16 Network interfaces of thick AP

A basic overview of the network interface screen for thick AP is given below:

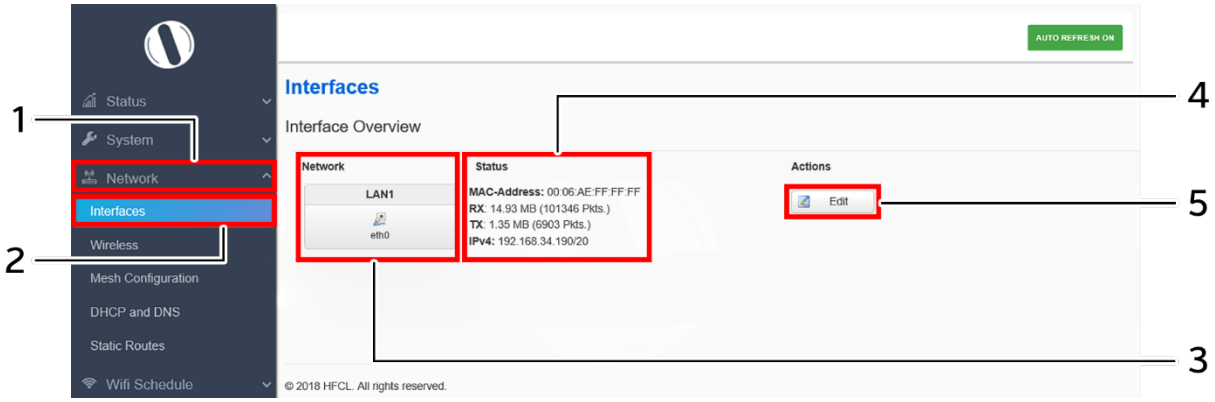

Figure 33: Basic overview of the interface configuration screen for thick AP

Follow the steps given below to view/edit the interface configuration of thick AP:

Table 27: List of actions to view/edit the network configuration of thick AP

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	Interfaces	Click on "Interfaces" option
3.	Network/Interface overview	Displays the type of network interface available in the device. The above figure shows the LAN interface overview
4.	Status	Displays the status of the LAN interface with the respect to the parameters shown in above figure
5.	Edit	Click on "Edit" option to configure the LAN-interface settings

The user can click on "edit" option to further modify the following configurations:

1. General setup

16.1 General Network interface setup configuration for thick AP

The default IP address of the access point is set to 192.168.1.1. The user can change the current static IP address of the device from this screen. DHCP client (DHCP 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 DHCP client or DHCPv6 client, the device will automatically get the IP address (IPv4 or IPv6) from the DHCP server.

Click on the "Edit" option in interface screen as shown in "Figure 33: Basic overview of the interface configuration screen for thick AP". A basic overview of the network interface setup configuration screen to switch network protocol is given below:

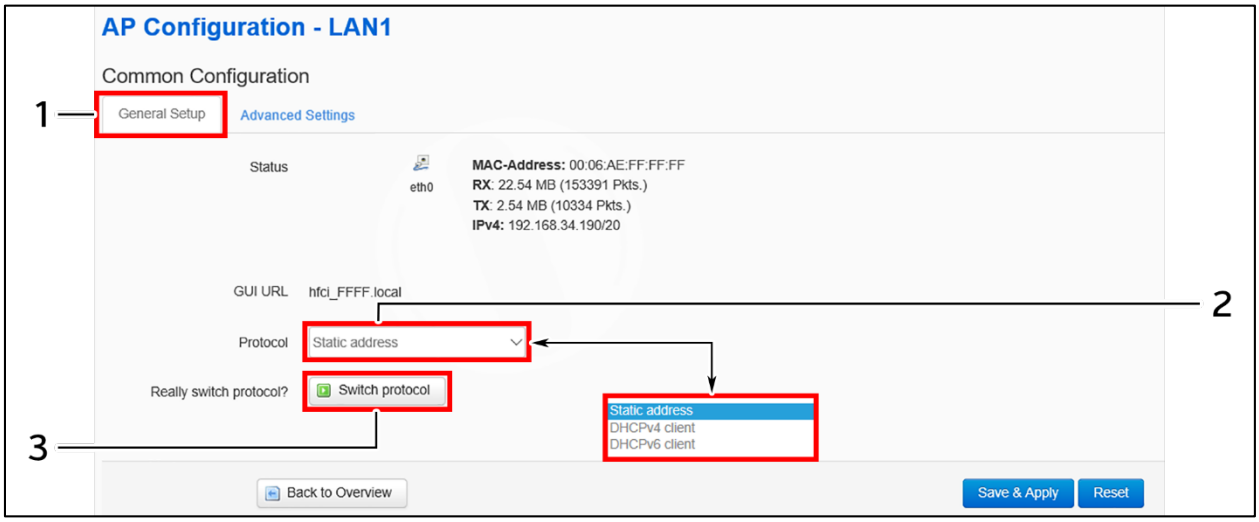

Figure 34: Basic overview of the network interface setup configuration screen to switch protocol for thick AP

Follow the steps given below to switch network protocol:

Table 28: List of actions to switch network protocol for thick AP

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

16.1.1 Static IP configuration for thick AP

The default IP address of the access point is set to 192.168.1.1. User can change the default IP address with an unused IP address. Refer “Figure 34: Basic overview of the network interface setup configuration screen to switch protocol for thick AP” and set the protocol to static address.

Refer the figure below to provide the static address parameters:

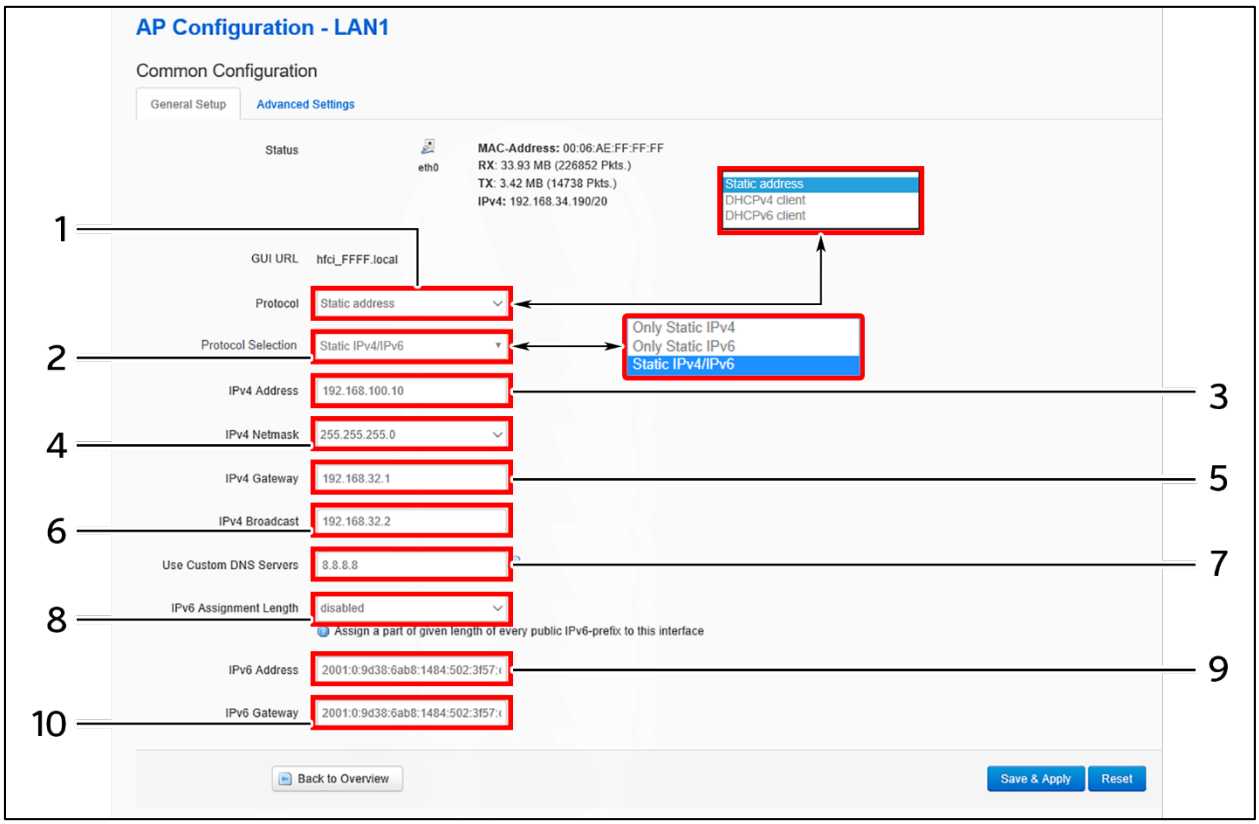

Figure 35: Basic overview of static address parameters for general network interface setup for thick AP

Follow the steps given below to provide static address parameters for thick AP:

Table 29: List of actions to provide static address parameters for thick AP

Callout	Name	Description
1.	Protocol	The protocol is set to “”Static address”. Enter the following parameters for the same
2.	Protocol Selection	Set the static address protocol to IPv4/IPv6/IPv4 & IPv6. Below parameters are shown with respect to IPv4 & IPv6 protocol selection
3.	IPv4 address	Enter the “IPv4 address”. This is a unique address of the Host/Device eg.192.168.100.10
4.	IPv4 netmask	Enter the “IPv4 netmask”. This specifies the number of bits for network part and host part e.g.255.255.255.0

Callout	Name	Description
5.	IPv4 gateway	Enter the “IPv4 gateway”. Gateway address is given to reach other network device e.g.192.168.100.254
6.	IPv4 broadcast	Enter the “IPv4 broadcast”. Broadcast address is to broadcast message in a network e.g. 192.168.100.255
7.	Use custom DNS servers	Enter the “DNS server”. Click on add icon to add multiple DNS servers. DNS server is to resolve the transition of domain name to IP and IP to domain name
8.	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. Provide below parameters if IPv6 prefix length is set to disabled
9.	IPv6 address	Enter the “IPv6 address”. Unique address of the Host/Device e.g.2001:11::100
10.	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.

16.1.2 DHCPv4 client configuration for thick AP

If the protocol is set to DHCPv4 client, the device will automatically get the IPv4 address from the DHCP server. Refer “Figure 34: Basic overview of the network interface setup configuration screen to switch protocol for thick AP” and set the protocol to DHCPv4 client.

