successful and that the upgrade has begun:

   ```
   $ curl -i -k -X POST -u admin:admin \
   -H "Content-Type:application/octet-stream" \
   -H "X-File-Name:kb_sw-prod-DEVO OR NOMAD-4.2.0.plain" \
   --data-binary @kb_sw-prod-DEVO OR NOMAD-4.2.0.plain \
   https://10.0.0.01/rest/v002/configuration/software_upgrade
   % Total % Received % Xferd Average Speed Time Time Time Current
   ```

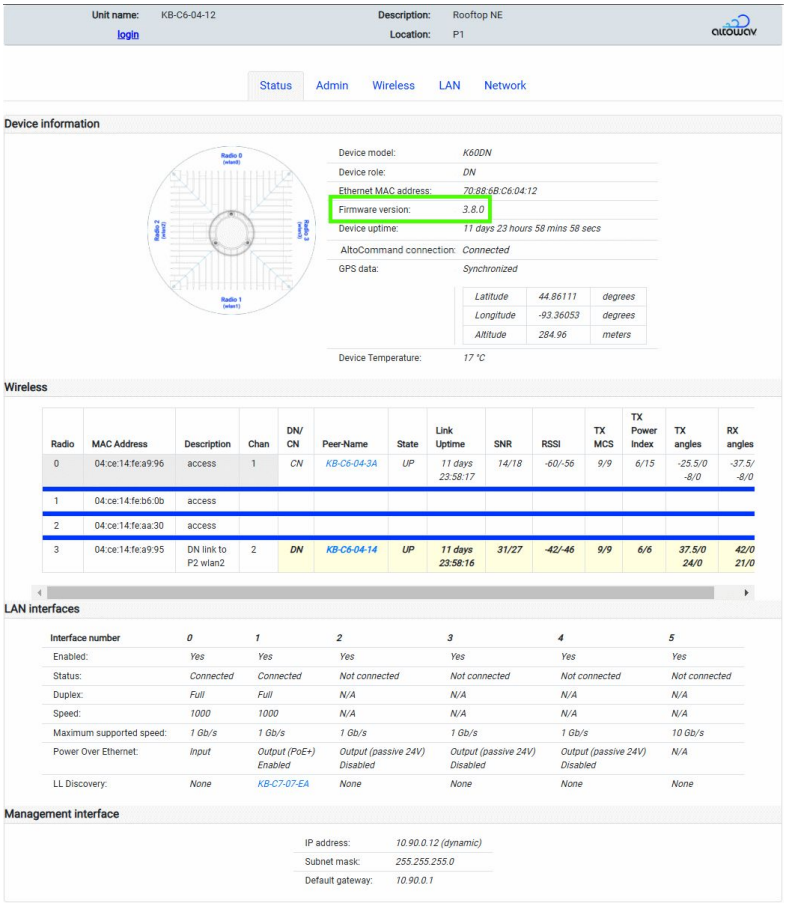
```
Dload Upload Total Spent Left Speed
100 34.1M 100 88 100 34.1M 15 6358k 0:00:05 0:00:05 --:--:-- 6301kHTTP/
1.1 100 Continue

HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: public, must-revalidate, proxy-revalidate
Content-Length: 88
Date: Sat, 01 Jan 2025 00:23:39 GMT
Server: lighttpd/1.4.73
{
"status":"starting",
"running-sw-version":"3.9.1",
"upgrade-running":"yes"
}
```

The upgrade may take up to several minutes to complete.

Verify that the firmware update was successful

Verify firmware update from the WebUI

1. Open the WebUI.
2. The firmware version is displayed on the **Status** page in the **Device Information** section:



Verify firmware update from the command line

1. Log in via ssh to the K60DN and K60CN1:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example, KB-C6-00-01) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Enter **control** mode:

   ```
   KB-C6-00-01> control
   KB-C6-00-01(control)>
   ```

3. Check the status of the device by using the **software status** command:

   ```
   KB-C6-00-01(control)> software status
   current-software-version: 4.2.0
   status: idle
   upgrade-running: no
   KB-C6-00-01(control)>
   ```

   Verify that the current-software-version matches the expected value of the upgrade.

Verify firmware update from the REST API

Use the `device/node_identity` API to return the firmware version:

```
$ curl -k -u admin:admin https://KB-C6-00-01/rest/v002/device/node_identity
  % Total    % Received % Xferd  Average Speed   Time    Time     Time
 Current
                                 Dload  Upload   Total   Spent    Left
 Speed
100   605  100   605    0     0   8188      0 --:--:-- --:--:-- --:--:--
 8402{
  "Ethernet MAC" : "70:88:6B:C6:00:01",
  "HW name" : "devo or nomad",
  "HW rev" : 2,
  "HW type code" : 82,
  "Node role" : "DN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo or nomad-2-LBKA0ZZ1SV1",
  "Serial number" : "00000000000000000001KB-C6-00-01:2",
  "authorized_org" : "",
  "bootloader version" :
"KBBLVERSION:1.3:prod:robot:2025-12-04_11-57-10:devo or nomad:1b565eb",
  "description" : "system description not set",
  "gps available" : 1,
  "location" : "system location not set",
  "name" : "KB-C6-00-01",
  "node type" : "PTP",
  "software" : "4.2.0"
}
```

Reboot a device

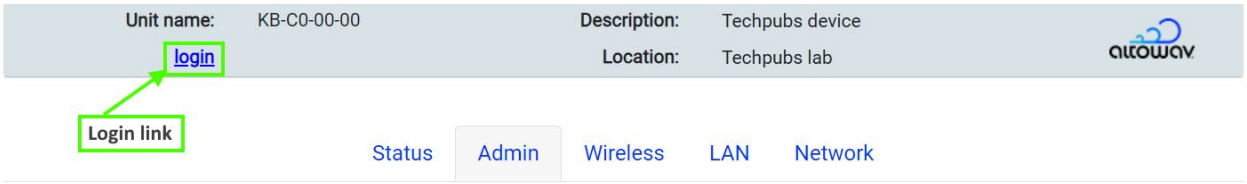
Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

1. Access the WebUI of the K60DN and K60CN1. In your browser's address bar, type:

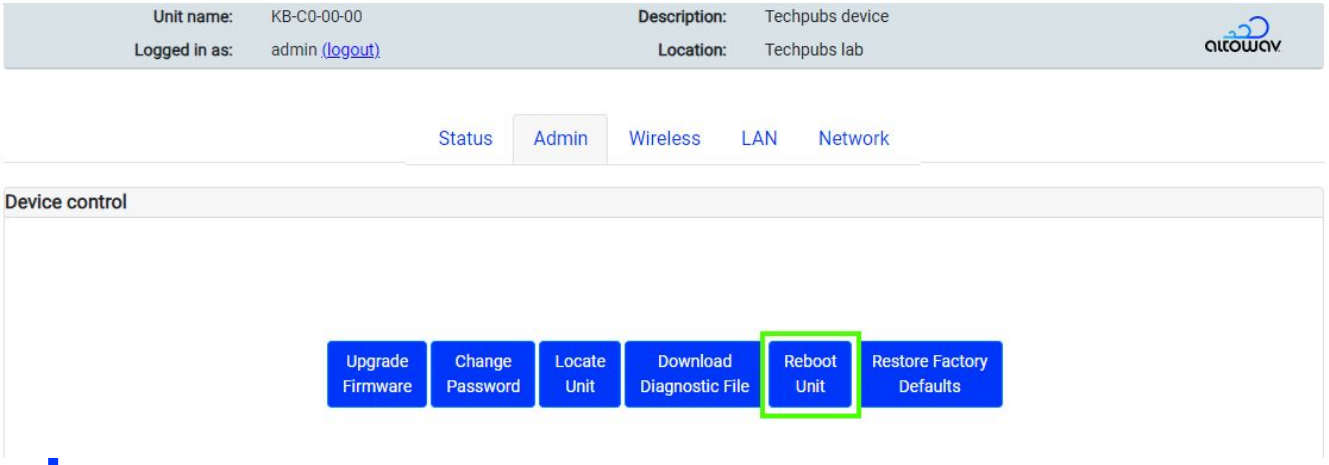
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Reboot Unit** button in the **Device control** section and wait until the reboot is complete.



> **Tip:** View the **Wireless** table on the **Status** tab to verify that links for this device have come up again.

If you are unable to reach the device's WebUI but are near the unit and can physically disconnect it from power, a power cycle will perform a hard reboot of the device.

Factory Reset

Use the **Restore Factory Defaults** button in the WebUI on the Admin tab to reset the unit to factory settings. The unit reboots after the factory reset.

Restore factory defaults by using the WebUI

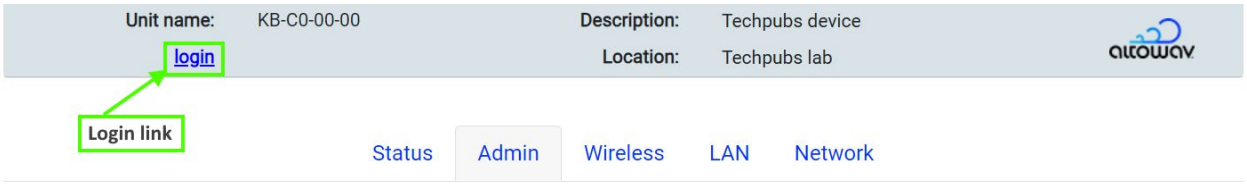
Use the **Restore Factory Defaults** button in the device's WebUI to reset the device.

1. Access the WebUI of the K60DN and K60CN1. In your browser's address bar, type:

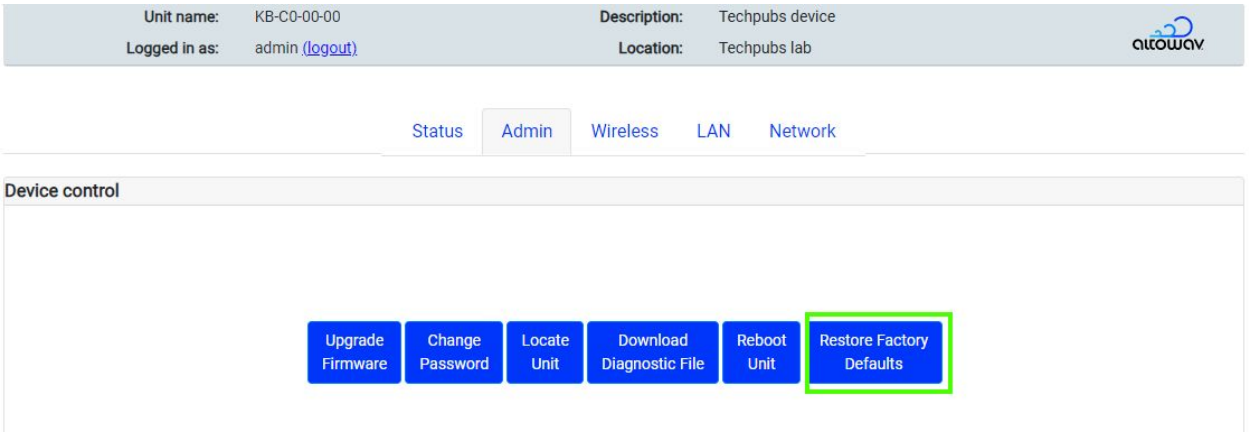
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Restore Factory Defaults** button in the **Device control** section.



5. A confirmation dialog opens. Enter the text **confirm factory reset** and click **OK**.

After the reset, the device reboots with factory default settings. The login credentials for the device return to **admin**. Reconfigure the device as necessary to reestablish radio links, set location and description, and configure the network settings.

