

Rosewill[®]



Trident - T600N

Wireless Dual Band Gigabit Router

User Manual

CONTENTS

INTRODUCTION	5	Wizard	27
PRODUCT OVERVIEW	6	Internet	31
Package Content	6	Status	32
LED Indicator	7	Dynamic IP	33
Back Panel Indicator	8	Static IP	34
Quick Setup Guide	9	PPPoE	35
Connecting Guide.....	9	PPTP	36
Wizard Setup Guide – Modem to LAN Setup	11	L2TP	38
Wizard Setup Guide – Wireless Setup	13	Wireless 2.4G	40
Wizard Setup Guide – Setup Successfully.....	14	Basic	41
Configuration Guide	15	Advanced	44
Web Management Guide	15	Security	46
System	16	Filter	50
Status	17	WPS	51
LAN	20	Client List	52
DHCP	23	Policy	53
Schedule	25	Wireless 5G	54
Log	26	Basic	55

CONTENTS

Advanced	58	Port Triggering	80
Security	60	ALG	81
Filter	64	UPnP	82
WPS	65	QoS	83
Client List	66	Routing	86
Policy	67	Tools	87
Firewall	68	Admin	88
Enable	69	Time	89
Advanced	69	DDNS	90
DMZ	70	Diagnosis	91
DoS	71	Firmware	92
MAC Filter	72	Backup / Factory Default	93
IP Filter	73	Reset	94
URL Filter	75	Physical Specification	95
Advanced	76	Troubleshooting	97
NAT	77		
Port Mapping	78		
Port Forwarding	79		

Safety Warning

- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do not allow anything to rest on the power adaptor or cord and do not place the product where anyone can walk on the power adaptor or cord.
- Do not use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do not attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do not use this product near water, eg, in wet basement, or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



INTRODUCTION

Thank you for purchasing this Rosewill Networking product. At Rosewill we believe that excellence is a standard. Our customers deserve nothing less than the best. By purchasing a Rosewill product you are choosing exceptional value, unrivaled customer service and top quality hardware. If you have any questions please feel free to contact us. We'd love to hear from you and thank you for your support!

Support: techsupport@rosewill.com

Call Center: (800) 575-9885

FAX: (626) 271-9504

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. *Rosewill* is a registered trademark of Rosewill Inc. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Rosewill Inc. Copyright © 2010 Rosewill Inc. All rights reserved. <http://www.rosewill.com>

PRODUCT OVERVIEW

Package Content:

- T600N Wireless Dual Band Gigabit Router
- Power Adapter for T600N
- Optimal Designed 5dBi 2.4GHz High Gain Antenna
- Quick Installation Guide
- Resource CD: User Manual, Quick Installation Guide
- RJ45 Cables

Note:

- Please make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.
- Using a power supply with a different voltage rating than the one included with the T600N may cause damage and void the warranty for this product.



PRODUCT OVERVIEW

LED Indicator



(From Left to Right)

- **WPS Button:** Push and hold for 3 seconds to enable WPS push button configuration.
- **WPS:** Wi-Fi Protected Setup activity. When the WPS mode is activated the WPS LED blinks as it awaits a connection.
- **Power:** Indicates when the Router is powered on. The LED will remain on.
- **2.4 GHz:** Blinks rapidly when the wireless data traffic is transmitted or received over the 2.4GHz wireless network.
- **5GHz:** Blinks rapidly when wireless data traffic is transmitted or received over the 5GHz wireless network.
- **Modem:** Indicates when modem is connected to the modem port on the back of the Router. The LED blinks rapidly when data is transmitted or received.
- **LAN:** Indicates when a networking device is connected to a wired port on the back of the Router. The LED blinks rapidly when wired data traffic is transmitted or received.

PRODUCT OVERVIEW

Back Panel Indicator



(From Left to Right)

- **DC-IN:** Power Adapter port. Output: 12V 1.25A, Input: 100-240v
- **LAN:** RJ-45 ports for connecting to wired computers or other network devices. (LAN 4~1 from left to right)
- **Modem:** RJ-45 port for connecting to your Broadband Modem
- **RESET:** Push once to reboot the Router. Hold down for 5-10 seconds to reset the Router back to factory settings.

QUICK SETUP GUIDE

Connecting Guide



1. Disconnect and Unplug your Existing Router

- Disconnect the RJ45 Cable in your existing router from your computer, broadband modem, and the power adapter from the power outlet.



2. Power Off your Modem and Remove the Backup Battery if any

- Remove the power adapter to power off your modem. Remove the modem's backup battery if your modem has one.



3. Connecting the T600N Wireless Router to your modem

- Plugs one end of your Ethernet Cable to the modem and the other end to your T600N's "modem" port.
- Since T600N supports Gigabit Network so it is recommended to use a **Cat 5 RJ45 Cable** to fully utilize your T600N.

QUICK SETUP GUIDE

Connecting Guide







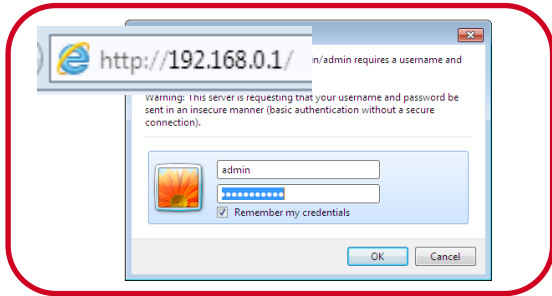
4. Power on the Modem

- Insert the backup battery back to your modem, and plug back your modem’s power adapter.
- Please wait 1~2 minutes the modem’s initialization to complete.



5. Power on your T600N Wireless Router and connect to your Computer

- Connects one end of the Ethernet Cable to your T600N’s LAN port    
- Connects the other end of the Ethernet Cable to your Computer or Note book.
- Plug in the power adapter of your T600N and power on your computer if it haven’t turn on.



6. Open your Web Browser and type in “192.168.0.1” in the address bar

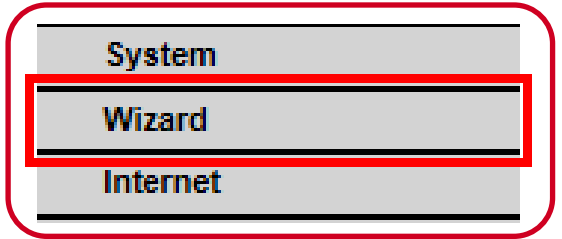
- When prompted, Enter the User Name and Password

User Name: admin
Password: admin

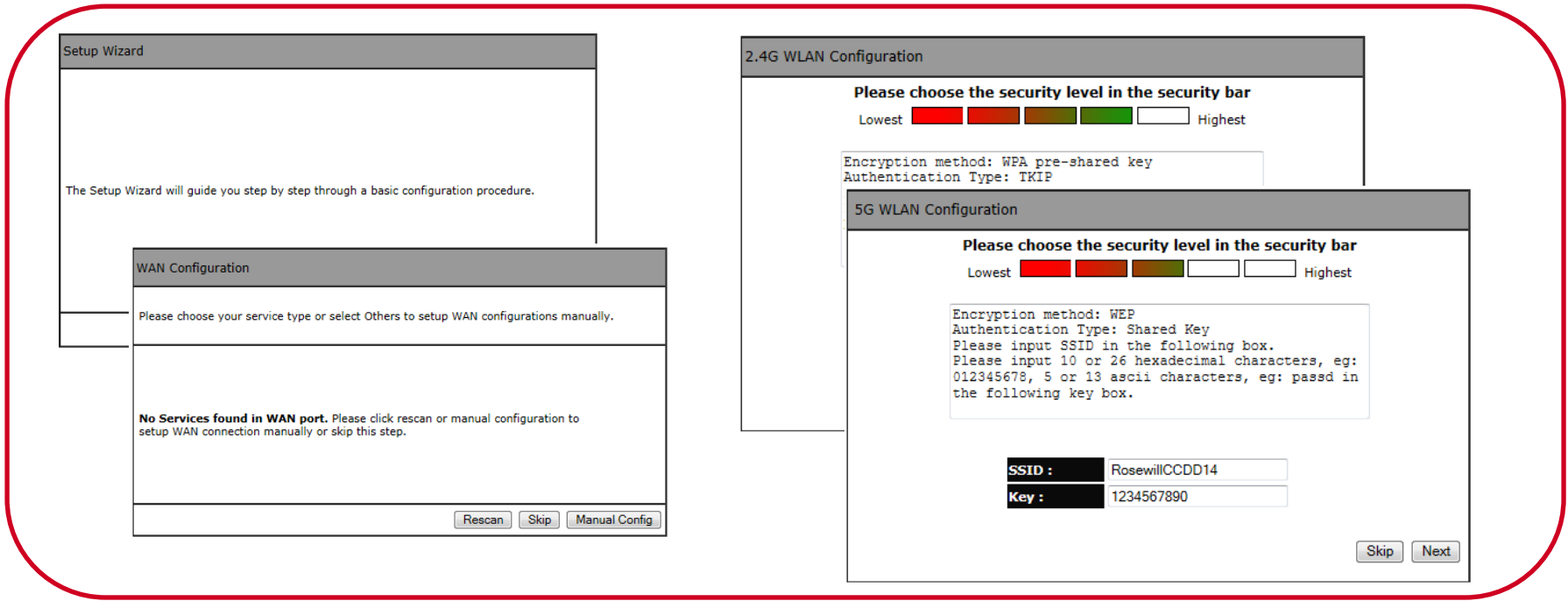
QUICK SETUP GUIDE

Wizard Setup Guide – Modem to LAN Setup

7. Setup Wizard

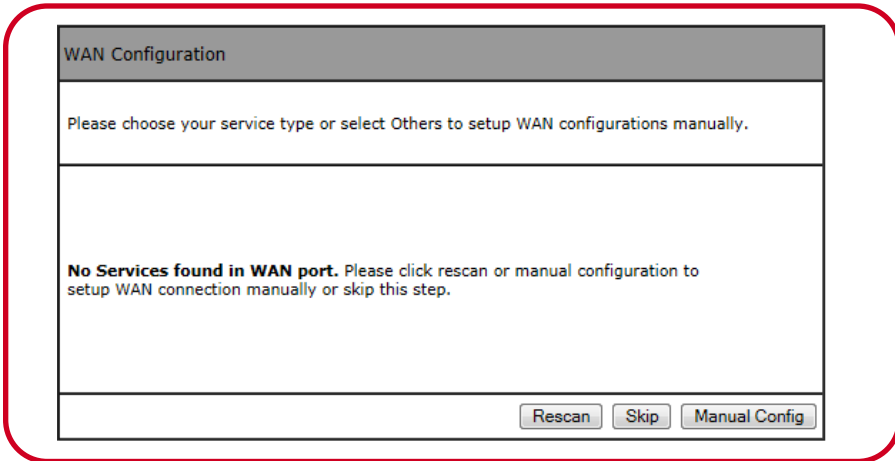
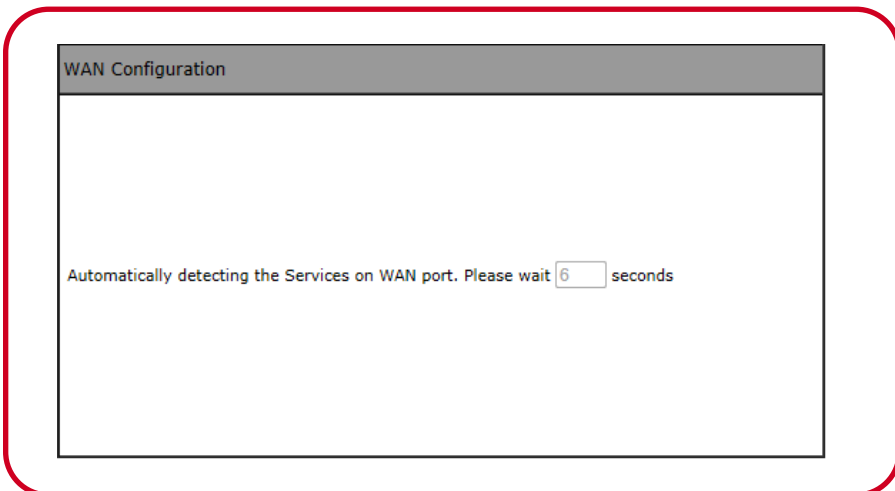


- Click on **Wizard** on the menu on the left side of the screen.
- Select **“Next”** twice to continue, T600N will Auto-Detect your Network and guide you through a step by step in both WAN to LAN and Wireless setting. Please see following page for Wizard details. (If your connection was not detected here, you will need to manually complete the setup.)



