



Wireless Router RNX-N400LX
User Manual

Default IP Address: 192.168.1.254

Default Login Name: admin

Default Password: guest

(Please change Default Login Name and Password once you entered into the Management Page, and keep a record of your new Login Name and Password)

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.



Table of Contents

1	INTRODUCTION	6
	1.1 OVERVIEW.....	6
	1.2 KEY FEATURES.....	6
	1.3 PACKAGE CONTENTS	7
	1.4 PRODUCT LAYOUT AND LED SIGNAL.....	7
	1.5 NETWORK + SYSTEM REQUIREMENTS.....	9
	1.6 RNX-N400LX PLACEMENT	9
	1.7 HARDWARE SETUP	9
2	SETUP	11
	2.1 PREPARE YOUR PC FOR RNX-N400LX'S CONFIGURATION	11
	2.11 For OS of Microsoft Windows 7:	11
	2.12 For OS of Microsoft Windows Vista:	13
	2.13 For OS of Microsoft Windows 2000/ XP:.....	14
	2.14 For OS of Microsoft Windows 95/ 98/ Me:.....	15
	2.15 For OS of Microsoft Windows NT:.....	15
	2.2 CONNECTING TO RNX-N400LX'S WEB MANAGEMENT	16
	2.21 Connecting using Web Browser:.....	16
3	RNX-N400LX WEB MANAGEMENT PAGE.....	17
	3.1 SETUP WIZARD:	17
	3.11 Welcome to Setup Wizard:.....	17
	3.12 Operation Mode:	18
	3.13 Time Zone Setting:	18
	3.14 LAN Interface Setup:.....	18
	3.15 WAN Interface Setup:.....	19
	3.16 Wireless Basic Setting:.....	19
	3.17 Wireless Security Setup:.....	20
	3.2 OPERATION MODE:.....	20
	3.3 WIRELESS.....	21
	3.31 Wireless Basic Settings:	21
	3.32 Wireless – Advanced Setting	22
	3.33 Wireless – Security Setup	24
	3.34 Wireless – Access Control.....	25
	3.35 Wireless – WDS Settings.....	26
	3.351 WDS Security Setup	26
	3.352 WDS AP Table	27
	3.36 Wireless – Site Survey	27
	3.37 Wireless – WPS.....	28
	3.38 Wireless – Schedule.....	29
	3.4 TCP/IP SETTINGS:	29
	3.41 LAN Interface.....	29
	3.411 Static DHCP Setup	30
	3.42 WAN Interface Setup.....	31
	3.421 WAN Interface Setup - Static IP	31
	3.422 WAN Interface Setup – DHCP client.....	33
	3.423 WAN Interface Setup – PPPoE.....	34
	3.424 WAN Interface Setup – PPTP	36
	3.5 FIREWALL:	38
	3.51 Firewall - Port Filtering.....	38
	3.52 Firewall - IP Filtering.....	39

3.53 Firewall - MAC Filtering	40
3.54 Firewall – Port Forwarding	41
3.55 Firewall – URL Filtering	42
3.56 Firewall – DMZ	43
3.6 QoS:	44
3.7 MANAGEMENT:	45
3.71 Management – Status	45
3.72 Management – Statistics	47
3.73 Management – DDNS.....	47
3.74 Management – Time Zone Setting	48
3.75 Management – Denial-of-Service	49
3.76 Management – Log.....	50
3.77 Management – Upgrade Firmware.....	50
3.78 Management – Save/Reload Settings	51
3.79 Management – Password	51
APPENDIX A – FREQUENTLY ASKED QUESTIONS (FAQ)	52
1. WHAT IS AND HOW TO FIND MY COMPUTER’S IP AND MAC ADDRESS?	52
2. WHAT IS WIRELESS LAN?	53
3. WHAT ARE ISM BANDS?	53
4. HOW DOES WIRELESS NETWORKING WORK?	53
5. WHAT IS BSSID?	54
6. WHAT IS ESSID?	55
7. WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE?	55
8. WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS?	55
9. WHAT IS WEP?	55
10. WHAT IS FRAGMENT THRESHOLD?.....	56
11. WHAT IS RTS (REQUEST TO SEND) THRESHOLD?	56
12. WHAT IS BEACON INTERVAL?	57
13. WHAT IS PREAMBLE TYPE?.....	57
14. WHAT IS SSID BROADCAST?	57
15. WHAT IS WI-FI PROTECTED ACCESS (WPA)?.....	57
16. WHAT IS WPA2?	58
17. WHAT IS 802.1X AUTHENTICATION? PROTOCOL (TKIP)?.....	58
18. WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)?	58
19. WHAT IS ADVANCED ENCRYPTION STANDARD (AES)?	58
20. WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)?	59
21. WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)?	59
22. WHAT IS UNIVERSAL PLUG AND PLAY (UPnP)?	59
23. WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE?	59
24. WHAT IS CLONE MAC ADDRESS?	59
25. WHAT IS DDNS?	60
26. WHAT IS NTP CLIENT?.....	60
27. WHAT IS VPN?.....	60
28. WHAT IS IPSEC?	60
29. WHAT IS WLAN BLOCK RELAY BETWEEN CLIENTS?.....	60
30. WHAT IS WMM?	60
31. WHAT IS WLAN ACK TIMEOUT?	61
32. WHAT IS MODULATION CODING SCHEME (MCS)?	61
33. WHAT IS FRAME AGGREGATION?	61
APPENDIX B – PRODUCT SPECIFICATION.....	62
APPENDIX C – FCC INTERFERENCE STATEMENT	63
APPENDIX D – IC INTERFERENCE STATEMENT	65

Before We Begin

- Please configure RNX-N400LX with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using RNX-N400LX, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on RNX-N400LX, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.
- Please first check your package content when you receive RNX-N400LX. You should have the following:



1 Introduction

1.1 Overview

Thank you for purchasing the RNX-N400LX. The Wireless LAN Broadband Router is an affordable IEEE 802.11b/g with 802.11n Draft 2.0 Wireless router solution; provides family and SOHO an affordable solution for high performance, secure, manageable and reliable WLAN. RNX-N400LX is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Switch that connects your wired-Ethernet devices together at incredible speeds.

At 150Mbps wireless transmission rate, RNX-N400LX's wireless technology using advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel to give you seamless access to multimedia content. Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, RNX-N400LX can encode all wireless transmissions with 64bit/128bit WEP or WPA, WPA2 and WPA mix support personal (PSK) and enterprise encryption.