Refer the figure below and switch the protocol to DHCPv4 client for thick AP:

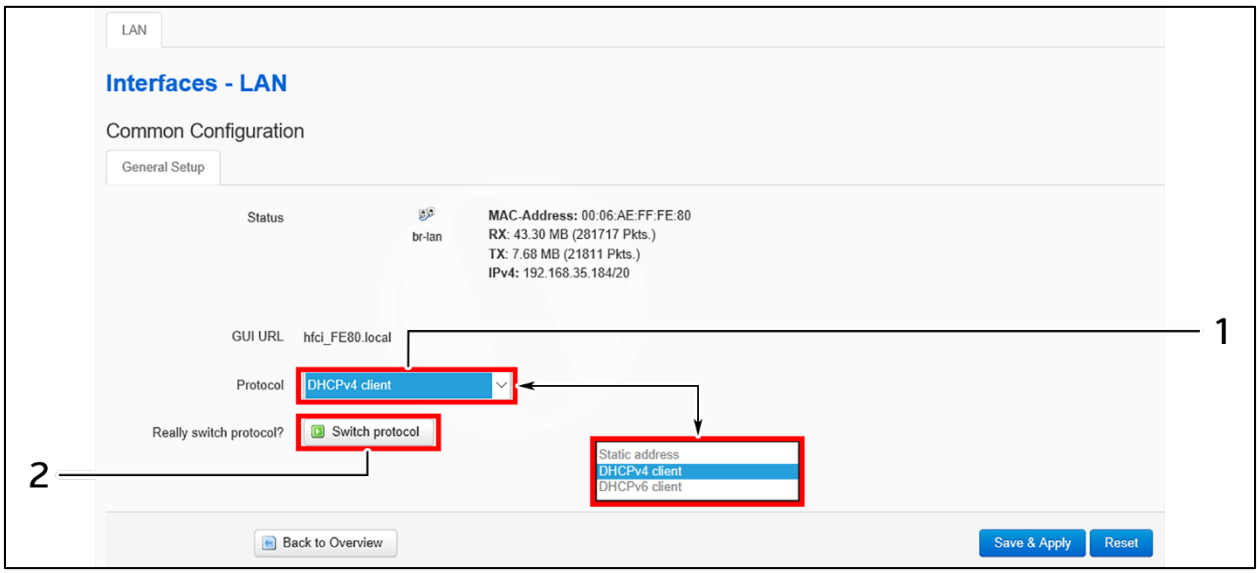

Figure 36: Basic overview of network interface screen to set the protocol to DHCPv4 for thick AP

Follow the steps given below to set the protocol to DHCPv4 for thick AP:

Table 30: List of actions to set the protocol to DHCPv4 for thick AP

Callout	Name	Description
1.	Protocol	Set the protocol from the dropdown list (Static address/DHCPv4 client/DHCPv6 client) to DHCPv4
2.	Really switch protocol	Click on “Switch protocol” to confirm the protocol switch

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

16.1.3 DHCPv6 client configuration for thick AP

If the protocol is set to DHCPv6 client, the device will automatically get the IPv6 address from the DHCP server. Refer “Figure 34: Basic overview of the network interface setup configuration screen to switch protocol for thick AP” and set the protocol to DHCPv6 client.

Refer the figure below and switch the protocol to DHCPv6 client for thick AP:

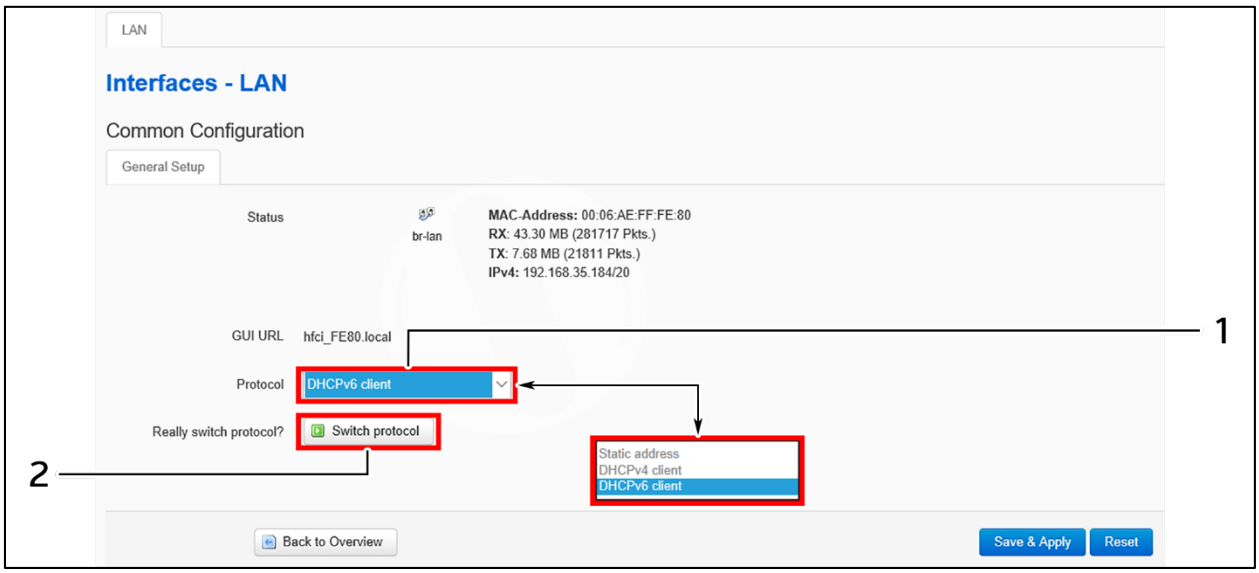

Figure 37: Basic overview of network interface screen to set the protocol to DHCPv6 for thick AP

Follow the steps given below to set the protocol to DHCPv6 for thick AP:

Table 31: List of actions to set the protocol to DHCPv6 for thick AP

Callout	Name	Description
1.	Protocol	Set the protocol from the dropdown list (Static address/DHCPv4 client/DHCPv6 client) to DHCPv6
2.	Really switch protocol	Click on “Switch protocol” to confirm the protocol switch

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

16.2 Network/Wireless/Radio and SSID configuration of thick AP

The wireless configuration screen of thick AP GUI enables the user to view and configure radio and SSID parameters. Multiple SSID can be added separately for 2.4 and 5 GHz radio. Radio configuration remains same for all SSIDs operating at the respective 2.4 and 5 GHz radio. All clients associated with respective SSID are also listed in a tabular form in this screen along with some basic information.

A basic overview of the wireless configuration screen for thick AP is given below:

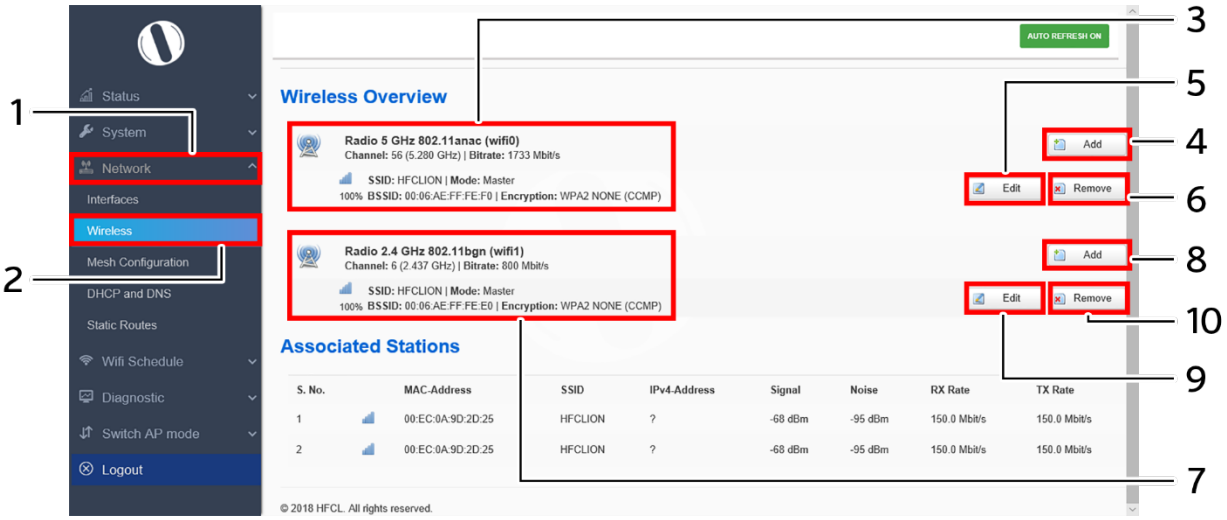

Figure 38: Basic overview of the wireless configuration screen for thick AP

Follow the steps given below to view the wireless configuration of thick AP:

Table 32: List of actions to view the wireless configuration of thick AP

Callout	Name	Description
1.	Network	Click on “Network” dropdown
2.	Wireless	Click on “Wireless” option
3.	5 GHz overview	Displays the overview of 5 GHz radio along with the list of associated SSIDs as shown in the above figure
4.	Add SSID/Radio Configuration	Click on the “Add” option to configure a new SSID or to update the radio configuration parameters at 5 GHz
5.	Edit SSID	Click on “Edit” option to modify the parameters of respective SSID configuration at 5 GHz
6.	Remove SSID	Click on “Remove” option to delete the respective SSID at 5 GHz
7.	2.4 GHz overview	Displays the overview of 2.4 GHz radio along with the list of associated SSIDs as shown in the above figure
8.	Add SSID/Radio Configuration	Click on the “Add” option to configure a new SSID or to update the radio configuration parameters at 2.4 GHz
9.	Edit SSID	Click on “Edit” option to modify the parameters of respective SSID configuration at 2.4 GHz
10.	Remove SSID	Click on “Remove” option to delete the respective SSID at 2.4 GHz

16.2.1 5 GHz radio configuration

This screen provides the user with options to configure the 5 GHz radio parameters such as channel bandwidth, respective channel or the channel selection process, and the power for the radio signal transmission. Refer the "Figure 38: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (4) to configure 5 GHz radio parameters.

