

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



User Manual for GSF- 9364(4G) Cellular Gateway

Content

Chapter 1 Brief Introduction of Product	4
1.1 General	4
1.3 Working Principle	6
1.4 Specifications.....	6
Chapter 2 Installation Introduction.....	9
2.1 General.....	9
2.2 Encasement List	9
2.3 Installation and Cable Connection.....	9
2.4 Power	13
2.5 Indicator Lights Introduction	13
2.6 Reset Button Introduction.....	13
Chapter 3 Configuration and Management	15
3.1 Configuration Connection.....	15
3.2 Access the Configuration Web Page.....	15
3.3 Management and configuration.....	17
3.3.1 Setting	17
3.3.3.1 Basic Setting	17
3.3.1.1 Dynamic DNS	30
3.3.1.2 MAC Address Clone	31
3.3.1.3 Advanced Cellular Gateway.....	31
3.3.1.4 VLANs	33
3.3.1.5 Networking.....	34
3.3.2 Wireless.....	37
3.3.2.1 Basic Settings.....	37
3.3.3 Services.....	41
3.3.3.1 Services.....	41
3.3.4 VPN	44
3.3.4.1 PPTP.....	44
3.3.4.2 L2TP	45
3.3.4.3 OPENVPN	47
3.3.4.4 IPSEC.....	52
3.3.4.5 GRE.....	54

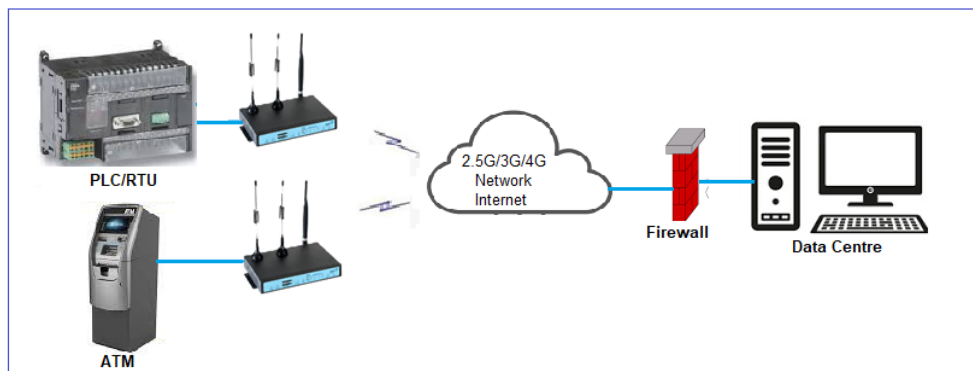
3.3.5	Security.....	56
3.3.5.1	Firewall.....	56
3.3.6	Access Restrictions.....	59
3.3.6.1	WAN Access.....	59
3.3.6.3	Packet Filter.....	62
3.3.7	NAT	63
3.3.7.1	Port Forwarding	63
3.3.7.2	Port Range Forward.....	65
3.3.7.3	DMZ.....	66
3.3.8	QoS Setting.....	66
3.3.8.1	Basic.....	66
3.3.8.2	Classify	68
3.3.9	Applications.....	68
3.3.9.1	Serial Applications	68
3.3.10	Administration	70
3.3.10.1	Management.....	70
3.3.10.2	Keep Alive	73
3.3.10.3	Commands	73
3.3.10.4	Factory Defaults.....	74
3.3.10.5	Firmware Upgrade	74
3.3.11	Status	76
3.3.11.1	Cellular Gateway	76
3.3.11.2	WAN	78
3.3.11.3	BKUP WAN	80
3.3.11.4	LAN	82
3.3.11.5	Wireless.....	84
3.3.11.6	Bandwidth.....	86
3.3.11.7	Sys-Info	88
Chapter 4 Appendix.....		92

Chapter 1 Brief Introduction of Product

1.1 General

GSF9364 series CELLULAR GATEWAY is a kind of cellular terminal device that provides data transfer function by public cellular network. Also, it supports double link backup function. It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232 (or RS485/RS422), Ethernet and WIFI port that can conveniently and transparently connect one device to a cellular network, allowing you to connect to your existing serial, Ethernet and WIFI devices with only basic configuration.

It has been widely used on M2M fields, such as intelligent transportation, smart grid, industrial automation, telemetry, finance, POS, water supply, environment protection, post, weather, and so on.



1.2 Features and Benefits

Design for Industrial Application

- High-powered industrial cellular module
- High-powered industrial 32bits CPU
- Adapt Dual Module design to ensure the stable and reliable of the Cellular Gateway
- Support low-consumption mode, including sleep mode, scheduled online/offline mode, scheduled power-on/power-off mode (optional)
- Housing: iron, providing IP30 protection.
- Power range: DC 5~36V
- Support hardware and software WDT
- Support auto recovery mechanism, including online detect, auto redial when offline to make Cellular Gateway always online
- Ethernet port: 1.5KV magnetic isolation protection
- RS232/RS485/RS422 port: 15KV ESD protection
- SIM/UIM port: 15KV ESD protection

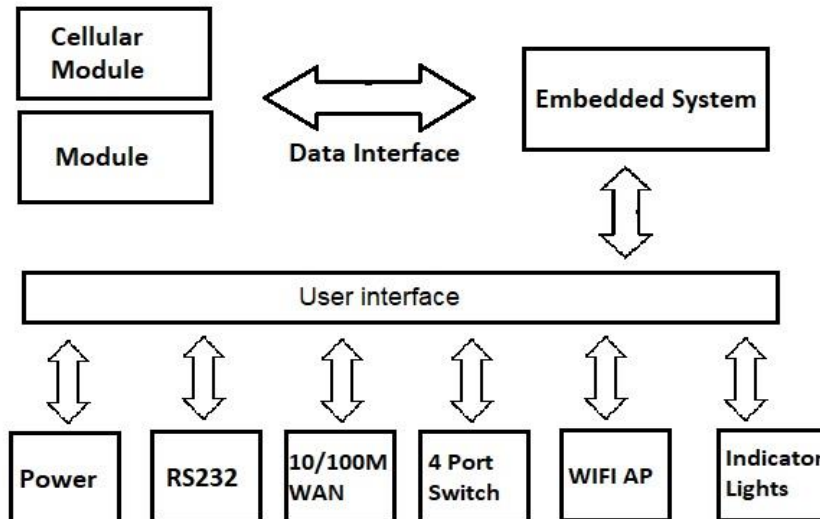
- Power port: reverse-voltage and overvoltage protection
- Antenna port: lightning protection(optional)

Standard and Convenience

- Support standard RS232(or RS485/RS422), Ethernet and WIFI port that can connect to serial, Ethernet and WIFI devices directly
- Support standard WAN port and PPPOE protocol that can connect to ADSL directly
- Support intellectual mode, enter into communication state automatically when powered
- Provide management software for remote management
- Support several work modes
- Convenient configuration and maintenance interface (WEB or CLI)
- Support master module, standby module and WAN (PPPOE, ADSL) (optional) triple link backup
- Support multiple WAN access methods, including static IP, DHCP, L2TP, PPTP, PPPOE, 3G/4G
- Support VPN client (PPTP, L2TP, OPENVPN, IPSEC and GRE)(only for VPN version)
- Support VPN server (PPTP, L2TP, OPENVPN, IPSEC and GRE)(only for VPN version)
- Support local and remote firmware upgrade, import and export configure file
- Support NTP, RTC embedded
- Support multiple DDNS provider service
- Support VLANs, MAC Address clone, PPPoE Server
- WIFI support 802.11b/g/n. support AP, client, Adhoc, Repeater, Repeater Bridge and WDS(optional) mode
- WIFI support WEP,WPA,WPA2 encryption, Support RADIUS authentication and MAC address filter
- Support multi online trigger ways, including SMS, ring and data. Support link disconnection when timeout
- Support APN/VPDN
- Support DHCP server and client, firewall, NAT, DMZ host , URL block, QoS, ttraff, statistics, real time link speed statistics etc
- Full protocol support , such as TCP/IP, UDP, ICMP, SMTP, HTTP, POP3, OICQ, TELNET, FTP, SNMP, SSHD, etc
- Schedule Reboot, Schedule Online and Offline, etc

1.3 Working Principle

The principal chart of the Cellular Gateway is as following:



1.4 Specifications

Cellular Specification

ITEM	CONTENT
L/L LTE/ LTE WIFI Cellular Gateway	
Standard and Band	TDD-LTE、FDD-LTE、EVDO、WCDMA、TD-SCDMA、CDMA1X、GPRS/EDGE
Bandwidth	FDD-LTE (Download speed:100Mbps, Upload speed:50Mbps)
	TDD-LTE (Download speed:61Mbps, Upload speed:18Mbps)
	CDMA2000 1X EVDO Rev A (Download speed:3.1Mbps, Upload
	speed:1.8Mbps)
	WCDMA (Download speed:42Mbps, Upload speed:5.76Mbps)
	TD-SCDMA (Download speed:4.2Mbps, Upload speed:2.2Mbps)
TX power	<23dBm

WIFI Specification

Item	Content
Standard	IEEE802.11b/g/n
Bandwidth	IEEE802.11b/g: 54Mbps (max) IEEE802.11n: 150Mbps (max)
Security	WEP, WPA, WPA2, etc. WPS (optional)
TX power	20dBm(11n),24dBm(11g),26dBm(11b)
RX sensitivity	<-72dBm@54Mbps

Hardware System

Item	Content
CPU	Industrial 32bits CPU
FLASH	16MB(Extendable to 64MB)
DDR2	128MB

Interface Type

Item	Content
WAN	1 10/100 Mbps WAN port(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
LAN	4 10/100 Mbps Ethernet ports (RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection.
Serial	1 RS232(or RS485/RS422) port, 15KV ESD protection Data bits: 5, 6, 7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space(optional), mark(optional) Baud rate: 2400~115200 bps
Indicator	"Power", "System", "Online-1", "Online-2", " Local Network ", "WAN", "WIFI", "Signal Strength"
Antenna	Cellular:2 Standard SMA female interface, 50-ohm, lightning protection(optional) WIFI: 1 Standard SMA male interface, 50-ohm, lightning protection(optional)
SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
Power	Standard 3-PIN power jack, reverse-voltage and overvoltage protection
Reset	Restore the Cellular Gateway to its original factory default settings

