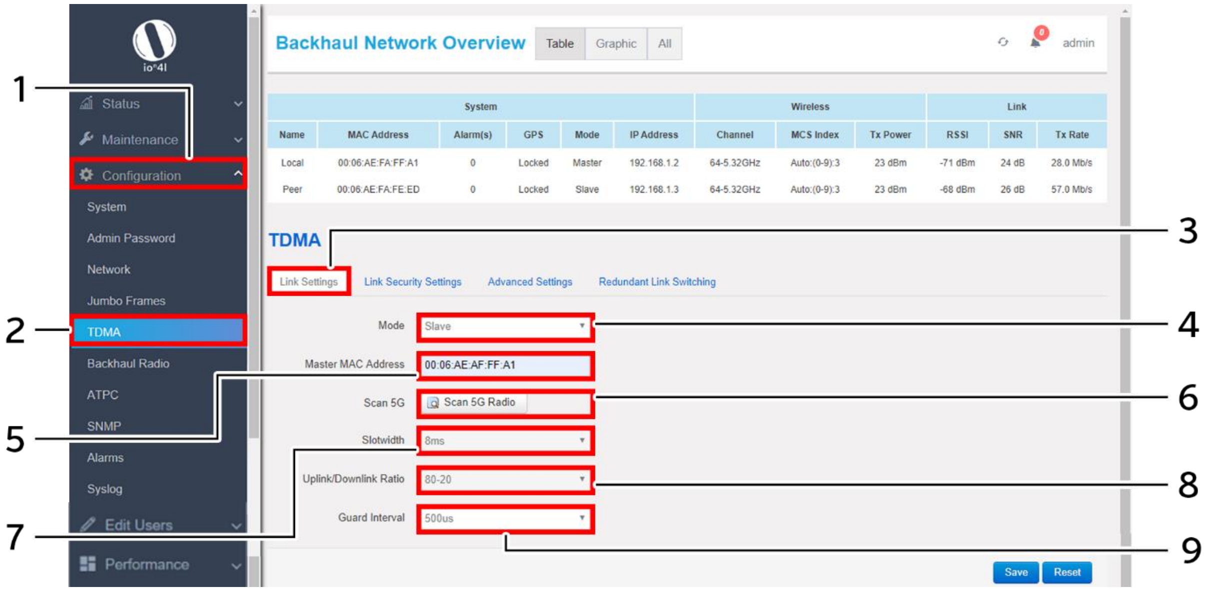
11.5.1.3 *Link settings of Slave device in a P2P or P2MP link*

A basic overview of the TDMA Configuration screen/Link settings of Slave device in a P2P or P2MP link is given below:



System						Wireless			Link		
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):3	23 dBm	-71 dBm	24 dB	28.0 Mb/s
Peer	00:06:AE:FA:FE:ED	0	Locked	Slave	192.168.1.3	64-5.32GHz	Auto:(0-9):3	23 dBm	-68 dBm	26 dB	57.0 Mb/s

Mode: Slave
Master MAC Address: 00:06:AE:AF:FF:A1
Scan 5G: Scan 5G Radio
Slotwidth: 8ms
Uplink/Downlink Ratio: 80-20
Guard Interval: 500us

Figure 32: Link settings screen of Slave device in a P2P or P2MP link

Follow the steps given below and configure the link settings of Slave device in a P2P or P2MP link for the UBR:

Table 26: List of actions to configure the link settings of Slave device in a P2P or P2MP link

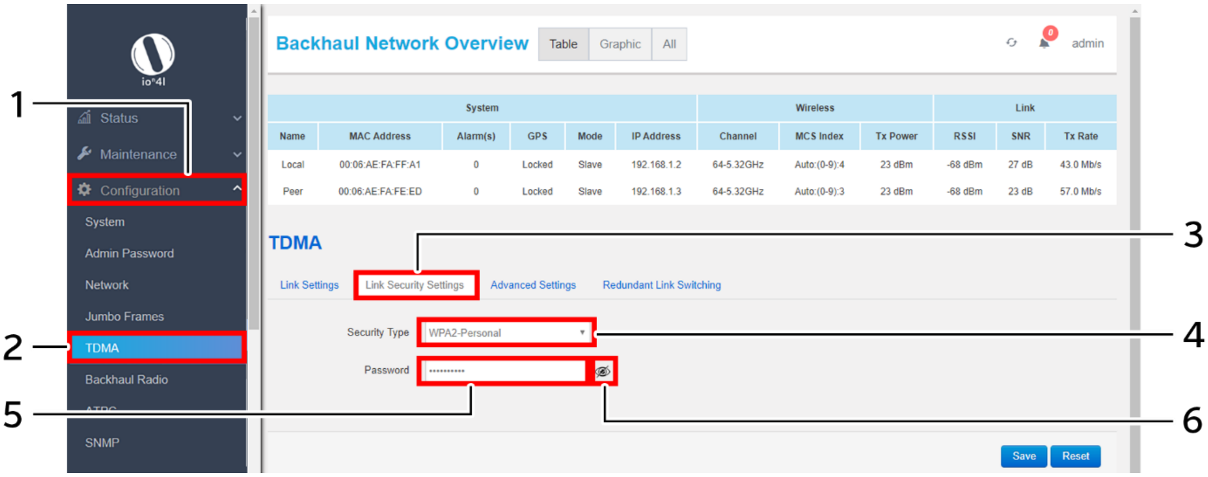
Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	TDMA	Click on "TDMA" option
3.	Link Settings	Click on "Link Settings" option
4.	Mode	Select the "Mode" to Slave from the dropdown list (Master/Slave)
5.	Master UID	Enter the "Master UID". Master UID is needed in salve devices to allow their association with master device. The master UID is the MAC address of the master device
6.	Scan 5G	Click on this option and scan nearby 5G radio devices if the user does not want to enter the Master UID manually. Select the desired MAC address from the scanned list
7.	Slot width	This parameter will be in sync with the linked master device
8.	Downlink/ Uplink Ratio	This parameter will be in sync with the linked master device. This ratio controls the bandwidth to be used for downlink and uplink from the device. E.g.: 20-80 means- Downlink = 20% of the total available bandwidth is used in downlink

Callout	Name	Description
		Uplink = 80% of the total available bandwidth is used in uplink
9.	Guard Interval	This parameter will be in sync with the linked master device

Click “Save” to save the Link settings or click “Reset” to configure the same again.

11.5.2 Link Security Settings

Link security depends on the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. WPA2 is the most secure protocol and recommended for better security of your wireless network. A basic overview of the Link Security Settings screen is given below:



System						Wireless			Link		
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Slave	192.168.1.2	64-5.32GHz	Auto:(0-9):4	23 dBm	-68 dBm	27 dB	43.0 Mb/s
Peer	00:06:AE:FA:FE:ED	0	Locked	Slave	192.168.1.3	64-5.32GHz	Auto:(0-9):3	23 dBm	-68 dBm	23 dB	57.0 Mb/s

Security Type: WPA2-Personal

Password: ••••••••••

Figure 33: Basic overview of the Link Security Settings screen

Follow the steps given below and configure the link security settings for the UBR:

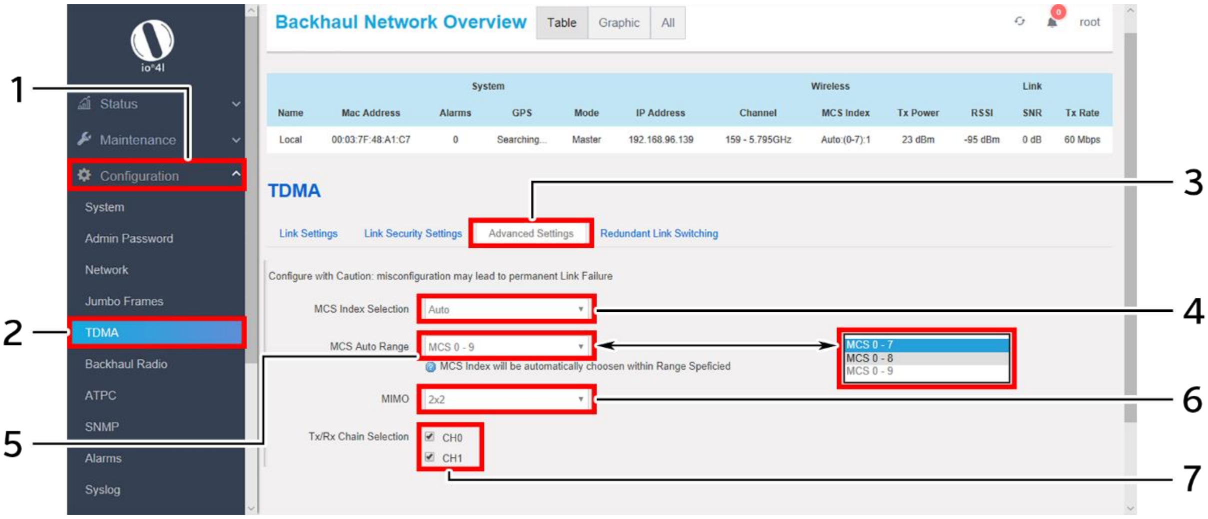
Table 27: List of actions to configure the link security settings for the UBR

Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	TDMA	Click on “TDMA” option
3.	Link Security Settings	Click on “Link Security Settings” option
4.	Link Security Type	Select the “Link Security Type” from the dropdown list (WPA/WPA2/None). The user can select any one of WPA or WPA2 security type depending upon the device compatibility. No password is needed, if security type is set to “None”
5.	Link password	Enter the “Link password”
6.	View/Hide	Click the “View/Hide” icon to view or hide the password

Click “Save” to save the link security settings or click “Reset” to configure the same again.

11.5.3 Advanced Settings

A basic overview of the advanced TDMA settings screen is given below:



System						Wireless			Link		
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

Configure with Caution: misconfiguration may lead to permanent Link Failure

MCS Index Selection: Auto

MCS Auto Range: MCS 0 - 9

MCS Index will be automatically choosen within Range Speficied

MCS 0 - 7
MCS 0 - 8
MCS 0 - 9

MIMO: 2x2

Tx/Rx Chain Selection: ☑ CH0 ☑ CH1

Figure 34: Basic overview of the advanced TDMA settings screen

Caution: Misconfiguration might leads to permanent link failure

Follow the steps given below and configure the advanced TDMA settings for the UBR:

Table 28: List of actions to configure the advanced TDMA settings for the UBR

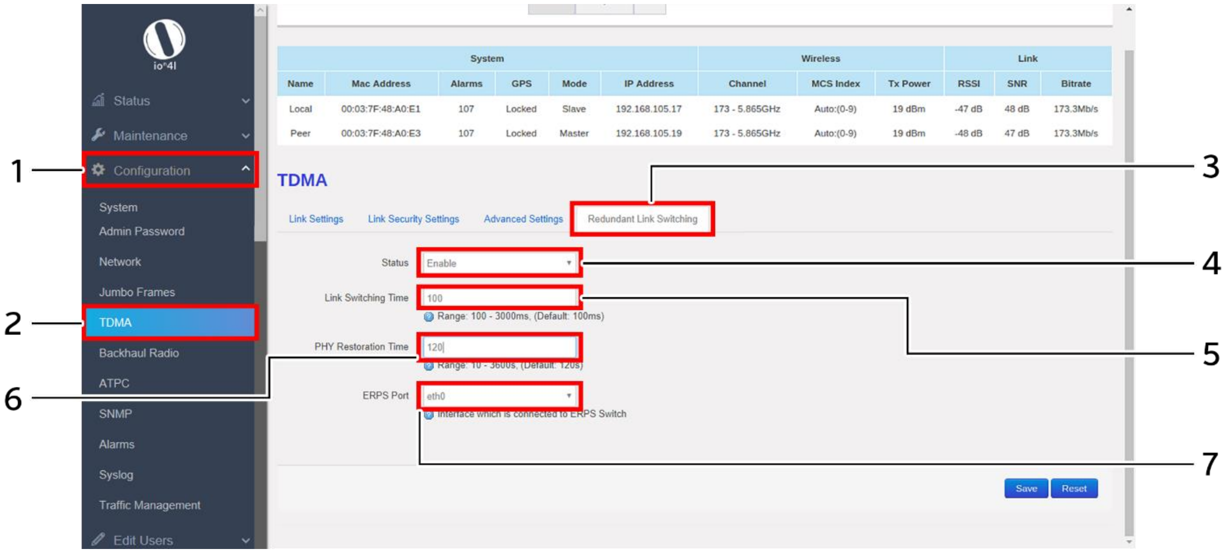
Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	TDMA	Click on "TDMA" option
3.	Advanced Settings	Click on "Advanced Settings" option
4.	MCS Index Selection	MCS index is set to "Auto", select the auto range below
5.	MCS Auto Range	Set the range of auto selection from the dropdown list (MCS- 0 to 7, 0 to 8, 0 to 9), if MCS index selection is set to "Auto". The auto MCS index algorithm will set the value with in the selected range
Or		
6.	No of Spatial Streams (NSS)	Select the spatial streams from the dropdown list (1x1 or 2x2)
7.	Tx/Rx Chain Selection	Click on the selection box and select a single chain or multiple chains as per the NSS. If the NSS is set to 1x1, one chain will be available for selection and if the NSS is set to 2x2, two chains will be available for selection. Only selected chains will contribute for transmission in the link

Click "Save" to save the advanced TDMA settings or click "Reset" to configure the same again.

11.5.4 Redundant Link Switching

This screen provides options to comply with 1+1 switching feature. An ERPS switch is used between two established links. One link is set to primary which is used in ideal cases and the other behaves as secondary which comes online whenever the primary link is broken or down.