A basic overview of the 5 GHz radio configuration screen is given below:

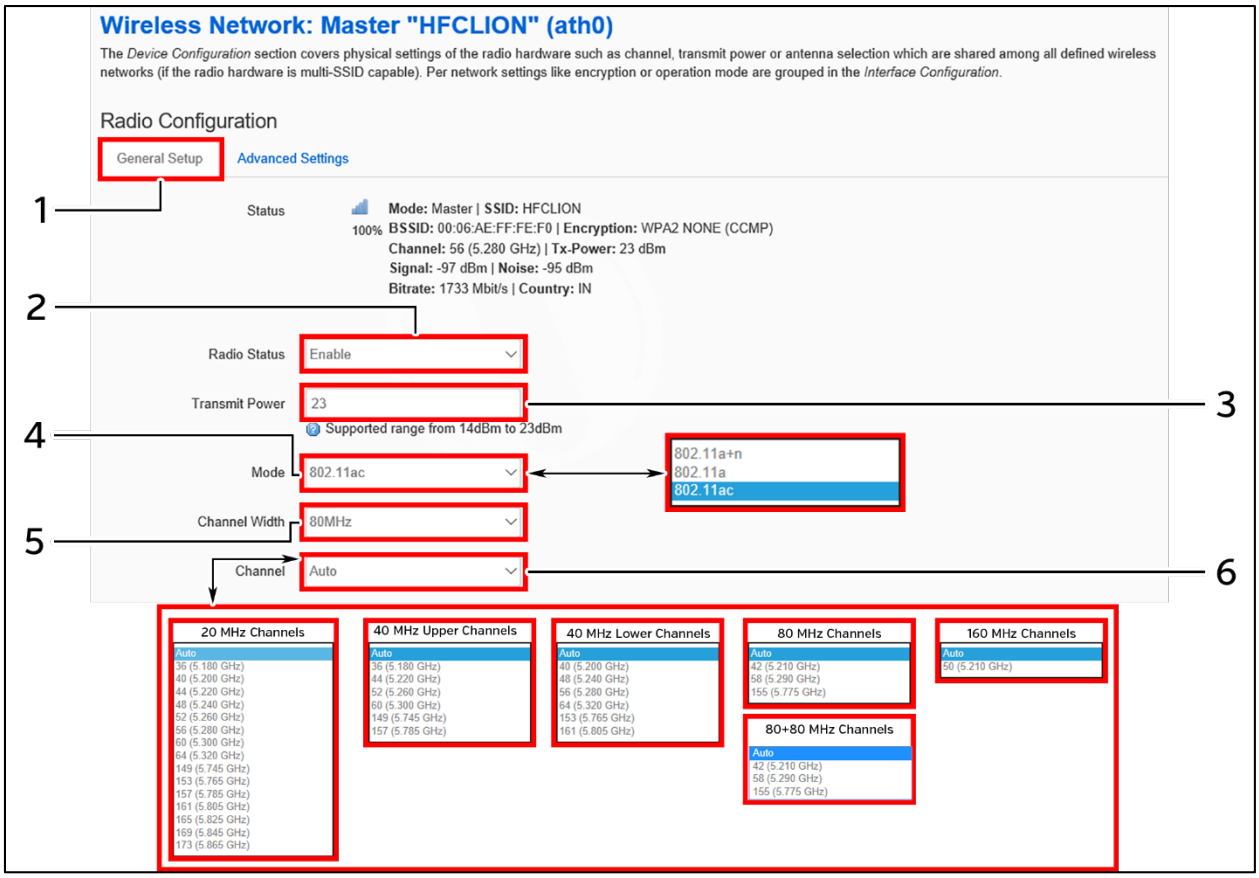

Figure 39: Basic overview of the 5 GHz radio configuration screen

Follow the steps given below and for 5 GHz radio configuration of thick AP:

Table 33: List of actions for 5 GHz radio configuration of thick AP

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	Radio Status	Enable or disable the 5 GHz radio with this option
3.	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 14 dBm to 23 dBm

Callout	Name	Description
4.	Mode	Select the radio operating mode from the dropdown list (802 11a/ac/a+n). Channel width and channel list varies with respect to the selected mode (802 11a/ac/a+n)
5.	Channel Width	Select the “Channel Width” from the dropdown list (20 MHz/40 MHz-Lower/40 MHz -Upper/80 MHz/ 80+80 MHz/160 MHz)
6.	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: 36/40/44/48/52/56/60/64/149/ 153/157/161/165/169/173. For 40 MHz Lower channel width, available channels are: 40/48/56/60/64/ 153/161. For 40 MHz Upper channel width, available channels are: 36/44/52/60/149/157. For 80 and 80+80 MHz channel width, available channels are: 42/58/155. For 160 MHz channel width, available channel is 50

Click “Save & Apply” to save the 5 GHz radio configuration of thick AP or click “Reset” to configure the same again.

16.2.2 2.4 GHz radio configuration

This screen provides the user with options to configure the 2.4 GHz radio parameters such as channel bandwidth, respective channel or the channel selection process, and the power for the radio signal transmission. Refer the "Figure 38: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) to configure 2.4 GHz radio parameters.

A basic overview of the 2.4 GHz radio configuration screen is given below:

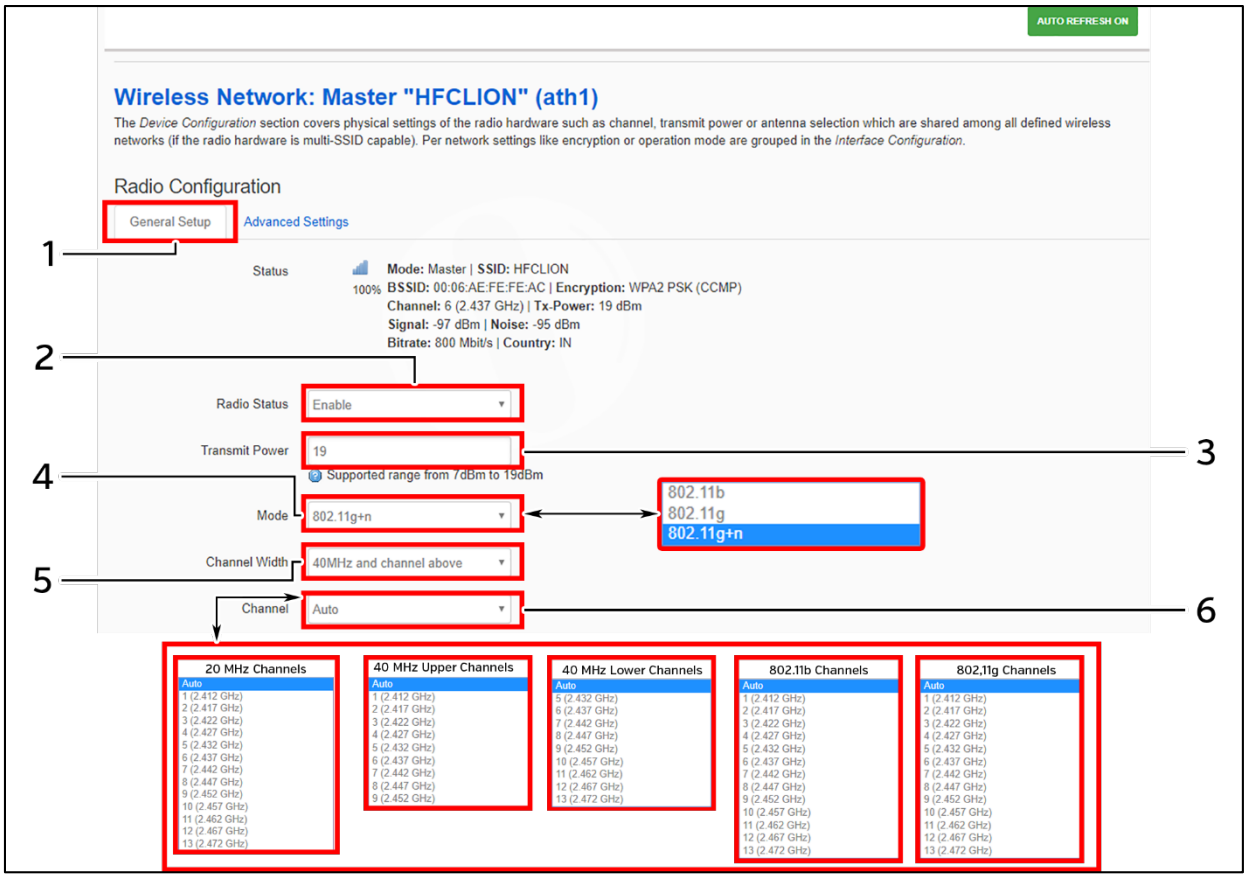

Figure 40: Basic overview of the 2.4 GHz radio configuration screen

Follow the steps given below and for 2.4 GHz radio configuration of thick AP:

Table 34: List of actions for 2.4 GHz radio configuration of thick AP

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	Radio Status	Enable or disable the 2.4 GHz radio with this option
3.	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 7 dBm to 19 dBm
4.	Mode	Select the radio operating mode from the dropdown list (802 11b/g/g+n). Channel width and channel list varies with

Callout	Name	Description
		respect to the selected mode (802 11b/g/g+n). Channel width parameter is required, if the mode is set to “802.11b/g”
5.	Channel Width	Select the “Channel Width” from the dropdown list (20 MHz/40 MHz-Lower/40 MHz -Upper). This parameter is needed only if the mode is set to “802.11g+n”
6.	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: 1/2/3/4/5/6/7/8/9/10/11/12/13 For 40 MHz Lower channel width, available channels are: 5/6/7/8/9/10/11/12/13. For 40 MHz Upper channel width, available channels are: 1/2/3/4/5/6/7/8/9. Available channels in 802.11b/g are: 1/2/3/4/5/6/7/8/9/10/11/12/13

Click “Save & Apply” to save the 2.4 GHz radio configuration of thick AP or click “Reset” to configure the same again.

16.2.3 Advanced radio configuration (2.4 GHz and 5 GHz)

This screen provides the user with options to configure the advanced radio parameters (2.4 GHz and 5 GHz) such as country code and Tx/Rx chain mask. Refer the "Figure 38: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) for 2.4 GHz or Add SSID/Radio Configuration option (4) for 5 GHz to configure advanced radio parameters.

A basic overview of the advanced radio parameters (2.4 GHz and 5 GHz) configuration screen is given below:

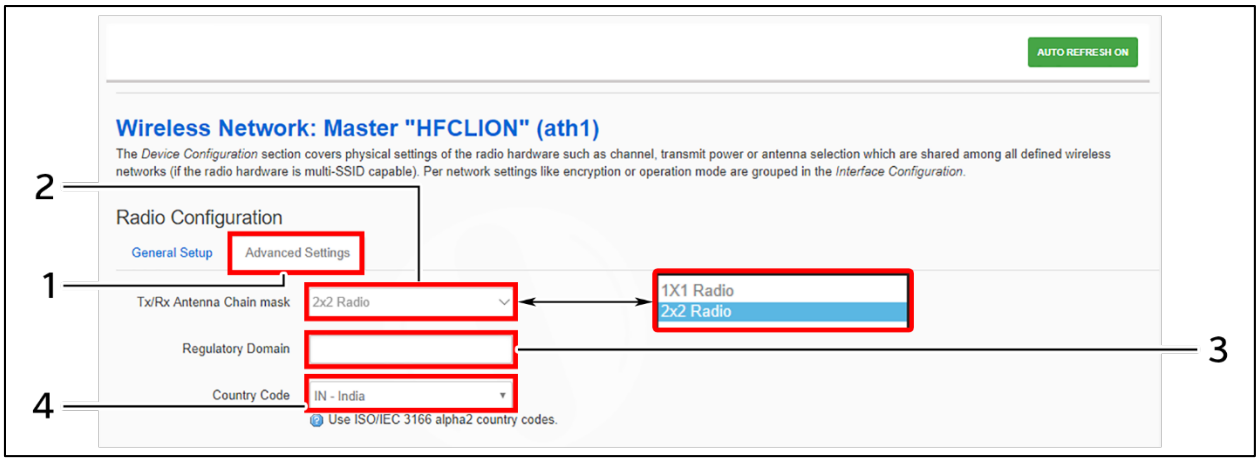

Figure 41: Basic overview of the advanced radio parameters (2.4 GHz and 5 GHz) configuration screen

Follow the steps given below for advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP:

Table 35: List of actions for advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP

Callout	Name	Description
1.	Advanced Settings	Click on "Advanced Settings" option
2.	Tx/Rx Antenna Chain mask	Select the chain mask from the dropdown list (1x1/2x2)
3.	Regulatory Domain	Enter the regulatory domain
4.	Country Code	Select the country code from the dropdown list. Channels are listed in accordance to the selected country

Click "Save & Apply" to save the advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP or click "Reset" to configure the same again.

