11.12 Syslog Configuration

Logs relevant to the UBR application software are displayed in the Diagnostic/System Log screen for monitoring purpose. The same can be uploaded to an external server and the configuration for the same is performed in this screen. Event messages or corresponding messages will be sent to the logging server based on the configured log level. A basic overview of the Syslog Configuration screen is given below:

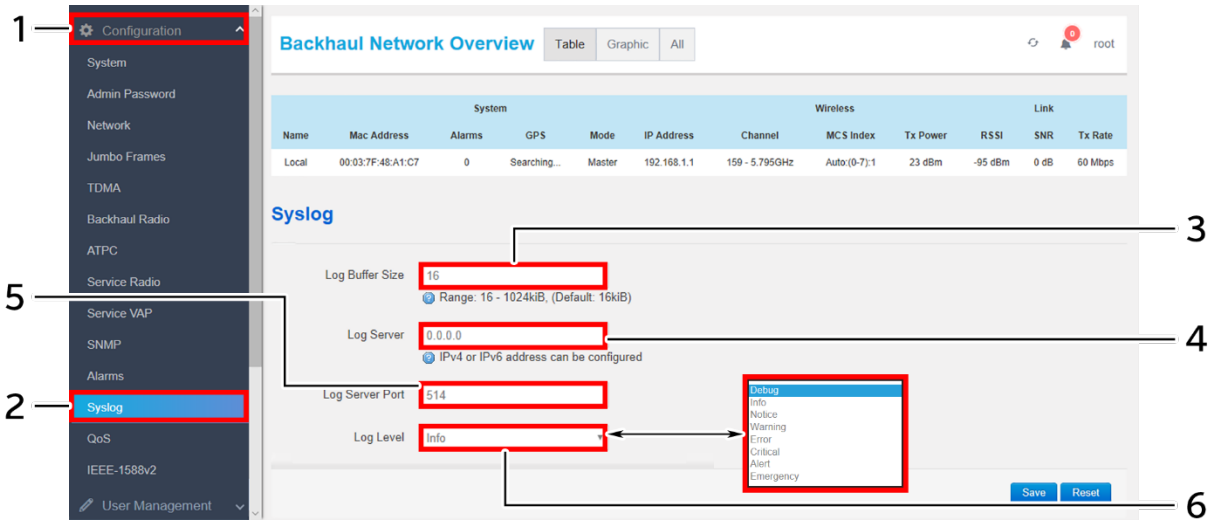

Figure 48: Basic overview of the Syslog Configuration screen

Follow the steps given below and configure the Syslog settings for the UBR:

Table 40: List of actions to configure the Syslog settings

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Syslog	Click on "Syslog" option
3.	Log Buffer Size	Enter the value for "System log buffer size". This options determine the size of the log to be displayed in system log screen. Once the log size has reached the "System log buffer size" limit (16-1024 kiB), only new logs are displayed in the GUI and old logs are discarded. Logs are uploaded at external server at all time irrespective of the buffer size.
4.	Log Server	Enter the "External system log server" address. The system logs are uploaded to the external server on regular interval if the external server is specified with this option
5.	Log server port	Enter the "Log server port" number
6.	Log output level	Select the "Log output level" from the dropdown list (Debug/Info/Notice/Warning/Error/Critical/Alert/Emergency). Categorization of the system logs is specified in the backend. The selection of "Log output level" determines the type of logs to be displayed in system log screen. The "Debug" option shows all of the system logs. E.g.: If "Debug" is selected, all logs from debug to emergency will be logged and if "Notice" is selected, logs from Notice to Emergency will be logged

Click "Save" to save the Syslog configuration or click "Reset" to configure the same again.

11.13 Configuration of traffic management (Quality of Service)

Quality of service (QoS) involves controlling and managing network traffic by setting priorities for specific types of data (background, best effort, video, and audio traffic) on the network. IEEE P802.1p is the name of a task group that provides a mechanism for implementing quality of service (QoS) at the media access control (MAC) level.

Quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic.

DSCP is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks. It provides low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.

11.13.1 VLAN QoS with Default Policy

A basic overview of the VLAN QoS Configuration screen with default policy is given below:

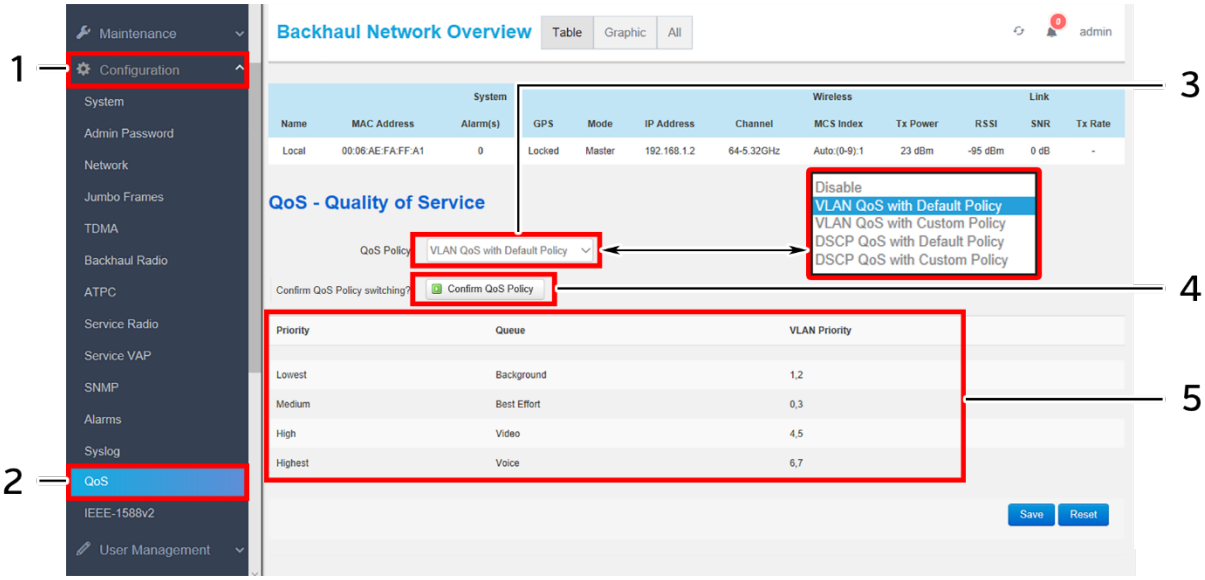

Figure 49: Basic overview of the VLAN QoS Configuration screen with default policy

Follow the steps given below and configure the VLAN QoS with default policy for the UBR:

Table 41: List of actions to configure the VLAN QoS with default policy

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	QoS	Click on "QoS" option
3.	QoS Policy	Set the QoS policy to "VLAN QoS with Default Policy" from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/

Callout	Name	Description
		DSCP QoS with Default Policy/ DSCP QoS with Custom Policy)
4.	Confirm QoS Policy switching	Click on "Confirm Qos Policy" option to change the QoS policy
5.	Default VLAN Priority	Displays the default VLAN priority for voice, video, best effort, and background traffic queues

Refer the above figure to check the priority levels for voice, video, best effort, and background traffic queues. Click "Save" to save the QoS configuration or click "Reset" to configure the same again.

11.13.2 VLAN QoS with Custom Policy

A basic overview of the VLAN QoS Configuration screen with custom policy is given below:

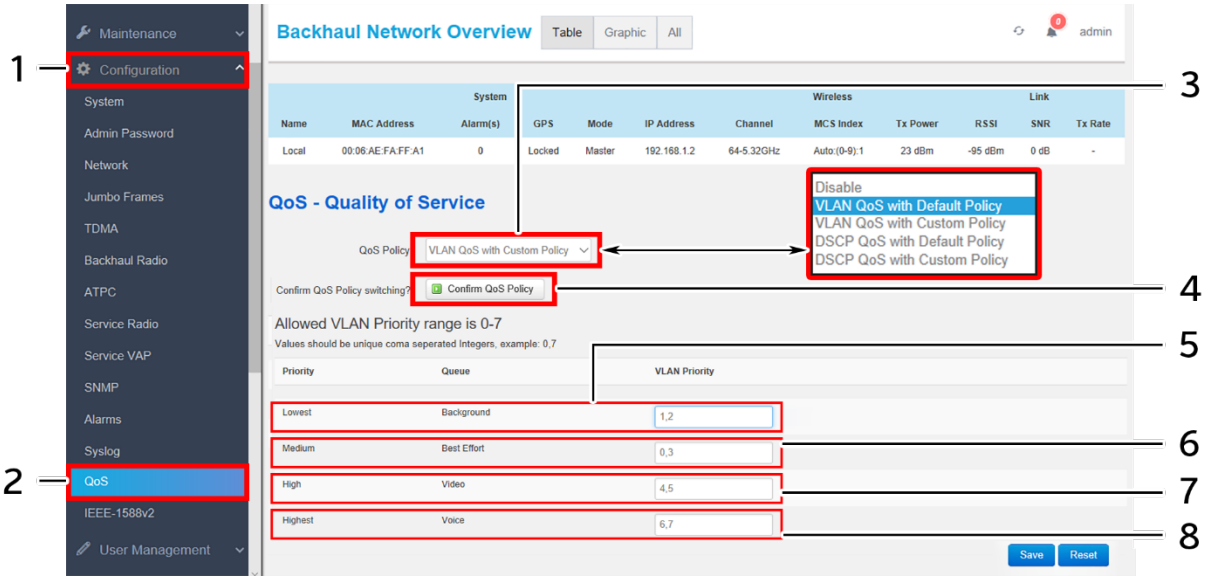

Figure 50: Basic overview of the VLAN QoS Configuration screen with custom policy

Follow the steps given below and configure the VLAN QoS with custom policy for the UBR:

Table 42: List of actions to configure the VLAN QoS with custom policy

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	QoS	Click on "QoS" option
3.	QoS Policy	Set the QoS policy to "VLAN QoS with Custom Policy" from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/ DSCP QoS with Default Policy/ DSCP QoS with Custom Policy)
4.	Confirm QoS Policy switching	Click on "Confirm Qos Policy" option to change the QoS policy
5.	VLAN-Lowest-Background	Set the VLAN priority value for background traffic queue
6.	VLAN-Medium- Best Effort	Set the VLAN priority value for best effort traffic queue
7.	VLAN-High-Video	Set the VLAN value for video traffic queue
8.	VLAN-Highest-Voice	Set the VLAN value for voice traffic queue

Refer the above figure to check the priority levels for voice, video, best effort, and background traffic queues. Click "Save" to save the QoS configuration or click "Reset" to configure the same again.