San Telequip (P) Ltd.,
 504 & 505 Deron Heights, Baner Road
 Pune 411045, India
 Phone : +91-20-27293455, 9764027070, 8390069393
 email : info@santelequip.com



Power Input

Item	Content
Standard Power	DC 12V/1.5A
Power Range	DC 5~36V

Consumption

Working condition	Consumption
Standby	290~360mA@12VDC
Communication	340~610mA@12VDC
Schedule shutdown	2.57~4.2mA@12DVC

Physical Characteristics

Item	Content
Housing	Iron, providing IP30 protection
Dimensions	207x135x28 mm
Weight	810g

Environmental Limits

Item	Content
Operating Temperature	-35~+75°C (-31~+167°F)
Storage Temperature	-40~+85°C (-40~+185°F)
Operating Humidity	95% (non-condensing)

Chapter 2 Installation Introduction

2.1 General

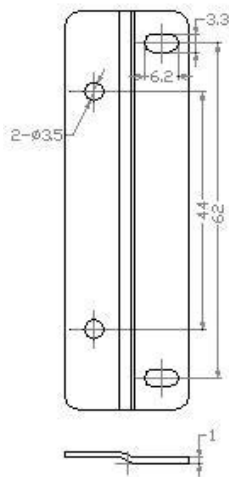
The Cellular Gateway must be installed correctly to make it work properly.
Warning: Forbid to install the Cellular Gateway when powered!

2.2 Encasement List

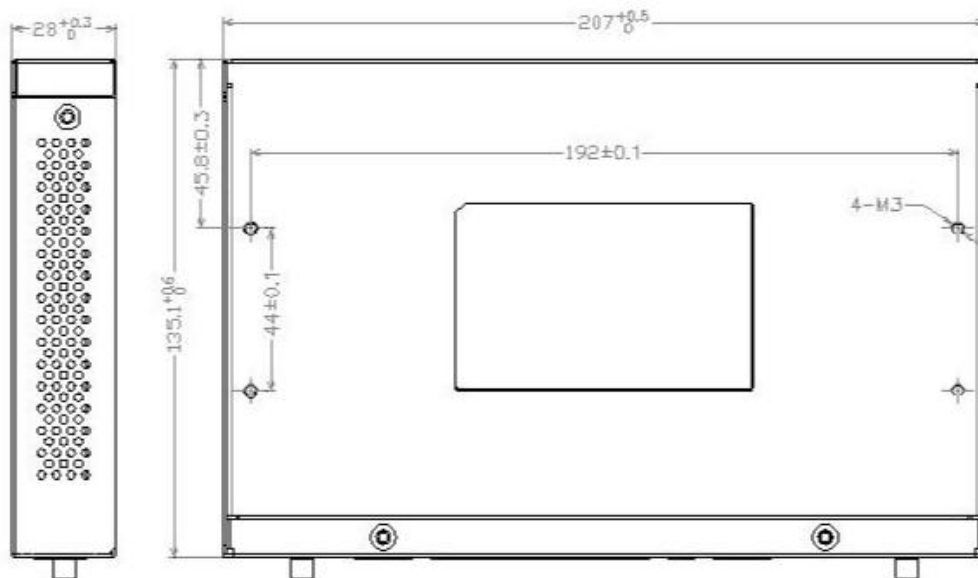
Name	Quantity	Remark
Cellular Gateway host	1	
Cellular antenna (Male SMA)	2	
WIFI antenna (Female SMA)	1	
Network cable	1	
Console cable	1	optional
Power adapter	1	optional

2.3 Installation and Cable Connection

Stator and routing equipment of screw specification for: M3 * 5 mm countersunk head screws (black)



Fixed Size



Cellular Gateway Size

Installation of SIM/UIM card:

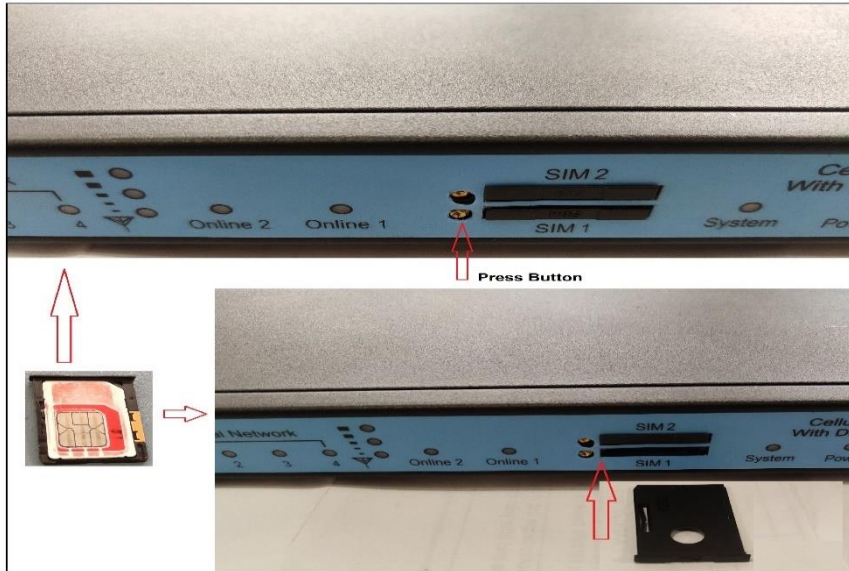
SIM/UIM-1: For the main link

SIM/UIM-2: For the backup link

L/L LTE/LTE WIFI CELLULAR GATEWAY	SIM/UIM-1: LTE (main link) SIM/UIM-2: LTE (backup link)
-----------------------------------	--

Firstly power off the Cellular Gateway, and press the out button of the SIM/UIM card outlet with a needle object. Then the SIM/UIM card sheath will flick out at once. Put SIM/UIM card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UIM card outlet.

Warning: Forbid to install SIM/UIM card when powered!



Installation of antenna:

Screw the SMA male pin of the cellular antenna to the female SMA interface of the Cellular Gateway with sign “ANT”.

Screw the SMA female pin of the WIFI antenna to the male SMA interface of the Cellular Gateway with sign “WIFI”.

Warning: The cellular antenna and the WIFI antenna can not be connected wrongly. And the antennas must be screwed tightly, or the signal quality of antenna will be influenced!

Installation of cable:

Insert one end of the network cable into the switch interface with sign “Local Network”, and insert the other end into the Ethernet interface of user’s device. The signal connection of network direct cable is as follows:

RJ45-1	RJ45-2	Colour
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown



Insert the RJ45 end of the console cable into the RJ45 outlet with sign “console”, and insert the DB9F end of the console cable into the RS232 serial interface of user’s device. The signal connection of the console cable is as follows:

Console line definition (RS232 & RS485)						
RJ45	Color	Signal	DB9F	Description	Direction (Cellular Gateway)	RS485 Signal
1	White/ Orange	CTS	8	Clear To Send	Output	D+
2	Orange	DSR	6	Data Set Ready	Output	D-
3	White/Green	RXD	2	Receive Data	Output	-
4	Blue	DCD	1	Data Carrier Detect	Output	-
5	White/Blue	GND	5	System Ground		-
6	Green	TXD	3	Transmit Data	Input	-
7	White/Brown	DTR	4	Data Terminal Ready	Input	-
8	Brown	RTS	7	Request To Send	Input	-



2.4 Power

The power range of the Cellular Gateway is DC 5 to 36V.

Warning: When we use other power, we should make sure that the power can supply power above 8W.

We recommend user to use the standard DC 12V/1.5A power.

2.5 Indicator Lights Introduction

The Cellular Gateway provides following indicator lights: "Power", "System", "Online-1", "Online-2", "Local Network", "WAN", "WIFI", "Signal Strength".

Indicator Light	State	Introduction
Power	ON	Cellular Gateway is powered on
	OFF	Cellular Gateway is powered off
System	BLINK	System works properly
	OFF	System does not work
Online-1	ON	The main link has logged on network
	OFF	The main link hasn't logged on network
Online-2	ON	The backup link has logged on network
	OFF	The backup link hasn't logged on network
Local	OFF	The corresponding interface of switch is not connected
	ON / BLINK	The corresponding interface of switch is connected /Communicating
WAN	OFF	The interface of WAN is not connected

San Telequip (P) Ltd.,
 504 & 505 Deron Heights, Baner Road
 Pune 411045, India
 Phone : +91-20-27293455, 9764027070, 8390069393
 email : info@santelequip.com



	ON / BLINK	The interface of WAN is connected /Communicating
WIFI	OFF	WIFI is not active
	ON	WIFI is active
Signal Strength	One Light ON	Signal strength is weak
	Two Lights ON	Signal strength is medium
	Three Lights ON	Signal strength is good

2.6 Reset Button Introduction

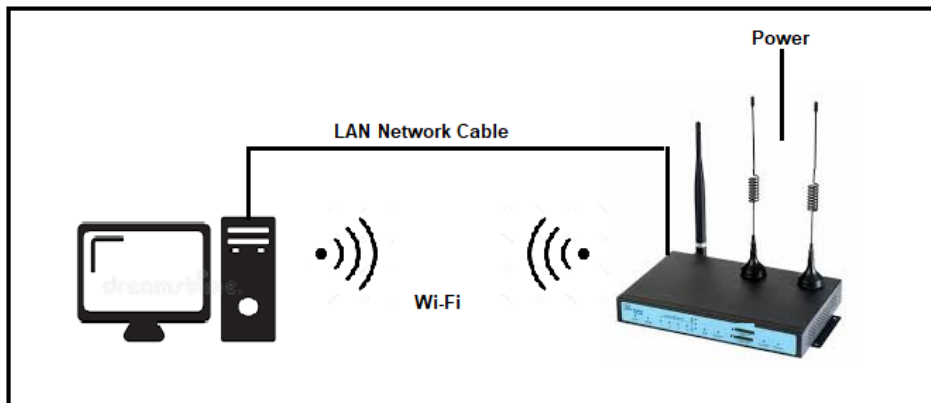
The Cellular Gateway has a “Reset” button to restore it to its original factory default settings. When user press the “Reset” button for up to 15s, the Cellular Gateway will restore to its original factory default settings and restart automatically

Chapter 3 Configuration and Management

This chapter describes how to configure and manage the Cellular Gateway.