QUICK SETUP GUIDE

Wizard Setup Guide – Modem to LAN Setup

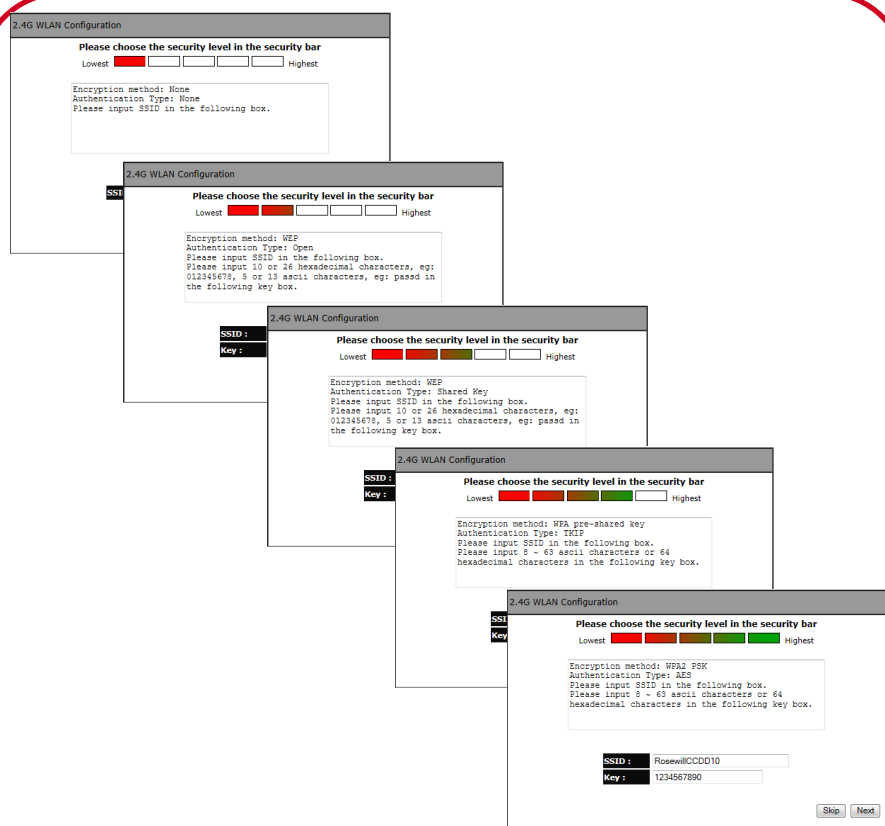


8. Setup Wizard

1. After click twice on “**Next**” confirming to start on the Wizard setup process, T600N will automatically detect your Connection from the ISP. You will need to provide T600N the following information once the connecting method was detected.
2. T600N is able to detect Static IP, Dynamic IP, PPP over Ethernet, PPTP, and L2TP connection methods.
 - **PPPoE:** PPPoE requires you having the **User Name** and **Password** provided by your ISP. Normally happens when using DSL connection.
 - **Dynamic IP (DHCP):** DHCP does not require entering anything. Usually happens when getting connection from an existing internet Connection.
 - **Static IP (Fixed):** Fixed requires you entering a set IP address, Subnet Mask, Gateway IP Address, Primary DNS, and/or Secondary DNS. These information will provided by your ISP and normally happens when using Cable connection.
 - **Manually Configuration:** If no WAN Connection was detected, you will need to manually enter the necessary information to connect to your ISP. You may want to check the cable connection and **Rescan**.

QUICK SETUP GUIDE

Wizard Setup Guide – Wireless Setup



5 Security Levels for Wireless Encryption

9. Setup Wizard Guide

1. Once the setup for Modem to LAN complete, you will continue to set up the Wireless configuration.
2. The Wizard will start with **2.4G WLAN Configuration**, then **5G WLAN Configuration**:

- **2.4G WLAN Configuration:**

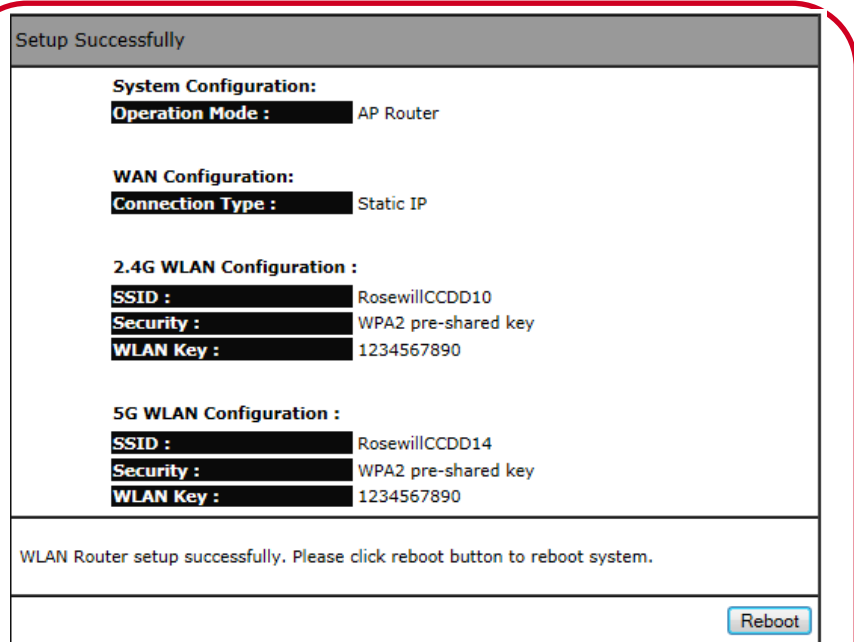
- There are 5 levels of Wireless Encryption you can set. From the lowest security level to the highest level's WPA2 PSK. Please follow the instruction in the window to set you SSID and password Key.

- **5G WLAN Configuration:**

- There are 5 levels of Wireless Encryption you can set. From the lowest security level to the highest level's WPA2 PSK. Please follow the instruction in the window to set you SSID and password Key.

QUICK SETUP GUIDE

Wizard Setup Guide – Setup Successfully



System is rebooting, please wait | 43 | seconds

10. Setup Wizard

1. Once the setup complete, you will see a summary window show up tells you to **Reboot** the Router's System to make all changes effective.
2. The Reboot process will take 45 seconds.
3. After the Reboot process , the Status window of the T600N will popup.

11. Admin Password Changes

1. When you finish the Wizard setup, please click on "**Tools**" on the left hand side's menu to change the default Password for login into your T600N from "**admin**" to your desired Password.
2. Please write down this password somewhere and keep it for your future use.
3. This is very important because the default password may be an easy access for people who wants to hack into your network.

Congratulations, T600N is now successfully configured, and your settings are now saved. You may now connect other devices directly to the 4 wired ports on the back panel or connect wirelessly to T600N.

If you have question, Please feel free to contact us:

Support: techsupport@rosewill.com

Call Center: (800) 575-9885

CONFIGURATION GUIDE

Web Management Guide

System
Wizard
Internet
Wireless 2.4G
Wireless 5G
Firewall
Advanced
Tools

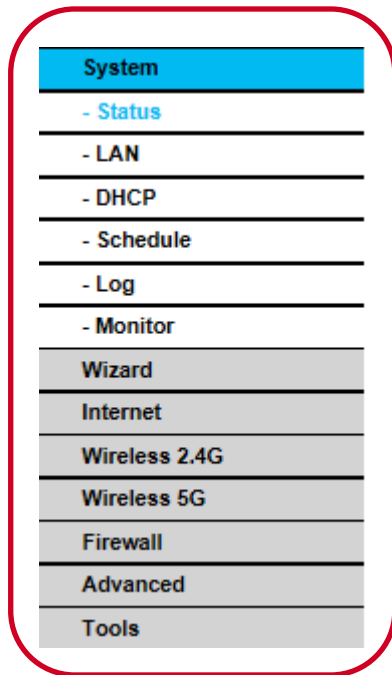
For Details on how to manage each function, please see each Correspondence Section.

Web Management Detail: There are 8 main functions on the left of the Web-based utility.

- **System:** System includes the Status details, LAN setting, DHCP setup, Schedule, Log, and Monitor on T600N
- **Wizard:** A step by step setup Wizard on the basic connection for T600N
- **Internet:** Internet allows you to manually configure the connection to the Modem (Connecting to the Internet). You can configure the connection between Dynamic IP, Static IP, PPPoE, PPTP, and L2TP depending on how your ISP provides the service to you.
- **Wireless 2.4G:** You can configure the 2.4GHz Wireless signals here. The adjustable Functions are Basic Setup, Advanced Setup, Security, Filter, WPS, Client List, and Policy.
- **Wireless 5G:** You can configure the 5GHz Wireless signals here. The adjustable Functions are Basic Setup, Advanced Setup, Security, Filter, WPS, Client List, and Policy.
- **Firewall:** Firewall allows you to protect your internet from outside attack with the function of DMZ, Denial of Service (DoS), MAC Filter, IP Filter, and URL Filter.
- **Advanced:** The Advance Feature allows you to configure T600N based on your usage. You can configure NAT/Hardware Accelerator, Port Mapping, Port Forwarding, Port Triggering, ALG, UPnP, QoS, and Routing.
- **Tools:** T600N's administration related function setup

CONFIGURATION GUIDE

System



System
- Status
- LAN
- DHCP
- Schedule
- Log
- Monitor
Wizard
Internet
Wireless 2.4G
Wireless 5G
Firewall
Advanced
Tools

System: You can review the device information and manage the basic WIRED connection here:

- **Status:** Display the summary of the current system status.
- **LAN:** Configure the wired network
- **DHCP:** Configure dynamically allocated IP addresses
- **Schedule:** Setting the Activation time for certain functions, ex: Firewall.
- **Log:** Viewing system operations records and network activity events
- **Monitor:** Viewing the current network traffic bandwidth usage

CONFIGURATION GUIDE

System – Status – 1

System	
Model	T600N: Wireless Gigabit Dual Band Router
Mode	AP Router
Uptime	19 min 22 sec
Current Date/Time	2011/01/01 00:19:25
Hardware version	1.0.0
Serial Number	000000001
Application version	1.0.1
WAN Settings	
Attain IP Protocol	Dynamic IP Address
IP address	---
Subnet Mask	---
Default Gateway	---
MAC address	00:AA:BB:CC:DD:11
Primary DNS	---
Secondary DNS	---

Status: In the Status section, you can review the System, WAN Settings, LAN Settings, and WLAN Settings information here:

- **System:**
 - **Model:** The model name of this product.
 - **Mode:** The router’s operating mode: Default as AP Router.
 - **Uptime:** The amount of time that this device has been active.
 - **Current Date/Time:** The current system date and time.
 - **Hardware Version:** The hardware version number of T600N.
 - **Serial Number:** The serial number of the T600N. The serial number is required for customer service or support.
 - **Application Version:** The firmware version number of the T600N.

- **WAN Settings:**
 - **Attain IP Protocol:** Displays the IP protocol in use for the T600N. It can be a dynamic or static IP address.
 - **IP Address:** The router’s IP address as designated by an ISP provider.
 - **Subnet Mask:** The router’s WAN subnet mask as designated by an ISP provider.
 - **Default Gateway:** The router’s gateway address as designated by an ISP provider.
 - **MAC Address:** The router’s WAN MAC address. The router’s MAC address is located on the label on the back side of the router.
 - **Primary DNS:** The primary DNS of an ISP provider.
 - **Secondary DNS:** The secondary DNS of an ISP provider

CONFIGURATION GUIDE

System – Status – 2

LAN Settings

IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC address	00:00:00:F2:2A:BA

WLAN Settings

Wireless 2.4G Setting

Channel 11

SSID_1

ESSID	RosewillCCDD10
Security	Disable
BSSID	00:AA:BB:CC:DD:10
Associated Clients	0

Status: In the Status section, you can review the System, WAN Settings, LAN Settings, and WLAN Settings information here:

- **LAN Settings:**
 - **IP Address:** T600N’s local IP address. The default LAN IP address is **192.168.0.1**.
 - **Subnet Mask:** T600N’s local subnet mask.
 - **DHCP Server:** The DHCP setting status (Default: **Enabled**).
 - **MAC Address:** T600N’s LAN MAC address.
- **WLAN Settings:**
 - **Wireless 2.4G Setting:**
 - **Channel:** The communications channel used by all stations, or computing devices, on the network.
 - **ESSID:** The ID value of a set of one or more interconnected basic service sets (BSSs).
 - **Security:** The security setting status (Default: **Disabled**).
 - **BSSID:** The unique ID of the BSS using the above channel value in this router. The ID is the MAC address of the BSSs access point.
 - **Associated Clients** The number of clients associated with this SSID.
 - **Wireless 5G Setting:**

CONFIGURATION GUIDE

System – Status – 3

WLAN Settings

Wireless 5G Setting

Channel 36

SSID_1

ESSID RosewillCCDD14

Security Disable

BSSID 00:AA:BB:CC:DD:14

Associated Clients 0

Status: In the Status section, you can review the System, WAN Settings, LAN Settings, and WLAN Settings information here:

- **Wireless 5G Setting:**

- **Channel:** The communications channel used by all stations, or computing devices, on the network.
- **ESSID:** The ID value of a set of one or more interconnected basic service sets (BSSs).
- **Security:** The security setting status (Default: **Disabled**).
- **BSSID:** The unique ID of the BSS using the above channel value in this router. The ID is the MAC address of the BSSs access point.
- **Associated Clients** The number of clients associated with this SSID.

CONFIGURATION GUIDE

System – LAN – 1

You can enable the broadband router's DHCP server to dynamically allocate IP address to your LAN clients. The broadband router must have any IP Address for the Local Area Network.

LAN IP

IP address :
IP Subnet Mask :
802.1d Spanning Tree :

DHCP Server

DHCP Server :
Lease time :
Start IP :
End IP :
Domain name :

DNS Servers

DNS Servers Assigned by DHCP Server
First DNS Server :
Second DNS Server :

LAN: Configure the wired network settings in the LAN section. The router's IP is defined in the **IP Address** field. The default setting of the DHCP server is set to enabled so that network clients can be automatically assigned a virtual IP addresses.

Advanced users may configure DNS server settings to meet specific requirements. Changing the settings in this section are not necessary for most situations.

Note: Please keep the default values if you are not certain with the effects of changing the values.

CONFIGURATION GUIDE

System – LAN – 2

LAN IP

IP address : 192.168.0.1
 IP Subnet Mask : 255.255.255.0
 802.1d Spanning Tree : Disabled

LAN IP:

- **IP address:** Configure the router's LAN IP address
- **IP Subnet Mask:** Configure the router's LAN Subnet Mask
- **802.11d Spanning Tree:** The 802.1d Spanning Tree settings is disabled by default. When enabled, the spanning tree protocol is applied to prevent network loops (transmissions won't pass the same node twice to reach the destination).

DHCP Server

DHCP Server : Enabled
 Lease time : Forever
 Start IP : 192.168.0.100
 End IP : 192.168.0.200
 Domain name : T600N

DHCP Server: The DHCP server assigns IP addresses to the devices on the LAN.

- **DHCP Server:** Enable or disable the DHCP server (Default: Enabled).
- **Lease Time:** Configure the amount of time each allocated IP address can be used by a client.
- **Start IP:** The first IP address in the range of addresses assigned by the router.
- **End IP:** The last IP address in the range of addresses assigned by the router.
- **Domain Name:** The domain name of the router.