1.2 Key Features

Features	Advantages
RAM 16MB, Maximum support Session up to, Data Rate up to 150Mbps**	Maximizes the performance and ideal for media-centric applications like streaming video, gaming and Voice over IP technology.
Four 10/100 Mbps Fast Switch Ports (Auto-Crossover)	Scalability, extend your network.
Firewall security with port filtering, IP filtering, MAC filtering, port forwarding, trigger port, DMZ hosting and URL filtering functions	Avoids the attacks of Hackers or Viruses from Internet
Support 802.1x Authenticator, 802.11i (WPA/WPA2, TKIP and AES under both PSA and enterprise mode), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security
WDS (Wireless Distribution System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater

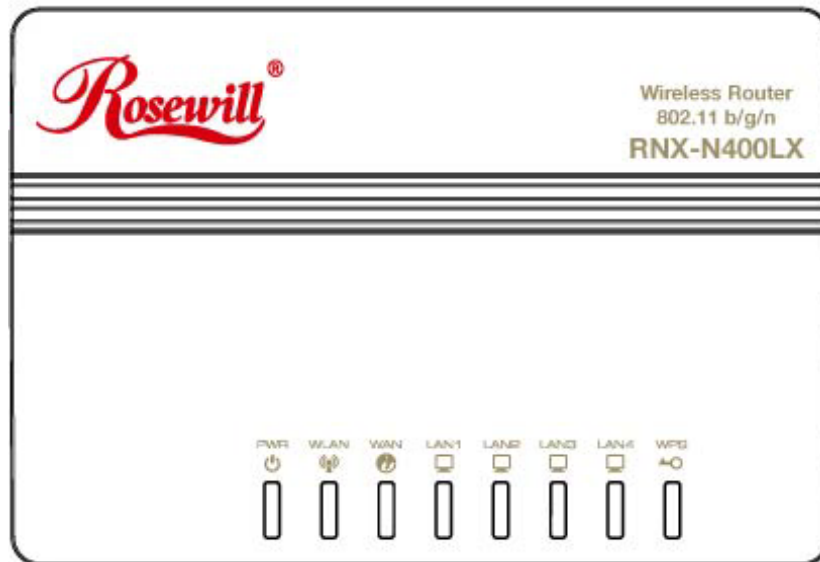
** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.




1.3 Package Contents

Please open the package and make sure that you have all items listed below. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

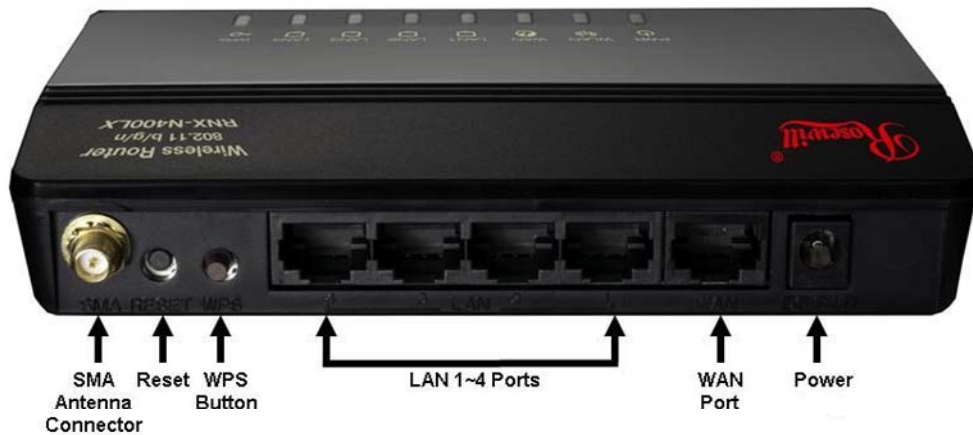
1. 1x 802.11n Draft 2.0 RNX-N400LX Router
2. 1x 2dBi 2.4GHz Detachable Antenna
3. 1x 100V~240V Power Adapter
4. 1x CD (Quick Installation Guide, User Manual, and Setup Wizard program)

1.4 Product Layout and LED Signal



LED	Status	Description
PWR 	On	RNX-N400LX is receiving power and functioning properly.
	Blinking	RNX-N400LX is performing test or reset
	Off	RNX-N400LX is power off
It will take about 50 seconds to complete the boot up sequence after powered on the RNX-N400LX; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.		
WLAN 	Blinking	Data is transmitting or receiving.
	Off	No data is transmitting or receiving.
WAN 	On	RNX-N400LX's WAN port is linking
	Blinking	RNX-N400LX is sending/receiving data through WAN

	Off	RNX-N400LX's WAN port is not linking
LAN1 □	On	RNX-N400LX's LAN port is linking
LAN2 □	Blinking	RNX-N400LX is sending/receiving data through LAN port
LAN3 □	Off	RNX-N400LX's LAN port is not linking
LAN4 □	On	Press Button to start searching
WPS □	Blinking	RNX-N400LX is sending/receiving data through WAN
	Off	Default – No Link



Port/Connector/Button	Description
SMA Antenna Connector	Wireless LAN Antenna connector
Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.
WPS Button	Push the WPS button implementation to reduce the network configuration steps, and also easy to implement network security.
LAN 1~4 Ports	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
WAN Port <u>(Data that going in from Modem)</u>	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.

Power	The power jack allows an external DC power supply connection.
--------------	---

1.5 Network + System Requirements

To begin using the RNX-N400LX, make sure you meet the following as minimum requirements:

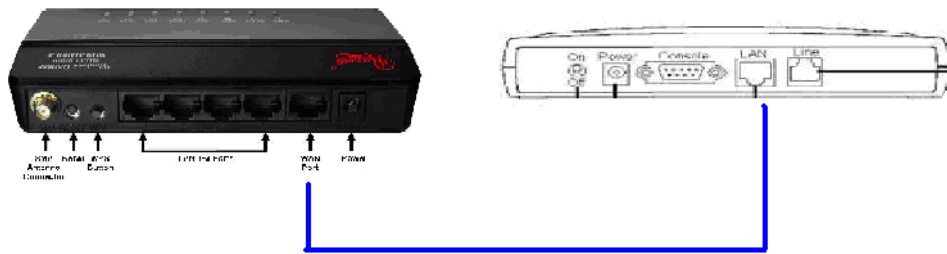
- PC/Notebook.
- Operating System that supports Web Browsers
 - Microsoft Windows
 - Mac OS
 - Linux
- 1 Free Ethernet port on your PC/NB
- WiFi card/USB dongle (802.11b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- Web-Browser (Internet Explorer, Safari, Firefox, Opera etc.)
- Ethernet compatible CAT5 cables.

1.6 RNX-N400LX Placement

RNX-N400LX is suggested to place on a flat surface, or you can mount it on a wall. However, for optimal performance, place your RNX-N400LX in the center of your office (or your home) that is away from any potential source of interference, such as a metal wall, microwave oven, and 2.4GHz cordless phone. If the antennas are not positioned correctly, performance loss may occur.

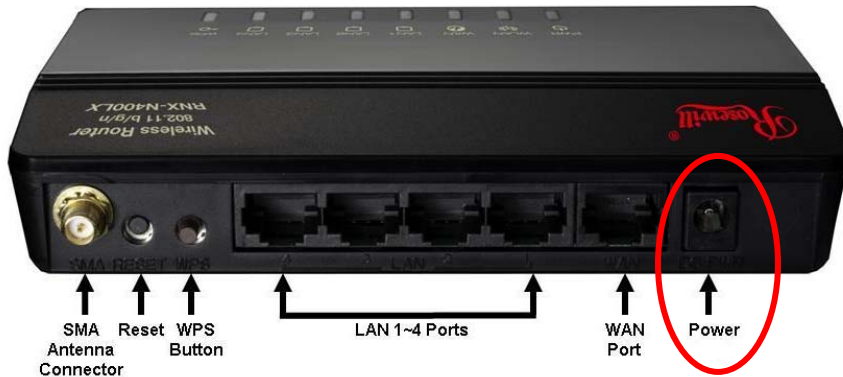
1.7 Hardware Setup

- Place the RNX-N400LX to the best optimum transmission location. The best transmission location for your RNX-N400LX is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.
- Connect RNX-N400LX to your wired network. Connect the Ethernet WAN interface of RNX-N400LX by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.