3.1 Configuration Connection

Before configuration, you should connect the Cellular Gateway and your configuration PC with the supplied network cable. Plug the cable's one end into the Local Network port of the Cellular Gateway, and another end into your configure PC's Ethernet port. The connection diagram is as following:



Please modify the IP address of PC as the same network segment address of the Cellular Gateway, for instance, 192.168.1.9. Modify the mask code of PC as 255.255.255.0 and set the default gateway of PC as the Cellular Gateway's IP address (192.168.1.1).

3.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connect users' PC to the Cellular Gateway. There are eleven main pages: Setting, Wireless, Service, VPN, Security, Access Restrictions, NAT, QoS Setting, Applications, Management and Status. Users enable to browse slave pages by click one main page.

Users can open IE or other explorers and enter the Cellular Gateway's default IP address of 192.168.1.1 on address bar, then press the button of Enter to visit page Web management tool of the Cellular Gateway. The user's login in the web page at the first name, there will display a page shows as blow to tip users to modify the default user name and password of the Cellular Gateway. Users have to click "change password" to make it work if they modify user name and password.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Router Management

Your Router is currently not protected and uses an unsafe default username and password combination, please change it using the following dialog!

Router Password

Router Username

admin

Router Password

•••••

Re-enter to confirm

•••••

Change Password

After access to the information main page

GSF9364 Router

Menu

- Setup
- Wireless
- Services
- VPN
- Security
- NAT
- Access Restrictions
- QoS Setting
- Applications
- Administration
- Status

System Information

Router

Router Name	GSF9364
Router Model	GSF9364
LAN MAC	54:D0:84:0C:33:FA
WAN MAC	54:D0:84:0C:33:FA
Wireless MAC	54:D0:84:0C:33:FC
WAN IP	100.83.88.138
BKUP WAN IP	0.0.0.0
LAN IP	192.168.1.1

Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	GSF9364
Channel	1 (2412 MHz)
TX Power	100 mW
Rate	150 Mb/s

Wireless Packet Info

Received (RX)	0 OK, no error
Transmitted (TX)	0 OK, no error

Services

DHCP Server	Enabled
radauth	Disabled
USB Support	Enabled

Memory

Total Available	122.3 MB / 128.0 MB
Free	87.2 MB / 122.3 MB
Used	35.1 MB / 122.3 MB
Buffers	3.9 MB / 35.1 MB
Cached	13.5 MB / 35.1 MB
Active	7.8 MB / 35.1 MB
Inactive	13.4 MB / 35.1 MB

Wireless

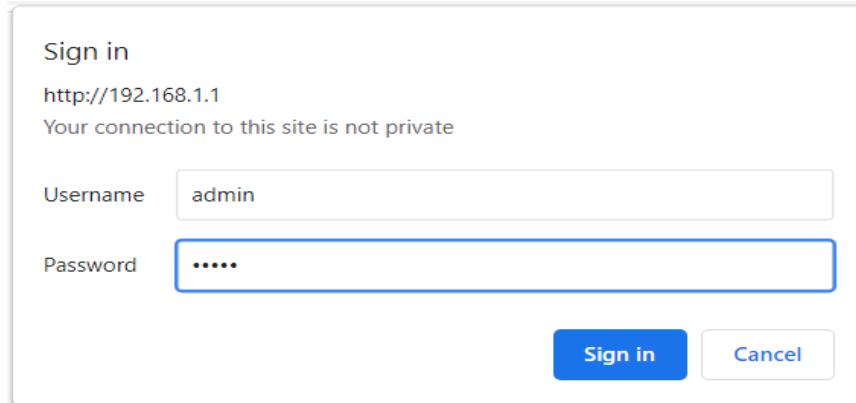
Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
- None -			



Sign in
http://192.168.1.1
Your connection to this site is not private

Username

Password

Users need to input user name and password if it is their first time to login. Input correct user name and password to visit relevant menu page. Default user name is root, password is admin. (Available to modify user name and password on management page, then click submit)

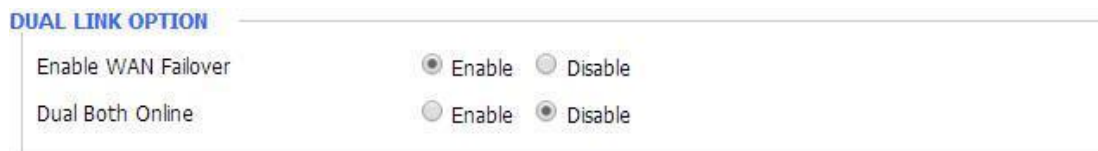
3.3 Management and configuration

3.3.1 Setting

The Setup screen is the first screen users will see when accessing the Cellular Gateway. Most users will be able to configure the Cellular Gateway and get it work properly using only the settings on this screen. Some Internet Service Providers (ISPs) will require users to enter specific information, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address. This information can be obtained from your ISP, if required.

3.3.3.1 Basic Setting

DUAL LINK OPTION



DUAL LINK OPTION

Enable WAN Failover ☒ Enable ☐ Disable

Dual Both Online ☐ Enable ☒ Disable

Enable dual link option to enable dual both online Cellular Gateway. Click disable means to enable only single link (main link), and backup link does not enable to work. If link enable, then there are Configure options for dual both online:

Enable: All default data will be sent via main link to Internet when main link is online. If main link is offline and backup link is online, then it will switch to backup link, and default data will send via backup link to Internet network. Meanwhile, main link is trying to reconnect, the

transfer will turn back to main link if it reconnects successful. In general, working mode come first, backup link is to backup.

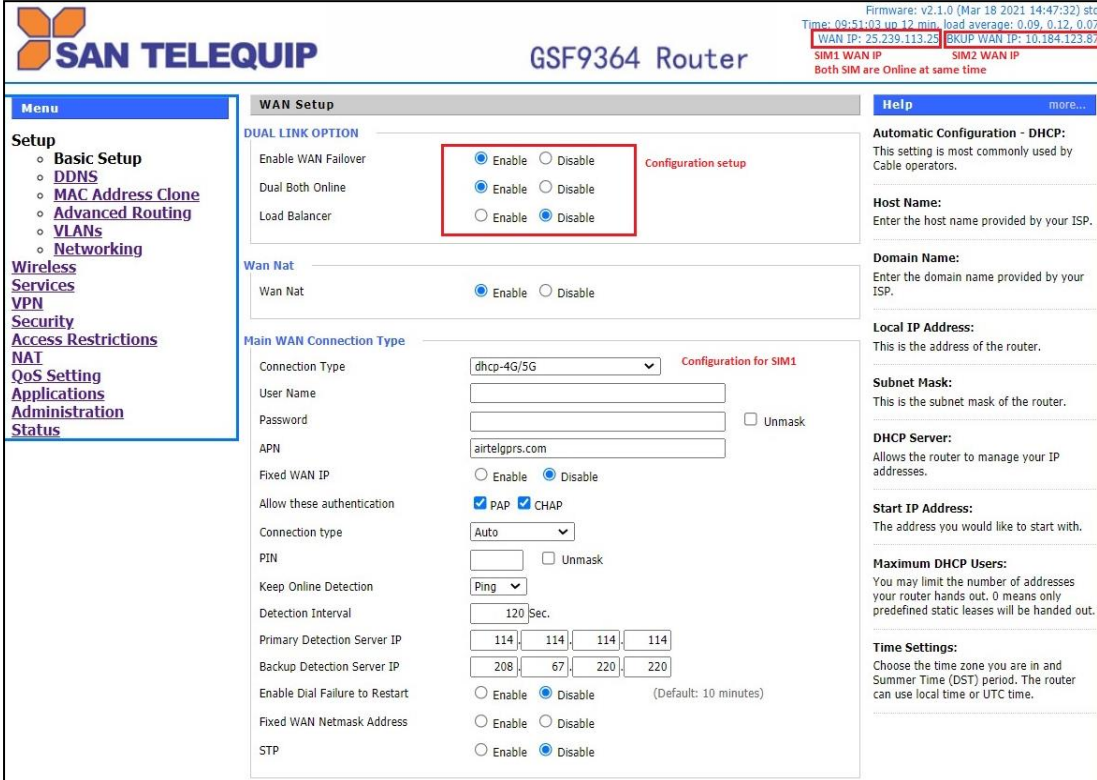
Note: If both sims are online and enable load balancer and load shunt, detailed data movement please refer to the menu of load Arrange

GSF-9364 Load Balancing Testing

When "WAN failure Enable" and "Dual both online" but "load balance" is disabled, Both SIM 1 and SIM 2 will online at the same time, but data will go through SIM 1. Bandwidth will be SIM 1's bandwidth.

Configuration Setting

SIM1 is a primary and SIM2 is Backup SIM. This setting is configurable between SIM1 and SIM2.



The screenshot displays the configuration page for the GSF9364 Router. The interface includes a top status bar with firmware version (v2.1.0), time, and WAN/SIM status. A left sidebar contains a menu with categories like Setup, Wireless Services, VPN, Security, and Access Restrictions. The main content area is titled 'WAN Setup' and contains several sections: 'DUAL LINK OPTION' with radio buttons for 'Enable WAN Failover', 'Dual Both Online', and 'Load Balancer'; 'Wan Nat' with a radio button for 'Wan Nat'; 'Main WAN Connection Type' with a dropdown for 'Connection Type' and fields for 'User Name', 'Password', 'APN', and 'Fixed WAN IP'; and 'Keep Online Detection' with a dropdown for 'Detection Interval' and fields for 'Primary Detection Server IP' and 'Backup Detection Server IP'. The right sidebar contains a 'Help' section with links to 'Automatic Configuration - DHCP', 'Host Name', 'Domain Name', 'Local IP Address', 'Subnet Mask', 'DHCP Server', 'Start IP Address', 'Maximum DHCP Users', and 'Time Settings'.