16.2.4 SSID configuration

Refer the "Figure 38: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) for 2.4 GHz or Add SSID/Radio Configuration option (4) for 5 GHz to configure new SSIDs. Click on Edit option (9) for 2.4 GHz or Edit option (5) for 5 GHz to edit existing SSIDs. This screen provides the user with options to configure the SSID operating at both 2.4 and 5 GHz radio. The SSID configuration parameters are further categorized as follows:

1. General setup
2. Wireless Security
3. MAC Filter
4. Advanced Settings

16.2.4.1 *SSID/General setup (2.4 GHz and 5 GHz)*

Three type if SSIDs are created from this screen as follows:

1. **Access Point SSID:** By default the SSID mode is set to "Access Point". This type of SSID is used by the clients to connect with the respective access point.
2. **Access Point WDS SSID:** This type of SSID mode is used to achieve wireless distribution system feature. Apart from operating as a normal access point SSID to serve the connecting clients, these SSIDs also act as repeaters for client access points of wireless distribution system. This type of SSID is needed for a client WDS SSID to complete the WDS link. Make sure to create at least one Access Point WDS SSID before configuring any Client WDS SSID.
3. **Client WDS SSID:** This type of SSID mode is used to achieve wireless distribution system feature. These SSIDs are used by the client access points of wireless distribution system to connect with the respective service provider Access Point WDS SSID.

Refer the "Figure 38: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (4) to configure 5 GHz radio parameters or click on Add SSID/Radio Configuration option (8) to configure 2.4 GHz radio parameters. A basic overview of the screen to configure general SSID parameters is given below:

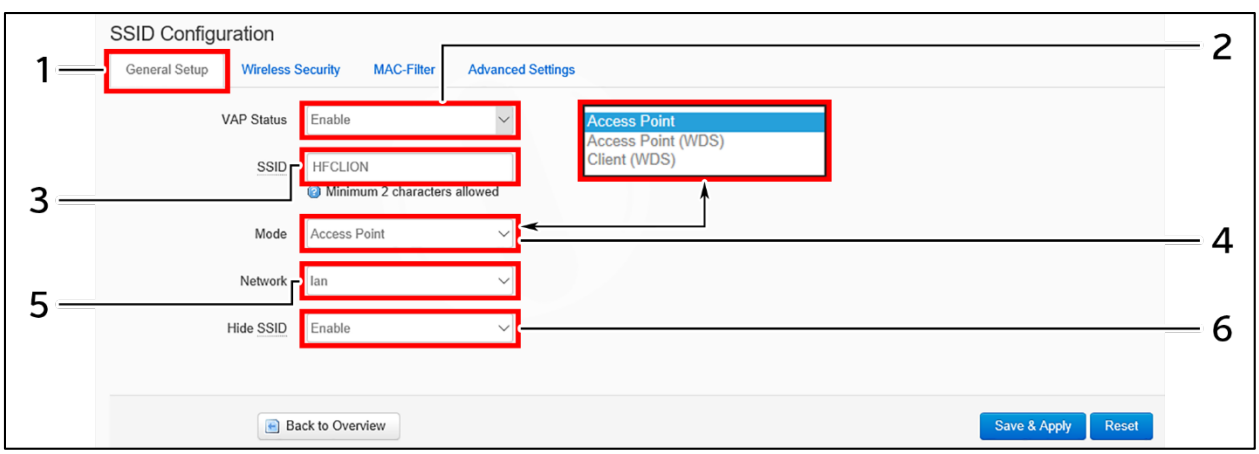

Figure 42: Basic overview of the screen to configure general SSID parameters

Follow the steps given below and configure the general SSID parameters:

Table 36: List of actions to configure the general SSID parameters

Callout	Name	Description
1.	General Setup	Click on “General Setup” option
2.	VAP Status	Enable or disable the VAP with this option. Once disabled, the SSID will not be available in the search anymore.
3.	SSID	Enter a unique name for the SSID
4.	Mode	Select the SSID operating mode from the dropdown list (Access Point/Access Point WDS/Client WDS). If “Client WDS” option is selected, provide the valid parameters of Access Point WDS SSID
5.	Network	Select the network interface from the dropdown list
6.	Hide SSID	Enable/Disable SSID broadcast with this option. Once disabled, the SSID will not be available in the search anymore. The user can still associate with the SSID if valid authenticated credentials are provided

Click “Save & Apply” to save the general SSID configuration of thick AP or click “Reset” to configure the same again.

16.2.4.2 *SSID/Wireless security (2.4 GHz and 5 GHz)*

By default the wireless security is set to "No Encryption", and other options are provided to change the encryption accordingly as follows:

1. **No Encryption:** Any device can connect to the network. Not recommended.
2. **WPA-PSK(Wi-Fi Protected Access):** WPA is part of the wireless security standard (802.11i) standardized by the Wi-Fi Alliance and was intended as an intermediate measure to take the place of WEP while the 802.11 standard was being prepared. It supports TKIP/AES encryption. The personal authentication is the pre-shared key (PSK) that is an alphanumeric passphrase shared with the wireless peer.
3. **WPA2-PSK:** WPA2 is the implementation of security standard specified in the final 802.11i standard. It supports AES encryption and this option uses pre-shared key (PSK) based authentication.
4. **WPA-PSK/WPA2-PSK Mixed mode:** Allows both WPA and WPA2 clients to connect simultaneously using PSK authentication.
5. **WPA2-EAP:** Allows you to use WPA2 with RADIUS server authentication.

A basic overview of the screen to configure wireless security parameters of SSID is given below:

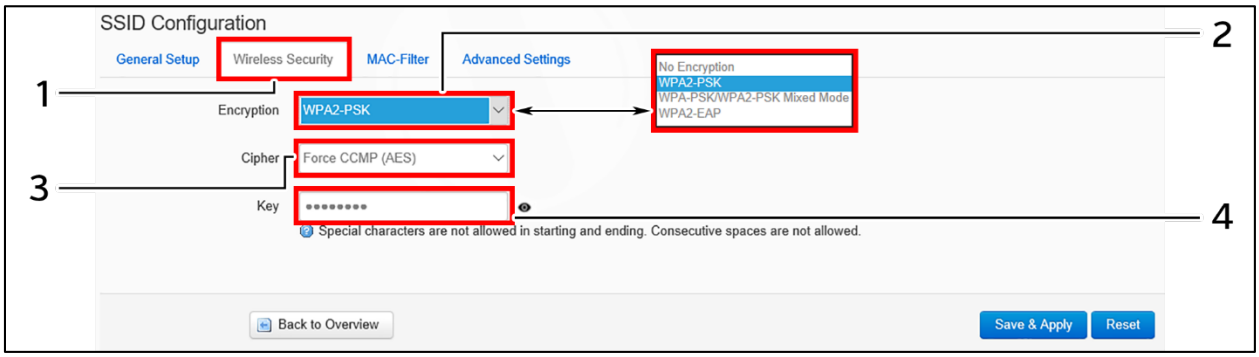

Figure 43: Basic overview of the screen to configure wireless security parameters of SSID

Follow the steps given below and configure the wireless security parameters of SSID:

Table 37: List of actions to configure the wireless security parameters of SSID

Callout	Name	Description
1.	Wireless Security	Click on "Wireless Security" option
2.	Encryption	Select the encryption protocol from the dropdown list (Open/WPA-PSK/WPA2-PSK/ WPA2-PSK_Mixed_Mode/ WPA2-EAP). No passphrase is needed in case of "Open" type network authentication protocol
3.	Cipher	This a read only parameter and the user doesn't need to do anything with "cipher" option, by default "Auto" option is selected.
4.	Key	Enter a unique password for the SSID

Click "Save & Apply" to save the wireless security configuration of SSID or click "Reset" to configure the same again.

16.2.4.3 *SSID/MAC filter (2.4 GHz and 5 GHz)*

The user can add multiple MAC addresses with allow and deny policy and the same is mapped with respective SSID. A basic overview of the screen to configure the MAC filter for SSID configuration is given below:

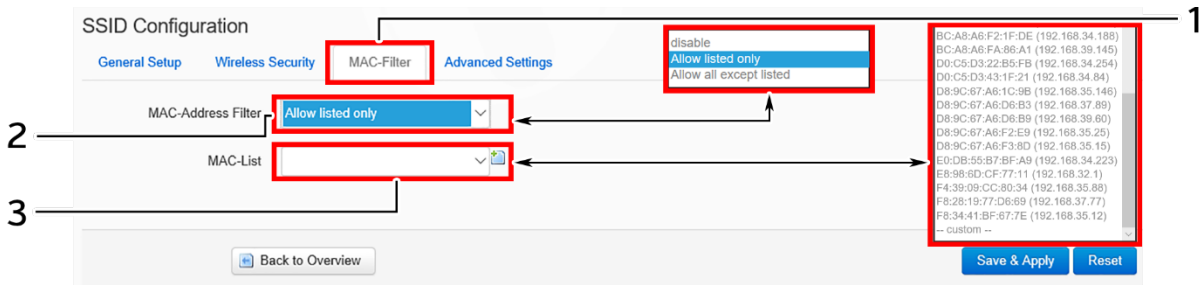

Figure 44: Basic overview of the screen to configure the MAC filter for SSID configuration

Follow the steps given below and configure the MAC filter for SSID configuration:

Table 38: List of actions to configure the MAC filter for SSID configuration

Callout	Name	Description
1.	MAC-Filter	Click on “MAC-Filter” option
2.	MAC address filter	Click on the dropdown and disable or set the allow/deny policy for the MAC filter
3.	MAC List	Click on the dropdown and select the MAC address from the list or click on “Custom” to add the MAC address manually. Click on the “+” icon to add multiple MAC addresses

Click “Save & Apply” to save the MAC filter configuration or click “Reset” to configure the same again.

