K4

EdgeFusion

Server

User Guide

Revision History

Date	Version	Remark
15-July-2021	1.0	Created K4 EdgeFusion Server user guide.
29-August-2021	1.1	Added the SIM Orientation for EdgeFusion Server section in Chapter 1 Installing K4 EdgeFusion Server.

Table of Content

List of Figures

List of Tables

About EdgeFusion Server User Guide

The EdgeFusion User Guide provides information on how you can manage the K4 Edge server.

Intended Audience

This guide is helpful for both beginner and experienced system hardware engineers who will be installing, commissioning, and monitoring the K4 Edge server.

How this Guide is Organized

This guide includes the following chapters.

1. Installing K4 EdgeFusion Server. This chapter provides an introduction to the K4 Edge server and its interfaces. In addition to this, the chapter provides steps to install the K4 Edge server on the vessel.
2. Commissioning K4 Edge Server. This chapter provides the steps to commission the K4 Edge server.
3. Monitoring. This chapter provides the steps to monitor the K4 Edge server after the K4 Edge server installation.
4. Debugging. This chapter provides the steps to debug and resolve the issues raised by the clients.

Convention used in this Guide

The following conventions are used throughout the guide.

- *Italic* Figures and tables links are in *italic*.
- **Bold** Buttons and the name of the pages are in **bold**.

K4 Support

If you face a problem while installing or commissioning the K4 Edge Server, then you can connect to the K4 support through the following channels to resolve it.

- ***Mail***. You can send us your problem to ***support@k4mobility.com***
- ***Phone Call***. You can talk about your problem with the K4 support, call ***1-800-964-2084***.

1 Installing K4 EdgeFusion Server

The K4 On-vessel Equipment is logically and physically connected to WAN equipment on one side and connected to the LAN of the yacht or vessel on the other side. For configuration, see *Figure 1-1*

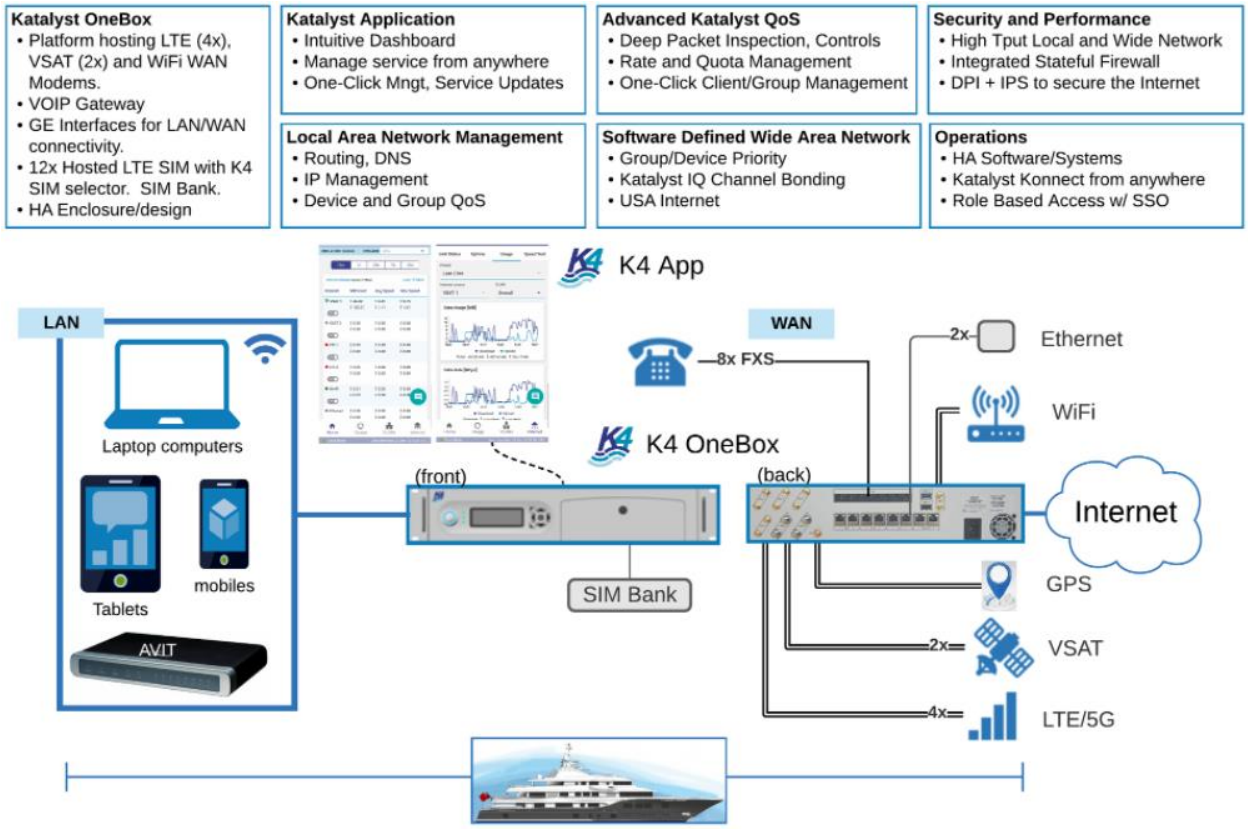


Figure 1-1 Configuration of Equipment

Figure 1-2 shows the network topology of the ship.

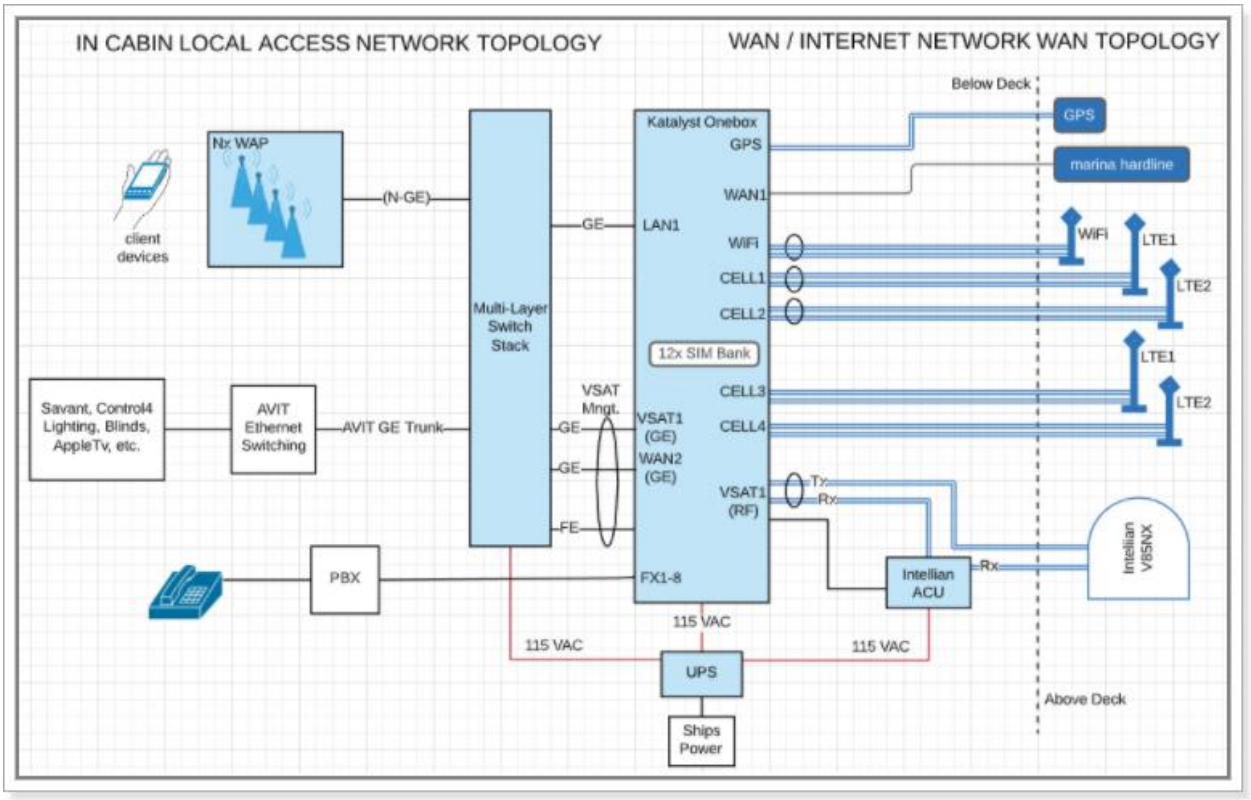


Figure 1-2 Network Topology

For more information on the network topology, see the K4 Edge server user manual or contact K4 Mobility.

1.1 Unboxing K4 EdgeFusion Server

K4 EdgeFusion server is a robust steel body server and shipped to the location with utmost care. The weight of the EdgeFusion server is less than 16 lbs. However, the weight will vary based on the configuration. Following are the dimensions of the server:

H x W x D = 3.5” (2U) x 16” x 18”

Airflow input is available on the right-hand side of the server and top of the server for the efficient inflow of the air in the server. Exhaust is installed on the left-hand side of the server to keep the server cool for efficient performance of the server.

It is highly recommended that the server room temperature be maintained between 10°C (50°F) and 28°C (82°F) as well as humidity less than 90% non-condensing. It is essential to maintain optimal temperature and humidity in the server room. Overheating of the server may damage the server.

1.2 K4 EdgeFusion External Ethernet Port Connections

EdgeFusion server comes with multiple ports physically located front and rear of the server. *Figure 1-3* shows the front view of the server.

Figure 1-3 Front View

Figure 1-4 shows the front connectors of the server.

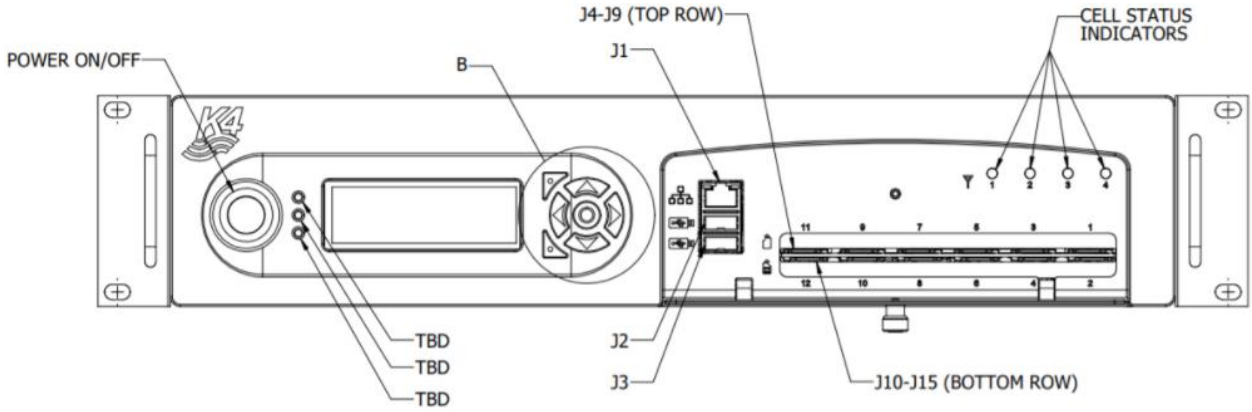


Figure 1-4 Front Connectors

Figure 1-5 shows the rear view of the server.

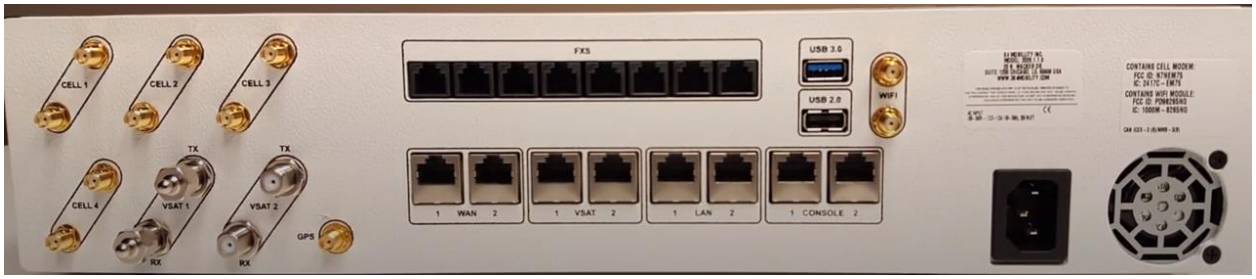


Figure 1-5 Rear View

Figure 1-6 shows the rear connectors of the server.

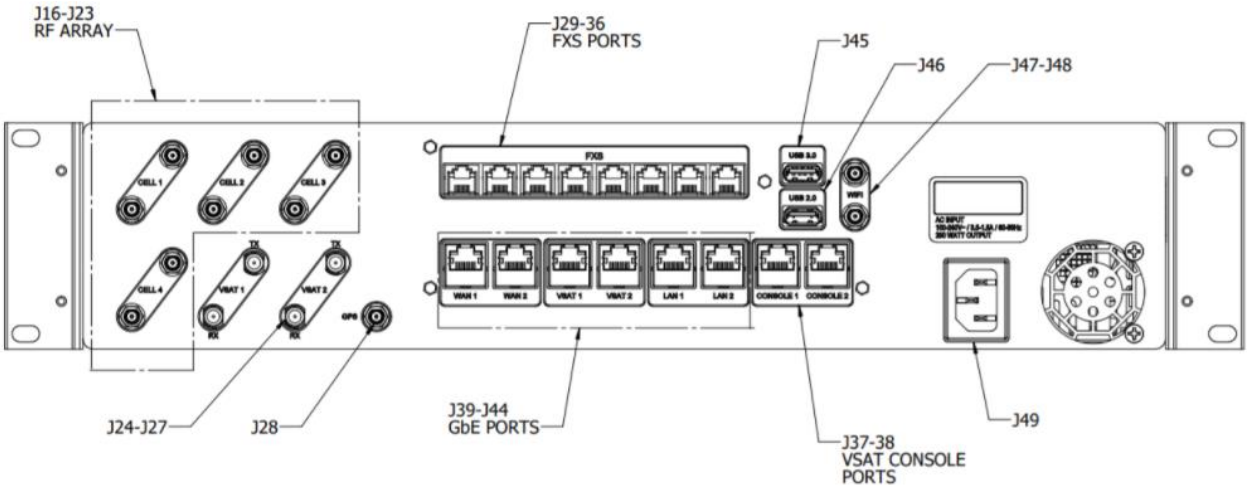


Figure 1-6 Rear Connectors

Table 1-1 describes the Ethernet Interfaces that are available on the K4 server. For a rear view of the server, see *Figure 1-6*.

Table 1-1: Ethernet Interfaces Usage Information

Connector	K4 Edge Application Interface	Usage
Front RJ45 (J1)	Maintenance port	To be used to connect the maintenance laptop to the connection point to EdgeFusion. To be used for server setup to provide DHCP IP to the Laptop.
WAN 1 (J39)	WAN port 1	To be used for WAN Ethernet. This is Ethernet Hardline at the dock.
WAN 2 (J40)	WAN port 2	To be used for WAN Ethernet.
VSAT 1 (J41)	VSAT Management port from the 1st iQ200 / VSAT Modem to the ACU.	To be used to connect VSAT1 Antenna Control Unit (ACU).
VSAT 2 (J42)	VSAT Management port from the 2nd iQ200 / VSAT Modem to the ACU.	To be used to connect VSAT2 ACU.

Connector	K4 Edge Application Interface	Usage
LAN 1 (J43)	LAN port 1	To be used for primary connectivity to LAN.
LAN 2 (J44)	LAN port 2	Secondary LAN - Active/Active Primary - TBD.
USB	USB Interfaces for peripheral connectivity (keyboard, mouse)	To be used for K4 maintenance.

Table 1-2 describes the Ethernet Interfaces that are available on the K4 server. For a rear view of the server, see *Figure 1-6*.

Table 1-2: Radio Interface Usage Information

Connector	K4 Edge Application Interface	Usage
GPS (1x female SubMiniature version A (SMA)	GPS Rx Antenna, power provided via coax and one LTE modem.	To be used to provide details about position.
Wi-Fi (2x female SMA)	802.11 ac/a/b/g/n 2x2 MIMO, 1166 Mbps	To be used to provide marina Wi-Fi access.
LTE 1-4 (2x female SMA per LTE modem)	4x Sierra Wireless CAT12 LTE Modems (EM7565) - 600/150 Mbps per modem.	To be used to access LTE 1, LTE 2, LTE 3 and LTE 4 ports.
VSAT 1-2 (2x female F-Type 75 Ohm per VSAT modem)	2x iQ200 modems.	To be used to access VSAT 1 and VSAT 2 ports.

1.3 SIM Orientation for EdgeFusion Server

It is essential to insert the SIM in the correct orientation in the SIM slot on the EdgeFusion Server. Incorrect SIM insertion orientation will damage the SIM or SIM will not work.

You must insert the SIM with the gold-plated side facing the circuit board infused in the SIM slot. For the gold-plated side of the SIM, see *Figure 1-7*.

Figure 1-7 SIM

The EdgeFusion Server has a SIM bank that includes multiple SIM slots. The SIM orientation will vary based on the odd and even number of the SIM slots.

You must insert the SIM with the gold-plated side facing down in the odd numbered SIM slots, see *Figure 1-8*.

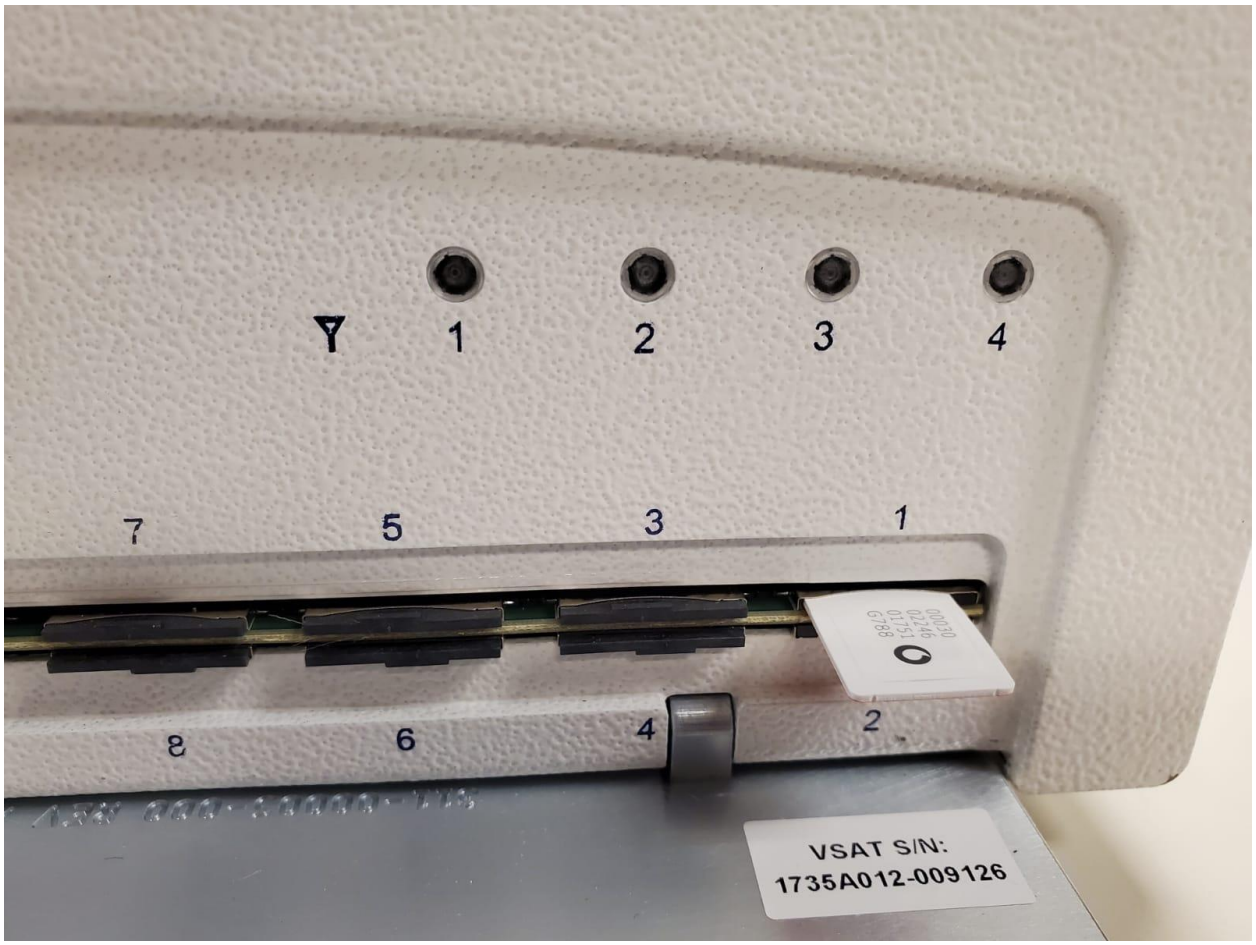


Figure 1-8 Gold-plated Side Face Down Orientation for Odd Numbered SIM Slots

You must insert the SIM with the gold-plated side facing up in the even numbered SIM slots, see *Figure 1-9*.

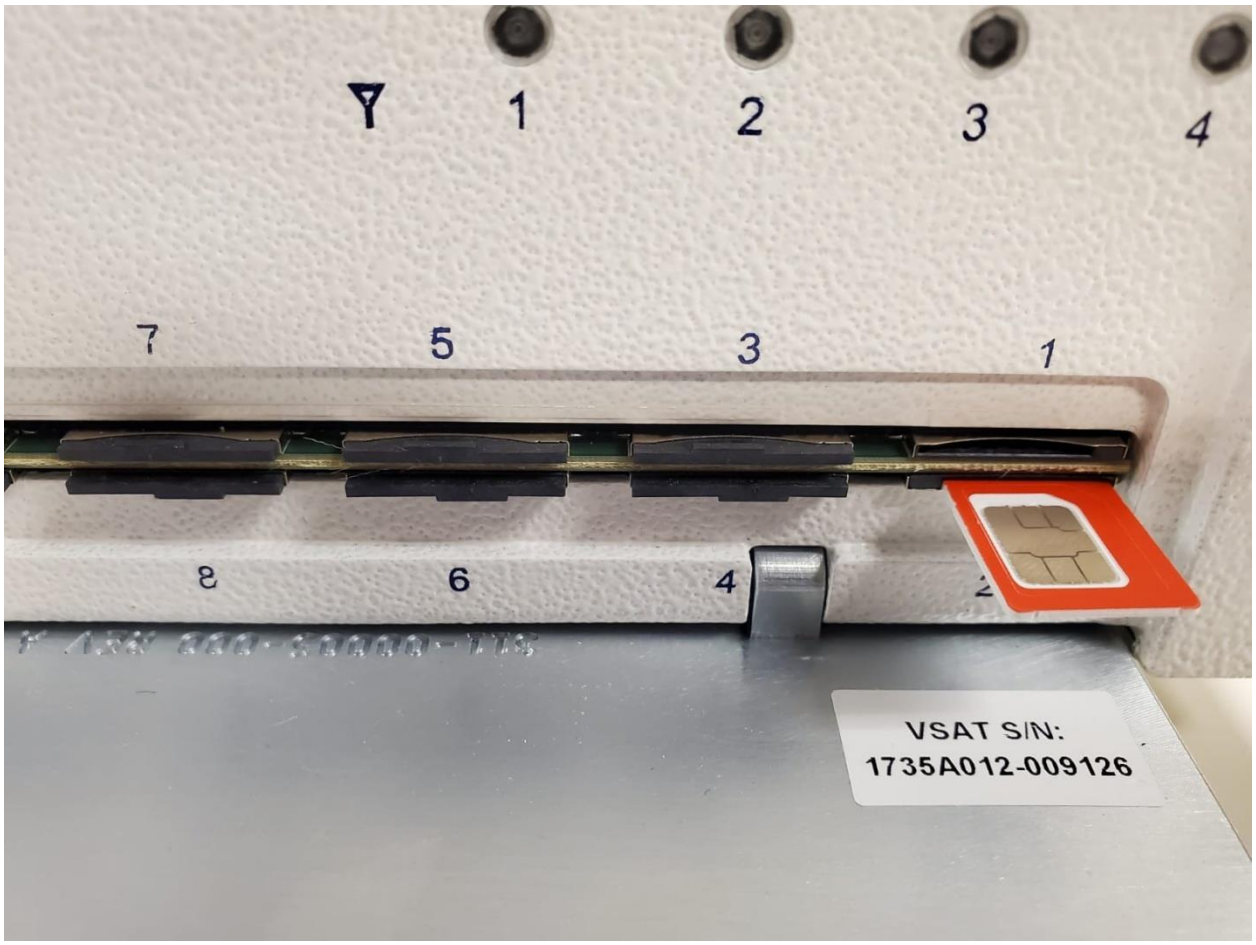


Figure 1-9 Gold-plated Side Face Up Orientation for Even Numbered SIM Slots

1.4 Preinstalled Interfaces on EdgeFusion Sever

The EdgeFusion server comes with the following preinstalled interfaces.

- Very Small Aperture Terminal (VSAT)
- Long-Term Evolution (LTE)
- Wi–Fi

- Ethernet WAN Interface (Marina hardline)
- Ethernet LAN Interface
- Voice over Internet Protocol (VoIP) Adapter

1.4.1 VSAT Interfaces

EdgeFusion will support up to two VSATs i.e., VSAT1 and VSAT2. In addition to this, EdgeFusion will have built-in advance iDirect iQ200 VSAT modems with the following basic capabilities.

- DVB-S2 (up to 45 Mbps) / DVB-S2X (up to 100 Mbps) outbound.
- Supports a full range of DVB-S2X MODCODS up to 256APSK.
- Adaptive TDMA up to 15 Mbps, 16QAM
- Ideal for both fixed and mobility applications.
- Security features with 256-bit AES Link Encryption.
- 10 MHz and 50 MHz references for BUC compatibility.
- Open AMIP compatibility for ease of integration.
- Optimized Layer 2 and Layer 3.

Both the modems are preconfigured. For details, see *Table 1-3*.

Table 1-3: VSAT Modem Configuration

Category		Description
LNB Support		This is for 22 KHz tone for High / Low band.
If Interface, Impedance		Type “F”, Zo=75 Ohms.
Frequency Range	Transmit	950 - 2150 MHz
	Receive	950 - 2150 MHz
Tuning Step Size	Transmit	10 Hz
	Receive	55 KHz
RF Power	Transmit	• Pmax of +0 dBm to Pmin of -35 dBm. • Max composite wide band receive level
	Receive, Maximum	• 5 dBm for symbol rates. 45 Msps. • 10 dB above wanted signal power level for symbol rates > 45 Msps.

<table>
<tr><th colspan="2">Category</th><th colspan="2">Description</th></tr>
<tr><td></td><td>Receive, Minimum</td><td colspan="2">Minimum Receive Level: -115+10*log (Fsym(sps)) single carrier
Receive adjust-ability- AGC Dynamic Range adjustment</td></tr>
<tr><td colspan="2" rowspan="5">Tx SSB Phase Noise</td><td>Frequency</td><td>Phase Noise</td></tr>
<tr><td>1 KHz</td><td>-85 dBc/Hz</td></tr>
<tr><td>10 KHz</td><td>-95 dBc/Hz</td></tr>
<tr><td>100 KHz</td><td>-90 dBc/Hz</td></tr>
<tr><td>1 MHz</td><td>-110 dBc/Hz</td></tr>
<tr><td colspan="2">Receiver Noise Figure</td><td colspan="2">15 dB</td></tr>
<tr><td colspan="2">Transmit Carrier Suppression</td><td colspan="2">≤ -35 dBc</td></tr>
<tr><td colspan="2">Discrete Spurs and Harmonic Content</td><td colspan="2">In-band (900-2150 MHz), with output at -30 dBm: -35 dBc</td></tr>
</table>

1.4.2 LTE Interface

The K4 EdgeFusion contains Sierra Wireless CAT12 EM7565 4G LTE radios/modems. For details about the modems, see Networking Modules | 5G NR, 4G LTE, LTE-A Pro | Sierra Wireless. It has global support and supports the entire LTE band.

Ideally, the LTE antenna should be installed above the deck of the vessel and adhere to a single LTE modem to a single LTE antenna connectivity policy. This will enhance the performance and reliability of the LTE system on EdgeFusion. K4 recommends the following LTE antennas.

- Poynting 402 Multiple Input Multiple Output (MIMO) antenna has diverse 2x2 antenna ports. Therefore, 4x Poynting 402 w/ 2x ports (8x total LMR cable runs) can be installed to optimize LTE performance and redundancy. For details about the OMNI 402 antenna, see OMNI-402 or copy and paste the https://poynting.tech/antennas/omni-402 link in a browser.
- Similar in performance to Poynting 402 antenna, cylindrical and smaller Venteve MIMO LTE antenna 698-2700MHz 2/4dBi LTE Omni Surface Mount Antenna with 2 SMA Connectors can be installed. For details about the antenna, see Mount Antenna or visit Venteve.

- Venteve Single Input Single Output (SISO) LTE antenna model 698-2700MHz 6/7dBi LTE Fiberglass Omni Antenna with 1 N-Style Connector has an edge over other antennas due to its relatively long stick but it is the uniform antenna. For details about the fiberglass antenna, see Fiberglass Antenna.

If EdgeFusion is installed higher up in the vessel with few obstructions (e.g. SunDeck cabinet) then paddle antenna and/or cylindrical and smaller Venteve MIMO LTE antenna can be mounted to the rack to ease installation.

It is highly recommended that before installing the LTE antenna on the vessel you consult with K4 about the LMR cable sizing, lengths, and connectors to be used.

EdgeFusion LTE radios are designed to use one of the SIMs from the SIM Bank of 12 SIMs that are preinstalled on the EdgeFusion. Using the Cellular mobility software of K4 EdgeFusion, SIM/LTE radios can be configured. For this, K4 may require limited technical input or specification from the operator.

NOTE: K4 will provide 12 SIMs either installed in the SIM Bank from the factory, or a SIM BOX will be provided with installation instructions to install 12 SIMS into the K4 EdgeFusion SIM Bank.

1.4.3 GPS Interface

The GPS antenna must be connected to the J28 port. Positioning data is critical to assure reliable LTE, VSAT, and Wi-Fi modem usage by the K4 Edge Service. GPS antenna interface is a female SMA, and the antenna utilized should have an integrated LNA powered via the Coaxial cable connection. The minimal gain from the GPS antenna (w/ LNA) should be 25 dBm. For details, see SPECIFICATION.

1.4.4 Wi-Fi Interface (Marina Wi-Fi)

The EdgeFusion supports a single Wi-Fi client radio. This can be used to provide Marina Wi-Fi access to EdgeFusion. The Wi-Fi radio supports 802.11ac/n/b/g/a, with the radio being 2x2 and can support a maximum data rate of over 1 Gbps. The Wi-Fi modem supports the 2x female SMA connections. It is highly recommended that both ports must be connected and above the deck GPS antenna must be installed for optimal performance.

K4 recommends the following above the deck GPS antenna.

