AirStream 4000/4001 WiMAX CPE

User Manual v1.0

AIRSPAN NETWORKS LTD. CONFIDENTIAL

This document and the information contained in it is confidential information of Airspan Networks Ltd (Airspan), and shall not be used, or publish, or disclosed, or disseminated outside of Airspan in whole or in part without Airspan's consent. This document contains trade secrets of Airspan. Reverse engineering of any or all of the information in document is prohibited. The copyright notice does not imply publication of this document

CONFIDENTIAL INFORMATION
Information contained herein is proprietary to Airspan for whose benefit
confidentiality shall be maintained.

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25cm between the radiator & your body.

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

Table of Contents

List of Figures

1 Introduction

Airspan's WiMAX CPE products are 802.16e WAVE II compliant terminal devices designed for wireless service operators to offer integrated wireless data and voice services over the 802.16e networks. The CPE products will help service providers to rapidly reach targeted customer and gain market share.

Both indoor and outdoor models are available for different application environment needs and the end customer can choose a variety of product models with different user interfaces (data port, voice port, and WiFi option). The CPE can also support multiple frequency bands to meet different operator or country deployment needs. The sophisticated QoS feature also helps service providers to better control data traffic in their wireless networks. All Airspan CPE products are equipped with advance capability to differentiate end user traffic, marks traffic with different priorities, and policing traffic at the edge of their networks. These capabilities are vital for service providers to avoid service disruption caused by malicious users.

Airspan's CPE products provide multiple management interfaces to allow local or over the air provision and management of the device. The supported user management interface and management protocol include console access, telnet, WEB, SNMP, FTP, TFTP, TR-069 and future OMA-DM. Airspan also offers standard based device management solution for auto provision, firmware management and remote monitoring and maintenance.

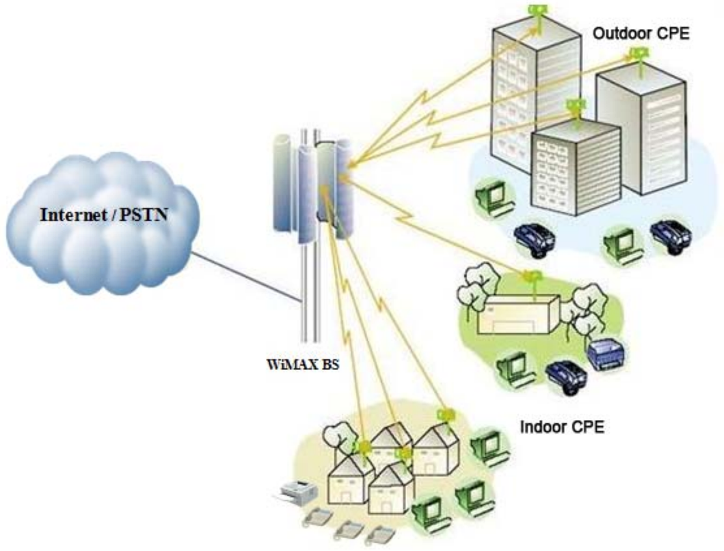


Figure 1. WiMAX CPE Application in 802.16e Network

This manual provides user reference information necessary for configuration and provisioning of AirStream 4000/4001 CPE product. It can also be used by technical support engineers for troubleshooting and problem resolution.

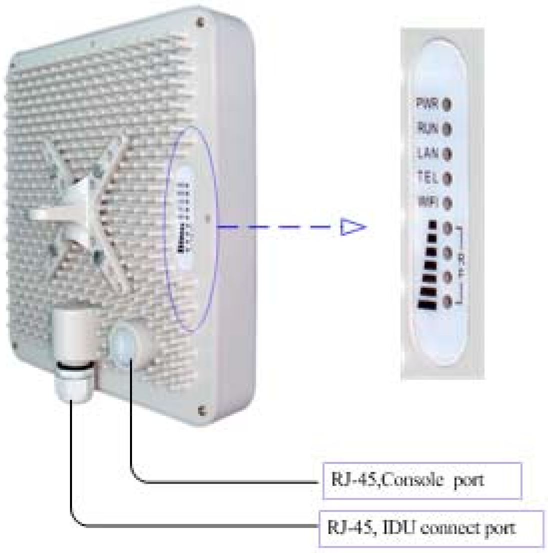
2 Product Specifications

2.1 Product Model Overview

Model	Appearance	Description & User Interface
Airstream 4000/4001		■ Antennal Gain: 15dbi ■ One 10/100M Ethernet Port (RJ-45) ■ One RJ11 Port (AirStream 4001 only) ■ LED Indicator: PWR, RUN, WiMAX (4), LINE ■ 48V/0.4A VDC PoE, ODU Power < 15 Watts ■ Dimensions: 265 mm × 265 mm × 130 mm ■ Weight: less than 3 Kg

2.2 User Interface Description

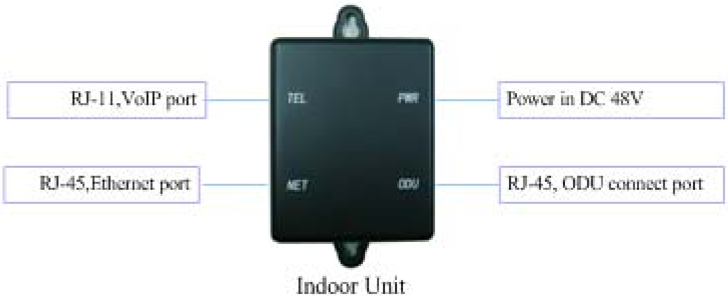
ODU LED DESCRIPTION



LED	DESCRIPTION	FUNCTION
PWR	Power Indictor	■ Stable light indicates system is powered on.
RUN	System Status	■ Fast flash indicates the device is booting up. Slow flash indicates the system is running and ready.
RF	WiMAX & WAN Networking Status	■ Solid purple light indicates the device is connected and the WiMAX signal strength is excellent. ■ Solid green light indicates the device is connected and the WiMAX signal strength is good. ■ Solid red light indicates the device is connected but the WiMAX signal strength is poor. ■ Light off indicates WiMAX is not connected at all.
LAN	Networking Status Indicator	■ Light off indicates LAN is not connected. ■ Solid light indicates LAN is connected but no data activity. ■ Flash light indicates LAN is transmitting data currently.

LED	DESCRIPTION	FUNCTION
PHONE	Phone Line Status	■ Stable ON indicates the line is not ready for use or faulty. ■ Stable OFF indicates the line is ready for use. ■ Flashing Light indicates a call is in progress on the port.

IDU PANEL INTERFACE DESCRIPTION



INTERFACE	FUNCTION	DESCRIPTION
DC Power	Power Input Jack	Use 48V /0.4A DC Power adapter supplied with the CPE. Misuse of power may cause damage to the device.
ODU	RJ45 Interface to connect ODU	
NET	RJ45 Interface to Local Area Network	Local Area Network interface (RJ45), to connect to computer, or a hub or switch. Depending on the product model, either 1 or 4 ports can be available.
Phone Ports (Optional)	RJ11 Interfaces to Legacy Phones and Fax (4001 Model Only)	Two RJ11 phone jacks available to connect legacy phones or fax machines. Depending on its model, either a shared line or two independent lines can be installed.

2.3 WiMAX Interface Specification

Frequency Bands	698-765MHz,
Radio Access	802.16e Wave 2, 2x2 MIMO
Operation Mode	TDD
Channel Bandwidth	3.5MHz, 5 MHz, 7Mhz,, 10 MHz
RF Power & Antenna	➢ 24dBm at antenna port ➢ 8dbi (698-765MHz)
Modulation	QPSK, 16QAM, 64QAM
FFT	1024/512 FFT points
FEC	Convolution Code and Turbo Code
Authentication	TTLS (MD5/CHAPv2) and TLS

2.4 Data Networking Features

Wireless Networking	Support both bridge and router mode

	DHCP or static IP address assignment
	Support IP_CS and ETH_CS
	One MAC address assigned by the vendor
LAN Port Networking	Built-in DHCP server for LAN devices (The default IP address for the LAN interface is 192.168.0.1)
	LAN User Access Control
Ethernet Interface	IEEE802.3 10Base Ethernet
	IEEE802.3u 100Base Ethernet (Fast Ethernet)
	IEEE802.3x Auto/Full/half duplex flow control
	MTU 1428 or 1528 Bytes (Configurable)
QoS Management	Classification of voice, data and management traffic
	802.1p/q, DSCP or TOS marking based on traffic classification
	Prioritized processing of voice and management data traffic
VLAN Networking	802.1q VLAN Tagging based on traffic classes
	VLAN trunking support over a single WAN IP interface
VPN Feature	VPN pass-through (PPTP and L2TP/IPSEC)
	Built-in L2TP client
Firewall Support	IP and port based traffic filtering
	DMZ & Virtual Server mapping support
NTP	NTP protocol support for acquiring timing from NTP servers.

2.5 Voice Features (AirStream 4001 Model Only)

Supported Protocol	SIP Session Initiation Protocol
	RTP Real Time Transfer Protocol
	RTCP Real Time Transfer Control Protocol
Networking Support	Soft switch based networking or CPE to CPE peer to peer networking
Voice Encoder	G.711, G729, G.723 or G.726
Noise Control	Comfort Noise Generation & level control
Echo suppressing	G.165/G.168-2000 echo suppress
Silence process	Silence detection and suppressing
FAX	T.30 (fax and modem), T38
Delay and Packet Lose Process	Delay and jitter control/ Packet lose equalization
POTS Line Distance	> 1Km
Voice Services	Basic and enhanced supplementary services, value added line features

2.6 Management Features

The WiMAX CPE products support the following user management interface:

- WEB based management interface
- Remote management via Telnet

For network management interface, the following are supported:

- SNMP, TFTP and SYSLOG reporting for Alarms
- Standard TR-069 management client
- OMA-DM management client in future release

For individual CPE firmware and configuration data file management, the user can use the following methods:

- Firmware and configuration file upgrade or backup via HTTP WEB interface
- Firmware upgrade via TFTP and FTP

3 Getting Started

3.1 Packing list

Upon receiving the product, please unpack the product package carefully. Each product is shipped with the following items:

CPE Products	Quantity	Note
Main Unit （ODU）	1	
PoE adapter（IDU）	1	
48V/0.4A DC Power Adapter	1	
PC Ethernet Cable	1	
User CD (optional)	1	
Product Warranty Card	1	

If you find any of the items is missing, please contact our local distributor immediately.

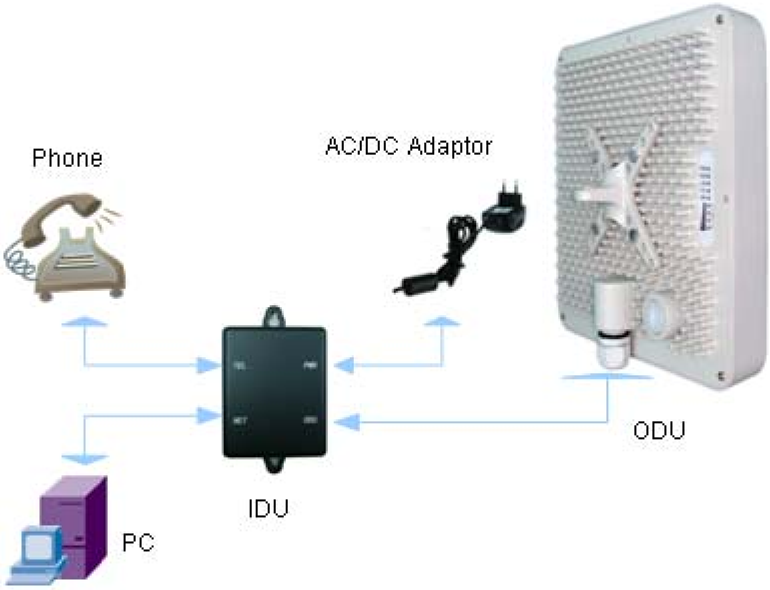
3.2 Installation

To power on the device, the indoor CPE should use a 48V/0.4A DC power supply from the adapter. All power adapters can operate in 90-250V AC range and therefore can be used in different countries. Once the device is powered, the user should wait for about 1 minute before the device becomes operational. A slowly flashing CPE RUN LED light indicates the system has completed the startup procedure.

To connect PC, LAN switch or other type of IP device to the CPE, the user should use standard CAT5 Ethernet cable and connect to the appropriate LAN port. Once connected the CPE LAN LED indicator should be on.

To use the phone service, user can simply plug the phone line into the CPE RJ11 port. If the line is not registered or configured, a fast busy tone will be provided and corresponding LED light will be solidly on.

3.3 Connect



4 Managing CPE Devices

The WiMAX CPE product supports three main management interfaces: TELNET, WEB and TR-069 management from local or from remote central offices.

User name and password are required for access to management functions. There are two levels or privileges: administrators' privilege and normal users' privileges.

- Administrator's privilege is designed for service providers to provision a CPE device before selling or leasing out to end users. By supplying administrator's user name and password, a technician has access to all configurations of a CPE device. Default user name for administrator's privileges is "admin". Default password is "admin".
- Users' privilege is provisioned for end users to make limited changes of configurations for a CPE device. Most of other configurations are not visible when accessed with normal user's privileges. Default user name and password for user is "user".

4.1 Managing CPE via Telnet Access

To Telnet into CPE device, the IP address of its WAN interface or LAN interface must be known:

- Default IP address for the LAN interface is 192.168.0.1, unless the configuration has been modified.
- The IP address for WAN interface is usually acquired from service provider's network after CPE connects to the WiMAX network.

4.1.1 Telnet Access to CPE from LAN Segment

The user may Telnet into the CPE by specifying the IP address of CPE LAN interface. The default IP Address of the CPE LAN interface is 192.168.0.1.

The CPE acts as a DHCP server for hosts in LAN segment by default, unless this feature is disabled. Control Station may dynamically acquires an IP address from CPE built-in DHCP server.

After IP connectivity is established between the Control Station and CPE, the user may Telnet into the CPE.

4.1.2 Telnet Access from Wireless Interface Segment

The user may also Telnet into the CPE by specifying the wireless IP address of the CPE device. Access from Wireless interface is very helpful for remote troubleshooting.

The wireless IP address is usually acquired via DHCP once the CPE is connected into the service provider's network. To find out the wireless IP, Support technician may seek end user's help to find out IP address of the wireless interface of CPE located in customer premise. The easiest way for end users is to follow the instructions outlined in Section 4.2.1. End users may be given a user name and password with lower privilege to access limited information stored in the CPE.

CAUTION	**Telnet from remote location is not recommended as user name and password are sent in clear text. Malicious users may sniff IP packets and find administrator's credentials easily.**

4.2 Managing CPE via Web Browser

It is a preferred way to manage the CPE using a Web browser from a local or remote host, for example, Internet Explorer in Windows operation systems.

The reader has the option to access the CPE using the LAN interface or wireless IP if it is known.

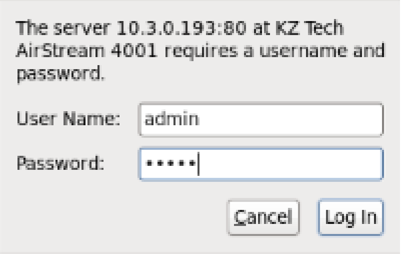
- The default IP address for the LAN interface is 192.168.0.1, unless the configuration has been modified.
- The WAN IP is usually acquired from service provider's network after CPE connects to the network.

4.2.1 Access CPE from LAN Interface

Connect the LAN port of Control Station (a PC) directly to the LAN port of the CPE, or in-indirectly via an Ethernet hub or switch. By default, the CPE will act as a DHCP server for hosts in the LAN segment unless this feature is disabled. The Control Station can dynamically acquire an IP address from CPE's built-in DHCP server.

After IP layer connectivity is established between the Control Station and the CPE, the user may launch a Web browser and specify http://192.168.0.1 in the address bar. A window will pop up requesting user name and password. If the device WiMAX WAN IP assigned is within the same subnet as the LAN IP, the LAN IP by default will be automatically switched to 10.10.0.1.

Input user name and password, and then click on the "OK" button. After a successful log on, the welcome page of web management interface will appear.



The server 10.3.0.193:80 at KZ Tech AirStream 4001 requires a username and password.

User Name: admin

Password: •••••

Figure 2. Logon Web Page

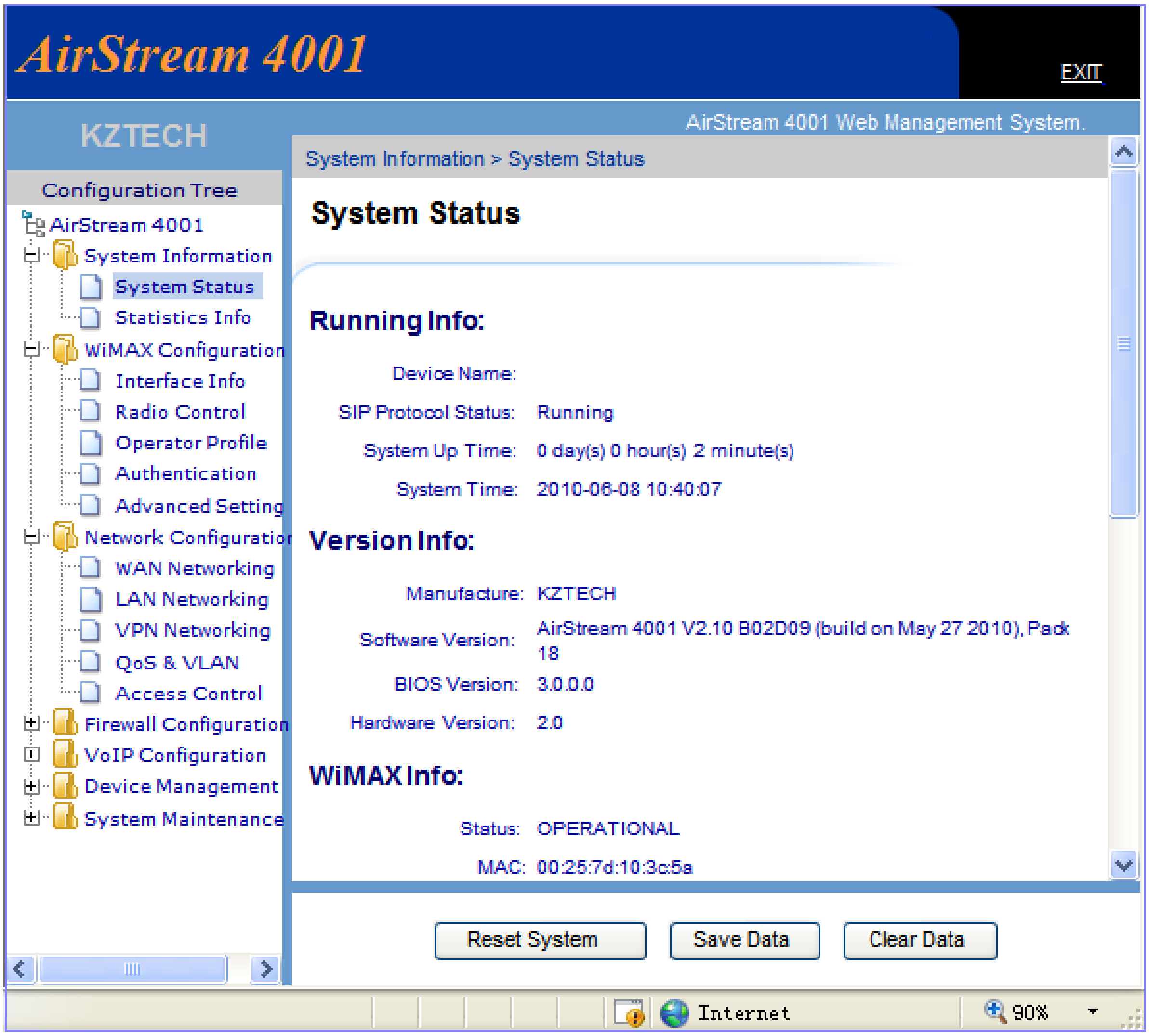
4.2.2 Access CPE Device from WAN Segment

Service providers may access the CPE Web management interface remotely, by specifying the CPE wireless IP address obtained after connecting to the service provider network.

As the wireless IP address is dynamically assigned by the service provider, the support technician may seek end user's help to find out the IP address of wireless interface for the CPE located in customer premise. The end user can retrieve the wireless IP by following the instructions outlined in Section 4.2.1.

4.2.3 Welcoming Page

Once the user logs in into the WEB management server, the following Welcome page of IX253P CPE will be displayed.



System Status

Running Info:

Device Name:
SIP Protocol Status: Running
System Up Time: 0 day(s) 0 hour(s) 2 minute(s)
System Time: 2010-06-08 10:40:07

Version Info:

Manufacture: KZTECH
Software Version: AirStream 4001 V2.10 B02D09 (build on May 27 2010), Pack 18
BIOS Version: 3.0.0.0
Hardware Version: 2.0

WiMAX Info:

Status: OPERATIONAL
MAC: 00:25:7d:10:3c:5a

Figure 3. WiMAX CPE Web Management Interface

The left frame in the above web page shows the Configuration Tree, which provides links to detailed configuration pages.

Configuration management of IX253P CPE is categorized into seven major groups:

- System Information
- WiMAX Configuration
- Network configuration
- Firewall Configuration
- VoIP Configuration
- Device Management
- System Maintenance

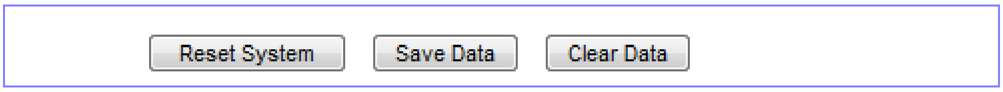
Items in Configuration Tree are arranged from top to down according to frequency of use. The tree map can be navigated by clicking on the item link.

♦ Detailed Configuration Window

The middle right frame in the browser window has the largest display area. It is used to display detailed configuration. Certain configuration pages can not be fully displayed in the screen. Scroll the vertical bar down in the right to view information that may not be displayed.

♦ Reset System, Save Data and Clear Data

The lower right frame of the web page has three buttons:



Effective configuration data are stored in RAM (Random Access Memory). Once the CPE is powered off, all effective configurations in RAM will be lost unless they are saved into non-volatile flash memory.

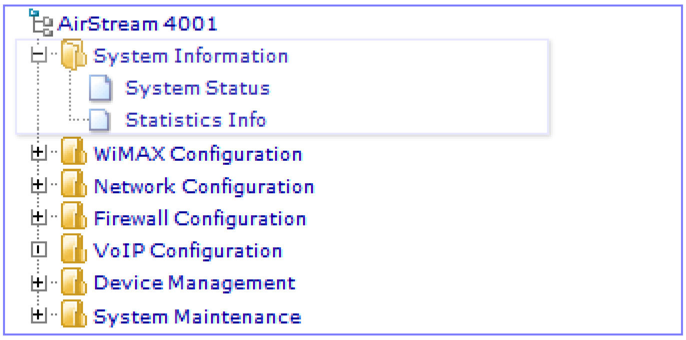
Information	**Users are advised to save configuration changes, after Applying changes in the Detailed Configuration Window.**

Device configuration in RAM can be saved, by clicking on **[Save Data]** button, into non-volatile flash memory, which can be reloaded automatically every time when CPE boots up. Device configuration can be restored to factory default by clicking on **[Clear Data]**.

Resetting system will shutdown all processes and reboots the CPE device. The system software will be reloaded. The system software will read configuration data saved in non-volatile flash memory during the boot process.

