DVG-2030S

Operation Manual

TABLE OF CONTENTS

Note:

- Reprinting and duplicating the portion or all of the contents of this manual is prohibited.
- The specifications and information regarding the products in this manual are subject to change without notice.
- All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference.

Please read this manual carefully before installation

For further safety, there are some symbols in this manual are highlighted with various graphics as below to indicate important information.

Warning Must be followed carefully to avoid bodily injury.

Caution Must be observed to avoid damage to the equipment.

The following symbols explain that if someone handles the product erroneously may cause the harm to the customer or the property.

Prohibit Prohibition item has been shown.

Electricity Represent the possibility of electricity has been shown.

High Temperature Represent the possibility of the injury due to high temperature has been shown.

Ignite Represent the possibility of smoke or igniting has been shown.

When using this product

Warning

- Do not insert objects through the slots. Take care not to spill liquid on this product.
- Place this product on a flat, stable surface that is larger than this product. This product will not operate properly if it is tilted or at an angle.
- Do not touch the power supply with the moist hands.
- Only Use the AC units included with this product.

- Please inspect and clean the AC units every half of one year or one year.
- Do not use a damaged or frayed power cord.
- Use only the type of power source indicated on this product label.
- Unplug the power cord subject to abnormal heat, smoke, sound and smells.
- Do not attempt to service this product yourself. (Disassemble, repair, and modify included).
- Do not block the openings in this product's cabinet.
- Do not place or storage this product in humidity.
- When the product moves to the place subject to rapid changes in temperature, please do not use immediately.
- Please keep the product away from the place where is high temperature.
- Please unplug the power cord during lightning.
- After using this product long period of time, unplug the power cord from the outlet.

When choosing a place for this product

When installing this product, please pay attention to the followings especially. Because of it, this product may cause damaged.

Caution


Prohibit


- The room where this product is operated must maintain a temperature between 0~60° C and the humidity between 5~90 %(non-condensing).
- Do not place this product at the place where always be stepped on the power cord.
- Do not place this product outside.
- Keep it away from direct sunlight and heat sources.
- Please do not place this product in dusty place.
- Avoid places subject to shocks.
- Do not place this product near the liquid, including water or oil.

Characteristics

DVG-2030S equipped IP telephone function, and it is the broadband router.

- Thirty RJ-11 Foreign Exchange Station (FXS) port for IP telephony
- Equipping two 10BASE-T/100BASE-TX Ethernet interfaces with auto detection (crossover/non-crossover).
- The Ethernet link speed of 10Mbps/100Mbps, duplex/half duplex communication methods are recognized automatically.
- Equipping security protect function
- The IP filter and the modification of setting restrict the packet which passes DVG-2030S.
- Because the DHCP server is loaded, network setting of the personal computer can be simplified.
- Configure all kinds of settings through the web browser. (Initial setting for the browser is http://192.168.1.1)
- Software upgrades over the network for new and improved services.

Copyright Statement

1 Preface

1.1 Document Control

Document ID	DVG-2030S
Document Name	
Document Version	V0002=V0.02
Originator	
Approval Date	2005/02/15
Status	Approval
Approver	

1.2 Revision History

Version	Date	Author(s)	Major Changes
V0.01	Nov 02, 2004	Jack Lin	Initial Draft
V0.02	Jan 17, 2005	Jack Lin	Base on v2.02 to modify this manual

1.3 Glossary

List and describe here any and all terms and acronyms used in this document that may be unfamiliar to the audience.

Term	Definition
IAD	Integrate Access Device
DUT	Device Under Test

2 Introduction

The DVG-2030S provides cost-effective, toll-quality telephone voice, modem and fax calls over the packet switching network such as the Internet. The analog telephony information could be packetized and transported over the Internet Protocol (IP), offering reliable transmission via the existing packet switching network.

The excellent flexibility of WAN interface allows connecting with a broadband access media on ADSL/Cable Modem that provide a fast way to connect with the DVG-2030S via backbone network. To provide multiple user a low cost, high performance telephone call.

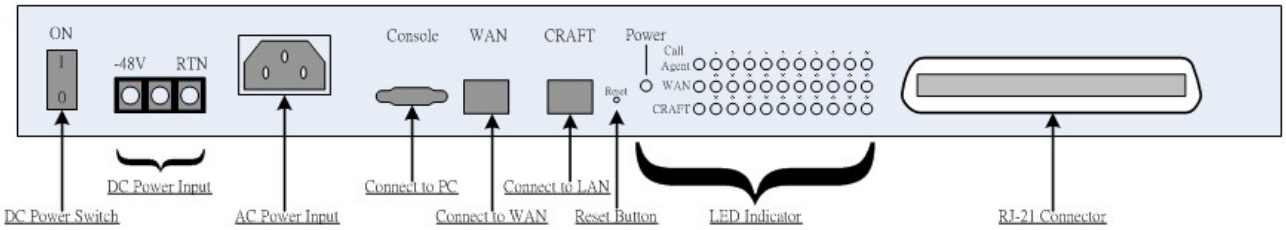
2.1.1. Features

- Support RFC2543bis04 SIP (Session Initiation Protocol).
- Compliant to RFC3261 SIP (Session Initiation Protocol).
- RJ-11 * 30 Foreign Exchange Station (FXS) ports for IP telephony.
- Telephone ports on a single RJ21X 64-PIN female connector
- Up to 30 simultaneous voice calls
- Support simultaneous voice and data communications, voice conversations in the FXS port with CODEC: G.711(a-law/ μ-law), G.723, G.729 support.
- Connecting to the broadband access network via an auto-negotiated 10/100 Base-T Ethernet interface
- Support IPv4 routing function.
- Support DHCP client in WAN interface and LAN interface (CRAFT) provides a DHCP server.
- Support Network Time Protocol (NTP) and Event Log
- Support SNMP Network Management and Private MIB
- Software remote upgrade with FTP, TFTP or HTTP
- Remote configuration and diagnosis through Web Browser, Telnet, Console, and SNMP
- Configurable QoS tagging (VLAN/Diffserv/ToS) on voice egress packet
- Echo Cancellation
- Comfort Noise Generation (CNG)
- DTMF detection and generation
- Modem and FAX detection and transport
- Software Configurable Audio Gain Control
- DNS proxy
- Support IP filter and MAC filer for Internet security.
- Support Line Polarity Reversal
- IP static routing/NAPT/RIP
- Support IP filter and MAC filter for Internet security.
- DNS proxy

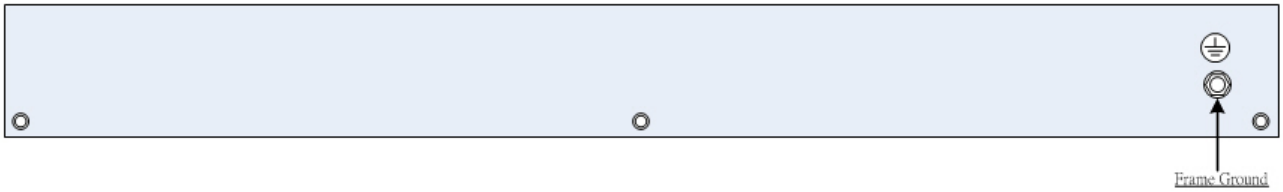
- Line test function

2.2 Physical Description

2.2.1. Front Panel



2.2.2. Rear Panel



AC Power

Connect to the AC power source.

Range: 90 ~ 264VAC

Frequency: 47 ~ 63 Hz

Current: 2.0A (max.) at 115VAC-60Hz, 1.0 A (max.) at 230VAC-50Hz

Connector & Button

Connector/Button	Description
Console	Connect to local computer via COM port. One DB-9 Female connector, the operating baud rate is 115200bps.
WAN	Ethernet 10/100 Base-T RJ-45 connectors for connection to broadband access device.
CRAFT (LAN)	One Ethernet 10/100 Base-T RJ-45 connector, Connect to local computer via an Ethernet connection.
Reset Default	To reset device to factory defaults, power off the gateway box first. Push a small, stiff object into the **Reset** hole and press down the button. Keep pressing and power on the gateway, then release the button once the power is on.
VoIP (RJ-21 connector)	Telephony connector. RJ-21*64-PIN connector for connecting to 30 terminals (telephone/fax/modem) with telephone cord.

Connector/Button	Description
FG (Frame Ground Connector)	Connect to earth ground in use.(note: reference to 2.3.1)

LED Indicator

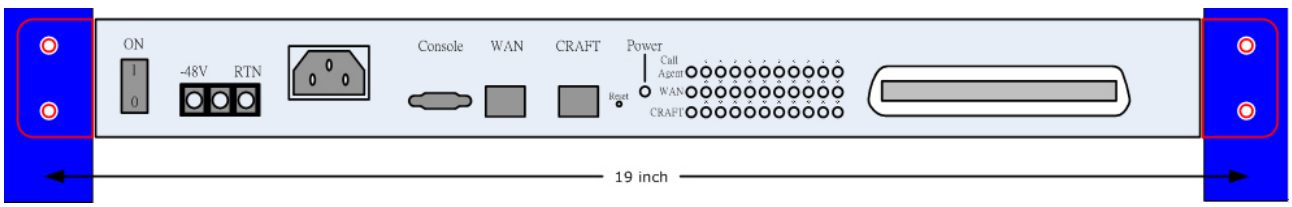
The LEDs on the front panel provides status indication of DVG-2030S operation as described below:

Label	Status	Description
Power	Amber Solid	Power On
	Amber Off	Power Off
Call Agent	Green Solid	SIP registration is successful
	Green Blink	SIP registration is in progress
	Green Off	SIP registration is failed
WAN	Green Solid	WAN port gets IP and ready
	Green Blink	Data traffic
	Green Off	WAN port does not get IP or Ethernet link down
CRAFT (LAN)	Green Solid	Cable is connected.
	Green Blink	Data traffic
	Green Off	Cable is not connected.
VoIP 1~30	Green Solid	Off hook
	Green Blink	Phone is ringing
	Green Off	Off-hooking or in VoIP conversation

2.3 Install procedure

Before installation, please check the following requirements with your system:

2.3.1. Site Environment Preparation



- The dimensions are: 430mm (W) x 44mm (H) x 380mm (D). The DVG-2030S can be mounted in a 19 -inch rack with ears and screws.

- Operating temperature: 0~60 ℃, the ambient temperature is other than the requirement, an air conditioner might be needed.
- Humidity: 5% to 90% (non-condensing)
- AC power source: 90 to 264 V, 47 to 63 Hz.
- Rear panel need connect with a protective earth shell be provided, which has a permanent connection to protective earth with a cross-sectional area of not less than 2.5 mm^2.
- Lightning Protection:

  a. Install the device including all the wiring connected to the device in a lightning-protected or lightning-free area.

  b. Ensure the line Tip and Ring wire will not be exposed to any positive voltage transient (compare to power ground) or voltage lower than -85V.

2.3.2. System Requirement

- Internet access, via cable or ADSL modem with Ethernet Interface.
- A computer equipped with 10/100Base-T Ethernet card and with TCP/IP protocol installed.
- Microsoft Internet Explorer 6.0 / Netscape 7.0 or later version (for web configuration).
- One standard phone set (DTMF/10pps/20pps) and phone.
- Subscribe to a VoIP system company (VoIP service provider) for VoIP services.

2.3.3. Cable Connection Procedure

Connect the following cables to the IAD.

- **WAN connection** – connect to the broadband service.

Connect one end of RJ-45 Ethernet cord to the WAN port of the IAD; plug the other end to the Ethernet jack of the broadband access device.

- **Telephony Connector** – connect to the analog telephony device.

Connect the analog telephony device to the Telephony Connector. If a 90° turn cover kit connector is in used, tighten the only screw provided with the connector to the female connection on the IAD and use the Velcro tape to secure and strengthen the connection. If a 180° cover kit of the connector is in used, tighten the 2 screws provided with the connection to the female connection on the IAD.

- **CRAFT (LAN) connection** – connect to a single PC.

Attach one end of a "straight-through" RJ-45 Ethernet cable to the CRAFT port of the IAD; plug the other end to the Ethernet port of the local computer. After the cable connections described above is done, connect the power connector with the power source.

- **Power connection** – Connect to the power source.

Turn off the DC power switch of front panel. Connect the AC/DC power cord to the correct port on the front panel, and the other end to a power source. Turn on the DC power switch of front panel, if DC power fed. The Power LED will be lit in amber color to indicate the device is having power. The WAN/CRAFT LEDs will be lit in green color if the device is connected with the other network devices respectively.

3 Network setting of the personal computer

Using LAN cable to connect with device and personal computer. It is possible to access device via Web Browser. The hardware of the personal computer is necessary to access device, as well as the software.

Hardware:

. The personal computer which has Ethernet interface or Ethernet NIC (Network Interface Card) equipped.

Memo ***Concerning the setting method of the Ethernet interface, please refer to the manual which belongs to the personal computer or the Ethernet card.***

Software:

- Web browser software 〈 For Windows〉

  Microsoft Internet Explorer Ver. 6.0 or later version

  Netscape Communicator Ver.7.0 or later version

- Web browser software 〈 For Macintosh 〉

  Microsoft Internet Explorer Ver. 5.0

3.1 Setting up the TCP/IP

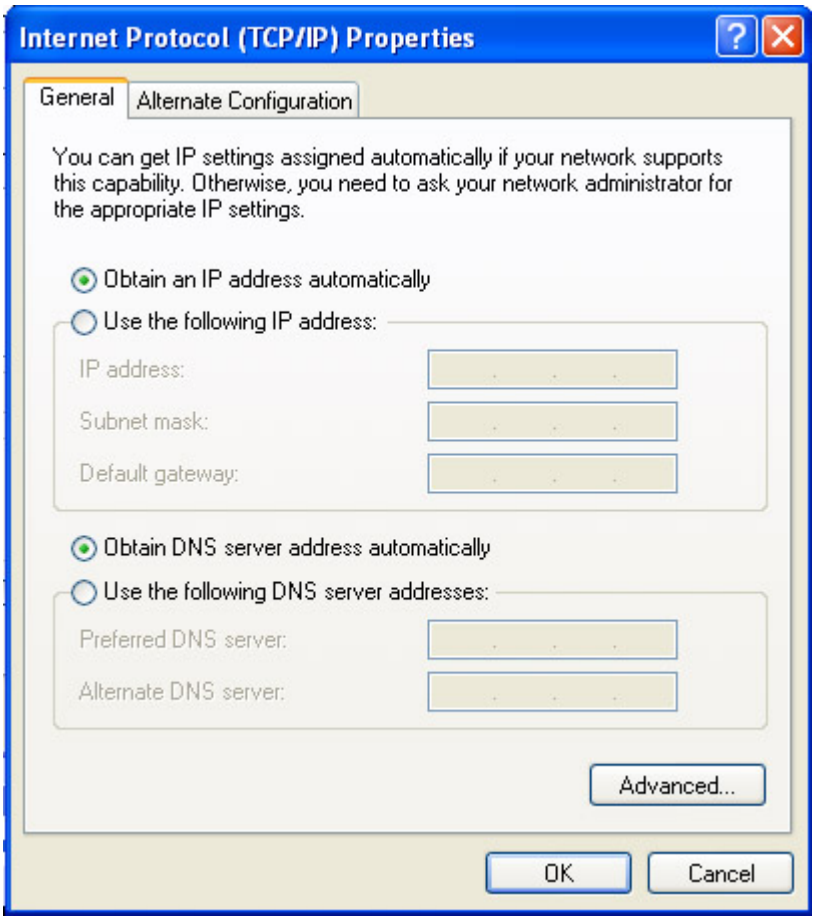
In order to accessing device from the PC, it is necessary to set up TCP/IP protocol for Ethernet interface. Here, it explains the steps to set up the TCP /IP.

Memo ***(LAN) has the function which automatically assigns IP address (DHCP server function). If the setting which can acquire IP address automatically on personal computer side is done, it is possible to access immediately.***

For Windows XP

Setting the TCP/IP

1. please click [**Start**] -> selecting [**Control Panel**]
2. Click the [**Network and Internet Connections**] and then select the [**Network Connections**] icon.
3. Select the [**Local Area Connection**] icon for the applicable Ethernet adapter. Double-click the [**Local Area Connection**].
4. The [**Local Area Connection**] Status screen will appear. Click the [**Properties**] button.
5. Select [**Internet Protocol (the TCP/IP)**] and click the [**Properties**] button.
6. Select [**Obtain an IP address automatically**]

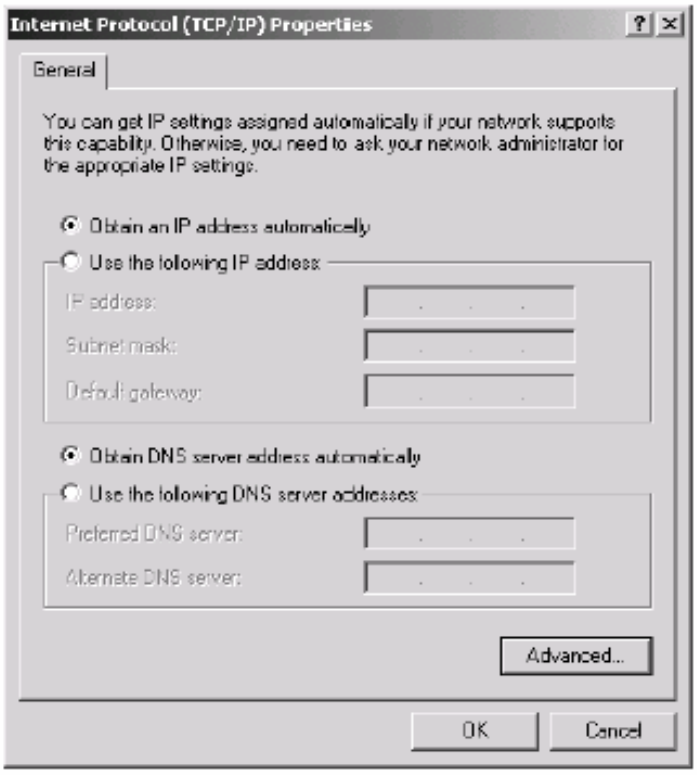


7. Please select [Obtain DNS server address automatically].
8. Please click [OK] To complete the PC configuration.

For Windows 2000

Setting the TCP/IP

1. Please click [**Start**] -> [**Setting**] -> selecting [**Control Panel**] .
2. Double-click [**Network and Dial-Up connection**].
3. Select the [**Local Area Connection**] icon for the applicable Ethernet adapter. Double-click the [**Local Area Connection**].
4. Select [**Internet Protocol(TCP/IP)**] and click the [**Properties**] button.
5. Select [**Obtain an IP address automatically**]

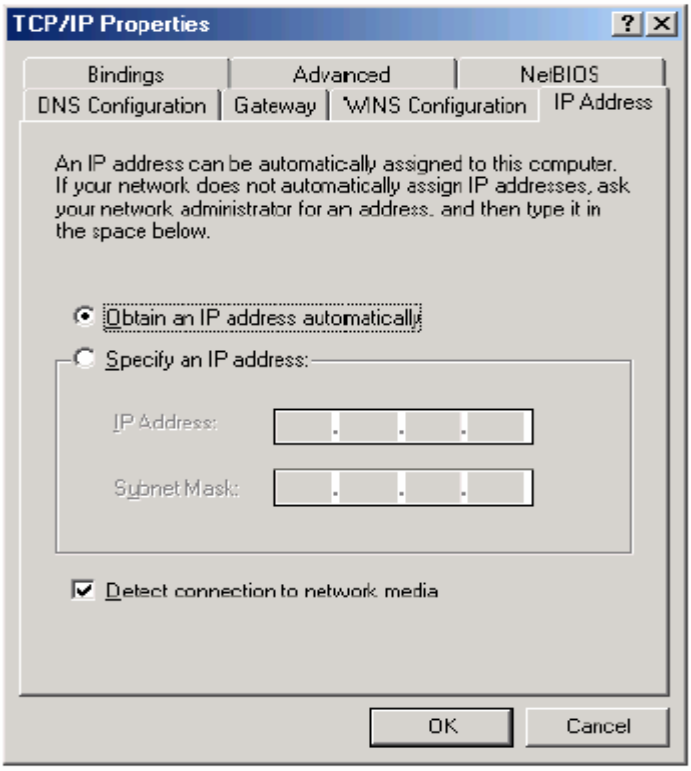


6. Please select [Obtain DNS server address automatically].
7. Please click [OK] to complete the PC configuration

For Windows ME/98/95

Setting the TCP/IP

1. Please click [**Start**] -> [**Setting**] ->selecting [**Control Panel**] .
2. Double-click [**Network**].
3. Select the [**TCP/IP**] line for the applicable Ethernet adapter. Click the [**Properties**].

