

# IX-T01 WiFi

## IX-T01 WiFi Extended User Manual



# IX-T01 WiFi

## Product summarize

### Product Feature

- ◆ Integrates router, wireless access point, four-port switch and firewall in one
- ◆ Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
- ◆ MIMO technology utilizes reflection signal to increase eight times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
- ◆ Provides 150Mbps transmission rates
- ◆ Supports WMM to make your voice and video more smooth
- ◆ Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
- ◆ Supports remote/local Web management
- ◆ Supports wireless Roaming technology and ensures high-efficient wireless connections
- ◆ Supports wireless SSID stealth mode and MAC address access control
- ◆ Supports Auto MDI/MDIX
- ◆ Provides system log to record the status of the router
- ◆ Supports MAC address filtering, NAT, NAPT
- ◆ Supports UPnP and DDNS
- ◆ Supports the access control over 30 MAC addresses
- ◆ Supports DHCP server/client
- ◆ Supports SNTP
- ◆ Supports auto wireless channel selection
- ◆ Supports WDS function (wireless distribution system)

# IX-T01 WiFi

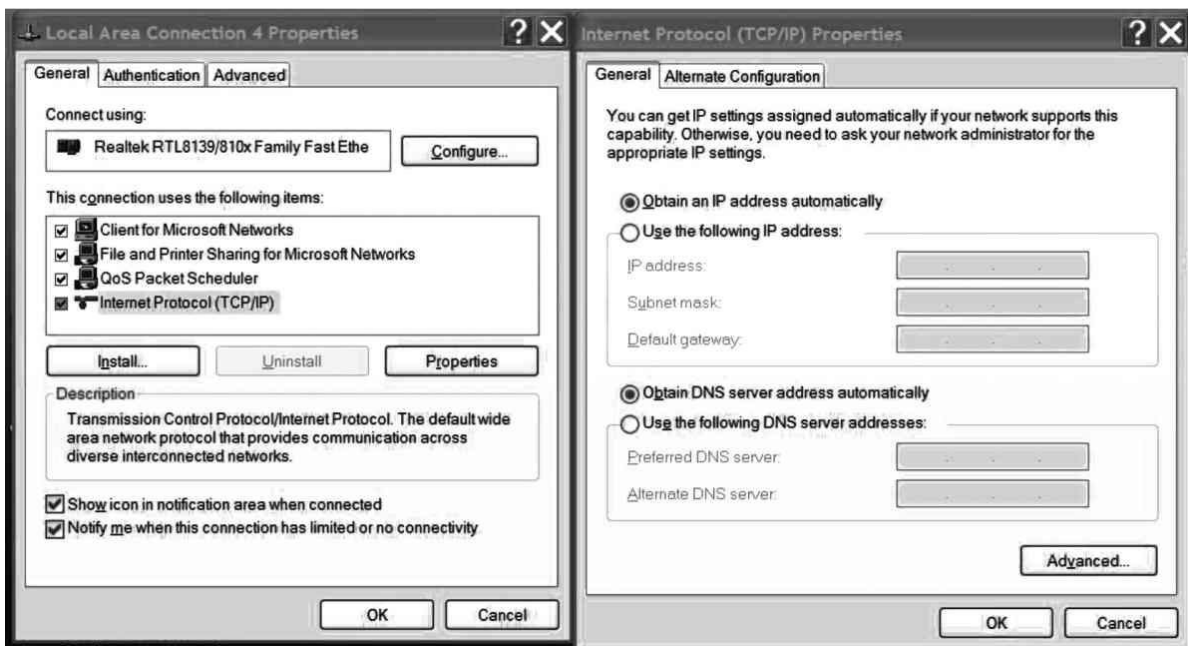
## 1 : Software Configuration

### Basic Configuration

1) Search the wireless network, connect to IX-T01 WiFi



2) Set the IP address. You can set static IP or you can enable DHCP. Set your IP address through the properties of "Internet Protocol (TCP/IP)". Generally, the DHCP server of the router is on, so please select "Obtain an IP address automatically" and "Obtain DNS server address automatically" under the "General" tab.



# IX-T01 WiFi

## Tips:

Only when the DHCP server of the router is enabled should you select “Obtain an IP address automatically”. You can set the IP address by yourself instead. However, the IP address of the computer and router should be set within the same subnet and may not share an IP address. The default IP address is 192.168.16.254 and the subnet mask is 255.255.255.0, so the IP address should not be 192.168.16.254.

3) You can find the assigned address under the “Support” tab as follows:



4) Click on Start | Programs | Accessories | Command Prompt, type ping 192.168.16.254, and press Enter (as shown below). If the screen displays the following figure, your PC has connected to the router successfully.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.16.254

Pinging 192.168.16.1 with 32 bytes of data:

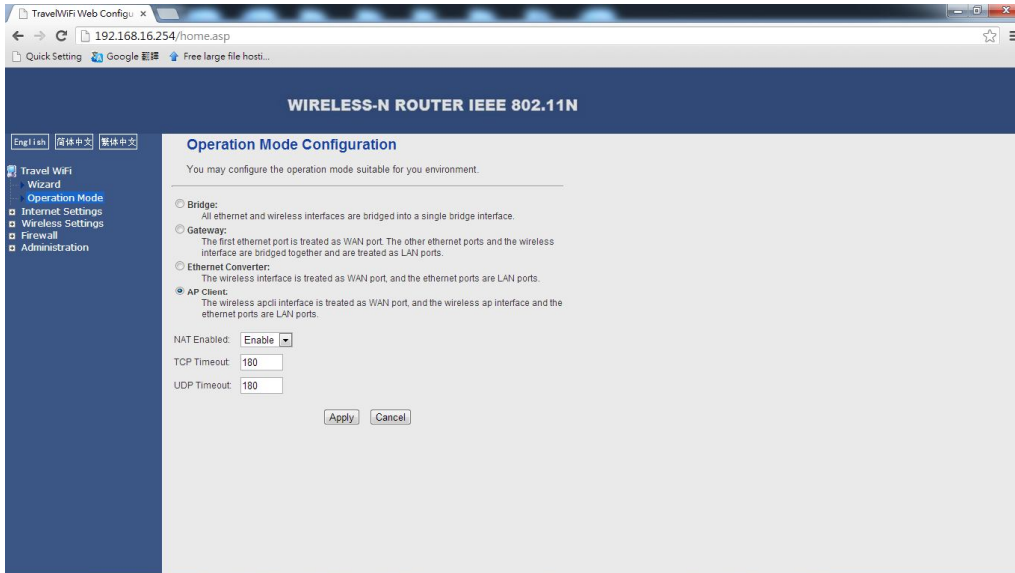
Reply from 192.168.16.254 : bytes=32 time<1ms TTL=64
Reply from 192.168.16.254 : bytes=32 time<1ms TTL=64
Reply from 192.168.16.254 : bytes=32 time<1ms TTL=64
Reply from 192.168.16.254 : bytes=32 time<1ms TTL=64

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

# IX-T01 WiFi

5) To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, <http://192.168.16.254> Press "Enter". Click "OK".



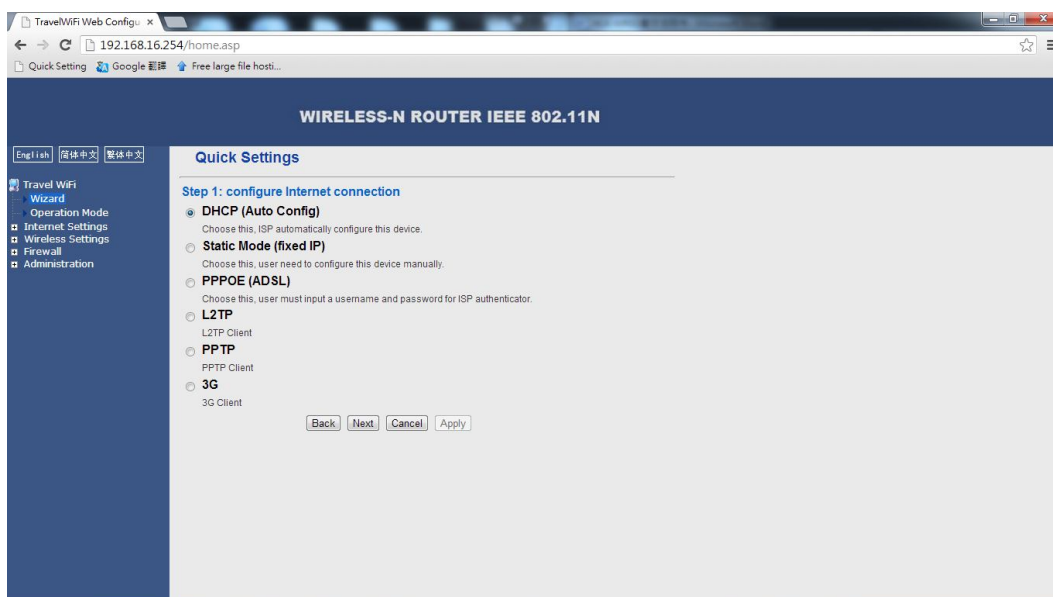
Congratulations! You have log in the manage website

## 1. Quick Set-Up

The router supports various functions and provides a quick setup The wizard can guide you to finish the basic setting, even though you may be unfamiliar with the router.