11.13.3 DSCP QoS with Default Policy

A basic overview of the DSCP QoS Configuration screen with default policy is given below:

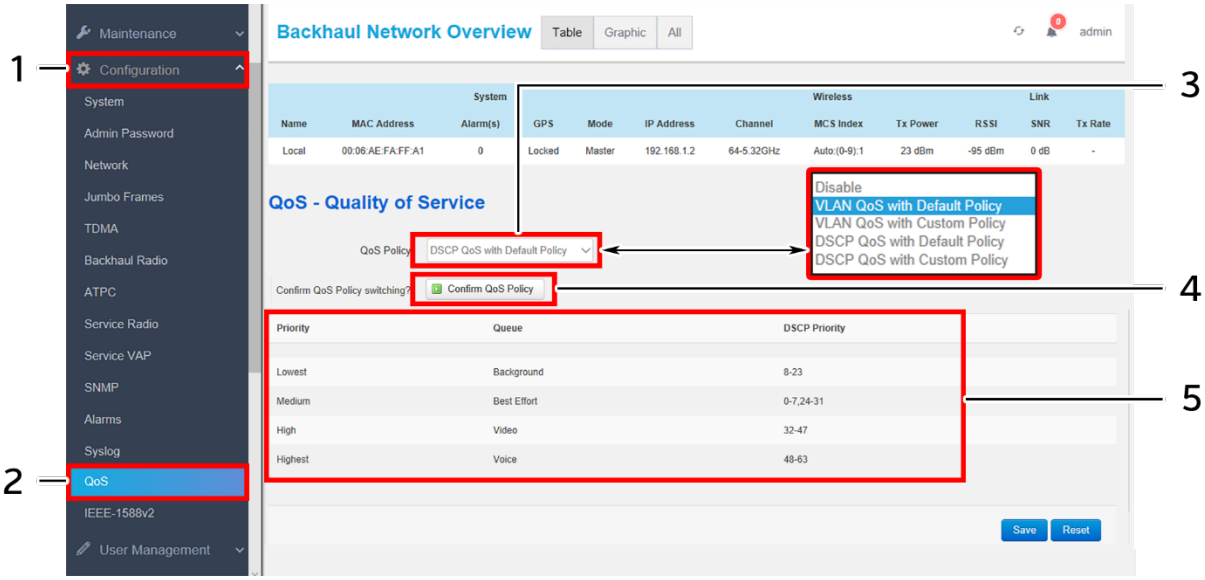

Figure 51: Basic overview of the DSCP QoS Configuration screen with default policy

Follow the steps given below and configure the DSCP QoS with default policy for the UBR:

Table 43: List of actions to configure the DSCP QoS with default policy

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	QoS	Click on "QoS" option
3.	QoS Policy	Set the QoS policy to "DSCP QoS with Default Policy" from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/ DSCP QoS with Default Policy/ DSCP QoS with Custom Policy)
4.	Confirm QoS Policy switching	Click on "Confirm Qos Policy" option to change the QoS policy
5.	Default DSCP Priority	Displays the default DSCP priority for voice, video, best effort, and background traffic queues

Refer the above figure to check the priority levels for voice, video, best effort, and background traffic queues. Click "Save" to save the QoS configuration or click "Reset" to configure the same again.

11.13.4 DSCP QoS with Custom Policy

A basic overview of the DSCP QoS Configuration screen with custom policy is given below:

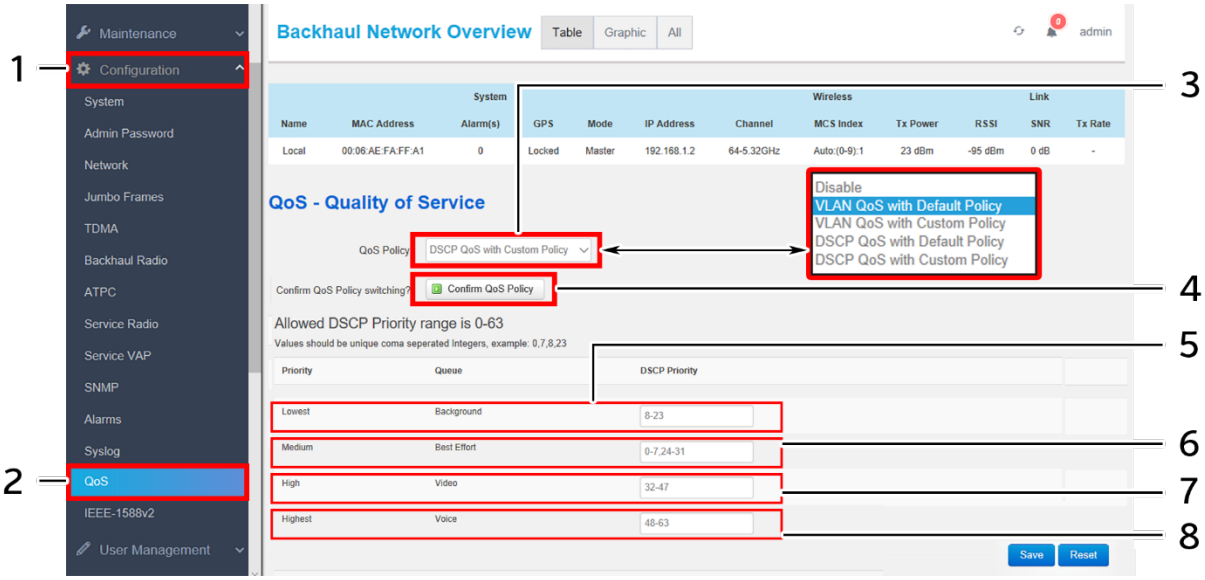

Figure 52: Basic overview of the DSCP QoS Configuration screen with custom policy

Follow the steps given below and configure the DSCP QoS with custom policy for the UBR:

Table 44: List of actions to configure the DSCP QoS with custom policy

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	QoS	Click on "QoS" option
3.	QoS Policy	Set the QoS policy to "DSCP QoS with Custom Policy" from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/ DSCP QoS with Default Policy/ DSCP QoS with Custom Policy)
4.	Confirm QoS Policy switching	Click on "Confirm Qos Policy" option to change the QoS policy
5.	DSCP-Lowest-Background	Set the DSCP priority value for background traffic queue
6.	DSCP-Medium- Best Effort	Set the DSCP priority value for best effort traffic queue
7.	DSCP-High-Video	Set the DSCP value for video traffic queue
8.	DSCP-Highest-Voice	Set the DSCP value for voice traffic queue

Refer the above figure to check the priority levels for voice, video, best effort, and background traffic queues. Click "Save" to save the QoS configuration or click "Reset" to configure the same again.

11.14 IEEE-1588v2 Grand-Master Configuration

The Grandmaster Clock supports IEEE-1588 PTP Version 2 and delivers Nano-second time and frequency synchronization for customer network environment. PTP Grandmaster Clocks not only provides a highly accurate source of synchronization for PTP (Precision Time Protocol) networks but also provide ToD (Time-of-Day) and Frequency Synchronization. The grand master gets the initial time synchronization updates from the GPS.

The 4x4 UBR device support both one step and two step clocking mode to comply with Precision Time Protocol. One step clocking mode updates the time delay on the fly itself with the transmitted data packet and is recommended with L4 sync mode for better performance. Configuration choice is dependent on the type of participating devices in the network.

A basic overview of IEEE-1588v2 Grand-Master Configuration screen is given below:

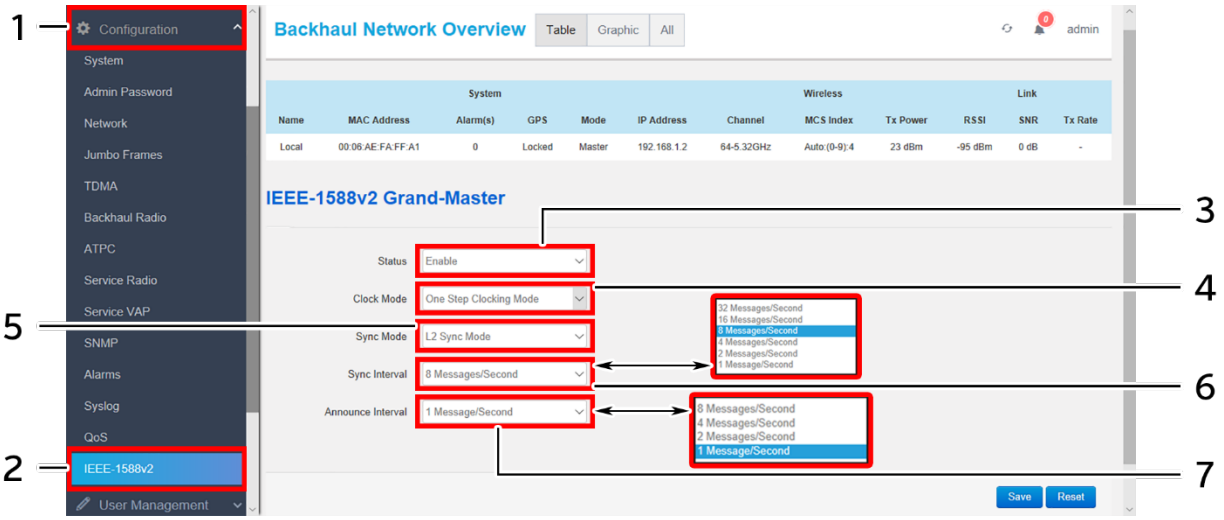

Figure 53: Basic overview of IEEE-1588v2 Grand-Master Configuration screen

Follow the steps below to configure the IEEE-1588v2 Grand-Master settings:

Table 45: List of actions to configure the IEEE-1588v2 Grand-Master

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	IEEE-1588v2	Click on "IEEE-1588v2" option
3.	Status	Enable/Disable the "IEEE-1588v2" feature. Provide following parameters if enabled
4.	Clock Mode	Select the "Clock Mode" to one step clocking mode or 2 step clocking mode from the dropdown list
5.	Sync Mode	Select the "Sync Mode" to L2 sync mode or L4 sync mode from the dropdown list
6.	Sync Interval	Select the "Sync Interval" from the dropdown list (32/16/8/4/2/1 messages per second). This parameter defines the number of messages sent in a second to synchronize clocks across the network
7.	Announce interval	Select the "Announce interval" from the dropdown list (8/4/2/1 messages per second). The grandmaster clock declares its availability across the network by sending defined number of messages every second

Click "Save" to save the IEEE-1588v2 Grand-Master configuration or click "Reset" to configure the same again.

12 User Management

The UBR GUI is designed with options to add multiple users. Added users can be configured with different access capabilities. The admin can add a new user, delete the existing one, and can even change the user's access to maintenance, configuration, and diagnostics screens or their further options.