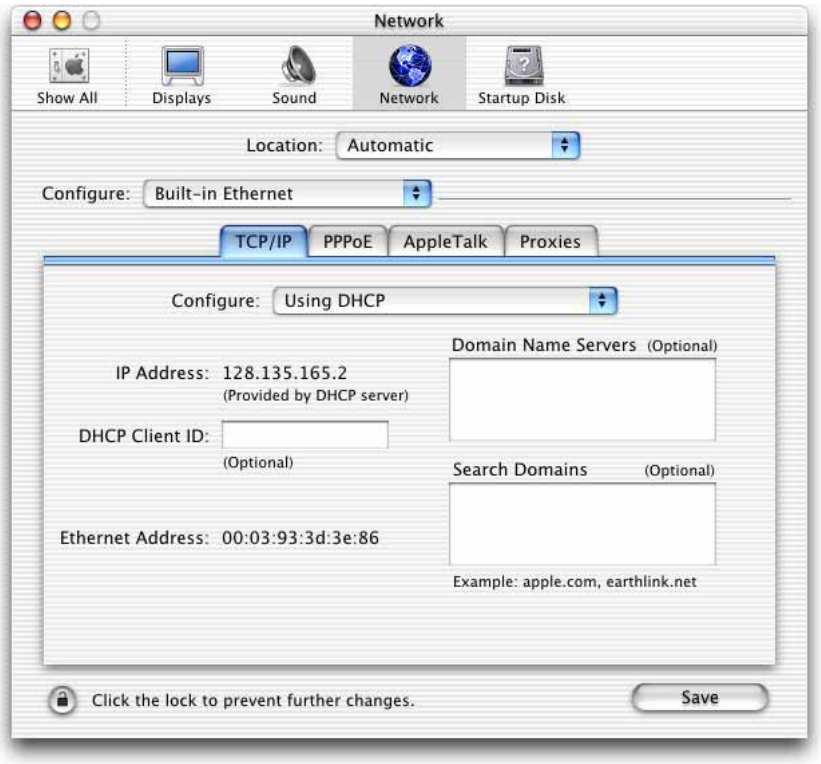


4. Select [**Obtain an IP address automatically**]
5. Please click [**OK**] and click [**Yes**] to restart the PC.

For Macintosh (Mac OS X)

Setting the TCP/IP

1. Select 「 **System Preferences** 」 from Apple Menu.
2. Click 「 **Network** 」 icon in the System Preferences window,
3. Leave the 「 **Location** 」 drop-down menu set to "Automatic".
4. From the 「 **Configure** 」 menu just below the location menu, select "Built-in Ethernet".
5. Click on the 「 **TCP/IP** 」 tab to display the TCP/IP panel.
6. From the TCP/IP panel's 「 **Configure** 」 drop-down menu, select "Using DHCP".
7. After making any changes click on the 「 **Save** 」 button below



3.2 Verification of TCP/IP configuration

The following procedures verify the IP address which is assigned to the personal computer.

ATTENTION: When appropriate IP address is not assigned, it cannot access device. Please renew the IP address when the PC cannot be assigned correct IP address. After verifying the following points, please restart your personal computer.

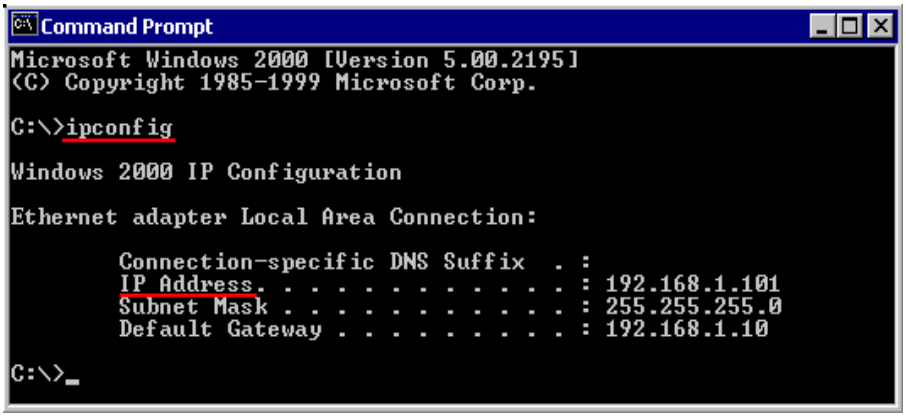
- Is the LAN cable connected? (Does CRAFT LED light up?)
- Is TCP/IP protocol configured properly? (Refer 3.1 Setting up the TCP/IP)
- Is the Ethernet card installed?

For Windows XP/ 2000

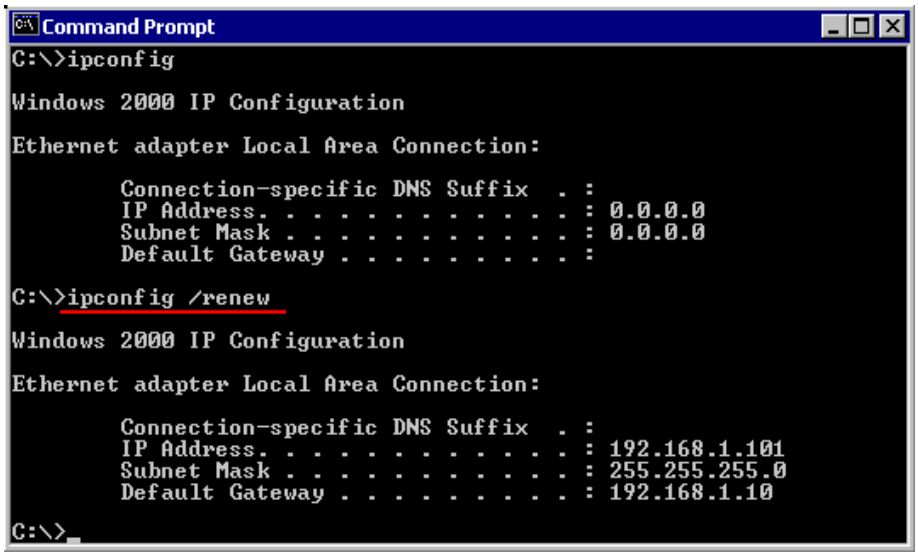
Please click [**Start**] - [**All Programs**] (for Windows 2000 [**Programs**]) - [**Accessories**] and select [**Command Prompt**].

Please type 「 **ipconfig** 」 and hit 「 **Enter** 」

Setting contents of the TCP/IP are indicated on the line of 「 **IP Address** 」



If the IP address information which is allotted to the personal computer is not correct. Please type 「 **ipconfig/renew** 」 and hit 「 **Enter** 」, renew IP address.



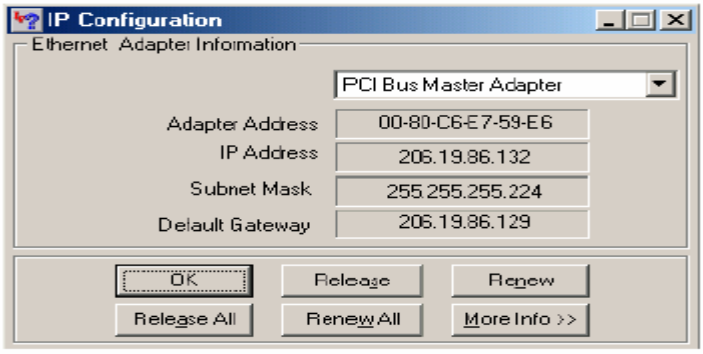
For Windows ME/98/95

Please click [**Start**] - and select [**RUN**]

[**RUN**] the dialogue box is indicated.

Please type 「 **winipcfg** 」 in the input column and press 「 **OK** 」

[**IP configuration**] are indicated .

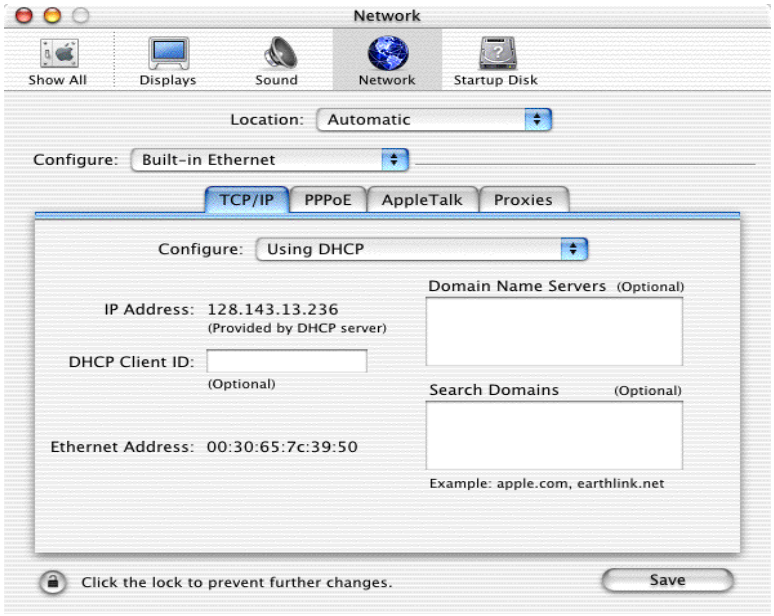


Select your adapter name — the Ethernet card or USB device.

Click [**Renew**] then click 「 **OK** 」

For Macintosh (Mac OS X later)

1. Select 「 **System Preferences** 」 from Apple Menu.
2. Click 「 **Network** 」 icon in the System Preferences window.



3. Please verify that IP address which is indicated.

For Mac OS, it is impossible to update IP address information using command. Please unplug and plug the LAN cable wire, or restart the personal computer.

4 Quick Setup

This chapter describes basic configurations to quickly set up the IAD. For advanced features such as VLAN, TOD, SNMP and other functions, please refer to next chapters.

4.1 Provisioning Requirements

The following is the basic requirements for Quick Set Up:

- Broadband Ethernet access to the Call Agent.
- A local computer equipped with:

- 10/100Base-T Ethernet connection

- Support TCP/IP protocol

- Microsoft Internet Explorer 5.0 or later (for web configuration).

- For provisioning verification, at least one standard touch-tone telephone connected to the IAD via a telephony cable.

4.2 Configuring the local computer to access IAD via CRAFT port

The easiest way to access the IAD is through the local CRAFT port. In order to access the IAD through the local CRAFT port, the local PC and the IAD's IP must under the same subnet. By default, the IP of the CRAFT port is 192.168.1.1 and the DHCP server is enabled (to assign IP address to the devices connected to the CRAFT port). To set the PC in the same subnet as the IAD, configure the PC to either fixed or dynamic IP addressing.

4.3 Checking the IP of the local computer

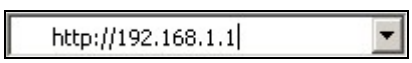
Please refer chapter 3.

4.4 Quick configuration for DVG-2030S

Follow the steps below to quickly set up the IAD.

4.4.1. Step 1. Enter the IP of the IAD

Launch the web browser, enter the IP of the IAD (factory default 192.168.1.1) on the browser's URL field, and press **Enter**.



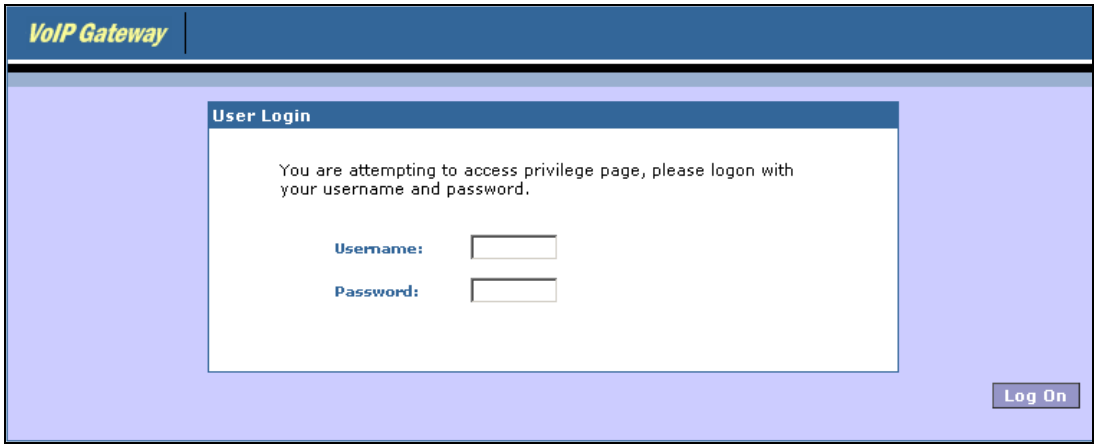
Home page - DVG-2030S will display this page while user access every time

4.4.2. Step 2. Enter “User Name” & “Password”

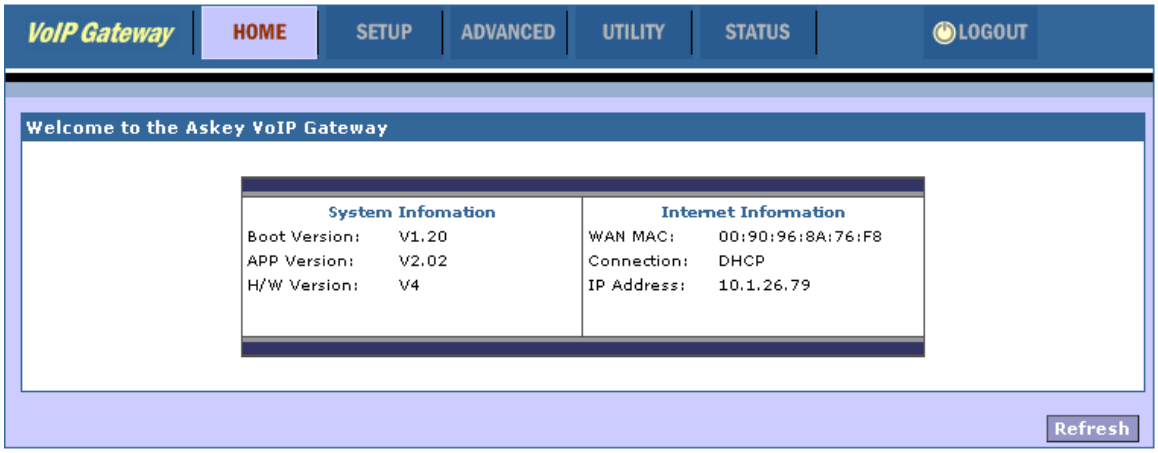
Click “SETUP / ADVANCE / UTILITY / STATUS”. Device will ask user key in “Username” and “Password”.

The administrator’s name and password. The factory default settings are:

- User Name: admin
- Password: admin



DVG-2030S will show the system information (firmware version and WAN port information), if login successful.

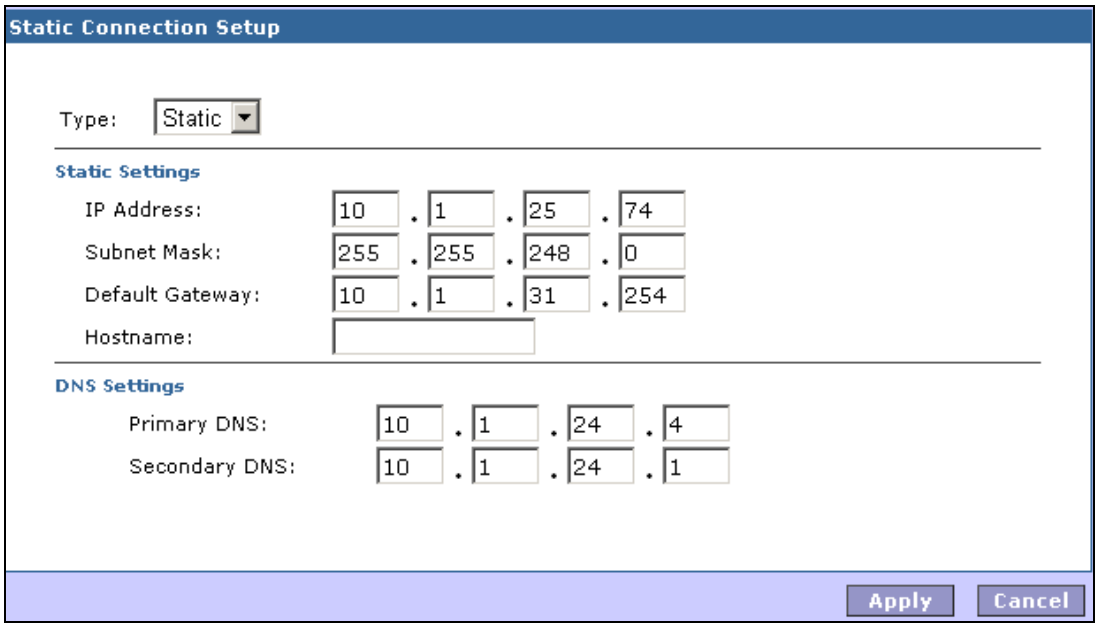


4.4.3. Step 3. SETUP-WAN Interface

Click **SETUP** → **WAN SETUP** → chose WAN interface type → fill WAN port information in associated fields → **Apply**.

4.4.3.1. Static IP

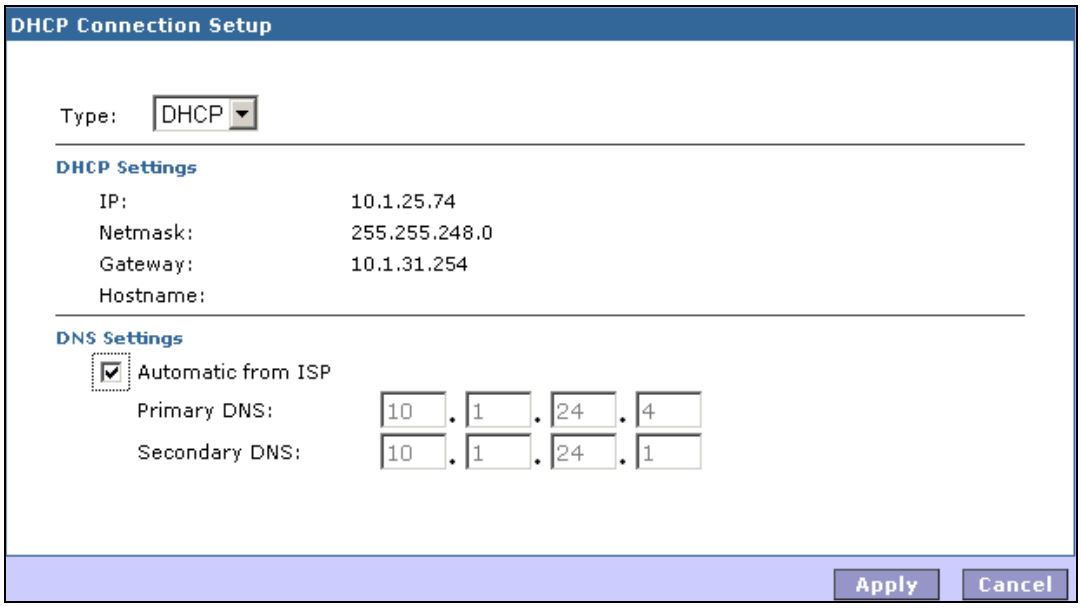
If "**Static**" is selected, then filling in the **IP Address, Subnet Mask, Default Gateway, Hostname, Primary DNS** and **Secondary DNS** in associated fields.



DHCP

If "**DHCP**" is selected, then filling in the **IP Address, Subnet Mask, Default Gateway** and **Hostname** in associated fields. WAN port is supposed to obtain a dynamic IP address from the DHCP server along with other DHCP options

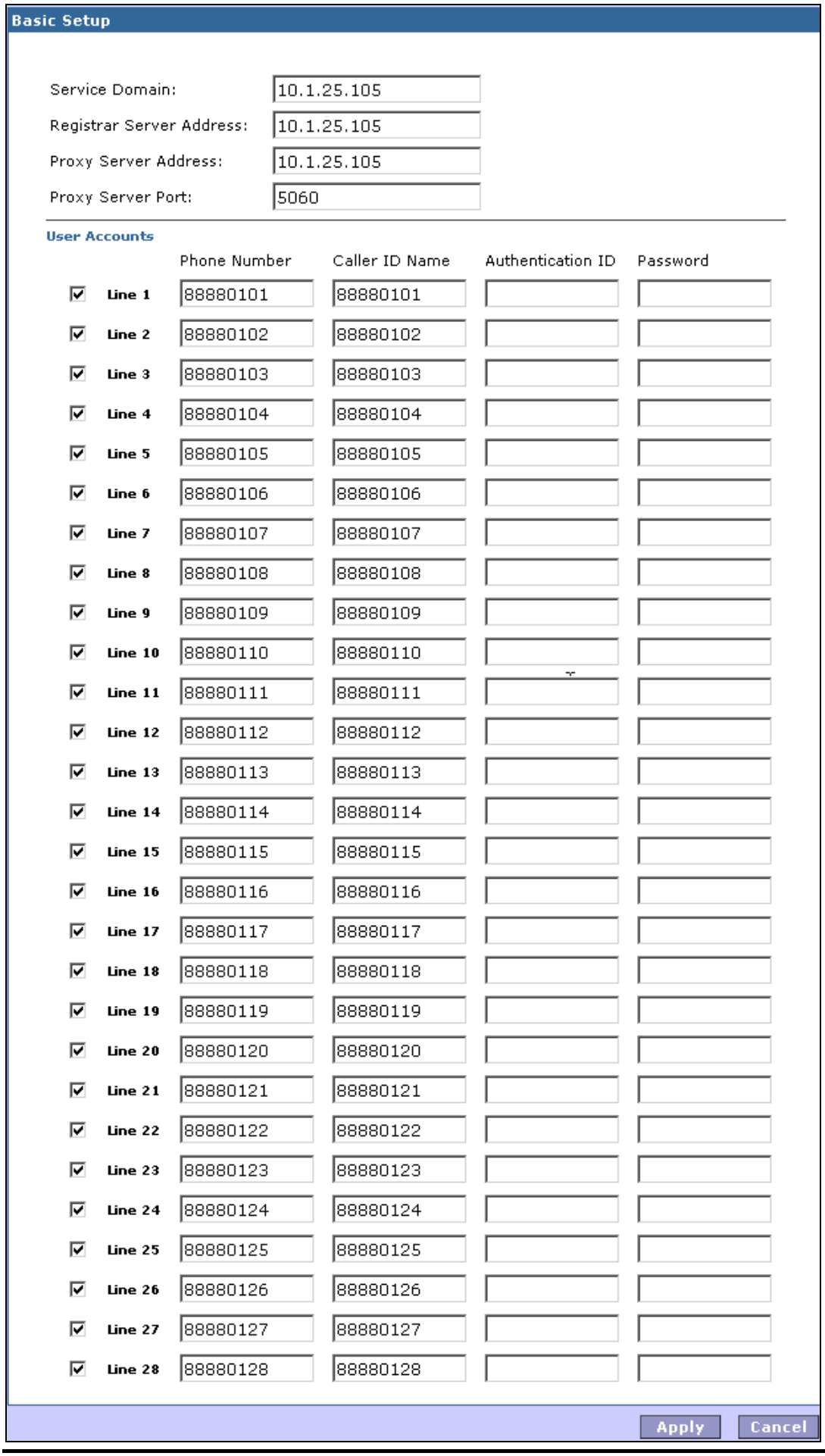
Automatic from ISP: Configure DNS server automatically or manually.