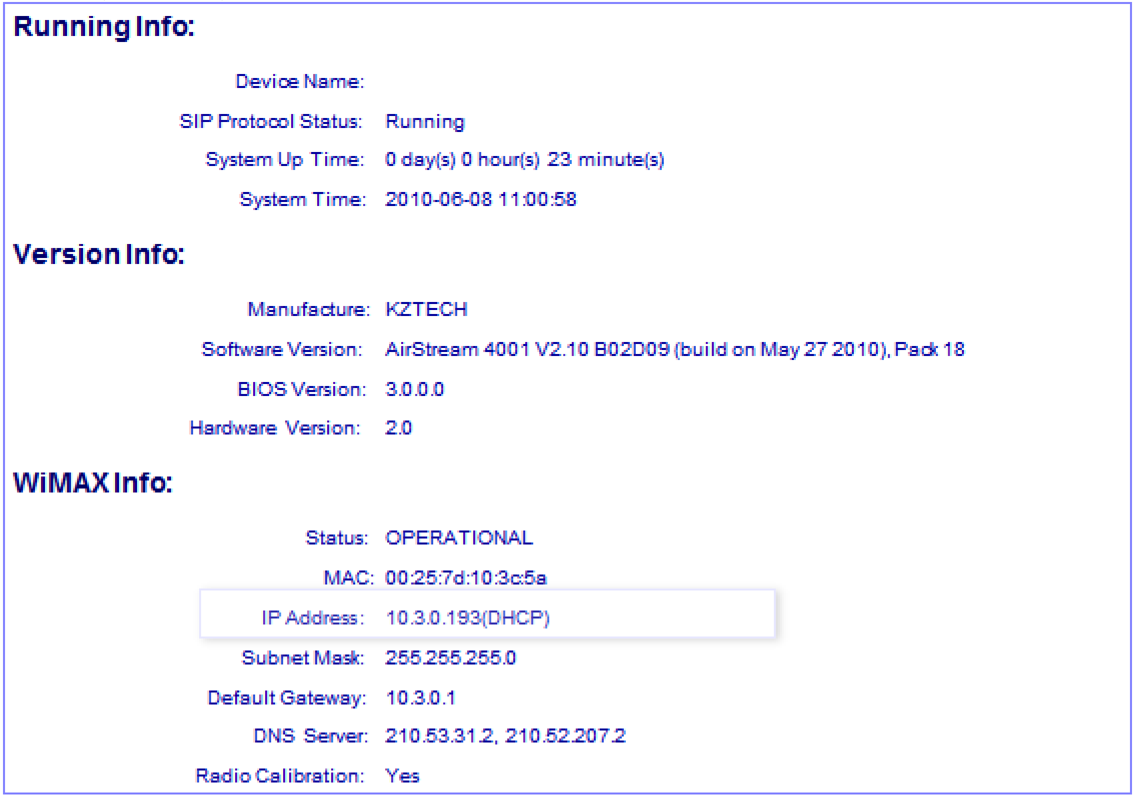
5 System Information

System Information provides both system running status, data (TCP/UDP, RTP) and voice traffic statistics info. It helps user to get a overall view of the device operation status.



5.1 System Status

In System Status, plenty of info of the CPE is given, such as Running Info, Version Info, WiMAX Info, Voice Line Info, LAN info, PPP Info.



Running Info:

Device Name:

SIP Protocol Status: Running

System Up Time: 0 day(s) 0 hour(s) 23 minute(s)

System Time: 2010-06-08 11:00:58

Version Info:

Manufacture: KZTECH

Software Version: AirStream 4001 V2.10 B02D09 (build on May 27 2010), Pack 18

BIOS Version: 3.0.0.0

Hardware Version: 2.0

WiMAX Info:

Status: OPERATIONAL

MAC: 00:25:7d:10:3c:5a

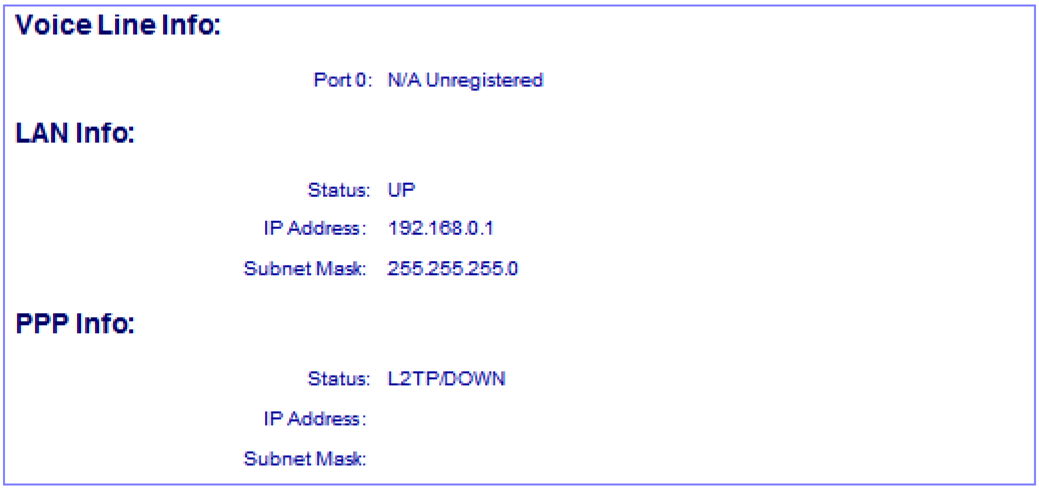
IP Address: 10.3.0.193(DHCP)

Subnet Mask: 255.255.255.0

Default Gateway: 10.3.0.1

DNS Server: 210.53.31.2, 210.52.207.2

Radio Calibration: Yes



Voice Line Info:

Port 0: N/A Unregistered

LAN Info:

Status: UP

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

PPP Info:

Status: L2TP/DOWN

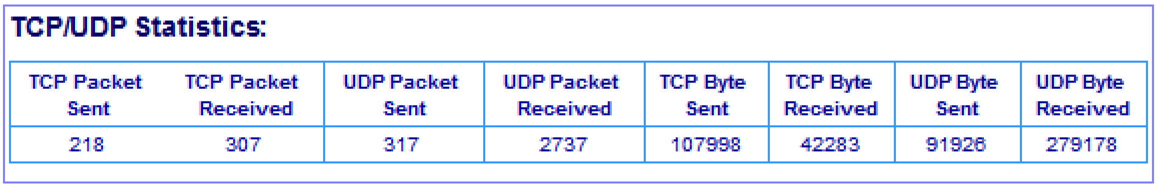
IP Address:

Subnet Mask:

5.2 Statistics Info

Click the "Statistic Info" page, you can review the data and call statistics information of the device.

5.2.1 Data Statistics

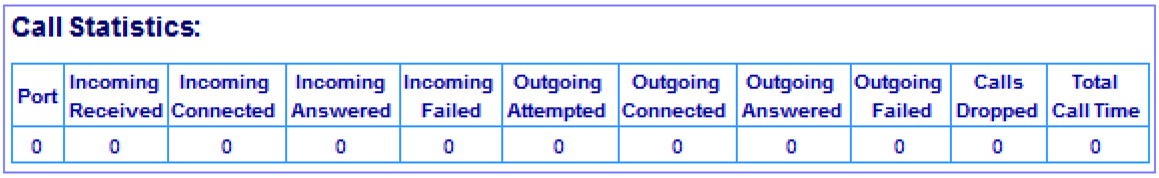


TCP/UDP Statistics:

TCP Packet Sent	TCP Packet Received	UDP Packet Sent	UDP Packet Received	TCP Byte Sent	TCP Byte Received	UDP Byte Sent	UDP Byte Received
218	307	317	2737	107998	42283	91926	279178

TCP/UDP Statistics supply both TCP & UDP traffic information in terms of packet numbers and traffic volume in bytes.

5.2.2 Call Statistics



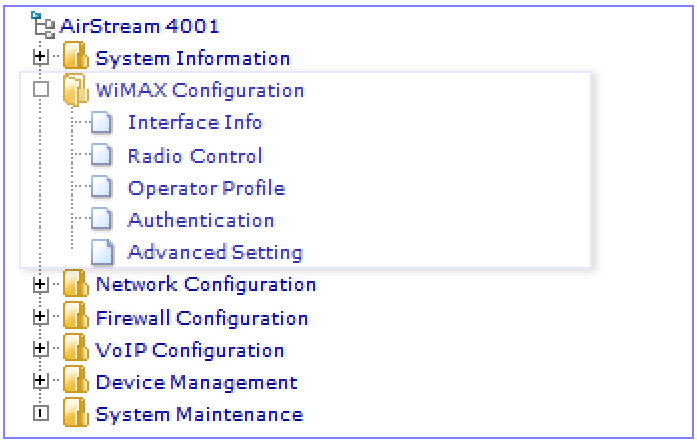
Call Statistics:

Port	Incoming Received	Incoming Connected	Incoming Answered	Incoming Failed	Outgoing Attempted	Outgoing Connected	Outgoing Answered	Outgoing Failed	Calls Dropped	Total Call Time
0	0	0	0	0	0	0	0	0	0	0

Call statistics provides various call statistic figures for both incoming and outgoing calls as shown in the above table. The information helps to know the user usage and find out the abnormality in voice calling.

6 WiMAX Configuration

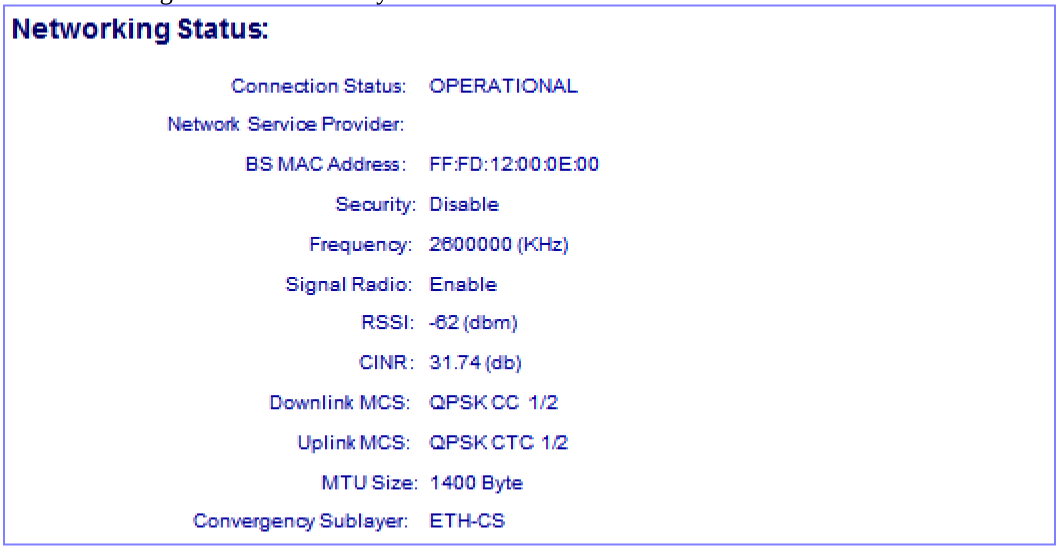
The WiMAX Configuration allows user to view and configure the WiMAX interface. It provides five basic functions: interface information display, radio control management, operator profile, authentication and advanced setting.



- AirStream 4001
  - System Information
  - WiMAX Configuration
    - Interface Info
    - Radio Control
    - Operator Profile
    - Authentication
    - Advanced Setting
  - Network Configuration
  - Firewall Configuration
  - VoIP Configuration
  - Device Management
  - System Maintenance

6.1 WiMAX Interface Info

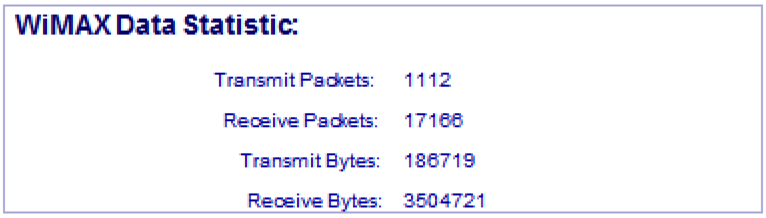
When clicking on the "Interface Info" link, the following WiMAX interface information is displayed. The networking status is a summary of current wireless link connection.



Networking Status:

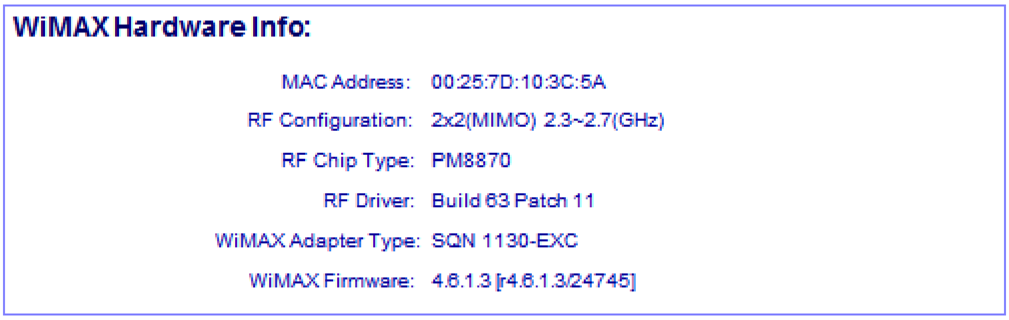
Connection Status:	OPERATIONAL
Network Service Provider:	
BS MAC Address:	FF:FD:12:00:0E:00
Security:	Disable
Frequency:	2600000 (KHz)
Signal Radio:	Enable
RSSI:	-62 (dbm)
CINR:	31.74 (db)
Downlink MCS:	QPSK CC 1/2
Uplink MCS:	QPSK CTC 1/2
MTU Size:	1400 Byte
Convergency Sublayer:	ETH-CS

The WiMAX data statistics shows the wireless data traffic amount and the hardware info displays the underlying WiMAX chipset and driver information.



WiMAX Data Statistic:

Transmit Packets:	1112
Receive Packets:	17166
Transmit Bytes:	186719
Receive Bytes:	3504721

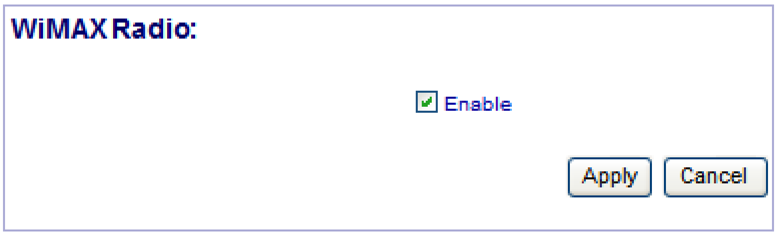


WiMAX Hardware Info:

MAC Address:	00:25:7D:10:3C:5A
RF Configuration:	2x2(MIMO) 2.3~2.7(GHz)
RF Chip Type:	PM8870
RF Driver:	Build 63 Patch 11
WiMAX Adapter Type:	SQN 1130-EXC
WiMAX Firmware:	4.6.1.3 [r4.6.1.3/24745]

6.2 Radio Control

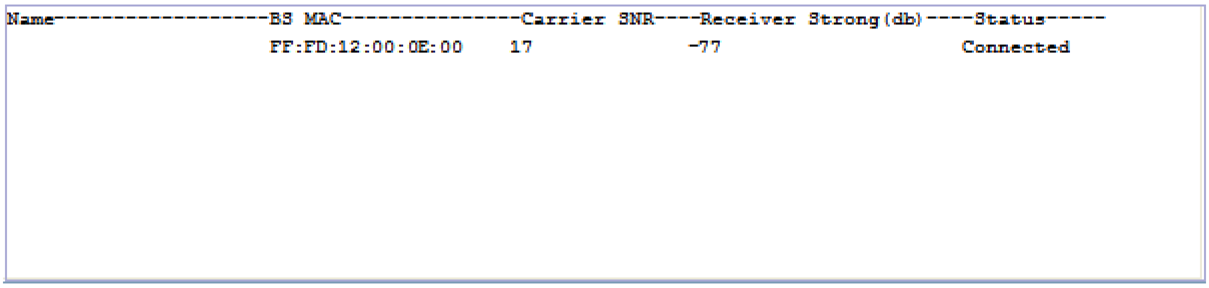
The Radio Control management allows user to temporally disable the WiMAX connection. But by default, the WiMAX radio will always be on when the CPE just powered up or undergo a restart.



WiMAX Radio:

☑ Enable

The nearby BS list shows the list of Base Stations that the CPE device can connect to. The user can select and switch to connect a different base station.

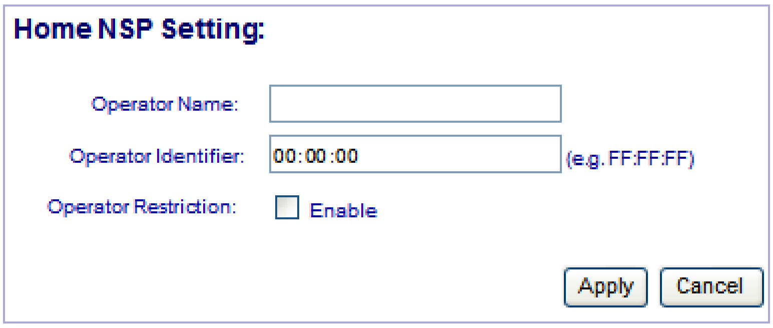


```
Name-------------------BS MAC---------------Carrier SNR----Receiver Strong(db)----Status-----
                       FF:FD:12:00:0E:00    17            -77                    Connected
```

6.3 Operator Profile

The Operator Profile deals with configurations of wireless channel, preferred NAP and NSP setting for roaming and network hand over processing.

The operator name and identifier can be added here. You can also choose to enable operator restriction or not. Note the operator restriction needs to be configured with a valid operator identifier.



Home NSP Setting:

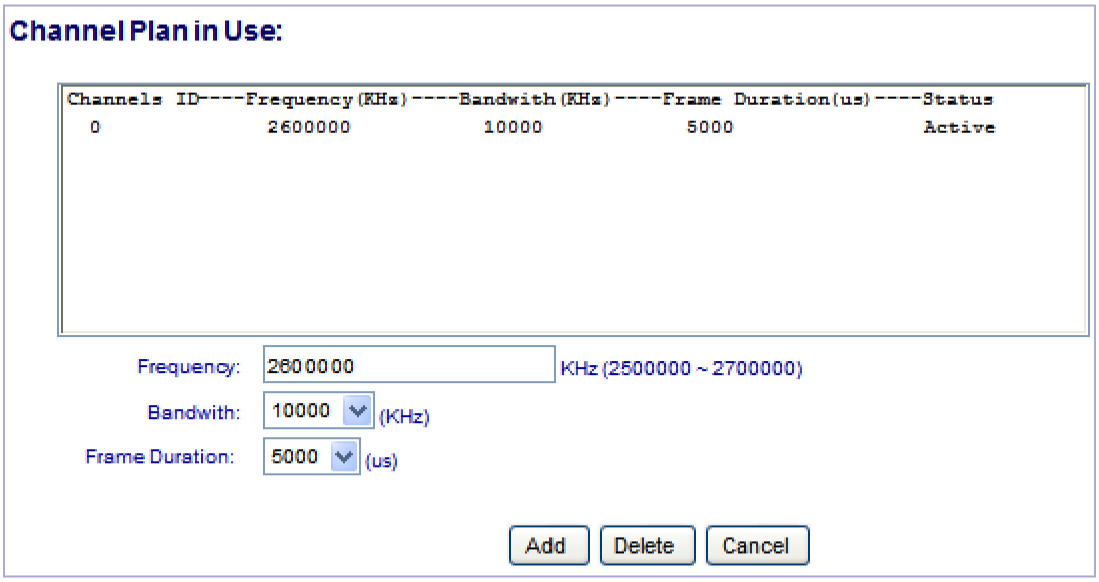
Operator Name:

Operator Identifier: 00:00:00 (e.g. FF:FF:FF)

Operator Restriction: □ Enable

To configure a channel, the user must specify the frequency, channel bandwidth and frame duration. Multiple channels can be added and the CPE will automatically search for available channel to connect.

Most of network setting will be pre-configured in factory for service operator. But if no channel is configured by user, the default channel will be automatically added to the channel list during the device power on.



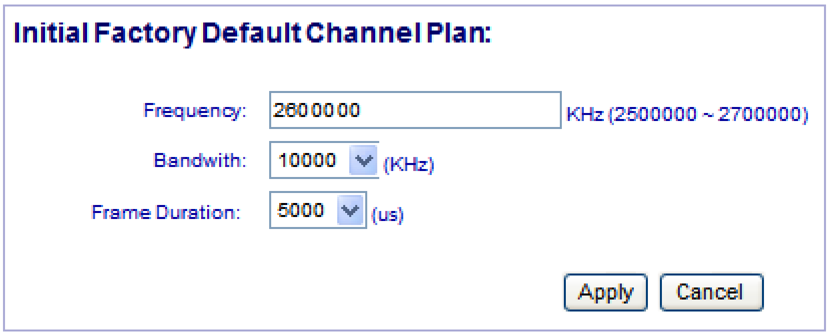
Channel Plan in Use:

```
Channels  ID----Frequency(KHz)----Bandwith(KHz)----Frame  Duration(us)----Status
  0              2600000          10000          5000                Active
```

Frequency: 2600000 KHz (2500000 ~ 2700000)

Bandwith: 10000 (KHz)

Frame Duration: 5000 (us)



Initial Factory Default Channel Plan:

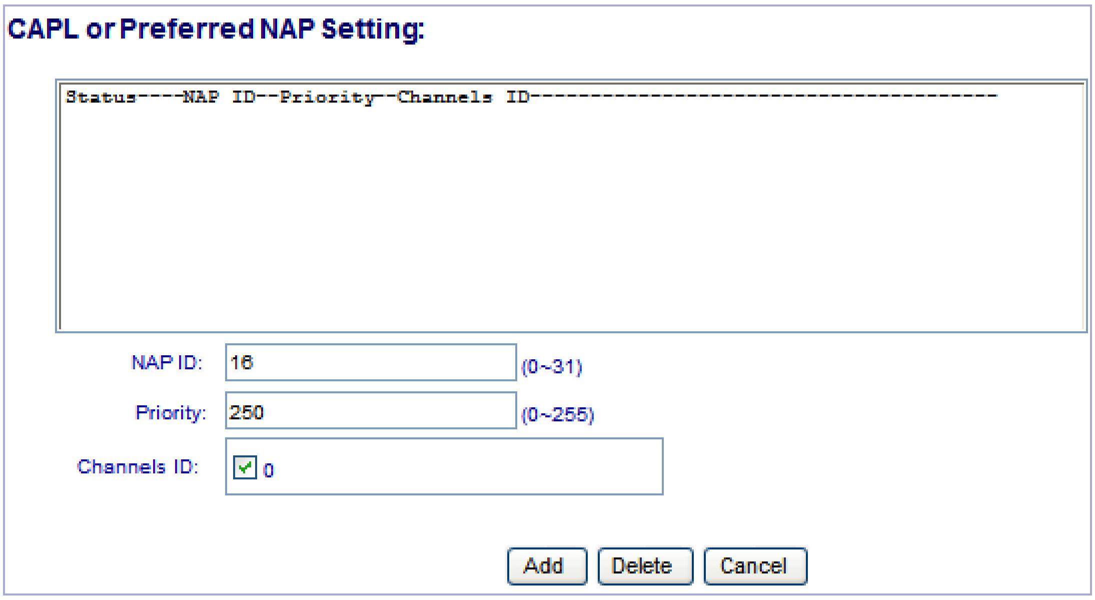
Frequency: 2600000 KHz (2500000 ~ 2700000)

Bandwith: 10000 (KHz)

Frame Duration: 5000 (us)

To enable access and roaming services, use the following to configure:

- Prefered network access provider or Contacted Access Provider List
- Predered network serviec prpvider or Roaming Access Provider List



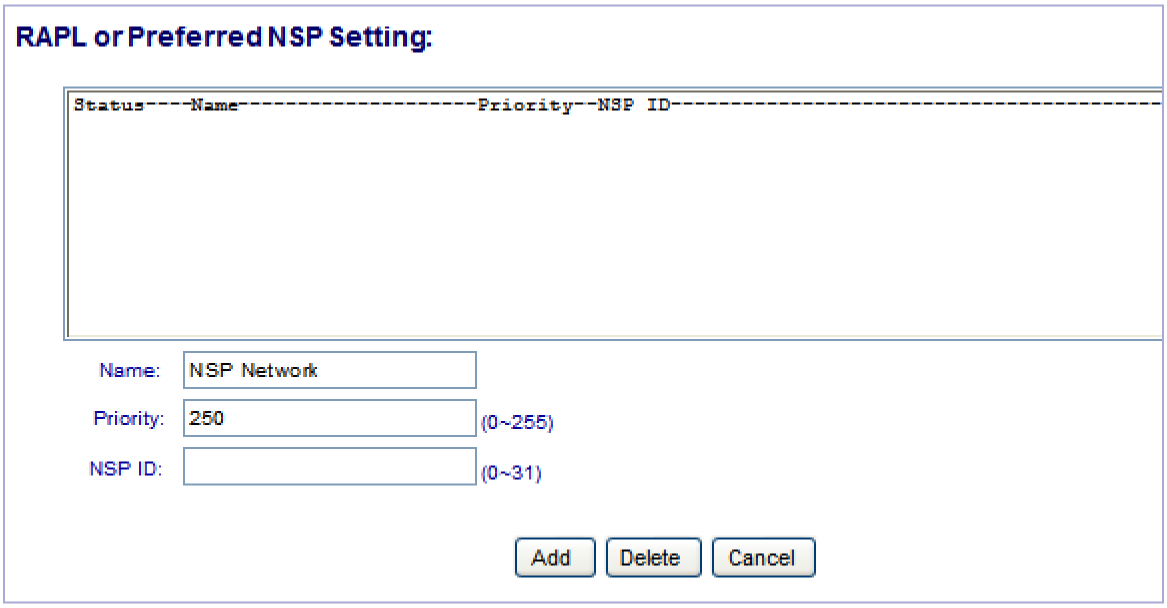
CAPL or Preferred NAP Setting:

```
Status----NAP ID--Priority--Channels ID----------------------------------------
```

NAP ID: 16 (0~31)

Priority: 250 (0~255)

Channels ID: ☑ 0



RAPL or Preferred NSP Setting:

```
Status----Name--------------------Priority--NSP ID----------------------------------------
```

Name: NSP Network

Priority: 250 (0~255)

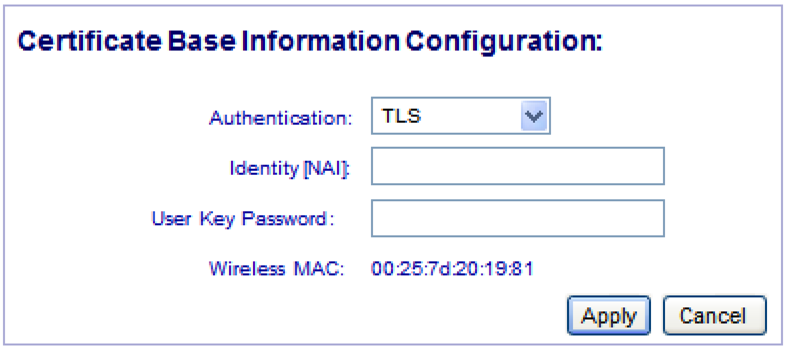
NSP ID: (0~31)

6.4 Authentication Setting

The CPE supports both TTL and TTLS authentication for user access. The authentication can also be disabled for the CPE device. Both root and user certificate are supported and can be over-written via WEB interface.

