R-300NP Wireless Router

User Manual

無線路由器(WIFI)

Handlink

Handlink Technologies Inc.

6830607-0010G EN V1.0

Copyright Notice

Disclaimer

We shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from furnishing this material, or the performance or use of this product. We reserve the right to change the product specification without notice. Information in this document may change without notice.

Trademarks

Microsoft Win98, Windows 2000 , WinXP, Win Vista and Win7 are registered trademarks of Microsoft Corporation.

General: All other brand and product names mentioned herein may be registered trademarks of their respective owners. Customers should ensure that their use of this product does not infringe upon any patent rights. Trademarks mentioned in this publication are used for identification purposes only and are properties of their respective companies.

Table of Contents

1 Introduction -- 5

1-1 Package Contents -- 5

1-2 Features -- 5

1-3 Precautions --- 5

1-4 Outlook-- 6

1-4-1 Front Panel --- 6

1-4-2 Rear Panel-- 7

1-5 Technical Specifications -- 8

1-5-1 Hardware Specifications -- 8

1-5-2 Software Specifications --10

2 Installation --12

2-1 Installation Requirements---12

2-2 Hardware Setup ---13

3. Configuring the R-300NP ---14

3-1 Wizard Setup---14

3-2 Advanced Setup---22

3-2-1 System---23

3-2-2 WAN/LAN --25

3-2-3 Server ---31

3-2-4 Authentication--32

3-2-5 Bandwidth--32

3-2-6 Filtering ---34

3-2-7 Port forwarding ---36

3-2-8 Syslog---36

3-2-9 Session Trace ---40

3-2-10 SNMP ---42

3-2-11 Wireless --43

3-2-12 Firewall ---47

3-3 System Status ----------49

3-3-1 System----------49

3-3-2 Current User ----------51

3-3-3 DHCP Clients ----------52

3-3-4 Session List ----------52

3-4 System Tools----------52

3-4-1 Configuration----------53

3-4-2 Firmware ----------54

3-4-3 System Account ----------56

3-4-4 PING Command----------56

3-4-5 Restart ----------57

3-4-6 Logout ----------57

Appendix A Regulations/EMI Compliance ----------58

Appendix D LIMITED WARRANTY ----------60

1 Introduction

R-300NP is the best WiFi solution provider for venue owner and its customers. Using our system, the venue owner could be able to provide the free WiFi service that is safe and legally compliant. The Venue Owner can use R-300NP and Coolbee WiFi service to promote the store to customer.

1-1 Package Contents

Please inspect your package. The following items should be included:

- One R-300NP
- One Power Adapter
- Two detachable Antennas
- One Ethernet Cable
- One Quick Installation Guide
- One Wi-Fi sticker

If any of the above items are damaged or missing, please contact your dealer immediately.

1-2 Features

- Wireless data rates up to 300Mbps
- IP Plug and Play (iPnP)
- Comprehensive security

  64/128-bit WEP encryption

  WPA encryption

  WPA2 Encryption

  IP/URL filtering
- Intelligent Management

Note: *The "iPnP" Function only can be used with TCP/IP-based Network.*

1-3 Precautions

- Never remove or open the cover.
- Never install the system in the wet locations.
- Use only the original fitting power adapter otherwise there is a danger of severe electrical shock.
- Avoid exposing the R-300NP to direct sunlight or another heat source.
- Choose a well-ventilated area to position your R-300NP.

1-4 Outlook

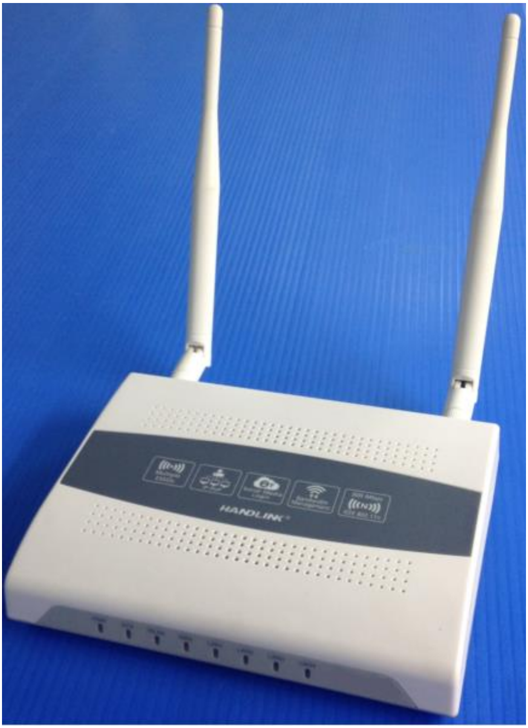


Figure 1 Outlook

1-4-1 Front Panel

The front panel of the R-300NP is shown as below.

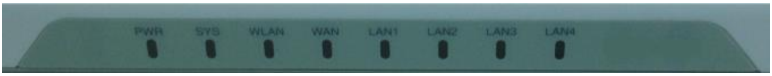


Figure 2 Front Panel

LED Indicators

LED	State	Description
PWR	Off	The device is not receiving electrical power.
	On	The device is receiving electrical power.
SYS	Off	The device status is defective.
	On	The device is up and running.

	Blinking	During firmware upgrade, the system LED will be blinking.
WLAN	Off	The Wireless is not ready.
	On	The device has established a valid wireless connection.
	Blinking	The Wireless connection is active.
WAN	Off	The WAN is not connected.
	On	The WAN has a valid 10/100Mbps network connection.
	Blinking	The WAN is sending or receiving packet.
LAN-1~ **LAN-4**	Off	The LAN is not connected.
	On	The LAN has a valid 10/100Mbps network connection.
	Blinking	The LAN is sending or receiving packet.

1-4-2 Rear Panel

The rear panel of R-300NP is shown as below.

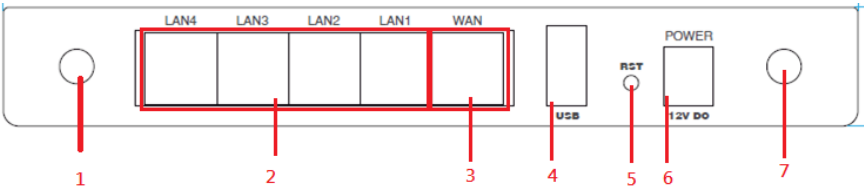


Figure 3 R-300NP Rear Panel

1. Antenna

2. LAN Ports (1-4)

3. WAN/PoE port

4. USB

5. Reset

6. Power jack

7. Antenna

The rear panel of WG-701/WG-606 is shown as below.

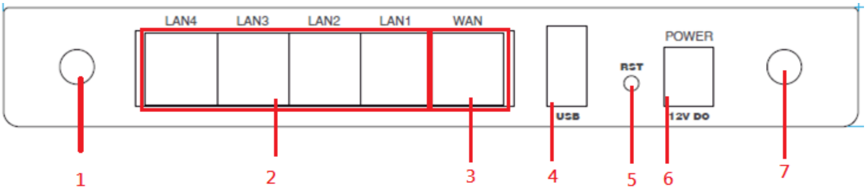


Figure 4 R-300NP Rear Panel

1. Antenna

2. LAN Ports (1-4)

3. WAN Port

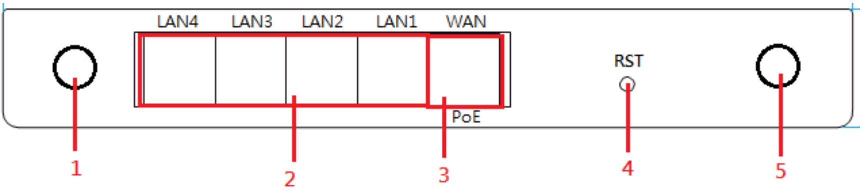
4. USB

5. Reset

6. Power jack

7. Antenna

The rear panel of AP-300NP is shown as below.



1. Antenna

2. LAN Ports (1-4)

3. WAN/PoE Port

4. Reset

5. Antenna

1-5 Technical Specifications

1-5-1 Hardware Specifications

Network Specification

IEEE802.3 10BaseT Ethernet

IEEE802.3u 100BaseTX Fast Ethernet

IEEE802.11g Wireless LAN

ANSI/IEEE 802.3 NWay auto-negotiation

Wi-Fi Compatible

Connectors

Four LAN Ports (10BaseT/100BaseTX Auto cross-over)

One WAN Port (10BaseT/100BaseTX Auto cross-over)

External Antenna Type

4dBi (Max) Dual detachable diversity antenna with reverse SMA

LED Indicators

One POWER LED

One WAN 10/100M Link/Activity LED

Four LAN 10M/100M Link/Activity LEDs

One Wireless Link/Activity LED

One System LED

Power Requirement

R-300NP:

External Power Adapter:

Power input: 12V, 1A

Power consumption: Under 5 Watts

PoE:

Power input: 48Vdc, 0.4A, IEEE 802.3at Compliance

Power consumption: Under 5 Watts

WG-701:

External Power Adapter:

Power input: 12V, 1A

Power consumption: Under 5 Watts

WG-606:

External Power Adapter:

Power input: 12V, 1A

Power consumption: Under 5 Watts

AP-300NP:

PoE:

Power input: 48Vdc, 0.4A, IEEE 802.3at Compliance

Power consumption: Under 5 Watts

Environment Conditions

Operating Temperature: 0 to 40°C

Storage Temperature: -10 to 60°C

Operating Humidity: 10~90% non-condensing

Storage Humidity: 10% to 90% non-condensing

Certifications

FCC,CE,NCC, BSMI,NTC(Thailand)

Dimension

Size:222 (L) x 143 (W) x 36 (H) mm

Weight: About 400 g (Net)

Mounting

Desktop, Wall mounted

1-5-2 Software Specifications

Networking

- IP Plug and Play (iPnP)
- WEP 64/128bit
- WPA-PSA (TKIP)
- WPA2-PSK(AES)
- WPA/WPA2 Mix Mode-PSK (AES)
- DHCP Server (RFC 2131)
- Static IP WAN Client
- DHCP WAN Client
- PPPoE WAN Client (RFC 2516)
- PPTP WAN Client
- NAT (RFC 1631)
- NTP (Network Time Protocol) Support

Wireless

- Wireless IEEE802.11n

User Authentication

- Facebook Authentication
- Access Form

Security and Firewall

- Layer 2 Isolation
- SSL Administration
- VPN Pass through (IPSec/PPTP/L2TP)
- Pass through Destination IP/URL
- Pass through Source IP/MAC
- Restricted Destination Filtering IP/URL
- Anti-DDOS

Management

- Administrator / Front Desk Access Management
- Access Control List Management (ACL)
- Remote Browser-based Configuration and management
- Firmware Upgrade (RFC 1350) via HTTP/TFTP
- Backup/Restore/Factory Default Setting
- Port Forwarding

- System Information Table
- Real-time Current User List / DHCP Clients List /
- Session List / Account List
- Syslog
- Bandwidth control per device
- Session control per device
- Session Trace
- SNMP (Read Only)
- Ping Command

2 Installation

The followings are instructions for setting up the R-300NP. Refer to the illustration and follow the simple steps below to quickly install your R-300NP.

2-1 Installation Requirements

Before installing the R-300NP, make sure your network meets the following requirements.

The R-300NP requires one of the following types of software:

- Windows XP/Vista/7
- Red Hat Linux 7.3 or later version
- MAC OS X 10.2.4 or later version
- Web Browser Software (Microsoft I.E or Firefox , Google Chrome)
- One computer with an installed 10Mbps, 100Mbps or 10/100Mbps Ethernet card
- UTP network Cable with a RJ-45 connection (Package contents)

Note:

1. The gateway’s default IP address setting is “10.59.1.1”.

2. The gateway’s default subnet mask setting is “255.255.255.0”.

2-2 Hardware Setup

1. Connect the R-300NP WAN port to modem by Ethernet cable.(Usually, the ISP will provide one Ethernet cable along with the modem)

2. Connect the R-300NP LAN port to PC by Ethernet cable.

3. Install the antennas.

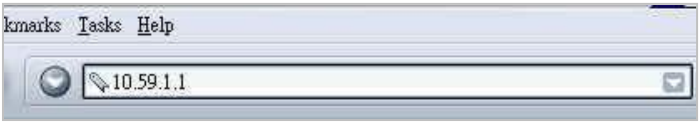
4. Plug in the power adapter. The R-300NP will be booted once the power is connected.

5. Check the LED status of SYS, WAN, LAN and WLAN, the network connection is valid if the LED turned on.

3. Configuring the R-300NP

3-1 Wizard Setup

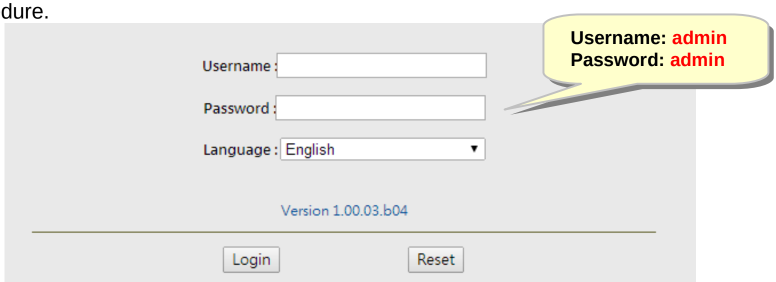
Step 1: Open your browser, and then enter the factory default IP address **10.59.1.1** in your browser's location box. Press **Enter**.



10.59.1.1

Figure 5 Web Browser

Step 2: The R-300NP login page will appear. Typing the factory default Username "**admin**" and Password "**admin**" then click **Login**. If you are first time setting the system, the wizard setup screen will appear as figure 7. You will be guided, step-by-step, through a basic setup procedure.


Username:

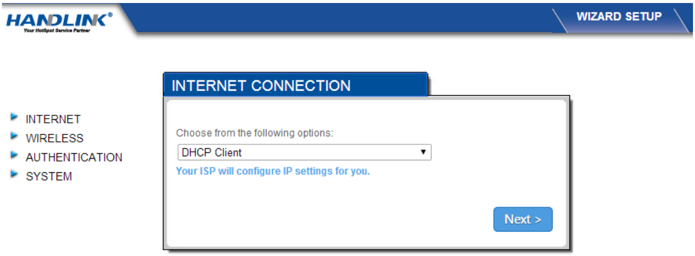
Password:

Language: English

Version 1.00.03.b04

Username: admin
Password: admin

Figure 6 R-300NP login page



Choose from the following options:

DHCP Client

Your ISP will configure IP settings for you.

Figure 7 Wizard Setup Screen

Note:

☞ *This Web agent is best viewed with IE 9.0 or Chrome and above browsers.*

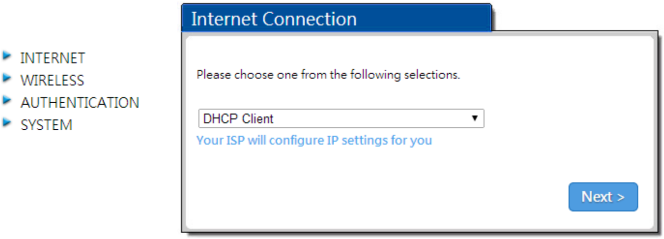
☞ *Username and Password can consist of up to 20 alphanumeric characters and are case sensitive.*

☞ *If for some reason your password is lost or you cannot gain access to the R-300NP Configuration Program, please press the reset button to load the device to manufacturer defaults.*

☞ *If the R-300NP doesn't send packet in 5 minutes (default), the R-300NP wills logout automatically.*

Step 3: Internet Connection Setting

Select the appropriate Internet connection type to connect to your ISP.