- Single Ventev 3x3 2.4/5Ghz 4/6dBi Wi-Fi Omni Antenna with 3 N-Style Connectors antenna dome. Use the first two ports of the three available ports. Connect SMA female to EdgeFusion and terminate N-type on the antenna. For details, see Wi-Fi Antenna.

- Two Venteve 1x1 2.4/5Ghz Omni-antenna sticks would require two 2.4/5GHz 4/7dBi Wi-Fi Omni Antenna with I N-Style Connector. For details, see Antenna Stick.
- Two Poynting 1x1 2.4/5Ghz OMNI-496 antenna sticks. For details, see OMNI-496.

1.4.5 Ethernet WAN Interface (Marina Hardline)

Ethernet WAN interface can be set up as a DHCP Client (ideal case) or even a static IP configuration. The Ethernet configuration from OneBox is a 1000baseT Copper interface that can negotiate the supported Ethernet rate.

If a 1000baseSX fiber interface is needed, then it is highly recommended to introduce a copper line to fiber Ethernet converter. That model can be considered as it will be transparent to both ends of the link.

K4 recommends procuring the following.

- TP-Link Gigabit SFP Fiber Media Converter - MC220L - Network Adapters. For details, see Network Adapters.
- SFP - TP-Link TL-SM311LM - SFP (mini-GBIC) transceiver module-GigE - TL-SM311LM - Network Adapters. For details, see SFP.

1.4.6 Ethernet LAN Interface (LAN1)

If VLAN on the vessel requires internet access or if the OneBox supports various LAN services such as - DHCP, DNS, and Inter VLAN routing services, then K4 needs detail about the yacht's LAN. However, every VLAN-s in the yacht's LAN would map to one of the following.

- To a group of endpoints connected on Ethernet.
- To a Wi-Fi SSID.

This is an example.

Using an 8-port managed VLAN-aware switch, LAN is installed on a yacht. For a sample, see *Figure 1-10*.

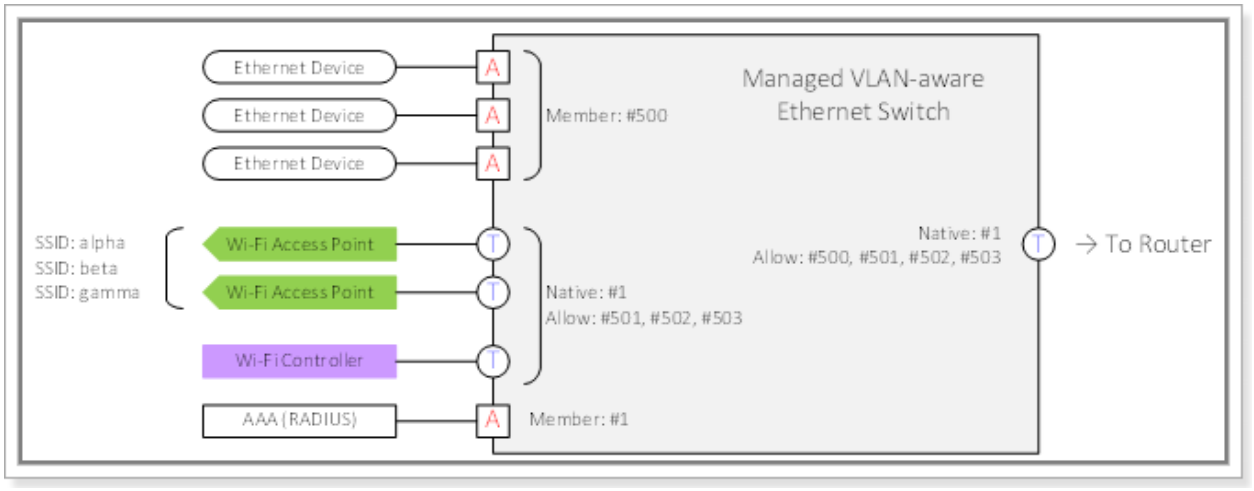


Figure 1-10 Yacht LAN

The reference to the Router in the above picture refers to the K4 Edge Server.

For details, see *Table 1-4*.

Table 1-4: Yacht LAN Information

Ports	Description
A	These are access ports. An access port is a port that sends and receives untagged Ethernet frames. These are considered to belong to that VLAN whose access port is a member.
T	These are trunk ports. A trunk port is a port that sends and receives tagged Ethernet frames for the entire VLAN tags that are marked as allowed. The trunk port can also send and receive untagged frames. These are considered to belong to the VLAN tag marked native to that trunk port.

1.4.7 Voice over Internet Protocol Interface

K4 EdgeFusion supports a single VoIP adapter, Grandstream HT818 [8-port POTS voice gateway FXS RJ-11 ports], see J29 – J36 ports on EdgeFusion server. The VoIP adapter converts POTS on-vessel between OneBox and the PBX to/from a VoIP data stream (SIP and RTP) off vessel over the WAN interfaces available to OneBox.

EdgeFusion can send the VoIP traffic over any WAN / Link based on the configuration of the system.

Every FXS port provisioned and connected to the PBX will have a configured PSTN number associated with it. Therefore, any extension connected to the PBX and mapped to use that FXS port/line will use the associated PSTN on that port for inbound and outbound calls.

Managing PBX will breach the scope of K4. Therefore, PBX must be managed separately and mapping must be done there. Ideally, 2 POTS lines are provisioned on a vessel, and 10-50 extensions are available on a yacht or vessel, see *Figure 1-11*.

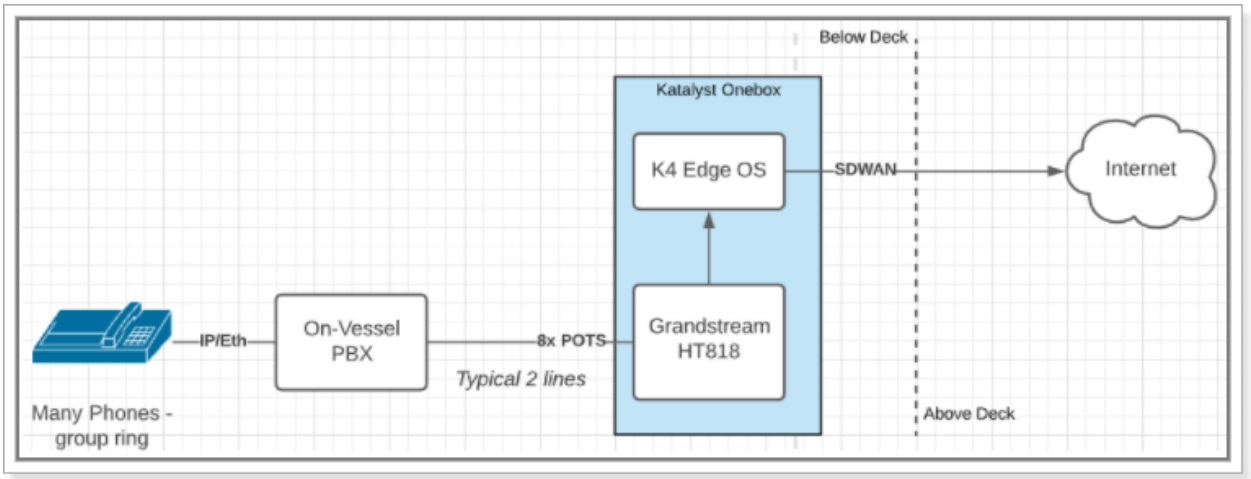


Figure 1-11 Basic OneBox FXS connectivity to the onboard PBX

NOTE: K4 Edge OS supports SDWAN functions; the VoIP data stream can utilize any WAN interface for VoIP services.

1.5 Installing K4 EdgeFusion Server

To install the K4 server, perform the following steps.

1. Mount the EdgeFusion server over the wall or suitable location near the physical antenna using the mounting flanges.
2. Tighten the server with screws.

   NOTE: Mounting flanges and screws are also provided by the server rack.
3. Connect the server to UPS to maintain the uninterrupted power supply to the server while main or input power to the server fails.

   It is highly recommended to use and connect the 5P550R | Eaton 5P UPS | Eaton UPS to the EdgeFusion server. For details about the UPS, see Eaton UPS.
4. Plug in the AC power cord of the server to UPS and connect the other end to the connector J49 located at the rear of the server.

The server has an internal 250W ATX-style power supply with an AC power cord. This consumes 75 watts per hour. *Table 1-5* describes the voltage and rating of the server.

Table 1-5: Voltage and Rating

Voltage	Rating
AC Line Voltage	88 - 264 VAC
AC Line Frequency	47/63 Hz

5. Connect the VSAT1 and VSAT2 to J24 – J27 ports.

   External antenna and ACU must be connected to Radio and Ethernet ports of the EdgeFusion iQ200 VSAT modem, see *Figure 1-12*.

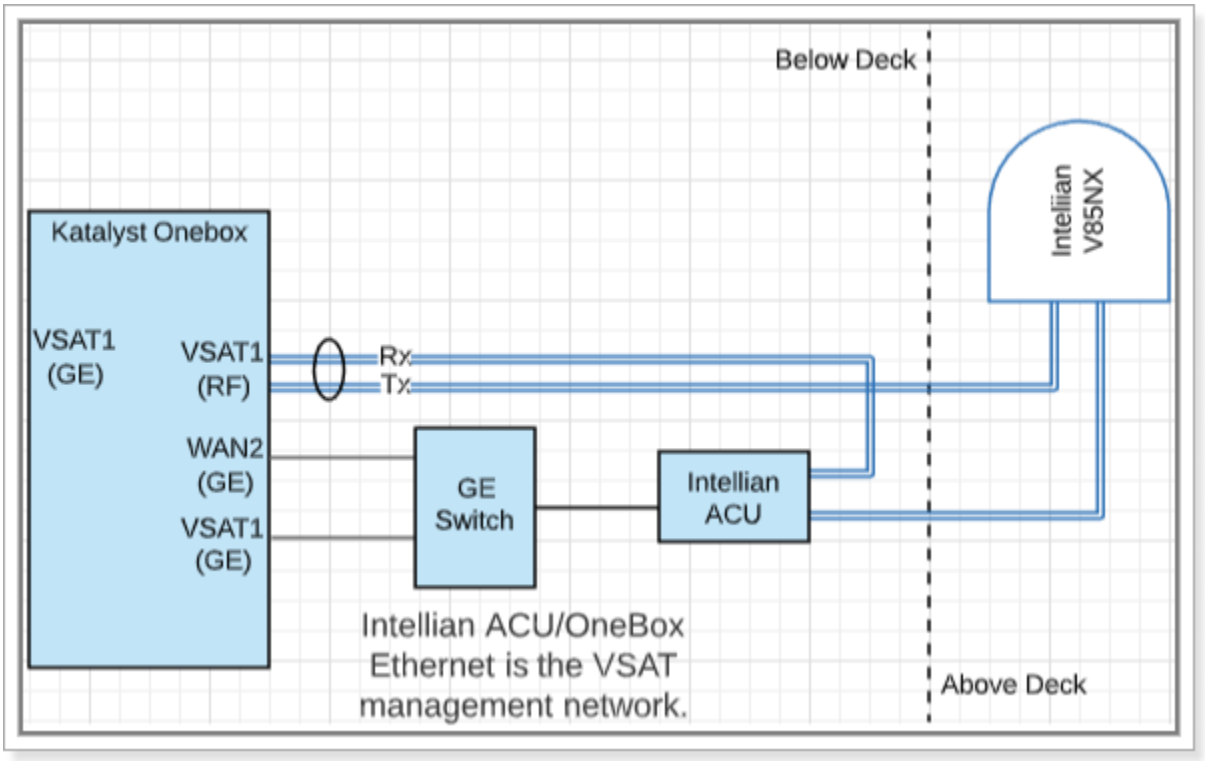


Figure 1-12 Radio and Ethernet connection between VSAT modem and ACU

NOTE: ACU/BDU may vary for every yacht.

K4 EdgeFusion will append source network address translation (NAT) in the entire client/server data for uplink transmission by mapping an IP address to this port before routing the data packet to the network.

6. Connect the LTE antenna/modem to the J16-J23 ports. For connectivity, see *Figure 1-13*. EdgeFusion will utilize only LTE radios/modems attached with LTE antennas.

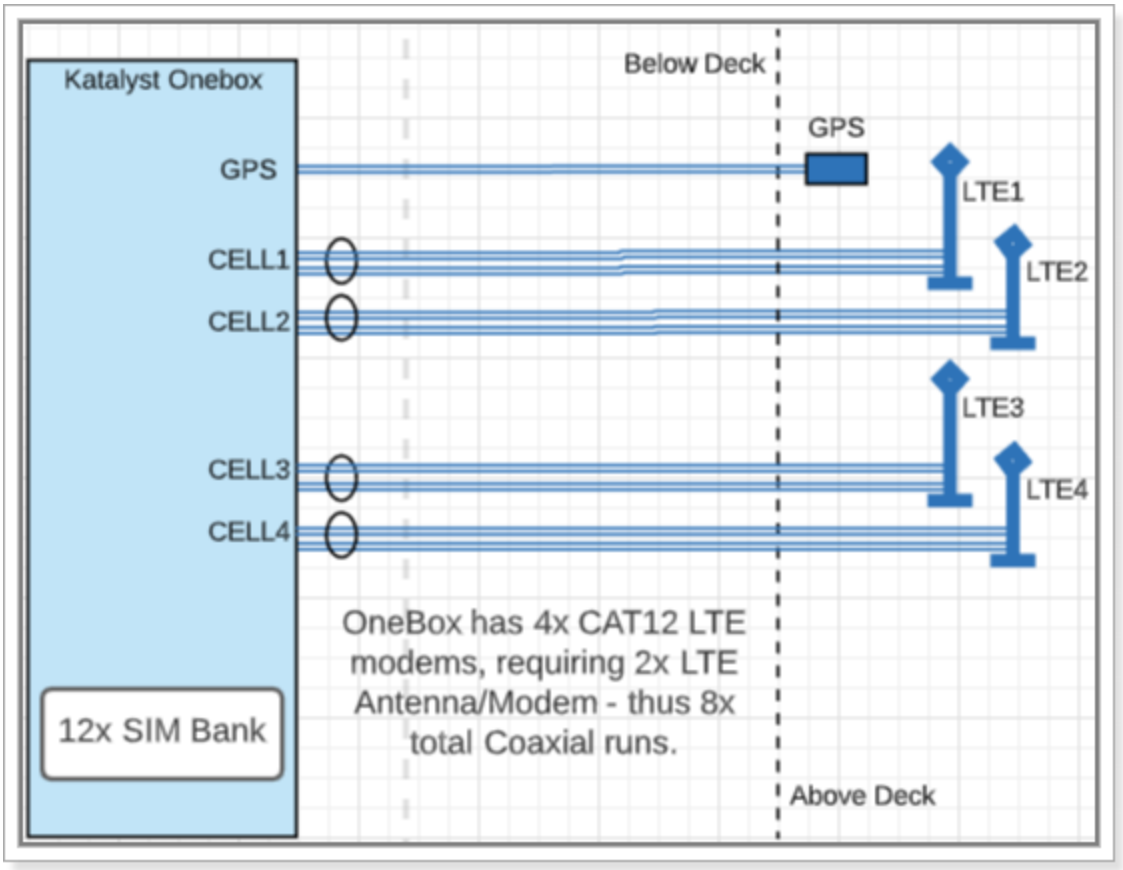


Figure 1-13 EdgeFusionConnectivity with LTE Antenna

K4 EdgeFusion will append source NAT in the entire client/server data for uplink transmission by mapping an IP address to this port before routing the data packet to the network.

7. Install the GPS antenna and then connect the antenna to the J28 port on the EdgeFusion server.

8. Install the above deck Wi-Fi antenna and connect to the J47 and J48 ports.

   If the above deck Wi-Fi antenna cannot be installed, or the EdgeFusion is mounted near the top of the yacht or vessel, then one of the following antennas can be mounted.

   2.4/5GHz 4/6dBi Wi-Fi Omni Antenna with 3 N-Style Connectors to the top of the cabinet. The antenna is 6x7 inches and cylindrical in shape.

   Or,

   Two paddle antennas can be mounted on the back of the EdgeFusion system. It is highly recommended to mount Panorama PWB-24-58 Dual Band 2.4/5.0GHz Wi-Fi Terminal Paddle Antenna and PWB-24-58-RSMARV - Network Antennas. For details, see Paddle Antenna. For connectivity, see *Figure 1-14*.

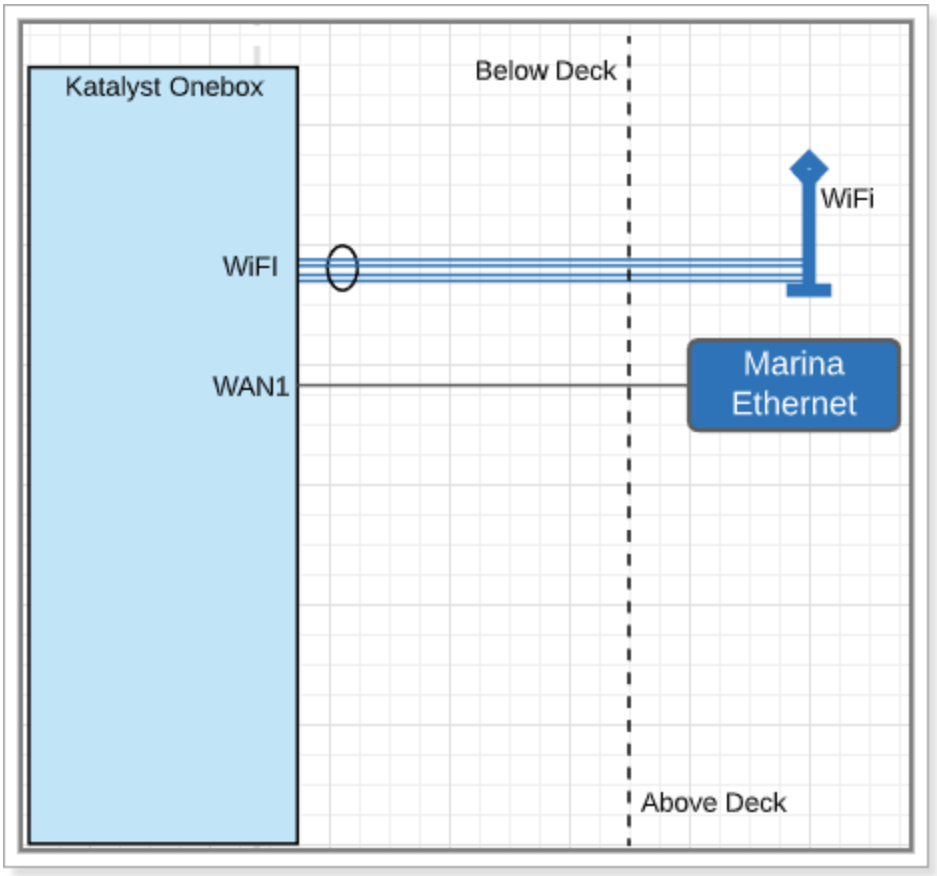


Figure 1-14 Wi-Fi Connectivity

K4 can scan/configure/accept, or pre-configure profiles with priority.

K4 EdgeFusion will append source NAT in the entire client/server data for uplink transmission by mapping an IP address to this port before routing the data packet to the network.

9. Connect the Ethernet WAN Interface to the EdgeFusion server.

   K4 EdgeFusionwill append source NAT in the entire client/server data for uplink transmission by mapping an IP address to this port before routing the data packet to the network.

10. Connect LAN1 to the J43 port on the EdgeFusion server.
11. Connect ship's LAN to a Multilayered Switching Framework (MLS) that is connected to the Wireless Access Points directly or through a WAP POE Switch, and to wired devices.
12. Connect a trunk of MLS to the EdgeFusion server for visibility of LAN network, be it local (layer 2 visibility - observes client MAC addresses) or routed whereby the MLS terminates the L2 and routes client IP to the EdgeFusion server.
13. Connect VoIP adapter to the J29-36 ports.

The K4 EdgeFusion server is installed successfully.

2 Commissioning K4 Edge Server

Using the vessel's LAN, multiple devices connect to the internet on a vessel. Therefore, the vessel will incur huge costs and uncontrolled usage of limited bandwidth. K4 equipment will enable you to define and enforce flexible and granular policies. You can enforce the policy to the following.

- Individual user
- Groups of users
- Groups of devices

Using the K4 Edge Configuration Wizard you can commission the Edge server. You can access the wizard on various browsers such as - Microsoft Edge, Google Chrome, Mozilla Firefox, or Apple Safari.

The steps specified to commission the Edge server in this chapter are limited to version 5.3.6.9 of the K4 Edge Configuration Wizard. Therefore, before commissioning the Edge server you must verify the version of the K4 Edge Configuration Wizard. You must procure the following information from your organization.

- Authentic URL
- User name or login ID
- Login Password

You must perform the unique seven (7) steps to commission the K4 Edge server for the vessel.

2.1 Getting Started

2.1.1 Log On to K4 Edge Configuration Wizard

This section describes how to log on to the K4 Edge Configuration Wizard.

To log on to the K4 Edge Configuration Wizard, perform the following steps.

1. Open a browser.
2. Enter the authentic URL of the K4 Edge Configuration Wizard in the address bar of a browser. The **Login** page appears, see *Figure 2-1*. To enter data in the respective fields, see *Table 2-1*.

Or,

Enter http://10.254.240.1/ in the address bar of a browser. The **Login** page appears, see *Figure 2-1*. To enter data in the respective fields, see *Table 2-1*.

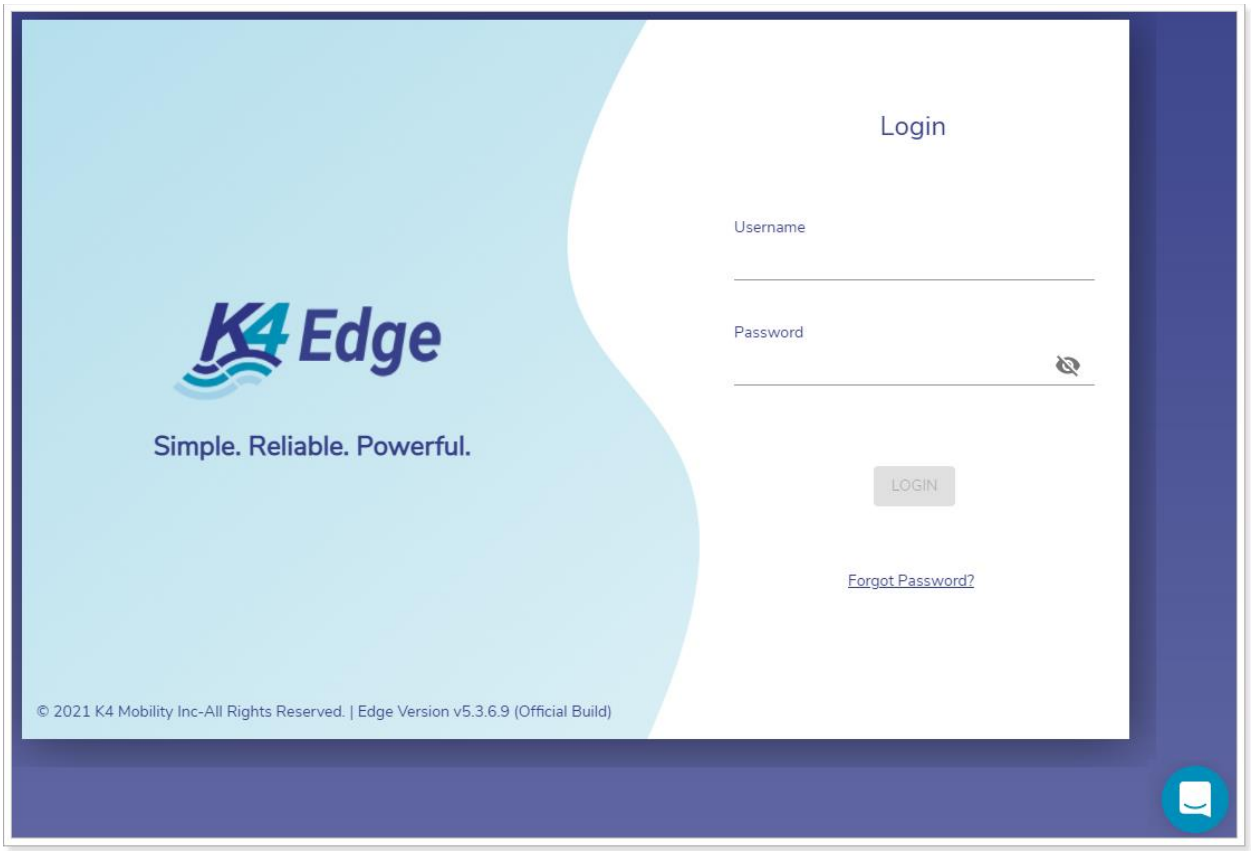


Figure 2-1 Login Page

Table 2-1 Login Information

Fields	Description
Username	Enter your username or login ID.
Password	Enter your login password

The **LOGIN** button becomes available.

3. Click **LOGIN**.

While configuring the K4 Edge server for the first time, it is mandatory to configure the configure security questions. Therefore, the **Security Questions** pop-up window appears, see *Figure 2-2*.

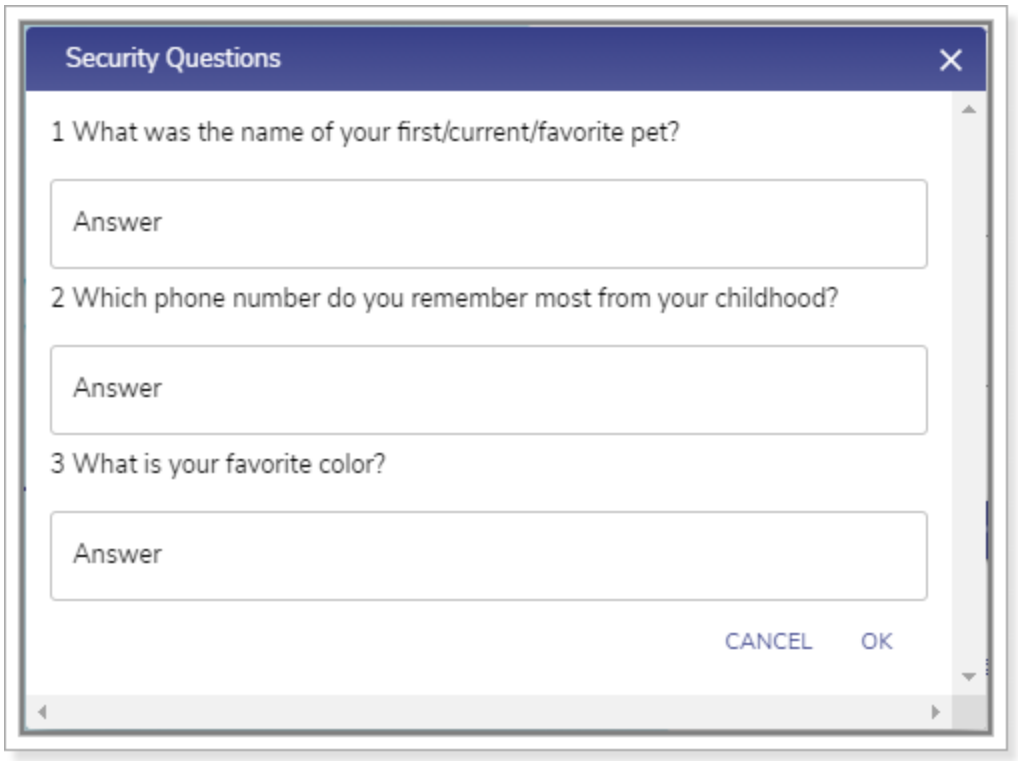


Figure 2-2 Security Questions

It is mandatory to answer the entire security question. Once the security questions are answered, save the answers or note down the answers or remember the answers and then click **OK**.

NOTE: Security questions intend to validate the user. While resetting the login password, you will be asked the security questions. You are required to answer the security questions correctly. You can refer to the answers that you have saved. An incorrect answer may lead to restricting the access of the K4 Edge server.

Figure 2-3 Home Page

The home page is the **first step** page to create the WAN profile.

To understand the home page, see *Figure 2-4*.

Figure 2-4 Classification of Home Page

The home page includes the following sections.

- Vessel Name. The name of your vessel is displayed at the top of a page.
- Notification. This displays the system alerts.
- More. This includes additional options.
- Steps to create the WAN profile.

2.1.2 Logout

To logout from the wizard, click the vertical ellipsis and then click **Logout**, see *Figure 3-3*.

Perform **Step 2: WAN Links**.

2.2 Step 2: WAN Links

Details about the WANs connected to the K4 Edge server become available on the **WAN Links** page.

To view details about the WAN links, perform the following steps.