CONFIGURATION GUIDE

System – LAN – 3

DNS Servers

DNS Servers Assigned by DHCP Server

First DNS Server :

Second DNS Server :

DNS Server: The domain name system (DNS) server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are four options to choose from:

- 1. From ISP:** Select From ISP to retrieve the DNS address value from the ISP
 - 2. User-Defined:** Select User-Defined to assign a custom DNS server address
 - 3. DNS Relay:** Select DNS Relay to forward all queries to a relay, which in turn sends them to an ISP's DNS server
 - 4. None:** Select None to assign no server
- **First DNS Server:** Configure the first, or primary, DNS server. (Default as **DNS Relay**)
 - **Second DNS Server:** Configure the second, or secondary, DNS server. (Default as **None**)
-
- Click **Apply** to Save settings

CONFIGURATION GUIDE

System – DHCP – 1

DHCP Client Table

The DHCP shows the client table of IP addresses which assigned to the clients by the broadband router's DHCP server. You can also manually assign the IP address based on MAC address.

IP address	MAC address	Expiration Time
192.168.0.100	00:0D:60:2D:70:DC	Forever

Refresh

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select

Delete Selected Delete All Reset Apply Cancel

DHCP: The DHCP here shows the client table of IP addresses which assigned to the clients. You can manually assigned the clients to certain IP addresses based on their MAC addresses.

Note: Please keep the default values if you are not certain with the effects of changing the values.

DHCP Client Table

The DHCP shows the client table of IP addresses which assigned to the clients by the broadband router's DHCP server. You can also manually assign the IP address based on MAC address.

IP address	MAC address	Expiration Time
192.168.0.100	00:0D:60:2D:70:DC	Forever

Refresh

DHCP Client Table: Displays the connected DHCP clients whose IP addresses are assigned by the DHCP server on the LAN.

Click **Refresh** to update the table.

CONFIGURATION GUIDE

System – DHCP – 2

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Enable Static DHCP IP: Click **Enable Static DHCP IP** to add more static DHCP IP addresses. Click **Add** to add after entered the IP address and MAC address. Click **Reset** to return the table to its previous state.

- **IP address:** Please enter the IP address range within 192.168.x.1 ~ 192.168.x.254 (x should be the same as the LAN IP's IP address, for example it should 0 here)
- **MAC address:** MAC address should be your desired client's MAC address. The format should be without ":". You can reference this on the DHCP Client Table above.

Current Static DHCP Table :

NO.	IP address	MAC address	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

Current Static DHCP Table: Active static DHCP addresses are listed along with the associated MAC addresses.

- **Delete Selected:** Click to remove a selected address.
- **Delete All:** Click to remove all addresses from the table.
- **Reset:** Click to return the table to its previous state.
- **Apply:** Click to save the settings.

CONFIGURATION GUIDE

System – Schedule

You can use the Schedule function to Start/Stop the service. The Schedule will start to run, when it get GMT Time from Time Server. In order for the Schedule to run correctly, please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
-----	-------------	---------	----------	--------

Schedule: You can use this function to start or stop Firewall service. Click **Enabled Schedule Table (up to 8)** to enable schedule function. Click **Add** to add more schedule task. Click **Edit** to modify the tasks.

Note: Please keep the default values if you are not certain with the effects of changing the values.

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

Schedule Description :

Service : Firewall

Days : Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time of day : All Day (use 24-hour clock)
From : To :

Add Schedule Task: To manage each Schedule Task on description, Service type, Days, and time.

- **Schedule Description:** You can name the task here.
- **Service:** You can click to select the service. Currently you can only select **Firewall**
- **Days:** You can select either everyday or any day of the week.
- **Time of Day:** You can select All Day or entering any time.
- **Apply:** Click to save the settings.

CONFIGURATION GUIDE

System – Log

This page is for viewing the system operation information.

```

day 1 00:55:06 [SYSTEM]: WLAN, start LLTD
day 1 00:55:05 [SYSTEM]: WLAN, LLTD Stopping
day 1 00:55:04 [SYSTEM]: UPnP, Stopping
day 1 00:55:03 [SYSTEM]: NET, start Firewall
day 1 00:55:03 [SYSTEM]: NET, start NAT
day 1 00:55:03 [SYSTEM]: NET, stop Firewall
day 1 00:55:03 [SYSTEM]: NET, stop NAT
day 1 00:55:03 [SYSTEM]: SCHEDULE, Schedule Stopping
day 1 00:55:03 [SYSTEM]: QoS, Stopping
    
```

Save Clear Refresh

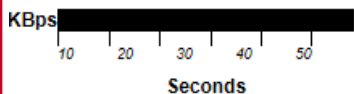
Log: The logging service records and displays important system information and activity on the network. The events will be store in the memory buffer which older data will overwrite when the buffer is full.

- **Save:** Click to store data to a log file.
- **Clear:** Click to empty the log file.
- **Refresh:** Click to empty the log file and begin updating it with new data.

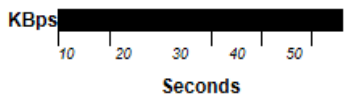
System – Monitor

You can monitor the bandwidth with below tools. The page will refresh in every five seconds.

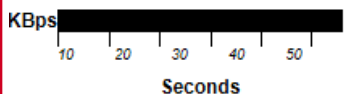
Bandwidth Monitor (2.4G WLAN)



Bandwidth Monitor (5G WLAN)



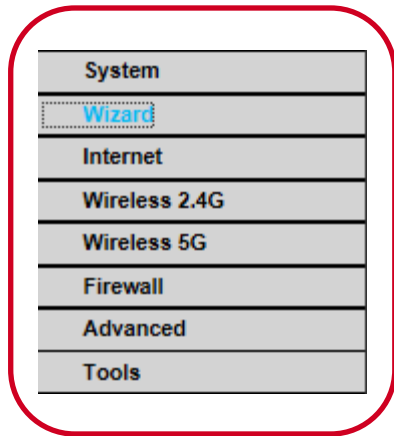
Bandwidth Monitor (WAN)



Monitor: View the display bandwidth usage for LAN and WLAN traffic.

CONFIGURATION GUIDE

Wizard

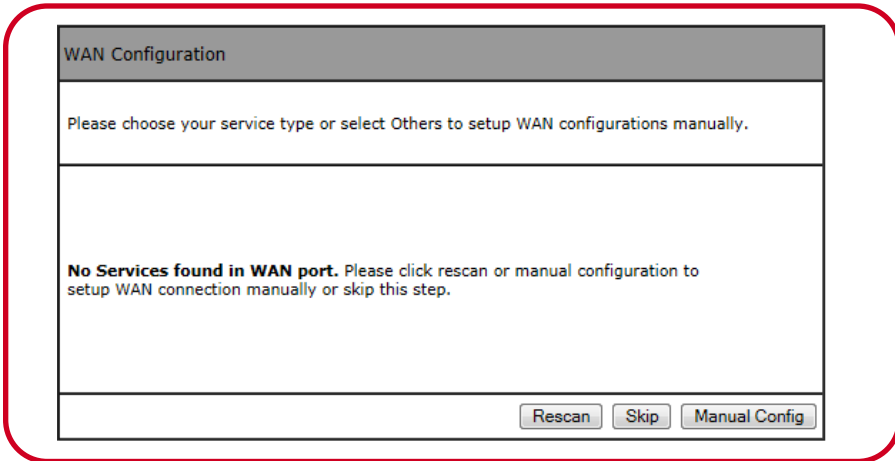
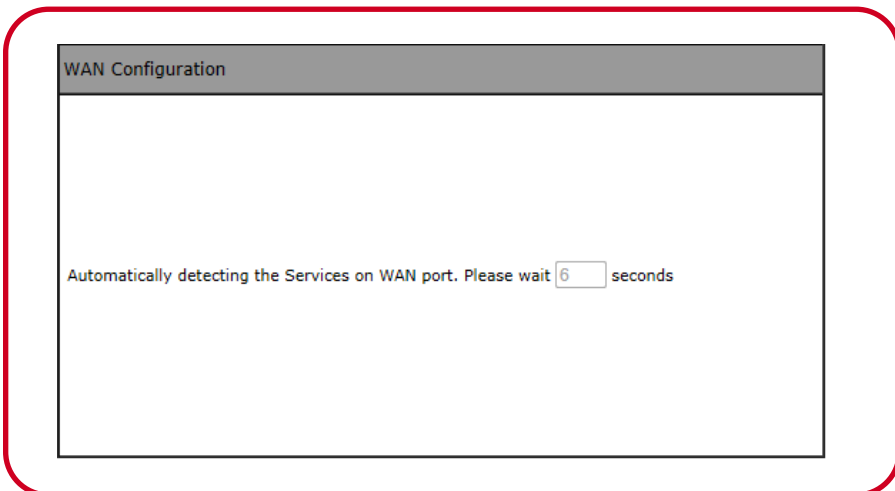


Wizard: The Setup Wizard helps T600N in automatically detecting the connection to your ISP.

Please follow this steps in the Wizard to complete your Setting.

CONFIGURATION GUIDE

Wizard – Modem to LAN Setup



Setup Wizard

1. After click twice on “**Next**” confirming to start on the Wizard setup process, T600N will automatically detect your Connection from the ISP. You will need to provide T600N the following information once the connecting method was detected.
2. T600N is able to detect Static IP, Dynamic IP, PPP over Ethernet, PPTP, and L2TP connection methods.
 - **PPPoE:** PPPoE requires you having the **User Name** and **Password** provided by your ISP. Normally happens when using DSL connection.
 - **Dynamic IP (DHCP):** DHCP does not require entering anything. Usually happens when getting connection from an existing internet Connection.
 - **Static IP (Fixed):** Fixed requires you entering a set IP address, Subnet Mask, Gateway IP Address, Primary DNS, and/or Secondary DNS. These information will provided by your ISP and normally happens when using Cable connection.
 - **Manually Configuration:** If no WAN Connection was detected, you will need to manually enter the necessary information to connect to your ISP. You may want to check the cable connection and **Rescan**.

CONFIGURATION GUIDE

Wizard – Wireless Setup

The image shows five overlapping screenshots of the 2.4G WLAN Configuration wizard, illustrating the selection of security levels. Each window displays a security level bar with five segments, and the selected level is indicated by a colored segment. The encryption method and authentication type change as the security level increases. The final window shows the SSID 'Rosew#CCDD10' and Key '1234567890'.

5 Security Levels for Wireless Encryption

Setup Wizard Guide

1. Once the setup for Modem to LAN complete, you will continue to set up the Wireless configuration.
2. The Wizard will start with **2.4G WLAN Configuration**, then **5G WLAN Configuration**:

- **2.4G WLAN Configuration:**

- There are 5 levels of Wireless Encryption you can set. From the lowest security level to the highest level's WPA2 PSK. Please follow the instruction in the window to set you SSID and password Key.

- **5G WLAN Configuration:**

- There are 5 levels of Wireless Encryption you can set. From the lowest security level to the highest level's WPA2 PSK. Please follow the instruction in the window to set you SSID and password Key.

CONFIGURATION GUIDE

Wizard – Setup Successfully

Setup Successfully

System Configuration:
Operation Mode : AP Router

WAN Configuration:
Connection Type : Static IP

2.4G WLAN Configuration :
SSID : RosewillCCDD10
Security : WPA2 pre-shared key
WLAN Key : 1234567890

5G WLAN Configuration :
SSID : RosewillCCDD14
Security : WPA2 pre-shared key
WLAN Key : 1234567890

WLAN Router setup successfully. Please click reboot button to reboot system.

System is rebooting, please wait 43 seconds

Setup Wizard

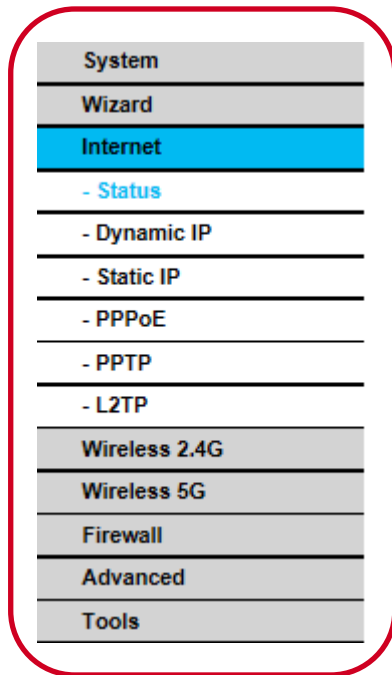
1. Once the setup complete, you will see a summary window show up tells you to **Reboot** the Router's System to make all changes effective.
2. The Reboot process will take 45 seconds.
3. After the Reboot process , the Status window of the T600N will popup.

Admin Password Changes

1. When you finish the Wizard setup, please click on "**Tools**" on the left hand side's menu to change the default Password for login into your T600N from "**admin**" to your desired Password.
2. Please write down this password somewhere and keep it for your future use.
3. This is very important because the default password may be an easy access for people who wants to hack into your network.

CONFIGURATION GUIDE

Internet



System
Wizard
Internet
- Status
- Dynamic IP
- Static IP
- PPPoE
- PPTP
- L2TP
Wireless 2.4G
Wireless 5G
Firewall
Advanced
Tools

Internet: You can review the device information and manage the basic WIRED connection here:

- **Status:** Display the summary of the Internet status and type of connection.
- **Dynamic IP:** Setup a dynamic IP connection to an Internet service provider (ISP). (Used mostly for Dorm or Office connection)
- **Static IP:** Setup a static IP connection to an ISP. (Used mostly for Cable connection)
- **PPPoE:** Setup a PPPoE connection to an ISP. (Used mostly for DSL connection)
- **PPTP:** Setup a PPTP connection to an ISP. (Used mostly for VPN connection)
- **L2TP:** Setup an L2TP connection to an ISP. (Used mostly for VPN connection)

CONFIGURATION GUIDE

Internet – Status

View the current internet connection status and related information.

WAN Settings

Attain IP Protocol	Dynamic IP Address
IP address	---
Subnet Mask	---
Default Gateway	---
MAC address	00:AA:BB:CC:DD:11
Primary DNS	---
Secondary DNS	---

Renew

Status: It shows a summary of the current Internet connection information In this Internet Status:

- **WAN Settings:**
 - **Attain IP Protocol:** Display the IP Protocol type used for the T600N (Dynamic IP Address or Static IP Address).
 - **IP Address:** The router’s WAN IP address.
 - **Subnet Mask:** The router’s WAN subnet mask.
 - **Default Gateway:** The ISP’s gateway IP address.
 - **MAC Address:** The router’s WAN MAC address. The router’s MAC address is located on the label on the back side of the router.
 - **Primary DNS:** The primary DNS address of an ISP provider.
 - **Secondary DNS:** The secondary DNS address of an ISP provider.