Please choose one from the following selections.

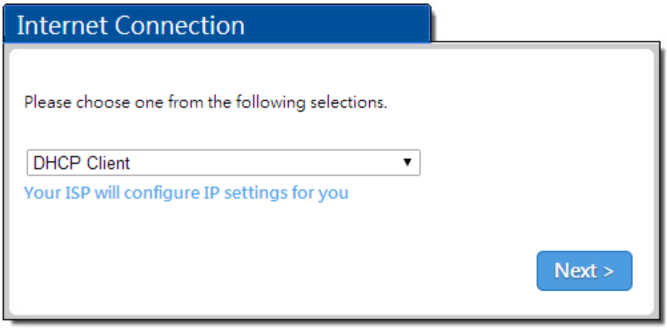
DHCP Client

Your ISP will configure IP settings for you

Figure 8 Internet Connection Setting Screen

- **DHCP Client**

The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your ISP. If your xDSL/Cable comes with this feature, please enable Use DHCP Client.



Please choose one from the following selections.

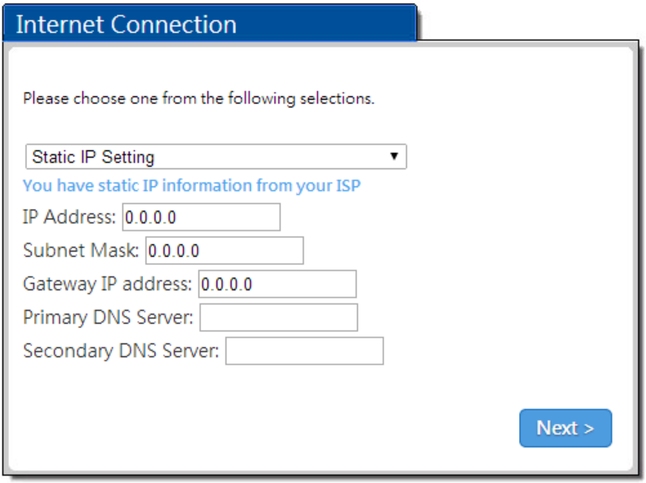
DHCP Client

Your ISP will configure IP settings for you

Figure 9 Internet Connection Setting Screen—DHCP Client Setting

- **Static IP Setting**

If **Static IP Setting** is selected, below setting screen will appear. Enter the IP address information provided by your ISP.



Internet Connection

Please choose one from the following selections.

Static IP Setting ▾

You have static IP information from your ISP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway IP address: 0.0.0.0

Primary DNS Server:

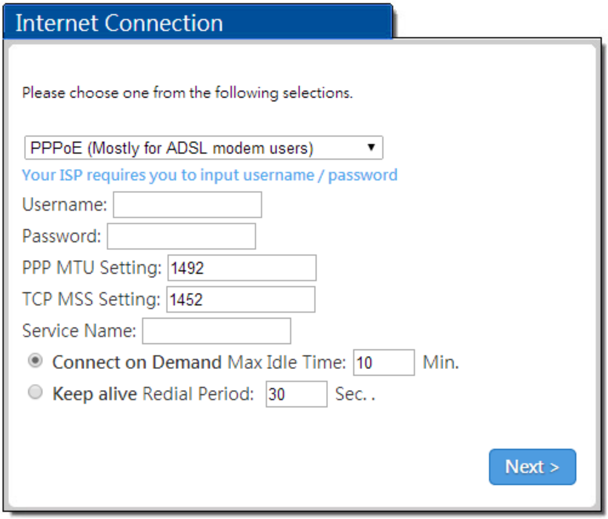
Secondary DNS Server:

Figure 10 Internet Connection Setting Screen—Static IP Setting

Item	Default	Description
IP Address	0.0.0.0	Enter the IP address provided by your ISP.
Subnet Mask	0.0.0.0	Enter the subnet mask for the IP address.
Gateway IP Address	0.0.0.0	Enter the Gateway IP Address provided by your ISP.
Primary DNS Server	Empty	Enter the primary DNS server IP address for the xDSL/Cable connection (provided by your ISP).
Secondary DNS Server	Empty	Enter the secondary DNS server IP address for the xDSL/Cable connection (provided by your ISP). If the primary DNS Server IP were not available, meanwhile, Secondary DNS Server IP would start in the same time.

- **PPPoE (Mostly for ADSL modem users)**

If “PPPoE” is selected, below setting screen will appear. Enter the username, password and other major fields.



Internet Connection

Please choose one from the following selections.

PPPoE (Mostly for ADSL modem users) ▾

Your ISP requires you to input username / password

Username:

Password:

PPP MTU Setting: 1492

TCP MSS Setting: 1452

Service Name:

● Connect on Demand Max Idle Time: 10 Min.

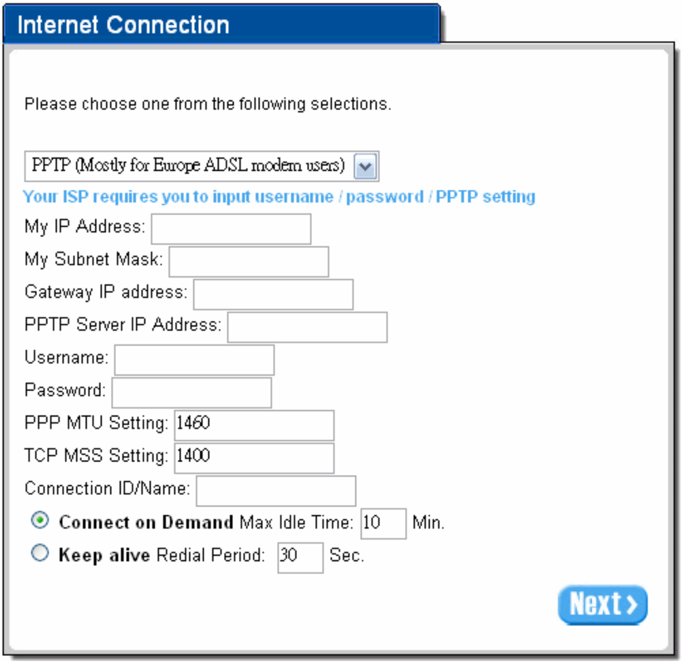
○ Keep alive Redial Period: 30 Sec. .

Figure 11 Internet Connection Setting Screen—PPPoE Setting

Item	Default	Description
Username	Empty	Enter the user name provided by your ISP.
Password	Empty	Enter the user password provided by your ISP.
PPP MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1452	MSS (Maximum Segment Size) specifies maximum segment size.
Service Name	Empty	Enter the service name provided by your ISP.
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your R-300NP to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your R-300NP to automatically re-establish your connection as soon as you attempt to access the Internet again
Max Idle Time	10 Min.	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPPoE enabled Internet access connected indefinitely, even when it sits idle.
Redial Period	30 sec.	

- **PPTP (Mostly for Europe ADSL modem users)**

If “PPTP” is selected, then this screen will appear. Fill out all the information provided by your ISP.



Internet Connection

Please choose one from the following selections.

PPTP (Mostly for Europe ADSL modem users)

Your ISP requires you to input username / password / PPTP setting

My IP Address:

My Subnet Mask:

Gateway IP address:

PPTP Server IP Address:

Username:

Password:

PPP MTU Setting: 1460

TCP MSS Setting: 1400

Connection ID/Name:

● **Connect on Demand** Max Idle Time: 10 Min.

○ **Keep alive** Redial Period: 30 Sec.

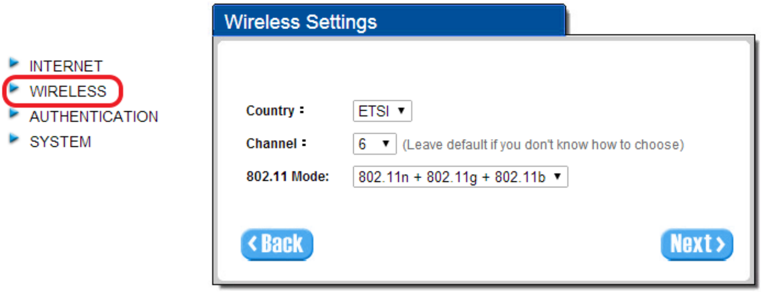
Figure 12 Internet Connection Setting Screen—PPTP Client Setting

Item	Default	Description
My IP Address	Empty	Enter the PPTP local IP address provided by your ISP.
My Subnet Mask	Empty	Enter the PPTP local Subnet Mask IP address for the IP address (My IP Address).
Gateway IP Address	Empty	Enter the PPTP server Gateway IP address provided by your ISP.
PPTP Server IP Address	Empty	Enter the PPTP server IP address provided by your ISP.
Username	Empty	Enter the user name provided by your ISP.
Password	Empty	Enter the user password provided by your ISP.
PPP MTU Setting	1460	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.
Connection ID/Name	Empty	Enter the connection ID or connection name.

Item	Default	Description
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your R-300NP to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your R-300NP to automatically re-establish your connection as soon as you attempt to access the Internet again.
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPTP enabled Internet access connected indefinitely, even when it sits idle.
Redial Period	30 sec.	

Step 4: Wireless Setting

This page allows you to define Country, Channel and 802.11 mode for wireless connection.



Wireless Settings

Country : ETSI

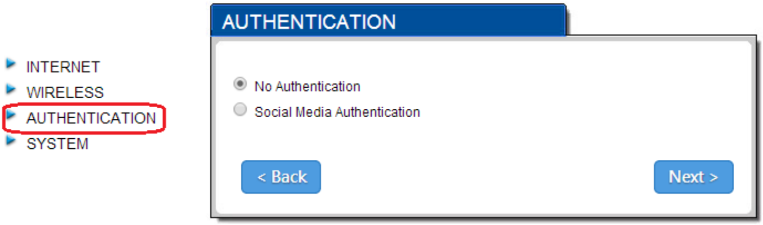
Channel : 6 (Leave default if you don't know how to choose)

802.11 Mode: 802.11n + 802.11g + 802.11b

Figure 13 Wireless Setting Screen

Item	Default	Description
Country	ETSI	Select Wireless region you located.
Channel	6	Enter the channel ID for wireless connection. You could choose from Ch1 to Ch11.
802.11 Mode	802.11n+802.11g+802.11b	Enter the 802.11 Mode for wireless connection 802.11n+802.11g+802.11b 802.11n+802.11g 802.11g+802.11b 802.11n only 802.11g only 802.11b only

Step 5: Authentication Service Setting



● No Authentication
○ Social Media Authentication

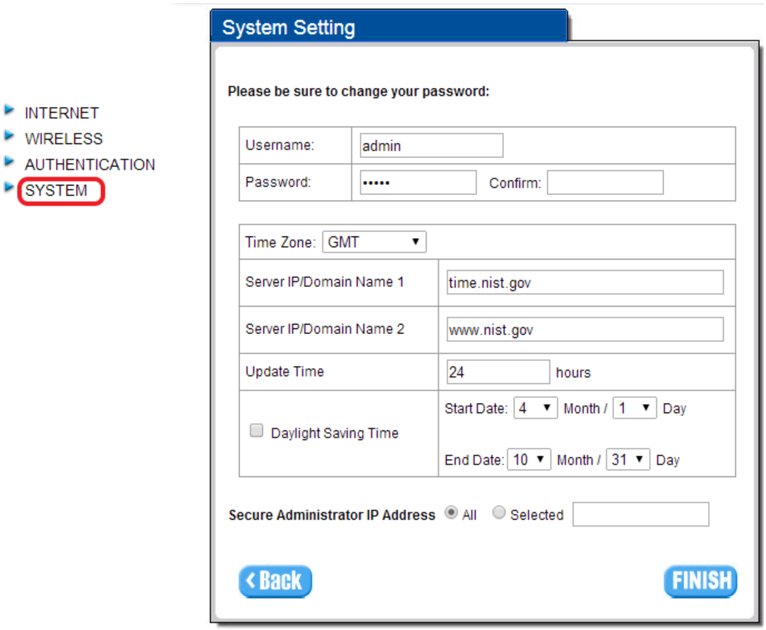
Figure 14 Authentication Service Setting Screen

Item	Default	Description
Authentication	No Authentication	**No Authentication -** Subscriber can direct access to the Internet without enter username and password. **Social Media Authentication -** R-300NP provides Built-in Authentication for service provider to build up an Internet service with Coolbee WiFi service.

Note:

If you want to active Social Media Authentication by Coolbee WiFi, please refer to Appendix A.

Step 6: System Setting



System Setting

Please be sure to change your password:

Username: admin

Password: ••••• Confirm:

Time Zone: GMT ▾

Server IP/Domain Name 1: time.nist.gov

Server IP/Domain Name 2: www.nist.gov

Update Time: 24 hours

□ Daylight Saving Time — Start Date: 4 ▾ Month / 1 ▾ Day; End Date: 10 ▾ Month / 31 ▾ Day

Secure Administrator IP Address ● All ○ Selected

Figure 15 System Setting Screen

Item	Default	Description
Username	admin	Enter the user name. The user name can consist of up to 20 alphanumeric characters and is case sensitive.
Password	admin	Enter the user password. The password can consist of up to 20 alphanumeric characters and is case sensitive.
Confirm	Empty	Enter the user password again to confirm the password.
Time Zone	GMT	Enter the Time Zone for the system.
Server IP/Domain Name 1	time.nist.gov	Enter NTP Server IP or Domain
Server IP/Domain Name 2	www.nist.gov	Enter NTP Server IP or Domain
Update Time	24 hours	Enter the number of hours for update time.

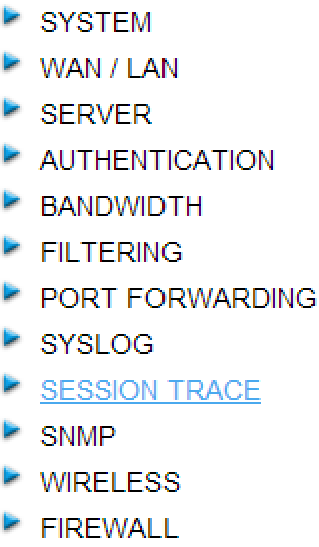
Daylight Saving Time	Disable	The system time won't be effected by daylight saving.
		If you set the Daylight Saving Time (DST) on the R-300NP. Please adjust the start date and end date.
Secure Administrator IP Address	All	This function allows remote user to management the device. You can specify one or any IP addresses for remote control the system.