1. Click on the **Start** page or click **WAN Links**. The **WAN Links** page appears see *Figure 2-5*.

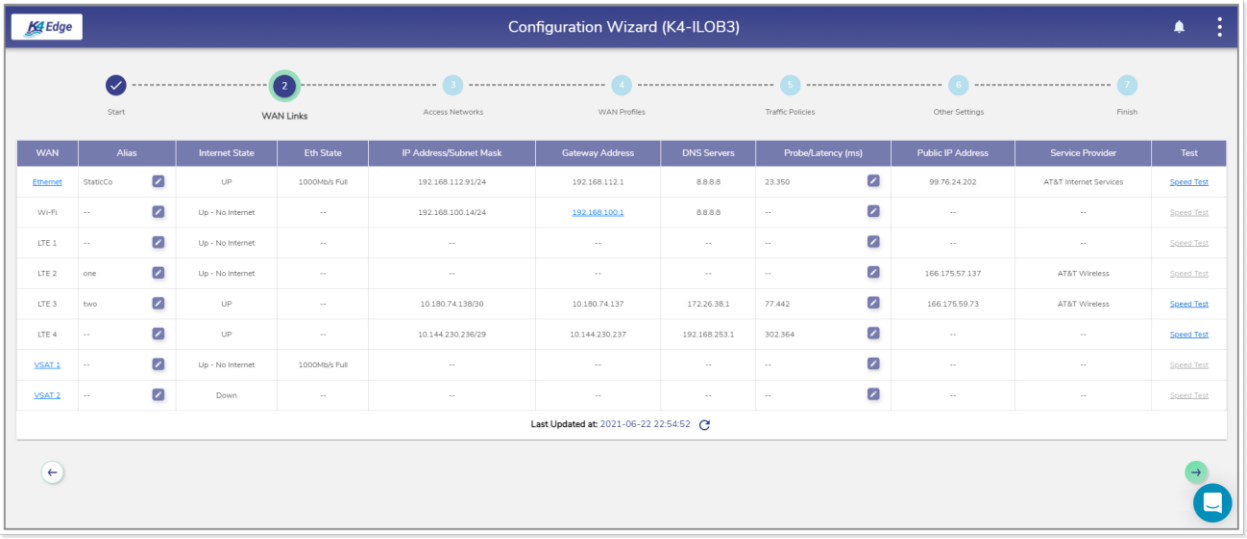


Figure 2-5 WAN Link Page

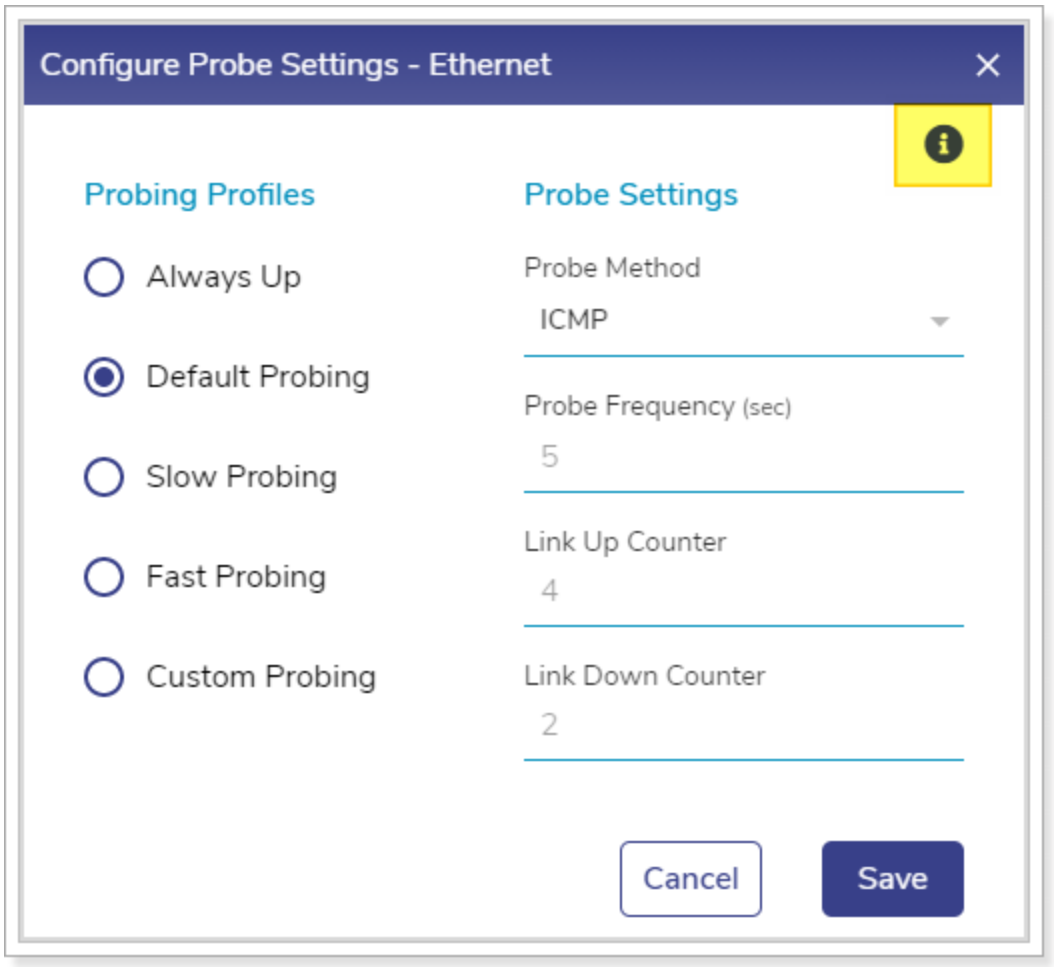


Figure 2-6 Configure Probe Settings

Return

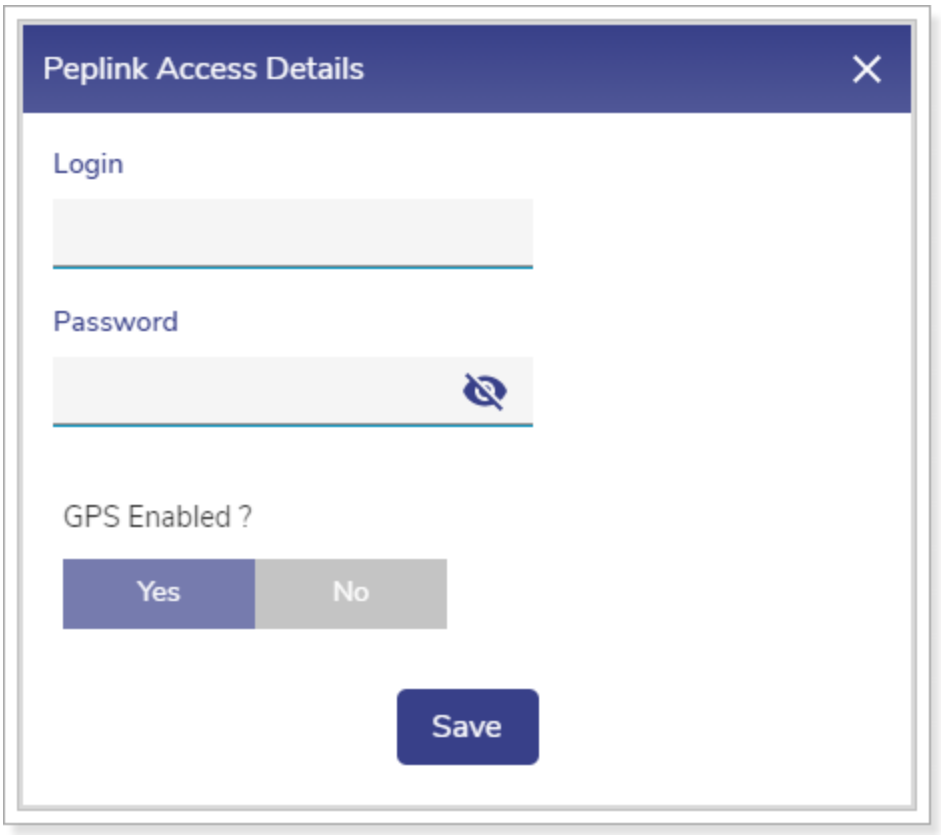


Figure 2-7 Peplink Access Details

Return

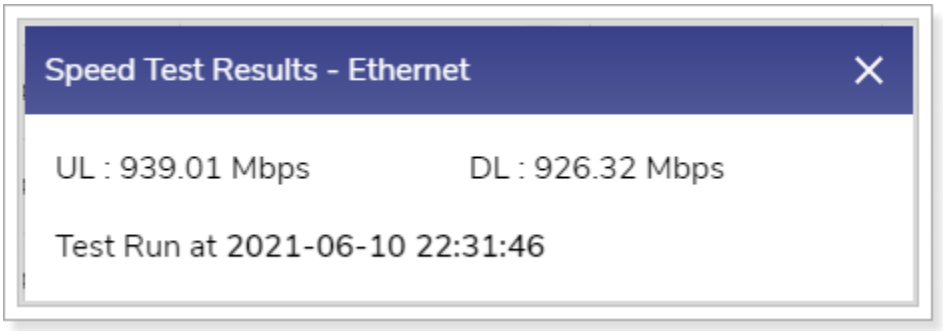


Figure 2-8 Speed Test Result

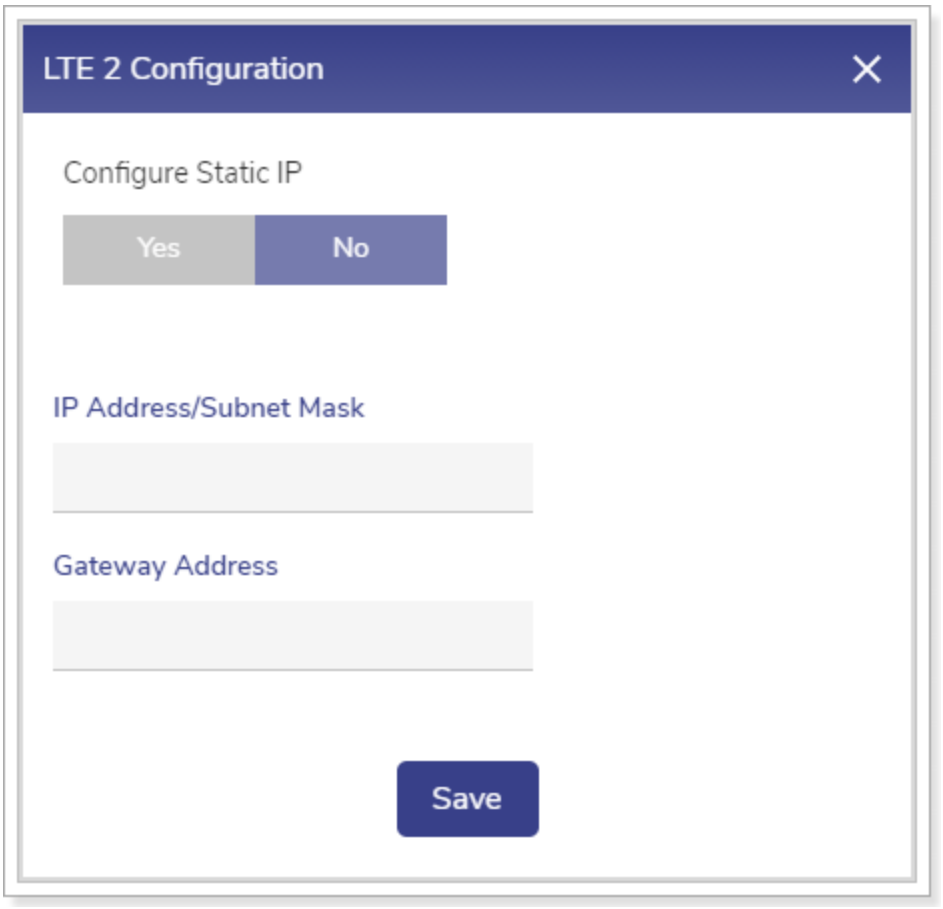


Figure 2-9 Static IP Configuration of LTE

Return

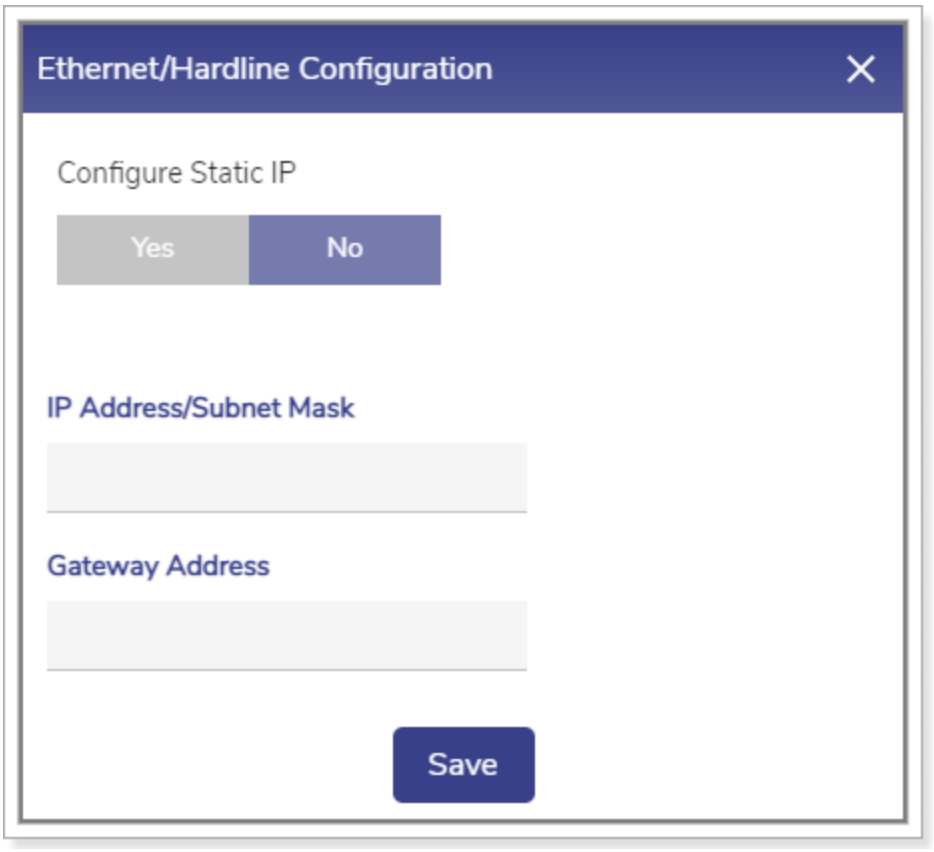


Figure 2-10 Static IP Configuration of Ethernet or Hardline

Return

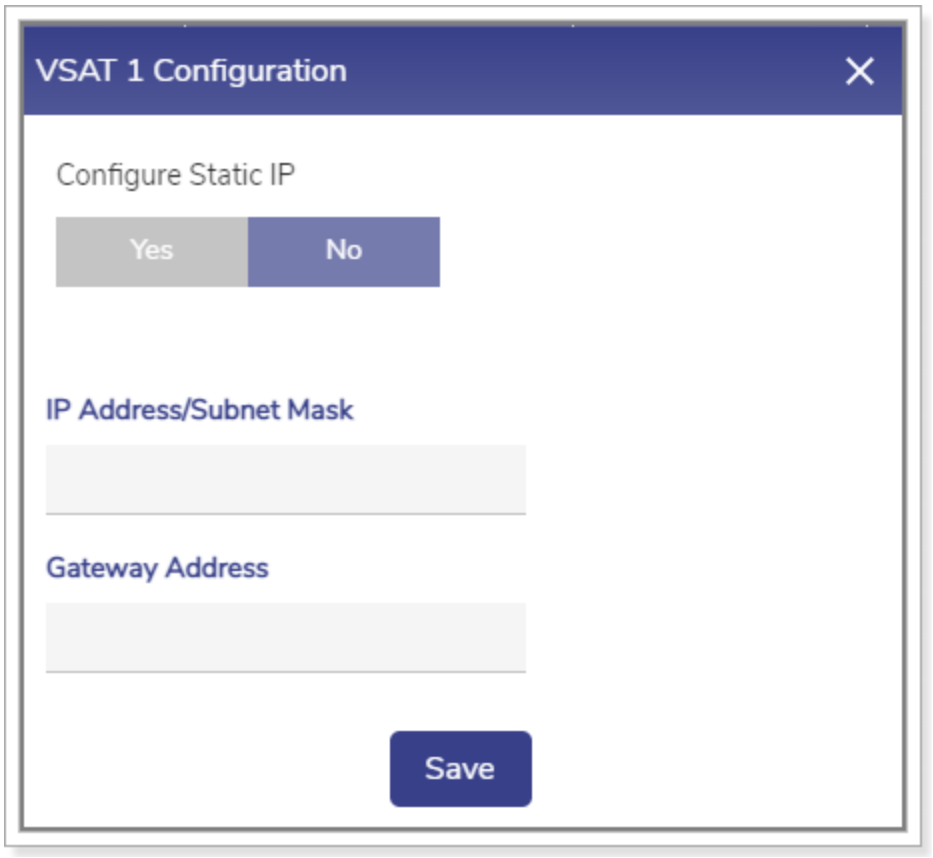


Figure 2-11 Static IP Configuration of VSAT

Return

If the status of the WAN link is **Up**, then the various details such as – WAN link, state of the link, IP address or Subnet Mask populates on the WAN Links page. For details, see *Table 2-2*.

Table 2-2 WAN Links Information

Fields	Description	Configuration
WAN	This indicates the WAN links that are available on the vessel. You can configure the static IP address of a WAN link as the Static IP has advantages and the following are a few advantages. • Easy to manage with DNS. • It would be easier to work	**To configure the static IP of a WAN link, perform the following steps.** 1. Click a WAN Link. The WAN Configuration pop-up window appears. For LTE, see *Figure 2-9*. For Ethernet/Hardline, see *Figure 2-10*. For VSAT, see *Figure 2-11*. 2. Click **Yes** in the **Configure Static IP** field. 3. Enter the IP address and subnet

Fields	Description	Configuration
	remotely through a VPN or other remote services using the WAN link. • It is reliable to access the geo-location based services using the WAN link. • It is reliable for audio and video communications through VoIP using the WAN link.	mask number in the **IP Address/Subnet Mask** field. 4. Enter the gateway address in the **Gateway Address** field. 5. Click **Save**.
Alias	You can give an alias name to the entire WAN link.	**To configure the alias name, perform the following steps.** 1. Click  to the corresponding WAN link. 2. Enter a unique alias name of your choice. 3. Click ✓. Alias name of the WAN is saved. Or, To exit without giving an alias name, click ⊗.
Internet State	This indicates the current status of the WAN link. Following are the statuses of the WAN link. • Up. This indicates that internet connectivity is available on the vessel. • Down. This indicates that internet connectivity is not available on the vessel.	NA
Eth State	This indicates the maximum capacity of the respective Ethernet cable connected to the server.	NA

Fields	Description	Configuration
IP Address/Subnet Mask	This indicates the address of the network, host or device address, and subnet number.	NA
Gateway Address	This indicates that the internet modems and switches on the VLANs can be reached through the gateway address. The hardware is provided by the respective companies or vendors. The K4 boxes connect to the network of the companies or vendors to establish internet connectivity on the vessel.	Click the IP address link. You will be routed to the URL of the company. To procure details and services (data consumed by the WAN link and signal strength etc.) offered by the respective company or vendor, click  peplink. The **Peplink Access Details** pop-up window appears, see *Figure 2-7*. Enter the required details in the respective fields and click **Save**. You will be routed to the URL of the company.
DNS Server	This indicates the initial DNS used by the device to convert the name of the host to an IP address. However, a maximum of three DNSs' can be configured.	NA
Probe/Latency (ms)	Latency indicates the delay between the action and response in milliseconds. **NOTE:** Latency is available for the WAN link whose status is **Up**. You can configure the probe settings for the WAN link.	**To configure the probe settings, perform the following steps.** 1. Click  to the corresponding WAN link. The **Configure Probe Settings** pop-up window appears, see *Figure 2-6*. 2. Click a probing profile in the **Probing Profiles** field. To procure details about the probing profile, point the mouse to  . Details about the probe profiles become available. To disable the probe, select the **Always Up** profile of the profile. Disabling the WAN link probe will

Fields	Description	Configuration
		expose the following threats. • Reduce the probe rate to a few times an hour • The speed test will be disabled • It will also impact the WAN link usage and reliability. Therefore, it is highly recommended that don't disable the probe. However, the WAN link can be disabled for high costs low priority links. 3. Configure the following probe settings in the **Probe Settings** field. • Probing Method. Click one of the following probing methods. • ICMP. This engages lesser bandwidth to do a probe. However, many WAN access networks may block ICMP to evade the potential security threat. • HTTP. • Probe Frequency (sec). Enter the probe frequency at which the probe to be performed. If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down values will become available. To define the probe frequency, you must select the **Custom Probing** profile of the probe and enter the probe frequency within the range of 1 to 3600. • Link Up Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the WAN link is up. If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down

Fields	Description	Configuration
		values will become available. To define the link up counter, you must select the **Custom Probing** profile of the probe and enter the link up counts within the range of 1 to 100. • Link Down Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the WAN link is down. If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down values will become available. To define the probe frequency, you must select the **Custom Probing** profile of the probe and enter the link down counts within the range of 1 to 100. **4.** Click **Save**.
Public IP Address	This indicates the public or global IP address used to access the internet. The public or global IP address is assigned by the internet service provider (ISP).	NA
Service Provider	This indicates the name of ISP.	NA
Test	You can measure the performance of a specific WAN link in real-time.	Click **Speed Test**. The **Speed Test Results** pop-up window appears, see *Figure 2-8*. The speed test result will include the upload and download speed in Mbps and time stamp i.e. date and time when the speed test was performed. The speed test can be performed for the WAN link whose state is Up.

To update the page, click (Refresh).

Perform **Step 3: Access Networks**.

2.3 Step 3: Access Networks

You can configure the following three types of networks supported.

- Connected Networks
- Managed Connected Networks (Traditional VLAN-s)
- Managed Routed Networks

To configure the connected network, perform the following steps.

1. Click on the **WAN Links** page or click **Access Networks**. The **Access Networks** page appears, see *Figure 2-12*.

Figure 2-12 Access Networks

Return

1. Click **Tabular View**. By default, details about the network are available in the Tabular form, see *Figure 2-12*.

   Or,

   Click **Expanded View**. The details about the network are available in the expanded form, see *Figure 2-13*.

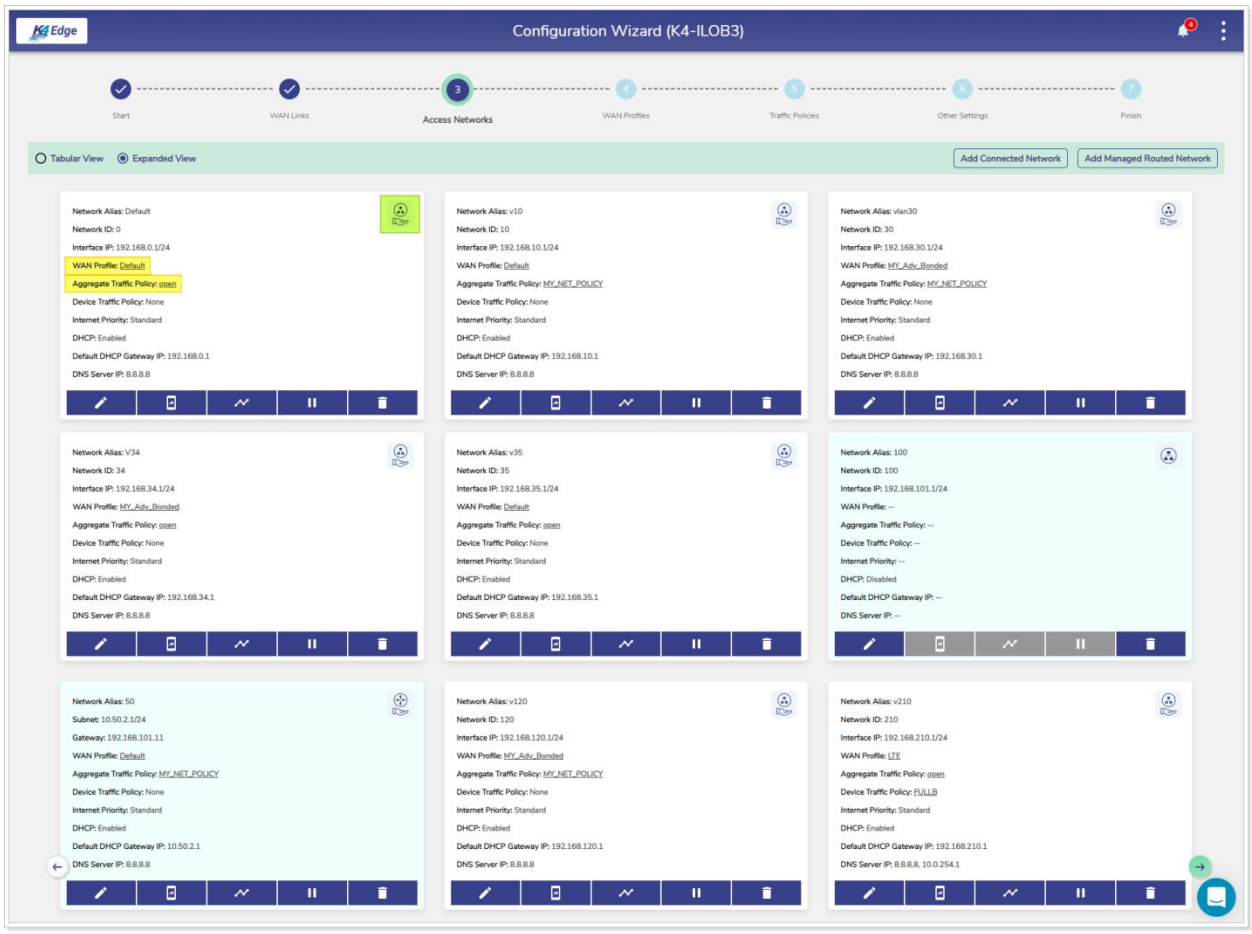


Figure 2-13 Expanded View

The connected networks are displayed with a color background.

To view the network type, point the mouse at the upper right corner of the network, see *Figure 2-13*.

To modify details of the WAN profile of the network, click the WAN profile link, see *Figure 2-13*. The **WAN Profiles** page appears. For details, see *Figure 2-27*.

To modify details of the aggregate traffic policy, click the aggregate traffic policy link, see *Figure 2-13*. The **Traffic Profiles** page appears. For details, see *Figure 2-30*.

2. Click **Add Connected Network**. The **Add Connected Network** page appears, see *Figure 2-14*.

NOTE: This indicates that configuring multiple local networks to be used by the users' basis on the hierarchy. This is an example.

You can configure the local network for the crew of the vessel, a local network for the captain of the vessel, and a local network for the owner of the vessel distinctly.

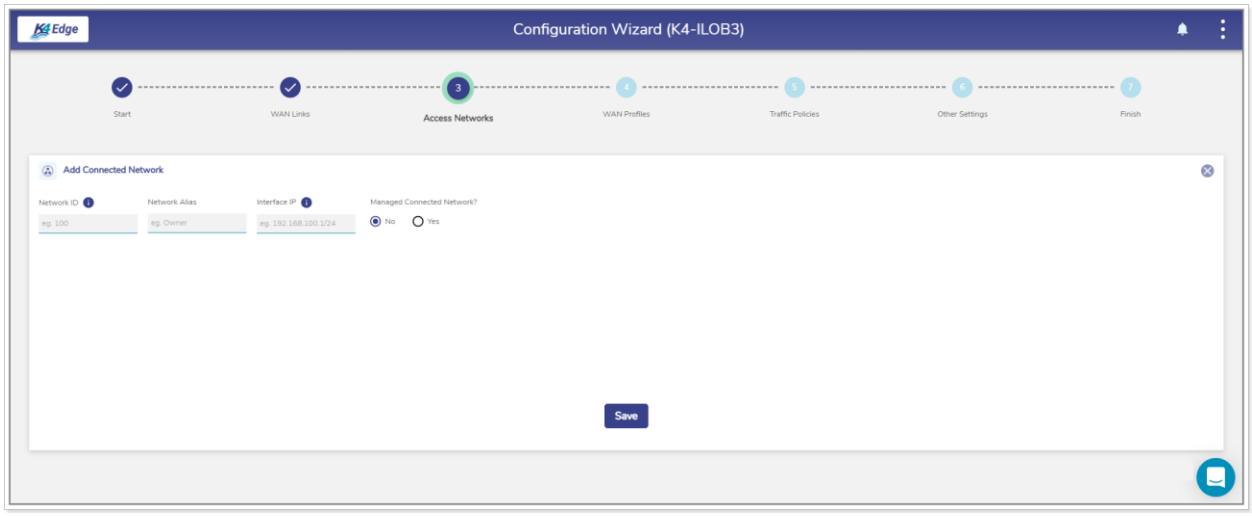


Figure 2-14 Add Connected Network

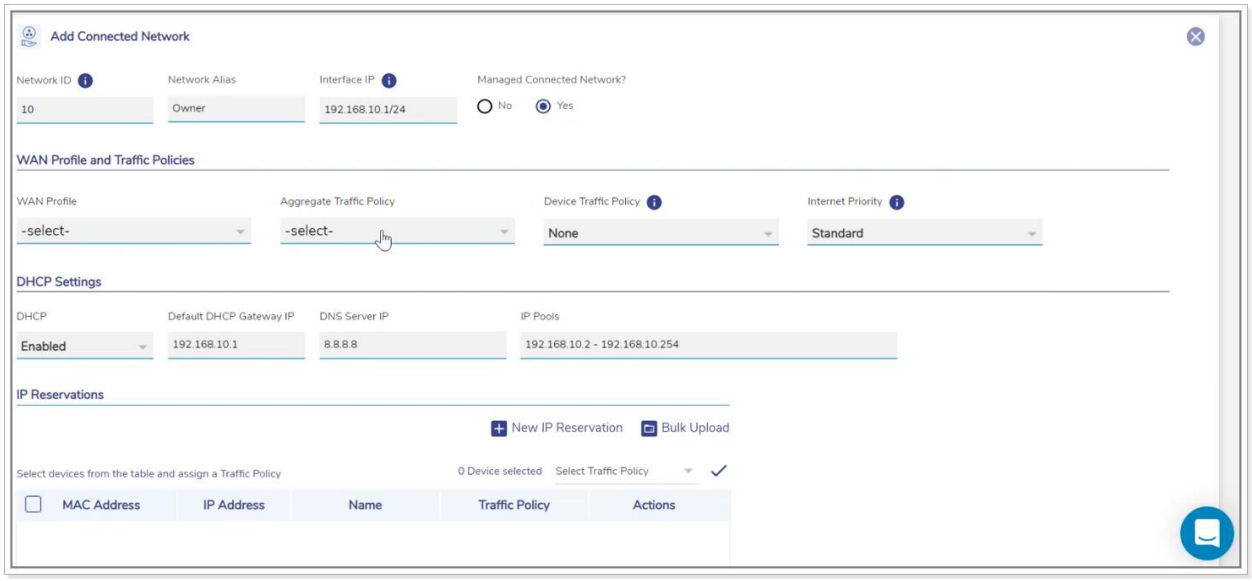


Figure 2-15 Configure Manage Connected Network

Return

Figure 2-16 Bulk Upload IP Reservations

Return

Table 2-3 Connected Network Information

Fields	Description
Network ID	Enter a unique numeric ID from 2 to 4090. For details about the network ID, click ⓘ to the corresponding network ID. **NOTE:** Network ID is known as a VLAN ID. Once the network ID is configured, you cannot modify or update the VLAN ID or network ID in the future.
Network Alias	Enter a unique alias of the network.
Interface IP	Enter an interface IP address and subnet mask.
Managed Connected Network	Click one of the following options. • No. This indicates that by default, you will configure the unmanaged connected network is configured. • Yes. To manage and configure the connected network, click **Yes**. The network configuration section becomes available, see *Figure 2-15*. **NOTE:** The Managed Connected Network is the Traditional VLAN-s.
WAN Profile and Traffic Policies	
WAN Profile	Click a WAN profile. **NOTE:** If you are assigning the WAN profile initially after the K4 server installation, then only the default WAN profile will become available. However, you can configure the distinct WAN profiles. Therefore, the entire WAN profiles will become available. For details about configuring the WAN profiles, see *Step 4: WAN*

Fields	Description
	Profiles on page *60*.
Aggregate Traffic Policy	Click a network traffic policy. **NOTE:** If you are assigning the network traffic policy initially after the K4 server installation, then only the default network traffic policy will become available. However, you can configure the distinct network traffic policies. Therefore, the entire network traffic policies will become available. For details about configuring the network traffic policies, see *Step 5: Traffic Policies* on page *64*. The **Aggregate Traffic Policy** will be applicable to VLAN.
Device Traffic Policy	Click a device traffic policy. **NOTE:** If you are assigning the device traffic policy initially after the K4 server installation, then only the default device traffic policy will become available. However, you can configure the distinct device traffic policies. Therefore, the entire device traffic policies will become available. For details about configuring the device traffic policies, see *Step 5: Traffic Policies* on page *64*. You can assign the traffic policy to a device from also **Step 6: Other Settings**. For details, see *Step 6: Other Settings* on page *72*. However, the traffic policy last assigned to a device from any step will override the traffic policy of that device. Following is an example. Previously, the traffic policy was assigned to a device from **Step 3: Access Networks**. A new traffic policy is assigned to a device from **Step 6: Other Settings**. Therefore, the traffic policy assigned to a device from **Step 6: Other Settings** will override the existing traffic policy of that device.
Internet Priority	Click an internet priority. For details, click  to the corresponding Internet Priority. **NOTE:** Real-time priority works best for only voice/video call applications.
DHCP Settings	
DHCP	To enable DHCP so that a DHCP can automatically assign the IP address and the other allied configuration details to a host on a network to communicate with the endpoints, click **Enable**.