A Basic overview of the user management screen is given below:

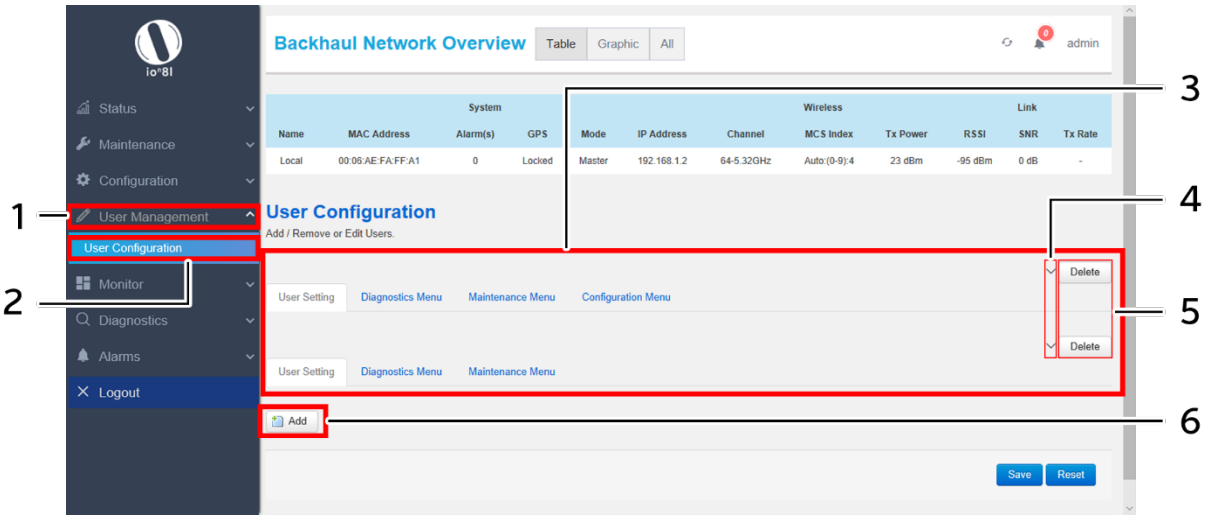

Figure 54: Basic overview of user configuration screen

Follow the steps below to view the list of added users:

Table 46: List of actions to view the list of added users

Callout	Name	Description
1.	User Management	Click on "User Management" dropdown
2.	User Configuration	Click on "User Configuration" option
3.	User List	Displays the list of existing users
4.	Edit User Configuration	Click on the dropdown to view or edit the configuration of respective user. Refer "Add a new User" section below for user configuration parameters
5.	Delete	Click on "Delete" option of the respective user and remove the same from the list
6.	Add	Click on the "Add" option to configure a new user. Refer "Add a new User" section below for user configuration parameters

12.1 Add a new User

Refer "Figure 54: Basic overview of user configuration screen" and click on "Add" option (6). A basic overview of the user management screen to add a new user with managed access to diagnostics, maintenance, and configuration screens is given below:

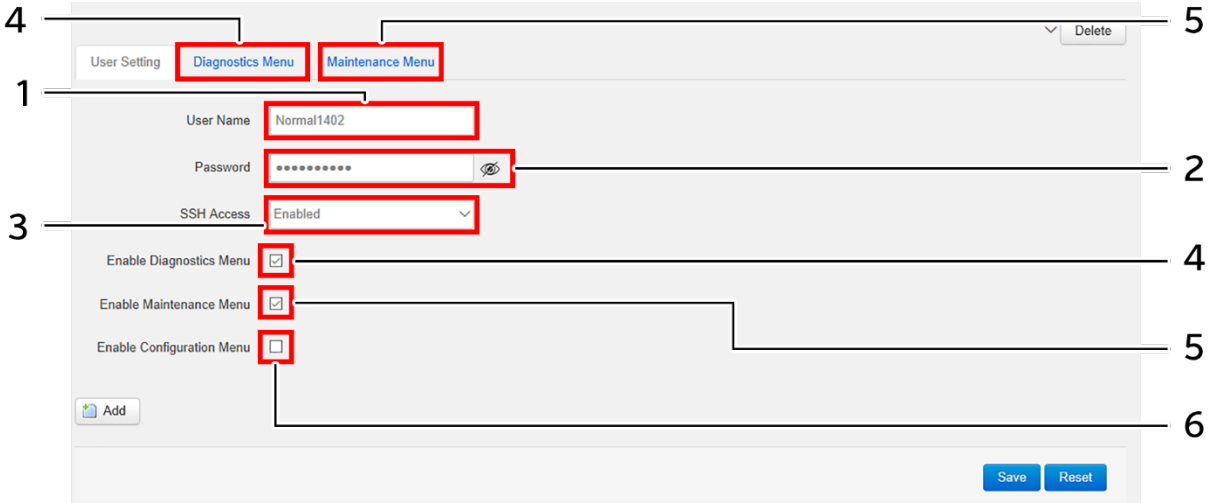

Figure 55: Basic overview of user configuration parameters

Follow the steps below to add a new user with managed access to diagnostics, maintenance, and configuration screens:

Table 47: List of actions to configure new user access and parameters

Callout	Name	Description
1.	User Name	Enter a unique name for the user
2.	Password	Enter a unique password for the respective user
3.	SSH Access	Enable/Disable the SSH access for the user
4.	Enable Diagnostics Menu	This check box is provided to allow or restrict the user to access diagnostic screen and its features. Click and select the check box to allow the user to access the diagnostics screen or uncheck the box to restrict the user from accessing the same. If the check box is selected a diagnostic tab gets added on top as shown in above figure. The user's access to the diagnostic screen is further manageable through this tab. Refer "User Access Configuration to Diagnostics screen options" for more details
5.	Enable Maintenance Menu	This check box is provided to allow or restrict the user to access maintenance screen and its features. Click and select the check box to allow the user to access the maintenance screen or uncheck the box to restrict the user from accessing the same. If the check box is selected a maintenance tab gets added on top as shown in above figure. The user's access to the maintenance screen is further manageable through this tab. Refer

Callout	Name	Description
		"User Access Configuration to Maintenance screen options" for more details
6.	Enable Configuration Menu	This check box is provided to allow or restrict the user to access configuration screen and its features. Click and select the check box to allow the user to access the configuration screen or uncheck the box to restrict the user from accessing the same. If the check box is kept deselected as shown in above figure, no configuration tab gets added on top and the user is restricted from accessing the same. However, if the user is configured with access to configuration screen then access to the same is further manageable through the respective tab which gets added on top. Refer "User Access Configuration to Configuration screen options" for more details

Click "Save" to save the user configuration or click "Reset" to configure the same again.

12.1.1 User Access Configuration to Diagnostics screen options

This screen provides the user with options to further manage the access privileges of a newly added user to diagnostics screen options, if the respective user has been configured with access to diagnostics screen. Refer "Figure 55: Basic overview of user configuration parameters" and click on "Diagnostic Menu" tab (4) located on top.

A basic overview of the screen to further manage the user access to diagnostic screen options is given below:

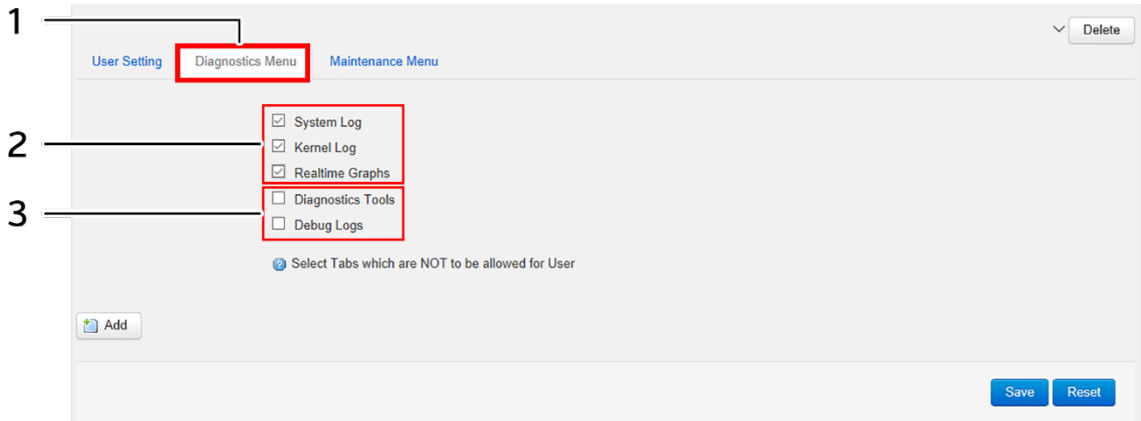

Figure 56: User configuration screen to further manage the user access to diagnostic screen options

Follow the steps below and further manage the user access to diagnostic screen options:

Table 48: List of actions to configure the user's access for maintenance screen options

Callout	Name	Description
1.	Diagnostics Menu	Click on "Diagnostics Menu" tab

Callout	Name	Description
2.	Allow Access	Click on the check box and select options available in diagnostics screen. The respective user will have access to selected screens
3.	Restrict Access	Click on the check box and deselect options available in diagnostics screen. The respective user will not have access to selected screens

Click “Save” to save the user configuration or click “Reset” to configure the same again.

12.1.2 User Access Configuration to Maintenance screen options

This screen provides the user with options to further manage the access privileges of a newly added user to maintenance screen options, if the respective user has been configured with access to maintenance screen. Refer "Figure 55: Basic overview of user configuration parameters" and click on "Maintenance Menu" tab (5) located on top.

A basic overview of the screen to further manage the user access to maintenance screen options is given below:

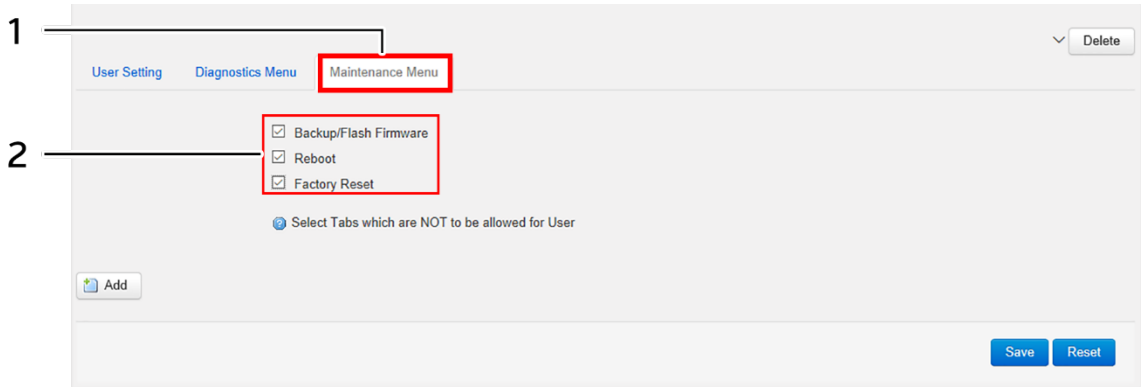

Figure 57: User configuration screen to further manage the user access to maintenance screen options

Follow the steps below and further manage the user access to maintenance screen options:

Table 49: List of actions to configure the user's access for maintenance screen options

Callout	Name	Description
1.	Maintenance Menu	Click on "Maintenance Menu" tab
2.	Allow Access	Click on the check box and select options available in maintenance screen. The respective user will have access to selected screens. Deselect the check box to restrict the user to access respective screens

Click "Save" to save the user configuration or click "Reset" to configure the same again.

12.1.3 User Access Configuration to Configuration screen options

This screen provides the user with options to further manage the access privileges of a newly added user to configuration screen options, if the respective user has been configured with access to configuration screen. Refer "Figure 55: Basic overview of user configuration parameters" and click on "Configuration Menu" tab (6).