*Click "**FINISH**" button to save the settings then the system will restart.*

3-2 Advanced Setup

The Advanced Setup allows you to configure advanced settings related to accessing the Internet, including,

1. SY
2. W
3. SE
4. AU
5. BA
6. FI
7. PO
8. SY
9. SE
10. SN
11. W
12. FI



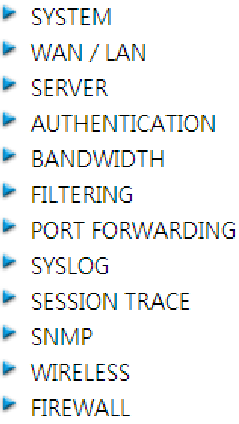
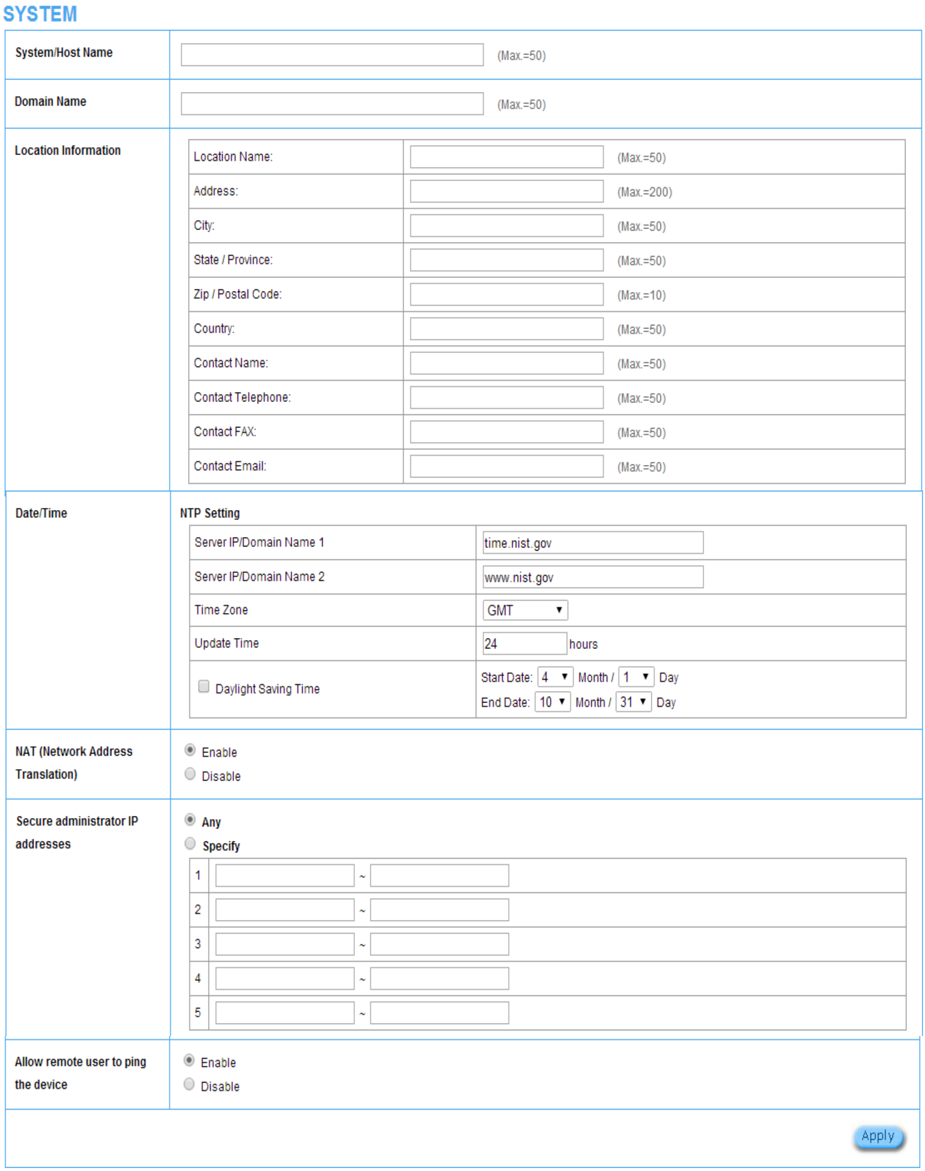


Figure 16 Advanced Setting Item Screen

***Note:** After change the settings of device, please click "**Apply**" button to save the new settings.*

3-2-1 System

Define the R-300NP System configuration.



SYSTEM

System/Host Name	(Max.=50)
Domain Name	(Max.=50)

Location Information

Location Name:		(Max.=50)
Address:		(Max.=200)
City:		(Max.=50)
State / Province:		(Max.=50)
Zip / Postal Code:		(Max.=10)
Country:		(Max.=50)
Contact Name:		(Max.=50)
Contact Telephone:		(Max.=50)
Contact FAX:		(Max.=50)
Contact Email:		(Max.=50)

Date/Time

NTP Setting

Server IP/Domain Name 1	time.nist.gov
Server IP/Domain Name 2	www.nist.gov
Time Zone	GMT ▼
Update Time	24 hours
□ Daylight Saving Time	Start Date: 4 ▼ Month / 1 ▼ Day End Date: 10 ▼ Month / 31 ▼ Day

NAT (Network Address Translation)

● Enable
○ Disable

Secure administrator IP addresses

● Any
○ Specify

1		~	
2		~	
3		~	
4		~	
5		~	

Allow remote user to ping the device

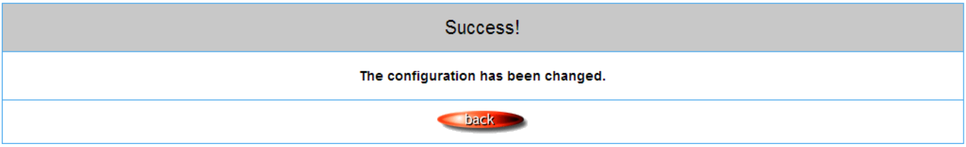
● Enable
○ Disable

Figure 18 System Setting Screen

Item	Default	Description
System/Host Name	Empty	The system name can consist of up to 50 alphanumeric characters.
Domain Name	Empty	The Domain name can consist of up to 50 alphanumeric characters.
Location Information	Empty	Key in your location information.
Date/Time		
NTP Setting	Disable	Enables or disables NTP (Network Time Protocol) Time Server. Network Time Protocol can be utilized to synchronize the time on devices across a network.
Server IP/Domain Name	Empty	Enter the IP address/domain name of NTP server.
Time Zone	GMT+8:00	Select the appropriate time zone for your location.
Update Time	24 hours	Enter the number of hours for update time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
	Month/Day	Set the Daylight Saving Time (DST) on the R-300NP. Adjust the start date and end date.
NAT (Network Address Translation)		
NAT	Enable	Enables or disables NAT Address Translation function.
Secure administrator IP Addresses	Any	Options: Any or Specify. Administrator can specify 5 IP addresses or a range to allow remote control access from network.
Allow remote user to ping the device	Enable	This function allows remote user to ping the R-300NP through Internet. Ping is normally used to test the physical connection between two devices, to ensure that everything is working correctly.

Apply *Click “**Apply”** button to save the new settings.*

After click “**Apply”** button, the dialog box will appear as Figure. Click “**back”** button to back to previous page.



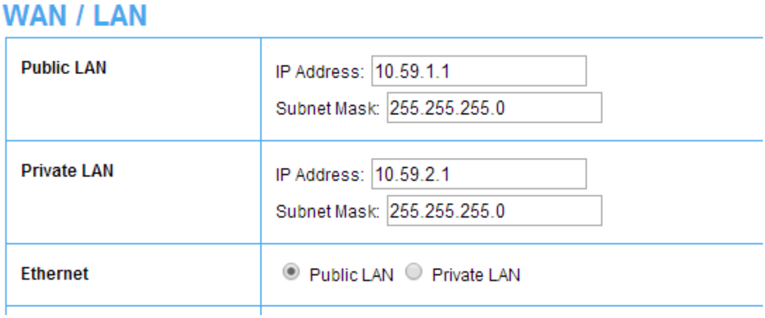
Success!

The configuration has been changed.

Figure 19 Dialog Box

3-2-2 WAN/LAN

- **Device IP (LAN IP) Setting**



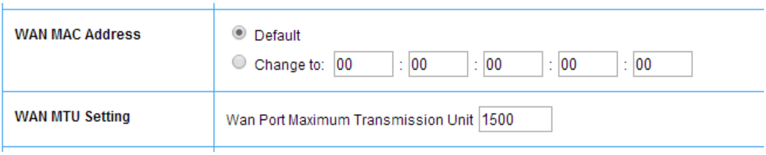
WAN / LAN

Public LAN	IP Address: 10.59.1.1 Subnet Mask: 255.255.255.0
Private LAN	IP Address: 10.59.2.1 Subnet Mask: 255.255.255.0
Ethernet	● Public LAN ○ Private LAN

Figure 20 Device IP (LAN IP) Setting

Item	Default	Description
Public LAN		
IP Address	10.59.1.1	The internal LAN IP address of your Wireless Subscriber Server Gateway for public LAN.
Subnet Mask	255.255.255.0	Enter the subnet mask for public IP address.
Private LAN		
IP Address	10.59.1.1	The internal LAN IP address of your Wireless Subscriber Server Gateway for private LAN.
Subnet Mask	255.255.255.0	Enter the subnet mask for private IP address.
Ethernet	Public LAN	You could choose which Ethernet to use for the internet connection.

- **WAN MAC Address**

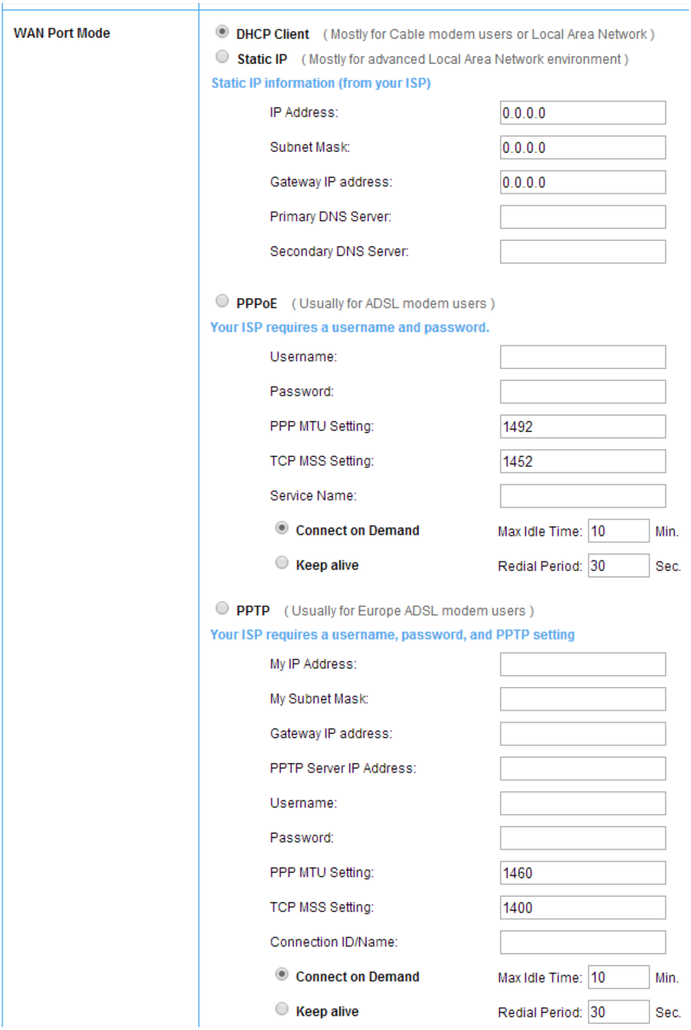


WAN MAC Address	● Default ○ Change to: 00 : 00 : 00 : 00 : 00
WAN MTU Setting	Wan Port Maximum Transmission Unit 1500

Figure 21 WAN MAC Address Setting

Item	Default	Description
WAN MAC Address	Default	The default MAC address is set to the WAN physical interface on device.
WAN MTU Setting	1500	You could set the MTU in this column.

- **WAN Port Mode**



WAN Port Mode

● DHCP Client (Mostly for Cable modem users or Local Area Network)

○ Static IP (Mostly for advanced Local Area Network environment)

Static IP information (from your ISP)

IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway IP address:	0.0.0.0
Primary DNS Server:	
Secondary DNS Server:	

○ PPPoE (Usually for ADSL modem users)

Your ISP requires a username and password.

Username:	
Password:	
PPP MTU Setting:	1492
TCP MSS Setting:	1452
Service Name:	

● Connect on Demand — Max Idle Time: 10 Min.

○ Keep alive — Redial Period: 30 Sec.

○ PPTP (Usually for Europe ADSL modem users)

Your ISP requires a username, password, and PPTP setting

My IP Address:	
My Subnet Mask:	
Gateway IP address:	
PPTP Server IP Address:	
Username:	
Password:	
PPP MTU Setting:	1460
TCP MSS Setting:	1400
Connection ID/Name:	

● Connect on Demand — Max Idle Time: 10 Min.

○ Keep alive — Redial Period: 30 Sec.

Figure 22 WAN Port Mode Setting

DHCP Client

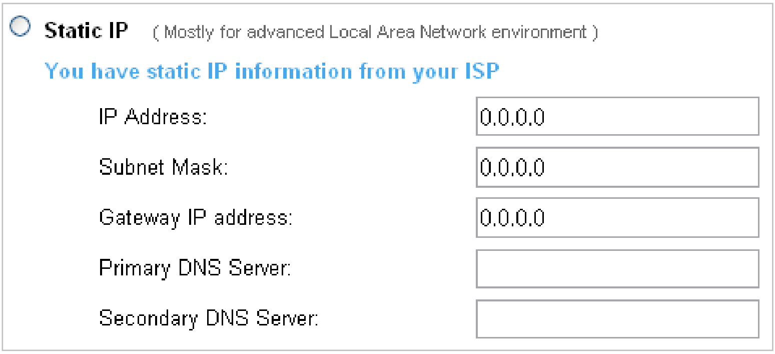
The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your ISP. If your xDSL/Cable comes with this feature, please enable Use DHCP Client.

○ DHCP Clients (Mostly for Cable modem users or Local Area Network)

Figure 23 DHCP Client Setting Screen

Static IP

If Static IP Setting is selected, this screen will appear. Enter the IP address information provided by your ISP.



○ Static IP (Mostly for advanced Local Area Network environment)

You have static IP information from your ISP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway IP address: 0.0.0.0

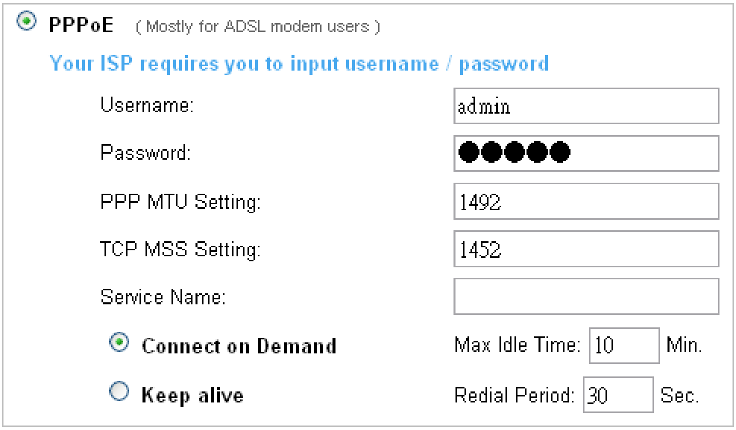
Primary DNS Server:

Secondary DNS Server:

Figure 24 Static IP Setting Screen

Item	Description
IP Address	Enter the IP address for the xDSL/Cable connection (provided by your ISP).
Subnet Mask	Enter the subnet mask for the IP address.
Gateway IP Gateway	Enter the Gateway IP address for the xDSL/Cable connection (provided by your ISP).
Primary DNS Server	A primary DNS server IP address for the xDSL/Cable connection (provided by your ISP).
Secondary DNS Server	A secondary DNS server IP address for the xDSL/Cable connection (provided by your ISP). If the primary DNS Server IP were not available, the secondary DNS Server IP would start in the same time.