CONFIGURATION GUIDE

Internet – Dynamic IP

You can select the type of the account you have with your ISP provider.

Hostname :	<input type="text"/>
MAC address :	<input type="text" value="000000000000"/> <input type="button" value="Clone MAC"/>
DNS Servers	
DNS Servers Type	<input type="text" value="From ISP"/> ▼
First DNS Server	<input type="text" value="0.0.0.0"/>
Second DNS Server	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Dynamic IP: Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.

- **Host name:** Assign a name for the internet connection type. This field can be blank.
- **MAC address:** Enter the MAC address of the devices' network interface card (NIC) in the MAC address field and click **Clone MAC**.

Note: Some ISP providers require registering the MAC address of the network interface card (NIC) connected directly to the cable or DSL modem. Clone MAC masks the router's MAC address with the MAC address of the device's NIC.

DNS Server: The DNS server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are two options to choose from: From ISP or User-Defined. Select From ISP to retrieve the DNS address value from the ISP; select User-Defined to assign a custom DNS server address.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Internet – Static IP

You can select the type of the account you have with your ISP provider.

IP address:	<input type="text"/>
IP Subnet Mask :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS :	<input type="text"/>
Secondary DNS :	<input type="text"/>
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Static IP: Setting a static IP address allows an administrator to set a specific IP address for the router and guarantees that it can not be assigned a different address.

- **IP Address:** This section is to enter the IP address provided to the router by ISP.
- **IP Subnet Mask:** This section is to enter the IP Subnet Mask provided to the router by ISP.
- **Default Gateway:** This section is to enter the Default Gateway provided to the router by ISP.
- **Primary DNS:** This section is to enter the Primary DNS provided to the router by ISP.
- **Secondary DNS:** This section is to enter the Secondary DNS provided to the router by ISP, if any.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Internet – PPPoE

You can select the type of the account you have with your ISP provider.

Login :	<input type="text"/>
Password :	<input type="password"/>
Service Name	<input type="text"/>
MTU :	<input type="text" value="1492"/> (512<=MTU Value <=1492)
Authentication type :	<input type="text" value="Auto"/> ▼
Type :	<input type="text" value="Keep Connection"/> ▼
Idle Timeout :	<input type="text" value="10"/> (1-1000 Minutes)
DNS Servers	
DNS Servers Type	<input type="text" value="From ISP"/> ▼
First DNS Server	<input type="text" value="0.0.0.0"/>
Second DNS Server	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet.

- **Login:** Enter the username assigned by an ISP.
- **Password:** Enter the password assigned by an ISP.
- **Service Name:** Enter the service name of an ISP (optional).
- **MTU:** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an internet transmission (PPPoE default: 1492). The MTU size can be set between 512 and 1492.
- **Authentication Type:** Select the type of authentication provided by the ISP: Auto, PAP, or CHAP. If unsure of the best setting, select Auto.
- **Type:** Configure the connection type between the router and the ISP. Choose between Keep Connection, Automatic Connection or Manual Connection.
- **Idle Timeout:** Configure the maximum idle time (1 to 1,000 minutes) allowed for an inactive connection.

DNS Server: The DNS server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are two options to choose from: From ISP or User-Defined. Select From ISP to retrieve the DNS address value from the ISP; select User-Defined to assign a custom DNS server address.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Internet – PPTP – 1

You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :	Dynamic IP Address ▼
Hostname :	<input type="text"/>
MAC address :	000000000000 <input type="button" value="Clone MAC"/>

WAN Interface Settings :

WAN Interface Type :	Static IP Address ▼
My IP Address :	<input type="text"/>
My Subnet Mask :	<input type="text"/>
Gateway IP Address :	<input type="text"/>

PPTP: The point-to-point tunneling protocol (PPTP) is used in association with virtual private networks (VPNs). There are two parts to a PPTP connection: the WAN interface settings and the PPTP settings.

- **WAN Interface Settings – Dynamic IP Address:**

- **WAN Interface Type:** Select Dynamic IP Address to assign an IP address provided by an ISP.
- **Hostname:** Enter the service name of an ISP (optional).
- **MAC address:** Enter the MAC address of the device's network interface card (NIC) in the MAC address field and click Clone MAC.

- **WAN Interface Settings – Static IP Address:**

- **WAN Interface Type:** Select Static IP Address to assign a specific IP address for the router.
- **My IP Address:** Enter the custom IP address. Normally provided by the ISP.
- **My Subnet Mask:** Enter the custom Subnet Mask. Normally provided by the ISP.
- **Gateway IP Address:** Enter the custom gateway IP address. Normally provided by the ISP.

CONFIGURATION GUIDE

Internet – PPTP – 2

PPTP Settings :

Login :	<input type="text"/>
Password :	<input type="password"/>
Service IP address :	<input type="text"/>
Connection ID :	<input type="text" value="0"/> (Optional)
MTU :	<input type="text" value="1400"/> (512<=MTU Value <=1492)
Type :	<input type="text" value="Keep Connection"/> ▼
Idle Timeout :	<input type="text" value="10"/> (1-1000 Minutes)
DNS Servers	
DNS Servers Type	<input type="text" value="From ISP"/> ▼
First DNS Server	<input type="text" value="0.0.0.0"/>
Second DNS Server	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

PPTP Settings:

- **User Name:** Enter the username assigned by your ISP.
- **Password:** Enter the password assigned by your ISP.
- **Service IP Address:** Enter the PPTP server IP address provided by your ISP.
- **Connection ID:** Enter the connection ID provided by your ISP (optional).
- **MTU:** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size (Default: 1462) permitted for an internet transmission. The MTU size can be set between 512 and 1492.
- **Type:** Configure the connection type between the router and the ISP. Choose between Keep Connection, Automatic Connection or Manual Connection.
- **Idle Timeout:** Configure the maximum amount of time, in minutes, allowed for inactive Internet connection. The Internet connection will be dropped when the maximum idle time is reached. Valid values are between one and one thousand.

DNS Server: The DNS server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are two options to choose from: From ISP or User-Defined. Select From ISP to retrieve the DNS address value from the ISP; select User-Defined to assign a custom DNS server address.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Internet – L2TP – 1

You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :	Dynamic IP Address	<input type="button" value="Clone MAC"/>
Hostname :	<input type="text"/>	
MAC address :	000000000000	

WAN Interface Settings :

WAN Interface Type :	Static IP Address
My IP Address :	<input type="text"/>
My Subnet Mask :	<input type="text"/>
Gateway IP Address :	<input type="text"/>

L2TP: The layer 2 tunneling protocol (L2TP) is used in association with virtual private networks (VPNs). There are two parts to a L2TP connection: the WAN interface settings and the L2TP settings.

- **WAN Interface Settings – Dynamic IP Address:**
 - **WAN Interface Type:** Select Dynamic IP Address to assign an IP address provided by an ISP.
 - **Hostname:** Enter the service name of an ISP (optional).
 - **MAC address:** Enter the MAC address of the device's network interface card (NIC) in the MAC address field and click Clone MAC.
- **WAN Interface Settings – Static IP Address:**
 - **WAN Interface Type:** Select Static IP Address to assign a specific IP address for the router.
 - **My IP Address:** Enter the custom IP address. Normally provided by the ISP.
 - **My Subnet Mask:** Enter the custom Subnet Mask. Normally provided by the ISP.
 - **Gateway IP Address:** Enter the custom gateway IP address. Normally provided by the ISP.

CONFIGURATION GUIDE

Internet – L2TP – 2

L2TP Settings :

Login :	<input type="text"/>
Password :	<input type="text"/>
Service IP address :	<input type="text"/>
MTU :	<input type="text" value="1460"/> (512<=MTU Value <=1492)
Type :	<input type="text" value="Keep Connection"/> ▼
Idle Timeout :	<input type="text" value="10"/> (1-1000 Minutes)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

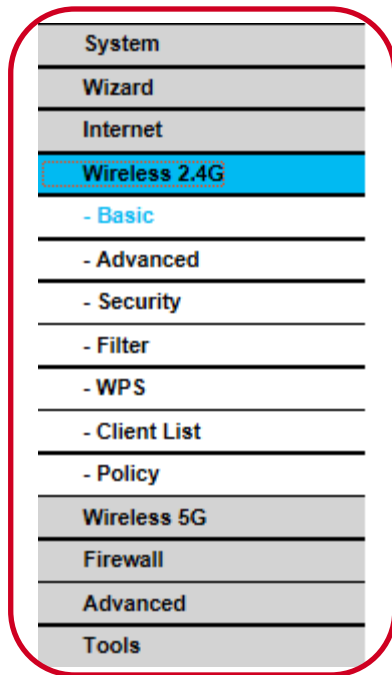
L2TP Settings:

- **Login:** Enter the username assigned by your ISP.
- **Password:** Enter the password assigned by your ISP.
- **Service IP Address:** Enter the L2TP server IP address provided by your ISP.
- **MTU:** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size (Default: 1462) permitted for an internet transmission. The MTU size can be set between 512 and 1492.
- **Type:** Configure the connection type between the router and the ISP. Choose between Keep Connection, Automatic Connection or Manual Connection.
- **Idle Timeout:** Configure the maximum amount of time, in minutes, allowed for inactive Internet connection. The Internet connection will be dropped when the maximum idle time is reached. Valid values are between one and one thousand.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G



System
Wizard
Internet
Wireless 2.4G
- Basic
- Advanced
- Security
- Filter
- WPS
- Client List
- Policy
Wireless 5G
Firewall
Advanced
Tools

Wireless 2.4G: View and edit settings for 2.4G wireless network connectivity:

- **Basic:** Configure the minimum settings required to setup a wireless network connection.
- **Advanced:** Configure the advanced network settings.
- **Security:** Configure the wireless network security settings.
- **Filter:** Configure a list of clients that are allowed to wirelessly connect to the network.
- **WPS:** Automate the connection between the a wireless device and the router using an 8-digit PIN.
- **Client:** List View the 2.4G wireless devices currently connected to the network.

CONFIGURATION GUIDE

Wireless 2.4G – Basic – 1 – AP

Radio : Enable Disable

Mode : AP

Band : 2.4 GHz (802.11b/g/n)

Enable SSID#: 1

SSID1 : RosewillCCDD10

Auto Channel : Enable Disable

Channel : 11

Apply Cancel

Mode : AP

Band : AP
WDS

Band : 2.4 GHz (802.11b/g/n)

Enable SSID#: 2.4 GHz (802.11b)
2.4 GHz (802.11g)

SSID1 : 2.4 GHz (802.11b/g)
2.4 GHz (802.11n)

Auto Channel : 2.4 GHz (802.11b/g/n)

Basic: You can manage the basic Wireless 2.4GHz functions here.

- **Radio:** Enable or disable the wireless radio. If the wireless radio is disabled, there will not be any wireless signal.
- **Mode:** Select the wireless operating mode for the router. Two modes are available: Access Point (**AP**) or Wireless Distribution System (**WDS**) mode.
 - **AP:** Provides a wireless connection access point for wireless devices.
 - **Band:** Select a wireless standard for the network from the following options:
2.4 GHz (B), 2.4 GHz (G), 2.4 GHz (N), 2.4 GHz (B+G), 2.4 GHz (B+G+N)
 - **Enable SSID#:** Select the number of wireless groups, you can enable up to 4 SSID groups.
 - **SSID[#]:** Enter the name of the wireless network(s).
 - **Auto Channel:** Enable or disable having the router automatically select a channel for the wireless network. Auto channel is enabled by default. Select disable to manually assign a specific channel. (Default = **Disable**)
 - **Check Channel Time:** When auto channel is enabled, select time period that the system checks the appropriate channel for the router.
 - **Channel** When auto channel is disabled, select a channel to assign to the wireless network. Valid value are from one to eleven in the US.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Basic – 2 – WDS

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	WDS ▼
Band :	2.4 GHz (802.11b/g/n) ▼
Enable SSID#:	1 ▼
SSID1 :	RosewillCCDD10
Channel :	11 ▼
MAC address 1 :	000000000000
MAC address 2 :	000000000000
MAC address 3 :	000000000000
MAC address 4 :	000000000000
WDS Data Rate :	300M ▼
Set Security :	<input type="button" value="Set Security"/>
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

WDS: Allows the wireless network to be expanded using multiple access points without wired connections.

- **Radio:** Enable or disable the wireless radio. If the wireless radio is disabled, there will not be any wireless signal.
- **Mode:**
 - **WDS:** Allows the wireless network to be expanded using multiple access points without wired connections.
 - **Channel** Select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.
 - **MAC Address [#]** Enter the MAC address (es) for the wireless access point(s) that you want to connect to here. (you will also need to enter T600N's MAC address into the wireless access point(s) you want to connect with)
 - **WDS Data Rate** Select the data rate for the WDS.
 - **Set Security** Click Set Security to display the WDS security settings screen. For security configuration settings, refer to “WDS Security Settings Screen” on next page.

Note: In order for WDS to work, there are some basic requirements:

1. Both AP need to be able support WDS function.
2. Both AP need to have same SSID, and same Channel.
3. When set to WDS, both AP's MAC addresses will be needed.
4. Both AP's WDS encryption and password has to be the same.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Basic – 3 – WDS Security

Set Security :

Encryption :

Encryption :

Key Length :

Key Format :

Default key :

Encryption Key 1 :

Encryption Key 2 :

Encryption Key 3 :

Encryption Key 4 :

Encryption :

WPA type : WPA(TKIP) WPA2(AES)

Pre-shared Key Format :

Pre-shared Key :

WDS: Allows the wireless network to be expanded using multiple access points without wired connections.