Fields	Description
Default DHCP Gateway IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address.
DNS Server IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address. **NOTE:** You can assign a maximum of three DNS IP addresses.
IP Pools	The default sequential range of the IP addresses becomes available. You can assign a new range of the sequential IP address. For this, click and delete the IP address range and then assign a new sequential range of the IP address. You can assign multiple sequential IP address range excluding the specific IP addresses of that range. This is an example. 192.168.10.2-192.168.10.100, 192.168.10.151-192.168.10.200, 192.168.10.220-192.168.10.254 The following IP addresses will not be assigned to the device in the network. • 192.168.10.101-192.168.10.150 • 192.168.10.2-201.168.10.219 DHCP will assign the IP address to a device in the specified network basis on the IP address range.
IP Reservations	
MAC Address	To reserve an IP address for a device, click **New IP Reservation**, and then enter the MAC address of a device.
IP Address	Enter IP address from the sequential IP address range specified in the IP Pools field.
Name	Enter a name for the device.
Traffic Policy	Click a traffic policy to be assigned to the device. **NOTE:** Inherit indicates that the device will inherit the device policy of the network.
Bulk Upload	**To upload details about the IP reservation, perform the following steps.** 1. Click **Bulk Upload**. The **Bulk upload IP Reservations** pop-up window

Fields	Description
	appears, see *Figure 2-16*. 2. To download the bulk IP reservation template, click Download Reservations. 3. Fill in the required details in the file, and then save the file. 4. Click **Upload Reservations**, browse the file, and then upload the IP reservation file.

3. Click **Save**.
4. Click **Add Managed Routed Network**. The **Add Managed Routed Network** page appears, see Figure 2-17. To enter data in the respective fields, see *Table 2-4*.

NOTE: Managed Routed Networks linked to the Unmanaged Connected Network are available in a group with a color background.

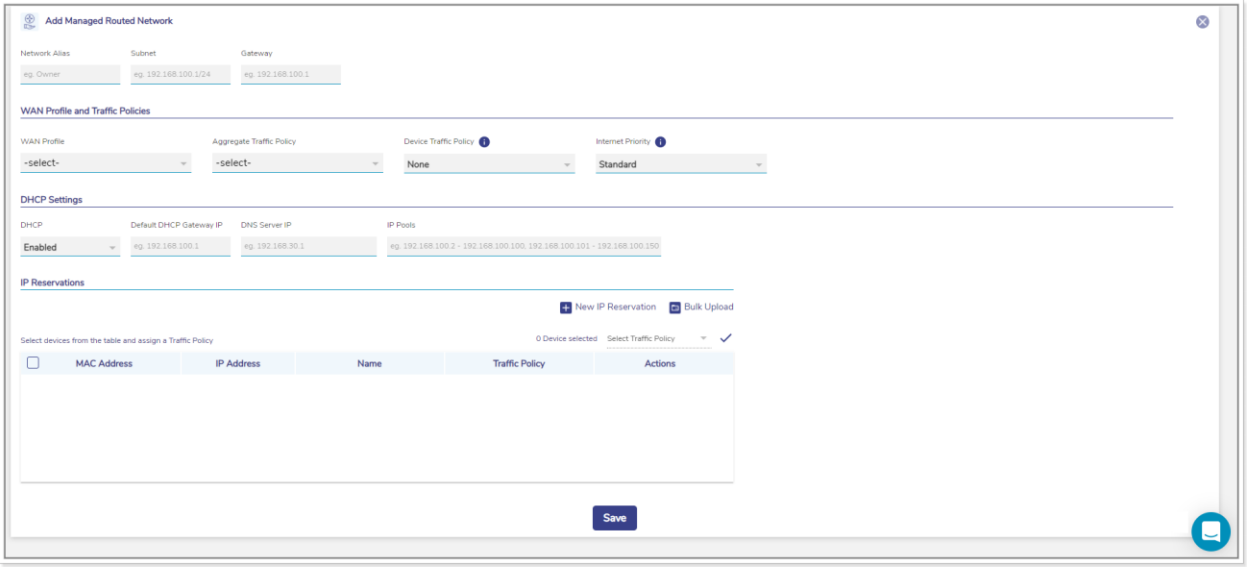


Figure 2-17 Add Managed Routed Network

Table 2-4 Managed Routed Network Information

Ports	Description
Network Alias	Enter a unique alias of the network.
Subnet	Enter the subnet basis on the interface IP address and mask that was configured while configuring the connected network.
Gateway	Enter the IP address of the device managing the communication with the external network.

Ports	Description
	NOTE: You must assign the IP address basis on the interface IP address that was configured while configuring the connected network.
WAN Profile and Traffic Policies	
WAN Profile	Click a WAN profile. **NOTE:** If you are assigning the WAN profile initially after the K4 server installation, then only the default WAN profile will become available. However, you can configure the distinct WAN profiles. Therefore, the entire WAN profiles will become available. For details about configuring the WAN profiles, see *Step 4: WAN Profiles* on page *60*.
Aggregate Traffic Policy	Click a network traffic policy. **NOTE:** If you are assigning the network traffic policy initially after the K4 server installation, then only the default network traffic policy will become available. However, you can configure the distinct network traffic policies. Therefore, the entire network traffic policies will become available. For details about configuring the network traffic policies, see *Step 5: Traffic Policies* on page *64*.
Device Traffic Policy	Click a device traffic policy. **NOTE:** If you are assigning the device traffic policy initially after the K4 server installation, then only the default device traffic policy will become available. However, you can configure the distinct device traffic policies. Therefore, the entire device traffic policies will become available. For details about configuring the network traffic policies, see *Step 5: Traffic Policies* on page *64*.
Internet Priority	Click an internet priority. For details, click  to the corresponding Internet Priority. **NOTE:** Real-time priority works best for only voice/video call applications.
DHCP Settings	

Ports	Description
DHCP	To enable DHCP so that a DHCP can automatically assign the IP address and the other allied configuration details to a host on a network to communicate with the endpoints, click **Enable**.
Default DHCP Gateway IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address.
DNS Server IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address. **NOTE:** You can assign a maximum of three DNS IP addresses.
IP Pools	The default sequential range of the IP addresses becomes available. You can assign a new range of the sequential IP address. For this, click and delete the IP address range and then assign a new sequential range of the IP address. You can assign multiple sequential IP address range excluding the specific IP addresses of that range. This is an example. 192.168.10.2-192.168.10.100, 192.168.10.151-192.168.10.200, 192.168.10.220-192.168.10.254 The following IP addresses will not be assigned to the device in the network. • 192.168.10.101-192.168.10.150 • 192.168.10.2-201.168.10.219 DHCP will assign the IP address to a device on the specified network basis on the IP address range.
IP Reservations	
MAC Address	To reserve an IP address for a device, click **New IP Reservation**, and then enter the MAC address of a device.
IP Address	Enter IP address from the sequential IP address range specified in the IP Pools field.
Name	Enter a name for the device.
Traffic Policy	Click a traffic policy to be assigned to the device. **NOTE:** Inherit indicates that the device will inherit the device policy

Ports	Description
	of the network.
Bulk Upload	**To upload details about the IP reservation, perform the following steps.** 1. Click **Bulk Upload**. The **Bulk upload IP Reservations** pop-up window appears, see *Figure 2-16*. 2. To download the bulk IP reservation template, click Download Reservations. 3. Fill in the required details in the file, and then save the file. 4. Click **Upload Reservations**, browse the file, and then upload the IP reservation file.

To configure the WAN profile through the **Access Networks** page, click the WAN profile link. The **WAN Profiles** page appears. For details, see *Step 4: WAN Profiles* on page *60*.

To configure the aggregate traffic policy and device traffic policy through the **Access Networks** page, click the aggregate traffic policy or device traffic policy link. The **Traffic Profiles** page appears. For details, see *Step 5: Traffic Policies* on page *64*.

2.3.1 Modifying Network

To modify details about the network, perform the following steps.

1. Click  to the corresponding network under the **Action** section on the **Access Networks** page. The **Updated Connected Network** page appears, see *Figure 2-18*. To enter data in the respective fields, see *Table 2-3*.

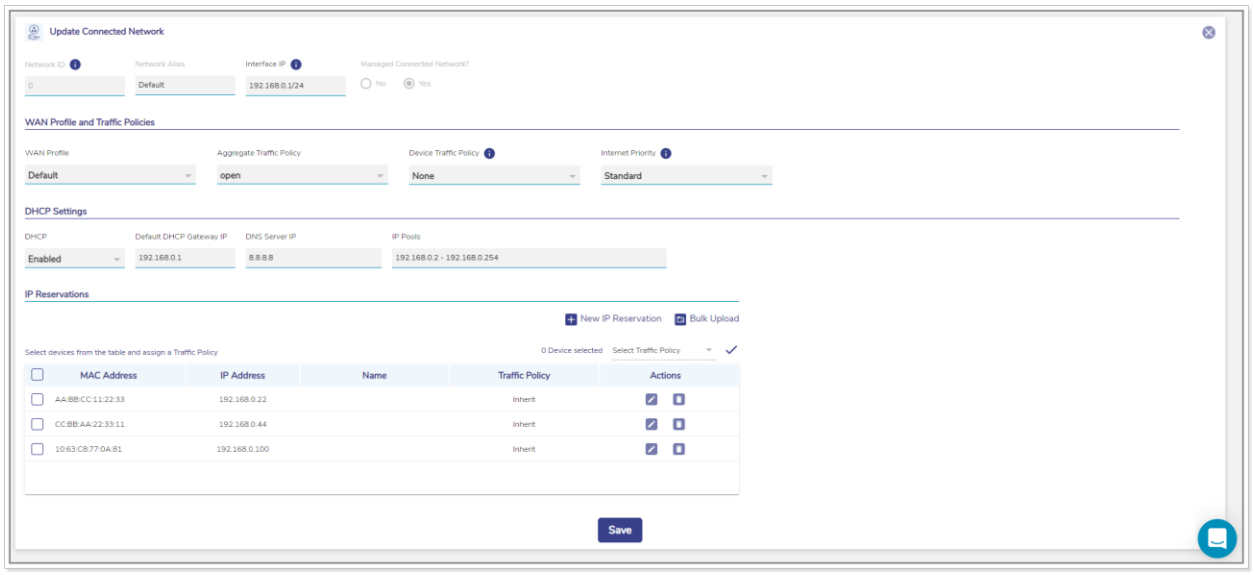


Figure 2-18 Update Connected Network

2. Click **Save**.

2.3.2 Modifying Device Profile

To modify the device profile, perform the following steps.

1. Click  to the corresponding network under the **Action** section on the **Access Networks** page. The **Device Profile** page appears, see *Figure 2-19*. To enter data in the respective fields, see *Table 2-3*.

Figure 2-19 Update Device Profile

2. Click **Save**.

You can add a new device profile. For this, click **Device Profile**. To enter data in the respective fields, see *Table 2-3*.

You cannot modify the device profiles of the connected network.

2.3.3 Viewing Network Usage Data

To view network usage data, perform the following steps.

1. Click  to the corresponding network under the **Action** section on the **Access Networks** page. The **Network Usage** page appears, see *Figure 2-20*. For details about the fields, see *Table 2-5*.

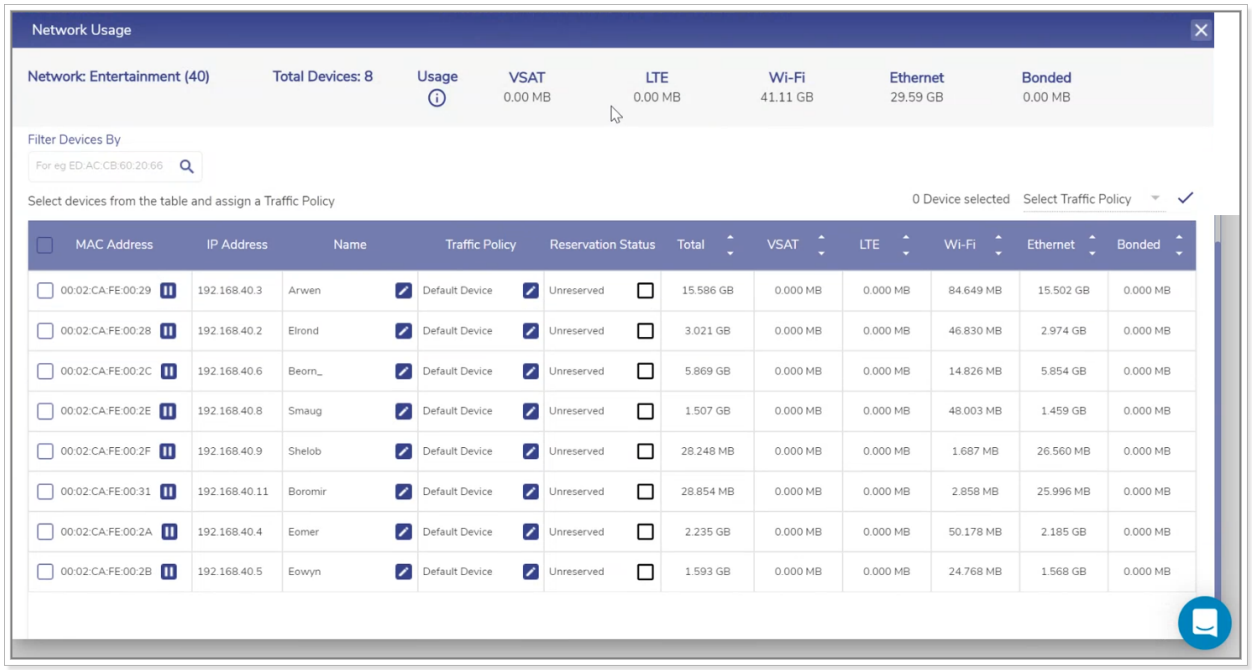


Figure 2-20 Network Usage

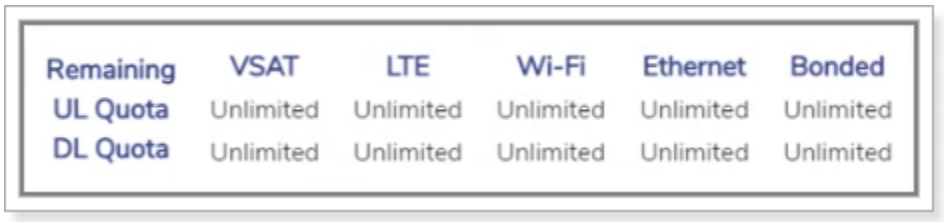


Figure 2-21 Quota Details

Return

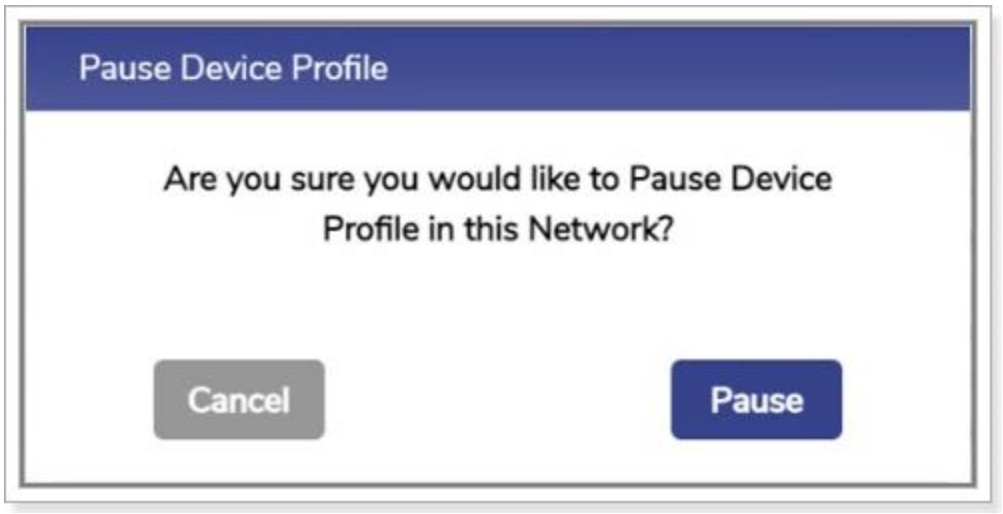


Figure 2-22 Pause Device Profile Confirmation Message

Return

Figure 2-23 Resume Device Profile Confirmation Message

Return

Table 2-5: Network Usage Information

Fields	Description
Network	This indicates the name of the network
Total Devices	This indicates the count of the devices connected to the network.
Usage	This indicates details about the quota of the network. To view the quota details, click ⓘ. Details about the quota are displayed, see *Figure 2-21*.

Fields	Description
VSAT	This indicates the total data consumed by the VSAT.
LTE	This indicates the total data consumed by the LTE.
Wi-Fi	This indicates the total data consumed by the Wi-Fi.
Ethernet	This indicates the total data consumed by the ETHERNET.
Bonded	This indicates the total data consumed by the Bonded.
Filter Devices By	Enter the MAC address of the specific device. Details about the device become available.
MAC Address	This indicates the MAC address of the device connected to the network. 1. To pause the device, click . The **Pause Device Profile** confirmation message pop-up window appears, see *Figure 2-22*. 2. Click **Pause**. The (resume button) becomes available and the row of the device is highlighted by a color. Or, 1. To resume the device, click . The **Resume Device Profile** confirmation message pop-up window appears, see *Figure 2-23*. 2. Click **Resume**.
IP Address	This indicates the IP address assigned to the device.
Name	This indicates the alias name of the device. To modify the alias name, click and modify the alias name.
Traffic Policy	This indicates the traffic policy assigned to the device. To modify the traffic policy, click and modify the traffic policy. For details, see *Step 5: Traffic Policies* on page *64*. **To assign the traffic policy to multiple devices, perform the following steps.** 1. Select the check box to the corresponding device. The count of the devices selected is displayed in the **Devices Selected** field. 2. Click **Select Traffic Policy**. 3. Click the traffic policy to be assigned the devices selected. Or,

Fields	Description
	To assign the traffic policy to the devices in bulk, perform the following steps 1. Select the check box to the corresponding **MAC Address** field. The count of the devices selected is displayed in the **Devices Selected** field. 2. Click **Select Traffic Policy**. 3. Click the traffic policy to be assigned the devices selected.
Reserved Status	This indicates that whether the IP address assigned to the device is reserved. To reserve the IP address of the device, click the corresponding check box. Or, To un-reserve the IP address of the device, clear the check box.
Total	This indicates the sum of the data consumed by the device on the following WAN links. • VSAT • LTE • Wi-Fi • Ethernet • Bonded
VSAT	This indicates the quantum of the data consumed by the device on the VSAT. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, Ethernet, and Bonded links is displayed in the **Total** field.
LTE	This indicates the quantum of the data consumed by the device on the LTE. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, Ethernet, and Bonded links is displayed in the **Total** field.
Wi-Fi	This indicates the quantum of the data consumed by the device on the Wi-Fi. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, Ethernet, and Bonded links is displayed in the **Total** field.

Fields	Description
Ethernet	This indicates the quantum of the data consumed by the device on the Ethernet. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, Ethernet, and Bonded links is displayed in the **Total** field.
Bonded	This indicates the quantum of the data consumed by the device on the Bonded. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, Ethernet, and Bonded links is displayed in the **Total** field.

2.3.4 Pausing or Resuming Network Traffic

To pause the network traffic, perform the following steps.

1. Click ⏸ to the corresponding network under the **Action** section on the **Access Networks** page. The **Pause Network Traffic** confirmation message pop-up window appears, see *Figure 2-24*.

Figure 2-24 Pause Network Traffic Confirmation Message

2. Click **Pause**. The Resume Network Traffic ▶ button becomes available and the row of the network is highlighted by a color.

You cannot pause the network traffic of the connected network.

To resume the network traffic, perform the following steps.

1. Click to the corresponding network under the **Action** section on the **Access Networks** page. The **Resume Network Traffic** confirmation message pop-up window appears, see *Figure 2-25*.

Figure 2-25 Resume Network Traffic Confirmation Message

2. Click **Resume**.

The network traffic on the network resumes.

2.3.5 Deleting Network

To delete the network, perform the following steps.

1. Click to the corresponding network under the **Action** section on the **Access Networks** page. The **Delete Network** confirmation message pop-up window appears, see *Figure 2-26*.

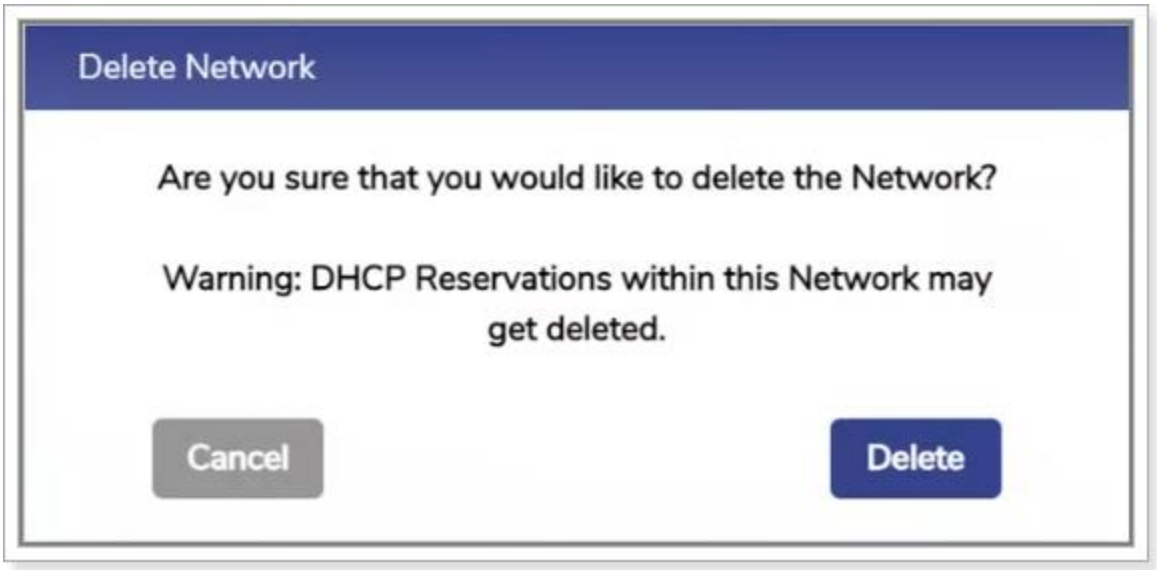


Figure 2-26 Delete Network Confirmation Message

2. Click **Delete**.

The network is successfully deleted. It will impact the DCP reservations. Therefore, it is highly recommended to verify the network details before deleting the network.

Perform **Step 4: WAN Profiles**.

2.4 Step 4: WAN Profiles

While the K4 server is installed on the vessel, by default, the priority of the enabled WANs is configured in the WAN Profile and assign to the VLANs. However, you create multiple WAN profiles of your choice.

To create a WAN profile, perform the following steps.

1. Click on the **Access Networks** page or click **WAN Profiles**. The **WAN Profiles** page appears, see *Figure 2-27*.

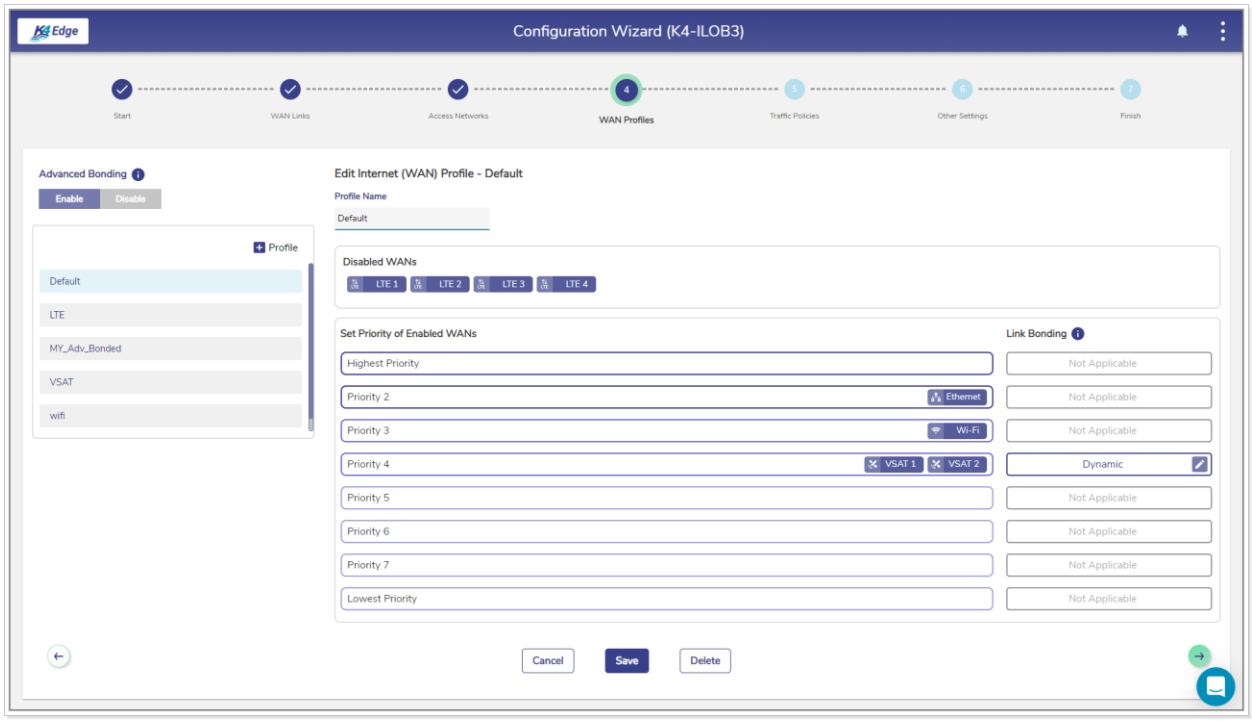


Figure 2-27 Create WAN Profile

You can create multiple WAN profiles and then associate the WAN profile to VLAN.

2. Click **+ Profile**. The **Profile Name** field becomes available under the **Edit Internet (WAN) Profil**e section. To enter data in the respective fields, see *Table 2-6*.

Table 2-6: Profile Information

Fields	Description
Profile Name	Enter a name of the profile.
Disabled WANs	Disabled WAN sources are displayed.
Set Priority of Enabled WANs	
Highest Priority	**To assign the like WAN links to a priority level, perform the following steps.** Drag and drop the like WAN links available under the **Disabled WANs** section. By default, only the like WAN bonding can be assigned to the priority levels. You can assign also the unlike WANs to the priority levels, by enabling the **Advanced Bonding**. However, **Advanced Bonding** is a licensed feature of the K4 Mobility and is available with only US Internet features. Therefore, you must ensure that the license of the Advanced Bonding is available for your vessel.

Fields	Description
	To assign the unlike WAN to the priority levels, perform the following steps 1. Click **Enable** under the **Advanced Bonding** link section. For details about the advanced bonding link, point the mouse to to the corresponding **Advanced Bonding**. By default the advanced bonding link is disabled. 2. Drag and drop the unlike WAN link available under the **Disabled WANs** section. **NOTE:** You can configure only single Advanced Bonding in a profile. By default, the link bonding **Dynamic** with pre-configured weighting % is configured for both like and unlike WAN links. For details about the types of link bonding, point the mouse to to the corresponding **Link Bonding**. You can configure the weighting % of the WAN link. **To configure the weighting %, perform the following steps.** 1. Click **Dynamic** under the link bonding section. The **Bonding Mechanism** pop-up window appears, see *Figure 2-28*. 2. Click **Static**. The **Weighting % (applicable for Static Bonding)** section becomes available. 3. Enter the weighting % for the WAN links. You must ensure that the sum of the weighting % for both like and unlike WAN links must be 100%. This is an example of the like WAN link. You can configure 40 the weighting % for the LTE1 and 60 the weighting % for the LTE2. As, sum of both weighting % (40 + 60) = 100. This is an example of the unlike WAN link. You can configure 40 the weighting % for the VSAT1, 30 the weighting % for the LTE1, and 30 the weighting % for the LTE2. As, sum of the weighting % (40 + 30 + 30) = 100. 4. Click **Done**. The **Create Internet** (**WAN) Profiles** page appears, see *Figure 2-27*. If an error occurred due to a probe of the WAN, then an error message is displayed, see *Figure 2-29*. **NOTE:** The Link Bonding will not be available for a single WAN

Fields	Description
	link. Therefore, weighting % cannot be configured.
Priority 2	Refer to Highest Priority.
Priority 3	Refer to Highest Priority.
Priority 4	Refer to Highest Priority.
Priority 5	Refer to Highest Priority.
Lowest Priority	Refer to Highest Priority.