A basic overview of the screen to further manage the user access to configuration screen options is given below:

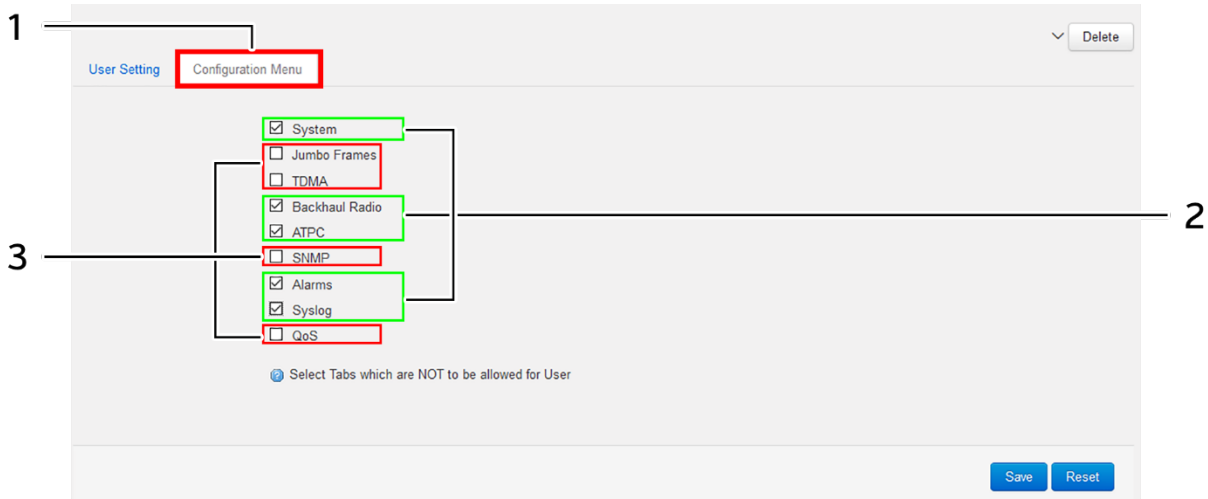

Figure 58: User configuration screen to further manage the user access to configuration screen options

Follow the steps below and further manage the user access to configuration screen options:

Table 50: List of actions to configure the user's access for configuration screen options

Callout	Name	Description
1.	Configuration Menu	Click on "Configuration Menu" tab
2.	Allow Access	Click on the check box and select options available in configuration screen. The respective user will have access to selected screens
3.	Restrict Access	Click on the check box and deselect options available in configuration screen. The respective user will not have access to selected screens

Click "Save" to save the user configuration or click "Reset" to configure the same again.

13 Monitor screen

The performance of the connected UBR is monitored from this screen. The list of options available for the user is given below:

1. Real-time Graphs/Load
2. Real-time Graphs/Traffic
3. Real-time Graphs/Signal & Noise
4. Real-time Graphs/Channel Interference
5. Real-time Graphs/Tx Power

13.1 Real-time Graphs/Load

The real time load graph shows the CPU load of last 3 min and the graph is refreshed at every 3 sec interval. In addition to the displayed graph the user can find the average and the peak CPU load values of the respective UBR.

A basic overview of the Real-time Graphs/Load screen is given below:

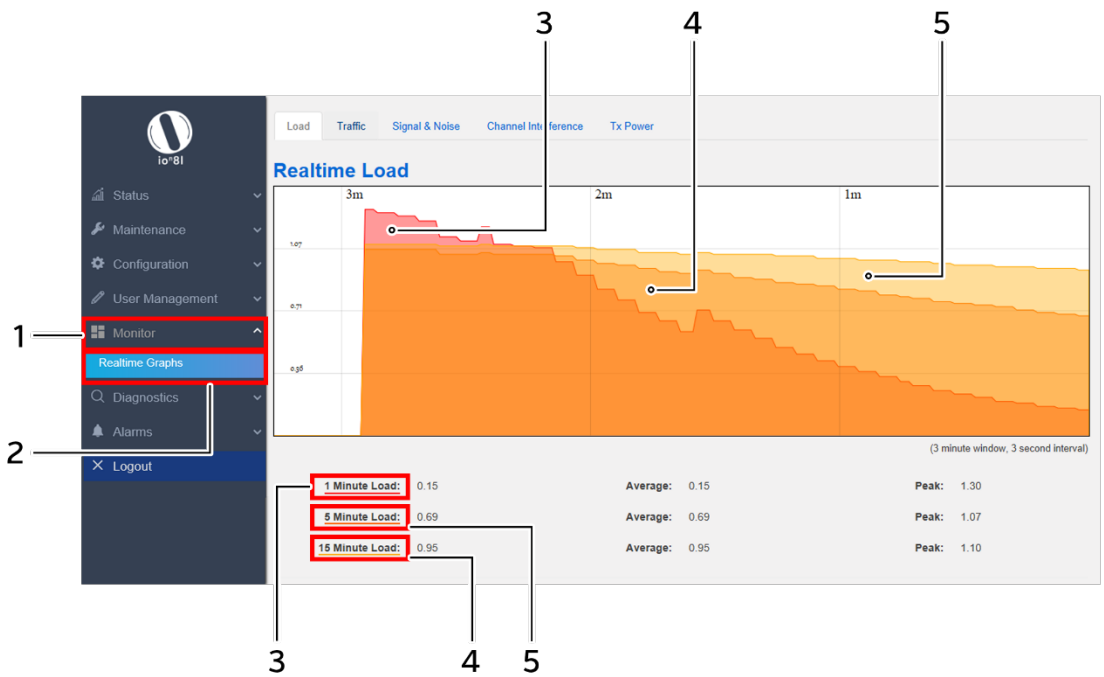

Figure 59: Basic overview of the Real-time Graphs/Load screen

Follow the steps given below to view the real-time load graphs for the UBR:

Table 51: List of actions to view real-time load graphs

Callout	Name	Description
1.	Monitor	Click on "Monitor" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	1 Minute Load	Displays the color coded load in last 1 minute
4.	5 Minute Load	Displays the color coded load in last 5 minute
5.	15 Minute Load	Displays the color coded load in last 15 minute

13.2 Real-time Graphs/Traffic

The real time traffic graph shows the traffic at backhaul interface, LAN interface and at Ethernet interface in last 3 min. The graph is refreshed at every 3 sec interval. In addition to the displayed graph the user can find the inbound and outbound traffic along with average and the peak traffic values of the respective UBR.

A basic overview of the Real-time Graphs/Traffic screen is given below:

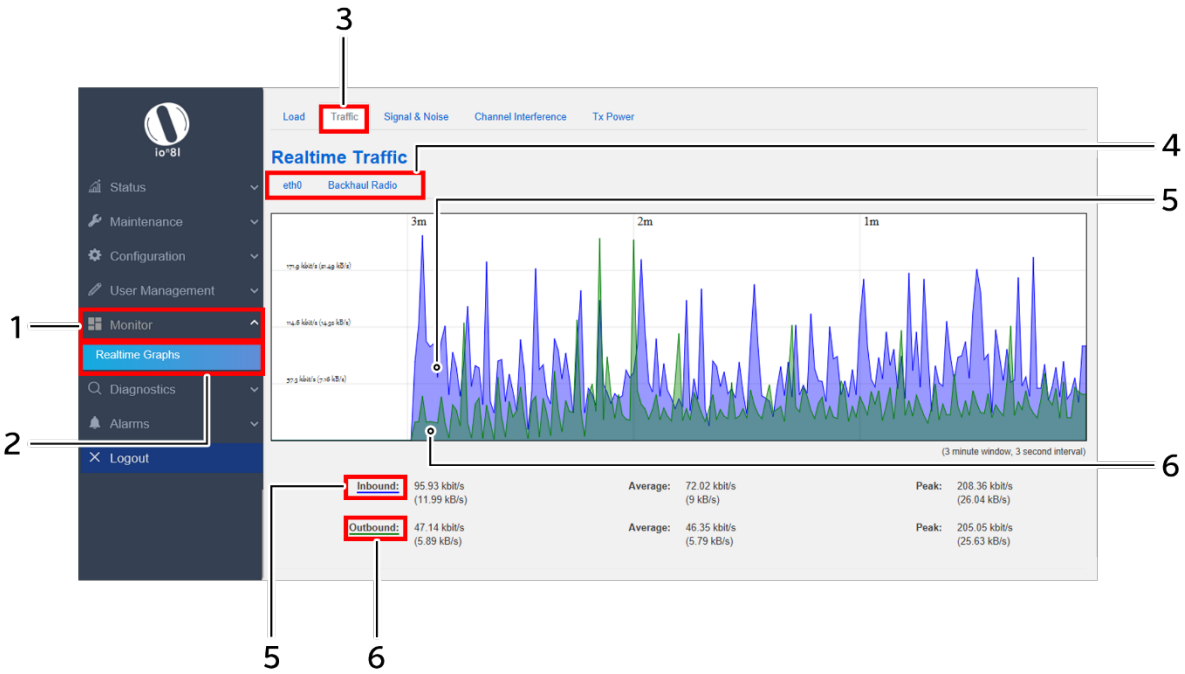

Figure 60: Basic overview of the Real-time Graphs/Traffic screen

Follow the steps given below to view the real-time traffic graphs for the UBR:

Table 52: List of actions to view real-time traffic graphs

Callout	Name	Description
1.	Monitor	Click on “Monitor” dropdown
2.	Real-time graphs	Click on “Real-time graphs” option
3.	Traffic	Click on “Traffic” option
4.	Real-time Traffic	Select the interface to check the traffic
5.	Inbound	Displays the inbound traffic at the selected interface in color coded format
6.	Outbound	Displays the outbound traffic at the selected interface in color coded format

13.3 Real-time Graphs/Signal & Noise

The graph shows the wireless signal and noise status to explain the real-time wireless status in last 3 minutes. The graph is refreshed at every 3 sec interval. In addition to the displayed graph the user can find the signal and noise values along with average and the peak values of the respective UBR.

A basic overview of the Real-time Graphs/ Signal & Noise screen is given below:

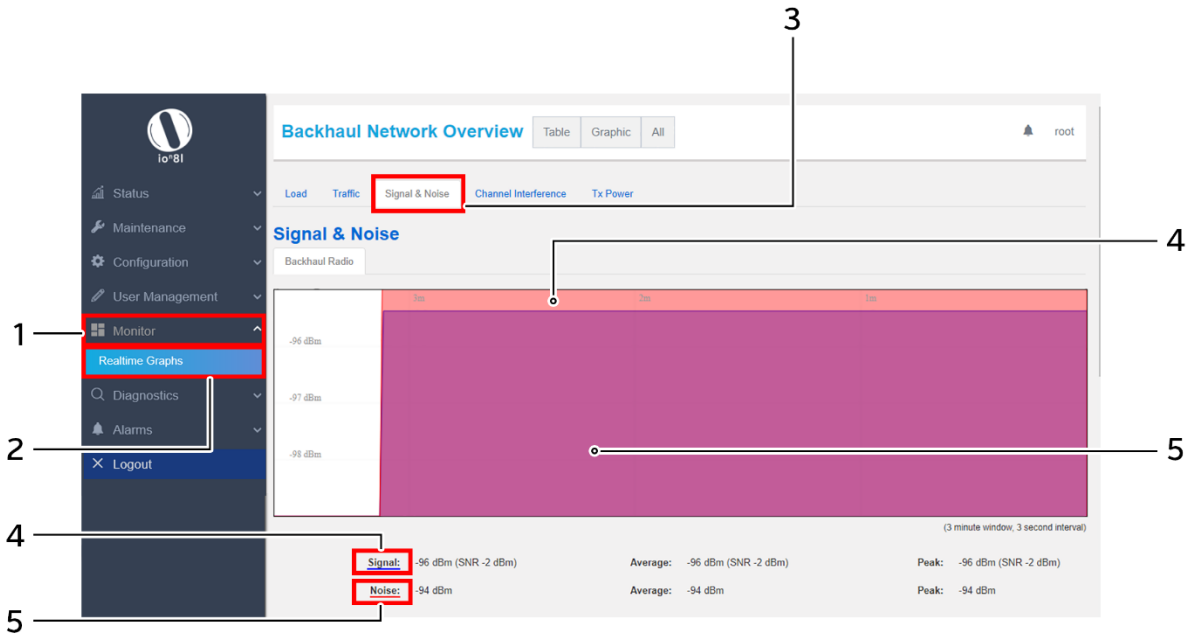

Figure 61: Basic overview of the Real-time Graphs/Signal & Noise screen

Follow the steps given below to view the real-time Signal & Noise graphs for the UBR:

Table 53: List of actions to view real-time Signal & Noise graphs

Callout	Name	Description
1.	Monitor	Click on "Monitor" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	Signal & Noise	Click on "Signal & Noise" option
4.	Signal	Displays the strength of wireless radio signal in color coded format
5.	Noise	Displays the noise in the wireless radio signal in color coded format

13.4 Real-time Graphs/Channel Interference

The graph shows the real-time channel interference. A basic overview of the screen is given below:

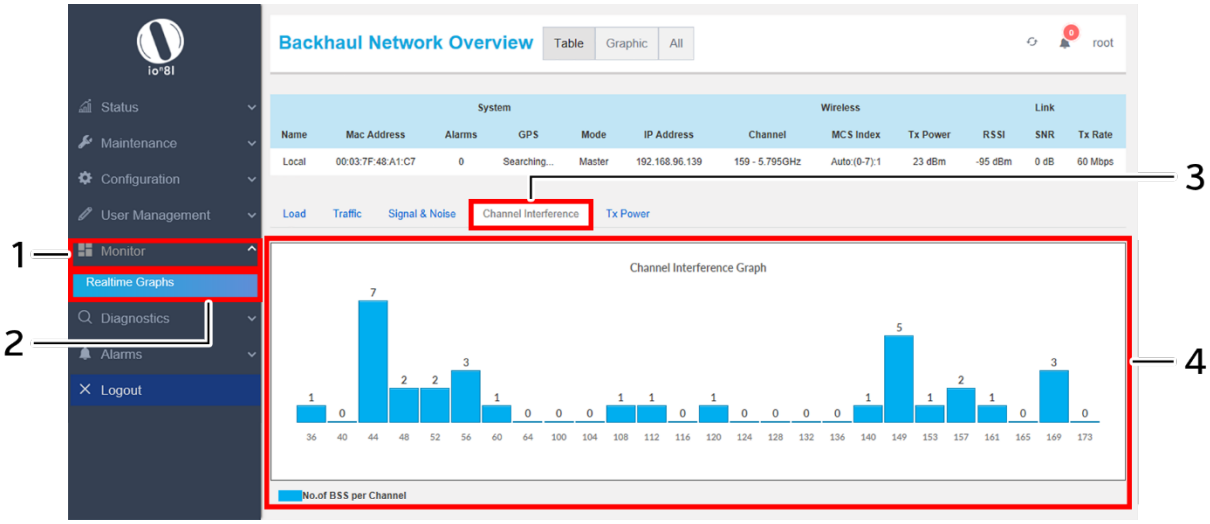

Figure 62: Basic overview of the Real-time Graphs/Tx Channel Interference screen

Follow the steps given below to view the real-time channel interference graphs for the UBR:

Table 54: List of actions to view real-time channel interference graphs

Callout	Name	Description
1.	Monitor	Click on "Monitor" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	Channel Interference	Click on "Channel Interference" option
4.	Channel Interference graph	Displays the channel interference graph

13.5 Real-time Graphs/Tx Power

The graph shows the real-time Tx power status of transmitted signal in last 3 minutes. The graph is refreshed at every 3 sec interval.

A basic overview of the Real-time Graphs/Tx Power screen is given below:

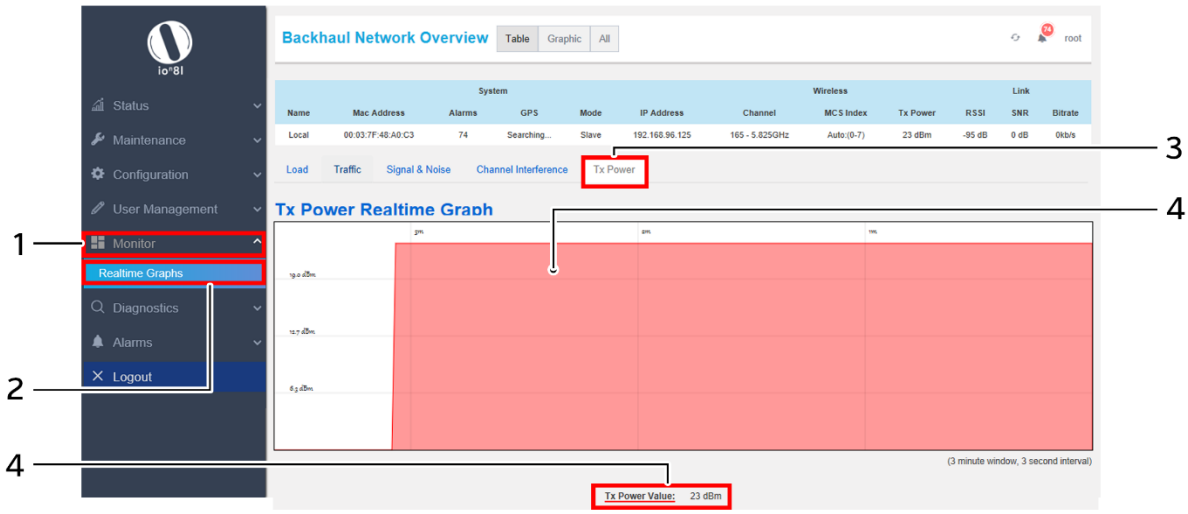

Figure 63: Basic overview of the Real-time Graphs/Tx Power screen

Follow the steps given below to view the real-time Tx Power graphs for the UBR:

Table 55: List of actions to view real-time Tx Power graphs

Callout	Name	Description
1.	Monitor	Click on "Monitor" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	Tx Power	Click on "Tx Power" option
4.	Tx Power value	Displays the Tx power value in color coded format

14 Diagnostics screen

The diagnostic activities of the connected UBR are executed from this screen. The list of options available for the user is given below:

1. System Log
2. Kernel Log
3. Diagnostic Tools
4. Debug logs

14.1 System Log

The size of the log displayed in system log screen is based on the "System log buffer size" limit specified in the syslog configuration screen. Once the log size has reached the limit, only new logs will be shown and old logs will be stored in the database but will not be shown in this screen.

A basic overview of the System Log screen is given below:

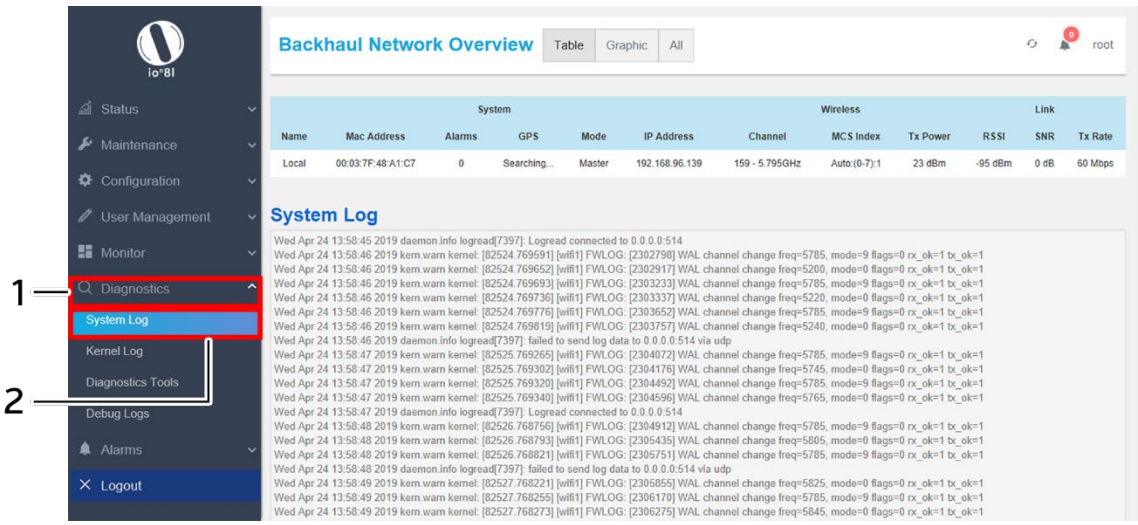

Figure 64: Basic overview of the System Log screen

Follow the steps given below to view the system log for the UBR:

Table 56: List of actions to view the system log

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	System Log	Click on "System Log" option. Logs relevant to the UBR application software are displayed here for monitoring purpose

14.2 Kernel Log

Boot logs, driver logs, Wi-Fi and firmware related logs are listed in this screen. Kernel log will be accumulated from boot up time till shut down time of the respective UBR.

A basic overview of the Kernel Log screen is given below:

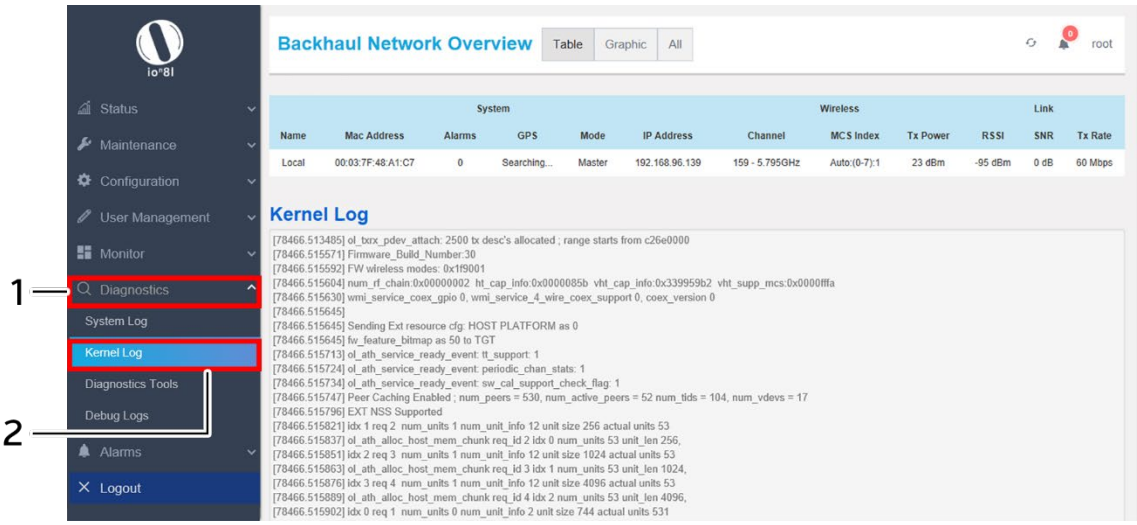

Figure 65: Basic overview of the Kernel Log screen

Follow the steps given below to view the Kernel log for the UBR:

Table 57: List of actions to view the kernel log

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Kernel Log	Click on “Kernel Log” option

14.3 Diagnostic Tools

As part of diagnostics, the user can perform the following activities:

1. The user can check if the link connection is established or not with "Ping" option
2. The user can trace the route of the established link with "Traceroute" option
3. The user can look for the server address with the help of domain name by using "Nslookup" option