A basic overview of the redundant link switching screen is given below:



System						Wireless			Link		
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Bitrate
Local	00:03:7F:48:A0:E1	107	Locked	Slave	192.168.105.17	173 - 5.865GHz	Auto:(0-9)	19 dBm	-47 dB	48 dB	173.3Mb/s
Peer	00:03:7F:48:A0:E3	107	Locked	Master	192.168.105.19	173 - 5.865GHz	Auto:(0-9)	19 dBm	-48 dB	47 dB	173.3Mb/s

TDMA

Status: Enable

Link Switching Time: 100
Range: 100 - 3000ms, (Default: 100ms)

PHY Restoration Time: 120
Range: 10 - 3600s, (Default: 120s)

ERPS Port: eth0
Interface which is connected to ERPS Switch

Figure 35: Basic overview of the redundant link switching screen

Follow the steps given below and configure the redundant link switching for the UBR:

Table 29: List of actions to configure the redundant link switching for the UBR

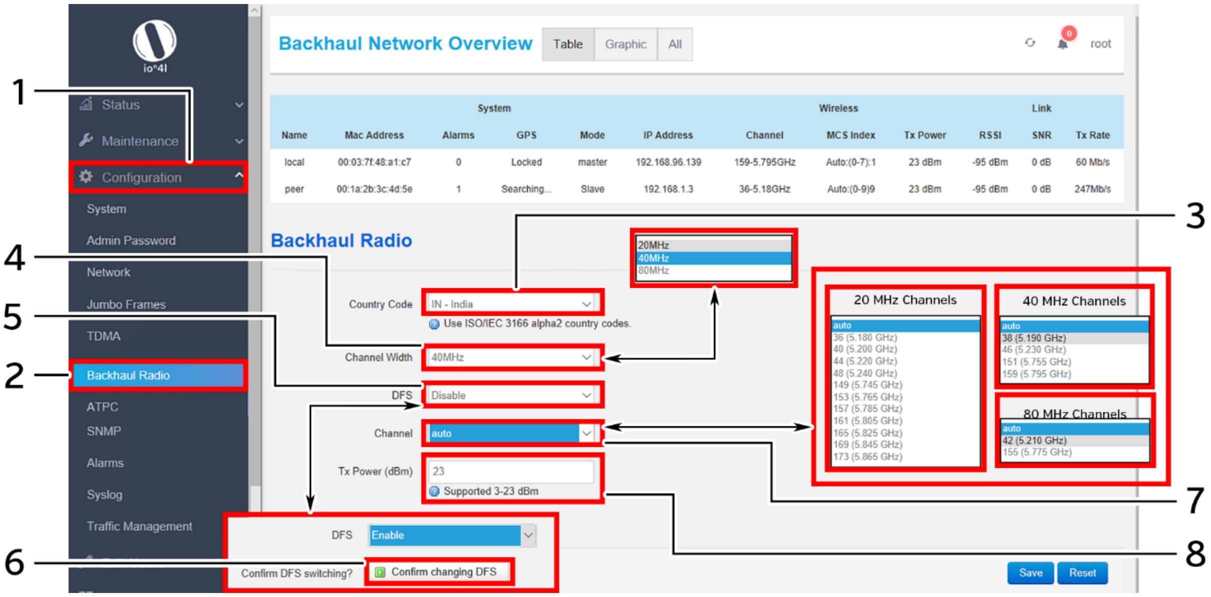
Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	TDMA	Click on “TDMA” option
3.	Redundant Link Switching	Click on “Redundant Link Switching” option
4.	Status	Enable or Disable the redundant link switching. Enter the following parameters if enabled
5.	Link Switching Time	Set the link switching time within the range of 100 to 3000 milliseconds
6.	PHY Restoration Time	Set the PHY restoration time within the range of 10 to 3600 seconds. When two links are connected through a switch which supports ERPS protocol, one link is the primary link and the other behaves as secondary. During any scenario when switching happens, this parameter defines the user configured time to bring up the ethernet of the broken link again
7.	ERPS Port	Select the interface connected to ERPS switch from the dropdown list. Displays the only interface of 2x2 UBR device

Click “Save” to save the redundant link switching or click “Reset” to configure the same again.

11.6 Backhaul Radio Configuration

This screen provides the user with options to configure the backhaul radio parameters such as channel bandwidth, respective channel or the channel selection process, and the power for the radio signal transmission. The backhaul portion of the network comprises the intermediate links between the core network, or backbone network, and the small subnetworks at the "edge" of the entire hierarchical network. Backhaul solution in this section is detailed in context of wireless (point-to-point, point-to-multipoint over high-capacity radio links).

A basic overview of the Backhaul Radio Configuration screen is given below:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
local	00:03:7f:48:a1:c7	0	Locked	master	192.168.96.139	159-5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mb/s
peer	00:1a:2b:3c:4d:5e	1	Searching...	Slave	192.168.1.3	36-5.18GHz	Auto:(0-9)9	23 dBm	-95 dBm	0 dB	247Mb/s

Backhaul Radio

Country Code: IN - India
Use ISO/IEC 3166 alpha2 country codes.
Channel Width: 40MHz
DFS: Disable
Channel: auto
Tx Power (dBm): 23
Supported 3-23 dBm
DFS: Enable
Confirm DFS switching? ☑ Confirm changing DFS

Figure 36: Basic overview of the Backhaul Radio Configuration screen

Follow the steps given below and configure the backhaul radio settings for the UBR:

Table 30: List of actions to configure the backhaul radio settings

Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	Backhaul Radio	Click on “Backhaul Radio” option
3.	Country Code	Select the “Country Code” from the dropdown list
4.	Channel Width	Select the “Channel Width” from the dropdown list (20MHz/40MHz/80MHz)
5.	DFS	Enable or Disable DFS (Dynamic Frequency Selection). This parameter plays its role in auto channel selection mode. If the DFS option is enabled, all DFS channels will be part of auto channel selection criteria and will not be blocked for selection. A disabled DFS scenario blocks DFS channels in auto channel selection criteria.
6.	Confirm DFS Switching	Click on this option to confirm the DFS switching, if the DFS option is enabled. Ignore this step, if DFS is disabled

Callout	Name	Description
7.	Channel	Select the “Channel” from the dropdown list. The device will choose the channel by itself, if “auto” channel is selected. For 20 MHz channel width, available channels are: 36/40/44/48/149/153/157/161/ 165/169/173. For 40 MHz channel width, available channels are: 38/46/151/159. For 80 MHz channel width, available channels are: 42/155
8.	Tx Power (dBm)	Enter the “Tx Power” value. The wireless radio signal will be transmitted with the specified Tx power value. The user can set the Tx power value from the range of 3dBm to 23dBm

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

11.7 ATPC Configuration

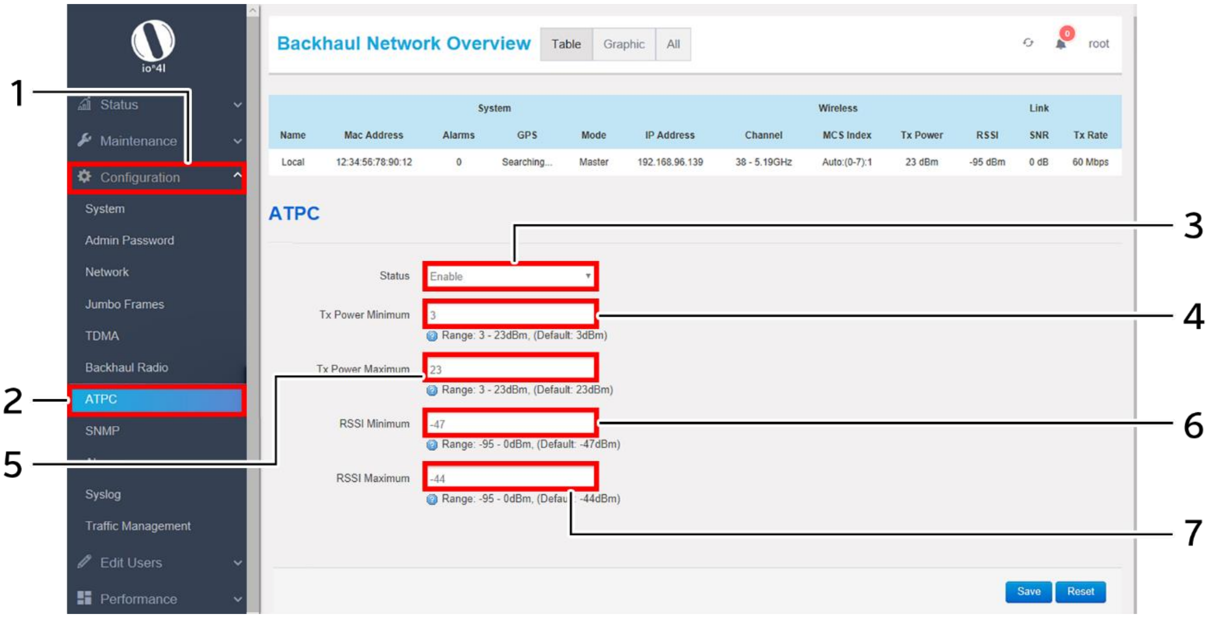
ATPC stands for Adaptive Transmission Power Control. This feature of UBR GUI enables the device to vary the power of transmitted signal to match the signal power of receiving end during “Fade” conditions (Reduced RSSI) such as heavy rainfall. ATPC can be used separately to ACM or together to maximize link uptime, stability, and availability. When the “fade” conditions (rainfall) are over, the ATPC system reduces the transmit power again. This reduces the stress on the microwave power amplifiers, which reduces power consumption, heat generation, and increases expected lifetime (MTBF).

ATPC (Automatic Transmit Power Control) is an advanced feature to ensure reliable transmission between master and slave in all weather conditions with minimal required transmit power. This reduces the stress on the power amplifiers, which reduces power consumption, heat generation and increases expected lifetime (MTBF).

ATPC will automatically increase the transmit power during fade conditions such as heavy rainfall. In ATPC, we need to define the range of signal strength (RSSI), so that ATPC will try to maintain that RSSI with minimum required transmit power in all weather conditions. Algorithm of ATPC is given below:

If the signal strength is degrading due to fading conditions, then we are increasing the transmission power gradually by one dBm. If the increased Tx power helps to maintain the desired RSSI of peer device, then the same Tx power is fixed in the board. If it fails to match the desired value, Tx power is again incremented and this process will be repeated until reaches desired RSSI. In other case, if the signal strength is higher than the required, then the power to transmit is wasted. Hence, the Tx power is reduced by one unit and it is compared as mentioned above.

A basic overview of the ATPC Configuration screen is given below:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	12:34:56:78:90:12	0	Searching...	Master	192.168.96.139	38 - 5.19GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

ATPC

Status: Enable

Tx Power Minimum: 3
Range: 3 - 23dBm, (Default: 3dBm)

Tx Power Maximum: 23
Range: 3 - 23dBm, (Default: 23dBm)

RSSI Minimum: -47
Range: -95 - 0dBm, (Default: -47dBm)

RSSI Maximum: -44
Range: -95 - 0dBm, (Defau : -44dBm)

Figure 37: Basic overview of the ATPC Configuration screen

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

Table 31: List of actions to configure the ATPC settings

Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	ATPC	Click on “ATPC” option
3.	ATPC Support	Enable/Disable the ATPC support. Enter the following parameters, if enabled
4.	Tx Power Minimum	Enter the minimum Tx power for ATPC calculations. It should not be less than 3 dBm
5.	Tx Power Maximum	Enter the maximum Tx power for ATPC calculations. It should not be more than 23 dBm
6.	RSSI Minimum	Enter the minimum RSSI for ATPC calculations. It should not be less than -95 dBm
7.	RSSI Maximum	Enter the maximum RSSI for ATPC calculations. It should not be more than 0 dBm

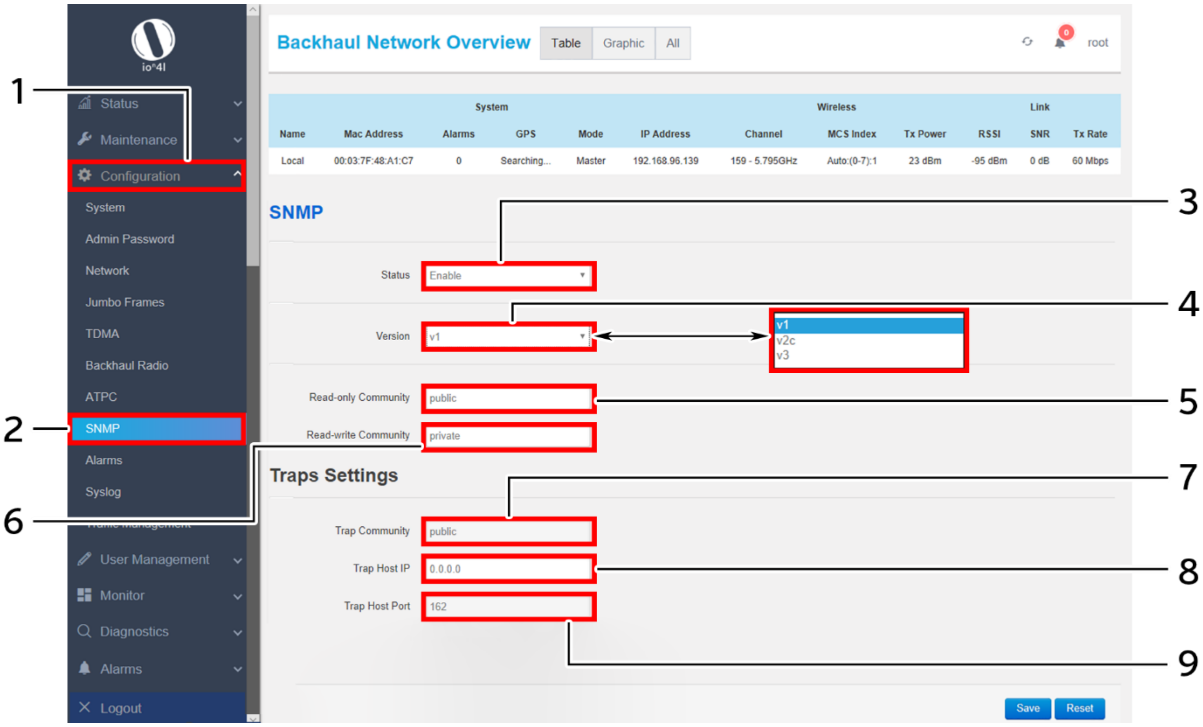
Click “Save” to save the ATPC configuration or click “Reset” to configure the same again. The ATPC algorithm will vary the transmission power accordingly to keep the RSSI within the range.

11.8 SNMP Configuration

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks. The SNMP configuration is also used for modifying that information to change device behavior. The ion's UBR device supports both SNMPv2 and SNMPv3 protocol. SNMP v3 is very similar to SNMP v2 (previous version) apart from the improved security model. SNMP v3 replaces the simple password sharing (as clear text) in SNMP v2 with a much more secure encoded security parameters.

SNMP Version-v1 & v2c:

A basic overview of the SNMP Configuration screen is given below:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

SNMP

Status: Enable

Version: v1

Read-only Community: public

Read-write Community: private

Traps Settings

Trap Community: public

Trap Host IP: 0.0.0.0

Trap Host Port: 162

Figure 38: Basic overview of the SNMP Configuration screen (v1 or v2c)

Follow the steps given below and configure the SNMP settings (v1 or v2c) for the UBR:

Table 32: List of actions to configure the SNMP settings (v1 or v2c)