RNX-N400LX and Modem Rear View
(WAN Port and LAN port Connection diagram between Wireless Router, and Modem)

- Supply DC power to the RNX-N400LX. Use only the AC/DC power adapter supplied with the RNX-N400LX; it may cause damage by using a different voltage power adapter.



RNX-N400LX Rear View

- Connect Ethernet cable between your PC/Notebook LAN port & one of the 4 available LAN ports on RNX-N400LX.



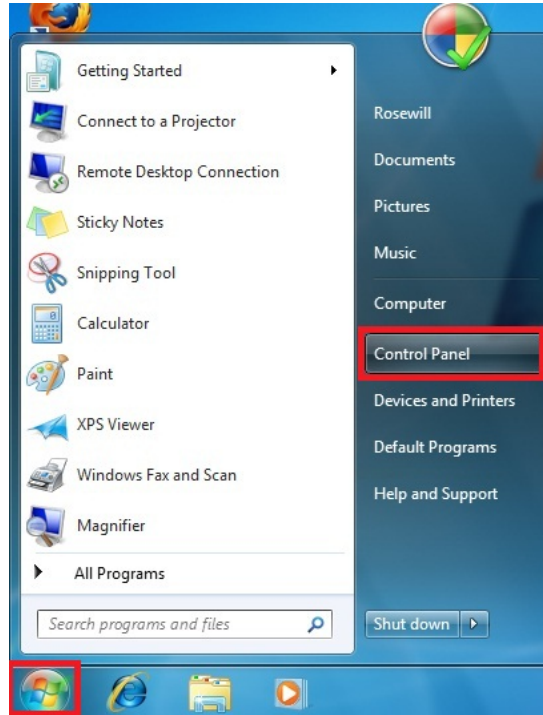
RNX-N400LX, PC, and Modem Rear View
(WAN Port and LAN port Connection diagram between PC, Wireless Router and Modem)

2 Setup

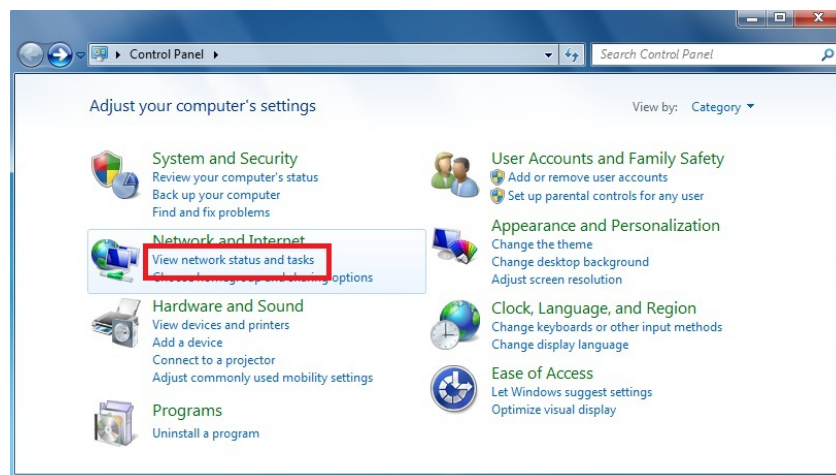
2.1 Prepare your PC for RNX-N400LX's configuration

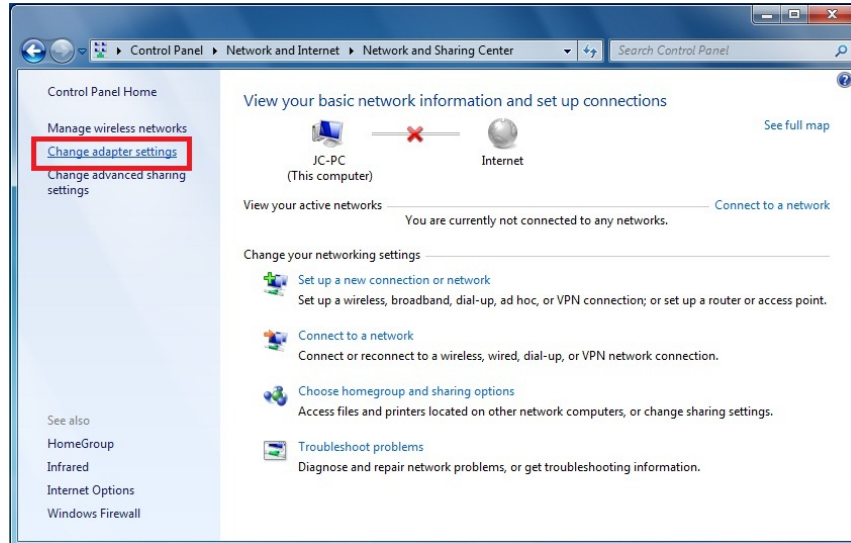
2.1.1 For OS of Microsoft Windows 7:

1. Click the **Start** button and select **Control Panel**. The **Control Panel** window will appear.

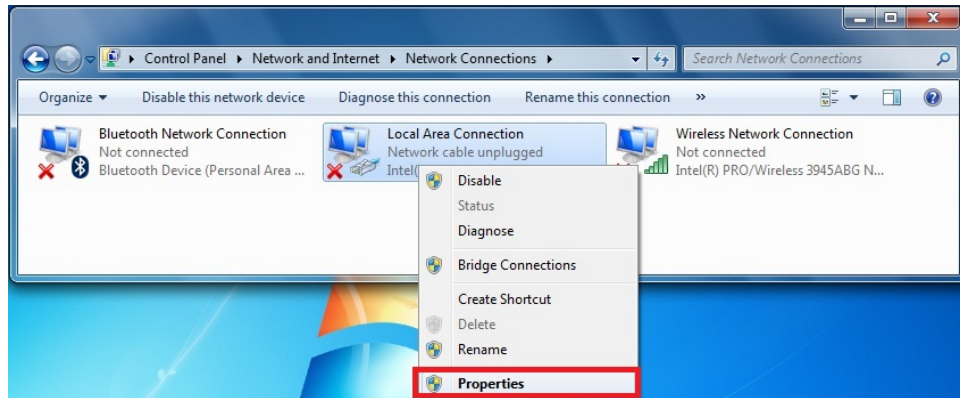


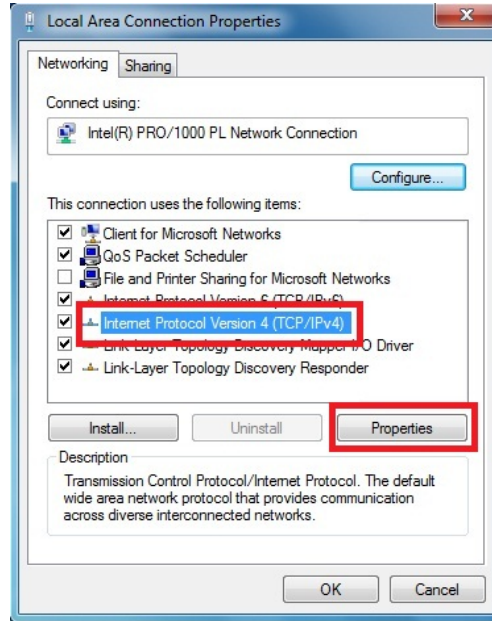
2. Move mouse and select **View network status and tasks** under **Network and Internet**. The **Network and Sharing Center** window will appear. Select **Change adapter settings**.