San Telequip GSF9364 Router

Firmware: v2.1.0 (Mar 18 2021 14:47:32) std
Time: 09:51:03 up 12 min, load average: 0.09, 0.12, 0.07
WAN IP: 25.239.113.25 SIM1 WAN IP: 10.184.123.8
SIM1 WAN IP: SIM2 WAN IP
Both SIM are Online at same time

Menu

- Setup
 - Basic Setup
 - DDNS
 - MAC Address Clone
 - Advanced Routing
 - VLANs
 - Networking
- Wireless Services
- VPN
- Security
- Access Restrictions
- NAT
- QoS Setting
- Applications
- Administration
- Status

WAN Setup

DUAL LINK OPTION

Enable WAN Failover ☒ Enable ☐ Disable Configuration setup

Dual Both Online ☒ Enable ☐ Disable

Load Balancer ☐ Enable ☒ Disable

Wan Nat

Wan Nat ☒ Enable ☐ Disable

Main WAN Connection Type

Connection Type: dhcp-4G/5G Configuration for SIM1

User Name:

Password: ☐ Unmask

APN: airtelgprs.com

Fixed WAN IP: ☐ Enable ☒ Disable

Allow these authentication: ☒ PAP ☒ CHAP

Connection type: Auto

PIN: ☐ Unmask

Keep Online Detection: Ping

Detection Interval: 120 Sec.

Primary Detection Server IP: 114 114 114 114

Backup Detection Server IP: 208 67 220 220

Enable Dial Failure to Restart: ☐ Enable ☒ Disable (Default: 10 minutes)

Fixed WAN Netmask Address: ☐ Enable ☐ Disable

STP: ☐ Enable ☒ Disable

Help

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

Subnet Mask:
This is the subnet mask of the router.

DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

Maximum DHCP Users:
You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.

Time Settings:
Choose the time zone you are in and Summer Time (DST) period. The router can use local time or UTC time.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com

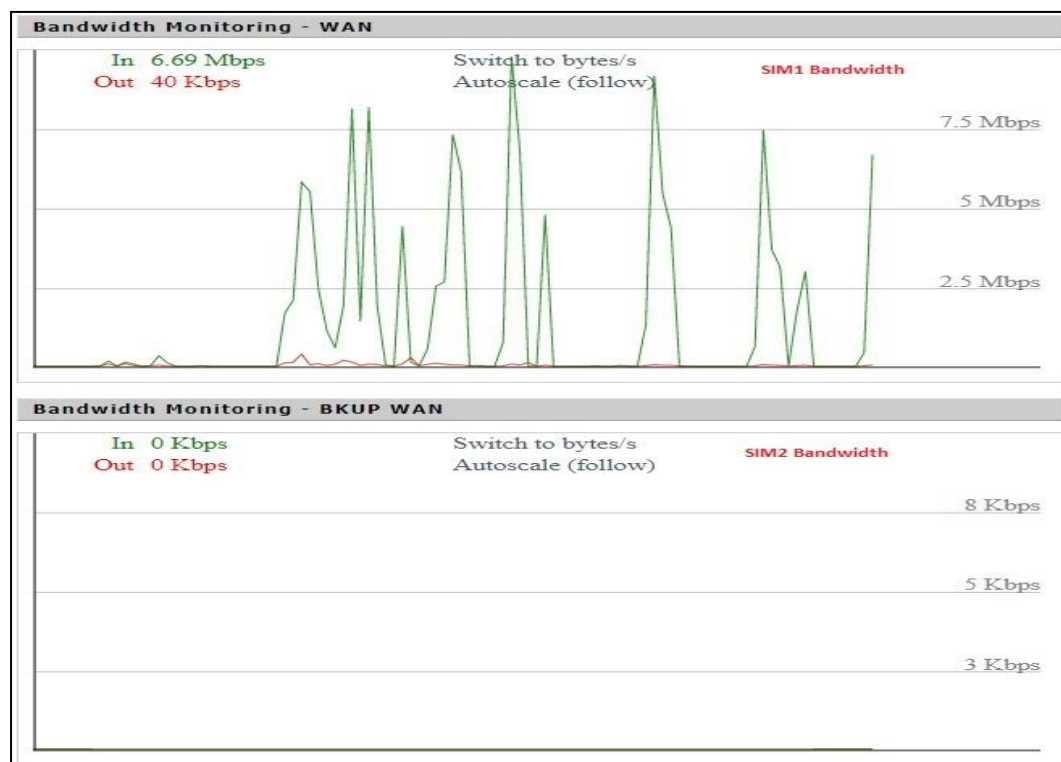


Bkup WAN Connection Type

Connection Type	dhcpc-bkup4G/5G	Configuration for SIM2
User Name		
Password		<input type="checkbox"/> Unmask
APN	jionet	
Allow these authentication	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP	
Connection type	Auto	
PIN		<input type="checkbox"/> Unmask
Keep Online Detection	Ping	
Detection Interval	120 Sec.	
Primary Detection Server IP	208 67 222 222	
Backup Detection Server IP	114 114 115 115	
Enable Dial Failure to Restart	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	(Default: 10 minutes)
Fixed WAN Netmask Address	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

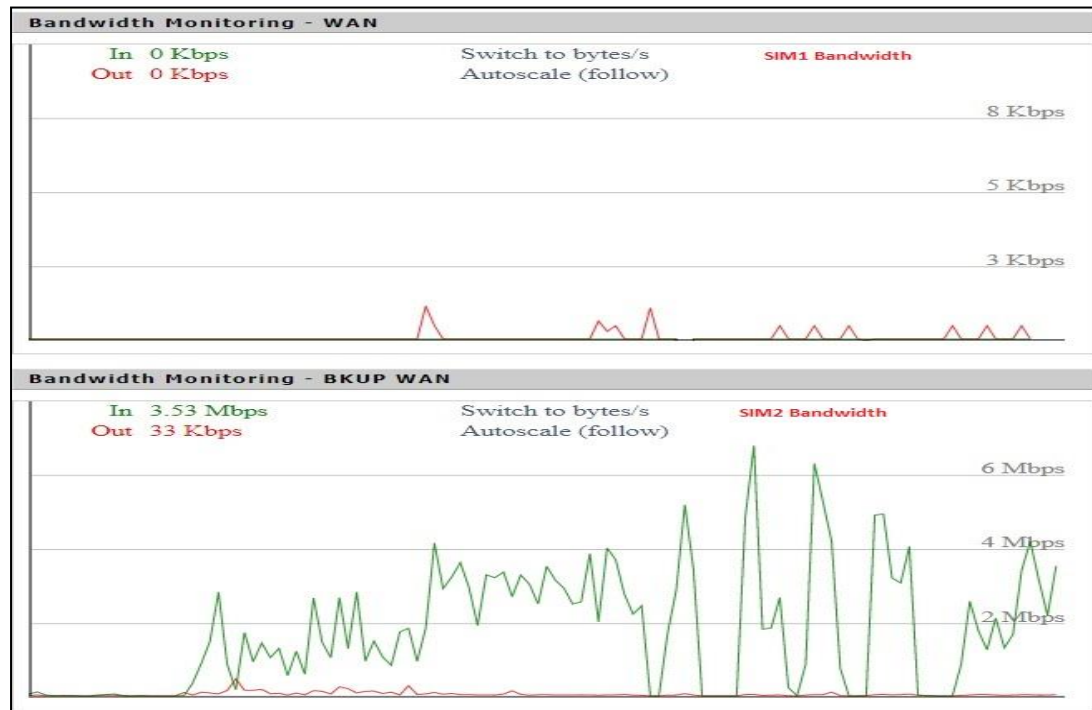
Bandwidth and Internet Speed test

Internet Running on Laptop. Internet will be activated only from SIM1.

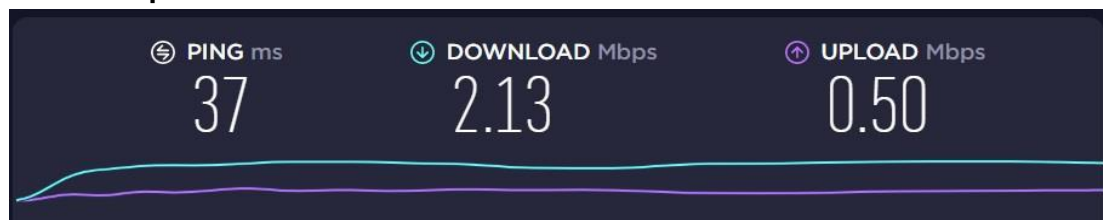


Remove SIM1 from SIM slot. Internet will be switch to SIM2 without interruption.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Internet Speed test



When "WAN failure Enable" and "Dual both online" but "load balance" is Enabled
Both SIM 1 and SIM 2 will be online at the same time, data will go through SIM 1 and SIM 2.
Bandwidth will be SIM 1+SIM 2's bandwidth.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Configuration Setting

SAN TELEQUIP GSF9364 Router

Firmware: v2.1.0 (Mar 18 2021 14:47:32) std
Time: 10:55:11 up 24 min, load average: 0.14, 0.13, 0.09
WAN IP: 10.182.131.231, BKUP WAN IP: 25.226.248.43

Menu

- Setup
 - Basic Setup
 - DDNS
 - MAC Address Clone
 - Advanced Routing
 - VLANs
 - Networking
- Wireless
- Services
- VPN
- Security

WAN Setup

DUAL LINK OPTION

- Enable WAN Failover: ☒ Enable ☐ Disable
- Dual Both Online: ☒ Enable ☐ Disable
- Load Balancer: ☒ Enable ☐ Disable

