Brand Name: Quanta

Quanta Computer, Inc.

IEEE802.16e WiMAX IAD (WV202)

User Manual

Version 1.0

Revision History

Revision	Date	By	Description	Reviewed By
0.1	09/03/2007	Terry	First edition	
0.2	09/07/2007	Terry	Refine format	
0.3	11/1/2007	Terry	Modify	
0.4	03/25/2008	Jud	Modify	
0.5	07/08/2008	Jud	Modify	
0.6	08/04/2008	Jud	1. Add the copyright description. 2. Update the newest UI and the description. 3. Add TR069	
0.7	08/12/2008	Jud	1. Modify the title to add brand name 2. Add the using notice.	
1.0	08/03/2009	Jud	3. Add Federal Communication Commission Interference Statement	

Federal Communication Commission Interference Statement

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

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

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

Due to the essential high output power natural of WiMAX device, use of this
device with other transmitter at the same time may exceed the FCC RF exposure
limit and such usage must be prohibited (unless such co-transmission has been approved by FCC in the future).

Copyright

Trademarks

QCI is a registered trademark of Quanta Computer Inc. Other trademarks and registered trademarks and logo mentioned in this publication are only used for identification purposes.

Notice

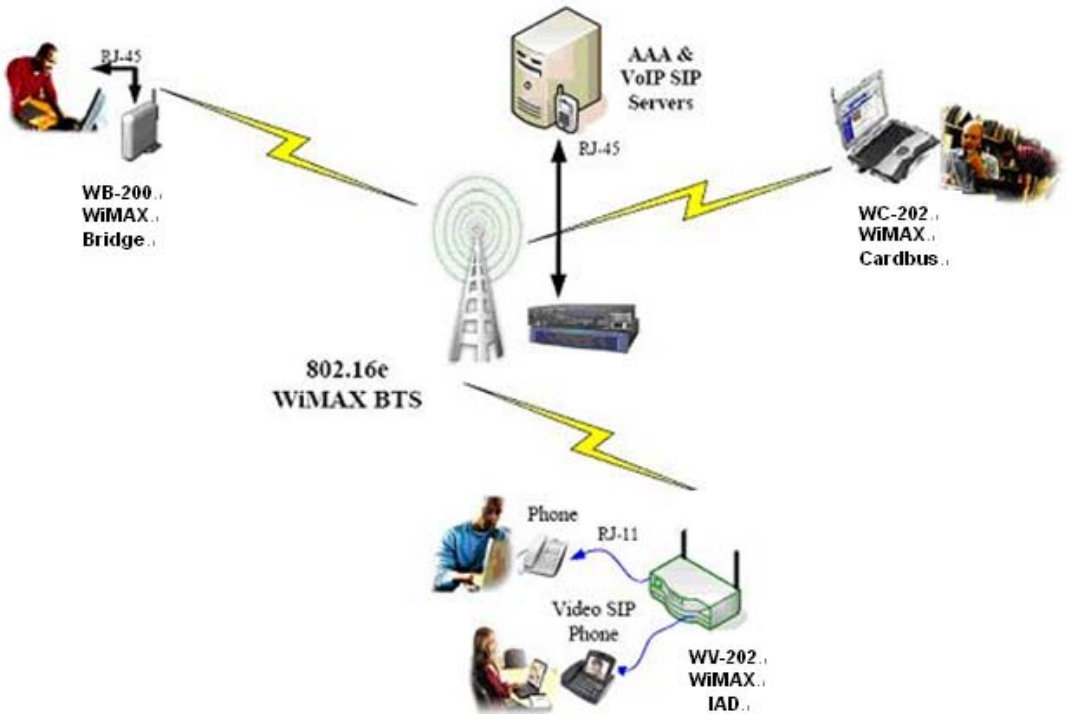
When the operator is using this product, and if this product has the signal interference in the same time, it will have noise interference in the telephone. But the noise interference is lower, it won't interfere the communication quality when operators are making the call. And this interference is normal status and under the product spec.

Table of Contents

1. Introduction

The WV202 WiMAX IAD is a WiMAX LAN router with two LAN ports, two VoIP (FXS) ports and one WiMAX WAN interface. The WV202 supports IEEE 802.16e-2005 state of the art Scalable OFDMA based Technology. It operates on 2.496 GHz ~ 2.69GHz frequency licensed band. It supports WiMAX forum Wave1 SISO specification and provides users a seamless broadband wireless access; VoIP calls at home, office. It acts as two devices in one box. First, there's a built-in two full-duplex 10/100 Base-T Ethernet ports that allows user to connect PC/NB or Ethernet switch devices together to extend the connectivity. Secondly, the routing functions tie these devices together and allow networked devices to share a high-speed broadband connection via the broadband WiMAX WAN port.

Look at below diagram show you the example usage model for WV202 with our others products (WC202 WiMAX Cardbus, WB200 WiMAX Bridge). With the WiMAX IAD at the center of your home or office network, you can share a high-speed Internet connection, files, and multi-player games with flexibility, speed, and security!



WiMAX Usage Model Example

1.1 Audience

This document is intended for system vendor who are using WV202 to build an Internet telephony gateway or server application. It is assumed that the reader has the general knowledge of VoIP applications and products.

1.2 Acronyms

API	Application Interface
ALG	Application Layer Gateway
ACI	Audio CODEC Interface
ADC	Analog to Digital Converter
CODEC	Coder / Decoder
DAC	Digital to Analog Converter
DC	Direct Current
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DTMF	Dual Tone Multi Frequency
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GMT	Greenwich Mean Time
IP	Internet Protocol
IPsec	Internet Protocol Security
L2TP	Layer 2 Tunnel Protocol
LAN	Local Area Network
MAC	Media Access Control
MII	Media Independent Interface
NAT	Network Address Translation
NTP	Network Time Protocol
PPTP	Point-to-Point Tunneling Protocol
RTP	Real-Time Transport Protocol
RTCP	Real-Time Transport Control Protocol (also known as RTP control protocol)
SIP	Session Initiation Protocol
SLIC	Subscriber Line Interface Circuit
STUN	Simple Traversal of UDP through NATs
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

2. Installation and Setup

2.1 Quick Start

2.1.1 WV202 WiMAX IAD factory default settings

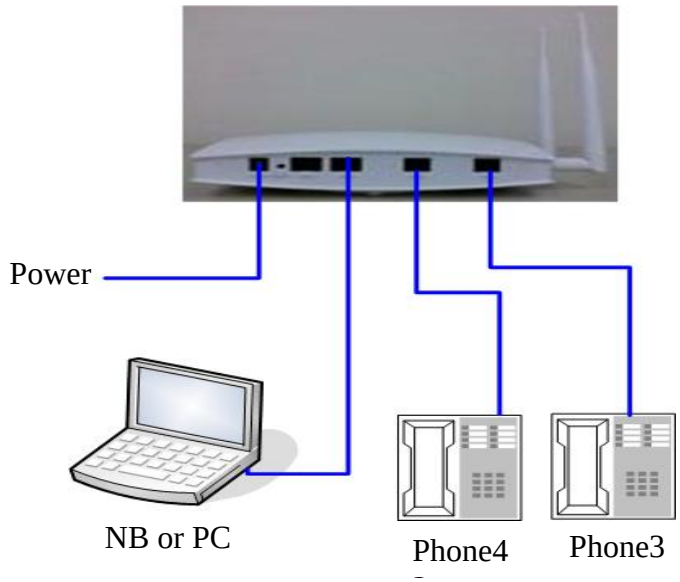
- LAN IP: 192.168.1.254
- Netmask: 255.255.255.0
- LAN DHCP: enable
- User Name/Password: root/root

2.1.2 How to configure WV202

To access the WiMAX IAD via Ethernet, the host computer must meet the following requirements:

- Equipped with an Ethernet network interface.
- Have TCP/IP installed.
- Allow the client PC to obtain an IP address automatically or set a fixed IP address.
- With a web browser installed: Internet Explorer 5.x or later.

The connection structure is as below:



The WiMAX IAD is configured with the default IP address of 192.168.1.254 and subnet mask of 255.255.255.0. Considering that the DHCP server is enabled by default, the DHCP clients should be able to access the WiMAX, or the host PC should be assigned an static IP address first for initial configuration. An example for static IP address can be set to “192.168.1.100”.

You also can manage the WiMAX IAD through a web browser-based manager. The WiMAX IAD manager uses the HTTP protocol via a web browser to allow you to set up and manage the device. The URL of management web site is : http://192.168.1.254. Following are the steps to login and control the IAD.

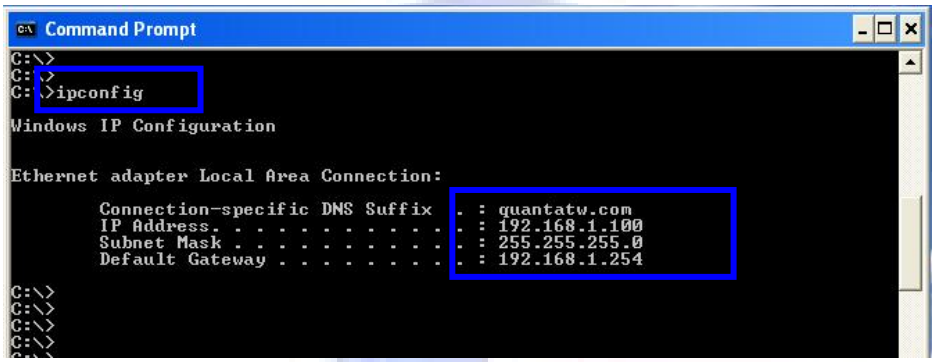
Step 1: Power on IAD, when the booting is finished, the LED stats of IAD is as below:

LED is always “ON”: “Power”, “FXS1”, “FXA2”

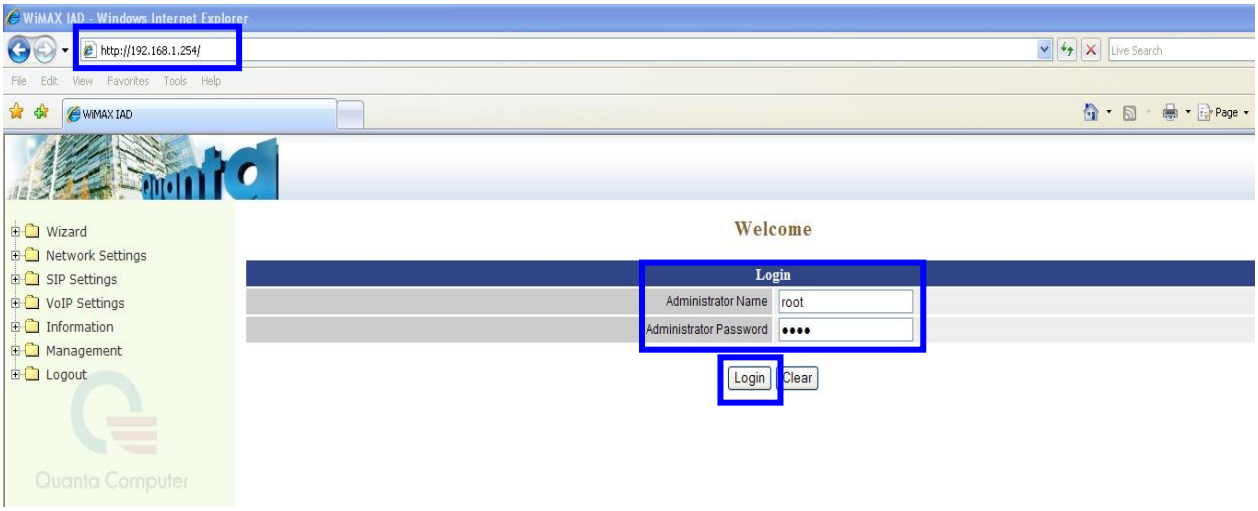
LED is always “OFF”: “WiMAX”, “LAN1”, “LAN2”, “System”

Step 2: Connect the network adapter of the PC to the LAN1 port on IAD.

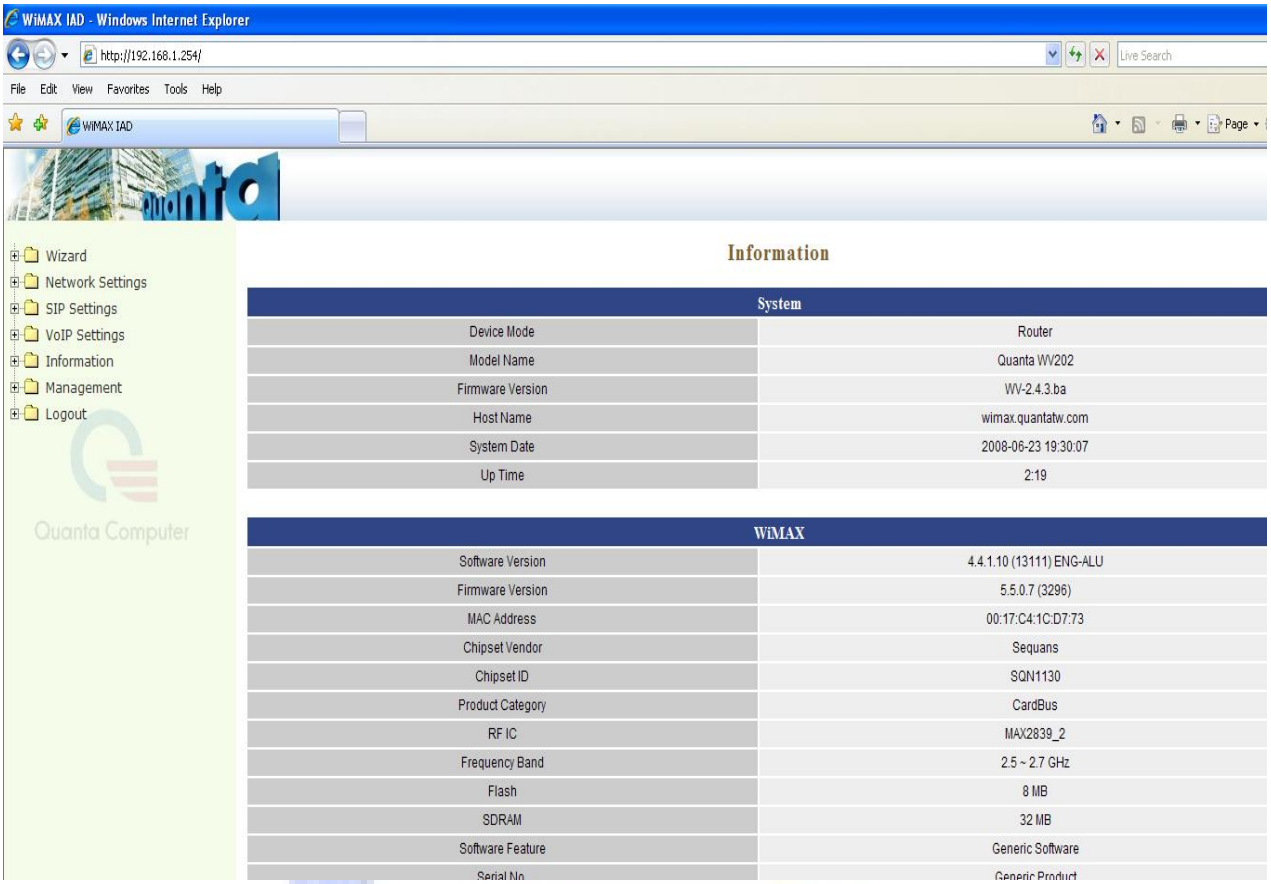
Step 3: Make sure the PC’s IP address getting from IAD DHCP server is 192.168.1.xxx. The default IP address is 192.168.1.100 for the first requested client.



Step 4: Open the browser and input the web control site: http://192.168.1.254 and input the login username and password: root/root, then click the “Login” button



Step 5: You will see the information page after login the web site.



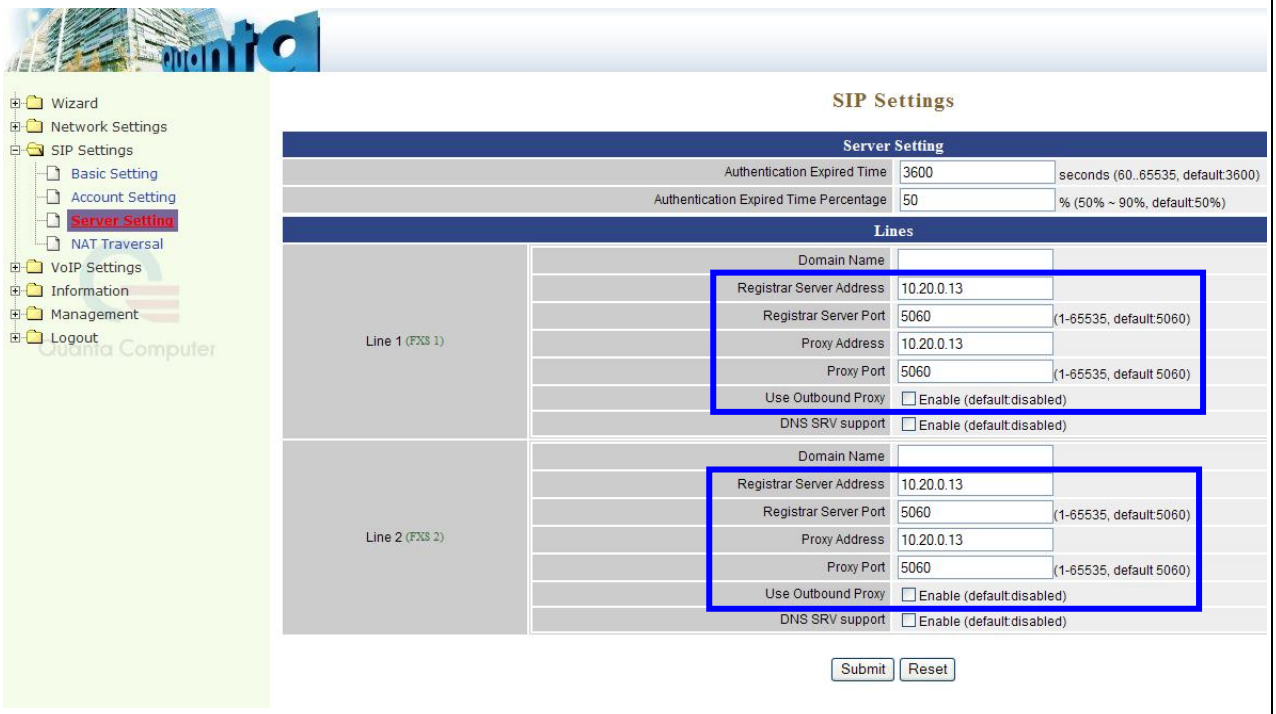
2.1.3 How to use VoIP?