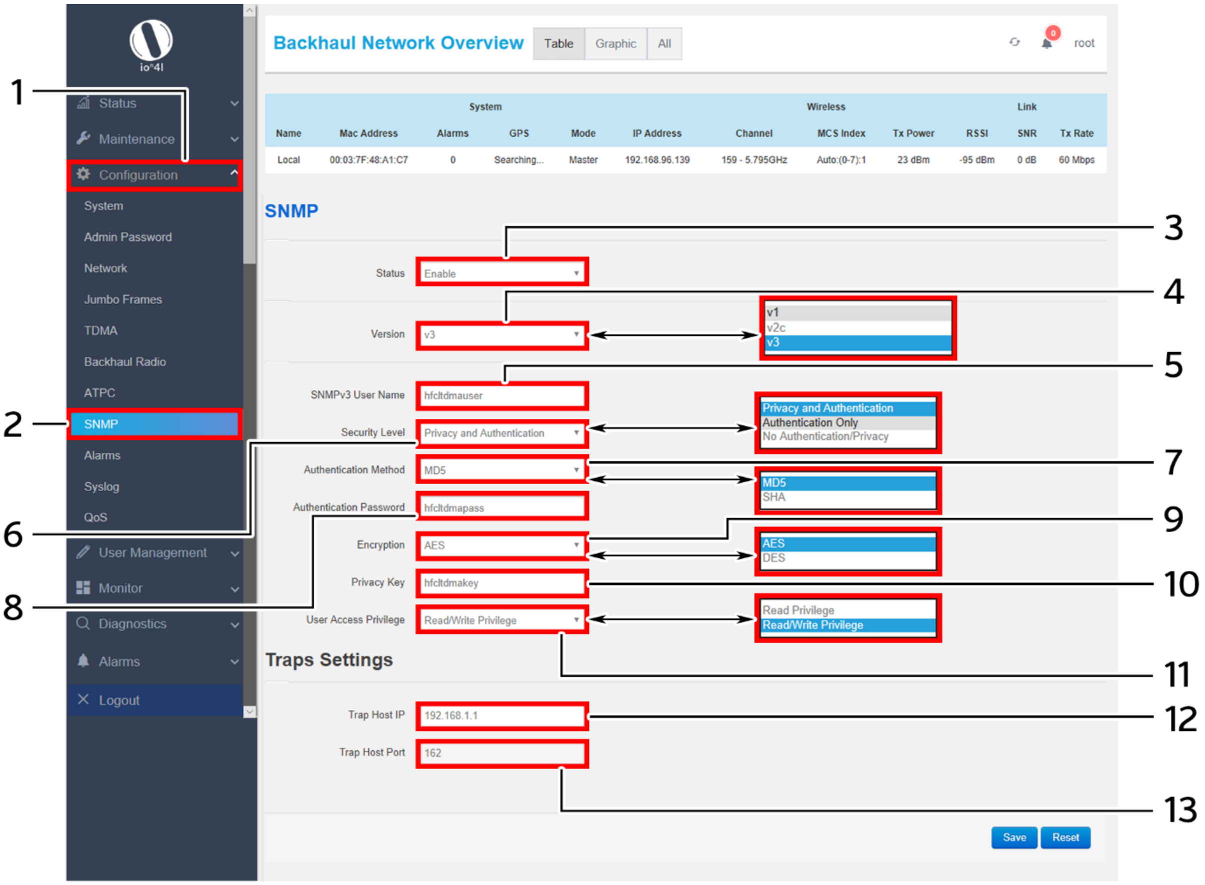
Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	SNMP	Click on "SNMP" option
3.	Status	Enable/Disable SNMP with this option. Provide below parameters if enabled
4.	SNMP Version	Set the version to v1 or v2c from the dropdown list (v1/v2c/v3) for the SNMP template
5.	Read Only Community	Enter a string for "Read Only Community". The same is matched with read community string of EMS SNMP template for authentication. The EMS can read the UBR data only if the strings are matched

Callout	Name	Description
6.	Read-Write Community	Enter a string for "Read-Write Community". The same is matched with write community string of EMS SNMP template for authentication. The EMS can write the UBR data only if the strings are matched
7.	Trap Community	Enter a string for "trap Community". The same is matched with trap community string of EMS SNMP template for authentication. The UBR will send the traps to the EMS only if the strings are matched. Traps are the events generated from the device and will be sent to the Trap Host IP
8.	Trap Host IP	Enter the "Trap Host IP" address (EMS IP Address). All the traps of the respective UBR are sent to the entered host IP
9.	Trap Host Port	Enter the "Trap Host port". Traps are sent to the particular application port

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

SNMP Version-v3:

A basic overview of the SNMP Configuration screen is given below:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

SNMP

Status: Enable

Version: v3 (v1 / v2c / v3)

SNMPv3 User Name: hfcltdmauser

Security Level: Privacy and Authentication (Privacy and Authentication / Authentication Only / No Authentication/Privacy)

Authentication Method: MD5 (MD5 / SHA)

Authentication Password: hfcltdmapass

Encryption: AES (AES / DES)

Privacy Key: hfcltdmakey

User Access Privilege: Read/Write Privilege (Read Privilege / Read/Write Privilege)

Traps Settings

Trap Host IP: 192.168.1.1

Trap Host Port: 162

Figure 39: Basic overview of the SNMP Configuration screen (v3)

Follow the steps given below and configure the SNMP settings (v3) for the UBR:

Table 33: List of actions to configure the SNMP settings (v3)

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	SNMP Configuration	Click on "SNMP Configuration" option
3.	Status	Enable/Disable SNMP with this option. Provide below parameters if enabled
4.	SNMP Version	Set the version to v3 from the dropdown list (v1/v2c/v3) for the SNMP template
5.	SNMPv3 User Name	Enter a unique name for the SNMPv3 template
6.	Security Level	Select the security level from the dropdown list (Privacy Authentication/Authentication Only/ No Authentication/Privacy). 1. Enter all of the following parameters, if security level is selected to "Privacy Authentication".

Callout	Name	Description
		2. Only “User Access Privilege” parameter is needed in case of “No Authentication/Privacy” type of security level. 3. In case the user has selected “Authentication Only” type of security level, “Authentication Method” and “Authentication Password” is required along with “User Access Privilege” parameter
7.	Authentication Method	Select the authentication method from the dropdown list (MD5/SHA)
8.	Authentication Password	Enter a password for the selected authentication method
9.	Encryption	Select the type of encryption from the dropdown list (AES/DES)
10.	Privacy Key	Enter a key for the type of selected encryption
11.	User Access Privilege	Select the type of privilege for the user from the dropdown list (Read Privilege/Read &Write Privilege)
12.	Trap Host IP	Enter the “Trap Host IP” address (EMS IP Address). All the traps of the respective UBR are sent to the entered host IP
13.	Trap Host Port	Enter the “Trap Host port”. Traps are sent to the particular application port

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

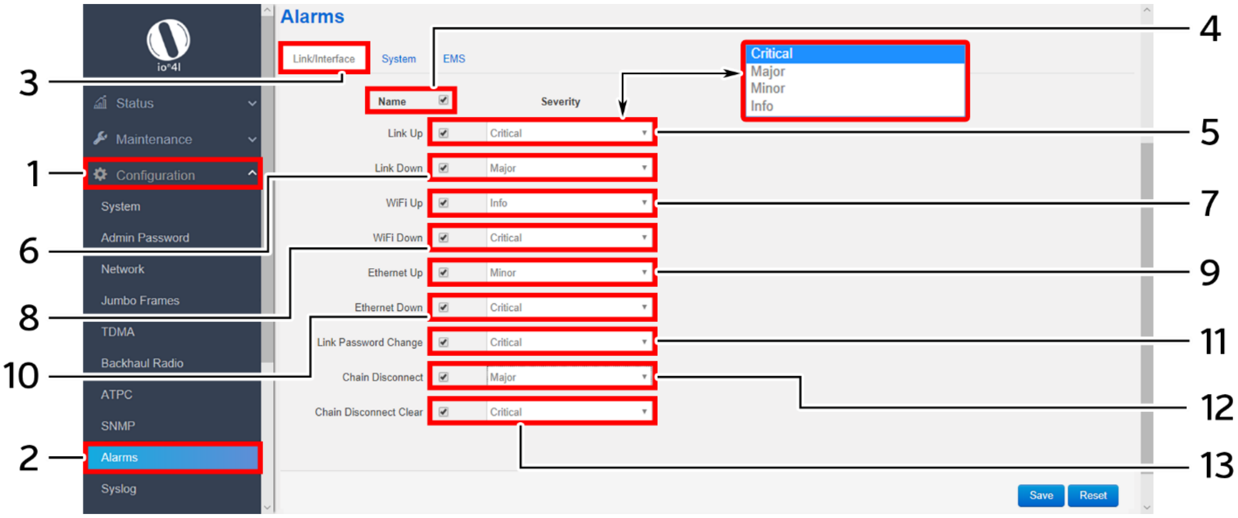
11.9 Alarms Configuration

The user can configure the traps for the respective UBR from this screen. The enabled traps are shown as notifications in the Overview toolbar on the top and will be sent to EMS as traps through SNMP settings. The Alarm screen is further categorized into following sections:

1. Link/Interface Alarms
2. System Alarms
3. SNMP Alarms
4. Alarms Settings

11.9.1 Link/Interface Alarms

A basic overview of the Alarm Configuration screen to configure link/interface alarms is given below:



Link Up ☑ Critical
Link Down ☑ Major
WiFi Up ☑ Info
WiFi Down ☑ Critical
Ethernet Up ☑ Minor
Ethernet Down ☑ Critical
Link Password Change ☑ Critical
Chain Disconnect ☑ Major
Chain Disconnect Clear ☑ Critical

Figure 40: Basic overview of the Alarm Configuration screen to configure link/interface alarms

Follow the steps given below and configure the link/interface alarms for the UBR:

Table 34: List of actions to configure Link/Interface Alarms

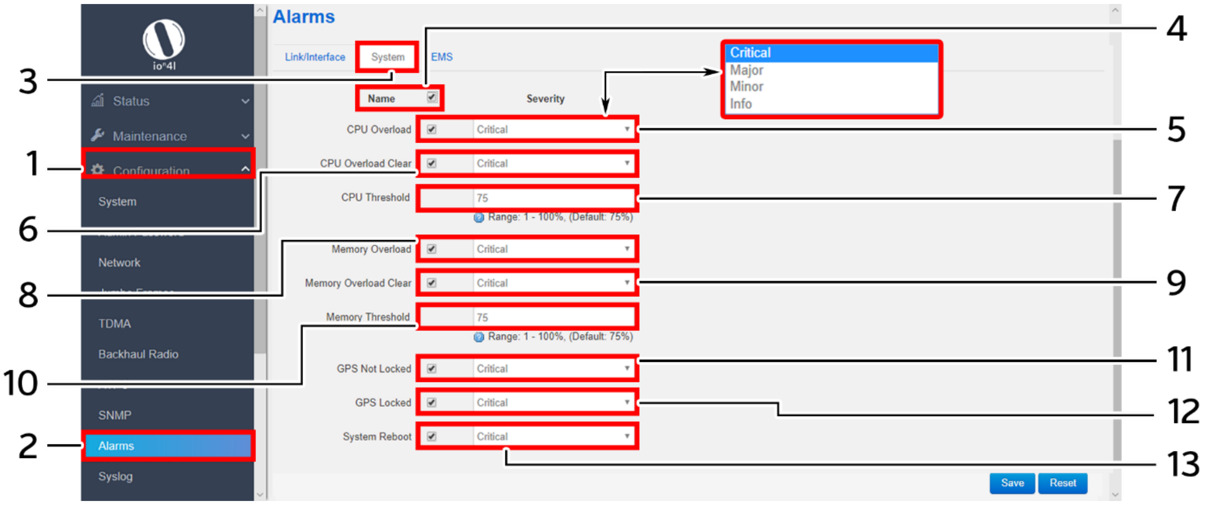
Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Alarms	Click on "Alarms" option
3.	Link/Interface Alarms	Click on "Link/Interface" option
4.	Select All Alarms	Click on the check box and select all alarms or select below alarms individually
5.	Link Up	Enable/Disable the "Link Up" alarm. If enabled, the notification of link up will be shown at local GUI and the trap will be sent to the EMS for the same. If "Link Up" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
6.	Link Down	Enable/Disable the "Link Down" alarm option. If enabled, the notification of link down will be shown at local GUI and the trap will be sent to the EMS for the

Callout	Name	Description
		same. If "Link down" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
7.	Wi-Fi up	Enable/Disable the "Wi-Fi up" alarm option. If enabled, the notification of Wi-Fi up will be shown at local GUI and the trap will be sent to the EMS for the same. If "Wi-Fi Up" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
8.	Wi-Fi down	Enable/Disable the "Wi-Fi down" alarm. If enabled, the notification of Wi-Fi down will be shown at local GUI and the trap will be sent to the EMS for the same. If "Wi-Fi down" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
9.	Ethernet Up	Enable/Disable the "Ethernet Up" alarm option. If enabled, the notification of ethernet up will be shown at local GUI and the trap will be sent to the EMS for the same. If "Ethernet Up" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
10.	Ethernet Down	Enable/Disable the "Ethernet Down" alarm option. If enabled, the notification of ethernet down will be shown at local GUI and the trap will be sent to the EMS for the same. If "Ethernet down" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
11.	Link Password Change	Enable/Disable the "Link Password Change" alarm. If enabled, the notification of link password change will be shown at local GUI and the trap will be sent to the EMS for the same. If "Link Password Change" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
12.	Chain Disconnect	Enable/Disable the "Chain Disconnect" alarm. If enabled, the notification of any disconnect in chain will be shown at local GUI and the trap will be sent to the EMS for the same. If "Chain Disconnect" alarm is enabled, set the severity level to Critical, Major, Minor, or Info
13.	Chain Disconnect Clear	Enable/Disable the "Chain Disconnect Clear" alarm. If enabled, the notification is shown at local GUI whenever the chain disconnect alarm is cleared and the trap for the same is sent to the EMS. If "Chain Disconnect Clear" alarm is enabled, set the severity level to Critical, Major, Minor, or Info

Click "Save" to save the link/interface alarms configuration or click "Reset" to configure the same again.

11.9.2 System Alarms

A basic overview of the Alarm Configuration screen to configure system alarms is given below:



Name ☑	Severity
CPU Overload	☑ Critical
CPU Overload Clear	☑ Critical
CPU Threshold	75 Range: 1 - 100%, (Default: 75%)
Memory Overload	☑ Critical
Memory Overload Clear	☑ Critical
Memory Threshold	75 Range: 1 - 100%, (Default: 75%)
GPS Not Locked	☑ Critical
GPS Locked	☑ Critical
System Reboot	☑ Critical

Figure 41: Basic overview of the Alarm Configuration screen to configure system alarms

Follow the steps given below and configure the system alarms for the UBR:

Table 35: List of actions to configure system Alarms

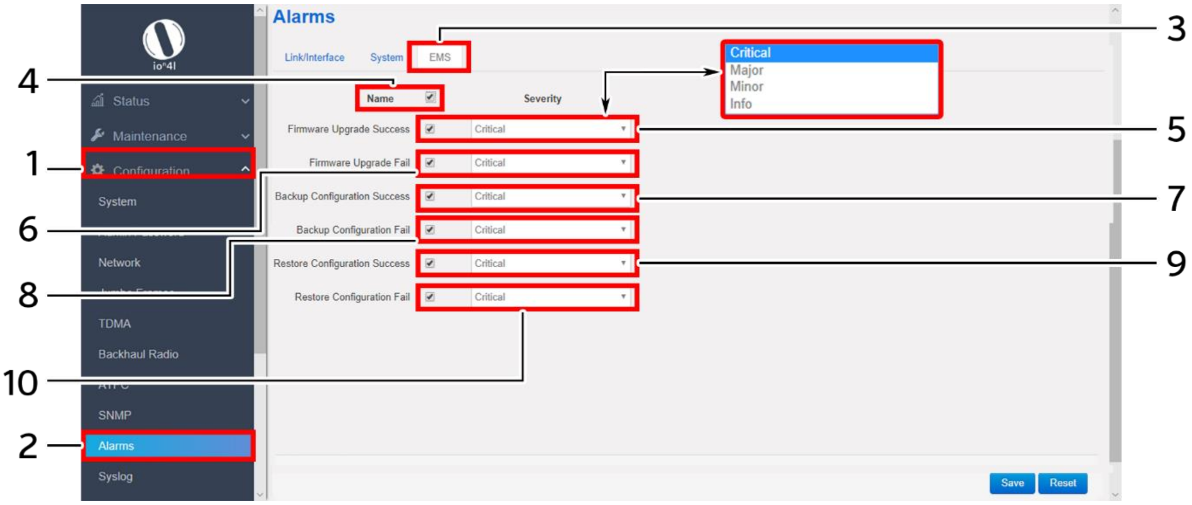
Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Event Alarm	Click on "Event Alarm" option
3.	System Alarms	Click on "System Alarms" option
4.	Select All Alarms	Click on the check box and select all alarms or select below alarms individually
5.	CPU Overload	Enable/Disable the "CPU Overload" alarm option. The CPU overload is determined with respect to the selected "CPU Threshold". If enabled, the notification of CPU overload will be shown at local GUI and the trap will be sent to the EMS for the same, once it has gone above the defined "CPU Threshold" value. Set the severity level to Critical, Major, Minor, or Info
6.	CPU Overload Clear	Enable/Disable the "CPU Overload Clear" alarm option. The CPU clear load is determined with respect to the selected "CPU Threshold". If enabled, the notification of CPU clear load will be shown at local GUI and the trap will be sent to the EMS for the same, once the CPU load has gone below the defined "CPU Threshold" value. Set the severity level to Critical, Major, Minor, or Info
7.	CPU Threshold	If "CPU Overload" alarm is enabled, set the threshold value for the same
8.	Memory Overload	Enable/Disable the "Memory Overload" alarm option. The memory overload of UBR is determined with respect to the selected "Memory Threshold". If enabled, the notification of memory overload will be shown at local GUI and the trap will be sent to the