The CPE may be shipped with the service provider default authentication information. Once connected to the network, the CPE can then be managed by the network management system to update the device authentication information.

For TLS authentication, the root certificate, user and user key certificate needs to be provisioned. Optional user key password can also be specified.



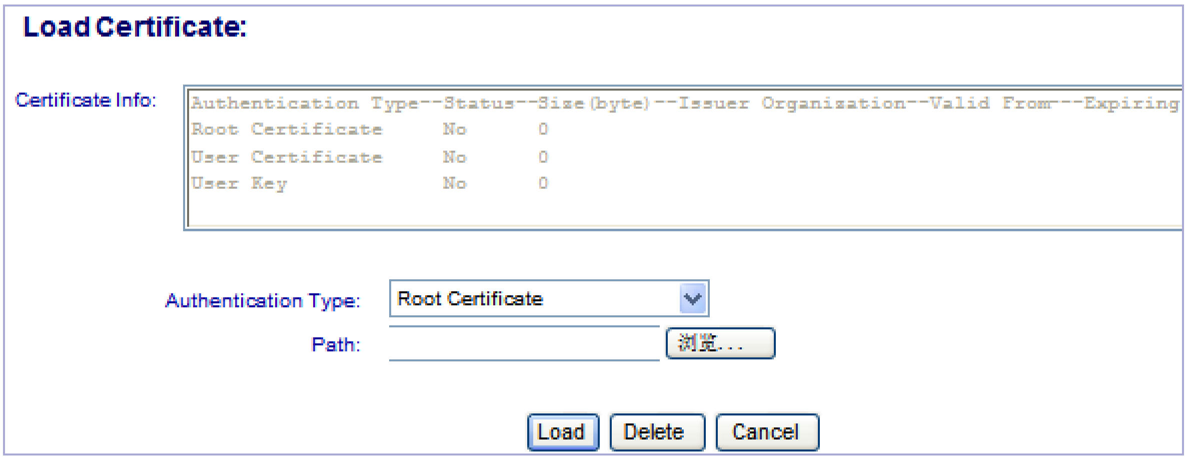
Certificate Base Information Configuration:

Authentication: TLS

Identity [NAI]:

User Key Password:

Wireless MAC: 00:25:7d:20:19:81



Load Certificate:

Certificate Info:

```
Authentication Type--Status--Size(byte)--Issuer Organization--Valid From---Expiring
Root Certificate     No      0
User Certificate     No      0
User Key             No      0
```

Authentication Type: Root Certificate

Path:

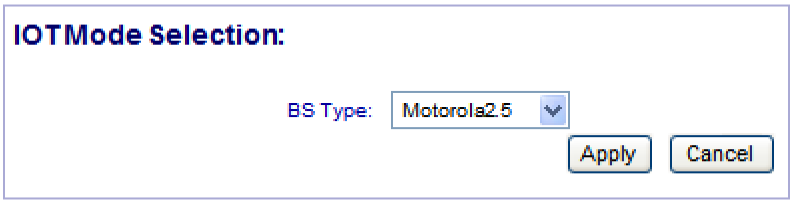
For TTLS authentication, both MD5 and CHAPv2 are supported. For a successful configuration of the TTLS authentication, the following must be provisioned:

- Root certificate
- Identify or Network Address Identified (NAI)
- Inner Identity or User Name
- Password

6.5 Advanced Setting

Use the advanced setting to select IOT Mode and configure MS Capability and Network Access options.

IOT Mode can be enabled with a selection of more than 17 popular base station types. The “Unified” mode is the default mode for IOT with many BS vendors.



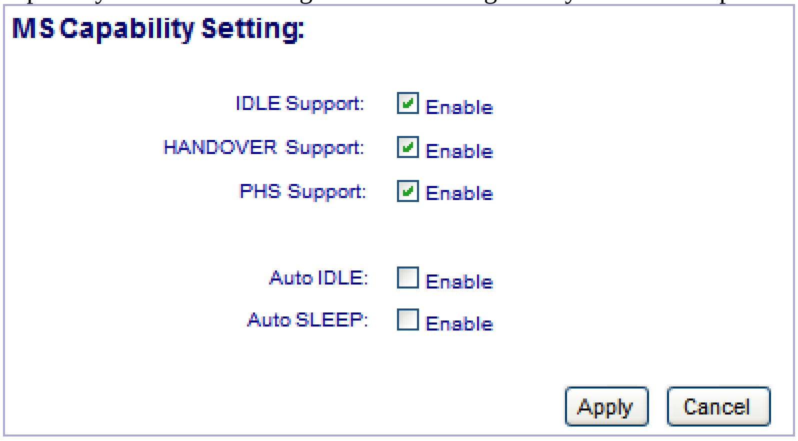
IOT Mode Selection:

BS Type: Motorola2.5

The advanced setting also allow user to configure MS Capability and Network Access settings including auto idle support, auto connect, and roaming and etc.

The MS by default supports IDLE, HANDOVER and IDLE. Depending on the BS type, these may need to be disabled for better interoperability. For BS that support IDLE and SLEEP operation, the CPE should enable the auto-idle and auto-sleep feature.

For Network Access settings, it is intended for service provider configuration. The auto-connect should be always enabled to allow seamless user connection. Enable Roaming option to obtain the service roaming capability. The rest of setting should be configured by the service operator and user should not alter them.



MS Capability Setting:

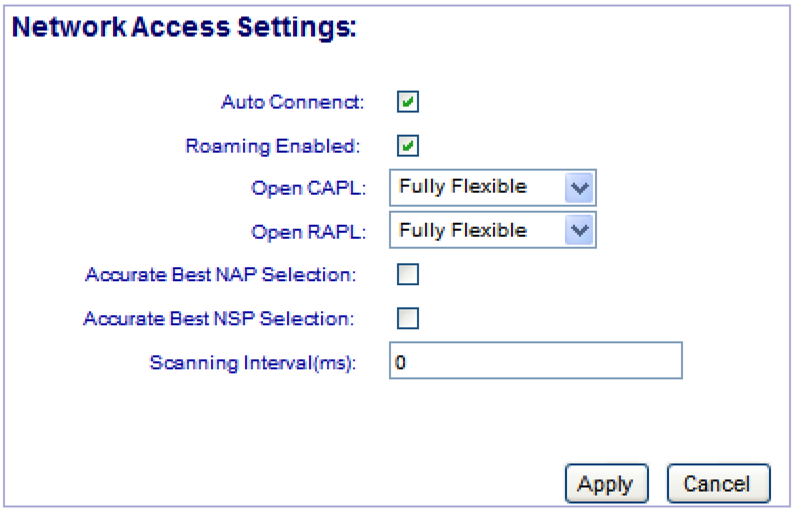
IDLE Support: ☑ Enable

HANDOVER Support: ☑ Enable

PHS Support: ☑ Enable

Auto IDLE: □ Enable

Auto SLEEP: □ Enable



Network Access Settings:

Auto Connenct: ☑

Roaming Enabled: ☑

Open CAPL: Fully Flexible

Open RAPL: Fully Flexible

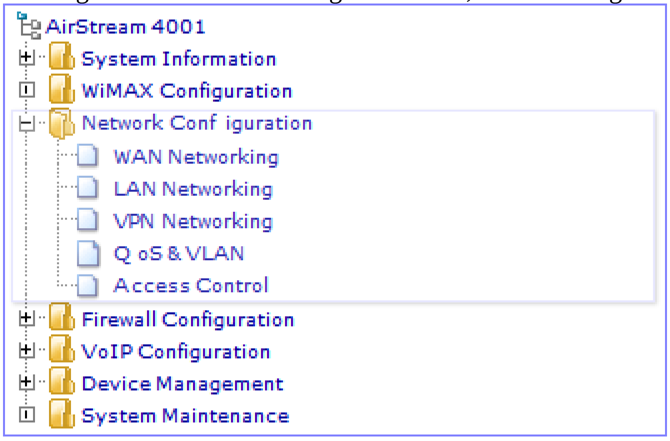
Accurate Best NAP Selection: □

Accurate Best NSP Selection: □

Scanning Interval(ms): 0

7 Network Configurations

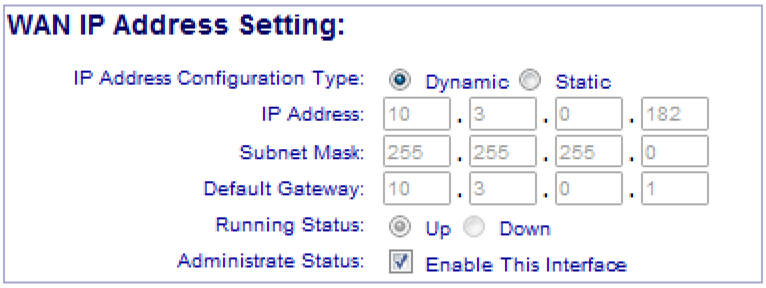
This section discusses the configuration to establish connectivity between a CPE and wireless network. When clicking on the Network Configuration link, the following menu will be displayed.



7.1 WAN Networking

Click on “WAN Networking” in the Configuration tree. The web page in the detailed configuration frame will show WAN IP Address Setting and DNS Configuration. For WiMAX access, dynamic IP should be enabled for WAN interface.

7.1.1 WAN IP Address Setting



WAN IP Address Setting:

IP Address Configuration Type: ● Dynamic ○ Static

IP Address: 10 . 3 . 0 . 182

Subnet Mask: 255 . 255 . 255 . 0

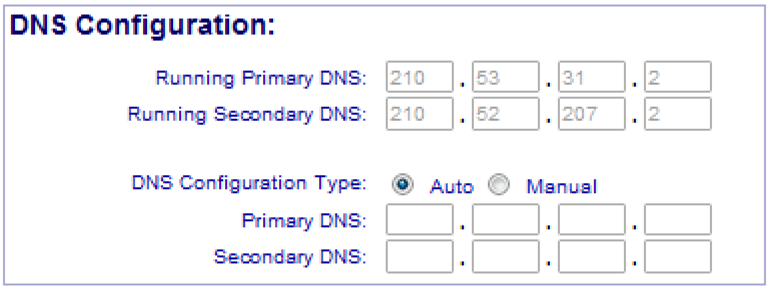
Default Gateway: 10 . 3 . 0 . 1

Running Status: ● Up ○ Down

Administrate Status: ☑ Enable This Interface

The interfaces can be shut down or brought up at electrical level. When the interface is up, the interface can be enabled or disabled at logical level. The interfaces may acquire an IP address dynamically, or be given a static IP address.

7.1.2 DNS Configuration



DNS Configuration:

Running Primary DNS: 210 . 53 . 31 . 2

Running Secondary DNS: 210 . 52 . 207 . 2

DNS Configuration Type: ● Auto ○ Manual

Primary DNS: . . .

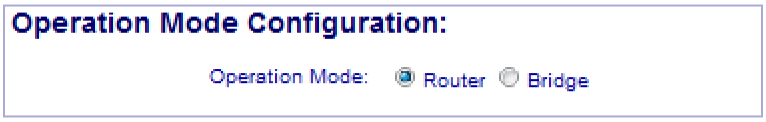
Secondary DNS: . . .

When wan interface acquires an IP address from the network, it is likely that information of DNS servers is provided by the DHCP servers in the network. Manual setting is not necessary. But it is also possible to manually specify DNS server address in the table above.

Note	**NAT must be enabled if DHCP server is enabled. DHCP server is enabled by default.**

7.2 LAN Networking

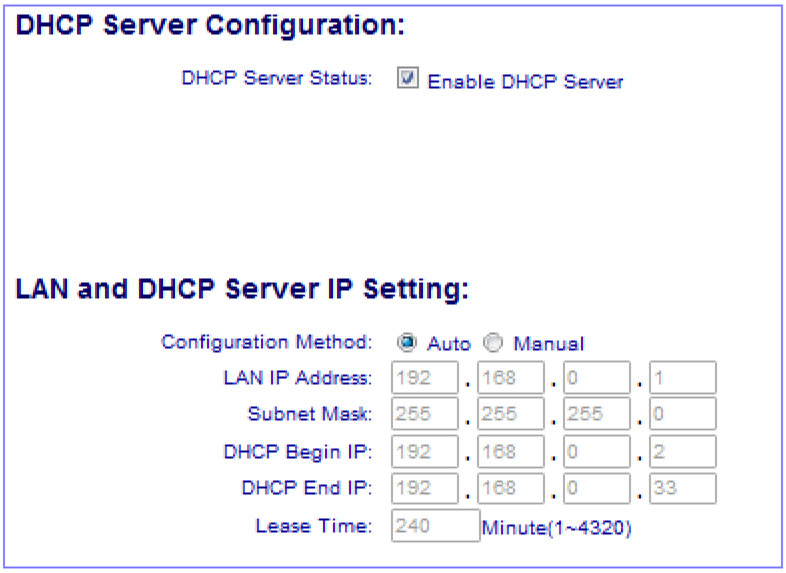
An operation mode of Router or Bridge can be selected via Web management.



Operation Mode Configuration:

Operation Mode: ● Router ○ Bridge

When choosing Router mode, you can also enable or disable DHCP Server, and configure LAN and DHCP Server IP.



DHCP Server Configuration:

DHCP Server Status: ☑ Enable DHCP Server

LAN and DHCP Server IP Setting:

Configuration Method: ● Auto ○ Manual

LAN IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Begin IP: 192 . 168 . 0 . 2

DHCP End IP: 192 . 168 . 0 . 33

Lease Time: 240 Minute(1~4320)

By default this DHCP server feature is enabled for LAN segment. A default IP address pool is allocated by the CPE. It is not recommended to change this setting in general. If readers do wish to specify an IP pool manually, please be reminded that the Gateway for LAN segment should be the IP address of CPE's LAN interface.

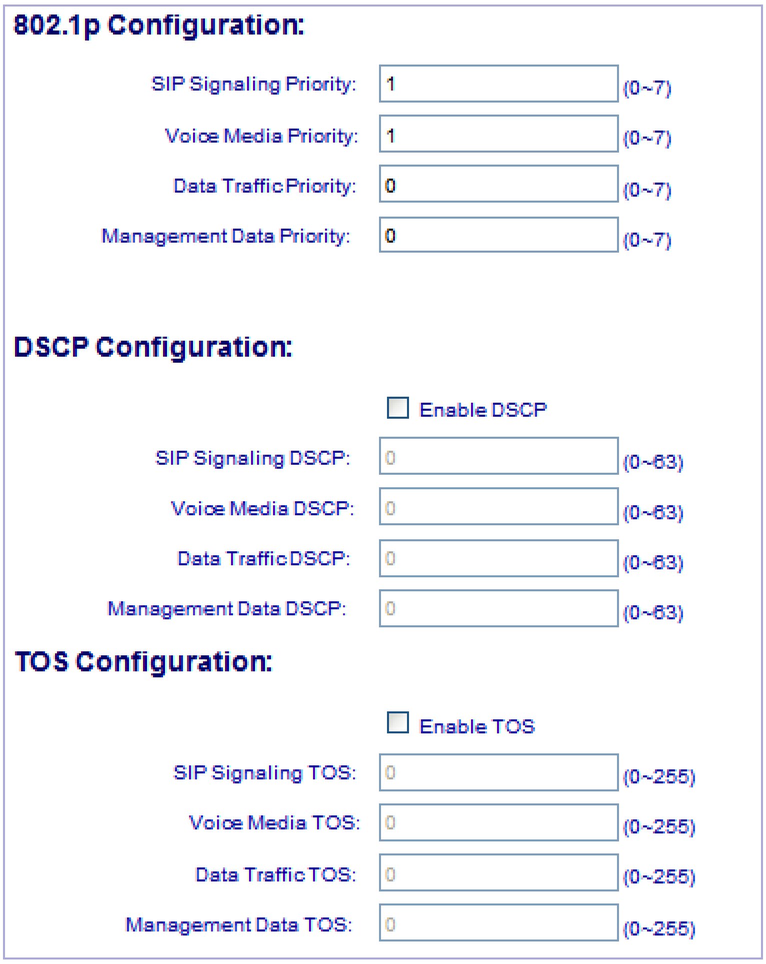
Notice	**The Gateway for LAN segment is usually the LAN interface of the CPE. If the IP pool for DHCP server is modified to other subnets, e.g. 192.168.1.0/24, the Gateway and IP address for the CPE LAN interface should be modified accordingly.**

7.3 QoS & VLAN

The CPE data traffic are classified into three types and each can be marked with certain QoS priorities, at layer two or layer three of the seven-layer OSI network model. At layer 2, 802.1p bits are used for QoS Marking. At layer 3, the DSCP field in IP header is used for QoS marking as shown by the following diagram. Note that DSCP and TOS marking cannot be configured at same time.

VLAN (Virtual Local Area Network) allows separation of traffic by a VLAN ID at layer two of the seven-layer OSI network model. VLAN may facilitate implementation of security measures, and QoS treatment. The CPE internally classifies traffic into three types, Voice (media and signaling), Data and Management traffic. The traffic types can be tagged with designated VLAN ID. All ingress traffics from LAN port are treated as data.

VLAN tagging for CPE LAN traffic can be enabled or disabled. VLAN IDs for Voice, Data and CPE Management traffic can be configured in this section. For the LAN port data, untagged LAN traffic will be automatically tagged at the WAN interface according to the traffic type.



802.1p Configuration:

SIP Signaling Priority:	1	(0~7)
Voice Media Priority:	1	(0~7)
Data Traffic Priority:	0	(0~7)
Management Data Priority:	0	(0~7)

DSCP Configuration:

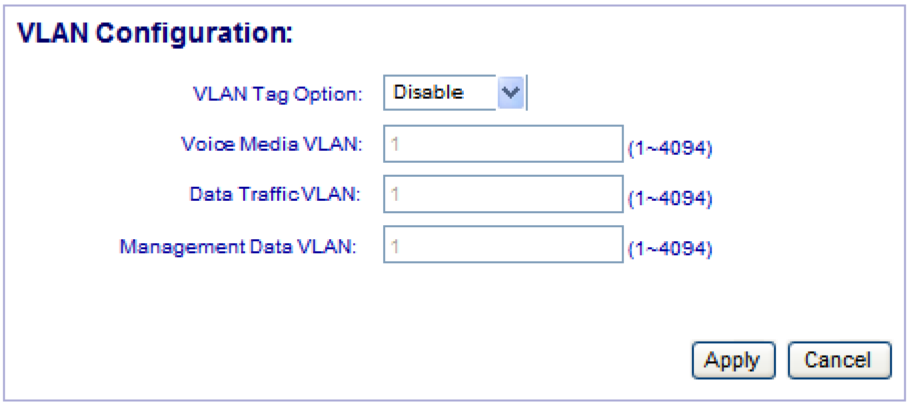
□ Enable DSCP

SIP Signaling DSCP:	0	(0~63)
Voice Media DSCP:	0	(0~63)
Data Traffic DSCP:	0	(0~63)
Management Data DSCP:	0	(0~63)

TOS Configuration:

□ Enable TOS

SIP Signaling TOS:	0	(0~255)
Voice Media TOS:	0	(0~255)
Data Traffic TOS:	0	(0~255)
Management Data TOS:	0	(0~255)

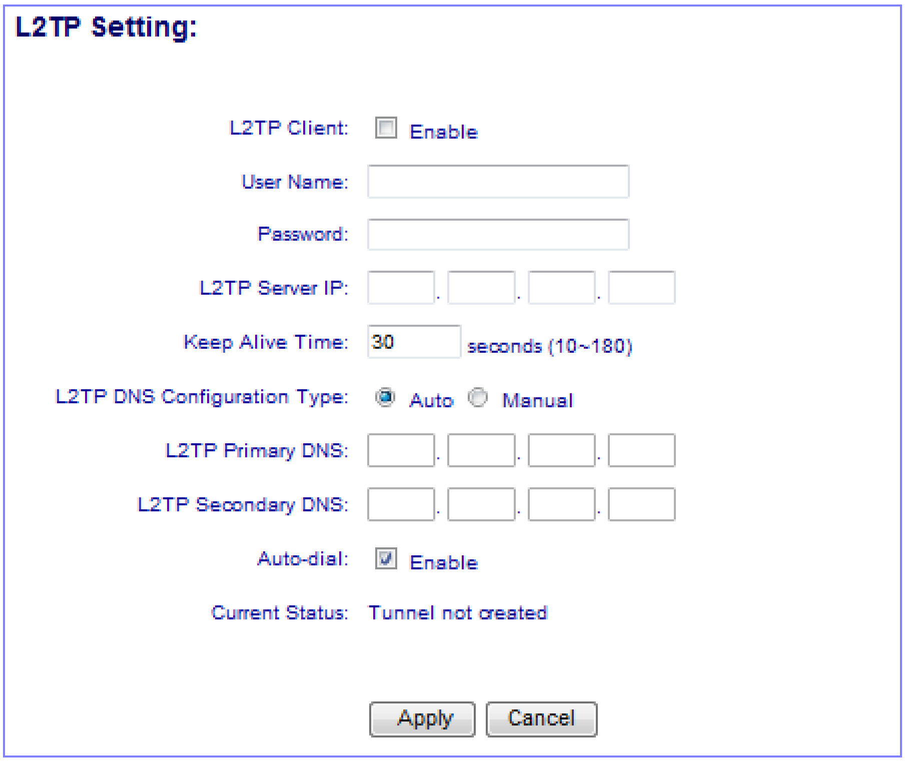


VLAN Configuration:

VLAN Tag Option:	Disable	
Voice Media VLAN:	1	(1~4094)
Data Traffic VLAN:	1	(1~4094)
Management Data VLAN:	1	(1~4094)

7.4 VPN Networking

To enable VPN networking for enterprise user, the CPE has integrated L2TP client function within the device. To use the L2TP function, the user needs to enable and configure the L2TP client as the following. Once the L2TP connection is established, all data from the LAN port will be forwarded to the L2TP server for processing.



L2TP Setting:

L2TP Client: □ Enable

User Name:

Password:

L2TP Server IP: . . .

Keep Alive Time: 30 seconds (10~180)

L2TP DNS Configuration Type: ● Auto ○ Manual

L2TP Primary DNS: . . .

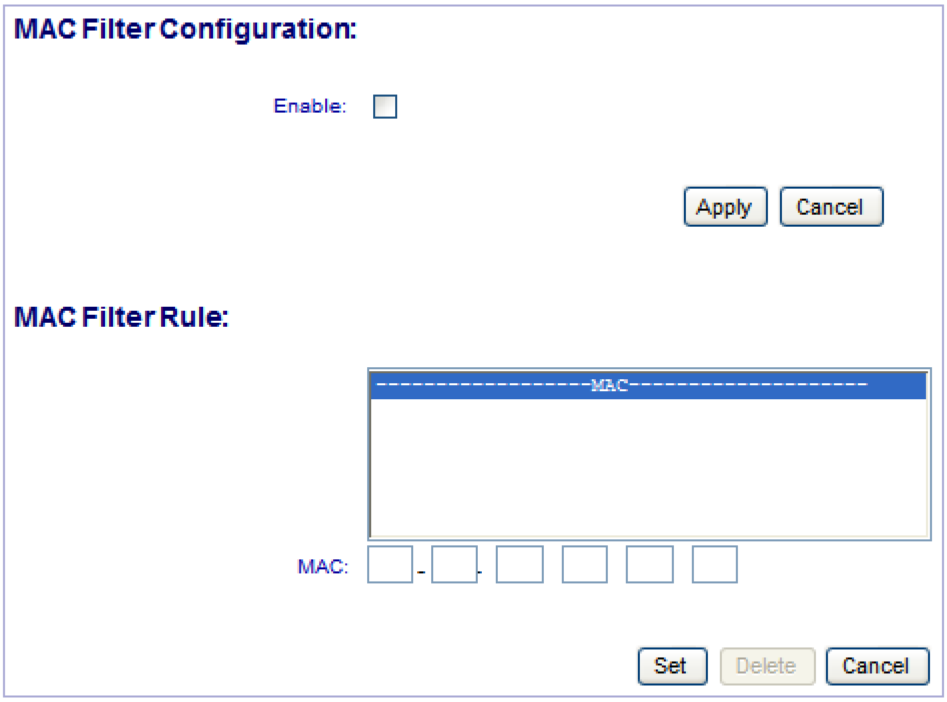
L2TP Secondary DNS: . . .