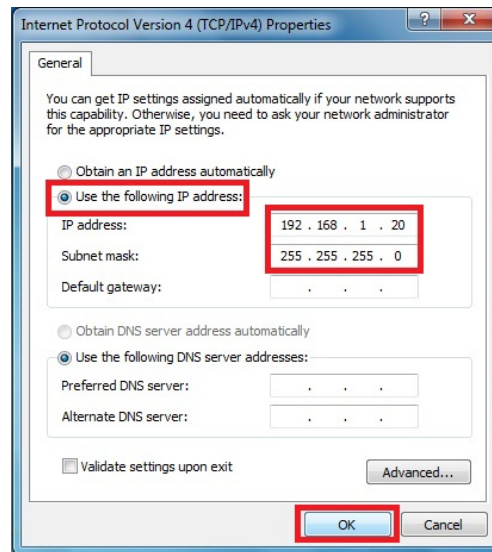
3. In **Network Connections** window, Mouse right click on **Local Area Connection** and select Properties, The **Local Area Connection Properties** window will popup. Move to choose **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties** button.





4. Move mouse and click **General** tab, Select **Use the following IP address** and type in values as following example.

- ✓ IP Address: **192.168.1.20**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
- ✓ IP Subnet Mask: **255.255.255.0**



5. Click **OK** to complete the IP parameters setting.

2.12 For OS of Microsoft Windows Vista:

1. Click the **Start** button and select **Settings**, then click **Control Panel**. The **Control Panel** window will appear.

2. Move mouse and double-click the right button on **Network Connections** item. The **Network Connections** window will appear. Double click **Local Area Connection** icon, then User Account Control window shown. Right click Continue button to set properties.
3. In **Local Area Connection Properties** window, Choose **Networking** tab, move mouse and click **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties** button.
4. Move mouse and click **General** tab, Select **Specify an IP address** and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
5. Click **OK** to complete the IP parameters setting.

2.13 For OS of Microsoft Windows 2000/ XP:

1. Click the **Start** button and select Settings, then click **Control Panel**. The **Control Panel** window will appear.
2. Move mouse and double-click the right button on **Network and Dial-up Connections** icon. Move mouse and double-click the **Local Area Connection** icon. The **Local Area Connection** window will appear. Click **Properties** button in the **Local Area Connection** window.
3. Check the installed list of **Network Components**. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
4. Select **Protocol** in the **Network Component Type** dialog box and click **Add** button.
5. Select **TCP/IP** in **Microsoft of Select Network Protocol** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to **Network** dialog box after the TCP/IP installation.
6. Select **TCP/IP** and click the properties button on the **Network** dialog box.
7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
8. Click **OK** to complete the IP parameters setting.

2.14 For OS of Microsoft Windows 95/ 98/ Me:

1. Click the **Start** button and select Settings, then click **Control Panel**. The **Control Panel** window will appear.
Note: Windows Me users may not see the Network control panel. If so, select **View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on **Network** icon. The **Network** window will appear.
3. Check the installed list of **Network Components**. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
4. Select Protocol in the Network Component Type dialog box and click Add button.
5. Select **TCP/IP** in **Microsoft of Select Network Protocol** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to **Network** dialog box after the TCP/IP installation.
6. Select **TCP/IP** and click the properties button on the **Network** dialog box.
7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
8. Click **OK** and reboot your PC after completes the IP parameters setting.

2.15 For OS of Microsoft Windows NT:

1. Click the **Start** button and select Settings, then click **Control Panel**. The **Control Panel** window will appear.
2. Move mouse and double-click the right button on Network icon. The Network window will appear. Click Protocol tab from the Network window.
3. Check the installed list of Network Protocol window. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.
4. Select Protocol in the Network Component Type dialog box and click Add button.
5. Select **TCP/IP** in **Microsoft of Select Network Protocol** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to **Network** dialog box after the TCP/IP installation.
6. Select **TCP/IP** and click the properties button on the **Network** dialog box.

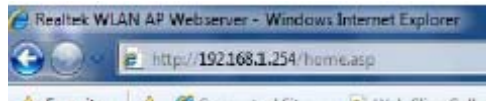
7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
8. Click **OK** to complete the IP parameters setting.

2.2 Connecting to RNX-N400LX's Web Management

You can use the web browser to enter into RNX-N400LX's setup page. Please connect RNX-N400LX with your computer and modem to start the setup process. (Instruction in 1.7 Hardware Setup)

2.21 Connecting using Web Browser:

RNX-N400LX's web management requires your web browser supports Java. (eg. Microsoft Internet Explorer 6.1 SP1 or above) Please open your desired Web browser, and type in `http://192.168.1.254` in the URL. You will be prompt to enter login name and password. Please use the default login and password for your first enter. (Login: admin; password: guest)



3 RNX-N400LX Web Management page

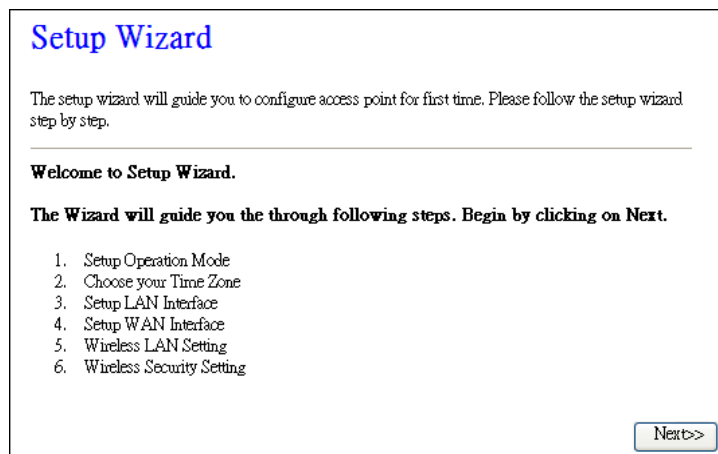
There are 7 major sections of RNX-N400LX which are **Setup Wizard**, **Operation Mode**, **Wireless**, **TCP/IP Settings**, **Firewall**, **QoS**, and **Management**.



3.1 Setup Wizard:

When you first connect to the web management page of RNX-N400LX, you will see the Setup Wizard page. It has the same setup steps as the Setup Wizard in your CD.

3.11 Welcome to Setup Wizard:



3.12 Operation Mode:

You can define your RNX-N400LX's Operation Mode in this step.

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
- Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

3.13 Time Zone Setting:

Here you can enable and configure whether to automatically update your time.

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

- Enable NTP client update**
- Automatically Adjust Daylight Saving**

Time Zone Select :

NTP server :

3.14 LAN Interface Setup:

You can setup the Local Area Network IP address and subnet mask.

3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:
 Subnet Mask:

3.15 WAN Interface Setup:

You can setup the WAN access type in this section by Static IP, DHCP, PPPoE, PPTP or L2TP.

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

3.16 Wireless Basic Setting:

This page is used to configure basic wireless parameters like Band, Mode, Network Type, SSID, Channel Number, Enable Mac Clone (Single Ethernet Client).

5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band:
 Mode:
 Network Type:
 SSID:
 Channel Width:
 ControlSideband:
 Channel Number:

Enable Mac Clone (Single Ethernet Client)

3.17 Wireless Security Setup:

You can set different encryption for your RNX-N400LX, either through **WEP**, **WPA**, and **WPA2**. Once complete, click **Finished** to complete the Setup Wizard.