Wan Nat

- Wan Nat: ☒ Enable ☐ Disable

Help

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

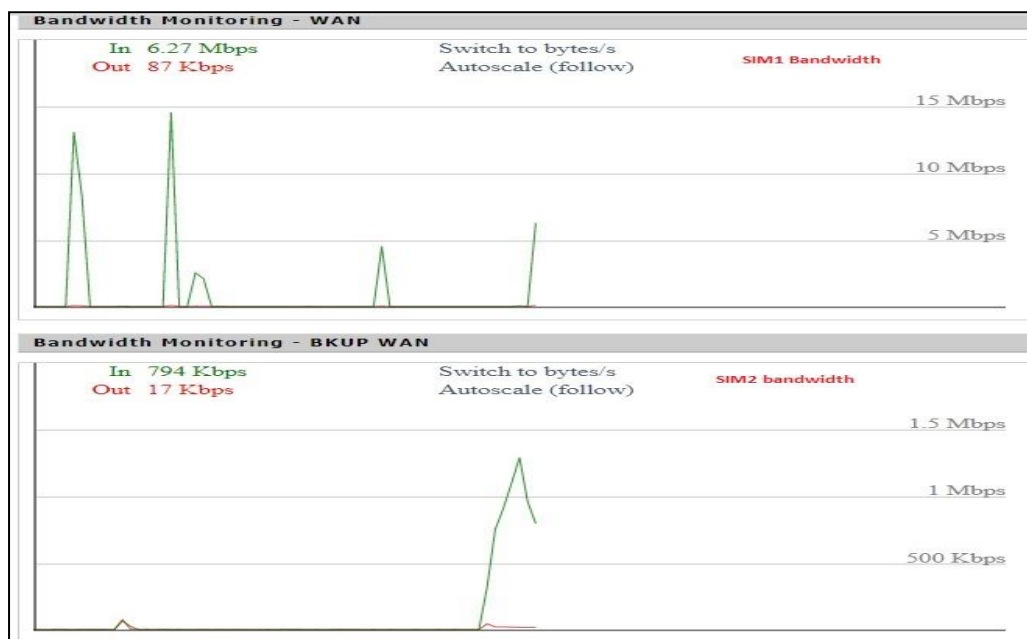
Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

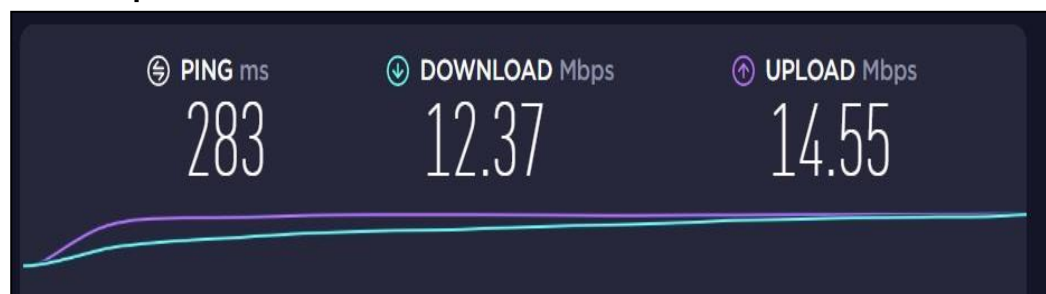
Local IP Address:

Bandwidth and Internet Speed test

Internet Running on Laptop. Internet will be activated from SIM1 and SIM2.



Internet Speed test



How will the TCP packets, from SIM1 & SIM2 be combined, to becoming meaningful data?

We use tcp socket which is long connection to assign to SIM1 and SIM2

Sending TCP Data

The TCP protocol is a byte stream service. It does not know anything about the format of the data being sent. It simply takes the data, encapsulates it into a TCP packet, and sends it to the remote peer. The TCP socket then keeps sent packets in memory and waits for an acknowledge from the remote peer.

If the packet is not acknowledged when the timeout expires, the same packet is resent. This process is repeated until a packet is either acknowledged or the TCP socket aborts the connection.

Disable: only one link can work between main link and backup link. If main link is online, it uses main link. If main link is offline, it switches to backup link. If main link is online again, it will not switch to main link. Only backup link is offline can it switch to main link.

Note: when users enable dual link option, they need to configure relevant keep online function if connection type of main link and backup link is 'Static IP' or 'DHCP'. Detailed configuration refers to Keep Online section. Connection type of main link and backup link forbid to be the same, and not under the same Ethernet port. For example, main link is 'Static IP', 'DHCP', or 'PPPOE', backup link must be 3G Link 1 or 3G Link 2, otherwise the page will appear corresponding hint.

Connection Type

Seven Ways: Disabled, Static IP, Automatic Configuration-DHCP, PPPOE, 3G Link 1, 3G Link 2, dhcp-4G, dhcp-bkup4G

Disabled

Connection Type	Disabled	▼
-----------------	----------	---

Forbid the setting of WAN port connection type

Static IP

Connection Type	Static IP
WAN IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Subnet Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Static DNS 1	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Static DNS 2	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Static DNS 3	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

WAN IP Address: Users set IP address by their own or ISP assigns

Subnet Mask: Users set subnet mask by their own or ISP assigns

Gateway: Users set gateway by their own or ISP assigns

Static DNS1/DNS2/DNS3: Users set static DNS by their own or ISP assigns

Automatic Configuration-DHCP

Connection Type Automatic Configuration - DHCP

IP address of WAN port gets automatic via DHCP

PPPOE

Connection Type PPPoE

User Name

Password ☐ Unmask

User Name: login the Internet

Password: login the Internet

3G Link 1

Connection Type 3G/UMTS/4G/LTE

User Name

Password ☐ Unmask

Dial String *99***1# (UMTS/3G/3.5G)

APN

PIN ☐ Unmask

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



User Name : login users' ISP (Internet Service Provider)
Password : login users' ISP
Dial String : dial number of users' ISP
APN : access point name of users' ISP
PIN : PIN code of users' SIM card

3G Link 2

Connection Type	3G/UMTS/4G/LTE	
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
Dial String	*99**1# (UMTS/3G/3.5G)	
APN	<input type="text"/>	
PIN	<input type="text"/>	<input type="checkbox"/> Unmask

User Name : login users' ISP (Internet Service Provider)
Password : login users' ISP
Dial String : dial number of users' ISP
APN : access point name of users' ISP
PIN : PIN code of users' SIM card

DHCP-4G

Connection Type	dhcp-4G/5G	
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
APN	airtelgprs.com	

User Name : login users' ISP (Internet Service Provider)
Password : login users' ISP
Dial String : dial number of users' ISP
APN : access point name of users' ISP

DHCP-bkup4G

Connection Type	dhcp-bkup4G	
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
APN	<input type="text"/>	

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



User Name : login users' ISP (Internet Service Provider)
Password : login users' ISP
Dial String : dial number of users' ISP
APN : access point name of users' ISP

Connection type

Connection type

Connection type: Auto, Force 4G, only 4G/3G/2G, Force 3G, Force 2G, prefer 3G, Prefer 2G options. If using 4G module, there has 4G network option. Users select different mode depending on their need

Keep Online Detection

Keep Online Detection
Enable Dial Failure to Restart ☒ Enable ☐ Disable (Default: 10 minutes)

This function is used to detect whether the Internet connection is active, if users set it and when the Cellular Gateway detect the connection is inactive, it will redial to users' ISP immediately to make the Connection active.

Detection Method:

None : do not set this function

Ping : Send ping packet to detect the connection, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

Route : Detect connection with route method, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP : Detect connection with PPP method, when choose this method, users should also configure "Detection Interval" item.

Detection Interval: time interval between two detections, unit is second

Primary Detection Server IP: the server used to response the Cellular Gateway's detection packet. These items only valid for method "Ping" and "Route".

Backup Detection Server IP: the server used to response the Cellular Gateway's detection packet. These items valid for method "Ping" and "Route".

Note: When users choose the “Route” or “Ping” method, it’s quite important to make sure that the “Primary Detection Server IP” and “Backup Detection Server IP” are usable and stable, because they have to response the detection packet frequently.

Force reconnect ☒ Enable ☐ Disable

Time

Force reconnects: this option schedules the pppoe or 3G reconnection by killing the pppd daemon and restart it.

Time: needed time to reconnect

Enable Dial Failure to Restart ☒ Enable ☐ Disable (Default: 10 minutes)

Enable Dial Failure to Restart: If the dial failure will be in the default time to restart

STP

STP ☐ Enable ☒ Disable

STP (Spanning Tree Protocol) can be applied to loop network. Through certain algorithm achieves path redundancy, and loop network cuts to tree-based network without loop in the meantime, thus to avoid the hyperplasia and infinite circulation of a message in the loop network

Optional Settings

Optional Settings

Router Name	<input type="text" value="GSF9364"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
MTU	<input type="text" value="Auto"/> <input type="text" value="1500"/>
Force Net Card Mode	<input type="text" value="Auto"/>

Cellular Gateway Name: set Cellular Gateway name

Host Name : ISP provides

Domain Name : ISP provides

MTU : Auto (1500) and manual (1200-1492 in PPPOE/PPTP/L2TP mode, 576-16320 in other modes)

Cellular Gateway Internal Network Settings

Cellular Gateway IP

Network Setup				
Router IP				
Local IP Address	192	168	1	1
Subnet Mask	255	255	255	0
Gateway	0	0	0	0
Local DNS	0	0	0	0
Loopback Address	10.254.0.222/32 eg:10.1.1.1			

Local IP Address : IP address of the Cellular Gateway

Subnet Mask : the subnet mask of the Cellular Gateway

The loopback interface is used to

Gateway : set internal gateway of the Cellular Gateway. If default, internal gateway is the address

of the Cellular Gateway

Local DNS : DNS server is auto assigned by network operator server. Users enable to use their own DNS server or other stable DNS servers, if not, keep it default

Loopback Address: The Loopback interface is a virtual network interface that your computer/Cellular Gateway uses to communicate with itself. They are not real physical interfaces. Identify the device. Other interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes. The only purpose of the loopback interface is to return the packets sent to it, i.e. whatever you send to it are received on the interface. It makes little sense to put a default route on the loopback interface, because the only place it can send packets to is the imaginary piece of wire that is looped from the output of the interface to the input.