Auto-dial: ☑ Enable

Current Status: Tunnel not created

7.5 Access Control

User can enable and setup MAC Filer to prevent computers with specified MAC address from accessing to CPE.



MAC Filter Configuration:

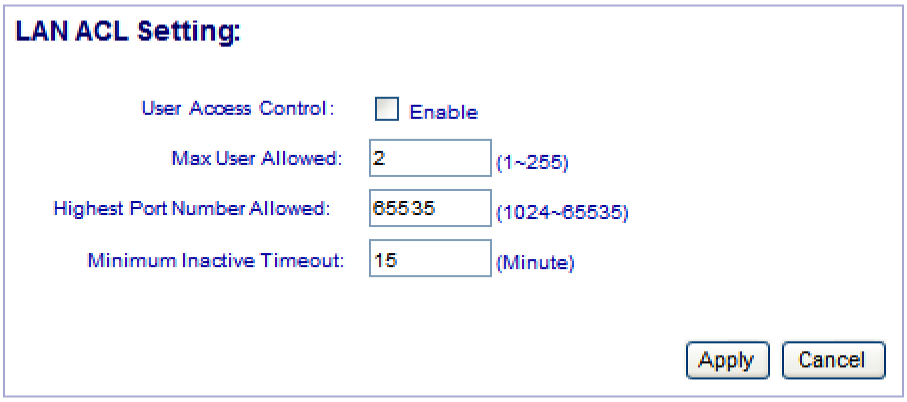
Enable: □

MAC Filter Rule:

-----------------MAC-------------------

MAC: - -

The operator can also configure the User Access Control to limit the device usage by the user. The Max User Allowed, Highest Port Number Allowed and Minimum Inactive Timeout can be configured to restrict the LAN device access.



LAN ACL Setting:

User Access Control: □ Enable

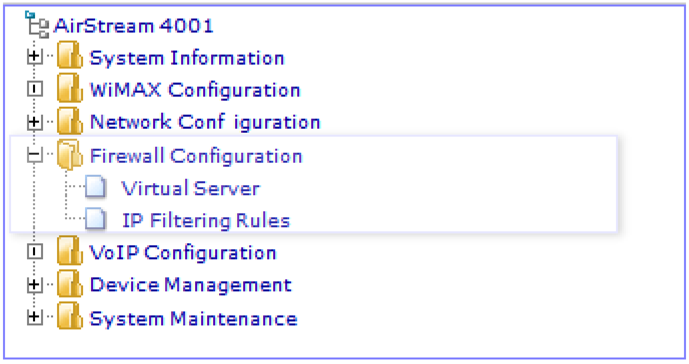
Max User Allowed: 2 (1~255)

Highest Port Number Allowed: 65535 (1024~65535)

Minimum Inactive Timeout: 15 (Minute)

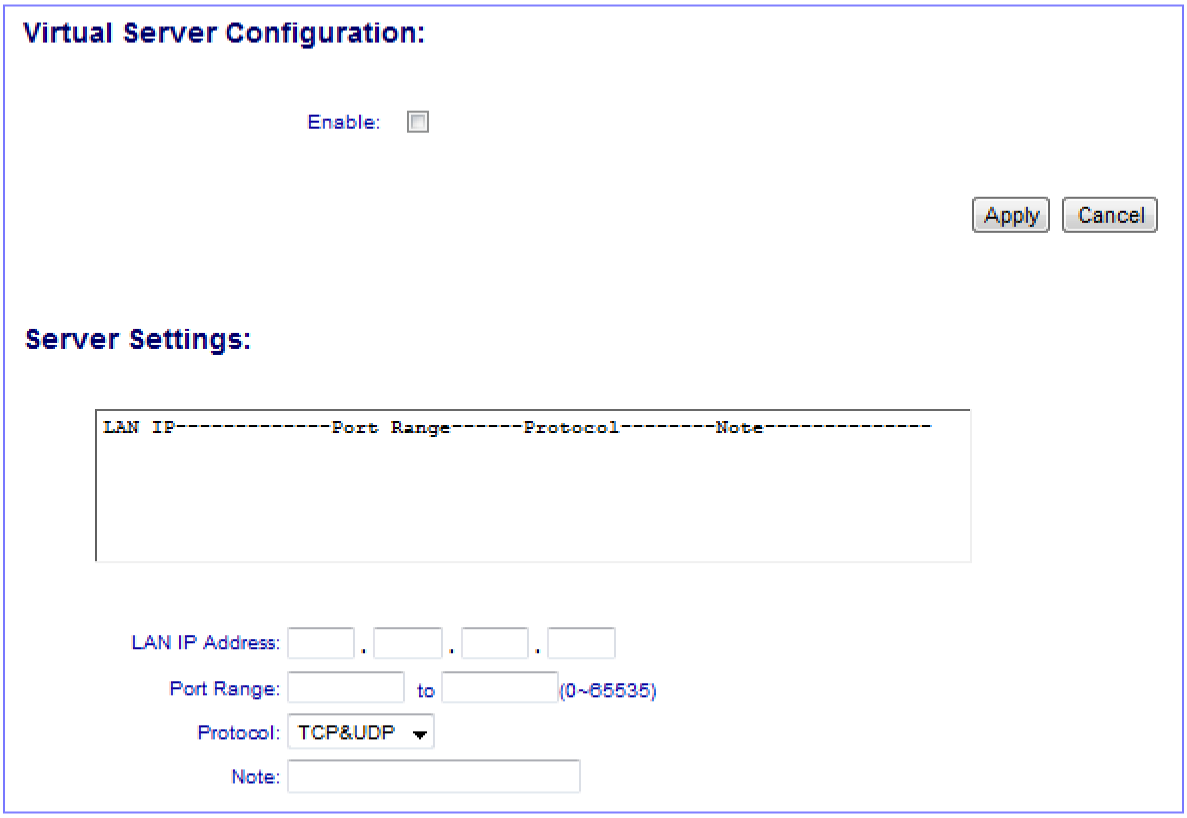
8 Firewall Configuration

Click “Firewall configuration” on the left configuration tree. And then you have the access to Virtual Server and IP Filtering Rules.



8.1 Virtual Server

Virtual Server function allows user to expose internal server to the Internet. The following configuration can be used to expose certain server IP and port number to Internet and support DMZ functions. Three traffic types (UDP, TCP, TCP&UDP) traffic types can also be specifed for virtual server mapping.



Virtual Server Configuration:

Enable: □

Server Settings:

```
LAN IP-------------Port Range------Protocol--------Note--------------
```

LAN IP Address: ___ . ___ . ___ . ___

Port Range: ___ to ___ (0~65535)

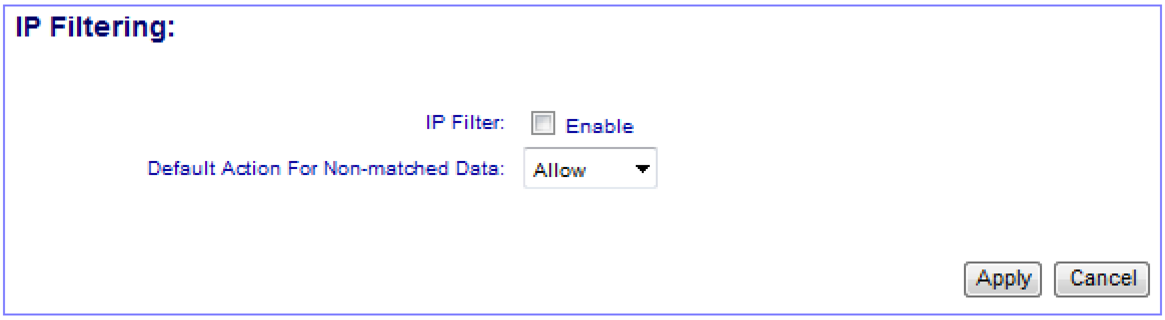
Protocol: TCP&UDP

Note: ___

8.2 IP Filtering Rules

IP Filter capability provides user the filter out unwanted traffic for security management. Either black or white rule can be specified for non-matching data traffic. The filtering rule can be created based protocol type, source and destination IP and port ranges.

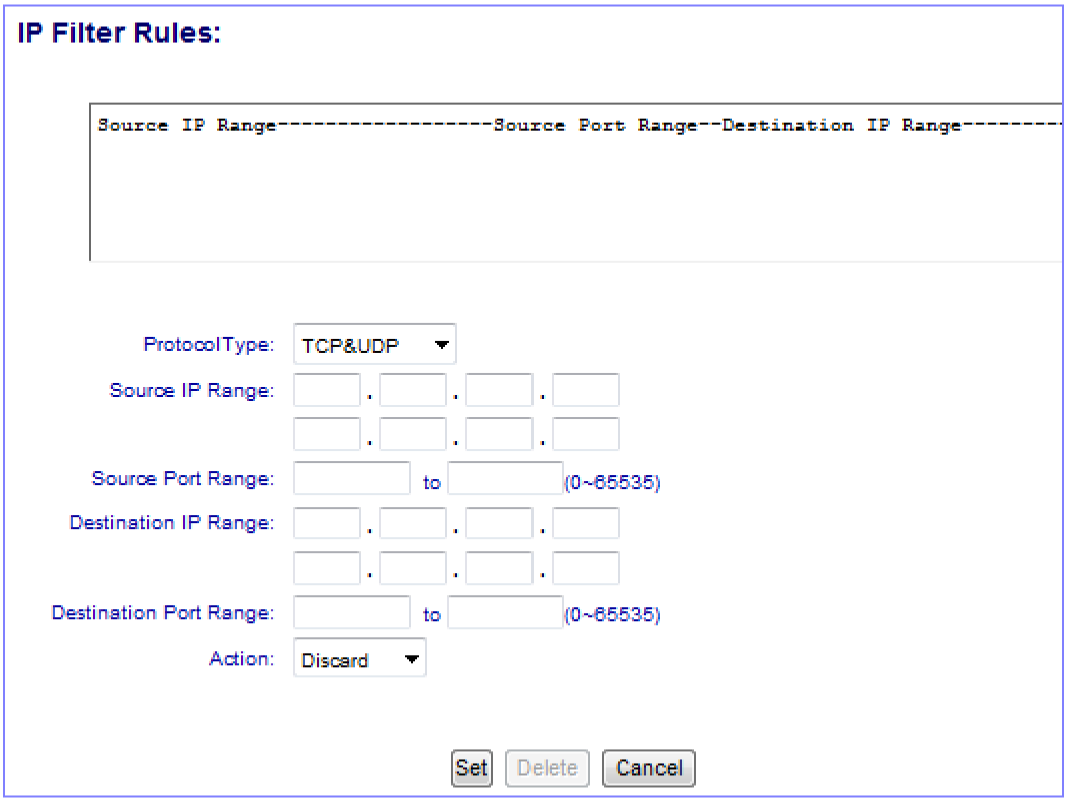
Note the IP filtering has a performance impact on the CPE processing capability. Therefore use is advised to minimize its usage whenever possible.



IP Filtering:

IP Filter: □ Enable

Default Action For Non-matched Data: Allow



IP Filter Rules:

```
Source IP Range------------------Source Port Range--Destination IP Range---------
```

ProtocolType: TCP&UDP

Source IP Range: . . .
. . .

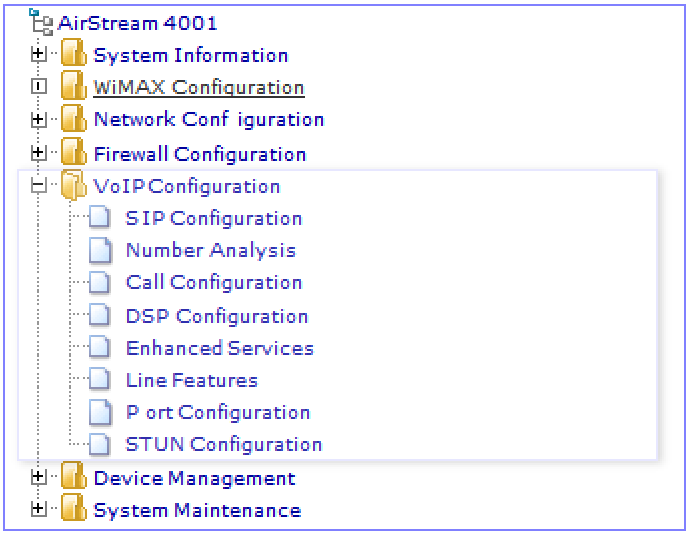
Source Port Range: to (0~65535)

Destination IP Range: . . .
. . .

Destination Port Range: to (0~65535)

Action: Discard

9 VoIP Configurations



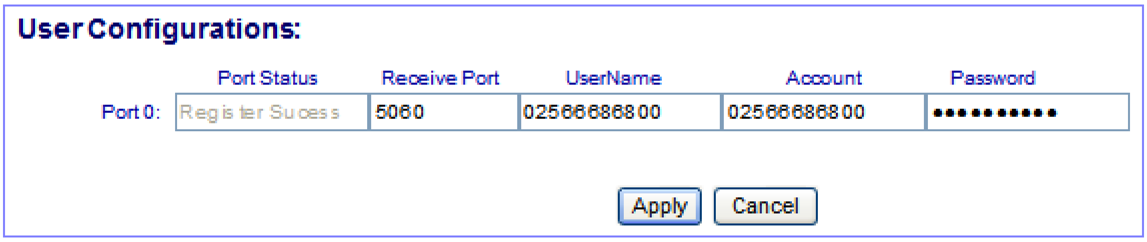
AirStream 4001
- System Information
- WiMAX Configuration
- Network Conf iguration
- Firewall Configuration
- VoIPConfiguration
  - S IP Configuration
  - Number Analysis
  - Call Configuration
  - DSP Configuration
  - Enhanced Services
  - Line Features
  - P ort Configuration
  - STUN Configuration
- Device Management
- System Maintenance

9.1 SIP Configuration

SIP related configurations concern CPE as a SIP client, Registrar and Proxy Servers.

Click on “SIP Configuration” in the Configuration Tree to access the related web management page.

9.1.1 User Configuration

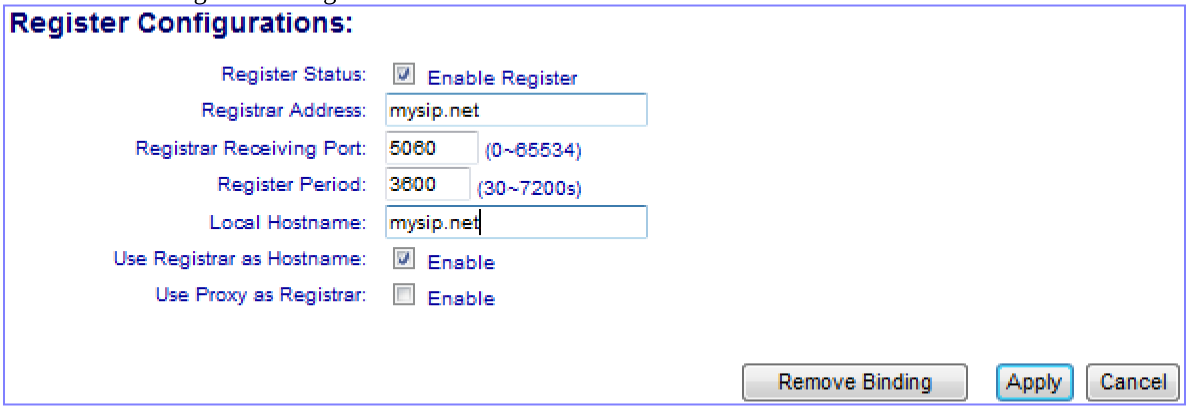


User Configurations:

	Port Status	Receive Port	UserName	Account	Password
Port 0:	Regis ter Sucess	5060	02566686800	02566686800	●●●●●●●●●●●

Internally FXS ports are counted from 0. Phone line 1 maps to FXS Port No 0. “User ID” maps to dial number. Apply settings if changes are made in the above section.

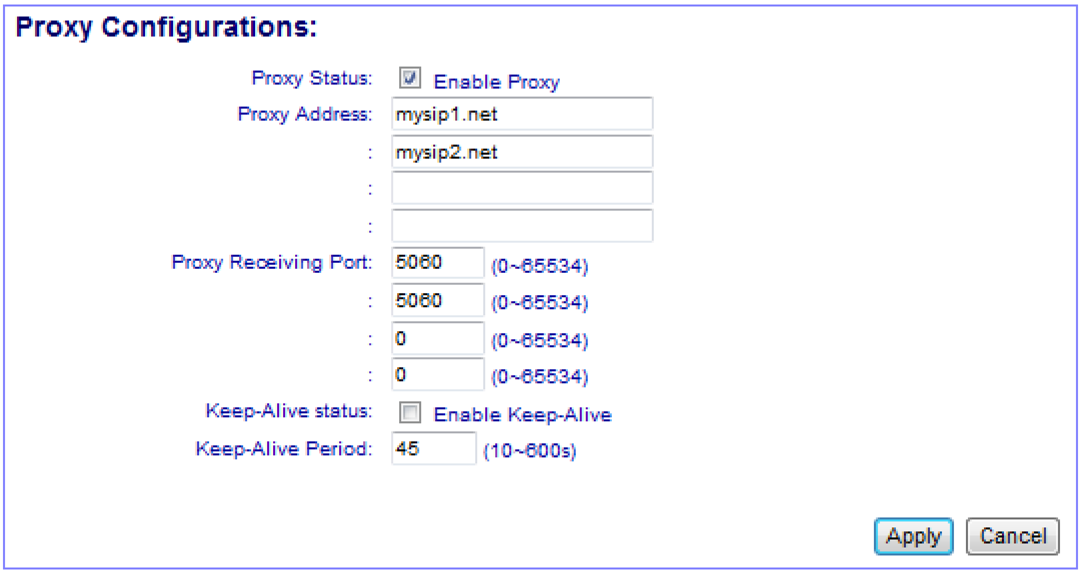
Next comes to Registrar configurations.



Register Configurations:

Register Status:	☑ Enable Register
Registrar Address:	mysip.net
Registrar Receiving Port:	5060 (0~65534)
Register Period:	3600 (30~7200s)
Local Hostname:	mysip.net
Use Registrar as Hostname:	☑ Enable
Use Proxy as Registrar:	☐ Enable

When “Enable Register” is enabled, registration message will be sent out. However when “Use Proxy as Registrar” is enabled, all registration message is sent to the IP address of the Proxy. When “Enable Register” is disabled, the IX253P CPE may be configured for point to point communications, which is typically used by an enterprise owning multiple office sites. Apply settings if changes are made in the above section.

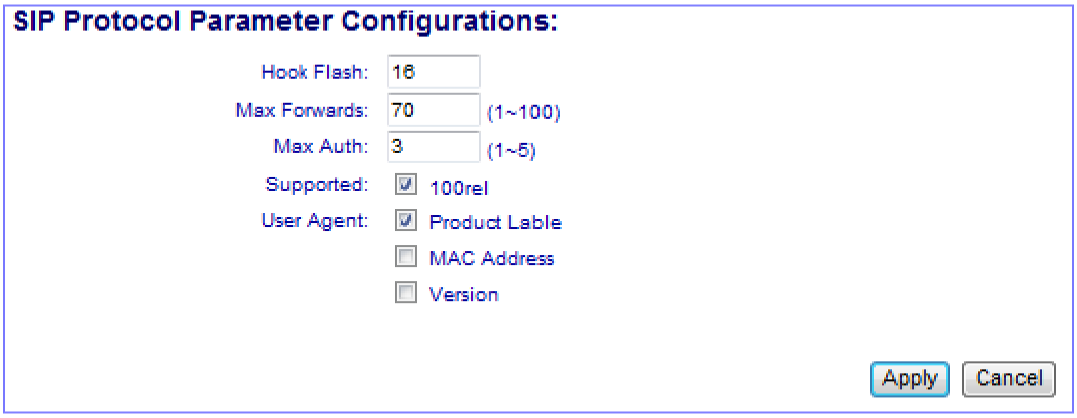


Proxy Configurations:

Proxy Status:	☑ Enable Proxy
Proxy Address:	mysip1.net
:	mysip2.net
:	
:	
Proxy Receiving Port:	5060 (0~65534)
:	5060 (0~65534)
:	0 (0~65534)
:	0 (0~65534)
Keep-Alive status:	□ Enable Keep-Alive
Keep-Alive Period:	45 (10~600s)

Proxy can be enabled and configured. And if more than one Proxy Addresses are supplied, the CPE will try each Proxy sequentially if a request to a Proxy times out with no responses. Apply settings if changes are made in the above section.

After completing all settings, you may uncheck “Enable Register” and apply settings to de-register the FXS port. Check “Enable Register” and apply settings again to perform another registration. If a registration is successful, “Port Status” under “User Configurations” should show “Register Success”.

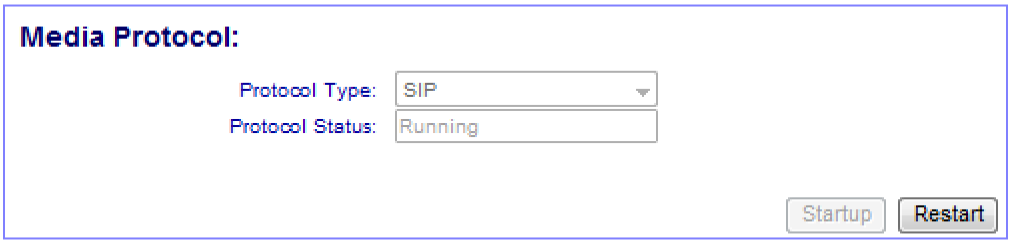


SIP Protocol Parameter Configurations:

Hook Flash:	16
Max Forwards:	70 (1~100)
Max Auth:	3 (1~5)
Supported:	☑ 100rel
User Agent:	☑ Product Lable
	□ MAC Address
	□ Version

SIP Protocol parameters, such as Hook Flash, Max Forwards and Max Auth can be configured.

For service provider networks, the SIP control protocol is the mainstream protocol selected by the telecommunication standardization bodies. For example, 3GPP and 3GPP2 have adopted SIP as the foundation for future communication networks.



Media Protocol:

Protocol Type:	SIP
Protocol Status:	Running

The CPE need not be reset if changes are made at application level, e.g. Proxy IP address change. However the media protocol can be restarted to effect changes.

Different VoIP network equipment vendors may have implemented SIP protocol in different ways. Table below summarizes the use of configuration values in various SIP messages.

Mapping of Configuration to SIP Messages

	Usage in SIP Messages	REGISTER and INVITE Message	Other SIP Messages
User ID	the "username" part of SIP URI in From, To, Contact attributes, e.g. "85412006" in 85412006@myisp.net. (The "host" part of SIP URI is taken from "Local Hostname" field.)	the "username" and "displayname" part of SIP URI in From, To, Contact attributes	the "username" and "displayname" part of SIP URI in From, Contact headers
Auth ID	the username used for digest authorization in REGISTER and INVITE requests	the "digest username" in Authorization attributes	usually not used
Auth Password	the password used for digest authorization in REGISTER and INVITE requests	used to calculate the "response" in Authorization attributes	usually not used
Registrar Address	the "request URI" in REGISTER request. It could be a domain name, or an IP address.	Request-URI, for example sip:mysip.com. Not used in INVITE message.	usually not used
Local Hostname	the "host" part of SIP URI in From “Attributes”. It could be a domain name e.g. "mysip.com" in , or an IP address. ("username" is taken from User ID field.)	the "host" part of SIP URI in From, To attributes	the "host" part of SIP URI in From, To headers and Request-URI
Proxy Address	the destination IP address to which SIP messages are sent to. It does not affect the content in SIP messages.	the destination IP address to which SIP messages are sent to	the destination IP address to which SIP messages are sent to

In SIP standards, the “User ID” could be a mix of alphabetic and numeric digits. However, in a network with analogue phones, “User ID” is recommended to use numeric digits only as the CPE takes user inputs from phone pad to construct “User ID” of the called party.

The “User ID” field should consist of numeric digits only.