Restore factory defaults by using a hard reset

If the WebUI or CLI is inaccessible due to a lost password or in cases where Network settings are inadvertently set to unworkable values, use a reset dongle to perform a Hard Reset on the device. The same reset dongle used for the K60 and K60x Gen2 devices can be used to reset the K60DN and K60CN1 devices.

To make a reset dongle:

1. Cut the end off of a short length of Ethernet cable with a plug, and strip the outer insulation from the end.
2. Short the white/orange, orange pair (pins 1 and 2 for T568B), by stripping their insulation and twisting them together. Leave the rest of the wires open, (do not connect them to anything.)
3. Remove the tab from the Ethernet plug to make inserting and removing the plug easy.

K60DN Hard Reset

Warning! Do not insert the reset dongle into any passive PoE output ports on the K60DN -- eth2, eth3, eth4.

1. Disconnect power from the K60DN.
2. Insert the Factory Reset dongle into the K60DN PoE output port labeled **LAN1 (54V)**. This port is also called Ethernet port1 in the WebUI.

3. Reconnect power and wait about 50 seconds. During this time, the LEDs flash the Hard Reset to Factory Defaults sequence: **B** is lit while **A** and **C** alternate on/off.
4. When the reset sequence completes, remove the dongle. The Hard Reset is complete.

Note: After the reset, normal operation resumes with factory settings.

> **Tip:** For ground-level resets on pole-mounted K60DNs or other hard to access units, install an Ethernet cable in the LAN1 port, running the other end to a secured lock box, or similar. Use a coupler to connect the dongle to that cable.

K60CN1 Hard Reset

1. Disconnect power from the K60CN1.
2. Insert the Factory Reset dongle into the K60CN1 **LAN** port.

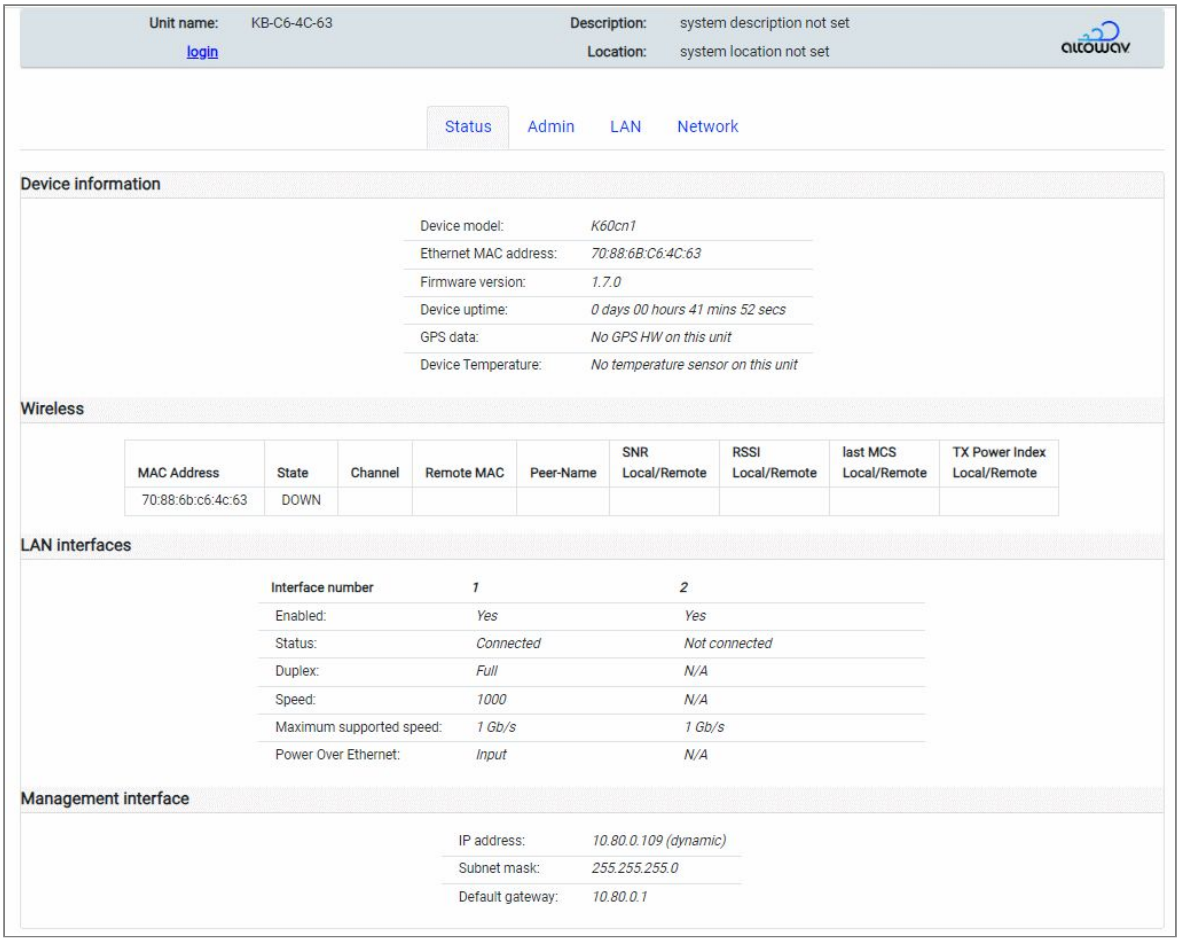
3. Reconnect power and wait about 50 seconds. During this time the LEDs flash the Hard Reset to Factory Defaults sequence: **Uplink(PoE)** is lit while **LAN** and **60G** alternate on/off.
4. When the reset sequence completes, remove the dongle. The Hard Reset is complete.

After the reset, the device reboots with factory default settings. The login credentials for the device return to **admin**. Reconfigure the device as necessary to reestablish radio links, set location and description, and configure the network settings.

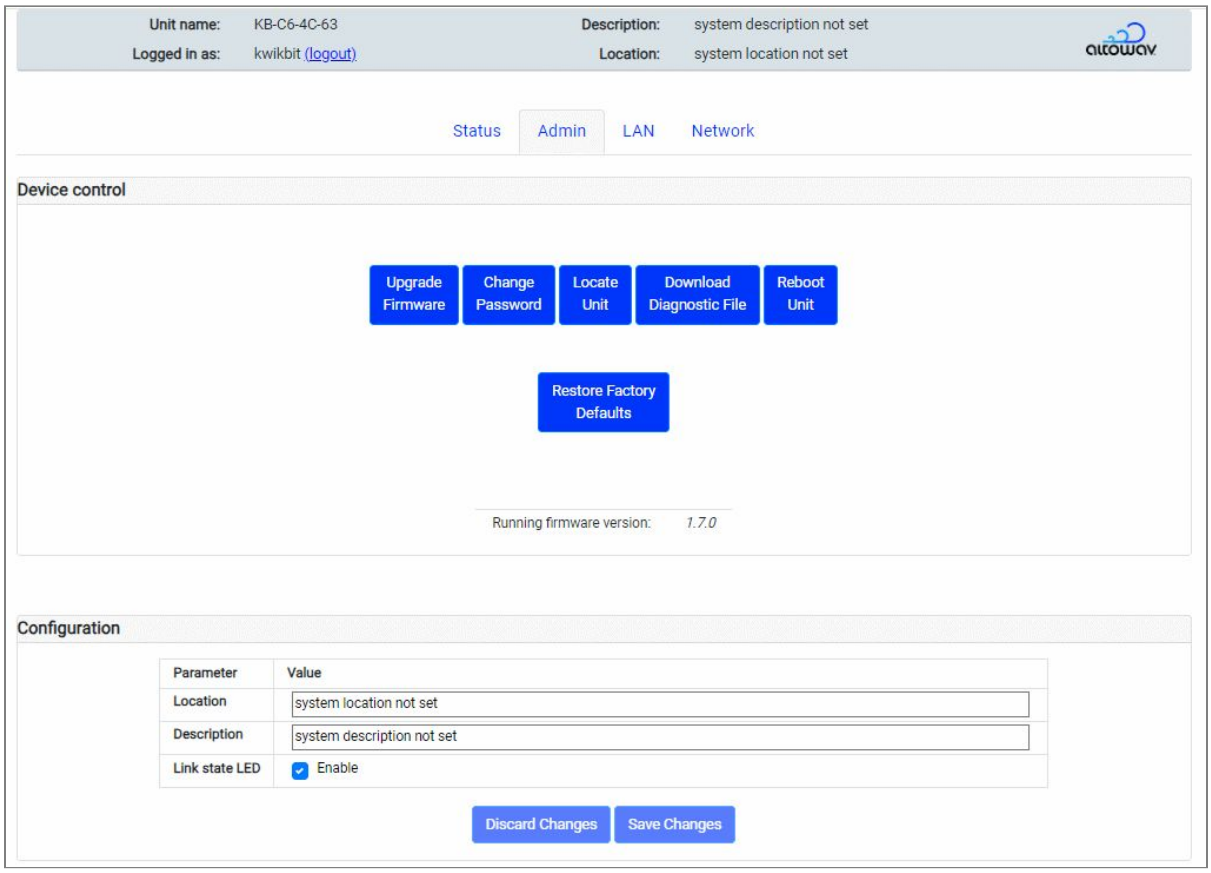
Factory Default WebUI Screenshots

The following screenshots show factory default values. In addition, default values for individual settings are listed in tool tips in the WebUI when the cursor hovers over the setting.