SIP Settings -> Account Setting

- Type User Name and Display Name
- Type Authentication User Name as the phone number
- Type Authentication Password
- Confirmed Password

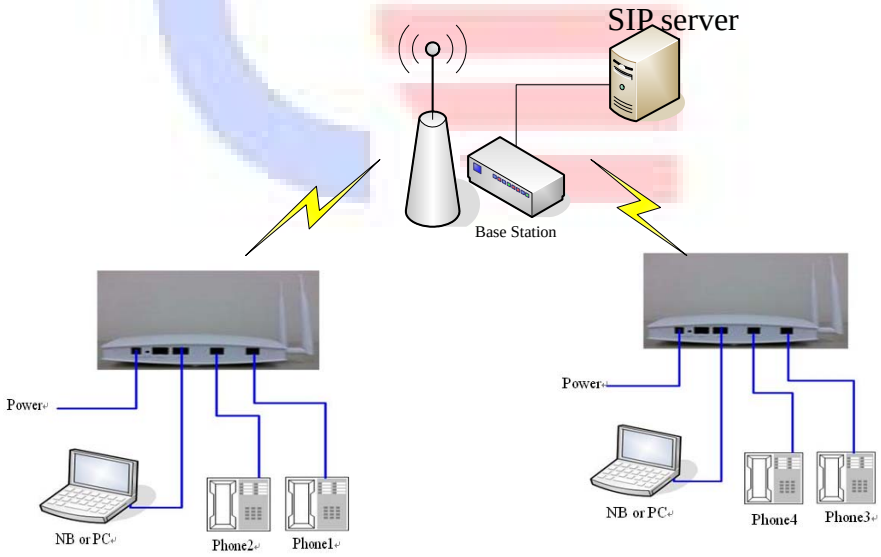
Please make sure the Authentication User Name and Authentication Password had been setup in SIP server.

SIP Settings -> Server Setting



- Type Registrar Server Address as your SIP server address
- Type Proxy Address to the same with SIP server
- Make sure WV202 has already registered to your Registrar Server then you can make VoIP call.

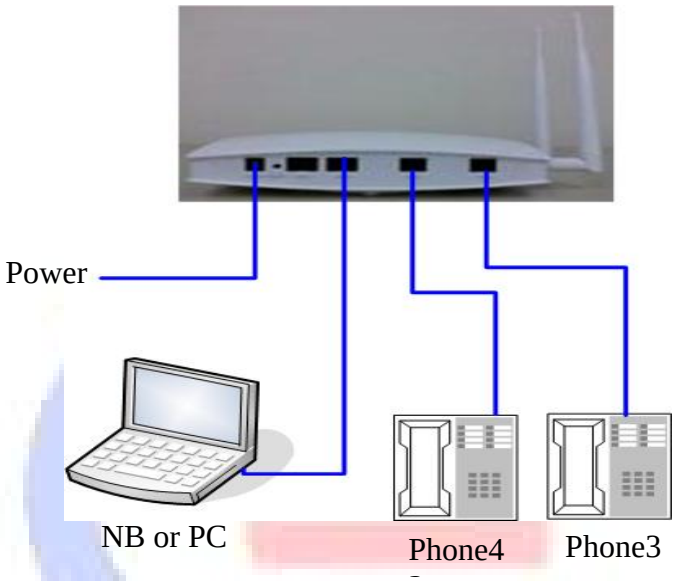
2.1.4 How to make a three way conference call?



- Make a call to the first party. For example: phone1 makes a call to phone2.
- "Flash hook" to hold the call. For example: phone1 “Flash hook”.
- Then you will hear a dial tone.
- Make the other call to the third party. For example: phone1 makes the other call to phone3.
- Dial "*71" to connect the two party calls for conferencing. For example: phone1 dials “*71”, then phone1, phone2 and phone3 are in a conference call.

3. Network Settings

All the network functions are set in this section. Before managing the IAD, please make sure you have set the connection structure as below and refer the settings in the section 2.1.2 How to configure WV202.



All the functions are supported as the following items.

- WAN
- Auto Connect
- WiMAX EAP
- LAN
- DHCP
- Static Route
- NAT
- Packet Filter
- URL Filter
- Security
- UPnP
- DDNS
- QOS
- TR069

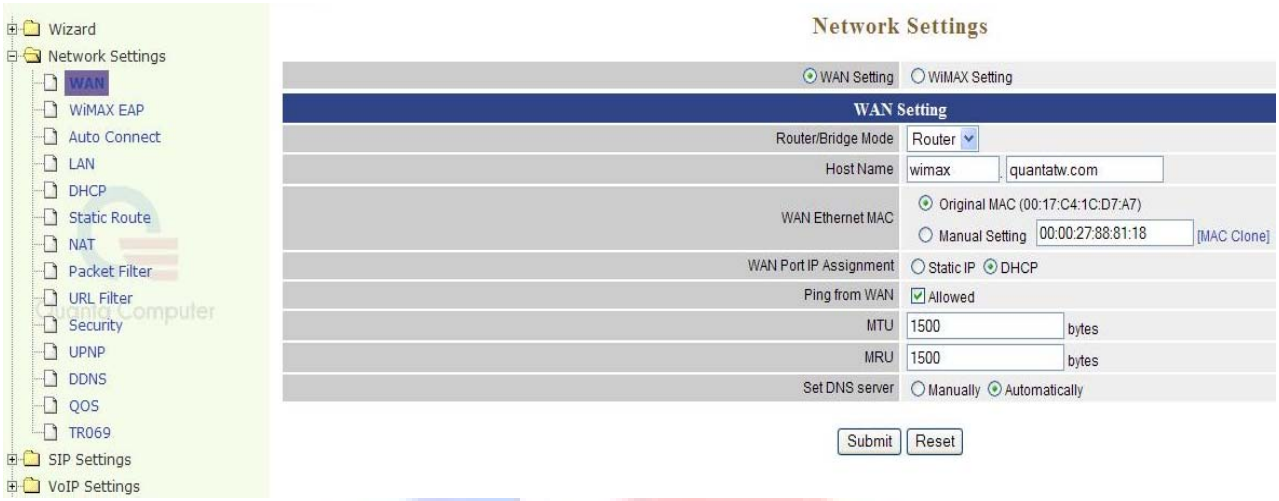
3.1 WAN

In WV202, the WAN is the WiMAX connection entry. There are two pages (WAN Setting and WiMAX Setting) to setting the TCP/IP settings and WiMAX frequency and bandwidth settings. The IAD is not yet supported the bridge mode for WAN.

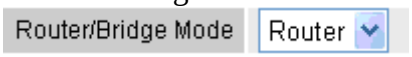
This chapter is going to introduce the function of each connection mode and the basic configuring steps that you have to do. If you do not follow the configuring steps for using these connection modes, you might get some connection problems and cannot connect to the Internet well.

3.1.1 WAN Setting

In this page, you can set the values about TCP/IP information like as IP address, MAC address, host name, MTU, MRU, and DNS server.



- Router / Bridge Mode



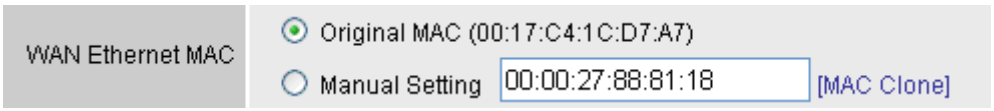
In this version it is just supported the “Router” mode to work as a gateway/router.

- Host Name

The Host Name field is optional but may be required by some Internet Service Providers. The default host name is wimax.quantatw.com. It is a computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address. Assign the domain name or IP address of your host computer.

When the host operating system is set up it is given a name. This name may reflect the prime use of the computer. For example, a host computer that is a web server may be called www.xxx.com. When we need to find the host name from an IP address we send a request to the host using its IP address. The host will respond with its host name.

➢ WAN Ethernet MAC



There are two methods to set the MAC address.

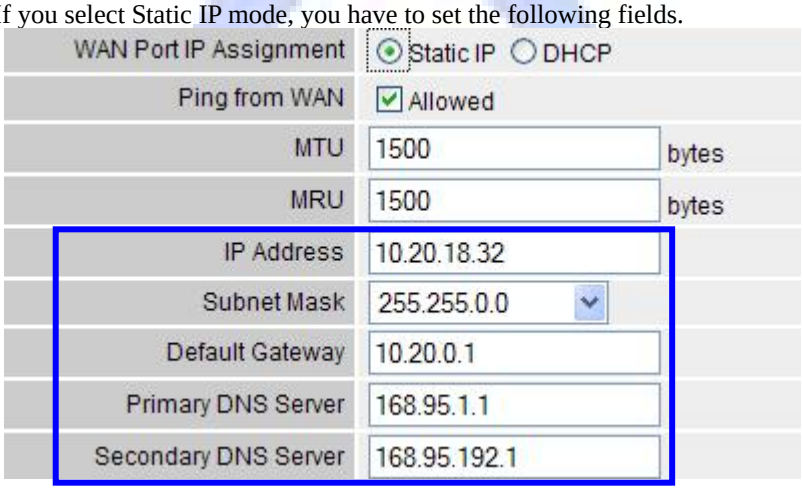
a. Original MAC
   The original MAC is the manufacture shipping MAC address.
b. Manual Setting
   You can set the specific MAC address in this field or set the MAC address of the computer you are using by clicking the "MAC Clone". After setting MAC address, please click "Submit" button.

➢ WAN Port IP Assignment

You have two methods to set the WAN port IP, one is Static IP mode and the other one is DHCP mode. The default setting is DHCP mode to get IP from DHCP server.

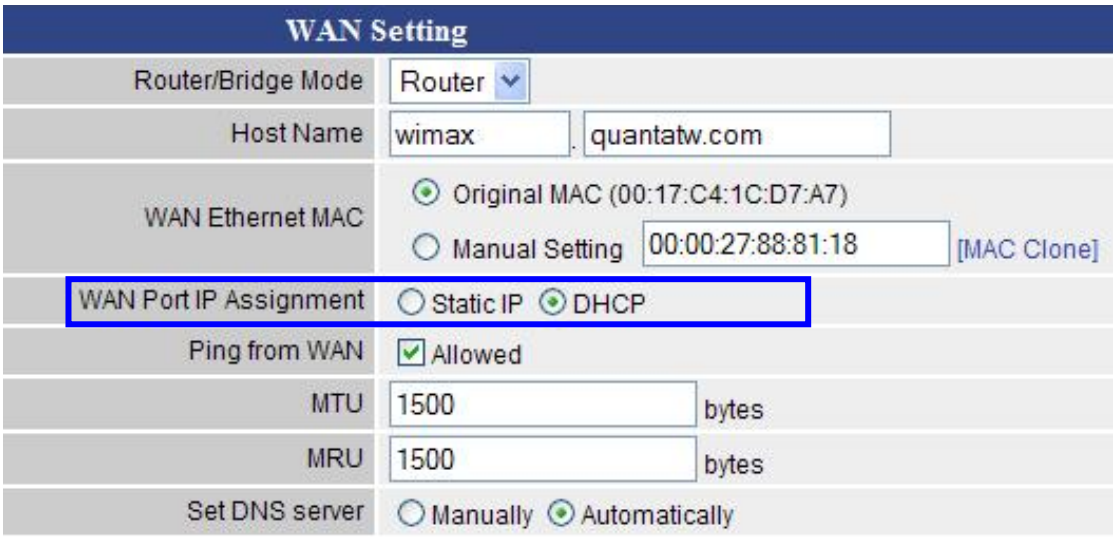
◆ Static IP Mode
When you want to set the WAN IP to a static IP address, you can select Static IP mode. Sometimes the ISP provider maybe gives you a static IP and requests you to set it for WAN port.

If you select Static IP mode, you have to set the following fields.



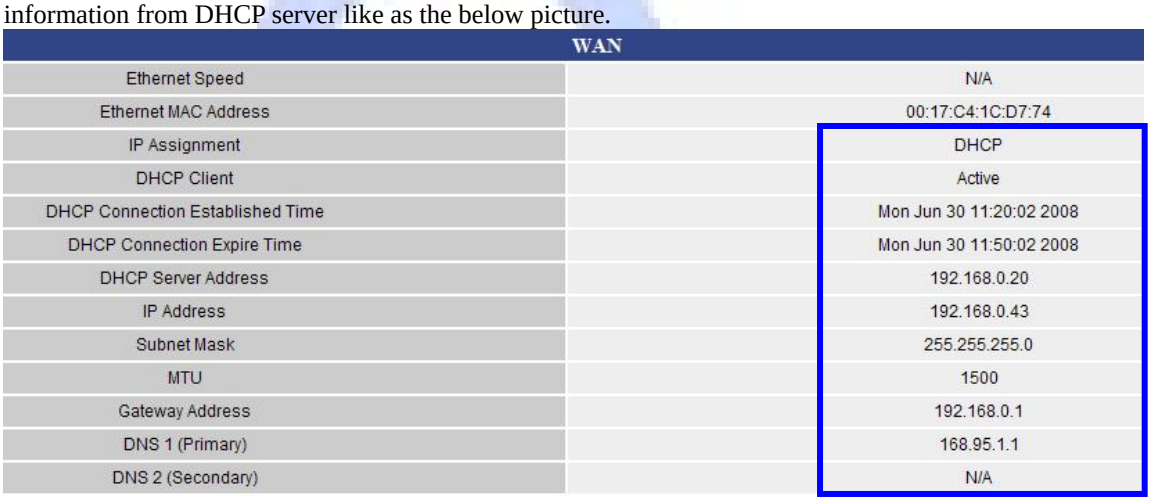
Field	Description	Default value
IP address	Enter the IP address provided by your ISP	10.20.18.32
Subnet Mask	Enter the subnet mask provided by your ISP.	255.255.0.0
Default Gateway	Enter the gateway provided by your ISP.	10.20.0.1
Primary DNS Server	DNS (Domain Name System) is for mapping a domain name to its assigned IP address. Enter the IP address for the primary DNS server. The IPS maybe provides you the IP address for DNS server.	168.95.1.1
Secondary DNS Server	Enter the IP address for the second DNS server	168.95.192.1

◆ DHCP mode

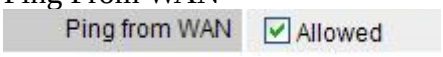


If you select DHCP mode for WAN port, the IAD will auto gets IP address, subnet mask and default gateway address from ISP's DHCP server.

After the WAN port is connected to WiMAX Base Station, the DHCP client will auto gets the information from DHCP server like as the below picture.



➢ Ping From WAN



Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating

The default setting is allowed user can ping the host computer from remote site. If you disallow, the host computer doesn't response any user who issues Ping IP address command from any remote sites.

Field	Description
Allowed Enable 	Response the ping information to remote client. (Default setting is enable)
Allowed Disable 	Doesn't response the ping information to remote client.

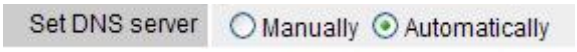
➢ MTU

MTU stands for Maximum Transmission Unit, the largest physical packet size, measured in bytes that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. The network MTU rate is set to 1500 bytes with default settings.

➢ MRU

MRU stands for Maximum Receiving Unit. the largest physical packet size, measured in bytes that a network can receive. Any messages larger than the MRU are divided into smaller packets before being received. The network MRU rate is set to 1500 bytes with default settings.

➢ Set DNS Server



DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a user-friendly, easy to remember name such as www.xxx.com. The DNS server converts the user-friendly name into its equivalent IP address.

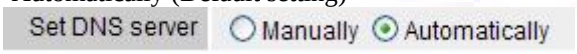
The original DNS specifications require that each domain name is served by at least 2 DNS servers for redundancy. When you run your DNS, web, and mail servers all on the same machine - if this machine goes down, it doesn't really matter that the backup DNS server still works.

The recommended practice is to configure the primary and secondary DNS servers on separate machines, on separate Internet connections, and in separate geographic locations.

- Primary DNS Server: Sets the IP address of the primary DNS server.
- Secondary DNS Server: Sets the IP address of the secondary DNS server.