PPPoE



◉ PPPoE (Mostly for ADSL modem users)

Your ISP requires you to input username / password

Username: admin

Password: ●●●●●

PPP MTU Setting: 1492

TCP MSS Setting: 1452

Service Name:

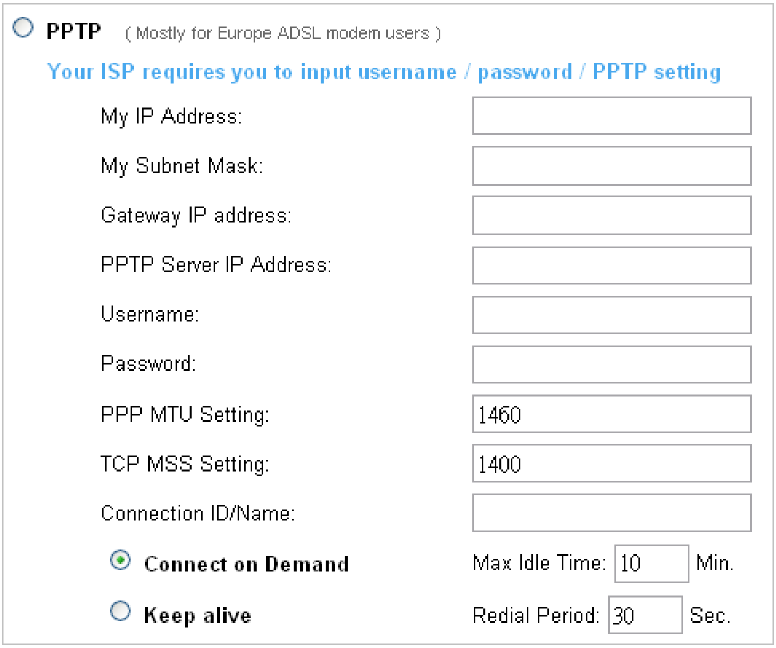
◉ Connect on Demand — Max Idle Time: 10 Min.

○ Keep alive — Redial Period: 30 Sec.

Figure 25 PPPoE Setting Screen

Item	Default	Description
User Name	Empty	Enter your PPPoE account name
Password	Empty	Enter your PPPoE password..
PPP MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1452	MSS (Maximum Segment Size) specifies maximum segment size.
Service Name	Empty	Enter the service name provided by your ISP. The service name can consist of up to 64 alphanumeric characters and is case sensitive.
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your R-300NP to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your R-300NP to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive.
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPPoE enabled Internet access connected indefinitely, even when it sits idle.
Redial Period	30 Seconds	

PPTP



○ **PPTP** (Mostly for Europe ADSL modem users)

Your ISP requires you to input username / password / PPTP setting

My IP Address:	
My Subnet Mask:	
Gateway IP address:	
PPTP Server IP Address:	
Username:	
Password:	
PPP MTU Setting:	1460
TCP MSS Setting:	1400
Connection ID/Name:	
● **Connect on Demand**	Max Idle Time: 10 Min.
○ **Keep alive**	Redial Period: 30 Sec.

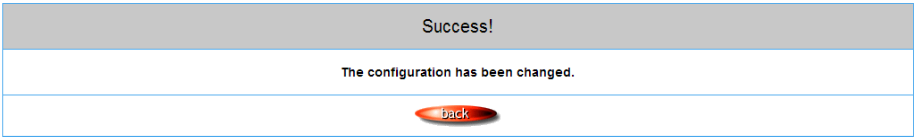
Figure 26 PPTP Setting Screen

Item	Default	Description
My IP Address	Empty	A PPTP local IP address for the xDSL/Cable connection (provided by your ISP).
My Subnet Mask	Empty	Enter the PPTP local IP address for the xDSL/Cable connection.
Gateway IP Address	Empty	A PPTP local default gateway for the xDSL/Cable connection (provided by your ISP).
PPTP Server IP Address	Empty	Enter the PPTP server IP address for the xDSL/Cable connection (provided by your ISP).
Username	Empty	Enter your PPTP account name.
Password	Empty	Enter your PPTP password.
PPP MTU Setting	1460	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.
Connection ID/Name	Empty	Enter the connection ID or connection name.

Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your R-300NP to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your R-300NP to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive.
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPTP enabled Internet access connected indefinitely, even when it sits idle.

Apply *Click “**Apply**” button to save the new settings.*

After click “**Apply**” button, the dialog box will appear as below. Click “**back**” button to go back to previous page.



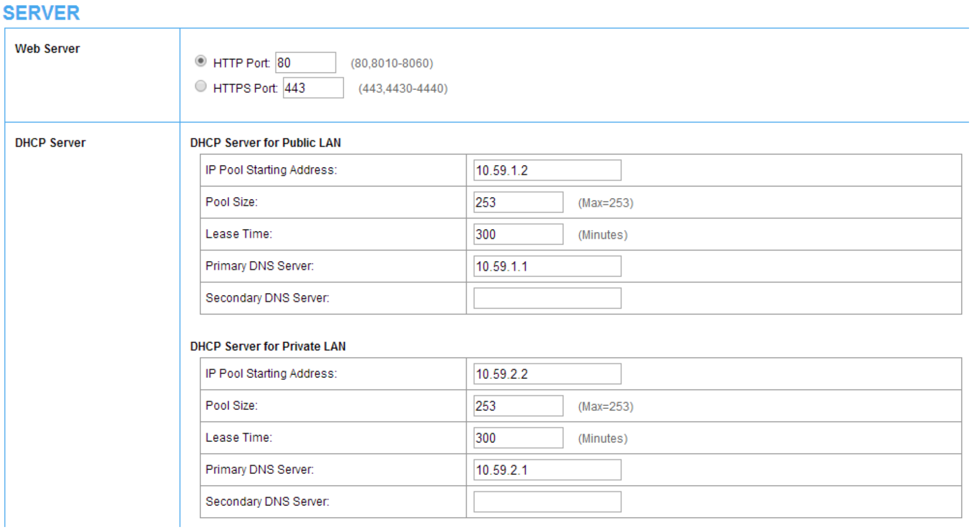
Success!

The configuration has been changed.

back

Figure 27 Dialog Box

3-2-3 Server



SERVER

Web Server

● HTTP Port: 80 (80,8010-8060)
○ HTTPS Port: 443 (443,4430-4440)

DHCP Server

DHCP Server for Public LAN

IP Pool Starting Address:	10.59.1.2
Pool Size:	253 (Max=253)
Lease Time:	300 (Minutes)
Primary DNS Server:	10.59.1.1
Secondary DNS Server:	

DHCP Server for Private LAN

IP Pool Starting Address:	10.59.2.2
Pool Size:	253 (Max=253)
Lease Time:	300 (Minutes)
Primary DNS Server:	10.59.2.1
Secondary DNS Server:	

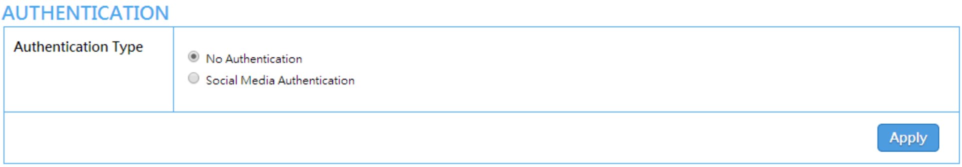
Figure 28 Server Setting Screen

Item	Default	Description
Web Server		
HTTP Port	80	Enter the HTTP port number. The HTTP port allowed range is 80 or 8010 to 8060.
HTTPS Port	443	Enter the HTTPS port number. The HTTPS port allowed range is 443 or 4430 to 4440.
DHCP Server for Public LAN		
IP Pool Starting Address	10.59.1.2	Enter the DHCP Pool Starting IP address for Public LAN
Pool Size	253	The DHCP pool size range is 1 to 253.
Lease Time	300	The DHCP lease time.
Primary DNS Server	168.95.1.1	Enter the IP address of primary DNS server.
Secondary DNS Server	Empty	Enter the IP address of secondary DNS server.
DHCP Server for Private LAN		
IP Pool Starting Address	10.59.2.2	Enter the DHCP Pool Starting IP address for Private LAN
Pool Size	253	The DHCP pool size range is 1 to 253.
Lease Time	300	The DHCP lease time.
Primary DNS Server	168.95.2.1	Enter the IP address of primary DNS server.
Secondary DNS Server	Empty	Enter the IP address of secondary DNS server.

Apply

*Click “**Apply**” button to save the new settings.*

3-2-4 Authentication


AUTHENTICATION

Authentication Type	● No Authentication ○ Social Media Authentication

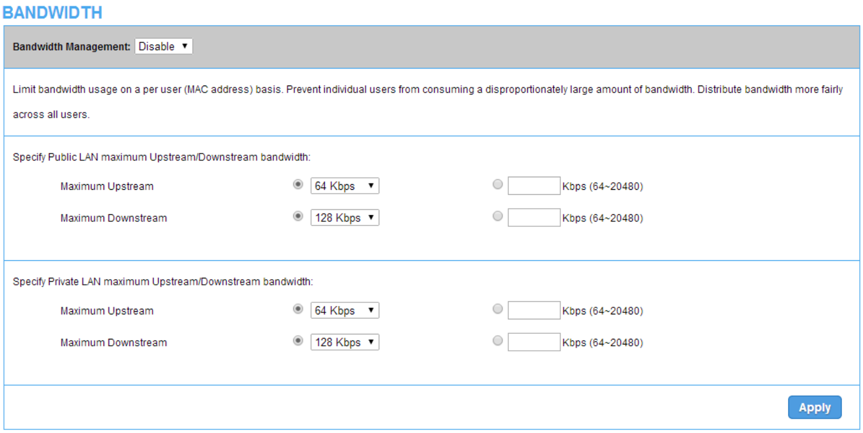
Figure 29 Authentication Setting Screen

Item	Default	Description
Authentication	No Authentication	**No Authentication -** Subscriber can direct access the Internet without enter username and password. **Social Media Authentication -** R-300NP provides Built-in Authentication for service provider to build up an Internet service with Coolbee WiFi service.

Apply *Click “**Apply**” button to save the new settings.*

3-2-5 Bandwidth

The function enables administrator to limit bandwidth usage on per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth. Every user gets a fair share of the available bandwidth.


BANDWIDTH

Bandwidth Management: Disable ▼

Limit bandwidth usage on a per user (MAC address) basis. Prevent individual users from consuming a disproportionately large amount of bandwidth. Distribute bandwidth more fairly across all users.

Specify Public LAN maximum Upstream/Downstream bandwidth:

Maximum Upstream	● 64 Kbps ▼	○ Kbps (64~20480)
Maximum Downstream	● 128 Kbps ▼	○ Kbps (64~20480)

Specify Private LAN maximum Upstream/Downstream bandwidth:

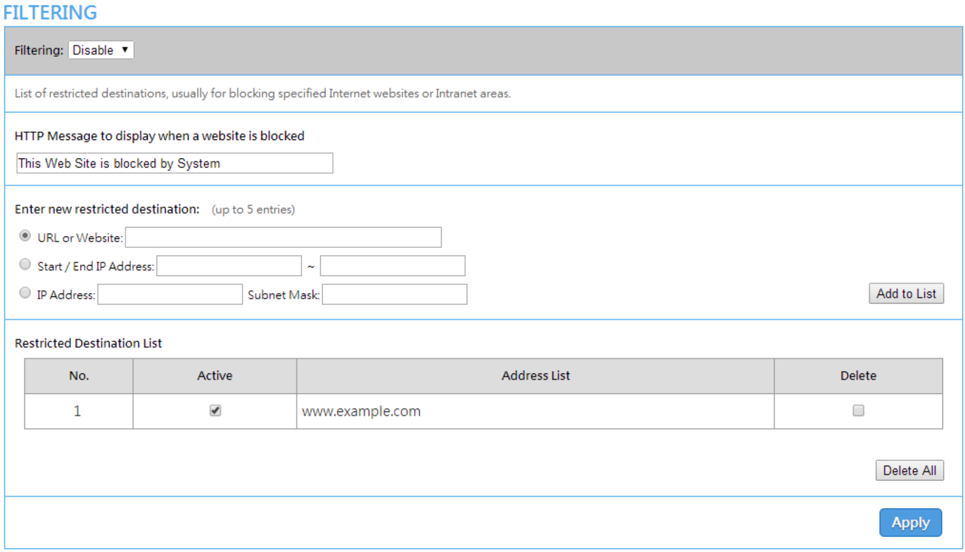
Maximum Upstream	● 64 Kbps ▼	○ Kbps (64~20480)
Maximum Downstream	● 128 Kbps ▼	○ Kbps (64~20480)

Figure 30 Bandwidth Setting Screen

Item	Default	Description
Bandwidth	Disable	Enables or disables Bandwidth Management.
Specify Public LAN maximum Upstream/Downstream bandwidth:		
Maximum Upstream	64Kbps	Specify the amount of upstream bandwidth. You can set the range by drop list：64K, 128K, 256K, 384K, 512K, 1.5Mbps, 3Mbps, 5Mbps, 10Mbps and 20 Mbps. Or key in by yourself, the range is from 64 ~20480Kbps
Maximum Downstream	128Kbps	Specify the amount of downstream bandwidth. You can set the range by drop list：64K, 128K, 256K, 384K, 512K, 1.5Mbps, 3Mbps, 5Mbps, 10Mbps and 20 Mbps. Or key in by yourself, the range is from 64 ~20480Kbps
Specify Private LAN maximum Upstream/Downstream bandwidth:		
Maximum Upstream	64Kbps	Specify the amount of upstream bandwidth. You can set the range by drop list：64K, 128K, 256K, 384K, 512K, 1.5Mbps, 3Mbps, 5Mbps, 10Mbps and 20 Mbps. Or key in by yourself, the range is from 64 ~20480Kbps
Maximum Downstream	128Kbps	Specify the amount of downstream bandwidth. You can set the range by drop list：64K, 128K, 256K, 384K, 512K, 1.5Mbps, 3Mbps, 5Mbps, 10Mbps and 20 Mbps. Or key in by yourself, the range is from 64 ~20480Kbps

3-2-6 Filtering

Filtering allows the administrator to have a list of restricted destinations, which is useful to block specified Internet websites or Intranet areas.



FILTERING

Filtering: Disable ▼

List of restricted destinations, usually for blocking specified Internet websites or Intranet areas.