- **Set Security:** You should see a popup window when click on **Set Security**. Please enter the same Encryption method and password of the device that you want to connect to.
- **WDS:** Allows the wireless network to be expanded using multiple access points without wired connections.
- **Channel** Select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.
- **MAC Address [#]** Enter the MAC address(es) for the wireless access point(s) that are part of the WDS.
- **WDS Data Rate** Select the data rate for the WDS.
- **Set Security** Click Set Security to display the WDS security settings screen. For security configuration settings, refer to “WDS Security Settings Screen” on next page.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Advance – 1

These Wireless LAN settings are suggested for more advanced users. These settings should not be changed unless you know what effect the changes will have on your broadband router.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1000 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data rate :	Auto <input type="button" value="v"/>	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	100% <input type="button" value="v"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Advance: Advanced settings available for the router.

Note: Incorrectly changing these settings may cause the device to stop function. Please make sure you know the effect before changing the settings

- **Fragment Threshold:** Enter the maximum size of a packet during data transmission. A value too low could lead to low performance.
- **RTS Threshold:** Enter the RTS threshold. If the packet size is smaller than the RTS threshold, the T600N does not use RTS/CTS to send the data packet.
- **Beacon Interval:** Enter the beacon interval. This is the amount of time that the T600N sets to synchronize the network.
- **Delivery Traffic Indication Message (DTIM) Period:** Enter the DTIM period. The DTIM is a countdown period informing clients of the next point of broadcast and multicast of messages over the network. Valid values are between 1 and 255.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Advance – 2

These Wireless LAN settings are suggested for more advanced users. These settings should not be changed unless you know what effect the changes will have on your broadband router.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1000 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data rate :	Auto <input type="button" value="v"/>	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	100% <input type="button" value="v"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Advance: Advanced settings available for the router.

Note: Incorrectly changing these settings may cause the device to stop function. Please make sure you know the effect before changing the settings

- **N Data Rate:** Select the N data rate. This is the rate in which the T600N will transmit data packets to wireless N compatible devices.
- **Channel Bandwidth:** Select the channel bandwidth. The factory default is Auto 20/40MHz. The default setting provides the best performance by auto selecting channel bandwidth.
- **Preamble Type:** Select the preamble type. Long Preamble provides better LAN compatibility and Short Preamble provides better wireless performance.
- **CTS Protection:** Select the type of CTS protection. Using CTS Protection can lower the data collisions between Wireless B and Wireless G devices and lower data throughput.
- **Tx Power:** Select the wireless signal strength level. Valid values are between 10% and 100%.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Security – 1

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection :	RosewillCCDD10
Broadcast SSID :	Enable
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	1234567890

Security: Enable security options on the wireless network to prevent unwanted connection to the wireless network.

- **SSID Selection:** Select the wireless network group to change the wireless security settings for..
- **Broadcast SSID:** Enable or disable broadcast SSID. Choose whether or not the wireless group is visible to other members.
- **Wi-Fi Multimedia (WMM):** Enable or disable Multimedia quality of server (QoS) to optimize the streaming for bandwidth sensitive data such as HDTV video streaming, online gaming, VoIP, videoconferencing, and etc.
- **Encryption:** Select the encrypt type for the router. You can select between WEP, WPA (WPA TKIP/ WPA2 AES / WPA2 Mix), Pre-Shared Key, WPA Radius. Please see next page for details on Encryption.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Security – 2 – WEP

SSID Selection :	RosewillCCDD10 ▼
Broadcast SSID :	Enable ▼
WMM :	Enable ▼
Encryption :	WPA pre-shared key ▼
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase ▼
Pre-shared Key :	1234567890
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WEP (Wired Equivalent Privacy) :

- **SSID Selection:** Select the wireless network group to change the wireless security settings for.
- **Authentication Type:** Select the type of authentication.
 - **Open System:** Wireless stations can associate with the T600N without WEP encryption
 - **Shared Key:** Devices must provide the corresponding WEP key(s) when connecting to the T600N .
 - **Auto**
- **Key Length:** Select between 64-bit and 128-encryption.
- **Key Type:** Select the type of characters used for the WEP Key: ASCII (5 characters) or Hexadecimal (10 characters).
- **Encryption Key [#]:** Enter the encryption key(s) used to encrypt the data packets during data transmission.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Security – 3 – WPA

SSID Selection :	RosewillCCDD10
Broadcast SSID :	RosewillCCDD10 RosewillCCDD10_2 RosewillCCDD10_3 RosewillCCDD10_4
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	1234567890
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WPA (Wi-Fi Protected Access) :

- **WPA Type:** Select the type of WPA.
 - **WPA Temporal Key Integrity Protocol (TKIP):** Generates a 128-bit key for each packet.
 - **WPA2 Advanced Encryption Standard (AES):** Government standard packet encryption which is stronger than TKIP.
 - **WPA2 Mixed:** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **Pre-Shared Key Type:** Select the type of pre-shared key as Passphrase (ASCII) or Hexadecimal.
- **Pre-Shared Key:** Enter the pre-shared Key value.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Security – 4 – WPA Radius

SSID Selection :	RosewillCCDD10 ▾
Broadcast SSID :	Enable ▾
WMM :	Enable ▾
Encryption :	WPA RADIUS ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	1812
RADIUS Server password :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WPA Radius (Wi-Fi Protected Access) : This encryption use a RADIUS server to authenticate wireless stations and provide a session key to encrypt data during communications. Most of the information should be provided by the Network administrator.

- **WPA Type:** Select the type of WPA.
 - **WPA Temporal Key Integrity Protocol (TKIP):** Generates a 128-bit key for each packet.
 - **WPA2 Advanced Encryption Standard (AES):** Government standard packet encryption which is stronger than TKIP.
 - **WPA2 Mixed:** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **RADIUS Server IP Address:** For entering the IP address of the server.
- **RADIUS Server Port:** For entering the port number of the server.
- **RADIUS Server Password:** For entering the password of the server.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – Filter

This function lets you to allow your wireless clients to connect based on their MAC addresses.

Enable Wireless Access Control

Description	MAC address
<input type="text"/>	<input type="text"/>

MAC Address Filtering Table :

NO.	Description	MAC address	Select

Filter: The filter function will allow you to control your wireless clients' connection based on their MAC addresses.

- **Enable Wireless Access Control:** When “**Enable Wireless Access Control**” is selected, only wireless clients with MAC addresses listed in the table are allowed to connect to the wireless network. If you enable without adding any client’s MAC address here, then T600N can only be access via wire cable.
 - **Description:** Enter a description of the device allowed to connect to the network.
 - **MAC address:** Enter the MAC address of the wireless device.

Click **Add** to add new device in the table or **Reset** to discard the changes.

- **MAC Address Filtering Table:** Showing the information on the Clients that has MAC address recorded.
 - **No.:** The sequence number of the device.
 - **Description:** The description of the device.
 - **MAC Address:** The MAC address of the device.
 - **Select:** Indicates the device(s) that can have actions performed on them.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 2.4G – WPS

WPS : Enable

Wi-Fi Protected Setup Information

WPS Current Status : Configured

Self Pin Code : 34259368

SSID : RosewillCCDD10

Authentication Mode : WPA2 pre-shared key

Passphrase Key:

WPS Via Push Button :

WPS via PIN :

WPS : Wi-Fi protected setup (WPS) is an easy way to allow wireless clients to connect to the T600N. Automate the connection between the device and the T600N using a button or a PIN #.

- **WPS:** Enable or disable WPS.
- **WPS Current Status:** A notification of whether or not wireless security is configured.
- **Self Pin Code:** An 8-digit PIN which is required when configuring the router for the first time in Windows 7 or Vista.
- **SSID:** Showing the name of the wireless network.
- **Authentication Mode:** The current security settings for the corresponding SSID.
- **Passphrase Key:** A randomly generated key created by the T600N during WPS.
- **WPS via Push Button:** Click **Start to Process** to activate WPS.
- **WPS via PIN:** Enter the PIN of a wireless device click **Start to Process** to activate WPS.

CONFIGURATION GUIDE

Wireless 2.4G – Client List

WLAN Client Table :

This WLAN Client Table shows client MAC address associate to this Broadband Router

Interface	MAC Address	Signal (%)	Idle Time
RosewillCCDD10	98:D6:8B:77:02:08	100	0 secs

[Refresh](#)

Client List: Here you can view the wireless client connects wirelessly to T600N.

- **Interface:** The type of network connected to the device.
- **MAC Address:** The MAC address of device connected to network.
- **Signal:** The signal strength of the device connected to the network.
- **Idle Time:** The amount of time the connected device has not been active on the network.

Click **Refresh** to update the information appear.

CONFIGURATION GUIDE

Wireless 2.4G – Policy

SSID 1 Connection Control Policy	
WAN Connection	Enable ▾
Communication between Wireless clients	Enable ▾
Communication between Wireless clients and Wired clients	Enable ▾

SSID 2 Connection Control Policy	
WAN Connection	Enable ▾
Communication between Wireless clients	Enable ▾
Communication between Wireless clients and Wired clients	Enable ▾

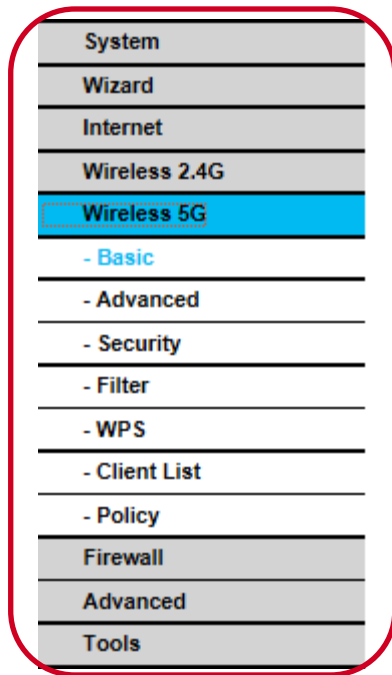
Policy: The policy here allows you to manage each SSID’s control feature. If you enable 4 SSIDs, you can manage all 4 SSIDs here.

- **WAN Connection: Enable** to allow the SSID to connect to the internet. **Disable** will turn the connection off.
- **Communication between Wireless clients: Enable** to allow the Wireless Clients to communicate with each other, share files and folders. **Disable** will turn the Communication off.
- **Communication between Wireless clients and Wired clients: Enable** to allow the Wireless Clients and Wired clients to communicate with each other, share files and folders. **Disable** will turn the Communication off.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G



Wireless 5G: View and edit settings for 5G wireless network connectivity:

- **Basic:** Configure the minimum settings required to setup a wireless network connection.
- **Advanced:** Configure the advanced network settings.
- **Security:** Configure the wireless network security settings.
- **Filter:** Configure a list of clients that are allowed to wirelessly connect to the network.
- **WPS:** Automate the connection between the a wireless device and the router using an 8-digit PIN.
- **Client:** List View the 5G wireless devices currently connected to the network.

CONFIGURATION GUIDE

Wireless 5G – Basic – 1 – AP

Radio : Enable Disable

Mode : AP

Band : 5 GHz (802.11a/n)

Enabled SSID#: 1

SSID1 : RosewillCCDD14

Channel : 36 5.180 GHz

Mode : AP

Band : WDS

Band : 5 GHz (802.11a/n)

Enabled SSID#: 5 GHz (802.11a)

SSID1 : 5 GHz (802.11n)

Enabled SSID#: 1

SSID1 : 1

Channel : 3

Channel : 36 5.180 GHz

40 5.200 GHz
44 5.220 GHz
48 5.240 GHz
149 5.745 GHz
153 5.765 GHz
157 5.785 GHz
161 5.805 GHz
165 5.825 GHz

Basic: You can manage the basic Wireless 5GHz functions here.

- **Radio:** Enable or disable the wireless radio. If the wireless radio is disabled, there will not be any wireless signal.
- **Mode:** Select the wireless operating mode for the router. Two modes are available: Access Point (**AP**) or Wireless Distribution System (**WDS**) mode.
 - **AP:** Provides a wireless connection access point for wireless devices.
 - **Band:** Select a wireless standard for the network from the following options:
5 GHz (802.11a), 5 GHz (802.11n), 5 GHz (802.11a/n)
 - **Enabled SSID#:** Select the number of wireless groups, you can enable up to 4 SSID groups.
 - **SSID[#]:** Enter the name of the wireless network(s).
 - **Auto Channel:** Enable or disable having the router automatically select a channel for the wireless network. Auto channel is enabled by default. Select disable to manually assign a specific channel. (Default = **Disable**)
 - **Check Channel Time:** When auto channel is enabled, select time period that the system checks the appropriate channel for the router.
 - **Channel** When auto channel is disabled, select a channel to assign to the wireless network.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Basic – 2 – WDS

Radio : Enable Disable

Mode : WDS

Band : 5 GHz (802.11a/n)

Enable SSID#: 1

SSID1 : RosewillCCDD10

Channel : 11

MAC address 1 : 000000000000

MAC address 2 : 000000000000

MAC address 3 : 000000000000

MAC address 4 : 000000000000

WDS Data Rate : 300M

Set Security :

WDS: Allows the wireless network to be expanded using multiple access points without wired connections.

- **Radio:** Enable or disable the wireless radio. If the wireless radio is disabled, there will not be any wireless signal.
- **Mode:** Select the wireless operating mode for the router. Two modes are available: Access Point (**AP**) or Wireless Distribution System (**WDS**) mode.
 - **WDS:** Allows the wireless network to be expanded using multiple access points without wired connections.
 - **Channel** Select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.
 - **MAC Address [#]** Enter the MAC address(es) for the wireless access point(s) that are part of the WDS.
 - **WDS Data Rate** Select the data rate for the WDS.
 - **Set Security** Click Set Security to display the WDS security settings screen. For security configuration settings, refer to “WDS Security Settings Screen” on next page.

Note: In order for WDS to work, there are some basic requirement:

1. Both AP needs to support WDS.
2. Both AP needs to have same SSID
3. Both AP needs to use same Channel.
4. When both AP set to WDS, they need to set each other's MAC addresses.
5. Both AP's WDS encryption and password should be set the same.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Basic – 3 – WDS Security

Set Security :

Encryption :

Encryption :

Key Length :

Key Format :

Default key :

Encryption Key 1 :

Encryption Key 2 :

Encryption Key 3 :

Encryption Key 4 :

Encryption :

WPA type : WPA(TKIP) WPA2(AES)

Pre-shared Key Format :

Pre-shared Key :

WDS: Allows the wireless network to be expanded using multiple access points without wired connections.