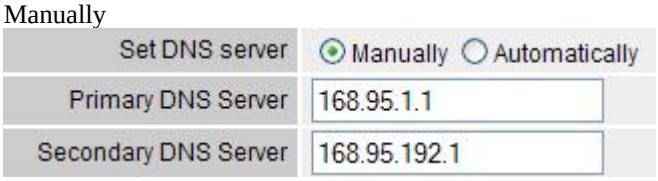
There are two methods to set the DNS server:

a. Automatically (Default setting)



When you select the Auto mode, the IP address of DNS server will be gotten from ISP's DHCP server. You will get IP address of the primary DNS server and the secondary DNS server.

b. Manually

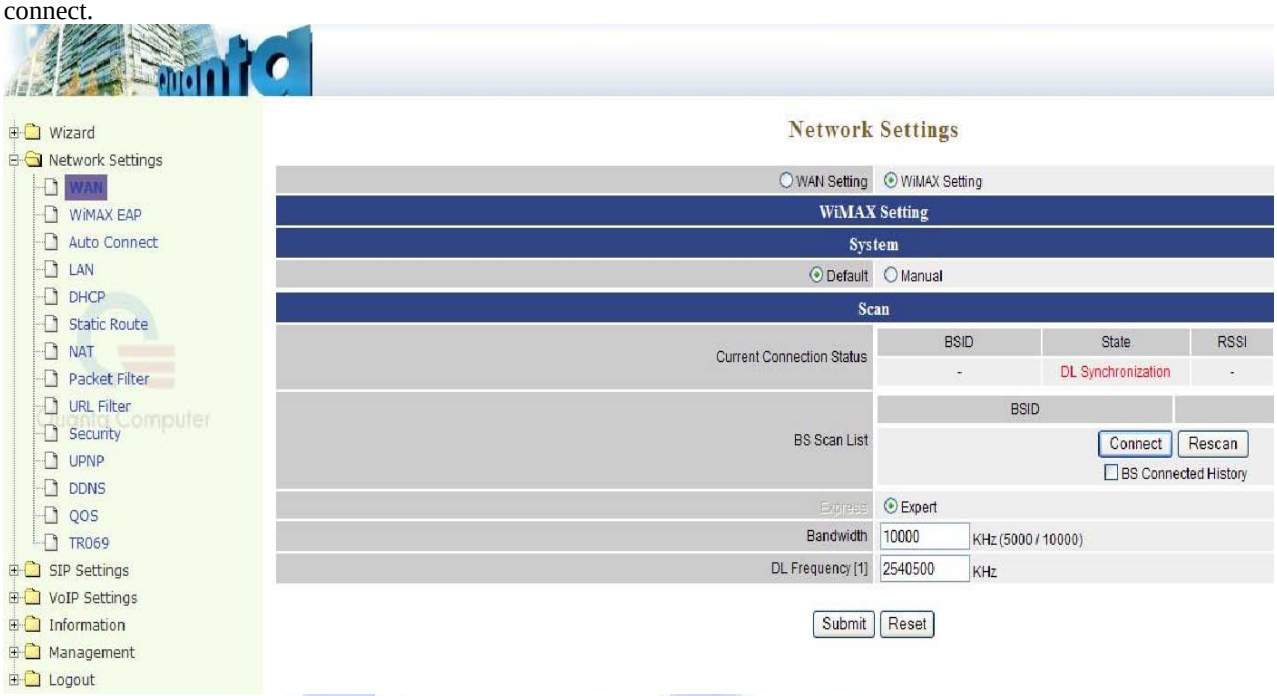


When you want to set the DNS server manually, you can select this mode to set primary DNS server and secondary DNS server as below.

Field	Description	Default value
Primary DNS Server	Sets the IP address of the primary DNS server	168.95.1.1
Secondary DNS Server	Sets the IP address of the secondary DNS server	168.95.192.1

3.1.2 WiMAX Setting

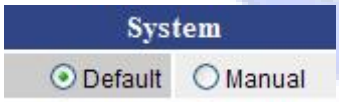
The WiMAX settings for connecting to BS are described in this section. You can set the WiMAX bandwidth and DL frequency from your ISP and to scan the BS to show how many BS can be found to connect.



- System page

To set the OFDM and the gap time of TTG and RTG has two methods.

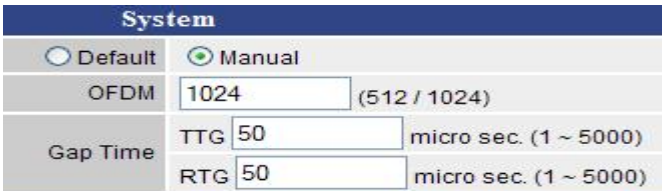
a. Default mode



In default mode, the default settings of the OFDM, TTG gap time and RTG gap time are as below.

Field	Description	Default value
OFDM	To input the FFT size in this field. The FFT size can be 512 or 1024 according to bandwidth is 5 MHz or 10 MHz.	1024
Gap Time TTG	Transmit/receive Transition Gap (TTG) is defined as the time between end of the last sample of the last OFDM-symbol of the UL and the start of the first sample of the preamble of the following DL frame.	50 micro seconds
Gap Time RTG	Receive/transmit Transition Gap (RTG) is defined as the time between end of the last sample of the last OFDM-symbol of the DL and the start of the first sample of the first OFDM-symbol of the UL frame	50 micro seconds

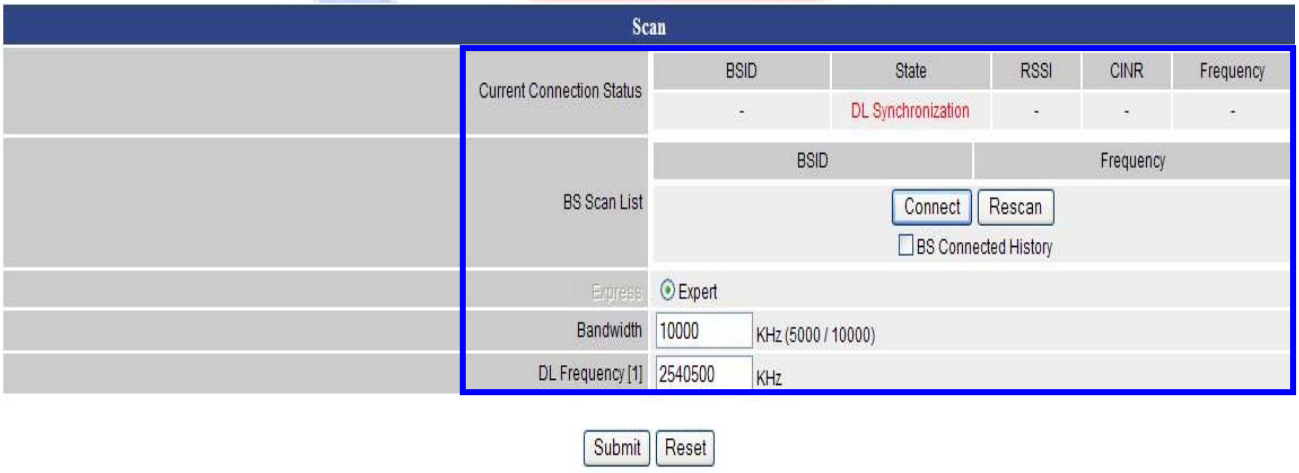
b. Manual mode



To manual set the following parameters for gap time and OFDM size to change different bandwidth responding BS.

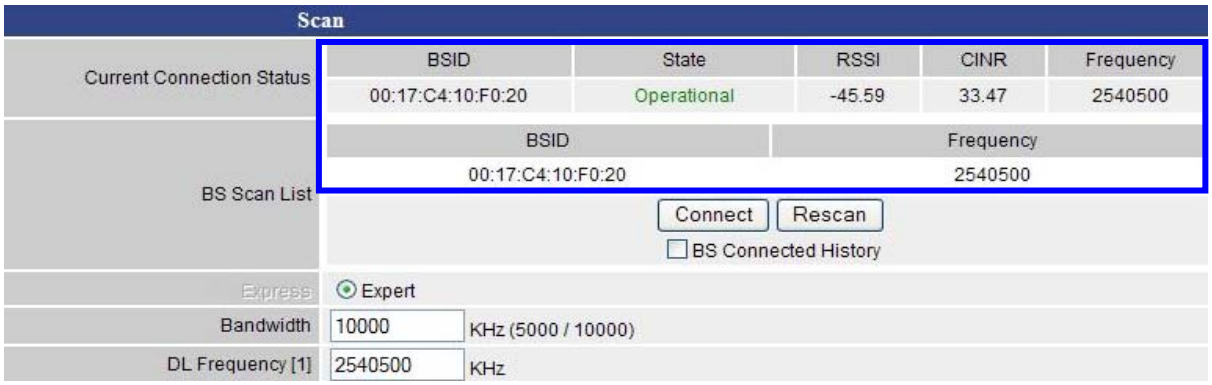
Field	Description	Default value
OFDM	To input the FFT size in this field. The FFT size can be 512 or 1024 according to bandwidth is 5 MHz or 10 MHz.	1024
Gap Time TTG	Transmit/receive Transition Gap (TTG) is defined as the time between end of the last sample of the last OFDM-symbol of the UL and the start of the first sample of the preamble of the following DL frame.	50 micro seconds
Gap Time RTG	Receive/transmit Transition Gap (RTG) is defined as the time between end of the last sample of the last OFDM-symbol of the DL and the start of the first sample of the first OFDM-symbol of the UL frame	50 micro seconds

➢ Scan page



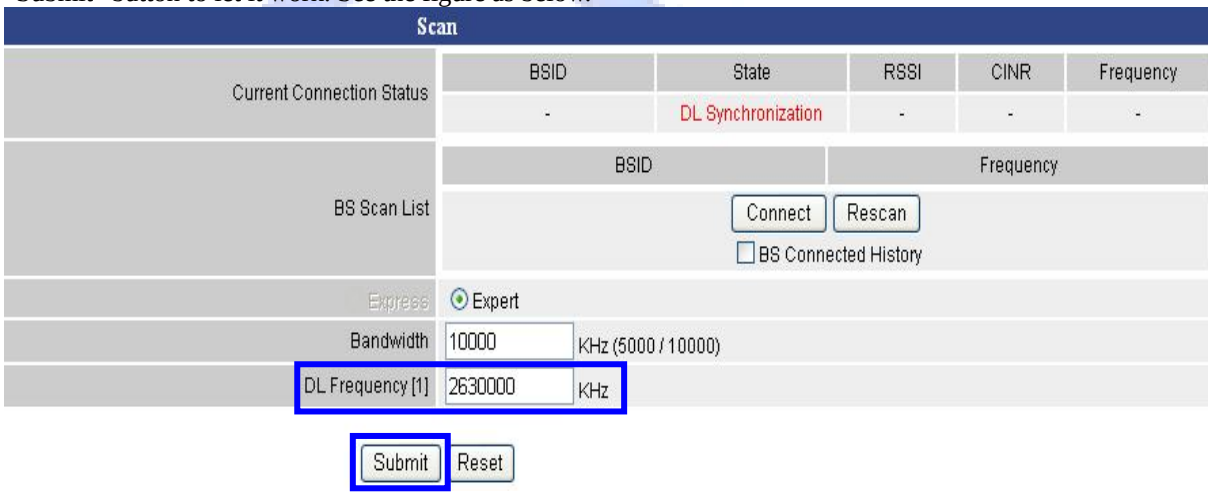
Field	Description	Default value
Current Connection Status	To show the information of the connected BS. It shows the BSID, State, RSSI, CINR, and Frequency data.	
BS Scan List	To show the BS list you scan with the DL frequency.	
Bandwidth	To set the Bandwidth for 5000 KHz (5 MHz) or 10000 (10 MHz) KHz by according to BS setting.	10000
DL Frequency[1]	To set the frequency from 2496000 KHz to 2699800 KHz by according to BS setting.	2540500

- To auto scan the BS is enabled as default setting, if the frequency of BS is the same with default setting 2540500 KHz, the BS will be auto scanned and shown in the BS scan list. Then the system will auto connects to the BS and shows the information of connected BS like as the figure below.

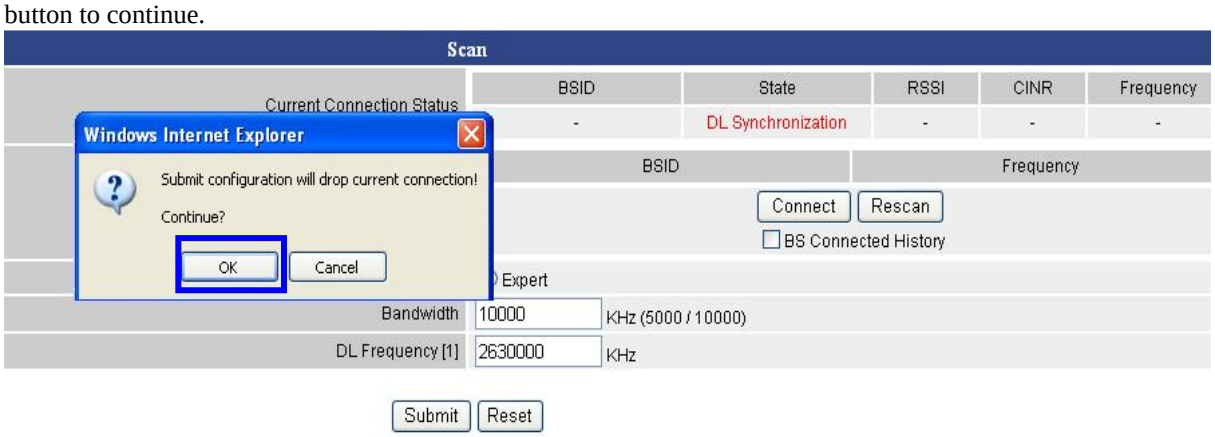


- If the frequency of BS is not the same with default setting, or you want to change BS with another frequency, please follow the steps as below.

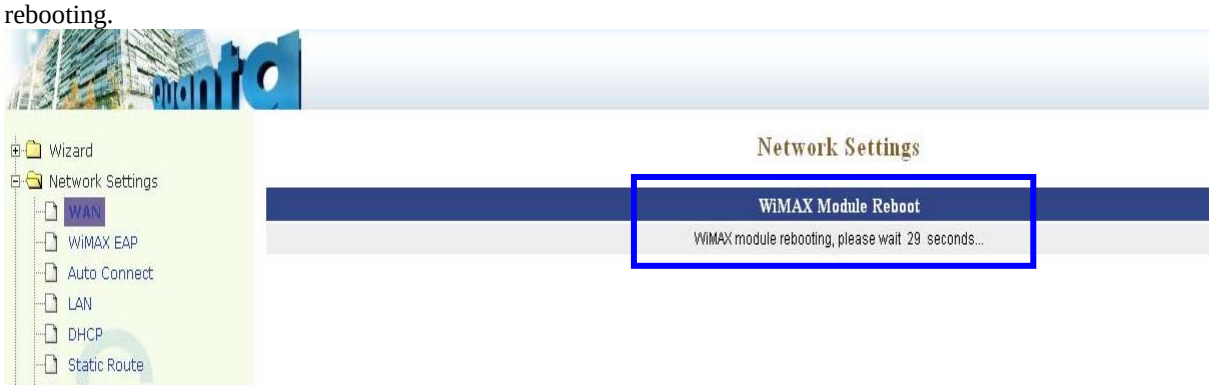
Step1. Setting the frequency from your ISP provider to the DL frequency[1] field. Then click the "Submit" button to let it work. See the figure as below.



Step2. Then it will show the message to drop current connection like as below. Please click "OK" button to continue.



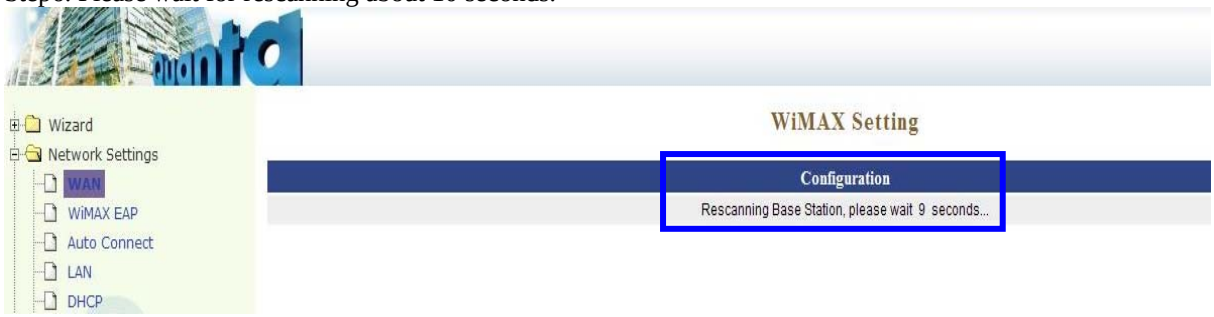
Step3. After changing the frequency, the WiMAX card will reboot. Please wait 30 seconds for rebooting.



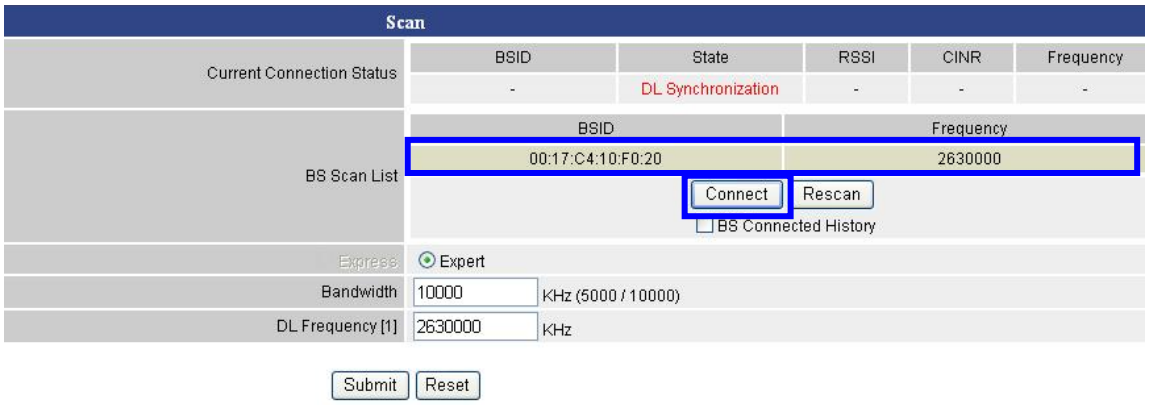
Step4. It will go back to the setting page. If there is no BS scanned in the BS scan list, please click "Rescan" button to rescan BS.