4.4.4. Step 4. Setup Telephone Number

- **Service Domain**: Domain Name address
- **Register Server Address**: Enter register server IP address
- **Proxy Server Address**: Enter Proxy server IP address
- **Proxy Server Port**: Default port number is 5060
- **Phone Number** : Enter the phone number that the user would like to use.
- **Caller ID Name**: Caller ID displayed on called party.

- **Authentication ID**：Enter the register ID that goes with this telephone number.
- **Password**：Enter the password that goes with this telephone number.



Basic Setup

Service Domain: 10.1.25.105
Registrar Server Address: 10.1.25.105
Proxy Server Address: 10.1.25.105
Proxy Server Port: 5060

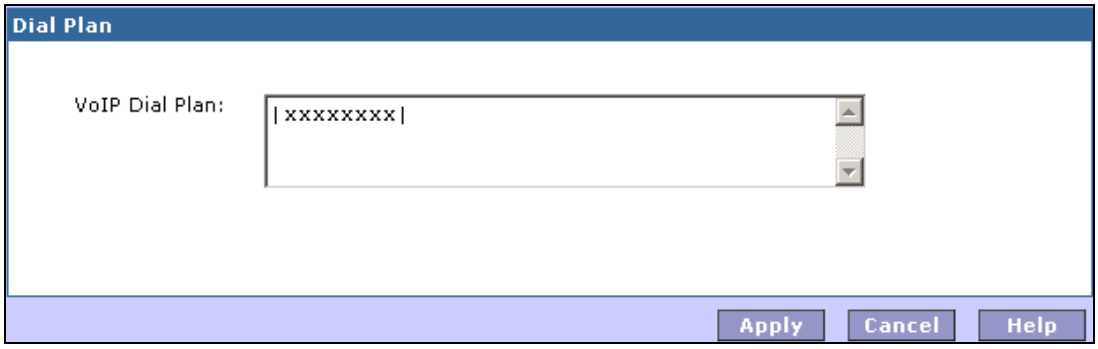
User Accounts

	Phone Number	Caller ID Name	Authentication ID	Password
Line 1	88880101	88880101		
Line 2	88880102	88880102		
Line 3	88880103	88880103		
Line 4	88880104	88880104		
Line 5	88880105	88880105		
Line 6	88880106	88880106		
Line 7	88880107	88880107		
Line 8	88880108	88880108		
Line 9	88880109	88880109		
Line 10	88880110	88880110		
Line 11	88880111	88880111		
Line 12	88880112	88880112		
Line 13	88880113	88880113		
Line 14	88880114	88880114		
Line 15	88880115	88880115		
Line 16	88880116	88880116		
Line 17	88880117	88880117		
Line 18	88880118	88880118		
Line 19	88880119	88880119		
Line 20	88880120	88880120		
Line 21	88880121	88880121		
Line 22	88880122	88880122		
Line 23	88880123	88880123		
Line 24	88880124	88880124		
Line 25	88880125	88880125		
Line 26	88880126	88880126		
Line 27	88880127	88880127		
Line 28	88880128	88880128		

Apply Cancel

4.4.5. Step 5. Dial Plan

Setup VoIP dial plan to provide a rule for VoIP outgoing call.



Dial plan can be configured with following characters: **"0~9", "x", ".T", "|", "[ ]"**

- **"0-9"**: Digit can be configured with 0~9.
- **"x"**: Define how many digits can be used in dial plan.
- **".T"**: Digits will be sent after timeout. Without timeout character, digits will be sent immediately after finish dialing. (Default 3 sec.)
- **"|"**: To separate dial plan from others.
- **"[]"**: If digits can be configured in various type, we can use a square bracket to define this digit.

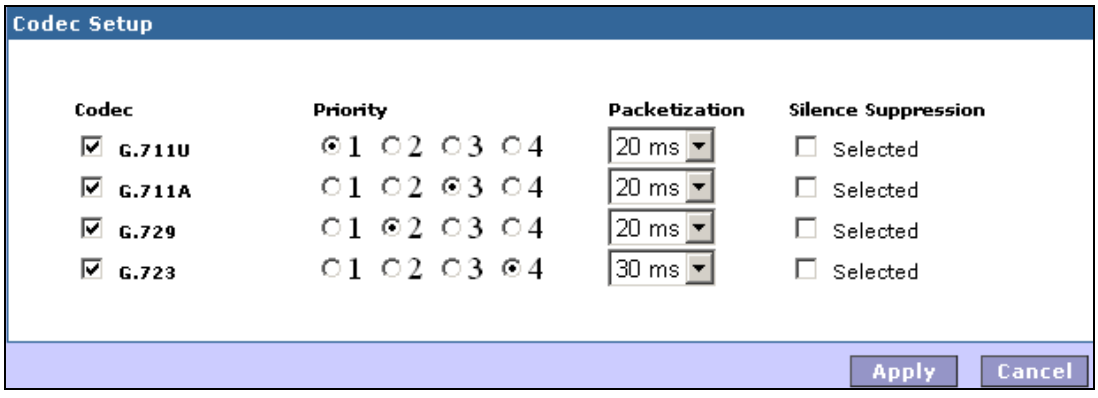
ex. If we configure dial plan as **[1-3]xxxx|xxxx.T** then dial

(1) **1**4567 or **2**4567 or **3**4567, digits will be sent immediately after finish dialing.

(2) 4123 or 5123 or 61234, the front four digits will be sent after timeout.

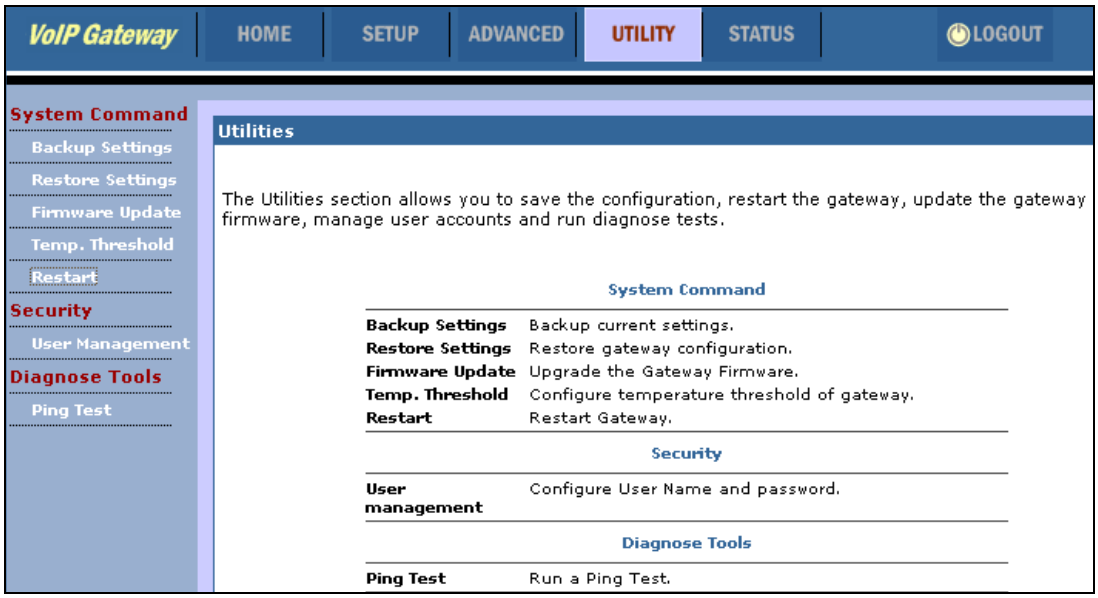
4.4.6. Step 6. CODEC Setup

It provides G.711 μ, G.711A, G.729 and G.723 CODEC to transfer voice.



4.4.7. Step 6. Restart

Select **UTILITY** → **Restart** to active all setting (step 1~5)



4.5 Usage of IP telephone

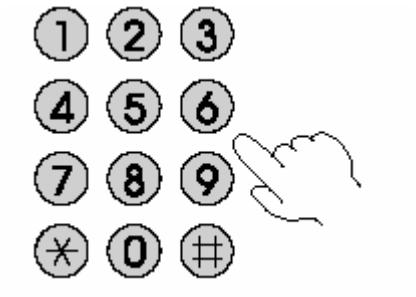
Owing to device, here is the introduction of dialing and answering the IP telephone.

4.5.1. Dialing (to use the telephone)

Using telephone, FAX, modem or the FAX equipped telephone with the standard telephone cord connects to the Phone port of DVG-2030S.

Pick up the headset.

Dial the telephone number after receive dial tone.



Distinguish the standard telephone and the IP telephone from the ring back tone

When the callee answers the phone, please speak.

When the conversation ends, please hang up the phone.

4.5.2. Answering (to answer the telephone)

The telephone rings.

Pick up the headset and answer the telephone.

When the conversation ends, please hang up the phone.

5 Configure DVG-2030S via Web

This chapter will show you how to configure device to function as Internet connectivity and VoIP service through Main Application. Detail description of device's configuration web page will be described later. If not having the relative information, please contact the ISP before proceeding.

5.1 Menu Item Configuration

This web configuration is displayed while connecting to device via web browser.

1. Open the web browser

   ATTENTION: Remember to enable "**Java Script**" on the web browser.

2. Please input the following HTTP-URL address in the address column of Web browser, and press "**Enter**".

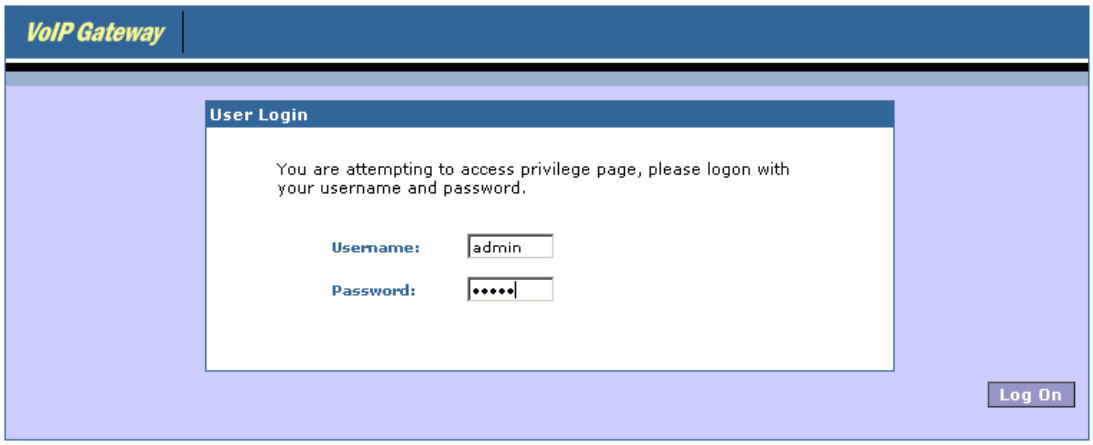
   http://192.168.1.1/ (It's default value of LAN IP address)

3. Input correct user name and password and click "**Log On**"

   User Name：**admin**

   Password：**admin**

   The above user name and password are default values. For security reason, it is better to change them after the router works normally. To modify the username and password, please refer to "**Utility**" item.



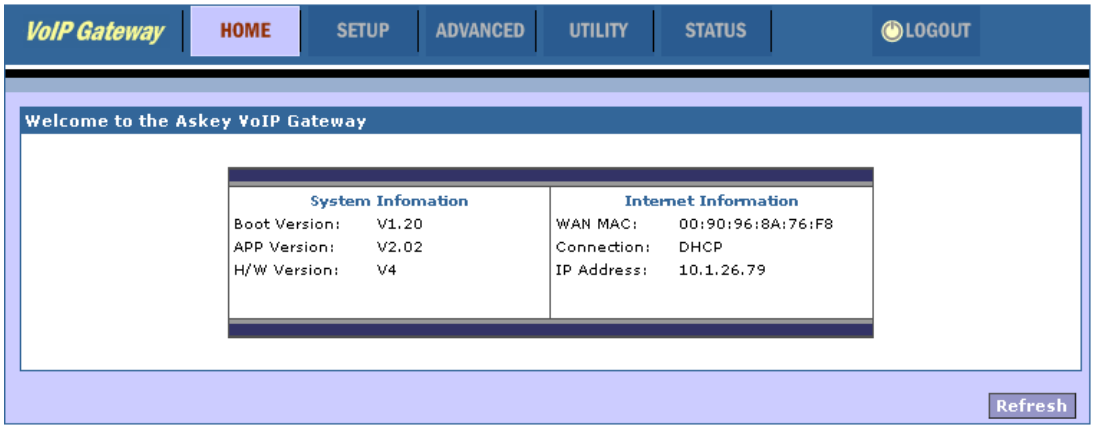
4. DVG-2030S Web Configuration

   The web page configuration is divided into menu frame and operation frame. If any item in menu frame such as "**HOME**", "**SETUP**", "**ADVANCED**", "**UTILITY**" or "**STATUS**" is selected, the content of operation frame may vary.

5.2 Function Overview

The Function Overview page is displayed in the main window when connecting device Web system.

5.2.1. Main Application

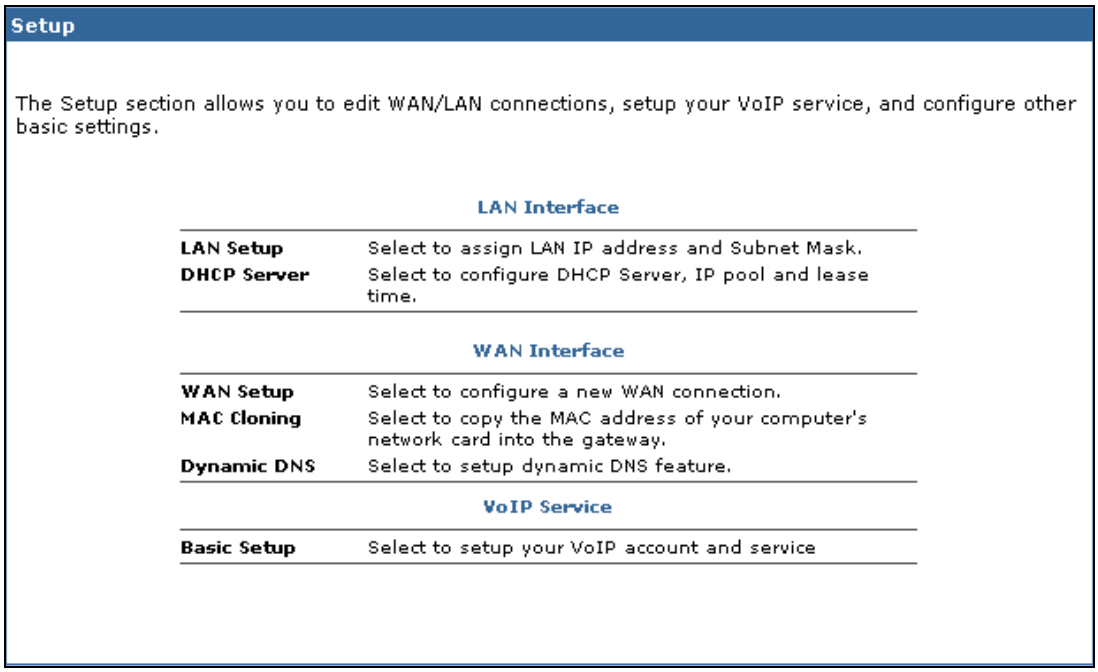


The device Web system can access the following features:

Page	Item	Sub-Item	Description
Home	System Info.		Show F/W and H/W version of device.
	Internet Info.		Show MAC, mode and IP address of WAN interface
Setup	LAN Interface	LAN Setup	Select to assign LAN IP address and Subnet Mask.
		DHCP Server	Select to configure DHCP Server, IP pool and lease time.
	WAN Interface	WAN Setup	Select to configure a new WAN connection.
		MAC Cloning	Select to copy the MAC address of your computer's network card into the gateway.
		Dynamic DNS	Select to setup dynamic DNS feature.
	VoIP Service	Basic Setup	Select to setup your VoIP account and service.
Advanced	Networking	Routing	Configure static and NAPT.
		UPnP	Configure UPnP settings.
		SNTP	Select SNTP to configure time server on Internet.
		SNMP	Configure SNMP Management.
		QoS	Configure quality of service settings.
		Remote Manage	Allows you to make changes to gateway's settings via the internet.
	Voice Setting	SIP Signaling	Configure the SIP signaling parameters.
		Dial Plan	Configure the dial plan.
		Codec Setup	Select to setup your preferred Codec.
		Call Features	Select to configure call wait, call hold...etc.
		Service Code	Select to configure call feature via keypad operation.
		Advanced	Select to setup out of band DTMF, and telephone setting.
Utility	System Command	Backup Setting	Backup current settings.
		Restore Setting	Restore gateway configuration.
		Firmware Update	Upgrade the Gateway Firmware.
		Temp. Threshold	Configure temperature threshold of gateway.
		Restart	Restart Gateway.
	Security	User Management	Configure User Name and password.

	Diagnose Tools	Ping Test	Run a Ping Test.
Status	General Info.	Product Info.	View the Product Information and Software Versions.
	Network Status	Interface Status	View the Statistics of different interfaces - Ethernet/DSL.
	VoIP Status	Phone Status	View the phone status
	System Log	Event Log	View Event Log messages.

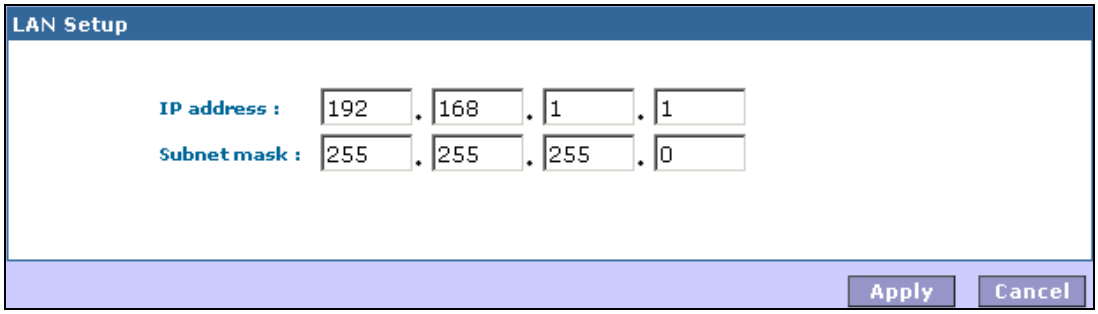
5.3 Setup



5.3.1. LAN Interface

LAN Setup

User can assign IP address and Subnet Mask for LAN Interface of DVG-2030S.



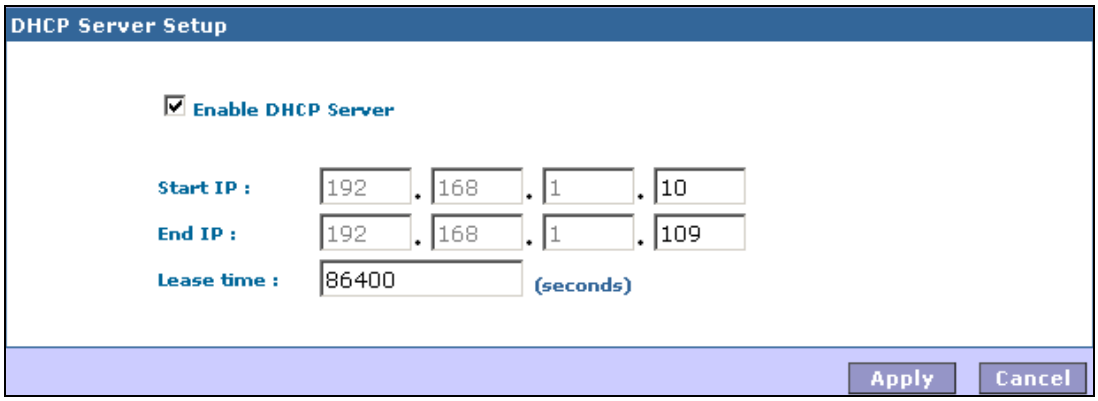
5.3.1.1. DHCP Server

DHCP Server : Allows you to enable (**ON**) or disable (**OFF**) DHCP server on the LAN side (default value is **ON)**.

Start IP : If **DHCP Server** is set to be **ON**, specify the first of the contiguous IP addresses to be assigned to client machines on your LAN (the default value is **192.168.1.10**).

End IP: Enter the end of IP addresses to be assigned (default value is **192.168.1.109**).

Lease Time : Specify the time (in seconds) that a network device can lease a private IP address before the device reassigning the IP address (default value is **86400** sec).