14.3.1 Check the network connection/status

A basic overview of the Diagnostic Tools screen to check the connection status is given below:

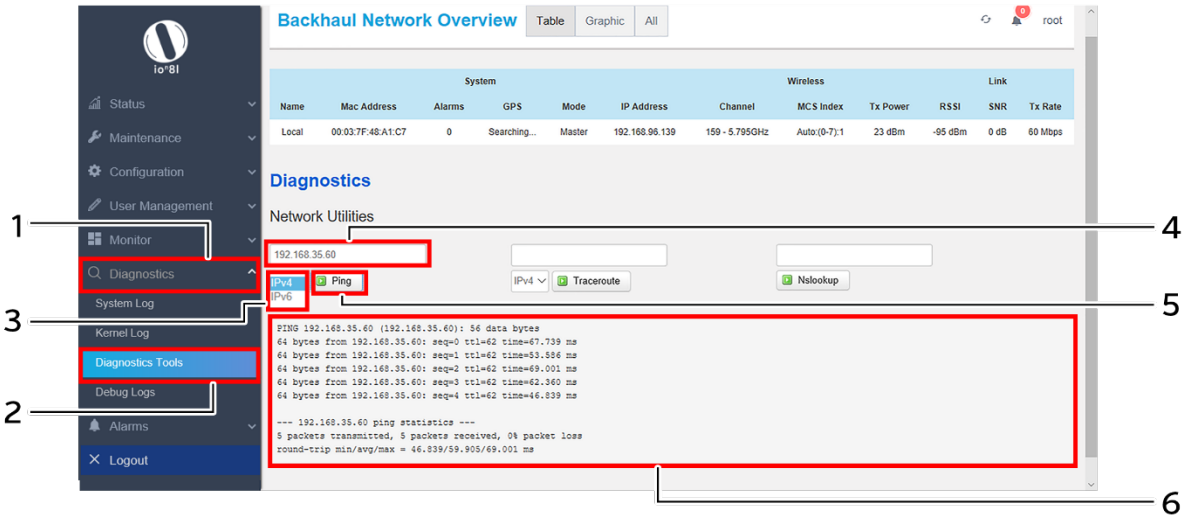

Figure 66: Basic overview of the diagnostics tool screen to check the connection status

Follow the steps given below to check the connection status:

Table 58: List of actions to check the connection status

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Diagnostics Tool	Click on "Diagnostics Tool" option
3.	Address type	Select the IP address type from the dropdown list (IPv4, IPv6)
4.	IP Address	Enter the IP address of the device with which the user wants to check the connection status
5.	Ping	Click on "Ping" option to check the connection status. It will check the network connection/status with entered IP address
6.	Feedback window	Check the response on the feedback window to know the connection status. The status is shown in terms of transmitted packets and received packets with packet data loss

14.3.2 Check the route of the established network connection

A basic overview of the Diagnostic Tools screen to check the route of established connection is given below:

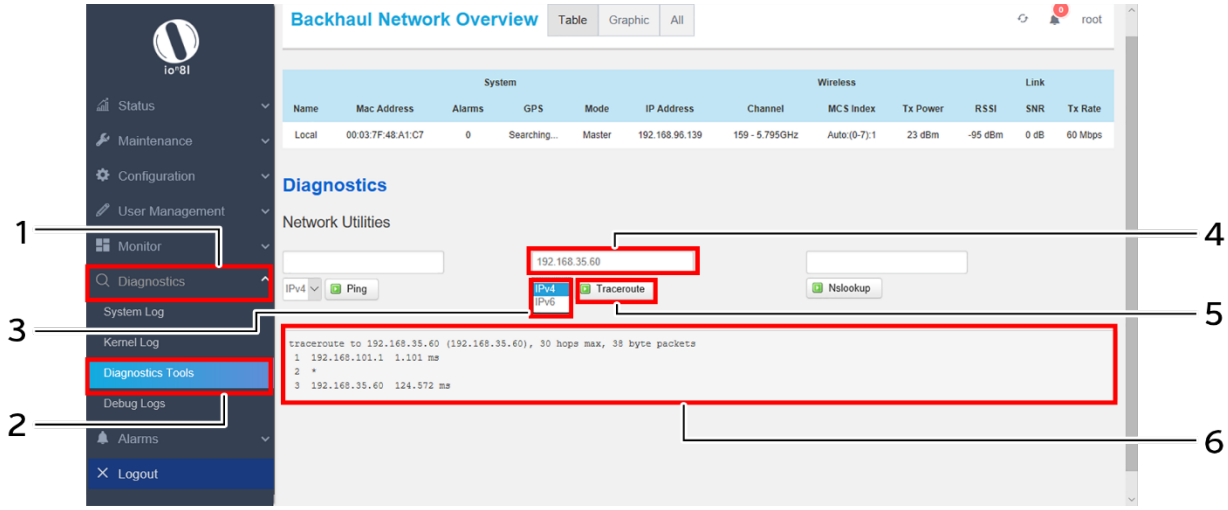

Figure 67: Basic overview of the diagnostics tool screen to check the route of established connection

Follow the steps given below to check the route of established connection:

Table 59: List of actions to check the route of established connection

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Diagnostics Tool	Click on “Diagnostics Tool” option
3.	Address type	Select the IP address type from the dropdown list (IPv4, IPv6)
4.	IP Address	Enter the IP address of the device with which the user wants to check the connection route
5.	Traceroute	Click on “Traceroute” option to check the connection route. It traces the network path/route to the entered IP address
6.	Feedback window	Check the response on the feedback window to know the connection route.

14.3.3 Identify the IP address with the domain name

A basic overview of the Diagnostic Tools screen to identify the IP address with the domain name is given below:

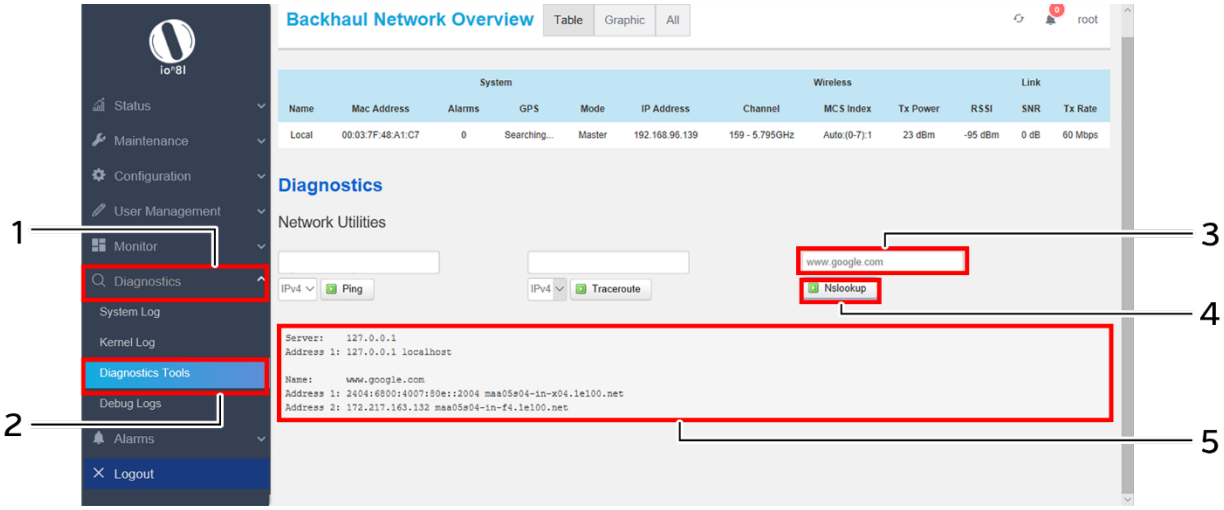

Figure 68: Basic overview of the diagnostics tool screen to identify the IP address with the domain name

Follow the steps given below to identify the IP address with the domain name:

Table 60: List of actions to identify the IP address with the domain name

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Diagnostics Tool	Click on “Diagnostics Tool” option
3.	Domain name	Enter the domain name
4.	Nslookup	Click on “Nslookup” option to check the connection route. It looks up for the IP of the mentioned domain name
5.	Feedback window	Check the response on the feedback window to know the IP address of the respective domain name. Make sure to enter the correct domain name.

14.4 Debug logs

The user can view and download the debugging information such as logs and configuration with the help of this feature. It helps the user to analyze and understand the root cause of any system failure.

A basic overview of the Diagnostic Tools screen to download debug logs is given below:

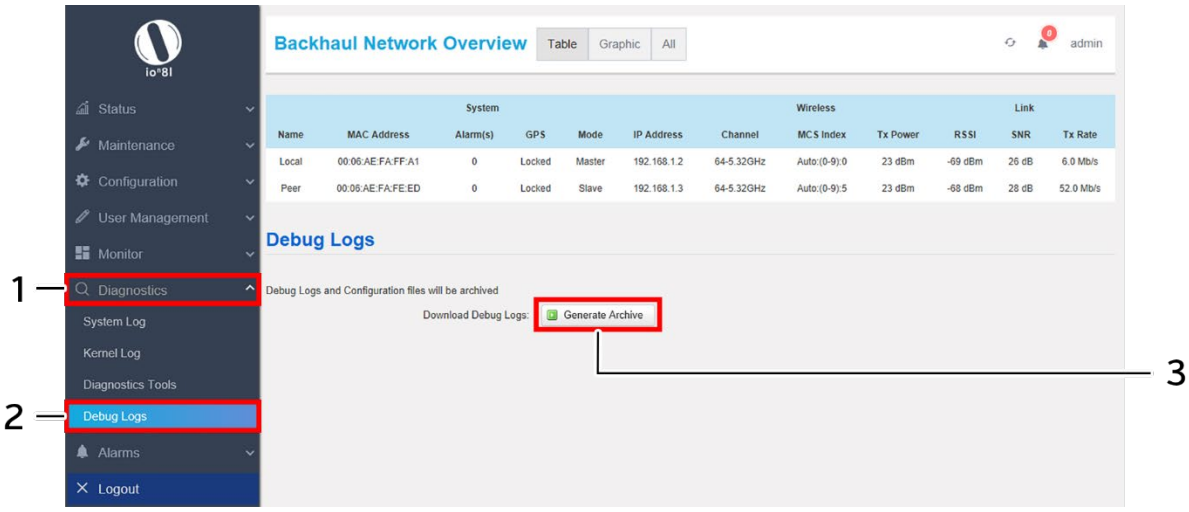

Figure 69: Basic overview of the Diagnostic Tools screen to download debug logs

Follow the steps given below to download debug logs:

Table 61: List of actions to download debug logs

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Debug logs	Click on “Debug logs” option
3.	Download Debug Bugs	Click on “Download Archive” option and download the debug logs in your drive

15 Alarms

This screen displays the active/info/historical alarms in a listed form along with the relevant information in the respective columns. The bell icon in Overview toolbar on the top will show the total number of unacknowledged alarms. The user is provided with options to acknowledge and delete the raised alarms in this screen.

15.1 Active Alarms

The alarms which are having significant negative event are listed in this screen e.g. Link Down, CPU over load, Memory over load, etc. These alarms need immediate user attention and are placed in active alarms screen. These alarms are moved from active alarms page to historical alarm page, once the active alarms are cleared. Active alarms are cleared from the screen whenever the negative event has been resolved and the corresponding alarm is raised at device GUI. The user can acknowledge any of the active alarm or can delete the same if needed.