Step5. It will show the message to drop current connection, please click "OK" button.

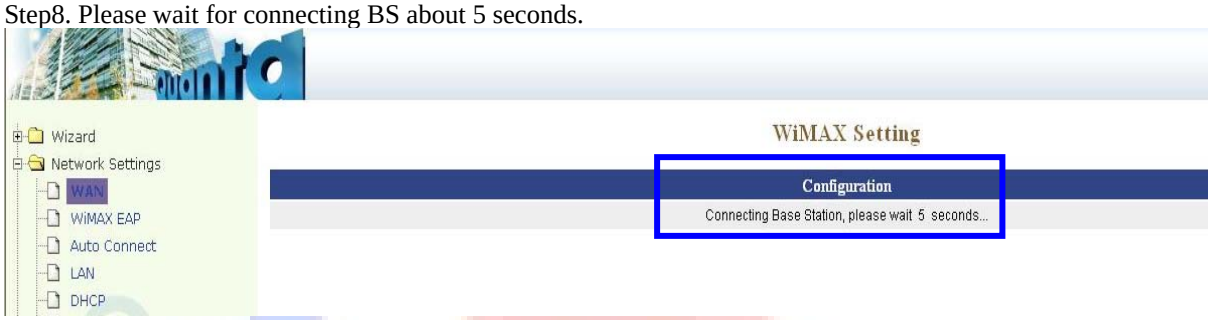
Step6. Please wait for rescanning about 10 seconds.



Step7. If there is no BS scanned, please repeat from step 4 to step 6 to rescan it; if the BS is scanned, it will be shown in the BS scan list. Please click the BSID of the scanned BD to mark the data, then click “Connect” button to connect the BS.



Step8. Please wait for connecting BS about 5 seconds.

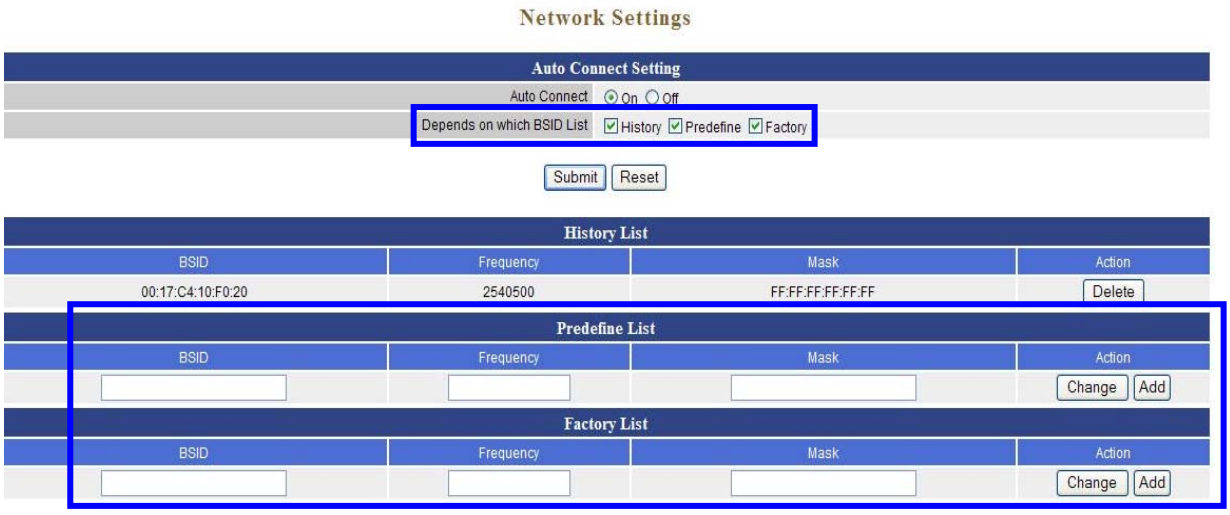


Step9. It will connect to the BS and show the connection status “Operational”.

3.2 Auto Connect

The Auto connect function will let IAD auto connect to WiMAX BS after booting up. There are some rules when you enable and disable this function.

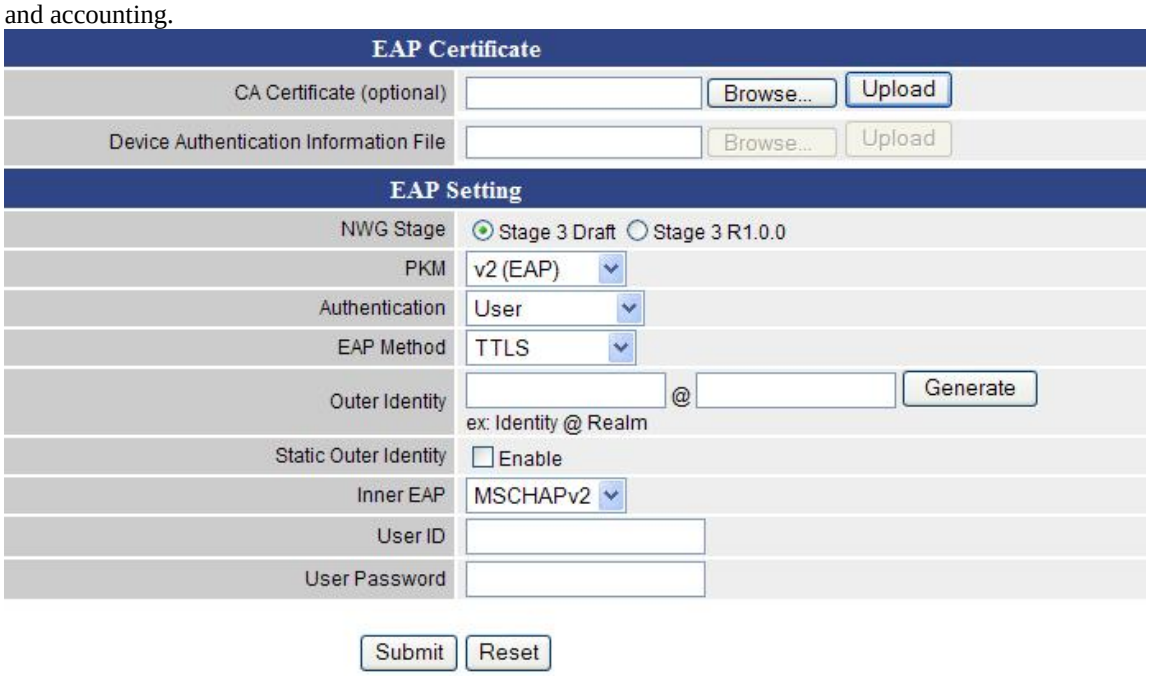
- If the Auto Connect button is “On”, WiMAX will try to connect with BS automatically.
- The default value of Auto Connect setting is “On”, if you rescan BS and connect to BS manual, the setting will be changed to “Off”.
- If the BSID list is by “History”, WiMAX IAD will connect to those BSs in the History list firstly.
- If several BSID entries in the history list, WiMAX IAD will connect to the BS which has the best CINR.
- The BS will be auto added in the history list after IAD has connected to the BS.
- You can manual add BS in the predefine list and factory list by enable “Predefine” and “Factory” function in the “Depends on which BSID List” field. See as below figure.



Field	Description	Default value
BSID	Input the BS’s BSID provided by ISP	
Frequency	Input the BS’s frequency provided by ISP	
Mask	Input the BS’s mask provided by ISP	
Change	Click this button to change the data of existed BS	
Add	Click this button to add the data of BS	

3.3 WiMAX EAP

EAP is used to communicate authentication information between the Supplicant and the Authentication Server. When you connect to BS with EAP authorization, an AAA (Authentication Authorization Accounting) server behind BS will confirm your authentication information, authorization and accounting.

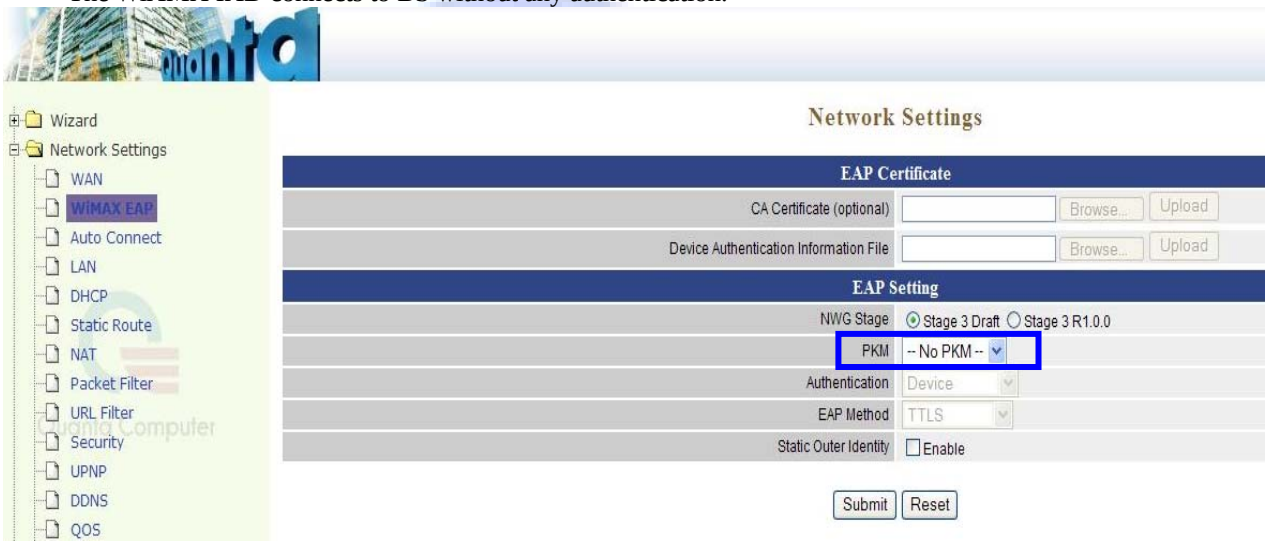


Field	Description	Default value
CA Certificate (optional)	To upload the CA certificate file provided by ISP when you select “User” or “User / Device” authentication. The CA certificate file is optional but depends on the AAA server request.	
Device Authentication Information File	To upload the device authentication information file provided by ISP when you select “Device” and “User / Device” authentication.	
NWG Stage	There are two stage of NWG (Network Working Group) to select. Base on the BS setting to select “Stage 3 Draff” or “Stage 3 R1.0.0”	Stage 3 Draff
PKM	Select “No PKM” (Private Key Management) or “v2(EAP)” for communicating with BS.	No PKM
Authentication	Three types to authenticate with AAA server or Radius server. “User” or “Device” or “User / Device”	User
EAP Method	Select TTLS (Technical Translation & Localization Services) Method or AKA (Authentication and Key Agreement) Method	TTLS
Outer Identity	The identity of this IAD to communicate with BS. It can be auto generated by clicking “Generate” button or can be set with any string between 16 bytes to 48 bytes manual. And the string only can be the combination with	

	numeral letters and English letters in lower case and upper case. Input the domain name in the filed after "@".	
Static Outer Identity	You can input any string which length is no limit when it is enable. The string can be set with any string between 16 bytes to 48 bytes manual. And the string only can be the combination with numeral letters and English letters in lower case and upper case.	Disable
Inner EAP	There are 4 Inner EAP (Extensible Authentication Protocol) to select. "MSCHAPv2" / "MSCHAP" / "CHAP" / "PAP"	MSCHAPv2
User ID	Input the user ID provided by ISP	
User Password	Input the user password provided by ISP	

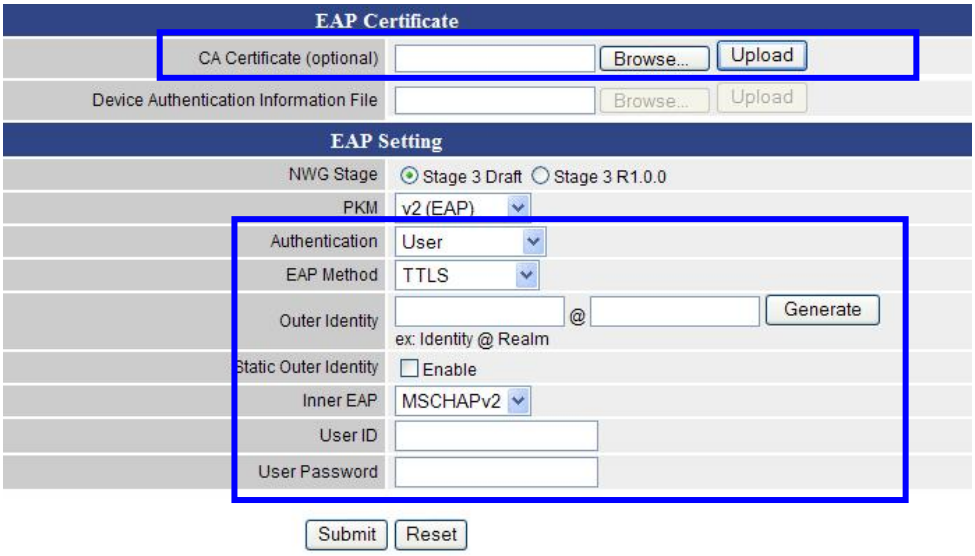
There are fore types for EAP setting to communicate authentication information with BS.

- Type1: No PKM setting
  The WiAMX IAD connects to BS without any authentication.

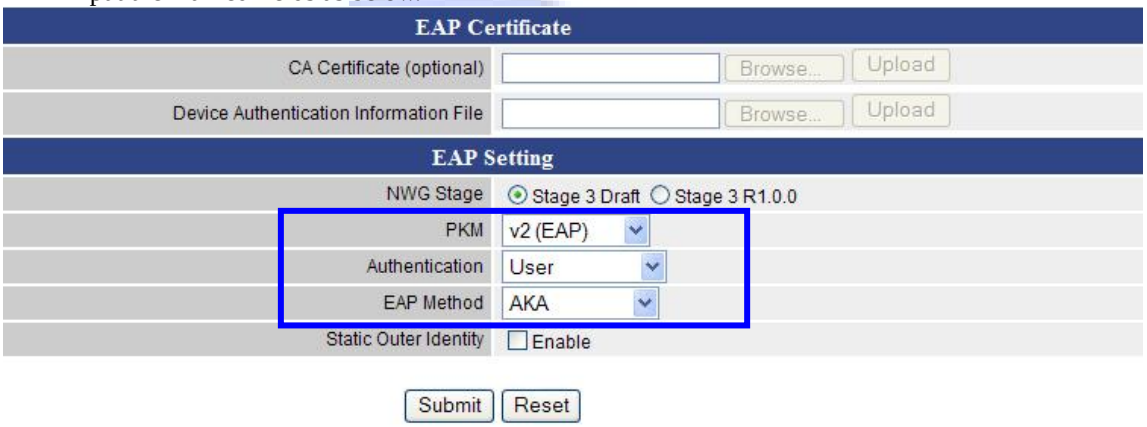


- Type2: V2(EAP) with "User" authentication
  In this type, there are two methods to communicate authentication information with BS.

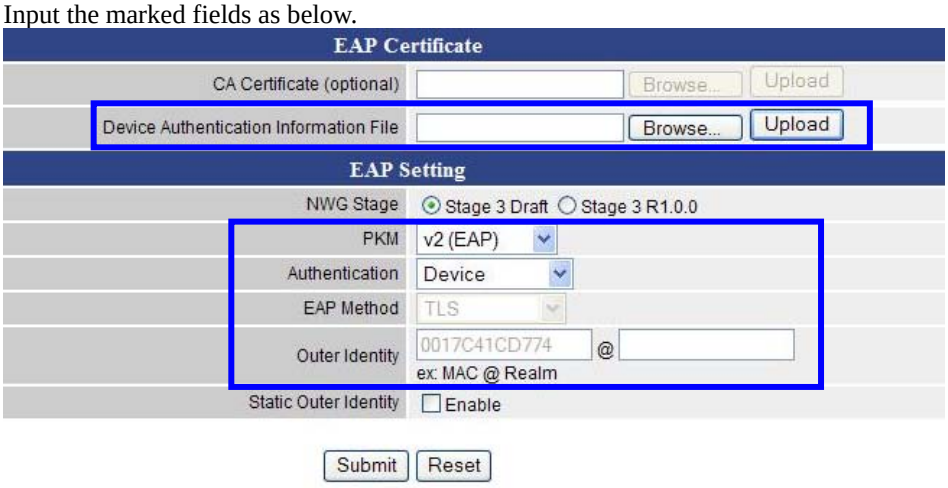
  - TTLS (Technical Translation & Localization Services) Method
    Input the marked fields as below.



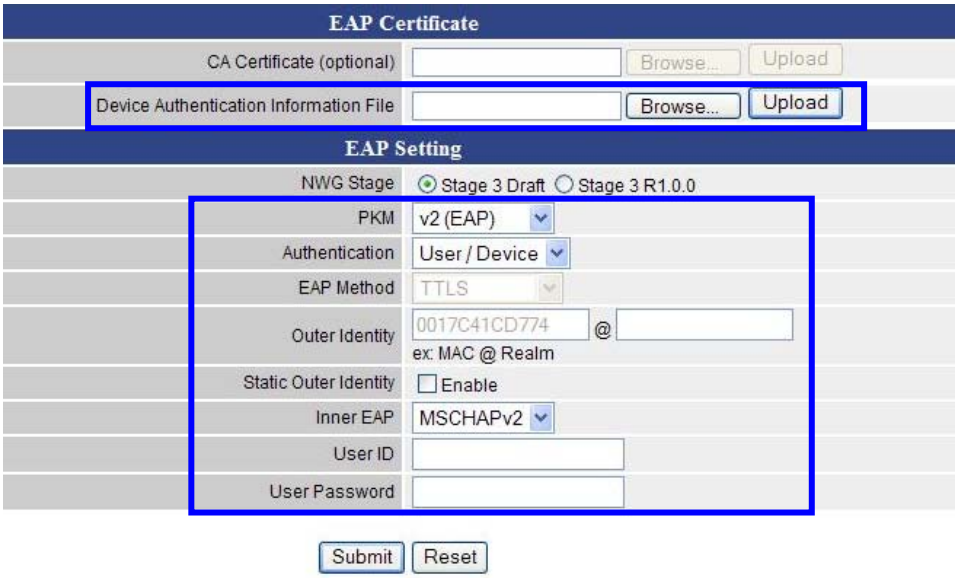
■ AKA (Authentication and Key Agreement) Method
Input the marked fields as below.