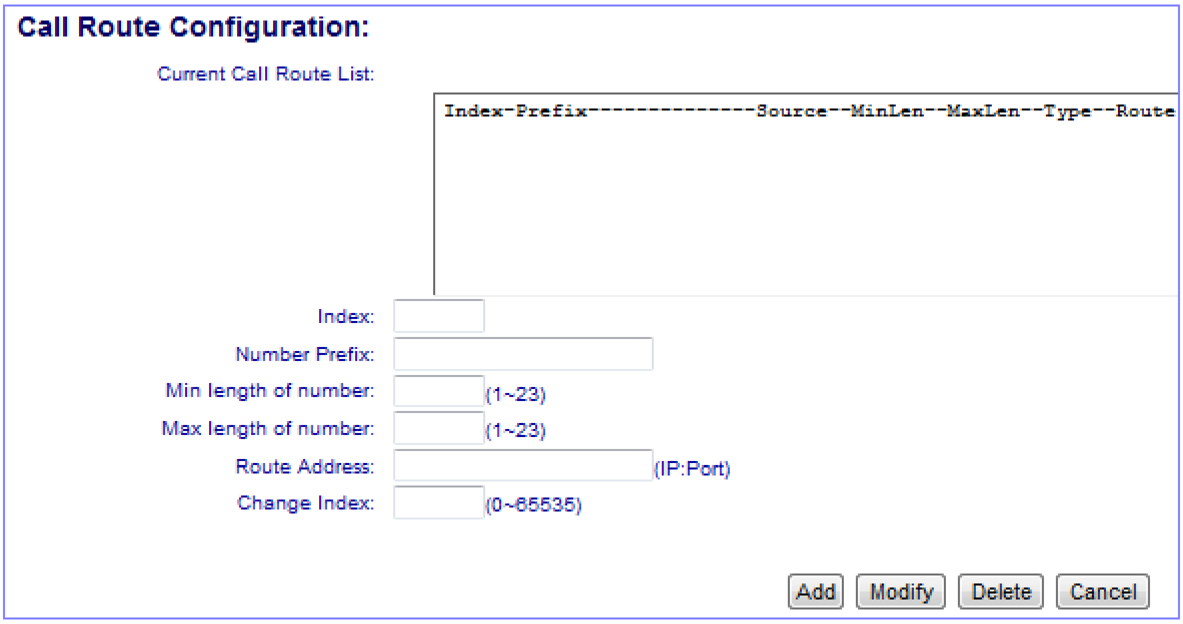
9.2 Number Analysis Configuration

The CPE collects dial numbers from external phone or fax. Dialed digits are analyzed before being sent out to other element in a VoIP network. Dial numbers can be modified according to specific needs. Rules can be setup to modify a dial number, if it meets certain condition.

Click on “Number Analysis Configuration” in the Configuration Tree. Conditions and associated actions on dial numbers are displayed in the detailed configuration window.
The conditions are defined in Call Route Configuration section. The actions are defined in Number Change Configuration section.

9.2.1 Conditions to Modified Dial Numbers

The Current Call Route List table shows conditions that triggers certain action on a dialed number string.



Call Route Configuration:

Current Call Route List:

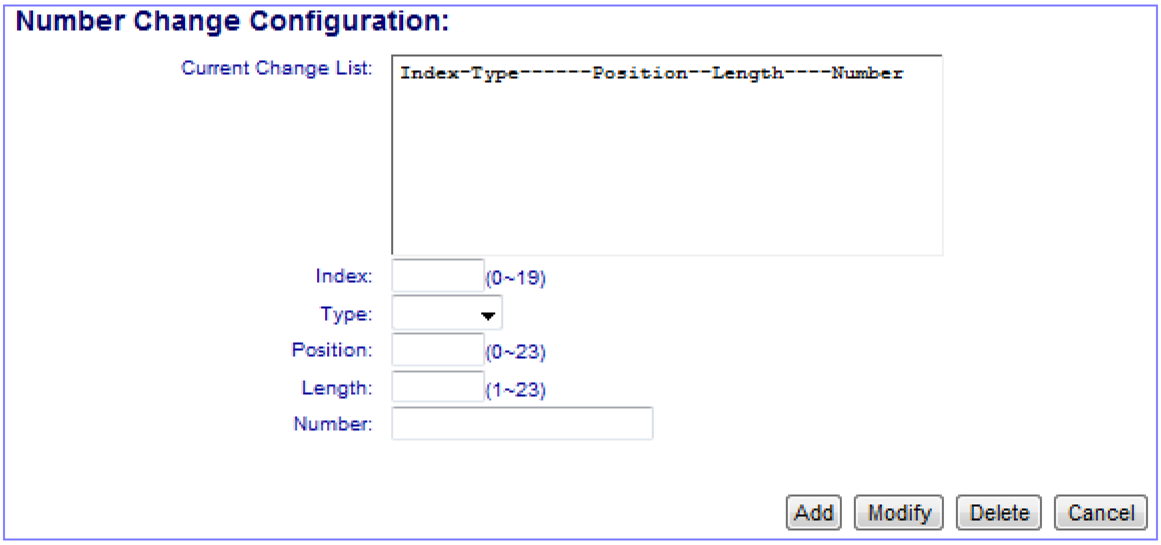
```
Index-Prefix--------------Source--MinLen--MaxLen--Type--Route
```

- “Number Prefix”, “Min Length of Number”, and “Max Length of Number” are used in combination to define a condition.
- “Route Address” may specify another SIP capable node to route a call. If this field is left empty, configuration in User Agents setup applies. This feature was widely used for point to point calls without involvement of Proxy servers, in early years of VoIP network evolution.
- “Change Index” specifies the index of an action in “Current Change List” table to be taken, if a dial number matches with the condition.

Example in the table shows that dial numbers starting with 021, is subject to the change defined in action 0 defined in the Current Change List.

9.2.2 Number Change Configurations

The “Number Change Configuration” section defines the actions to be taken, if a dial number meets certain conditions defined in “Call Route Section”.



Number Change Configuration:

Current Change List:

```
Index-Type------Position--Length----Number
```

- “Index” defines the index of action.
- “Type” defines type of changes. Certain digits can be inserted into a dialed number. Digits in a dial number can also be modified or deleted.

In the example, the change action, defined by entry with “Index” 0 in the “Current Change List”, inserts “8541 from the 3rd position of the number string.

So a dial number 0212401 is modified to 021 8541 2401 before the CPE device sends out a call invite.

9.3 Call Configuration

Call Configuration section defined a few behavior when a call is outgoing or incoming. Click on “Call Configuration” in the Configuration Tree. The following sections will be displayed in the detailed configuration window:

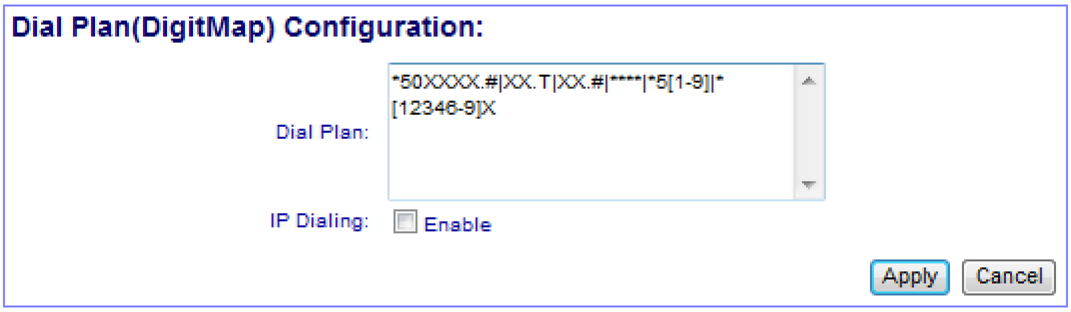
9.3.1 Dial Plan Configuration

The CPE collects dial numbers from external phone or fax. Dialed digits are collected as a whole before they are encapsulated in a call Invite message.

By default the CPE takes five second idle time after the last punch, as completion of user input. Digit mapping are introduced to allow faster recognition of dial completion. If the dialed digits, input by user from the phone pad, map with any pattern of DigitMaps defined in this section, collected digits are immediately processed.

Maximum 500 digit maps can be defined. Each digit map may consist up to 2048 characters. In the “Dial Plan (DigitMap) Configuration” textbox, each digitmap are separated by an “|” character. The string “XX.T|XX.#|P|****” consists of four digit maps:

- “*XX” means an asterisk followed by 2 digit of any number. Dial strings matching this pattern are used for service codes, which allows user interaction by end users, e.g disable or enable call forwarding. Refer to 9.5.1 for more detailed information.
- In “XX.T”, “XX” means any digits. “.” means any number of digits. T means a timer. The entire string means CPE wait for T seconds after the last user punch on phone pad.
- In “XX.#”, “XX” means any digits. “.” means any number of digits. The entire string means dialed digits can be processed by press “#” button. Whenever CPE receives an “#”, CPE considers that user inputs has completed, and start processing digits before “#” immediately.
- The last digit map “****” is defined for use by CPE itself. When user press “****”, the IP address of the CPE is announced in the ear set of the phone.



Dial Plan(DigitMap) Configuration:

Dial Plan: *50XXXX.#|XX.T|XX.#|****|*5[1-9]|*[12346-9]X

IP Dialing: □ Enable

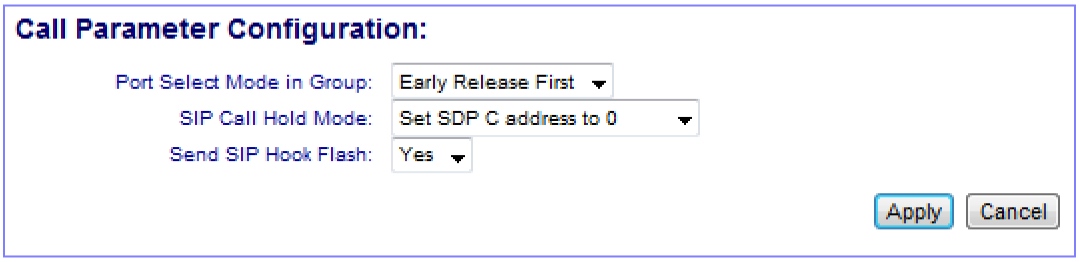
When IP Dialing is enabled, the CPE also allows call origination to an IP address input by user from key pads of a phone.

For example, call to 1000@10.3.50.55:5060 can be dialed by pressing the following numbers: 1000**10*3*50*55**5060.

9.3.2 Multiple Lines using a Single Account

Multiple phones may share one SIP address, or account. Port number 0-3 may use exactly the same “User ID”, “Auth Username”, etc. Phones connected to any port can make outgoing calls.

In this scenario, if there is an incoming call to the “User ID”, which local phone should ring? This is defined in “Call Parameter Configuration” in this section.



Call Parameter Configuration:

Port Select Mode in Group: Early Release First

SIP Call Hold Mode: Set SDP C address to 0

Send SIP Hook Flash: Yes

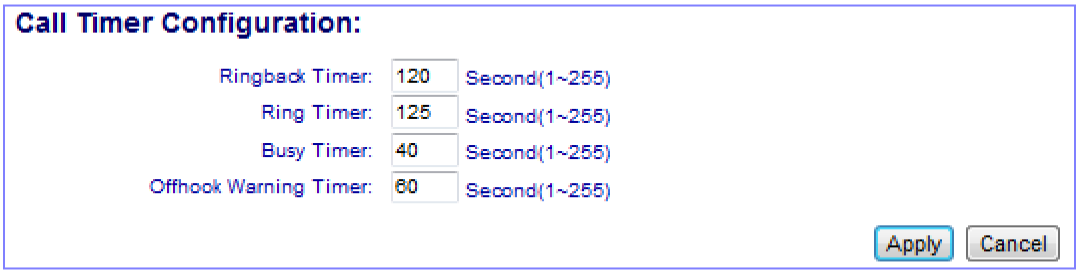
A few options are available in the drop down list of Port Select Mode in Group:

- Early Release First: the line which was released earliest receives an incoming call.
- Random: an incoming call is randomly dispatched to one of the lines.
- Order: an incoming call is dispatched to lines sequentially.

9.3.3 Call Timers

A few timers are defined in this section:

- Ringback Timer: A ringback tone, or audible ringing tone or ringback signal, is the audible ringing that is heard on the telephone line by the calling party after dialing and prior to the call being answered at the distant end. When A calls B from a CPE, if B does not answer the call, the "Ringback Timer" defines the maximum waiting time after which the CPE should tear down the call, (if A does not hang up the phone).
- Ring Timer: A ring tone is the sound made by a telephone to indicate an incoming call. When B calls A at a CPE, if A does not answer the call, the "Ring Timer" defines the maximum waiting time after which the CPE should tear down the call, (if B does not hang up the phone).
- Busy Timer: when A calls B, if B is busy, the "Busy Time" defines the maximum waiting time that the CPE should tear down the call, (if A does not hang up the phone).
- Offhook Warning Time: The maximum waiting time after which the CPE should send warning signals to the line.



Call Timer Configuration:

Ringback Timer: 120 Second(1~255)

Ring Timer: 125 Second(1~255)

Busy Timer: 40 Second(1~255)

Offhook Warning Timer: 60 Second(1~255)

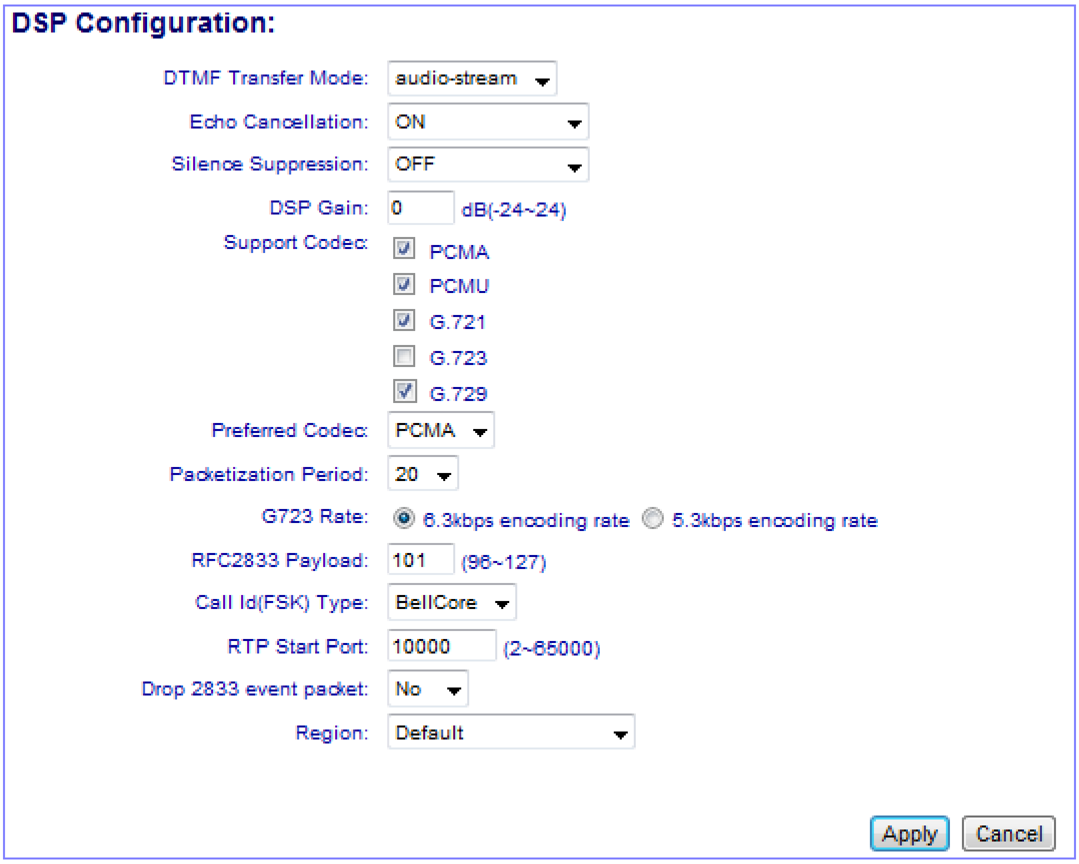
9.4 DSP Configuration

Voice is sampled and coded into digital bit stream, before they are packetized into IP packets. The following sections discuss various Codecs supported by the CPE

The parameters are explained in more details:

- DTMF Transfer Mode: DMTF stands for Dual-Tone Multi-Frequency (DTMF) signaling, which is used for transfer of telecommunication signal over the line in the voice-frequency band in legacy PSTN networks. In VoIP networks, legacy devices continues to use DMTF to send busy signal, Flash or alphanumerical digits. For example, a user may be required to key in a password to join a conference call, which is sent from legacy phone as DTMF signal, across the IX253P CPE, to the conference bridge. There are a few ways to transport DMTF tones from legacy devices, over a VoIP network.
    - Audio Stream: DTMF signals from legacy phones are packetized in RTP packets as audio stream. Transporting DTMF user inputs as audio stream works well in a data network with

good quality. However, in networks with poor quality, packet losses or disordered delivery of RTP packet may cause error. An alphanumerical digit input by the caller may be interpreted wrongly as another digit.



DSP Configuration:

DTMF Transfer Mode: audio-stream

Echo Cancellation: ON

Silence Suppression: OFF

DSP Gain: 0 dB(-24~24)

Support Codec: ☑ PCMA ☑ PCMU ☑ G.721 ☐ G.723 ☑ G.729

Preferred Codec: PCMA

Packetization Period: 20

G723 Rate: ● 6.3kbps encoding rate ○ 5.3kbps encoding rate

RFC2833 Payload: 101 (96~127)

Call Id(FSK) Type: BellCore

RTP Start Port: 10000 (2~65000)

Drop 2833 event packet: No

Region: Default

  - RFC2833: As a second option, the CPE can recognize the tones and translate them into a name, such as numeric input, or Flash. RFC2833 defined payload format for named telephone events, such as numeric input, or Flash.
  - Signal: means the DTMF tones are translated to application level parameters such as SIP.

- Echo Cancellation: can be turned ON or OFF.

- Silence Suppression: can be turned ON or OFF.

- DSP Gain: Default value is 0. It may be adjusted to increase or decrease voice volume.

- Supported Codec: IX253P CPE supports automatic negotiation of codec with the network. The Supported codecs, namely PCMa, PCMu, G.726, G.723, and G.729, are announced to the called party in SIP Invite messages.

- Preferred Codec: Preferred Codec should be chosen in line with service provider's strategy.

- Packetization Period: The period that a voice bit stream is packetized into an IP packet. The shorter the period, the less delay of voice. Typical values are 5, 10, 20 milliseconds.

- G723 Rate: G723 supports two encoding data rate. This option allows the choices of encoding rate using G.723 encoders.

- RFC2833 Payload: The payload value to send DMTF tones according to RFC2833.

- FSK Type: Frequency-shift keying (FSK) is a form of frequency modulation in which the modulating signal shifts the output frequency between predetermined values. DTMF is one of the FSK applications. It supports BellCore, ETSI, NTT options.

Information	G.723 and G.729 cannot be enabled at same time. PCMu or PCMa Law can be chosen in Line Configurations. Only one codec can be used at a time.

Most legacy fax devices adopt ITU-T Group 3 fax protocol published in 1990. The protocol is composed of server standards that specify different parts the fax call. Amongst them T.30 specification defined procedure to set up a fax call, determine the image size, encoding, transfer speed, the demarcation between pages, and the termination of the call. T.30 also references the various modem standards for handshaking (V.21 Channel 2 Model at 300mbps), and for image transfer (V.27 Ter, V.29, V.17, and subsequently V.34).

The simplest approach to transfer fax over an IP network is the bypass mode. CPE or other gateway devices simply samples all transmissions from fax machine using PCM (Pulse-code modulation) at 64kbps, and transports the bit string to the other gateway at edge of the network.

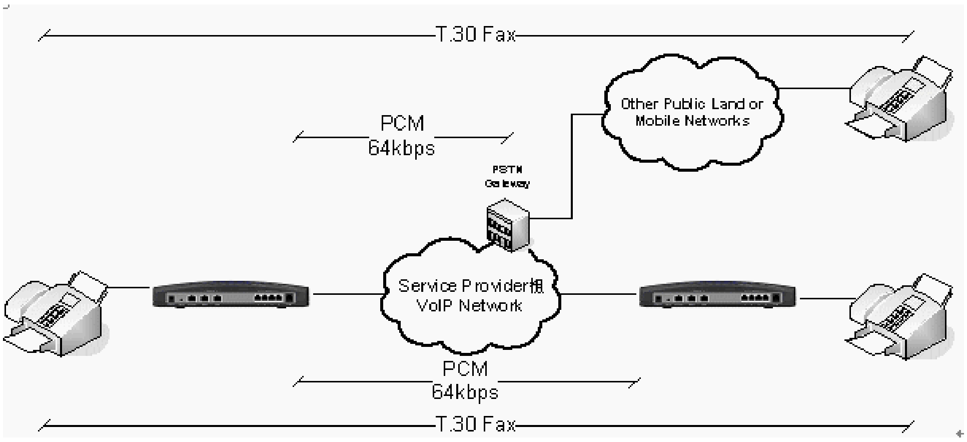

T.30 Fax
Other Public Land or Mobile Networks
PCM 64kbps
PSTN Gateway
Service Provider相 VoIP Network
PCM 64kbps
T.30 Fax

Figure 4. Transfer of T.30 Faxes in Transparent Mode

Transparent transfer provides no protection to packet loss, and requires big buffer in the in the gateway device to combat network delay jitter. Tolerance of round trip delay for the IP network is a stringent 2 seconds. Delay longer than that will cause failure of fax transmission.

More reliable and preferred method of delivery fax via an IP network is fax relay. The T.38 fax relay standard was devised in 1998 as a way to permit faxes to be transported across IP networks between existing G3 fax terminals.

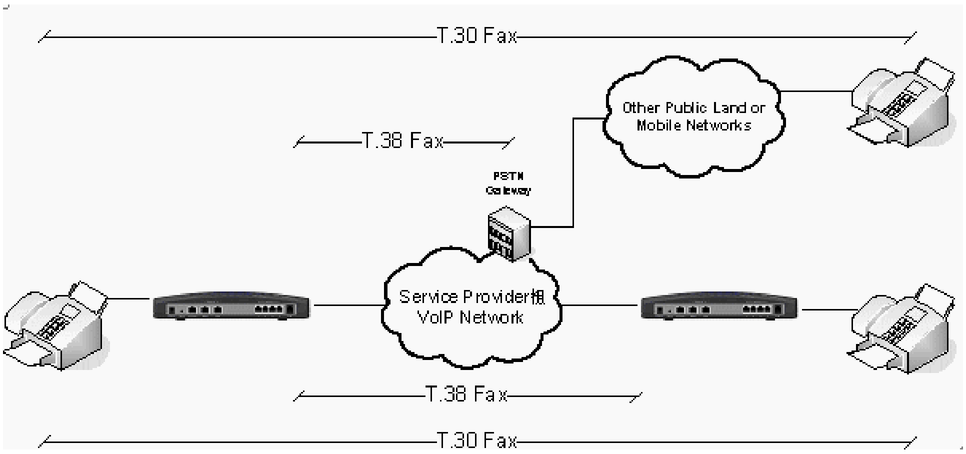
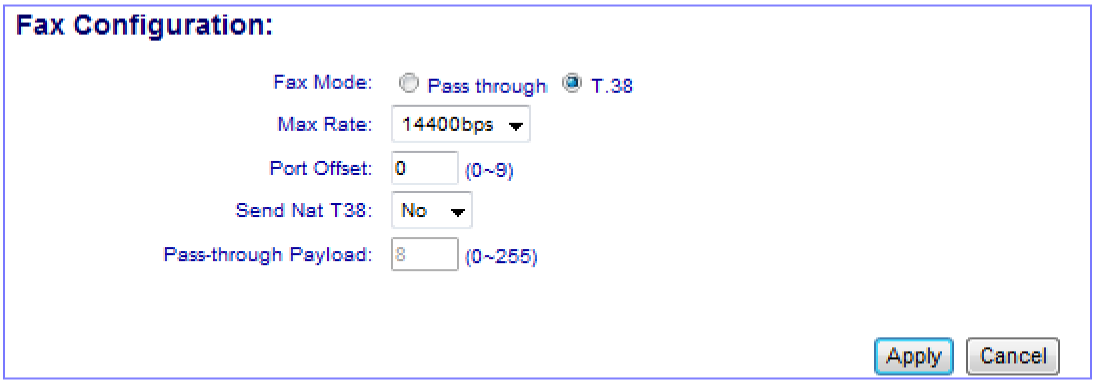

T.30 Fax
Other Public Land or Mobile Networks
T.38 Fax
PSTN Gateway
Service Provider相 VoIP Network
T.38 Fax
T.30 Fax

Figure 5. Transfer of T.30 Faxes using T.38 Fax Relay



Fax Configuration:

Fax Mode: ○ Pass through ● T.38

Max Rate: 14400bps

Port Offset: 0 (0~9)

Send Nat T38: No

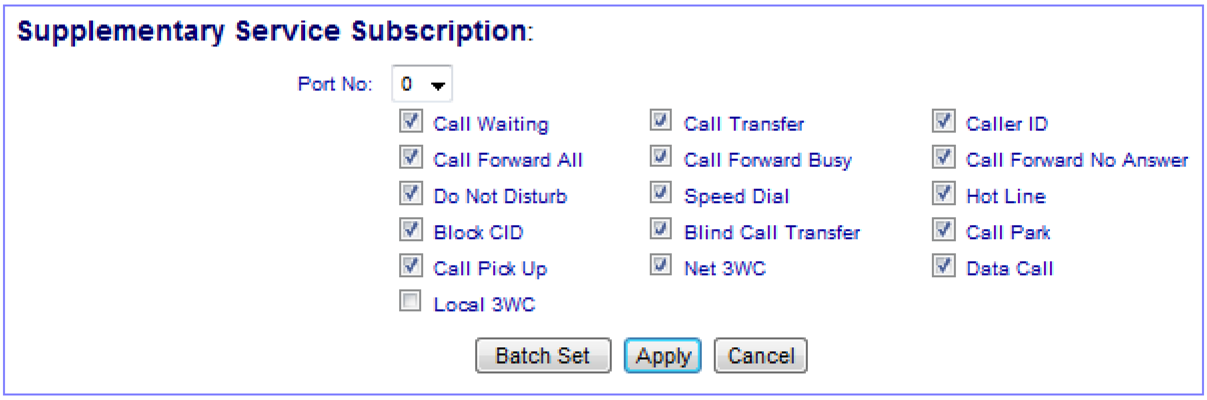
Pass-through Payload: 8 (0~255)

The configurations are explained in more details:

- Fax Mode: Transparent or T.38. The later is more preferred.
- Rate Management: Local TCF, and Transferred TCF. At this moment only Transferred TCF is supported.
- UDP Error Correction: Redundancy or FEC. At this moment, only Redundancy is supported. Redundancy method means payload transmitted in previous IP packet is repeated in a later packet.
- Max Buffer: (100~65535)
- Max Datagram: (50~65535)
- Max Rate: 2400bps, 4800bps, 7200bps, 9600bps, 12000bps, 14400bps.
- Port Offset: (0~9)
- Send NAT T38: No or Yes. If an external session boarder gateway is implemented in the network, choose No.