A basic overview of the active alarm screen is given below:

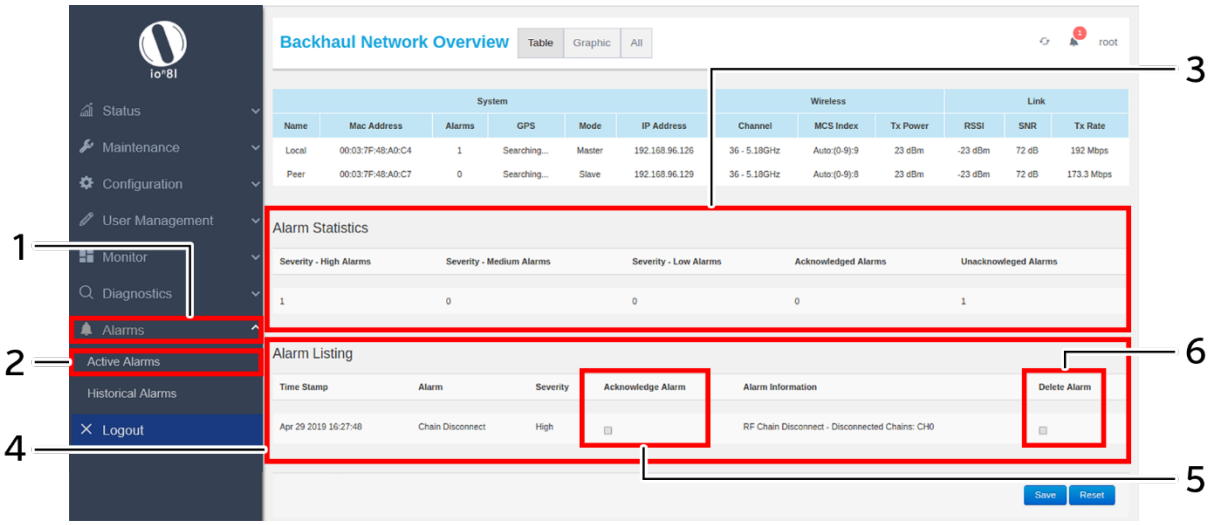

Figure 70: Basic overview of the active alarm screen

Follow the steps given below to view the active alarm listing and statistics:

Table 62: List of actions to view the active alarm listing and statistics

Callout	Name	Description
1.	Alarms	Click on "Alarms" dropdown
2.	Active Alarms	Click on "Active Alarms" option
3.	Alarms Statistics	Displays total count of the acknowledged, unacknowledged, and other active alarms based on their severity level.
4.	Alarms Listing	Displays all active alarms in the listed form. All alarms have their time stamp at which the alarm was generated, basic information, acknowledgement status, and severity level displayed with respect to each alarm
5.	Acknowledge Alarm	Option to acknowledge an active alarm. Click and select the check box to confirm the selection of respective alarm for acknowledgement action
6.	Delete	Option to delete an alarm. Click and select the check box to confirm the selection of respective alarm for deletion action

Click "Save" to save the user action of alarm acknowledgement or deletion of alarms, or click "Reset" to configure the same again. The acknowledged alarms will still be present in the active alarm screen, but the notification in Overview toolbar on the top will reduce in number.

15.2 Historical Alarms

All alarms which have been cleared from active alarm page are displayed in this screen. The user can acknowledge any of the alarm or can delete the same from this screen, if needed.

A basic overview of the historical alarm screen is given below:

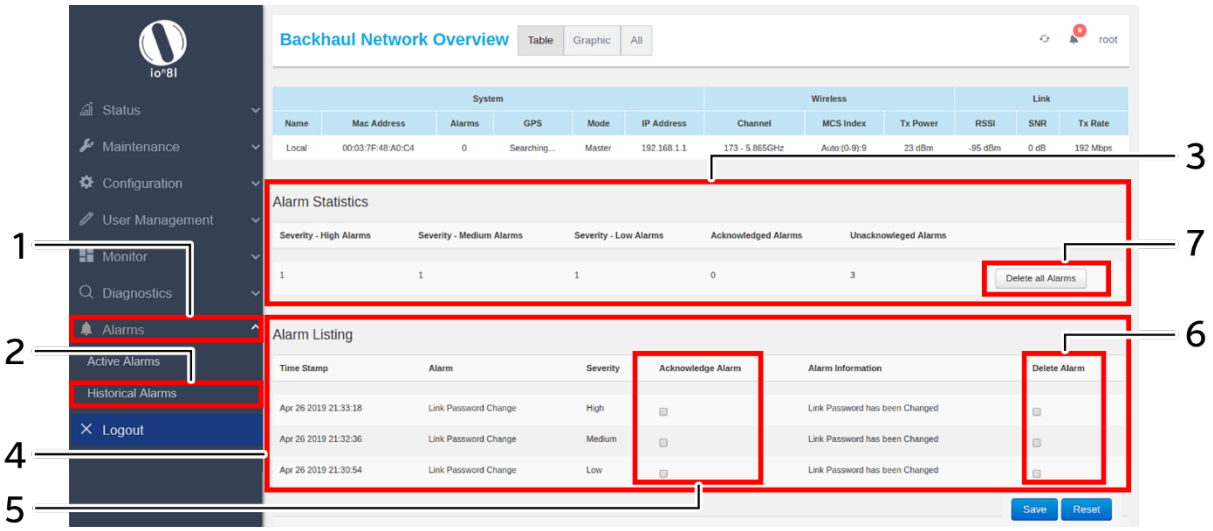

Figure 71: Basic overview of the historical alarm screen

Follow the steps given below to view the historical alarm listing and statistics:

Table 63: List of actions to view the historical alarm listing and statistics

Callout	Name	Description
1.	Alarms	Click on "Alarms" dropdown
2.	Historical Alarms	Click on "Historical Alarms" option
3.	Alarms Statistics	Displays total count of the acknowledged, unacknowledged, and other historical alarms based on their severity level.
4.	Alarms Listing	Displays all historical alarms in the listed form. All alarms have their time stamp at which the alarm was generated, basic information, acknowledgement status, and severity level displayed with respect to each alarm
5.	Acknowledge Alarm	Option to acknowledge an historical alarm. Click and select the check box to confirm the selection of respective alarm for acknowledgement action
6.	Delete	Option to delete an alarm. Click and select the check box to confirm the selection of respective alarm for deletion action
7.	Delete All	Click on the option to delete all info alarms

Click "Save" to save the user action of alarm acknowledgement or deletion of alarms, or click "Reset" to configure the same again. The acknowledged alarms will still be present in the historical alarm screen, but the notification in Overview toolbar on the top will reduce in number.

16 Logout

The user can click on the "logout" option to terminate the session as shown in the figure below:

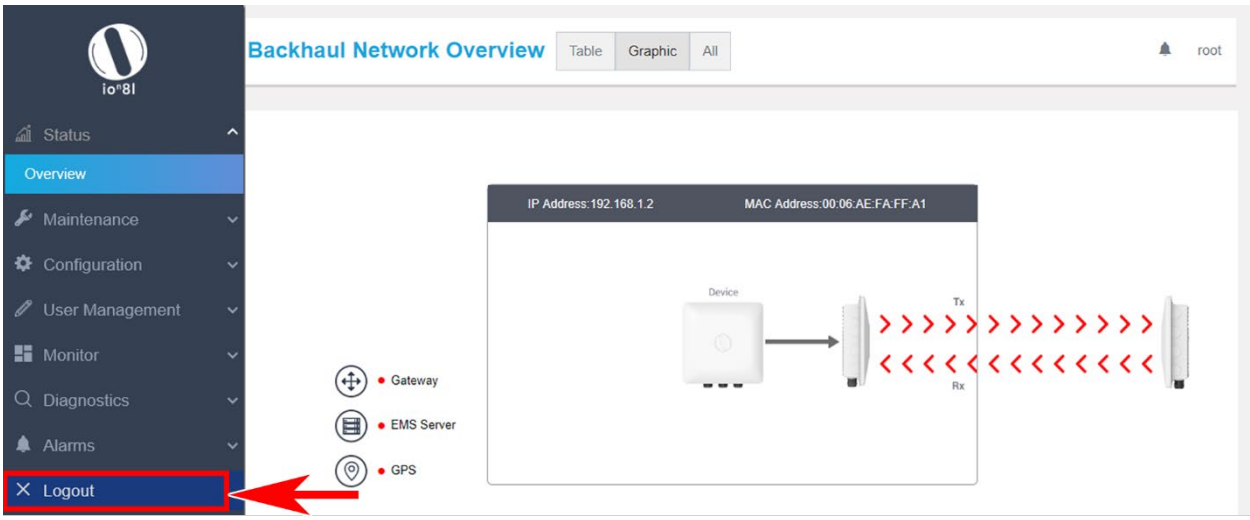

Figure 72: Basic overview of the UBR GUI with logout option

Once logged out the user will be presented with the login screen.

17 Installation Setup

The UBR device has four holes on the back side to attach a mounting bracket, as shown in "Figure 3: Back view of the 4x4 UBR" of this document. The mounting bracket is designed in such a way that the UBR can be mounted on the wall as well as on the pole with the help of an extra clamping bracket and its attaching parts. The external mounting bracket provides the freedom of movement to the UBR in both vertical and horizontal axis even after the mounting.

The mounting bracket is fixed onto the 4x4 UBR as shown in the figure below:

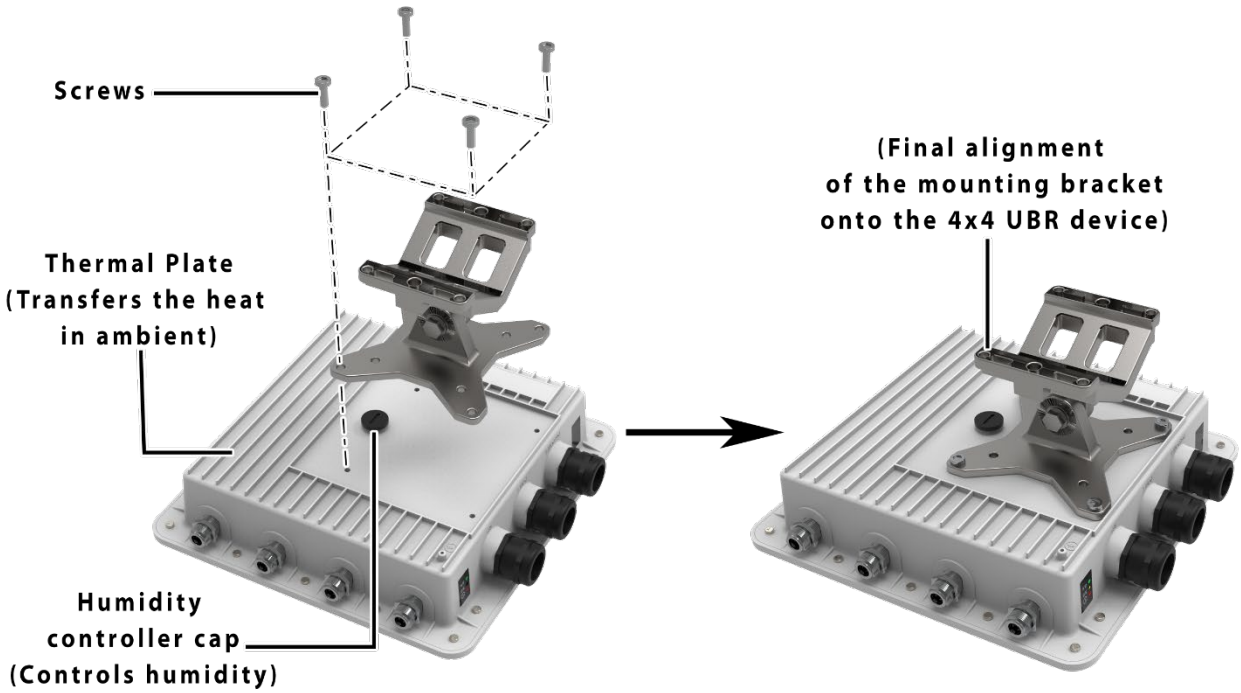

Figure 73: Mounting bracket alignment with the 4x4 UBR device

1. Align the holes of mounting bracket with the holes available at the back side of the 4x4 UBR device.
2. Use the supplied screws and fix the mounting bracket with 4x4 UBR device.