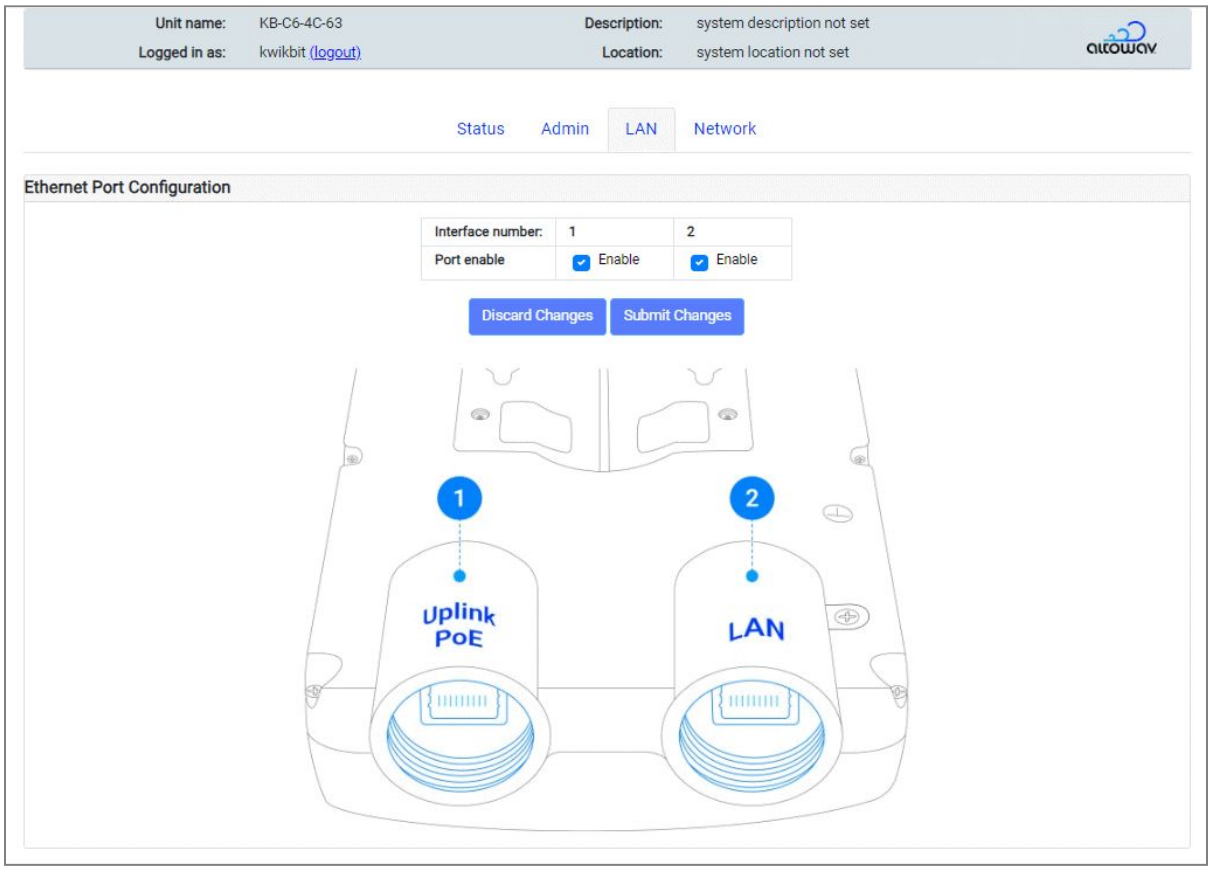
K60CN1 Factory Defaults - Status



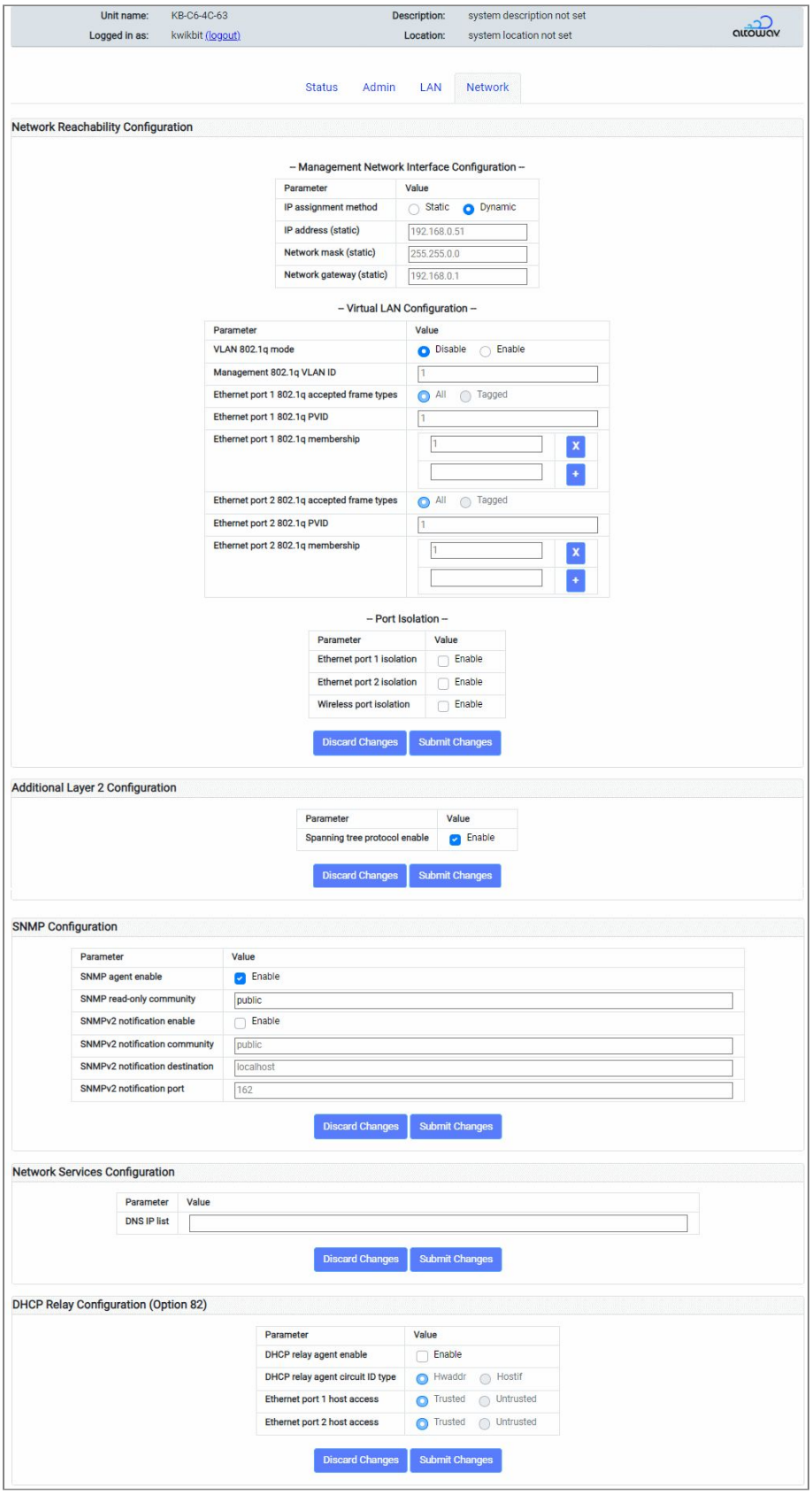
K60CN1 Factory Defaults - Admin



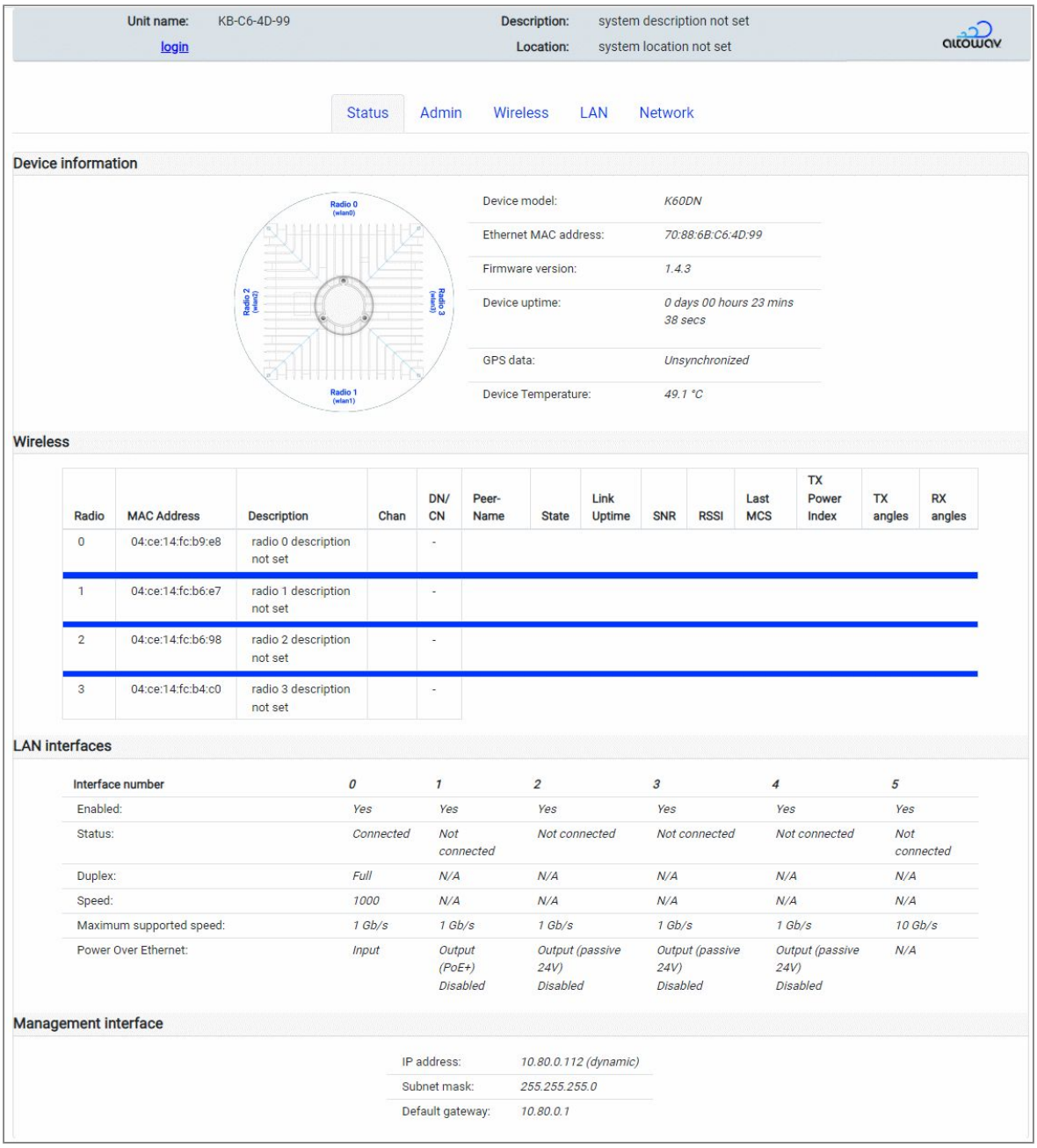
K60CN1 Factory Defaults - LAN



K60CN1 Factory Defaults - Network



K60DN Factory Defaults - Status



Unit name: KB-C6-4D-99 Description: system description not set
login Location: system location not set

Status | Admin | Wireless | LAN | Network

Device information

Device model:	*K60DN*
Ethernet MAC address:	*70:88:6B:C6:4D:99*
Firmware version:	*1.4.3*
Device uptime:	*0 days 00 hours 23 mins 38 secs*
GPS data:	*Unsynchronized*
Device Temperature:	*49.1 °C*

Wireless

Radio	MAC Address	Description	Chan	DN/CN	Peer-Name	State	Link Uptime	SNR	RSSI	Last MCS	TX Power Index	TX angles	RX angles
0	04:ce:14:fc:b9:e8	radio 0 description not set		-									
1	04:ce:14:fc:b6:e7	radio 1 description not set		-									
2	04:ce:14:fc:b6:98	radio 2 description not set		-									
3	04:ce:14:fc:b4:c0	radio 3 description not set		-									