9.5 Enhanced Services

The CPE supports a rich set of supplementary services. Click on "Enhanced Services", the following Supplementary Service Subscription are displayed in the right frame of browser window:



Supplementary Service Subscription:

Port No: 0

☑ Call Waiting ☑ Call Transfer ☑ Caller ID
☑ Call Forward All ☑ Call Forward Busy ☑ Call Forward No Answer
☑ Do Not Disturb ☑ Speed Dial ☑ Hot Line
☑ Block CID ☑ Blind Call Transfer ☑ Call Park
☑ Call Pick Up ☑ Net 3WC ☑ Data Call
□ Local 3WC

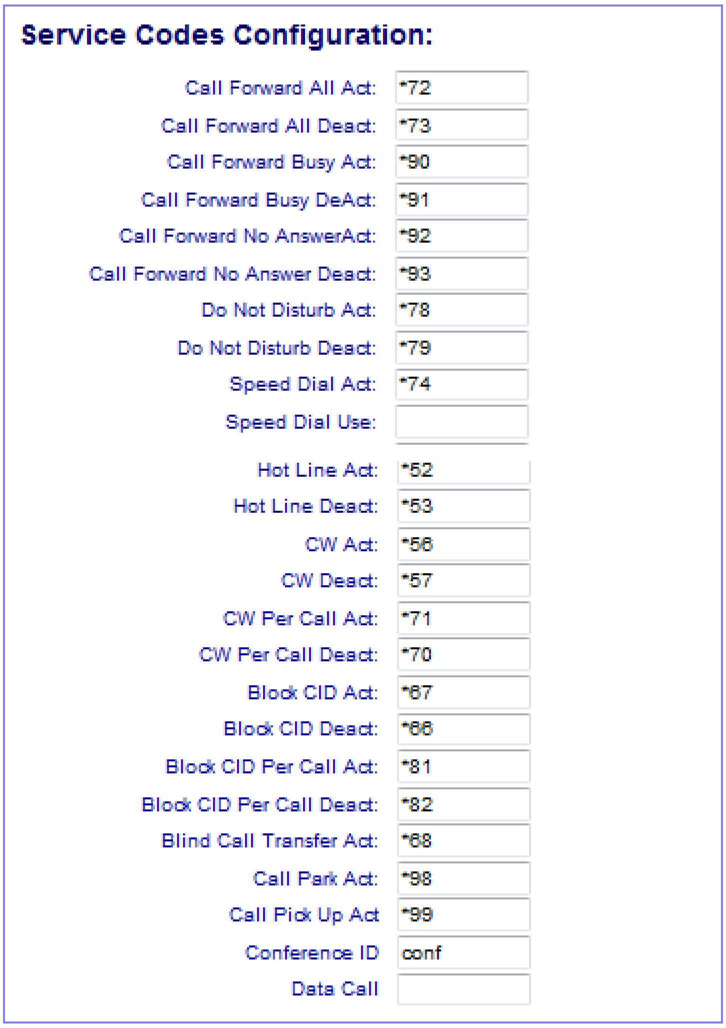
The CPE provide three level of control to supplementary services:

- Is the service enabled? Typically this is controlled by the service provider.
- Is the service activated? Typically this is controlled by end user, e.g. he may activate "call forwarding no answer" before he leaves his desk and goes home. Users may dial services codes to activate or activate these features.
- What parameter should be used for certain feature, e.g. which number to forward a call? This is

specified by user by dialing the service codes, e.g. *90075533639088 specifies that incoming calls should be forwarded to 075533639088.

9.5.1 Service Codes Configuration

Many of the enhanced services need to be provisioned with the proper activation codes to work with the soft switch. The default service codes are displayed below. Service codes are configurable.



Service Codes Configuration:

Call Forward All Act:	*72
Call Forward All Deact:	*73
Call Forward Busy Act:	*90
Call Forward Busy DeAct:	*91
Call Forward No AnswerAct:	*92
Call Forward No Answer Deact:	*93
Do Not Disturb Act:	*78
Do Not Disturb Deact:	*79
Speed Dial Act:	*74
Speed Dial Use:	
Hot Line Act:	*52
Hot Line Deact:	*53
CW Act:	*56
CW Deact:	*57
CW Per Call Act:	*71
CW Per Call Deact:	*70
Block CID Act:	*67
Block CID Deact:	*66
Block CID Per Call Act:	*81
Block CID Per Call Deact:	*82
Blind Call Transfer Act:	*68
Call Park Act:	*98
Call Pick Up Act	*99
Conference ID	conf
Data Call	

The Conference ID filed is used to set the corresponding network conference server name used in the network 3WC calling service (Applicable to Sonus Switch Only).

9.5.2 Use of Enhanced Services

The enhanced services are divided into local CPE terminal services and network services. Except Blind Call Transfer, Call Park and Call Pickup service codes are network based service activation codes, all other service codes are local CPE specific service codes. They are used by the user to activate or deactivate IAD local services via telephone dialing.

The CPE allows user to use a combination of flash hook and service codes dialing to access the enhanced services. The following combinations of operation are commonly used for user service operation.

Flash hook + press 1 – terminate the current call and connect to the held or new pending call.
Flash hook + press 2 – hold the current call and connect to the held call or new pending call.
Flash hook + press 3 – conference two calls that are being connected or held.

Some typical uses of the enhanced services are briefly described in the following as examples:

Call waiting:

For the second incoming call, the user has the following two options to take the new incoming call:

- Option 1 - flash hook and press 1, the old call will be dropped and the new call will be connected.
- Option 2 - flash hook and press 2, the old call will be hold and the new call will be connected. Flash hook and press 2 again will switch the connection to the previous call.

Call Transfer:

After receiving the call from the first party, user can flash the hook and dial the second party. After the second party answers the call, user has the following option to proceed:

- Option 1 - hang up the phone and transfer the first call to the second party.
- Option 2 - flash hook and press 1, the second party will be dropped and the first party will be connected.
- Option 3 - flash hook and press 2, the second party will be on hold and the first party will be connected. Flashing hook and press 2 again will switch the connection to the second party and etc.

Local and Net 3WC:

After establishing the two calls (one on hold and one connected), the user can conference three parties by flashing the hook and press 3. Of course, instead of conferencing, the user still has the option to switch calls by flash hook and press 1or 2.

Blind Transfer:

After receiving the call from the first party, the user dials the blind call transfer service codes (e.g. *68) and the second party number to transfer the call to second party. The user then hangs up the phone.

Call Park/Call Pickup:

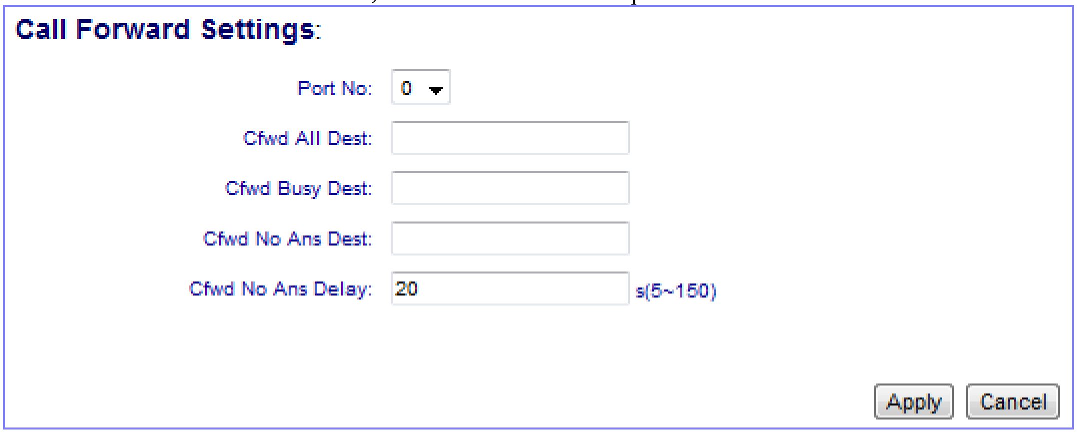
After receiving an incoming, the user flashes hook and dials the call park service code (e.g. *98) + another party number, the call will be parked for the second party in the network.

Another user can pickup the parked call by dialing the Call Pickup Service code of the call from the first party, and the user dials the blind call transfer service code (e.g. *99) and the second party number to retrieve the call.

If a parked call is not picked up within certain time, the call will be discarded by the system.

9.6 Line Features

User Settings specify user specific parameters for supplementary services. These settings will remain even their associated features are deactivated, so that users are not required to set them next time.



Call Forward Settings:

Port No: 0

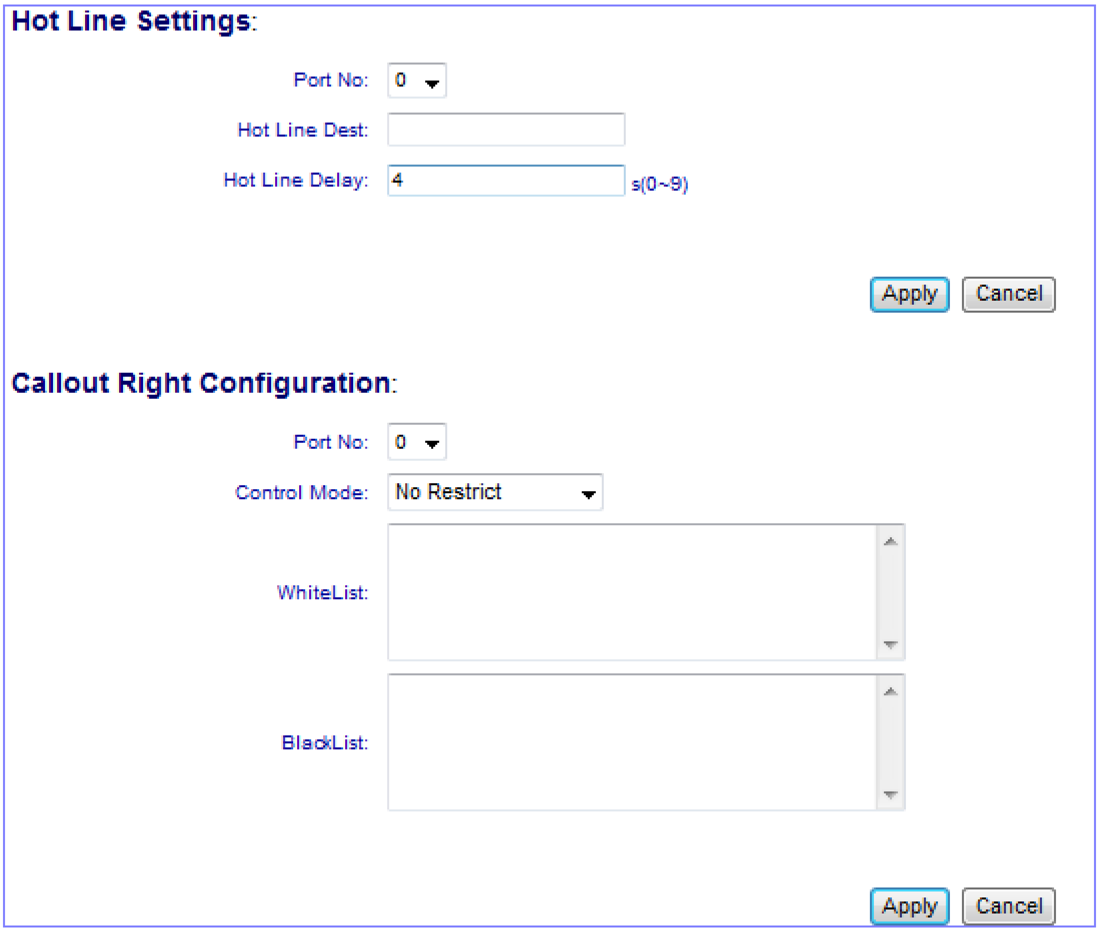
Cfwd All Dest:

Cfwd Busy Dest:

Cfwd No Ans Dest:

Cfwd No Ans Delay: 20 s(5~150)

Hotline refers to automatic dialing out to a pre-determined number, if a user takes a phone off hook but dials nothing. Hotline is configured on per FXS port basis.



Hot Line Settings:

Port No: 0

Hot Line Dest:

Hot Line Delay: 4 s(0~9)

Callout Right Configuration:

Port No: 0

Control Mode: No Restrict

WhiteList:

BlackList:

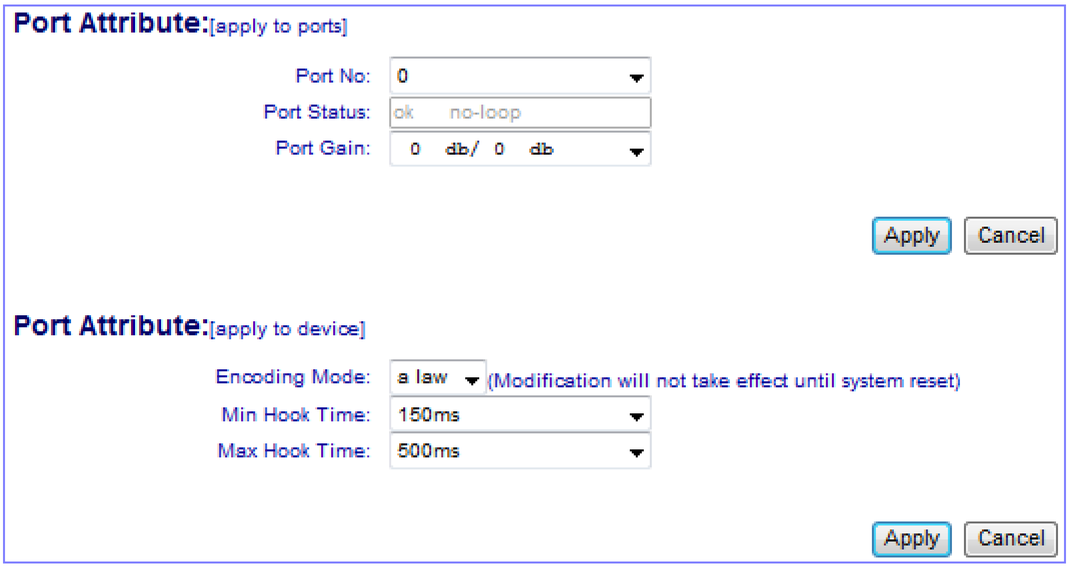
For each port, you are allowed to set the Whitelist and Blacklist. Blacklist gives the numbers which you are not allowed to call, and Whitelist gives you the only numbers you are allowed to call. Type in the number in the blank area directly, and a symbol "|" is used between two numbers.

9.7 Port Configuration

Port configuration defines physical and electrical layer parameters, such as port transmit power.
Click on "Port Configuration" in the Configuration menu to access management web page for port configurations.

9.7.1 Port Attribute

Most of the configurations are self explaining in the port attribute section.



Port Attribute:[apply to ports]

Port No: 0

Port Status: ok no-loop

Port Gain: 0 db/ 0 db

Port Attribute:[apply to device]

Encoding Mode: a law (Modification will not take effect until system reset)

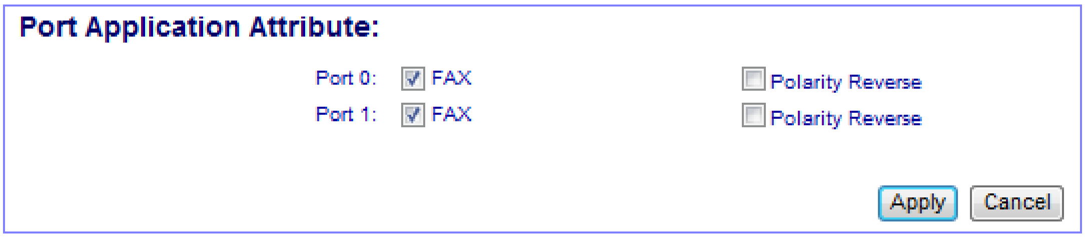
Min Hook Time: 150ms

Max Hook Time: 500ms

On Port Gain settings, the value before "/" is for transmission, the one after "/" is for receiving. The min and max hook times are relevant to the detection of a flash. If the phone is put on and off hook quickly and the duration is between min and max hook time, the operation is considered the same as pressing the Flash button.

9.7.2 Port Application Attribute

The CPE allows controlling fax function by each port. Configuration page is as follows:



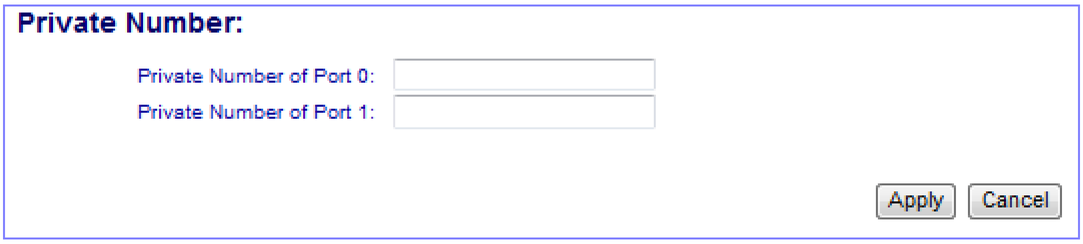
Port Application Attribute:

Port 0: ☑ FAX ☐ Polarity Reverse

Port 1: ☑ FAX ☐ Polarity Reverse

9.7.3 Private Number

Private numbers were used for point to point VoIP call setups without the involvement of Proxy server. This is not required for a service provider's network where VoIP core network infrastructure is implemented.



Private Number:

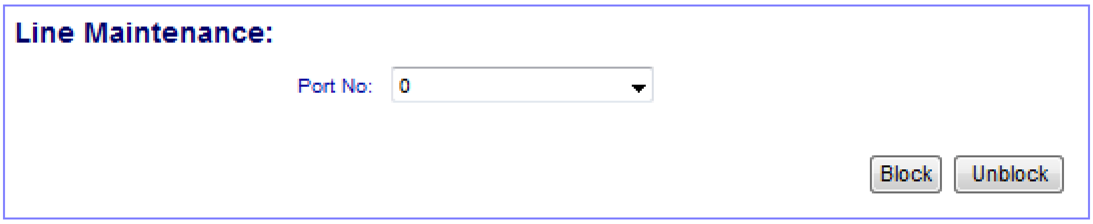
Private Number of Port 0:

Private Number of Port 1:

In the scenario with no proxy servers and registrar, dial numbers must be planned carefully. Let us use an example to elaborate this scenario.

9.7.4 Line Maintenance

The CPE may block some ports temporarily. This option maintains the user agent setting.



Line Maintenance:

Port No: 0

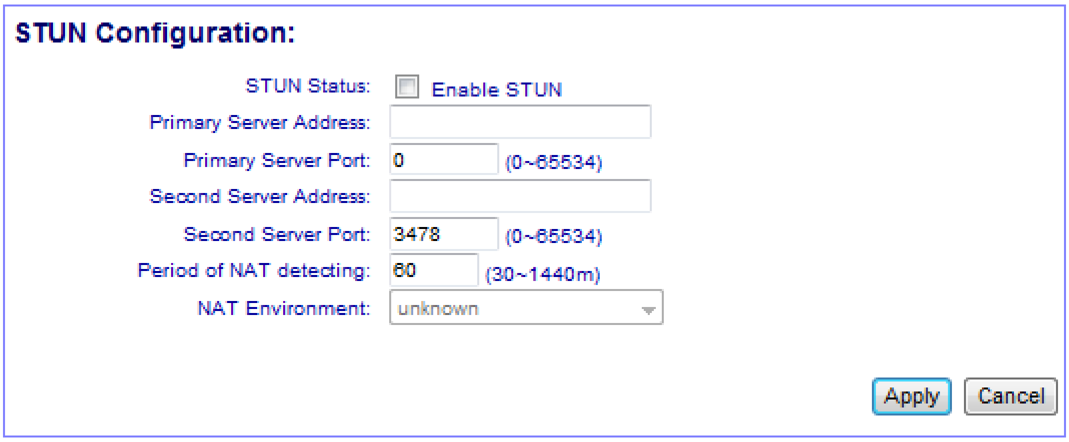
9.8 STUN Configuration

STUN (Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)) is a network protocol allowing clients behind NAT (or multiple NATs) to find out its public address, the type of NAT it is behind and the internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between two hosts that are both behind NAT routers.

Protocols like SIP use UDP packets for the transfer of sound and/or video and/or real-time text signaling traffic over the Internet. Unfortunately as both endpoints are often behind NAT, a connection cannot be set up in the traditional way. This is where STUN is useful.

STUN is a client-server protocol. A VoIP phone or software package may include a STUN client, which will send a request to a STUN server. The server then reports back to the STUN client what the public IP address of the NAT router is, and what port was opened by the NAT to allow incoming traffic back in to the network.

By default, a STUN server in the public domain larry.gloo.net has been configured as the secondary server. The Service Provider may specify address of its own STUN server, if implemented, as a primary server.



STUN Configuration:

STUN Status: □ Enable STUN

Primary Server Address:

Primary Server Port: 0 (0~65534)

Second Server Address:

Second Server Port: 3478 (0~65534)

Period of NAT detecting: 60 (30~1440m)

NAT Environment: unknown

The response also allows the STUN client to determine what type of NAT is in use, as different types of NATs handle incoming UDP packets differently. There are four main types of NAT:

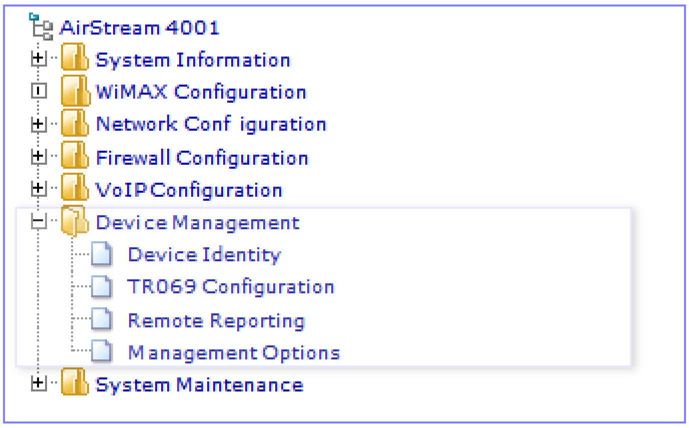
- full cone NAT,
- restricted cone NAT, and
- port restricted cone NAT.
- symmetric NAT (also known as bi-directional NAT)

The CPE has built in intelligence to work with three of four main types: full cone NAT, restricted cone NAT, and port restricted cone NAT, by pre-adjust the outgoing SIP messages and voice using public IP address and source port discovered.

The CPE will not work with symmetric NAT (also known as bi-directional NAT).