HTTP Message to display when a website is blocked

This Web Site is blocked by System

Enter new restricted destination: (up to 5 entries)

● URL or Website:

○ Start / End IP Address: ~

○ IP Address: Subnet Mask:

Add to List

Restricted Destination List

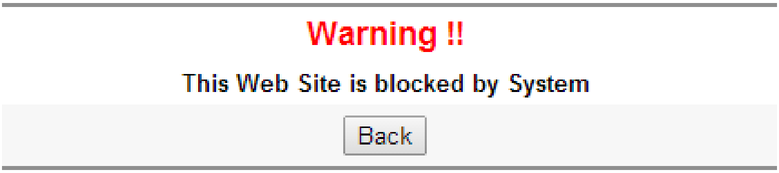
No.	Active	Address List	Delete
1	☑	www.example.com	□

Delete All

Apply

Figure 31 Filtering Setting Screen

Item	Default	Description
Filtering	Disable	Enables or disables filtering function. It could be set up to 5 entries.
HTTP Message to display when a website is blocked	The Web Site is blocked by System	Enter the http message. The maximum character of the HTTP message is 200. The warning page show as Figure 32.

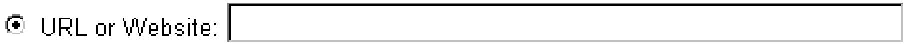
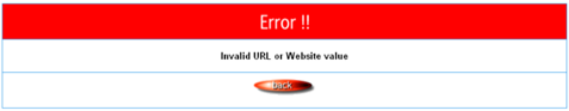
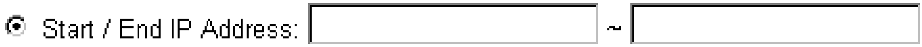
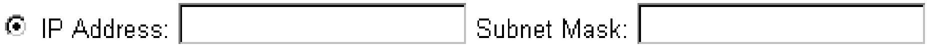


Warning !!

This Web Site is blocked by System

Back

Figure 32 Warning screen

Item	Default	Description
Restrict Destination  ○ URL or Website:		
URL or Website	Empty	Enter the URL Page of you wants to filter; please use this format such like “http://www.yahoo.com”. The maximum character of the URL Page is 50. If the URL format is wrong, the system will show the error message as below.  Error !! Invalid URL or Website value Back
 ○ Start / End IP Address: ~		
Start IP Address	Empty	Enter the start IP address of you wants to filter.
End IP Address	Empty	Enter the end IP address of you wants to filter.
 ○ IP Address: Subnet Mask:		
IP Address	Empty	Enter the destination IP address of you wants to filter.
Subnet Mask	Empty	Enter the destination subnet mask.
No	-	The index number of filtering address.
Active	Disable	Click on check box, active or inactive the filtering address.
Address List	-	Display the filtering address(s).
Delete	Disable	Select the check boxes and click ‘**Delete**’ to delete the filtering address(s).

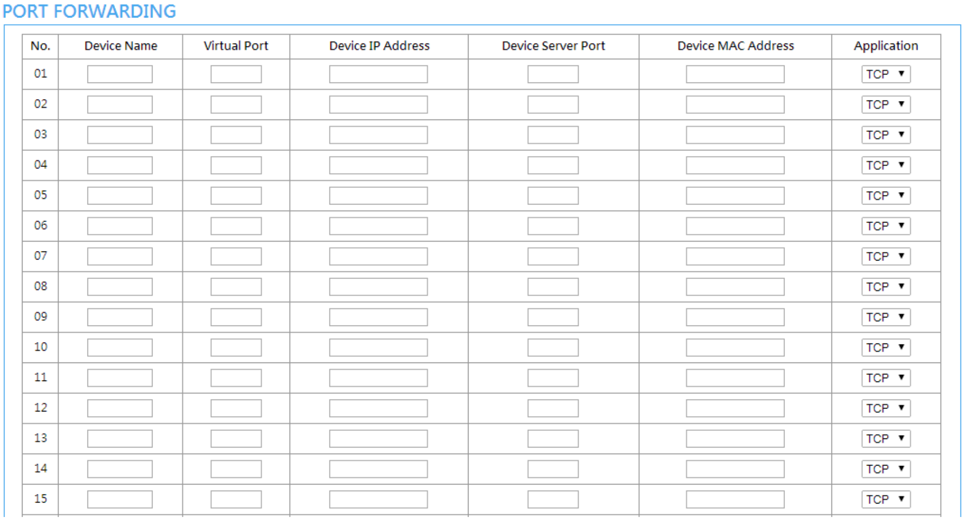
Add to List *Click “**Add to List”** button to add a new entry.*

Apply *Click “**Apply”** button to save the new settings.*

Delete All *Click “**Delete All** & **Apply”** button to delete all entries.*

3-2-7 Port forwarding

Administrator can set an entry of R-300NP which translating the address or port number of a packet to a new destination



PORT FORWARDING

No.	Device Name	Virtual Port	Device IP Address	Device Server Port	Device MAC Address	Application
01						TCP ▾
02						TCP ▾
03						TCP ▾
04						TCP ▾
05						TCP ▾
06						TCP ▾
07						TCP ▾
08						TCP ▾
09						TCP ▾
10						TCP ▾
11						TCP ▾
12						TCP ▾
13						TCP ▾
14						TCP ▾
15						TCP ▾

Figure 33 Port Forwarding Setting Screen

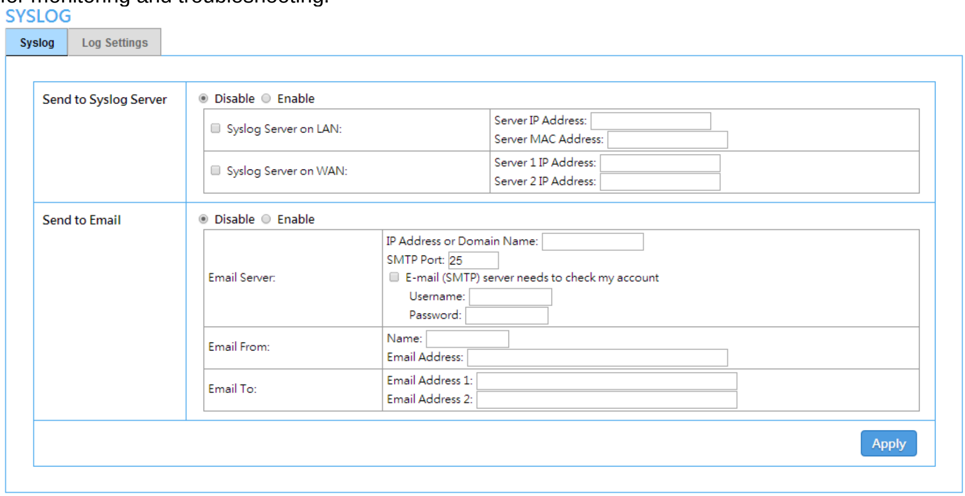
Item	Default	Description
Device Name	Empty	The LAN device name. The system could support up to 20 date at one time.
Virtual Port	0	The virtual port number valid range is 60001 to 60050 or 5900 to 5910.
Device IP Address	Empty	Enter the IP address of LAN device in the format “xxx.xxx.xxx.xxx”
Device Server Port	0	Enter the server port of LAN device.
Device MAC Address	Empty	The MAC address of LAN device. For input the device MAC address, please use this format such as”0050BA8D2296”.
Application	TCP	Select one protocol type of LAN device by clicking in the list box.

Apply *Click “**Apply”** button to save the new settings.*

Note: *The system does not support FTP.*

3-2-8 Syslog

The function allows the device to transmit event messages to your syslog server or your email address for monitoring and troubleshooting.



Send to Syslog Server: ● Disable ○ Enable

□ Syslog Server on LAN: Server IP Address: Server MAC Address:

□ Syslog Server on WAN: Server 1 IP Address: Server 2 IP Address:

Send to Email: ● Disable ○ Enable

Email Server: IP Address or Domain Name: SMTP Port: 25 □ E-mail (SMTP) server needs to check my account Username: Password:

Email From: Name: Email Address:

Email To: Email Address 1: Email Address 2:

Figure 34 Syslog Setting Screen

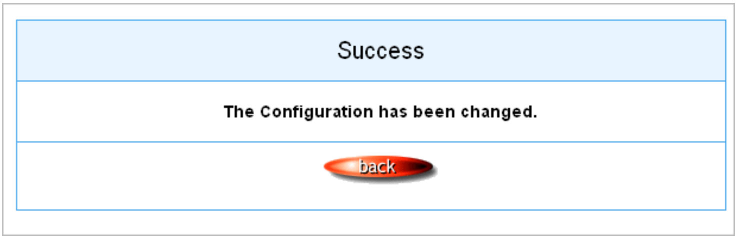
- **Syslog Setting**

Item	Default	Description
Send to Syslog Server	Disable	Enables or disables the syslog server function.
Syslog on LAN		
Server IP Address	Empty	Enter syslog server's IP address. The R-300NP will send all of its logs to the specified syslog server.
Server MAC Address	Empty	Enter the syslog server's MAC address. The R-300NP will send all of its logs to the specified syslog server.
Syslog on WAN		
Server 1 IP Address	Empty	Enter IP address of first syslog server.
Server 2 IP Address	Empty	Enter IP address of second syslog server.
Send to Email	Disable	Enables or disables the send to e-mail function.
E-mail Server		
IP Address or Domain Name	Empty	Enter the SMTP server IP address or domain name. The maximum allowed characters length is 50.
SMTP Port	25	The SMTP port allowed range is 25 or 2500 to 2599.
E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, please **enable** this check box. The username and password are supplied by your network administrator, SMTP server provider or ISP.

Username	Empty	Enter the username for the SMTP server.
Password	Empty	Enter the password for the SMTP server
Email From		
Name	Empty	Enter the name you would like to appear in the “message from” field of your outgoing message. The maximum allowed characters length is 20.
Email Address	Empty	Enter your e-mail address. This is the address others will use to send email to Email Address 1/Email Address 2.
Email To	Disable	Enables or disables the send to e-mail function.
Email Address 1	Empty	Enter your first e-mail address to receive the logs.
Email Address 2	Empty	Enter your second e-mail address to receive the logs.

Apply *Click “**Apply**” button to save the new settings.*

*After click “**Apply**” button, the dialog box will appear as below. Click “**Back**” button to return to Syslog setting screen.*

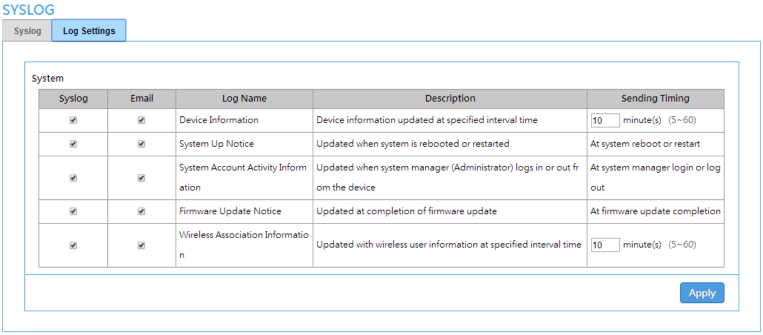


Success

The Configuration has been changed.

Figure 35 Success Dialog Box

- **Log Settings**



System

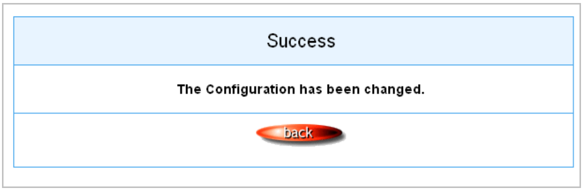
Syslog	Email	Log Name	Description	Sending Timing
☑	☑	Device Information	Device information updated at specified interval time	10 minute(s) (5~60)
☑	☑	System Up Notice	Updated when system is rebooted or restarted	At system reboot or restart
☑	☑	System Account Activity Inform ation	Updated when system manager (Administrator) logs in or out fr om the device	At system manager login or log out
☑	☑	Firmware Update Notice	Updated at completion of firmware update	At firmware update completion
☑	☑	Wireless Association Informatio n	Updated with wireless user information at specified interval time	10 minute(s) (5~60)

Figure 36 Log Settings Screen

Item	Default	Description
System		
Syslog	Unchecked	If checked, the log data will be sent by syslog.
Email	Unchecked	If checked, the log data will be sent by e-mail.
Item	**Interval Time**	**Description**
Device Information	10 minutes	The log included system information would be sent according to specified interval time. The time could be set from 5 to 60 minutes.
System Up Notice	When system rebooted or restarted	If device have been rebooted or restarted, the log will be sent.
System Account Activity Information	When system manager login or logout	A log will be sent if system manager (Administrator) login to or logout from the device
Firmware Update Notice	When firmware update completed	A log will be sent if firmware update completed
Wireless Association Information	10 minutes.	A log including wireless users information will be sent according to specified interval time. The time could be set from 5 to 60 minutes.

Apply *Click “**Apply**” button to save the new settings.*

After click “**Apply**” button, the success dialog box will appear. Click **“Back**” button to return to Logs setting screen.

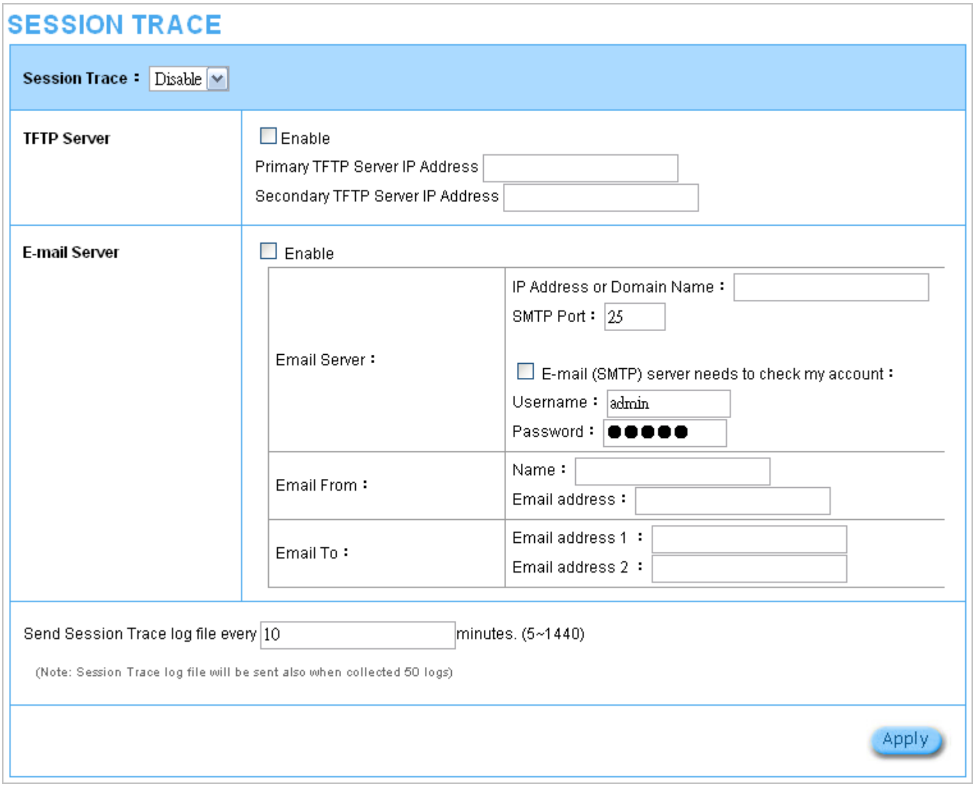

Success

The Configuration has been changed.