Callout	Name	Description
		EMS for the same, once it has gone above the "Memory Threshold" value. Set the severity level to Critical, Major, Minor, or Info
9.	Memory Overload Clear	Enable/Disable the "Memory Overload Clear" option. The memory clear load is determined with respect to the selected "Memory Threshold". If enabled, the notification of memory clear load will be shown at local GUI and the trap will be sent to the EMS for the same, once the memory load has gone below the "Memory Threshold" value. Set the severity level to Critical, Major, Minor, or Info
10.	Memory Threshold	If "Memory Overload" alarm is enabled, set the threshold value for the same
11.	GPS Not Locked	Enable/Disable the "GPS Not Locked" alarm option. If enabled, the notification of not locked GPS will be shown at local GUI and the trap will be sent to the EMS for the same Set the severity level to Critical, Major, Minor, or Info
12.	GPS Locked	Enable/Disable the "GPS Locked" alarm option. If enabled, the notification of locked GPS will be shown at local GUI and the trap will be sent to the EMS for the same Set the severity level to Critical, Major, Minor, or Info
13.	System Reboot	Enable/Disable the "System Reboot" alarm option. If enabled, the notification of system reboot will be shown at local GUI and the trap will be sent to the EMS for the same Set the severity level to Critical, Major, Minor, or Info

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

11.9.4 EMS Alarms

A basic overview of the Alarm Configuration screen to configure EMS alarms is given below:



Name ☑		Severity
Firmware Upgrade Success	☑	Critical
Firmware Upgrade Fail	☑	Critical
Backup Configuration Success	☑	Critical
Backup Configuration Fail	☑	Critical
Restore Configuration Success	☑	Critical
Restore Configuration Fail	☑	Critical

Figure 42: Basic overview of the Alarm Configuration screen to configure EMS alarms

Follow the steps given below and configure the EMS alarms for the UBR:

Table 36: List of actions to configure EMS Alarms

Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	Alarms	Click on “Alarms” option
3.	EMS Alarms	Click on “EMS” option
4.	Select All Alarms	Click on the check box and select all alarms or select below alarms individually
5.	Firmware Upgrade Success	Enable/Disable the “Firmware Upgrade Success” alarm option. If enabled, the notification of successful firmware upgrade is shown at local GUI whenever the firmware is upgraded with the latest version, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info
6.	Firmware Upgrade Fail	Enable/Disable the “Firmware Upgrade Fail” alarm option. If enabled, the notification of failed firmware upgrade is shown at local GUI whenever the firmware has failed to upgrade with the latest version, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info
7.	Backup Configuration Success	Enable/Disable the “Backup Configuration Success” alarm option. If enabled, the notification of successful backup is shown at local GUI whenever any backup is created for the UBR device, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info
8.	Backup Configuration Fail	Enable/Disable the “Backup Configuration Fail” alarm option. If enabled, the notification of failed backup is

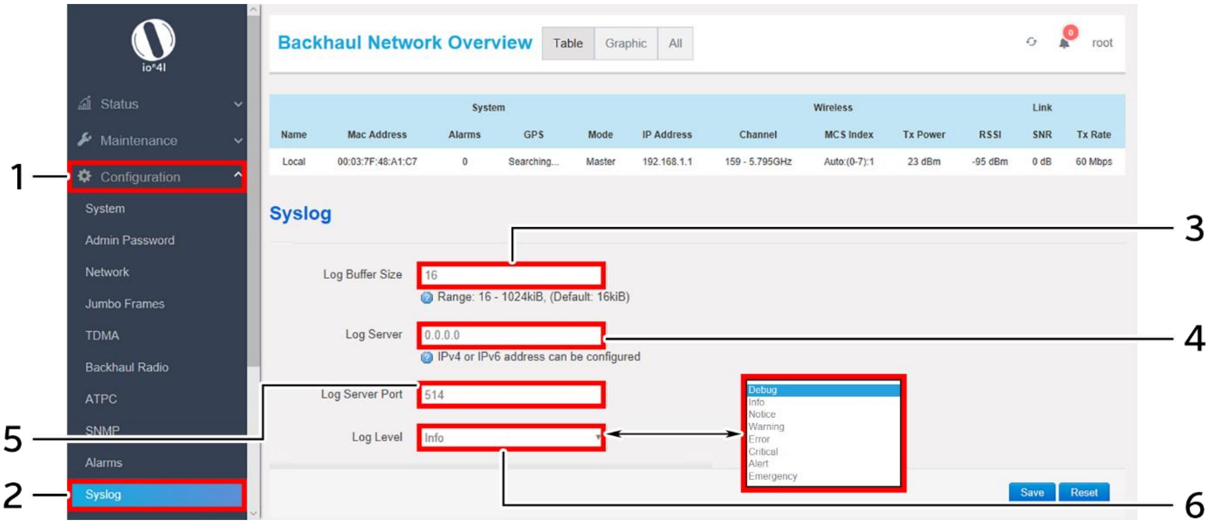
Callout	Name	Description
		shown at local GUI whenever the respective UBR device has failed to generate backup, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info
9.	Restore Configuration Success	Enable/Disable the "Restore Configuration Success" alarm option. If enabled, the notification of successful configuration upload is shown at local GUI whenever any backup or configuration file is restored in the UBR device, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info
10.	Restore Configuration Fail	Enable/Disable the "Restore Configuration Fail" alarm option. If enabled, the notification of failed configuration upload is shown at local GUI whenever any backup or configuration file has failed to be uploaded in the UBR device, and the trap is sent to the EMS for the same. Set the severity level to Critical, Major, Minor, or Info

Click "Save" to save the EMS Backup/Restore Alarms configuration or click "Reset" to configure the same again.

11.10 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 are sent to the logging server based on the configured log level.

A basic overview of the Syslog Configuration screen is given below:



System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.1.1	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

Syslog

Log Buffer Size: 16
Range: 16 - 1024kiB, (Default: 16kiB)

Log Server: 0.0.0.0
IPv4 or IPv6 address can be configured

Log Server Port: 514

Log Level: Info

Debug
Info
Notice
Warning
Error
Critical
Alert
Emergency

Figure 43: Basic overview of the Syslog Configuration screen

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

Table 37: 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.

11.11 Configuration of traffic management (Quality of Service)

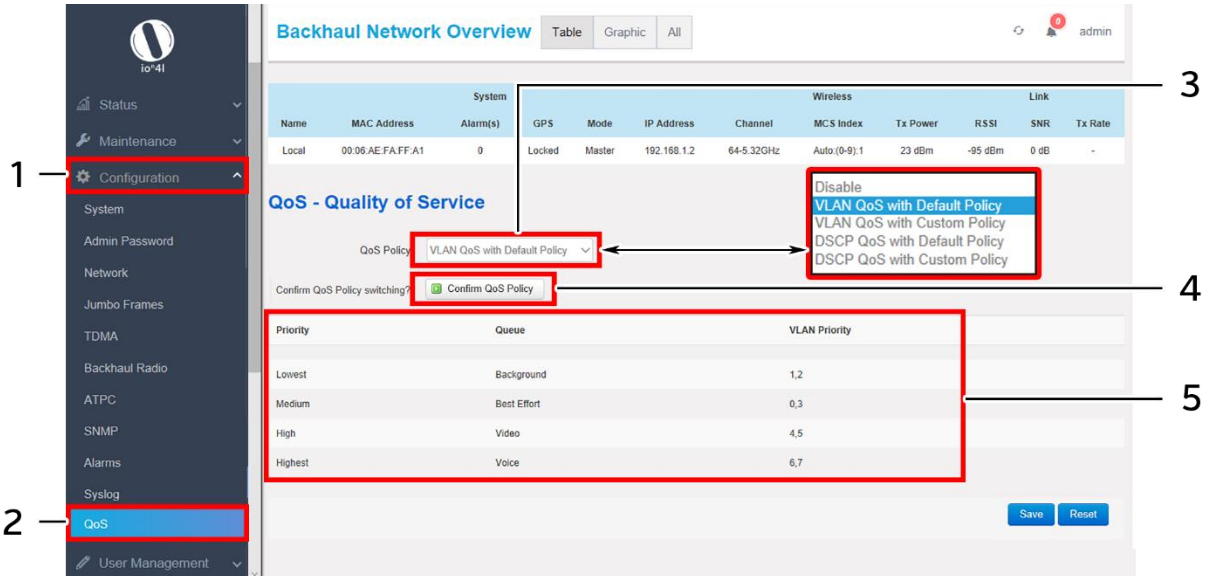
Quality of service (QoS) involves controlling and managing network traffic by setting priorities for specific types of data (background, best effort, video, and audio traffic) on the network. IEEE P802.1p is the name of a task group that provides a mechanism for implementing quality of service (QoS)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

11.11.1 VLAN QoS with Default Policy

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



		System				Wireless			Link	
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):1	23 dBm	-95 dBm	0 dB	-

QoS - Quality of Service

QoS Policy: VLAN QoS with Default Policy

Confirm QoS Policy switching? Confirm QoS Policy

Priority	Queue	VLAN Priority
Lowest	Background	1,2
Medium	Best Effort	0,3
High	Video	4,5
Highest	Voice	6,7

Figure 44: 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 38: List of actions to configure the VLAN QoS with default policy

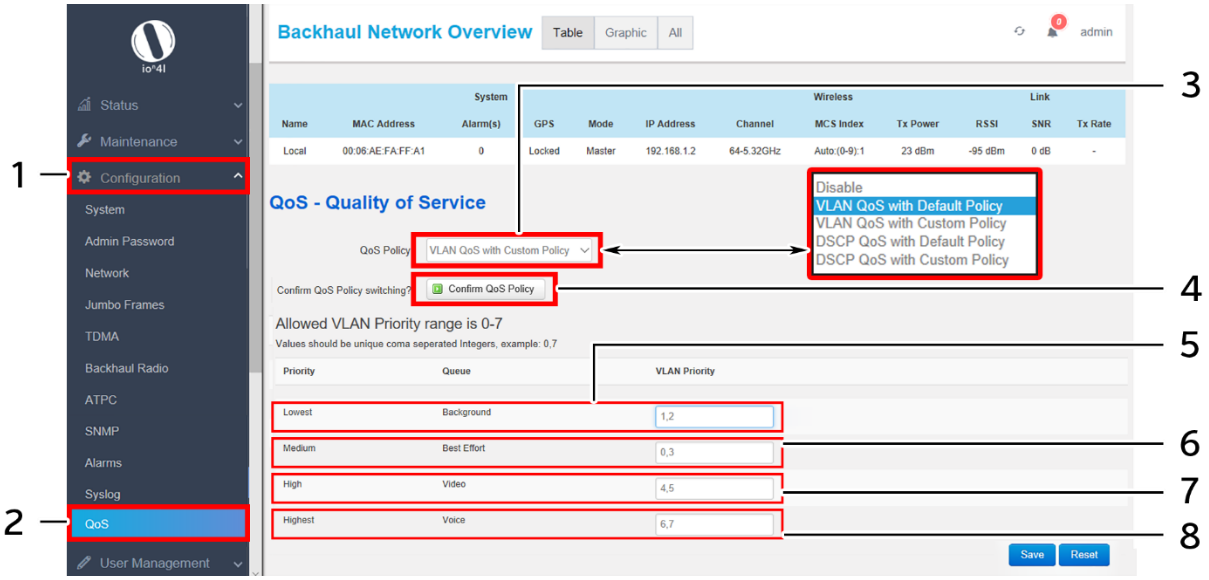
Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	QoS	Click on “QoS” option
3.	QoS Policy	Set the QoS policy to “VLAN QoS with Default Policy” from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/

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.

11.11.2 VLAN QoS with Custom Policy

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



System			Wireless							Link	
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):1	23 dBm	-95 dBm	0 dB	-

QoS - Quality of Service

QoS Policy: VLAN QoS with Custom Policy

Confirm QoS Policy switching?

Allowed VLAN Priority range is 0-7

Values should be unique coma seperated Integers, example: 0,7

Priority	Queue	VLAN Priority
Lowest	Background	1,2
Medium	Best Effort	0,3
High	Video	4,5
Highest	Voice	6,7

Figure 45: 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:

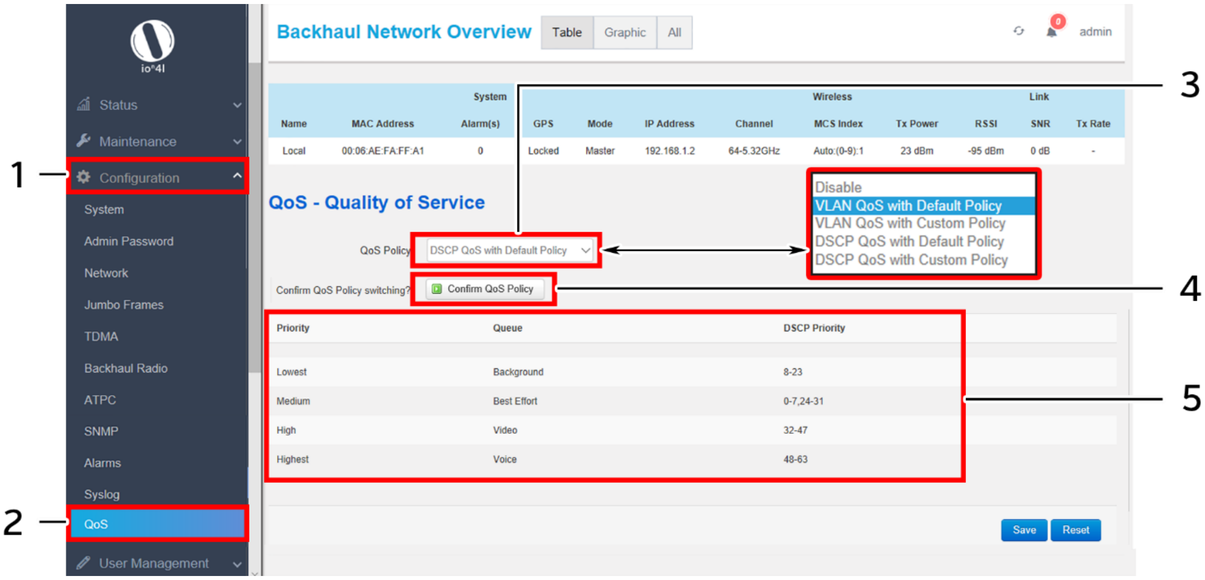
Table 39: List of actions to configure the VLAN QoS with custom policy

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.

11.11.3 DSCP QoS with Default Policy

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



	System		Wireless						Link		
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):1	23 dBm	-95 dBm	0 dB	-

QoS Policy: DSCP QoS with Default Policy

Confirm QoS Policy switching?