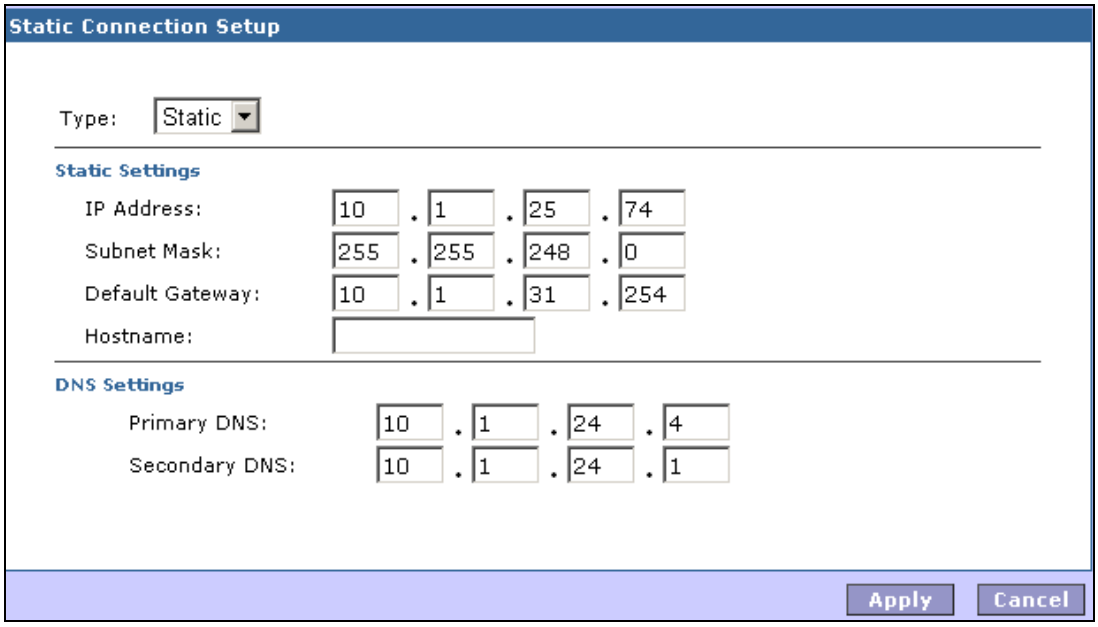
5.3.2. WAN Interface

Device can obtain WAN IP address through one of the following methods.

5.3.2.1. WAN Setup

- **Static IP**

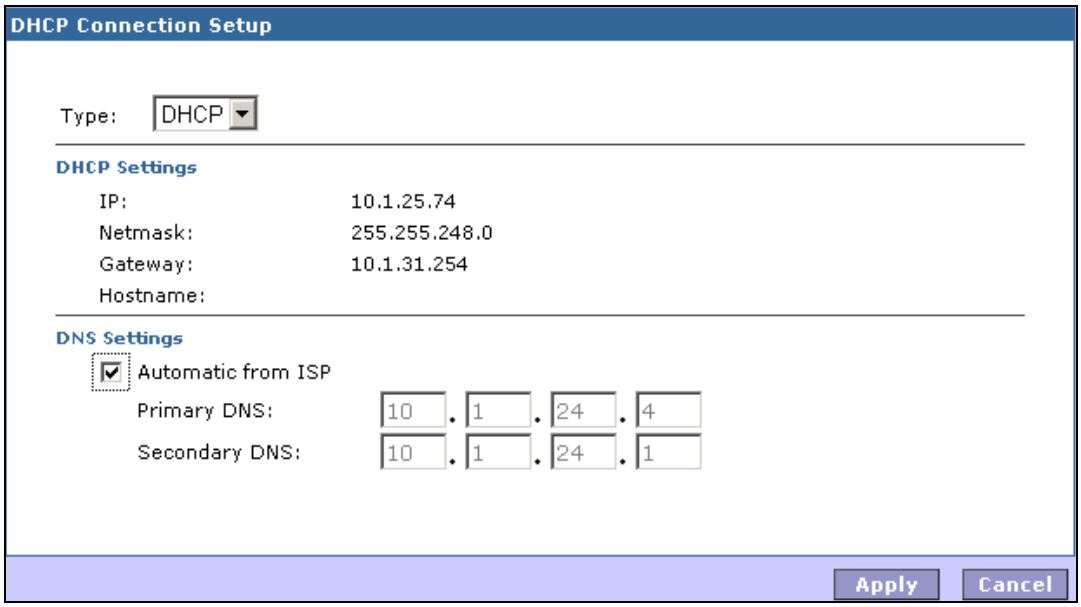
  If "**Static**" is selected, then filling in the **IP Address, Subnet Mask, Default Gateway, Hostname, Primary DNS** and **Secondary DNS** in associated fields.



- **DHCP**

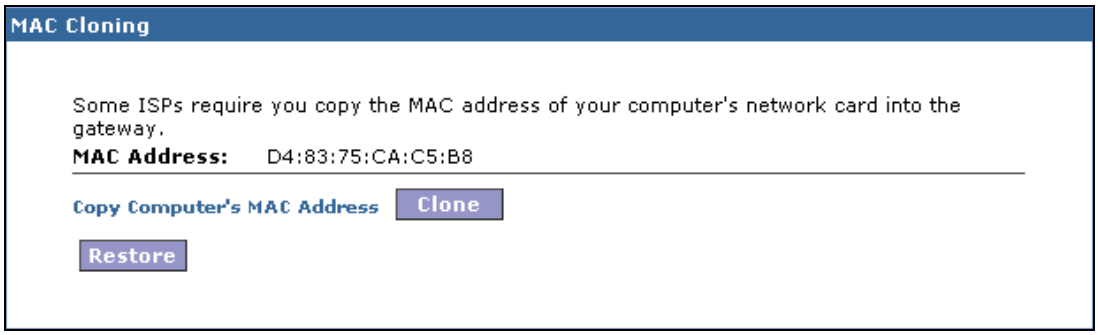
  If "**DHCP**" is selected, then filling in the **IP Address, Subnet Mask, Default Gateway** and **Hostname** in associated fields. WAN port is supposed to obtain a dynamic IP address from the DHCP server along with other DHCP options.

  Automatic from ISP: Configure DNS server automatically or manually.



MAC Cloning

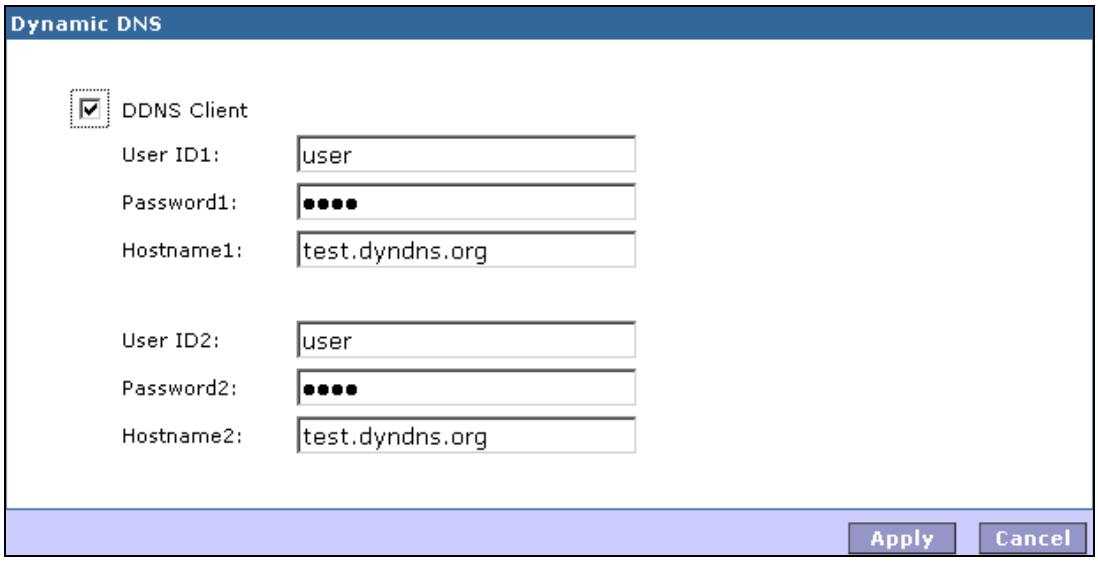
The ISP may record the MAC address of the user's computer and only let that particular computer connect to the Internet service. The gateway clone the MAC of the user's computer, then the gateway and the computer behind it can connect to the Internet. User must assess from LAN(CRAFT) port to execute this service.



Dynamic DNS

The Dynamic DNS service allows the gateway to alias a dynamic IP address to a static hostname, allowing the gateway to be more easily accessed from various locations on the Internet.

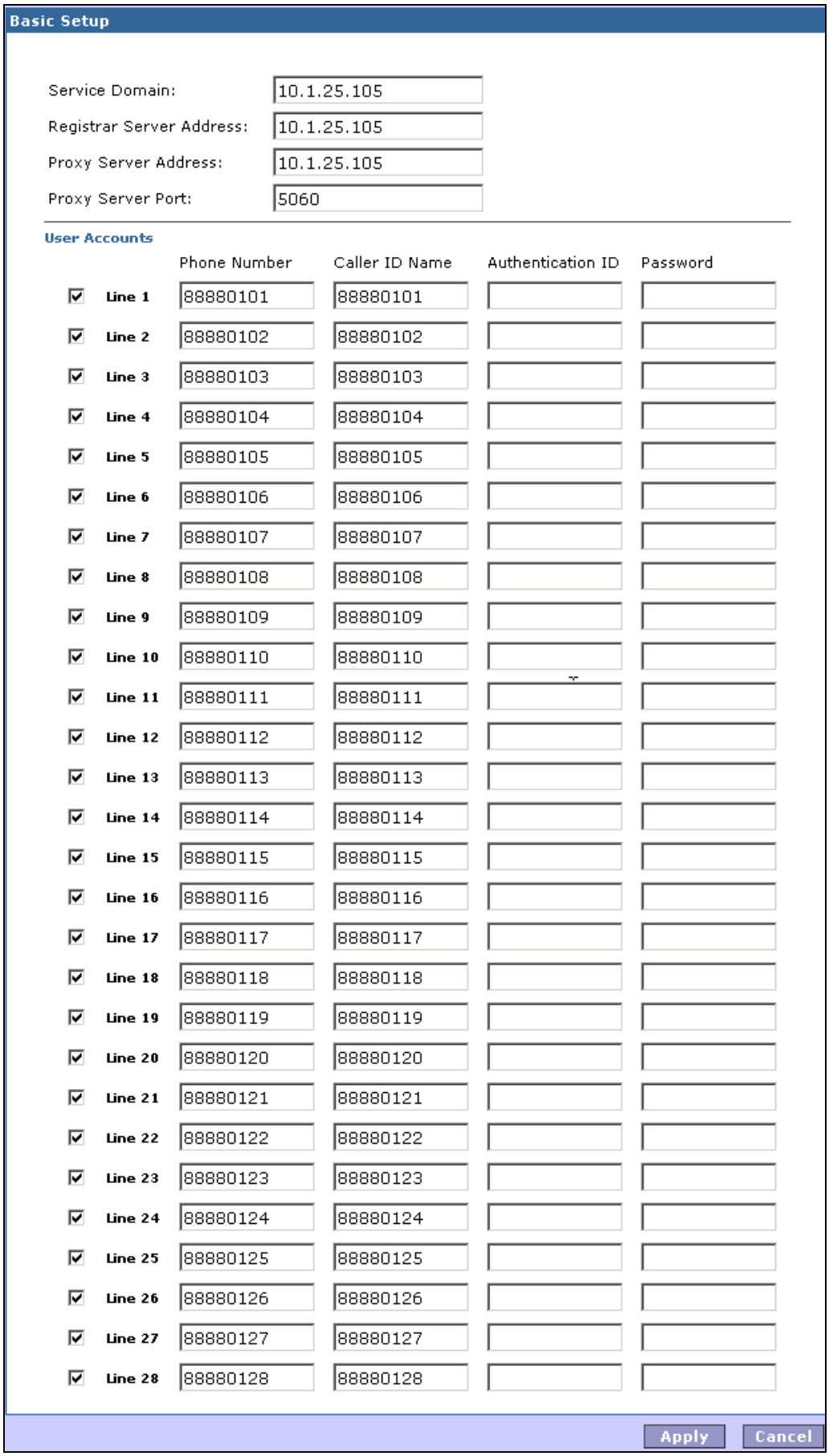
The user has to register on "**members.dyndns.org**" first, and then they can use this function.



5.3.3. VoIP Service

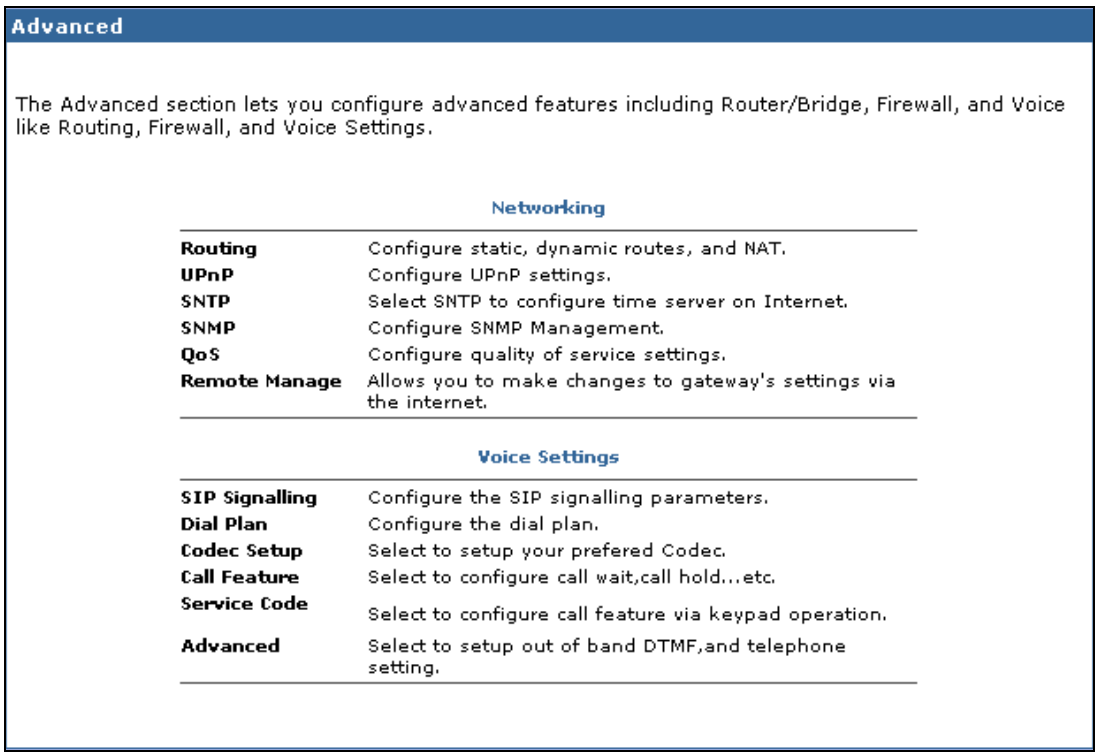
Basic Setup

- **Service Domain**: Domain Name address
- **Register Server Address**: Enter register server IP address
- **Proxy Server Address**: Enter Proxy server IP address
- **Proxy Server Port**: Default port number is 5060
- **Phone Number**：Enter the phone number that the user would like to use.
- **Caller ID Name**: Caller ID displayed on called party.
- **Authentication ID**：Enter the register ID that goes with this telephone number.
- **Password**：Enter the password that goes with this telephone number.


Basic Setup
Service Domain: 10.1.25.105
Registrar Server Address: 10.1.25.105
Proxy Server Address: 10.1.25.105
Proxy Server Port: 5060
User Accounts
Phone Number
Caller ID Name
Authentication ID
Password
Line 1 88880101 88880101
Line 2 88880102 88880102
Line 3 88880103 88880103
Line 4 88880104 88880104
Line 5 88880105 88880105
Line 6 88880106 88880106
Line 7 88880107 88880107
Line 8 88880108 88880108
Line 9 88880109 88880109
Line 10 88880110 88880110
Line 11 88880111 88880111
Line 12 88880112 88880112
Line 13 88880113 88880113
Line 14 88880114 88880114
Line 15 88880115 88880115
Line 16 88880116 88880116
Line 17 88880117 88880117
Line 18 88880118 88880118
Line 19 88880119 88880119
Line 20 88880120 88880120
Line 21 88880121 88880121
Line 22 88880122 88880122
Line 23 88880123 88880123
Line 24 88880124 88880124
Line 25 88880125 88880125
Line 26 88880126 88880126
Line 27 88880127 88880127
Line 28 88880128 88880128
Apply
Cancel

5.4 Advanced

Device provide advanced functions in this page.



5.4.1. Networking

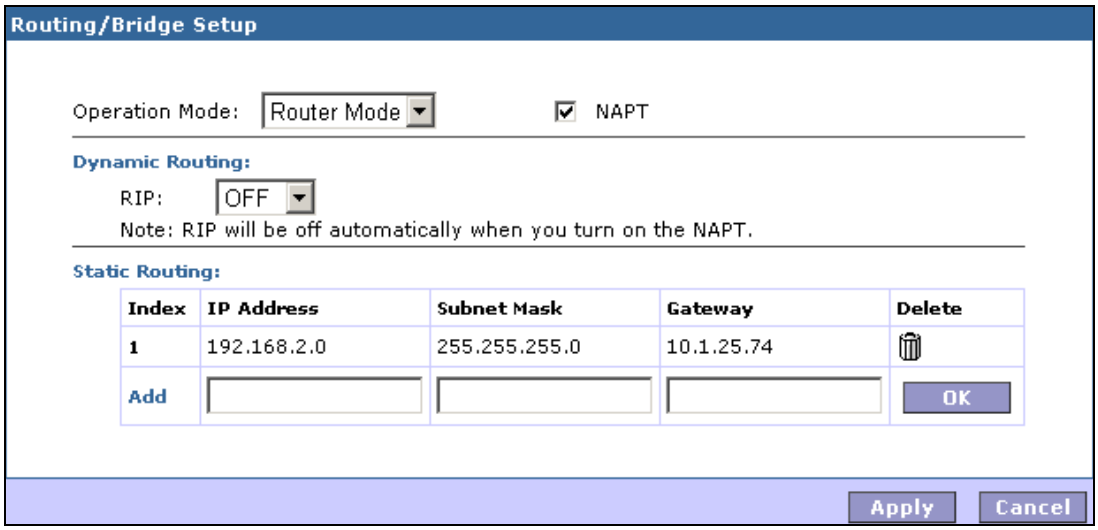
Routing

A Static Route is a manually defined path that redirects the IP packets to proper network. In most situations, users do not need to define static IP routes. User may need to define routes if:

- The network setup includes one or more routers that divide the network into two or more segments.
- User want to connect to a remote network that is beyond a directly connected node.

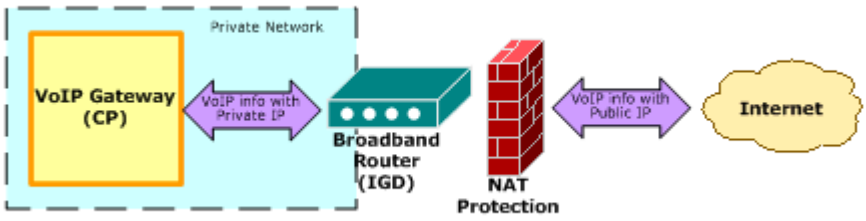
Destination Address/Mask : The destination IP address/mask of the network where data packets are to be sent.

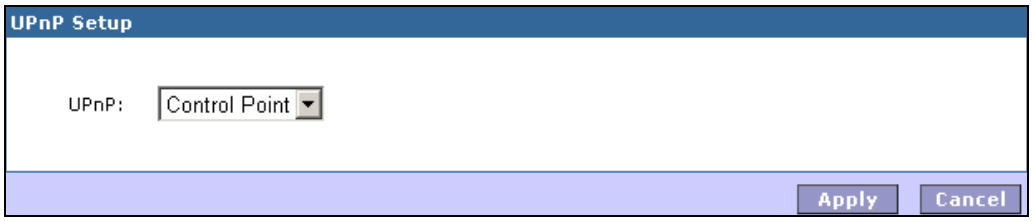
Gateway : The IP address of the interface linking to the remote network where data packets are to be sent



UPnP

User enables this function and the gateway can register to SIP server behind a NAT router. Device support UPnP control point only.





SNTP

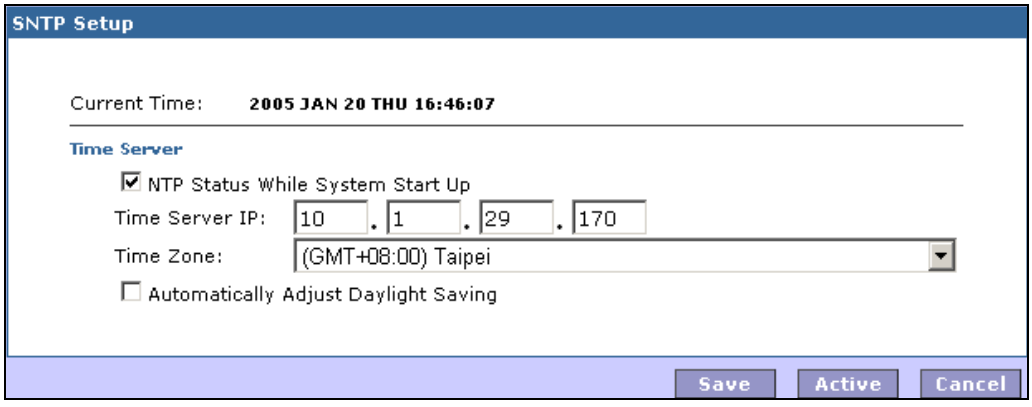
The gateway keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allow the gateway to synchronize the system clock to the global Internet. The synchronized clock in the gateway is used to record the security log.

NTP Status While System Start UP：To enable or disable the functionality here.

Time Server IP：Enter the IP address of Time server.

Time Zone：Select a time zone according to your geographic location.