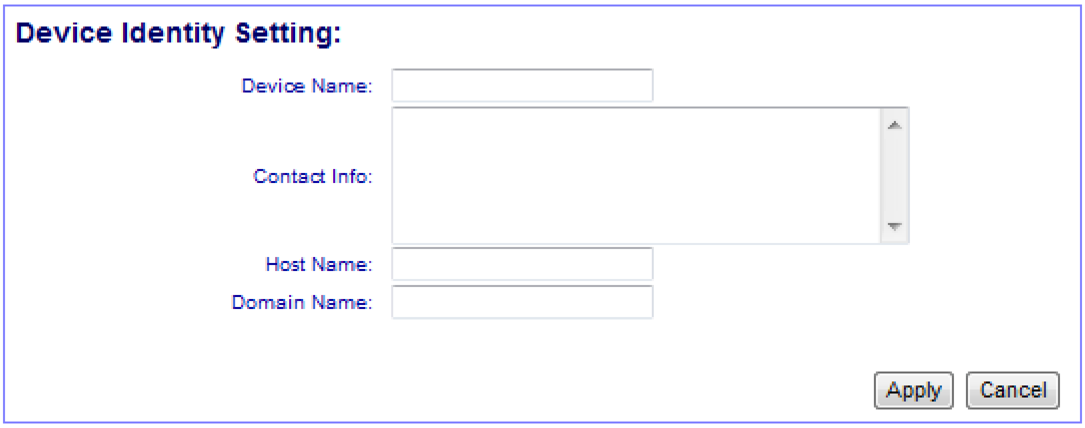
10 Device Management

When clicking on the Device Management link, you will be prompted with the follow navigation menu:



10.1 Device Identity

Use the following configuration page to add Device Name, Host Name, Domain Name and Contact Info for the CPE device.


Device Identity Setting:

Device Name:

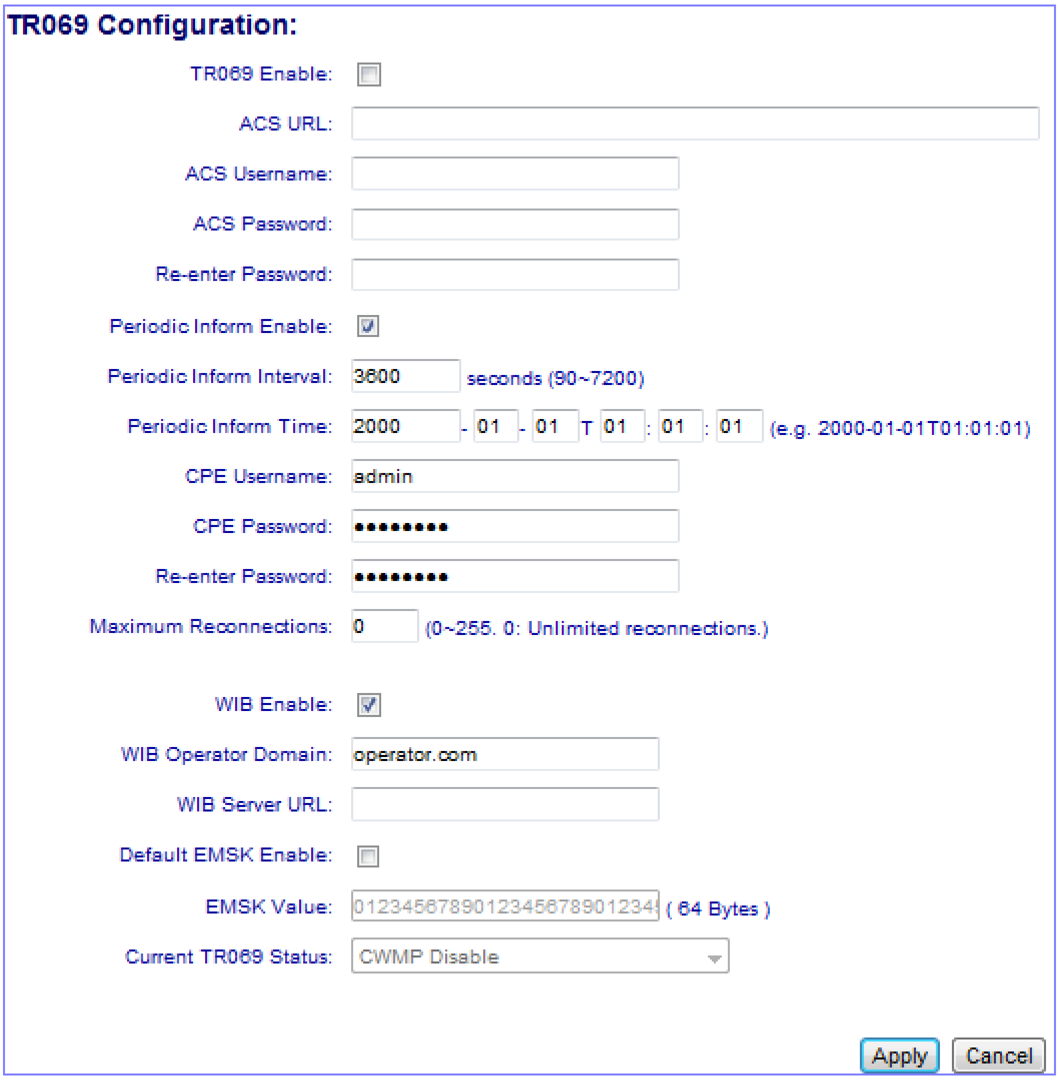
Contact Info:

Host Name:

Domain Name:

10.2 TR069 Configuration

To manage the CPE via TR069, you need to configure the TR-069 client. You can set the ASC URL manually by directly typing. Enter the ACS Username and ACS password for communication and authorization between CPE and ACS. If you want the CPE to send message to ACS periodically, please enable Periodic Inform, and set the periodic interval and time. CPE Username and CPE Password are verified when ACS sends connection request to CPE. Maximum Reconnections is the max times of reconnection in the case of connection failure.



TR069 Configuration:

TR069 Enable: ☐

ACS URL:

ACS Username:

ACS Password:

Re-enter Password:

Periodic Inform Enable: ☑

Periodic Inform Interval: 3600 seconds (90~7200)

Periodic Inform Time: 2000 - 01 - 01 T 01 : 01 : 01 (e.g. 2000-01-01T01:01:01)

CPE Username: admin

CPE Password: ●●●●●●●●●

Re-enter Password: ●●●●●●●●●

Maximum Reconnections: 0 (0~255. 0: Unlimited reconnections.)

WIB Enable: ☑

WIB Operator Domain: operator.com

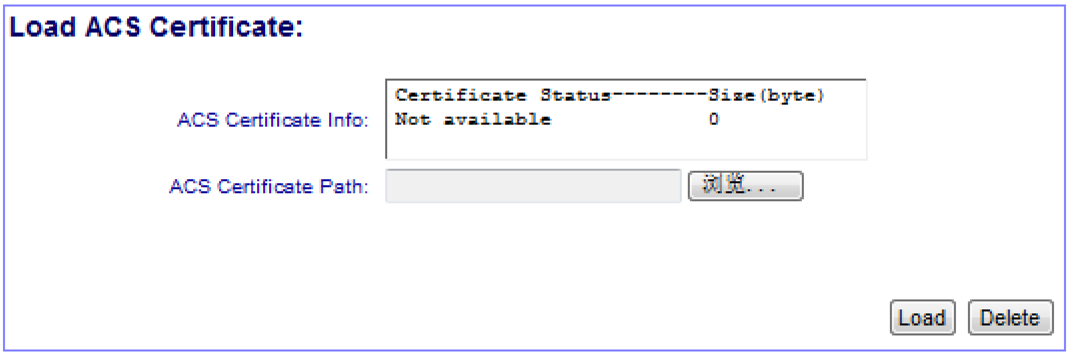
WIB Server URL:

Default EMSK Enable: ☐

EMSK Value: 0123456789012345678901234 (64 Bytes)

Current TR069 Status: CWMP Disable

You can also obtain the ACS URL automatically by enabling WIB. Set the WIB Operator Domain, WIB Server URL and EMSK Value (or enable the default EMSK) correctly to get the ACS URL, ACS Username and Password, and to renew the local Certificate.



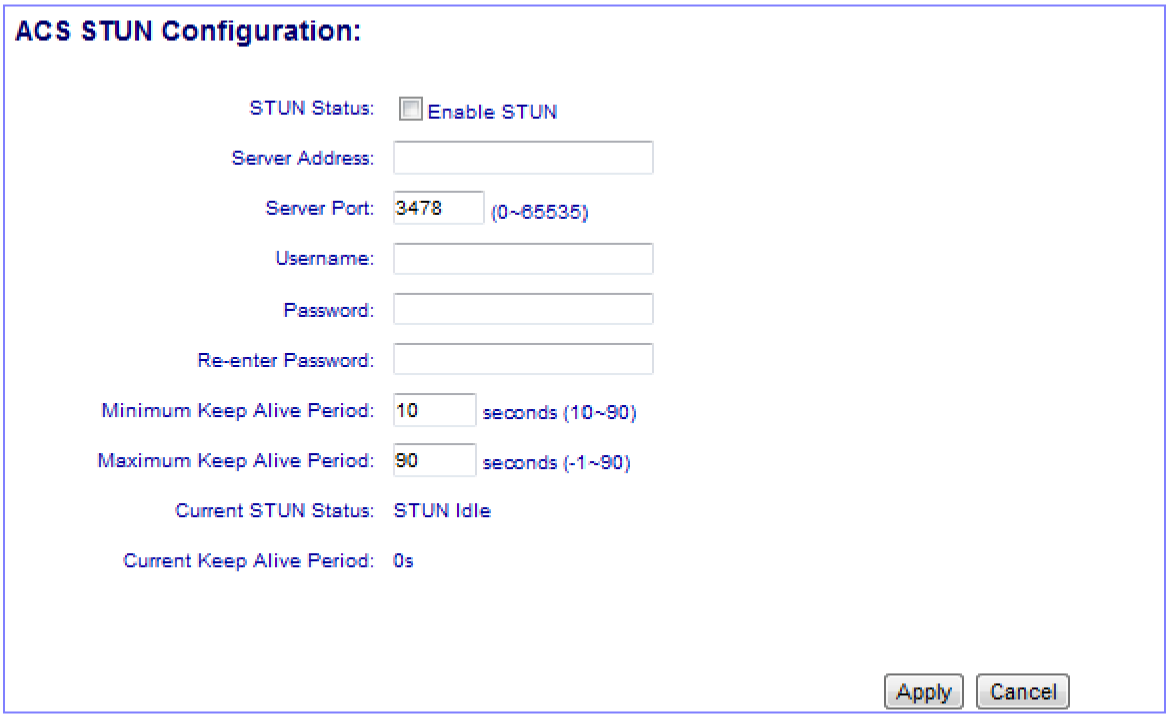
Load ACS Certificate:

ACS Certificate Info:

```
Certificate Status--------Size(byte)
Not available             0
```

ACS Certificate Path:

Choose the right path and load the right ASS Certificate. The ASC Certificate Info will be shown.



ACS STUN Configuration:

STUN Status: □ Enable STUN

Server Address:

Server Port: 3478 (0~65535)

Username:

Password:

Re-enter Password:

Minimum Keep Alive Period: 10 seconds (10~90)

Maximum Keep Alive Period: 90 seconds (-1~90)

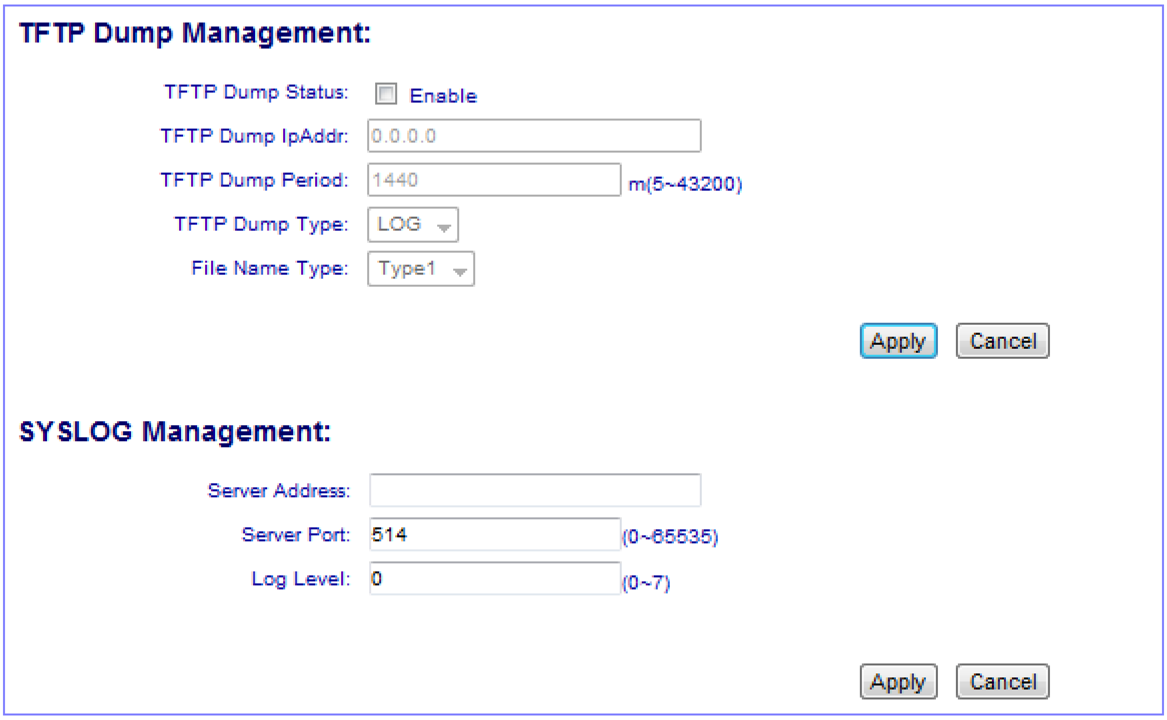
Current STUN Status: STUN Idle

Current Keep Alive Period: 0s

Enable the STUN to start the STUN function. You can set the server address, server port, username, password, minimum and maximum keep alive period.

10.3 Remote Reporting

Via the Web Management, the contents of log and alarm can be uploaded to specified server. Syslog and TFTP reporting are supported.



TFTP Dump Management:

TFTP Dump Status: □ Enable

TFTP Dump IpAddr: 0.0.0.0

TFTP Dump Period: 1440 m(5~43200)

TFTP Dump Type: LOG

File Name Type: Type1

SYSLOG Management:

Server Address:

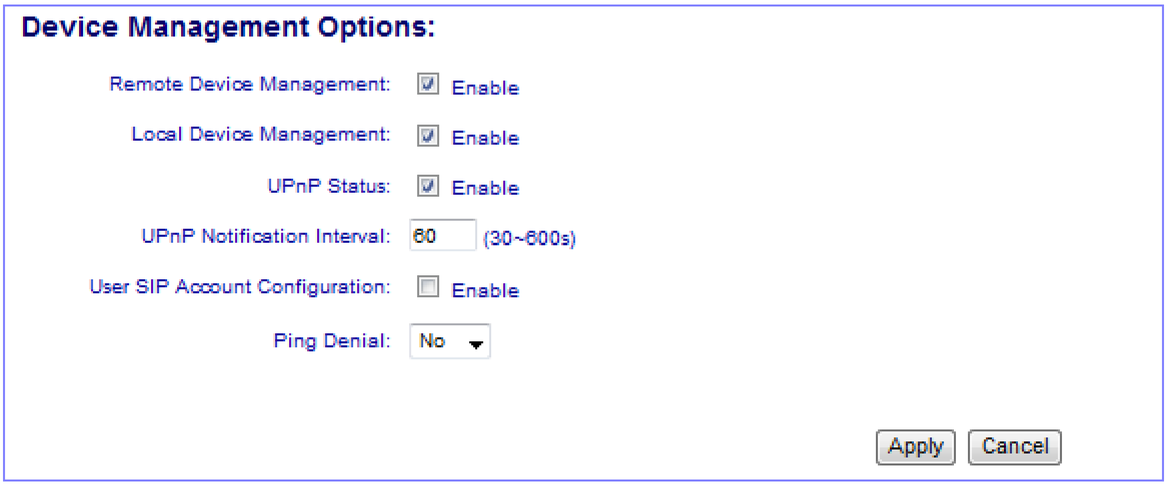
Server Port: 514 (0~65535)

Log Level: 0 (0~7)

10.4 Management Options

Management Options setting allows you enable or disable device management options according to your needs. Remote device management via WiMAX WAN or local management via LAN device can be controlled. Microsoft UPnP service is also configurable to allow Microsoft Windows user to browse the device directly from the desktop.

Administrator user can deny the Ping service on CPE and configure whether to allow user to configure the SIP account when logged on as “user”.



Device Management Options:

Remote Device Management: ☑ Enable

Local Device Management: ☑ Enable

UPnP Status: ☑ Enable

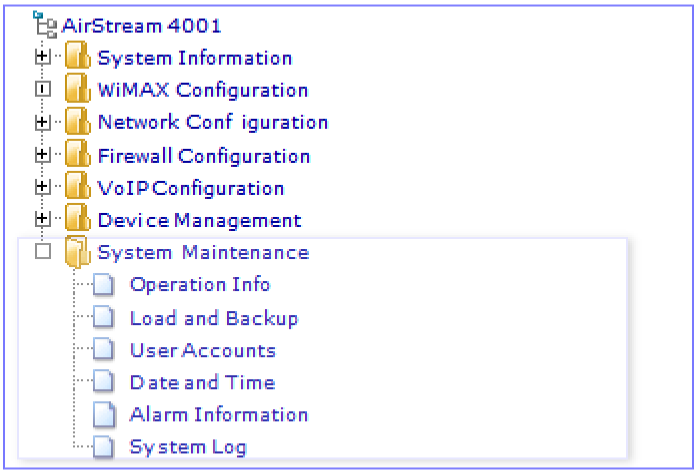
UPnP Notification Interval: 60 (30~600s)

User SIP Account Configuration: □ Enable

Ping Denial: No

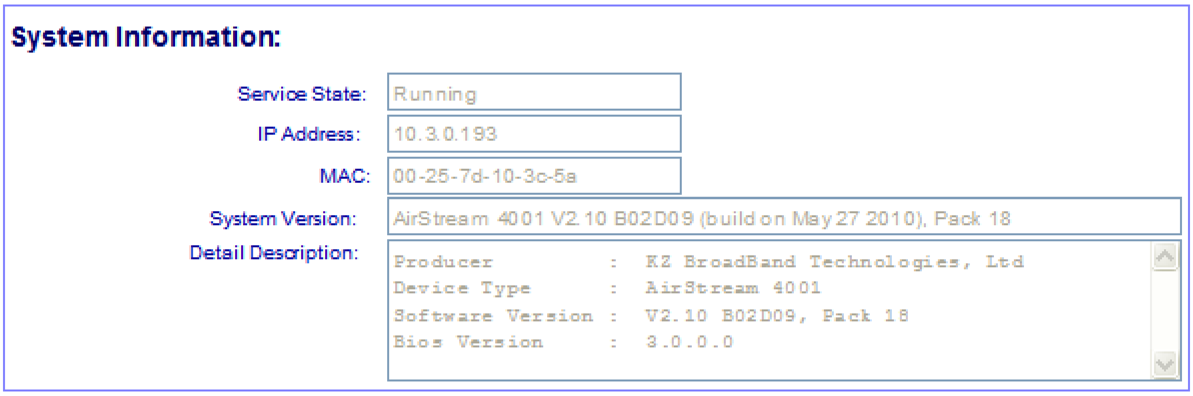
11 System Maintenance

Click on “System Maintenance” in the Configuration Tree in the left frame of browser window and then a subtree with several items will be shown.



11.1 Operation Information

By clicking “Operation Info” in the subtree, the following system information will be displayed in the detailed configuration frame:



System Information:

Service State: Running

IP Address: 10.3.0.193

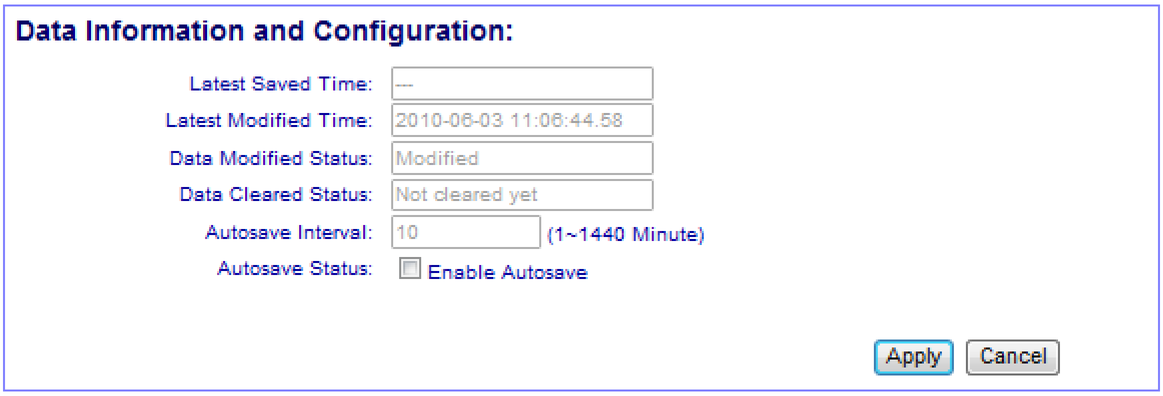
MAC: 00-25-7d-10-3c-5a

System Version: AirStream 4001 V2.10 B02D09 (build on May 27 2010), Pack 18

Detail Description:

```
Producer         :  KZ BroadBand Technologies, Ltd
Device Type      :  AirStream 4001
Software Version :  V2.10 B02D09, Pack 18
Bios Version     :  3.0.0.0
```

Basic system information of the device is shown, such as service state, IP address, MAC, System Version. The information cannot be modified.



Data Information and Configuration:

Latest Saved Time: ---

Latest Modified Time: 2010-06-03 11:06:44.58

Data Modified Status: Modified

Data Cleared Status: Not cleared yet

Autosave Interval: 10 (1~1440 Minute)

Autosave Status: □ Enable Autosave

The Data Information and Configuration is shown here, such as Latest Save Time, Latest Modified Time, Data Modified Status and Data Cleared Status. User can also configure the device to automatically save the configuration data into the flash memory periodically.

11.2 Load and Backup

This section demonstrates “Load” and “Backup” transaction via a web management interface. Let us start with discussion of a few terminologies:

Program refers to the file which contains binary instruction sets that controls the CPE system.

Data refers to the file which contains network and user specific configuration

Load refers to transferring of system program file or configuration data file from an external host into a CPE.

Backup means saving of configuration data file from a CPE to an external host.

TFTP and HTTP protocols are supported to Load and Backup new firmware and/or system configuration files.

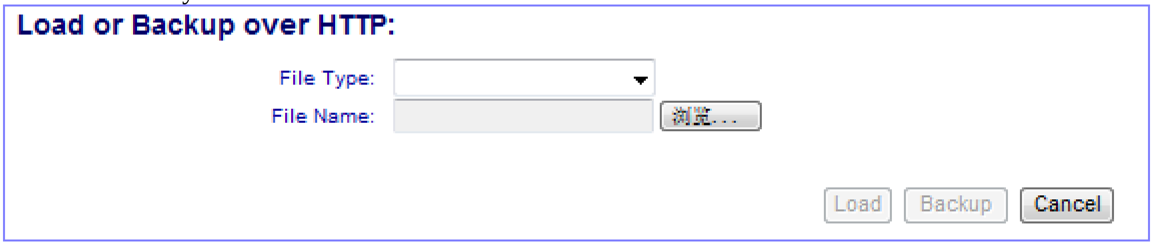
Configuration data can be backed up from CPE to an external host, or restored from external computer into a CPE IAD. The external host must have IP connectivity with the CPE device.

11.2.1 Load or Backup over HTTP

Similarly, the system firmware and configuration files can be loaded into the CPE via HTTP protocol. The configuration files can be backed from the CPE to the external host. The external host in this case is the computer which runs the web browser to access the network management pages.