Priority	Queue	DSCP Priority
Lowest	Background	8-23
Medium	Best Effort	0-7,24-31
High	Video	32-47
Highest	Voice	48-63

Figure 46: 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:

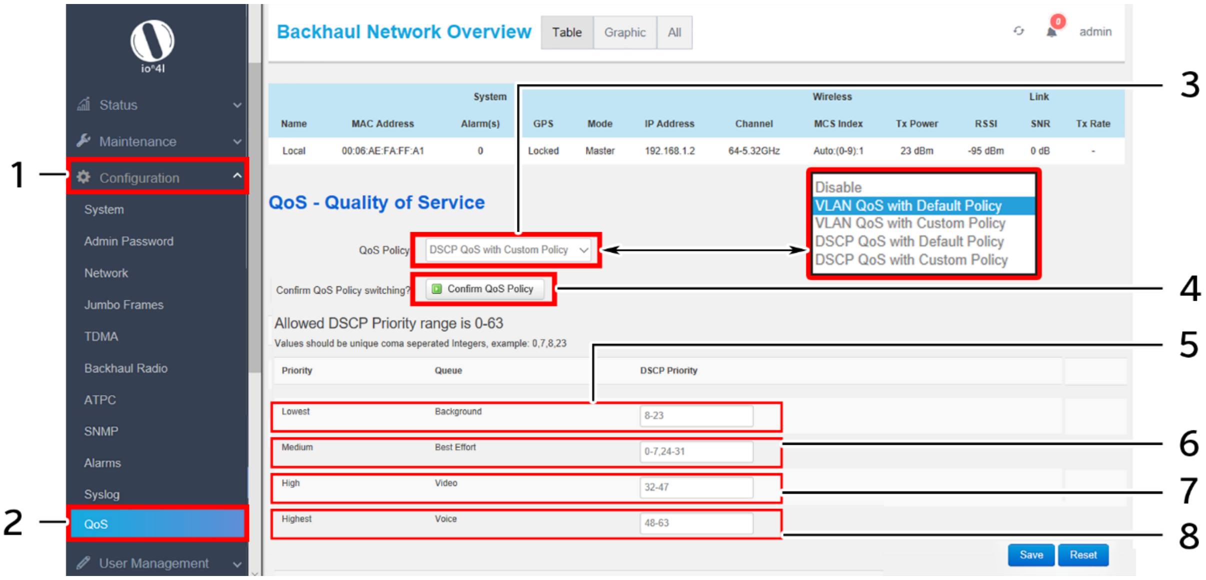
Table 40: List of actions to configure the DSCP QoS with default policy

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.

11.11.4 DSCP QoS with Custom Policy

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



System			Wireless							Link	
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):1	23 dBm	-95 dBm	0 dB	-

QoS Policy: DSCP QoS with Custom Policy

Disable
VLAN QoS with Default Policy
VLAN QoS with Custom Policy
DSCP QoS with Default Policy
DSCP QoS with Custom Policy

Confirm QoS Policy switching?

Allowed DSCP Priority range is 0-63

Values should be unique coma seperated Integers, example: 0,7,8,23

Priority	Queue	DSCP Priority
Lowest	Background	8-23
Medium	Best Effort	0-7,24-31
High	Video	32-47
Highest	Voice	48-63

Figure 47: 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 41: List of actions to configure the DSCP QoS with custom policy

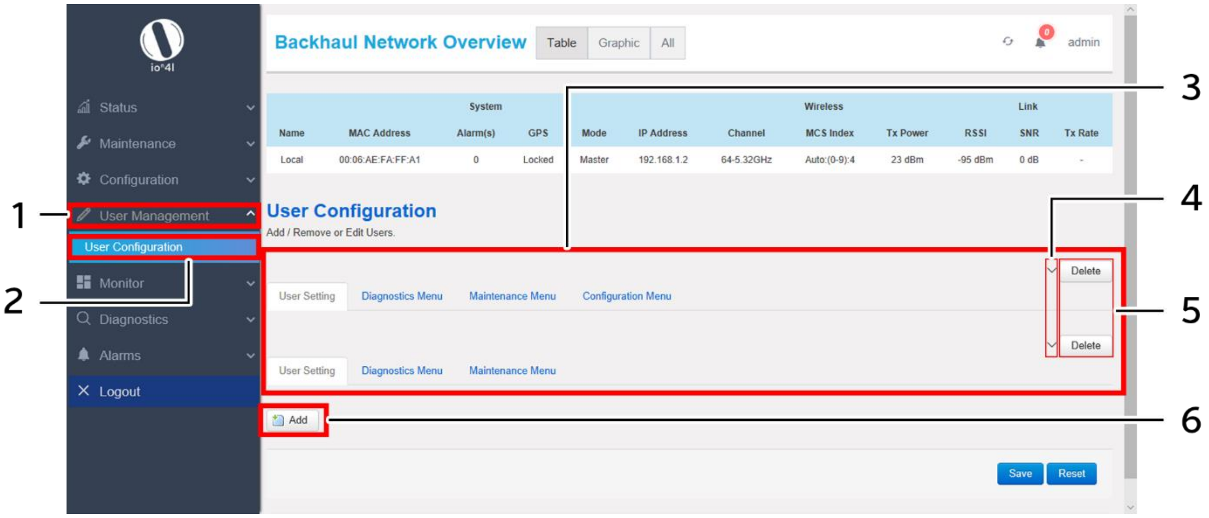
Callout	Name	Description
1.	Configuration	Click on “Configuration” dropdown
2.	QoS	Click on “QoS” option
3.	QoS Policy	Set the QoS policy to “DSCP QoS with Custom Policy” from the dropdown list (VLAN QoS with Default Policy/ VLAN QoS with Custom Policy/ DSCP QoS with Default Policy/ DSCP QoS with Custom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

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:



	System			Wireless					Link		
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):4	23 dBm	-95 dBm	0 dB	-

User Configuration

Add / Remove or Edit Users.

Figure 48: Basic overview of user configuration screen

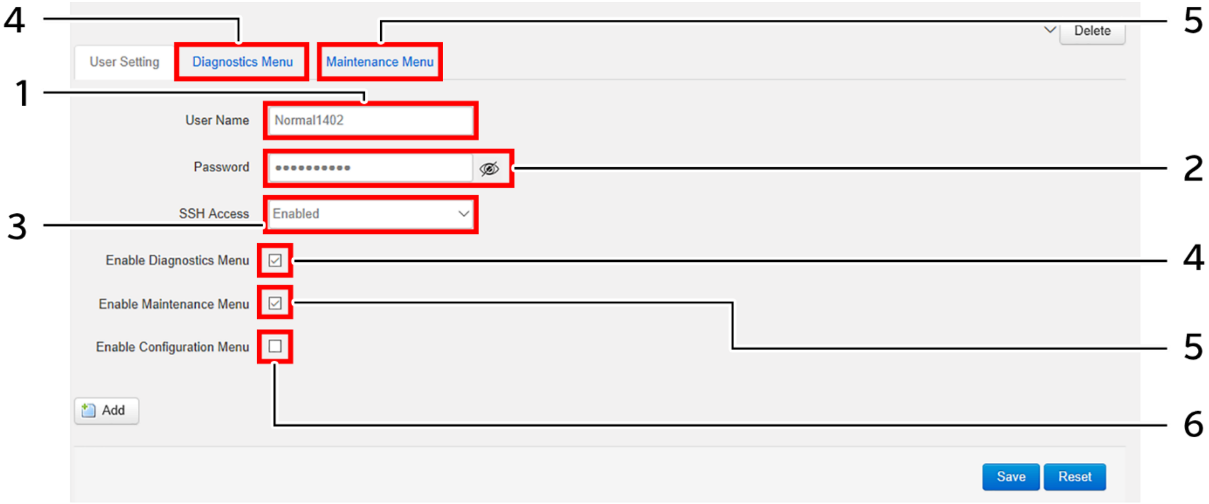
Follow the steps below to view the list of added users:

Table 42: 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 48: 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:



User Name: Normal1402

Password: ••••••••••

SSH Access: Enabled

Enable Diagnostics Menu ☑

Enable Maintenance Menu ☑

Enable Configuration Menu □

Figure 49: 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 43: 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 49: 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:

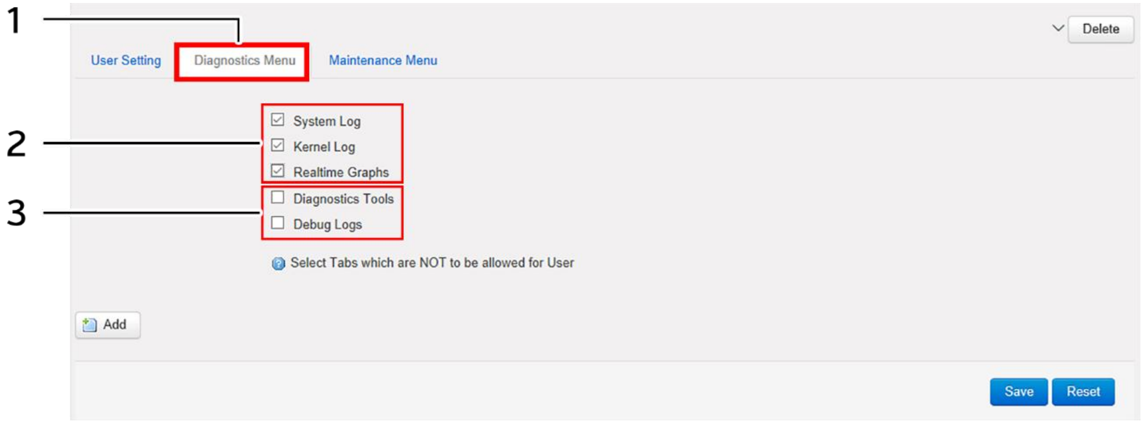


Figure 50: User configuration screen to further manage the user access to diagnostic screen options

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

Table 44: List of actions to configure the user's access for maintenance screen options

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

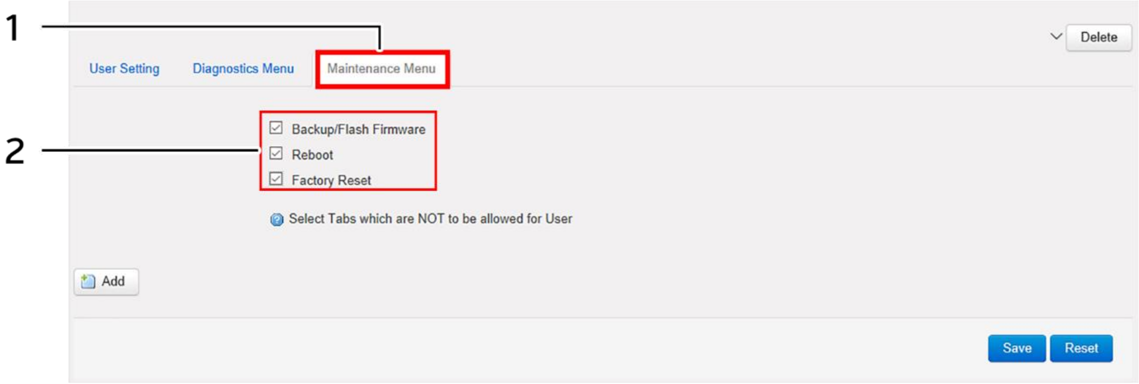
Callout	Name	Description
2.	Allow Access	Click on the check box and select options available in diagnostics screen. The respective user will have access to selected screens
3.	Restrict Access	Click on the check box and deselect options available in diagnostics screen. The respective user will not have 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 49: 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:



☑ Backup/Flash Firmware
☑ Reboot
☑ Factory Reset

Select Tabs which are NOT to be allowed for User

Figure 51: 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 45: 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 49: Basic overview of user configuration parameters" and click on "Configuration Menu" tab (6).

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

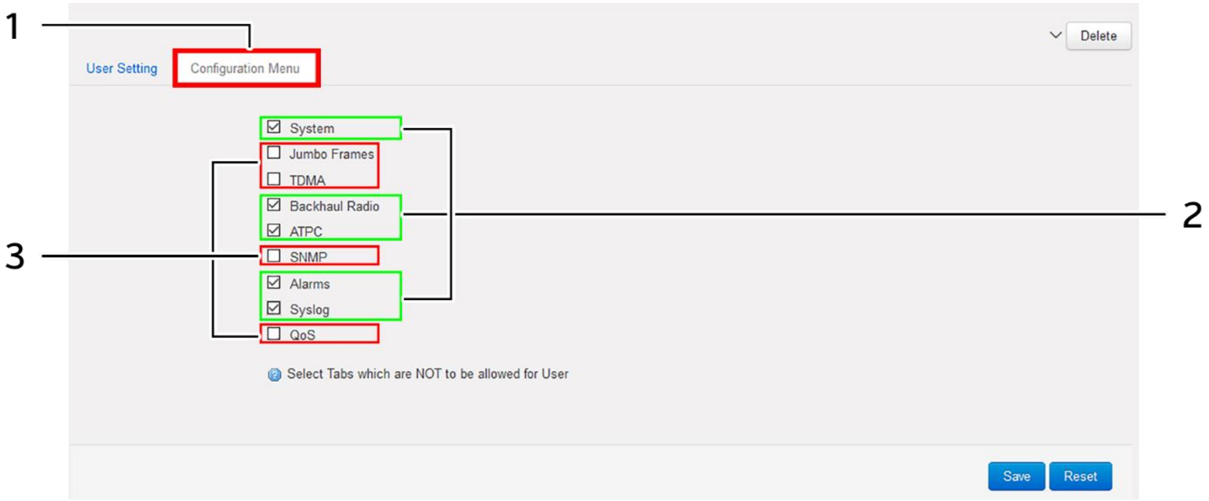


Figure 52: User configuration screen to further manage the user access to configuration screen options

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

Table 46: 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

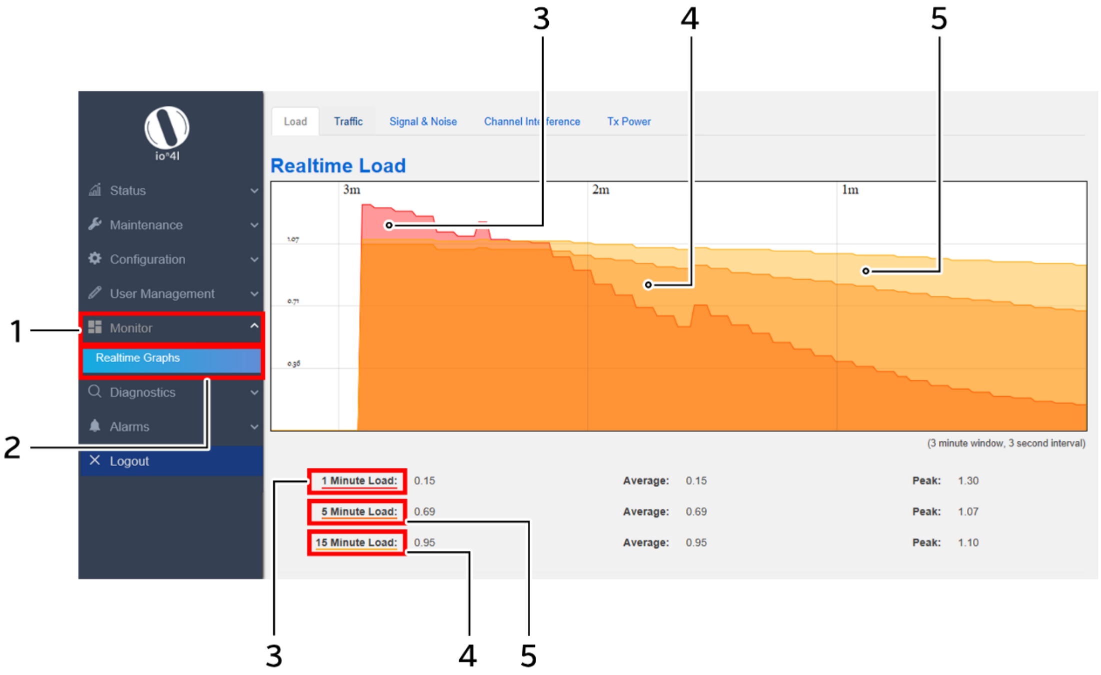
The performance of the connected UBR is monitored from this screen. The list of options available for the user is given below:

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:



1 Minute Load: 0.15 Average: 0.15 Peak: 1.30
5 Minute Load: 0.69 Average: 0.69 Peak: 1.07
15 Minute Load: 0.95 Average: 0.95 Peak: 1.10

Figure 53: Basic overview of the Real-time Graphs/Load screen

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

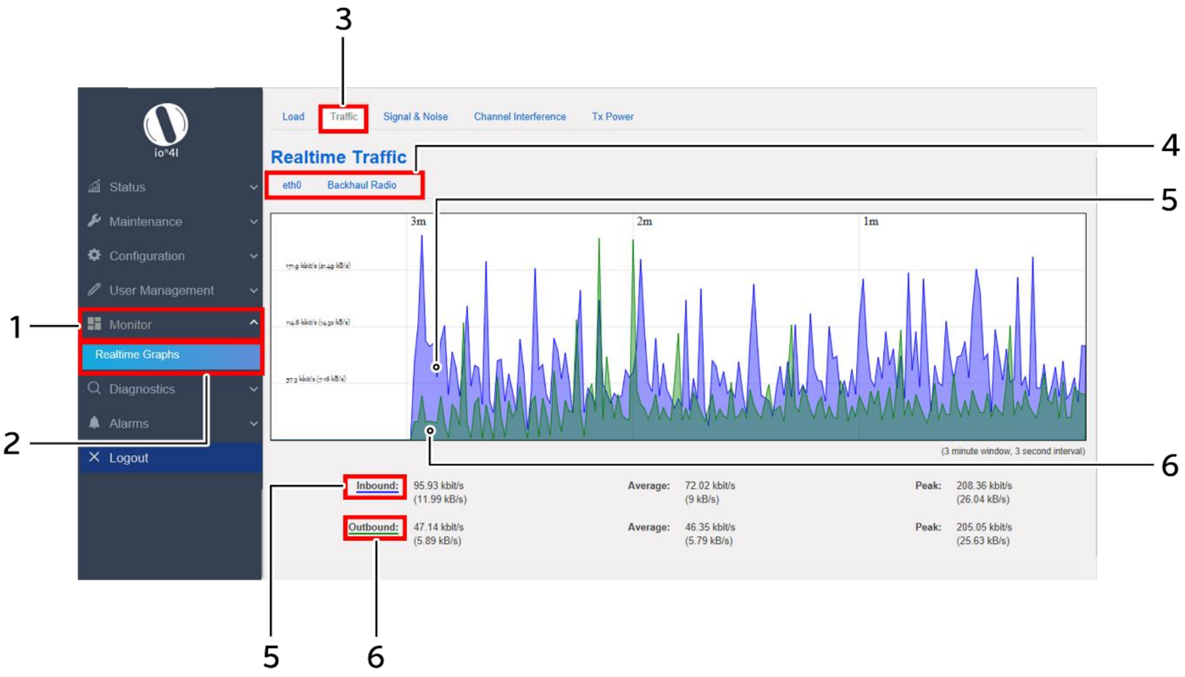
Table 47: List of actions to view real-time load graphs

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:



Inbound: 95.93 kbit/s (11.99 kB/s) Average: 72.02 kbit/s (9 kB/s) Peak: 208.36 kbit/s (26.04 kB/s)

Outbound: 47.14 kbit/s (5.89 kB/s) Average: 46.35 kbit/s (5.79 kB/s) Peak: 205.05 kbit/s (25.63 kB/s)

Figure 54: Basic overview of the Real-time Graphs/Traffic screen

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

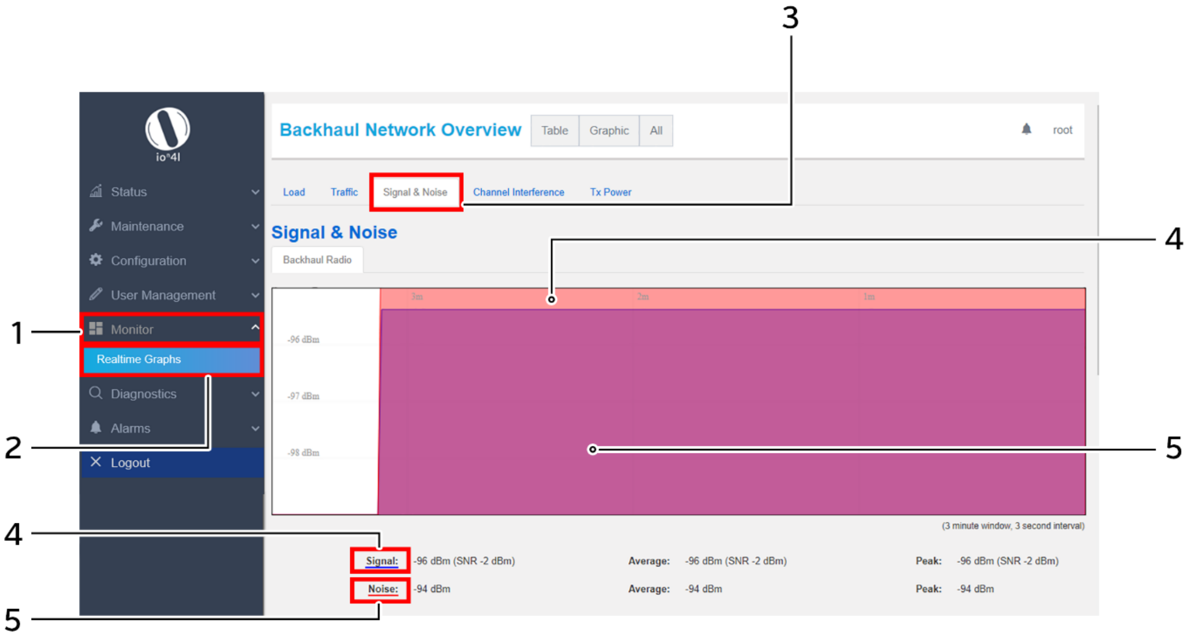
Table 48: List of actions to view real-time traffic graphs

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:



Signal: -96 dBm (SNR -2 dBm) Average: -96 dBm (SNR -2 dBm) Peak: -96 dBm (SNR -2 dBm)
Noise: -94 dBm Average: -94 dBm Peak: -94 dBm

Figure 55: Basic overview of the Real-time Graphs/Signal & Noise screen

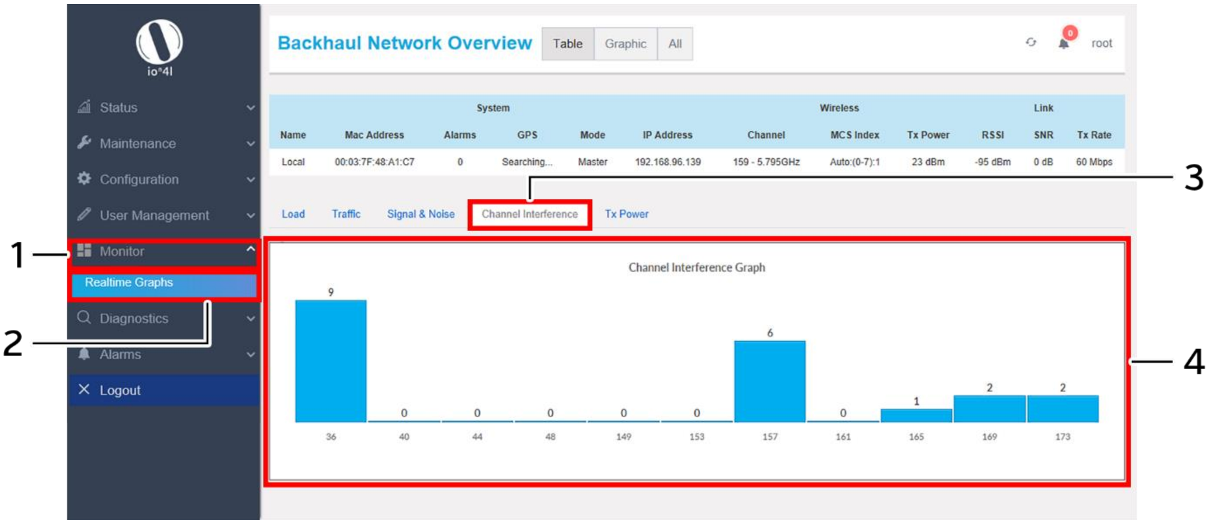
Follow the steps given below to view the real-time Signal & Noise graphs for the UBR:

Table 49: 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:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

Figure 56: 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:

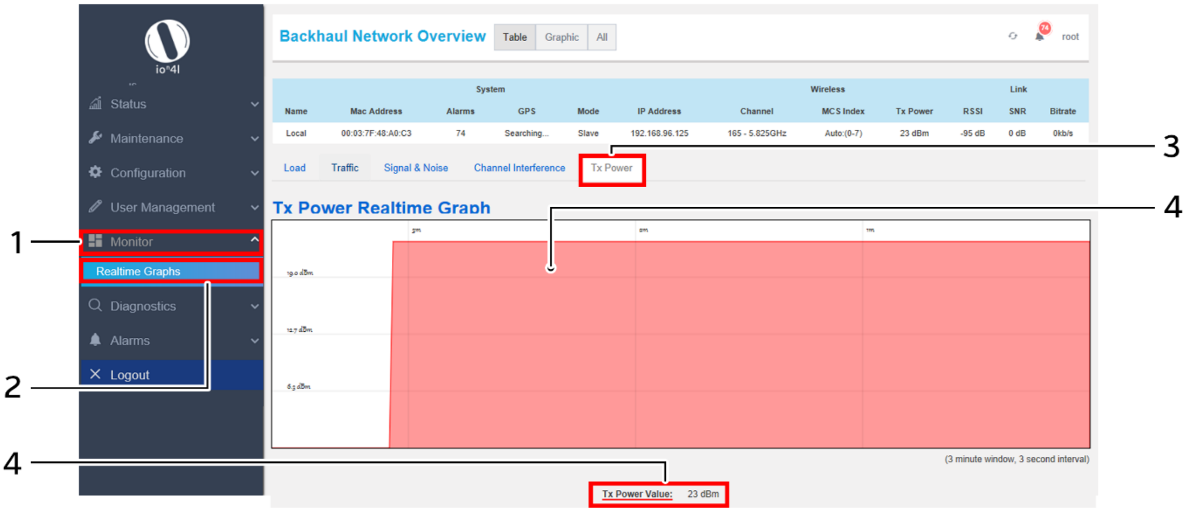
Table 50: List of actions to view real-time channel interference graphs

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:



		System					Wireless			Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Bitrate
Local	00:03:7F:48:A0:C3	74	Searching...	Slave	192.168.96.125	165 - 5.825GHz	Auto:(0-7)	23 dBm	-95 dB	0 dB	0kb/s

(3 minute window, 3 second interval)

Tx Power Value: 23 dBm

Figure 57: 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 51: 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

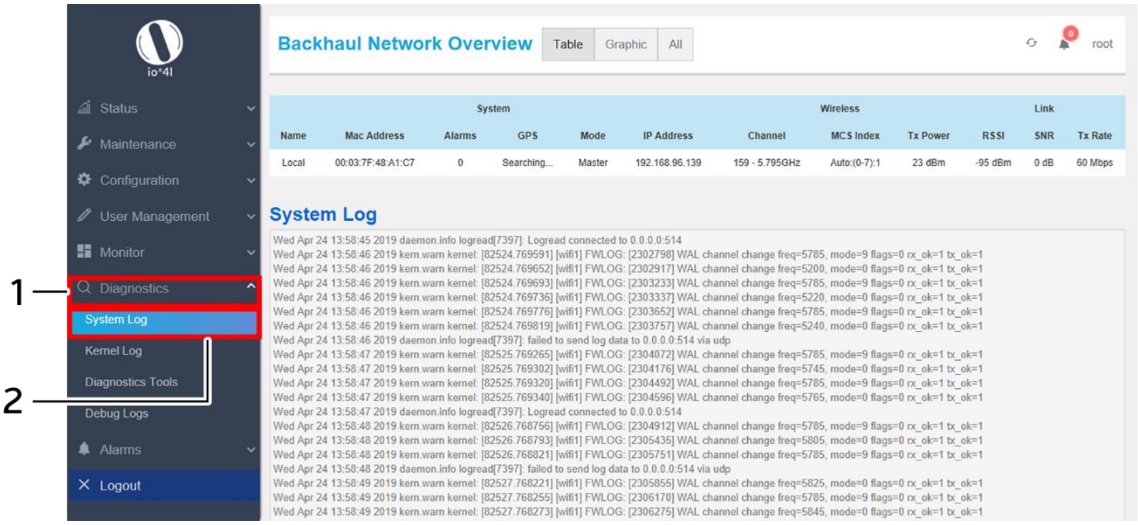
The diagnostic activities of the connected UBR are executed from this screen. The list of options available for the user is given below:

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:



System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

System Log

```
Wed Apr 24 13:58:45 2019 daemon.info logread[7397]: Logread connected to 0.0.0.0:514
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769591] [wifi1] FWLOG: [2302798] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769652] [wifi1] FWLOG: [2302917] WAL channel change freq=5200, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769693] [wifi1] FWLOG: [2303233] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769736] [wifi1] FWLOG: [2303337] WAL channel change freq=5220, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769776] [wifi1] FWLOG: [2303652] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 kern.warn kernel: [82524.769819] [wifi1] FWLOG: [2303757] WAL channel change freq=5240, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:46 2019 daemon.info logread[7397]: failed to send log data to 0.0.0.0:514 via udp
Wed Apr 24 13:58:47 2019 kern.warn kernel: [82525.769265] [wifi1] FWLOG: [2304072] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:47 2019 kern.warn kernel: [82525.769302] [wifi1] FWLOG: [2304176] WAL channel change freq=5745, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:47 2019 kern.warn kernel: [82525.769320] [wifi1] FWLOG: [2304492] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:47 2019 kern.warn kernel: [82525.769340] [wifi1] FWLOG: [2304596] WAL channel change freq=5765, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:47 2019 daemon.info logread[7397]: Logread connected to 0.0.0.0:514
Wed Apr 24 13:58:48 2019 kern.warn kernel: [82526.768756] [wifi1] FWLOG: [2304912] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:48 2019 kern.warn kernel: [82526.768793] [wifi1] FWLOG: [2305435] WAL channel change freq=5805, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:48 2019 kern.warn kernel: [82526.768821] [wifi1] FWLOG: [2305751] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:48 2019 daemon.info logread[7397]: failed to send log data to 0.0.0.0:514 via udp
Wed Apr 24 13:58:49 2019 kern.warn kernel: [82527.768221] [wifi1] FWLOG: [2305855] WAL channel change freq=5825, mode=0 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:49 2019 kern.warn kernel: [82527.768255] [wifi1] FWLOG: [2306170] WAL channel change freq=5785, mode=9 flags=0 rx_ok=1 tx_ok=1
Wed Apr 24 13:58:49 2019 kern.warn kernel: [82527.768273] [wifi1] FWLOG: [2306275] WAL channel change freq=5845, mode=0 flags=0 rx_ok=1 tx_ok=1
```

Figure 58: Basic overview of the System Log screen

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

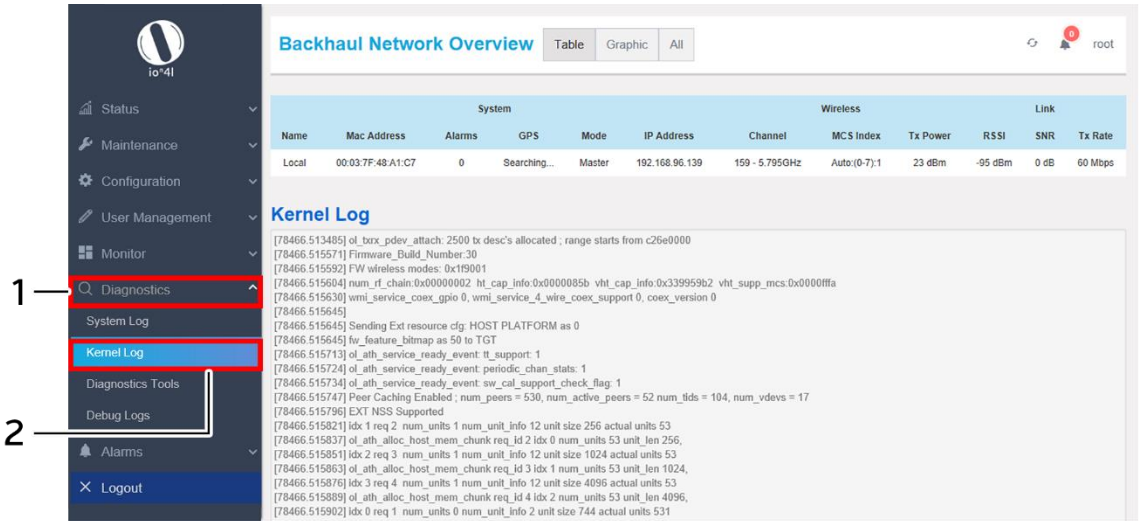
Table 52: List of actions to view the system log

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:



System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

Kernel Log

```
[78466.513485] ol_txrx_pdev_attach: 2500 tx desc's allocated ; range starts from c26e0000
[78466.515571] Firmware_Build_Number:30
[78466.515592] FW wireless modes: 0x1f9001
[78466.515604] num_rf_chain:0x00000002  ht_cap_info:0x0000085b  vht_cap_info:0x339959b2  vht_supp_mcs:0x0000fffa
[78466.515630] wmi_service_coex_gpio 0, wmi_service_4_wire_coex_support 0, coex_version 0
[78466.515645]
[78466.515645] Sending Ext resource cfg: HOST PLATFORM as 0
[78466.515645] fw_feature_bitmap as 50 to TGT
[78466.515713] ol_ath_service_ready_event: tt_support: 1
[78466.515724] ol_ath_service_ready_event: periodic_chan_stats: 1
[78466.515734] ol_ath_service_ready_event: sw_cal_support_check_flag: 1
[78466.515747] Peer Caching Enabled ; num_peers = 530, num_active_peers = 52 num_tids = 104, num_vdevs = 17
[78466.515796] EXT NSS Supported
[78466.515821] idx 1 req 2  num_units 1 num_unit_info 12 unit size 256 actual units 53
[78466.515837] ol_ath_alloc_host_mem_chunk req_id 2 idx 0 num_units 53 unit_len 256,
[78466.515851] idx 2 req 3  num_units 1 num_unit_info 12 unit size 1024 actual units 53
[78466.515863] ol_ath_alloc_host_mem_chunk req_id 3 idx 1 num_units 53 unit_len 1024,
[78466.515876] idx 3 req 4  num_units 1 num_unit_info 12 unit size 4096 actual units 53
[78466.515889] ol_ath_alloc_host_mem_chunk req_id 4 idx 2 num_units 53 unit_len 4096,
[78466.515902] idx 0 req 1  num_units 0 num_unit_info 2 unit size 744 actual units 531
```

Figure 59: Basic overview of the Kernel Log screen

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

Table 53: 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

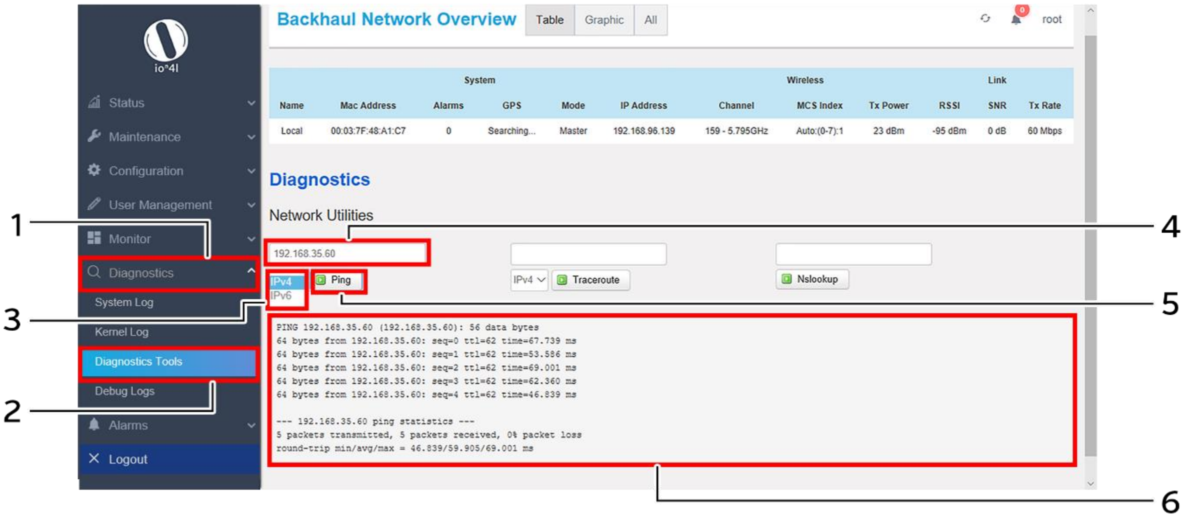
14.3 Diagnostic Tools

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:



	System					Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

192.168.35.60

```
PING 192.168.35.60 (192.168.35.60): 56 data bytes
64 bytes from 192.168.35.60: seq=0 ttl=62 time=67.739 ms
64 bytes from 192.168.35.60: seq=1 ttl=62 time=53.586 ms
64 bytes from 192.168.35.60: seq=2 ttl=62 time=69.001 ms
64 bytes from 192.168.35.60: seq=3 ttl=62 time=62.360 ms
64 bytes from 192.168.35.60: seq=4 ttl=62 time=46.839 ms

--- 192.168.35.60 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 46.839/59.905/69.001 ms
```

Figure 60: Basic overview of the diagnostics tool screen to check the connection status

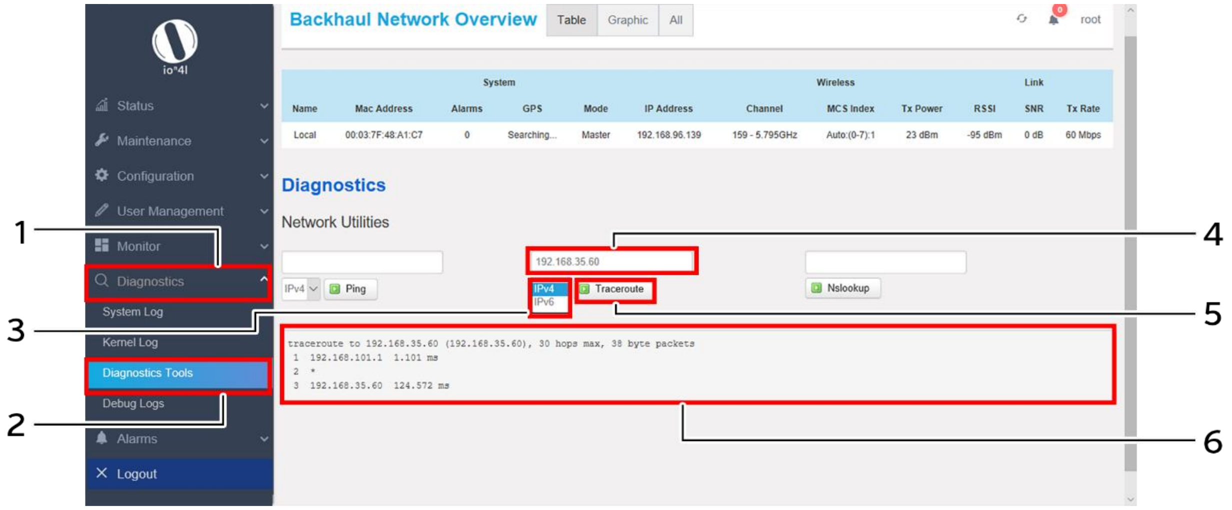
Follow the steps given below to check the connection status:

Table 54: 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:



Backhaul Network Overview

System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

Diagnostics

192.168.35.60

```
traceroute to 192.168.35.60 (192.168.35.60), 30 hops max, 38 byte packets
 1  192.168.101.1  1.101 ms
 2  *
 3  192.168.35.60  124.572 ms
```

Figure 61: Basic overview of the diagnostics tool screen to check the route of established connection

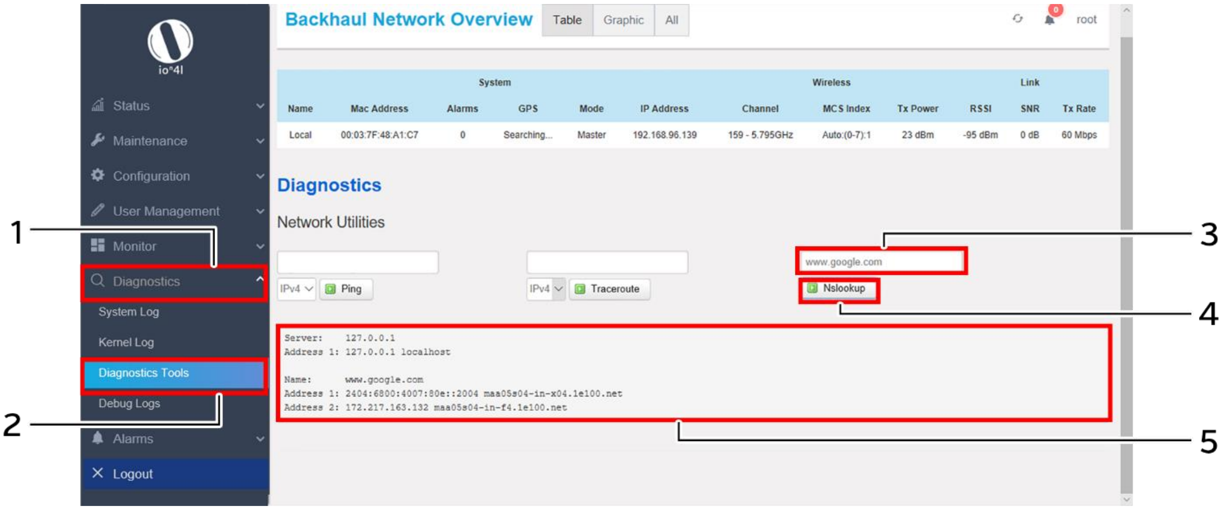
Follow the steps given below to check the route of established connection:

Table 55: 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:



System						Wireless				Link	
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A1:C7	0	Searching...	Master	192.168.96.139	159 - 5.795GHz	Auto:(0-7):1	23 dBm	-95 dBm	0 dB	60 Mbps

```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      www.google.com
Address 1: 2404:6800:4007:80e::2004 maa05s04-in-x04.1e100.net
Address 2: 172.217.163.132 maa05s04-in-f4.1e100.net
```

Figure 62: 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:

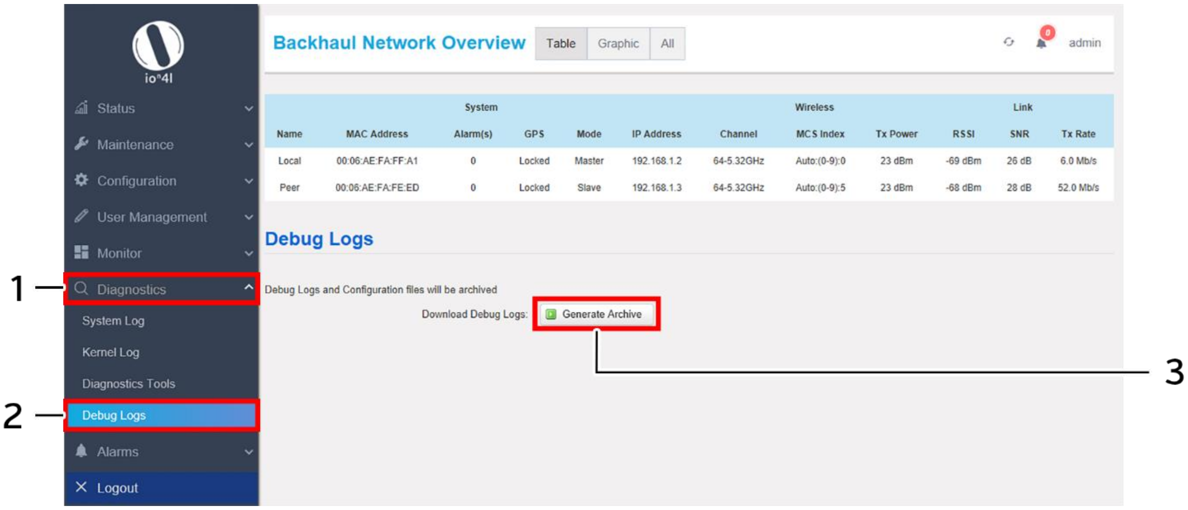
Table 56: List of actions to identify the IP address with the domain name

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:



Backhaul Network Overview

System						Wireless				Link	
Name	MAC Address	Alarm(s)	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:06:AE:FA:FF:A1	0	Locked	Master	192.168.1.2	64-5.32GHz	Auto:(0-9):0	23 dBm	-69 dBm	26 dB	6.0 Mb/s
Peer	00:06:AE:FA:FE:ED	0	Locked	Slave	192.168.1.3	64-5.32GHz	Auto:(0-9):5	23 dBm	-68 dBm	28 dB	52.0 Mb/s

Debug Logs

Debug Logs and Configuration files will be archived

Download Debug Logs:

Figure 63: Basic overview of the Diagnostic Tools screen to download debug logs

Follow the steps given below to download debug logs:

Table 57: 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

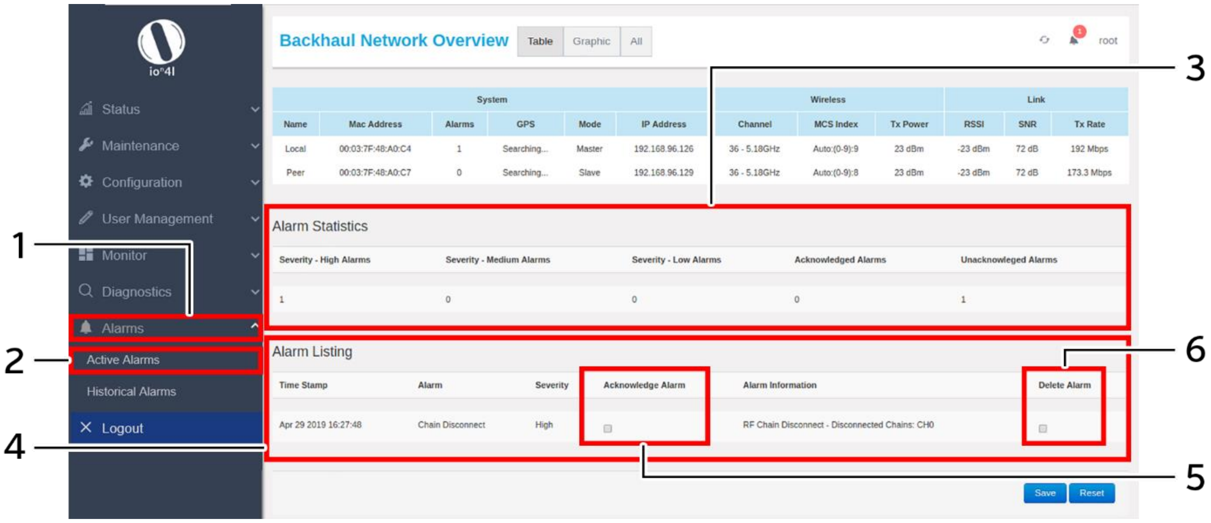
15 Alarms

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 positive or 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. Once the active alarms are cleared, the same are moved from active alarms page to historical alarm page. 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:



System						Wireless			Link		
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A0:C4	1	Searching...	Master	192.168.96.126	36 - 5.18GHz	Auto:(0-9):9	23 dBm	-23 dBm	72 dB	192 Mbps
Peer	00:03:7F:48:A0:C7	0	Searching...	Slave	192.168.96.129	36 - 5.18GHz	Auto:(0-9):8	23 dBm	-23 dBm	72 dB	173.3 Mbps

Alarm Statistics

Severity - High Alarms	Severity - Medium Alarms	Severity - Low Alarms	Acknowledged Alarms	Unacknowleged Alarms
1	0	0	0	1

Alarm Listing

Time Stamp	Alarm	Severity	Acknowledge Alarm	Alarm Information	Delete Alarm
Apr 29 2019 16:27:48	Chain Disconnect	High	□	RF Chain Disconnect - Disconnected Chains: CH0	□

Figure 64: Basic overview of the active alarm screen

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

Table 58: List of actions to view the active alarm listing and statistics

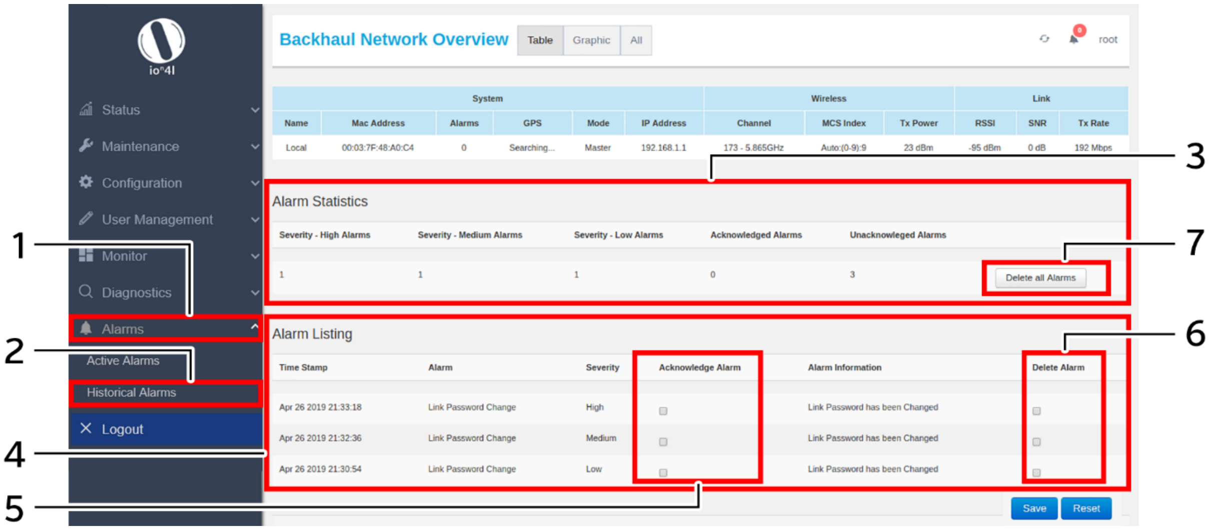
Callout	Name	Description
1.	Alarms	Click on "Alarms" dropdown
2.	Active Alarms	Click on "Active Alarms" option
3.	Alarms Statistics	Displays total count of the acknowledged, unacknowledged, and other active alarms based on their severity level.
4.	Alarms Listing	Displays all active alarms in the listed 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:



Backhaul Network Overview

System						Wireless			Link		
Name	Mac Address	Alarms	GPS	Mode	IP Address	Channel	MCS Index	Tx Power	RSSI	SNR	Tx Rate
Local	00:03:7F:48:A0:C4	0	Searching...	Master	192.168.1.1	173 - 5.865GHz	Auto:(0-9):9	23 dBm	-95 dBm	0 dB	192 Mbps

Alarm Statistics

Severity - High Alarms	Severity - Medium Alarms	Severity - Low Alarms	Acknowledged Alarms	Unacknowleged Alarms
1	1	1	0	3

Alarm Listing

Time Stamp	Alarm	Severity	Acknowledge Alarm	Alarm Information	Delete Alarm
Apr 26 2019 21:33:18	Link Password Change	High	□	Link Password has been Changed	□
Apr 26 2019 21:32:36	Link Password Change	Medium	□	Link Password has been Changed	□
Apr 26 2019 21:30:54	Link Password Change	Low	□	Link Password has been Changed	□

Figure 65: Basic overview of the historical alarm screen

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

Table 59: 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:

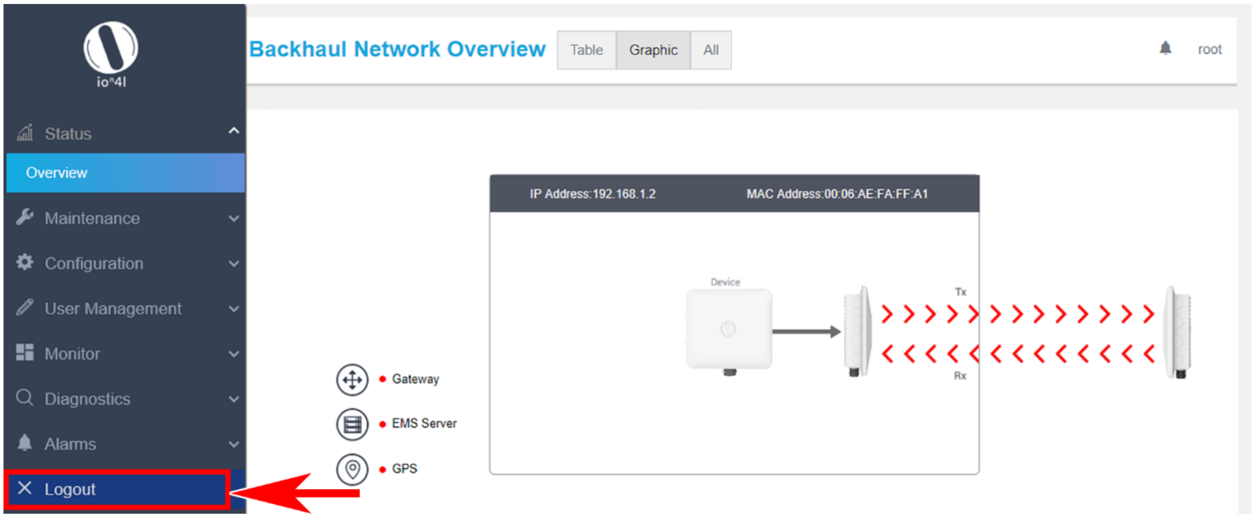


Figure 66: Basic overview of the UBR GUI with logout option

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

17 Installation Setup

2x2 UBR has four holes on its back side for the attachment of mounting bracket, as shown in “Figure 3: Back view of the 2x2 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 its attaching parts. It provides the freedom of movement to the UBR even after the mounting.

1. The mounting bracket is fixed onto the mounting holes of 2x2 UBR as shown in the figure below:

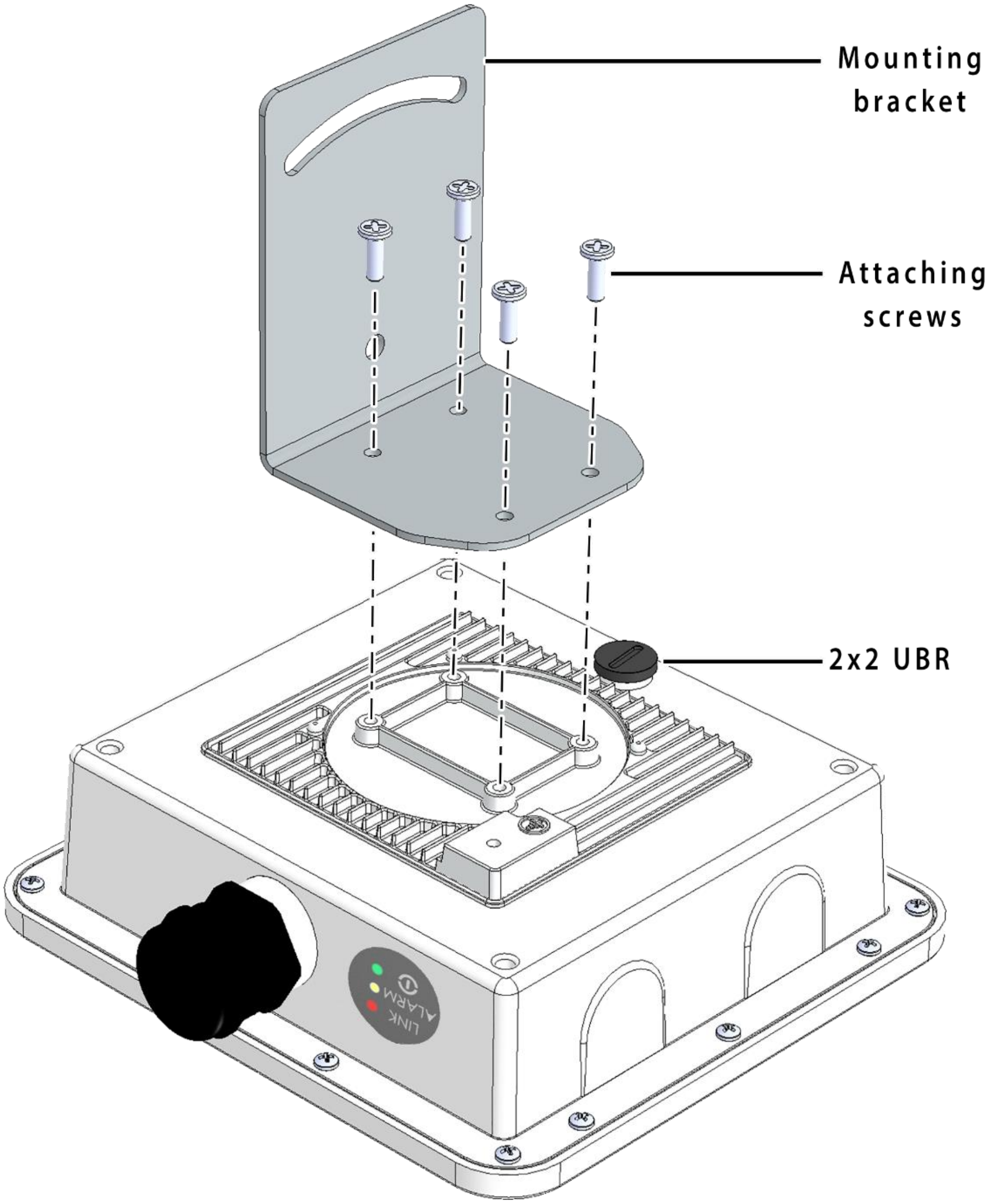


Figure 67: Mounting bracket attachment with the 2x2 UBR device

2. Final alignment of the mounting bracket with UBR is as shown below:

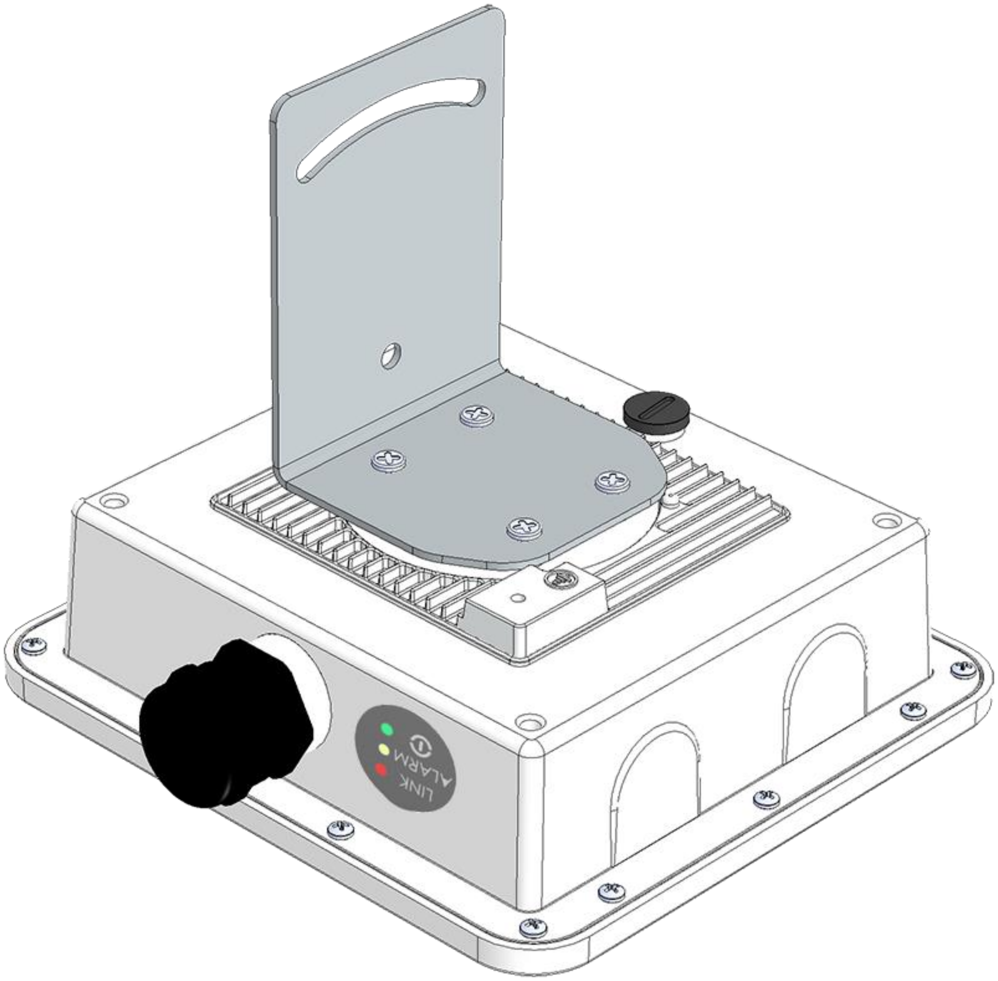


Figure 68: Mounting bracket alignment with the 2x2 UBR device

The mounting instructions of 2x2 UBR is detailed in further sections below.