Figure 37 Success Dialog Box

3-2-9 Session Trace

Session Trace is an intelligent function to help service provider to trace every user’s access behavior. When “session trace” is enable , the system will collect information such like destination IP, destination port, source IP, source MAC, source port by every user and send the collected information in text format file to specified TFTP server or Email Server.



SESSION TRACE

Session Trace : Disable

TFTP Server
□ Enable
Primary TFTP Server IP Address
Secondary TFTP Server IP Address

E-mail Server
□ Enable
Email Server : IP Address or Domain Name :
SMTP Port : 25
□ E-mail (SMTP) server needs to check my account :
Username : admin
Password : ●●●●●
Email From : Name :
Email address :
Email To : Email address 1 :
Email address 2 :

Send Session Trace log file every 10 minutes. (5~1440)

(Note: Session Trace log file will be sent also when collected 50 logs)

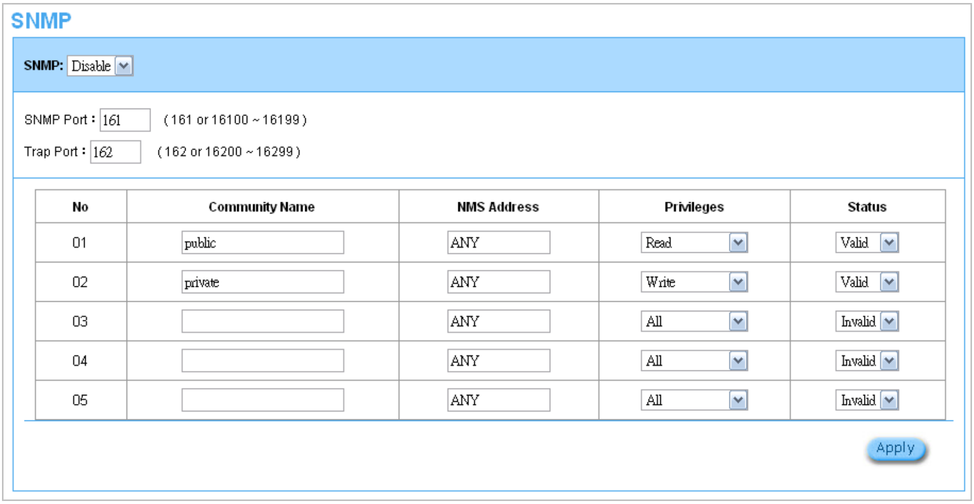
Figure 38 Session Trace Setting Screen

Item	Default	Description
Session Trace	Disable	Disables or enables session trace function.
TFTP Server	Disable	Disables or enables this function
Primary TFTP Server IP Address	Empty	Enter the IP address of the primary TFTP server.
Secondary TFTP Server IP Address	Empty	Enter the IP address of the second TFTP server.
E-mail Server	Disable	Disables or enables this function

Send to Email	Disable	Enables or disables the send to e-mail function.
IP Address or Domain Name	Empty	Enter the SMTP server IP address or domain name. The maximum allowed characters length is 50.
SMTP Port	Empty	The SMTP port allowed range is 25 or 2500 to 2599.
E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, click on check box. These values (username and password) are supplied by your network administrator, SMTP server provider or ISP.
Username	Empty	Enter the username for the SMTP server.
Password	Empty	Enter the password for the SMTP server
Email From		
Name	Empty	Enter the name you would like to appear in the “message from” field of your outgoing message. The maximum allowed characters length is 20.
Email Address	Empty	Enter your e-mail address. This is the address others will use to send email to Email Address 1/Email Address 2.
Email To		
Email Address 1	Empty	Enter your first e-mail address to receive the logs.
Email Address 2	Empty	Enter your second e-mail address to receive the logs.
Send Session Trace log file every~ minutes.	10 minutes	The field means to send the session trace log file every interval minutes. The value range is 5 to 1440 (minutes).

3-2-10 SNMP

The SNMP Agent Configuration screen enables you to access to your device via Simple Network Management Protocol. If you are not familiar with SNMP, please consult your Network Administrator or consult SNMP reference material. You must first enable SNMP on the SNMP Agent Configuration screen.



SNMP

SNMP: Disable

SNMP Port : 161 (161 or 16100 ~ 16199)

Trap Port : 162 (162 or 16200 ~ 16299)

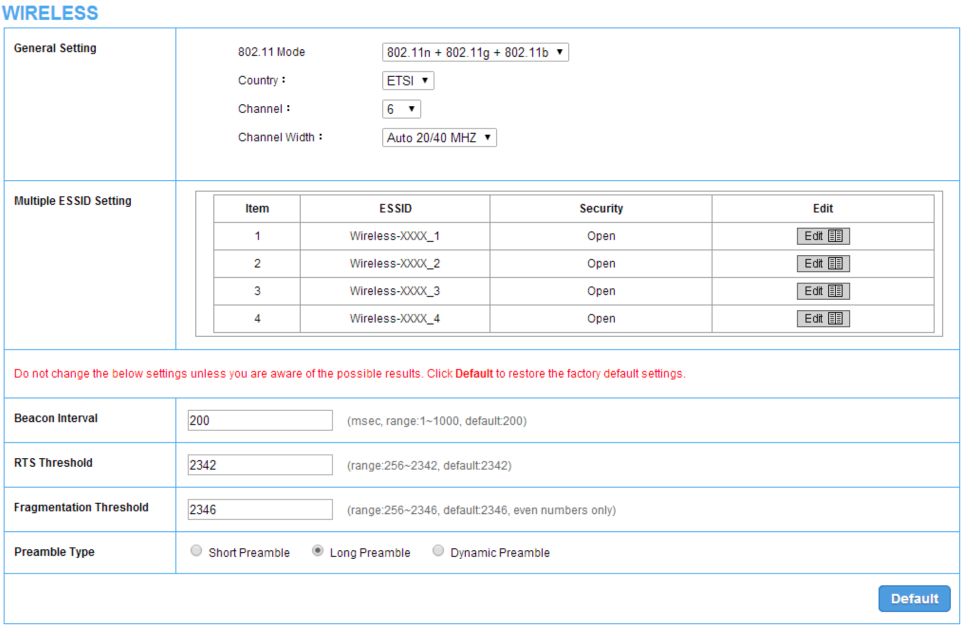
No	Community Name	NMS Address	Privileges	Status
01	public	ANY	Read	Valid
02	private	ANY	Write	Valid
03		ANY	All	Invalid
04		ANY	All	Invalid
05		ANY	All	Invalid

Figure 39 SNMP Setting Screen

Item	Default	Description
SNMP	Disable	Disables or enables the SNMP management.
SNMP Port	161	If the SNMP enables, also allowed to specific the SNMP port number via NAT. The allowed SNMP port numbers are 161 (default), 16100-16199 and Trap port numbers are 162 (default), 16200-16299. This Port setting is useful for remote control via NAT network.
Trap Port	162	
Configuration		
Community Name	public/private	Every unit with SNMP enable must be configured to recognize one or more community. The default setting for the community of entry 1 is “public” and for the entry 2 is “private” and others are empty.
NMS Address	ANY	The address of the NMS. The default settings for the NMS Networking are “ANY”.

Item	Default	Description
Privileges	Read/Write	Choose “Read”, “Write”, “Trap Recipients” and “All” for different privileges. The default setting of the entry 2 is “write” and others are “read”.
Status	Valid/Invalid	Chosen “Valid” or “Invalid”. The default setting of entry 1, 2 are valid and others are invalid.

3-2-11 Wireless



WIRELESS

General Setting

802.11 Mode: 802.11n + 802.11g + 802.11b ▼

Country : ETSI ▼

Channel : 6 ▼

Channel Width : Auto 20/40 MHZ ▼

Multiple ESSID Setting

Item	ESSID	Security	Edit
1	Wireless-XXXX_1	Open	Edit
2	Wireless-XXXX_2	Open	Edit
3	Wireless-XXXX_3	Open	Edit
4	Wireless-XXXX_4	Open	Edit

Do not change the below settings unless you are aware of the possible results. Click **Default** to restore the factory default settings.

Beacon Interval: 200 (msec, range:1~1000, default:200)

RTS Threshold: 2342 (range:256~2342, default:2342)

Fragmentation Threshold: 2346 (range:256~2346, default:2346, even numbers only)

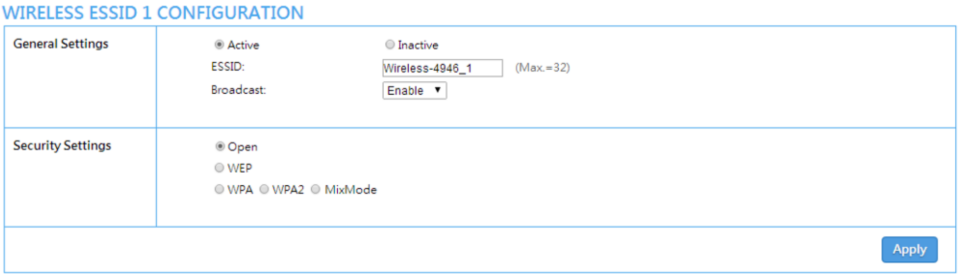
Preamble Type: ○ Short Preamble ● Long Preamble ○ Dynamic Preamble

Figure 40 Wireless Setting Screen

Item	Default	Description
General Settings		
802.11 Mode	802.11n+802.11g+802.11b	Choose one： -802.11n+802.11g+802.11b -802.11n+802.11g -802.11g+802.11b -802.11n only -802.11g only -802.11b only

Country	ETSI	Wireless Region. You could choose “ETSI” or “FCC”.
Channel	6	Select the channel ID for wireless connection.
Channel Width	Auto 20/40 MHZ	You could chose “Auto 20/40 MHZ” or “20 MHZ”
Multiple ESSID Setting		
ESSID	Wireless-XXXX _1 ~4	The R-300NP has 4 ESSID. The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters. Click “Edit”, then you can configure more detail of ESSID settings. The default ESSID name is Wireless-XXXX_1(to 4) “XXXX” is the last 4 digit of R-300NP WLAN MAC.
Beacon Interval	200	This value valid range is 1 to 1000 indicates the frequency interval of the beacon.
RTS Threshold	2342	This value valid range is 256-2342. This setting determines the packet size at which the R-300NP issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the R-300NP, or in areas where the clients are far apart and can detect only the R-300NP and not each other.
Fragmentation Threshold	2346	This setting determines the size at which packets are fragmented. Enter a setting ranging from 256 to 2346 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
Preamble Type	Long Preamble	The preamble type is a section of data at the head of a packet that contains information the R-300NP and client devices need when sending and receiving packets. The setting menu allows you to select a long, short or dynamic preamble type.

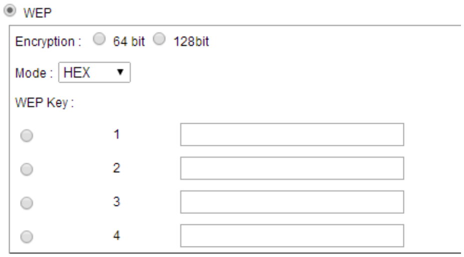
- **Edit the ESSID**

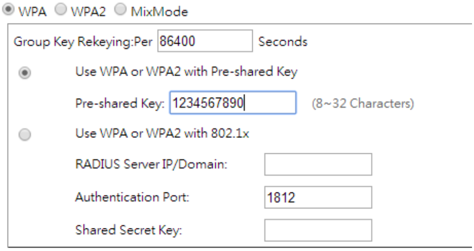


WIRELESS ESSID 1 CONFIGURATION

General Settings	● Active ○ Inactive ESSID: Wireless-4946_1 (Max.=32) Broadcast: Enable
Security Settings	● Open ○ WEP ○ WPA ○ WPA2 ○ MixMode

Figure 41 Wireless ESSID Setting Screen

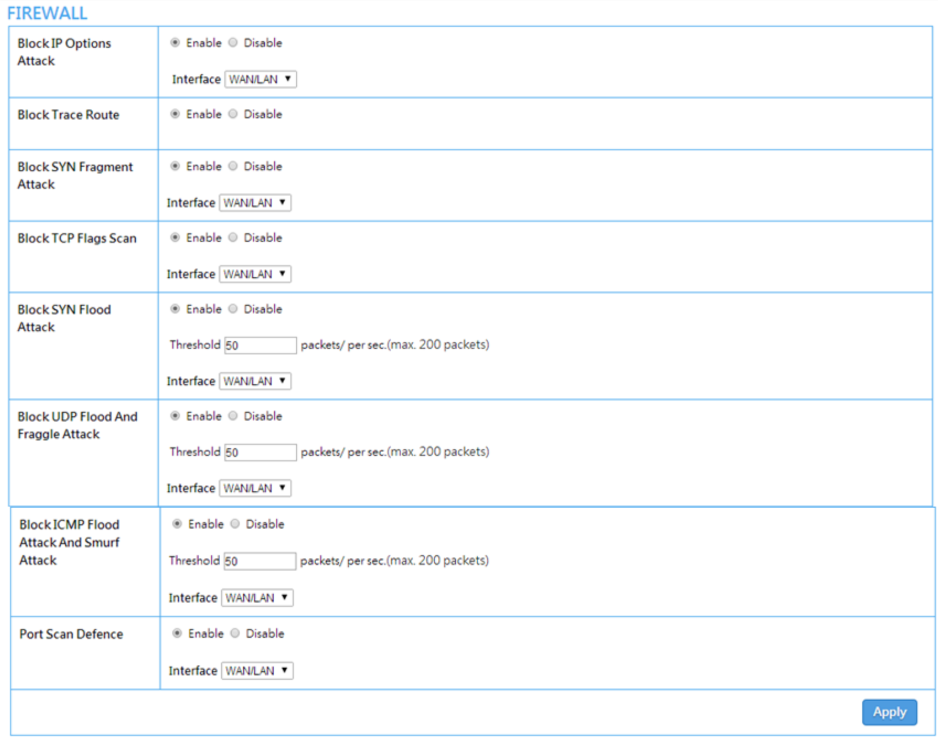
Item	Default	Description
General Settings		
ESSID	Active	You could set active or inactive for any ESSID. The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Broadcast	Enable	a method of transferring a message to all recipients simultaneously
Security Settings		
Security Settings	Open	This allows you to setting if there's any data encryption will be and what kind of encryption you would like to use.
Open		Data will transit without any data encryption.
WEP Encryption	Wired Equivalent Privacy Encryption  ● WEP Encryption : ○ 64 bit ○ 128bit Mode : HEX WEP Key : ○ 1 ○ 2 ○ 3 ○ 4	
Encryption	64 bit	The R-300NP supports 64-bit or 128 bit WEP encryption.
Mode	HEX	Options: HEX (Hexadecimal) and ASCII (American Standard Code for Information Interchange).
WEP Key	1	This selects which of the Keys that R-300NP uses when it transmits. You can change the selected encryption key any

		time to increase the security of your network. Note: You have to configure all WEP keys (1~4), and select one of the WEP key you would like to use this time. Enter 5 characters for ASCII 64-bit WEP Key. Enter 10 characters for Hex 64-bit WEP Key. Enter 13 characters for ASCII 128-bit WEP Key. Enter 26 characters for Hex 128-bit WEP Key.
WPA ,WPA2 and Mix mode Encryption	Wi-Fi Protected Access Encryption  ● WPA ○ WPA2 ○ MixMode Group Key Rekeying:Per 86400 Seconds ● Use WPA or WPA2 with Pre-shared Key Pre-shared Key: 1234567890 (8~32 Characters) ○ Use WPA or WPA2 with 802.1x RADIUS Server IP/Domain: Authentication Port: 1812 Shared Secret Key:	
Group Key Re-Keying	86400 Seconds	Enter a number in the field to set the force re-keying interval.
Use WPA with Pre-shared Key	Enable	
Pre-Shared Key	1234567890	Enter a pre-shared key from 8 to 32 case sensitive ASCII characters.
Use WPA with RADIUS	Disable	
Server IP	Empty	Enter the RADIUS server IP address or domain name. The maximum allowed characters length is 15.
Authentication Port	1812	Enter the authentication port number. The allowed numbers are from 0 to 65535.
Share Secret Key	Empty	Enter the RADIUS secret key

Apply Click “**Apply**” button to save the new settings.

