
300M 11n Wireless Router

User Manual

Version 1.1 | 12/18/2018

Table of Content

Chapter 1 Introduction	1
1.1 Features.....	1
1.2 System Requirement.....	1
1.3 Package Contents	2
Chapter 2 Hardware Installation	3
2.1 Led indicators	3
2.2 Back Rear Panel.....	3
2.3 Typical install	4
Chapter 3 Quick Installation Guide.....	5
3.1 Set the Network Configurations	5
3.2 Getting Started.....	7
3.3 Setup Wizard	8
Chapter 4 Configuring the Router.....	15
4.1 WAN Setup	15
4.1.1 WAN Setup.....	15
4.1.2 DDNS	16
4.2 LAN Setup	16
4.2.1 LAN Interface	16
4.2.2 Static DHCP	17
4.2.3 DHCP	18
4.3 Wireless Setup	18
4.3.1 Basic.....	18
4.3.2 Advanced.....	19
4.3.3 Security	20
4.3.4 Access	21
4.3.5 WDS	21
4.3.6 Site Survey	22
4.3.7 WPS	22
4.3.8 Schedule	22
4.4 Firewall	23
4.4.1 Forwarding	23
4.4.2 DMZ.....	24
4.4.3 Denial-of-Service.....	24
4.4.4 VLAN	24
4.5 Security.....	25
4.5.1 Port Filtering	25
4.5.2 IP Filtering	26
4.5.3 URL Filtering	27
4.5.4 MAC Filtering	27
4.6 QoS.....	27

4.7 System.....	28
4.7.1 Time Zone	28
4.7.2 Upgrade.....	29
4.7.3 Save/Reload.....	29
4.7.4 Password.....	29
4.7.5 Reboot.....	30
Chapter 5 Status	31
5.1 Status	31
5.2 Statistics	31
5.3 Log.....	32
Chapter 6 Logout	33

Chapter 1 Introduction

The Wireless Router is compatible with IEEE802.11b/g/n standard, which supports data rate up to 300Mbps in 2.4GHz band, which is also compatible with IEEE 802.11g/b wireless devices. The Wireless router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in 4-port switch and wireless AP, LAN users can share files, and playing network games all at a high speed. This device is also an Access Point. It has a built-in wireless LAN. Users can connect to Internet using wireless network interfaces anywhere within the range of its radio transmission. It's ideal for SOHO users who require instant and convenient access to Internet without the restriction of connecting cables.

1.1 Features

- Complies with 2.4GHz IEEE802.11n v2.0 and backward compatible with IEEE 802.11b/g standards
- Supports NAT/NAPT IP sharing
- WAN Protocols: PPPoE/Static IP/PPTP/DHCP
- Supports advanced 2T2R MIMO technology to enhance the throughput and coverage range significantly
- High speed data rate - up to 300Mbps
- Supports Virtual Server and DMZ
- Supports Wi-Fi Protected Setup (WPS) with reset button
- Supports 64/128-bit WEP encryption and WPA-PSK, WPA2-PSK security
- Supports WMM function to meet the multimedia transmission requirement
- Supports WDS mode
- Supports Special Applications (Port Triggers)
- Supports DDNS (DynDNS, TZO), and QoS
- Supports MAC/IP filtering and URL blocking
- Supports DHCP server and Anti-Dos firewall
- Web user interface (remote configuration)
- System status and security log
- Firmware upgradeable

1.2 System Requirement

- An Ethernet-Based Cable or xDSL modem
- An Ethernet Card on PC
- TCP/IP network protocol for each PC
- RJ45 Twisted-pair
- Microsoft IE (or Firefox or Netscape)

1.3 Package Contents

Please unpack the box and check the following items:






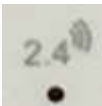
- One 300M 11n Wireless Router
- One Power Adapter
- One User Manual

Chapter 2 Hardware Installation

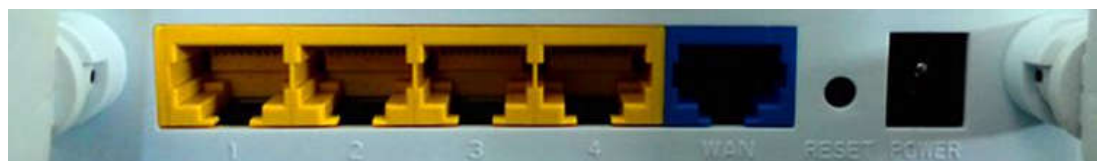
2.1 Led indicators

The top panel contains LED indicators that show the status of the unit.



Name	Status	Indication
 Power	Off	Power is off.
	On	Power is on.
 WPS	Flashing	The LED flashes about two minutes during WPS working.
 WAN 	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
 LAN(1-4)	Flashing	There is an active device linked to the corresponding port.
 2.4GHz	Off	The wireless function is disabled.
	Flashing	The wireless function is enabled. The router is working on 2.4GHz radio band.

2.2 Back Rear Panel



The following parts are located on the rear panel.

WAN: 10/100Mbps RJ45 port. The WAN port is where you will connect Cable/xDSL Modem or other LAN.

LAN (1,2,3,4): These four LAN ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network. If you connect this product with the Hub (or Switchboard) correctly, the router's corresponding LED and the Hub's (or the Switchboard's) must be illuminated.

WPS: With the router powered on, press the button about 2 second, it is WPS function

and the WPS LED will flash two minutes.

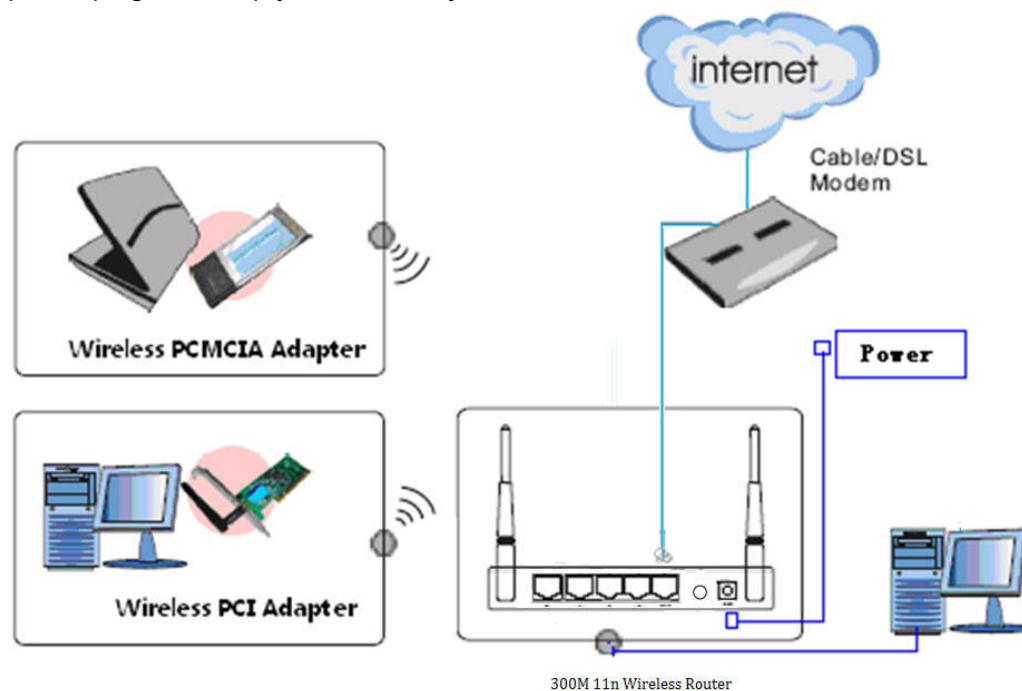
RESET: The Reset Button has two functions, WPS and Factory Default. With the router powered on, When selecting the WPS function, use a pin to press and hold the button about 2 seconds, the WPS LED will flash two minutes. The other one, use a pin to press and hold the button about 6 seconds, the router will restore to factory default.

POWER: The Power socket is where you will connect the power adapter. Please use the power adapter provided with this router.

Wireless antenna: To receive and transmit the wireless data.

2.3 Typical install

Before installing the router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.



1. Make sure all devices, including your PCs, modem, and router, are powered down.
2. Using an Ethernet network cable, connect the LAN or Ethernet network port of the cable or DSL modem to the router's WAN port.
3. Power on the cable or DSL modem, and power on the PC you wish to use to configure the router.
4. Connect the included power adapter to the router. And connect the other end of the adapter to an electrical outlet.

Chapter 3 Quick Installation Guide

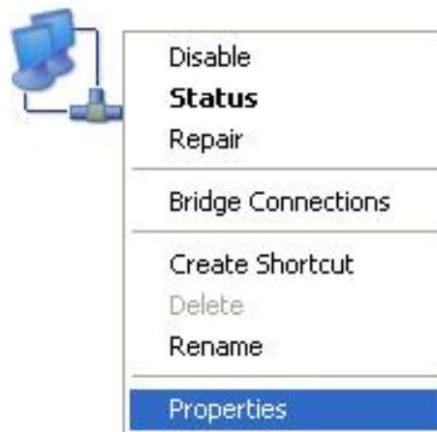
The chapter mainly presents how to enter the router's Web page and simple router settings. After you have finished the hardware installation (Please refer to chapter 2), the following steps will assist you to set the network configurations for you computer.

3.1 Set the Network Configurations

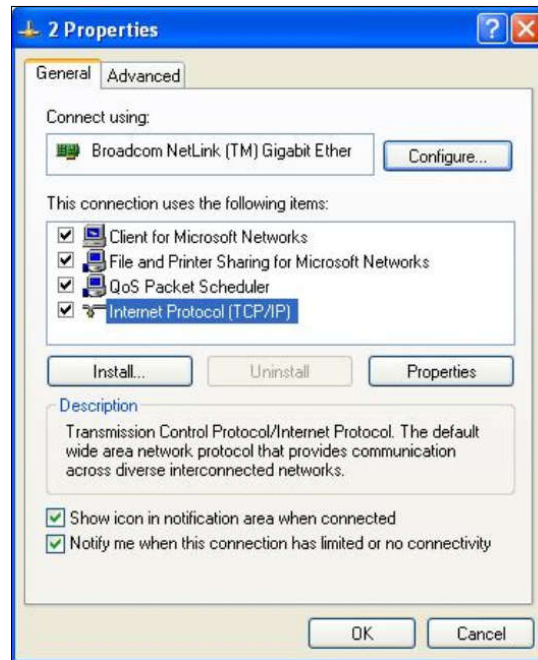
1. On your computer desktop right click **"My Network Places"** and select **"Properties"**.



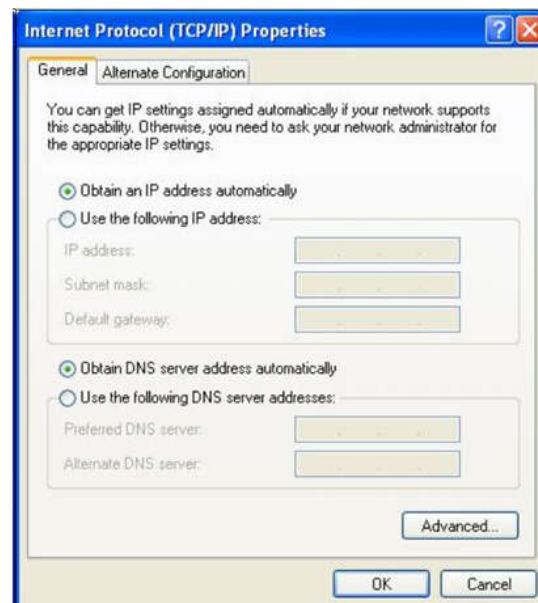
2. Right click **"Local Area Network Connection"** and select **"Properties"**.



3. Select **"Internet Protocol (TCP/IP)"** and click **"Properties"**.



4. Select **"Obtain an IP address automatically"** or select **"Use the following IP address(S)"**.
 - A. Select **"Obtain an IP address automatically"** and **"Obtain DNS server address automatically"**. Click **"OK"**.



B. "Use the following IP address (S)"

IP Address: 192.168.0.XXX: (XXX is a number from 1~254, except 30)

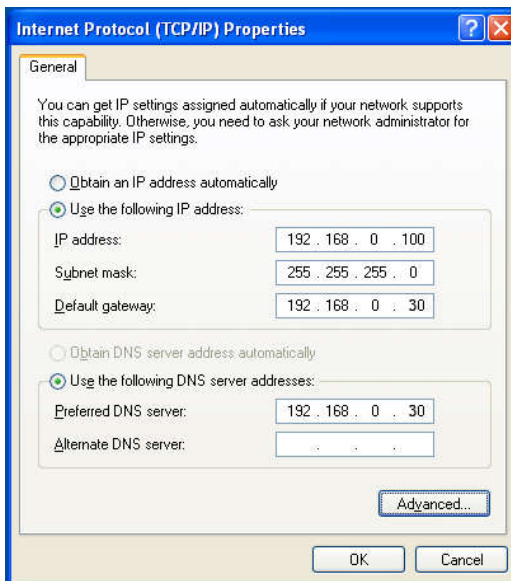
Subnet Mask: 255.255.255.0

Gateway: 192.168.0.30

DNS Server: You need to input the DNS server address provided by you ISP. Otherwise, you can use the router's default gateway as the DNS proxy server.

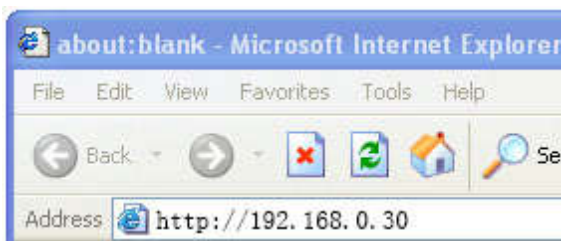
Tip: If you are not sure of the DNS server address, we recommend you to select "Obtain an IP address automatically (O)" and "Obtain a DNS server address

automatically”.



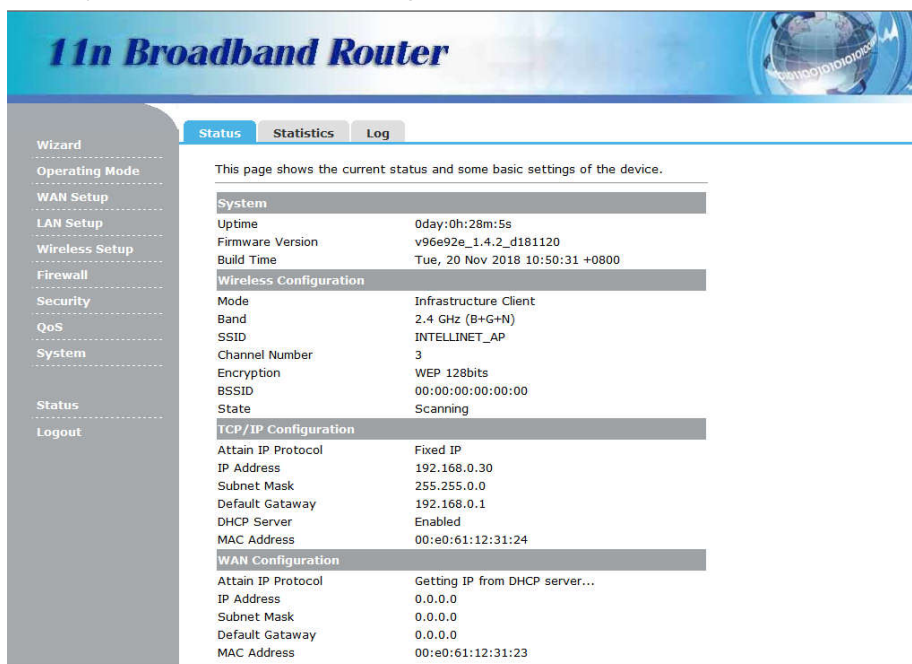
Click "OK" to save the configurations.

3.2 Getting Started



To access the configuration pages, open a web-browser such as Internet Explorer and enter the IP address of the router (**192.168.0.30**).
The Default User: **admin**
Password:

If successful, you can see the status page.



3.3 Setup Wizard

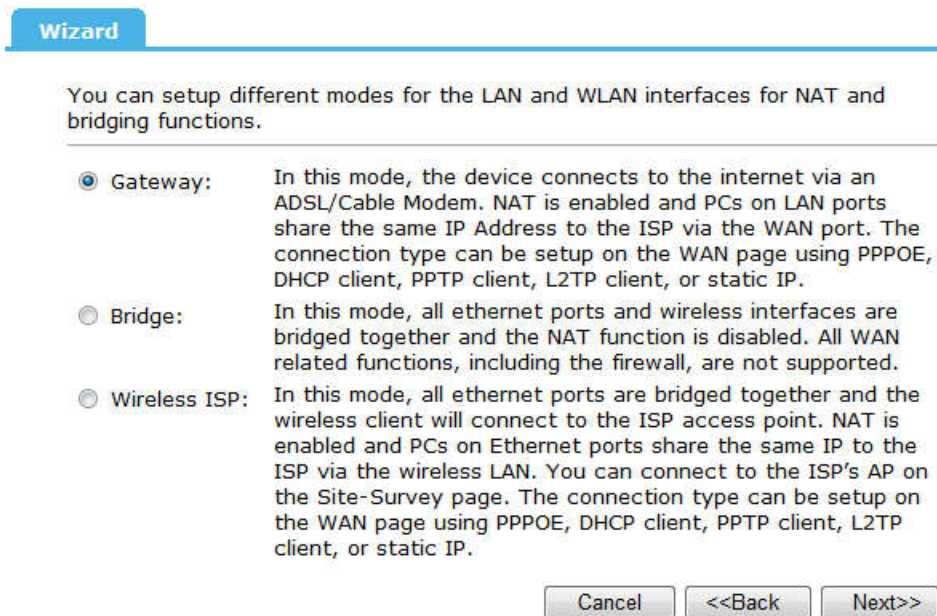
Click on "**Wizard**" pages, it will guide you to setup your router step by step in simple way. In this section, there are seven steps to do it.



Please follow the steps and complete the router configuration.

Step 1 Setup Operation Mode

The router supports three operation modes, **Gateway**, **Bridge** and **Wireless ISP**. And each mode is suitable for different use, please choose correct mode.



Step 2 Time Zone Setting

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. Daylight Saving can also be configured to automatically adjust the time when needed.

Wizard

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

Enable NTP client Update
 Automatically Adjust for Daylight Saving

Time Zone Select: (GMT+08:00)Taipei
NTP server: 131.188.3.220 - Europe

Cancel <<Back Next>>

Enable NTP client update: Check this box to connect NTP Server and synchronize internet time.

Automatically Adjust Daylight Saving: Check this box, system will adjust the daylight saving automatically.

Time Zone Select: Select the Time Zone from the drop-down menu.

NTP Server: Select the NTP Server from the drop-down menu.

Step 3 LAN Interface Setting

Setup the IP Address and Subnet Mask for the LAN interface.

Wizard

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

IP Address: 192.168.0.30
Subnet Mask: 255.255.0.0

Cancel <<Back Next>>

IP Address: Enter the IP address of your router. (**factory default:192.168.0.30**)

Subnet Mask: An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Step 4 WAN Interface Setting

The router support five access modes in the WAN side, please choose correct mode according to your ISP Service.

Mode 1 DHCP Client

Wizard

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

WAN Type:

Select DHCP Client to obtain IP Address information automatically from your ISP. This mode is commonly used for Cable modem services.

Mode 2 Static IP

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

Wizard

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

WAN Type:

IP Address:

Subnet Mask:

Default Gateway:

DNS:

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DNS: The DNS server information will be supplied by your ISP (Internet Service Provider).

Mode 3 PPPoE

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

Wizard

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

WAN Type:	<input type="text" value="PPPoE"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Cancel"/> <input type="button" value=" <<Back"/> <input type="button" value=" Next >>"/>	

User Name: Enter your PPPoE user name.

Password: Enter your PPPoE password.

Mode 4 PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with IP information and PPTP Server IP Address, of course it also includes a username and password. This mode is typically used for DSL services.

Wizard

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

WAN Type:	<input type="text" value="PPTP"/>
IP Address:	<input type="text" value="172.1.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Server IP Address:	<input type="text" value="172.1.1.1"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Cancel"/> <input type="button" value=" <<Back"/> <input type="button" value=" Next >>"/>	

IP Address: Enter the IP address.

Subnet Mask: Enter the subnet Mask.

Server IP Address: Enter the PPTP Server IP address provided by your ISP.

User Name: Enter your PPTP username.

Password: Enter your PPTP password.

Mode 5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.

Wizard

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

WAN Type:

IP Address:

Subnet Mask:

Server IP Address:

User Name:

Password:

IP Address: Enter the IP address.

Subnet Mask: Enter the subnet Mask.

Server IP Address: Enter the L2TP Server IP address provided by your ISP.

User Name: Enter your L2TP username.

Password: Enter your L2TP password.

Step 5 Wireless LAN Setting

For example, here we configure the basic parameters for 2.4GHz wireless network as the following screenshot:

Wizard

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

Band:

Mode:

Network Type:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Enable Mac Clone (Single Ethernet Client)

Band: This field determines the wireless mode which the Router works on.

2.4GHz (B) - Select if all of your wireless clients are 802.11b.

2.4GHz (G) - Select if all of your wireless clients are 802.11g.

2.4GHz (N) - Select if all of your wireless clients are 802.11n.

2.4GHz (B+G) - Select if you are using both 802.11b and 802.11g wireless clients..

2.4GHz (G+N) - Select if you are using both 802.11g and 802.11n wireless clients.

2.4GHz (B+G+N) - Select if you are using both 802.11b, 802.11g and 802.11n wireless clients.

Mode: Support AP, Client, WDS and AP+WDS mode.

Network Type: This type is only valid in client mode.

SSID: Service Set Identifier, it identifies your wireless network.

Channel Width: Select the channel width from the drop-down list.

Control Sideband: This relates to the channel number used for your wireless network. An upper band represents higher channels and vice versa.

Channel Number: Indicates the channel setting for the router.

Enable Mac Clone: Enable or disable MAC clone option. (You can use the "Mac Clone" button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with this MAC address.)

Step 6 Wireless Security Setup

Secure your wireless network by turning on the NONE, the WEP, the WPA(AES), the WPA2(AES) or WPA2 Mixed etc security feature on the router. This section you can set the NONE, the WEP, the WPA(AES), the WPA2(AES) or WPA2 Mixed etc security mode. The following picture shows how to set the NONE security.

The screenshot shows a 'Wizard' window with a blue header. Below the header is a horizontal line. The text reads: 'This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.' Below this text is a form with the following fields: 'Encryption:' with a dropdown menu set to 'NONE', 'Cancel', '<<Back', and 'Finished' buttons.

The following picture shows how to set the WEP security.

The screenshot shows a 'Wizard' window with a blue header. Below the header is a horizontal line. The text reads: 'This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.' Below this text is a form with the following fields: 'Encryption:' with a dropdown menu set to 'WEP', 'Key Length:' with a dropdown menu set to '128-bit', 'Key Format:' with a dropdown menu set to 'Hex (26 characters)', 'Key Setting:' with a text input field containing asterisks, 'Cancel', '<<Back', and 'Finished' buttons.

Key Length: Specify the Length of the key, 64-bit or 128-bit.

Key Format: Specify the format of the key, ASCII or hex.

Key Setting: Enter the key here, its format is limited by the key format, ASCII or Hex.

The following picture shows how to set WPA-PSK security, you can select WPA (TKIP), WPA2 (AES) and Mixed mode.

Wizard

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Encryption:

Pre-Shared Key Format:

Pre-Shared Key:

Pre-Shared Key Format: Specify the format of the key, passphrase or hex.

Pre-Shared Key: Enter the key here, its format is limited by the key format.

Click "Next" to set the 2.4GHz wireless network by the same method, and then click "Finish" button to complete the setting.

Through the wizard setup, you can complete the basic functions of a router settings to achieve Internet access. If you need more advanced setting of the router, please refer to the following chapters.

Chapter 4 Configuring the Router

4.1 WAN Setup

There are two submenus under the WAN Interface menu: **WAN Setup**, **DDNS**. Click any of them, and you will be able to configure the corresponding function.

4.1.1 WAN Setup

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

The screenshot shows the WAN Setup configuration page. On the left is a navigation menu with options: Wizard, Operating Mode, WAN Setup (highlighted with a red circle), LAN Setup, Wireless Setup, Firewall, Security, QoS, System, Status, and Logout. The main content area has two tabs: WAN Setup (active) and DDNS. Below the tabs is a descriptive paragraph: "This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type." The configuration fields include: WAN Type (DHCP), Host Name (empty), MTU Size (1500, with a note "(1400-1500 bytes)"), DNS 1 (0.0.0.0), DNS 2 (0.0.0.0), and MAC Address (000000000000). There are buttons for "Clone MAC" and "Recover MAC". A list of checkboxes includes: Enable uPNP (unchecked), Enable IGMP Proxy (checked), Enable Ping Access on WAN (unchecked), Enable Web Server Access on WAN (unchecked), Enable IPsec pass through on VPN connection (checked), Enable PPTP pass through on VPN connection (checked), Enable L2TP pass through on VPN connection (checked), and Enable IPv6 pass through on VPN connection (unchecked). At the bottom are "Apply" and "Reset" buttons.

4.1.2 DDNS

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

here'. At the bottom of the form are two buttons: 'Apply' and 'Reset'."/>

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

Enable DDNS

Service Provider: OrayDDNS

Domain Name: host.dyndns.org

User Name/Email:

Password/Key:

Note:
For Oray DDNS, you can create your Oray account [here](#)

Apply Reset

Service Provider: Select one from the drop-down menu, such as DynDNS, OrayDDNS or TZO.

Domain Name: Enter the domain name (Such as host.dyndns.org).

User Name/Email: Enter the user name or email the same as the registration name.

Password/Key: Enter the password you set.

4.2 LAN Setup

There are three submenus under the LAN Interface menu: **LAN Setup**, **Static DHCP**, **DHCP**. Click any of them, and you will be able to configure the corresponding function.

4.2.1 LAN Interface

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

IP Address: Enter the IP address of your router (**factory default: 192.168.0.30**).

Subnet Mask: An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Default Gateway: Enter the gateway IP address of your router.

DHCP: Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.

DHCP Client Range: The range of IP address the router DHCP server will assign to users and device connecting to the router.

DHCP Lease Time: The DHCP Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be “leased” this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 10080 minutes. The default value is 480 minutes.

Domain Name: Input the domain name of you network.

MAC Address: You can configure the MAC address of the LAN.

4.2.2 Static DHCP

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address.

IP Address: Enter the IP address which needs to be bound.

MAC Address: Enter the MAC address of the computer you want to assign the above IP address.

Comment: You can add some comment for this item.

Click "**Apply**" to add the entry in the list.

4.2.3 DHCP

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

LAN Setup	Static DHCP	DHCP
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.		
IP Address	MAC Address	Time Expired(s)
192.168.0.100	0x000ec6d6215c	23690
<input type="button" value="Refresh"/>		

Refresh: Click this button to refresh the data.

4.3 Wireless Setup

There are eight submenus under the Wireless 2.4G menu: **Basic**, **Advanced**, **Security**, **Access**, **WDS**, **Site Survey**, **WPS**, **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.3.1 Basic

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

Wizard

Operating Mode

WAN Setup

LAN Setup

Wireless Setup

Firewall

Security

QoS

System

Status

Logout

Basic Advanced Security Access WDS Site Survey WPS Schedule

This page can be configured to connect to a wireless client parameter access point, you can set the basic parameters of the wireless network.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: Client

Network Type: Infrastructure

SSID: INTELLINET_AP

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

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

SSID of Extended Interface: RTK 11n AP RPT0

Disable Wireless LAN Interface: Check this box to to disable the router's wireless features; uncheck to enable it.

Band: Select one mode from the following. The default is 2.4GHz (B+G+N) mode.

Mode: Support AP, Client, WDS and AP+WDS mode.

SSID: SSID (Service Set Identifier) is the unique name of the wireless network.

Channel Width: Select the channel width from the drop-down list.

Control Sideband: This relates to the channel number used for your wireless network. An upper band represents higher channels and vice versa.

Channel Number: Indicates the channel setting for the router.

Broadcast SSID: Select "Enable" to enable the device's SSID to be visible by wireless clients. The default is enabled.

WMM: It will enhance the data transfer performance of multimedia data when they're being transferred over wireless network.

Data Rate: Sets the maximum wireless data rate that your network will operate on.

Associated Clients: You can see the MAC Address, MAC address, transmission and reception packet counters for each associated wireless client.

4.3.2 Advanced

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

Basic **Advanced** Security Access WDS Site Survey WPS Schedule

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

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Preamble Type: Long Preamble Short Preamble

IAPP: Enabled Disabled

HS2: Enabled Disabled

Protection: Enabled Disabled

Aggregation: Enabled Disabled

Short GI: Enabled Disabled

WLAN Partition: Enabled Disabled

20/40MHz Coexist: Enabled Disabled

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

Fragment Threshold: This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets.

RTS Threshold: RTS stands for "Request to Send". This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2347. It is recommended not to modify this value in SOHO environment.

Beacon Interval: Enter a value between 20-1024 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons.

IAPP: Inter-Access Point Protocol.

Short GI: This function is recommended for it will increase the data capacity by reducing the guard interval time.

STBC: Space Time Block Coding improves reception by coding the data stream in blocks.

RF Output Power: Here you can specify the RF output power of router.

4.3.3 Security

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

Basic Advanced **Security** Access WDS Site Survey WPS Schedule

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication: Open System Shared Key Auto

Key Length:

Key Format:

Encryption Key:

4.3.4 Access

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

Basic Advanced Security **Access** WDS Site Survey WPS Schedule

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

Wireless Access Control Mode:

MAC Address:

Comment:

Current Access Control List:

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

Wireless Access Control Mode: If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point. The MAC Address format is 001122334455.

4.3.5 WDS

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, firstly you must set AP Mode to WDS or AP+WDS in basic setting, then enable WDS function and set another AP MAC which you want to communicate with. The WDS supports WEP and PSK security mode. Of course in order to make APs work, you have to keep them the same channel and security mode.

Basic Advanced Security Access **WDS** Site Survey WPS Schedule

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

Enable WDS

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address:	Tx Rate (Mbps)	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable WDS: Check this box to enable WDS function.

MAC Address: Enter the remote AP MAC address.

Data Rate: Sets the maximum wireless data rate that your network will operate on.

Comment: You can add some comment for this item.

4.3.6 Site Survey

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

This page provides a tool to scan for wireless networks. If an Access Point or IBSS is found, you could choose to connect to it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
None						

Next>>

4.3.7 WPS

WPS is designed to ease set up of security Wi-Fi networks and subsequently network management. This router supports WPS features for AP mode, AP+WDS mode, Infrastructure-Client mode, and the wireless root interface of Universal Repeater mode.

This page allows you to change the settings for WPS (Wi-Fi Protected Setup). Using this feature allows a wireless client to automatically synchronize its settings and easily and securely connect to the Access Point.

Disable WPS

Apply Reset

Auto-lock-down state: Unlocked Unlock

Self-PIN Number: 06195892

Assign Mac of Registrar:

PIN Configuration: Assign SSID of Registrar:

Start PIN

Push Button Configuration: Start PBC

STOP WSC: Stop WSC

Disable WPS: Check this box and clicking “Apply” will disable WPS function. WPS is turned on by default.

Self-PIN Number: It is AP’s PIN.

Start PBC: Clicking this button will invoke the Push Button Configuration of WPS. If one station wants to connect to the AP, it must click its PBC button in two minute. You can see the WPS LED flash this time.

Client PIN Number: The length of PIN is limited to four or eight numeric digits. If the AP and Station input the same PIN and click “Start PIN” button in two minutes, they will establish connection and setup their security key.

4.3.8 Schedule

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

This page allows you setup the wireless schedule rule. Do not forget to configure the system time before enabling this feature.

Enable Wireless Schedule

Days

Everday

Sun Mon Tue Wed Thu Fri Sat

Time

24 Hours

From : To :

4.4 Firewall

There are two submenus under the Server Setup menu: **Forwarding**, **DMZ**, **Denial-of-Service**, **VLAN**. Click any of them, and you will be able to configure the corresponding function.

4.4.1 Forwarding

If you configure the router as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.

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

Enable Port Forwarding

IP Address:

Protocol:

Port Range: -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>				

Enable Port Forwarding: Check this box will enable Port Forwarding function.

IP Address: That external User accesses the router will redirect to this local IP.

Port Range: The packet with this protocol and port will be redirected to the local IP.

Comment: You can add some comment for this item.

Current Port Forwarding Table: The table shows all you have configured. You can

delete one or all.

4.4.2 DMZ

If you have a client PC that cannot run Internet application properly from behind the NAT firewall or after configuring the Port Forwarding, then you can open the client up to unrestricted two-way Internet access.

Forwarding **DMZ** Denial-of-Service VLAN

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

Enable DMZ

DMZ Host IP Address:

Enable DMZ: Check this box will enable DMZ function.

DMZ Host IP Address: Enter DMZ host IP Address may expose this host to a variety of security risks.

4.4.3 Denial-of-Service

You can configure Denial-of-Service.

Forwarding DMZ **Denial-of-Service** VLAN

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

Enable DoS Prevention

<input type="checkbox"/> Whole System Flood: SYN	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="0"/> Packets/Second
<input type="checkbox"/> TCP/UDP PortScan	<input type="text" value="Low"/> Sensitivity
<input type="checkbox"/> ICMP Smurf	
<input type="checkbox"/> IP Land	
<input type="checkbox"/> IP Spoof	
<input type="checkbox"/> IP TearDrop	
<input type="checkbox"/> PingOfDeath	
<input type="checkbox"/> TCP Scan	
<input type="checkbox"/> TCP SynWithData	
<input type="checkbox"/> UDP Bomb	
<input type="checkbox"/> UDP EchoChargen	

4.4.4 VLAN

Entries in below table are used to configure vlan settings. VLANs are created to provide

the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

Forwarding DMZ Denial-of-Service **VLAN**

Entries in below table are used to configure vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

Enable VLAN

VLAN ID: (1-4094)

Forward Rule:

Tag Table

interface name	tagged	unTagged	not in this vlan
lan0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
lan1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
lan2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
lan3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
wan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
wlan0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Current VLAN setting table

VlanID	tagged interface	untagged interface	forward rule	modify	select
9		lan0 lan1 lan2 lan3 wlan0	NAT	<input type="button" value="modify"/>	<input type="checkbox"/>
8		wan	NAT	<input type="button" value="modify"/>	<input type="checkbox"/>

4.5 Security

The router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks.

There are four submenus under the Security menu: **Port Filtering**, **IP Filtering**, **URL Filtering**, **MAC Filtering**. Click any of them, and you will be able to configure the corresponding function.

4.5.1 Port Filtering

Port Filtering allows you to enable or disable TCP ports and UDP ports on computers or network devices. Port Filtering insulates your local computers from many TCP/IP security attacks, including internal attacks by malicious users.

Wizard
Operating Mode
WAN Setup
LAN Setup
Wireless Setup
Firewall
Security
QoS
System
Status
Logout

Port Filtering IP Filtering URL Filtering MAC Filtering

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

Enable Port Filtering

Port Range: -

Protocol: TCP+UDP ▾

Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable Port Filtering: Check this box will enable Port Filtering function.

Port Range:The port range that you want to filter.

Protocol: The protocol that you want to filter, either TCP, UDP, or Both.

Comment: You can add some comment for this item.

Current Filter Table: The table shows all you have configured. You can delete one or all.

4.5.2 IP Filtering

IP Filtering is used to block internet or network access to specific IP addresses on your local network. The restricted user may still be able to login to the network but will not be able to access the internet. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the user you wish to block.

Port Filtering IP Filtering URL Filtering MAC Filtering

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

Enable IP Filtering

Local IP Address: -

Protocol: TCP+UDP ▾

Comment:

Current Filter Table:

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

Enable IP Filtering: Check this box will enable IP Filtering function.

Local IP Address: The LAN device's IP address that you want to filter.

Protocol: The protocol that you want to filter, either TCP, UDP, or Both.

Comment: You can add some comment for this item.

Current Filter Table: The table shows all you have configured. You can delete one or all.

4.5.3 URL Filtering

URL filtering is used to deny LAN users from accessing the internet.

The screenshot shows the 'URL Filtering' configuration page. At the top, there are tabs for 'Port Filtering', 'IP Filtering', 'URL Filtering' (which is selected), and 'MAC Filtering'. Below the tabs, a text box explains: 'The URL filter is used to restrict LAN users access to the internet. Block those URLs which contain keywords listed below.' There is a checkbox labeled 'Enable URL Filtering'. Below it is a text input field for 'URL Address:'. There are 'Apply' and 'Reset' buttons. Below this is a section titled 'Current Filter Table:' which contains a table with two columns: 'URL Address' and 'Select'. Below the table are three buttons: 'Delete Selected', 'Delete All', and 'Reset'.

Enable URL Filtering: Check this box will enable URL Filtering function.

URL Address: The URL Address that you want to filter.

Current Filter Table: The table shows all you have configured. You can delete one or all.

4.5.4 MAC Filtering

MAC Filtering allows you to deny access to specific users connecting to the network. Each networking device has a unique address called a MAC address (a 12 digit hex number).

The screenshot shows the 'MAC Filtering' configuration page. At the top, there are tabs for 'Port Filtering', 'IP Filtering', 'URL Filtering', and 'MAC Filtering' (which is selected). Below the tabs, a text box explains: 'Entries in this table are used to restrict certain types of data packets from your local network passing to the Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' There is a checkbox labeled 'Enable MAC Filtering'. Below it are two text input fields: 'MAC Address:' and 'Comment:'. There are 'Apply' and 'Reset' buttons. Below this is a section titled 'Current Filter Table:' which contains a table with three columns: 'MAC Address', 'Comment', and 'Select'. Below the table are three buttons: 'Delete Selected', 'Delete All', and 'Reset'.

Enable MAC Filtering: Check this box will enable MAC Filtering function.

MAC Address: The LAN device's MAC address that you want to filter.

Comment: You can add some comment for this item.

Current Filter Table: The table shows all you have configured. You can delete one or all.

4.6 QoS

The QoS helps improve your network gaming performance by prioritizing applications. By default the bandwidth control are disabled and application priority is not classified automatically.

In order to complete this settings, please follow the steps below.

1. Enable this function.
2. Enter the total speed or choose automatic mode.

3. Enter the IP address or MAC address user want to control.
4. Specify how to control this PC with this IP address or MAC address, include Maximum or minimum bandwidth and its up/down speed.
5. Click Apply button to add this item to control table.

Wizard

Operating Mode

WAN Setup

LAN Setup

Wireless Setup

Firewall

Security

QoS

System

Status

Logout

QoS

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

Enable QoS

Mode: Bandwidth Shaping WFQ

Uplink Speed (Kbps): (1M=1024Kbps)

Downlink Speed (Kbps): (1M=1024Kbps)

QoS Rule Setting:

Address Type: IP MAC

Local IP Address:

Protocol:

Local Port:(1-65535) -

MAC Address:

Weight:

Mode:

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Current QoS Rules Table:

Local IP Address	MAC Address	Mode Valid	Uplink Bandwidth	Downlink Bandwidth	Weight Select
------------------	-------------	------------	------------------	--------------------	---------------

4.7 System

There are six submenus under the System menu: **Time Zone, Upgrade, Save/Reload Settings, Password, Reboot**. Click any of them, and you will be able to configure the corresponding function.

4.7.1 Time Zone

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

Wizard

Operating Mode

WAN Setup

LAN Setup

Wireless Setup

Firewall

Security

QoS

System

Status

Logout

Time Zone Upgrade Save/Reload Password Reboot

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

Current Time: 2018 Yr 11 Mon 20 Day 14 Hr 39 Mn 28 Sec

Time Zone Select:

Enable NTP client Update

Automatically Adjust for Daylight Saving

NTP server: 131.188.3.220 - Europe 0.0.0.0 (Manual IP Setting)

Copy Computer Time: Enter your PC's current time into the above blanks.

Time Zone select: Select your local time zone from this pull down list.

Enable NTP client Update: Check this box to connect NTP Server and synchronize internet time.

NTP Server: Select the NTP Server, then the router will get the time from the NTP Server preferentially.

4.7.2 Upgrade

You can upgrade latest Firmware in this page.

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

Firmware Version: v96e92e_1.4.2_d181120

Select File: 浏览...

Firmware Version: This displays the current firmware version.

4.7.3 Save/Reload

You can backup or restore the system configuration in this page.

This page allows you to save current settings to a file or reload the settings from a file that was saved previously. You can also reset the current configuration to factory defaults.

Save Settings to File:

Load Settings from File: 浏览...

Reset Settings to Default:

Save Settings to File: Get the router's settings and store it in your local computer.

Load Settings from File: Restore the settings from the file you backup before from your local computer, the router will go to the former settings.

Reset Settings to Default: Restore the system settings to factory default.

4.7.4 Password

To ensure the router's security, you will be asked for your password when you access the router's Web-based Utility. The default user name is **"admin"**, the default password is **""**. This page will allow you to modify the User name and passwords.

Time Zone	Upgrade	Save/Reload	Password	Reboot
-----------	---------	-------------	-----------------	--------

This page is used to setup an account to access the web server of the Access Point. An empty user name and password will disable password protection.

User Name:

New Password:

Confirm Password:

4.7.5 Reboot

You can reboot device via clicking the **Apply** button.

Time Zone	Upgrade	Save/Reload	Password	Reboot
-----------	---------	-------------	----------	---------------

You can click the Apply button to reboot the router.

Chapter 5 Status

There are three submenus under the Status menu: **Status, Statistics, Log**. Click anyone, you will see the following status.

5.1 Status

The System Status provides you with a snapshot of your router's current connections and settings.

The System Information section provides you with the router's firmware version and build. This is used to help our support department determine what firmware version your device is running. The Current Date / Time is the setting for the system clock.

The Wireless Configuration shows the details of the 2.4GHz wireless networks.

The TCP/IP Configuration displays the current configurations for local network IP address and DHCP server settings.

The WAN Configuration displays the information from your Internet Provider. If for some reason your Internet connection stops working, you may try running through the Smart Setup Wizard again.

The screenshot shows the router's web interface with the 'Status' menu selected. The left sidebar contains navigation options: Wizard, Operating Mode, WAN Setup, LAN Setup, Wireless Setup, Firewall, Security, QoS, System, Status (highlighted), and Logout. The main content area displays the following information:

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

System	
Uptime	0day:5h:4m:53s
Firmware Version	v96e92e_1.4.2_d181120
Build Time	Tue, 20 Nov 2018 10:50:31 +0800

Wireless Configuration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	INTELLINET_AP
Channel Number	1
Encryption	WEP 128bits
BSSID	00:00:00:00:00:00
State	Scanning

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.0.30
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
DHCP Server	Enabled
MAC Address	00:e0:61:12:31:24

WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:61:12:31:23

5.2 Statistics

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

The Wireless 1/2 LAN connection statistics shows all data activity for both the 5.0GHz wireless networks.

The Ethernet LAN connection statistics shows all data activity for all users physically connected to the wired ports on the router.

The Ethernet WAN connection statistics shows the data activity for all upload and download data over your Internet connection.

Status **Statistics** **Log**

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

Wireless LAN	<i>Sent Packets</i>	282620
	<i>Received Packets</i>	243649
Ethernet LAN	<i>Sent Packets</i>	6661
	<i>Received Packets</i>	5854
Ethernet WAN	<i>Sent Packets</i>	5637
	<i>Received Packets</i>	0

[Refresh](#)

5.3 Log

The System Log is useful for viewing the activity and history of your router. The System Log is also used by Amped Wireless technicians to help troubleshoot your router when needed. It is recommended that you enable logs in the event that troubleshooting is required. Click the **“Refresh”** to update the log. Click **“Clear”** to clear all shown information.

Status **Statistics** **Log**

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

Enable Log

System All Wireless DoS

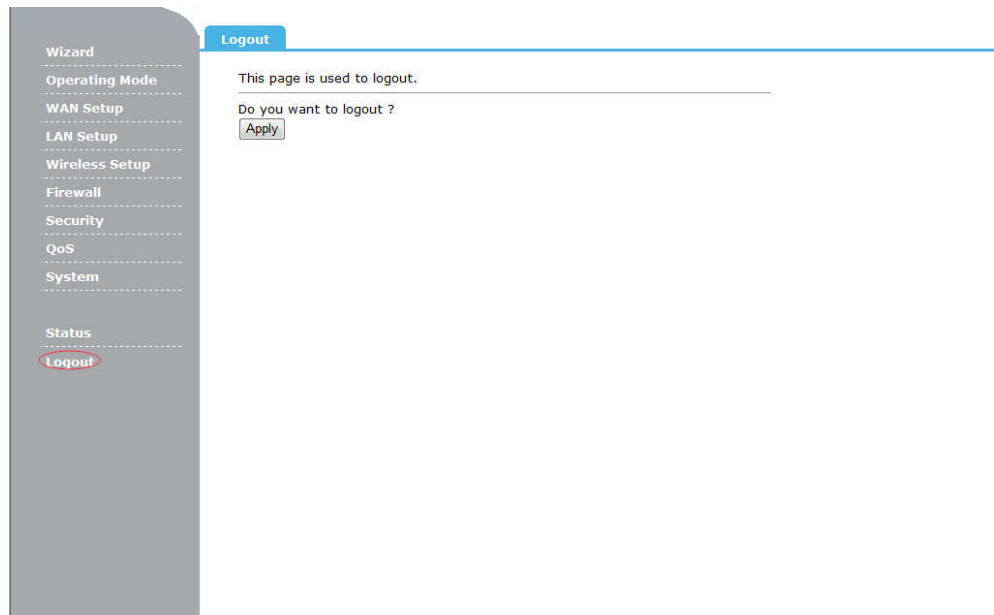
[Apply](#)

[Refresh](#) [Clear](#)

Enable Log: Click this box to enable Log.

Chapter 6 Logout

Choose “Logout”, and you will be back to the login screen.



Supplier's Declaration of Conformity 47 CFR § 2.1077 Compliance Information

Unique Identifier: (525404-300N)

Responsible Party – U.S. Contact Information

IC INTRACOM USA, Inc.

550 Commerce Blvd, Oldsmar, Florida
34677

Phone: +1-813-855-0550, ext. 230

Direct Fax: +1-813-371-1775

Direct Person :Dave Sousa

FCC Compliance Statement

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

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause

harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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