16.2.4.4 *SSID/Advanced settings (2.4 GHz and 5 GHz)*

A basic overview of the screen to configure the advanced parameters of SSID configuration is given below:

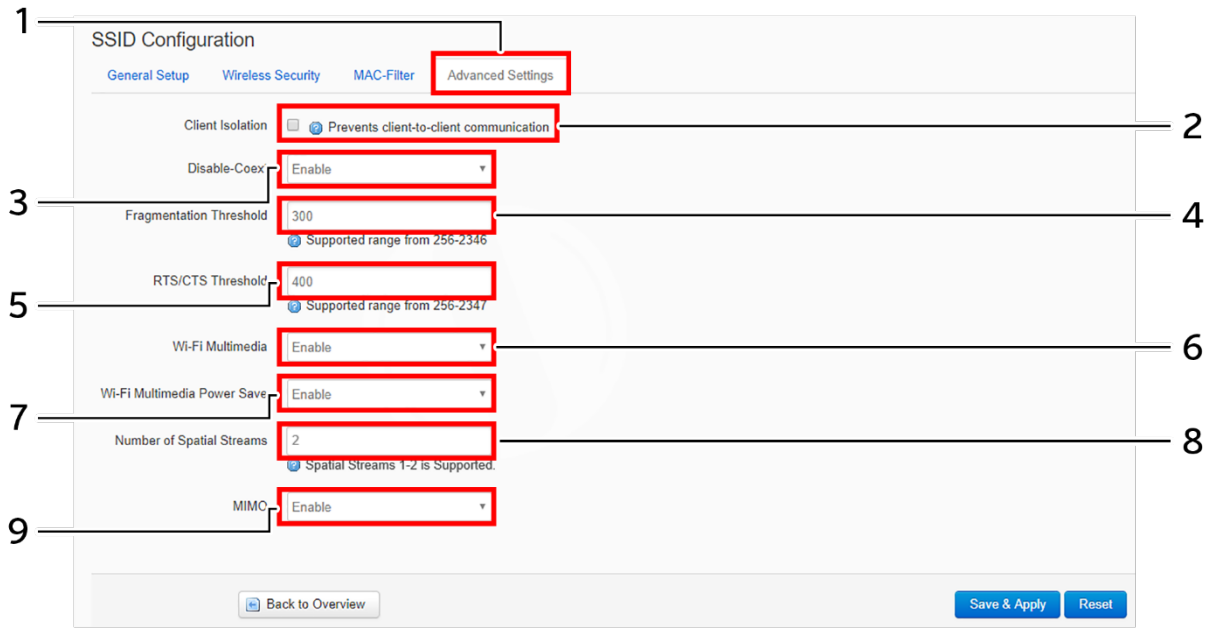

Figure 45: Basic overview of the screen to configure the advanced parameters of SSID configuration

Follow the steps given below and configure the advanced parameters of SSID configuration:

Table 39: List of actions to configure the advanced parameters of SSID configuration

Callout	Name	Description
1.	Advanced Settings	Click on “Advanced Settings” option
2.	Client Isolation	Click on the check box and enable or disable the client isolation feature. If the feature is enabled, it prevents client to client communication
3.	Disable-Coext	Enable/Disable the co-existence option
4.	Fragmentation Threshold	Set the fragmentation threshold value. The supported range is between 256 to 2346
5.	RTS/CTS Threshold	Set the RTS/CTS Threshold value. The supported range is between 256 to 2347
6.	Wi-Fi Multimedia	Enable/Disable the Wi-Fi Multimedia option
7.	Wi-Fi Multimedia Power Save	Enable/Disable the Wi-Fi Multimedia Power Save option
8.	Number of Spatial Streams	Set the number of spatial streams between 1 to 4
9.	MIMO	Enable/Disable the MIMO feature. This option is available only for 5 GHz radio SSID
Note: The MIMO feature is not available in 2.4 GHz radio SSID		

Click “Save & Apply” to save the advanced parameters of SSID configuration or click “Reset” to configure the same again.

16.3 Network/Mesh configuration of thick AP

A wireless mesh network serves as a network of radio nodes organized in a mesh topology. All APs participating in mesh topology does not need to have a wired connection for backhaul connectivity and only one root AP serves that purpose.

Mesh configuration require access points to operate in two operating modes as follows:

1. **Root Access Points:** Root Access Points have wired connections, for example, Ethernet backhaul to a wired network and to Wireless LAN Controller.
2. **Repeater:** Repeats wireless signals to extend range without being connected with cable to Access Point, or with clients.

Mesh configuration allows access points to connect with each other in mesh topology. An access point (Root AP) is connected to the wired network with the use of wireless connections over the 802.11 radio backhaul and other access points act as repeaters in mesh topology.

A basic overview of the mesh configuration screen for thick AP is given below:

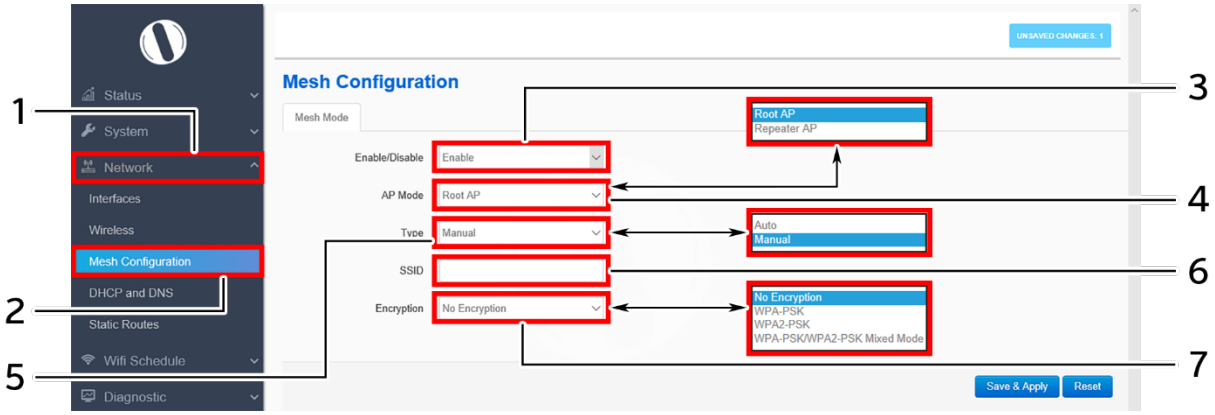

Figure 46: Basic overview of the mesh configuration screen for thick AP

Follow the steps given below to view the mesh configuration of thick AP:

Table 40: List of actions to view the mesh configuration of thick AP

Callout	Name	Description
1.	Network	Click on “Network” dropdown
2.	Mesh Configuration	Click on “Mesh Configuration” option
3.	Mesh Mode	Enable or disable the mesh mode. If enabled, provide the following parameters
4.	AP Mode	Select the contributing mode of the access point in the mesh topology from the drop down list (Root AP/Repeater AP). If the AP mode is set to “Root AP”, make sure that the AP is connected to the wired network
5.	Type	Select the type of mesh configuration from the dropdown list (Auto/Manual). In case of “Auto” the connection between and root AP and repeater AP is fixed automatically and in case of “manual” the user need to define the SSID and

Callout	Name	Description
		encryption parameters. For a successful mesh configuration the SSID and the encryption parameters of root and repeater APs should match with each other
6.	SSID	Enter a unique name for the mesh SSID. Only a single SSID is used throughout the mesh network. This SSID operates in two hidden modes, one as master (receiver) and the other as managed (provider). Between a root AP and repeater AP, the managed mode of the root AP SSID connects with the master mode of the repeater AP. Between two repeater APs, the managed mode SSID of the 1st repeater AP connects with the master mode of the next repeater AP. This way all APs are connected wirelessly with each other in a mesh network. If any of the repeater is missing from the mesh network, the associated repeater AP connects itself with the next available repeater or Root AP in a similar way as discussed above
7.	Encryption	Select the encryption protocol from the dropdown list (Open/WPA-PSK/WPA2-PSK/ WPA2-PSK_Mixed_Mode). No passphrase is needed in case of “Open” type network authentication protocol

Click “Save & Apply” to save the advanced parameters of SSID configuration or click “Reset” to configure the same again.

16.4 DHCP and DNS configuration of thick AP

The AP itself can act as a DHCP service provider for the connected clients and configuration for the same is executed from this screen. A basic overview of the screen to enable thick AP as DHCP server is given below:

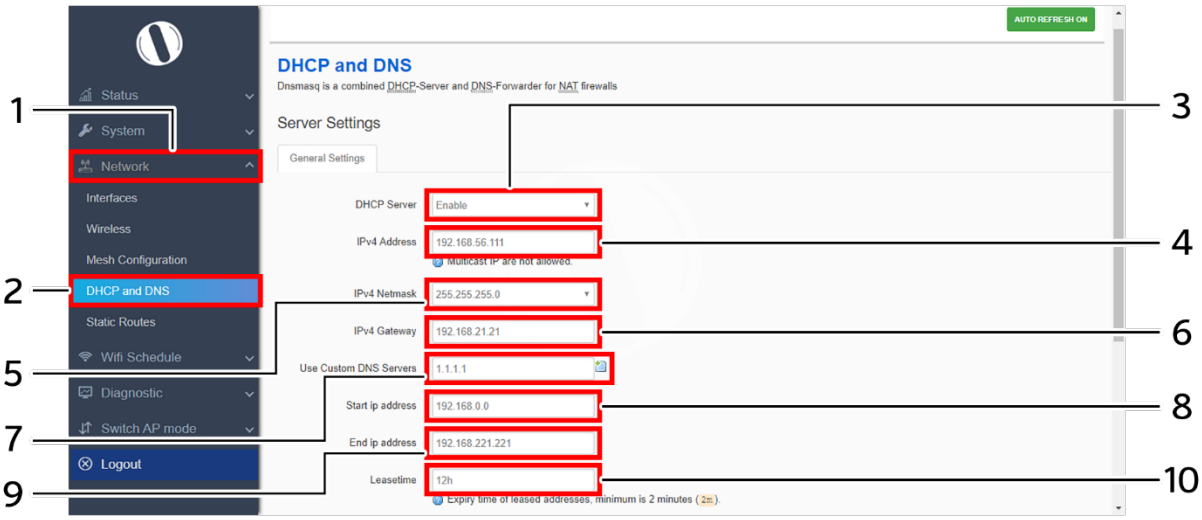

Figure 47: Basic overview of the screen to enable thick AP as DHCP server

Follow the steps given below to enable thick AP as DHCP server:

Table 41: List of actions to enable thick AP as DHCP server

Callout	Name	Description
1.	Network	Click on “Network” dropdown
2.	DHCP and DNS	Click on “DHCP and DNS” option
3.	DHCP Server	Enable the thick AP as DHCP server and enter the following parameters
4.	IPv4 Address	Enter the address in IPv4 format for the DHCP server
5.	IPv4 Netmask	Select the netmask from the dropdown list
6.	IPv4 Gateway	Enter the address in IPv4 format for the DHCP gateway
7.	Use Custom DNS Servers	Enter the IP address for DNS server. Click on add icon and multiple DNS servers
8.	Start IP Address	Enter a start IP address. The DHCP server assigns the new IP addresses to the clients from the defined start IP address
9.	End IP Address	Enter an end IP address. The DHCP server assigns the IP addresses to the clients till the defined end IP address
10.	Lease Time	Enter a value to set a limit on the lease time. New addresses will be assigned to the associated clients once the previous lease has expired as per the specified lease time

Click “Save & Apply” to enable thick AP as DHCP server or click “Reset” to configure the same again.