6. Wireless Security Setup

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.

Encryption:

Key Length:

Key Format:

Key Setting:

3.2 Operation Mode:

Operation Mode is a quick setup on how you would like RNX-N400LX to perform as. You have the options Gateway, Bridge, and Wireless ISP.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
- Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Item	Description
Gateway	Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode
Bridge	Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
Wireless ISP	Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all router's functions
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous

configuration setting.

3.3 Wireless

You can set how your RNX-N400LX broadcast and how wireless LAN clients may connect to your RNX-N400LX.

3.3.1 Wireless Basic Settings:

Here you can change wireless encryption settings as well as wireless network parameters.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band:

Mode:

Network Type:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Broadcast SSID:

WMM:

Data Rate:

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

Item	Description
Disable Wireless LAN Interface	Click on to disable the wireless LAN data transmission.
Band	Click to select: 2.4GHz(B) 2.4GHz(G) 2.4GHz(N) 2.4GHz(B+G) 2.4GHz(G+N)

	2.4GHz(B+G+N)
Mode	Click to select: AP Client WDS AP+WDS wireless mode. (WDS Security Setting in 3.8) ** Please note change mode will result in around 1~3 minutes delay of internet connection due to system reboot and internet re-connects.
Network Type	While Mode is selected to be Client. Click to select the network type infrastructure or Ad hoc.
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Width	Select the operating channel width 20 MHz or 40 MHz. [N band only]
Control Sideband	Select the Sideband with Upper or Lower for channel width 40MHz. [N band only]
Channel Number	Select the wireless communication channel from pull down menu.
Broadcast SSID	Click to enable or disable the SSID broadcast function.
WMM	Click Enabled/Disabled to enable WMM feature.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS.
Associated Clients	Click the Show Active Clients button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Enable Mac Clone (Single Ethernet Client)	Take Laptop NIC MAC address as wireless client MAC address. [Client Mode only]
SSID of Extended	Click to enable Universal Repeater Mode
Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.32 Wireless – Advanced Setting

These settings are for technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your RNX-N400LX.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Preamble Type: Long Preamble Short Preamble

IAPP: Enabled Disabled

Protection: Enabled Disabled

Aggregation: Enabled Disabled

Short GI: Enabled Disabled

RF Output Power: 100% 70% 50% 35% 15%

Item	Description
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. This is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.
Preamble Type	Click to select the Long Preamble or Short Preamble support on the wireless data packet transmission. The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.
IAPP (Inter Access Point Protocol)	Click to enable or disable the IAPP function.
Protection	Protect 802.11n user priority.
Aggregation	Click to enable or disable the Aggregation function.
Short GI	Click to enable or disable the short Guard Intervals function.
RF Output Power	To adjust transmission power level.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.33 Wireless – Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, and WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

Wireless Security Setup

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.

Select SSID: Root AP - AP Apply Changes Reset

Encryption: WEP

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: *****

Item	Description
Select SSID	Select the SSID from multiple APs
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or WPA-Mixed.
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function
Authentication Type	Click to select the authentication type in Open System, Shared Key or Auto selection.
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as "WEP2") keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Encryption Key	Secret key of WEP security encryption function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).
WPA Cipher Suite	Select the Cipher Suite for WPA encryption. Either TKIP or AES encryption
WPA2 Cipher Suite	Select the Cipher Suite for WPA encryption. Either TKIP or AES encryption
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only]
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Enable Pre-	Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]

Authentication	
Authentication RADIUS Server	Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.34 Wireless – Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no other wireless clients will be able to connect if the list contains no entries.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: ▼

MAC Address: **Comment:**

Current Access Control List:

MAC Address	Comment	Select
00:02:72:81:86:01	PC-1	<input type="checkbox"/>
00:00:55:66:66:50	PC-2	<input type="checkbox"/>

Item	Description
Wireless Access Control Mode	Click the Disabled , Allow Listed or Deny Listed of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN Broadband Router.
MAC Address	Fill in the MAC address of client to register this WLAN Broadband Router access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this WLAN Broadband Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.35 Wireless – WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

Data Rate: ▼

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Item	Description
Enable WDS	Click the check box to enable wireless distribution system.
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Set Security	Click button to configure wireless security like WEP(64bits) , WEP(128bits) , WPA(TKIP) , WPA2(AES) or None
Show Statistics	It shows the TX, RX packets, rate statistics.
Delete Selected	Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.351 WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs.

WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:

WEP Key Format:

WEP Key:

Pre-Shared Key Format:

Pre-Shared Key:

3.352 WDS AP Table

This section will show you the WDS Statistics.

WDS AP Table

This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.

MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:02:72:81:86:0a	22	0	0	150
00:02:72:81:86:0b	22	0	0	150

Item	Description
MAC Address	It shows the MAC Address within WDS.
Tx Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Tx Errors	It shows the statistic count of error sent packets on the Wireless LAN interface.
Rx Packets	It shows the statistic count of received packets on the wireless LAN interface.
Tx Rate (Mbps)	It shows the wireless link rate within WDS.
Refresh	Click to refresh the statistic counters on the screen.
Close	Click to close the current window.

3.36 Wireless – Site Survey

You use this section to view or search to connect other Wireless Signal near yours. Under Client mode, you will see **Select** on the end which allows you to connect to that wireless signal.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal
TEST2-AP	00:1a:ef:01:01:01	7 (B+G)	AP	no	65
MyWLAN	00:1a:ef:00:b6:30	11 (B+G)	AP	WPA-PSK	55
Adam G.S	00:1a:ef:01:d1:20	11 (B+G)	AP	no	37
2F Ap	00:1a:ef:00:00:b7	1 (B+G)	AP	no	31
TEST1-AP	00:e0:4c:81:86:21	1 (B+G)	AP	no	23

Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Refresh	Click the Refresh button to re-scan site survey on the screen.
Connect	Click the Connect button to establish connection.

3.37 Wireless – WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize its setting and connect to the Access Point in a minute without any hassle.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number: 18864540

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

Item	Description
Disable WPS	Click on to disable the Wi-Fi Protected Setup function.
WPS Status	Show WPS status is Configured or Un-Configured .
Self-PIN Number	Fill in the PIN Number of AP to register the wireless distribution

	system access capability.
Push Button Configuration	The Start PBC button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Current Key Info	Authentication: It shows the Authentication is opened or closed. Encryption: It shows the Encryption mode. Key: It shows the Encryption key.
Client PIN Number	Fill in the Client PIN Number from your Client sites.

3.38 Wireless – Schedule

This section will help you set the wireless broadcast schedule. You will need to set System time before using this feature

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Enable Wireless Schedule

Days :

Everyday Sun Mon Tue Wed Thu Fri Sat

Time :

24 Hours From : To :

3.4 TCP/IP Settings:

This section allows you to set your Local Network IP address and how your RNX-N400LX connects to the internet via modem.