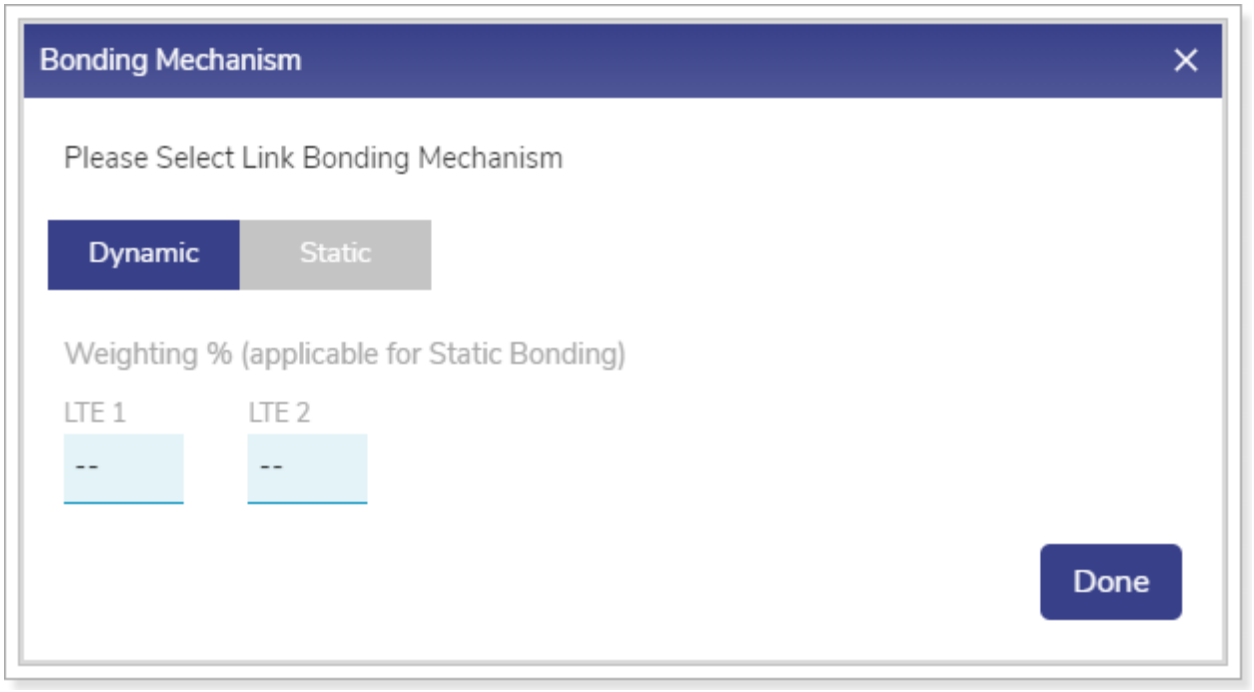


Figure 2-28 Bonding Mechanism for Like WANs

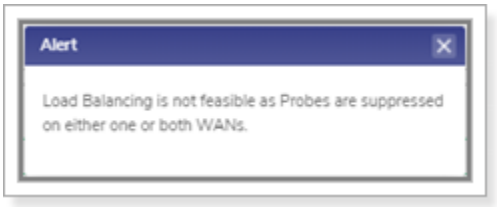


Figure 2-29 Error Message

Once the WAN link is assigned to the priority levels, the server will verify the network basis on the priority levels. This is an example.

You set the following priority levels of enabled WANs.

Highest Priority – LTE 1 and LTE 2.

Priority 2 – VSTA 1 and VSAT 2.

Priority 3 – Ethernet.

Priority 4 – Wi-Fi

Initially, the server will verify whether the LTE network is available as the LTE is assigned the highest priority. If the LTE network is available, then the internet connection will be established through the LTE network. Otherwise, the server will verify whether the VSAT network is available as the VSAT is assigned the priority 2 level. The process will continue up to the priority level configured.

The server will distribute the traffic basis on the weighting % configured for the WAN links.

3. Click **Save**.

WAN profile configured successfully. The WAN profile will become available while configuring the networks. For details, see *Step 3: Access Networks* on page *43*.

Perform **Step 5: Traffic Policies**.

2.5 Step 5: Traffic Policies

When the K4 server is installed on the vessel, by default, the network level and device level traffic policies are configured. The network level policy will be applicable under the Aggregate Traffic Policy and the device level policy will be applicable under the Device Traffic Policy.

1. Click  on the **WAN Profiles** or click **Traffic Policies**. The **Traffic Profiles** page appears, see *Figure 2-30*.

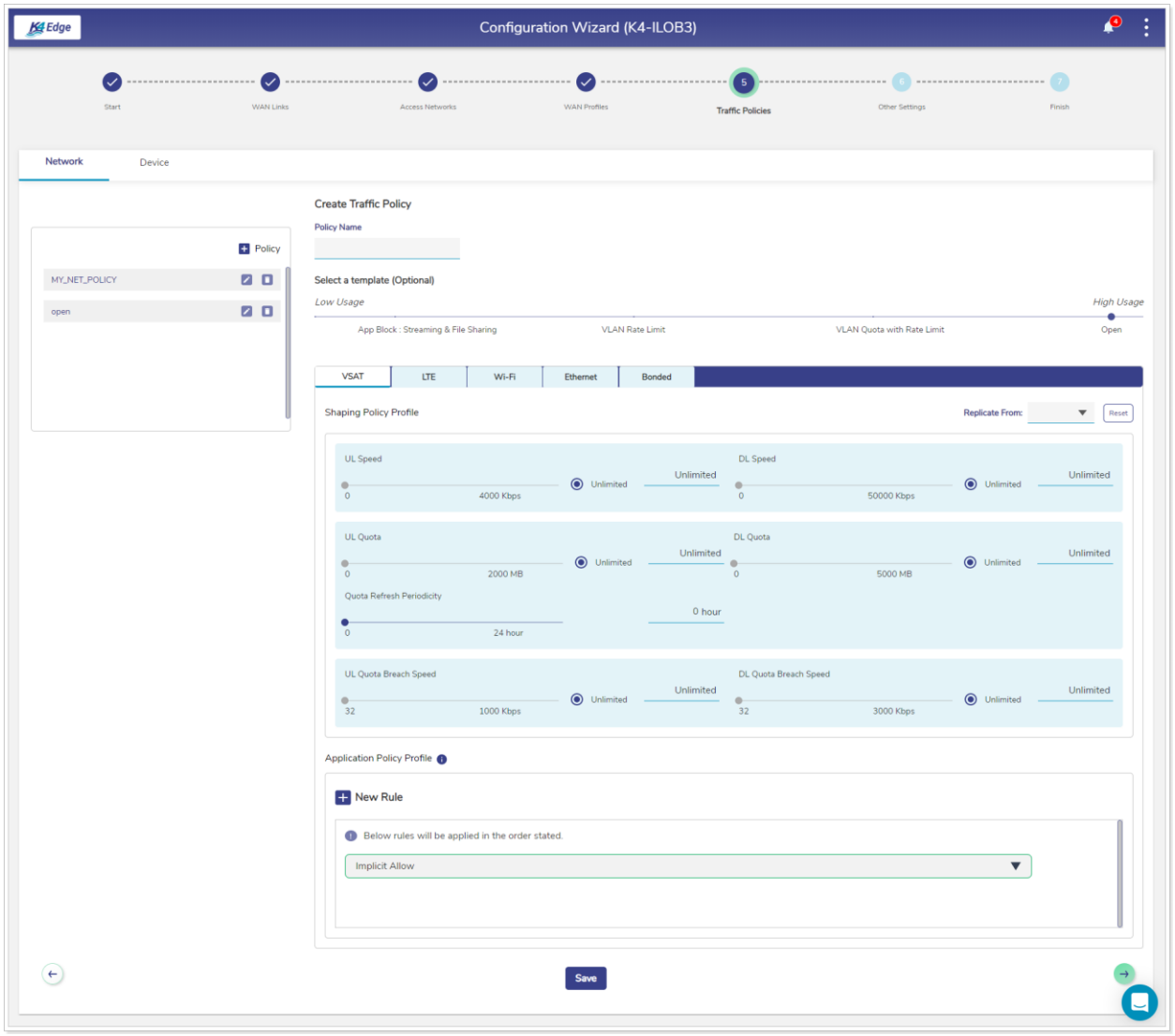


Figure 2-30 Traffic Policies

2. Click **Network**.

   By default, the **Network** is selected.

3. Click **+ Policy**. The **Policy Name** field becomes available under the **Create Traffic Policy** section. To enter data in the respective fields, see *Table 2-7*.

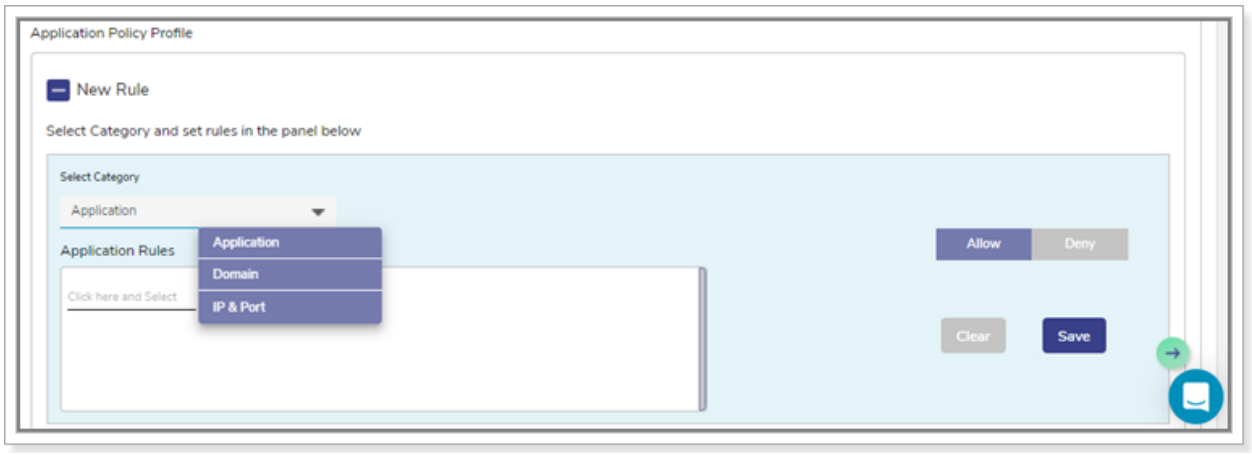


Figure 2-31 Category List

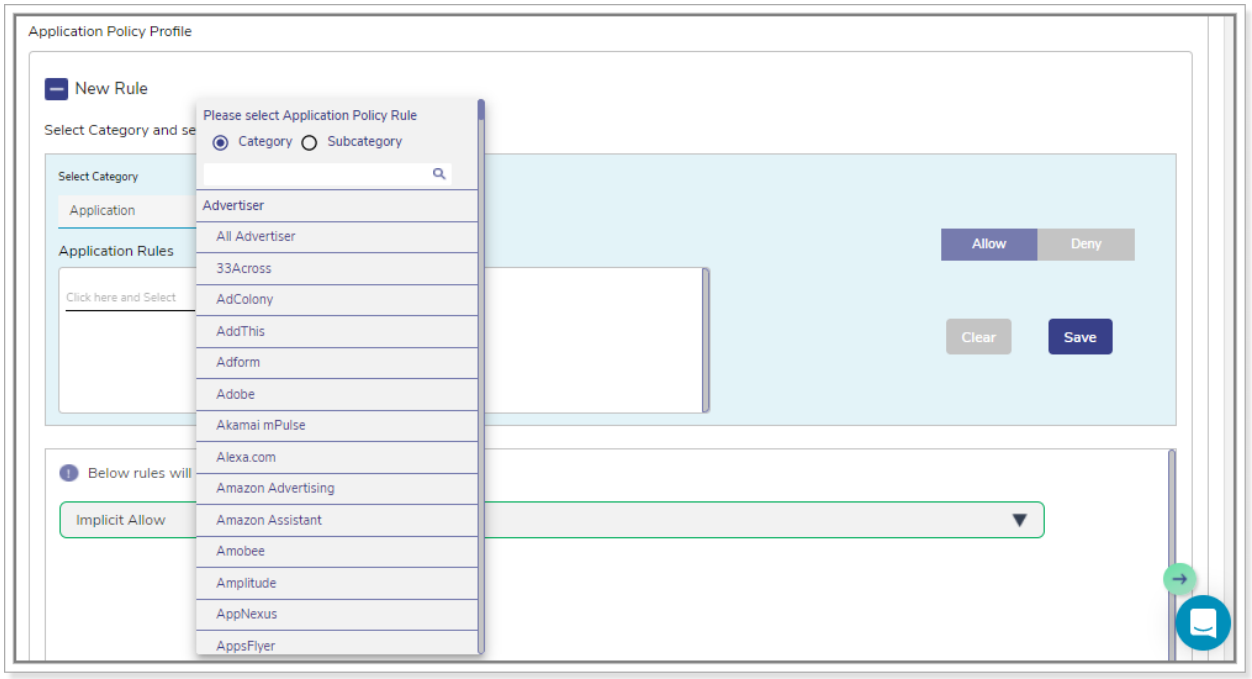


Figure 2-32 Application Rule

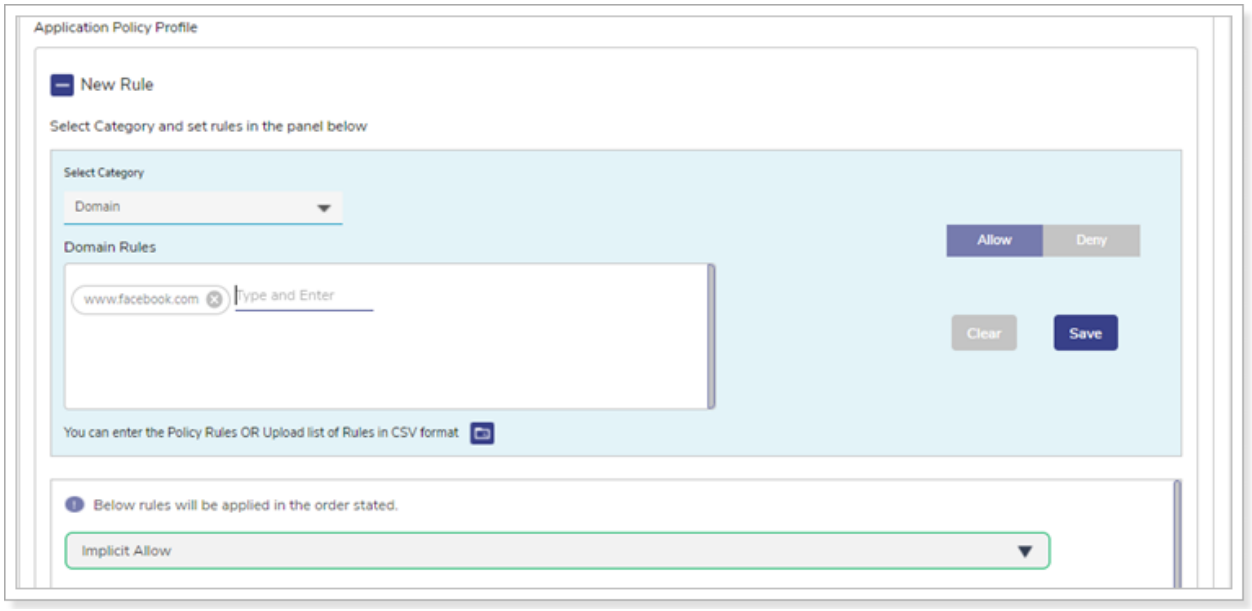


Figure 2-33 Domain Rule

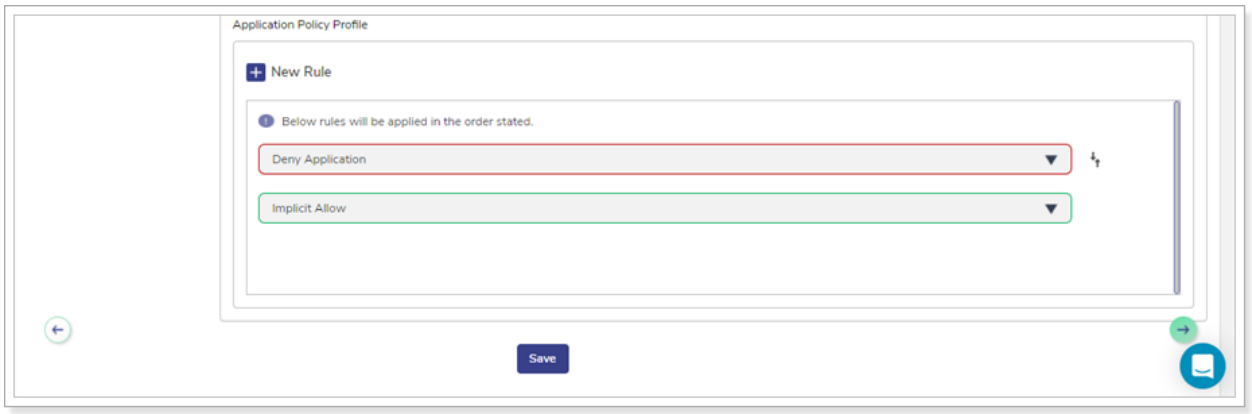


Figure 2-34 Application Allow or Deny

Table 2-7: Traffic Policy Information

Ports	Description
Policy Name	Enter the name of the policy.
Select a template (Optional)	Click a template that is to be assigned to a WAN and then click one of the following WAN tabs. • VSAT • TE • Wi-Fi • Ethernet. A template will include pre-configured UL Speed, DL Speed, UL Quota,

Ports	Description
	DL Quota, Quota Refresh Periodicity, UL Quota Breach Speed, and DL Quota Breach Speed. However, you can modify the template. You can assign a template with the pre-configured traffic policy, or re-configure the traffic policy of a template, or configure the traffic policy based on your requirement through the **Open** template. By default, the **Open** template is selected.
Shaping Policy Profile	
UL Speed	Toggle the upload speed. The upload (UL) speed **Unlimited** is either cleared or selected. The speed configured is displayed to the corresponding **UL Speed**.
DL Speed	Toggle the download speed. The download (DL) speed **Unlimited** is either cleared or selected. The speed configured is displayed to the corresponding **DL Speed**.
UL Quota	Toggle the upload quota. This indicates the permissible quota up to which the user can upload the data. The UL quota **Unlimited** is either cleared or selected. The quota configured is displayed to the corresponding **UL Quota**.
DL Quota	Toggle the download quota. This indicates the permissible quota up to which the user can download the data. The DL quota **Unlimited** is either cleared or selected. The quota configured is displayed to the corresponding **DL Quota**.
Quota Refresh Periodicity	To configure the expiry of hours post which the upload quota and download quota will be refilled or reset to the pre-configured upload quota and download quota respectively. Toggle the hours. The refresh periodicity configured is displayed to the corresponding **Quota Refresh Periodici**ty.
UL Quota Breach Speed	To configure the upload speed that will be applicable after the UL quota is exhausted, toggle the speed. **NOTE:** This indicates the UL speed that will be applicable after the UL quota is exhausted. The UL quota breach speed will continue until the UL quota is refill basis on the quota refresh periodicity configured

Ports	Description
	The speed **Unlimited** is either cleared or selected. The breach speed configured is displayed to the corresponding **UL Quota Breach Speed**.
DL Quota Breach Speed	To configure the download speed that will be applicable after the DL quota is exhausted, toggle the speed. **NOTE:** This indicates the DL speed that will be applicable after the DL quota is exhausted. The DL quota breach speed will continue until the DL quota is refill basis on the quota refresh periodicity configured The speed **Unlimited** is either cleared or selected. The breach speed configured is displayed to the corresponding **DL Quota Breach Speed**.
Replicate From	**To replicate the traffic policy of a WAN, perform the following steps.** 1. Click **Replicate From**. 2. Click a WAN whose traffic policy to be applied to the WAN. You can re-configure the replicated traffic policy.
Application Policy Profile	
New Rule	To create a new rule, click **New Rule**. The Category and Application **Rules** fields become available.
Select Category	Click a category, see *Figure 2-31*. **NOTE:** By default, the **Application** category is selected. Therefore, the Application Rules field becomes available, see *Figure 2-32*. Or, If you select the **Domain** category, then the Domain Rules field becomes available, see *Figure 2-33*. Or, If you select the **IP & Port** category, then the IP & Port field becomes available. In addition to this, the entire categories are by default **Allowed**. Therefore, by default **Implicit Allow** rule becomes available under the **Application Policy Profile** section. You cannot modify the **Implicit Allow** rule.

Ports	Description
Application Rules	**To apply or deny application rules, perform the following steps.** 1. Click under the **Application Rules** section. The list becomes available, see *Figure 2-32*. 2. Click **Category** or **Subcategory**. List based on the selected **Category** or **Subcategory** becomes available. 3. Click a category or subcategory. 4. To allow the application, click **Allow**. Or, To block the application, click **Deny**. **NOTE:** By default, **Allow** is selected. 5. Click **Save**. The allowed and blocked application becomes available, see *Figure 2-34*. **NOTE:** There can be a single deny and single allow rule per category or an implicit allow or an implicit deny rule. If you select the **Application Rule** in the Select Category field, then the Application Rules field becomes available.
Domain Rules	**To apply or deny domain rules, perform the following steps.** 1. Click under the Domain Rules section. 2. Enter the name of the domain in one of the following formats. • domain.com • domain1.domain2.com • *.domain.com, Where, * can be any value. **NOTE:** You can enter multiple domain names. 3. To allow the domain, click **Allow**. Or, To block the domain, click **Deny**. **NOTE:** By default, **Allow** is selected. 4. Click **Save**. The allowed and blocked domain becomes available, see *Figure 2-34*.

Ports	Description
	NOTE: You can also upload the rule list in CSV format. If you select **Domain Rule** in the Select Category field, then the Domain Rules field becomes available.
IP & Port	**To apply or deny IP and port rules, perform the following steps.** 1. Click under the IP & Port section. 2. Enter IP and port in one of the following formats. • a.b.c.d • a.b.c.d/x • a.b.c.d:/x:y • a.b.c.d/x:y-z • a.b.c.d:y-z • a.b.c.d:y Where, x is a subnet and its value can be from 0 (zero) to 32. y and z are port numbers and its value can be from 0 (zero) to 65535. a/b/c/d are IP and its value can be from 0 (zero) to 255. **NOTE:** You can enter IP and ports. 3. To allow the IP, click **Allow**. Or, To block the IP, click **Deny**. **NOTE:** By default, **Allow** is selected. 4. Click **Save**. The allowed and blocked IP and the port become available. **NOTE:** If you select **IP & Port** in the Select Category field, then the IP & Port field becomes available.
Implicit Allow/Deny Rules	To implicit allow the final policy, click **Implicit Allow/Deny Rules**, and then click **Allow**. Or, To implicit allow the final policy, click **Implicit Allow/Deny Rules**, and then click **Deny**.

4. Click **Save**.
5. Click **Device** and then continue from step *3* on page *65*.

Network traffic policy and device traffic policy configured successfully. The network traffic policy will become available to assign to the aggregate traffic policy, and the device traffic policy will become available to assign to the device traffic policy while configuring the **Managed Connected Network**. For details, see *Step 3: Access Networks* on page *43*.

In addition to this, the device traffic policy will become available to assign to the specific MAC address while configuring the **Other Settings**.

Perform **Step 6: Other Settings**.

2.6 Step 6: Other Settings

You can configure the global device traffic policy, static route, US internet and firewall, and DNS proxy. The global settings will override the network (VLAN) policy.

1. Click on the **Traffic Profiles** page or click **Other Settings**. The **Other Settings** page appears, see *Figure 2-35*.

Figure 2-35 Other Settings

2. Click **Device Traffic Policies**. The **Add Device** and **Device Traffic Policies** section becomes available, see *Figure 2-36*. To enter data in the respective fields, see *Table 2-8*.

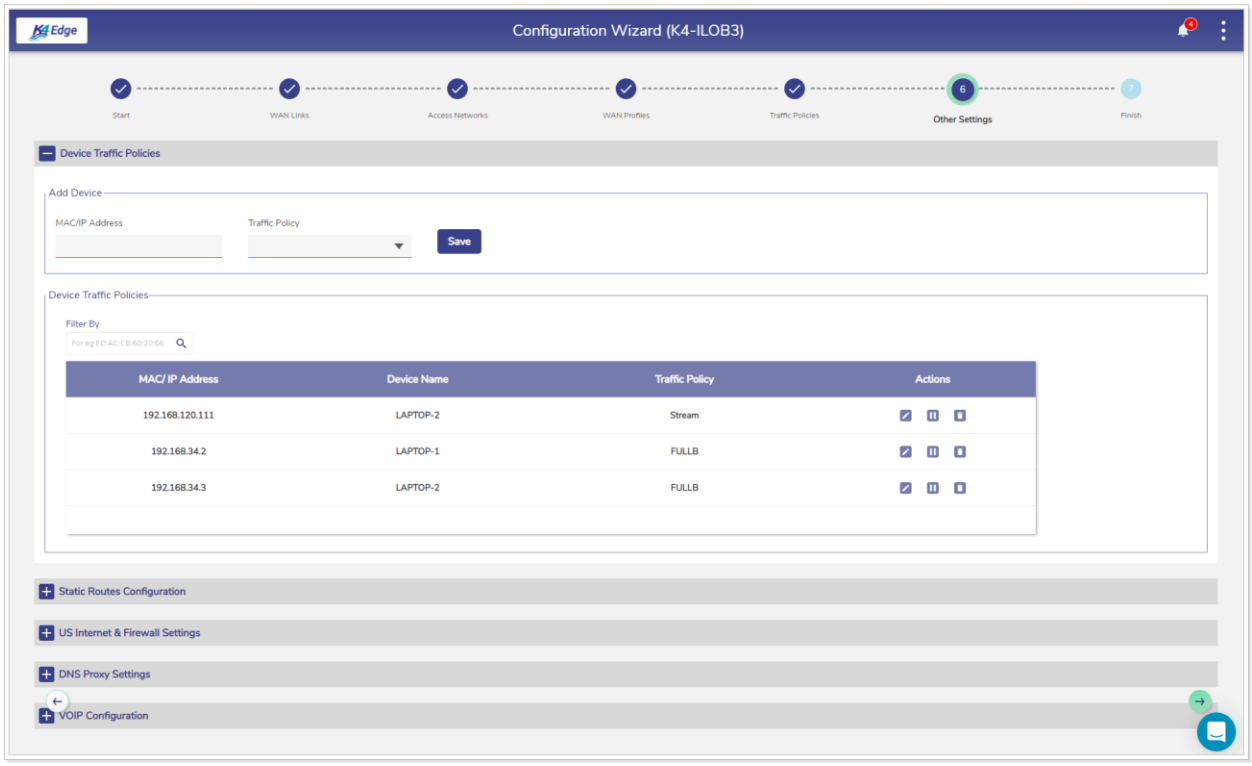


Figure 2-36 Device Traffic Policy

Table 2-8 Device Traffic Policies Information

Ports	Description
Add Device	
MAC/IP Address	Enter the MAC or IP address of a device. Or, Click the box and select a MAC or IP address. **NOTE:** The devices connected to the entire network become available.
Traffic Policy	In the **Traffic Policy** list, click a traffic policy to be assigned to the MAC or IP address specified in the MAC/IP Address field and then click **Save**. **NOTE:** The device traffic policy created while configuring the traffic policies will become available. For details about the traffic policy, see *Step 5: Traffic Policies* on page *64*. You can assign the traffic policy to a device from also **Step 3: Access Networks**. For details, see *Step 3: Access Networks* on page *43*. However, the traffic policy last assigned to a device from any step will override the traffic

Ports	Description
	policy of that device. Following is an example. Previously, the traffic policy was assigned to a device from **Step 3: Access Networks**. A new traffic policy is assigned to a device from **Step 6: Other Settings**. Therefore, the traffic policy assigned to a device from **Step 6: Other Settings** will override the existing traffic policy of that device.
Device Traffic Policies or Filter By	Details about the MAC or IP address become available under the **Device Traffic Policies** or **Filter By** section. **To assign a new traffic policy to a MAC or IP address, perform the following steps.** 1. Click to the corresponding MAC/IP address. The box becomes available to the corresponding MAC/IP address. 2. Click and select a new traffic policy to be assigned to the MAC/IP address. Or, To stop the traffic policy of a MAC/IP address, click to the corresponding MAC/IP address. The device basis on the MAC/IP address in the network will stop. To resume the traffic policy, click **Resume**. Or, **To delete the traffic policy of a MAC/IP address, perform the following steps.** 1. Click to the corresponding MAC/IP address. The confirmation message box appears. 2. Click **OK**.

3. Click **Static Route Configuration**. The **Add Static Routes** section becomes available, see *Figure 2-37*.

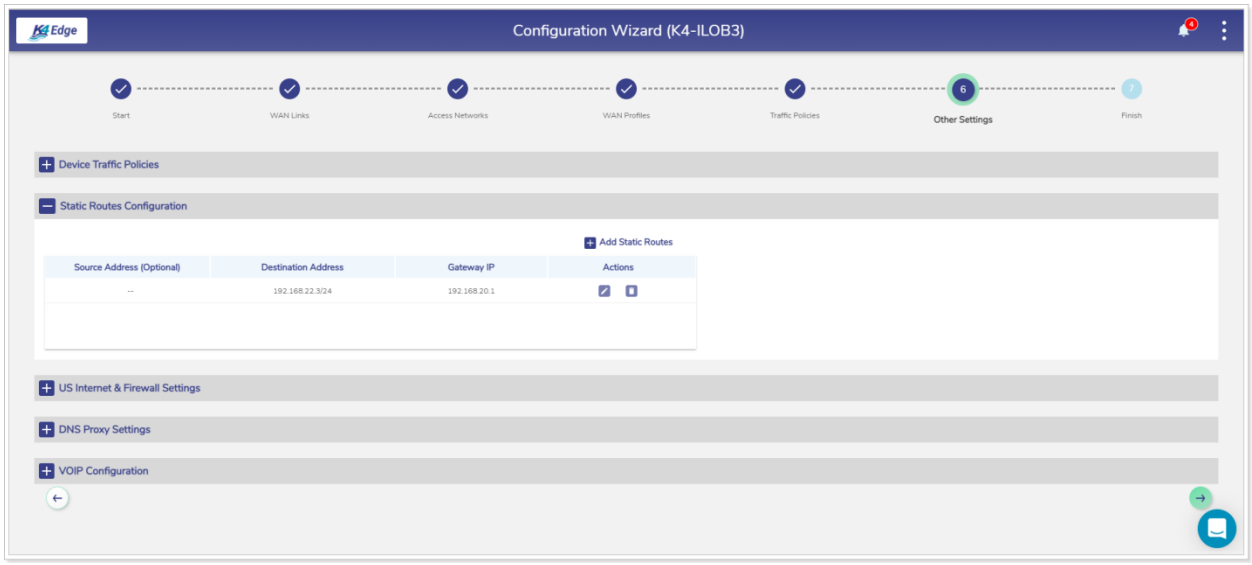


Figure 2-37 Add Static Route

4. Click **Add Static Routes**. The route section becomes available, see *Figure 2-38*. To enter data in the respective fields, see *Table 2-9*.