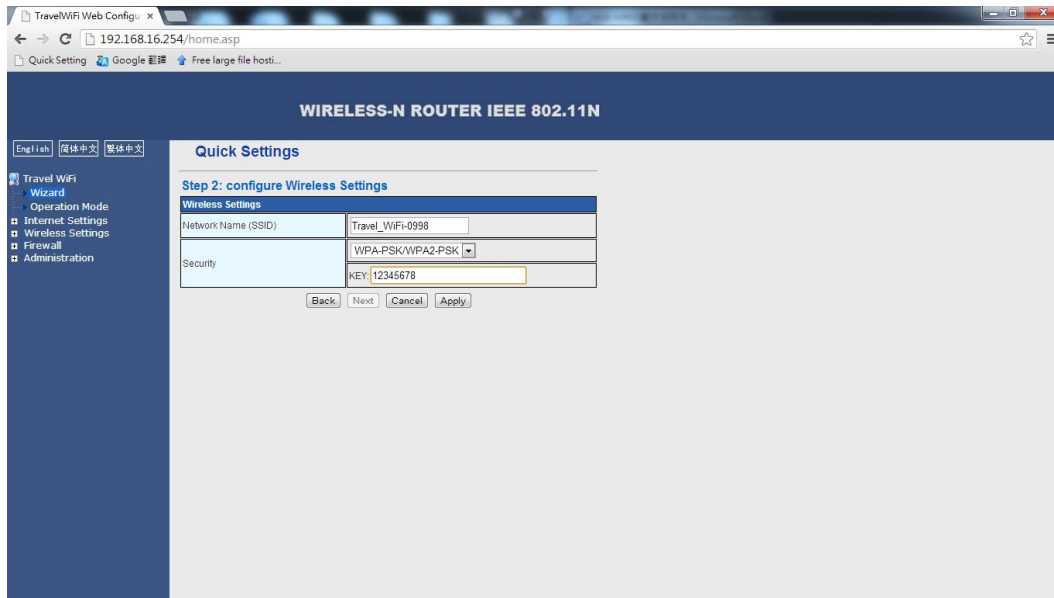
( 1 ) Click on Quick Setup in the left margin and click on Next in the right margin under "Quick setting". This will start the procedure for setting the router

( 2 ) This product supports any of 5 frequently-used modes to access a network. Choose one to suit your need. The default mode is pre-selected, which would support the parameters that are provided by your ISP. The other 4 modes below that default mode would require parameter settings for the network connection. If you do not know the parameters, please ask your ISP. After choosing a mode, click on the Next button



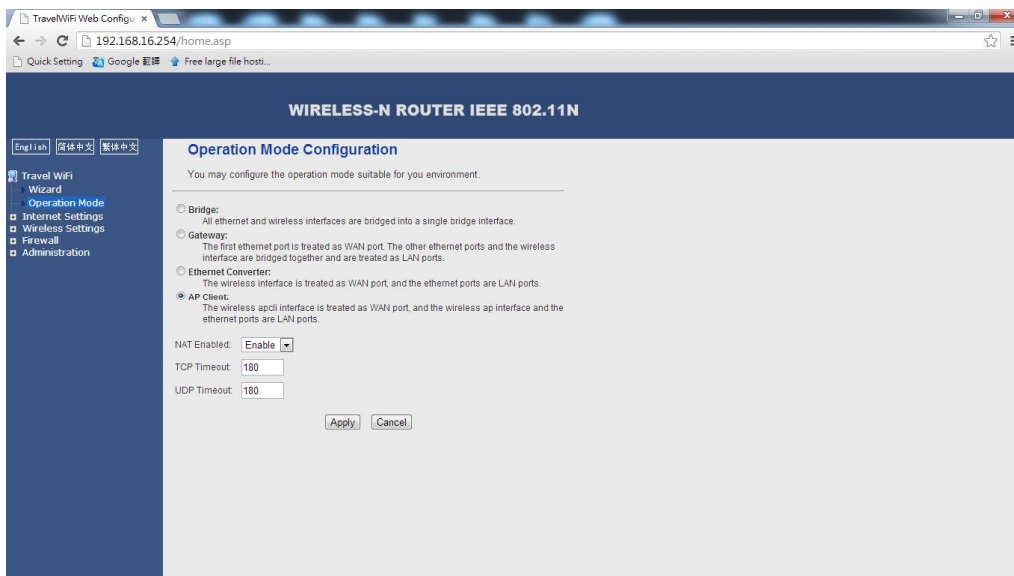
# IX-T01 WiFi

( 3 ) You can set a network name and corresponding encryption security for your wireless network settings, as shown below. Click on the Apply button to submit the setting information. The system will then reboot the computer to complete the router basic setting.



## Operation Mode

IX-T01 WiFi series wireless broadband router as a powerful router, it supports bridge mode and gateway mode, default mode is gateway.



## Bridge mode:

The router acts as an AP when operation mode is set to bridge mode. Also, the WEB managing function and all RJ-45 ports on the rear panel serve as LAN ports. Until now, the router has been acting only as a switch. It has been unable to access the WAN and the firewall has been disabled.

# IX-T01 WiFi

**Gateway mode:**

Gateway is the default mode. It is used to enable the NAT function to enable the router to transmit information easily with the Internet

**Ethernet Converter:**

The wireless interface is treated as WAN port, and the ethernet ports are LAN ports

**AP Client**

This mode the router is a AP, can connect to other wireless router also it can establish another wireless network, The RJ45 is LAN. This function can be used to make your wireless more farther.

# IX-T01 WiFi

## 2 . Internet settings

### 2.1. WAN Connection Mode:

This router supports several common methods of WAN connections. Select the connection method to what your network operator uses and select the correct parameter information (likely provided by your ISP). Then, you can share the Internet normally. If you use dynamic connection, 3G dial-up connection, PPPoE dial-up connection, etc., there are two ways to verify whether the connection will work. One way is to browse the web site directly, and the other is to distinguish it according to the Internet configuration state.

### . Connection Mode 1 Static IP

**wan title**

Choose your connection type and their parameters here.

---

---

WAN Connection Type:

Static Mode	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="4.4.4.4"/>

MAC Clone	
Select	<input type="text" value="Disable"/>

MTU value setting	
MTU Value	<input type="text" value="1492"/>

In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields.

**IP Address:** Here enter the WAN IP address provided by your ISP.

**Subnet Mask:** Enter the WAN Subnet Mask here.

**Gateway:** Enter the WAN Gateway here.

**Primary DNS Server:** Enter the Primary DNS server provided by your ISP.

**Secondary DNS Server:** Enter the secondary DNS



# IX-T01 WiFi

## Connection Mode 2: Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect

WAN Connection Type:	DHCP (Auto config) ▼
<b>DHCP Mode</b>	
Hostname(Optional)	<input type="text"/>
<b>MAC Clone</b>	
Select	Disable ▼
<b>MTU value setting</b>	
MTU Value	1492
Save Apply Cancel	

## Connection Mode 3: ADSL Virtual Dial-up (Via PPPoE)

Enter the User Name and Password provided by your ISP

WAN Connection Type:	PPPoE (xDSL) ▼
<b>PPPoE Mode</b>	
User Name	pppoe_user
Password	●●●●●●●●
Verify Password	●●●●●●●●
Operation Mode	Keep Alive ▼
	Keep Alive Mode: Redial Period 60 seconds
	On demand Mode: Idle Time 5 minutes
Connect Disconnect	
<b>MAC Clone</b>	
Select	Disable ▼
<b>MTU value setting</b>	
MTU Value	1492
Save Apply Cancel	

# IX-T01 WiFi

## Connection Mode 4: L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP use a L2TP connection, your ISP will provide you with a username and password please fill in the parameters.

L2TP provides two access modes.

If the L2TP offered by your ISP is Dynamic IP: Please select Dynamic IP.

If the L2TP offered by your ISP is Static IP: Please fill in the parameters provided by your ISP. After configuration.

WAN Connection Type:		L2TP
<b>L2TP Mode</b>		
Server IP	l2tp_server	
User Name	l2tp_user	
Password	●●●●●●●●	
Address Mode	Static	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.254	
Operation Mode	Keep Alive	
	Keep Alive Mode: Redial Period 60 seconds	
<b>MAC Clone</b>		
Select	Disable	
<b>MTU value setting</b>		
MTU Value	1492	
Save      Apply      Cancel		

**L2TP Server IP:** Enter the Server IP provided by your ISP.

**User Name:** Enter L2TP username.

**Password:** Enter L2TP password.

**Address Mode:** Select "Static" if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

**IP Address:** Enter the L2TP IP address supplied by your ISP.

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP.

**Default Gateway:** Enter the Default Gateway supplied by your ISP.

# IX-T01 WiFi

## Connection Mode 5: PPTP

If the connection is “PPP Tunneling Protocol”, please input the following parameters provided by your ISP: Server IP Address, User Name, and Password.

PPTP provides two access modes.

If the PPTP offered by your ISP is Dynamic IP: Please select Dynamic IP.

If the PPTP offered by your ISP is Static IP: Please fill in the parameters provided by your ISP. After configuration Click “**Apply**”, Router will Reboot.

WAN Connection Type:		PPTP
<b>PPTP Mode</b>		
Server IP	pptp_server	
User Name	pptp_user	
Password	●●●●●●●●	
Address Mode	Static	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.254	
Operation Mode	Keep Alive	
	Keep Alive Mode: Redial Period 60 seconds	
<b>MAC Clone</b>		
Select	Disable	
<b>MTU value setting</b>		
MTU Value	1492	
Save      Apply      Cancel		

**PPTP Server IP:** Enter the Server IP provided by your ISP.

**User Name:** Enter PPTP username provided by your ISP.

**Password:** Enter PPTP password provided by your ISP.

**Address Mode:** Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

**IP Address:** Enter the PPTP IP address supplied by your ISP.

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP.