Network Address Server Settings (DHCP)

These settings for the Cellular Gateway's Dynamic Host Configuration Protocol (DHCP) server functionality configuration. The Cellular Gateway can serve as a network DHCP server. DHCP server automatically assigns an IP address for each computer in the network. If they choose to enable the Cellular Gateway's DHCP server option, users can set all the computers on the LAN to automatically obtain an IP address and DNS, and make sure no other DHCP server in the network.

DHCP Type	<input type="text" value="DHCP Server"/>
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1. <input type="text" value="100"/>
Maximum DHCP Users	<input type="text" value="50"/>
Client Lease Time	<input type="text" value="1440"/> minutes
Static DNS 1	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Static DNS 2	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Static DNS 3	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
WINS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

DHCP Type: DHCP Server and DHCP Forwarder

Enter DHCP Server if set DHCP Type to DHCP Forwarder as blow:

DHCP Type	<input type="text" value="DHCP Forwarder"/>
DHCP Server	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

DHCP Server: keep the default Enable to enable the Cellular Gateway's DHCP server option. If users have already have a DHCP server on their network or users do not want a DHCP server, then select Disable

Start IP Address: enter a numerical value for the DHCP server to start with when issuing IP addresses. Do not start with 192.168.1.1 (the Cellular Gateway's own IP address).

Maximum DHCP Users: enter the maximum number of PCs that users want the DHCP server to assign IP addresses to. The absolute maximum is 253 if 192.168.1.2 is users' starting IP address. **Client Lease Time:** the Client Lease Time is the amount of time a network user will be allow disconnection to the Cellular Gateway with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

Static DNS (1-3): the Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Users' ISP will provide them with at least one DNS Server IP address. If users wish to utilize another, enter that IP address in one of these

fields. Users can enter up to three DNS Server IP addresses here. The Cellular Gateway will utilize them for quicker access to functioning DNS servers.

WINS: the Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If users use a WIN'S server, enter that server's IP address here. Otherwise, leave it blank.

DNSmasq: users' domain name in the field of local search, increase the expansion of the host option, to adopt DNSmasq can assign IP addresses and DNS for the subnet, if select DNSmasq, dhcp service is used for the subnet IP address and DNS.

Time Settings

NTP Client	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Time Zone	UTC+08:00 ▼
Summer Time (DST)	last Sun Mar - last Sun Oct ▼
Server IP/Name	<input type="text"/>

Select time zone of your location. To use local time, leave the checkmark in the box next to Use local time.

NTP Client: Get the system time from NTP server

Time Zone: Time zone options

Summer Time (DST): set it depends on users' location

Server IP/Name: IP address of NTP server, up to 32 characters. If blank, the system will find a server by default

Adjust Time

Adjust Time							
Auto ▼	2012	07	18	11	27	08	Set

Adjust Time: Auto and Manual way. Manual way needs to enter the time. Auto way is to get the time from PC web, click the bottom of setting to modify system time, has system adjust time service. They can change to adjust time by manual to achieve adjust time by the system if the system fails to get NTP server

After modify, click '**Save**' is to change but not take effect, click '**Apply Setting**' to take effect the change or click '**Cancel Changes**' to cancel it. Help information is on the right side of the page.

3.3.1.1 Dynamic DNS

If user's network has a permanently assigned IP address, users can register a domain name and have that name linked with their IP address by public Domain Name Servers (DNS). However, if their Internet account uses a dynamically assigned IP address, users will not know in advance what their IP address will be, and the address can change frequently. In this case, users can use a commercial dynamic DNS service, which allows them to register their domain to their IP address, and will forward traffic directed at their domain to their frequently-changing IP address.

DDNS Service: Cellular Gateway currently support DynDNS, freedns, Zoneedit, NO-IP,3322, easyDNS, TZO, DynSIP and Custom based on the user.

DDNS Service	3322.org	
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
Host Name	<input type="text"/>	
Type	Dynamic	
Wildcard	<input type="checkbox"/>	
Do not use external ip check	<input checked="" type="radio"/> Yes <input type="radio"/> No	

User Name: users register in DDNS server, up to 64 characteristics

Password: password for the user's name that users register in DDNS server, up to 32 characteristics

Host Name: users register in DDNS server, no limited for input characteristic for now

Type: depends on the server

Wildcard: support wildcard or not, the default is OFF. ON means *.host.3322.org is equal to host.3322.org

Do not use external ip check: enable or disable the function of 'do not use external ip check'

Force Update Interval: unit is day; try forcing the update dynamic DNS to the server by settled days

Options	
Force Update Interval	<input type="text" value="10"/> (Default: 10 Days, Range: 1 - 60)

Status

DDNS Status

Fri Nov 25 13:58:32 2011: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.

Fri Nov 25 13:58:32 2011: INADYN: IP read from cache file is '192.168.8.222'. No update required.

Fri Nov 25 13:58:32 2011: I:INADYN: IP address for alias 'testsixin.3322.org' needs update to '192.168.8.38'

Fri Nov 25 13:58:33 2011: I:INADYN: Alias 'testsixin.3322.org' to IP '192.168.8.38' updated successfully.

DDNS Status shows connection log information

3.3.1.2 MAC Address Clone

Some ISP need the users to register their MAC address. The users can clone the Cellular Gateway MAC address to their MAC address registered in ISP if they do not want to re-register their MAC address

☒ Enable ☐ Disable

Clone LAN MAC

00:AA:BB:CC:DD:43

Clone WAN MAC

00:AA:BB:CC:DD:44

Get Current PC MAC Address

Clone Wireless MAC

00:AA:BB:CC:DD:45

Clone MAC addresses can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

Noted that one MAC address is 48 characteristics, cannot be set to the multicast address, the first byte must be even. And MAC address value of network bridge br0 is determined by the smaller value of wireless MAC address and LAN port MAC address.

3.3.1.3 Advanced Cellular Gateway

Operating Mode: Gateway and Cellular Gateway

Operating Mode

Operating Mode

Gateway ▼

If the Cellular Gateway is hosting users' Internet connection, select Gateway mode. If another Cellular Gateway exists on their network, select Cellular Gateway mode.

Static Routing

Static Routing

Select set number

1 ()

Delete

Route Name

Metric

0

Destination LAN NET

0.0.0.0

Subnet Mask

0.0.0.0

Gateway

0.0.0.0

Interface

LAN & WLAN

Show Routing Table

Select set number : 1-50

Route Name : defined routing name by users, up to 25 characters

Metric : 0-9999

Destination LAN NET: the Destination IP Address is the address of the network or host to which users want to assign a static route

Subnet Mask : the Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

Gateway : IP address of the gateway device that allows for contact between the Cellular Gateway and the network or host.

Interface : indicate users whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network, necessary for certain software programs)

Show Routing Table

Routing Table Entry List			
Destination LAN NET	Subnet Mask	Gateway	Interface
192.168.1.1	255.255.255.255	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
192.168.1.0	255.255.255.0	0.0.0.0	WAN
169.254.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.1.1	LAN & WLAN

Refresh

Close

3.3.1.4 VLANs

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN <input type="button" value="v"/>
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>

VLANs function is to divide different VLAN ports by users' will. The system supports 16 VLAN port from VLAN0-VLAN15. However there is only 5 time ports (1 WAN port and 4 LAN port) divided by users themselves, and LAN port and WAN port disable to divide into one VLAN port meanwhile.

3.3.1.5 Networking

Bridging

Create Bridge

Bridge 0

br0

STP

Off

Prio

32768

MTU

1500

Add

Assign to Bridge

Add

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0 ra0

Auto Refresh Table

Bridging-Create Bridge: creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users are able to set the bridge priority order. The lowest number has the highest priority.

Bridging - Assign to Bridge: allows users to assign any valid interface to a network bridge. Consider setting the Wireless Interface options to Bridged if they want to assign any Wireless Interface here. Any system specific bridge setting can be overridden here in this field. Current Bridging Table: shows current bridging table

Create steps as below:

Click 'Add' to create a new bridge, configuration is as below:

Create Bridge

Bridge 0

br0

STP

Off

Prio

32768

MTU

1500

Bridge 1

br1

STP

On

Prio

32768

MTU

1500

Delete

Add

Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Bridge properties are as below:

Create Bridge

Bridge 0	br0	STP Off	Prio 32768	MTU 1500	Delete
Bridge 1	br1	STP On	Prio 32768	MTU 1500	Delete
IP Address	0.0.0.0				
Subnet Mask	0.0.0.0				
Add					

Enter relevant bridge IP address and subnet mask, click 'Add' to create a bridge.
 Note: Only create a bride can apply it.

Assign to Bridge

Assignment 0	none	Interface ra0	Prio 63	Delete
Add				

Assign to Bridge option: to assign different ports to created bridge. For example: assign port (wireless port) is ra0 in br1 bridge as below:

Prio means priority level: work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

Note: corresponding interface of WAN ports interface should not be binding, this bridge function is basically used for LAN port, and should not be binding with WAN port

If bind success, bridge binding list in the list of current bridging table is as below:

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0
br1	yes	ra0

Auto Refresh: On

To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:

Port Setup

Network Configuration eth2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration vlan0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration ra0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration apcli0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds1	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds3	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration br0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default

Port Setup: Set the port property, the default is not set

Network Configuration ra0 ☒ Unbridged ☐ Default

MTU

Multicast forwarding ☐ Enable ☒ Disable

Masquerade / NAT ☒ Enable ☐ Disable

IP Address

Subnet Mask

Choose not bridge to set the port's own properties, detailed properties are as below:

MTU : maximum transfer unit
 Multicast forwarding : enable or disable multicast forwarding
 Masquerade/NAT : enable or disable Masquerade/NAT
 IP Address : set ra0's IP address, and do not conflict with other ports or bridge
 Subnet Mask : set the port's subnet mask

Multiple DHCP Server

DHCP 0 Start Max Leasetime


Multiple DHCPD: using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Lease time means the client lease time, the unit is second,

click 'Save' or 'Apply' to put it into effect after setting.

Note: Only configure and click 'Save' can configure the next, can not configure multiple DHCP at the same time.