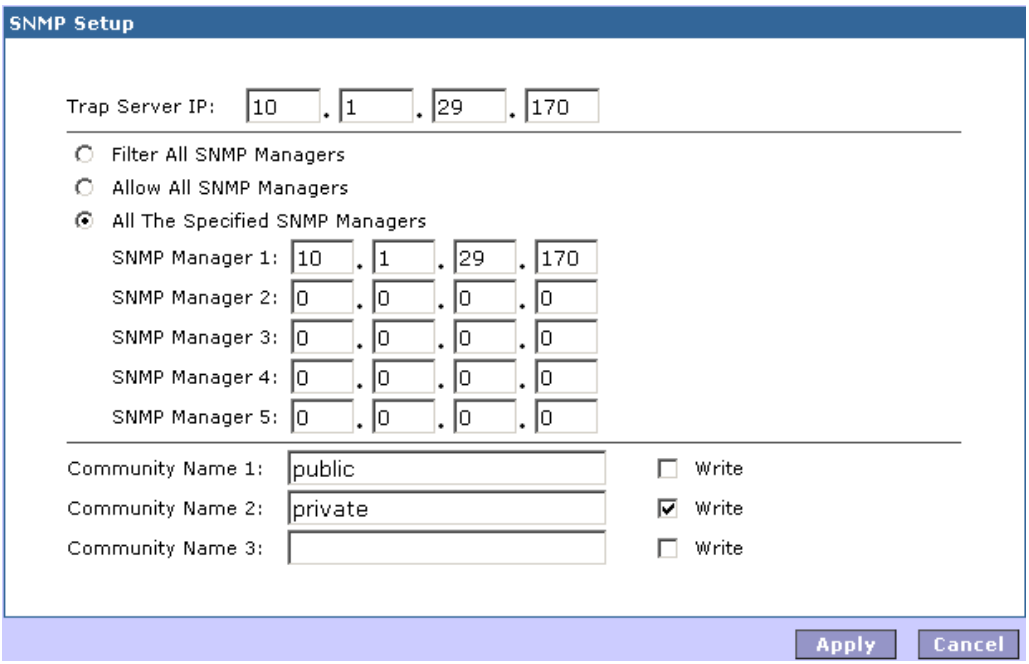
Daylight Savings Time：Select whether to enable or disable this feature.



SNMP

Device support SNMP(Simple Network Management Protocol). User can manage device via MIB browser with Device private MIB file.

- **Trap Server IP**: Setting Trap server IP. Device will send trap message while it abnormal.
- **SNMP Managers**: Device provide 3 type methods to filter SNMP manager(**Filter all**/ **Allow all**/ **Specified**)
- **SNMP Managers**: Device support community name to set **READ**/ **WRITE** authority of SNMP.



QoS

Type of Service(ToS) : used by applications to indicate priority and QoS for each frame. The gateway determines prioritization by the information from the IP header ToS field. To use TOS, user should define the first two bits of ToS field of an IP packet：(1) Precedence and (2) ToS field.

Precedence：From the drop-down, select the desired precedence which specifies the importance or priority of the traffic:

- 0 – Routine
- 1 – Priority
- 2 – Immediate
- 3 – Flash
- 4 – Flash Override
- 5 – CRITIC/ECP
- 6 – Internetwork Control
- 7 – Network Control

Delay：To generate a Low Delay service parameter that will minimize delay.

Throughput：To generate a High Throughput service parameter that will maximize throughput.

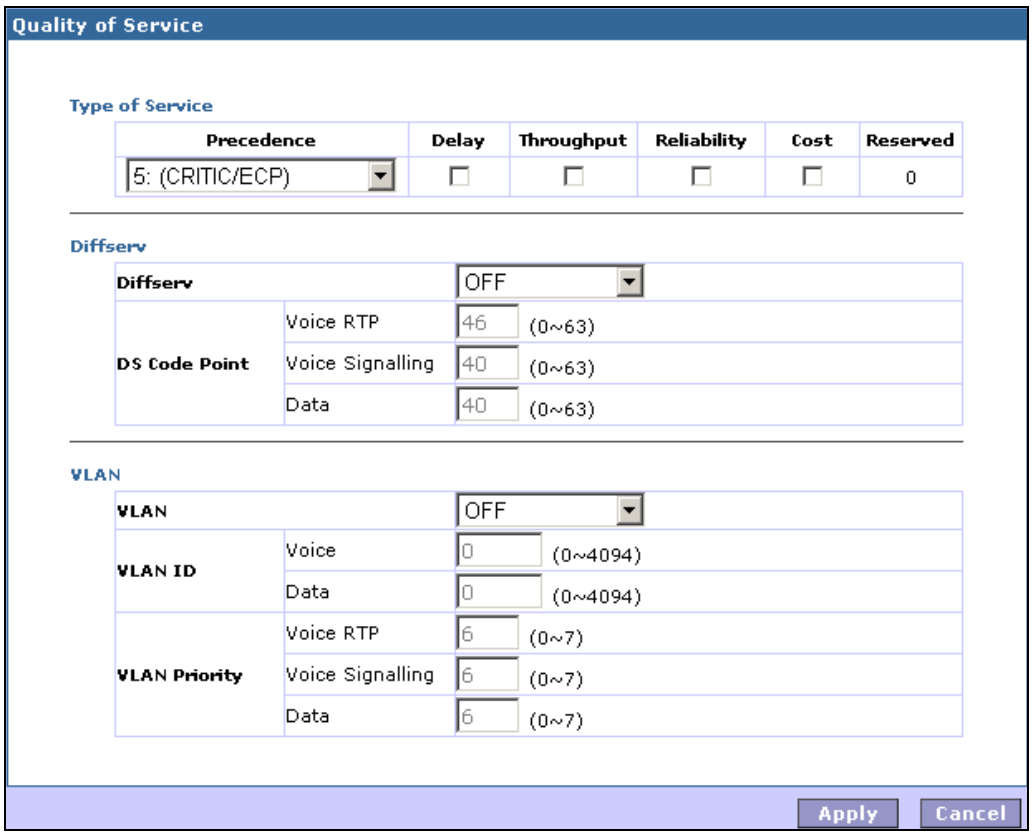
Reliability：To generate a High Reliability service parameter that will maximize reliability.

Cost：To generate a Low Monetary Cost service parameter that will minimize monetary cost.

When DiffServ function is disable, the VoIP gateway uses this setting as default for VOICE traffic.

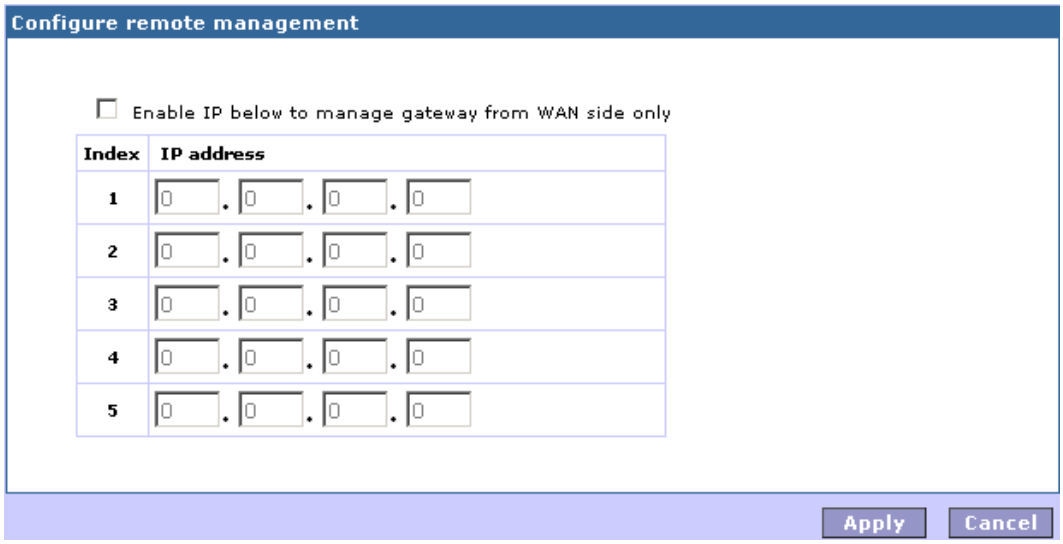
Diffserv setting：Specify the DS Code Point from 1~63 for each category. In the voice part, the voice packets are divided into two categories：one is for Voice, Voice band Data, Clear Channel Data and the other is used for GW to Call Agent Signaling & RFC2833/T38 signaling and the WAN interface management traffic Telnet/SNMP/HTTP. User can optionally choose to configure the Diffserv only for Voice or for both Voice and Data.

VLAN：The VoIP gateway supports software VLAN tag function. It can add VLAN tag for VOICE traffic only (VLAN Mode 1) or for both VOICE and DATA traffic (VLAN Mode 2). VOICE traffic can be classified into two classes: RTP (/RTCP) packets and signaling packets. Management traffic is defined as DHCP, Telnet, HTTP, and SNMP packets from WAN port, and is treated as VOICE signaling traffic. User can set different VLAN priority for different traffic class.



Remote Manage

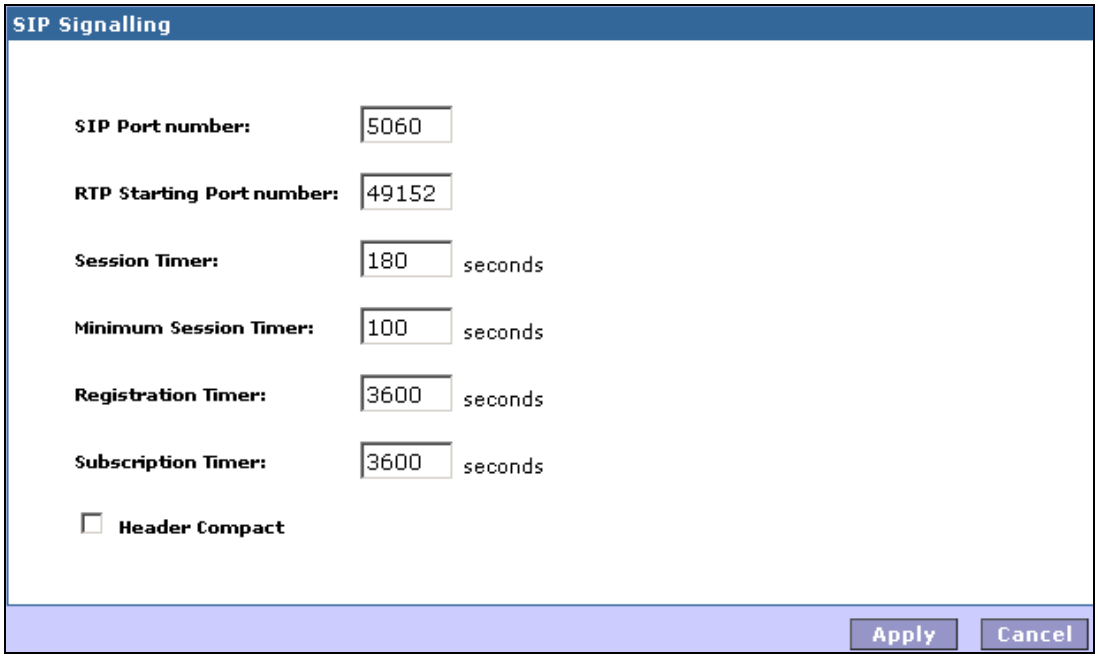
Remote management prevent from making change to the gateway's setting from WAN side except the specific five IP. While disable the function, user can login the gateway and change any setting from anywhere on the Internet.



5.4.2. Voice Setting

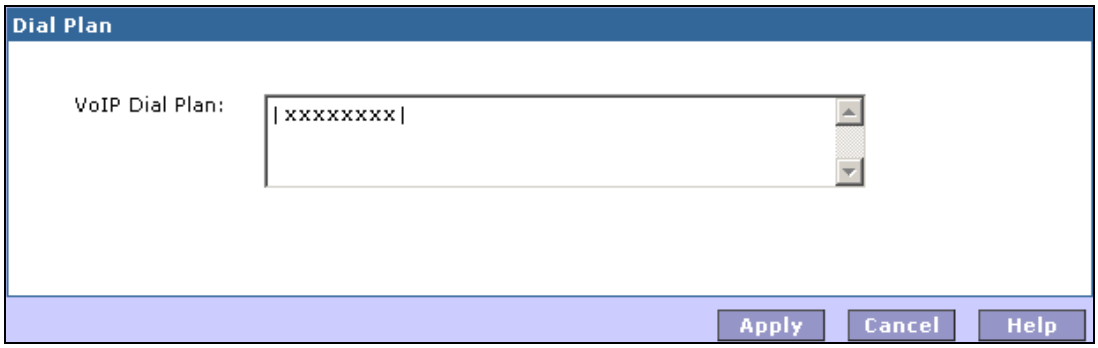
SIP Signaling

This page provides detail setting of SIP protocol.



Dial Plan

Setup VoIP dial plan to provide a rule for VoIP outgoing call.



Dial plan can be configured with following characters: **"0~9", "x", ".T", "|", "[ ]"**

- **"0-9"**: Digit can be configured with 0~9.
- **"x"**: Define how many digits can be used in dial plan.
- **".T"**: Digits will be sent after timeout. Without timeout character, digits will be sent immediately after finish dialing. (Default 3 sec.)
- **"|"**: To separate dial plan from others.
- **"[]"**: If digits can be configured in various type, we can use a square bracket to define this digit.

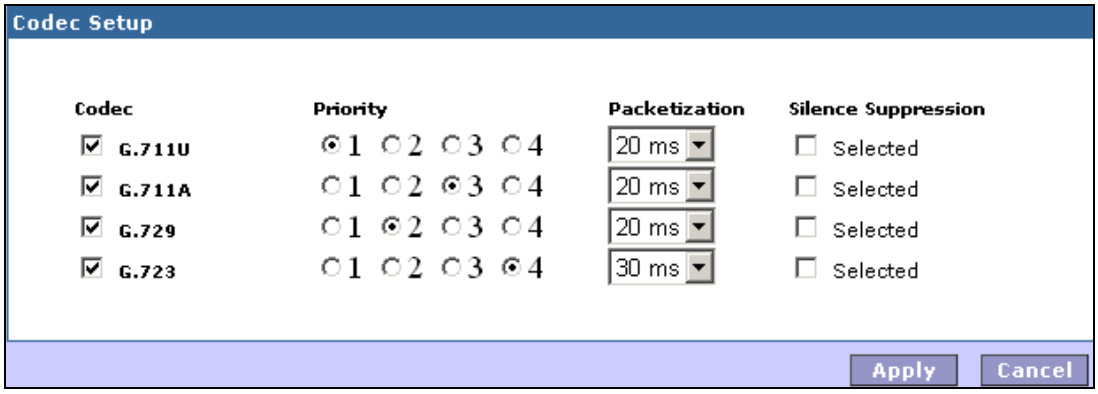
Ex. If we configure dial plan as **[1-3]xxxx|xxxx.T** then dial

(1) **1**4567 or **2**4567 or **3**4567, digits will be sent immediately after finish dialing.

(2) 4123 or 5123 or 61234, the front four digits will be sent after timeout.

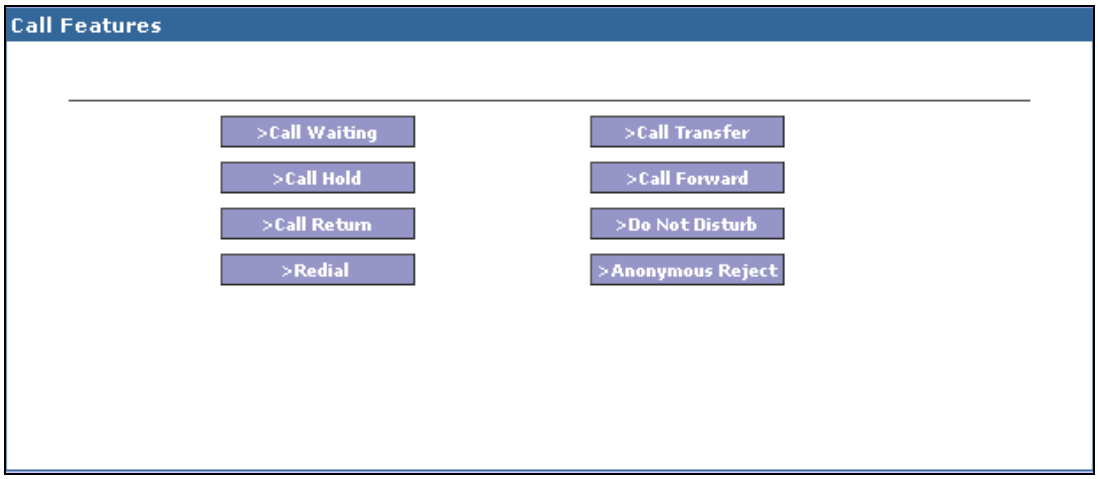
Codec Setup

Device provide G.711 μ, G.711A, G.729 and G.723 CODEC to transfer voice.

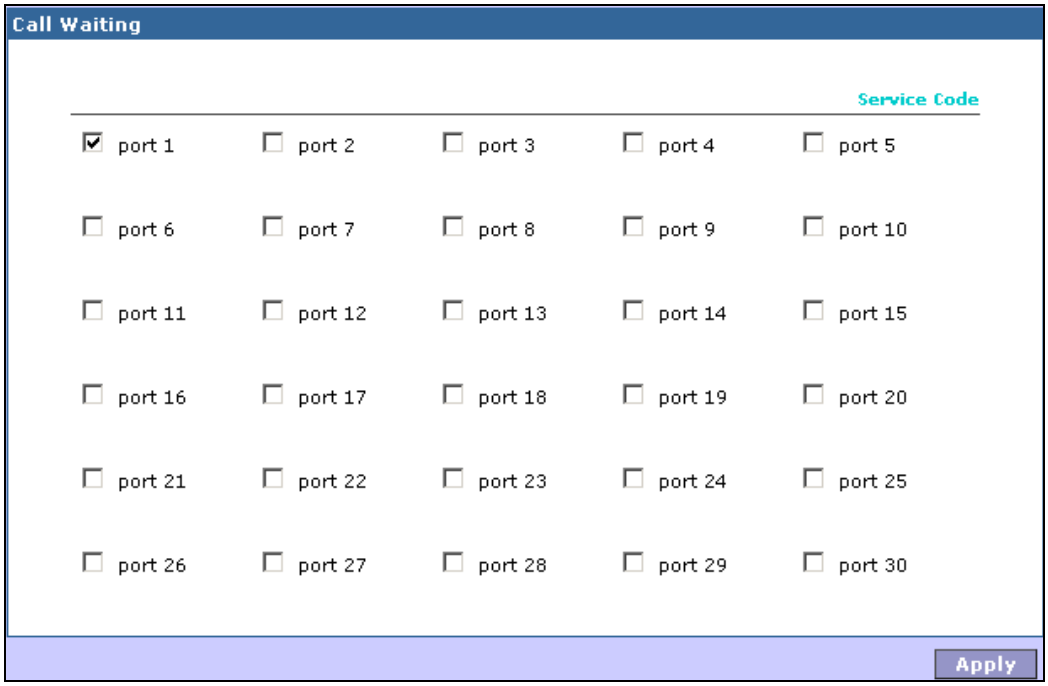


Call Features

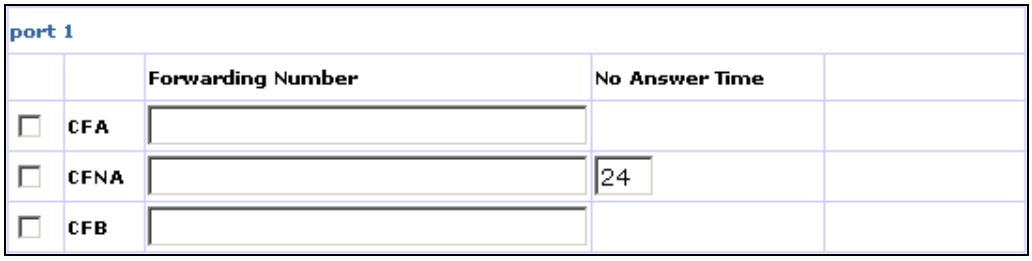
Device support call waiting, call hold, call return, redial, call transfer(CFNA, CFA, CFB), call forward, don't disturb and anonymous reject.



Device support call feature by port.



The forwarding number can entry by WEB, command and telephone



Service Code

This page displays the service code of call feature. User can refer this page to activate/ deactivate/ setting call features.