➢ Type3: V2(EAP) with “Device” authentication
Input the marked fields as below.



➢ Type4: V2(EAP) with “User / Device” authentication
Input the marked fields as below.

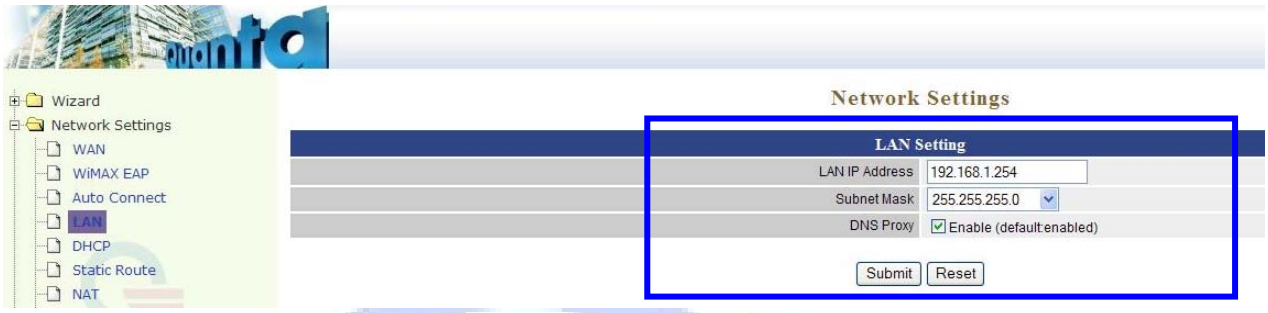

EAP Certificate
CA Certificate (optional)
Browse...
Upload
Device Authentication Information File
Browse...
Upload
EAP Setting
NWG Stage
Stage 3 Draft
Stage 3 R1.0.0
PKM
v2 (EAP)
Authentication
User / Device
EAP Method
TTLS
Outer Identity
0017C41CD774
@
ex: MAC @ Realm
Static Outer Identity
Enable
Inner EAP
MSCHAPv2
User ID
User Password
Submit
Reset

3.4 LAN Setting

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 192.168.1.254 with a subnet mask of 255.255.255.0.

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

- LAN IP Address: Assign the IP address of LAN server, default is 192.168.1.254
- Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0.



Field	Description	Default value
LAN IP Address	Input the LAN IP address	192.168.1.254
Subnet Mask	Select the subnet mask	255.255.255.0
DNS Proxy	Enable / Disable the DNS proxy function	Enable

3.4.1 DNS Proxy

A proxy server is a computer network service that allows clients to make indirect network connections to other network services. The default setting is Enable the DNS proxy server.

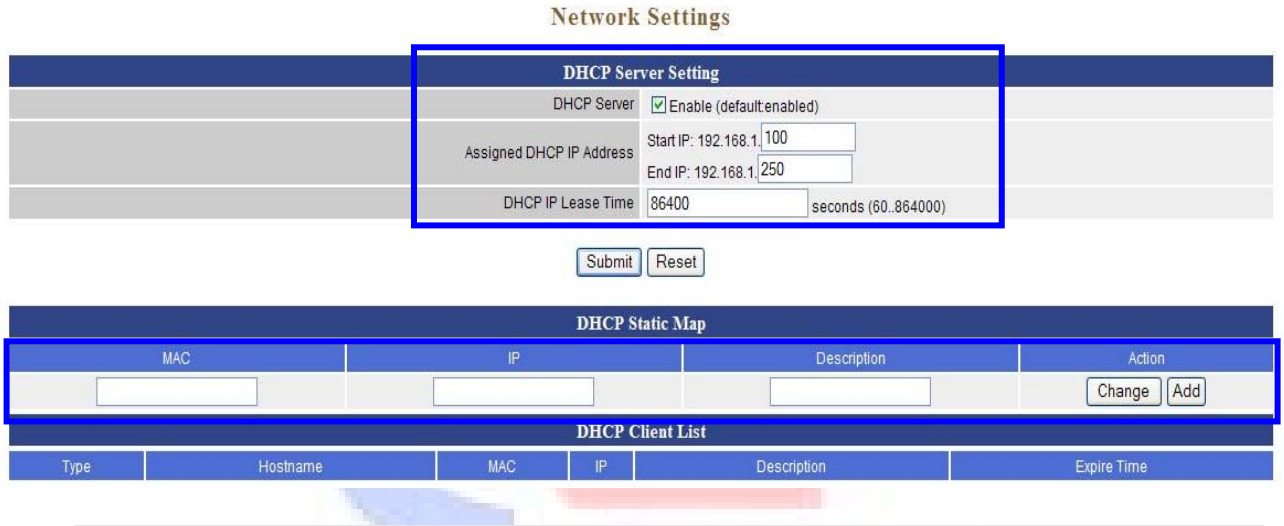
Enable the DNS Proxy which will relay users'/clients' DNS requests to a real DNS server IP address. Users no need to specify real DNS server IP address.

3.5 DHCP

3.5.1 DHCP Server

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is starting up and request an IP address to be logged on to the network. The device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled in the unit. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP client computers connected to the unit will have their information displayed in the DHCP Client List table. The table will show the Type, Host Name, IP Address, MAC Address, Description, and Expired Time of the DHCP lease for each client computer.

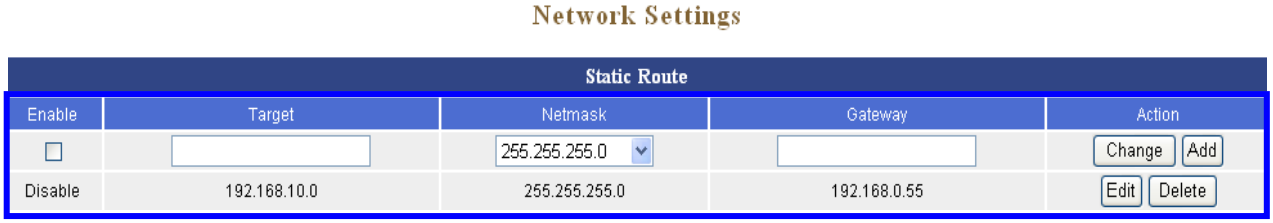


Field	Description	Default value
DHCP Server	Enable or Disable the DHCP server to dynamic release IP to the connected client in LAN.	Enable
Assigned DHCP IP Address	Enter the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.	Start IP: 192.168.1.100 End IP: 192.168.1.250
DHCP IP Lease Time	Assign the length of time for the IP lease, default setting is 86400 seconds.	86400
MAC	Input the MAC address of the client which you want to add.	
IP	Input the IP address of the client which you want to add.	
Description	Input the description of the client which you want to add.	
Change	Click "Change" button to change the data for existed map.	
Add	Click "Add" button to add the DHCP static mapping data.	

3.6 Static Route

Static routes are special routes that the network administrator manually enters into the router configuration. You could build an entire network based on static routes. The problem with doing this is that when a network failure occurs, the static route will not change without you performing the change. This isn't a good thing if the failure occurs during the middle of the night, or while you are on vacation.

The routing table allows the user to configure and define all the static routes supported by the router.



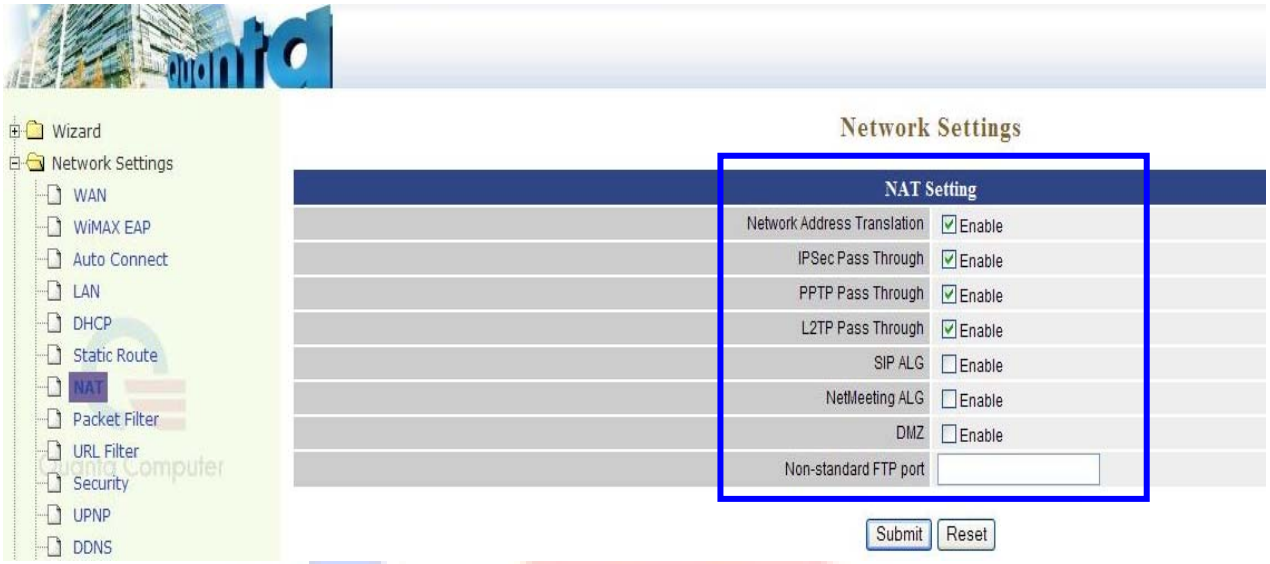
Field	Description	Default value
Enable	Enable/Disable the static route.	Disable
Target	Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route.	
Netmask	The subnet mask that will be AND'd with the destination IP address and then compared with the Target to see if this is the target route.	255.255.255.0
Gateway	The IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP address of the router Action – Insert a new Static Route entry or update a specified entry	
Change	Click "Change" button to modify one of the list routes and to change the value.	
Add	Click "Add" button to add more routes for different target domain	
Edit	Click "Edit" button to edit the route date.	
Delete	Click "Delete" button to delete the unneeded routes.	

3.7 NAT

NAT (Network Address Translation) serves three purposes:

1. Provides security by hiding internal IP addresses. Acts like firewall.
2. Enables a company to access internal IP addresses. Internal IP addresses that are only available within the company will not conflict with public IP.
3. Allows a company to combine multiple ISDN connections into a single internet connection.

3.7.1 NAT Setting



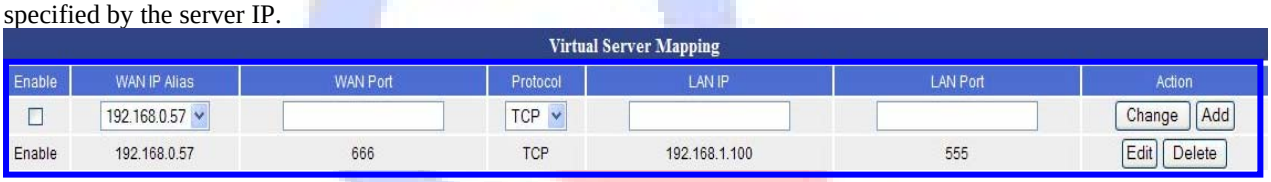
Field	Description	Default value
Network Address Translation	Enable/Disable NAT.	Enable
IPSec Pass Through	IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Enable/Disable this framework verification	Enable
PPTP Pass Through	PPTP (Point-to-Point Tunneling Protocol) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Enable/Disable this protocol verification.	Enable
L2TP Pass Through	L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. Enable/Disable this function.	Enable
SIP ALG	SIP (Session Initiation Protocol) is a signaling protocol	Disable

	for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.	
NetMeeting ALG	Enable or disable to support or not support NetMeeting packets.	Disable
DMZ	In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.	Disable
Non-Standard FTP port		Disable

3.7.2 Virtual Server Mapping

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network. You will only need to input the LAN IP address of the computer running the service and enable it.

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP.

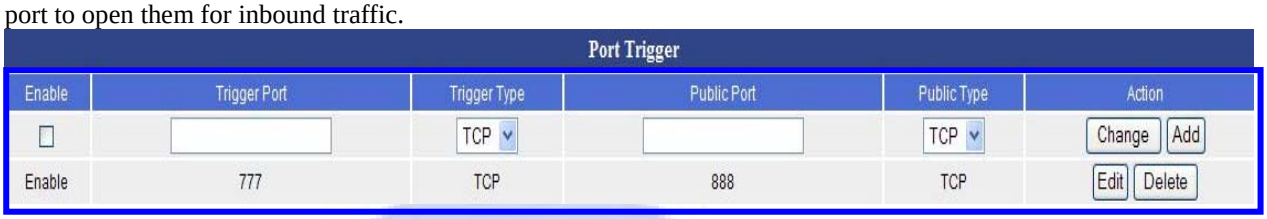


Field	Description	Default value
Enable	Enable/Disable the virtual server mapping, default setting is Disable	Disable
WAN IP Alias	Select which WAN IP address to mapping local IP address.	
WAN Port	The port number on the WAN side that will be used to access the virtual service. Enter the WAN Port number, e.g. enter 80 to represent the Web (http server), or enter 25 to represent SMTP (email server). Note: You can specify maximum 32 WAN Ports.	
Protocol	The protocol used for the virtual service. Select a protocol type is TCP or UDP.	TCP
LAN IP	The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.	
LAN Port	The port number of the service used by the Private IP computer. Enter the LAN port number.	
Change	Click change button to modify an existed mapping item.	

Add	Click add button to add a new mapping server.
Edit	Click edit button to edit the existed item.
Delete	Click delete button to delete the unneeded item.

3.7.3 Port Trigger

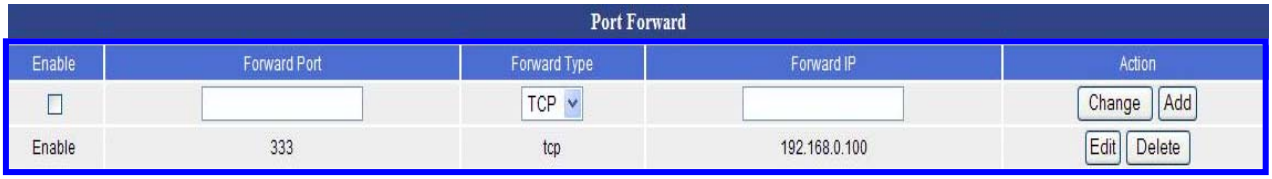
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol), then enter the public ports associated with the trigger port to open them for inbound traffic.



Field	Description	Default value
Enable	Enable/Disable the port trigger, default setting is disabled.	Disable
Trigger Port	This is the port used to trigger the application. It can be either a single port or a range of ports.	
Trigger Type	This is the protocol used to trigger the special application.	TCP
Public Port	This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.	
Public Type	This is the protocol used for the special application.	TCP
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

3.7.4 Port Forward

Port forwarding is the act of forwarding a network port from one network node to another. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside via a NAT-enabled router. Port forwarding allows remote computers (e.g. public machines on the Internet) to connect to a specific computer within a private LAN. The forwarding protocol type can be set in TCP or UDP protocol.



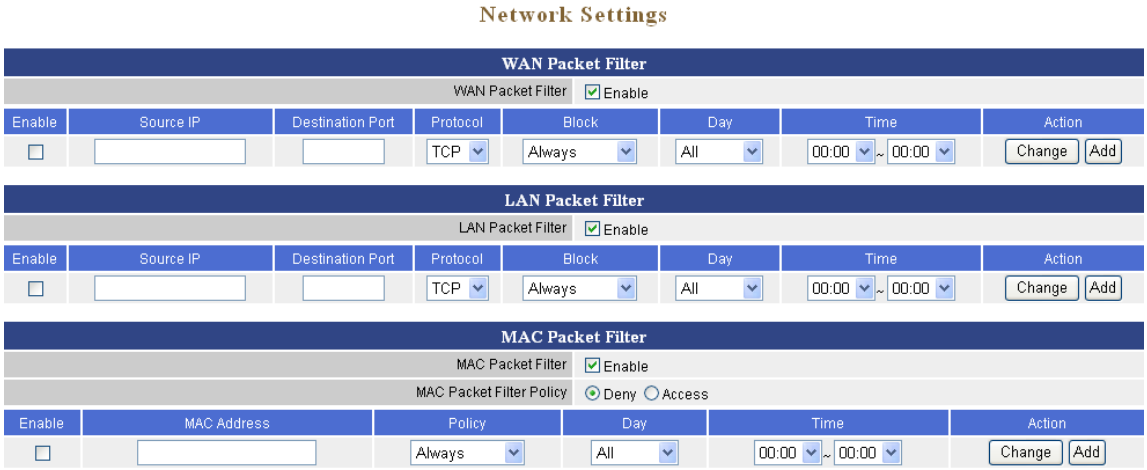
Field	Description	Default value
Enable	Enable/Disable the port Forward, default setting is disabled .	Disable
Forward Port	This is the port used to forward the packets to a port on a private IP address in LAN. It can be either a single port or a range of ports.	
Forward Type	This is the protocol used to trigger the special application.	TCP
Forward IP	The IP address in LAN that you want to forward the packets to it	
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

3.8 Packet Filter

Filters are used to deny or allow LAN computers from accessing the Internet. Within the local area network, the unit can be setup to deny Internet access to computers using the assigned IP or MAC addresses. The unit can also block users from accessing restricted web sites.