3.3.2 Wireless

3.3.2.1 Basic Settings



Wireless Network ☒ Enable ☐ Disable

Physical Interface ra0 - SSID [San-Telequip] HWAddr []

Wireless Mode

Wireless Network Mode

Wireless Network Name (SSID)

Wireless Channel

Wireless SSID Broadcast ☒ Enable ☐ Disable

Network Configuration ☐ Unbridged ☒ Bridged

Virtual Interfaces

Add

Save Apply Settings Cancel Changes

Wireless Network : "Enable", radio on.
: "Disable", radio off.

Wireless Mode : AP, Client, Adhoc, Repeater, Repeater Bridge four options.

Wireless Network Mode:

Mixed : Support 802.11b, 802.11g, 802.11n wireless devices.
BG-Mixed : Support 802.11b, 802.11g wireless devices.
B-only : Only supports the 802.11b standard wireless devices.
B-only : Only supports the 802.11b standard wireless devices.
G-only : Only supports the 802.11g standard wireless devices.
NG-Mixed : Support 802.11g, 802.11n wireless devices.
N-only : Only supports the 802.11g standard wireless devices.

Wireless Network Name (SSID): The SSID is the network name shared among all devices in wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Wireless Channel: A total of 1-13 channels to choose more than one wireless device environment please try to avoid using the same channel with other devices.

Channel Width : 20MHZ and 40MHZ.

Extension Channel : Channel for 40MHZ, you can choose upper or lower.

Wireless SSID Broadcast :

Enable : SSID broadcasting.

Disable : Hidden SSID.

Network Configuration:

Bridged : Bridge to the Cellular Gateway, under normal circumstances, please select the bridge.

Unbridged : There is no bridge to the Cellular Gateway, IP addresses need to manually configure.

Network Configuration	<input checked="" type="radio"/> Unbridged <input type="radio"/> Bridged
Multicast forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Masquerade / NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Virtual Interfaces : Click Add to add a virtual interface. Add successfully, click on the remove, you can remove the virtual interface

Virtual Interfaces	
Virtual Interfaces ra1 SSID [dd-wrt_vap] HWAddr [00:AA:BB:CC:DD:16]	
Wireless Network Name (SSID)	<input type="text" value="dd-wrt_vap"/>
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged
<input type="button" value="Add"/> <input type="button" value="Remove"/>	

AP Isolation : This setting isolates wireless clients so access to and from other wireless clients are stopped.

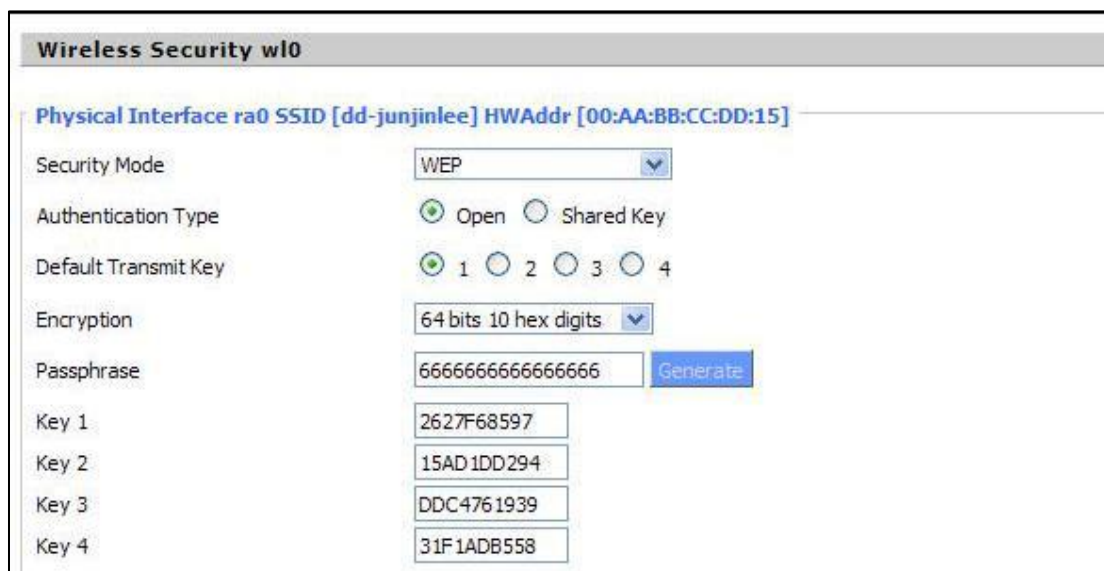
Note : Save your changes, after changing the "Wireless Mode", "Wireless Network Mode", "wireless width", "broadband" option, please click on this button, and then configure the other options.

3.3.2.2 Wireless Security

Wireless security options used to configure the security of your wireless network. This route is a total of seven kinds of wireless security mode. Disabled by default, not safe mode is enabled. Such as changes in Safe Mode, click Apply to take effect immediately.



The screenshot shows the 'Wireless Security wlo' configuration window. At the top, it displays 'Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]'. Below this, the 'Security Mode' is set to 'Disabled' in a dropdown menu. At the bottom, there are two buttons: 'Save' and 'Apply Settings'.



The screenshot shows the 'Wireless Security wlo' configuration window with WEP settings. The 'Security Mode' is set to 'WEP'. Under 'Authentication Type', 'Open' is selected. For 'Default Transmit Key', key '1' is selected. The 'Encryption' is set to '64 bits 10 hex digits'. A 'Passphrase' field contains '6666666666666666' with a 'Generate' button next to it. Below the passphrase, four keys are listed: Key 1 (2627F68597), Key 2 (15AD1DD294), Key 3 (DDC4761939), and Key 4 (31F1ADB558).

WEP : Is a basic encryption algorithm is less secure than WPA. Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

Authentication Type : Open or shared key

Default Transmit Key : Select the key form Key 1 - Key 4 key.

Encryption : There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP,

select the desired encryption bit, and enter a passphrase or up to four WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid

hexadecimal characters are "0"-"9" and "A"-"F"

Passphrase : The letters and numbers used to generate a key.

Key1-Key4 : Manually fill out or generated according to input the pass phrase.

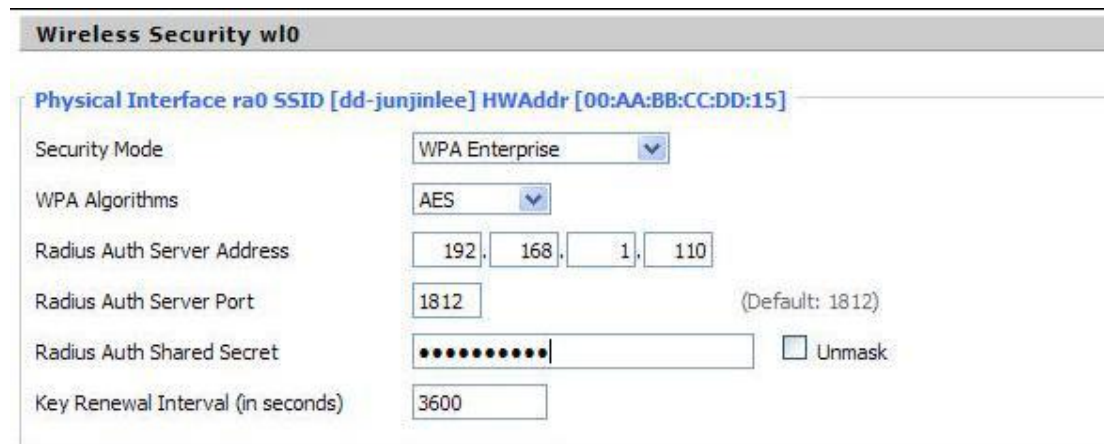


The screenshot shows the 'Wireless Security w10' configuration window. At the top, it displays 'Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]'. The 'Security Mode' is set to 'WPA Personal'. The 'WPA Algorithms' are set to 'AES'. The 'WPA Shared Key' is masked with dots, and there is an 'Unmask' checkbox. The 'Key Renewal Interval (in seconds)' is set to '3600', with a note '(Default: 3600, Range: 1 - 99999)'. At the bottom, there are 'Save' and 'Apply Settings' buttons.

WPA Personal/WPA2 Personal / WPA2 Person Mixed: TKIP/AES/TKIP+AES dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allow WPA Personal and WPA2 Personal client mix.

WPA Shared Key: Between 8 and 63 ASCII character or hexadecimal digits. .

Key Renewal Interval (in seconds): 1-99999



The screenshot shows the 'Wireless Security w10' configuration window. At the top, it displays 'Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]'. The 'Security Mode' is set to 'WPA Enterprise'. The 'WPA Algorithms' are set to 'AES'. The 'Radius Auth Server Address' is set to '192.168.1.110'. The 'Radius Auth Server Port' is set to '1812', with a note '(Default: 1812)'. The 'Radius Auth Shared Secret' is masked with dots, and there is an 'Unmask' checkbox. The 'Key Renewal Interval (in seconds)' is set to '3600'.

WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external RADIUS server to perform user authentication.

WPA Algorithms : AES/TKIP/: TPIP+AES.

Radius Auth Sever Address : The IP address of the RADIUS server.

Radius Auth Server Port : The RADIUS Port (default is 1812)

Radius Auth Shared Secret : The shared secret from the RADIUS server

Key Renewal Interval (in seconds) : 1-99999

3.3.3 Services

3.3.3.1 Services

DHCP Server

DHCPd assigns IP addresses to users' local devices. While the main configuration is on the setup page users can program some nifty special functions here.