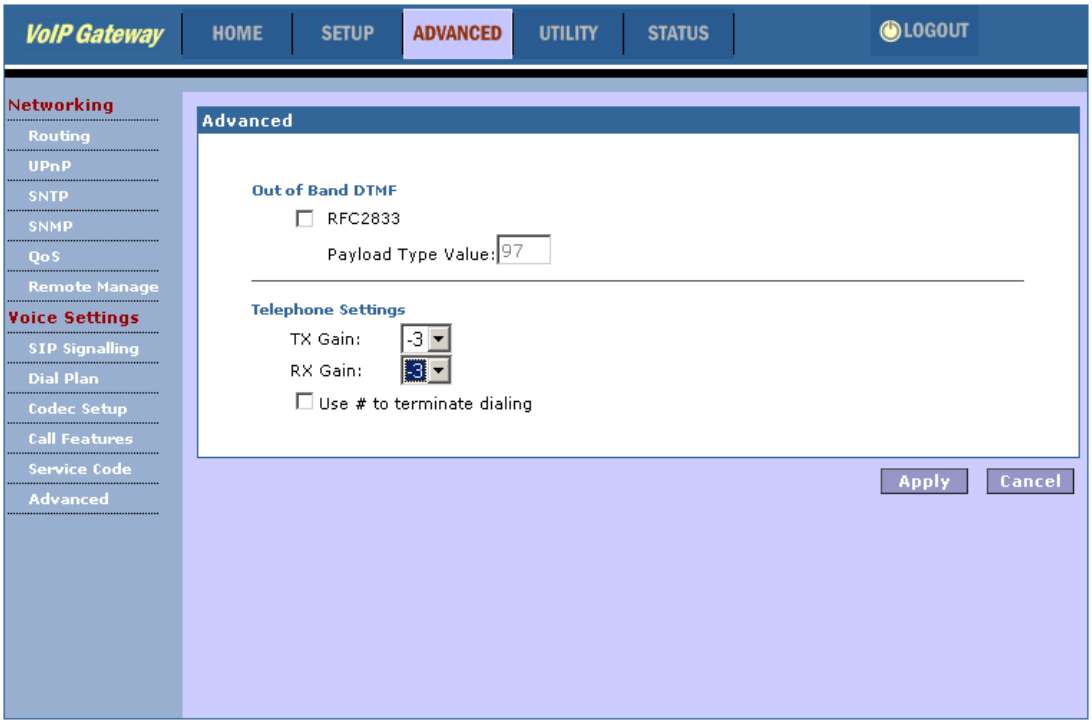
Service Code

Feature		Function	Service Code
Call Forwarding	1	Add Call Forwarding Address	*84
	2	Activate CFA	*88
	3	Deactivate CFA	*89
	4	Activate CFNA	*86
	5	Activate CFB	*87
	6	Deactivate CFNA and CFB	*85
Call Transfer	7	Activate Call Transfer	*57
	8	Deactivate Call Transfer	*56
	9	Attended call transfer dial prefix	*58
	10	unattended call transfer dial prefix	*59
Redial	11	Activate Redial	*71
	12	Deactivate Redial	*72
	13	Redial	*68
Do Not Disturb	14	Activate do not disturb	*47
	15	Deactivate do not disturb	*46
Anonymous Call Reject	16	Activate anonymous call reject	*49
	17	Deactivate anonymous call reject	*48
Call Hold	20	Activate Call Hold	*51
	21	Deactivate Call Hold	*50
Call Waiting	22	Activate Call Wait	*61
	23	Deactivate Call Wait	*60
Call Return	24	Activate Call Return	*53
	25	Deactivate Call Return	*52
	26	Call Return	*69

Apply

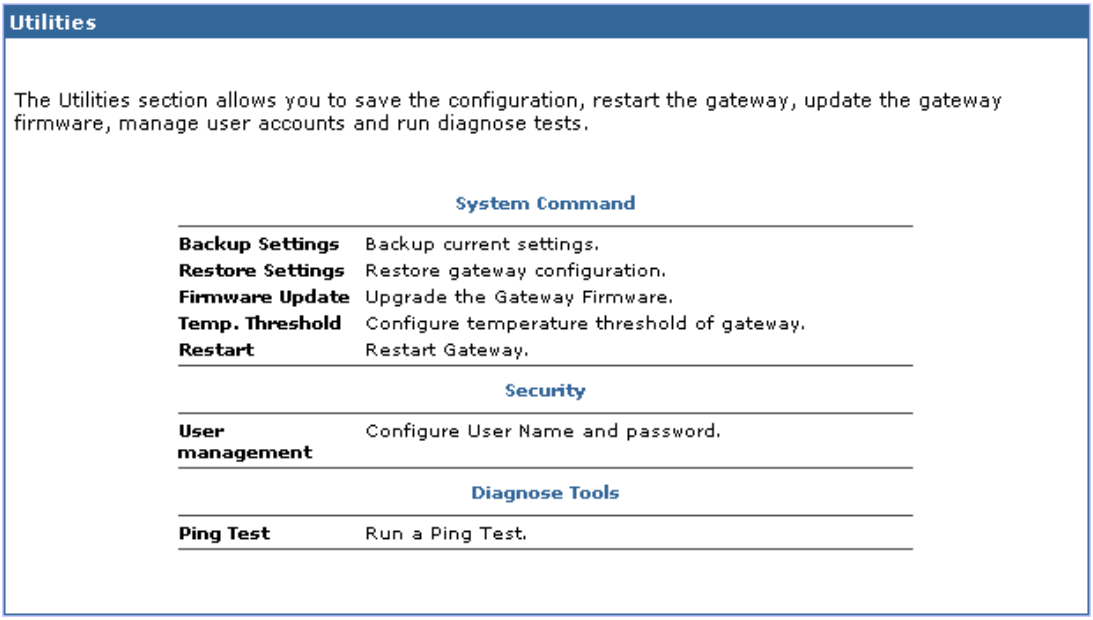
Advanced

Device support RFC2833 and gain control.



5.5 Utility

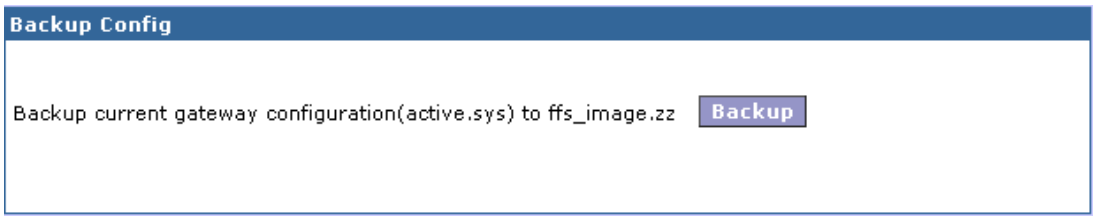
Device support configuration restore and backup, firmware upgrade, modify password and ping function in this page.



5.5.1. System Command

Backup Setting

Device support backup configuration via HTTP.

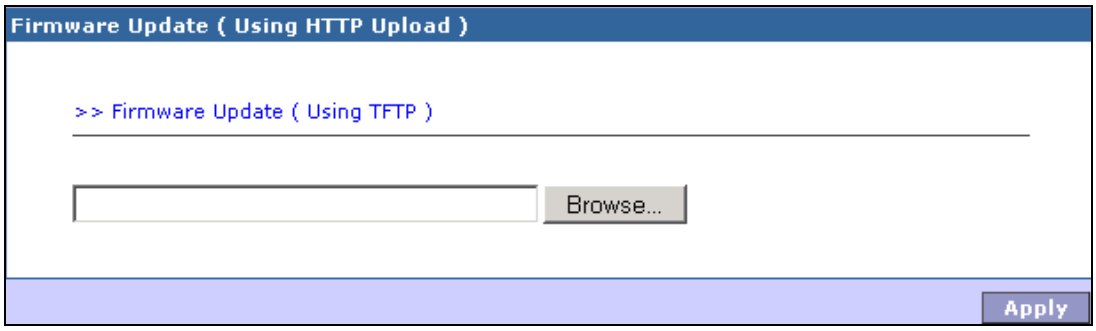


Restore Setting

Device support restore configuration via HTTP.

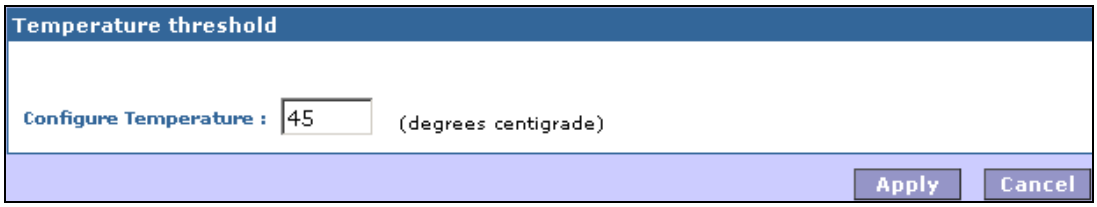
Firmware Update

Device support firmware upgrade via HTTP and TFTP.



Temp. Threshold

Device will send alarm trap to trap server, the system temperature over the threshold and send clear trap while system temperature under the threshold.



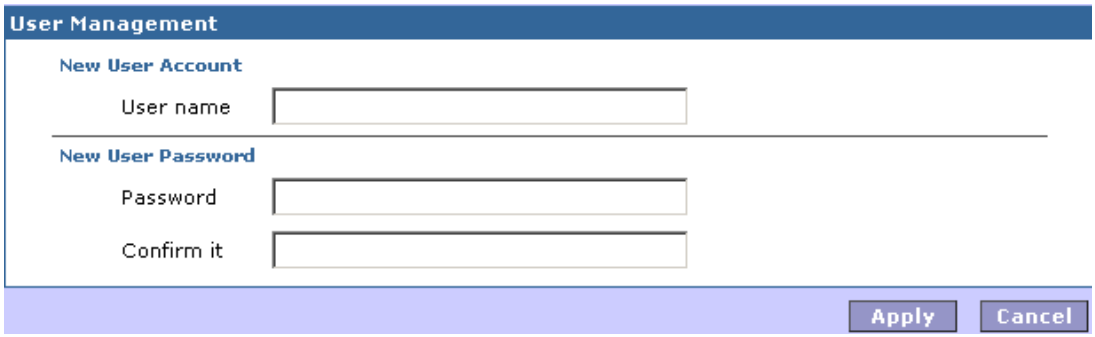
Restart

This page provide user to restart Device to reboot the system.

5.5.2. Security

User Management

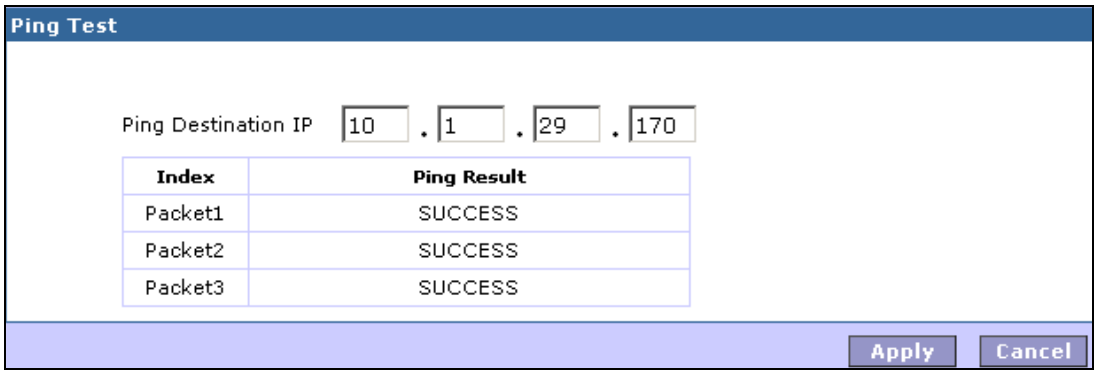
This page provide user to modify **User name** and **Password**.



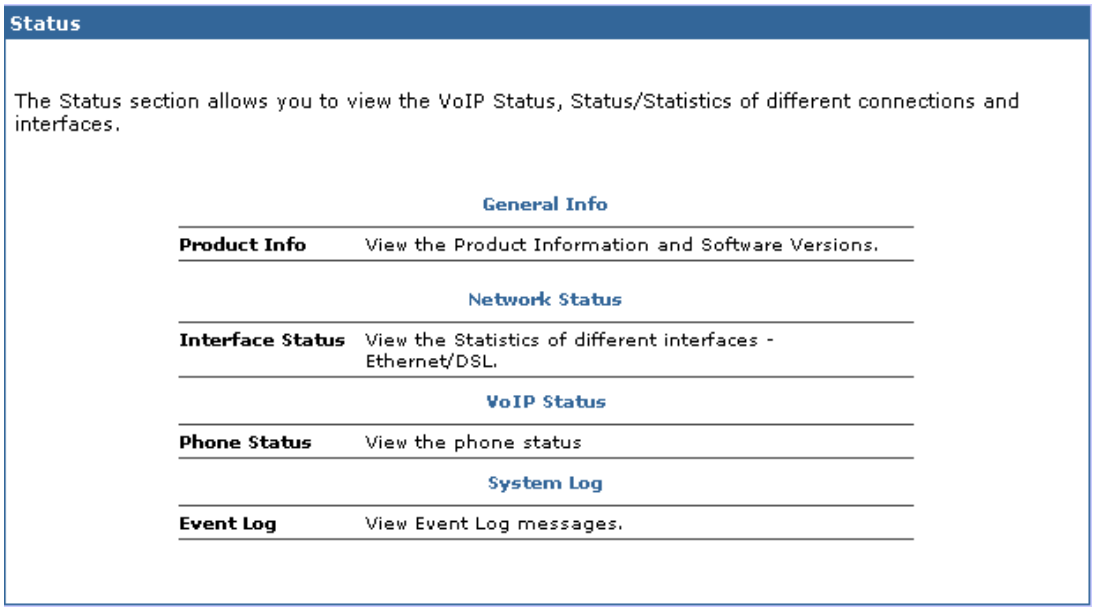
5.5.3. Diagnose Tools

Ping Test

This page provide user to ping other IP address to check the connection.



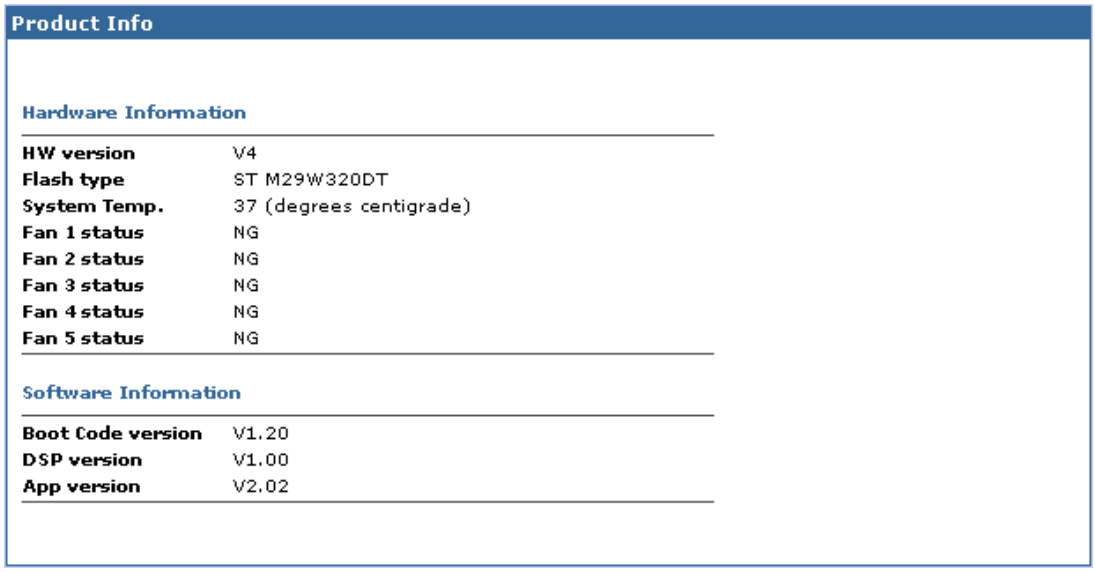
5.6 Status



5.6.1. General Info.

Product Info.

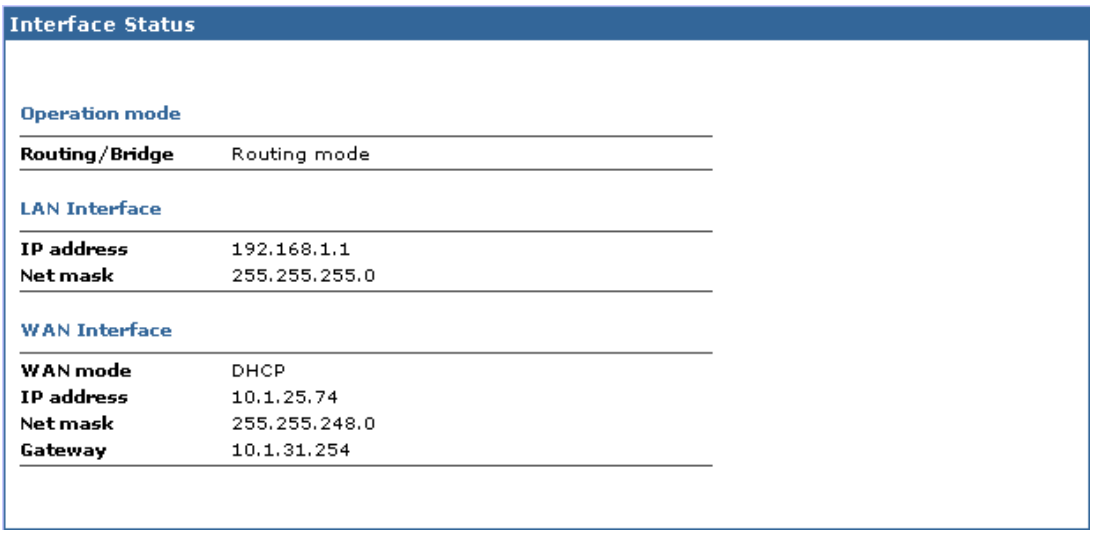
Device provide hardware and firmware information in this page.



5.6.2. Network Status

Interface Status

Device shown the system mode, LAN(CRAFT) and WAN interface information in this page.



5.6.3. VoIP Status

Phone Status

Device display VoIP port status in this page.

Phone Status

Service status

Registration Server Address	: 10.1.25.105
Proxy Server Address	: 10.1.25.105
Service Domain	: 10.1.25.105
SIP Port number	: 5060

Phone status

Port	Phone number	Caller ID Name	Status
Line 1	88880101	88880101	Registration OK
Line 2	88880102	88880102	Registration OK
Line 3	88880103	88880103	Registration OK
Line 4	88880104	88880104	Registration OK
Line 5	88880105	88880105	Registration OK
Line 6	88880106	88880106	Registration OK
Line 7	88880107	88880107	Registration OK
Line 8	88880108	88880108	Registration OK
Line 9	88880109	88880109	Registration OK
Line 10	88880110	88880110	Registration OK
Line 11	88880111	88880111	Registration OK
Line 12	88880112	88880112	Registration OK
Line 13	88880113	88880113	Registration OK
Line 14	88880114	88880114	Registration OK
Line 15	88880115	88880115	Registration OK
Line 16	88880116	88880116	Registration OK
Line 17	88880117	88880117	Registration OK
Line 18	88880118	88880118	Registration OK
Line 19	88880119	88880119	Registration OK
Line 20	88880120	88880120	Registration OK
Line 21	88880121	88880121	Registration OK
Line 22	88880122	88880122	Registration OK
Line 23	88880123	88880123	Registration OK
Line 24	88880124	88880124	Registration OK
Line 25	88880125	88880125	Registration OK
Line 26	88880126	88880126	Registration OK
Line 27	88880127	88880127	Registration OK
Line 28	88880128	88880128	Registration OK
Line 29	88880129	88880129	Registration OK
Line 30	88880130	88880130	Registration OK

5.6.4. System Log

Event Log

Device will keep 10 entries of event log in this page.

Status

Index	Date Time	Class	Level	Message
1	THU JAN 20 18:06:32 2005	SYSTEM	Alert	NTP: current time is THU JAN 20 18:06:32 2005
2	Up Time: 0 day, 00:00:17	TCPIP	Alert	Get IP from DHCP server
3	Up Time: 0 day, 00:00:15	SYSTEM	Info	System Startup, WAN IP:10.1.25.74
4	Up Time: 0 day, 00:00:10	TCPIP	Alert	WAN Interface Up
5	THU JAN 20 18:05:14 2005	SYSTEM	Alert	REBOOT
6	THU JAN 20 16:46:07 2005	SYSTEM	Alert	NTP: current time is THU JAN 20 16:46:07 2005
7	Up Time: 0 day, 00:00:16	TCPIP	Alert	Get IP from DHCP server
8	Up Time: 0 day, 00:00:14	SYSTEM	Info	System Startup, WAN IP:10.1.25.74
9	Up Time: 0 day, 00:00:10	TCPIP	Alert	WAN Interface Up
10	Up Time: 0 day, 00:37:26	SYSTEM	Alert	REBOOT

6 Command Line Interface (CLI)

Although the IAD is most conveniently to be configured and managed via the Web-based provisioning interface described in the previous chapter, it is also possible to use a text-based Command Line Interface (CLI). Certain advanced features of IAD are ONLY accessible by means of CLI. There are two ways to access the CLI interface of the IAD:

- Telnet (via standard telnet "port 23" to the IAD WAN or CRAFT port)
- Console (direct RS232 connection to a computer running a terminal emulation software)

6.1 CLI Connection

6.1.1. Connecting to the CLI via Telnet

The IAD can be accessed via Telnet from the provisioning computer within the Succession network to the IAD's WAN or local CRAFT interface. To configure via Telnet, launch telnet program that complies with the TCP/IP standard using Port 23 and connect to the IP address of the IAD.

6.1.2. Connecting to the CLI interface through the console port

Another way to invoke the CLI is to connect a terminal station such as a VT-100 or a PC based computer running terminal emulation program (such as HyperTerminal) connect to the RS-232 console port of the IAD. Use a 9-pin RS-232 cable to connect the device's console port to the serial COM port of the PC. Then configure the terminal with the following communication parameters:

- Baud rate: 115200 bps
- Data bits: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control: none

6.1.3. Login to the CLI interface

When logging on to the IAD, enter the appropriated Login ID and Password. The factory defaults are:

User Name: **admin**, Password: **admin**

User Name: **user**, Password: **user**

After successfully login, the prompt [login id]# will appear. The IAD allows up to 10 concurrent telnet sessions at the same time. If there is no command input for a period of time (pre-defined by command "net set telt <time in sec>"), telnet will be disconnected automatically.

Note: The CLI commands in telnet and console interface are the same. But the detail of the IAD initial boot up procedure can only be monitored via Console interface.

6.2 System Command

- **? / help**

Description: Show the first token of each command.

- **info**

Description: Show the IAD information.

- **delete config**

Description: Delete all setting in Device

- **activate**

Description: This command moves configuration data from the Temporary memory block to the Active area, where it can actually be used. Thus a user can make multiple changes in the Temporary memory using set commands, then active the changes by a single "activate" command. Configuration data in the Active area is only available while the IAD remains in operation. If the "reset" command is issued to reboot the device, or if the device is manually reset, the IAD will reload the pre-stored data from the non-volatile memory into the Active area.

- **commit**

Description: This command is used to save the currently active configuration data, invoked by the activate command, into the nonvolatile memory. If the reset command is issued, or if the device is manually reset, the IAD will reload the pre-stored data from the nonvolatile memory into the Active area.