3.41 LAN Interface

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:
Subnet Mask:
Default Gateway:
DHCP:
DHCP Client Range: -
Static DHCP:
Domain Name:
802.1d Spanning Tree:
Clone MAC Address:

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
Default Gateway	Fill in the default gateway for LAN interfaces out going data packets.
DHCP	Click to select Disabled , Client or Server in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the Active DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]
Static DHCP	Select enable or disable the Static DHCP function from pull-down menu. [Server mode only]
Set Static DHCP	Manual setup Static DHCP IP address for specific MAC address. [Server mode only]
Domain Name	Assign Domain Name and dispatch to DHCP clients. It is optional field.
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be Cloned
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.411 Static DHCP Setup

Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Item	Description
IP Address	If you select the Set Static DHCP on LAN interface, fill in the IP address for it.
MAC Address	If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.
Comment	Fill in the comment tag for the registered Static DHCP.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Static DHCP List	It shows IP Address MAC Address from the Static DHCP.
Delete Selected	Click to delete the selected clients that will be removed from the Static DHCP list.
Delete All	Click to delete all the registered clients from the Static DHCP list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.42 WAN Interface Setup

This part is used to configure the parameters for wide area network that connects to the WAN port of your WLAN Broadband Router. Here you may change the access method to **Static IP**, **DHCP**, **PPPoE** or **PPTP** by click the item value of **WAN Access Type**.

3.421 WAN Interface Setup - Static IP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

IP Address:

Subnet Mask:

Default Gateway:

MTU Size: (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Item	Description
Static IP	Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets.
MTU Size	Fill in the MTU size of MTU Size. The default value is 1400.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN Connection	Click the checkbox to enable IPsec packet pass through.
Enable PPTP pass through on VPN Connection	Click the checkbox to enable PPTP packet pass through.
Enable L2TP pass through on VPN Connection	Click the checkbox to enable L2TP packet pass through.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.422 WAN Interface Setup – DHCP client

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

Host Name:

MTU Size: (1400-1492 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Item	Description
DHCP Client	Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.
Host Name	Fill in the host name of Host Name. The default value is empty.
MTU Size	Fill in the MTU size of MTU Size. The default value is 1400.

Attain DNS Automatically	Click to select getting DNS address for DHCP support. Please select Set DNS Manually if the DHCP support is selected.
Set DNS Manually	Click to select getting DNS address for DHCP support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN Connection	Click the checkbox to enable IPsec packet pass through.
Enable PPTP pass through on VPN Connection	Click the checkbox to enable PPTP packet pass through.
Enable L2TP pass through on VPN Connection	Click the checkbox to enable L2TP packet pass through.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.423 WAN Interface Setup – PPPoE

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

Host Name:

MTU Size: (1400-1492 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Item	Description
PPPoE	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Password	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Service Name	Fill in the service name of Service Name. The default value is empty.
Connection Type	<p>Select the connection type from pull-down menu. There are Continuous, Connect on Demand and Manual three types to select.</p> <p>Continuous connection type means to setup the connection through PPPoE protocol whenever this WLAN AP Router is powered on.</p> <p>Connect on Demand connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog</p>

	<p>implemented to close the PPPoE connection while there are no data sent out longer than the idle time set.</p> <p>Manual connection type means to setup the connection through the PPPoE protocol by clicking the Connect button manually, and clicking the Disconnect button manually.</p>
Idle Time	If you select the PPPoE and Connect on Demand connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400.
Attain DNS Automatically	Click to select getting DNS address for DHCP support. Please select Set DNS Manually if the DHCP support is selected.
Set DNS Manually	Click to select getting DNS address for DHCP support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN Connection	Click the checkbox to enable IPsec packet pass through.
Enable PPTP pass through on VPN Connection	Click the checkbox to enable PPTP packet pass through.
Enable L2TP pass through on VPN Connection	Click the checkbox to enable L2TP packet pass through.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.424 WAN Interface Setup – PPTP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

IP Address:

Subnet Mask:

Server IP Address:

User Name:

Password:

MTU Size: (1400-1460 bytes)

Request MPPE Encryption

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP

Enable IGMP Proxy

Enable Ping Access on WAN

Enable Web Server Access on WAN

Enable IPsec pass through on VPN connection

Enable PPTP pass through on VPN connection

Enable L2TP pass through on VPN connection

Item	Description
PPTP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.
Enable Dynamic Mode	Click to select PPTP Dynamic support on WAN interface for IP address assigned automatically from a PPTP server.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Gateway	If you select the Static PPTP support on WAN interface, fill in the gateway for WAN interface out going data packets.

Server IP Address	Enter the IP address of the PPTP Server.
Server Domain Name	Assign Domain Name and dispatch to PPTP servers. It is optional field.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400.
Request MPPE Encryption	Click the checkbox to enable request MPPE encryption.
Attain DNS Automatically	Click to select getting DNS address for DHCP support. Please select Set DNS Manually if the DHCP support is selected.
Set DNS Manually	Click to select getting DNS address for DHCP support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN Connection	Click the checkbox to enable IPsec packet pass through.
Enable PPTP pass through on VPN Connection	Click the checkbox to enable PPTP packet pass through.
Enable L2TP pass through on VPN Connection	Click the checkbox to enable L2TP packet pass through.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

Note: PPTP Gateway:

Your ISP will provide you with the Gateway IP Address. If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have PPTP gateway then enter the ISP's Gateway IP address above.

3.5 Firewall:

This part provides you with abilities to control the security of your network.

3.51 Firewall - Port Filtering

Port filtering is used to restrict the flow of data packets flow by controlling different ports from your local network to Internet through this router. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
20-21	TCP+UDP	FTP	<input type="checkbox"/>
5900	TCP+UDP	realvnc	<input type="checkbox"/>

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range Protocol Comments	To restrict data transmission from the local network on certain ports, fill in the range of start-port and endport, and the protocol, also put your comments on it. The Protocol can be TCP, UDP or Both. Comments let you know about whys to restrict data from the ports.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.52 Firewall - IP Filtering

IP filtering is used to restrict the flow of data packets flow by controlling the IP from your local network to Internet through this router. Use of such filters can be helpful in securing or restricting your local network.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address: Protocol: Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.1.9	TCP+UDP	office	<input type="checkbox"/>
192.168.1.10	TCP+UDP	PC	<input type="checkbox"/>

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address Protocol Comments	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol; also put your comments on it. The Protocol can be TCP, UDP or Both. Comments let you know about whys to restrict data from the IP address.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.53 Firewall - MAC Filtering

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address: **Comment:**

Current Filter Table:

MAC Address	Comment	Select
00:1a:4d:40:ad:7f	test pc	<input type="checkbox"/>

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address Comments	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. Comments let you know about whys to restrict data from the MAC address.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.54 Firewall – Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some port of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address: Protocol: Port Range: - Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.1.7	TCP+UDP	5900	realvnc	<input type="checkbox"/>
192.168.1.7	TCP+UDP	5631-5632	pcanywhere	<input type="checkbox"/>

Item	Description
Enable Port Forwarding	Click to enable the Port Forwarding security function.
Local IP Address Protocol Port Range Comment	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments. The Protocol can be TCP, UDP or Both. The Port Range for data transmission. Comments let you know about whys to allow data packets forward to the IP address and port number.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.55 Firewall – URL Filtering

URL Filtering can help to restrict users from access specific websites by blocking the address.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL Filtering

URL Address:

Apply Changes

Reset

Current Filter Table:

URL Address	Select
www.google.com.tw	<input type="checkbox"/>
www.yahoo.com.tw	<input type="checkbox"/>
www.msn.com.tw	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address. (Please enter complete URL address; eg. www.xxxxx.com)
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.56 Firewall – DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ

DMZ Host IP Address:

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.6 QoS:

QoS function helps to improve your online experience by ensuring that your set traffic is prioritized over other network traffic, such as gaming traffic over FTP or Web.

QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps):

QoS Rule Setting:

Address Type: IP MAC

Local IP Address: -

MAC Address:

Mode:

Bandwidth (Kbps):

Comment:

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Bandwidth	Comment	Select
192.168.1.2 - 192.168.1.200	----	Guaranteed minimum bandwidth	512		<input type="checkbox"/>

Item	Description
Enable QoS	Click to enable the QoS function.
Automatic Uplink Speed	Enable to allow RNX-N400LX to automatically adjust the upload speed
Manual Uplink Speed (Kbps)	If not enable automatic uplink speed, you will need to assign an upload speed.
Address Type	Select what will your network be control by. Either through IP or MAC
Local IP Address	If select to control by IP, you will need to provide a range of the IP which you want to use QoS functions.
MAC Address	If select to control by MAC, you will need to provide MAC address which you want to use QoS functions.
Mode	You will have two options; either by Guaranteed Minimum Bandwidth or by Restricted Maximum Bandwidth .
Bandwidth (kbps)	You can set the actual controlled bandwidth under either the minimum or Maximum bandwidth.
Comments	You can put your comments here to help manage this rule.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.7 Management:

Management section helps you with overall RNX-N400LX setup including a brief overview on Status, traffic statistics, DDNS, Denial of Service and others which can help you utilizing and managing RNX-N400LX better.

3.71 Management – Status

Status shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	1day:1h:14m:4s
Firmware Version	v1.3
Build Time	Thu Apr 30 16:45:15 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Rosenn111-N400LX
Channel Number	7
Encryption	Disabled
BSSID	00:e0:4c:81:96:b1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:b1
WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	59.115.129.197
Subnet Mask	255.255.255.255
Default Gateway	61.230.48.254
MAC Address	00:e0:4c:81:96:b9

Item	Description
System	
Uptime	It shows the duration since WLAN AP Router is powered on.
Firmware version	It shows the firmware version of WLAN AP Router.
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN AP Router. The SSID is the unique name of WLAN AP Router and shared among its service area, so all device sat tempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function
Associated Clients	It shows the number of connected clients (or station, PCs).
BSSID	It shows the BSSID address of the WLAN AP Router. BSSID is a six-byte address.
LAN configuration	
IP Address	It shows the IP address of LAN interfaces of WLAN AP Router.

Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN AP Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of WLAN AP Router.
WAN configuration	
Attain IP Protocol	It shows how the WLAN AP Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.
IP Address	It shows the IP address of WAN interface of WLAN AP Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN AP Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of WLAN AP Router.

3.72 Management – Statistics

This section shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	<i>Sent Packets</i>	8079
	<i>Received Packets</i>	39832
Ethernet LAN	<i>Sent Packets</i>	0
	<i>Received Packets</i>	3
Ethernet WAN	<i>Sent Packets</i>	1274
	<i>Received Packets</i>	3657

3.73 Management – DDNS

This section can help to configure Dynamic DNS service to have DNS with dynamic IP address.

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : DynDNS

Domain Name : host.dyndns.org

User Name/Email:

Password/Key:

Note:

For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)

For DynDNS, you can create your DynDNS account [here](#)

Apply Change

Reset

Item	Description
Enable DDNS	Click the checkbox to enable DDNS service.
Service Provider	Click the drop down menu to pickup the right provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.74 Management – Time Zone Setting

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2008 Mon 8 Day 25 Hr 21 Mn 50 Sec 20

Time Zone Select : (GMT+08:00)Taipei

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server : 192.5.41.41 - North America

(Manual IP Setting)

Apply Change

Reset

Refresh

3.75 Management – Denial-of-Service

A **denial-of-service attack (DoS attack)** is an attempt to make a computer resource unavailable to its intended users. You can use this part to enable and setup protection to prevent attack by hacker’s program. This provides more security for users.

Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DoS Prevention

- Whole System Flood: SYN Packets/Second
- Whole System Flood: FIN Packets/Second
- Whole System Flood: UDP Packets/Second
- Whole System Flood: ICMP Packets/Second
- Per-Source IP Flood: SYN Packets/Second
- Per-Source IP Flood: FIN Packets/Second
- Per-Source IP Flood: UDP Packets/Second
- Per-Source IP Flood: ICMP Packets/Second
- TCP/UDP PortScan Sensitivity
- ICMP Smurf
- IP Land
- IP Spoof
- IP TearDrop
- PingOfDeath
- TCP Scan
- TCP SynWithData
- UDP Bomb
- UDP EchoChargen

Enable Source IP Blocking Block time (sec)

Item	Description
Enable DoS Prevention	Click the checkbox to enable DoS prevention
Whole System Flood / Per-Source IP Flood...	Enable and setup prevention in details.
Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.

3.76 Management – Log

Log function provides option for you to store what happen to your router.

System Log

This page can be used to set remote log server and show the system log.

Enable Log

system all
 wireless
 DoS

Enable Remote Log
 Log Server IP Address:

```

Oday 07:37:21 br0: port 4(wlan0-wds1) entering learning state
Oday 07:37:21 br0: port 4(wlan0-wds1) entering forwarding state
Oday 07:37:21 br0: topology change detected, propagating
Oday 07:37:21 br0: port 1(eth0) entering listening state
Oday 07:37:21 br0: port 3(wlan0-wds0) entering learning state
Oday 07:37:21 br0: port 3(wlan0-wds0) entering forwarding state
Oday 07:37:21 br0: topology change detected, propagating
Oday 07:37:21 br0: port 1(eth0) entering learning state
Oday 07:37:21 br0: port 1(eth0) entering forwarding state
Oday 07:37:21 br0: topology change detected, propagating
Oday 07:42:18 wlan0: A wireless client (00:E0:4C:01:04:12) was rejected due to
access control for 152 times in 5 minutes
Oday 07:47:18 wlan0: A wireless client (00:E0:4C:01:04:12) was rejected due to
access control for 64 times in 5 minutes
          
```

Item	Description
Enable Log	Click the checkbox to enable log.
System all	Show all log of wireless broadband router.
Wireless	Only show wireless log
DoS	Only show Denial-of-Service log
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP Address	Input the remote log IP address.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen.

3.77 Management – Upgrade Firmware

You can upgrade the Access Point firmware to new version. **Please note, do not power off the device during the upload because it may crash the system.**

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

3.78 Management – Save/Reload Settings

You can save current settings to a file or reload the settings from the file that was previously saved. Besides, you could reset the current configuration to factory default.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

3.79 Management – Password

This page is used to set the account to access the web server of Access Point.

Empty user name and password will disable the protection.

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

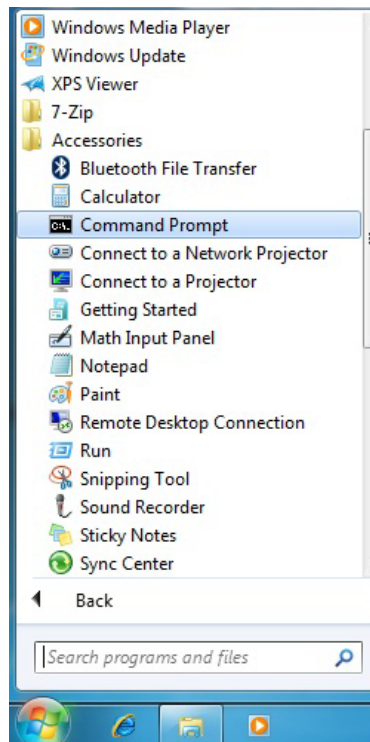
Appendix A – FREQUENTLY ASKED QUESTIONS (FAQ)

1. What is and how to find my Computer's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address. The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

1. Open the DOS Command program in the Microsoft Windows.



2. Type in ipconfig /all then press the Enter button.

```

C:\Users>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Q2-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : wlanrouter

Wireless LAN adapter Wireless Network Connection 3:

Connection-specific DNS Suffix . . : wlanrouter
Description . . . . . : 802.11n USB Wireless LAN Card #2
Physical Address. . . . . : 00-02-6F-51-8E-FC MAC Address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::396f:d9b5:81e6:bhbc%18 (Preferred)
IPv4 Address. . . . . : 192.168.0.102 (Preferred) IP Address
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 16, 2009 8:40:33 AM
Lease Expires . . . . . : Monday, October 14, 2019 8:40:33 AM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 Iaid . . . . . : 352322159
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-5C-7D-A3-00-16-41-AA-D6-2D

DNS Servers . . . . . : 192.168.0.1
Primary WINS Server . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 00-16-CE-E6-C7-FB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

```

3. Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Address.

2. What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

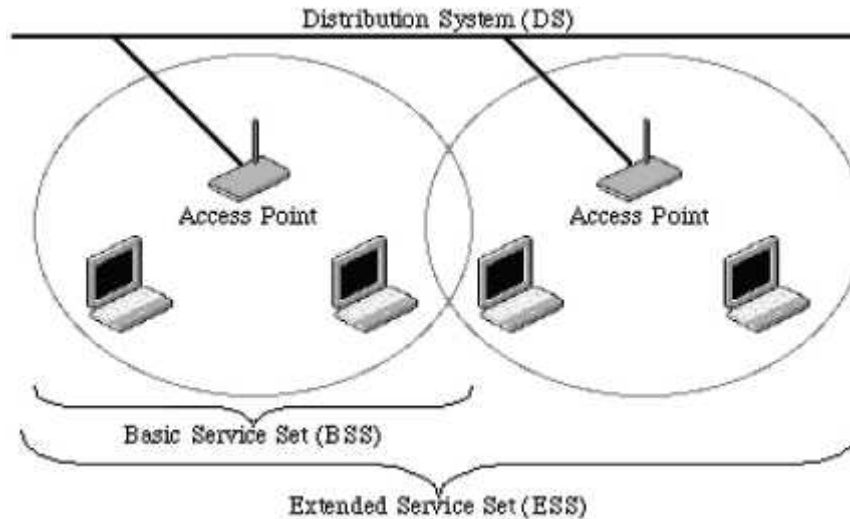
3. What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4. How does wireless networking work?

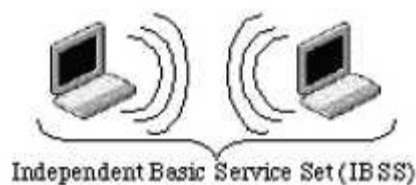
The 802.11 standard define two modes: **Infrastructure mode** and **Ad hoc mode**. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration

is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single sub-network. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

5. What is BSSID?

BSSID is a six-byte address that distinguishes a particular access point from others. **BSSID** also known as SSID which serves as a network ID or name.

6. What is ESSID?

The Extended Service Set ID (**ESSID**) is the name of the network you want to access. It is used to identify different wireless networks.

7. What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture... etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences

- Minimizing the number of walls and ceilings that wireless signal has to go through
- Position the WLAN antenna for best reception.
- Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors ... etc.
- Add additional WLAN Access Points if necessary.

8. What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

9. What is WEP?

WEP is an optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy (WEP) generates secret shared

encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers. WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

10. What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

11. What is RTS (Request to Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/ CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. This setting is useful for networks with many clients. With many clients, and a high network load, there will be

many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

12. What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion. Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

13. What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

14. What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point. Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

15. What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access. To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

16. What is WPA2?

It is the second generation of WPA which based on the final IEEE 802.11i amendment to the 802.11 standard.

17. What is 802.1x Authentication? Protocol (TKIP)?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284. Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

18. What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol (TKIP), pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

19. What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next generation cryptography algorithm, which will replace DES and 3DES.

20. What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet. IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

21. What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

22. What is Universal Plug and Play (UPnP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

23. What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

24. What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients

will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

25. What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for users who own the DNS server to utilize dynamic WAN IP address.

26. What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

27. What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to-point private link via shared or public network.

28. What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

29. What is WLAN Block Relay between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an Access Point (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

30. What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a

wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

31. What is WLAN ACK TIMEOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

32. What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of an AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

33. What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

34. What is Guard Intervals (GI)?

A GI is a period of time between symbol transmissions that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol. The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.

Appendix B – Product Specification

Hardware Feature

Dimensions (L x W x H)	146 x 100 x 24 (mm); 5.74" x 3.93" x 0.94"
Physical Interface	<p>WAN: 10/100 Fast Ethernet RJ-45 x 1</p> <p>LAN: 10/100 Fast Ethernet RJ-45 x 4</p> <p>Reset button</p> <p>Power Jack</p> <p>WPS button (WiFi Protected Setup)</p>
LEDs Status	<p>Power Status</p> <p>WAN (Internet connection)</p> <p>10/100Mbps LAN1~LAN4</p> <p>WLAN (Wireless connection)</p> <p>WPS</p>
Power Requirements	<p>Power Supply: 200 to 240 VDC \pm 10% (ETSI) 100 to 120 VDC \pm 10% (FCC)</p> <p>Device: 12V DC/1A</p>
Reset Button	The reset button is built into the rear panel. Use this button to restore the RNX-N400LX to its factory default settings. Press for 1 second to restart the device. Continuously press for 10 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Environment	<p>Temperature Range</p> <p>0 to 60°C - Operating, (32°F~140°F)</p> <p>Humidity (non-condensing)</p> <p>10% ~90% typical</p>

Appendix C – FCC Interference Statement

Federal Communication Commission Interference 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 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: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

- . In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- . In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- . In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Italian:

In alcuni Paesi si applicano i requisiti per il funzionamento in interni-esterni, i requisiti di licenza e i canali consentiti, come descritto si seguito:

- In Italia l'utente finale deve richiedere una licenza all'Autorità competente nazionale per il funzionamento in esterni del device.

Dutch:

Vereisten voor werking indoor versus outdoor, licentie vereisten en toegestane kanalen voor gebruik zijn van toepassing in bepaalde landen zoals hieronder beschreven.

- In België is outdoor gebruik enkel toegestaan gebruik makend van de 2.46 - 2.4835 GHz band: Kanaal 13.

French:

Conditions requises pour des installations intérieures ou extérieures, licences requises et canaux autorisés dans certains pays comme décrits ci-dessous:

- En Belgique, l'installation extérieure est seulement autorisée sur la bande 2.46 - 2.4835 GHz:: Canal 13
- En France, l'installation extérieure est seulement autorisée sur la bande 2.4 2.454 GHz : Canal 1-7

Appendix D – IC Interference Statement

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Thank you for purchasing a quality Rosewill Product.

Please register your product at: www.rosewill.com for complete warranty information and future support for your product.