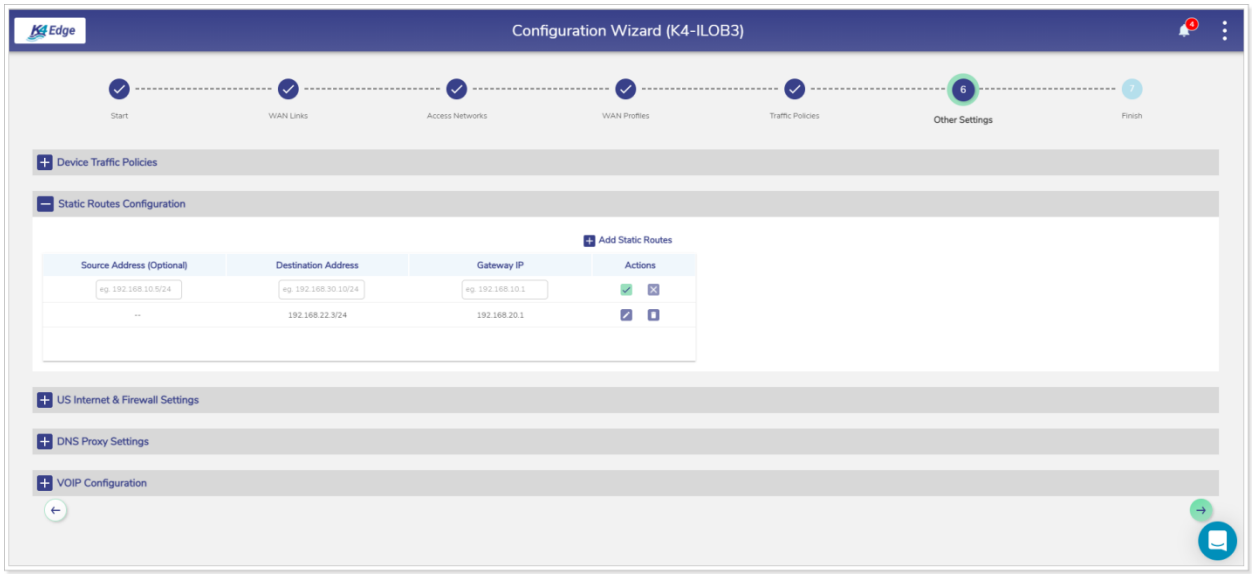


Figure 2-38 Add Static Route

Table 2-9: Static Route Information

Ports	Description
Source Address (Optional)	Enter the source IP address and subnet mask.
Destination	Enter the destination IP address and subnet mask that is to be routed to

Ports	Description
Address	a specific router.
Gateway IP	Enter the IP address of the router to which the traffic to be routed. This indicates that the traffic with a source IP address and a destination IP will be routed to the router with an IP address specified in the Gateway IP field. This is an example. Source Address (Optional) 92.168.10.5/24 Destination Address 192.168.10.5/24 Gateway IP 192.168.10.1 The traffic with a source IP address/subnet mask 92.168.10.5/24 and a destination IP address/subnet mask 192.168.10.5/24 will be routed to a router with an IP address 192.168.10.1.
Action	Click .

5. Click **US Internet & Firewall Settings**. The **US Internet & Firewall Settings** section becomes available, see *Figure 2-39*. To enter data in the respective fields, see *Table 2-10*.

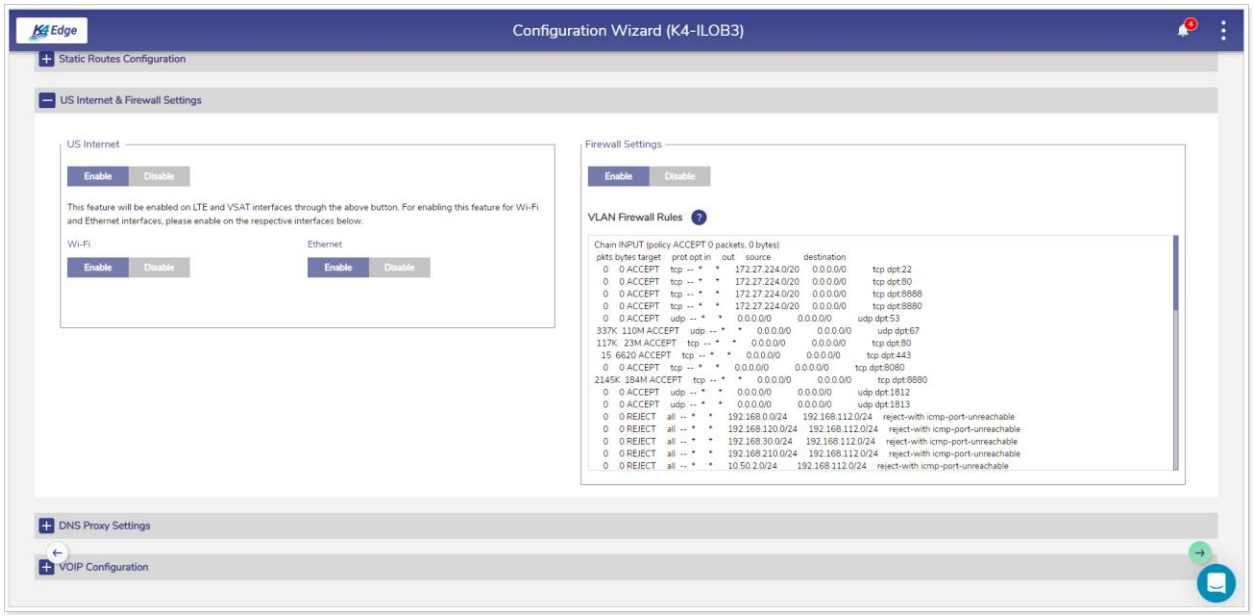


Figure 2-39 US Internet & Firewall Settings

Table 2-10: US Internet & Firewall Settings Information

Ports	Description
US Internet	To enable the US internet on the vessel, click **Enable**. Therefore, the US internet will become accessible from the vessel irrespective of the current

Ports	Description
	location of the vessel. By default, the **Enable** is selected. Therefore, the US internet will become accessible on the LTE and VSAT. You can enable the US internet on the vessel while the vessel is docked and accessing the network through Wi-Fi and Ethernet. For this, click **Enable** under the **Wi-Fi** and **Ethernet**.
Firewall Settings	To enable the firewall settings, click **Enable**. Or, To disable the firewall settings, click **Disable**. For details about the firewall settings, click ? to the corresponding **VLAN Firewall Rules**.

6. Click **DNS Proxy Settings**. The **Domain/Host Mapping**, **DNS Forwarder**, and **DNS Cache** sections become available, see *Figure 2-40*.

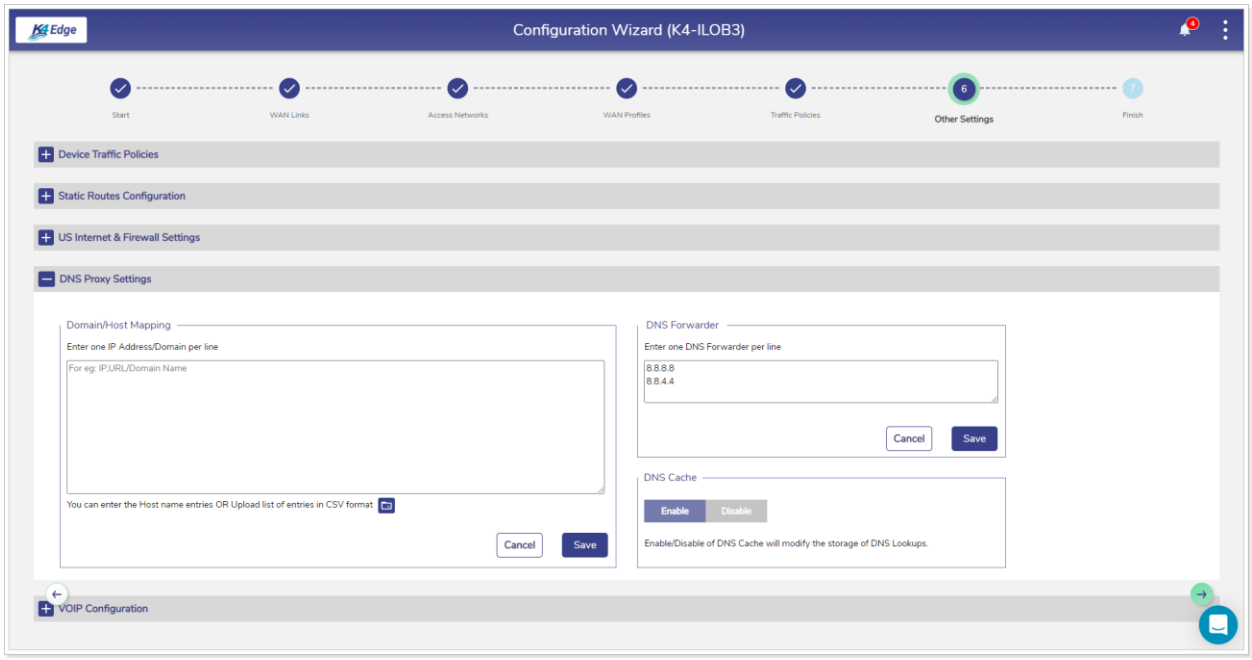


Figure 2-40 Configure DNS Proxy

Table 2-11: DNS Proxy Information

Ports	Description
Domain/Host Mapping	1. Enter an IP address and suffix domain on a single line. 2. Click **Save**.

Ports	Description
	Or, 1. To configure multiple domains and host mapping, enter the IP address and suffix domain on a distinct line, and perform this step on every line. Or, You can upload the list of the domain/host mapping also in the Comma Separated Value (CSV) format. For this, click and upload the CSV file. 2. Click **Save**.
DNS Forwarder	1. Enter only one DNS forwarder on every line. 2. Click **Save**.
DNS Cache	To enhance the DNS lookups, click **Enable**.

The other settings are successfully configured.

7. Click **VOIP Configuration**. The **WAN Profile for VOIP** sections become available, see *Figure 2-40*.

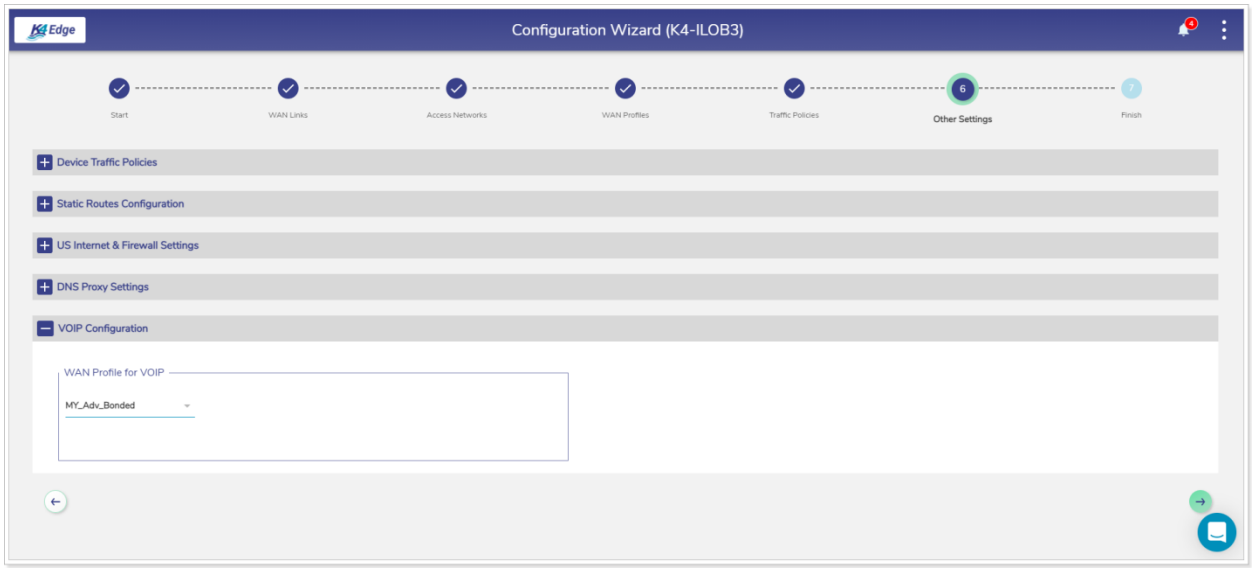


Figure 2-41 VOIP Configuration

In the list, click a WAN profile for VoIP.

Perform **Step 7: Finish**.

2.7 Step 7: Finish

Click on the **Other Settings** page or click **Finish**. The **Finish** page appears, see *Figure 2-42*.

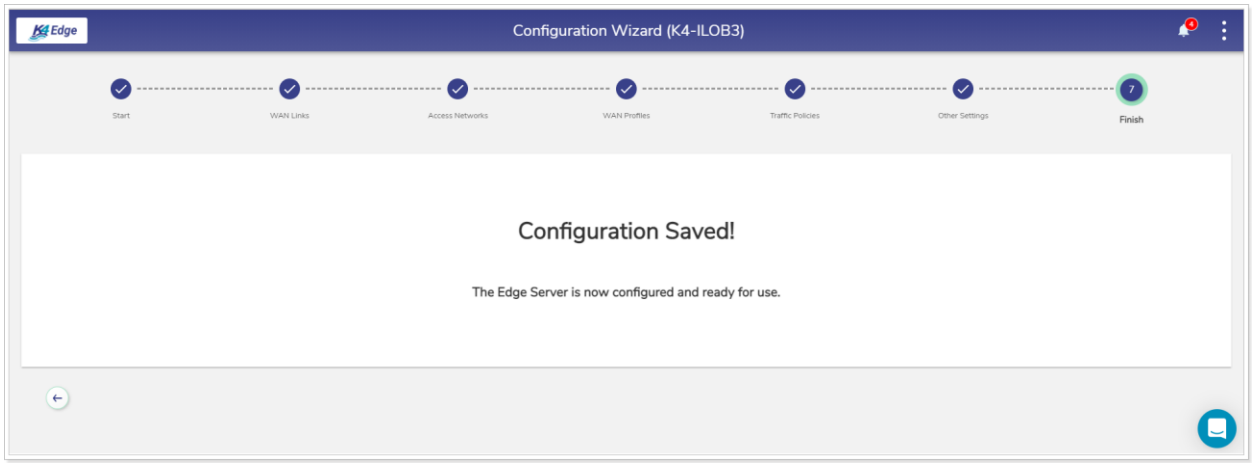


Figure 2-42 Finish

The K4 Edge Server was configured successfully.

3 Monitoring

You can monitor the VSAT. LTE, VoIP, the performance of the WANs, and track the usage of the WANs.

3.1 Monitoring Alerts

System alerts are raised based on the following scenarios.

- When VLAN/Device/Enterprise User consumptions exceed thresholds.
- Traffic will pause on the VLAN/Device/Enterprise User.
- Active Internet Sources is unavailable.

Following are the severity levels of the system alerts.

- Critical
- Major
- Minor
- Info
- Warning

To view the alerts, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.

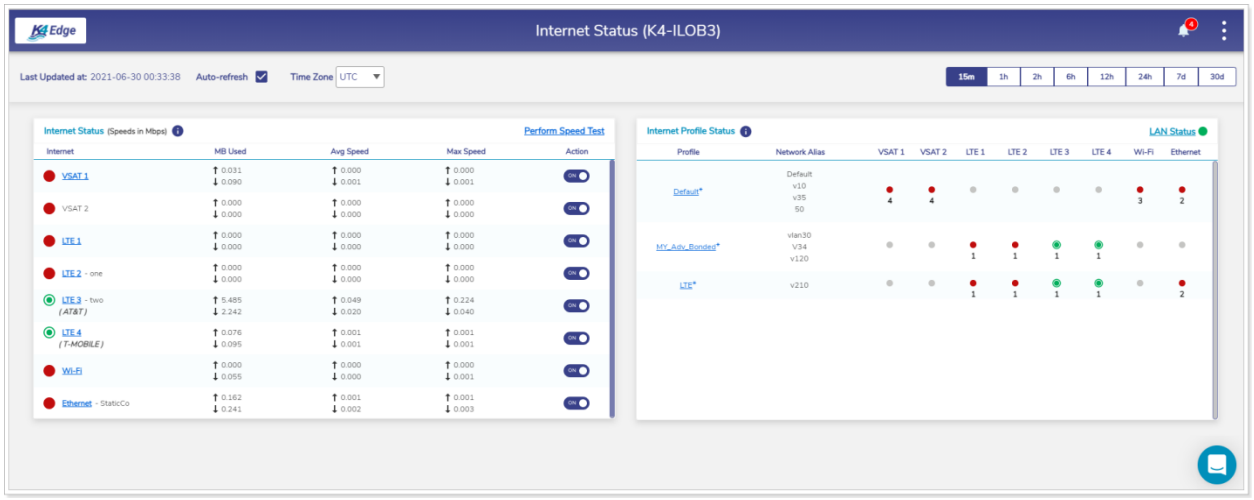


Figure 3-1 Status of Internet

2. Click the bell icon, see *Figure 2-4*. The **Notifications** pop-up window appears, see *Figure 3-2*.

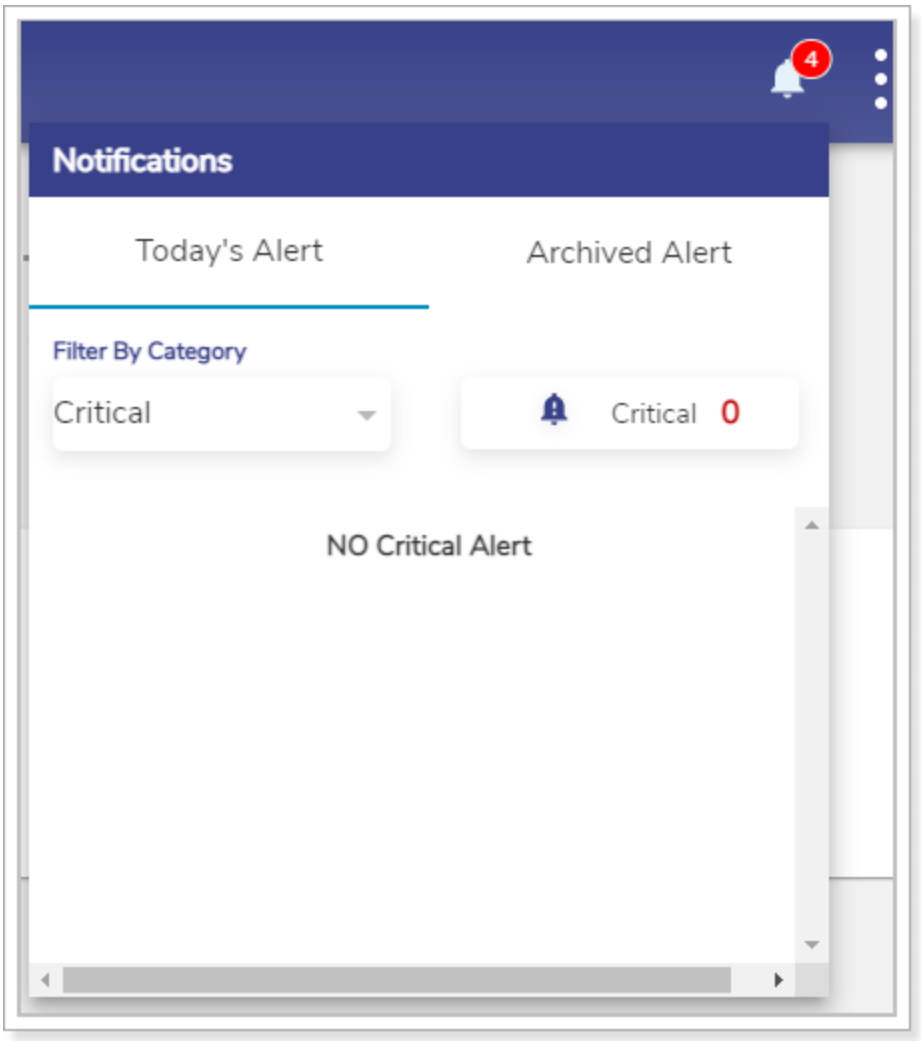


Figure 3-2 Alerts and Notifications

The count of the alerts is displayed over the bell icon, see *Figure 3-2*.

3. Click **Today's Alert**. The current day alerts will become available under the **Today's Alert** tab.
4. You can filter the alerts based on the severity levels. For this, click the drop-down arrow under the **Filter By Category** section. Details about the alerts are displayed. In addition to this, the count of the alerts based on the severity level is displayed.
5. Click **Archived Alert**. The entire alerts up to the previous day are automatically archived and will become under the **Archived Alert** tab.

3.2 Monitoring K4 Edge

After configuring the K4 Edge server, you can perform the following tasks.

- View details about your account.
- View details about the system.
- Access the K4 Edge Configuration Wizard.
- View the current status of the WAN links.
- View the performance chart.
- View the usage status.

3.2.1 My Account

To view details about the account, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.

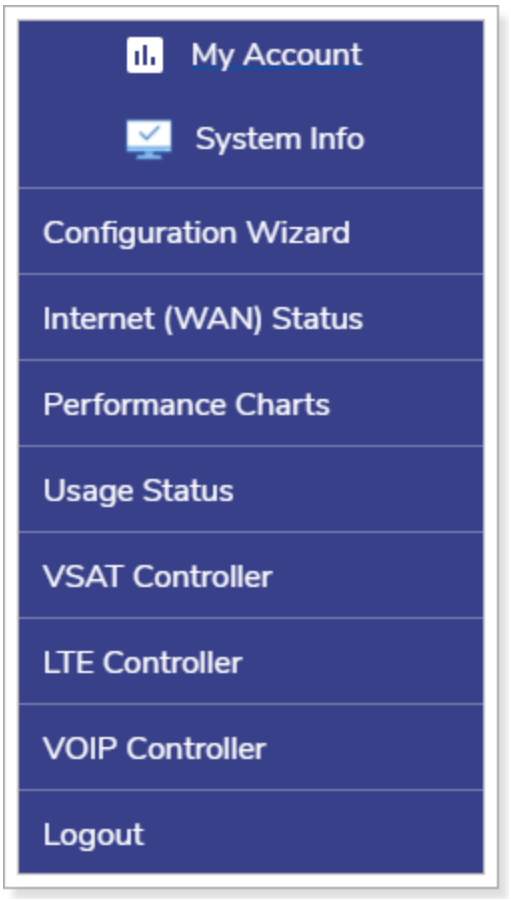


Figure 3-3 Options

3. Click **My Account**. The account details become available, see *Figure 3-4*.

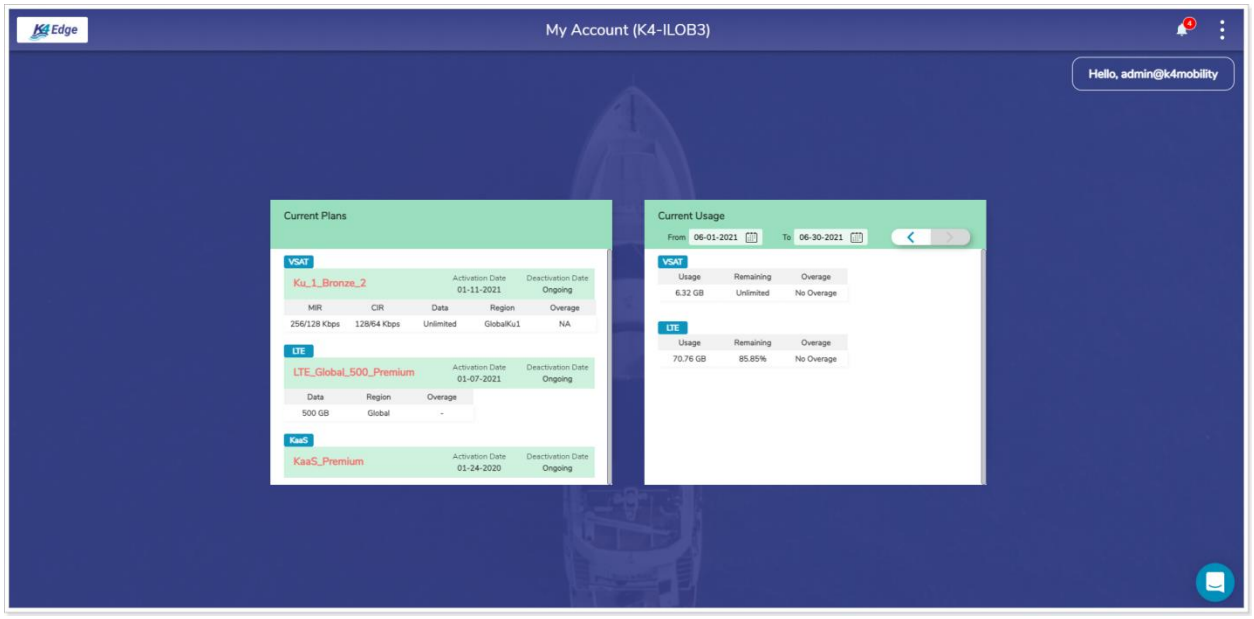


Figure 3-4 Information about Account

Following details become available.

- Current Plans. This indicates the current plans of the entire WAN links available to the vessel.
- Current Usage. This indicates the internet usage on the vessel based on the billing cycle of the WAN link.

3.2.2 System Information

To view details or information about the system, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **System Info**. The **System Information** pop-up window appears, see *Figure 3-5*. For details about the system information, see Table 3-1.

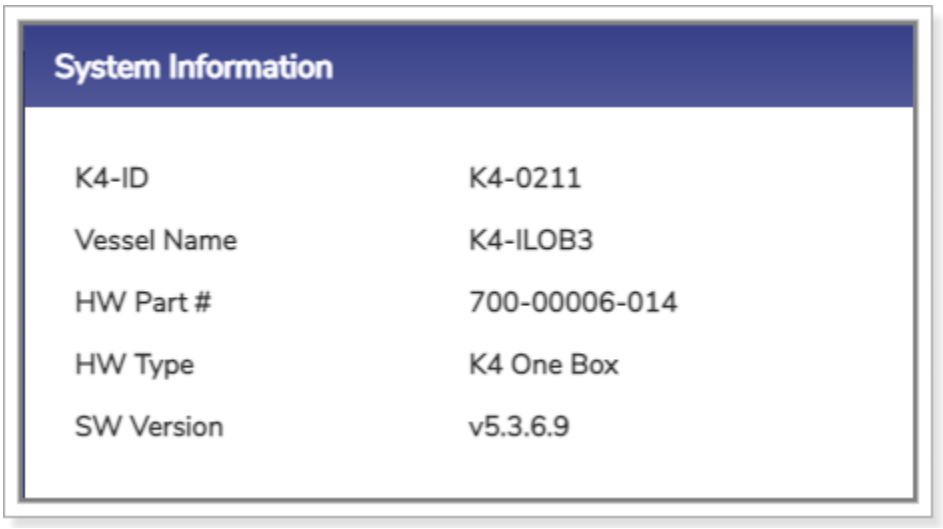


Figure 3-5 System Information

Table 3-1 Details about System

Fields	Description
K4-ID	This value is specified while registering your vessel.
Vessel Name	This is the name of your vessel which is specified while installing the K4 Edge Server.
HW Part #	This is a unique part number of the OneBox server.
HW Type	This is the name of the server that you are accessing through the K4 Edge Configuration Wizard.

Fields	Description
SW Version	This is the version of the K4 Edge Configuration Wizard used to configure the WAN profiles.

3.2.3 Configuration Wizard

To access the K4 Edge Configuration Wizard, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Configuration Wizard**. The home page appears, see *Figure 2-3*.

For details, see *Commissioning K4 Edge Server* on page *29*.

3.2.4 Internet (WAN) Status

Once the K4 Edge is configured, you can monitor the status of the internet status or WAN links of the vessel.

To view internet status, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Internet (WAN) Status**. **Internet Status** page appears, see *Figure 3-1*.