**Default Gateway:** Enter the Default Gateway supplied by your ISP

# IX-T01 WiFi

## 2.2 LAN Connection Mode

The screenshot shows the 'Local Area Network (LAN) Settings' page of a WIRELESS-N ROUTER IEEE 802.11N. The page is in English and features a navigation menu on the left. The main content area is titled 'Local Area Network (LAN) Settings' and includes a sub-section 'LAN Setup' with a table of configuration fields. The fields are as follows:

LAN Setup	
IP Address	192.168.16.254
Subnet Mask	255.255.255.0
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	48-02-2A-00-09-97
DHCP Type	Server
Start IP Address	192.168.16.100
End IP Address	192.168.16.200
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.16.254
Secondary DNS Server	8.8.8.8
Default Gateway	192.168.16.254
Lease Time	86400
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
802.1d Spanning Tree	Disable
LLTD	Disable
IGMP Proxy	Disable
UPNP	Disable
PPPoE Relay	Disable
DNS Proxy	Enable

At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

# IX-T01 WiFi

**MAC Address:** The Router's physical MAC address as seen on your local network, which is unchangeable.

**IP Address:** The Router's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.16.1 is the default value

**Subnet Mask:** It's shown the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value

**DHCP Server:** Activate the checkbox to enable DHCP server

**IP Address Start/End:** Enter the range of IP address for DHCP server distribution.

**Subnet Mask:** Set a matching subnet mask according to the initial/end IP address.

**Primary DNS Server:** Fill in the Primary DNS server address (optional) provided by your ISP.

**Secondary DNS Server:** Fill in the Secondary DNS server address (optional) provided by your ISP.

**Default Gateway:** Set the gateway of the DHCP server according to the router's LAN IP address. The router's default gateway is 192.168.16.1.

**lease time:** The effective time (in seconds) of the dynamic IP address that the DHCP server allocates to the client host. The default is 86400. (86,400 seconds = 1 day). During this time, the server will not assign IP addresses to other hosts. (You can set the time according to your preference, which can improve the void IP address recovery efficiency of DHCP server.) Static specifies: You can set a scheme for DHCP to comply. Every time that DHCP assigns IP addresses automatically, it assigns a fixed IP address to the user's device. If necessary, fill in the designated MAC address and IP address.

**MAC address:** The MAC address of the PC that reserves a static IP address. (Example: 00:0C:43:80:88.)

**IP address:** The reserved IP address for a host in a network. (Example: 192.168.16.254.)

**802.11d Spanning Tree:** The Spanning Tree protocol, defined in 802.1d, is a bridge-to-bridge protocol in the link management. It provides a redundancy of pathways to prevent a cycle path. There is no default value.

**LLTD:** Options include Enabled, Disabled, and Open, Once there is an LLTP client, information about the router will display automatically.

**IGMP proxy:** It inhibits the occurrence of a multicast flood by effectively obtaining and controlling the user's information. This helps to reduce a network side agreement and the network load. There is no default.

**UPNP:** The router provides UPNP to P2P intranet software. There is no default.

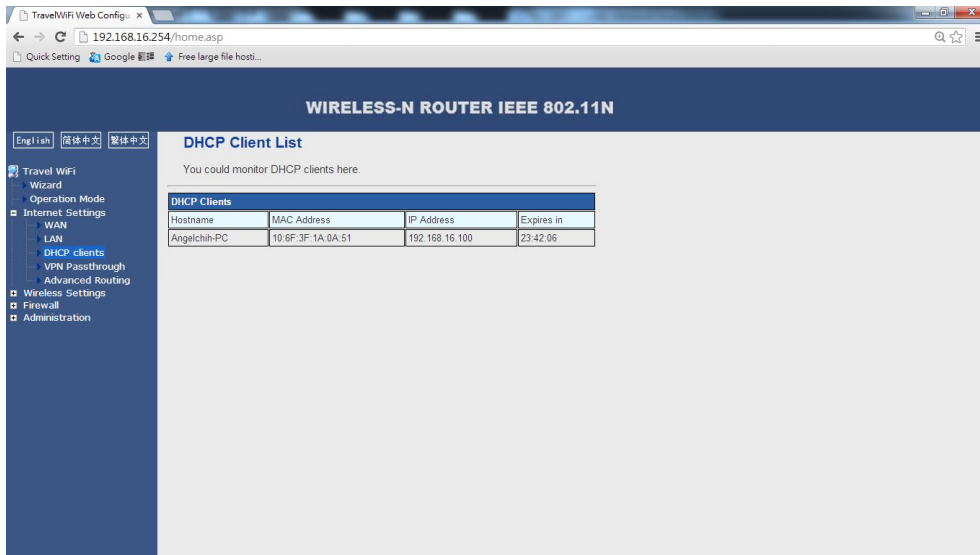
**Router advertising:** The router will send out or reply to broadcast information between each node at a fixed cycle to indicate its existence. There is no default.

**PPPOE Relay:** This function makes a local computer dial PPPoE separately and directly in the gateway mode. There is no default.

# IX-T01 WiFi

## 2.3 DHCP Clients

Select Internet Settings | DHCP clients to check the related computer information of the DHCP that automatically assigns IP addresses in the LAN such as network name, MAC address, IP address and expiration time.

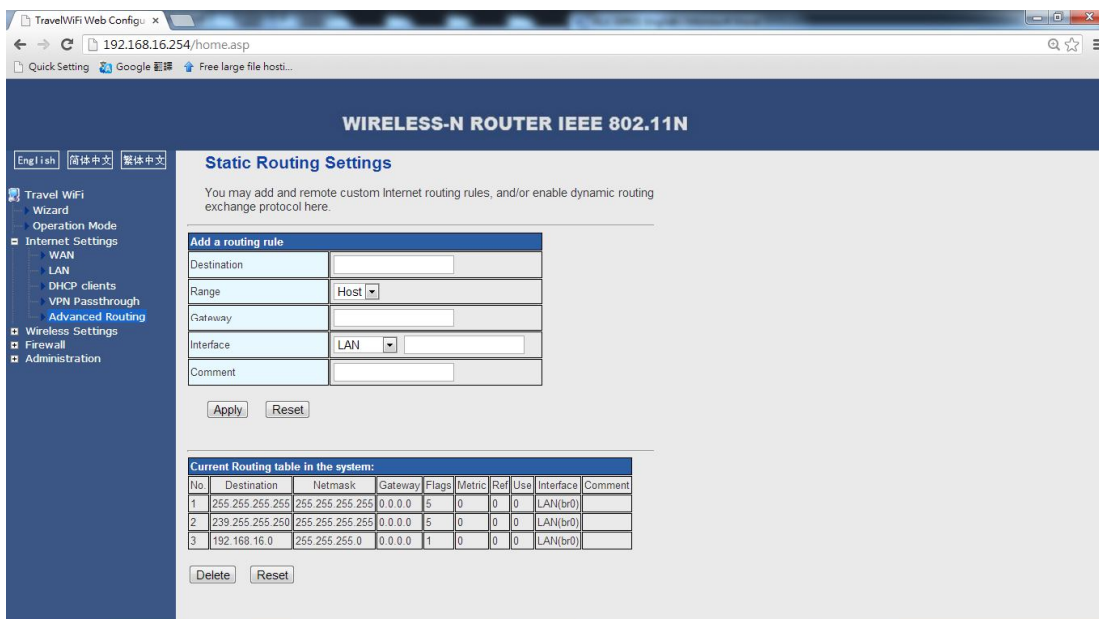


You could monitor DHCP clients here

Expires in: The length of the IP address lease

## 2.4 Advanced Routing

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here. This function is an option to add specific routing to a specific host if necessary. Appropriate use of static routers in a network can reduce routing selection problems and data overload of routing streams, so it can increase the transmitting speed of data packets. By setting the addresses of the IP, subnet mask, and gateway, a routing table can be set up. The destination IP address and subnet mask are used to determine a target network/host so that the router can send data packets to esignated target network/hosts through the gateway.



# IX-T01 WiFi

## 3 . Wireless Settings

### 3.1 Basic Settings

The screenshot shows the 'Basic Wireless Settings' page for a 'WIRELESS-N ROUTER IEEE 802.11N'. The page is in English. The left sidebar contains a navigation menu with options like 'Travel WiFi Wizard', 'Operation Mode', 'Internet Settings', 'Wireless Settings', 'Advanced', 'Security', 'WDS', 'WPS', 'Station List', 'Statistics', 'Firewall', and 'Administration'. The main content area is titled 'Basic Wireless Settings' and includes a sub-header 'Wireless Network' and 'HT Physical Mode'. Below these are various configuration fields and checkboxes.

Wireless Network	
Driver Version	2.6.0.1
Radio On/Off	<input type="button" value="RADIO OFF"/>
WiFi On/Off	<input type="button" value="WiFi OFF"/>
Network Mode	11b/g/n mixed mode
Network Name(SSID)	Travel_WiFi-0998 <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID1	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID2	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID3	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID4	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID5	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID6	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID7	<input type="text"/> <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	48:02:2A:00:09:97
Frequency (Channel)	2452MHz (Channel 9)
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2472MHz (Channel 13)
Space Time Block Coding(STBC)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
20/40 Coexistence	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Other	
HT TxStream	1
HT RxStream	1

Buttons: Apply, Cancel

**Radio On/Off:** On: the wireless router will radio Off:the router will not radio

**Wifi On/Off:** The router will broadcast the ssid if turn on. Turn Off means hide the ssid

**Network Mode:** Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.

**Multiple SSID:** Main Service Set Identifier. It's the "name" of your wireless network.

**Minor SSID:** Minor Service Set Identifier. It is optional.

**Broadcast (SSID):** Select "enable" to enable the device's SSID to be visible by wireless clients.

**BSSID:** It is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP

**Channel:** From the drop-menu, it is for selecting the working channels of the wireless network. Please select from 1 to 13, or select AutoSelect to select different channels. **Channel Bandwidth:** Select wireless work frequency 20M or 20/40M.