This packet filter is used to inspect each packet for user defined content, such as an IP address but does not track the state of sessions.

It is a feature incorporated into routers and bridges to limit the flow of information based on predetermined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.



WAN Packet Filter

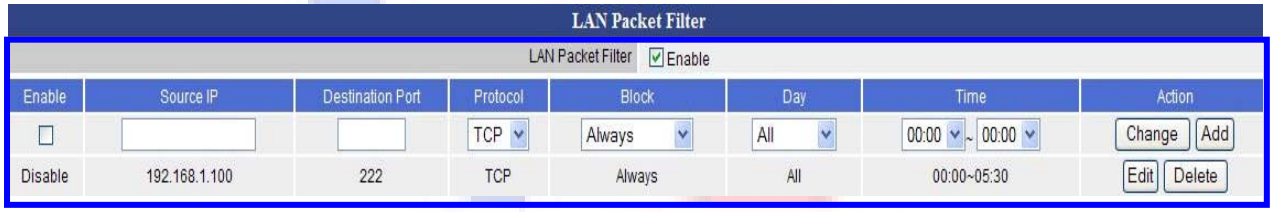
Use IP Filters to deny particular WAN IP addresses from the Internet. You can deny special port number or all ports for a specific IP address. You will need to input the WAN IP address(es) of the computer(s) that will be denied, and input which port of WAN side that you want to deny for accessing..

Field	Description	Default value
WAN Packet Filter	Enable / Disable the packets filter function in WAN port.	Enable
Enable	Enable/Disable the WAN packet filter, default setting is Disable	Disable
Source IP	The IP address of the WAN computer that will be denied access to the Internet. You can also add a range of IP addresses.	
Destination Port	The single port that will be denied to access.	

Protocol	This is the protocol type that will be used with the Port that will be blocked.	TCP
Block	You can block the IP address of the WAN computer always or by schedule	Always
Day	If Block set to “by schedule”, you need to determine which day(s) will be performed	All
Time	If Block set to “by schedule”, you need to determine which time will be performed	00:00 ~ 00:00
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

LAN Packet Filter

Use IP Filters to deny particular LAN IP addresses from accessing the Internet. You can deny special port number for a specific IP address. You will need to input the LAN IP address(es) of the computer(s) that will be denied Internet access, and input which port of LAN side that you want to deny for accessing..

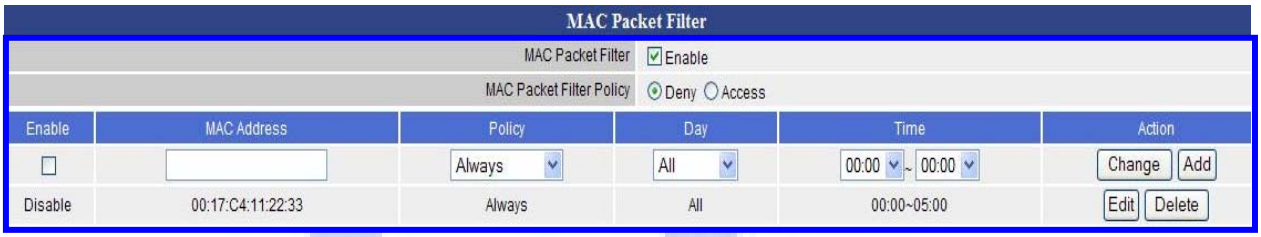


Field	Description	Default value
LAN Packet Filter	Enable / Disable the packets filter function in LAN port.	Enable
Enable	Enable/Disable the LAN packet filter, default setting is Disable	Disable
Source IP	The IP address of the LAN computer that will be denied access to the Internet. You can also add a range of IP addresses.	
Destination Port	The single port that will be denied access to the Internet. If no port is specified, all ports will be denied access.	
Protocol	This is the protocol type that will be used with the Port that will be blocked.	TCP
Block	You can block the IP address of the WAN computer always or by schedule.	Always
Day	If Block set to “by schedule”, you need to determine which	All

	day(s) will be performed.	
Time	If Block set to “by schedule”, you need to determine which time will be performed.	00:00 ~ 00:00
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

MAC – Packet Filter

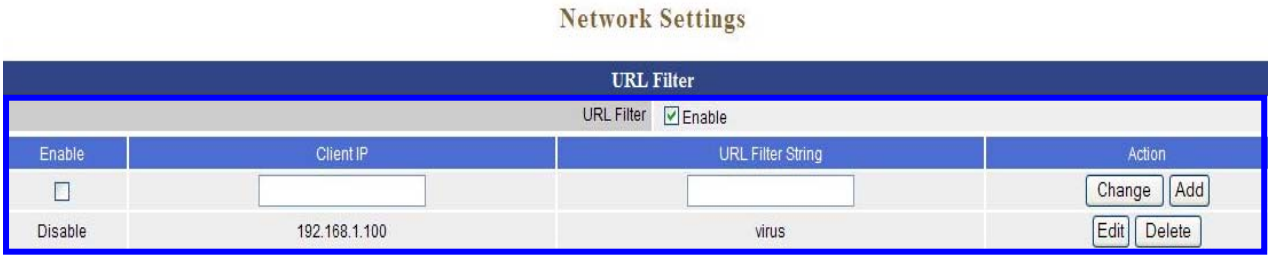
Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the unit.



Field	Description	Default value
MAC Packet Filter	Enable / Disable the packets filter function in LAN port.	Enable
MAC Packet Filter Policy	Two way to determine the policies you want to deny or access.	Deny
Enable	Enable/Disable the MAC packet filter, default setting is disabled.	Disable
MAC Address	The MAC address of the computer in the LAN (Local Area Network) to be used in the MAC filter table. Enter the MAC address of LAN port, e.g. 00:00:27:88:81:18.	
Policy	You can block the MAC address of the LAN computer always or by schedule	Always
Day	If Block set to “by schedule”, you need to determine which day(s) will be performed.	All
Time	If Block set to “by schedule”, you need to determine which time will be performed.	00:00 ~ 00:00
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

3.9 URL Filter

With security reason, the URL Filter provides the enterprise to manage and restrict employee access to non-business or undesirable content on the Internet. URL Filter is a web solution that blocks web-sites access according the URL Filter String no matter the URL string is found full or partial matched with a keyword.
For example, if you add URL Filter String with keyword “sex”, the WV202 will limit local hosts to access the web site or web pages such as “www.sex.com” or “www.fronthost.com/sex/index.html”.



Field	Description	Default value
URL Filter	Enable/Disable the URL Filter, default setting is disabled.	Enable
Enable	Enable/Disable the MAC packet filter, default setting is disabled.	Disable
Client IP	The host computer which will be blocked to access the Internet.	
URL Filter String	The pattern which will be blocked. For example, “yahoo.com” or keyword “sex”.	
Change	Click change button to modify an existed item.	
Add	Click add button to add a new item	
Edit	Click edit button to edit the existed item.	
Delete	Click delete button to delete the unneeded item.	

3.10 Security

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
User can enable the “Intrusion Detection” function in the “Security” page to detect the intrusions and enable the “Drop Malicious Packet” function to drop the malicious packets.

Field	Description	Default value
Intrusion Detection	Enable/Disable the intrusion detection.	Disable
Drop Malicious Packet	Enable/Disable the drop malicious packet.	Disable

3.11 UPnP

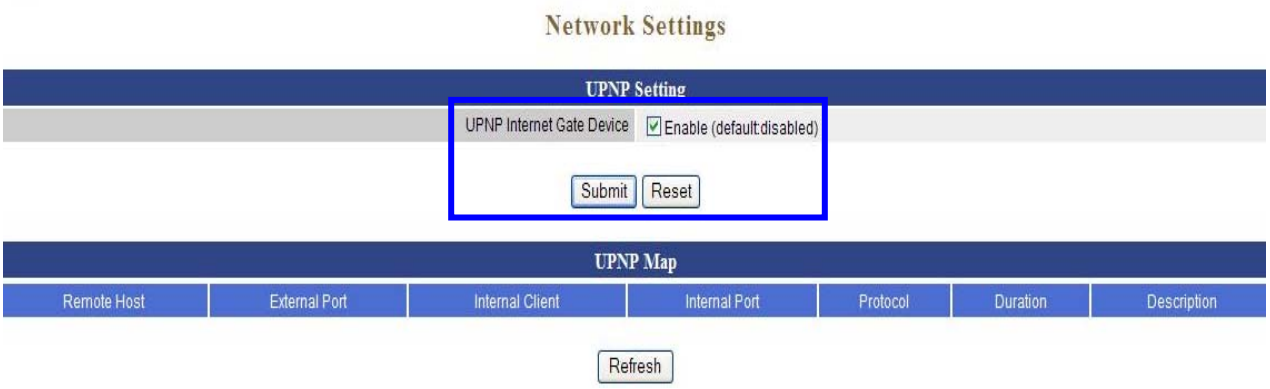
UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The WV202 is an UPnP enabled router and will only work with other UPnP devices/softwares. If you do not want to use the UPnP functionality, it can be disabled by canceling the “Enable” item..

UPnP is architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices to automatically connect with one another and work together to make networking - particularly home networking - possible for more people.

The UPnP Internet Gateway Device (IGD) is an “edge” interconnect device between a residential Local Area Network (LAN) and the Wide Area Network (WAN), providing connective to the Internet.

With UPnP support, the MSN message can communicate over NAT. In other words, the user of the windows Massager behind the firewall/NAT device will be able to connect the peer for voice and video conferencing.

UPnP (Universal Plug-and-Play). Network architecture based on TCP/IP and intended to allow terminals to be networked without the need for configuration. In the Barricade router, for example, the correct ports are automatically opened for applications like Net meeting, online games, etc. You can choose to enable or disable the UPnP Service.



Field	Description	Default value
UPNP Internet Gate Device	Enable/Disable the UPNP function.	Disable

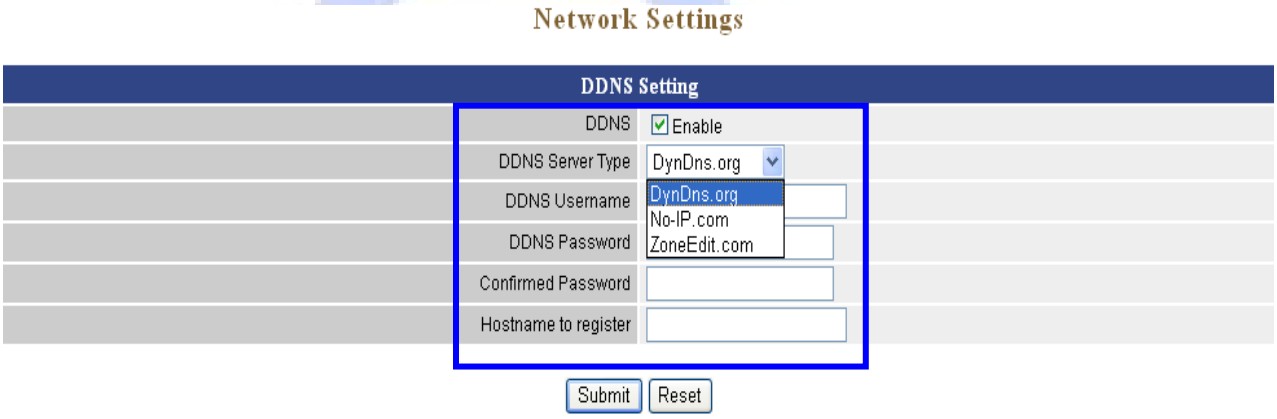
3.12 DDNS

The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet.

Without DDNS, the users should use the WAN IP to reach internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported, you apply a DNS name (e.g., www.xxx.com) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.xxx.com regardless of the WAN IP.

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, you can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname.

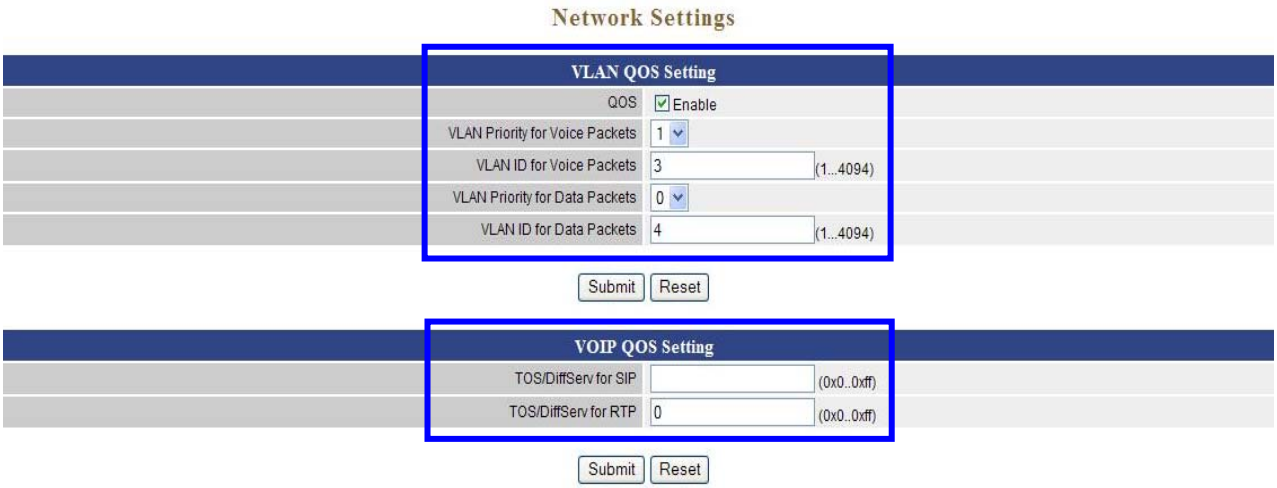
Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.
DDNS is a method of keeping a domain name linked to a changing (dynamic) IP address. If you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the WV202, you can setup your DDNS service and the WV202 will automatically update your DDNS server every time it receives a different IP address.



Field	Description	Default value
DDNS	Enable/Disable the DDNS service, default setting is disabled.	Disable
DDNS Server Type	The WV202 support three types of DDNS, DynDns.org / No-IP.com / ZoneEdit.com.	DynDns.org
DDNS Username	The username which you register in DynDns.org , No-IP.com or ZoneEdit.com website.	
DDNS Password	The password which you register in DynDns.org , No-IP.com or ZoneEdit.com website.	
Confirmed Password	Confirm the password which you typing.	
Hostname to register	The hostname which you register in DynDns.org , No-IP.com or ZoneEdit.com website.	

3.13 QoS

The QOS (Quality Of Service) is to guarantee that the Voice and Data should be transmitting at the same time and data couldn't influence the Voice quality. When TOS bits is enabled, it will guarantee the Voice have the first priority pass through the TOS enable devices.

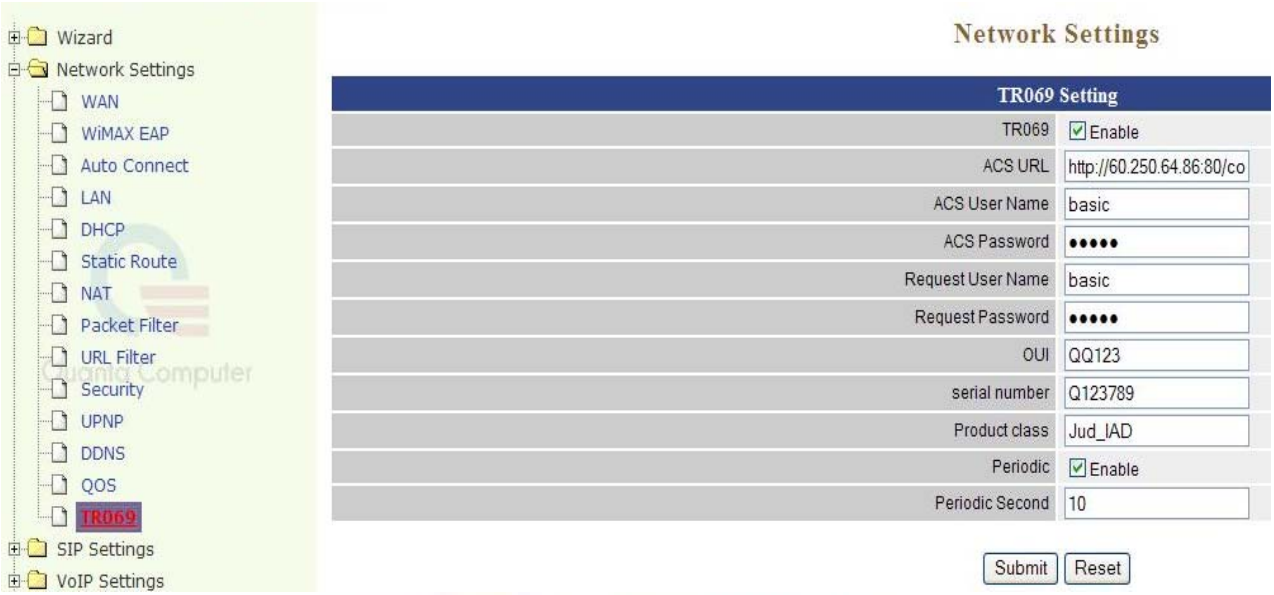


Field	Description	Default value
QOS	Enable/Disable the QOS Service. Default setting is disabled.	Disable
VLAN Priority for Voice Packets	The priority value for voice packet. Default is 1.	1
VLAN ID for Voice Packets	The voice VLAN ID. Default is 3.	3
VLAN Priority for Data Packets	The priority value for data packet. Default is 0.	0
VLAN ID for Data Packets	The data VLAN ID. Default is 4.	4
TOS / DiffServ for SIP	This option enables the phone to support QOS for SIP traffic in a network. This makes sense only if all parts of the involved network also support QOS. Assign the priority value from 0 to 255. Default is 0.	
TOS / DiffServ for RIP	This option enables the phone to support QOS for RTP traffic in a network. This makes sense only if all parts of the involved network also support QOS. Assign the priority value from 0 to 255. Default is 0.	0

3.14 TR069

The TR069 is the CPE WAN Management Protocol, intended for communication between a CPE and Auto-Configuration Server (ACS). ACS can remote manage the CPE and modify the settings via TR069 protocol. The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

When you enable the TR069 function and want to manage this IAD, please make sure the connection is worked between IAD and ACS. The IAD will send the request packets to ACS and ACS will feedback the request packets from IAD.



