11.3.1 General network setup configuration

Click on the "Edit" option in network screen as shown in "Figure 26: Basic overview of the network configuration screen". DHCP client (DHCPv4 client or DHCPv6 client) option is to get the dynamic IP address from reachable DHCP server in the network. Once the protocol is set to DHCPv4 client or DHCPv6 client, the device will automatically get the IP address (IPv4 or IPv6) from the DHCP server.

A basic overview of the general network setup configuration screen to switch from DHCP client to static address is given below:

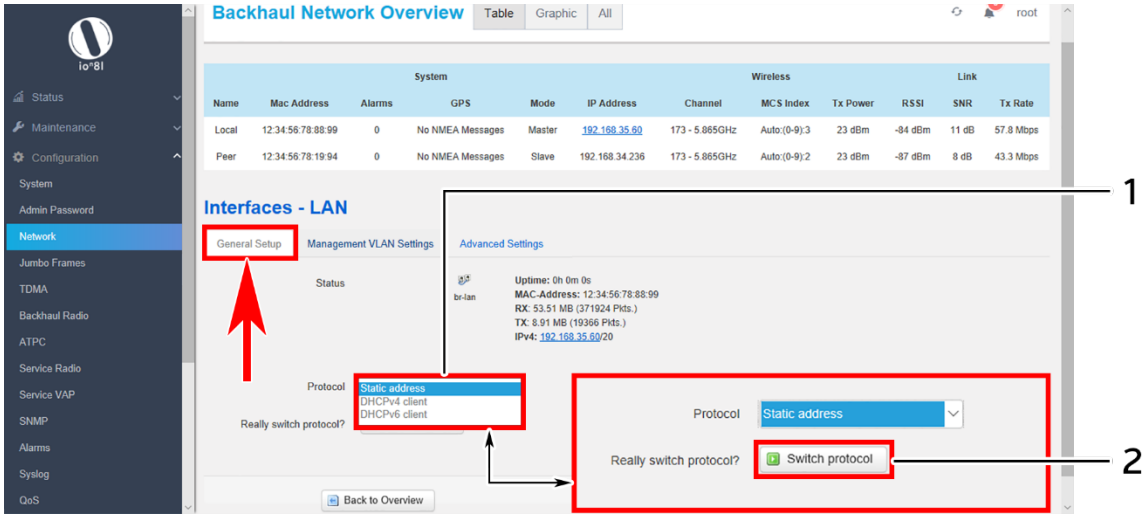

Figure 27: Basic overview of general setup switch protocol from DHCP client to Static address

Follow the steps given below to switch from DHCP client protocol to static address and change the general network setup configuration manually:

Table 19: List of actions to switch protocol from DHCP client to Static address

Callout	Name	Description
1.	Protocol	Select the protocol to "Static address" from the dropdown list (Static address/DHCPv4 client/DHCPv6 client)
2.	Really switch protocol	Click on "Switch protocol" to confirm the protocol switch from DHCP client to static address

11.3.1.1 *Static address configuration*

Refer the figure below to provide the static address parameters:

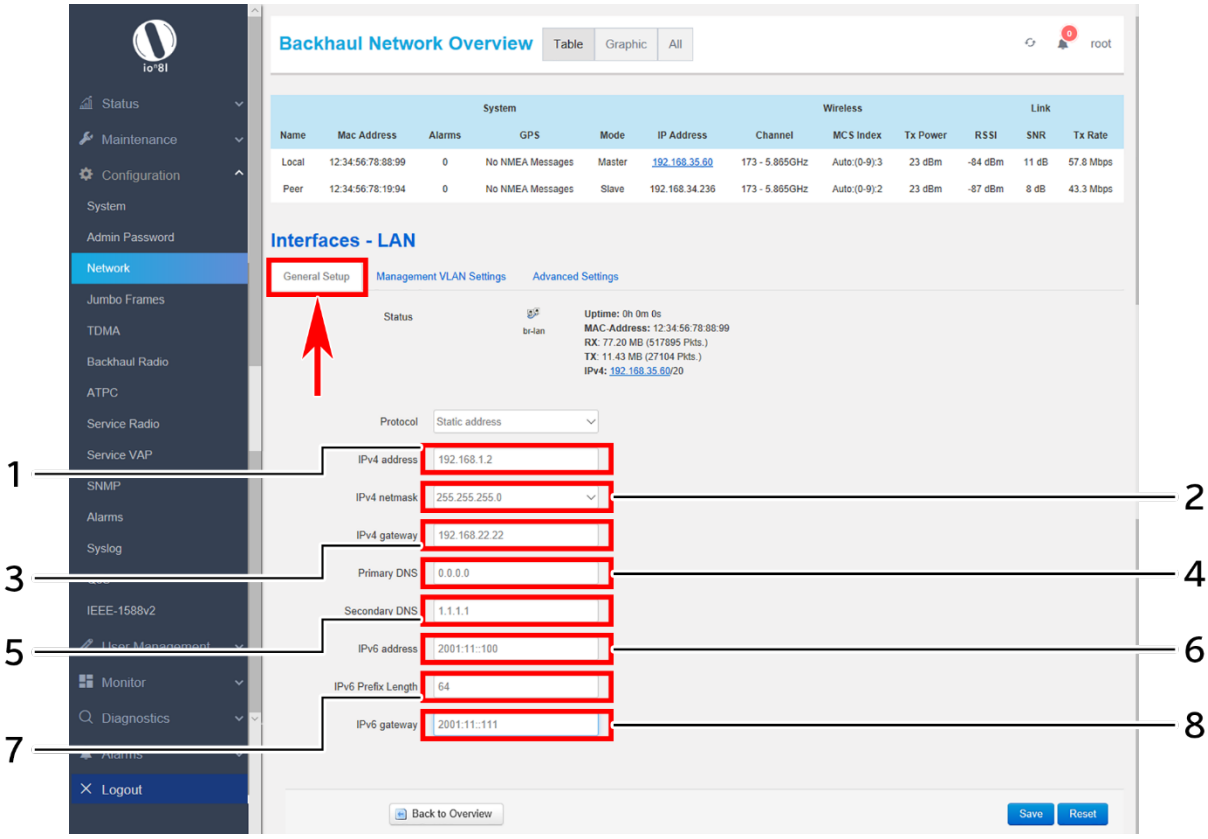

Figure 28: Basic overview of static address parameters for general network setup

Follow the steps given below to provide static address parameters:

Table 20: List of actions to provide static address parameters

Callout	Name	Description
1.	IPv4 address	Enter the "IPv4 address". This is a unique address of the Host/Device eg.192.168.100.10
2.	IPv4 netmask	Enter the "IPv4 netmask". This specifies the number of bits for network part and host part e.g.255.255.255.0
3.	IPv4 gateway	Enter the "IPv4 gateway". Gateway address is given to reach other network device e.g.192.168.100.254
4.	Primary DNS	Enter the IP address of "Primary DNS server". DNS server is to resolve the transition of domain name to IP and IP to domain name
5.	Secondary DNS	Enter the IP address of "Secondary DNS server". DNS server is to resolve the transition of domain name to IP and IP to domain name
6.	IPv6 address	Enter the "IPv6 address". Unique address of the Host/Device e.g.2001:11::100

Callout	Name	Description
7.	IPv6 prefix length	Specify the prefix length for IPv6 address. Specifies the number of bits that belong to network part. The prefix-length specifies a range of devices e.g. IPv6 prefix length = 64 means range of IP addresses between 2001:0DB8:ABCD:0012:0000:0000:0000:0000 and 2001:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF
8.	IPv6 gateway	Enter the "IPv6 gateway". Gateway address is given to reach other network device e.g.2001:11::1

Click "Save" to save the general network setup configuration or click "Reset" to configure the same again.