**HT TxStream:** RF Transmit Stream.

**HT RxStream:** RF Receive Stream.

# IX-T01 WiFi

## 3.2 Advanced Wireless Settings

TravelWiFi Web Configurator

192.168.16.254/home.asp

### WIRELESS-N ROUTER IEEE 802.11N

English 简体中文 繁体中文

#### Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable(only in A band)
Country Code	None

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	WMM Configuration

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply Cancel

**BG protection Mode:** Auto by default. You can select On or Off.

**Beacon Interval:** Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.

**Fragment Threshold:** Do not modify default value if you don't know what it is, default value is 2346.

**RTS Threshold:** Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.

**TX Power:** You can set the output power of wireless radio. Unless you're using this wireless router in a really big space, you may not have to set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).

**WMM Capable:** It will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is / not sure if you need it, it's safe to set this option to 'Enable', however, default value is enabling.

**APSD Capable:** It is used for auto power-saved service. The default is disabled



# IX-T01 WiFi

## 3.3 Security Settings

### 1.WEP Settings

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources.

**SSID Choice:** Select SSID to be configured security. The device supports to configure different security classes between the main SSID and the subordinate SSID.

**Security Mode:** There are several different security modes; you can choose one from mixed WEP, WPA-Personal, WPA-Enterprise, etc.

**Default Key:** Select a valid encryption key.

**WEP Key1, 2, 3, 4:** Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be **ASCII Characters** or **Hexadecimal Digits**

TravelWiFi Web Configu x

192.168.16.254/home.asp

Quick-Setting Google 翻譯 Free large file hosti...

### WIRELESS-N ROUTER IEEE 802.11N

English 简体中文 繁體中文

#### Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

**Select SSID**

SSID choice: Travel\_WiFi-0998

**"Travel\_WiFi-0998"**

Security Mode: OPENWEP

**Wire Equivalence Protection (WEP)**

Default Key: Key 1

WEP Keys	WEP Key 1 :	<input type="text"/>	Hex
	WEP Key 2 :	<input type="text"/>	Hex
	WEP Key 3 :	<input type="text"/>	Hex
	WEP Key 4 :	<input type="text"/>	Hex

**Access Policy**

Policy: Disable

Add a station Mac:

Apply Cancel

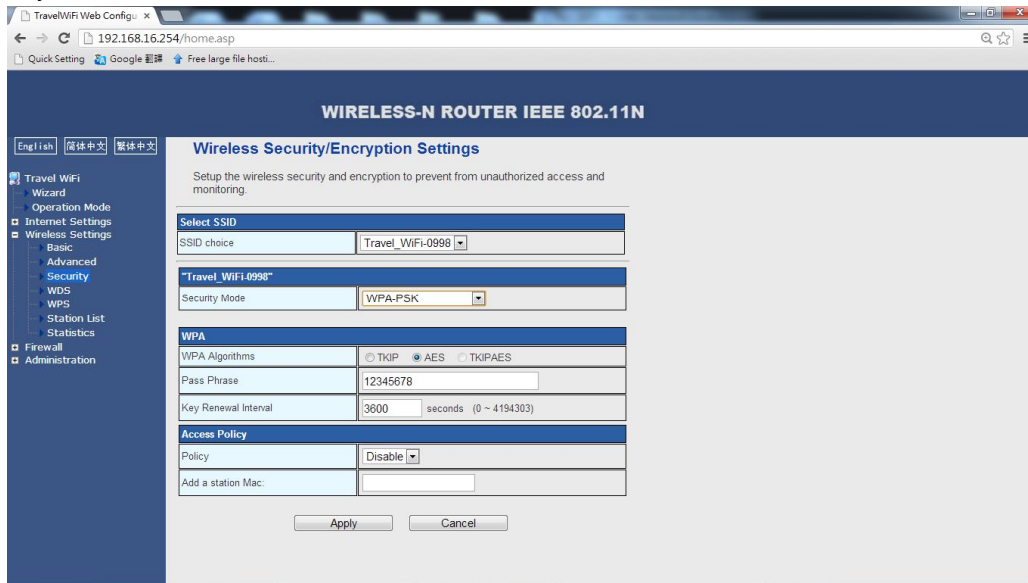
# IX-T01 WiFi

**2.WPA-PSK (Wi-Fi Protected Access),** a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP Temporal Key Integrity Protocol or AES Advanced Encryption Standard ) and can change the keys dynamically on every authorized wireless device.

**WPA Algorithms:** Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

**Pass Phrase:** Enter the key which must have 8-63 ASCII characters.

**Key Renewal Interval:** Enter the key renewal period. It is to tell the Router how often to change the keys.



The screenshot shows the 'Wireless Security/Encryption Settings' page for a 'WIRELESS-N ROUTER IEEE 802.11N'. The page is in English. The settings are as follows:

Select SSID	
SSID choice	Travel_WiFi-0998

"Travel_WiFi_0998"	
Security Mode	WPA-PSK

WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)

Access Policy	
Policy	Disable
Add a station Mac:	

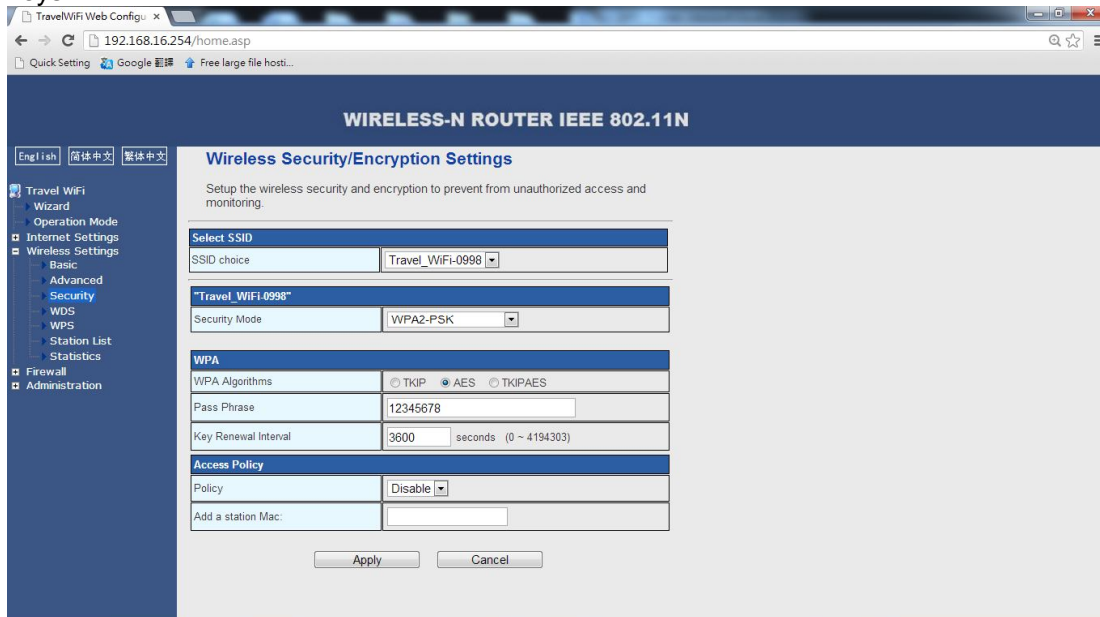
Buttons: Apply, Cancel

**3.WPA2-PSK (Wi-Fi Protected Access version 2),** It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.

**WPA Algorithms:** Select key Algorithms such as TKIP, AES and TKIP&AES.

**Pass Phrase:** Enter the key which must have 8-63 ASCII characters.

**Key Renewal Interval:** Enter the key renewal period. It is to tell the Router how often to change the keys.



The screenshot shows the 'Wireless Security/Encryption Settings' page for a 'WIRELESS-N ROUTER IEEE 802.11N'. The page is in English. The settings are as follows:

Select SSID	
SSID choice	Travel_WiFi-0998

"Travel_WiFi_0998"	
Security Mode	WPA2-PSK

WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)

Access Policy	
Policy	Disable
Add a station Mac:	

Buttons: Apply, Cancel

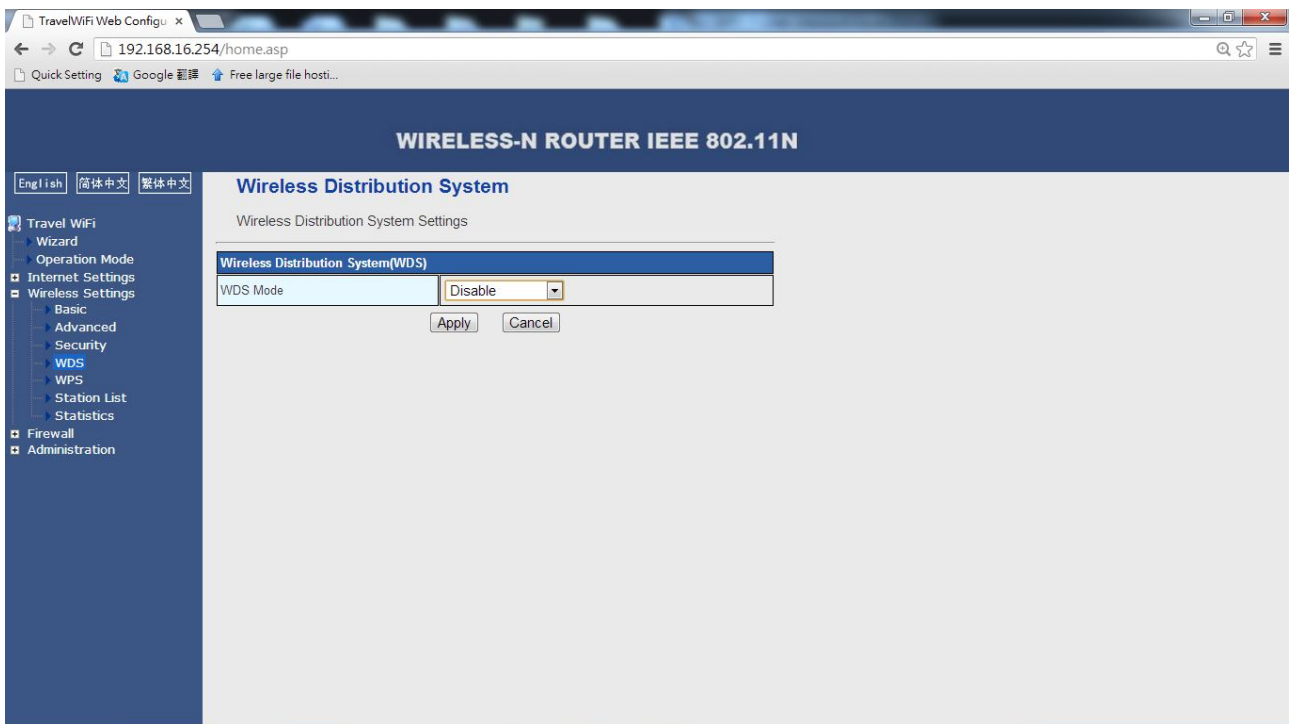
# IX-T01 WiFi

## 3.4 WDS

Click on Wireless Settings | WDS, enter your wireless distribution system interface to enable the WDS, or select the WDS (Wireless Distribution System) mode. WDS opens the WDS function on the radio equipment, establishes the WDS trust and communication, extends the expansion wireless signal, and enables wide wireless network coverage.

Note: In order to use this function, the users must all be equipped with the WDS function and must all be WDS members. Also, the channel of each transmission point must not set the automatic channel choice. The same channel and same working mode are required to be set at each transmission point. WDS member machines are located in different IP addresses of an identical network segment. If the DHCP function is needed, enable just one of the machines and disable other DHCPs. Use the identical product brand (model and series) to obtain better compatibility and to enable the connection for as long as possible.

All IX-T01 WiFi products support 3 modes: Lazy Mode, Bridge Mode, and Repeater Mode.



# IX-T01 WiFi

## Lazy Mode

There is no need to fill in the BSSID of the opposite party in this mode. The WDS connection is now a passive connection, so the other party should fill in the BSSID address of the router. This means that the WDS mode of the other party's machine can only be in a non-Lazy mode (Bridge or repeater mode). Also, the WDS connections of the machines must be in the same physical mode, they must be on the same wireless channel (not on Auto), and they must have the same wireless encryption type (not supporting the Mix encryption type like WPAPSKWPA2PSK). The machines must each have unique IP addresses on the same network. Open only DHCP function; close other DHCP function.

**Phy Mode:** Select the supporting Physical mode (CCK, OFDM, or HTMIX). The same physical mode must exist for all of the connecting equipment.

**Encrypt Type:** Select NONE (no encryption type). There are 3 types: WEP, TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard). You can set a maximum of 4 different types and can use these types to connect to 4 different clients. Note: The same encryption type must exist for all of the equipment to the connection to be established.

**Encrypt Key:** Input a new key here after choosing the encryption type.

## Bridge Mode

The Bridge mode requires the BSSID of the other client to be filled in. The AP SSID of this router will be shielded so that the wireless client will not be able to determine this router. The wired client can use a WAN port to access the Internet.

**Phy Mode:** Select the supporting physical mode (CCK, OFDM, or HTMIX). The same physical mode is required for all connecting equipment.

**Encrypt Type:** Select NONE (no encryption type). There are 3 types: WEP, TKIP (Temporal Key Integrity Protocol), and AES (Advanced Encryption Standard). You can set a maximum of 4 different types and can use these types to connect to 4 different clients. Note: The same encryption type must exist for all connecting equipment in order to establish a connection.

**AP MAC address:** Fill in the BSSID of the WDS connecting equipment. You can fill in 4 different BSSIDs in order to enable one-to-many connections.

## Repeater Mode

You have to input the BSSID of the connected equipment. Either a wireless client or a wired client (not a bridge) can connect to the network in the WDS mode.

# IX-T01 WiFi

## 3.5 WPS

WPS (Wi-Fi Protected Setup) is a standard to establish an easy and secure wireless client and router. It is created by the Wi-Fi Alliance, so you don't need to choose the encryption type or to set the key. You can set the WPS by inputting the right PIN code or by pressing the WPS/RESET button on the panel.

The screenshot shows the 'Wi-Fi Protected Setup' configuration page in a web browser. The page title is 'WIRELESS-N ROUTER IEEE 802.11N'. The browser address bar shows '192.168.16.254/home.asp'. The page has a navigation menu on the left with options like 'Travel WiFi', 'Wizard', 'Operation Mode', 'Internet Settings', 'Wireless Settings', 'Basic', 'Advanced', 'Security', 'WDS', 'WPS', 'Station List', 'Statistics', 'Firewall', and 'Administration'. The main content area is titled 'Wi-Fi Protected Setup' and contains three sections: 'WPS Config', 'WPS Summary', and 'WPS Progress'. The 'WPS Config' section has a 'WPS' dropdown menu set to 'Enable' and an 'Apply' button. The 'WPS Summary' section displays various parameters: WPS Current Status (Idle), WPS Configured (No), WPS SSID (Travel\_WiFi-0998), WPS Auth Mode (WPA2-PSK), WPS Encryp Type (AES), WPS Default Key Index (2), WPS Key(ASCII) (12345678), and AP PIN (00024556) with a 'Generate' button. There is also a 'Reset OOB' button. The 'WPS Progress' section has radio buttons for 'PIN' (selected) and 'PBC', a PIN input field, and an 'Apply' button. The 'WPS Status' section shows 'WSC: Idle' and a 'Cancel' button.

**WPS Config:** Select the Enable or Disable WPS function. You need to enable the WPS before you can use the WPS button on the panel to set the PBC encryption. (The default is Disabled.)

**WPS Summary:** This displays the parameters of the current WPS settings, including: WPS current status, SSID, authentication mode, encryption type, AP PIN, etc.

**Reset OOB:** Click this button to restore all WPS configurations to the default value.

**WPS Progress:** It supports 2 ways to configure WPS settings: PBC (Push-Button Configuration) and PIN (Personal Identification Number).

**PBC:** Select PBC or press the WPS button on the panel of the Router to 1 second. The WPS indicator will blink, allowing you to enable the client to implement the WPS/PBC.

**PIN:** You have to know the PIN code of the client for this option. Fill in the code and save it and use the same code for the client.

**WPS Status:** It displays the WPS current status. There are 3 states:

**WSC Idle:** It shows that the WPS current status is free.

**WSC Start WSC Process:** It shows that the WPS current status is sending a message.

**WSC Success:** It shows that access of the client to AP is successful and that a WPS connection has been established.

# IX-T01 WiFi

## 3.6 AP Client

This website will appear when the IX-T01 WiFi work at ap client mode.  
Choose a network, and press connect, it will appear the interface below:

The screenshot shows the 'AP Client Feature' configuration page. The page title is 'WIRELESS-N ROUTER IEEE 802.11N'. The left sidebar contains a navigation menu with 'AP Client' selected. The main content area has a heading 'AP Client Feature' and a sub-heading 'You could configure AP Client parameters here.' Below this is a form for 'AP Client Parameters' with the following fields:

SSID	AE-1
MAC Address (Optional)	
Security Mode	WPAPSK
Encryption Type	AES
Pass Phrase	Ae12345678

Below the form are 'Apply', 'Cancel', and 'SCAN' buttons. Underneath is a 'Site Survey' table:

Ch	SSID	BSSID	Security	Signal(%)	W-Moe	ExtCh	NT
5	Masco AP	84:c9:b2:7a:66:3c	WPA2PSK/TKIPAES	0	11b/g	NONE	In
6	Travel_WiFi-9A9E	48:02:2a:83:9a:9c	WPA2PSK/AES	60	11b/g/n	NONE	In
8	wedtex01	60:a4:4c:39:f3:58	WPA2PSK/AES	20	11b/g/n	BELOW	In
9	AE-1	b0:48:7a:e6:5f:dc	WPAPSK/TKIPAES	5	11b/g/n	BELOW	In

Type in the password and apply, it will connect to your another wireless router.

## 3.7 Station List

The screenshot shows the 'Station List' page. The page title is 'WIRELESS-N ROUTER IEEE 802.11N'. The left sidebar contains a navigation menu with 'Station List' selected. The main content area has a heading 'Station List' and a sub-heading 'You could monitor stations which associated to this AP here.' Below this is a table for 'Wireless Network' with the following data:

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
10:6F:3F:1A:0A:51	1	0	3	6	20M	0	0

You may monitor stations associated with the AP here.

# IX-T01 WiFi

## 4. Firewall

### 4.1. MAC/IP Binding

Input the MAC and IP of the need to control equipment , when this equipment get IP is different from set the IP , this equipment will be unable to access to the network, and when the equipment get IP and set the IP consistent are the same, but MAC is different, this equipment will be unable to access the network also

The screenshot shows the 'MAC/IP/Port Filtering Settings' page of a 'WIRELESS-N ROUTER IEEE 802.11N'. The page is in English and has a navigation menu on the left. The main content area is divided into three sections: 'Basic Settings', 'MAC/IP/Port Filter Settings', and 'Current MAC/IP/Port filtering rules in system'.

**Basic Settings**

MAC/IP/Port Filtering	Disable
Default Policy -- The packet that don't match with any rules would be:	Dropped

Buttons:

**MAC/IP/Port Filter Settings**

Source MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	None
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Accept
Comment	<input type="text"/>

(The maximum rule count is 32.)

Buttons:

**Current MAC/IP/Port filtering rules in system:**

No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									

Buttons:

# IX-T01 WiFi

## 4.2 MAC/IP/PORT Filtering

This function is used to manage the clients connected to the router, so that you can limit the client's Internet access. Before using this function, you need to choose Accept or Drop. A datapackage that does not match the rule will be Accept or Drop. Then, fill in the corresponding rules. The rules depend on your needs, so not all of the information needs to be filled in. As an example, if you want to prohibit a client whose IP address is 192.168.16.146 from accessing the Internet, just choose Accept and fill in 192.168.16.146 for the source IP address. This function can improve LAN user security and manageability.

The screenshot shows the configuration interface for a WIRELESS-N ROUTER IEEE 802.11N. The main heading is 'MAC/IP/Port Filtering Settings'. Below the heading, there is a note: 'You may setup firewall rules to protect your network from viruses, worms and malicious activity on the Internet.' The interface is divided into two main sections: 'Basic Settings' and 'MAC/IP/Port Filter Settings'. In the 'Basic Settings' section, 'MAC/IP/Port Filtering' is set to 'Disable' and 'Default Policy -- The packet that don't match with any rules would be:' is set to 'Dropped'. In the 'MAC/IP/Port Filter Settings' section, there are fields for 'MAC address', 'IP Address', 'Protocol' (set to 'None'), 'Dest Port Range', 'Source Port Range', 'Action' (set to 'Accept'), and 'Comment'. There are 'Apply' and 'Reset' buttons for both sections.

**MAC/IP/Port Filtering:** If you want to enable this function, select Enable. (The default is Disable.)

**Default Policy:** You can state that packets that don't match any rules are to be dropped or accepted.

**MAC address:** Enter the MAC address for which you want to define a rule.

**Dest IP Address:** Enter the destination IP address you want to filter.

**Source IP Address:** Enter the source IP address you want to filter.

**Protocol:** Select a protocol to control data packages.

**Dest Port Range:** Enter the destination IP address you want to control. The start port number must not be greater than the end port number.

**Source Port Range:** Enter the source IP address you want to control. The start port number must not be greater than the end port number.

**Action:** Drop or accept the defined rule.

**Comment:** Describe the rule.



# IX-T01 WiFi

## 4.3 Port forwarding

Port forwarding (port mapping) is the process of setting a virtual server to establish mapping relations between: WAN IP address, external port LAN server IP address, and internal port and LAN server IP addresses. This function allows the WAN user to access services (web, email, FTP, etc.) via the LAN server. By default, the wireless router will block initiating connection requests from the Internet to guarantee the security of the LAN. If you want to allow Internet users to access a server within the LAN, set up a virtual server.

WIRELESS-N ROUTER IEEE 802.11N

Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server Settings	
Virtual Server Settings	Disable
IP Address	
Port Range	
Protocol	TCP&UDP
Comment	

Apply Reset

Current Virtual Servers in system:				
No.	IP Address	Port Range	Protocol	Comment

Delete Selected Reset

Single virtual Server Settings	
Single virtual Server Settings	Disable
IP Address	
Public port	
Private port	
Protocol	TCP&UDP
Comment	

Apply Reset

**Virtual Server Settings:** Enable or Disable the virtual server. (The default is Disabled.)

**IP address:** Enter the IP address of the internal network which you want to set as a virtual server (like 192.168.16.254).

**Port Range:** Server port range of the host in the internal network (like 80).

**Protocol:** Select the program protocol (TCP/UDP/TCP&UDP). (The default is TCP&UDP.)

**Comment:** Enter a comment. (Example for configuration above: "Visit 80 port. It will turn to the host whose IP address is 192.168.16.254").

**Current Virtual Servers in system:** Displays a list of virtual servers.

**Single Virtual Server Settings:** Enable or disable a single virtual server. (The default is Disable.)

**IP address:** Enter the IP address of the internal network which you want to set as a single virtual server.

**Common Port:** It is the port used to access the virtual server by client.

**Private Port:** It is the real port opened by the virtual server.

**Protocol:** Select a program protocol (TCP/UDP/TCP&UDP).

**Comment:** Enter a comment.

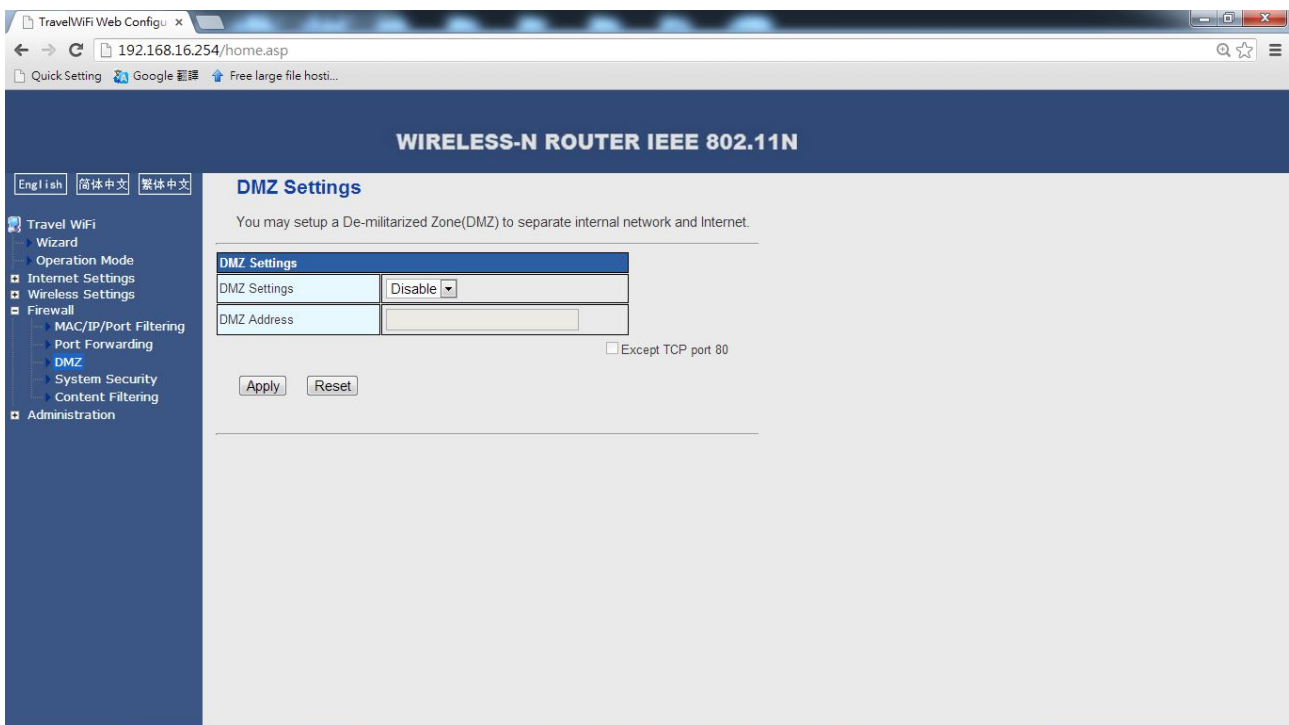
**Current Single Virtual Server in system:** It shows a list of virtual servers.

# IX-T01 WiFi

## 4.4 DMZ

The DMZ host is the default virtual server. Its priority is lower than that of a virtual server. When a wireless router receives a connection request from an external network, the router scans the server list according to the number of the server port. If there is a matching port, it sends this request to the corresponding virtual server. If there is not, it checks for a matching DMZ host and sends a request to it; if it can't find the host, it abandons the request. As for a detailed setting, you only need to fill in the host IP address, choose Enable, and click on Apply to save it.

**Note:** If you enable the DMZ function, this host will be exposed in the WAN, which would compromise its security. When you set the DMZ function, ensure that the number of port that is accessed is the same as the number of the port which the DMZ host enables.



**DMZ Settings:** Enables or disables DMZ host.

**DMZ IP Address:** Enables the IP address of the computer you want to display.

# IX-T01 WiFi

## 4.5 System Security

Select Firewall | System Security to enable or disable the remote management. You can allow or forbid a PC in the WAN network management router by using the WAN IP address of the router to access a web page. You can enable or disable ping packages and ping requests in the WAN filter, port scan block, SYN flood and SPI firewall function.

Caution: If you enable the SPI firewall function, some firewall functions (like IP/MAC/PORT filtering) may stop working.

The screenshot displays the 'System Security Settings' page of a 'WIRELESS-N ROUTER IEEE 802.11N'. The browser address bar shows '192.168.16.254/home.asp'. The page title is 'WIRELESS-N ROUTER IEEE 802.11N'. The left sidebar contains a navigation menu with 'System Security' selected. The main content area is titled 'System Security Settings' and includes the instruction: 'You may configure the system firewall to protect AP/Router itself from attacking.' Below this, there are five sections, each with a dropdown menu:

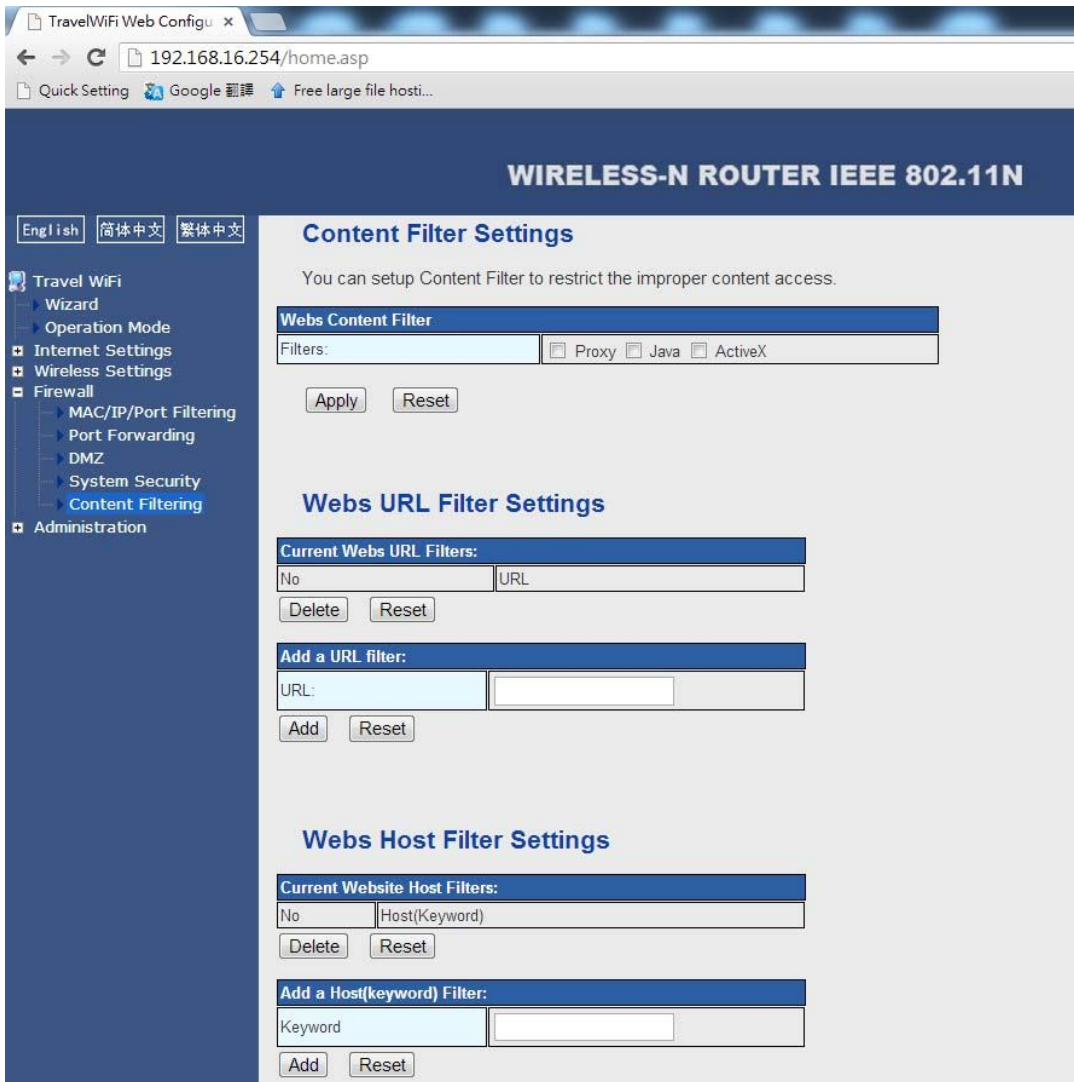
- Remote management**: Remote management (via WAN) is set to 'Deny'.
- Ping form WAN Filter**: Ping form WAN Filter is set to 'Disable'.
- Block Port Scan**: Block port scan is set to 'Disable'.
- Block SYN Flood**: Block SYN Flood is set to 'Disable'.
- Stateful Packet Inspection (SPI)**: SPI Firewall is set to 'Disable'.

At the bottom of the settings area, there are 'Apply' and 'Reset' buttons.

# IX-T01 WiFi

## 4.6 Content Filtering

In this interface, you can set Proxy, Java, and ActiveX content filtering in a web page when you browse. You can also set URL filtering rules according to your demand (by domain name, host name, and keywords) to prohibit a LAN PC from accessing a website



**Webs Content Filter:** Select appropriate filter rules according to your demand. There are 3 types of filters:

**Proxy:** Filter out web pages offered by agencies.

**Java:** Filter out Java in web pages.

**Active-X:** Filter out Active-X controls in web pages.

**Current Webs URL Filtrates (filters):** It is the set rule of URL filters. If you wish, you can delete the rule: select it and click on the Delete button.

**Add a URL filter:** Enter the URL address you want to filter. Click on the Add button to prohibit a website from being accessed. The new URL filter will appear at the top of the list. **Current Webs Host Filtrates:** It shows the defined rule of host filtrates. if you want to remove it, please select it and click on the Delete button.

**Add a Host filter:** Enter the keywords of the host name you want to filter and click on the Add button to prohibit the access of a website. The new keywords will appear at the top of the list.

# IX-T01 WiFi

## 5.Administration

### 5.1. Management

In the left pane, click on Administration | Management to set configurations such as: language, administration account, password, current time, NTP (Network Time Protocol), and DNS server

The screenshot displays the 'System Management' configuration page for a 'WIRELESS-N ROUTER IEEE 802.11N'. The interface includes a language selector (English, 简体中文, 繁體中文), a navigation tree on the left, and three main configuration sections: Language Settings, Administrator Settings, and NTP Settings. Each section has an 'Apply' and 'Cancel' button.

Language Settings	
Select Language	English
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Administrator Settings	
Account	admin
Password	•••••
WatchDog	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

NTP Settings	
Current Time	Sat Jan 1 03:31:52 UTC 2000 <input type="button" value="Sync with host"/>
Time Zone:	(GMT-11:00) Midway Island, Samoa
NTP Server	
NTP synchronization(hours)	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Select Language:** Choose one of 3 languages and click on the Apply button to finish the language setting.

**Account:** Enter a new user name for the device. (The default is admin).

**Password:** Enter a new password. (The default is admin.)

Click on the Apply button. The system will reboot and then ask you to enter the changed account name or password. If you forget the account name or password, then press and hold the reset button on the rear panel for 5 seconds to allow the system to reboot and restore all configurations to the factory-default settings.

**Current time:** The current time displays. Click on Sync with host to set time on the router to the time of the host.

**Time zone:** Choose your time zone (such as GMT+08:00 China, Hong Kong if you are in China).

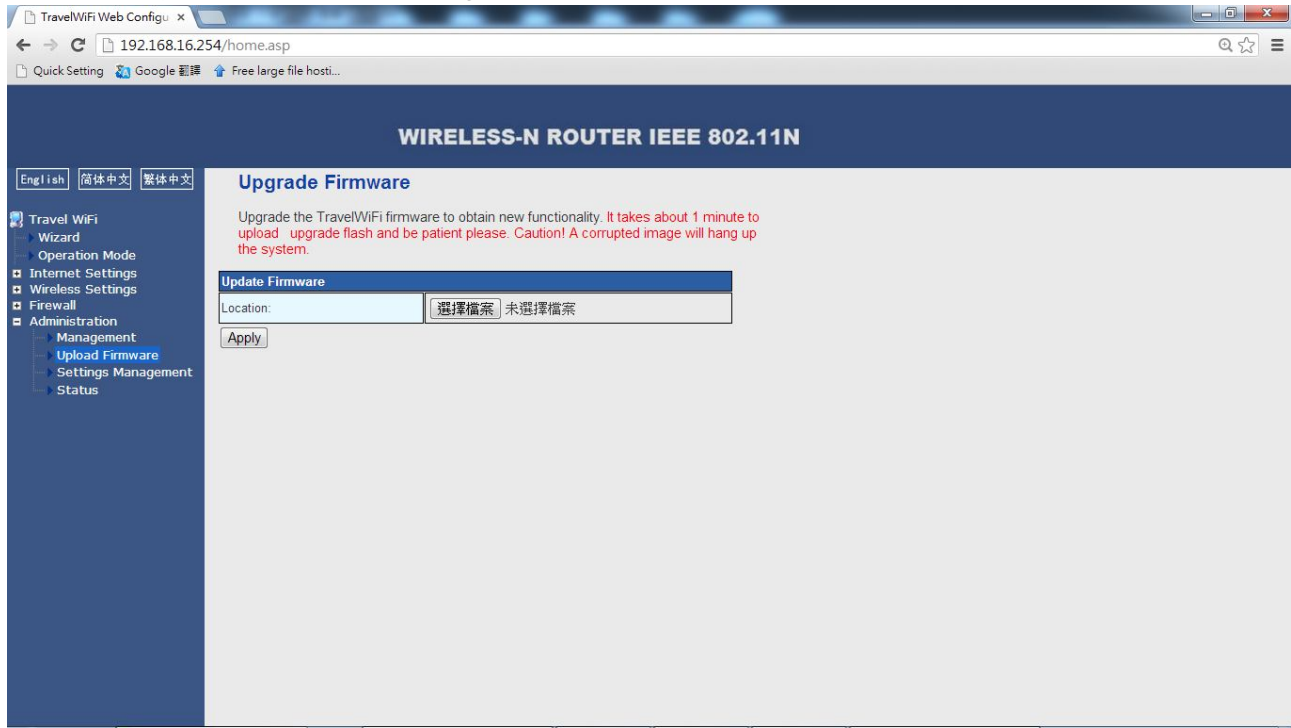
**NTP server:** Input the URL address of the NTP server (such as Asia Pacific NTP server if you are in China).

**NTP synchronization (hours):** This is the synchronization interval time with the NTP server.

# IX-T01 WiFi

## 5.2 Upload Firmware

Click “Administration | Upload Firmware” in the left pane to upgrade the firmware and update the system startup loader program.



**Update Firmware:** Click on Browse to choose the latest firmware file for the router. Click on the Apply button to upgrade it. The firmware will upgrade and then the system will reboot.

**Update Boot loader:** Click on Browse to choose the latest system-loader program file for the router and then click on the Apply button to update it.