Field	Description	Default value
TR069	Enable / Disable the TR069 function	Disable
ACS URL	The URL of ACS (Auto Configuration Server) for connecting. Depending on different security mechanism, the URL will be different, like as with SSL security or not.	
ACS User Name	The user name is provided by ACS for IAD to connect	
ACS Password	The password is provided by ACS for IAD to connect	
Request User Name	When user wants to mount device to the system, user must send a connection request to the device including the username and password. The user name and password are also used when user notify the device	

Request Password	When user wants to mount device to the system, user must send a connection request to the device including the username and password. The user name and password are also used when user notify the device	
OUI	An Organizationally Unique Identifier (OUI) is a unique identifier value for different organization. This settings is not the needed item for connecting between CPE and ACS, it's depending on the connecting requirement of ACS.	
Serial number	The unique serial number of this device is used to connect to ACS.	
Product Class	The product class is the description of this product.	
Periodic	To enable or disable the periodic function that CPE will auto send connection request to ACS periodic.	Disable
Periodic Second	It's the time to send the connection request periodic to ACS	

4. SIP Settings

SIP (Session Initiation Protocol) is a request-response protocol, dealing with requests from clients and responses from servers. Participants are identified by *SIP URLs*. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

- Basic Setting
- Account Setting
- Server Setting
- NAT Traversal

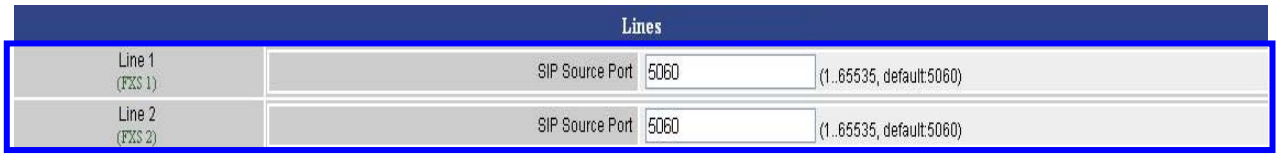
4.1 Basic Setting

SIP Settings

Basic Setting		
Session Timer Flag	☐ Enable (default: disabled)	
Session Timer	1800	seconds (90..65535, default:1800)
Media Port Start	5000	(1024-65535, default:5000)
Media Port End	5009	(1024-65535, default:5009)
Transport	◉ UDP (default) ○ TCP	
SIP Time Interval	500	(100-1000, default:500)
Timeout for Invite	12	(1-100, default:12)
Timeout for Ring Back	180	(1-300, default:180)
Timeout for Release	4	(1-10, default:4)
Registration Retry Count	65535	(1-65535, default:65535)
Registration Retry Interval	30	(1-65535, default:30)
PING Interval	0	(0-65535, default:0)
PRACK Flag	☐ Enable (default:disabled)	
SIP User Agent Name	VOIP_Agent_001	

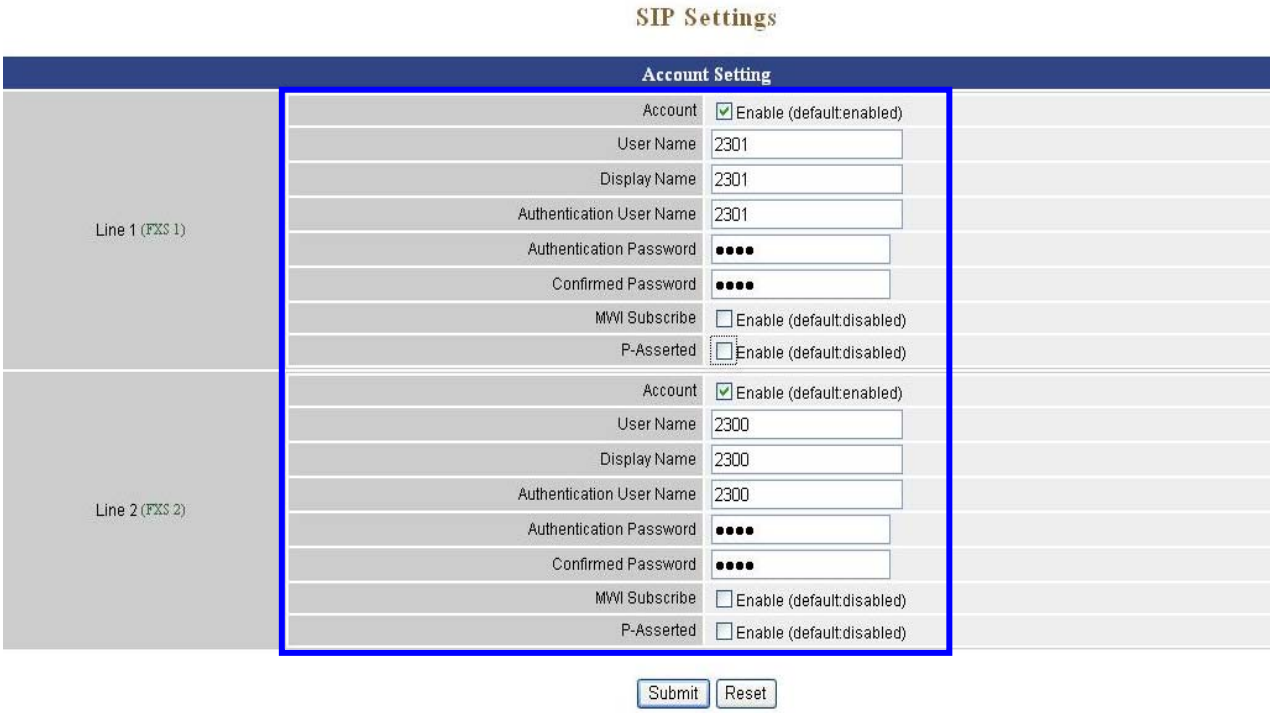
Field	Description	Default value
Session Timer Flag	Disable / Enable the session timer to refresh Sip sessions. Default setting is disabled.	Disable
Session Timer	SIP session refresh time interval. The time interval in which the phone periodically refresh SIP sessions by sending repeated INVITE or Update request, depending on session type. Its range is 90 to 65535, default setting is 1800 seconds.	1800

Media Port Start	The starting range of port for RTP. Port number for initial of sending RTP packet. Its range is 1024 to 65535, default setting is 5000.	5000
Media Port End	The ending range of port for RTP. Its range is 1024 to 65535, default setting is 5009	5009
Transport	Assigns the default SIP transport protocol. UDP – UDP (User Datagram Protocol) provides very few error recovery services, offering instead a direct way to send and receive datagram over an IP network. It's used primarily for broadcasting messages over a network. Here the UDP is a default setting. TCP (Transmission Control Protocol) guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.	UDP
SIP Time Interval	SIP time interval in milliseconds. The default setting is 500 msec.	500
Timeout for Invite	INVITE message timeout value. Assigns a value 1 to 100, default setting is 12 seconds. It denotes if an INVITE request was sent, and a response is not received from the remote site within the allotted time (the value of Invite Timeout). The present request will be dropped and a new connection request will be initiated.	12
Timeout for Ring Back	Timeout value for dropping a call after receiving 180 responses. Ring back is an intermittent audio tone that a caller in a telephone system hears after dialing a number, when the distant end of the circuit is receiving a ringing signal. It can be generated by the servicing switch of either the called party or the calling party. It is not generated by the called instrument. The default setting is 180 seconds.	180
Timeout for Release	BYE message timeout value. Assigns a time interval 1 to 10, default setting is 4 seconds.	4
Registration Retry Count	When the SIP registration is failed, it will retries to registry again after the Registration Retry Interval time. You can set how many times to retry SIP registration. The default setting is the maximum number ‘65535’.	65535
Registration Retry Interval	The interval time to retry SIP registration. The default setting is 30 seconds.	30
Ping Interval	It is the interval time to execute ping the SIP server.	0
PRACK Flag	Indicates if INVITE messages sent on the specified trunk group require reliable provisional responses. This is used to deliver provisional responses (like alerting) reliably and is useful for SIP trunks. The default setting is disabled.	Disable
SIP User Agent Name	The name of the SIP User Agent.	VOIP_Agent_001



Field	Description	Default value
SIP Source Port	Assign the SIP port number of terminal adapter. Its range is 1 to 65535, default setting is 5060.	5060

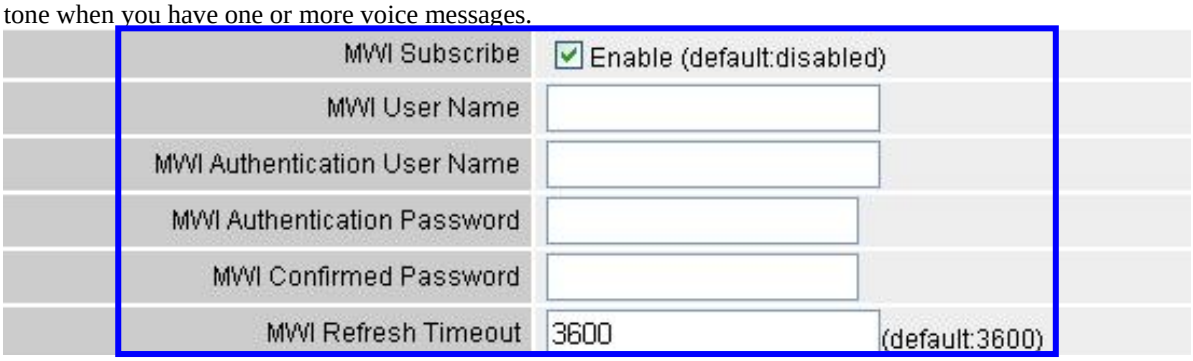
4.2 Account Setting



There are two ports can be setup for SIP account.

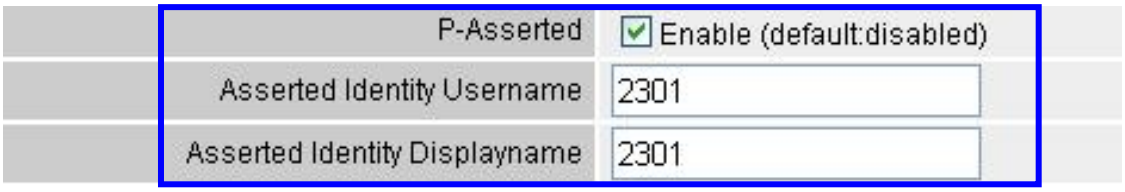
Field	Description	Default value (Line1 / Line2)
Account	To disable / enable the account settings. The default value is disabled.	Enable / Enable
User Name	The user name Provided from your ISP.	2301 / 2300
Display Name	This text message will be sent between the callee and caller and will show on LCD panel for general using.	2301 / 2300
Authentication User Name	User name for authentication. Maximum 36 characters.	2301 / 2300
Authentication Password	User password for authentication. Maximum 24 characters.	2301 / 2300
Confirmed Password	Enter the password again, this is used to confirm user password for authentication. Maximum 24 characters.	2301 /2300
MWI Subscribe	Message Waiting Indication (MWI) To disable / enable the function for the VoIP phone to ask for MWI (Message Waiting Indication) periodically.	Disable / Disable
P-Asserted	To disable / enable the P-Asserted function, the default setting is disabled.	Disable / Disable

Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have one or more voice messages.



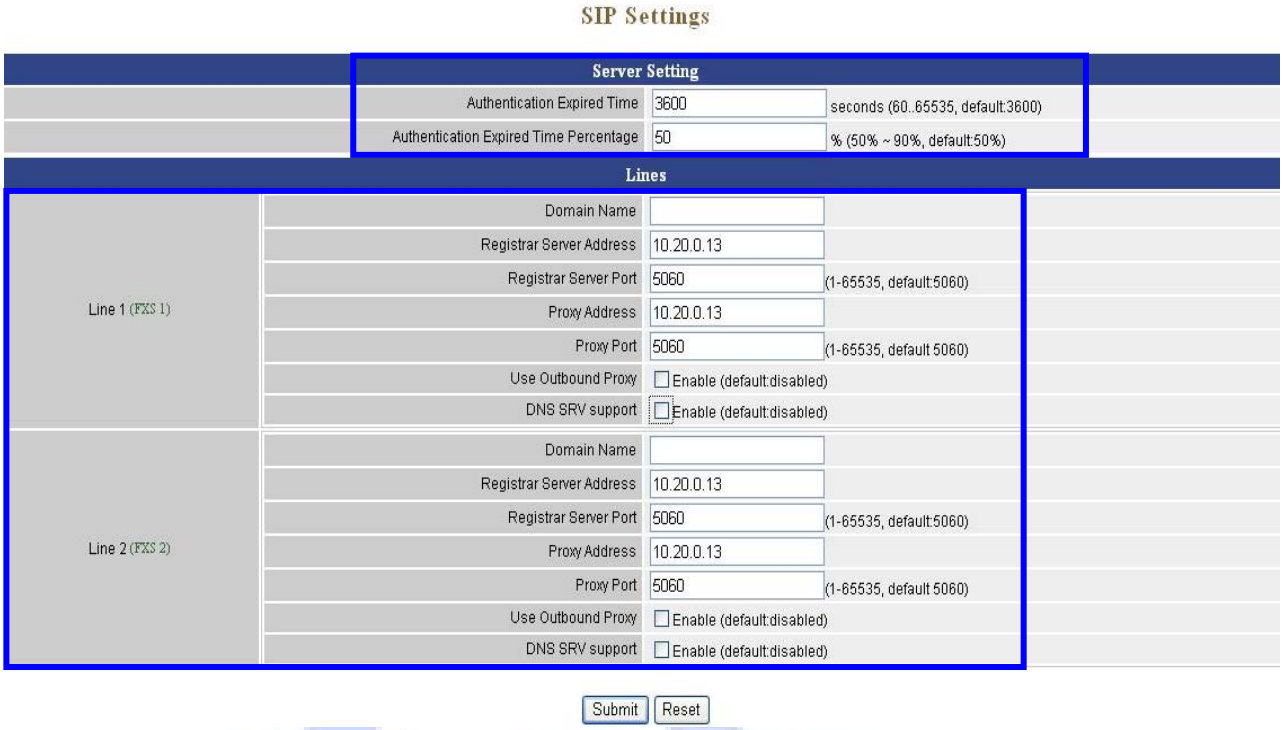
Field	Description	Default value (Line1 / Line2)
MWI Subscribe	Message Waiting Indication (MWI) To disable / enable the function for the VoIP phone to ask for MWI (Message Waiting Indication) periodically.	Disable / Disable
MWI User Name	The username for MWI.	
MWI Authentication User Name	User name for authentication. Maximum 36 characters	
MWI Authentication Password	User password for authentication. Maximum 24 characters.	
MWI Confirmed Password	Enter the password again, this is used to confirm user password for authentication. Maximum 24 characters.	
MWI Refresh Timeout	The time to refresh MWI, it will stops to refresh MWI when the message-waiting time is over this time setting. The default setting is 3600 seconds.	3600 / 3600

P-asserted header is used when you want to send some extra number other than calling, called. Assume the SIP Invite request is with numbers, and the Call agent wants to out pulse charge number. It does that in the P-asserted header. The P-Asserted-Identity header is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.