- **Set Security:** You should see a popup window when click on **Set Security**. Please enter the same Encryption method and password of the device that you want to connect to.
- **WDS:** Allows the wireless network to be expanded using multiple access points without wired connections.
- **Channel** Select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.
- **MAC Address [#]** Enter the MAC address(es) for the wireless access point(s) that are part of the WDS.
- **WDS Data Rate** Select the data rate for the WDS.
- **Set Security** Click Set Security to display the WDS security settings screen. For security configuration settings, refer to “WDS Security Settings Screen” on next page.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Advance – 1

These Wireless LAN settings are suggested for more advanced users. These settings should not be changed unless you know what effect the changes will have on your broadband router.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1000 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data rate :	<input type="text" value="Auto"/>	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	<input type="text" value="100 %"/>	

Advance: Advanced settings available for the router.

Note: Incorrectly changing these settings may cause the device to stop function. Please make sure you know the effect before changing the settings

- **Fragment Threshold:** Enter the maximum size of a packet during data transmission. A value too low could lead to low performance.
- **RTS Threshold:** Enter the RTS threshold. If the packet size is smaller than the RTS threshold, the T600N does not use RTS/CTS to send the data packet.
- **Beacon Interval:** Enter the beacon interval. This is the amount of time that the T600N sets to synchronize the network.
- **Delivery Traffic Indication Message (DTIM) Period:** Enter the DTIM period. The DTIM is a countdown period informing clients of the next point of broadcast and multicast of messages over the network. Valid values are between 1 and 255.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Advance – 2

These Wireless LAN settings are suggested for more advanced users. These settings should not be changed unless you know what effect the changes will have on your broadband router.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1000 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data rate :	Auto <input type="button" value="v"/>	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	100% <input type="button" value="v"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Advance: Advanced settings available for the router.

Note: Incorrectly changing these settings may cause the device to stop function. Please make sure you know the effect before changing the settings

- **N Data Rate:** Select the N data rate. This is the rate in which the T600N will transmit data packets to wireless N compatible devices.
- **Channel Bandwidth:** Select the channel bandwidth. The factory default is Auto 20/40MHz. The default setting provides the best performance by auto selecting channel bandwidth.
- **Preamble Type:** Select the preamble type. Long Preamble provides better LAN compatibility and Short Preamble provides better wireless performance.
- **CTS Protection:** Select the type of CTS protection. Using CTS Protection can lower the data collisions between Wireless B and Wireless G devices and lower data throughput.
- **Tx Power:** Select the wireless signal strength level. Valid values are between 10% and 100%.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Security – 1

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection :	RosewillCCDD10 ▾
Broadcast SSID :	Enable ▾
WMM :	Enable ▾
Encryption :	WPA pre-shared key ▾
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase ▾
Pre-shared Key :	1234567890

Security: Enable security options on the wireless network to prevent unwanted connection to the wireless network.

- **SSID Selection:** Select the wireless network group to change the wireless security settings for..
- **Broadcast SSID:** Enable or disable broadcast SSID. Choose whether or not the wireless group is visible to other members.
- **Wi-Fi Multimedia (WMM):** Enable or disable Multimedia quality of server (QoS) to optimize the streaming for bandwidth sensitive data such as HDTV video streaming, online gaming, VoIP, videoconferencing, and etc.
- **Encryption:** Select the encrypt type for the router. You can select between WEP, WPA (WPA TKIP/ WPA2 AES / WPA2 Mix), Pre-Shared Key, WPA Radius. Please see next page for details on Encryption.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Security – 2 – WEP

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection :	RosewillCCDD10
Broadcast SSID :	Enable
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	1234567890

WEP (Wired Equivalent Privacy) :

- **SSID Selection:** Select the wireless network group to change the wireless security settings for.
- **Authentication Type:** Select the type of authentication.
 - **Open System:** Wireless stations can associate with the T600N without WEP encryption
 - **Shared Key:** Devices must provide the corresponding WEP key(s) when connecting to the T600N .
 - **Auto**
- **Key Length:** Select between 64-bit and 128-encryption.
- **Key Type:** Select the type of characters used for the WEP Key: ASCII (5 characters) or Hexadecimal (10 characters).
- **Encryption Key [#]:** Enter the encryption key(s) used to encrypt the data packets during data transmission.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Security – 3 – WPA

SSID Selection :	RosewillCCDD10
Broadcast SSID :	RosewillCCDD10 RosewillCCDD10_2 RosewillCCDD10_3 RosewillCCDD10_4
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	1234567890
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WPA (Wi-Fi Protected Access) :

- **WPA Type:** Select the type of WPA.
 - **WPA Temporal Key Integrity Protocol (TKIP):** Generates a 128-bit key for each packet.
 - **WPA2 Advanced Encryption Standard (AES):** Government standard packet encryption which is stronger than TKIP.
 - **WPA2 Mixed:** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **Pre-Shared Key Type:** Select the type of pre-shared key as Passphrase (ASCII) or Hexadecimal.
- **Pre-Shared Key:** Enter the pre-shared Key value.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Security – 4 – WPA Radius

SSID Selection :	RosewillCCDD10 ▾
Broadcast SSID :	Enable ▾
WMM :	Enable ▾
Encryption :	WPA RADIUS ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	1812
RADIUS Server password :	<input type="text"/>

Apply Cancel

WPA Radius (Wi-Fi Protected Access) : This encryption use a RADIUS server to authenticate wireless stations and provide a session key to encrypt data during communications. Most of the information should be provided by the Network administrator.

- **WPA Type:** Select the type of WPA.
 - **WPA Temporal Key Integrity Protocol (TKIP):** Generates a 128-bit key for each packet.
 - **WPA2 Advanced Encryption Standard (AES):** Government standard packet encryption which is stronger than TKIP.
 - **WPA2 Mixed:** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **RADIUS Server IP Address:** For entering the IP address of the server.
- **RADIUS Server Port:** For entering the port number of the server.
- **RADIUS Server Password:** For entering the password of the server.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – Filter

This function lets you to allow your wireless clients to connect based on their MAC addresses.

Enable Wireless Access Control

Description	MAC address
<input type="text"/>	<input type="text"/>

Add

Reset

MAC Address Filtering Table :

NO.	Description	MAC address	Select

Delete Selected

Delete All

Reset

Apply

Cancel

Filter: The filter function will allow you to control your wireless clients' connection based on their MAC addresses.

- **Enable Wireless Access Control:** When “**Enable Wireless Access Control**” is selected, only wireless clients with MAC addresses listed in the table are allowed to connect to the wireless network. If you enable without adding any client's MAC address here, then T600N can only be access via wire cable.
 - **Description:** Enter a description of the device allowed to connect to the network.
 - **MAC address:** Enter the MAC address of the wireless device.

Click **Add** to add new device in the table or **Reset** to discard the changes.

- **MAC Address Filtering Table:** Showing the information on the Clients that has MAC address recorded.
 - **No.:** The sequence number of the device.
 - **Description:** The description of the device.
 - **MAC Address:** The MAC address of the device.
 - **Select:** Indicates the device(s) that can have actions performed on them.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Wireless 5G – WPS

WPS : Enable

Wi-Fi Protected Setup Information

WPS Current Status : Configured

Self Pin Code : 34259368

SSID : RosewillCCDD10

Authentication Mode : WPA2 pre-shared key

Passphrase Key:

WPS Via Push Button :

WPS via PIN :

WPS : Wi-Fi protected setup (WPS) is an easy way to allow wireless clients to connect to the T600N. Automate the connection between the device and the T600N using a button or a PIN #.

- **WPS:** Enable or disable WPS.
- **WPS Current Status:** A notification of whether or not wireless security is configured.
- **Self Pin Code:** An 8-digit PIN which is required when configuring the router for the first time in Windows 7 or Vista.
- **SSID:** Showing the name of the wireless network.
- **Authentication Mode:** The current security settings for the corresponding SSID.
- **Passphrase Key:** A randomly generated key created by the T600N during WPS.
- **WPS via Push Button:** Click **Start to Process** to activate WPS.
- **WPS via PIN:** Enter the PIN of a wireless device click **Start to Process** to activate WPS.

CONFIGURATION GUIDE

Wireless 5G – Client List

WLAN Client Table :

This WLAN Client Table shows client MAC address associate to this Broadband Router

Interface	MAC Address	Signal (%)	Idle Time
RosewillCCDD10	98:D5:8B:77:02:08	100	0 secs

Refresh

Client List: Here you can view the wireless client connects wirelessly to T600N.

- **Interface:** The type of network connected to the device.
- **MAC Address:** The MAC address of device connected to network.
- **Signal:** The signal strength of the device connected to the network.
- **Idle Time:** The amount of time the connected device has not been active on the network.

Click **Refresh** to update the information appear.

CONFIGURATION GUIDE

Wireless 5G – Policy

The screenshot shows the configuration interface for the Wireless 5G Policy. It is divided into two sections: SSID 1 and SSID 2. Each section has three rows of settings, each with a dropdown menu currently set to 'Enable'. The settings are: WAN Connection, Communication between Wireless clients, and Communication between Wireless clients and Wired clients.

SSID 1 Connection Control Policy	
WAN Connection	Enable
Communication between Wireless clients	Enable
Communication between Wireless clients and Wired clients	Enable

SSID 2 Connection Control Policy	
WAN Connection	Enable
Communication between Wireless clients	Enable
Communication between Wireless clients and Wired clients	Enable

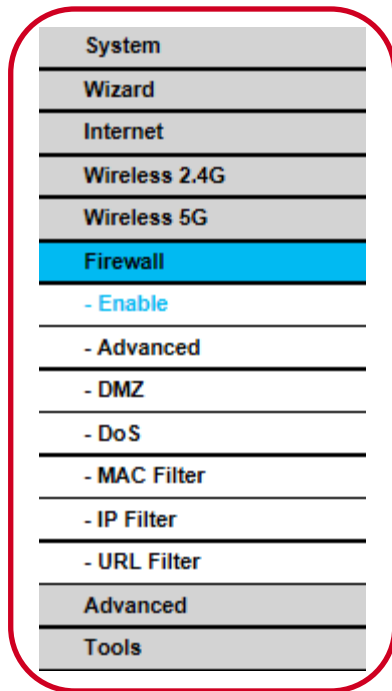
Policy: The policy here allows you to manage each SSID’s control feature. If you enable 4 SSIDs, you can manage all 4 SSIDs here.

- **WAN Connection: Enable** to allow the SSID to connect to the internet. **Disable** will turn the connection off.
- **Communication between Wireless clients: Enable** to allow the Wireless Clients to communicate with each other, share files and folders. **Disable** will turn the Communication off.
- **Communication between Wireless clients and Wired clients: Enable** to allow the Wireless Clients and Wired clients to communicate with each other, share files and folders. **Disable** will turn the Communication off.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall



Firewall: View and configure settings for firewall rule sets.

- **Status:** Display the summary of the current system status.
- **Enable:** Enable or disable the network firewall. (Default **Enable**)
- **Advanced:** Configure virtual private network (VPN) packets.
- **DMZ:** Redirect packets from the WAN port IP address to a particular IP address on the LAN.
- **DoS:** Enable or disable blocking of denial of service (DoS) attacks.
- **MAC Filter:** Uses to allow or deny the LAN clients from accessing the internet by MAC Address.
- **IP Filter:** Uses to allow or deny the LAN clients from accessing the internet by IP Address.
- **URL Filter:** Filtering the website visit by entering the key words and full URL addresses.

CONFIGURATION GUIDE

Firewall – Enable & Advanced

Firewall Function automatically detects and blocks Denial of Service (DoS) attacks, and supports URL blocking, packet filtering and SPI (Stateful Packet Inspection).

Firewall : Enable Disable

Apply

Description	Select
VPN L2TP Pass-Through	<input checked="" type="checkbox"/>
VPN PPTP Pass-Through	<input checked="" type="checkbox"/>
VPN IPSec Pass-Through	<input checked="" type="checkbox"/>
IPv6 Pass-Through	<input checked="" type="checkbox"/>
PPPoE Pass-Through	<input type="checkbox"/>

Apply

Cancel

Firewall: The firewall function automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and stateful packet inspection (SPI) are also supported. The details of the attack and the timestamp are recorded in the security log.

- **Firewall:** Enable or disable the firewall of the T600N.

Advanced: The router supports VPN pass-through which allows virtual private networking (VPN) packets to pass through the firewall.

- **VPN Pass-through:** Select to allow VPN packets to pass through the firewall.
- **VPN L2TP Pass-through:** Select to allow L2TP connection method over a VPN.
- **VPN PPTP Pass-through:** Select to allow PPTP connection method over a VPN.
- **VPN IPSec Pass-through:** Select to allow IPSec connection method over a VPN.
- **IPv6 Pass-through:** Select to allow IPv6 packets to pass through the Router .
- **PPPoE Pass-through:** Select to allow clients to directly connect to internet via PPPoE.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

Enable DMZ

Local IP Address : Please select a PC. ▾

DMZ: Configuring a device on the LAN as a demilitarized zone (DMZ) host allows unrestricted two-way Internet access for Internet applications, such as online video games, to run from behind the NAT firewall. The DMZ function allows the router to redirect all packets going to the WAN port IP address to a particular IP address on the LAN. The difference between the virtual server and the DMZ function is that a virtual server redirects a particular service or Internet application, such as FTP, to a particular LAN client or server, whereas a DMZ redirects all packets, regardless of the service, going to the WAN IP address to a particular LAN client or server. A DMZ host allows a computer to have all its connections and ports completely open during data transmission.

Note: The PC defined as a DMZ host is not protected by the firewall and is vulnerable to malicious network attacks. Do not store or manage sensitive information on the DMZ host.

- **Enable DMZ:** Click Enable DMZ to activate the DMZ function.
- **Local IP Address:** Enter the IP Address of the device on the LAN. (This is best to co-work with **Static DHCP IP** on page 22).

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – DoS

The Firewall can detect and block DoS (Denial of Service) attacks. DoS attacks flood your internet connection with invalid packets and connection requests which makes Internet access becomes unavailable.