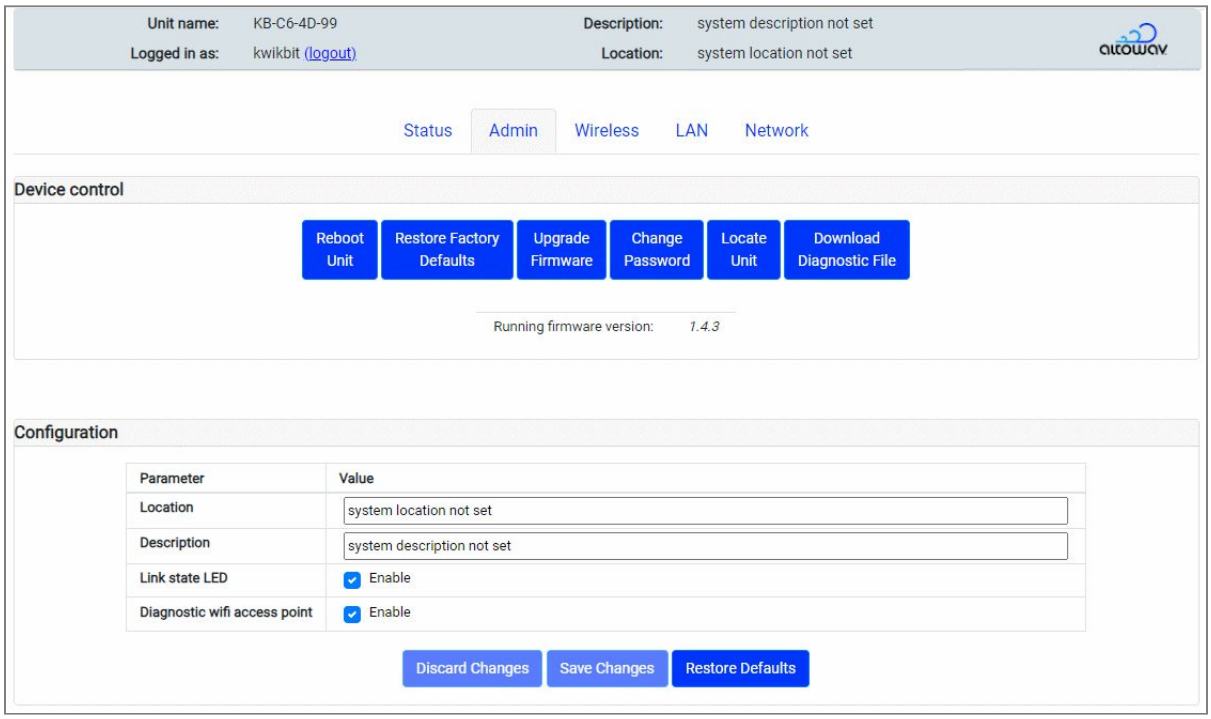
LAN interfaces

Interface number	*0*	*1*	*2*	*3*	*4*	*5*
Enabled:	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Status:	*Connected*	*Not connected*	*Not connected*	*Not connected*	*Not connected*	*Not connected*
Duplex:	*Full*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Speed:	*1000*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Maximum supported speed:	*1 Gb/s*	*1 Gb/s*	*1 Gb/s*	*1 Gb/s*	*1 Gb/s*	*10 Gb/s*
Power Over Ethernet:	*Input*	*Output (PoE+) Disabled*	*Output (passive 24V) Disabled*	*Output (passive 24V) Disabled*	*Output (passive 24V) Disabled*	*N/A*

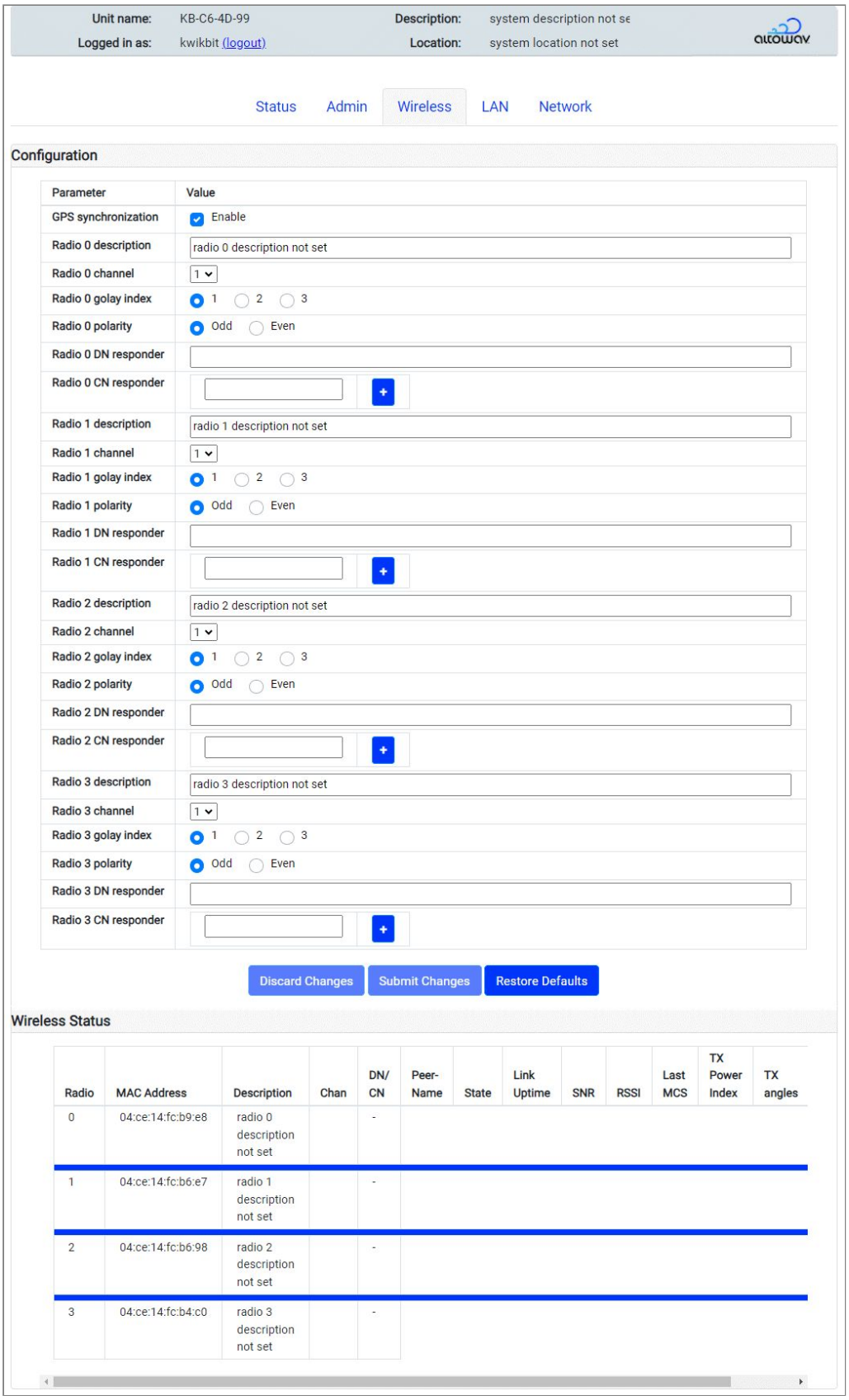
Management interface

IP address:	*10.80.0.112 (dynamic)*
Subnet mask:	*255.255.255.0*
Default gateway:	*10.80.0.1*