11.3.2 Management VLAN settings

The primary benefit of using a management VLAN is improved network security. When all management traffic is on a separate VLAN ID, it is much harder for unauthorized users to make changes to your network or monitor network traffic.

A basic overview of the management VLAN settings screen is given below:

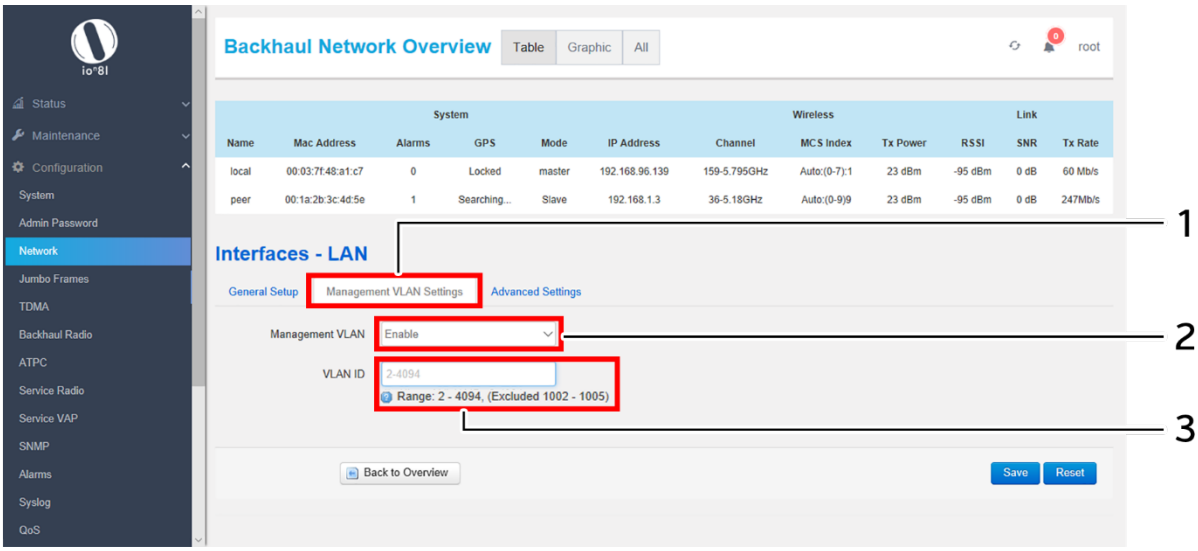

Figure 29: Basic overview of management VLAN settings screen

Click on the "Edit" option in network screen as shown in "Figure 26: Basic overview of the network configuration screen". Follow the steps given below to configure management VLAN settings:

Table 21: List of actions to configure management VLAN settings

Callout	Name	Description
1.	Management VLAN Settings	Click on "Management VLAN Settings" option
2.	Management VLAN	Select "Enable/Disable" option from the dropdown list
3.	VLAN ID	Enter the "VLAN ID", if Management VLAN is enabled

Click "Save" to save the management VLAN settings or click "Reset" to configure the same again.

11.3.3 Advanced network settings

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

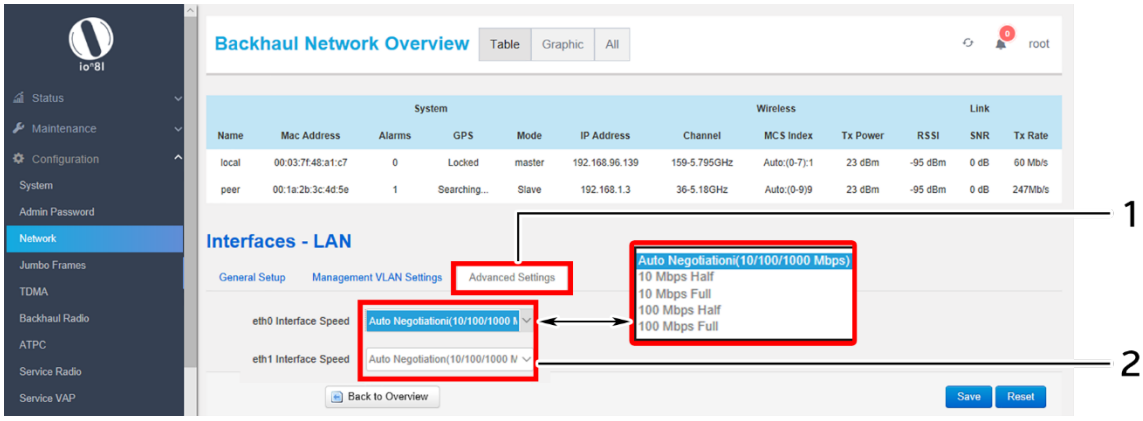

Figure 30: Basic overview of network advanced settings

Click on the "Edit" option in network screen as shown in "Figure 26: Basic overview of the network configuration screen". Follow the steps given below to configure network advanced settings:

Table 22: List of actions to configure network advanced settings

Callout	Name	Description
1.	Advanced Settings	Click on "Advanced Settings" option
2.	Ethernet Interface Speed	Select the interface speed (Eth0 & Eth1) from the dropdown list (10 Mbps-Half Duplex/ 10 Mbps-Full Duplex/100 Mbps-Half Duplex/ 100 Mbps-Full Duplex) or select "Auto Negotiation". The user can restrict the respective UBR to the selected ethernet interface speed

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

11.4 Jumbo Frames Settings

A basic overview of the screen to configure jumbo frames is given below:

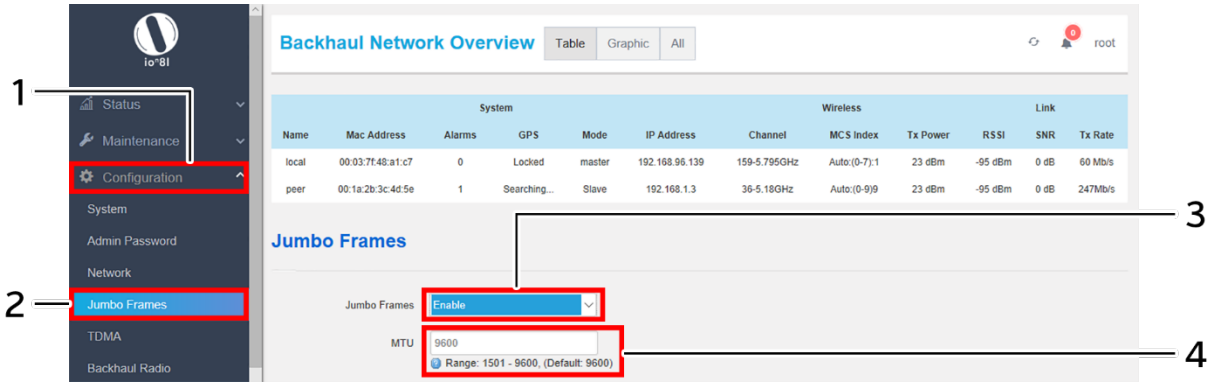

Figure 31: Basic overview of the screen to configure jumbo frames

Follow the steps given below to configure jumbo frame settings:

Table 23: List of actions to configure jumbo frames

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Jumbo Frames	Click on "Jumbo Frames" option
3.	Enable/Disable Jumbo Frames	Enable or Disable the jumbo frames. Enter the MTU value in the below parameter, if enabled.
4.	MTU	Enter the "MTU" value within the range of 1500 to 9600

Click "Save" to save the jumbo frame settings or click "Reset" to configure the same again.

11.5 TDMA Configuration

Time-division multiple access (TDMA) is a channel access method for shared-medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots. The users transmit in rapid succession, one after the other, each using its own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity.

Slot width is a feature in TDMA communication to provide equal opportunity of communication for devices in TDMA. Each TDMA slot width consists of data transfer time and guard time. During the data transfer time, data will be exchanged between the master and slave. Guard time is to ensure that data is received by the receiver.

The master device allocates the slot width for the slave devices. This slot width information broadcasted to all the slaves by beacons. After receiving beacons, the scheduler in the slave devices schedules TX and RX times in the slot for the slave device. The slot width is configured to 8ms.

The TDMA configuration screen has following options:

1. Link Settings
2. Link Security Settings
3. Advanced Settings
4. Redundant Link Switching

11.5.1 Link Settings

The UBR radio supports 4x4 MIMO (Multiple-Input and Multiple-Output) and TDMA up to 256QAM. MIMO refers to a practical technique for sending and receiving more than one data signal simultaneously over the same radio channel by exploiting multipath propagation.

The UBR can be configured for P2P and P2MP communication links. The term point-to-point communications (P2P) means a wireless data link between two fixed points. Point-to-multipoint communication (P2MP) is accomplished via a distinct type of one-to-many connection, providing multiple paths from a single location to multiple locations.

Link established between participating devices depends on the selected link type (P2P or P2MP) and mode type (master or slave). The link configuration for the master can be configured from the GUI and the slave device receives the link configuration from the respective master device. The various scenarios are discussed separately in below sections.

11.5.1.1 *Link settings of Master device in a P2P link*

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

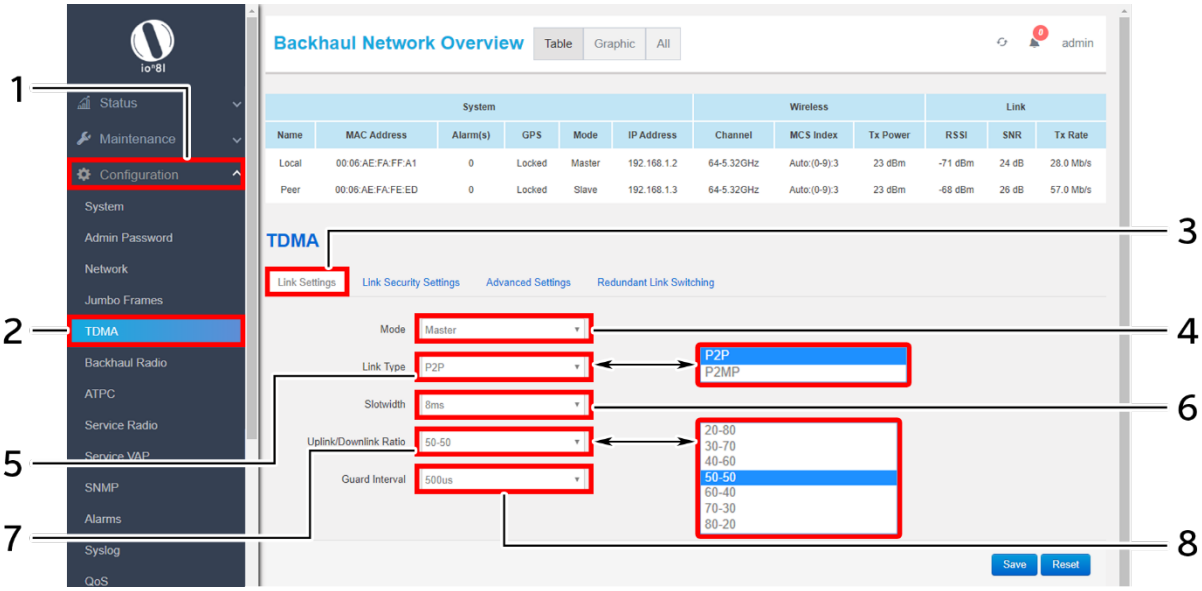

Figure 32: Link settings screen of Master device in a P2P link

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

Table 24: List of actions to configure the link settings of Master device in a P2P 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 Master from the dropdown list (Master/Slave)
5.	Link Type	Select the "Link Type" to P2P from the dropdown list (P2P/P2MP)
6.	Slot width	Set the "Slot width" to 125Hz-8ms
7.	Downlink/ Uplink Ratio	Select the "Downlink/ Uplink Ratio" from the dropdown list (20-80/30-70/40-60/50-50/60-40/70-30/80-20). 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 Uplink = 80% of the total available bandwidth is used in uplink
8.	Guard Interval	Enter the "Guard Interval" in the multiples of 10 within the range of 0 to 500ms. The Guard Interval (GI) is effectively a very short pause between packet transmissions to allow for any false information to be

Callout	Name	Description
		ignored. Longer guard intervals make for more reliable wireless.

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

11.5.1.2 Link settings of Master device in a P2MP link

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

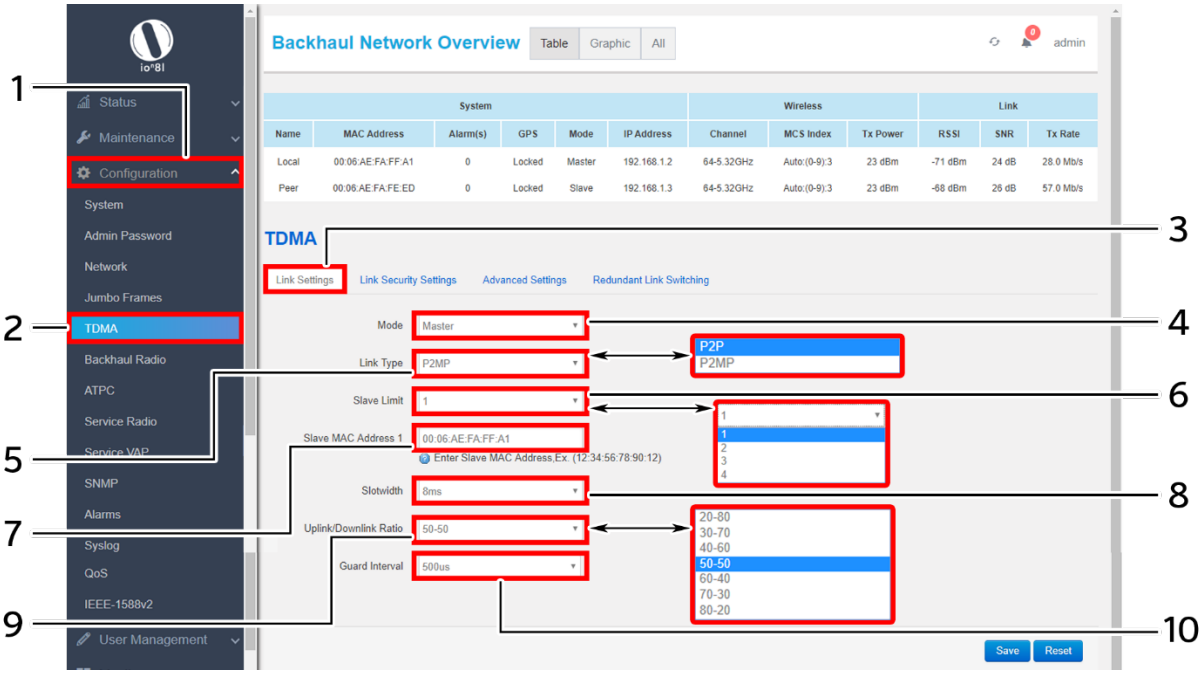

Figure 33: Link settings screen of Master device in a P2MP link

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

Table 25: List of actions to configure the link settings of Master device in a 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 Master from the dropdown list (Master/Slave)
5.	Link Type	Select the "Link Type" to P2MP from the dropdown list
6.	Limit Slave	Select the number of slaves from the "Limit Slave" dropdown list (1/2/3/4)
7.	Slave UID	Enter the "Slave UID". Slave UID is needed in the master to allow the association of slaves which has

Callout	Name	Description
		their MAC address configured. Slave UID is the MAC address of the slave
8.	Slot width	Set the "Slot width" to 125Hz-8ms
9.	Downlink/ Uplink Ratio	Select the "Downlink/ Uplink Ratio" from the dropdown list (20-80/30-70/40-60/50-50/60-40/70-30/80-20). 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 Uplink = 80% of the total available bandwidth is used in uplink
10.	Guard Interval	Enter the "Guard Interval" in the multiples of 10 within the range of 0 to 500ms. The Guard Interval (GI) is effectively a very short pause between packet transmissions to allow for any false information to be ignored. Longer guard intervals make for more reliable wireless.

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

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:

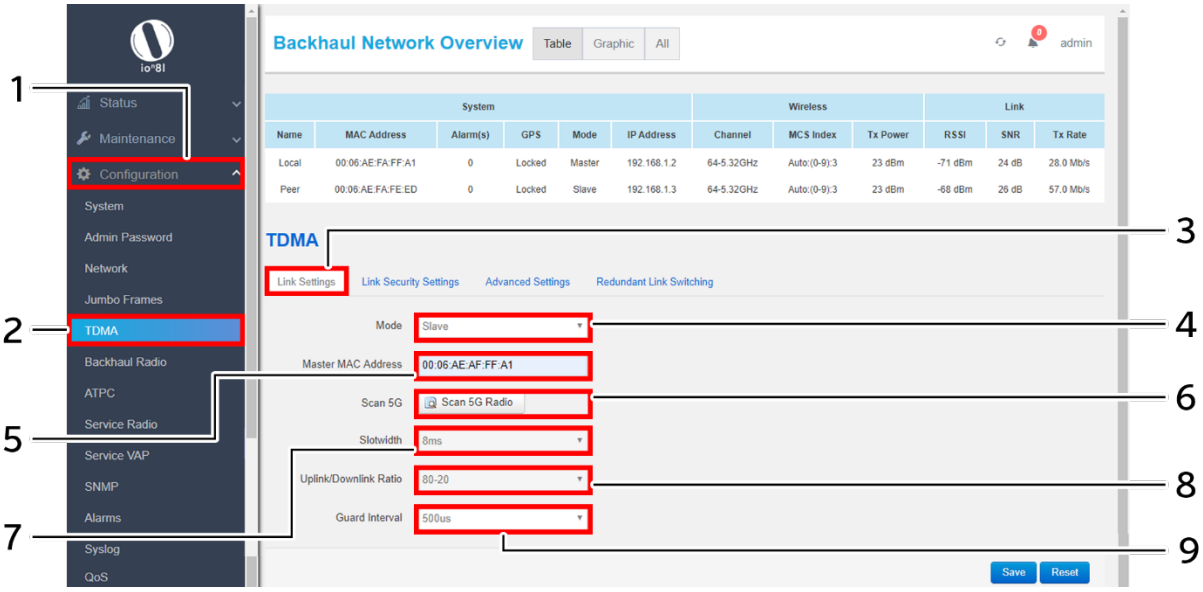

Figure 34: Link settings screen of Slave device in a P2P or P2MP link

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-

Callout	Name	Description
		Downlink = 20% of the total available bandwidth is used in downlink 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:

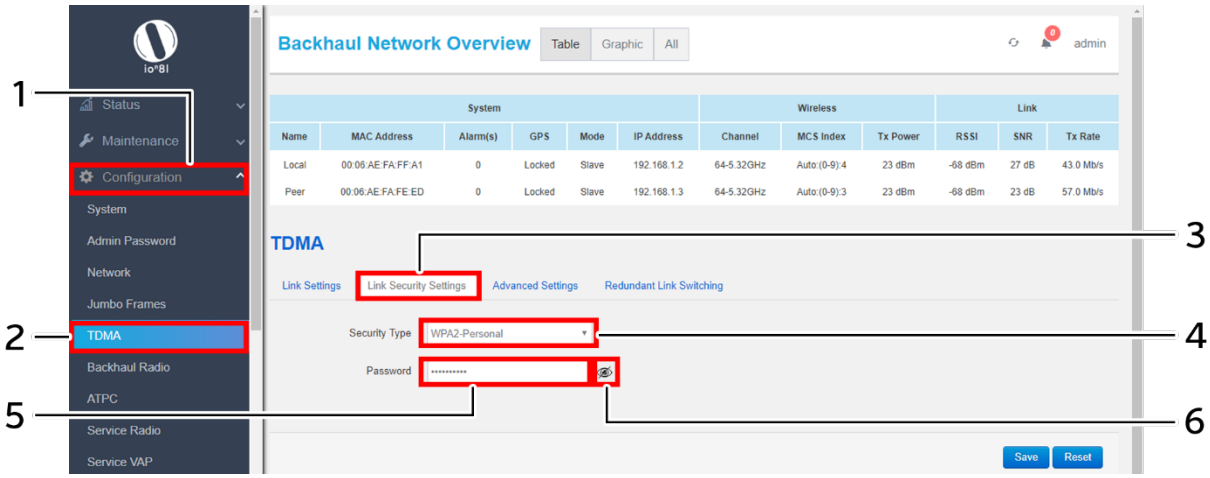

Figure 35: Basic overview of the Link Security Settings screen

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.	Security Type	Select the "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:

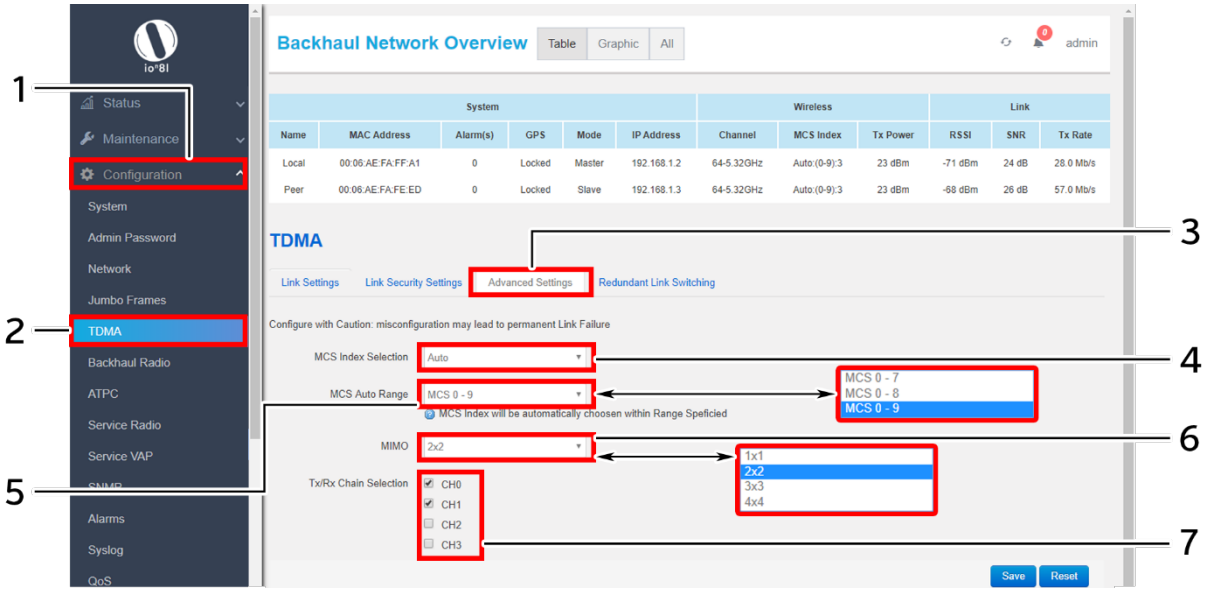

Figure 36: Basic overview of the advanced TDMA settings screen

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	Set the MCS index to "Auto" and specify the "MCS Auto Range" in next step
5.	MCS Auto Range	Set the range of auto selection from the dropdown list (MCS- 0 to 7, 0 to 8, 0 to 9). The auto MCS index algorithm will set the value with in the selected range
6.	MIMO	Select the spatial streams from the dropdown list (1x1/ /2x2/3x3/4x4).
7.	Tx/Rx Chain Selection	Click on the selection box and select a single chain or multiple chains as per the NSS. If the MIMO is set to 1x1, one chain is allowed for selection and if the MIMO is set to 2x2, two chains are allowed for selection. Similarly the concept applies for 3x3 and 4x4 MIMO option. 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:

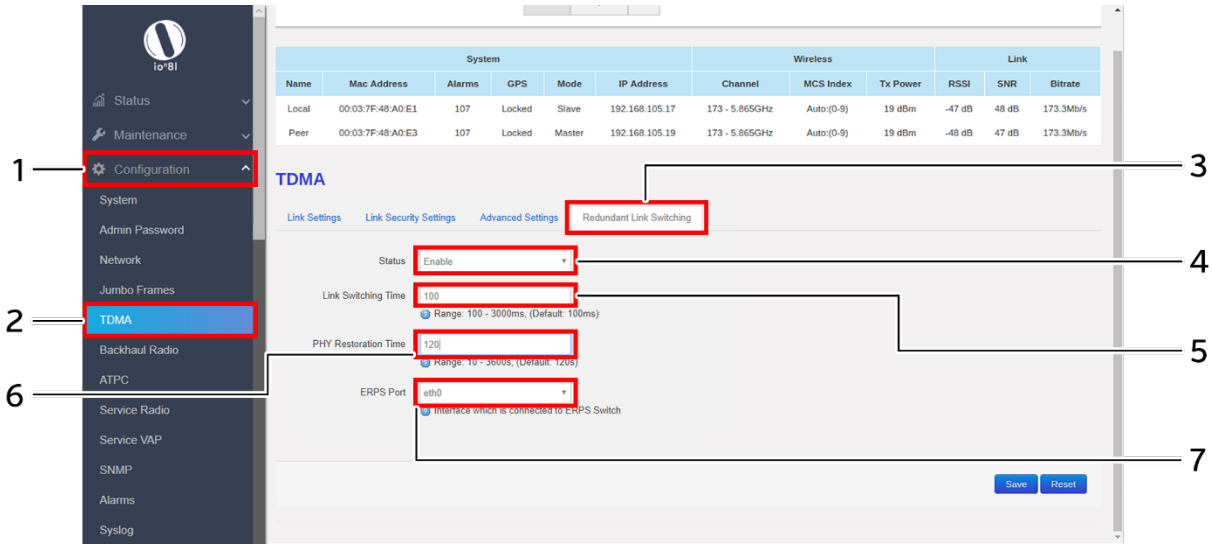

Figure 37: Basic overview of the redundant link switching screen

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 Restoring Time	Set the link restoring 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

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:

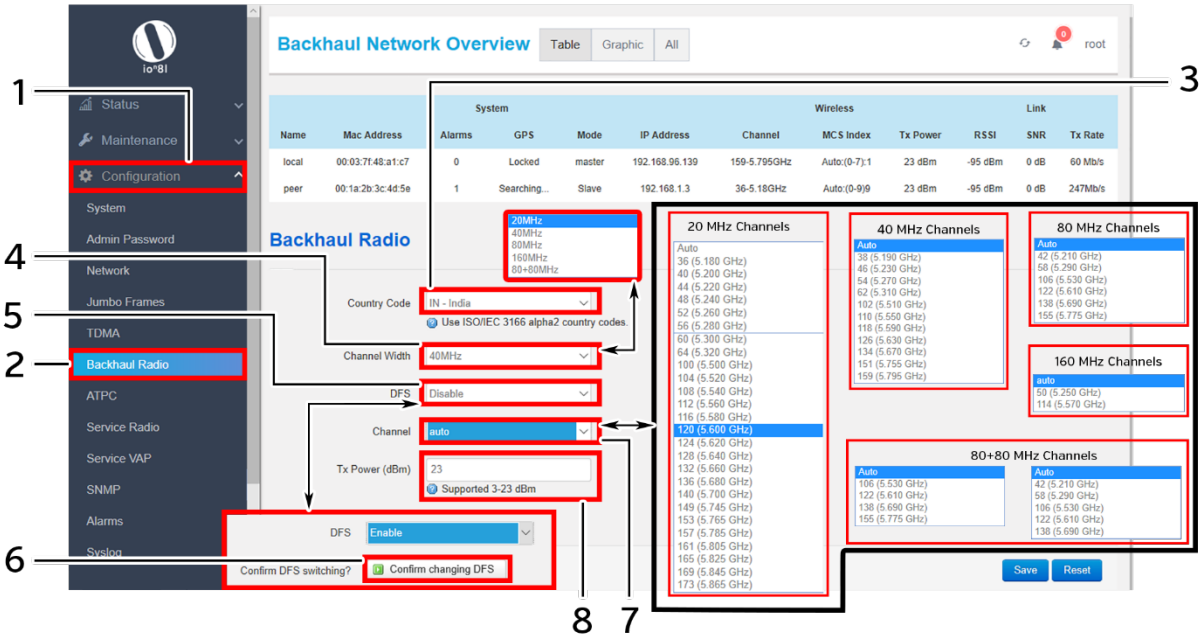

Figure 38: Basic overview of the Backhaul Radio Configuration screen

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/160 MHz/80+80 MHz)
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.

Callout	Name	Description
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
7.	Channel	Select the "Channel" from the dropdown list. The device will choose the channel by itself, if "Auto" channel is selected
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:

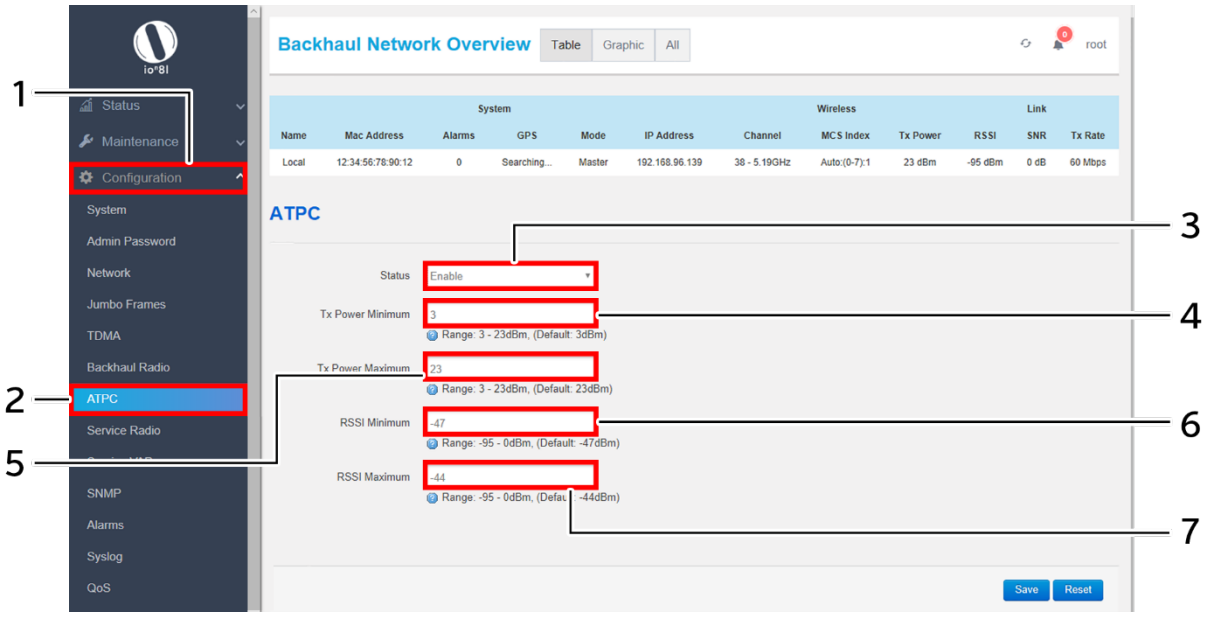

Figure 39: Basic overview of the ATPC Configuration screen

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 Service Radio Configuration

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

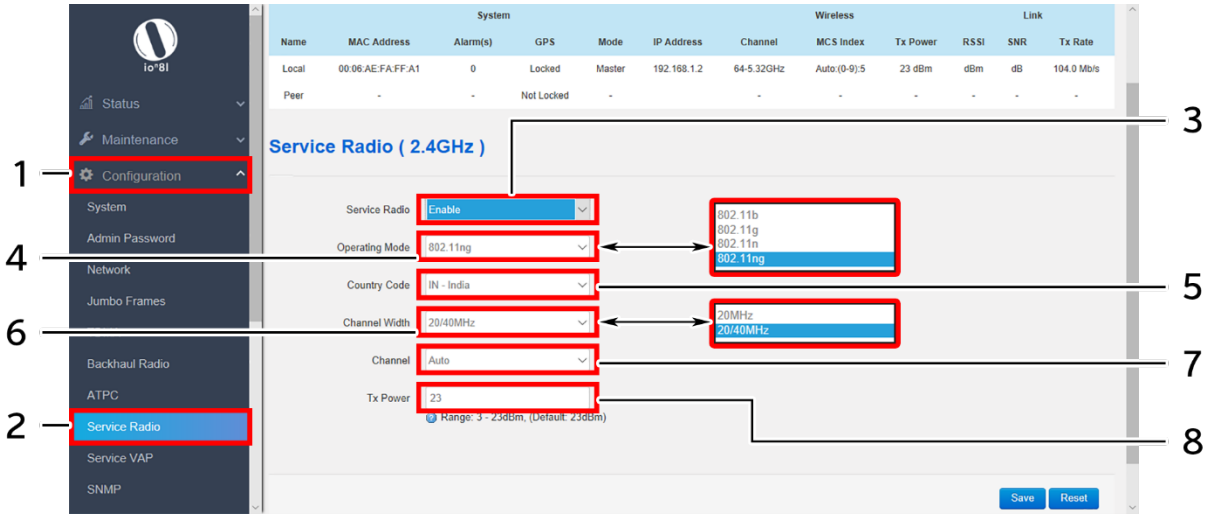

Figure 40: Basic overview of the Service Radio Configuration screen

Follow the steps given below and configure the Service Radio settings for the UBR:

Table 32: List of actions to configure the Service Radio settings

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Service Radio	Click on "Service Radio" option
3.	Service Radio Support	Enable/Disable the Service Radio support. Enter the following parameters, if enabled
4.	Operating Mode	Select the mode of operation for the radio from the dropdown list (802.11b/802.11g/802.11n/802.11ng)
5.	Country Code	Select the country code from the dropdown list
6.	Channel Width	Set the channel width from the dropdown list (20 or 20/40 MHz)
7.	Channel	Select the channel from the dropdown list. The device will choose the channel by itself, if "Auto" channel is selected
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 Service Radio configuration or click "Reset" to configure the same again.

11.9 Service VAP Configuration

A basic overview of the Service VAP Configuration screen is given below:

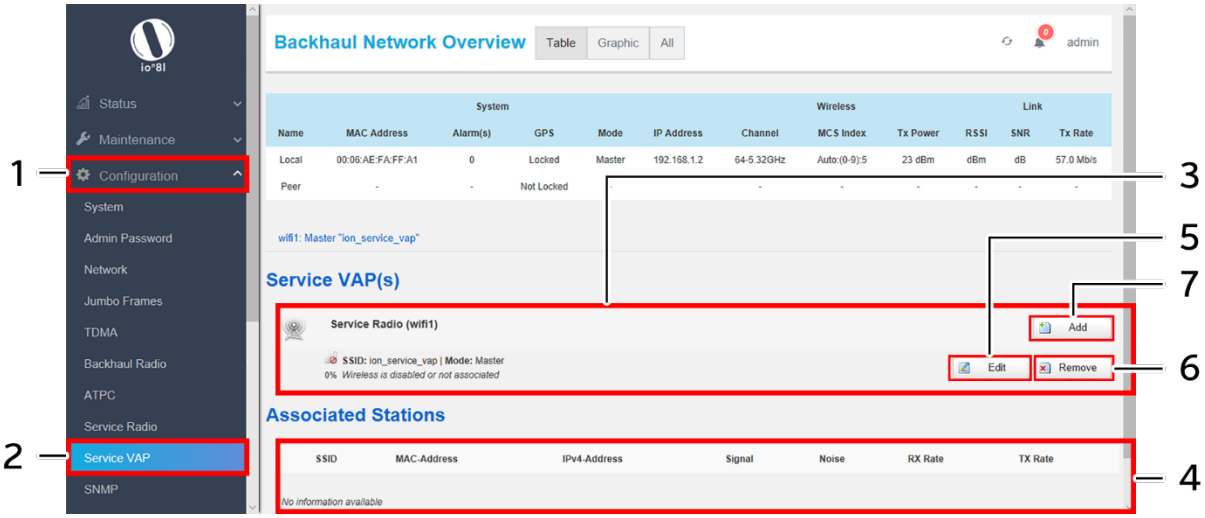

Figure 41: Basic overview of the Service VAP Configuration screen

Follow the steps given below and configure the Service VAP for the UBR:

Table 33: List of actions to configure the Service VAP

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Service VAP	Click on "Service VAP" option
3.	VAP List	Displays all configured VAPs in a listed form along with some basic information as shown in above figure
4.	Associated Stations	Displays all associated stations in a listed form along with some basic information in respective information columns as shown in above figure
5.	Edit	Click on this option to edit the configuration parameters of an existing VAP. Refer "Figure 42: Basic overview of the Service VAP Configuration parameters"
6.	Remove	Click on this option to remove an existing VAP from the list
7.	Add	Click on this option to add a new VAP. Refer "Figure 42: Basic overview of the Service VAP Configuration parameters"

Once the user has clicked on "Add" option (7), few parameters are needed for VAP configuration as shown in figure below:

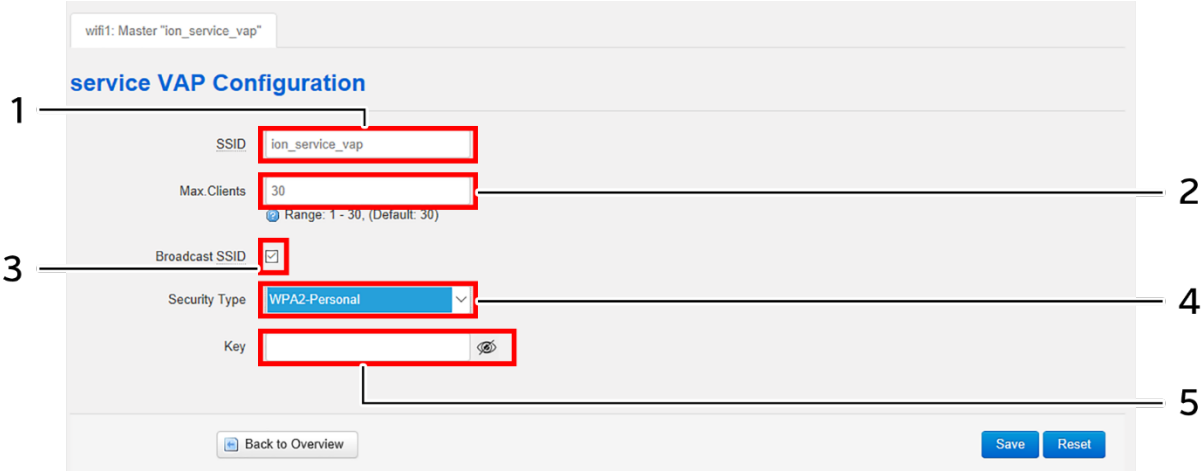

Figure 42: Basic overview of the Service VAP Configuration parameters

Follow the steps given below and provide the Service VAP parameters:

Table 34: List of actions to configure the Service VAP parameters

Callout	Name	Description
1.	SSID	Enter a name for the new SSID
2.	Max Clients	Set the number of clients to be allowed for the respective SSID. Max 30 clients can connect to a SSID
3.	Broadcast SSID	Click and select the check box to enable the SSID to broadcast. If the Broadcast SSID option is disabled, the respective SSID does not appear in the SSID discovery of any device. However clients can provide the SSID name/password manually and connect to the SSID.
4.	Security Type	Select the "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.	Key	Enter a unique password for the SSID

Click "Save" to add a new VAP or click "Reset" to configure the same again. Once a new VAP is configured the same is reflected in the "VAP List" (Refer callout 3 in "Figure 41: Basic overview of the Service VAP Configuration screen").

11.10 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:

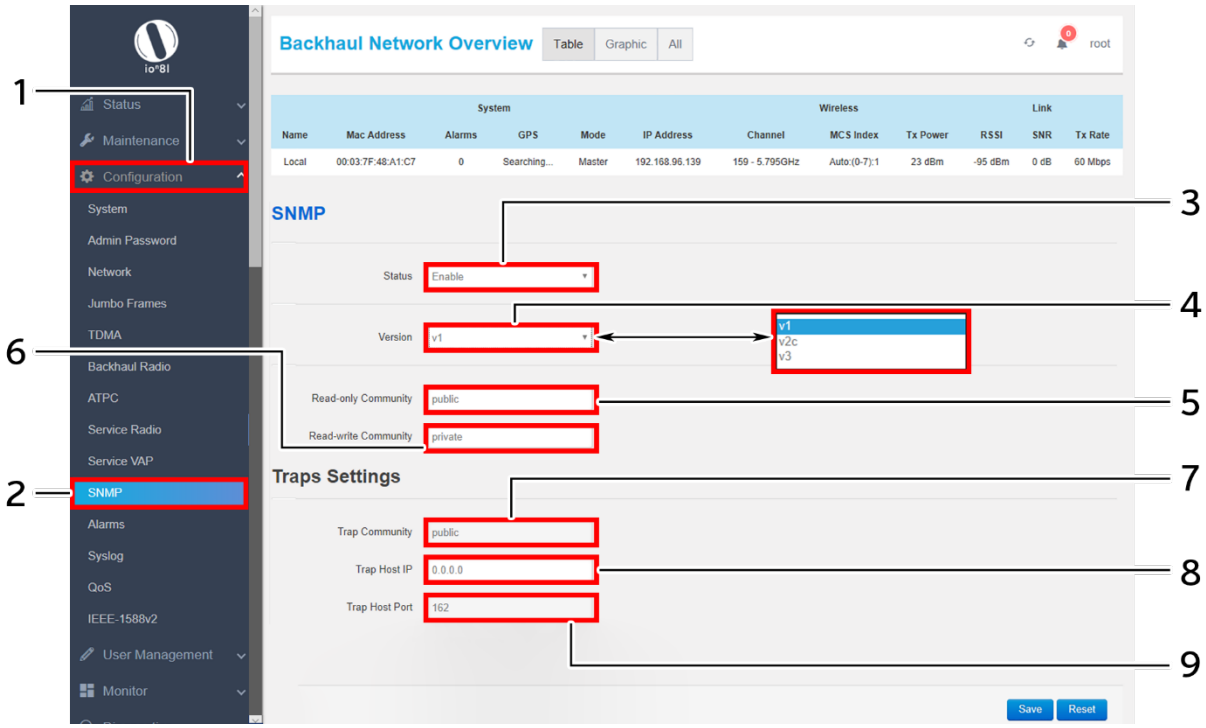

Figure 43: Basic overview of the SNMP Configuration screen (v1 or v2c)

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

Table 35: 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:

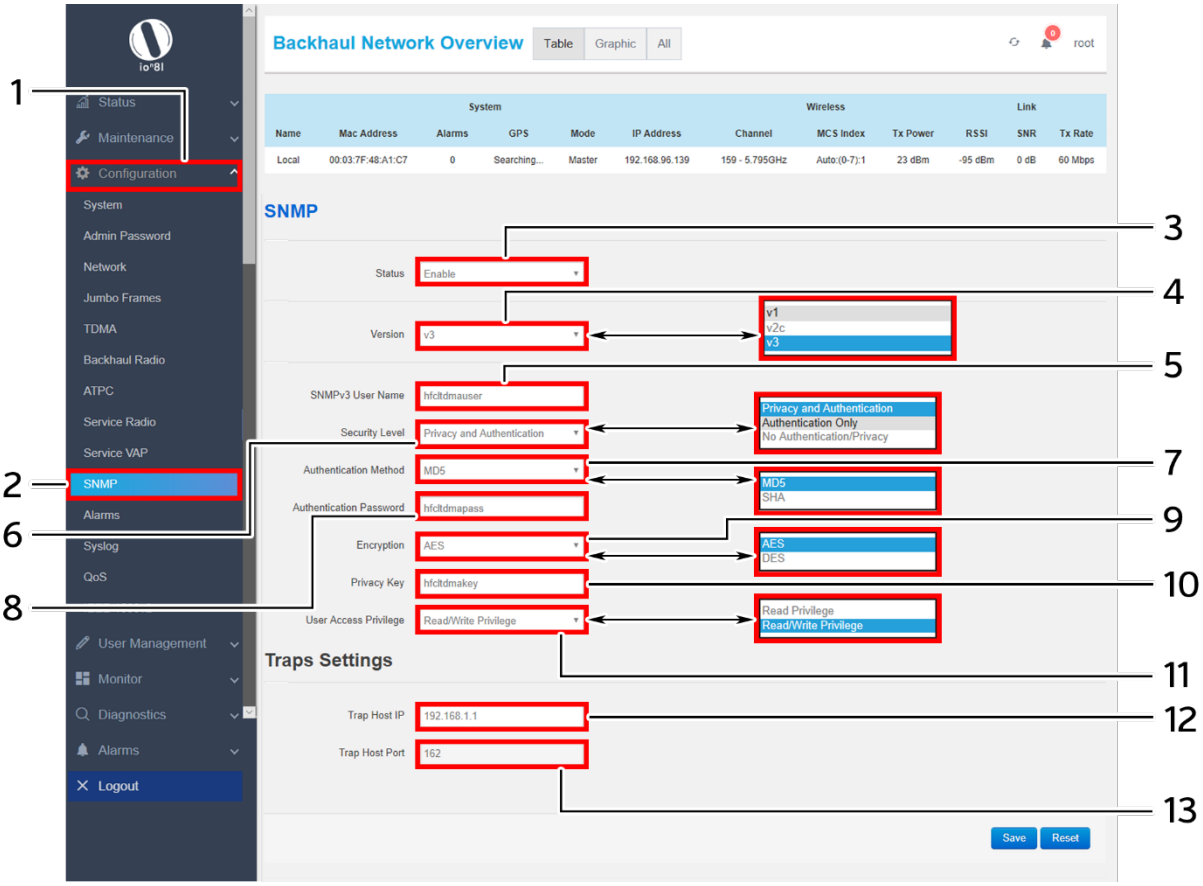

Figure 44: Basic overview of the SNMP Configuration screen (v3)

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

Table 36: 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.