Field	Description	Default value (Line1 / Line2)
P-Asserted	To disable / enable the P-Asserted function, the default setting is disabled.	Disable / Disable
Asserted Identity Username	The name of asserted identity.	2301 / 2300
Asserted Identity Displayname	This text message will be sent between the callee and caller and will show on LCD panel for general using.	2301 / 2300

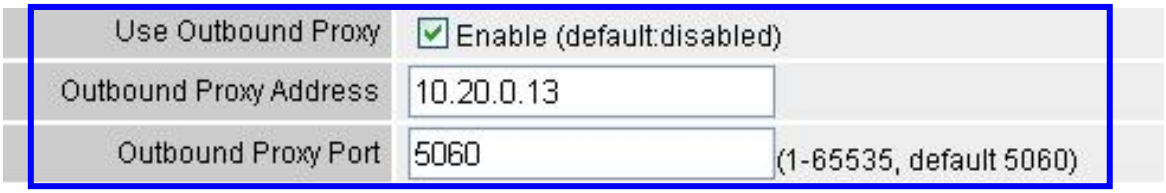
4.3 Server Setting



Field	Description	Default value
Authentication Expired Time	SIP registration expired time. Assigns the time interval from 60 – 65535, default setting is 3600 seconds.	3600
Authentication Expired Time Percentage	Before the expired time is timeout, IAD need to send a re-register packet to SIP server for keeping the connection. To set how many percentage of the expired time to send the register packets.	50

Field	Description	Default value (Line1 / Line2)
Domain Name	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.	
Registrar Server Address	Assigns the SIP Register Server's IP address.	10.20.0.13 / 10.20.0.13
Registrar Server Port	Port number of SIP Register Server. Assigns a value from 1 to 65535, default setting is 5060.	5060 / 5060
Proxy Address	The IP address of a SIP proxy server receives requests from clients and forwards them to another server.	10.20.0.13 / 10.20.0.13
Proxy Port	Port number of SIP proxy Server. Assigns a value from 1	5060 / 5060

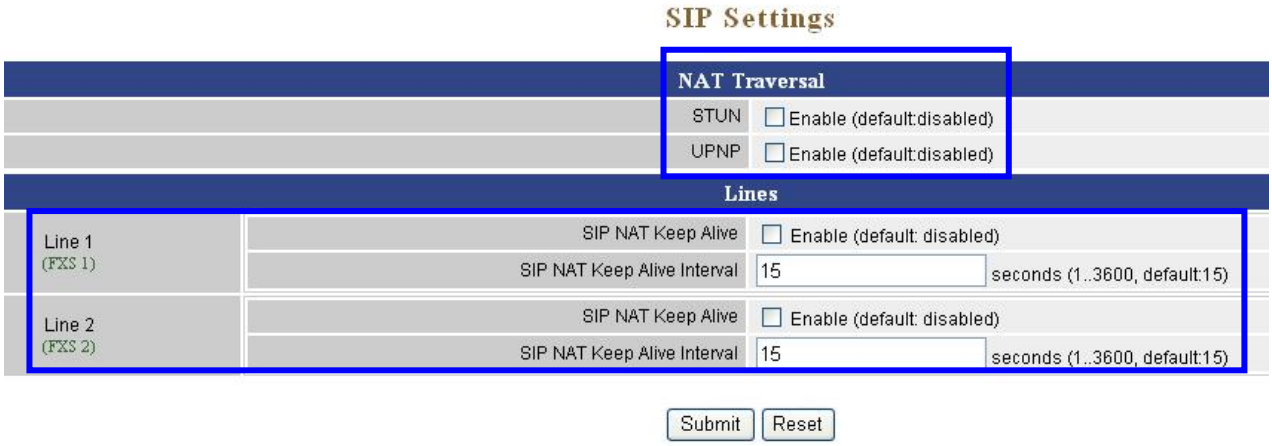
	to 65535, default setting is 5060.	
Use Outbound Proxy	Enable/Disable this flag for out-bound (out-session and in-session) requests. Default setting is disabled.	Disable / disable
DNS SRV Support	To disable / enable the DNS SRV lookups for the SIP proxy server.	Disable / Disable



Field	Description	Default value (Line1 / Line2)
Use Outbound Proxy	Enable/Disable this flag for out-bound (out-session and in-session) requests. Default setting is disabled.	Disable / Disable
Outbound Proxy Address	Outbound Proxy server's IP address. Assigns the server's IP which is in charge of call-out service.	10.20.0.13 / 10.20.0.13
Outbound Proxy Port	Port number of Outbound Proxy Server. Assigns a number from 1 to 65535, default setting is 5060.	5060 / 5060

4.4 NAT Traversal

VoIP NAT Traversal is a technology allowing IP phones or gateways capable of making and receiving calls behind NAT router. In brief, if your IP phone or gateway is using private IP and you want to talk with users over Internet WV202 supports two ways to handle this issue:
(1) Implement STUN (Simple Traversal of UDP through NATs) to learn the IP address of NAT WAN port and then automatically fake WAN address on SIP and RTP on IP phone or gateway
(2) UPnP between NAT router and IP phone



Field	Description	Default value
STUN	Enable/Disable STUN function. Default setting is disabled.	Disable
UPNP	Enable/Disable STUN function. Default setting is disabled.	Disable

Field	Description	Default value (Line1 / Line2)
SIP NAT Keep Alive	Enable/Disable NAT Keep Alive function. If enable NAT traversal function, the SIP client will sends the NAT keep alive packets. Default setting is disabled.	Disable / Disable
SIP NAT Keep Alive Interval	The interval time to send the NAT keep alive packets. Assigns a value from 1 to 3600, default setting is 15 seconds.	15 / 15

Field	Description	Default value
STUN	Enable/Disable STUN function. Default setting is disabled.	Disable
STUN Server Address	The IP address of STUN server. The STUN server allows clients to find out their public address, the type of NAT they are behind and the internet side port associated by the NAT with a particular local port	0.0.0.0

5. VoIP Settings

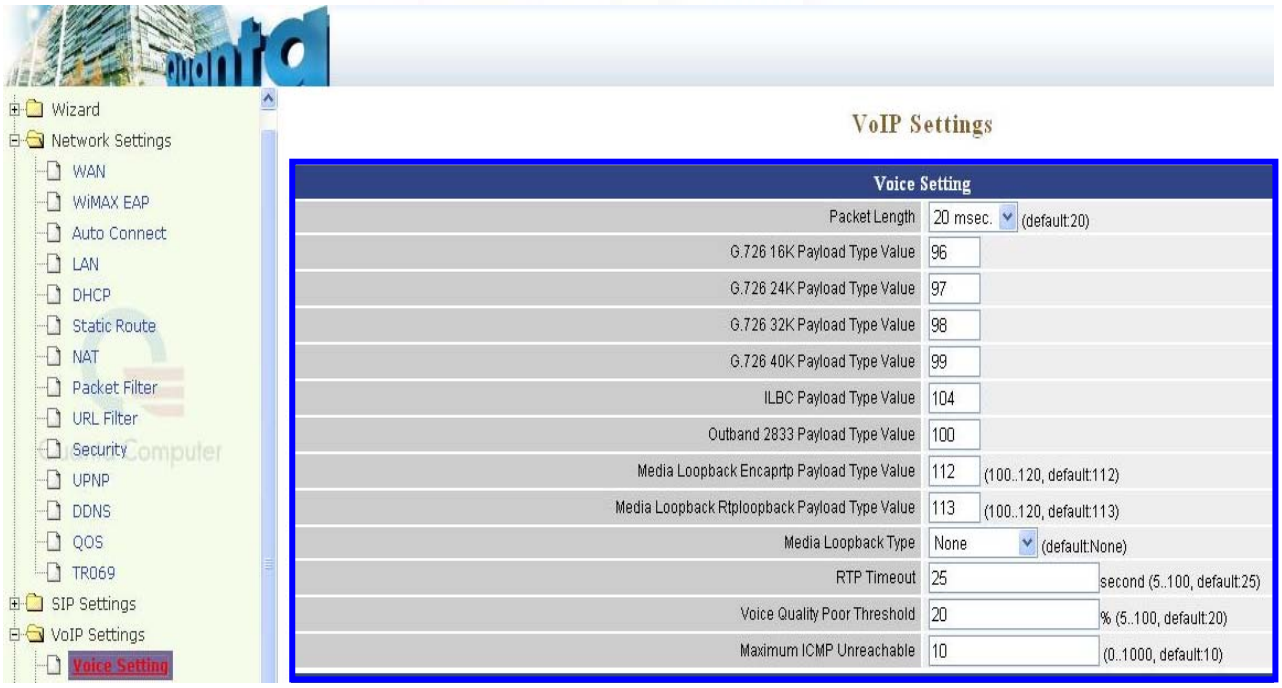
The VoIP setting contains the following items:

- Voice Setting
- Tone Setting
- Call Service
- FXS Port
- FAX Setting
- General Dialing
- Phone Book
- Call Screen

5.1 Voice Setting

The parameters in “Voice Setting” will be worked in all FXS port (FXS1 and FXS2), like as the payload type value in different codec and RTP settings. And some parameters can be set to different values in line1 (FXS1) and line2 (FXS2), like as setting different priority of different codec, DTMF settings, and Tx/Rx gain value in all lines (Line1 and Line2).

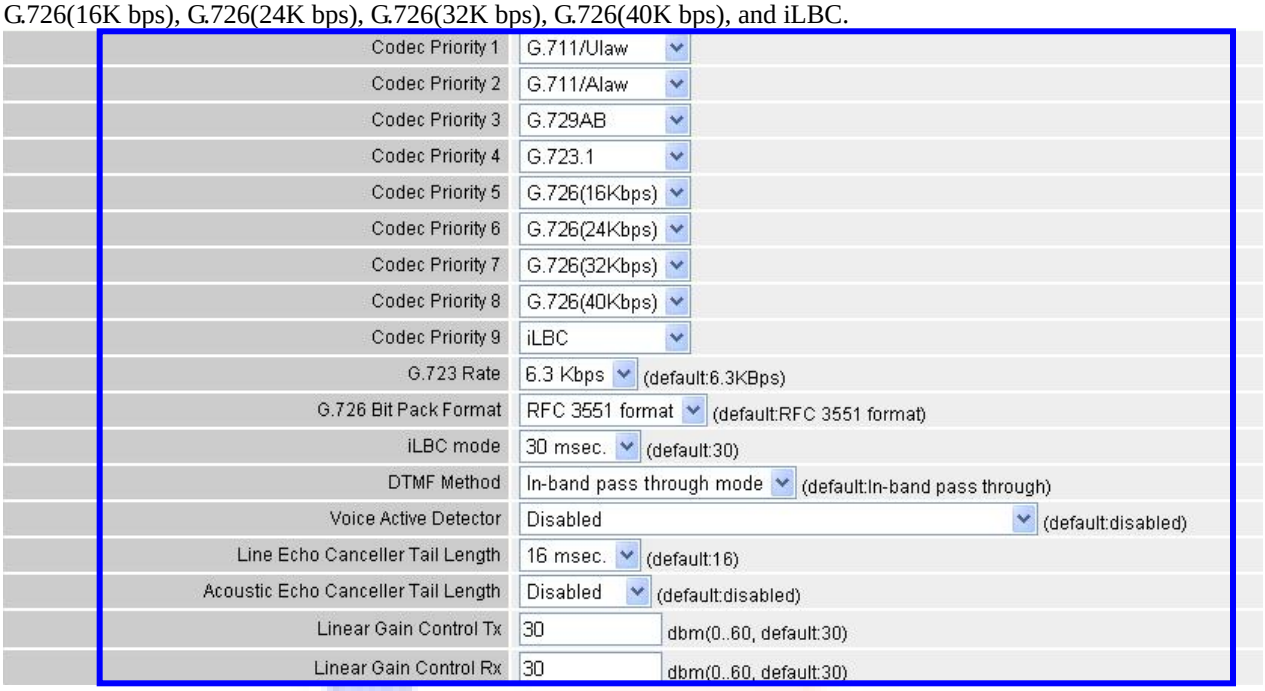
RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.



Field	Description	Default value
Packet Length	The timing to send packets. Default setting is 20 msec.	20 msec
G.726 16K Payload Type Value	Define the payload type value in RTP packets for codec G.726 16K.	96
G.726 24K Payload Type Value	Define the payload type value in RTP packets for codec G.726 24K.	97
G.726 32K Payload Type Value	Define the payload type value in RTP packets for codec G.726 32K.	98
G.726 40K Payload Type Value	Define the payload type value in RTP packets for codec G.726 40K.	99
ILBC Payload Type Vlaue	Define the payload type value in RTP packets for ILBC Payload Type Value.	104
Outband 2833 Payload Type Value	Define the payload type value in RTP packets for Outband 2833 Payload Type Value.	100
Media Loopback Encaprtp Payload Type Value	Define the payload type value in RTP packets for Media Loopback Encaprtp Payload Type Value. Assigns a value from 100 to 120, default setting is 112.	112
Media Loopback Rtploopback Payload Type Value	Define the payload type value in RTP packets for Media Loopback Rtploopback Payload Type Value. Assigns a value from 100 to 120, default setting is 113.	113
Media Loopback Type	There are 3 loopback types for the media transfer. (1) Media - This loopback is activated as close as possible to the analog interface and after the decoder so that the RTP packets are subsequently re-encoded prior to transmission back to the sender. (2) Encaprtp –Each received packet MUST be encapsulated in a different packet (3) Rtploopback- In this mode, the RTP packets are looped back to the sender at a point before the encoder/decoder function in the receive direction to a point after the encoder/decoder function in the send direction.	None
RTP Timeout	The timeout value setting for RTP packets to wait the response.	25
Voice Quality Poor Threshold	The measurement for the voice quality. If the voice packets lost over this value, the call will be drop. Assigns a value from 5% to 100%, default setting is 20%.	20
Maximum ICMP Unreachable	Allowable the maximum number of consecutive ICMP destination unreachable responses. ICMP differs in purpose from TCP and UDP in that it is usually not used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host. Assigns a number from 10 to 100, default setting is 10. The count of unreachable ICMP packets. If the value is over this maximum value, the call will be drop.	10

5.1.1 Codec

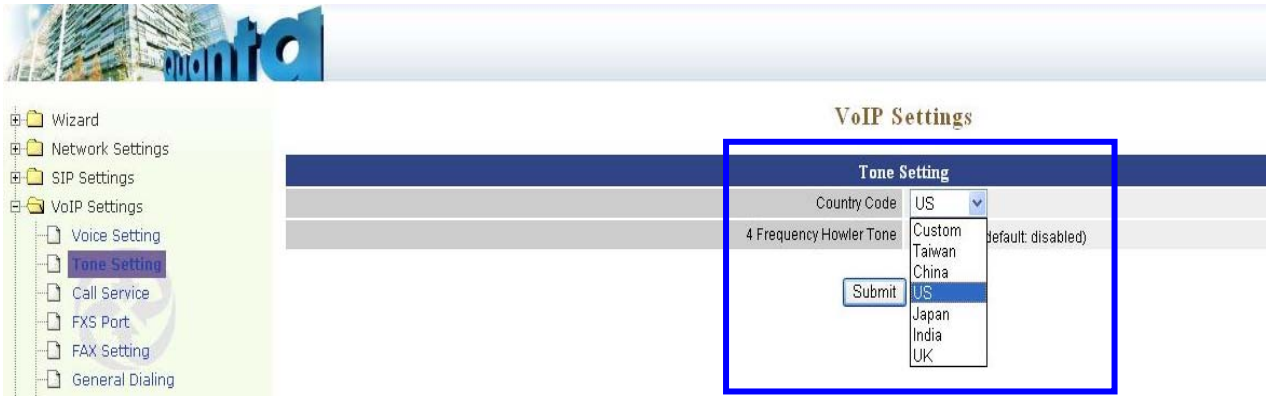
A CODEC (COmpressor/DECompressor) is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 9 kinds of codec, G.711/Ulaw, G.711/Alaw, G.729, G.723, G.726(16K bps), G.726(24K bps), G.726(32K bps), G.726(40K bps), and iLBC.



Field	Description	Default value Line1 / Line2
Codec Priority 1	The priority 1 of codec algorithm to compress the voice signal into data packets.	G.711/Ulaw / G.711/Ulaw
Codec Priority 2	The priority 2 of codec algorithm to compress the voice signal into data packets.	G.711/Alaw / G.711/Alaw
Codec Priority 3	The priority 3 of codec algorithm to compress the voice signal into data packets.	G.729AB / G.729AB
Codec Priority 4	The priority 4 of codec algorithm to compress the voice signal into data packets.	G.723.1 / G.723.1
Codec Priority 5	The priority 5 of codec algorithm to compress the voice signal into data packets.	G.726(16Kbps) / G.726(16Kbps)
Codec Priority 6	The priority 6 of codec algorithm to compress the voice signal into data packets.	G.726(24Kbps) / G.726(24Kbps)
Codec Priority 7	The priority 7 of codec algorithm to compress the voice signal into data packets.	G.726(32Kbps) / G.726(32Kbps)

Codec Priority 8	The priority 8of codec algorithm to compress the voice signal into data packets.	G.726(40Kbps) / G.726(40Kbps)
Codec Priority 9	The priority 9 of codec algorithm to compress the voice signal into data packets.	iLBC / iLBC
G.723 Rate	To select which mode for codec G.723. With the ability to provide data at two-bit rates (5.3 Kbps or 6.3 Kbps), G.723 is able to deliver near toll-quality performance at a low bit rate.	6.3 Kbps / 6.3 Kbps
G.726 Bit Pack Format	To select the packet format for codec G.726.	RFC 3551 format / RFC 3551 format
iLBC mode	RTP Payload length. Select a length from the pull-down menu, default setting is 30 msec.	30 msec. / 30 msec.
DTMF Method	Control how the Device handles the tones that your telephone makes when you push its buttons. You should use the same mode with your VoIP service provider uses. In-band pass through mode - send the DTMF tones in SIP messages In-band PCMU mode - is typically used in North America and Japan In-band PCMA mode - is typically used in Europe Out-bank 2833 relay - send the DTMF tones in RTP packets	In-band pass through mode / In-band pass through mode
Voice Active Detector	Enable/Disable this function. There are three types of silence suppression: 1. Silence Suppression Enabled - NO CNG 2. Silence Suppression Enabled - Only G.711 Annex II type 3. Silence Suppression Enabled - Codec Specific CN.	Disabled / Disabled
Line Echo Canceller Tail Length	Tail length for line echo cancellation.	16 msec. / 16 msec.
Acoustic Echo Canceller Tail Length	Tail length for acoustic echo cancellation.	Disabled / Disabled
Linear Gain Control Tx	Voice gain control for transmitting.	30 dbm / 30 dbm
Linear Gain Control Rx	Voice gain control for receiving.	30 dbm / 30 dbm

5.2 Tone Setting



This IAD supports configuration of pre-configured audible tones based on the geographical location. Adjust the tone frequency according to each country.

Telephony developers working in VoIP, PBXs, VoIP gateways, phones, modems and other PSTN technologies that are developing products internationally have to know the varying international call progress tones that differ from country-to-country. To custom the call progress tones, you should search on a specific call progress tone (e.g. dial tone, busy tone, call waiting tone…etc.) for their frequency, wavelength, period, amplitude, speed, and cadence. Click Tone Setting and select a country from the pull-down menu.

Field	Description	Default value
Country code	Select the country for the tone setting	US
4 Frequency Howler Tone	Howler tone means that a subscriber can hear a high frequency tone to notify subscriber not hanging on well.	Disabled

When you select the country code “Custom”, you can set the detail settings as below for dial tone, busy tone, ringback tone and call waiting tone.