3-2-12 Firewall

A firewall protects your network against threats from the public Internet. Here you can enable or disable R-300NP's firewall.



FIREWALL

Block IP Options Attack	● Enable ○ Disable Interface WAN/LAN ▼
Block Trace Route	● Enable ○ Disable
Block SYN Fragment Attack	● Enable ○ Disable Interface WAN/LAN ▼
Block TCP Flags Scan	● Enable ○ Disable Interface WAN/LAN ▼
Block SYN Flood Attack	● Enable ○ Disable Threshold 50 packets/ per sec.(max. 200 packets) Interface WAN/LAN ▼
Block UDP Flood And Fraggle Attack	● Enable ○ Disable Threshold 50 packets/ per sec.(max. 200 packets) Interface WAN/LAN ▼
Block ICMP Flood Attack And Smurf Attack	● Enable ○ Disable Threshold 50 packets/ per sec.(max. 200 packets) Interface WAN/LAN ▼
Port Scan Defence	● Enable ○ Disable Interface WAN/LAN ▼

Figure 42 Firewall Setting Screen

Item	Default	Description
Block IP Options Attack	Enable WAN/LAN	The R-300NP will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security because it will carry significant information, such as security, closed user group parameters, a series of Internet addresses, routing messages...etc. **Interface:** WAN/LAN, WAN, LAN
Block Trace Route	Enable	The R-300NP will not forward any trace route packets if you enable this item.
Block SYN Fragment Attack	Enable WAN/LAN	The R-300NP will drop any packets that having SYN flag and having mote fragment setting if you enable

		this item. **Interface:** WAN/LAN, WAN, LAN
Block TCP Flags Scan	Enable WAN/LAN	Any TCP packet with anomaly flag setting will be dropped if you enable this item. Those scanning activities include no flag scan, FIN without ACK scan, SYN FIN scan, Xmas scan and full Xmas scan. **Interface:** WAN/LAN, WAN, LAN
Block SYN Flood Attack	Enable 50 packets/ per sec WAN/LAN	Enable the SYN flood defense function to prevent the TCP SYN packets' attempt to exhaust the limited-resource of R-300NP. Once the TCP SYN packets exceeded the defined value, the R-300NP will start to discard the subsequent TCP SYN packets. **Interface:** WAN/LAN, WAN, LAN
Block UDP Flood And Fraggle Attack	Enable 50 packets/ per sec WAN/LAN	Once the UDP packets exceeded the defined value, the R-300NP will start to discard the subsequent UDP packets. **Interface:** WAN/LAN, WAN, LAN
Block ICMP Flood Attack And Smurf Attack	Enable 50 packets/ per sec WAN/LAN	Similar to the UDP flood defense function, once the thresholds of ICMP packets have exceeded the defined value, the R-300NP will discard the ICMP echo requests coming from the Internet. And R-300NP will also ignore any broadcasting ICMP echo request. **Interface:** WAN/LAN, WAN, LAN
Port Scan Defence	Enable WAN/LAN	Enables/disables R-300NP from responding to Internet based port scans. This feature is designed to protect your private local network from Internet based hackers who attempt to gain unsolicited access your network by detecting open IP ports on R-300NP. **Interface:** WAN/LAN, WAN, LAN

3-3 System Status

Display R-300NP system basic status, including,

1. System
2. Current User
3. DHCP Clients
4. Session List

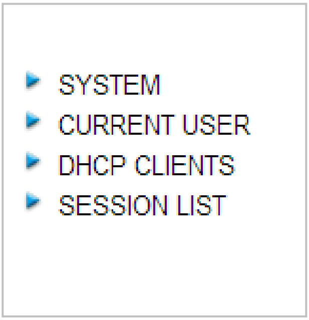
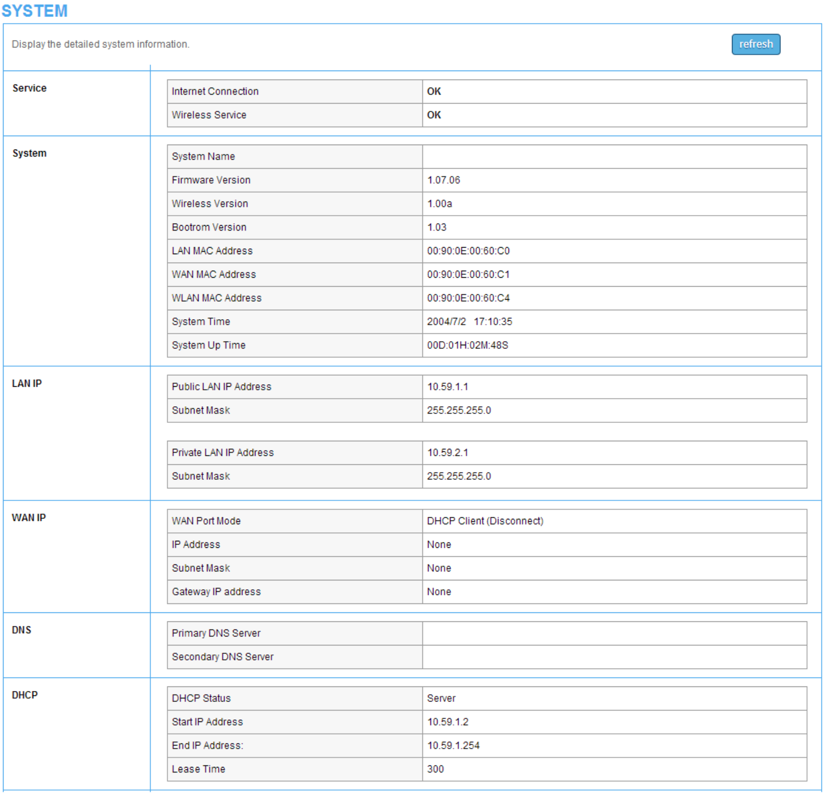


Figure 43 System Status Item Screen

3-3-1 System

The System Information Menu displays current system basic information including the service connection message, host name, LAN, WAN, DHCP Configuration, DNS, E-mail Redirection, SSL Certificate, network traffic Information and the system firmware version.

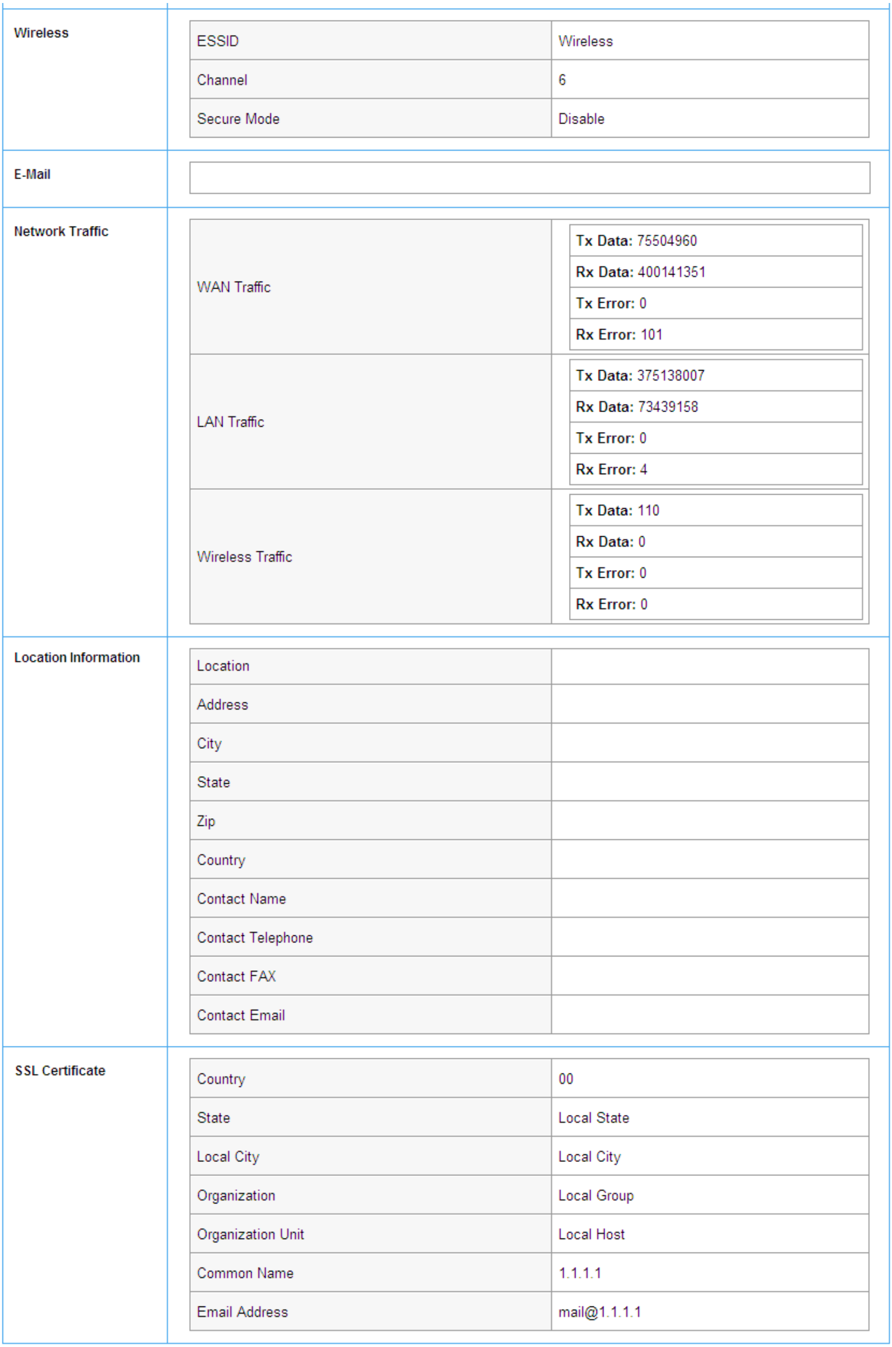


SYSTEM

Display the detailed system information.

Service	Internet Connection	OK
	Wireless Service	OK
System	System Name	
	Firmware Version	1.07.06
	Wireless Version	1.00a
	Bootrom Version	1.03
	LAN MAC Address	00:90:0E:00:60:C0
	WAN MAC Address	00:90:0E:00:60:C1
	WLAN MAC Address	00:90:0E:00:60:C4
	System Time	2004/7/2 17:10:35
	System Up Time	00D:01H:02M:48S
LAN IP	Public LAN IP Address	10.59.1.1
	Subnet Mask	255.255.255.0
	Private LAN IP Address	10.59.2.1
	Subnet Mask	255.255.255.0
WAN IP	WAN Port Mode	DHCP Client (Disconnect)
	IP Address	None
	Subnet Mask	None
	Gateway IP address	None
DNS	Primary DNS Server	
	Secondary DNS Server	
DHCP	DHCP Status	Server
	Start IP Address	10.59.1.2
	End IP Address:	10.59.1.254
	Lease Time	300

Figure 44 System Status Screen

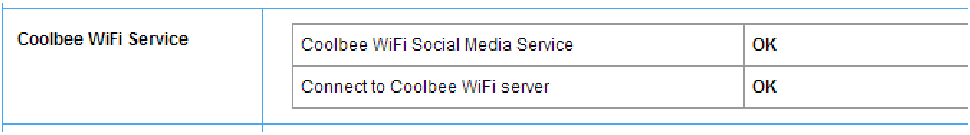


Wireless	ESSID	Wireless
	Channel	6
	Secure Mode	Disable
E-Mail		
Network Traffic	WAN Traffic	**Tx Data:** 75504960 **Rx Data:** 400141351 **Tx Error:** 0 **Rx Error:** 101
	LAN Traffic	**Tx Data:** 375138007 **Rx Data:** 73439158 **Tx Error:** 0 **Rx Error:** 4
	Wireless Traffic	**Tx Data:** 110 **Rx Data:** 0 **Tx Error:** 0 **Rx Error:** 0
Location Information	Location	
	Address	
	City	
	State	
	Zip	
	Country	
	Contact Name	
	Contact Telephone	
	Contact FAX	
	Contact Email	
SSL Certificate	Country	00
	State	Local State
	Local City	Local City
	Organization	Local Group
	Organization Unit	Local Host
	Common Name	1.1.1.1
	Email Address	mail@1.1.1.1

Figure 45 System Status Screen

- **R-300NP connect to Coolbee WiFi service**

If you R-300NP have registered on Coolbee WiFi and have been switch to Coolbee WiFi mode(Social Media Authentication enable), you will see the status of Coolbee WiFi on the top of the system page as below.



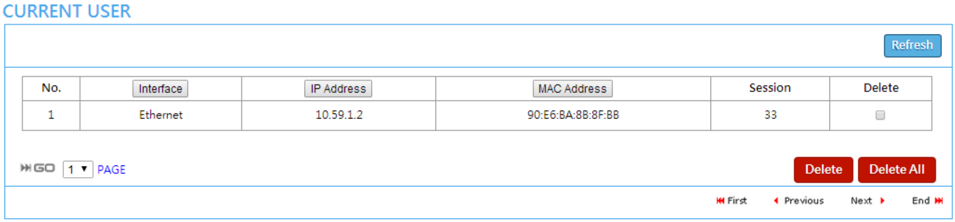
Coolbee WiFi Service

Coolbee WiFi Social Media Service	OK
Connect to Coolbee WiFi server	OK

Figure 46 System Status Screen

3-3-2 Current User

Display the current logged-in subscribers' status. It allows the service provider to disconnect any subscribers.



CURRENT USER

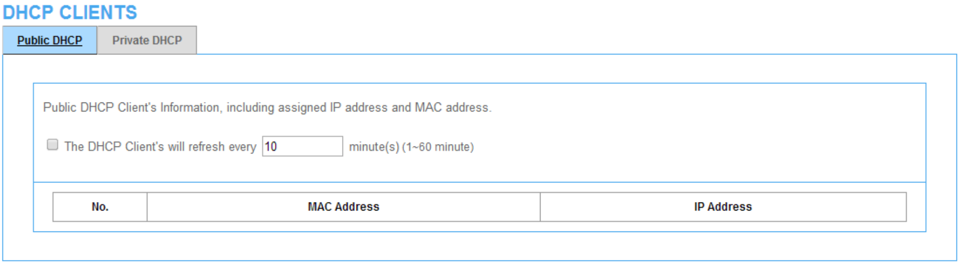
No.	Interface	IP Address	MAC Address	Session	Delete
1	Ethernet	10.59.1.2	90:E6:BA:8B:8F:BB	33	□

Figure 47 Current User List (No Authentication)

Item	Description
Refresh	Click on refresh button to update the current user list page.
IP Address	Click the column button to sort the column in ascending/descending order.
MAC Address	Click the column button to sort the column in ascending/descending order.
Delete	Select the check boxes and click "**Delete**" to delete accounts.
Delete All	Delete all accounts in current user list.