Note: To activate any CLI command immediately, use the "activate" command after the CLI command without reboot the IAD. The activate command may only be used between calls; it usually tears down any calls in progress when it is invoked. To save the new configuration entered by any CLI command into the non-volatile memory, use "commit" command to save the setting. In other words, use both "active" and "commit" commands to ensure the new change will take effective permanently.

- **flash save**

Description: **activate** + **commit**.

- **reboot**

Description: Reboot the IAD.

- **version**

Description: Show the version of Boot code, DSP code and VoIP image.

- **sys show country**

Description: Show the Device's tone set.

- **sys set country (0~13)**

Description: Set the Device's country set(ringing and tone).

Country Types: 0 → US,
1 → Japan,
2 → Hong Kong,
3 → Australia,
4 → China,
9 → New Zealand,
10 → Europe

Example: net set country 0

- **logout**

Description: Logout from command line.

6.3 Set Password

- **net set id <Administrator ID>**

Description: Set the provision web/telnet/console interface access ID of administrator mode.

- **net show id**

Description: Show the provision web/telnet/console interface access ID of administrator mode.

- **net set pwd < Administrator Password>**

Description: Set the provision web/telnet/console interface access password of administrator mode.

- **net show pwd**

Description: Show the provision web/telnet/console interface access password of administrator mode.

- **net set uid <User ID>**

Description: Set the provision web/telnet/console interface access ID of user mode.

- **net show uid**

Description: Show the provision web/telnet/console interface access ID of user mode.

- **net set upwd <Password>**

Description: Set the provision web/telnet/console interface access password of user mode.

- **net show upwd**

Description: Show the provision web/telnet/console interface access password of user mode.

- **net set telt <0~240 seconds>**

Description: Set the period of time (sec) to terminate an inactive telnet session.

0→ no limit

- **net show telt**

Description: Show the period of time (sec) to terminate an inactive telnet session.

- **net set http_timeout <0~255 minutes>**

Description: Set the period of time (minute) to terminate an inactive HTTP session.

0→ no limit

- **net show http_timeout**

Description: Show the period of time (minute) to terminate an inactive HTTP session.

6.4 CRAFT (LAN) Interface

- **net set ip <xxx.xxx.xxx.xxx>**

Description: Set the IP address of the CRAFT (LAN) port.

Example: net set ip 192.168.1.1

- **net show ip**

Description: Show the IP address of the CRAFT (LAN) port.

- **net set mask <Net Mask>**

Description: Set the subnet mask of the CRAFT (LAN) port.

Example: net set mask 255.255.255.0

- **net show mask**

Description: Show the subnet mask of the CRAFT (LAN) port.

- **net show mac**

Description: Show CRAFT (LAN) MAC address.

6.5 WAN Interface

- **net set wan_mode <0: Fix IP / 1:DHCP / 2: PPPoE>**

Description: Enable or disable the DHCP client on the WAN port.

0 or fix → WAN Mode = Fixed IP.

1 or dhcp → WAN Mode = DHCP Mode.

2 or pppoe → Device not support PPPoE.

Example: net set wan_mode 1

- **net show wan_mode**

Description: Show WAN port's mode.

- **net set ipwan <IP Address>**

Description: Set the IP address of the WAN port when WAN port is fix IP mode.

Example: net set ipwan 192.168.2.1

- **net show ipwan**

Description: Show the IP address of the WAN port.

- **net set maskwan <Net Mask>**

Description: Set the subnet mask of the WAN port is fix IP mode.

Example: net set maskwan 255.255.255.0

- **net show maskwan**

Description: Show the subnet mask of the WAN port.

- **net set gateway <xxx.xxx.xxx.xxx>**

Description: Show the subnet mask of the WAN port.

Description: Set the default gateway IP address for the WAN port interface.

Example: net set gateway 192.168.2.254

- **net show gateway**

Description: Show the default gateway IP address of the WAN port interface.

- **net show macwan**

Description: Show WAN MAC address.

- **net set hostname <Host Name, Max 32 chars>**

Description: Set the hostname. When IAD request an IP address from DHCP server, the hostname will be filled in DHCP client's host name information.

Example: net set hostname DLINK

- **net show hostname**

Description: Show the DHCP client's host name.

- **net show wan_access**

Description: Show the WAN access mode.

- **net set wan_access [1|2]**

Description: Set the WAN access mode.

1 → Deny all access from WAN except to listed 5 entries.

2 → Allow all access from WAN. (Default value)

Example: net set wan_access 2

- **net show wan_access_ip**

Description: Show the WAN access IP entries.

- **net set wan_access_ip <0~4> (xxx.xxx.xxx.xxx)**

Description: Set the IP address which allows this specified address access from WAN port while WAN_access function is enable.

Please input "0.0.0.0" to remove this entry

Example: net set wan_access_ip 1 10.1.29.170

6.6 SIP Command

6.6.1.1. RFC2833

- **sip show 2833_rtp_pltype**

Description: Show the RTP payload type of RFC2833 packets.

- **sip set 2833_rtp_pltype (rtp payload type 97-127)**

Description: Set the RTP payload type of RFC2833 packets. The default value is 97.

- **sip show 2833flag**

Description: Show the RFC2833 flag.

- **sip set 2833flag [0(Disable) / 1(Enable)]**

Description: Enable or disable RFC2833. The default value is ON.

6.6.1.2. RFC3262

- **sip show 3262flag**

Description: Show the flag of RFC3262.

- **sip set 3262flag [0(Disable) / 1(Enable)]**

Description: Enable or disable RFC3262 PRACK. The default value is ON.

6.6.1.3. SIP Signaling

- **sip show branch**

Description: Show flag of branch ID.

- **sip set branch [0(Disable) / 1(Enable)]**

Description: Enable or disable the branch ID. The default value is OFF.

- **sip show domain**

Description: Show the service domain.

- **sip set domain <Max 31 chars, null to empty service domain>**

Description: Set the SIP service domain.

- **sip show pxy_srv**

Description: Show the Proxy server.

- **sip set pxy_srv (ip/ domaina name)**

Description: Set the Proxy server address.

Example: sip set pxy_srv 10.1.25.105

- **sip show reg_srv**

Description: Show the SIP Register server address.

- **sip set reg_srv <ip / domain>**

Description: Set the SIP Register server address.

Example: sip set reg_srv 10.1.25.105

- **sip show reg_mode**

Description: Show theSIP register mode.

- **sip set reg_mode <0(Auto refresh) / 1(Prohibition) / 2(peer2peer)>**

Description: Set the register mode.

0 → Auto register and refresh.

1 → Never send register to SIP server

2 → Peer to Peer Mode

- **sip show sip_port**

Description: Show the SIP port number.

- **sip set sip_port <1024 ~ 49152>**

Description: Set the SIP port number.

- **sip show tel_num <1~30>**

Description: Show the telephone number per port.

- **sip set tel_num <1~30> <Max 51 chars, null for empty telephone number>**

Description: Set the port number per port.

Example: sip set tel_num 1 88880101

- **sip show tel_name <1~30>**

Description: Show the caller ID.

- **sip set tel_name <1~30> <Max 15 chars >**

Description: Set the caller ID.

Example: sip set tel_name 1 jack

- **sip show reg_id <1~30>**

Description: Show the register ID.

- **sip set reg_id <1~30> <Max 31 chars>**

Description: Set the register ID if server required .

- **sip show reg_pwd <1~30>**

Description: Show the register password.

- **sip set reg_pwd <1~30> <Max 31 chars>**

Description: Set the register password if server required.

6.6.1.4. Voice CODEC

- **sip show codec_pri**

Description: Show CODEC priority.

- **sip set codec_pri <g711mu_pri> <g711a_pri> <g729_pri> <g723_pri>**

Description: Set the priority of CODEC.

Priority: 0 → Not Use

1 → First priority

2 → 2nd priorities

3 → 3rd priorities

4 → Last priority

Example: sip set codec_pri 2 1 3 0

6.6.1.5. Others

- **sip show idt**

Description: Show the inter digit timeout.

- **sip set idt <3~10 secs>**

Description: Set the inter digit timeout timer.

Example: sip set idt 4

6.7 DHCP Server

- **net set dhcpsrv <DHCP Server Flag [0 : 1 : OFF : ON]>**

Description: Set the DHCP server activation on the CRAFT (LAN) port.

Example:

net set dhcpsrv 0 → disable LAN(CRAFT) port DHCP server

net set dhcpsrv 1 → enable LAN(CRAFT) port DHCP server (**default**)

- **net show dhcpsrv**

Description: Show LAN(CRAFT) port DHCP server flag state.

- **net set dhcpsrvip <IP Address>**

Description: Set the first of the contiguous IP addresses to be assigned to the DHCP clients on CRAFT (LAN) port.

Example: net set dhcpsrvip 192.168.1.10

- **net show dhcpsrvip**

Description: Show the first of the contiguous IP addresses assigned to the DHCP clients on CRAFT (LAN) port.

- **net set dhcpipnum <1~253>**

Description: Set the maximum number of IP addresses to be assigned by the DHCP server.

Example: net set dhcpipnum 100

- **net show dhcpipnum**

Description: Show the maximum number of IP addresses assigned by the DHCP server.

- **net set dhcplease <DHCP Lease Time>**

Description: If the built-in DHCP server is enabled, set the DHCP server lease time in seconds.

Example: net set dhcplease 240

- **net show dhcplease**

Description: Show the DHCP server lease time.

- **dhcpserv show**

Description: Show the DHCP client's information of LAN(CRAFT) port.

6.8 DNS Server

- **net set dns <DNS Flag [0 : 1 : OFF : ON]>**

Description: Enable/disable the IAD's DNS proxy function.

Example:

net set dns 0 → disable DNS proxy

net set dns 1 → enable DNS proxy (default)

- **net show dns**

Description: Show the DNS proxy status of IAD.

- **net set dnsip pri <IP Address>**

Description: Set the primary DNS server IP address.

Example: net set dnsip pri 10.1.1.3

- **net set dnsip sec <IP Address>**

Description: Set the secondary DNS server IP address.

Example: net set dnsip sec 10.1.1.12

- **net show dnsip**

Description: Show all the DNS servers IP addresses.

- **net set dnsmode [0(From flash) /1(From network)]**

Description: Set DNS obtain method.

- **net show dnsmode**

Description: Show the DNS obtain method.

6.9 UPnP

- **upnp show**

Description: Show the current information of UPnP.

- **upnp set flag <flag: (1/3)>**

Description: Set the UPnP flag.

1 => Disable UPnP function.

3 => Support UPnP control point function.

6.10 Static Route

- **route add <Destination IP Address> mask <MASK> <Gateway IP Address>**

Description: Add a new route entry into the routing table.

Example: route add 192.168.2.0 mask 255.255.255.0 192.168.2.1

Note: The maximum number of route entry is 16.

- **route delete <Destination IP Address> <MASK>**

Description: Delete a route entry from the routing table.

Example: route add 192.168.2.0 255.255.255.0

- **route print**

Description: Show the entire routing table.

- **route print static**

Description: Shoe the static route entries.

6.11 SNMP

- **snmp set comm<1~3> <Community name> < read/write>**

Description: Set the SNMP community name, which is in fact the password used to access the SNMP Agent.

Example:

snmp set comm1 public → Set community name 1 is public with read access right.

snmp set comm2 private read → Set community name 2 is private with read access right.

snmp set comm3 abc write → Set community name 3 is abc with write access right.

Note: snmp set comm3 "" → Delete the community name 3.

- **snmp set filter < SNMP Filter Flag [0/ 1/ 2] >**

Description: Set the policy of SNMP traffic filtering.

0→ Filter all SNMP traffic

1→ Allow all SNMP traffic

2→ Allowing the specified SNMP managers

Example: snmp set filter 1

- **snmp set manager < SNMP Manager No : 1~5> <IP Address>**

Description: Set the IP address of the SNMP managers (1 – 5). Up to five SNMP Managers can be defined for Device.

Example: net set snmpmanager 2 192.168.1.10

Note: Set 0.0.0.0 To Delete SNMP Manager

- **snmp set trap <Trap Server IP Address>**

Description: Set the IP address of the SNMP trap server to send the SNMP traps to.

Example: snmp set trap 192.168.2.254

- **snmp show**

Description: Show the SNMP information, including the community names, SNMP manager filter information and Trap server IP.

6.12 Clone

- **clone <ip or mac>**

Description: Cloning the specified MAC address to WAN port MAC address.

Example: clone 00:90:96:11:22:33

- **clone show**

Description: Show the real and clone MAC address.

- **clone restore**

Description: Restore WAN port address to real MAC address.

6.13 DDNS (Dynamic DNS)

- **ddns show**

Description: Show the DDNS status and DDNS server information.

- **ddns set flag <flag(1(ON)/0(OFF))>**

Description: Set the DDNS status.

1 → Enable DDNS function.

0 → Disable DDNS function.

- **ddns set id <server 1/2> <id>**

Description: Set the DDNS ID.

Example: ddns set id 1 dlink

- **ddns set pwd <server 1/2> <pwd>**

Description: Set the DDNS password.

Example: ddns set pwd 1 dlink

- **ddns set host <server 1/2> <host name>**

Description: Set the DDNS hostname.

Example: ddns set host 1 dlink

- **ddns set srv <server 1/2> <server>**

Description: Set DDNS server address.

Device support DDNS server "**members.dyndns.org**" currently.

6.14 SNTP(TOD)

- **ntp show**

Description: Show the current user setting for TOD.

- **ntp set flag <NTP Flag [0 : 1 : OFF : ON]>**

Description: Set the NTP mode while system starts up.

0 or off → Disable NTP function.

1 or on → Enable NTP function.

- **ntp start**

Description: Enable the NTP client to obtain the system clock.

- **ntp stop**

Description: Disable the NTP client.

- **ntp time**

Description: Show the current time

- **ntp set ip <Time Server IP Address>**

Description: Set the NTP Server IP.

Example: ntp set ip 192.168.1.1

- **ntp set zone <GMT+/-XX:XX>**

Description: Set the time zone.

Example: ntp set zone +08:00

- **ntp set dst <on(1)/off(0)>**

Description: Enable/disable daylight savings time.

0 or off → No daylight savings time.

1 or on → Use daylight savings time.

6.15 QoS

- **net set vlan <VLAN Flag>**

0→ Disable VLAN

1→ Enable Voice VLAN

2→ Enable Data Access VLAN

Description: Enable/disable the VLAN function.

- **net show vlan**

Description: Show the VLAN flag.

- **qos show**

Description: Show the current setting for TOS (Type Of Service), VLAN (Virtual LAN) and Diffserv.

- **qos set tos <Value>**

Description: Set TOS (Type of Service). Each voice packet from the IAD will tag this value into the TOS field of its IP header if VLAN flag is disabled.

Value	Precedence	Delay	Throughput	Reliability	Cost	Reserved
0	000(Routine)	0	0	0	0	0
32	001(Priority)	0	0	0	0	0
64	010(Immediate)	0	0	0	0	0
96	011(Flash)	0	0	0	0	0
128	100(Flash Override)	0	0	0	0	0
160	101(CRITIC/ECP)	0	0	0	0	0
192	110(Internetwork Control)	0	0	0	0	0
224	111(Network Control)	0	0	0	0	0

Example: qos set tos 162 → CRITIC/ECP & Cost

- **qos set vid (voice/data) (0~4094)**

Description: Set the VLAN ID for voice or data. Each voice packet from the IAD will tag this value into VLAN ID field of the Ethernet header if VLAN is enabled.

- **qos set vtag (1/2/data) (0~7)**

Description: Set VLAN priority value. Each voice packet from the IAD will tag this value into VLAN tag field of the Ethernet header if VLAN is enabled.

Example: qos set vtag 1 5

- **net set dscp [0(Disable) / 1(Enable)]**

Description: Set DSCP flag to enable or disable DSCP.

- **net show dscp**

Description: Show the status of DSCP function.

- **qos set dscp (1/2/data) (0~63)**

Description: Set DiffServ code-point value. Each voice packet from the IAD will tag this value into the TOS field of IP header if DSCP is enabled.

<Category>:

1: for User Traffic Category 1.

Which is used for Voice, Voiceband Data, and Clear Channel Data.

2: for User Traffic Category 2.

Which is used for IAD to Call Agent signaling & RFC2833/T.38 Signaling.

6.16 IP Packet Filter Configuration

- **net set ipfilter <IP Packet Filter Flag [0 : 1 : OFF : ON]>**

Description: Enable/disable the IP packet filter function.

Example:

net set ipfilter 0 → disable IP packet filter function

net set ipfilter 1 → enable IP packet filter function

- **net show ipfilter**

Description: Show the IP packet filter flag (ON/OFF).

- **ipfilter add <IP Address> <DA/SA> <Direction> <Protocol>**

Description: Add an IP packet filter item into the IP packet filter table.

<DA/SA>: Specifies whether the designated IP address is DA or SA in the packet (0/DA; 1/SA).

<Direction>: Specifies whether the designated IP address is from LAN, WAN or both (WAN/0; LAN/1; Both/2).

<Protocol>: Specifies whether which protocol of the designated IP address is in the packet (0/None; 6/TCP; 17/UDP).

- **ipfilter del <IP Address>**

Description: Delete an IP packet filter entry from the IP packet filter table.

- **ipfilter print**

Description: Show all IP packet filter entry.

6.17 MAC Packet Filter Configuration

- **net set macfilter [0(Disable) / 1(Enable)]**

Description: Enable/disable the MAC filter function.

Example:

net set macfilter 0 → disable MAC packet filter function

net set macfilter 1 → enable MAC packet filter function

- **net show macfilter**

Description: Show the MAC packet filter flag (ON/OFF).

- **macfilter add <MAC Address>**

Description: Add an MAC packet filter entry to the MAC filter table.

- **macfilter del <MAC Address>**

Description: Delete an MAC packet filter entry from the MAC filter table.

- **macfilter print**

Description: Show all MAC packet filter entry.

6.18 NAPT Configuration

- **net set nat <NAPT Flag [0 : 1 : OFF : ON]>**

Description: Enable/disable the NAPT function.

- **net show nat**

Description: Show the NAPT flag (ON/OFF).

- **napt add <local ip> <sp> <ep> <protocol:TCP(6)/UDP(17)> <enable> <sp2> <ep2> <descript ion (max length=50)>**

Description: Add the specified IP address on the LAN port to NAPT proxy list with specified port number and protocol type.

Example: napt add 192.168.1.101 21 30 TCP 1 101 120 test_entry

- **napt del <local ip> <start port> <end port> <protocol:TCP(6)/UDP(17)>**

Description: Remove the specified IP address on the LAN port on the NAPT proxy list.

- **napt print <all/tcp/udp/icmp>**

Description: Show the NAPT specified proxy list.

- **napt static**

Description: Show the NAPT entries.

- **napt show**

Description: Show NAPT information and status.

6.19 RIP

- **net set rip <RIP Flag [0 : 1 : 2]>**

0 → Disable.

1 → Support RIP1.

2 → Support RIP2.

Description: Set RIP function.

- **net show rip**

Description: Show the RIP function status.

- **rip**

Description: Show the RIP entries.

6.20 Monitor

6.20.1. Hardware Status

- **monitor show**

Description: Show system temperature, temperature threshold and fan status.

- **monitor set temp <Temperature Threshold in centigrade [0~70]>**

Description: Set the temperature threshold to send alarm trap to Trap server.

6.20.2. Event Log

- **event print <start-index> <count>**

Description: Print <Count> event log entries from <Start-Index>.

Example: event print 1 10

- **event reset**

Description: Reset event log (clear all existing event log entries)

6.20.3. ARP Table

- **arp –a**

Description: Display the current ARP table.

- **arp -s <IP Address> <MAC Address>**

Description: Add an ARP entry into the ARP table.

Example: arp –s 192.168.1.1 AA:BB:CC:11:22:33

- **arp –d <IP Address>**

Description: Remove an ARP entry from the ARP table.

Example: arp –d 192.168.1.1

- **arp –t**

Description: Flush all entries in the system ARP table.

6.20.3.1. Routing Table

- **route print**

Description: Display the routing table of the IAD.

6.20.3.2. IP packet filter Table

- **ipfilter print**

Description: Show the IP packet filter table.

6.20.3.3. MAC Filter Table

- **macfilter print**

Description: Show the MAC filter table.

6.21 Caller ID Display

- **sip show show_cid**

Description: Show the flag of caller ID.

- **sip set show_cid [0(Disable)/ 1(Enable)]**

Description: Enable or disable the caller ID function.

- **sys show callerid**

Description: Show the caller ID display mode.

- **sys set callerid <0~3>**

Description: Set the caller ID display mode.

0→ During Ringing(North America/ Europe)

1→ DT-AS(Europe)

2→ RP-AS(Europe)

3→ LR+DT-AS(Europe)

6.22 Utility

6.22.1. Ping Test

- **ping <X.X.X.X> [-t|-n <Count>]**

Description: It is used to confirm access to a network IP address.

-t → Ping the specified host until stopped. To stop, press **Control**-**C** (console login).

-n Count → Count number of echo requests to send.

Example: ping 192.168.2.1

6.22.2. Software Upgrade

- **ftp2 putimage X.X.X.X filename [f/F]**

Description: Dump all flash data into one file via FTP.

F: Force disconnects the conversation and upgrades the image.

- **tftp X.X.X.X filename [f/F]**

Description: Download the Boot Code, DSP code or Application Code file via TFTP.

F: Force disconnects the conversation and upgrades the image.

Example: tftp 10.1.29.170 DVG-2030S_v201_ap.zz

- **tftp2 putimage X.X.X.X filename [f/F]**

Description: Dump all flash data into one file via TFTP.

F: Force disconnects the conversation and process the procedure.

- **ftp <host> <file> [f/F]**

Description: Download the Boot Code, DSP code or Application Code file via FTP.