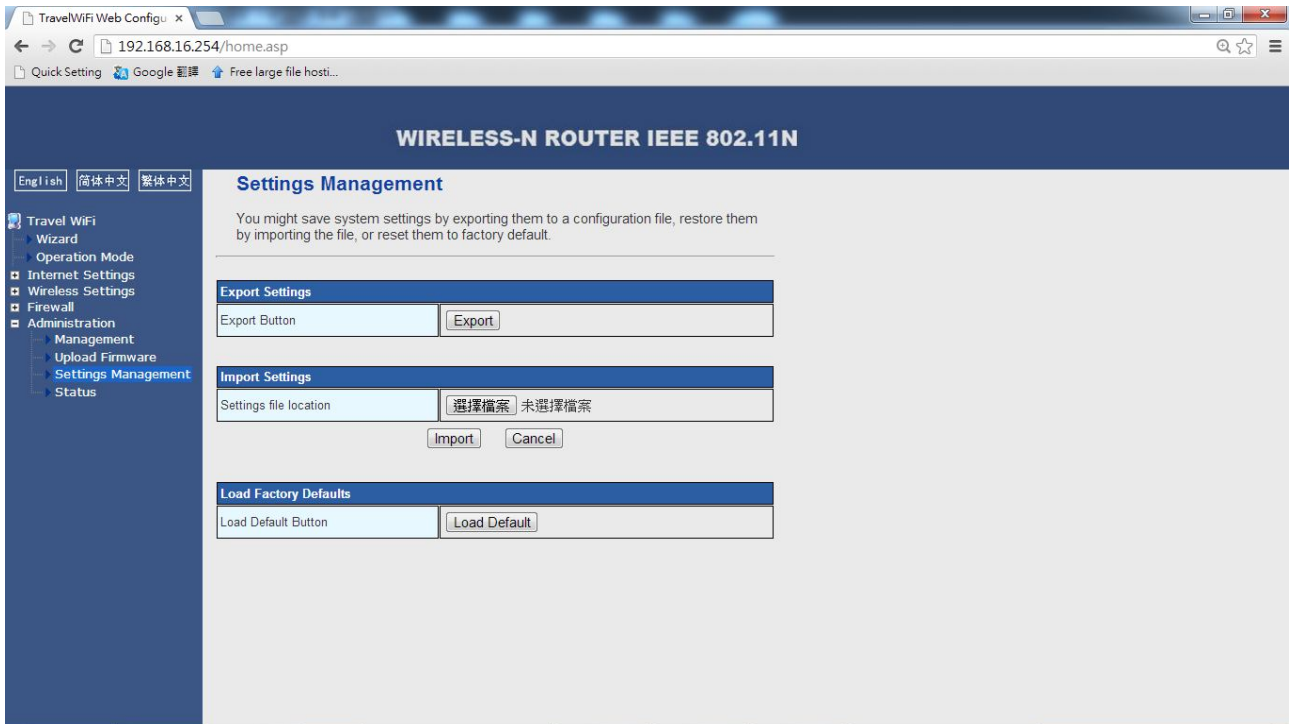
**Important Note:** Do not turn off the power or disconnect the network from the router while the router is upgrading, otherwise the process may hang up or the equipment may get damaged.

**Note:** Before upgrading the router, ensure that the file is the latest one and that the corresponding product is the product of same series.

# IX-T01 WiFi

## 5.3 Settings Management

In the left pane, click on Administration | Settings Management, you can save the system settings by exporting them to a configuration file. Restore the settings by importing the file and resetting them to the factory defaults



**Export Settings** Click on Export to export the current system settings to a certain point. The file name is the default value and cannot be changed.

**Import Settings:** Click on Browse to see the directory to which you exported the system setting files, choose the file, and then click on the Import button and reboot the system.

**Load Defaults:** Click on this button to reset all of the configurations to the default values, which means that you will lose all of the settings you previously set for the router. The system will then reboot.

**Note:** Please save the current configurations before importing another configuration file or restoring factory settings

# IX-T01 WiFi

## 5.4 Status

In the left pane, click on Administration | Status to see on this page: SDK version, system uptime, system platform, operation mode, Internet configurations, and local network.

WIRELESS-N ROUTER IEEE 802.11N

English 简体中文 繁體中文

Travel WiFi

- Wizard
- Operation Mode
- Internet Settings
- Wireless Settings
- Firewall
- Administration
  - Management
  - Upload Firmware
  - Settings Management
  - Status

### Access Point Status

Let's take a look at the status of TravelWiFi Platform.

System Info	
SDK Version	V1.4
System Up Time	4 hours, 10 mins, 14 secs
Operation Mode	AP Client Mode

Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	48 02 2A 00 09 98

Local Network	
Local IP Address	192.168.16.254
Local Netmask	255.255.255.0
MAC Address	48 02 2A 00 09 97

### Ethernet Port Status

not support

## Appendix A: Common Troubleshooting Methods

Appendix A provides some methods to resolve problems you may meet when you install the IX-T01 WiFi broadband router and some steps to take to analyze the problems using diagnostic tools.

If you cannot resolve the problems, please contact Technical Supporter

1.Problem: Power indicator does not light.

Solution: Check that the power supply is working and that you are using the proper power adapter.

2.Problem: WAN indicator does not light when a network cable is plugged in.

Solution:Check that the network cable has been inserted correctly into the WAN port.

3.Problem: LAN indicator does not light when a network cable is plugged in.

Solution: Check that the power connector and Internet cables are ok.

Check the connection from the cable to the port.

Check whether the Ethernet card is installed correctly in the PC.

4.Problem: Failed to visit the WEB setting page.

Solution: Ensure that your browser (IE6+ or Firefox 1.5+) is the latest version and that you have Java installed on your computer.

5.Problem: Cannot save the setting that I altered on the web page.

Solution: Ensure that after you complete your configuration changes on the interface that you click on the Apply button and that you then reload the system.

6.Problem: What should a user do if he knows nothing about the router's firewall when he enables the firewall function?

Solution: A router's firewall has strict rules, so a common user should disable the firewall.

Only a user who is familiar with setting a router should consider setting a firewall. Before setting



# IX-T01 WiFi

## Appendix B: Technical Terms

### 1. DHCP (Dynamic Host Configuration Protocol)

Dynamically allocates IP address, subnet mask and gateway for host in the network.

### 2. DHCP Server (Dynamic Host Configuration Protocol Server)

A device that runs Dynamic Host Configuration Protocol, it is used to allocate IP address for DHCP client.

### 3. DNS (Domain Name Server)

It resolves a domain name (like www.yahoo.com) into a corresponding IP address (like 216.115.108.243). A DNS message is distributed in the DNS server for the entire Internet, so the DNS server will check the domain name that we send a request to and search for the corresponding IP address when we visit a website. If this DNS server can't find the IP address, it will send the request to a superior DNS server to continue searching for an IP address.

### 4. FTP (File Transfer Protocol)

A protocol describes that how to transfer files between each computer in the network.

### 5. HTTP (Hypertext Transfer Protocol)

It is a standard protocol for transmission of web page.

### 6. ICMP (Internet Control Message Protocol)

Used to send an error message and some important network information (like for ping command).

### 7. IEEE (Institute of Electrical and Electronics Engineers)

It is a technical institution that specially define international standard.

### 8. ISP (Internet Service Provider)

A person provides Internet accessing service.

### 9. LAN (Local Area Network)

Generally it means intranet, such as home network, internal network of small or medium-sized enterprise, such as an intranet (private network).

### 10. MAC (Media Access Control)

MAC address is the hardware (permanent physical) address of a device that is specified by the manufacturer, connected to a shared network medium. It is composed of 6 pairs of hexadecimal characters (like 00-0F-E2-80-65-25). Each network component has a globally unique MAC address.

### 11. NAT (Network Address Translation)

It allows for more than one computer to be in a LAN sharing an IP address of the public network, shields LAN users who access the Internet. It plays an important role in ensuring network security. Usually it is used by broadband routers.

### 12. NIC (Network Interface Card)

Located in a PC, it provides a physics port to a cable connected to it. If it is an Ethernet NIC, it usually uses RJ-45 port.

### 13. Ping

The ping command sends a message from one computer to another to check whether it is reachable and active. It is a tool used to test whether the local computer can interchange information with another computer on the network. The local computer sends a message to a specified computer and if that computer receives the message, it responds to the local computer.

### 14. PPP (Point-to-Point Protocol)

Link layer communication protocol.

### 15. RJ-45

A standard plug used to connect to an Ethernet switch, a concentrator and a router. A direct connecting

# IX-T01 WiFi

cable and a crossover cable usually make use of this plug with a route function.

16. TCP/IP (Transmission Control Protocol/Internet Protocol)

It defines a group of protocols including TCP/IP.

17. Telnet

An interactive program based on character, is used to enable a client (user on a computer) to log on to a distant host (another computer) via the Internet, Telnet allows user remote login and setting device.

18. USB (Universal Serial Bus)

Serial interface used to connect printer or scanner to computer. BR304 USB interface provided is used to connect a host.

19. WAN (Wide Area Network)

A data communication network covering large geographic range (like Internet).

20. Web page

The website file on WWW, every website contains text and images hyperlink link with other web page.

Homepage is Web page at top level of a website.

21. Broadcast

It sends data to all computers in a network.

22. Domain name

The unique key component of a URL, identifies a file on a website, managed by ICANN (Internet Corporation for Assigned Names and Numbers). Because it can be used to replace corresponding IP address, so it is very convenient for user.

23. Ethernet

A network technology for LANs, usually uses twisted-pair cable for transmission. Ethernet data transfer rates (radio frequency signals) between computers either 10 Mbps or 100 Mbps.

24. Firewall

It protects computer or LAN from visit or malicious attack.

25. Package

Data transferred on a network. Each package is made up of data and message such as source address (data sender) and destination address (data receiver).

26. Port

It is physical interface on computer or router in which a connector is plugged to allow data in or out.

27. Protocol

A group of rules used to manage data transmission. Interconnected equipment must follow these rules to transfer data successfully.

28. Long distance

A remote user like staff member on business trip logging in to company network far away.

29. Route

Path taken for data to travel between transmission point and receiving point, a router is equipped with route function. The rules, please plan all of the Internet activities that the LAN users need.