3-3-3 DHCP Clients

The DHCP client table shows the current DHCP users for both Public DHCP and Private DHCP.



DHCP CLIENTS

Public DHCP Client's Information, including assigned IP address and MAC address.

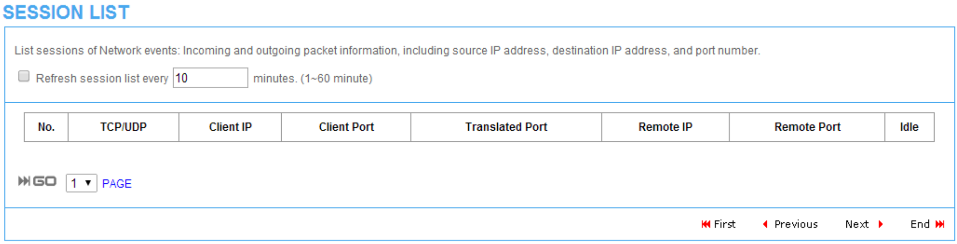
□ The DHCP Client's will refresh every 10 minute(s) (1~60 minute)

No.	MAC Address	IP Address

Figure 48 Current User Screen

3-3-4 Session List

The administrator could remote monitor the real time usage status of R-300NP via this page.



SESSION LIST

List sessions of Network events: Incoming and outgoing packet information, including source IP address, destination IP address, and port number.

□ Refresh session list every 10 minutes. (1~60 minute)

No.	TCP/UDP	Client IP	Client Port	Translated Port	Remote IP	Remote Port	Idle

Figure 49 Session List Screen

3-4 System Tools

This allows service provider or administrator to process Firmware upgrade, change password and backup or restore configuration.

1. CONFIGURATION
2. FIRMWARE
3. SYSTEM ACCOUNT
4. PING COMMAND
5. RESTART
6. LOGOUT

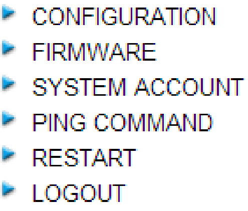
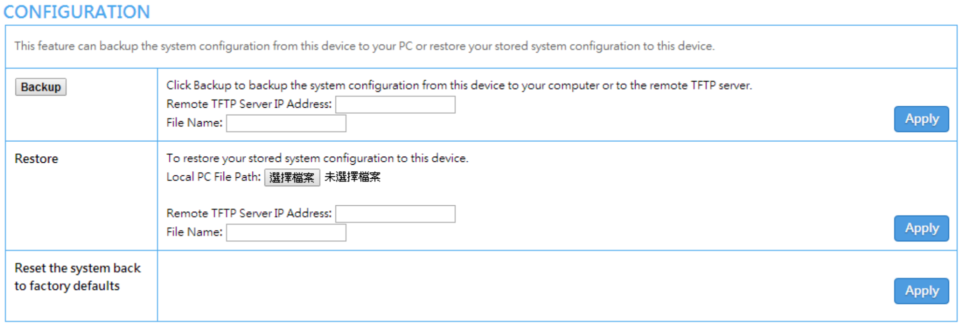


Figure 50 System Tools Item

3-4-1 Configuration

Use the Configuration item to save, restore or reset configuration parameters of the R-300NP.



CONFIGURATION

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.

Backup

Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server.

Remote TFTP Server IP Address:

File Name:

Apply

Restore

To restore your stored system configuration to this device.

Local PC File Path: 選擇檔案 未選擇檔案

Remote TFTP Server IP Address:

File Name:

Apply

Reset the system back to factory defaults

Apply

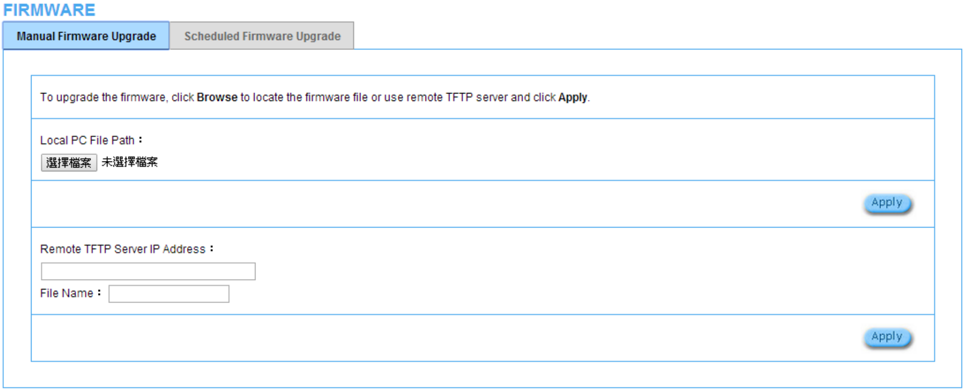
Figure 51 Configuration Setting Screen

Item	Default	Description
Backup	Click it to save the system configuration to your computer. (The default file name is “export.cfg”) or it could be save to the TFTP you assigned.	
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server that you would like to store the system backup file.
File Name	Empty	Enter the file name for the system backup file.
Restore	Click it to restore your system configuration, you could choose the file from your computer or TFTP server.	
Local PC File Path	Empty	Enter the file pathname of the system configuration file in the Local PC File Path field.
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server where the system configuration file is stored.
File Name	Empty	Enter the file name that you use to restore the system.
Reset the system back to factory defaults	Click it to erase all setting and back to factory default.	

3-4-2 Firmware

This function allows you to upgrade the firmware of your R-300NP.

● **Manual Firmware Upgrade**



FIRMWARE

To upgrade the firmware, click **Browse** to locate the firmware file or use remote TFTP server and click **Apply**.

Local PC File Path：

選擇檔案 未選擇檔案

Apply

Remote TFTP Server IP Address：

File Name：

Apply

Figure 52 Manual Firmware Upgrade Setting Screen

Item	Default	Description
This allow administrator to upgrade the firmware via local file.		
Local PC File Path	Empty	Select the file from local PC.
This allows administrator use TFTP server to upgrade firmware.		
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.

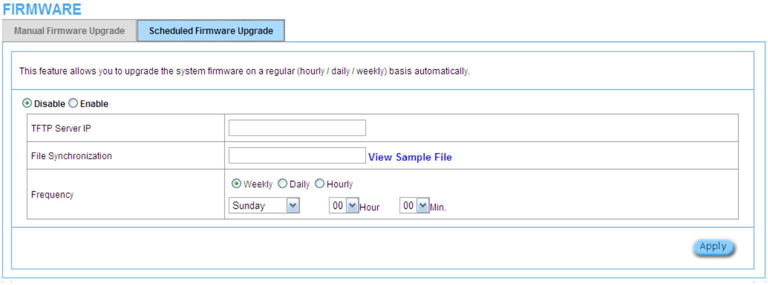
Note:

1. Before downloading the new firmware, users must save the configuration file for restore configuration parameters of the device.

2. Do not remove power during the upgrade process. This will damage the unit.

● Scheduled Firmware Upgrade

Scheduled Firmware Upgrade is a program that enables an automatic upgrade to the latest firmware version through the TFTP server.



FIRMWARE

Manual Firmware Upgrade | Scheduled Firmware Upgrade

This feature allows you to upgrade the system firmware on a regular (hourly / daily / weekly) basis automatically.

● Disable ○ Enable

TFTP Server IP	
File Synchronization	View Sample File
Frequency	● Weekly ○ Daily ○ Hourly Sunday 00 Hour 00 Min.

Apply

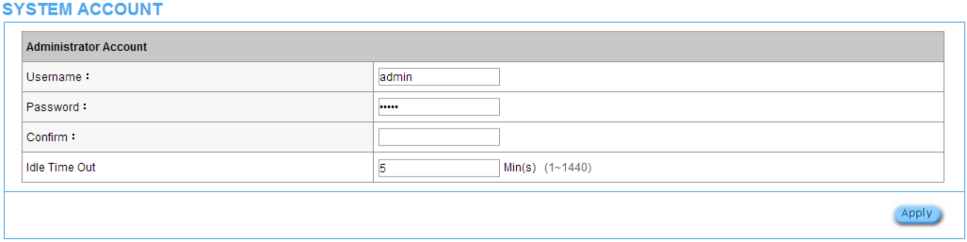
Figure 53 Scheduled Firmware Upgrade Setting Screen

Item	**Default**	**Description**
Disable/Enable	Disable	Disable or enable the scheduled firmware upgrade function.
TFTP Server IP	Empty	Enter the IP address of TFTP Server.
File Synchronization	Empty	Enter the file name and location in the File Synchronization field.
View Sample File	Click the button to display synchronization file example.	
Frequency	Weekly	Set the firmware upgrade time. The default value is “Weekly”.

***Note:** Do not turn the power off during the upgrade process. This will damage the unit.*

3-4-3 System Account

Use the System Account screen to change the administrator setting.



SYSTEM ACCOUNT

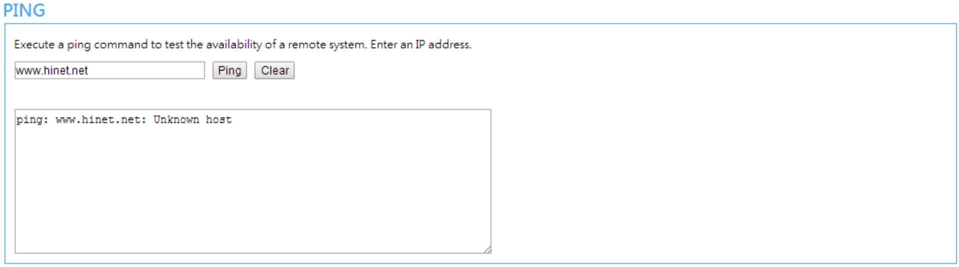
Administrator Account	
Username :	admin
Password :	•••••
Confirm :	
Idle Time Out	5 Min(s) (1~1440)

Figure 54 System Account Setting Screen

Item	Description
Username	The username can consist of up to 20 alphanumeric characters and is sensitive.
Password	The password can consist of up to 20 alphanumeric characters and is sensitive.
Confirm	The password for confirmation.
Idle Time Out	The user idle time out valid is 1 to 1440 minutes. If the idle time out is set as 5 minutes, it means if the account doesn't send packet in 5 minutes, the account will logout automatically.

3-4-4 PING Command

The Ping function can check the R-300NP networking connect status.



PING

Execute a ping command to test the availability of a remote system. Enter an IP address.

www.hinet.net

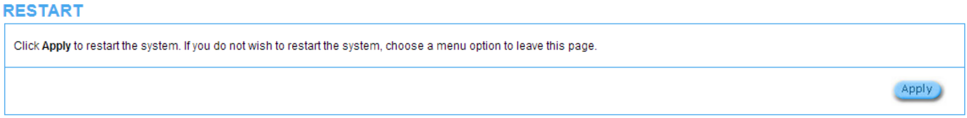
```
ping: www.hinet.net: Unknown host
```

Figure 55 Ping Command Screen

Item	Description
IP or URL	Enter the IP address or the URL link of the unit that you would like to check.

3-4-5 Restart

If your R-300NP is not running normally, you can choose this option to restart R-300NP. Click the "**Apply**" button to restart the R-300NP with all of your settings remaining the same.

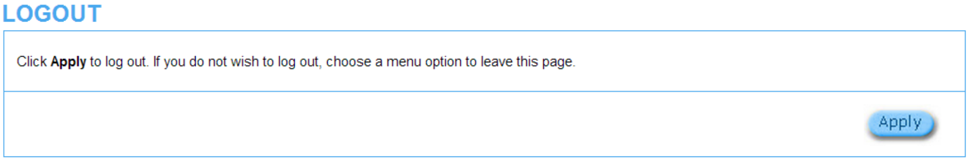


Click **Apply** to restart the system. If you do not wish to restart the system, choose a menu option to leave this page.

Figure 56 Restart Screen

3-4-6 Logout

If you would like to leave the configuration page, please click "**Apply**" to exit.



Click **Apply** to log out. If you do not wish to log out, choose a menu option to leave this page.

Figure 57 Logout Screen

Appendix A Regulations/EMI Compliance

FCC Warning statement

For FCC 15b devices

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

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

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

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 RF Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

NCC Statement

低功率射頻電機設備警語

依據低功率電波輻射性電機管理辦法

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

NTC Thailand:

“This telecommunication equipment conforms to NTC technical requirement.”

Appendix D LIMITED WARRANTY

What the warranty covers:

We warrant its products to be free from defects in material and workmanship during the warranty period. If a product proves to be defective in material or workmanship during the warranty period, we will at its sole option repair or replace the product with a like product. Replacement product or parts may include remanufactured or refurbished parts or components.

How long the warranty is effective:

The Easy Hotspot Kit is warranted for one year for all parts and one year for all labor from the date of the first consumer purchase.

Who the warranty protects:

This warranty is valid only for the first consumer purchaser.

What the warranty does not cover:

1. Any product, on which the serial number has been defaced, modified or removed.
2. Damage, deterioration or malfunction resulting from:
   a. Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
   b. Repair or attempted repair by anyone not authorized by us.
   c. Any damage of the product due to shipment.
   d. Removal or installation of the product.
   e. Causes external to the product, such as electric power fluctuations or failure.
   f. Use of supplies or parts not meeting our specifications.
   g. Normal wears and tear.
   h. Any other cause that does not relate to a product defect.
3. Removal, installation, and set-up service charges.

How to get service:

1. For information about receiving service under warranty, contact our **Customer Support**.
2. To obtain warranted service, you will be required to provide (a) the original dated sales slip, (b) your name, (c) your address, (d) a Description of the problem and (e) the serial number of the product.
3. Take or ship the product prepaid in the original container to your dealer, and our service center.
4. For additional information, contact your dealer or our **Customer Service Center**.

Limitation of implied warranties:

THERE ARE NO WARRANTIED, EXPRESSED OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION CONTAINED HEREIN INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Exclusion of damages:

OUR LIABILITY IS LIMITED TO THE COST OF REPAIR OR REPLACEMENT OF THE PRODUCT.

We SHALL NOT BE LIABLE FOR:

1. DAMAGE TO OTHER PROPERTY CAUSED BY ANY DEFECTS IN THE PRODUCT, DAMAGES BASED UPON INCONVENIENCE, LOSS OF USE OF THE PRODUCT, LOSS OF TIME, LOSS OF PROFITS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, INTERFERENCE WITH BUSINESS RELATIONSHIPS, OR OTHER COMMERCIAL LOSS, EVEN IF ADVISED OF THE POSSIBLITY OF SUCH DAMAGES.
2. ANY OTHER DAMAGES, WHETHER INCIDENTAL, CONSEQUENTIAL OR OTHERWISE.
3. ANY CLAIM AGAINST THE CUSTOMER BY ANY OTHER PARTY.