16.4.1 Static/Active lease settings

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. A basic overview of the screen to configure a static lease is given below:

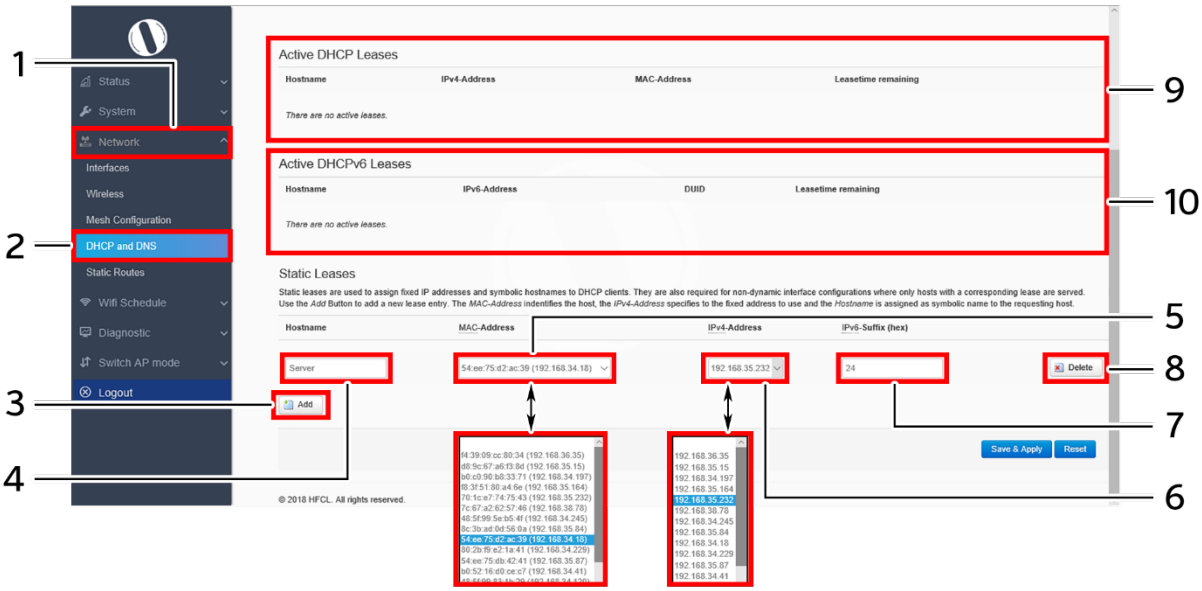

Figure 48: Basic overview of the screen to configure a static lease

Follow the steps given below to configure a static lease:

Table 42: List of actions to configure a static lease

Callout	Name	Description
1.	Network	Click on “Network” dropdown
2.	DHCP and DNS	Click on “DHCP and DNS” option
3.	Add	Click on “Add” option to add a new static lease. The user can add multiple static leases
4.	Host Name	Provide a unique name to the static lease for identification
5.	MAC-Address	Click on the dropdown and select a MAC-address from the list. The selected MAC-address identifies the host
6.	IPv4 Address	Click on the dropdown and select an IPv4-address from the list. The selected IPv4-address is assigned to the host as a fixed address
7.	IPv6-Suffix	Enter the IPv6-suffix for the host

Click “Save & Apply” to save the static lease or click “Reset” to configure the same again.

8.	Delete	Click on the “Delete” option to remove the respective static lease
9.	Active DHCP Leases	Displays all active IPv4 leases in a listed form
10.	Active DHCPv6 Leases	Displays all active IPv6 leases in a listed form

16.5 Static Routes

User can configure static routes and redirect packets to the destination network. A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.

A basic overview of the static route configuration screen for thick AP is given below:

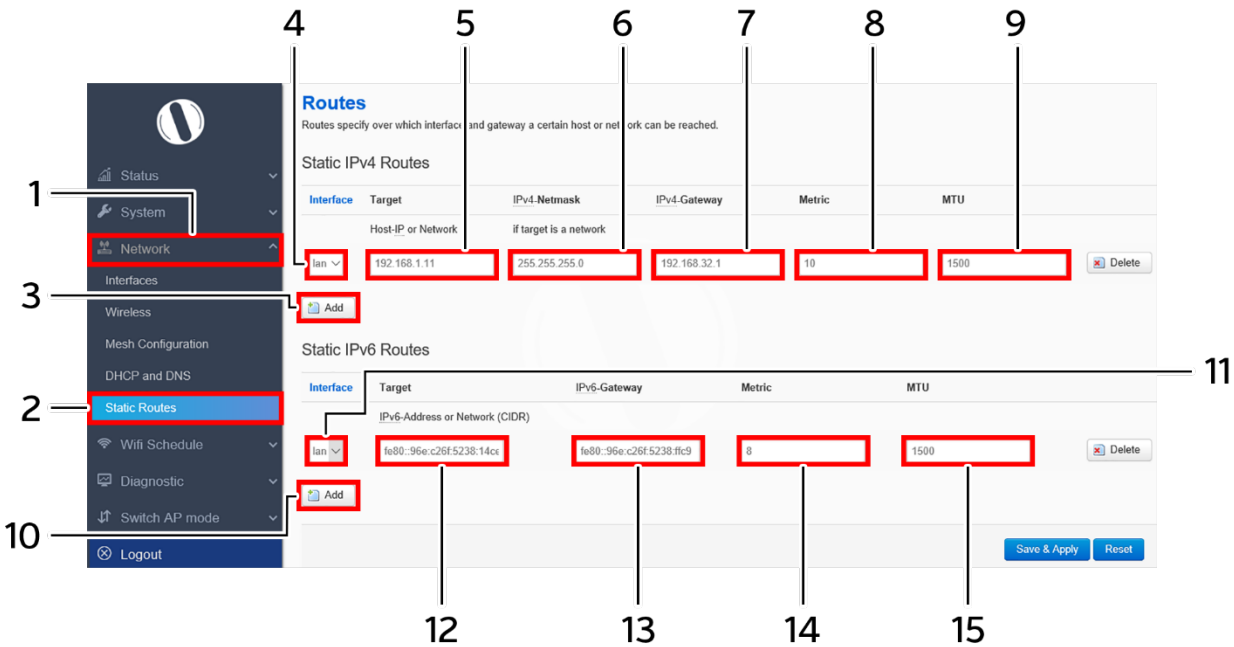

Figure 49: Basic overview of the static route configuration screen for thick AP

Follow the steps given below for static route configuration of thick AP:

Table 43: List of actions for static route configuration of thick AP

Callout	Name	Description
1.	Network	Click on “Network” dropdown
2.	Static Route	Click on “Static Route” option
		Static IPv4 Routes
3.	Add	Click on “Add” option to add a new static route in IPv4 format
4.	Interface	Select the physical network interface through which this route is accessible from the dropdown list (WAN or LAN)
5.	Target	Enter the IP address of the destination host or network in IPv4 format to which the route leads.
6.	IPv4-Netmask	Enter the IPv4 netmask for the destination host or network. By default subnet mask is set to 255.255.255.255
7.	IPv4-Gateway	Enter the IP address of the gateway in IPv4 format through which the destination host or network can be reached. If the current AP is being used to connect network with the Internet, then your gateway IP is the AP's IP address. If you

Callout	Name	Description
		have another router handling your network's Internet connection, enter the IP address of that router instead
8.	Metric	Enter a value that defines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen
9.	MTU	Enter the MTU size, by default it is set to 1500.

Click “Save & Apply” to save the static IPv4 route configuration or click “Reset” to configure the same again.

Static IPv6 Routes		
10.	Add	Click on “Add” option to add a new static route in IPv6 format
11.	Interface	Select the physical network interface through which this route is accessible from the dropdown list (WAN or LAN)
12.	Target	Enter the IP address of the destination host or network in IPv6 format to which the route leads.
13.	IPv6-Gateway	Enter the IP address of the gateway in IPv6 format through which the destination host or network can be reached. If the current AP is being used to connect network with the Internet, then your gateway IP is the AP's IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead
14.	Metric	Enter a value that defines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen
15.	MTU	Enter the MTU size, by default it is set to 1500.

Click “Save & Apply” to save the static IPv6 route configuration or click “Reset” to configure the same again.

17 Wi-Fi Schedule

This screen is provided with options to create, edit, or delete a Wi-Fi schedule. A basic overview of the screen is given below:

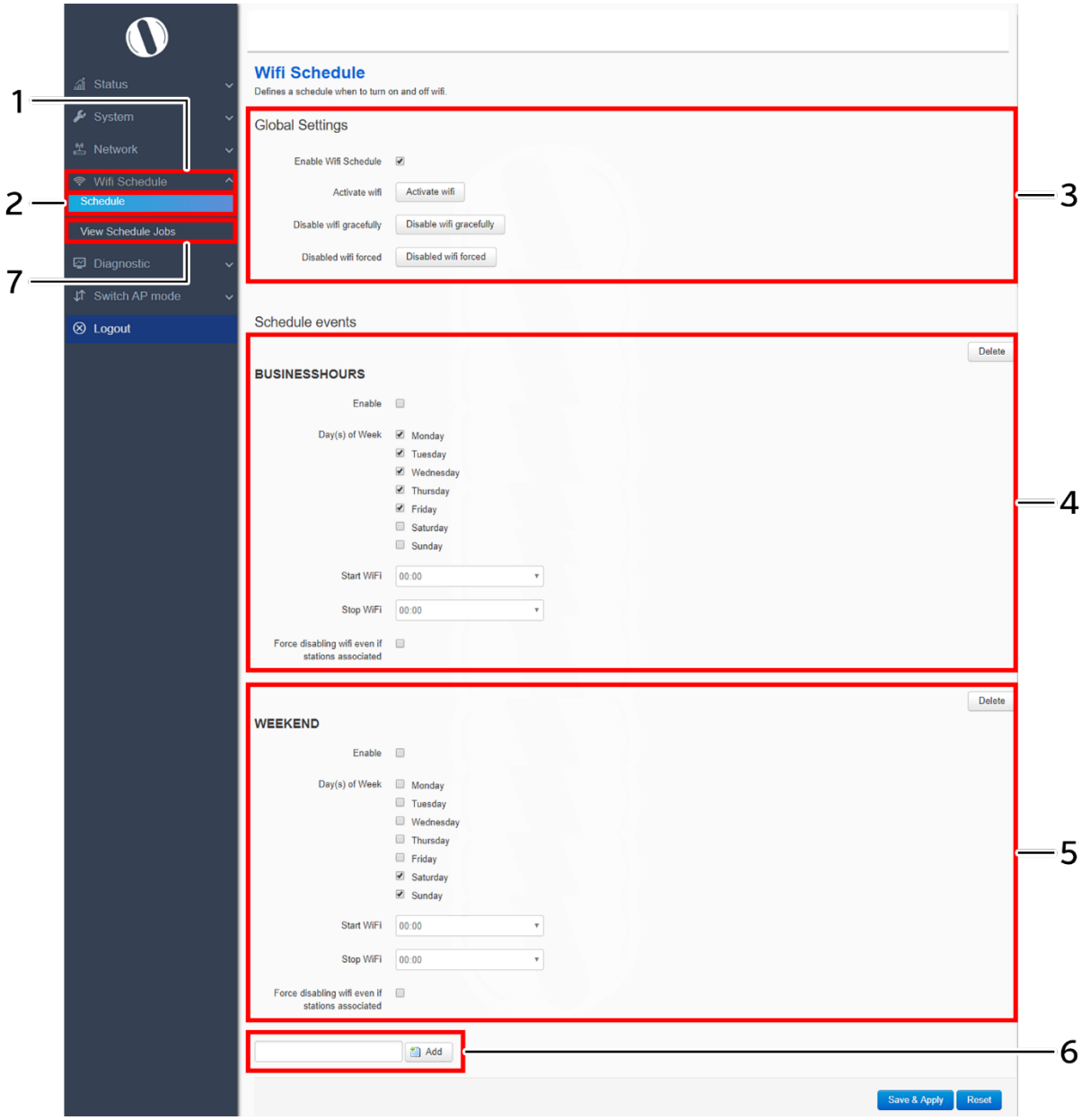

Figure 50: Basic overview of the Wi-Fi schedule screen

Follow the steps given below to create, edit, or delete a Wi-Fi schedule:

Table 44: List of actions to create, edit, or delete a Wi-Fi schedule

Callout	Name	Description
1.	Wi-Fi Schedule	Click on "Wi-Fi Schedule" dropdown
2.	Schedule	Click on "Schedule" option
3.	Global Settings	Configure the Global settings for a schedule. Refer image above for parameters
4.	Schedule Event/Business Hours	Enable and set the schedule in business hours for selected global settings. If saved, the global settings are applied at set schedule
5.	Schedule Event/Weekend Hours	Enable and set the schedule in weekend hours for selected global settings. If saved, the global settings are applied at set schedule
6.	Add	Click on "Add" option to create a new schedule
7.	View Scheduled Jobs	Click on the option to view the scheduled jobs

Click "Save & Apply" to save the static Wi-Fi schedule or click "Reset" to configure the same again.

18 Diagnostics

Following are the diagnostic features provided in thick AP GUI.

18.1 Routes

This screen is provided to view the active routes on the system. A basic overview of the screen to view the active routes is given below:

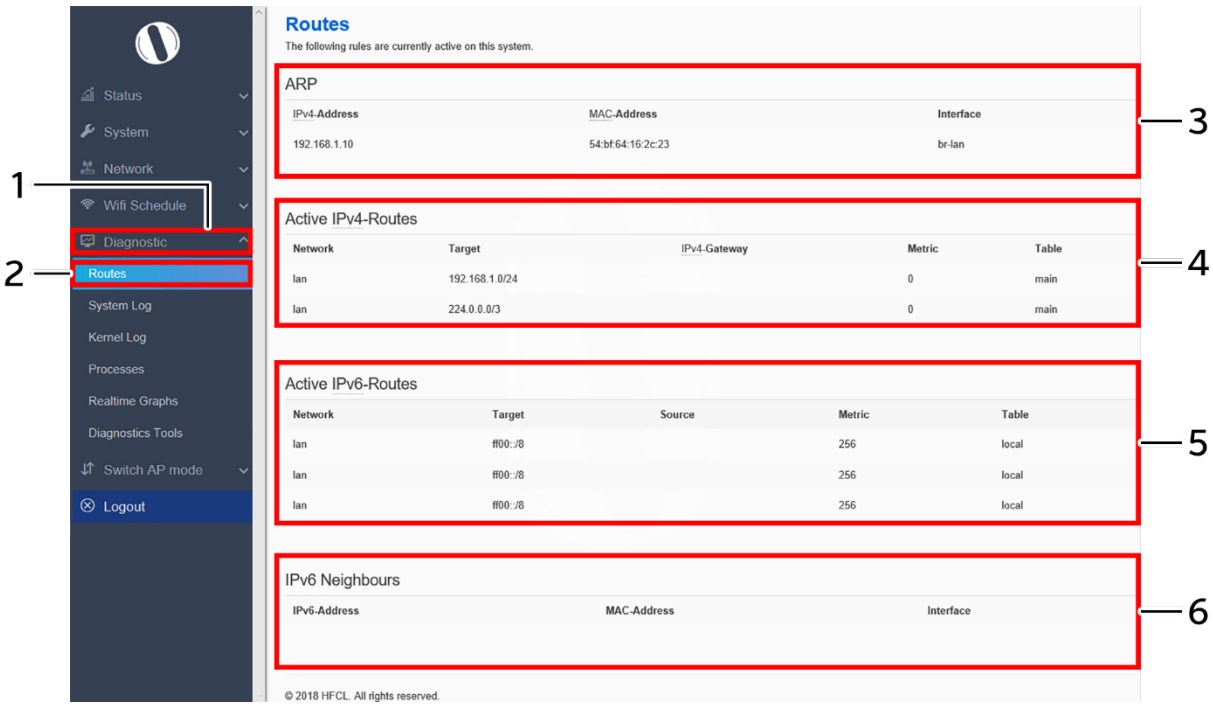

Figure 51: Basic overview of the screen to view the active routes

Follow the steps given below to view the active routes on the system:

Table 45: List of actions to view the active routes on the system

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Routes	Click on “Routes” option
3.	ARP	Displays the MAC addresses of all reachable IPs. The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address associated with a given internet layer address, typically an IPv4 address.
4.	Active IPv4 Routes	Displays all the IPv4 routes which are active at present
5.	Active IPv6 Routes	Displays all the IPv6 routes which are active at present
6.	IPv6 Neighbors	Displays neighboring IPv6 devices of NDP enabled devices. The Neighbor Discovery Protocol (NDP) is a protocol in the Internet protocol suite used with IPv6. It operates at the link layer of the Internet model, and is responsible for gathering various information

Callout	Name	Description
		to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices

18.2 System Log

This screen is provided to view the AP logs if the user faces any issue or wants to view the back-end logs. Only new logs are shown in this screen. However, old logs are stored in the database but will not be shown in this screen.

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

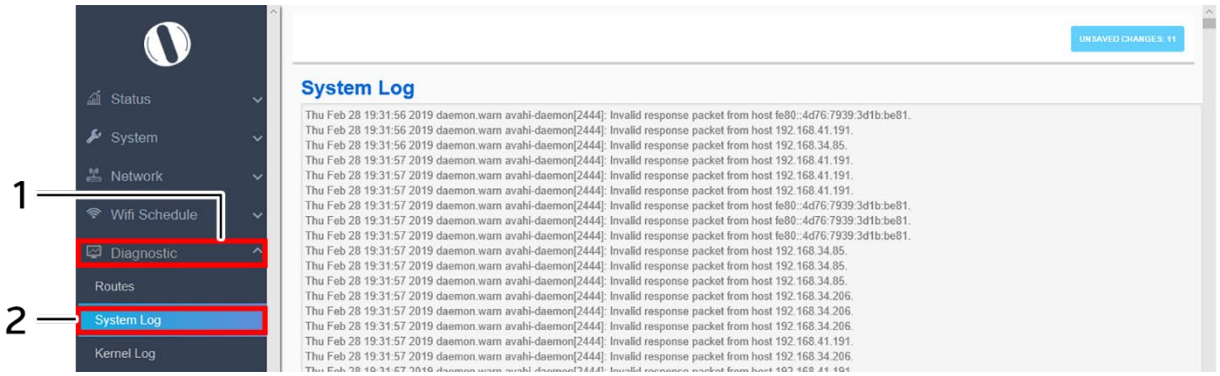

Figure 52: Basic overview of the System Log screen

Follow the steps given below to view the system log of AP:

Table 46: 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 AP application software are displayed here for monitoring purpose

18.3 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 AP.

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

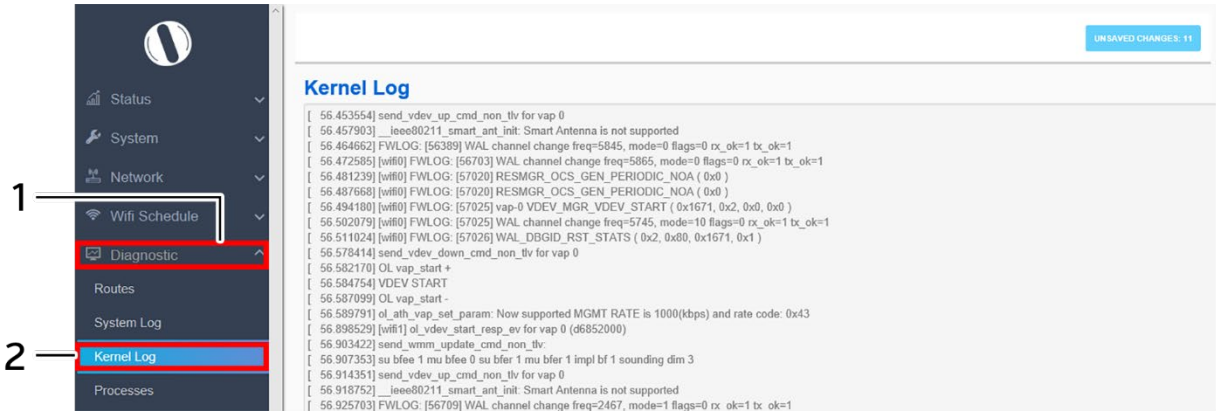

Figure 53: Basic overview of the Kernel Log screen

Follow the steps given below to view the Kernel log of the AP:

Table 47: 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

18.5 Real-time Graphs

The real time load/traffic 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 inbound and outbound traffic of the associated SSIDs, bridge interface, and Ethernet interfaces along with average and the peak traffic values. A basic overview of the Real-time graphs traffic screen is given below:

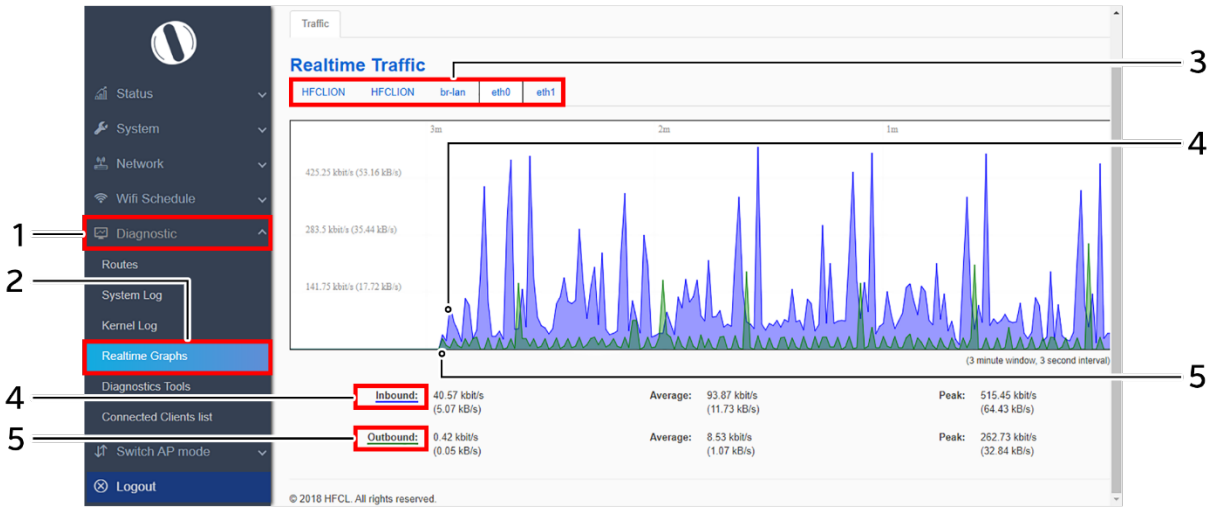

Figure 54: Basic overview of the Real-time graphs/ traffic

Follow the steps given below to view the real-time traffic graphs of the AP:

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

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Real-time graphs	Click on “Real-time graphs” option
3.	Real-time Traffic	Select any of the interface to check the inbound and outbound traffic across it. The graphs are available to show the traffic across SSIDs, Bridge Interface, and Ethernet Interface (eth-0 and eth-1)
4.	Inbound	Displays the inbound traffic at the selected interface in color coded format
5.	Outbound	Displays the outbound traffic at the selected interface in color coded format

18.6 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

18.6.1 Check the network connection/status

This utility is used to test connectivity between the respective AP and another device on the network. A basic overview of the Diagnostic Tools screen to check the connection status is given below:

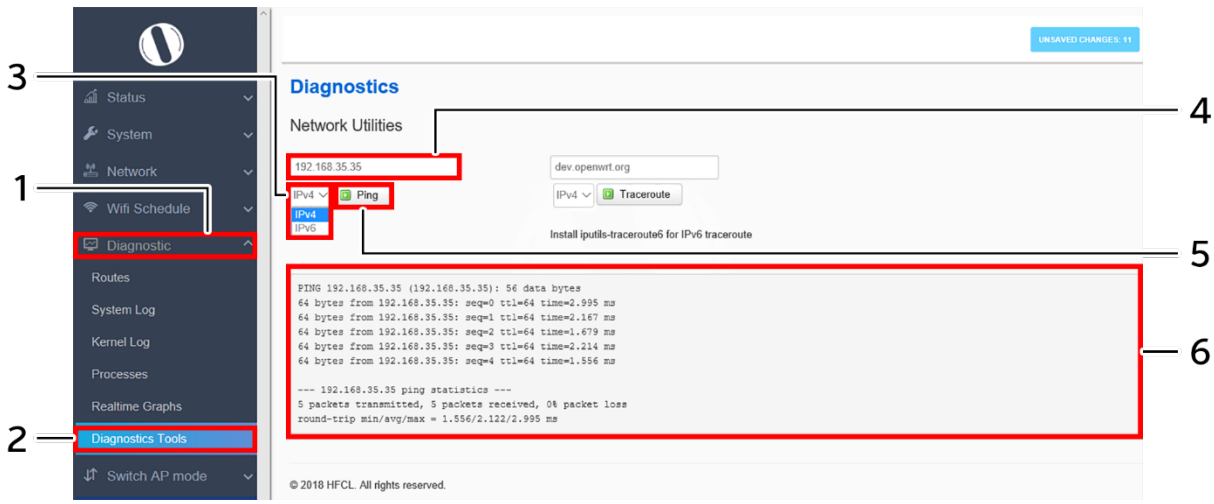

Figure 55: Basic overview of the diagnostics tool screen to check the connection status

Follow the steps given below to check the connection status:

Table 49: List of actions to check the connection status

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Diagnostics Tools	Click on “Diagnostics Tools” 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

18.6.2 Check the route of the established network connection

This utility will display all the routers present between the destination IP address and this AP. Up to 30 “hops” (intermediate routers) between the AP and the destination can be monitored.

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

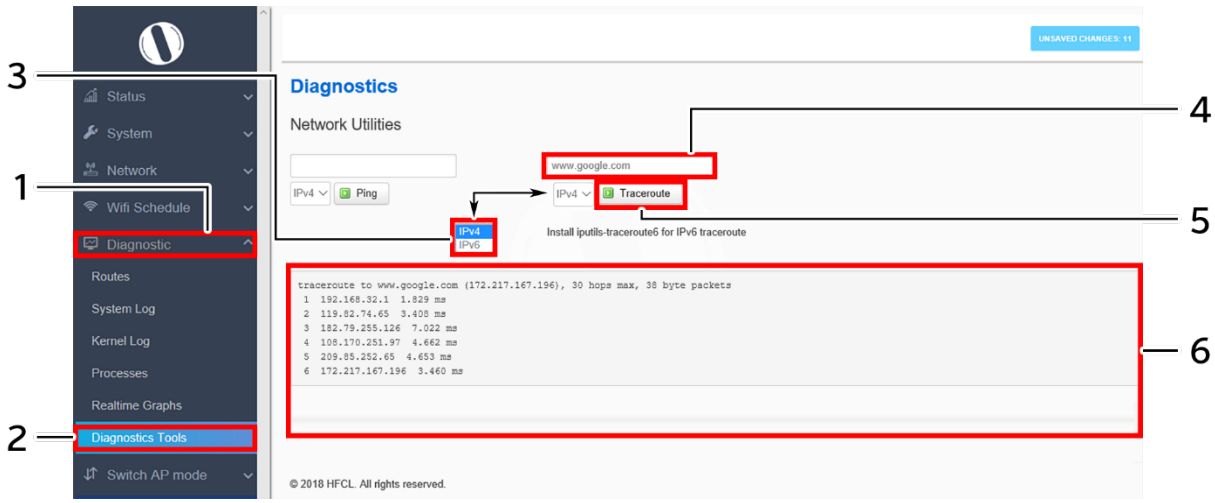

Figure 56: Basic overview of the diagnostics tool screen to check the route of established connection

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

Table 50: 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 or the domain name of the destination 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 or domain name
6.	Feedback window	Check the response on the feedback window to know the connection route.

18.7 Connected Clients

The list of connected clients along with the relevant information in respective information columns is populated in this screen. A basic overview of the screen to show connected clients is given below:

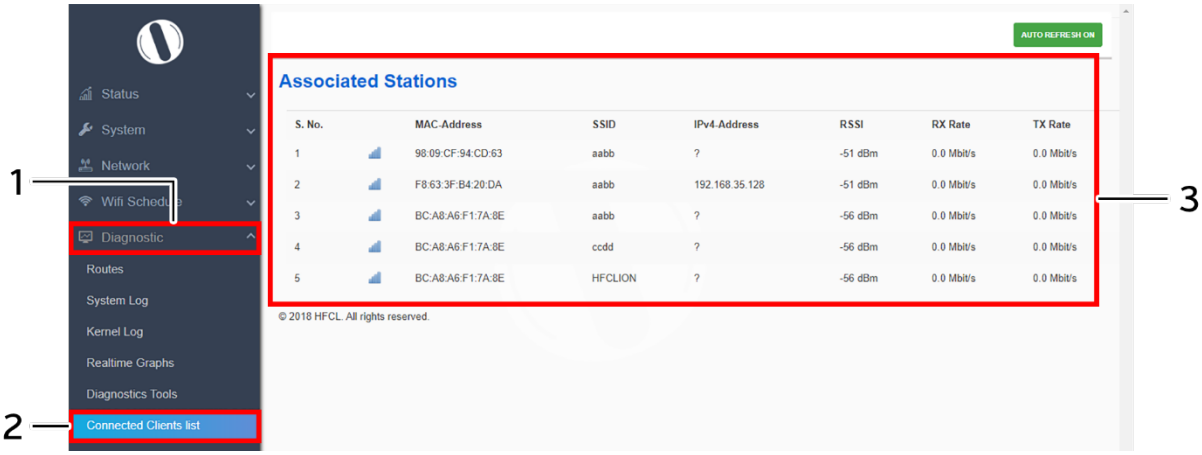

Figure 57: Basic overview of the screen to show connected clients

Follow the steps given below to view connected clients:

Table 51: List of actions to view connected clients

Callout	Name	Description
1.	Diagnostics	Click on “Diagnostics” dropdown
2.	Connected Clients	Click on “Connected Clients” option
3.	Client List	Displays all connected clients a listed form. Refer the above image for more information on relevant information with respect to connected clients

19 Switch AP Mode

A basic overview of the screen to switch mode from thick AP to thin AP is given below:

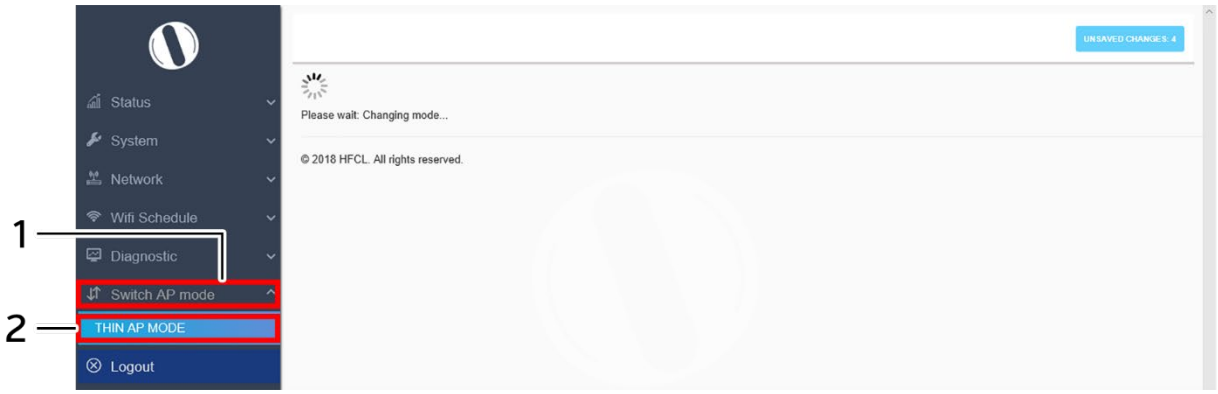

Figure 58: Basic overview of the screen to switch mode from thick AP to thin AP

Follow the steps given below to switch mode from thick AP to thin AP:

Table 52: List of actions to switch mode from thick AP to thin AP

Callout	Name	Description
1.	Switch AP Mode	Click on “Switch AP Mode” dropdown
2.	Thin AP Mode	Click on “Thin AP Mode” option

The screen displays the message as “Please wait changing mode”

20 Logout

Click on the logout option to terminate the user session.

.