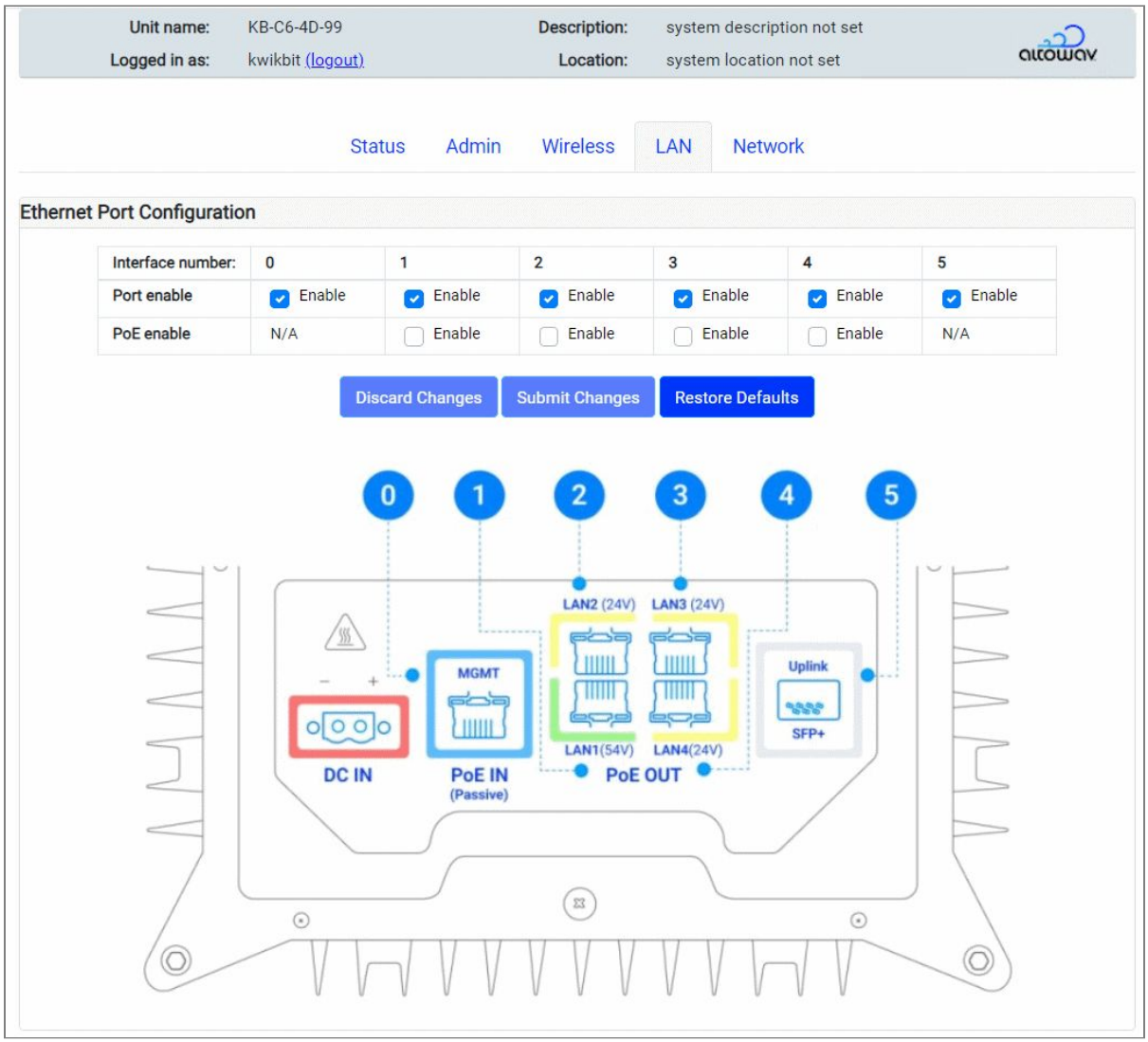
K60DN Factory Defaults - Admin



K60DN Factory Defaults - Wireless

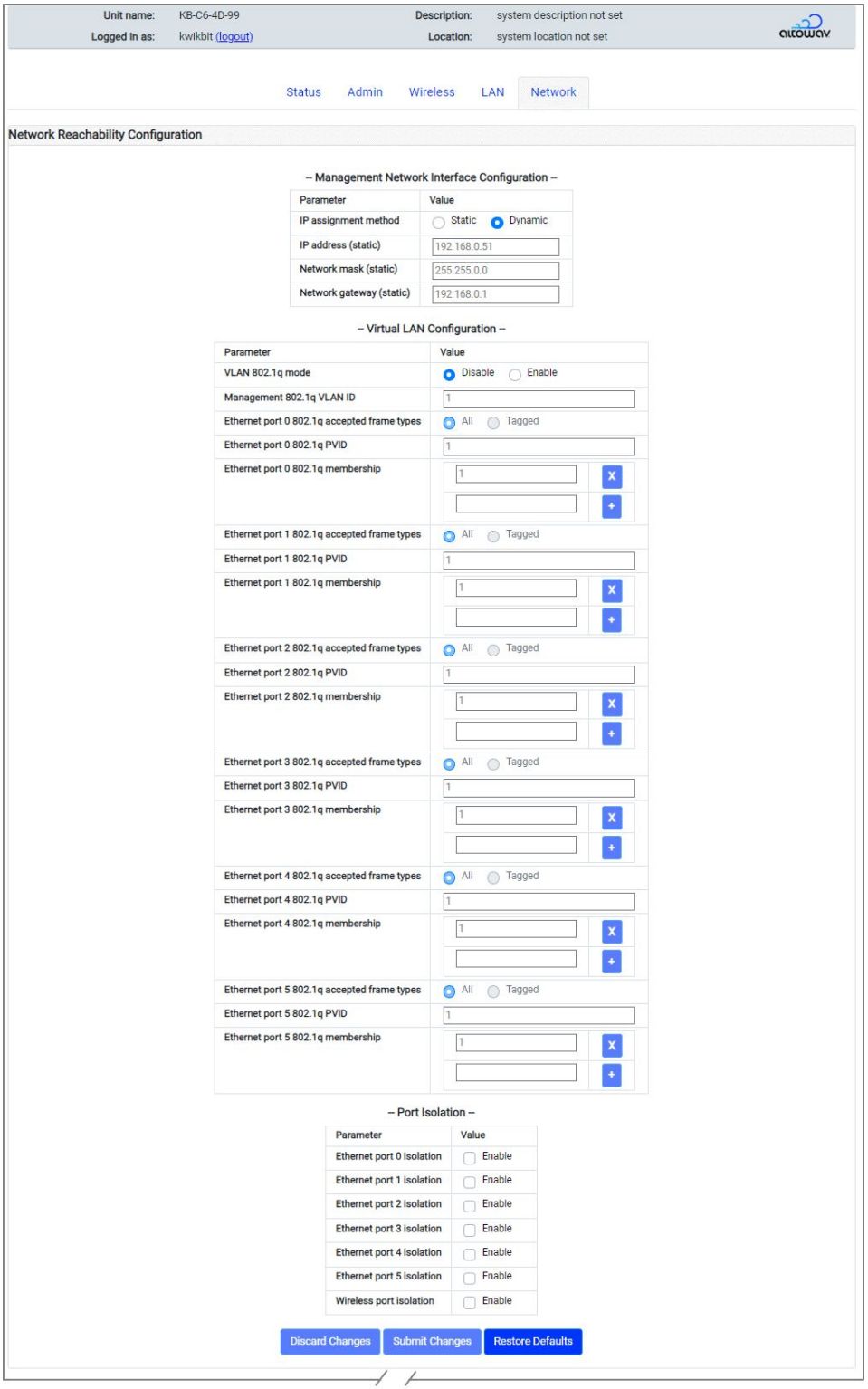


K60DN Factory Defaults - LAN

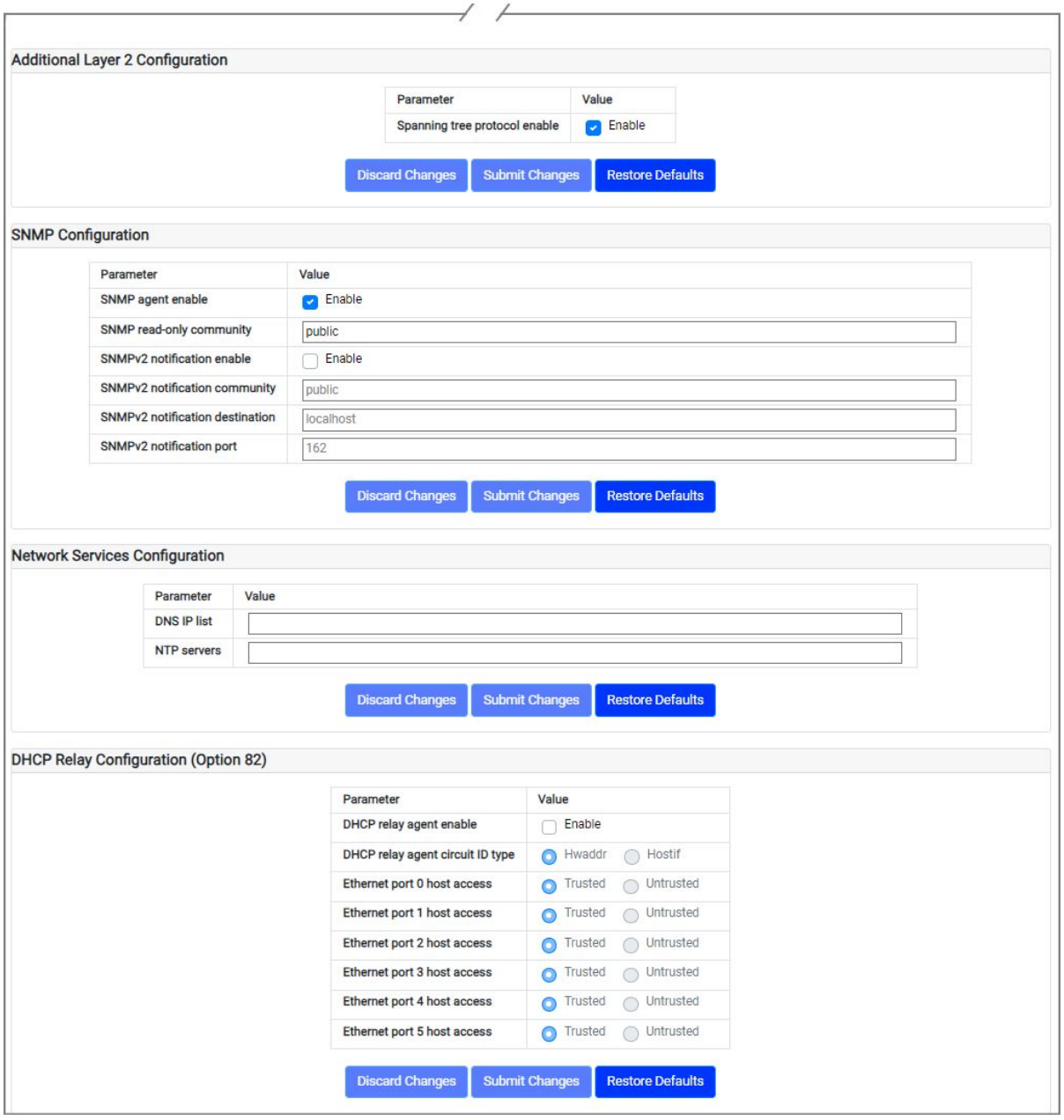


K60DN Factory Defaults - Network

The Network tab defaults for the K60DN are shown in the two images that follow. First the top of the K60DN Network tab with default settings.



The bottom of the Factory default Network tab for the K60DN WebUI.



Troubleshooting

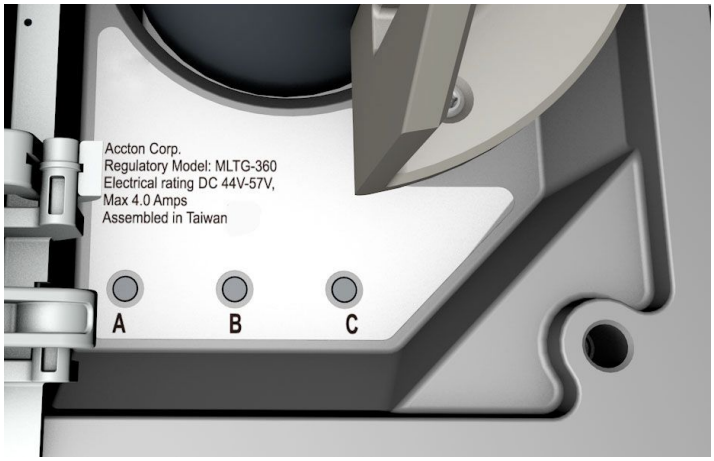
This chapter contains the following topics:

LED Indicator Lights

LED lights on each device show the state of the unit by displaying different sequences. The K60DN and K60CN1 sequences are listed in this topic.

K60DN

LEDs on the bottom of the K60DN show connections and activity.



These functions are indicated with A, B, C LED indicators.

Normal operation:

- **A** indicates an external Ethernet link.
- **B** is the power indicator.
- **C** indicates wireless link(s).

Boot-up sequence:

B blinks on once. Then **A**, **B**, **C** are off and the LAN port lights are on for 10-50 seconds. Then lights resume normal operation with **B** on steady and **A** and **C** lighting up as external Ethernet links and wireless links become active.

Device location sequence:

B is on, while **A** and **C** are blinking.

Hard reset to factory defaults sequence:

B is lit while **A** and **C** alternate on/off. (**A** is lit and **C** is off, then **A** is off and **C** is lit, repeating.)

Note, the Hard Reset sequence is not shown when the K60DN is restored to factory defaults through the WebUI or the CLI.

Error sequence:

Conditions for error sequences include overheating, radio errors during startup, or other errors.

B is off. **A** and **C** are lit steady, no flashing.

Note, if the K60DN shuts down due to overheating, all LEDs will go off.

Manufacturing state:

Shown with a back-and-forth sequence - **A** blinks, **B** blinks, **C** blinks, **B** blinks, **A** blinks, repeating and timed to look like a smooth back-and-forth motion of the lights.

K60CN1

LEDs on the back of the K60CN1 show connections and activity.

These functions are indicated with LAN, Uplink(PoE), and 60G LED indicators.

Normal operation:

- **LAN** is lit to indicate an external Ethernet link. (Green)
- **Uplink(PoE)** is the power indicator. (Red)
- **60G** indicates a wireless link. (Blue)

Boot-up sequence:

All lights are on for 25 seconds. Then all lights are off for 10-50 seconds. Then lights resume normal operation.

Device location sequence:

Uplink(PoE) is on, while **LAN** and **60G** are blinking.

Hard reset to factory defaults sequence:

Uplink(PoE) is lit while **LAN** and **60G** alternate on/off. (**LAN** is lit and **60G** is off, then **LAN** is off and **60G** is lit, repeating.)

Note, the hard reset sequence is not shown when the K60CN1 is restored to factory defaults through the WebUI or the CLI.

Error sequence:

Conditions for error sequences include radio errors during startup, or other errors.

Uplink(PoE) is off. **LAN** and **60G** are lit steady, no flashing.

Manufacturing state:

Shown with a back-and-forth sequence - LAN blinks, Uplink(PoE) blinks, 60G blinks, Uplink(PoE) blinks, LAN blinks, repeating and timed to look like a smooth back-and-forth motion of the lights.

How to Power-cycle a Device

Power-cycling a device may be done during installation, after re-aiming a device or less commonly during troubleshooting an issue.

Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

To power-cycle the K60DN or K60CN1, simply disconnect it from power and reconnect it. Wait for the device to fully power up and reconnect.

> **Tip:** For devices running firmware versions prior to v1.8.1, avoid several consecutive power-cycles in rapid sequence, because they may result in a hard reset to factory defaults.

Lost Password

If a K60DN and K60CN1 device password is lost, the device may have to be reset to factory defaults.

After the reset, operation resumes with factory default settings, including the default password: **admin**.

Download a Diagnostic File

Altowav is committed to providing high quality technical support. If you encounter an unusual issue that you cannot easily solve through standard troubleshooting, please contact us at support@altowav.com with the following information:

- Your contact information.
- The type and model of hardware with the issue.
- Product serial number.
- A description of the issue.

We also recommend that you provide a diagnostic log of device interactions and conditions.

Note: A diagnostic log file captures historical information about a device's operation. It is important to download the diagnostic file before rebooting or power-cycling a device as part of troubleshooting. Rebooting or power-cycling will clear the log file history.