F: Force disconnects the conversation and upgrades the image.

- **httpdl <server ip> <filename>**

Description: Download the Boot Code, DSP code or Application Code file via HTTP.

6.23 Loop Test Feature

This section describes how to use the **loop** command to perform remote diagnosis on the copper loop wiring. The operator can use this function to test the conditions of the:

- Resistance Measurements
- Voltage Measurements
- Capacitance Measurements
- Current Measurements
- GR909 TEST

6.23.1. Resistance Measurements

- **loop lt <command> <chn> [<t>]**

Command:

ltr	(chn)	: Resistance Ring-Tip (time = 0ms)
ltr_rt	(chn,t)	: Resistance Ring-Tip
ltr_rg	(chn,t)	: Resistance Ring-Ground
ltr_tg	(chn,t)	: Resistance Tip-Ground
ltr_ohk	(chn)	: Resistance Off-Hook

chn: Channel number (0,1,2,3,..)

t: Settling time (ms)

6.23.2. Voltage Measurements

- **loop lt <command> <chn>**

Command:

ltvf_rtd	(chn)	: Foreign Voltage Ring-Tip (DC)
ltvf_rta	(chn)	: Foreign Voltage Ring-Tip (AC)
ltvf_rgd	(chn)	: Foreign Voltage Ring-Ground (DC)
ltvf_rga	(chn)	: Foreign Voltage Ring-Ground (AC)
ltvf_tgd	(chn)	: Foreign Voltage Tip-Ground (DC)
ltvf_tga	(chn)	: Foreign Voltage Tip-Ground (AC)
ltvd_rtd	(chn)	: Feeded Voltage Ring-Tip (DC)
ltvd_rgd	(chn)	: Feeded Voltage Ring-Ground (DC)
ltvd_tgd	(chn)	: Feeded Voltage Tip-Ground (DC)
ltvr_rtd	(chn)	: Ring Voltage Ring-Tip (DC)
ltvr_rta	(chn)	: Ring Voltage Ring-Tip (AC)
ltvr_rgd	(chn)	: Ring Voltage Ring-Ground (DC)
ltvr_rga	(chn)	: Ring Voltage Ring-Ground (AC)

ltvr_tgd (chn) : Ring Voltage Tip-Ground (DC)

ltvr_tga (chn) : Ring Voltage Tip-Ground (AC)

ltvb_vdd (chn) : Battery Voltage VDD

chn: Channel number (0,1,2,3,..)

6.23.3. Capacitance Measurements

- **loop lt <command> <chn>**

Command:

ltc_rt (chn) : Capacitance Ring-Tip

ltc_rg (chn) : Capacitance Ring-Ground

ltc_tg (chn) : Capacitance Tip-Ground

chn: Channel number (0,1,2,3,..)

6.23.4. Current Measurements

- **loop lt <command> <chn> [<f> <t>]**

Command:

lita (chn) : Transversal Current AC

lila (chn) : Longitudinal Current AC

litd (chn) : Transversal Current DC

lild (chn) : Longitudinal Current DC

lid (chn) : Leakage Current DC

lisetf (chn,f) : Set Ring Frequency (Hz)

lisets (chn,t) : Set Settling Time (ms)

liset (chn,f,t) : Set Ring Frequency (Hz) and Settling Time (ms)

liget (chn) : Get Ring Frequency (Hz) and Settling Time (ms)

chn: Channel number (0,1,2,3,..)

t: Settling Time (ms)

f: Frequency (Hz)

6.23.5. GR909 TEST

- **loop lt gr909 <channel> <0~5>**

chn: Channel number (0,1,2,3,..)

0 : LTEST_GR909_HAZARDOUS_VOLTAGE

1 : LTEST_GR909_FOREIGN_FORCE

2 : LTEST_GR909_RESISTIVE_FAULT

3 : LTEST_GR909_RECEIVER_OFF_HOOK

4 : LTEST_GR909_RINGER

7 Network Management

This chapter introduces the SNMP design of the Device. It supports standard RFC1213 MIB, and the proprietary MIB described in the chapter. The Device can also be interoperable with powerful IAD EMS server acts like network management and operation support systems.

Before using Device SNMP feature, please refer SNMP configuration.

7.1 mtaFirmwareGroup

mtaFirmwareGroup contains five MIBs.

- mtaVoIPImageVersion

The MIB is to get mta VoIP image version.

- mtaBootCodeVersion

The MIB is to get mta boot code image version.

- mtaDSPImageVersion

The MIB is to get mta DSP image version.

- mtaFirmwareUpgrade

This MIB, mtaFirmwareUpgrade, provides a function for software upgrade. Its format is "tftp://IPv4/filename". If administrator uses SNMP "set" a new filename in the TFTP server address, then GW downloads the software from the specified location "IPv4". And IAD will update the firmware after operator to reboot it via another MIB. However, If there is any active call in progress, the software upgrade process will abort. Therefore, if you agree to interrupt the service please add option 'F' or 'f' as the TFTP command suffix to force the software upgrade process, e.g., "tftp://IPv4/filename f". The filename MUST be in the format below.

- **Application Code: xxx_ap.zz**
- **Boot Code: xxx_bc.zz**
- **DSP Code: xxx_dsp.zz**

- mtaFirmwareUpgradeResultGroup

The MIB is to get the latest result of mta firmware download. If the upgrade process is successful, the object displays the downloaded file name. If the upgrade process is unsuccessful, the object displays "fail". The upgrade result will not be kept in Flash memory, which means that the MIB will get empty result (Null) after the IAD boots up.

- mtaVoIPUpgradeResult

There are three situations caused different MIB results.

9. When the IAD just boots up, This MIB will get empty result (Null).
10. When the IAD upgrades successfully, IAD will reboot automatically.
11. When the IAD upgrades unsuccessfully. This MIB will get mta VoIP image upgrade result.

- mtaBOOTCODEUpgradeResult

The MIB is to get mta Boot code upgrade result, no matter it's successful or failure.

- mtaDSPUpgradeResult

The MIB is to get mta DSP image upgrade result, no matter it's successful or failure.

- mtaTELCFGUpgradeResult

The MIB is to get mta Telcfg file upgrade result, no matter it's successful or failure.

7.2 mtaControlsGroup

mtaControlsGroup contains MIBs: mtaResetNow, mtaResetToDefault, mtaSaveAsDefault, mtaTemperatureThreshold, mtaTemperature, mtaFan1Status and mtaFan2Status.

- mtaResetNow

Set the value to (2) or (3) causes IAD to reboot. Read it always returns (0) or (1). When mtaResetNow is set to true, the following actions occur:
(1) All connections are flushed locally.
(2) All current actions, such as ringing, terminate immediately if reboot successfully.
(3) Requests for notifications, such as notification based on digit map recognition, are flushed if reboot successfully
(4) All endpoints are disabled if reboot successfully.

(5) The box reboot and send warm reboot trap.

Value:
0 -- Normal (Initial value, IAD start up status, this value only for SNMP get)
1 -- Reboot abort ! (After reseting and abort due to call on progress, this value only for SNMP get)
2 -- Reboot (Reboot, this value only for SNMP set)
3 -- Forced reboot (Reboot immediately, even if call on progress, this value only for SNMP set)

- mtaResetToDefault

Set this object true(1) causes the device to be reset to default.

Read this object always returns false(2).

- mtaSaveAsDefault

Set this object true(1) causes the current configurations to be saved as default.

Read this object always returns false(2).

7.3 mtaVoiceInterfaceGroup

mtaVoiceInterfaceGroup contains as following:

- voiceVAD

Set this object enable(1) enable the silence suppression function.

Set this object disable(0) disable the silence suppression function.

- voiceSoftSwitchLedStatus

Off(0), Flash(1), On(2)

- sipRegisterServer

Set and read SIP register server from this mib for a SIP call.

- sipProxyServer

Set and read SIP register server from this mib for a SIP call.

- sipTelNumberTable

Set and get telephone number of IAD. SipTelNumberTable includes telNumIndex and sipTelNumber. You can use "TableView" to list the "sipTelNumberEntry".

- sipRegisterIDTable

Set and get register ID of IAD. SipRegisterIDTable includes sipRegIDIndex and sipRegisterID. You can use "TableView" to list the "sipRegisterIDEntry".

- sipRegisterPwdTable

Set and get register PWD of IAD. SipRegisterPwdTable includes sipRegPwdIndex and sipRegisterPwd. You can use "TableView" to list the "sipRegisterPwdEntry".

7.4 mtaSystemModeGroup

mtaSystemModeGroup only contains a MIB:

- systemMode.

The MIB, systemMode, specifies the operation mode of GW between router mode(0) and bridge mode(1). If your network consists of only one or two networks using the same protocol and the traffic is not heavily loaded, we may configure GW as bridge. Otherwise, we would need to set GW to act as a router for better performance.

- modelType

To be define.

7.5 mtaWANInterfaceGroup

mtaWANInterfaceGroup contains MIBs: wanIPAssignment, wanIPAddress, wanSubnetMask, wanDefaultGateway, and wanMACAddress.

- wanIPAssignment

Set this object staticIP(0) such that WAN IP address is static.

Set this object dhcp(1) such that WAN IP address is from DHCP server.

- wanIPAddress

Set or get the IP address of the WAN interface of GW.

- wanSubnetMask

Set or get the subnet mask of the WAN interface of GW.

- wanDefaultGateway

Set or get the IP address of the default gateway.

- wanMACAddress

Set or get the WAN MAC address.

7.6 mtaLANInterfaceGroup

mtaLANInterfaceGroup contains MIBs: lanIPAddress and lanSubnetMask.

- lanIPAddress

The IP Address of the LAN interface of GW.

- lanSubnetMask

The subnet mask of the LAN interface of GW.

7.7 mtaDHCPServConfigurationGroup

mtaDHCPConfigurationGroup contains MIBs: dhcpDHCPServerOn, dhcpStartAssignedIP, dhcpAssignedIPCount, and dhcpLeaseTime.

- dhcpDHCPServerOn

Only available when IAD is configured in the router mode, GW may act as the DHCP server over the LAN interface. If we set dhcpDHCPServerOn to ON(1), then the DHCP server function of GW is opened, and vice versa.

- dhcpStartAssignedIP

If DHCP server is set to be ON, specify the first of the contiguous IP addresses to be assigned to client machines on our LAN.

- dhcpAssignedIPCount

Specify the number of IP addresses to be assigned, if GW act as DHCP server.

- dhcpLeaseTime

The lease time of DHCP server, if GW acts as DHCP server.

These MIBs above are only accessible on the router mode.

7.8 mtaNATConfigurationGroup

GW supports NAT function for translating private IP addresses to public IP addresses.

- natNATOn

This allows PCs on the LAN to access the public Internet. The MIB, natNATOn, is the only one in the mtaNATConfigurationGroup. It can be set to enable/diable the NAT function.

This MIB, natNATOn, is only accessible on the router mode.

7.9 mtaDNSConfigurationGroup

mtaDNSConfigurationGroup contains three MIBs: dnsDNSServerOn and dnsDNSServerPrimary, dnsDNSServerSecondary.

- dnsDNSServerOn

If set this MIB to ON(1), then GW will act as DNS server proxy. DNS server proxy will forward the DNS requests to DNS server for PCs on the LAN.

- dnsDNSServerPrimary

The IP address of primary DNS Server.

- dnsDNSServerSecondary

The IP address of primary DNS Server

These MIBs above are only accessible on the router mode.

7.10 mtaRIPConfigurationGroup

mtaRIPConfigurationGroup only contains a MIB:

- ripRIPMode

It has three values: disable(0), RIP1(1), and RIP(2). RIP provides consistent routing and reachability information among routers on their local networks. The differences between RIP1 and RIP2 are authentication and subnet recognition.

This MIB, ripRIPMode, is only accessible on the router mode.

7.11 mtaSNMPConfigurationGroup

mtaSNMPConfigurationGroup contains six MIBs: snmpTrapServer, snmpCommunityName1, snmpCommunityName2, snmpCommunityName3 and TrapLevel.

- snmpTrapServer

We can set IP address of trap server through the MIB. All SNMP traps that are from GW will send to this location.

- snmpCommunityNameX (X = 1, 2, 3)

On SNMPv1 and SNMPv2, if element manager would like to access GW through SNMP, the community string of it must be identical with the one of GW. We provide three community strings for administrator to set. You can set the community to both read and write in the 1004S-FXO and 1004S-FXS.

- snmpTrapLevel

To minimize the traffic from the IAD traps messages impact to network performance. Administrator is allowed to set five levels of trap levels to determine what kind of the traps can be delivered from IAD.

0: enable all Traps including the warning Trap.

1: enable critical, major, and minor Traps.

2: enable the critical and major Traps.

3: enable critical Traps.

4: disable all Traps.

7.12 mtaPortStatusGroup

mtaPortStatusGroup includes PortIndex and PortStatus. You can use "TableView" to list the "PortStatusTableEntry".

- portIndex

Read Only. The MIB show how many port in the box. You need to use "WALK" to get the return value.

- portStatus

Read Only. The MIB is used to report currently line status, includes "on-hook", "off-hook", "power ringing" and "port disable". You need to use "WALK" to get the return values.

7.13 Summary

MIB	Group	Support
MIB-II (RFC1213 compliant)	System	Yes
	Interface	Yes
	At	No
	IP	Yes
	ICMP	Yes
	TCP	Yes
	UDP	Yes
	Egp	No
	SNMP	Yes
Private MIBs	mtaFirmwareGroup	Yes
	MtaControlsGroup	Yes
	mtaVoiceInterfaceGroup	Yes
	mtaSystemModeGroup	Yes
	mtaWANInterfaceGroup	Yes
	mtaLANInterfaceGroup	Yes
	mtaDHCPServConfigurationGroup	Yes
	mtaNATConfigurationGroup	Yes
	mtaDNSConfigurationGroup	Yes
	mtaRIPConfigurationGroup	Yes
	mtaSNMPConfigurationGroup	Yes
	mtaPortStatusGroup	Yes

7.14 SNMP version 2.1- Traps

The following TRAPs are supported in SNMP design release 2.1. The trap is SNMP v1 based, so any of the SNMP trap server should be able to read the traps sent from IAD.

1. All the trap message should send via WAN interface to assigned trap server only
2. Trap message format: Binding info should include "Trap Level + Module name & VoIP firmware version + IAD Source IP address + Box name + Trap description".

We assigned Trap ID for each type of IAD trap, Generic ID is follow standard SNMP trap category, and Specific Trap is used to identified by Enterprise level trap.

Trap Type	Condition to release TRAP	Trap Level	*Generic ID	*Specific ID	Model support
ColdStart	After turning on the power ON or resetting SW	1 (Critical)	0	0	ALL
WarmStart	Soft reset (reboot from web/telnet/console)	2 (Major)	1	0	ALL
AuthenticationFailure	When Receiving a SNMP message which include an unrecognized community When console/telnet/http connection fail in login ID/password	2 (Major)	4	0	ALL
LossCommunication	While IAD receive error code 500/900 or no response from Proxy server with timeout	1 (Critical)	6	0	ALL
	Clear Trap while IAD receive 2xx code	5 (Clear)	6	0	
FirmwareUpgradeSuccess	Upgrade the firmware successful, also bind with firmware version name	3 (Minor)	6	4	ALL
FirmwareUpgradeFailure	AD send trap if the TFTP software download is not finished within certain period of time It may caused by the following reasons: - Image name is not correct. - Invalid TFTsP IP address - Image Type Error - Image header CRC error - Flash programming fail - Checksum check fail - Call in progress was detect, the TFTP download was given up.	2 (Major)	6	5	ALL
TrafficWarning	1. WAN port traffic busy	1 (Critical)	6	6	ALL
	2.Clear Trap when the Traffic Busy problem become normally	5 (Clear)	6	6	
ConnetToProxyServer	1. When IAD can not connection to the Proxy Server.	1 (Critical)	6	7	ALL
	2. When IAD connect to the Proxy Server	5 (Clear)	6	7	ALL
ConfigurationChange	When the IAD key configuration is changed	4 (Warning)	6	10	ALL

Notes:

- **Loss Communication** Trap and Clear Trap format

LossCommunication and SIP transient error
1) While IAD receive error code 500/900 or no response from Proxy Server
Format: *[Direction] [Line Number] [Error_Code*] [reason]*
e.g. "GWC->GW Line 0 503 The server is unavailabel. "
2) Clear Trap while IAD receive 2xx
Format: *[Direction] [Line Number] [Error_Code*] [reason]*
e.g. "GWC->GW Line 0 503 The server is unavailable."

Notes:

The table below lists that the IAD can provide error messages. For additional error messages such as some 5xx error messages not listed in the table or 9xx error messages, please provide those descriptions for reference.

Error Code*	Meaning
400	The request could not be understood.
500	The server internal error.
503	The server is unavailable.

- ConfigurationChange

IAD will send the configChangeTrap per command set. Once the command is executed, this Trap will be sent and the new configuration just modified by Administrator will be included in the Trap Description field. But IAD can not bind more than one commands in a Trap which include all the modified items.

Currently IAD will support the following "Configuration Change"

Configuration Change
GW WAN IP
Register Server IP
Proxy Server IP

- Five Clear traps are created in SNMP 2.1 for EMS interoperation.
  - LossCommunication,
  - TrafficWarning,
  - ConnetoProxyServer

7.15 Security

Device will filter SNMP traffic from non-authorized internal hosts. We provide a configuration item to set the IP address of SNMP manager, so that the SNMP GW will only accept the SNMP request from the specified host. If any other hosts whose IP address is invalid would like to access Device, Device will reject that request and send a trap to notify administrator.

8 Software Upgrade

The IAD software contents four components:

Application code

DSP code

Boot code

The chapter describes the normal procedure to download and upgrade the IAD's software. It is recommended to refer to the release note of new software changes before upgrading the IAD. Release notes always contain important information about the new software or upgrade procedure that must be taken into consideration.

8.1 Software Upgrade Procedure

Before starting the download process, it is recommended to configure the TFTP server Timeout (seconds) and the Maximum re-transmits options to an appropriate value according to the network traffic condition.

When upgrading the IAD to a new software image, it is recommended to upgrade the Boot Code, DSP first, only if any of these components upgrade is required. After downloading the Boot Code, DSP file through TFTP, the IAD will not automatically reboot. IAD Device need reboot immediately to load the new software.

Note: After downloading the Boot Code, DSP, the IAD will not automatically reboot. Therefore, if only either of these components needs to be upgraded, manually reboot the IAD in order to run the new software.

8.2 Software Upgrade Mode

There are two modes for software upgrade in this release.

- **Normal Mode:** When using this mode, the IAD will check port status before upgrade. If any call activity is detected, it will reject the upgrade request and send a warning trap message. If no active call is detected, the IAD blocks all the ports to prohibit any call attempt and followed by the software image download. During this process, all of IAD ports will not process call to avoid service interruption. It is recommended that the operator to use this conditional software upgrade procedure to minimize the interrupt to the live phone service.
- **Forced Mode:** In this mode, the IAD will proceed the software upgrade regardless of the port status.

Warning: It will drop all the on-going calls (if any) and complete the software upgrade process.

9 Appendix A: Technical Specification

9.1 Telephony

Item	Definition
Number of analog POTS port	30 with over voltage & current protection
Loop length	Up to 7KM (24 AWG.)
Ringing equivalency	REN*5 @1400Ω/20Hz
Ringing voltage	65Vrms @ REN*5, up to 90Vrms
On-Hook DC Voltage	50V
Line Impedance	600Ω
Call control protocol	RFC2543 & RFC3261
Codec support and PCM interface	G.729A, PCMU, PCMA, G.723
Packetization rate	10~30ms(PCMU, PCMA, G.729A), 30~60ms(G.723)
Echo cancellation	G.165 and G.168
Fax transmission	Group 3
Data modem transmission	V.22, V.22bis, V.32, V.32bis, V.33, V.90
Autonomous codec up speed	Autonomously transition from G.729a to G.711 for Fax/Modem transmission over voice band data
Out-of-band fax transmission	T.38
Out-of-band DTMF tone transmission	RFC2833
Silence suppression	G.711 Appendix II and G.729 Annex B
Comfort noise generation	G.711 Appendix II and G.729 Annex B
De-jitter buffer	Dynamically adjustable subject to the variability of jitter in the IP network, typical twice of the codec packetization time
Packet loss concealment	Yes
DTMF digit collection and generation	Yes
Tone generation	Call Server supervision
Polarity Reversal support	Yes

9.2 Performance

Item	Definition
Simultaneous call setups	Up to 30
Call rate per hour per endpoint	400 calls

9.3 OAM&P

Item	Definition
IP address and FQDN assignment	DHCP or manual
Remote Management	HTTP, Telnet, SNMP
Remote firmware upgrade	DHCP/TFTP, HTTP, Telnet, SNMP
Local Management	via RS232 Console Port or Ethernet CRAFT(LAN) Port
System clock synchronization	RFC1305 TOD/NTP
SNMP MIB support.	MIB-II RF1213 (exclude EGP group) & proprietary MIB

Quality of Service (QoS) classification Differentiated Service Code Point (DSCP) and IEEE 802.1p/q VLAN

9.4 Installation and Operating Environment

Item	Definition
Packaging Type	Industrial-grade enclosure for ANSI and ETSI rack and cabinet compliance
Dimension	Width x Depth x Height = 430mm x 380mm x 44mm
Weight	5.5 Kg
Network connectivity	RJ-45 10/100 Base-T Ethernet with auto detection of straight/cross Ethernet cable
Telephony interface	RJ21X 64-pin female connector
Console port interface	DB-9 female connector
Operating temperature	0 ~ 60 °C
Storage temperature	0 ~ 70 °C
Humidity	5 ~ 90 % non-condensing
Input AC voltage	90 ~ 264 V, 47 ~ 63 Hz
Input DC volta+ge (optional)	-56 ~ -42 Vdc
Power consumption	96 W maximum