The mounting instructions of 4x4 UBR is detailed in further sections below.

17.1 4x4 UBR mounting to the Pole

To mount the device on a pole, an extra clamping bracket is needed along with the mounting bracket. Follow the steps given below and mount the device on pole:

1. Attach the mounting bracket to the back side of the UBR device as shown in "Figure 73: Mounting bracket alignment with the 4x4 UBR device".
2. Firmly place the mounting bracket on the pole (make sure there is no movement) and attach the clamping bracket with M5-expansion bolts.

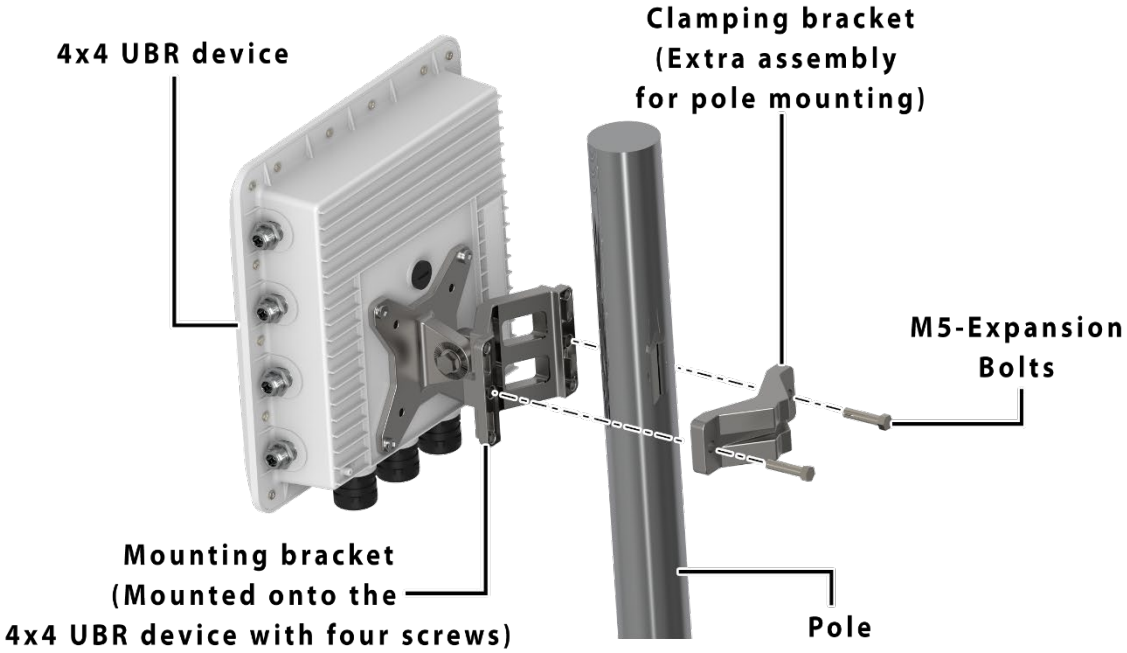

Figure 74: Overview of the 4x4 UBR device with pole and clamping bracket

3. The final alignment of 4x4 UBR in a pole mounting is shown in the figure below:

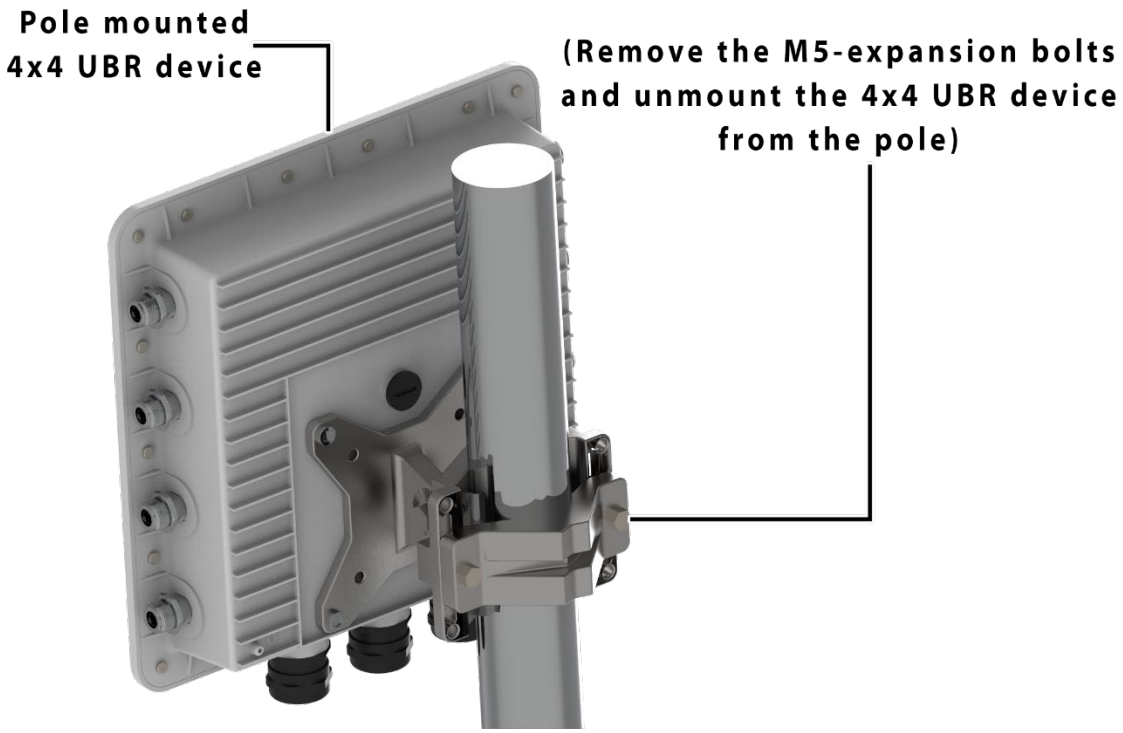

Figure 75: Basic overview of pole mounted 4x4 UBR device

17.2 4x4 UBR mounting to the Wall

To mount the device onto the wall, M5-expansion bolts and foundation bolts are needed along with the mounting bracket. Refer the image given below:

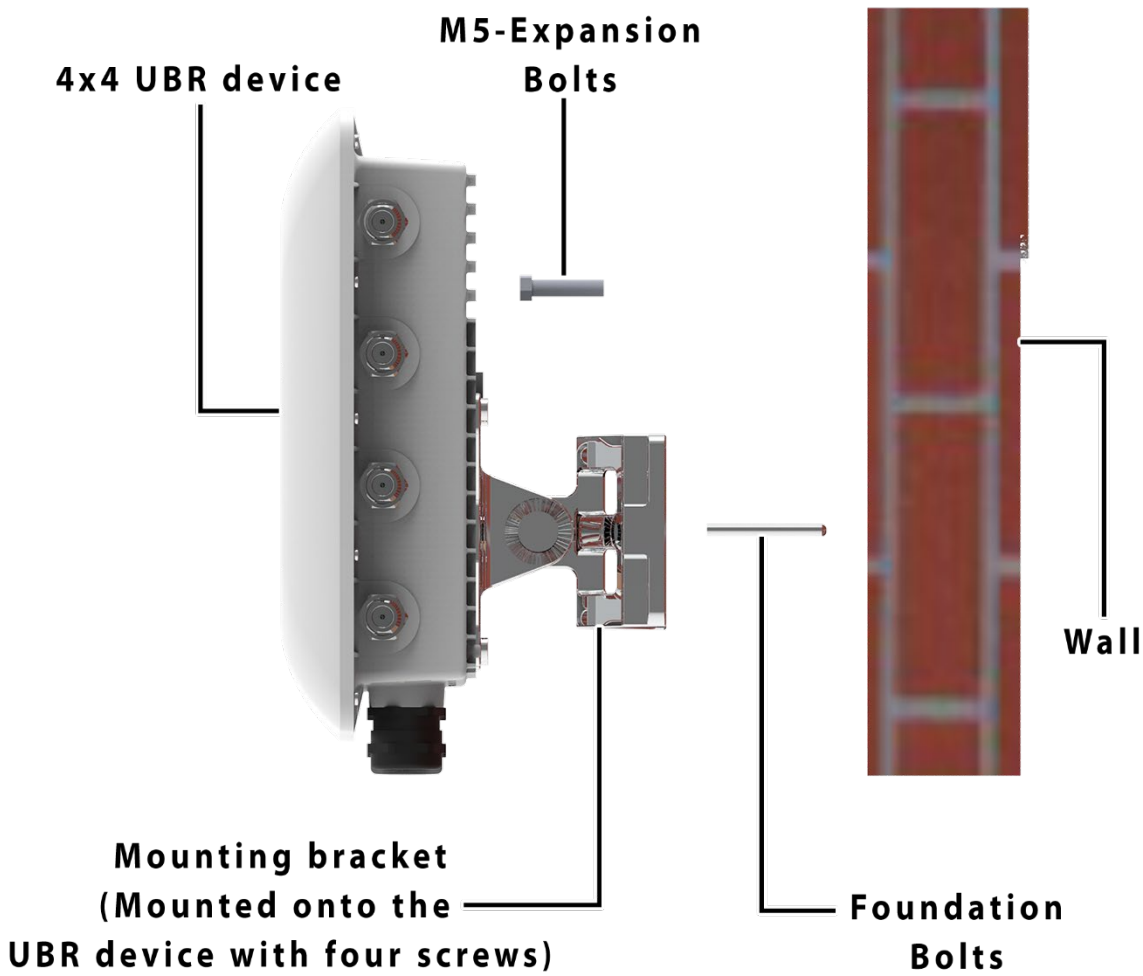

Figure 76: Items needed for mounting the device to wall

Follow the steps given below and mount the device onto the wall:

1. Attach the mounting bracket to the back side of the UBR device as shown in "Figure 73: Mounting bracket alignment with the 4x4 UBR device".
2. Take the reference from the printed sheet provided along with the mounting bracket and mark the position of the holes on the wall.
3. Use the drill machine to drill 2 holes with a drill tool on respective marked positions.