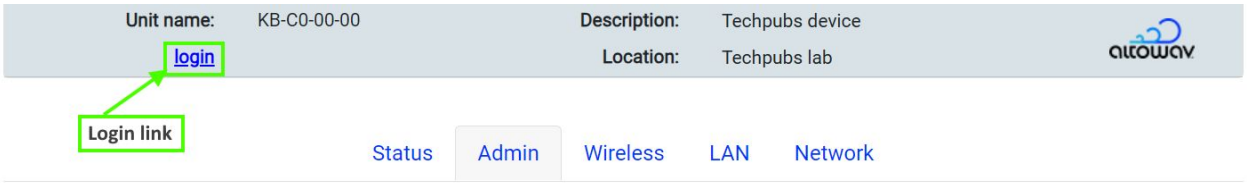
Follow these steps to download a diagnostic file for connected devices from the WebUI:

1. Access the WebUI of the K60DN and K60CN1. In your browser's address bar, type:

   https://*hostname*

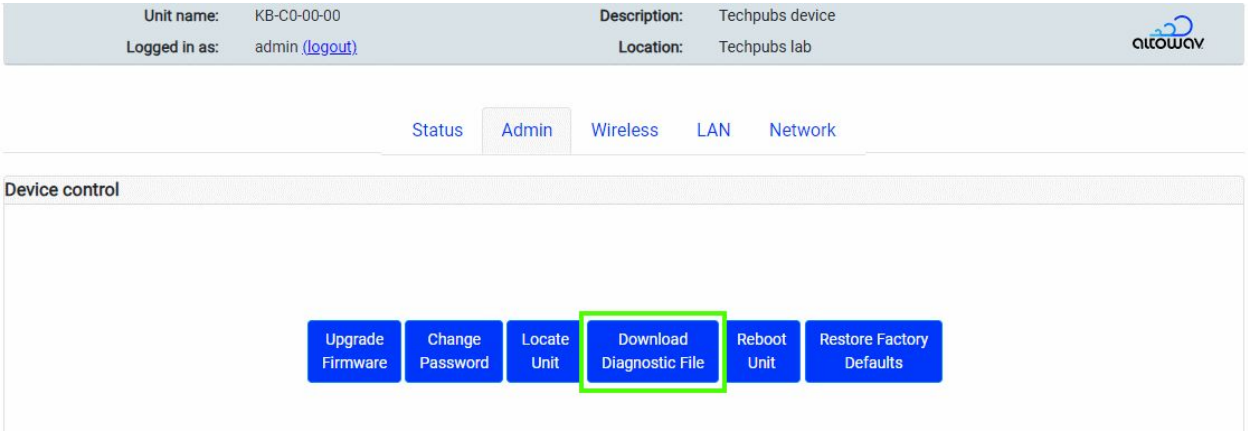
   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the K60DN and K60CN1 for more information.

2. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



3. Click on the **Admin** tab.

4. Click on the **Download Diagnostic File** button in the **Device control** section.



5. The file is sent to your system's default download location. The file name includes the host name (KB MAC) of the device and the date. For example, KB-C6-00-01_diag_2025-12-04-20-32-26.txt
6. Zip the file and attach it to an email to support@altowav.com or a ticket at support.altowav.com.

Create a diagnostic file from the REST API

1. Use the `admin/diagdump` API to create a diagnostic file from the REST API. For example, use the curl command to save the diagnostic information to a file named `diag_dump`, created in the current directory:
   `curl -k -o diag_file.txt -u admin:<password> https://<hostname>/rest/v002/admin/diagdump`

   where:
   - *password* is the password to log into the device. The default password is **admin**.
   - *hostname* is the hostname or IP address of the device.
2. Zip the file and attach it to an email to support@altowav.com or the ticket at support.altowav.com.

Connect to a K60DN via Wi-Fi

When a K60DN resets to factory defaults, Wi-Fi is enabled, allowing you to reach and reconfigure an otherwise unreachable unit via Wi-Fi.

Some uncommon scenarios where this may be useful:

- If the WebUI or CLI is inaccessible due to a lost password or in cases where Network settings were inadvertently set to unworkable values and a direct connection is not feasible due to where the unit is mounted. If the unit must be reset to factory defaults with the power cycle method to restore settings, a Wi-Fi connection may be useful to reconfigure settings.
- After the initial install of a unit, if links do not come up as expected per your design, a Wi-Fi connection could be used to verify and update configurations. This may be especially helpful in cases where the unit is rotated, resulting in sector orientation that is different from the design plan. Or in cases, where bench configuration was done improperly, the connection can be used to reconfigure DN responders. **Tip:** A better way to address this issue is to make sure links come up while a technician is still on the pole.
- In rare cases, the K60DN could become unreachable after configuration and operation in a network. If the unit cannot be reached via wireless link or Ethernet link, the unit may be reached via Wi-Fi.

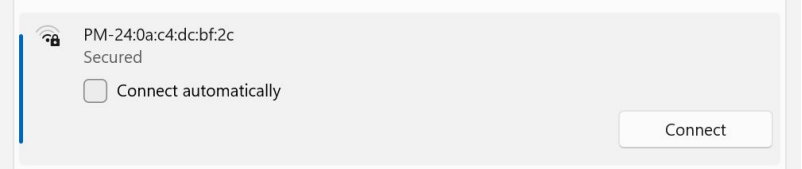
Note: This process should only to be used to reconnect an unconnected K60DN. Once connection is restored, use the WebUI or CLI to configure settings.

Prerequisites for connecting to the K60DN via Wi-Fi:

- You must be in close range to the K60DN in order to connect to it via Wi-Fi -- generally within 10 - 20 ft.
- A K60DN allows only one incoming connection to Wi-Fi at a time. If multiple technicians are onsite, only one may be connected.

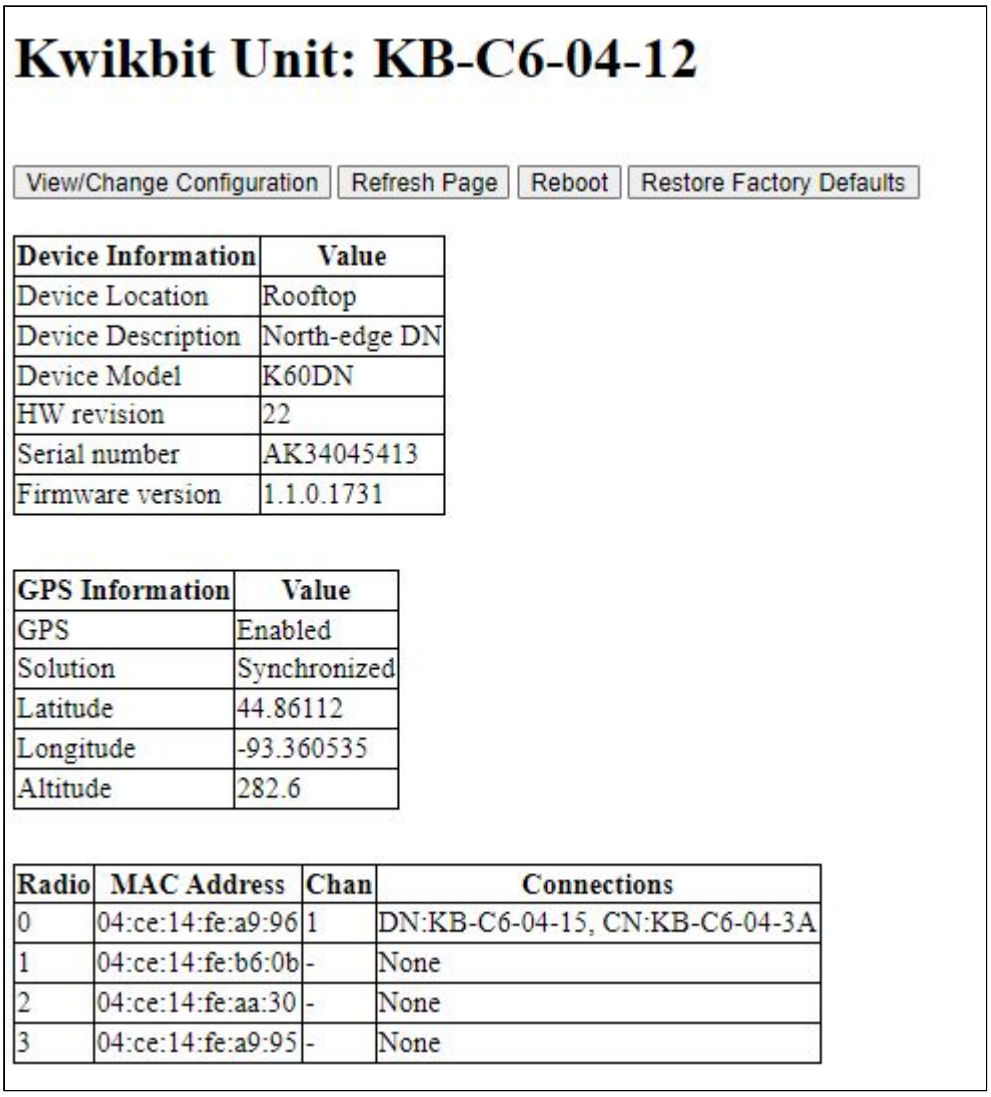
Steps to configure the K60DN via Wi-Fi:

1. Look for the PM MAC address in Wi-Fi search and connect to it. Make sure to clear any settings for **Connect automatically**. This prevents attempts to reconnect when you get into close proximity again later. Click **Connect**.



Enter the password when prompted: **facebook**

2. Enter the K60DN's static IP address **https://192.168.5.1** into the web browser address bar. Click the **Advanced** button and **Proceed** to the site.
3. The Kwikbit Unit page opens listing the name of the unit (KB-C6-xx-xx). Verify that it is the device you intend to connect to, then enter the password: **kwikbit**. The Status page opens.



Kwikbit Unit: KB-C6-04-12

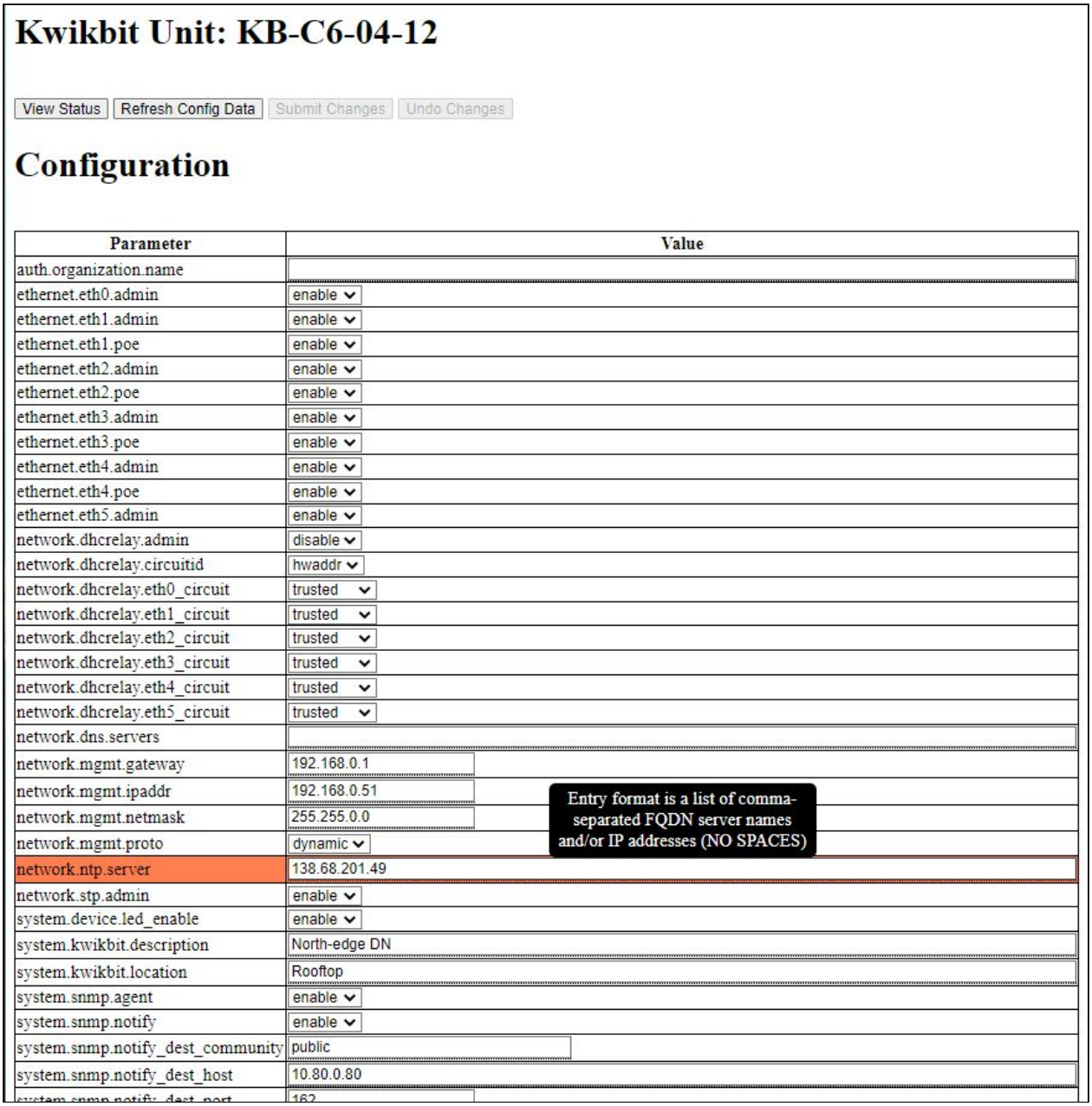
View/Change Configuration | Refresh Page | Reboot | Restore Factory Defaults

Device Information	Value
Device Location	Rooftop
Device Description	North-edge DN
Device Model	K60DN
HW revision	22
Serial number	AK34045413
Firmware version	1.1.0.1731

GPS Information	Value
GPS	Enabled
Solution	Synchronized
Latitude	44.86112
Longitude	-93.360535
Altitude	282.6

Radio	MAC Address	Chan	Connections
0	04:ce:14:fe:a9:96	1	DN:KB-C6-04-15, CN:KB-C6-04-3A
1	04:ce:14:fe:b6:0b	-	None
2	04:ce:14:fe:aa:30	-	None
3	04:ce:14:fe:a9:95	-	None

4. Click the **View/Change Configuration** button. Configuration parameters are listed alphabetically. Hover over an entry field for information about the expected format for the setting, as shown in the image below for `network.ntp.server`. The image shows a partial listing of the settings.



Kwikbit Unit: KB-C6-04-12

View Status | Refresh Config Data | Submit Changes | Undo Changes

Configuration

Parameter	Value
auth.organization.name	
ethernet.eth0.admin	enable
ethernet.eth1.admin	enable
ethernet.eth1.poe	enable
ethernet.eth2.admin	enable
ethernet.eth2.poe	enable
ethernet.eth3.admin	enable
ethernet.eth3.poe	enable
ethernet.eth4.admin	enable
ethernet.eth4.poe	enable
ethernet.eth5.admin	enable
network.dhcrelay.admin	disable
network.dhcrelay.circuitid	hwaddr
network.dhcrelay.eth0_circuit	trusted
network.dhcrelay.eth1_circuit	trusted
network.dhcrelay.eth2_circuit	trusted
network.dhcrelay.eth3_circuit	trusted
network.dhcrelay.eth4_circuit	trusted
network.dhcrelay.eth5_circuit	trusted
network.dns.servers	
network.mgmt.gateway	192.168.0.1
network.mgmt.ipaddr	192.168.0.51
network.mgmt.netmask	255.255.0.0
network.mgmt.proto	dynamic
network.ntp.server	138.68.201.49
network.stp.admin	enable
system.device.led_enable	enable
system.kwikbit.description	North-edge DN
system.kwikbit.location	Rooftop
system.snmp.agent	enable
system.snmp.notify	enable
system.snmp.notify_dest_community	public
system.snmp.notify_dest_host	10.80.0.80
system.snmp.notify_dest_port	162

Entry format is a list of comma-separated FQDN server names and/or IP addresses (NO SPACES)

5. Enter the changes, making sure the correct values are entered for the correct radio interfaces where applicable. **Note,** interfaces for Radio 0, Radio 1, Radio 2, and Radio 3 (in the WebUI) are also known as wlan0, wlan1, wlan2, wlan3 when editing configuration parameters via the REST API and CLI. Typical configuration changes used to address reachability issues include:
    - Channel - **`wireless.wlanx.channel`**
    - Golay code - **`wireless.wlanx.golay`**
    - Polarity - **`wireless.wlanx.polarity`**
    - DN responder - **`wireless.wlanx.DN_responder`**
    - GPS sync - **`wireless.device.gps_sync`**

6. After verifying the changes are set for the correct radio interfaces, click **Submit Changes** at the top of the page to finalize. If the entered changes are not correct, click **Undo Changes** and enter the correct settings.

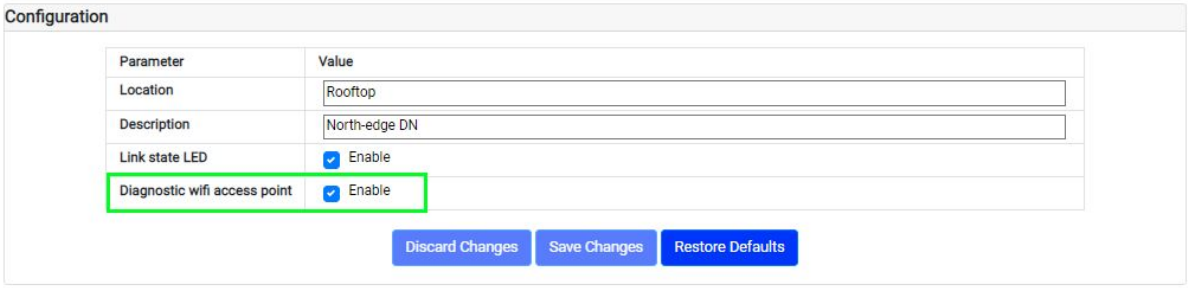
   Close the browser window to disconnect.

Congratulations. The K60DN is now reachable via airlink. Do any further configuration via the WebUI or CLI.

Enable / Disable Wi-Fi access to K60DN

Diagnostic Wi-Fi Access is enabled by default.

The configuration parameter for enabling and disabling Wi-Fi point for the K60DN is **`wifi.ap.admin.`** In the K60DN's standard WebUI, the setting can be found on the Admin tab in the Configuration section.



Note: Disabling this setting turns off the Wi-Fi access point completely, (not just the Wi-Fi user interface). The device will not be seen by a Wi-Fi search when this setting is disabled.

Unexpected Drop in MCS Level

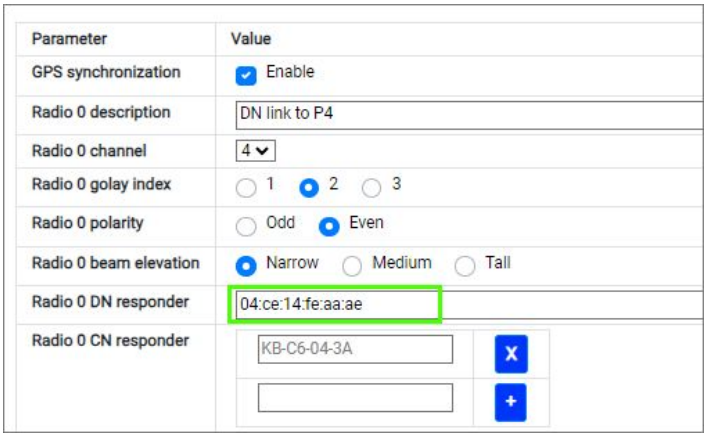
Two known cases where an unexpected drop in MCS level occurred for some K60DN links in a distribution network:

- After a power outage. When power was restored, K60DN links were re-established, but some formed at a lower than desired MCS level.
- When a firmware upgrade was scripted to occur on all K60DN units at once, rather than the recommended order of one K60DN at a time, starting with the K60DN furthest from the PoP. In addition, no lag time to re-establish links for the upgraded unit was built into the scripted upgrade.

Steps to resolve this issue by rebeamforming from the initiator side of the K60DN-K60DN link:

Note: These steps disrupt the affected link for a short period of time.

1. Check power levels for higher than normal usage. (This may indicate that increased power is attempting to remedy the lower MCS level automatically.)
2. Determine the MAC address for the K60DN radio sector on each end of the affected link. The lower radio MAC address of the two identifies the initiator for the link. For example, 04:ce:14:fe:a9:96 (lower MAC is initiator) and 04:ce:14:fe:aa:ae (higher MAC is responder).
3. **Disconnect the link.** Browse to the initiator's WebUI, Wireless tab and clear the **DN responder** field. Click **Submit Changes** and verify that the link is NOT shown in the Wireless Status table.
4. **Reconnect the link.** Re-enter the radio MAC address in the **DN responder** field and click **Submit Changes**. Verify the link is shown again in the Wireless Status table.



5. Verify the MCS level. Generate traffic as needed to adequately test MCS level for the link.

> **Tip:** For RF Engineers who want more information for diagnostic purposes, it may be useful to look at the syslog when rebeamforming to ensure no link pauses occur, as that

> might indicate another problem. (Syslog via CLI: use the **`syslog_show`** command. Syslog via the REST API: Use the following URL. **`https://<server_name>/rest/v002/device/syslog`**.)

Steps to resolve this by running kb_scan in the CLI to rebeamform:

Beamforming with **kb_scan** is done within a few degrees of the current link. Determine the MAC address for the K60DN radio interface on each end of the affected link.

1. SSH into a K60DN on one end of the link. (Initiator / responder roles do not matter for running kb_scan.)
2. Run these commands at the > prompt:
   A. **`control`**
   B. **`kb_scan <local radio MAC> <remote radio MAC>`**

   This schedules a relative periodic beamforming PBF) on the link. (PBF occurs per schedule and will also depend upon the number of **`kb_scan`** commands run. So, it could run immediately or take several minutes.) Once PBF begins, it takes about a second and during that time throughput is reduced to 50% on the link.

Check performance statistics for the link in the WebUI or via other monitoring. Note, reported TX angles and RX angles do not currently have enough granularity to observe much change. You can report values for beam index for a link via the REST API, **link_quality**.

Additional information about the **kb_scan** CLI command:

- It is available for K60DN (v1.3.0 and higher), but the remote devices for the link can be running earlier versions of firmware.
- For K60DN-K60CN1 links, kb_scan must be run from the K60DN. It is not available on the K60CN1.

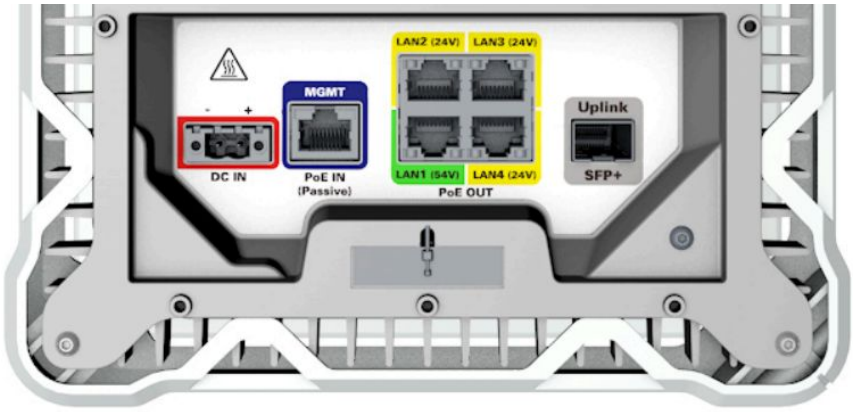
If these steps do not resolve the issue, start a ticket at support.altowav.com or Contact us.

Appendixes

Connecting K60DN to the Procet-1N

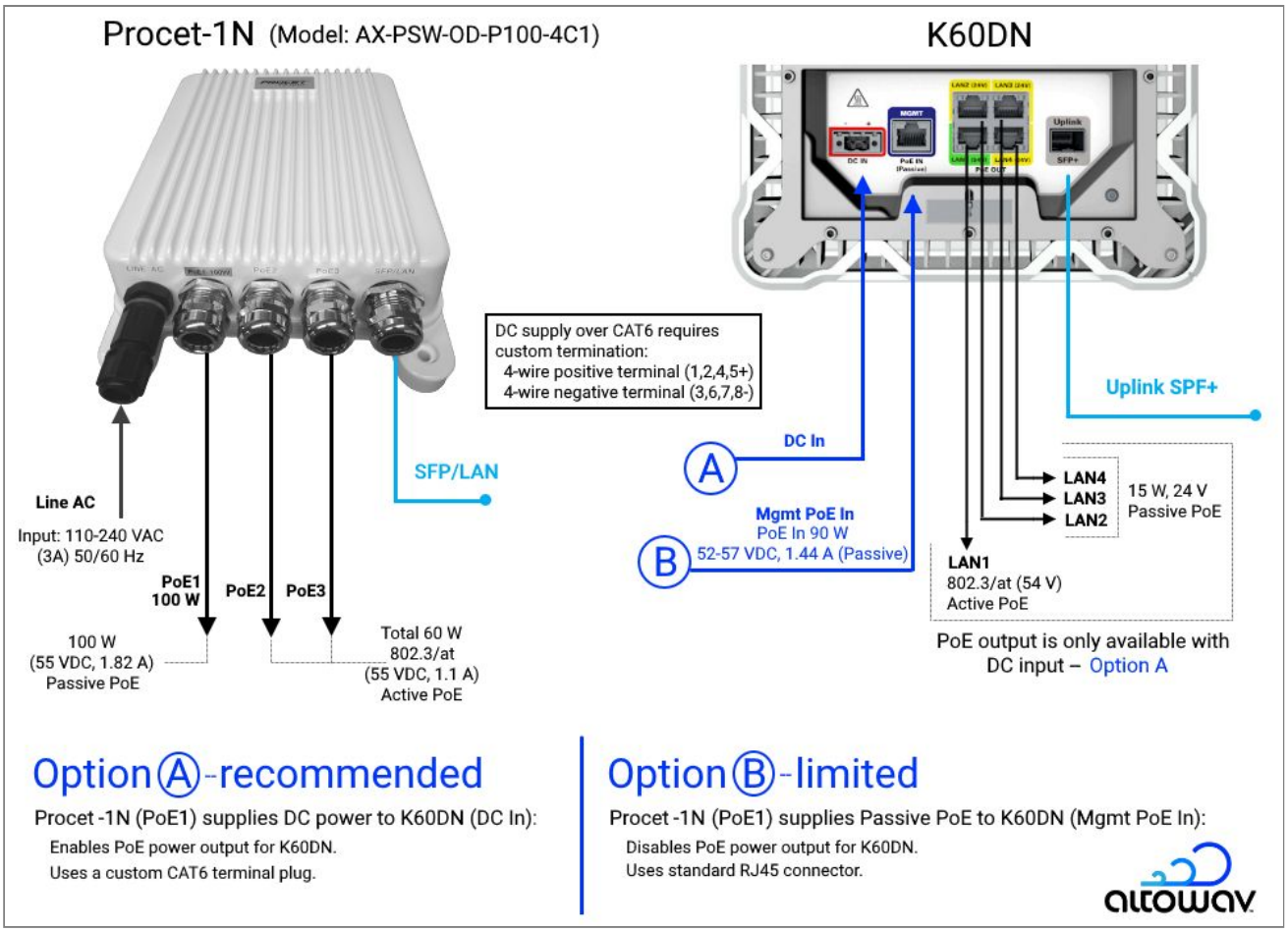
Power can be supplied to the K60DN via DC power input or via Passive PoE input. Some background:

- The K60DN requires DC power input to provide PoE power out on its RJ45 ports (LAN1, LAN2, LAN3, LAN4).
- If PoE power is supplied instead of DC power, the K60DN requires 90 W, 52-57 VDC, 1.44 A Passive PoE power for the MGMT PoE In port.
- Do not supply both DC power and PoE power at the same time!



An outdoor power supply, the Procet-1N, provides multiple power options. (Altowav Model: AX-PSW-OD-P100-4C1. Altowav PN: 1430-2410-3210.)

Select Option A or B for powering the K60DN:



Option Ⓐ- recommended - Procet-1N supplies power from **PoE1** to the **DCin** terminal on the K60DN using the custom CAT6 terminal plug.

Option A enables the PoE ports on the K60DN to be used, one 54 V and three 24 V (the combined available power for the ports is approximately 25 W). Using the Procet-1N ports, PoE2 and PoE3 with network connectivity, requires the Procet-1N SFP/LAN port to be connected to an available RJ45 port on the K60DN, (Mgmt PoE IN or one of the 24V ports are preferred). This makes up to six PoE ports available for accessories, four on the K60DN (1@54 V and 3@24V) and two on the Procet-1N switch (55 V).

Option Ⓑ- acceptable but limited - Procet-1N supplies power from PoE1 to the **Mgmt PoE In (Passive)** port on the K60DN using a standard RJ45 connector.

Option B Leaves ports PoE2 and PoE3 (55 V) available on the Procet-1N switch. The SFP/LAN connection from the Procet-1N switch is not needed for this configuration because the network connection is made between the Procet-1N PoE1 port and the K60DN Mgmt PoE IN port.

Steps to Connect the Procet-1N to the K60DN

1. Connect one end of outdoor-rated CAT6 cable to port **PoE1** on the Procet.
    a. Remove the outer cap assembly from port PoE1.
    b. Feed the Cat6 through the assembly and plug the RJ45 in securely. Listen for a click.
    c. Replace the outer cap assembly making sure not to over tighten.
2. Connect the other end of the CAT6 cable to the K60DN using Option A or Option B.

Option A: Wire and install the custom 2-pin plug for the DC In terminal on the K60DN

Attach the supplied 2-pin DC terminal plug (Altowav PN: 1432-0100-0002) to the outdoor-rated CAT6 cable for the K60DN **DC In** terminal.

PINS	T568B Color
Pin 1	white/orange stripe
Pin 2	orange solid
Pin 3	white/green stripe
Pin 4	blue solid
Pin 5	white/blue stripe
Pin 6	green solid
Pin 7	white/brown stripe
Pin 8	brown solid

a. Install the CAT6 wires from the Procet-1N switch PoE1 port to the positive/negative terminals in the following way.

   Positive terminal (+): 1, 2, 4, 5 - orange and blue pairs.

   Negative terminal (-): 3, 6, 7, 8 - green and brown pairs.

b. Insert the wires. Twist the wires together for each terminal. This helps to avoid shorts and nicks, and makes insertion easier.
c. Tighten the screws.
d. Plug into the **DC In** port on the K60DN and tighten the plug screws.

Option B: Plug the RJ45 into the Mgmt PoE Uplink port on the K60DN

This PoE option supplies passive power to the K60DN, simplifying the installation, but is limited because PoE output is not available on the K60DN LAN ports. This eliminates the option of connecting the K60DN to cameras, Wi-Fi, or other devices requiring PoE power. However, Procet-1N ports PoE2 and PoE3 can be used to power accessories.

Glossary

802.11ay — An enhanced standard for WLANs operating in the 60 GHz spectrum.

Backhaul — Networking infrastructure that connects a local subnetwork to the primary network. Also known as network backhaul.

Channel — In Wi-Fi networking, a channel is a specific frequency range within a broader range. The radios in AltoPlex devices can be configured to operate on one of four channels within the 60 GHz spectrum.

Device hostname — In AltoPlex devices, the device hostname uses the last three octets of the device's MAC address, with **KB** appended to the beginning. For example, KB-C6-00-01.

Distribution node — Distribution nodes serve as connected nodes in a distribution network. Distributions nodes can provide network access via a wired connection to the backhaul network, wired connections through a switch to other distribution nodes, and wireless connections to other distribution nodes and to .

DN — See .

Fixed wirelesss access — Networking technology that provides high-speed network access to a fixed location using a radio connection.

FWA — See Fixed wireless network.

GPON — Gigabit Passive Optical Network. A high-bandwidth mechanism for providing network access to a fibre optic backhaul network.

Golay index — An error correction mechanism used in wireless communications to mitigate co-channel interference. Wireless devices communicating on the same channel can mitigate interference by using different Golay indexes.

Hub-and-spoke — A network topology that involves central nodes with access to the backhaul network, and several nodes wirelessly connected to those central nodes.

Initiator — The that initially establishes a link with a remote device. By default, the intiator is the radio interface with the lower MAC address. See also responder.

MCS — Modulation Coding Scheme. AltoPlex devices use a weighted MCS value of 2-12. MCS is prioritized in AltoPlex devices. MCS and TX power are adjusted automatically based on Power/packet Error Rate (PER). A link will stay at MCS 9 when minimal network traffic is observed.

Node — A single AltoPlex device in a multi-device installation.

NTP — Network Time Protocol. Enables the synchronization of a device's time to an upstream NTP server.

Point-to-point — A network topology in which two devices are directly connected to each other.

Point-to-multipoint — A network topology in which multiple devices are connected to a central node. In a point-to-multipoint network, AltoPlex distribution nodes support one DN link and up to fifteen CN links.

Polarity — Polarity is a mechanism of TDMA used in determining when to transmit or receive during a timing cycle. Polarity is either odd or even.

P2P, **PtP** — See point-to-point.

PtMP, PMP — See point-to-multipoint.

Point of presence — The location or facility that connects to the Internet. Often this may be an equipment cabinet or similar location with fiber access to the primary network and/or the internet.

PoP — See point of presence.

PoP node — The distribution node (or nodes) that is directly connected to the primary network and/or the internet. This distinction is important for optimizing traffic when designing network topology. During deployment, the PoP node devices are the first installed. During firmware upgrades, they are typically the last upgraded.

Rebeamform — A process by which a low-performing wireless connection between two AltoPlex devices is replaced with another wireless connection.

Responder — An AltoPlex device that does not initially establish a link with another device, but instead responds a link initiation request from an initiator device. By default, the responder is the radio interface with the higher MAC address. This information may be useful for network design, and in rare cases during troubleshooting after a power outage.

Ring topology — A network topology in which devices are connected in a circular closed loop.

RSSI — Received Signal Strength Indicator. A measurement of how well a device can receive signals from external wireless devices.

SNMP — Simple Network Management Protocol. Used to monitor and report on all the devices in your network.

TDMA — Time Division Multiple Access, used with GPS synchronization for timing in AltoPlex devices.

TX power — Transmission power. Determines how powerful a transmitted signal is.