Block DoS : Enable Disable

Apply

Cancel

DoS: To enable blocking of denial of service (DoS) attacks, select the DoS option in the Firewall section. DoS attacks can flood the internet connection with the continuous transmission of data. Blocking these attacks ensures that the internet connection is always available.

- **Block DoS:** Click Enable to activate the block DoS Attack.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – MAC Filter

Enable MAC filtering

Deny all clients with MAC address listed below to access the network

Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address
<input type="text"/>	<input type="text"/>

Add

Reset

MAC Filtering table :

NO.	Description	LAN MAC Address	Select

Delete Selected

Delete All

Reset

Apply

Cancel

MAC Filter: Mac Filter is to control the LAN computer’s internet access ability.

- **Enable MAC filtering:** Click Enable to activate the MAC filter function
 - **Deny all clients with MAC address listed below to access the network:** Enable this will deny any device’s MAC address listed here from connecting to Internet.
 - **Allow all clients with MAC address listed below to access the network:** Enable this will allow only the device’s MAC address listed here from connecting to Internet.
 - **Description:** Enter a description of the device that you want to record to the MAC Filtering table.
 - **LAN MAC Address:** Enter the MAC address associate to the devices that you want to record to the MAC Filtering table.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

- **MAC Filtering Table:** This table records the LAN devices you want to filter. Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – IP Filter – 1

Enable IP Filtering Table

Deny all clients with IP address listed below to access the network
 Allow all clients with IP address listed below to access the network

Description :

Protocol :

Local IP Address : ~

Port range : ~

NO.	Description	Local IP Address	Protocol	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

IP Filter: IP Filter is use to control the LAN computer’s internet access ability.

- **Enable IP Filtering Table:** Click to activate the IP Filter function
 - **Deny all clients with IP address listed below to access the network:** Enable this will deny any device’s IP address listed here from connecting to Internet.
 - **Allow all clients with MAC address listed below to access the network:** Enable this will allow only the device’s MAC address listed here from connecting to Internet.
 - **Description:** Enter a description of the device that you want to record to the MAC Filtering table.
 - **Protocol:** You can select **Both, TCP, UDP** here. They are internet packet transmit methods, TCP are mainly for protocol that requires more detail such as Email, while UDP are protocols that require less checkup such as multimedia streaming.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Note: Incorrectly changing these settings may cause the device to stop function. Please make sure you know the effect before changing the settings

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – IP Filter – 2

Enable IP Filtering Table

Deny all clients with IP address listed below to access the network
 Allow all clients with IP address listed below to access the network

Description :

Protocol :

Local IP Address : ~

Port range : ~

NO.	Description	Local IP Address	Protocol	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

IP Filter: IP Filter is use to control the LAN computer’s internet access ability.

- **Enable IP Filtering Table:** Click to activate the IP Filter function
 - **Local IP Address:** You can enter a range of IP address here.
 - **Port Range:** Port Range is the internet socket port numbers used by protocol in range from 0 to 1023. They are used by system processes that provide widely used types of network services. Also port number range from 1024 to 49151 are registered ports which are signed **Internet Assigned Numbers Authority (IANA)** for specific service upon application by a requesting entity. For example, Adobe Flash uses TCP protocol and port number 843. Xbox LIVE uses TCP and UDP protocol and port number 3074. If you want to add a rule to control some users from accessing FTP, you can set **Local IP Address:** 192.168.0.100 ~ 192.168.0.200 and **Port range:** 21.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Note: Incorrectly changing these settings may cause the device to stop function and some of your programs unable to access the internet. Please make sure you know the effect before changing the settings

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Firewall – URL Filter

Enable URL Blocking

URL/keyword

Add

Reset

Current URL Blocking Table :

NO.	URL/keyword	Select
-----	-------------	--------

Delete Selected

Delete All

Reset

Apply

Cancel

URL Filter: URL Filter is use to block certain Website or keyword from the devices to access.

- **Enable URL Blocking:** Click to activate the URL Blocking function.
 - **URL/keyword:** Enter a complete website address or certain keyword. Then press **Add** to add into the **URL Blocking Table**.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced

System
Wizard
Internet
Wireless 2.4G
Wireless 5G
Firewall
Advanced
- NAT
- Port map.
- Port fw.
- Port tri.
- ALG
- UPnP
- QoS
- Routing
Tools

Advanced: View and configure advanced system and network settings:

- **NAT:** Enable or disable Network Address Translation (NAT); You can also enable or disable the Hardware accelerator here for optimal network performance.
- **Port Mapping:** Re-direct a range of service port numbers to a specified LAN IP address.
- **Port Forwarding:** Configure server applications to send and receive data from specific ports on the network.
- **Port Triggering:** Configure applications that require multiple connections and different inbound and outbound connections.
- **ALG:** Configure the application layer gateway (ALG).
- **UPnP:** Enable or disable Universal Plug and Play (UPnP) functionality.
- **QoS:** Configure the network quality of service (QoS) setting by prioritizing the uplink and downlink bandwidth.
- **Routing:** Configure static routing.

CONFIGURATION GUIDE

Advanced – NAT & Hardware Accelerator

NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass through a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT : Enable Disable

Hardware Accelerator boosts network performance (note: to achieve optimal result, QoS and bandwidth control features will be disabled).

Hardware Accelerator : Enable Disable

Apply

NAT: Network address translation (NAT) allows users on the LAN to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides firewall protection from hacker attacks and allows for mapping LAN IP addresses to WAN IP addresses with key services such as websites, FTP, video game servers, etc.

- **NAT:** Click **Enable** to activate the function.

Hardware Accelerator: Hardware Accelerator will boost the network performance, but QoS and bandwidth control will be disabled.

- **Hardware Accelerator:** Click **Enable** to activate the function.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – Port Mapping

Enable Port Mapping

Description :

Local IP :

Protocol :

Port range : ~

Current Port Mapping Table :

NO.	Description	Local IP	Type	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Port Mapping: Port Mapping allows you to redirect a particular range of service port numbers from the WAN to a particular LAN IP address.

- **Enable Port Mapping:** Click to activate this function.
 - **Description:** Enter a description of the device that you want to record to the MAC Filtering table.
 - **Local IP :** Enter the local IP address of the server behind the NAT firewall
 - **Protocol:** You can select Both, TCP, UDP here. They are internet packet transmit methods, TCP are mainly for protocol that requires more detail such as Email, while UDP are protocols that require less checkup such as multimedia streaming.
 - **Port Range:** Enter the range of ports to be forwarded.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Note: Incorrectly changing these settings may cause the device to stop function and some of your programs unable to access the internet. Please make sure you know the effect before changing the settings

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – Port Forwarding

Enable Port Forwarding

Description :

Local IP :

Protocol :

Local Port :

Public Port :

Current Port Forwarding Table :

NO.	Description	Local IP	Local Port	Type	Public Port	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

Port Forwarding: Port forwarding enables multiple server applications on a LAN to serve clients on a WAN over a single WAN IP address. The router accepts incoming client packets, filters them based on the destination WAN, or public, port and protocol and forwards the packets to the appropriate LAN, or local, port. Unlike the DMZ feature, port forwarding protects LAN devices behind the firewall.

- **Enable Port Forwarding:** Click **Enable Port Forwarding** to active port forwarding.
- **Description:** Enter notes or details about the forwarded port configuration.
- **Local IP:** Enter the local IP address of the server behind the NAT firewall.
- **Protocol:** Select the protocol to use for mapping from the following: TCP, UDP or Both.
- **Local Port:** Enter the LAN port number that WAN client packets will be forward to.
- **Public Port:** Enter the WAN port number that clients will send their packets to.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – Port Triggering

Enable Trigger Port

Description :

Popular applications :

Trigger port : ~

Trigger type :

Public Port :

Public type :

Current Trigger-Port Table :

NO.	Trigger port	Trigger type	Public Port	Public type	Name	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

Port Triggering: Some applications, such as online games, videoconferencing and VoIP telephony, require multiple ports for inbound and outbound traffic. If an application requires both an incoming and an outgoing port simultaneously, it is possible to configure static port forwarding to handle the packets. That is not an optimal solution because a static IP address must be configured for each device. With port triggering an application, local port or range of ports and a communication protocol can be mapped to a specific public port. Sending packets out over the local port triggers the router to open an incoming local port that is mapped to the same public port and application as the outgoing local port(s). The local application can communicate over the incoming and outgoing ports without the need for creating a fixed address.

- **Enable Port Triggering:** Click to activate the function.
 - **Description** Enter notes or details about the port triggered configuration.
 - **Popular Applications** Select a default application or add a new one.
 - **Trigger Port** Enter the application’s outbound port number(s).
 - **Trigger Type** Select the protocol to use for port triggering from the following: TCP, UDP or Both.
 - **Public Port** Enter the inbound port(s) for the application in the following format: 2300-2400 or 47624.
 - **Public Type** Select the protocol to use for the inbound port from the following: TCP, UDP or Both.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – ALG.

Description	Select
H323	<input type="checkbox"/>
MMS	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
Egg	<input type="checkbox"/>
IRC	<input type="checkbox"/>
Amanda	<input type="checkbox"/>
Quake3	<input type="checkbox"/>
Talk	<input type="checkbox"/>
IPsec	<input type="checkbox"/>
FTP	<input type="checkbox"/>
SIP	<input type="checkbox"/>

ALG: The ALG (Application Layer Gateway) serves as a window between correspondent application processes so that they may exchange information on an open environment.

- **ALG Table:** Select the listed applications that need ALG support and then the router will authorize them to pass through the NAT gateway.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – UPnP

- Enable the Universal Plug and Play (UPnP) Feature
- Allow users to make port forwarding changes through UPnP

Apply

UPnP: UPnP helps internet devices, such as gaming and videoconferencing, to access the network and connect to other registered UPnP devices..

- **Enable the Universal Plug and Play (UPnP) Feature:** Click to activate the UPnP function.
- **Allow users to make port forwarding changes through UPnP:** With this function activate, the users can use port forwarding changes in their devices.

Click **Apply** to apply the settings.

CONFIGURATION GUIDE

Advanced – QoS – 1

Total Bandwidth Settings

Uplink	Full ▼
Downlink	Full ▼

QoS : Priority Queue Bandwidth Allocation Disabled

QoS: QoS can prioritize bandwidth use such as video streaming, online gaming, VoIP telephony and videoconferencing to ensure stable and efficient network performance.

- **Total Bandwidth Settings:**

- **Uplink:** Select the maximum bandwidth speed for outbound traffic.
- **Downlink:** Select the maximum bandwidth speed for inbound traffic
- Click **Disabled** if you do not want to prioritize any data or protocol.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – QoS – 2

QoS : Priority Queue Bandwidth Allocation Disabled

Unlimited Priority Queue

Local IP Address	Description
<input type="text"/>	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	<input type="radio"/>	<input checked="" type="radio"/>	20,21
HTTP	<input type="radio"/>	<input checked="" type="radio"/>	80
TELNET	<input type="radio"/>	<input checked="" type="radio"/>	23
SMTP	<input type="radio"/>	<input checked="" type="radio"/>	25
POP3	<input type="radio"/>	<input checked="" type="radio"/>	110
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	Both <input type="text"/> ~ <input type="text"/>
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	Both <input type="text"/> ~ <input type="text"/>
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	Both <input type="text"/> ~ <input type="text"/>

QoS - Priority Queue: Set network resource usage based on specific protocols or port ranges. Incoming packets are processed based on the protocols’ position within the queue.

- **Unlimited Priority Queue:**
 - **Local IP:** Address Enter the local IP address of a device on the network. This device’s activity is not restricted by the QoS feature.
- **High/Low Priority Queue:** Specify the priority for different protocols. Additional protocols and port ranges can be added.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – QoS – 3

QoS : Priority Queue Bandwidth Allocation Disabled

Type :

Local IP range : ~

Protocol :

Port range : ~

Policy :

Rate(bps) :

Current QoS Table:

NO.	Type	Local IP range	Protocol	Port range	Policy	Rate (bps)	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>							

QoS – Bandwidth Allocation: Set network resource usage, for inbound and outbound traffic, based on local IP and port ranges.

- **Type:** Select Download or Upload to specific the direction of packet traffic.
- **Local IP Range:** Enter the local IP range of the current configuration.
- **Protocol:** Select the protocol to manage for the current configuration.
- **Port Range:** Enter the local port range of the current configuration.
- **Policy:** Select Min or Max to specify the type of configuration policy.
- **Rate (bps):** Select the bandwidth rate, in bits per second (bps), of the current configuration.

Click **Add** to save the settings to the table or **Reset** to discard the changes.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Advanced – Routing

To take Static Route effect, please disable NAT function.

Enable Static Routing

Destination LAN IP :

Subnet Mask :

Default Gateway :

Hops:

Interface : LAN

Add

Reset

Current Static Routing Table :

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Hops	Interface	Select

Delete Selected

Delete All

Reset

Apply

Cancel

Routing: Typically static routing does not need to be setup because the T600N has adequate routing information after it has been configured for Internet access. Static routing is only necessary if the router is connected to network under a different subnets.

Note: To enable routing, you will first need to disable NAT.