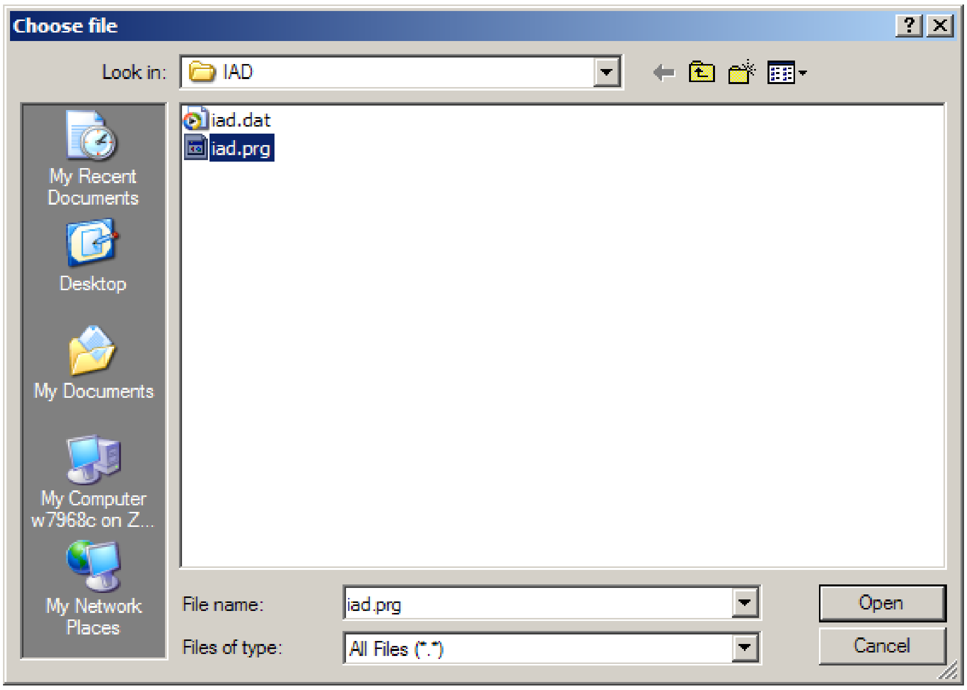
Information	**The external host in this case serves as a HTTP client. The CPE serves as a HTTP server.**

11.2.1.1 Load System Files to an CPE from a Web Browser



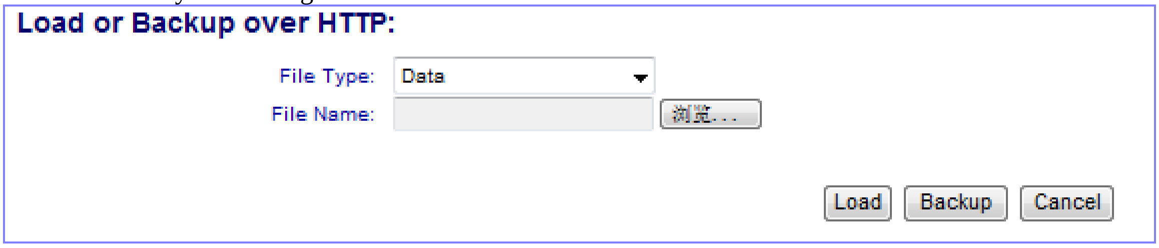
The steps of Load firmware via HTTP are as follows:

1. Obtain the latest version of system firmware. (e.g. iad.prg.)
2. Choose "Program" as the file type in the “File Type" list.
3. Click the "Browse" button, a dialogue box will appear as shown below.



4. Select the file “iad.prg”, click the “Open” button.
5. Click the [Load] button.
6. Reset system after loading finished.

11.2.1.2 Save system configurations from CPE


Load or Backup over HTTP:

File Type: Data

File Name:

The steps of backup configuration files via HTTP are as follows:

1. Choose the type of backup file as "Data" in the “File Type" column.
2. Click the “backup" button.
3. Click the “Save” button.
4. Select the file name and click the “Save” button.

Information	**Many web browsers implemented security features which blocks downloading of a file. Check your browser settings to see if no File Save dialogue box appears.**

11.2.2 Load or Backup over TFTP

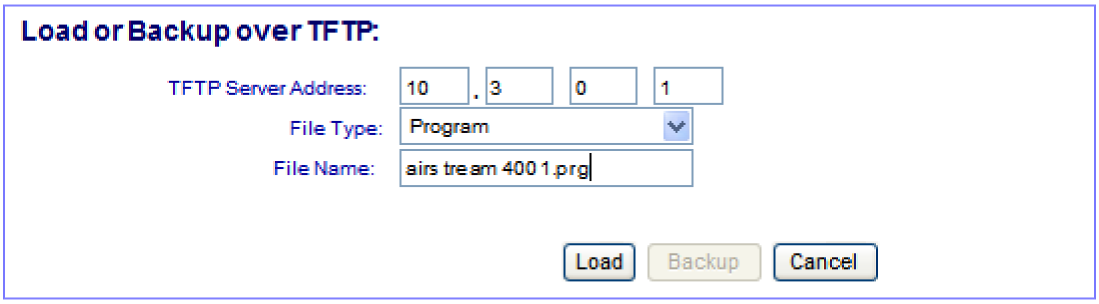
An external host running TFTP server can be used to backup the device configuration data, or restore configuration data to the IX253P device.

Information	**The external host in this case serves as the TFTP server. The IAD serves as a TFTP client.**

11.2.2.1 Load System Files from a TFTP Server

The steps of Load system software or configuration via TFTP are as follows:

1. Obtain the correct release of program file; the program file in this example is named “iad.prg”.
2. Obtain the IP address of the TFTP server. The IP address of the external host is 192.168.0.18
3. Type IP address of the TFTP server in the “TFTP server address" field.
4. Choose the type of the loaded files as "Program" in the “File Type" field.
5. Type the loaded file name in the "File Name" column.



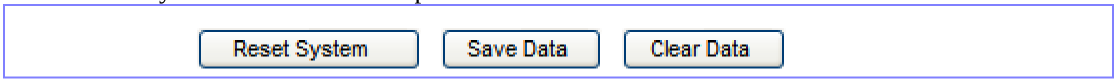
Load or Backup over TFTP:

TFTP Server Address: 10 . 3 0 1

File Type: Program

File Name: airstream4001.prg

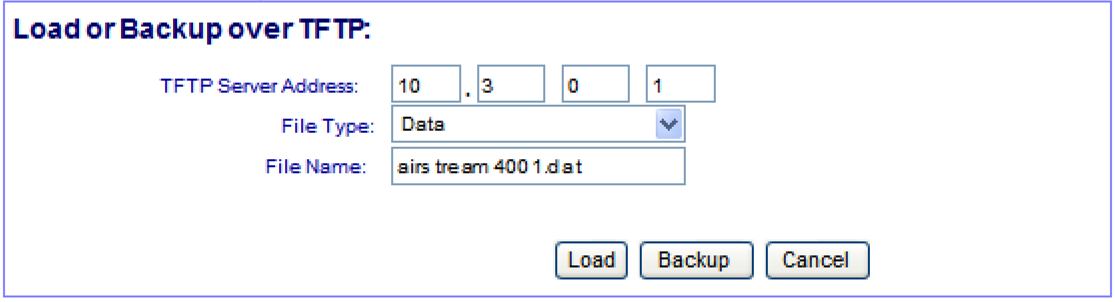
6. Click the “Load”.
7. Reset the system after successful update.



Typically it takes 3 minutes or longer to upload a firmware.

Caution	**Do not close WEB browser window during the process. Otherwise the system configuration may be corrupted.**

11.2.2.2 Backup Configuration Data to an TFTP Server



Load or Backup over TFTP:

TFTP Server Address: 10 . 3 0 1

File Type: Data

File Name: airstream4001.dat

The steps of backup over TFTP are as follows:

1. Obtain the IP address of the TFTP server.
2. Type the IP address of the TFTP server in the “TFTP server address" field.
3. Choose the type of the backup file as "Data" in the “File Type" list.
4. Input the backup file name in the "File Name" file.
5. Click "Backup" button. Examine whether the backup file has been successfully created.

11.3 User Account Management

The CPE implemented two levels of privileges: admin and user.

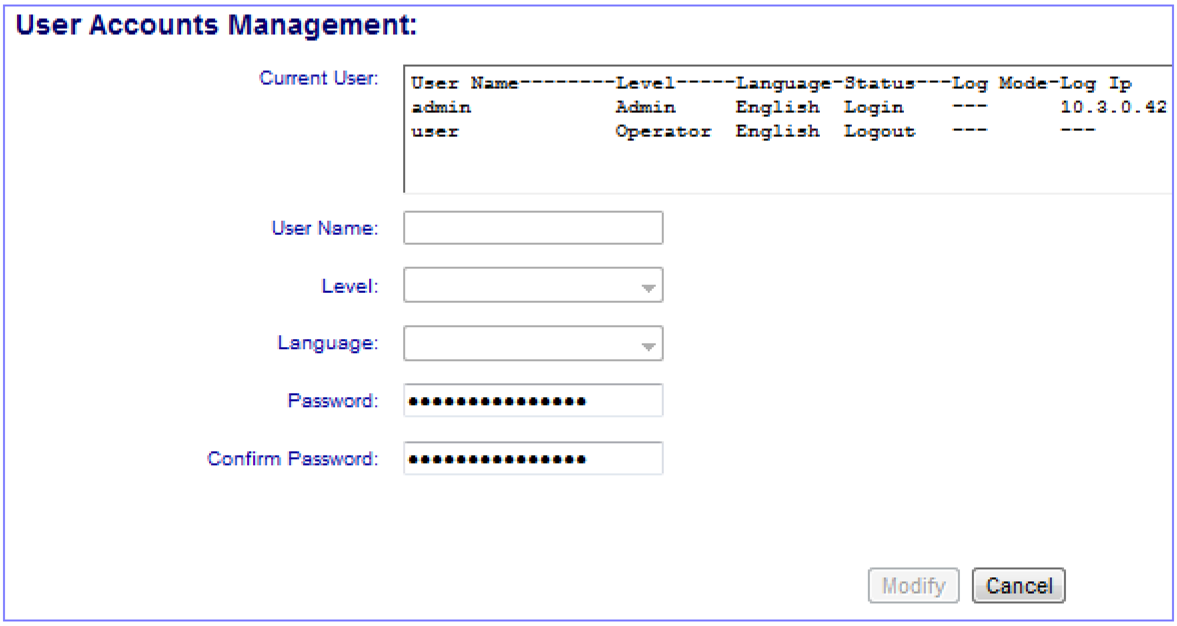
- **Administrator**’s privilege allows full control of the CPE system, e.g. system software upgrades. Administrator’s privilege provides maximum flexibility for service providers to integrate the CPE with its network.
- **User**’s privilege allows a limited subset of features and parameters that are customer specific.

Parameters that are prone to cause operational failure are forbidden from access, e.g. change of dial number.

Both admin and user has preferred language, and password setting.

User name	is the identifier of user, use admin or user to log on.
Level	is the privilege level of a certain user.
Language	defines default display language of web management pages for a user.

Click on the “User Account” in Configuration Tree. The following will be shown in the detailed configuration window.



User Accounts Management:

Current User:

```
User Name--------Level-----Language-Status---Log Mode-Log Ip
admin            Admin     English  Login    ---      10.3.0.42
user             Operator  English  Logout   ---      ---
```

User Name:

Level:

Language:

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

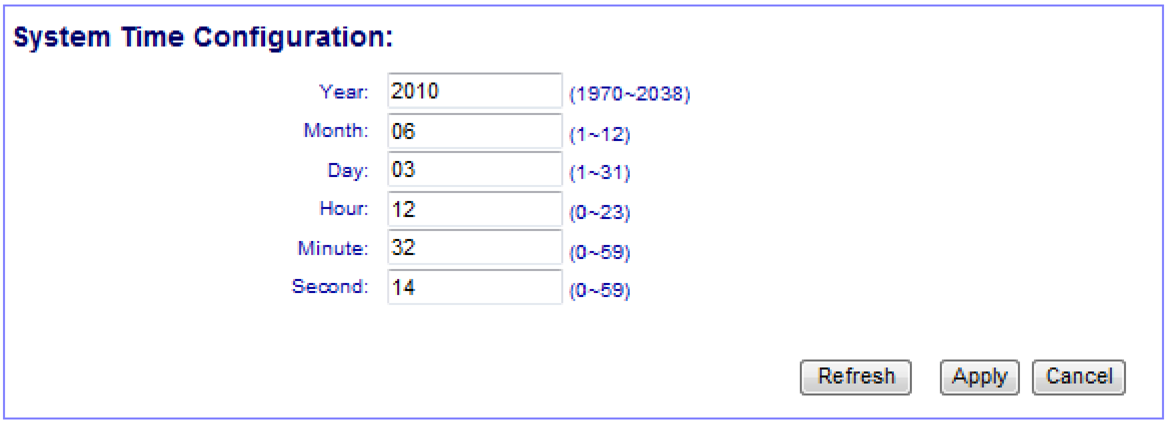
The table on top of the page displays the user accounts that are already provisioned in the IX253P CPE.

11.4 System Time

Click on “Date and Time” in the configuration tree in the left frame of browser window. The System Time will be displayed in the middle of the web page.

11.4.1 Date and Time Configuration

The web page does not update the displayed time automatically. Click on **[Refresh]** button to view current system time.



System Time Configuration:

Year: 2010 (1970~2038)

Month: 06 (1~12)

Day: 03 (1~31)

Hour: 12 (0~23)

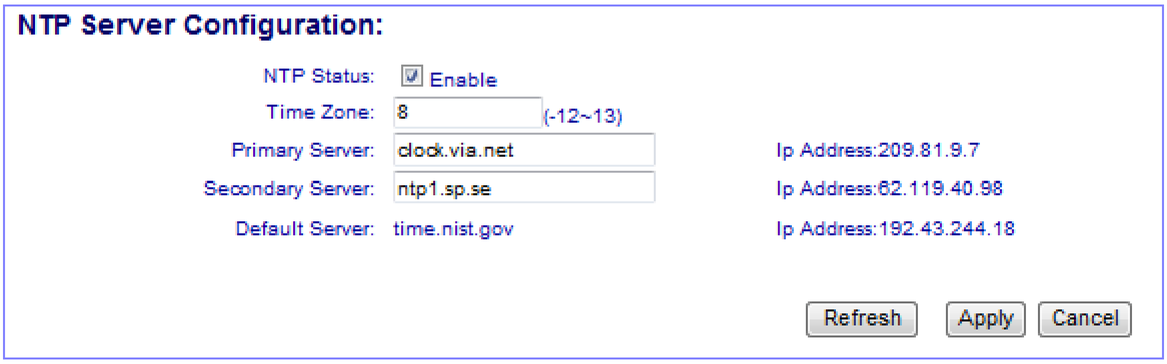
Minute: 32 (0~59)

Second: 14 (0~59)

To set system time, type in all the fields and click the **[Apply]** button.

11.4.2 NTP Server Configuration

The CPE also supports the NTP (Network Timing Protocol) to synchronize its system time with a clock source with higher accuracy.



NTP Server Configuration:

NTP Status: ☑ Enable

Time Zone: 8 (-12~13)

Primary Server: clock.via.net Ip Address:209.81.9.7

Secondary Server: ntp1.sp.se Ip Address:62.119.40.98

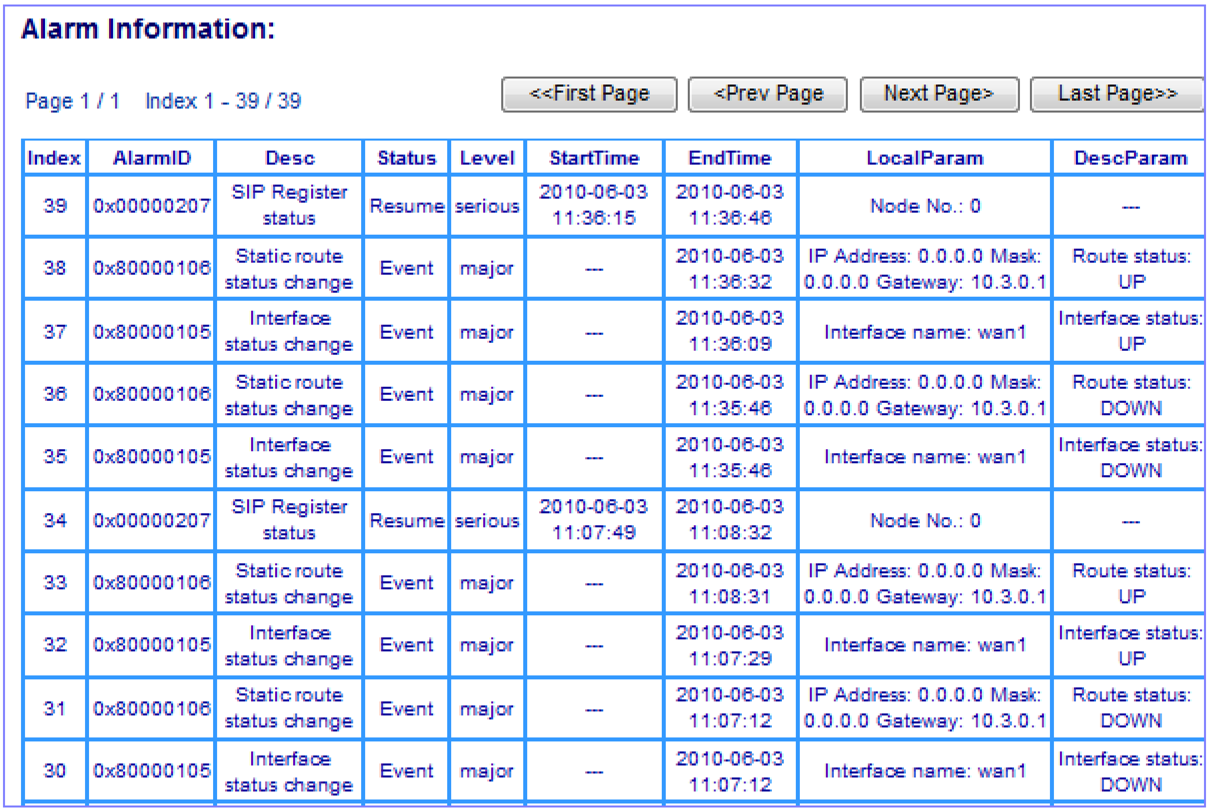
Default Server: time.nist.gov Ip Address:192.43.244.18

11.5 Alarms Information

The CPE capture system faults and report them in the Alarms Information web management page. The Alarm information provides traces of fault and helps troubleshooting the device.

11.5.1 Current and History Alarm

Click on “Alarm Information” in the Configuration Tree. All current and historical alarms will be displayed in the detailed configuration window.



Alarm Information:

Page 1 / 1 Index 1 - 39 / 39

Index	AlarmID	Desc	Status	Level	StartTime	EndTime	LocalParam	DescParam
39	0x00000207	SIP Register status	Resume	serious	2010-06-03 11:36:15	2010-06-03 11:36:46	Node No.: 0	---
38	0x80000106	Static route status change	Event	major	---	2010-06-03 11:36:32	IP Address: 0.0.0.0 Mask: 0.0.0.0 Gateway: 10.3.0.1	Route status: UP
37	0x80000105	Interface status change	Event	major	---	2010-06-03 11:36:09	Interface name: wan1	Interface status: UP
36	0x80000106	Static route status change	Event	major	---	2010-06-03 11:35:46	IP Address: 0.0.0.0 Mask: 0.0.0.0 Gateway: 10.3.0.1	Route status: DOWN
35	0x80000105	Interface status change	Event	major	---	2010-06-03 11:35:46	Interface name: wan1	Interface status: DOWN
34	0x00000207	SIP Register status	Resume	serious	2010-06-03 11:07:49	2010-06-03 11:08:32	Node No.: 0	---
33	0x80000106	Static route status change	Event	major	---	2010-06-03 11:08:31	IP Address: 0.0.0.0 Mask: 0.0.0.0 Gateway: 10.3.0.1	Route status: UP
32	0x80000105	Interface status change	Event	major	---	2010-06-03 11:07:29	Interface name: wan1	Interface status: UP
31	0x80000106	Static route status change	Event	major	---	2010-06-03 11:07:12	IP Address: 0.0.0.0 Mask: 0.0.0.0 Gateway: 10.3.0.1	Route status: DOWN
30	0x80000105	Interface status change	Event	major	---	2010-06-03 11:07:12	Interface name: wan1	Interface status: DOWN

11.5.2 Defined Alarms

The following Alarms have been defined for IX253P CPE Device

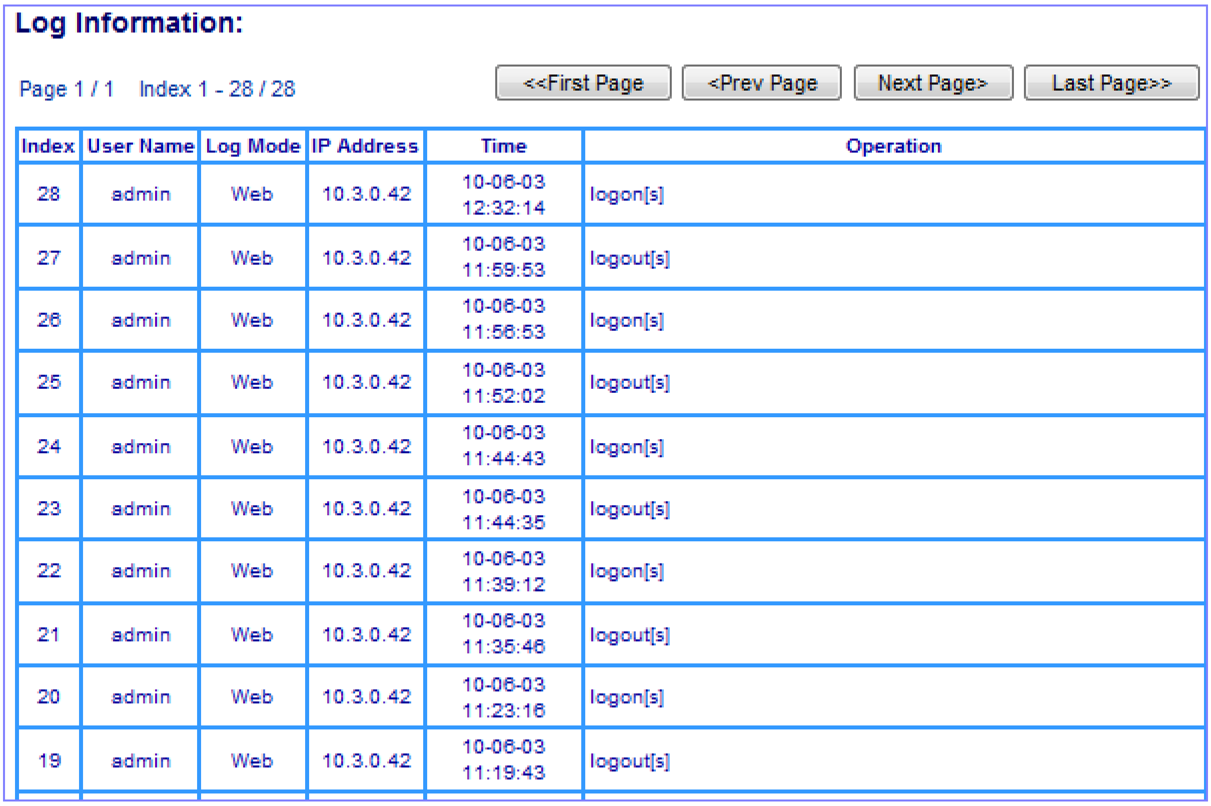
Alarm ID	Alarm Description
0x00000101	Node state alarm
0x00000102	Port state alarm
0x00000201	Media interface
0x00000206	H323 Register status
0x00000207	SIP Register status
0x00000801	Memory use status
0x00000802	CPU use status
0x80000104	Duplicate IP Address
0x80000105	Interface status change
0x80000106	Static route status change
0x80000107	Duplicate MAC Address
0x8000020D	RAI Out of Upper Value
0x8000020E	RAI Out of Low Value
0x80000301	Load file success
0x80000302	Load file failure
0x80000304	Flash data restore failed
0x80000801	CPU Tx packet failure
0x80000802	CPU Ethernet Rx packet loss
0x80000803	CPU Ethernet Rx busy
0x80000804	Lan Switch packet Tx collision
0x80000805	Lan Switch packet loss
0x80000806	RTP Rx packet loss

11.6 System Log

The CPE logs major system events automatically and store them in the system log, such as log in and out, system upgrades, and reset, etc.

Click on “Log Information” in the Configuration Tree, the system log will be shown in the detailed configuration window.

The chart below shows the system log of a CPE.



Log Information:

Page 1 / 1 Index 1 - 28 / 28

Index	User Name	Log Mode	IP Address	Time	Operation
28	admin	Web	10.3.0.42	10-06-03 12:32:14	logon[s]
27	admin	Web	10.3.0.42	10-06-03 11:59:53	logout[s]
26	admin	Web	10.3.0.42	10-06-03 11:56:53	logon[s]
25	admin	Web	10.3.0.42	10-06-03 11:52:02	logout[s]
24	admin	Web	10.3.0.42	10-06-03 11:44:43	logon[s]
23	admin	Web	10.3.0.42	10-06-03 11:44:35	logout[s]
22	admin	Web	10.3.0.42	10-06-03 11:39:12	logon[s]
21	admin	Web	10.3.0.42	10-06-03 11:35:46	logout[s]
20	admin	Web	10.3.0.42	10-06-03 11:23:16	logon[s]
19	admin	Web	10.3.0.42	10-06-03 11:19:43	logout[s]