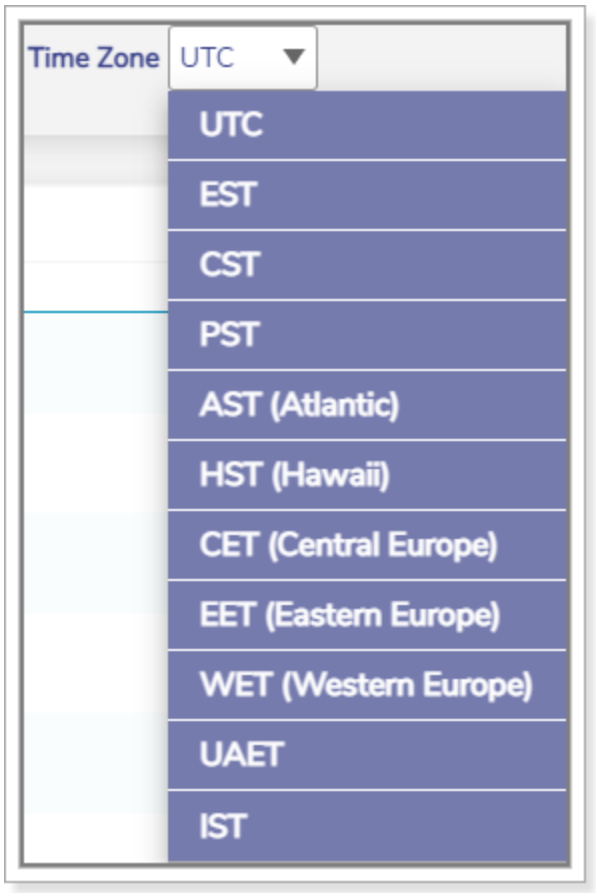


Figure 3-6 Time Zone

Return

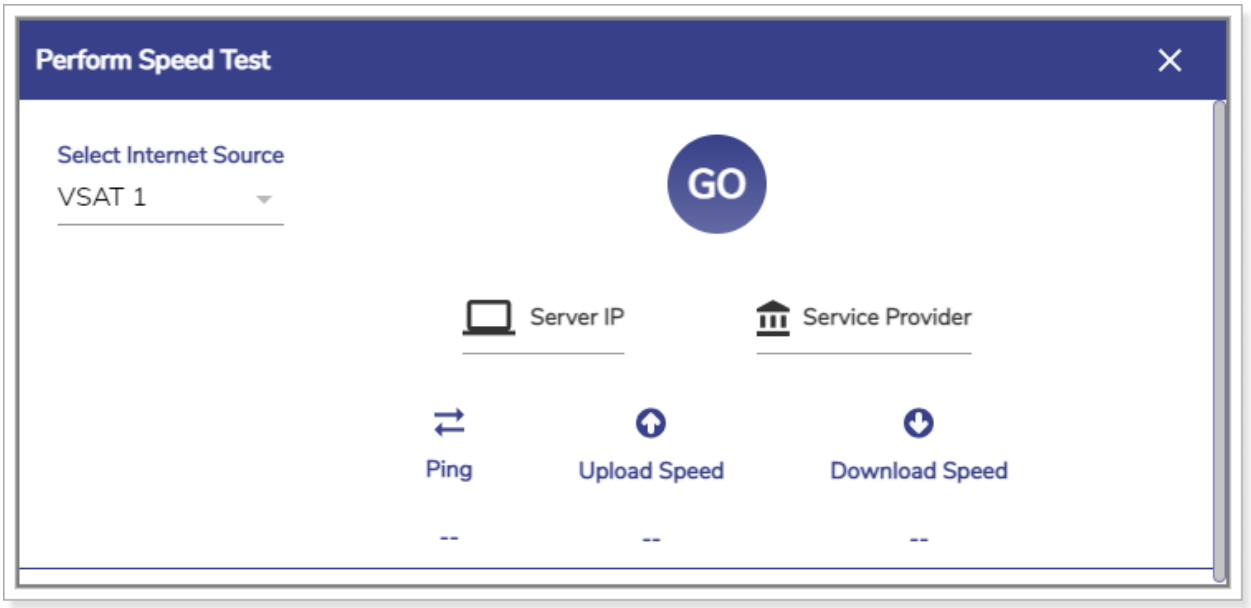


Figure 3-7 Perform Speed Test

Return

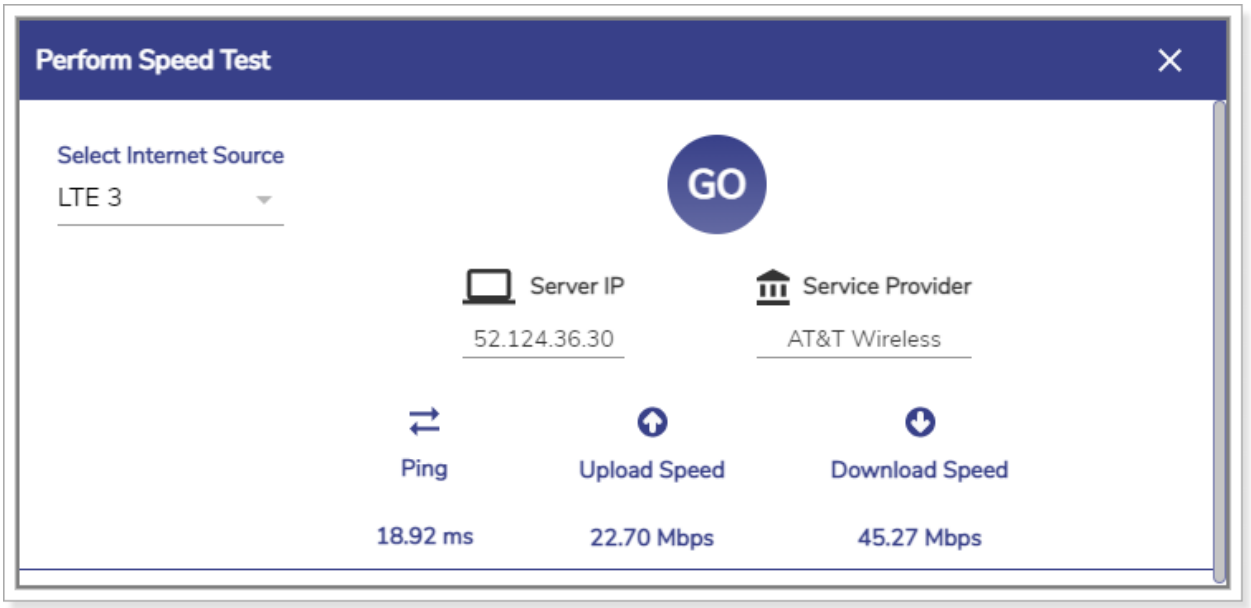


Figure 3-8 Speed Test Result

Return

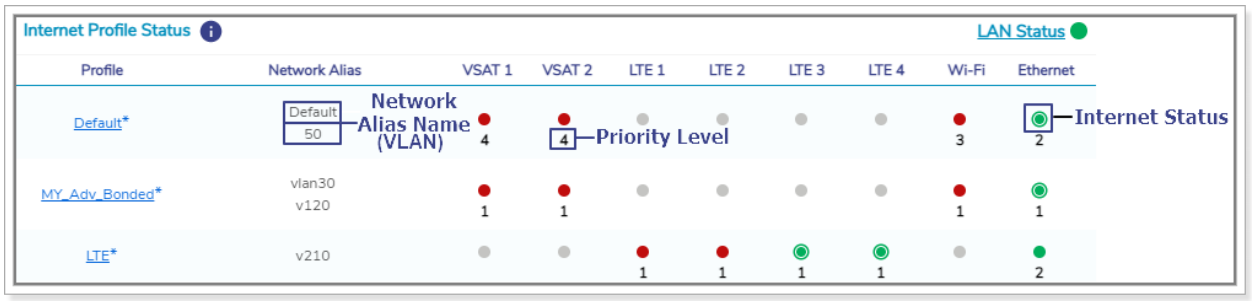


Figure 3-9 Internet Profile Status Details

Return

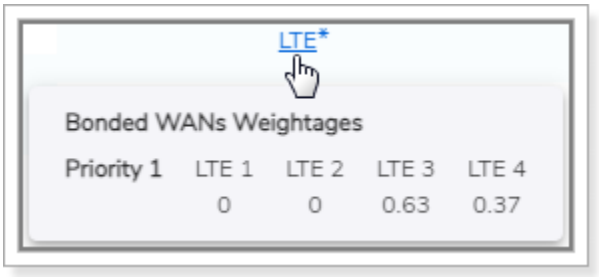


Figure 3-10 Bonded WAN Weightages

Return

Table 3-2 WAN Status Information

Fields	Description	Configuration
Auto-refresh	Whether the data on the page to be refreshed automatically. Data is updated at an interval of 30 seconds.	To automatically refresh the details about the WAN link, click the **Auto-refresh** check box.
Time Zone	To access the details about the WAN link basis on the time zone. By default, the UTC time zone is configured.	In the **Time Zone** link, click a time zone, see *Figure 3-6*.
	To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where, • m is minutes • h is hours • d is days	Click the periodicity at the upper-right corner of the page.

Fields	Description	Configuration
	By default, the periodicity of 15m is configured.	
Internet Status		
Internet Status	To view the status and speed of the WAN link or internet.	To view details about the internet status, point the mouse to .
Internet	Following are the statuses of the internet. • . Active. This indicates that the corresponding WAN link or internet is working and being used by the users on the vessel and the internet traffic is moving through that WAN link or internet. • . Standby. This indicates that the corresponding WAN link or internet is working but not being used by the users on the vessel and the internet traffic is not moving through that WAN link or internet. • . Disabled. This indicates that the corresponding WAN link or internet is disabled. Therefore, the internet will not work and the internet traffic will not move through that link or internet. • . Down. This indicates that the WAN link or internet is not working.	To access the controller of the respective WAN link or internet, click the WAN link or internet. And, To disable or enable the WAN link or internet, click **Action**. To access the controller of the respective WAN, click the WAN link. The respective WAN controller page appears.

Fields	Description	Configuration
Action	To disable or enable the WAN link or internet.	To disable the internet, switch off **Action**. Or, To enable the internet, switch on **Action**.
Perform Speed Test	Speed test only active internet can be performed.	**To perform the speed test, perform the following steps.** 1. Click **Perform Speed Test**. The **Perform Speed Test** page appears, see *Figure 3-7*. 2. In the **Select Internet Source** list, click an internet whose speed test to be performed. **NOTE:** Before performing the speed test, you must ensure that the internet up. 3. Click **GO**. The speed test result becomes available, see *Figure 3-8*.
Internet Profile Status		
Internet Profile Status	To view details about the profile of the WAN link or internet.	To view details about the internet profile status, point the mouse to  . For details, see *Figure 3-9*.
LAN Status		To access details about the network, click **LAN Status**. The **Access Networks** page appears, see *Figure 2-12*.
Profile	The name of the WAN or internet profile is displayed.	To view the bonded weightage of the WAN profile, point the mouse to the WAN profile. The Bonded WANs Weightages pop up window appears, see *Figure 3-10*. The sum of the bonded weightages must be 1.

3.2.5 Performance Chart

Once the K4 Edge is configured, you can monitor the performance of the internet or WAN links of the vessel.

To view the performance charts, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Performance Charts**. The **Performance Charts** page appears, see *Figure 3-11*. For a description, see *Table 3-3*.

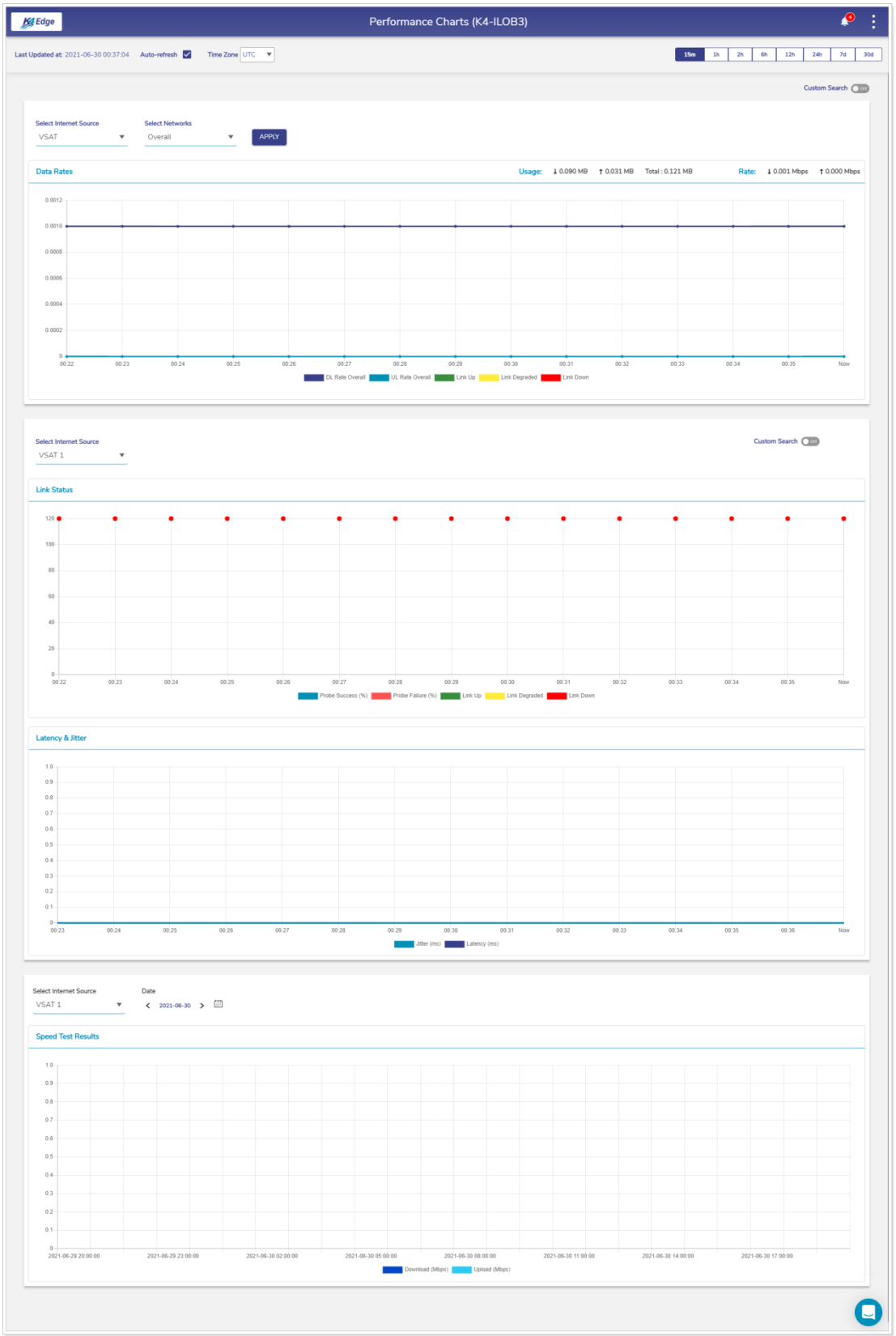


Figure 3-11 Performance Charts

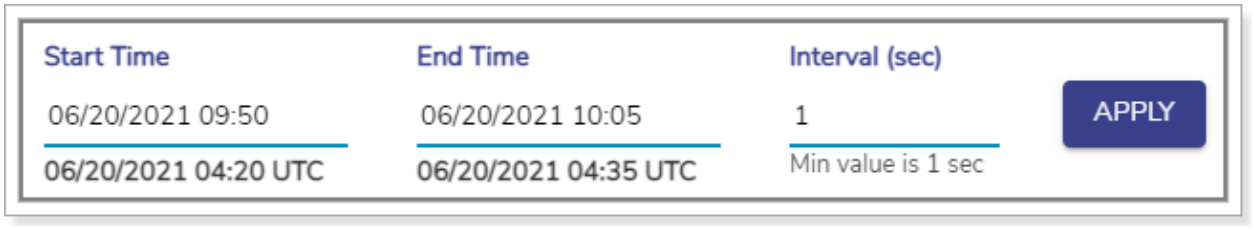


Figure 3-12 Custom Search of Link Status

Table 3-3 Performance Chart Information

Fields	Description	Configuration
Data Rates	DL/UL rates chart of the internet source for a specific network.	**To view the DU/DL rate chart for a network, perform the following steps.** 1. In the **Internet Source** list, click a WAN link or an internet source. 2. In the **Network** list, click single or multiple networks. 3. Click **Apply**. The performance chart is generated. To view the network level usages for VSAT and LTE, you must click either VSAT or LTE. The network level usages are not available for the VSAT1, VSAT2, LTE1, LTE2, LT3, and LTE4 WAN links. If the network selected in the **Networ**k list is not applicable to the internet source selected in the **Internet Source** list, then the alert will be displayed.
Link Status		To view the link status chart for a network, in the **Internet Source** list, click a WAN link or an internet source. The performance chart is generated. Or, **To view the link status chart for a network basis on a day and time, perform the following steps.** 1. Switch on the **Custom Search**. The **Start Time**, **End Time**, and **Interval (sec)** fields become available, see *Figure 3-12*. 2. Click **Start Time**. The calendar becomes

Fields	Description	Configuration
		available. 3. Select the start day and time. The start day and time becomes available in UTC. 4. Click **End Time**. The calendar becomes available. 5. Select the end day and time. The start day and time becomes available in UTC. 6. In the **Interval (sec)** field, click the minimum interval specified. 7. Click **Apply**. The chart is generated.
Speed Test Results		**To view the Speed Test Results chart, perform the following steps.** 1. In the **Internet Source** list, click a WAN link or an internet source. 2. Click the calendar in the **Date** field and select the date of when the speed test result chart to be generated. 3. Click **Apply**. The chart is generated.

3.2.6 Usage Status

Once the K4 Edge is configured, you can monitor the usage of the networks and devices associated to the network.

To view the usage charts, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-13*.

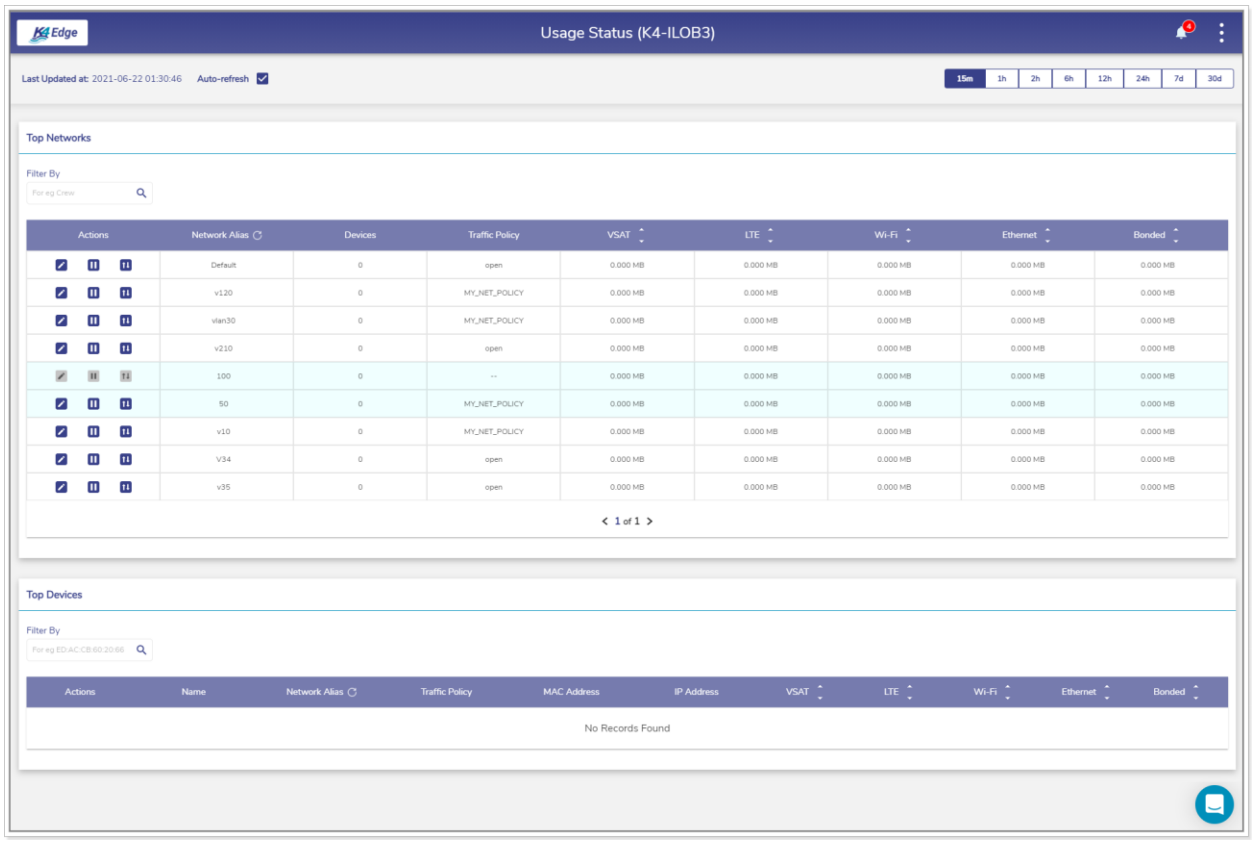


Figure 3-13 Usage Status

The **Usage Status** page includes the **Top Network** and **Top Devices** sections.

3.2.6.1 Top Networks

The following details are available under the **Top Networks** section.

- Traffic policy assigned to the network.
- Data usage of every WAN in the network.
- Count of the devices connected to the network.
- The routed access network and corresponding grouping.
- View details about the specific network, you can search that network.

To search the network, enter the name of the network in the Filter By field. Details of the network become available. The name of the network is displayed under the Network Alias field.

To view the details about the network based on periodicity, click the duration in the upper right of the page.

To modify the traffic policy of the network, perform the following steps.

1. Click to the corresponding routed network in the Action field under the **Top Networks** section. The **Edit Traffic Policy profile** page appears, see *Figure 3-14*.

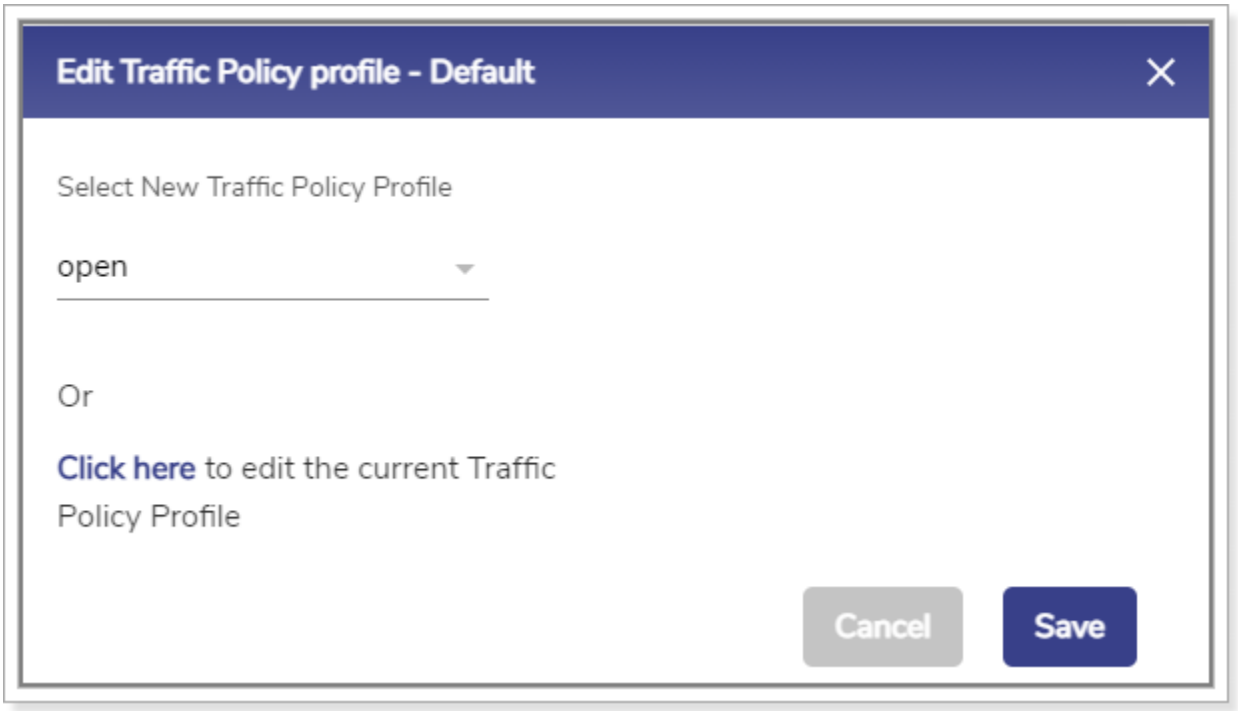


Figure 3-14 Edit Traffic Policy

2. In the **Select New Traffic Policy Profile** list, click a new traffic policy.

   Or,

   To modify the current traffic policy, click **Click here**. The **Traffic Policies** page appears. For details, see *Step 5: Traffic Policies* on page *64*.

3. Click **Save**.

To pause the internet of the network, perform the following steps.

1. Click to the corresponding routed network in the Action field under the **Top Networks** section. The **Pause Internet** page appears, see *Figure 3-15*.

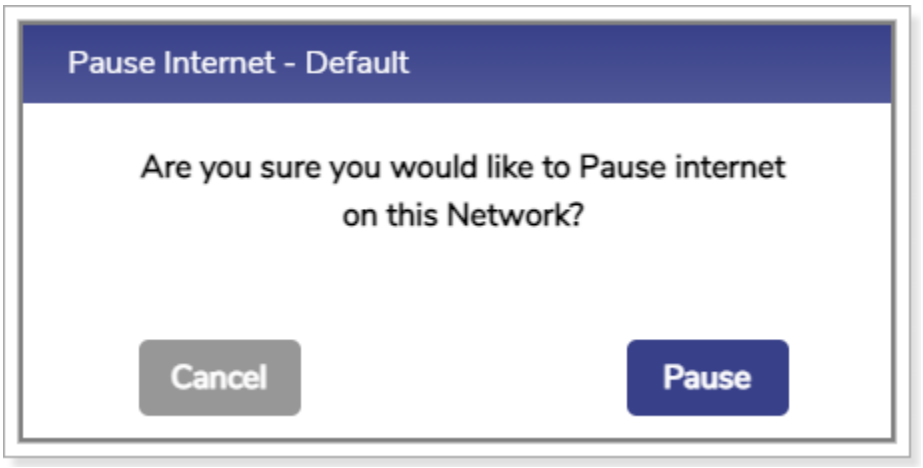


Figure 3-15 Pause Internet

2. Click **Pause**. The resume button becomes available.

   The internet is paused. However, it will not impact the other networks.

To resume the internet of the network, perform the following steps.

1. Click to the corresponding routed network in the Action field under the **Top Networks** section. The **Resume Internet** page appears, see *Figure 3-16*.

Figure 3-16 Resume Internet

2. Click **Resume**.

   The internet starts.

To view details about the traffic of the network, click to the corresponding routed network in the Action field under the **Top Networks** section. The **Traffic Details** page appears, see *Figure 3-17*.

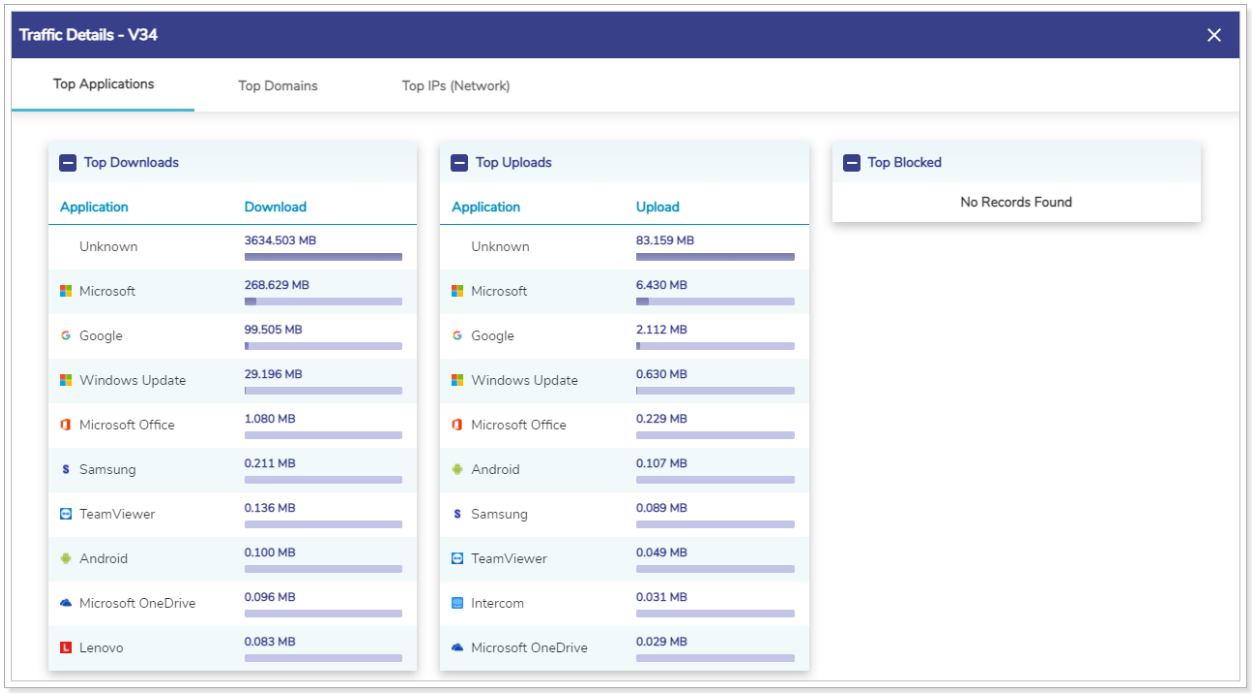


Figure 3-17 Traffic Details

To view details about the top applications, click **Top Applications**. By default, details about the top applications are available.

To view details about the top domains, click **Top Domains**.

To view details about the top IPs, click **Top IPs (Network)**.

3.2.6.2 Top Devices

The following details are available under the **Top Devices** section.

- All the devices connected to the entire network. Following is an example.

  If the sum of the devices in the Devices field under the **Top Network** section is 20, then the details about the entire 20 devices become available.
- Data consumed by the WANs in the network.
- MAC address of the device.

To search the device, enter the name of the network in the Filter By field. Details of the network become available. MAC address of the device is displayed under the MAC Address field.

To pause the internet of the device, perform the following steps.

1. Click  to the corresponding device in the Action field under the **Top Devices** section. The **Pause Internet** page appears.

2. Click **Pause**. The resume button becomes available.

   The internet is paused. However, it will not impact the other devices in the network

To resume the internet of the device, perform the following steps.

1. Click to the corresponding device in the Action field under the **Top Devices** section. The **Pause Internet** page appears.
2. Click **Resume**.

   The traffic starts.

To view details about the traffic of the device, click to the corresponding device in the Action field under the **Top Devices** section. The **Traffic Details** page appears.

3.2.7 VSAT Controller

Once the K4 Edge is configured, you can view analytics from the VSAT modem connected to the Edge Server.

To manage the VSAT controller, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **VSAT Controller**. The **VSAT Controller** page appears, see *Figure 3-18*. For details about the VSAT controller, see *Table 3-4*.

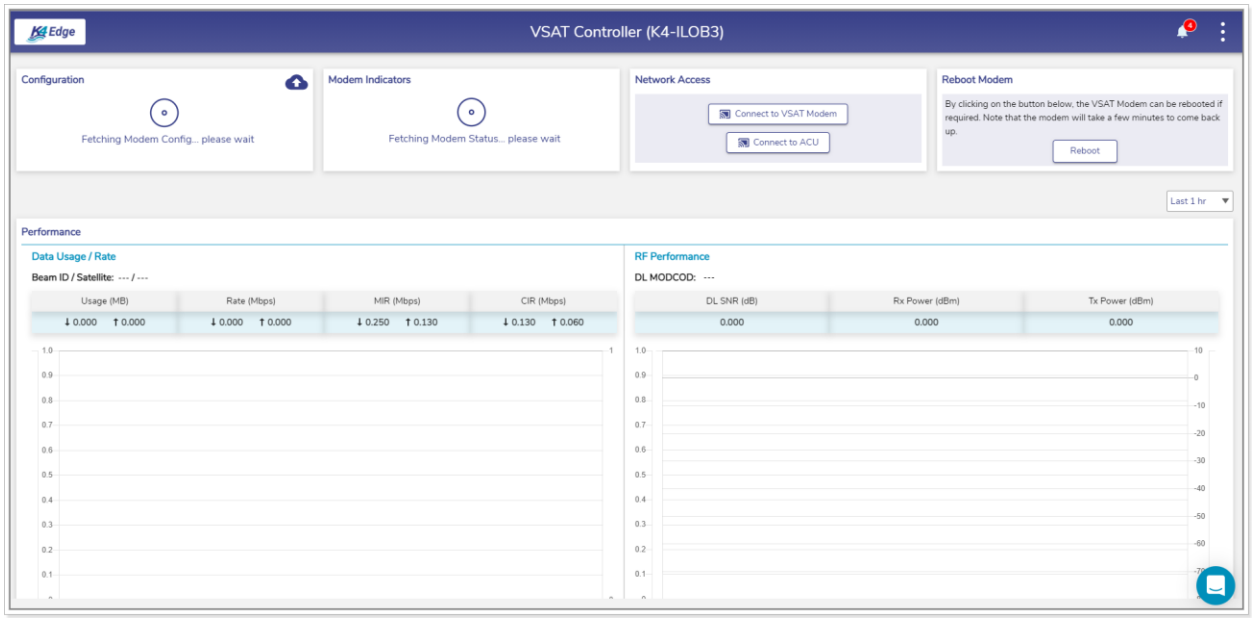


Figure 3-18 VSAT Controller

Table 3-4 VSAT Controller Information

Fields	Description	Configuration
Configuration	Following details of the VSAT Controller becomes available. • VSAT modem serial number • VSAT modem software version • Date and time when the details were uploaded	To upload the new configuration file of the VSAT modem, click  and then upload the configuration file.
Modem Indicators	Following details of the VSAT modem becomes available. • Receive (Rx) status • Transmit (Tx) status • Network status	
Network Access	To access the VSAT modem and ACU.	To connect to the VSAT modem, click **Connect to VSAT Modem**. Or, To connect the ACU, click **Connect to ACU**.
Reboot Modem		To reboot the VSAT modem, click **Reboot**.

To draw the performance chart basis on the periodicity, in the periodicity list click a periodicity. The following details become available under the **Performance** section.

- Data Usage / Rate
  - Beam ID / Satellite
  - Usage (MB)
  - Rate (Mbps)
  - MIR (Mbps)
  - CIR (Mbps)
- RF (VSAT Modem) Performance
  - Modulation constellation (MODCOD). This indicates the constellation and FEC code rate.
  - DL SNR (dB)

- Receive (Rx) power (dBm). >=-60 dBm is a good Rx power.
- Transit (Tx) power (dBm). >=30 is a good Tx power.

For VSAT signal strength, see *Table 3-5*.

Table 3-5 VSAT Signal Strength

Signal Strength Range	Status
Signal-to-Noise (SNR) Margin dB	
29dB and more	Excellent
20dB – 28dB	Better
11db – 20dB	Good
10dB and below is bad	Poor
Receive (Rx) Power dBm	
Transmit (Tx) Power dBm	

3.2.8 LTE Controller

Once the K4 Edge is configured, you can view analytics from the LTE modem connected to the Edge Server.

To manage the LTE controller, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.

3. Click **LTE Controller**. The **LTE Controller** page appears, see *Figure 3-19*. For details about the LTE controller, see *Table 3-6*.

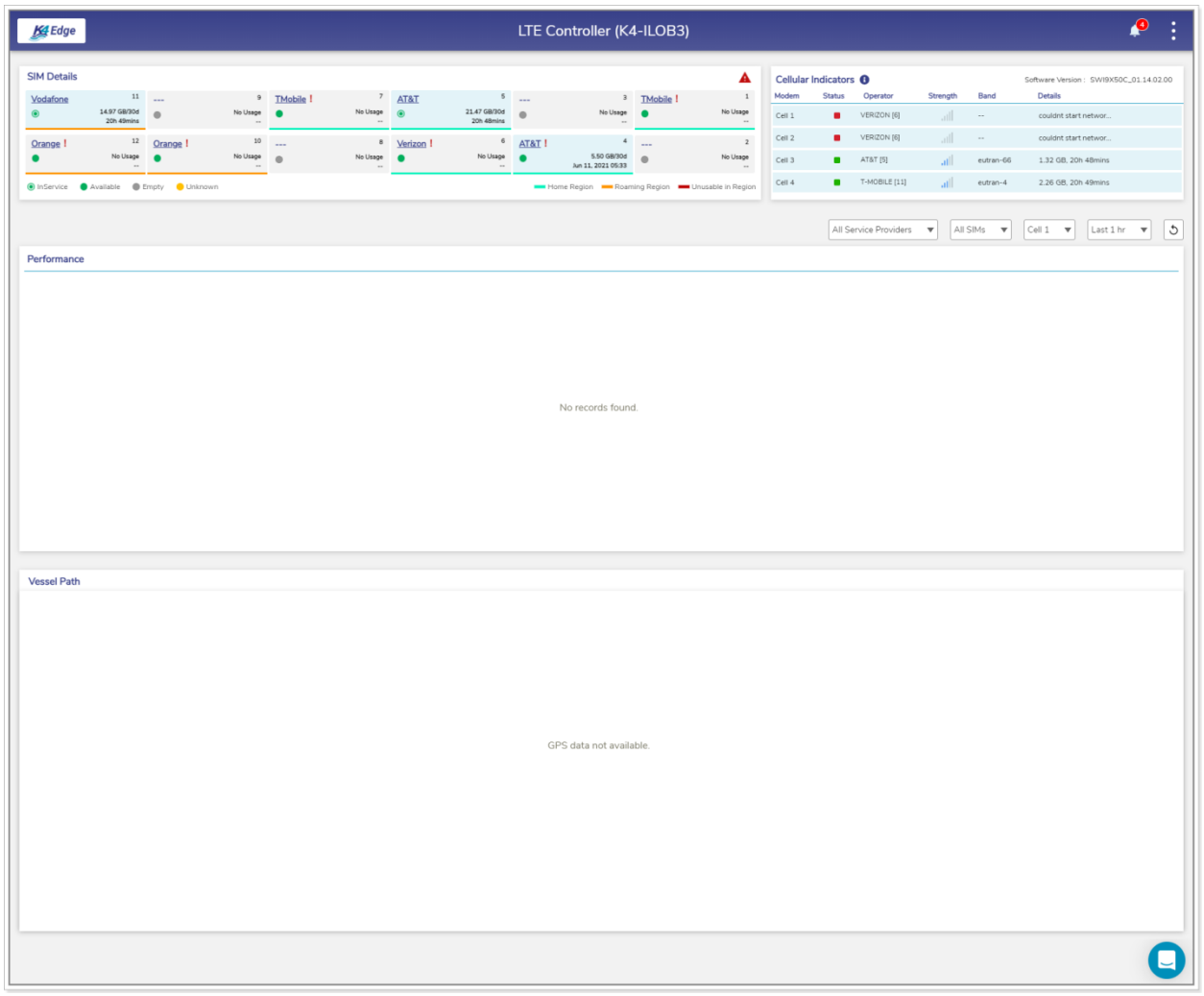


Figure 3-19 LTE Controller

Figure 3-20 Performance Chart

Return

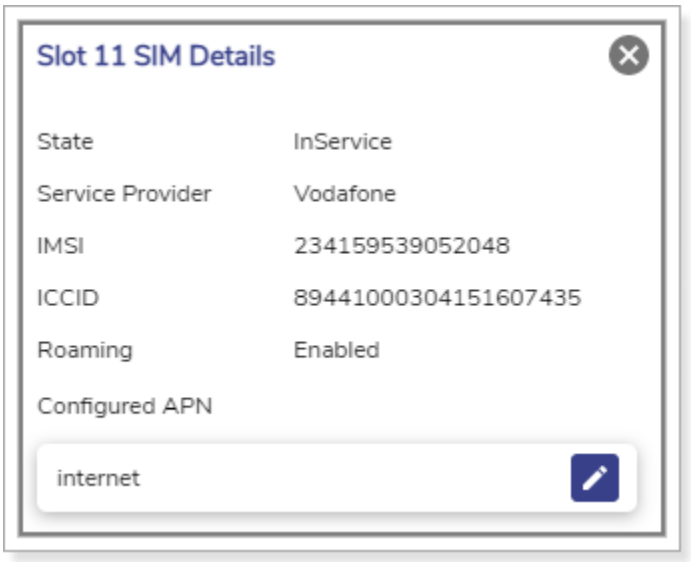


Figure 3-21 SIM Details

Return

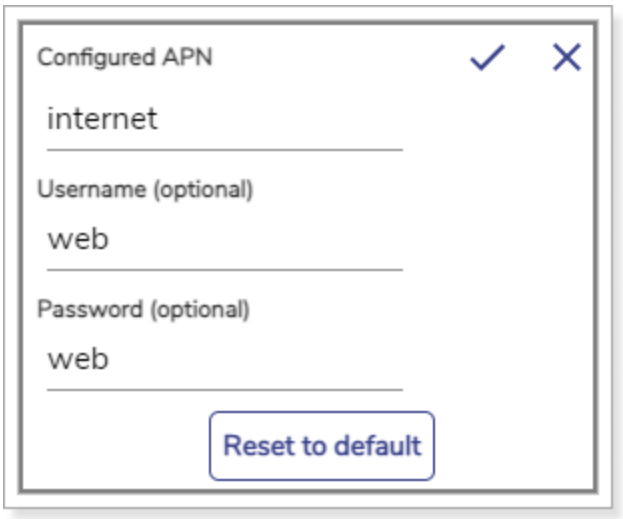


Figure 3-22 Configured APN

Return

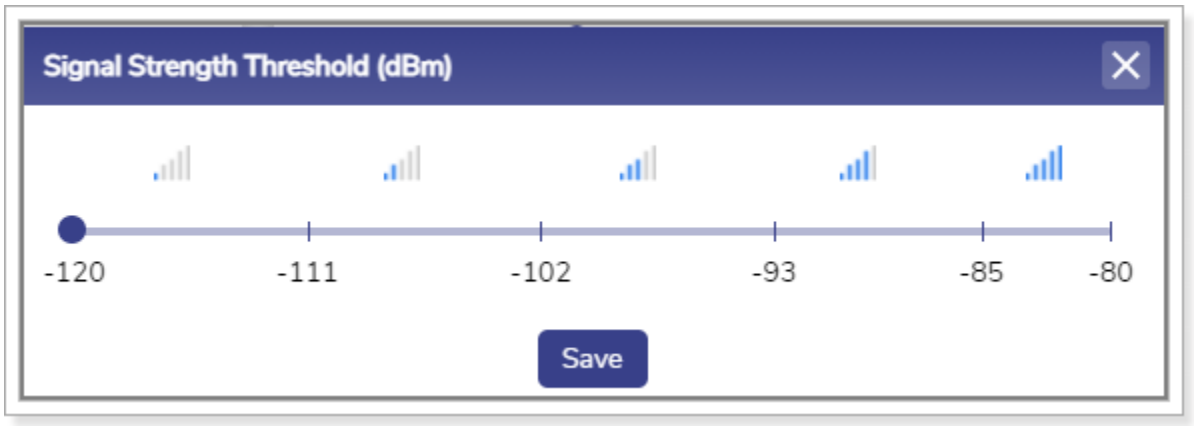


Figure 3-23 Signal Strength Threshold

Return

Figure 3-24 Signal Alert

Return

Table 3-6 LTE Controller Information

Fields	Description	Configuration
SIM Details		
SIM Details	Details about the SIM per SIM slot are available. Following are the statuses of the SIM. • . InService. This indicates that the SIM is in use. • . Available. This indicates that the SIM is available, but it is not in use. • . Empty. This indicates that the SIM is ready to use. • . Unknown. This indicates that the SIM is available in the slot but details about that SIM are not available in the database.	To view the performance chart basis on the data usage and signal strength, click the SIM details section. The chart becomes available, see *Figure 3-20*. To view details about a SIM, click the service provider in the SIM details section. The **Slot SIM Details** pop up window appears, see *Figure 3-21*. **To modify the APN, perform the following steps.** 1. Click . The **Configured APN** section becomes available, see *Figure 3-22*. 2. Modify the details and then click . Or, To reset the APN to default, click **Reset to default**. The APN is reset to the default configuration.

Fields	Description	Configuration
SIM Details		
	Provides information about the SIMs not available in the slot. However, details about the SIMs are available in the database.	To view details about the missing SIMs, click  . A list of the missing SIMs is displayed.
Cellular Indicators		
Modem	List of the LTE modems.	NA
Status	Status of the respective modem displays. Where, Red square indicates that the modem is inactive and not in use. Green Square indicates that the modem is active and in use.	NA
Operator	• List of the operator displays. • Slot number of the SIM of the operator displays in the square bracket. This is an example. VERIZON [6]	NA
Strength	• The strength of the signal is displayed. • You can configure the signal strength threshold. If the current signal strength is less than the signal strength threshold, then the signal strength is considered as bad signal strength.	**To configure the signal strength threshold, perform the following steps.** 1. Click  to the corresponding **Cellular Indicators**. The **Signal Strength Threshold (dBm)** pop up window appears, see *Figure 3-23*. **NOTE:** dBm stands for decibels per milliwatt and dB stands for decibels.

Fields	Description	Configuration
SIM Details		
	Therefore, the network having the signal strength more than the signal strength threshold is searched. Or, If the current signal strength is more than the signal strength threshold, then the signal strength is considered as good signal strength.	2. Click the signal strength. 3. Click **Save**. The **Alert** pop up window is displayed, see *Figure 3-24*. 4. Click **OK**. The signal strength threshold is updated. To view the signal strength of the cell, point the mouse to the signal under the **Strength** field.
Band	The band of the signal is displayed.	NA
Details	If the modem is active, then the quantum of the data consumed with duration is displayed. Otherwise, the status of the operator is displayed.	NA

The Vessel Path displays the path traveled by vessel.

To view the performance chart of the service providers, in the **All Service Providers** list, click a service provider.

To view the performance chart of the SIM, in the **All SIMs** list, click a SIM.

To view the performance chart of the cellular, in the **All Cellular** list, click a cell. The data usage rate chart and signal strength chart become available under the **Performance** section. For details about the signal strength, see *Table 3-7*.

Table 3-7 LTE Signal Strength

Signal Strength Range	Status
Reference Signal Received Power (RSRP) dBm	
-80 or near to zero (0)	Excellent
-80 to -90	Good

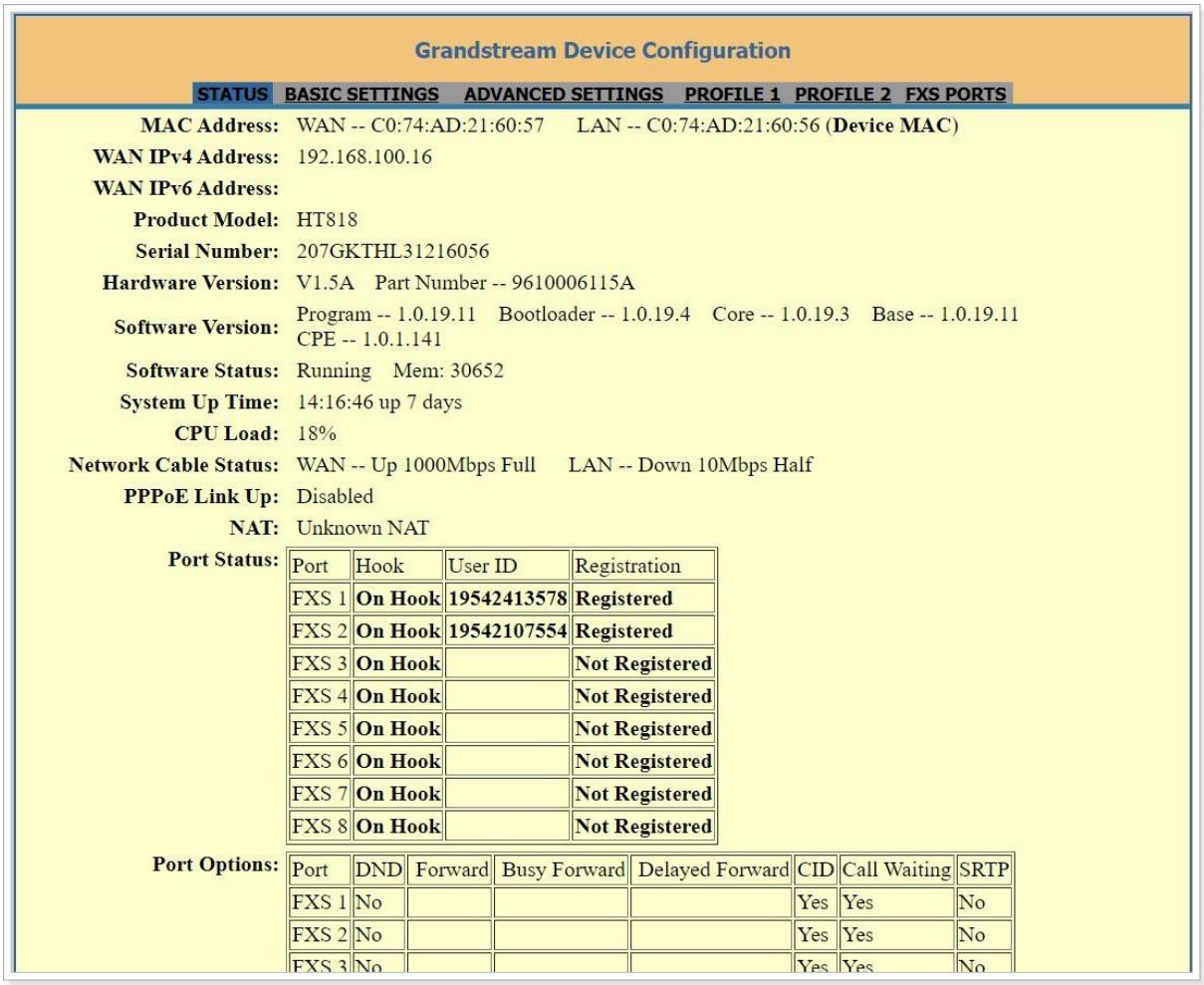
Signal Strength Range	Status
-90 to -100	Mid Cell
-100 or less	Poor
Reference Signal Received Quality (RSRQ) dB	
-10 or near to zero (0)	Excellent
-10 to -15	Good
-15 to -20	Mid Cell
-20 or less	Poor
Signal to Interference & Noise Ratio (SINR) dB	
>=20	Excellent
13 to 20	Good
0 to 13	Mid Cell
<=0	Poor

3.2.9 VoIP Controller

Once the K4 Edge is configured, you can view analytics from the LTE modem connected to the Edge Server.

To manage the LTE controller, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **VoIP Controller**. The **Grandstream Device Configuration** page appears.
4. Click the **STATUS** tab. The **STATUS** configuration page appears, see *Figure 3-25*.



Grandstream Device Configuration

STATUS | BASIC SETTINGS | ADVANCED SETTINGS | PROFILE 1 | PROFILE 2 | FXS PORTS

MAC Address: WAN -- C0:74:AD:21:60:57 LAN -- C0:74:AD:21:60:56 (**Device MAC**)

WAN IPv4 Address: 192.168.100.16

WAN IPv6 Address:

Product Model: HT818

Serial Number: 207GKTHL31216056

Hardware Version: V1.5A Part Number -- 9610006115A

Software Version: Program -- 1.0.19.11 Bootloader -- 1.0.19.4 Core -- 1.0.19.3 Base -- 1.0.19.11
CPE -- 1.0.1.141

Software Status: Running Mem: 30652

System Up Time: 14:16:46 up 7 days

CPU Load: 18%

Network Cable Status: WAN -- Up 1000Mbps Full LAN -- Down 10Mbps Half

PPPoE Link Up: Disabled

NAT: Unknown NAT

Port Status:

Port	Hook	User ID	Registration
FXS 1	**On Hook**	**19542413578**	**Registered**
FXS 2	**On Hook**	**19542107554**	**Registered**
FXS 3	**On Hook**		**Not Registered**
FXS 4	**On Hook**		**Not Registered**
FXS 5	**On Hook**		**Not Registered**
FXS 6	**On Hook**		**Not Registered**
FXS 7	**On Hook**		**Not Registered**
FXS 8	**On Hook**		**Not Registered**

Port Options:

Port	DND	Forward	Busy Forward	Delayed Forward	CID	Call Waiting	SRTP
FXS 1	No				Yes	Yes	No
FXS 2	No				Yes	Yes	No
FXS 3	No				Yes	Yes	No

Figure 3-25 Configure Status of VoIP Adapter

NOTE: For details about the Grandstream VoIP adapter, see *Voice over Internet Protocol Interface* on page 23.

5. Configure the status of the device.
6. Click the **PROFILE1** tab. The **PROFILE1** configuration page appears, see *Figure 3-26*.

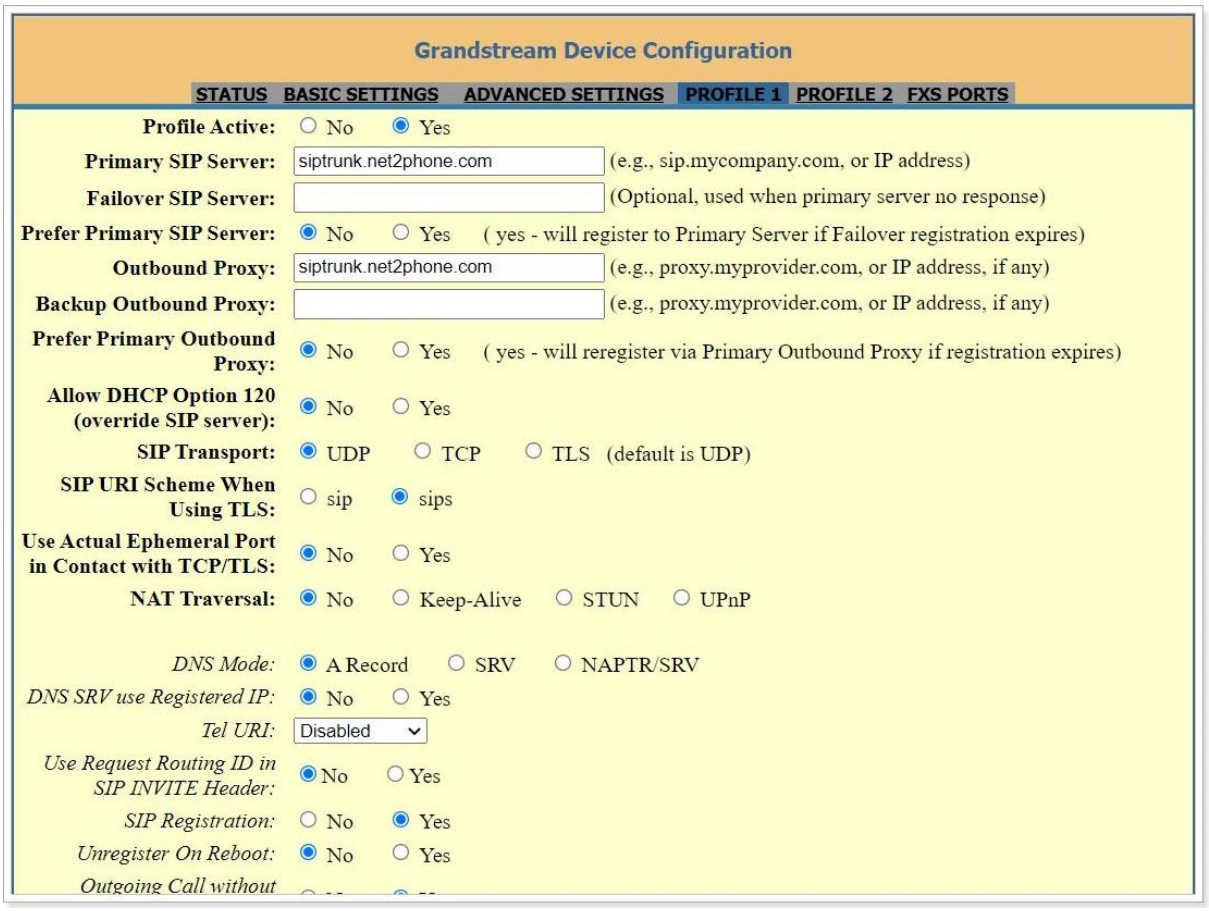


Figure 3-26 Configure Profile1 of VoIP Adapter

7. Configure the first profile of the device.
8. Click the **PROFILE2** tab. The **PROFILE2** configuration page appears, see *Figure 3-27*.

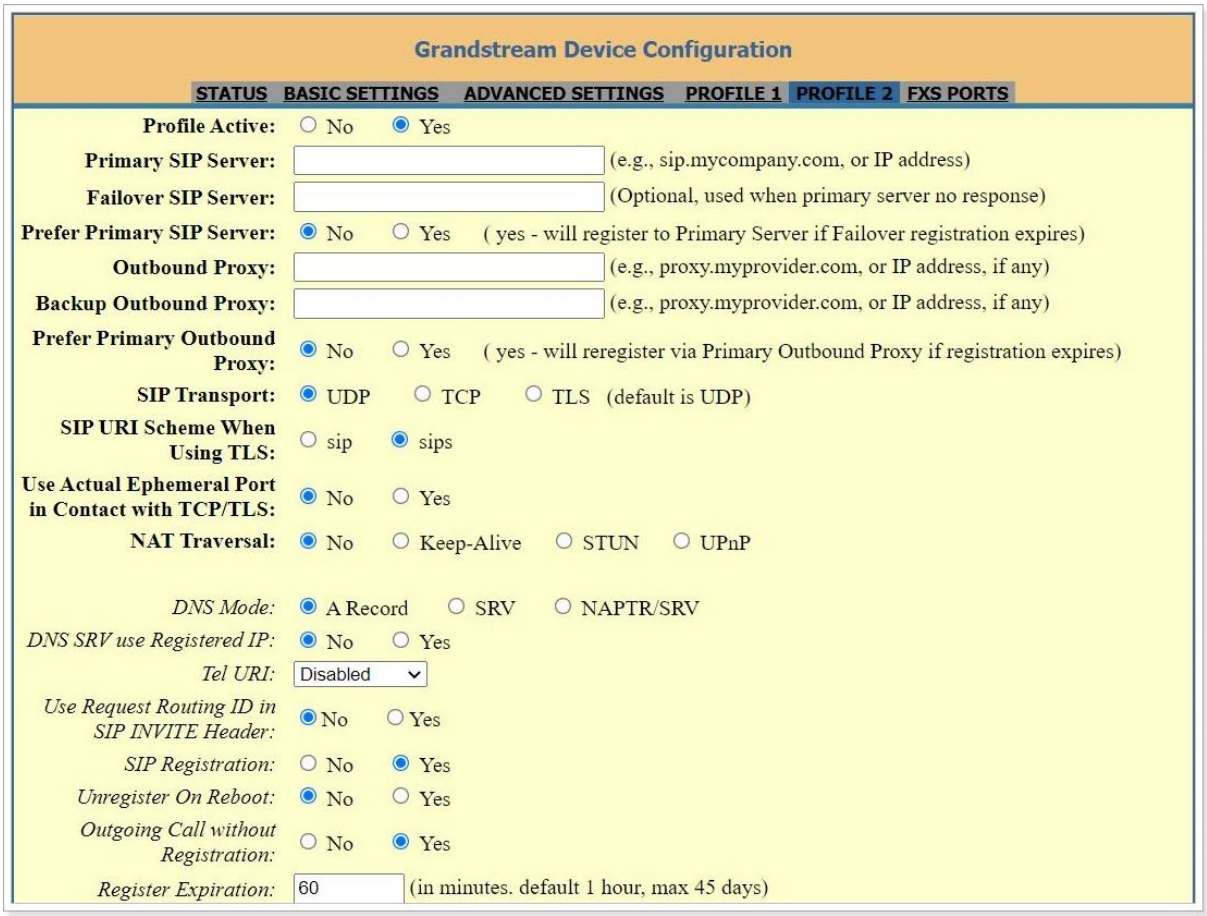


Figure 3-27 Configure Profile2 of VoIP Adapter

9. Configure the second profile of the device.

10. Click the **FXS PORTS** tab. The **FXS PORTS** configuration page appears, see *Figure 3-28*.

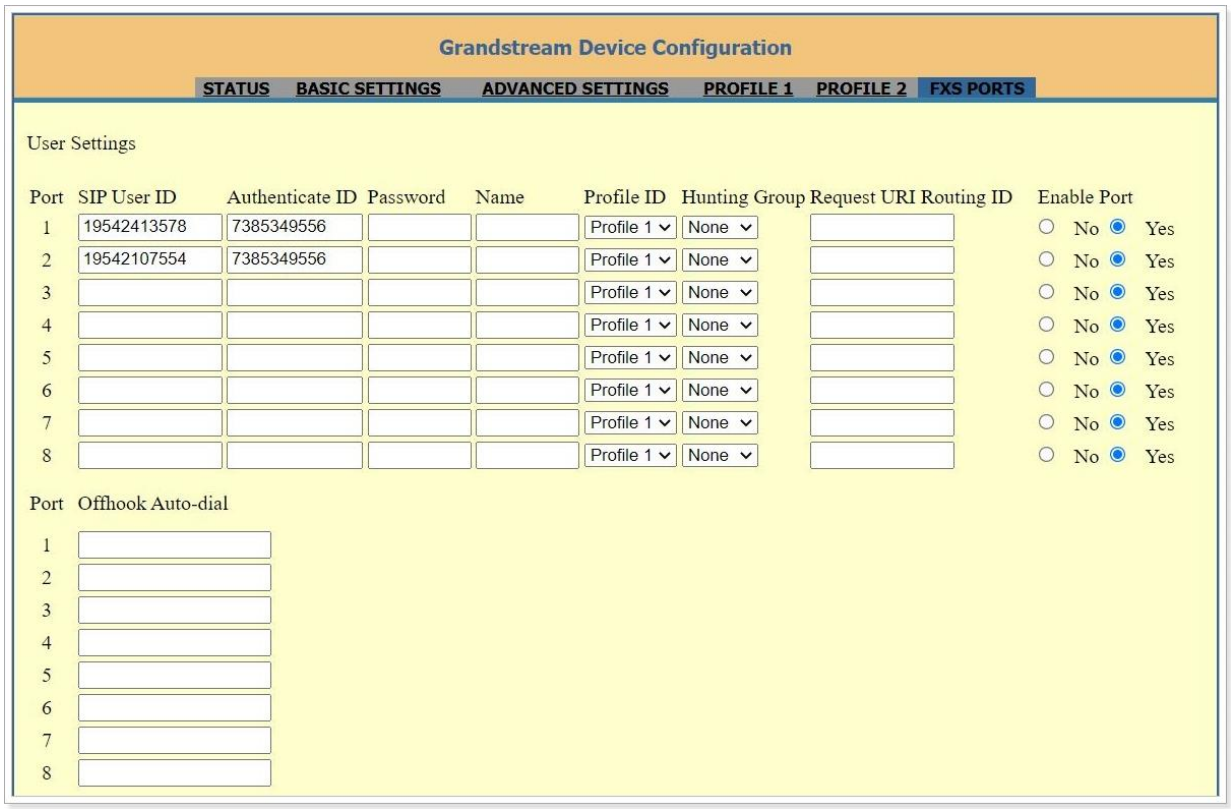


Figure 3-28 Configure FXS Ports of VoIP Adapter

The VoIP adapter is configured successfully, and the K4 Edge configuration wizard becomes available.

4 Debugging

You can debug or troubleshoot the common issues that arise on the vessel

4.1 Client cannot connect to the network

If the MAC address of the device of the client is not assigned to the network, then the client cannot connect to the network.

To verify whether the MAC address of the device is assigned to the network, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Configuration Wizard**. The home page appears, see *Figure 2-3*.
4. Click **Access Networks**. The **Access Networks** page appears, see *Figure 2-12*.
5. Perform steps to view network usage. For details, see *Viewing Network Usage Data* on page *54*.

   If the MAC address of the device is unavailable, then the client cannot connect to the network.

However, you can view the historical details about the network and device to verify whether the MAC address of the device is assigned to the network.

To view the historical details about the network, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-13*.
4. Perform steps to view details about the network and device. For details, see Top Networks on page 96 and Top Devices on page 99.

   If the MAC address of the device is unavailable, then the client cannot connect to the network.

4.2 Client cannot access the internet

If the internet of a network is paused, then the entire device connected to that network cannot access the internet. If the internet of a specific device is paused, then that device cannot access the internet.

To verify the status of the internet of the network and device, perform the following steps.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-13*.
4. Verify whether the internet is paused for the network under the **Top Networks** section. If the internet is paused, then resume the internet. For details, see *Top Networks* on page 96.

   Or,

   Verify whether the internet is paused for the device under the **Top Devices** section. If the internet is paused, then resume the internet. For details, see *Top Devices* on page 99.

4.3 Client cannot access an application

If the application, or domain, or IP address of the domain is blocked while configuring the traffic policy, then the client cannot access the application.

To verify the device traffic policy, perform the following policy.

1. Log on to the K4 Edge server. The **Internet Status** page appears, see *Figure 3-1*.
2. Click vertical ellipsis, see *Figure 2-4*. The options become available, see *Figure 3-3*.
3. Click **Other Settings**. The **Other Settings** page appears, see *Figure 2-35*.
4. Access the **Device Traffic Policies** section.
5. Verify the device traffic policy.
6. Click **Traffic Policies**. The **Traffic Profiles** page appears, see *Figure 2-30*.
7. Click **Device**.
8. Click  to the corresponding traffic policy.
9. Access the **Application Policy Profile** section.

Verify the rules configured and allow the application.

Index