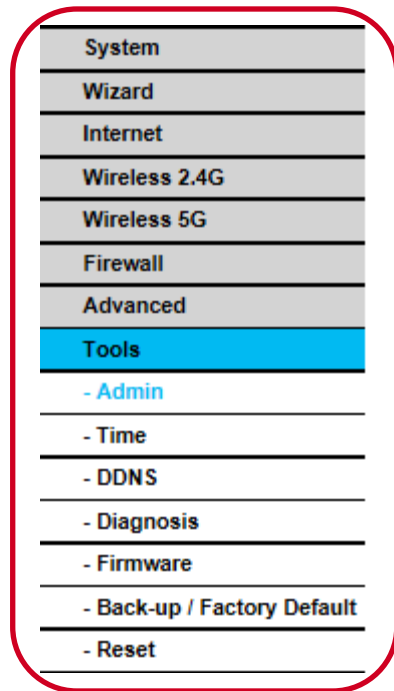
- **NAT Disabled:**

- **Enable Static Routing:** Click Enable Static Routing to activate the feature.
 - **Destination LAN IP:** Enter the LAN IP address of the destination device.
 - **Subnet Mask:** Enter the Subnet Mask of the destination device.
 - **Default Gateway:** Enter the default gateway IP address for the destination device.
 - **Hops:** Enter the maximum number of hops within the static routing that a packet is allowed to travel.
 - **Interface:** You can select LAN or WAN here.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools



System
Wizard
Internet
Wireless 2.4G
Wireless 5G
Firewall
Advanced
Tools
- Admin
- Time
- DDNS
- Diagnosis
- Firmware
- Back-up / Factory Default
- Reset

Tools: You can view and configure system and network tools settings:

- **Admin:** Configure the administrator password used to login to the router.
- **Time:** Configure the system time on the router.
- **DDNS:** Map a static domain name to a dynamic IP address.
- **Diagnosis:** Check if a specific computer is connected to the LAN.
- **Firmware:** Update the router's firmware.
- **Backup / Factory Default:** Load or save configuration settings from a backup file or restore the factory default settings.
- **Reset:** Manually reset the router.

CONFIGURATION GUIDE

Tools – Admin

You can change the password that you use to access the router, this is not your ISP account password.

Old Password :

New Password :

Repeat New Password :

Remote management allows the router to be configured from the Internet by a web browser, A username and password is still required to access the Web-Management interface.

Host Address	port	Enable
<input type="text"/>	8080	<input type="checkbox"/>

Admin: Change the router’s system password as well as setup a device to remotely configure the settings.

- **Password Setting:** Here you can change the login password for T600N. (Default is: Login: admin; pass: admin)
 - **Old Password:** Enter the existing administrator password.
 - **New Password:** Enter the new administrator password.
 - **Repeat New Password:** Re-type the new administrator password.
- **Remote Management:**
 - **Host Address:** Enter the designated host IP Address.
 - **Port:** Enter the port number (**Default: 8080**) for remote accessing management web interface. (Unless behind a corporate firewall that blocks some ports. Ports **80** and **443** are not typically blocked are for HTTP and HTTPS outbound traffic.)
 - **Enable:** Select to enable the Remote Management function.

Note: To access the settings of the T600N remotely, enter the router’s WAN IP address and port number. E.g, if your external IP is 114.127.3.123 and you use port 8080, enter “**http://114.127.3.123:8080**” You will still need to enter Login name and password to enter the router’s management page.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools – Time

Time Setup: Synchronize with the NTP Server ▼

Time Zone : (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼

NTP Time Server :

Daylight Saving : Enable
From January ▼ 1 ▼ To January ▼ 1 ▼

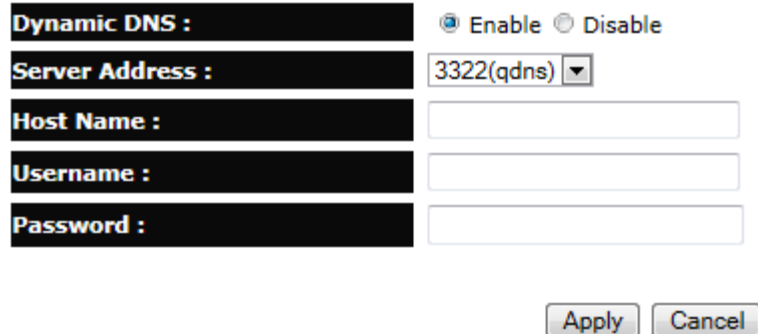
Time: Change the system time of the T600N and setup automatic updates through a network time protocol server (NTP).

- **Time Setup:** Select how the router obtains the current time.
- **Time Zone:** Select the time zone for the router.
- **NTP Time Server:** Enter the domain name or IP address of an NTP server.
- **Enable Daylight Saving:** Click to enable or disable daylight savings time.
 - **Start Time:** Select the date and time when daylight savings time starts.
 - **End Time:** Select the date and time when daylight savings time ends.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools – DDNS



Dynamic DNS : Enable Disable

Server Address : 3322(qdns) ▼

Host Name :

Username :

Password :

DDNS: Dynamic domain name service (DDNS) allows the administrator to map a static domain name to a dynamic IP address. A DDNS service provider, such as DynDNS, ZoneEdit or CyberGate, must provide an account, password, and static domain name to use this feature. DDNS particularly benefits end users that have their own websites or FTP sites.

- **Dynamic DNS:** Enable or Disable DDNS.
- **Server Address:** Select the DDNS Server Address.
- **Host Name:** Enter the DDNS provider static domain name.
- **Username:** Enter the username given by the DDNS provider.
- **Password:** Enter the password given by the DDNS provider.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools – Diagnosis



The screenshot shows a web interface for a ping test. It consists of two rows of input fields. The first row has a label 'Address to Ping :' on the left, an empty text input field in the middle, and a blue 'Start' button on the right. The second row has a label 'Ping Result :' on the left and an empty text input field in the middle.

Diagnosis: The diagnosis feature allow the administrator to verify that another device is available on the network and is accepting request packets. If the ping result returns alive, it means a device is on line. This feature does not work if the target device is behind a firewall or has security software installed.

- **Address to Ping:** Enter IP address of the device to ping.
- **Ping Result:** View the result message from the ping test.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools – Firmware

You can upgrade the firmware of the router here. The firmware you want to upgrade to will need to locate in your local hard drive. Click on Browse to select and locate the firmware for your update.

Firmware: Firmware is system software that operates and allows the administrator to interact with the router.

- To update the firmware version, follow these steps:
 1. Download the appropriate firmware for T600N from Rosewill's website.
 2. Click **Browse....**
 3. Browse the computer and select the firmware file.
 4. Click **Apply.**

Note: Upgrading firmware through a wireless connection is not recommended. Firmware upgrading must be performed while connected to an Ethernet (LAN port) with all other clients disconnected.

Click **Apply** to save the settings or **Cancel** to discard the changes.

CONFIGURATION GUIDE

Tools – Backup / Factory Default

Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings.

The screenshot shows a web interface with three main sections, each with a dark header and a light background. The first section is 'Restore to factory default' with a blue 'Reset' button. The second section is 'Backup Settings' with a grey 'Save' button. The third section is 'Restore Settings' with a grey 'Upload' button and a grey 'Browse...' button to its right.

Backup / Factory Default : Store multiple settings by saving the settings to a configuration file on the device.

- **Restore to factory default:** Click Reset to restore the T600N to factory defaults.
- **Backup Settings:** Click Save to save the current configuration on the T600N to a *.dlf file.
- **Restore Settings:** To restore saved settings, do the following:
 1. Click **Browse....**
 2. Browse the file system for location of the settings file (*.dlf).
 3. Click **Upload.**

CONFIGURATION GUIDE

Tools – Reset

In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button.

Reset: This feature allows the administrator to reboot the router in the event of a system hang up.

Click **Apply** to save the settings or **Cancel** to discard the changes.

PHYSICAL SPECIFICATION

General	
Standards	IEEE 802.3i/u/ab IEEE 802.11a/b/g/n
Protocols	UDP, TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP, ARP, ALG
Ports	1x 10/100/1000M WAN port 4x 10/100/1000M LAN ports
LEDs	PWR, 2.4GHz WLAN, WPS, WAN (Modem), 4x LAN, WPS, 5GHz WLAN
Safety & Emissions	FCC, CE



PHYSICAL SPECIFICATION

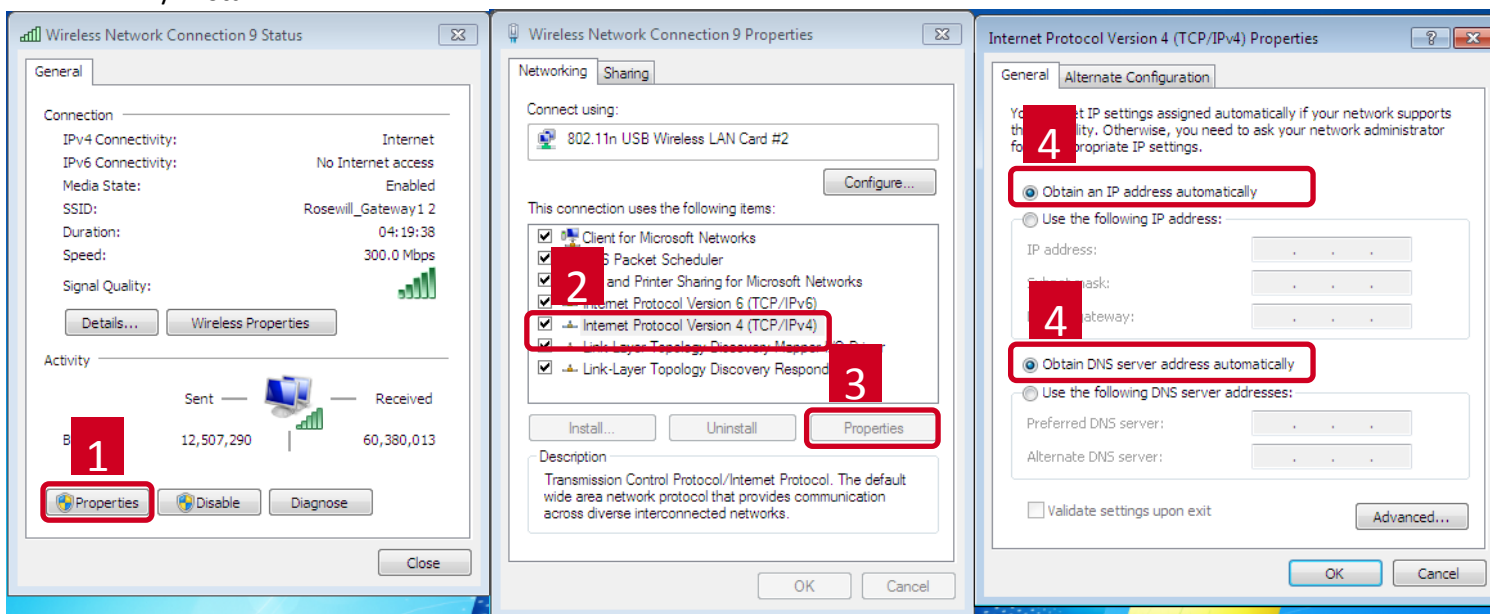
Wireless	
Frequency Band	2.4GHz / 5GHz
Radio Data Rate	2.4GHz – 300mbps and 5GHz – 300 mbps
Optimal Transmit Power	20 dBm
Modulation	Support 256/64/16/8-QAM, QPSK, BPSK, MCS0 ~ MCS15
Security	WEP, WPA (TKIP), WPA2 (AES), WPA Radius wireless encryption, 802.1x Authentication, and WPS
Antenna Gain	2x 5dBi R-SMA 2.4GHz External Antennas (SMA Connectors); 2x 3.5dB Internal 5GHz Internal Antenna
Environmental and Physical	
Temperature.	Operating : 0°C~40°C (32°F~104°F)
	Storage: -40°C~70°C (-40°F~158°F)
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 90% RH, Non-condensing
Weight & Dimension	6.69 x 4.33 x 0.98 in (17 x 11 x 2.5 cm) + 1.5 lbs (700g)

TROUBLESHOOTING

Problem. I follow the steps, but I am not able to open router's web management page after type in 192.168.1.1 on my web browser.

Solutions. 1. Check if your computer connected to T600N has being set as a "Fixed IP". You may want to change to "DHCP" setting.

- WIN7 / Vista



2. Check if your computer is connecting to any wireless / wired network other than T600N's.

3. You may have a IP conflict on your modem and the router. Please go to LAN Interface Setup and change the **IP Address** to 192.168.x.1 (x can be any number from 2 to 255), then click **Apply**.

TROUBLESHOOTING

Problem. My DSL connection is working, but I can not access the internet with T600N.

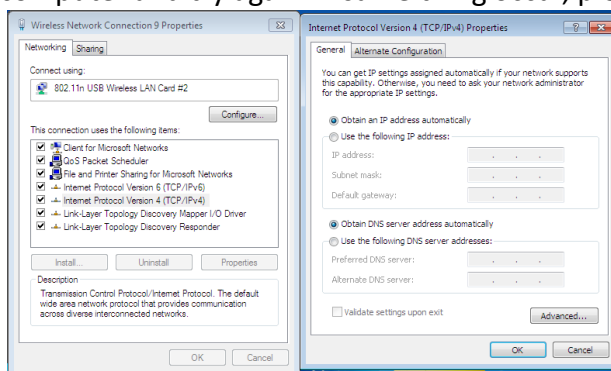
- **Solutions.** Your Internet Service Provider (ISP) may require the entering of Login and password. To enter, please click **PPPoE** under **Internet**. Then enter the connection information provided by your ISP.

Problem. The Setup Wizard does not detect or configure my network.

- **Solutions.**
 1. Reset your modem, and power off your T600N by unplug the power adapter then plug back in.
 2. Allow the wizard to detect your Internet connection one more time. Then follow the Wizard's instruction to complete.
 3. Or you can check with your ISP for the following connection methods under **Internet**:
 - **DSL Connection (Mostly as PPPoE Connection):** Your internet connection needs login information. Please check with ISP if you do not have on hand.
 - **Cable Modem Connection (Mostly as Dynamic IP or Static IP Connection):** Cable modem connection may require you to clone MAC address.
 - Click **Dynamic IP** under **Internet**, then under **MAC Address** select **Clone MAC** or manually enter the MAC address.
 - Click **Static IP** under **Internet**, then enter the **IP address** and other connecting information from the ISP.

Problem. My IP address show up as 169.254.x.x and my computer tells me that I have "Limited or no Connectivity"

- **Solutions.** Check if T600N's **LAN** under **System** and see if you enable the **DHCP Server**, also check if your computer is set as DHCP setting. (DHCP should look like below). Restart you computer and try again. If same thing occur, please try using another computer or the wireless connection.



Problem. I am not getting maximum signal strength when right next to my router.

- **Solutions.** The client may be too close to the router. You may want to step 5 ~ 10 feet away from the router. You can also change the wireless channel to avoid wireless interference. Recommended channels use are 1, 6, and 11.

Safety Statement

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. "To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications