RUT901 Wireless

The information in this page is updated in accordance with firmware version **RUT9M_R_00.07.07.1**.

□

Contents

- 1 Summary
- 2 Wireless
  - 2.1 SSIDS
    - 2.1.1 Global Settings
      - 2.1.1.1 General Setup
      - 2.1.1.2 Advanced Settings
    - 2.1.2 Interface Configuration
      - 2.1.2.1 General Setup
      - 2.1.2.2 Additional Settings
      - 2.1.2.3 Wireless Security
      - 2.1.2.4 MAC Filter
      - 2.1.2.5 Advanced Settings
      - 2.1.2.6 Fast Transition
      - 2.1.2.7 Fast Roaming
  - 2.2 Configuration examples
    - 2.2.1 Client Mode
    - 2.2.2 Mesh Mode
      - 2.2.2.1 Mesh Gateway
      - 2.2.2.2 Mesh Node
    - 2.2.3 Multi AP
      - 2.2.3.1 Access Points
  - 2.3 WiFi QR codes
- 3 Relay Configuration

Summary

The **Wireless** section of the Network tab can be used to manage and configure WiFi Access Points and WiFi Stations (clients) . This chapter of the user manual provides an overview of the Wireless section for RUT901 devices. If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should **turn on "Advanced WebUI" mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.

Wireless

RUT901 devices support IEEE 802.11b/g/n and 802.11e_WMM wireless technologies.

SSIDS

The **SSIDs** section is used to configure your wireless access points (AP) and wireless clients (STA).

Above is the overview of the SSIDS Overview window. It displays active access pointsand stations. Here you can turn on or off your WiFi interfaces, remove them or start configuring by clicking on

Edit button on the right side of interface.You can also configure your WiFi devices by clicking **Edit** button in the right side of each table header. To configure your Wireless device as Client press **Scan** button to scan the surrounding area and attempt to connect to a new wireless access point.

Global Settings

The **Global Settings** section is used for configuring WiFi hardware parameters. You can find this section by clicking the 'Edit' button next to a wireless device (not an interface) in the Network → SSIDS page:

General Setup

The **General Setup** section is used to turn a wireless device on or off, select the operating frequency (WiFi mode and channel), transmit power and define a country code.

A wireless 2.4 GHz WiFi channel requires a signaling band roughly 22 MHz wide, radio frequencies of neighboring channels numbers significantly overlap each other. Choose a WiFi channel according to the busyness of other channels. You can download a free WiFi analyzer app on your phone, laptop or other WiFi device and check which channel is the least populated.

Many home networks utilize routers that by default run on channel 6 on the 2.4 GHz band. Neighboring WiFi home networks that run over the same channel generate radio interference that can cause significant network performance slowdowns for users. Reconfiguring a network to run on a different wireless channel helps minimize these slowdowns. Therefore, pick a channel with no other active Access Points and preferably one that has no active Access Point on two adjacent channels on each side as well. If you don't feel like doing this, set the 'Channel' field to *Auto* and the device will pick the least busy channel in your location automatically.

Field	Value	Description
Enable	off | on; default: **on**	Turns Wireless device on or off.

Operating Frequency (2.4 GHz)		
Mode	N | Legacy; default: **N**	Wireless N (802.11n) supports a maximum theoretical transfer rate of 300mbps with 2 antennas. It can reach up to 450 Mbps with 3 antennas. Though typical speeds are more accurately around 130 Mbps. The legacy standards include 802.11a, 802.11b, and 802.11g.
Channel	Auto | 1 (2412 MHz) | 2 (2417 MHz) | 3 (2422 MHz) | 4 (2427 MHz) | 5 (2432 MHz) | 6 (2437 MHz) | 7 (2442 MHz) | 8 (2447 MHz) | 9 (2452 MHz) | 10 (2457 MHz) | 11 (2462 MHz); default: **Auto**	A wireless 2.4 GHz WiFi channel requires a signaling band roughly 22 MHz wide, radio frequencies of neighboring channels numbers significantly overlap each other. Therefore, pick a channel with no other active Access Points and preferably one that has no active Access Point on two adjacent channels on each side as well.
Width	20 MHz | 40 MHz; default: **20 MHz**	A 40 MHz channel width bonds two 20 MHz channels together, forming a 40 MHz channel width; therefore, it allows for greater speed and faster transfer rates. But not if those channels are crowded with noise and interference. In crowded areas with a lot of frequency noise and interference, a single 20MHz channel will be more stable. 40MHz channel width allows for greater speed and faster transfer rates but it doesn't perform as well in crowded areas.
Transmit Power	[5%...100%]; default: **100 %**	The transmit power of an access point radio is proportional to its effective range – the higher the transmit power, the more distance that a signal can travel, and/or the more physical materials that it can effectively penetrate and still have data successfully resolved at the receiver.
Country code	country code; default: **US - United States**	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard.

Advanced Settings

The **Advanced Settings** section is used to configure how the wireless Access Point will work from a hardware perspective.

Field	Value	Description
Operating Frequency (2.4 GHz)		
Allow legacy 802.11b rates	off | on; default: **on**	Turn on to enable connections that uses legacy 802.11b standard.
Distance Optimization	integer [0..65535]; default: **none**	HT Distance to farthest network member in meters.
Fragmentation threshold	integer [256..2346]; default: **none**	The smallest packet size that can be fragmented and transmitted by multiple frames. In areas were interference is a problem, setting a lower fragment threshold might help reduce the probability of unsuccessful packet transfers, thus increasing speed

RTS/CTS threshold	integer [0..2347]; default: **none**	RTS/CTS (Request to Send/Clear to Send) are mechanisms, used to reduce frame collisions introduced by the hidden node problem. It can help resolve problems arising when several access points are in the same area, contending
Force 40MHz mode	off | on; default: **off**	Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!
Beacon interval	integer [15..65535]; default: **none**	Beacon signal interval in seconds.

Interface Configuration

The **Interface Configuration** section is used to configure the parameters of Wireless Access Pointsor Clients. You can find this section by clicking the 'Edit' button next to a wireless device (not an interface) in the Network → SSIDs page:

General Setup

The **General Setup** tab contains basic options for SSID and network interface.

}}

Field	Value	Description
Enable	off | on; default: **on**	Enables or disables WiFi interface.
Mode	Client | Access Point | Mesh | Multi AP; default: **Access Point**	Defines what role this interface will do, Access point to supply WiFi for other devices, Client to use other devices WiFi for WWAN and Mesh to act as mesh network gateway or a node in a mesh network.
Access Point mode		
SSID	Factory SSID is different for every device; default:	Extended Service Set Identifier is a name used to identify access point which is shown when client tries to connect to it.
Password	string; default: **none**	• Custom passphrase used for authentication (at least 8 characters long). • Another option is to use the 'Dice' icon, which generates random passwords.
Network	network interfaces; default: **lan**	Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
802.11r Fast Transition	off | on; default: **off**	Enables fast roaming among access points that belong to the same Mobility Domain
Client mode		
Auto-reconnect	on | off; default: **on**	Enables automatic reconnection to the configured access point on connection loss.
SSID	Factory SSID is different for every device; default:	Extended Service Set Identifier is a name used to identify access point to which client will connect.

BSSID	mac address; default: **none**	Basic service set identifier.
Password	string; default: **none**	• Custom passphrase used for authentication (at least 8 characters long). • Another option is to use the 'Dice' icon, which generates random passwords.
Network	network interfaces; default: **Auto**	Choose the network you want to attach to this wireless interface or fill out the Custom field to define a new network (you will be redirected to the newly created network configuration page).
Mesh mode		
Mesh ID	integer; default: **none**	Mesh network identifier.
Password	string; default: **none**	• Custom passphrase used for authentication (at least 8 characters long). • Another option is to use the 'Dice' icon, which generates random passwords.
Network	network interfaces; default: **Auto**	Choose the network you want to attach to this wireless interface or fill out the Custom field to define a new network (you will be redirected to the newly created network configuration page).
Multi AP		
Network	network interfaces; default: **Auto**	Choose the network you want to attach to this wireless interface or fill out the Custom field to define a new network (you will be redirected to the newly created network configuration page).
Scan time (sec)	number; default: **60**	Time between scans of available access points (minimum 30 sec.)
Upload AP list	- (interactive button)	Uploads a list of access point configurations.

Additional Settings

Field	Value	Description
Access point		
Hide SSID	on | off; default: **off**	Hide Service Set Identifier
Isolate Clients	off | on; default: **off**	Prevents client to client communication on the same subnet.
802.11v BSS Transition Management	on | off; default: **off**	A suggestion (or advice) given to a client, which the client can choose to follow or ignore
802.11k Radio Resource Measurement	on | off; default: **off**	Helps devices search quickly for nearby APs that are available as roaming targets by creating an optimized list of channels.
Disassociate On Low Acknowledgement	off | on; default: **on**	Allow AP mode to disconnect stations/clients based on low Acknowledgement condition.

Field	Value	Description
Client & Multi AP		
Enable fast roaming	off | on; default: **off**	Requests background scans for the purpose of roaming within an ESS.

Field	Value	Description
Mesh		
Forward mesh peer traffic	off | on; default: **off**	Enables mesh peer traffic forwarding.
RSSI threshold for joining	integer [0..1]; default: **0**	0 = not using RSSI threshold, 1 = do not change driver default.

Wireless Security

The **Wireless Security** tab is used to determine what kind of encryption your WLAN will use.

Field	Value	Description
Encryption	No encryption | WPA-PSK | WPA2-PSK | WPA-PSK/WPA2-PSK Mixed Mode | WPA3-SAE | WPA2-PSK/WPA3-SAE Mixed Mode | OWE | WPA3-EAP Mixed Mode | WPA3-EAP; default: **WPA2-PSK/WPA3-SAE Mixed Mode**	The type of encryption used on this Wireless Interface. Opportunistic Wireless Encryption (**OWE**) - no password is required and all wireless traffic is encrypted (safer than **No Encryption**).
WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode, WPA3-EAP		
Cipher	Auto | Force CCMP (AES) | Force TKIP | Force TKIP and CCMP (AES); default: **Auto**	An algorithm for performing encryption or decryption.
WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode, WPA3-SAE, WPA2-PSK/WPA3-SAE Mixed Mode		
Password	string; default: **none**	• Custom passphrase used for authentication (at least 8 characters long). • Another option is to use the 'Dice' icon, which generates random passwords.

WPA-EAP, WPA2-EAP, WPA2-EAP/WPA3-EAP Mixed Mode, WPA3-EAP		
Radius-Authentication-Server	string; default: **none**	Ip address of the authentification server.
Radius-Authentication-Port	string; default: **none**	Default port for the server is 1812.
Radius-Authentication-Secret	string; default: **none**	Server's shared secret.
Radius-Accounting-Server	string; default: **none**	Ip address of the accounting server.
Radius-Accounting-Port	string; default: **none**	Default port for the server is 1813.
Radius-Accounting-Secret	string; default: **none**	Server's shared secret.
NAS id	string; default: **none**	Network access server identifier.
Client mode: WPA-EAP, WPA2-EAP, WPA2-EAP/WPA3-EAP Mixed Mode, WPA3-EAP		
EAP-Method	TLS | TTLS | PEAP | FAST; default: **TLS**	Network access server identifier.
Use PKCS#12 format	off | on; default: **off**	Use PKCS#12 file format for client certificate.
PKCS#12 client certificate file	- (interactive button)	Use PKCS#12 file format for client certificate.
PKCS#12 passphrase	string; default: **none**	Passphrase used to decrypt PKCS #12 certificates..
Certificate files from device	off | on; default: **off**	Choose this option if you want to select certificate files from device.
CA-Certificate	.crt file; default: **none**	This file can have one or more trusted CA certificates. If CA-Certificate is not included, server certificate will not be verified. This is insecure and a trusted CA-Certificate should always be configured when using EAP-TLS/TTLS/PEAP/FAST.
Client-Certificate	.crt file; default: **none**	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity..
Private Key	.key file; default: **none**	TLS client key file.
Password of Private Key	string; default: **none**	Password of Private Key.
Authentication	EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | EAP-TLS | PAP | CHAP | MSCHAP | MSCHAPv2; default: **EAP-GTC**	Used as the username for authentication.
Inner certificate files from device	off | on; default: **off**	Choose this option if you want to select certificate files from device.

Inner CA-Certificate	.crt file; default: **none**	Inner CA-Certificate.
Inner Client-Certificate	.crt file; default: **none**	Inner Client-Certificate.
Inner Private Key	.key file; default: **none**	Inner Private Key.
Password of inner Private Key	string; default: **none**	Password of inner Private Key.
Identity	string; default: **none**	Used as the username for authentication.
Anonymous Identity	string; default: **none**	Shown as username outside the encrypted tunnel. Not used for authentication.
Password	string; default: **none**	Used for authentication.

MAC Filter

The **MAC Filter** tab is used for setting up rules that allow or exclude devices with specified MAC addresses from connecting to your WiFi network. This tab is only visible when Wireless interface Mode is set to **Access Point**.

Field	Value	Description
MAC-address filter	Disable | Allow listed only | Allow all except listed; default: **Disable**	Defines how the MAC Filter should function. - **Allow listed only** – only allows devices with specified MAC addresses to connect to your Wireless Access Point. - **Allow all except listed** - blocks devices with specified MAC addresses from connecting to your Wireless Access Point.
MAC-List	MAC; default: **none**	List of MAC addresses to be included or excluded from connecting to your Wireless Access Point.
Remove from whitelist	off | on; default: **off**	Enables MAC removal from whitelist when device reaches IP block counter.

Advanced Settings

Field	Value	Description
Access point		
Short Preamble	off | on; default: **on**	Uses Short Preamble, it uses shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster.
DTIM interval	seconds; default: **none**	Delivery Traffic Indication Message Interval.
Time interval for rekeying GTK	seconds; default: **none**	Period of time in between automatic changes of the group key, which all devices on the network share.
Disable Inactivity Polling	off | on; default: **off**	Inactivity polling can be disabled to disconnect stations based on inactivity timeout so that idle stations are more likely to be disconnected even if they are still in range of the AP.

Station inactivity limit	seconds; default: **none**	Station inactivity limit in seconds. If a station/client does not send anything in st time frame, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not acknowledged, the station will be disassociated and then deauthenticated.
Maximum allowed Listen Interval	positive integer; default: **none**	Association will be refused if a client/station attempts to associate with a listen interval greater than this value.
WDS	off | on; default: **off**	A Wireless Distribution System (WDS) is a system that enables the wireless interconnection of access points (APs) in a network
WMM Mode	off | on; default: **on**	Wi-Fi Multimedia (WMM), previously known as Wireless Multimedia Extensions (WME), is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets according to four categories.

Field	Value	Description
Client		
Short Preamble	off | on; default: **on**	Uses Short Preamble, it uses shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster.
DTIM interval	seconds; default: **none**	Delivery Traffic Indication Message Interval.
Time interval for rekeying GTK	seconds; default: **none**	Period of time in between automatic changes of the group key, which all devices on the network share.
Disable Inactivity Polling	off | on; default: **off**	Inactivity polling can be disabled to disconnect stations based on inactivity timeout so that idle stations are more likely to be disconnected even if they are still in range of the AP.
Station inactivity limit	seconds; default: **none**	Station inactivity limit in seconds. If a station/client does not send anything in st time frame, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not acknowledged, the station will be disassociated and then deauthenticated.
Maximum allowed Listen Interval	positive integer; default: **none**	Association will be refused if a client/station attempts to associate with a listen interval greater than this value.
WDS	off | on; default: **off**	A Wireless Distribution System (WDS) is a system that enables the wireless interconnection of access points (APs) in a network

Field	Value	Description
Mesh & Multi AP		
DTIM interval	seconds; default: **none**	Delivery Traffic Indication Message Interval.
Time interval for rekeying GTK	seconds; default: **none**	Period of time in between automatic changes of the group key, which all devices on the network share.

Disable Inactivity Polling	off | on; default: **off**	Inactivity polling can be disabled to disconnect stations based on inactivity timeout so that idle stations are more likely to be disconnected even if they are still in range of the AP.
Station inactivity limit	seconds; default: **none**	Station inactivity limit in seconds. If a station/client does not send anything in st time frame, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not acknowledged, the station will be disassociated and then deauthenticated.
Maximum allowed Listen Interval	positive integer; default: **none**	Association will be refused if a client/station attempts to associate with a listen interval greater than this value.

Fast Transition

The **Fast Transition** tab is only available when in **General setup** section **802.11r Fast Transition** option is enabled.

Field	Value	Description
NAS id	string; default: **empty**	Used for fast transition and Radius server.
Mobility Domain	HEX string; default: **empty**	4-character hexadecimal ID
Reassociation Deadline	integer [1000..65535]; default: **empty**	Time units (TUs / 1.024 ms)
FT protocol	FT over DS | FT over Air; default: **FT over DS**	Defines how nagotiation will happen using Fast Transition protocol.

Fast Roaming

The **Fast Roaming** tab is only available when in **General setup** section **Client** mode is selected and in **Advanced settings** tab **Enable fast roaming** option is enabled.

Field	Value	Description
Mode	Simple | Learn; default: **Simple**	Defines how the MAC Filter should function. - **Simple:** Periodic background scans based on signal strengt - **Learn:** Learns channels used by the network and tries to avoid scans on other channels
Short interval	integer [5..86400]; default: **30**	Defines the interval between background scans (in seconds) if the actual signal level of the currently connected access point is worse than signal threshold
Long interval	integer [5..86400]; default: **300**	Defines the interval between background scans (in seconds) if the actual signal level of the currently connected access point is better than signal threshold
Signal threshold	integer [-90..-30]; default: **-70**	Defines a threshold (in dBm) that determines if short interval or longer interval will be used

Configuration examples

Client Mode

RUT901 can also work as a WiFi client. Configuring client mode is nearly identical to Access Point, except for the fact that most of the options are dictated by the WiFi Access Point that the router is connecting to. Changing them can result in an interrupted connection to that router.

To begin configuring WiFi Client first click the 'Scan' button to scan the surrounding area and attempt to connect to a new wireless access point.

After which you will be redirected to the window shown below, where you will see list of available WiFi Access Points in the area. Choose one according to your liking and press the **Join Network** button next to it.

You again will be redirected to following window, where you will need to enter WPA passphrase.

Next window that opens will be **Device Configuration**. Values there, mostly, should be left unchanged to avoid connection problems, because they are dictated by Access Point. Other than that, only difference from Access Point settings are in *Interface Configuration → General Setup* section, where **Mode** is set to **Client**, and **Network** attached to this wireless interface is **wifi1** instead of LAN

Click **Save & Apply** and if you configured correctly, you will have Wireless Client working.

Mesh Mode

RUT901 can also be configured as a mesh gateway or as a node (router) connecting to a mesh gateway.

When RUT901 is configured as **mesh gateway** it provides internet access to other mesh nodes. When configured as **mesh node** it acts as a mesh router which forwards traffic to and from mesh gateway. Nodes also connect other wireless devices to the network such as laptops and cellphones.

For complete wireless mesh network example please visit Wireless Mesh configuration example.

Mesh Gateway

When configuring RUT901 as a **mesh gateway** internet connectivity is **required**.

To begin click the 'Add' button below of wireless interface in the Network → Wireless page:

In **General Setup** tab change **Mode** to **Mesh**, set **Mesh ID** (this number has to be the same in all

nodes that connect to this wireless mesh network) and select desired **Network** which will be attached to the interface. Click **Save & Apply**.

Next navigate to **Wireless Security** tab and select **WPA3-SAE** encryption to add authentication layer. The password must match in all devices within the mesh network.

Lastly, in **Advanced Settings** tab enable **Forward mesh peer traffic** and set **RSSI threshold for joining** to -80. Leave the rest as set by default.

Click **Save & Apply** and if you configured correctly, you will have wireless mesh gateway ready.

Mesh Node

Mesh node is configured the same way as mesh gateway. Node has to match gateway's wireless mesh interface configuration. Additionally, WAN interface has to be setup as DHCP client:

1. Access router’s WebUI. Navigate to Network → WAN.

2. Press edit button on the right of the WAN interface.

3. Change Protocol to DHCP and select necessary device . Click **Save & Apply** and If everything was setup correctly, mesh node should be ready use.

Multi AP

The **Multi AP** feature is used to configure access to multiple wireless access points from one page. To create Multi AP wireless interface click the 'Add' button below of wireless interface in the Network → Wireless page:

In General Setup tab change Mode to Multi AP, select desired Network which will be attached to the interface. You can also select scan time and upload file with Access Points list.

Access Points

You can either configure multiple **access points** from this page of the WebUI or you can upload a file with a list of access point configurations. The file should contains WiFi access point configuration options and values, which should be defined as **option: value** (for example, *ssid: home_wifi*). The SSID option is mandatory.

Field	Value	Description
SSID	string; default: **none**	SSID of an access point.
Key	string; default: **none**	Pre-shared key, a custom passphrase used for user authentication (at least 8 characters long).
Enable	off | on; default: **off**	Turns an access point configuration on or off.
Delete	- (interactive button)	Deletes the access point configuration next to the button.

Option names in the file should be provided in lower case letters. AP list file example:

```
ssid: RUT_1
enable: 1
key: 12345678
ssid: RUT_2
enable: 0
key: 87654321
```

Once uploaded, the contents of the file should become visible in the Access Points list.

WiFi QR codes

Each WiFi interface has a specially designed QR code that contains information about the SSID and password of the WiFi network. After pressing the button , a QR code appears with the network's SSID and password, which you can download locally by pressing the 'Download' button. If you only want a QR code without additional information, uncheck the 'Include credentials' box.

Relay Configuration

The **Relay Configuration** section is used to relay and dynamically redirect incoming connections to a target host. Its main purpose is extending the wireless network. For example, when the device is in Wireless Station (client) mode, it can be used to bridge WAN and LAN interfaces to create a larger wireless network.
You can find a detailed usage example **here**.

Field	Value	Description
Enabled	off | on; default: **off**	Turns the relay configuration on or off.
Interface	network interface; default: **none**	Network interface associated with the wireless interface.
Wireless interface	network interface; default: **none**	Wireless interface associated with the relay configuration.