11.11 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. Alarm are stacked for 5 days. The event alarm screen is further categorized into following sections:

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

11.11.1 Link/Interface Alarms

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

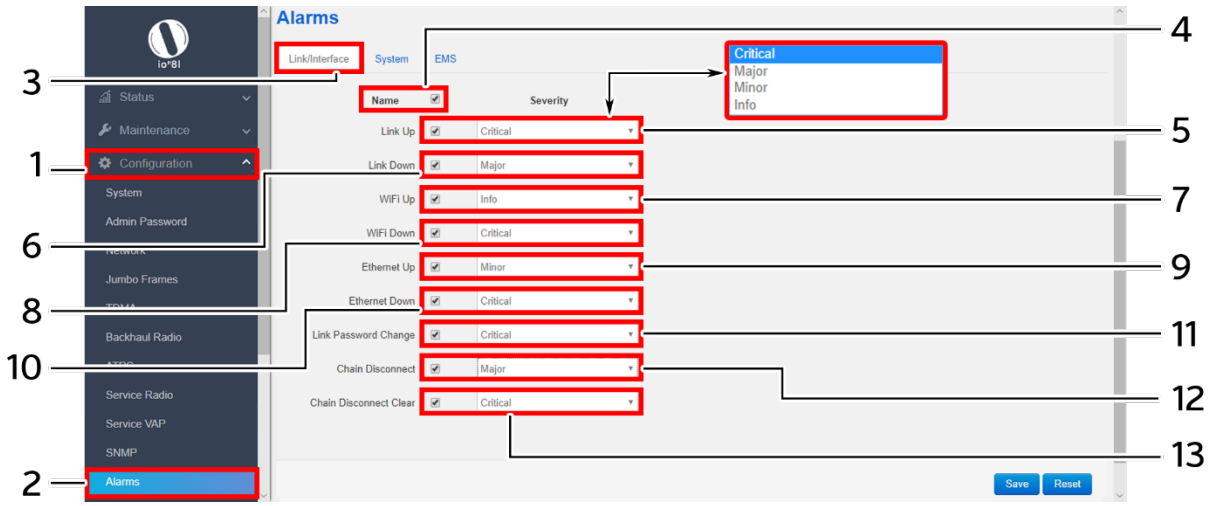

Figure 45: Basic overview of the Event Alarm Configuration screen to configure link/interface alarms

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

Table 37: 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.

11.11.2 System Alarms

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

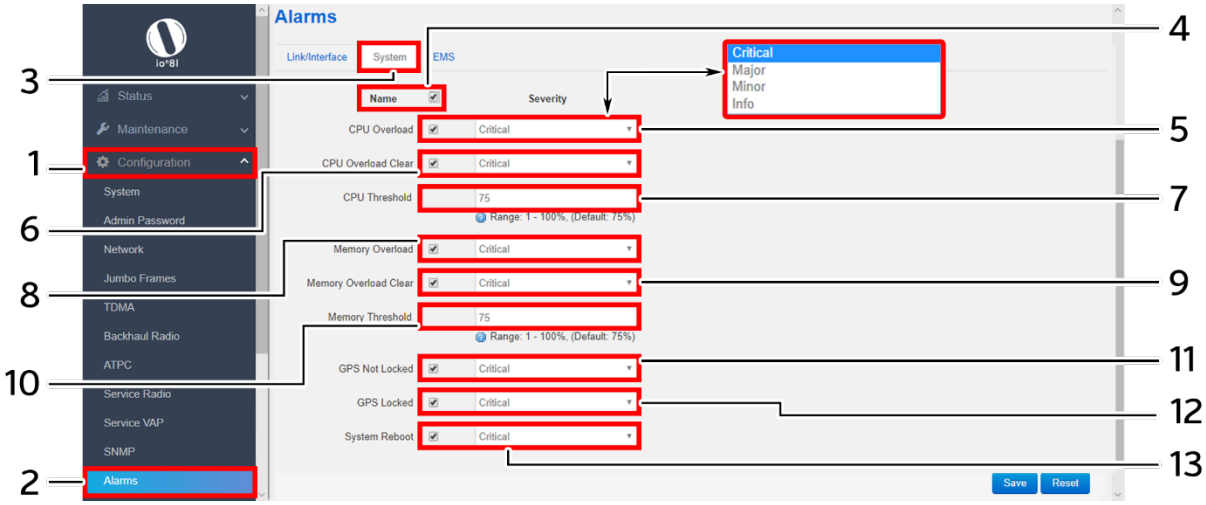

Figure 46: Basic overview of the Event Alarm Configuration screen to configure system alarms

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

Table 38: List of actions to configure system Alarms

Callout	Name	Description
1.	Configuration	Click on "Configuration" dropdown
2.	Alarms	Click on "Alarms" option
3.	System Alarms	Click on "System" 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

Callout	Name	Description
		enabled, the notification of memory 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 "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.

11.11.3 EMS Alarms

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

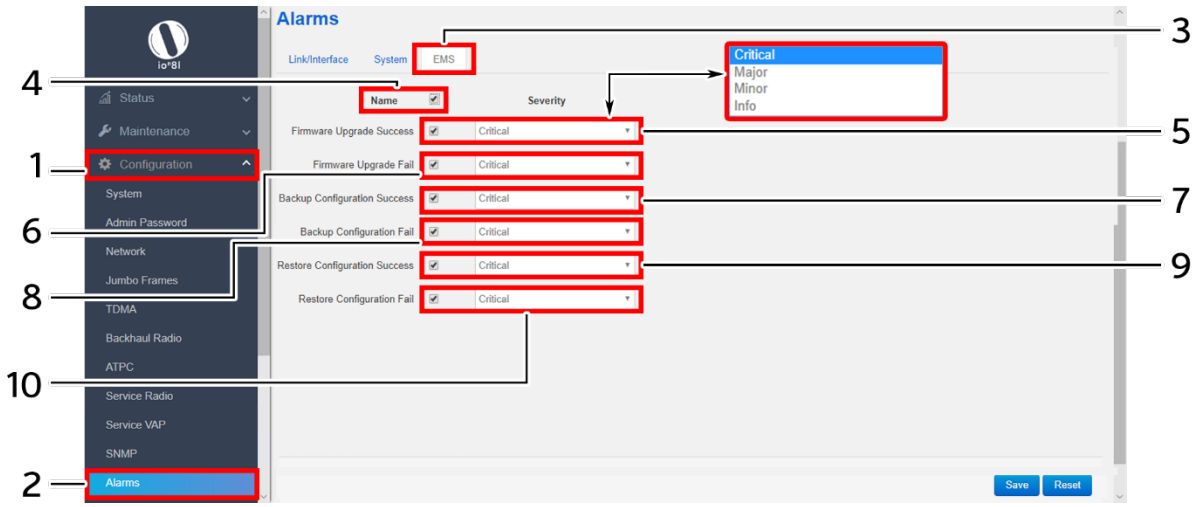

Figure 47: Basic overview of the Alarm Configuration screen to configure EMS alarms

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

Table 39: 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 alarms settings or click "Reset" to configure the same again.