DHCP Server



Additional DHCPd Options

Static Leases

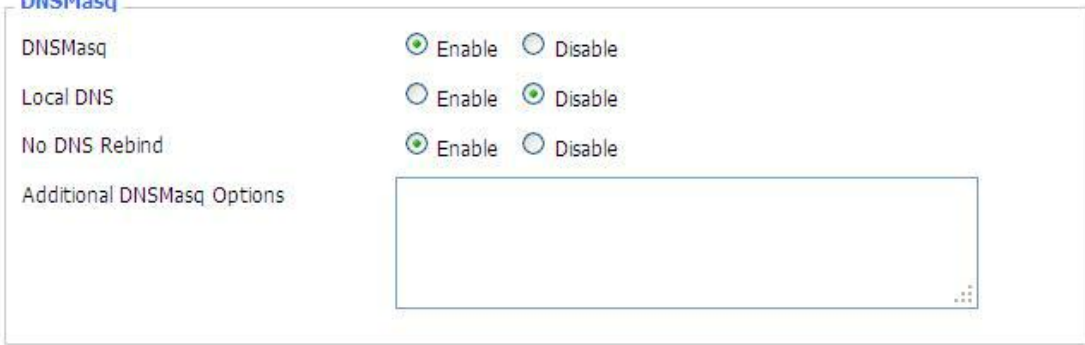
MAC Address	Host Name	IP Address	Client Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> minutes

Additional DHCPd Options: some extra options users can set by entering them

DNSmasq

DNSmasq is a local DNS server. It will resolve all host names known to the Cellular Gateway from dhcp (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers.

Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.



DNSMasq ☒ Enable ☐ Disable

Local DNS ☐ Enable ☒ Disable

No DNS Rebind ☒ Enable ☐ Disable

Additional DNSMasq Options

Local DNS: enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames

No DNS Rebind: when enabled, it can prevent an external attacker to access the Cellular Gateway's internal

Web interface. It is a security measure

Additional DNSMasq Options: some extra options users can set by entering them in

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Additional DNS Options.

Static allocation: dhcp-host=AB:CD: EF: 11:22:33,192.168.0.10, myhost, myhost. domain,12h
max lease number: dhcp-lease-max=2

DHCP server IP range: dhcp-range=192.168.0.110, 192.168.0.111,12h

SNMP

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Location	<input type="text" value="Unknown"/>
Contact	<input type="text" value="root"/>
Name	<input type="text" value="SanTelequip"/>
RO Community	<input type="text" value="public"/>
RW Community	<input type="text" value="private"/>

SNMP

Location : equipment location

Contact : contact this equipment management

Name : device name

RO Community: SNMP RO community name, the default is public, only to read.

RW Community: SNMP RW community name, the default is private, Read-write permissions

SSHD

Enabling SSHd allows users to access the Linux OS of their Cellular Gateway with an SSH client

Secure Shell

SSHd	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH TCP Forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Password Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Port	<input type="text" value="22"/> (Default: 22)
Authorized Keys	<input type="text"/>

SSH TCP Forwarding: enable or disable to support the TCP forwarding

Password Login : allows login with the Cellular Gateway password (username is root)

Port : port number for SSHd (default is 22)

Authorized Keys : here users paste their public keys to enable key-based login
(More secure than a simple password)

System log

Enable Syslogd to capture system messages. By default, they will be collected in the local file /var/log/messages. To send them to another system, enter the IP address of a remote

System Log

Syslogd	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Syslog Out Mode	<input checked="" type="radio"/> Net <input type="radio"/> Console
Remote Server	<input type="text"/>

syslog server.

Sys log Out Mode : two log mode

Net : the log information output to a syslog server

Console : the log information output to console port

Remote Server : if choose net mode, users should input a syslog server's IP Address and run a

sys log server program on it.

Telnet

Telnet

Telnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
--------	---

Telnet: enable a telnet server to connect to the Cellular Gateway with telnet. The username is root and the password is the Cellular Gateway's password.

Note: If users use the Cellular Gateway in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSHd and deactivate telnet.

WAN Traffic Counter

Ttraff Daemon: enable or disable wan traffic counter function

WAN Traffic Counter

ttraff Daemon	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
---------------	---

3.3.4 VPN

3.3.4.1 PPTP

PPTP Server

PPTP Server

PPTP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Broadcast support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Force MPPE Encryption	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DNS1	<input type="text"/>
DNS2	<input type="text"/>
WINS1	<input type="text"/>
WINS2	<input type="text"/>
Server IP	<input type="text"/>
Client IP(s)	<input type="text"/>
CHAP-Secrets	<div><input type="text"/></div>

Broadcast support : enable or disable broadcast support of PPTP server

Force MPPE Encryption : enable or disable force MPPE encryption of PPTP data

DNS1/DNS2/WINS1/WINS2: set DNS1/DNS2/WINS1/WINS2

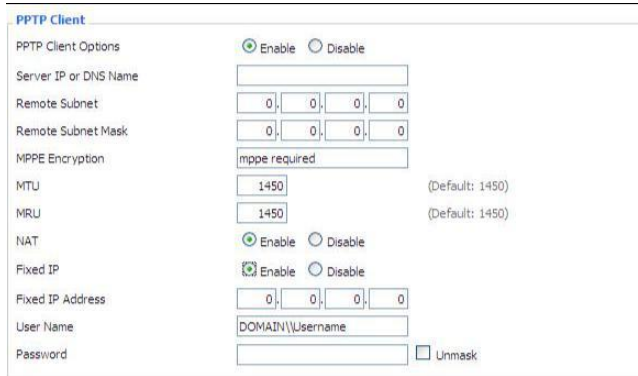
Server IP : input IP address of the Cellular Gateway as PPTP server, differ from LAN address

Client IP(s) : IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx

CHAP Secrets : user name and password of the client using PPTP service

Note: client IP must be different with IP assigned by Cellular Gateway DHCP. The format of CHAP Secrets is user * password *.

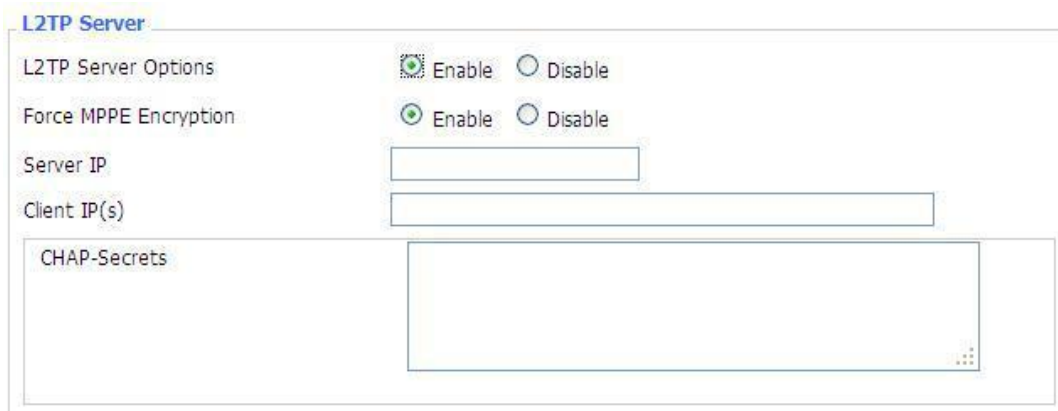
PPTP Client



Server IP or DNS Name:	PPTP server's IP Address or DNS Name
Remote Subnet	: the network of the remote PPTP server
Remote Subnet Mask	: subnet mask of remote PPTP server
MPPE Encryption	: enable or disable Microsoft Point-to-Point Encryption.
MTU	: Maximum Transmission Unit
MRU	: Maximum Receive Unit
NAT	: Network Address Translation
Fixed IP	: Enable or Disable Fixed IP
Fixed IP Address	: Fixed IP Address
User Name	: user name to login PPTP Server.
Password	: password to log into PPTP Server.

3.3.4.2 L2TP

L2TP Server



San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Force MPPE Encryption : enable or disable force MPPE encryption of L2TP data
Server IP: input IP address of the Cellular Gateway as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx
CHAP Secrets: user name and password of the client using L2TP service

Note: client IP must be different with IP assigned by Cellular Gateway DHCP. The format of CHAP Secrets is user * password *

L2TP Client

Gateway (L2TP Server): L2TP server's IP Address or DNS Name
Remote Subnet : the network of remote PPTP server
Remote Subnet Mask : subnet mask of remote PPTP server
MPPE Encryption : enable or disable Microsoft Point-to-Point Encryption
MTU : maximum transmission unit
MRU : maximum receive unit
NAT : network address translation
Fixed IP : Enable or Disable Fixed IP
Fixed IP Address : Fixed IP Address
User Name : user name to login L2TP Server
Password : password to login L2TP Server
Require CHAP : enable or disable support chap authentication protocol
Refuse PAP : enable or disable refuse to support the pap authentication
Require Authentication : enable or disable support authentication protocol

L2TP Client

L2TP Client Options ☒ Enable ☐ Disable

User Name

Password ☐ Unmask

Gateway (L2TP Server)

Remote Subnet

Remote Subnet Mask

MPPE Encryption

MTU (Default: 1450)

MRU (Default: 1450)

NAT ☒ Enable ☐ Disable

Fixed IP ☒ Enable ☐ Disable

Fixed IP Address

Require CHAP ☒ Yes ☐ No

Refuse PAP ☒ Yes ☐ No

Require Authentication ☒ Yes ☐ No

3.3.4.3 OPENVPN

OPENVPN Server

Start OpenVPN Server ☒ Enable ☐ Disable

Start Type ☐ WAN Up ☒ System

Config via ☒ Server ☐ Daemon

Server mode ☒ Router (TUN) ☐ Bridge (TAP)

Start Type : WAN UP----start after on-line, System----start when boot up
 Config via : GUI----Page configuration, Config File----config File configuration
 Server mode : Cellular Gateway (TUN)-route mode, Bridge (TAP)----bridge mode Cellular Gateway (TUN)

Network

Netmask

Network : network address allowed by OPENVPN server

Netmask : netmask allowed by OPENVPN server

Bridge (TAP):

DHCP-Proxy mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Pool start IP	<input type="text" value="0.0.0.0"/>
Pool end IP	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>

DHCP-Proxy mode : enable or disable DHCP-Proxy mode

Pool starts IP : pool start IP of the client allowed by OPENVPN server

Pool end IP : pool end IP of the client allowed by OPENVPN server

Gateway : the gateway of the client allowed by OPENVPN server

Netmask : netmask of the client allowed by OPENVPN server

Port	<input type="text" value="1194"/> (Default: 1194)
Tunnel Protocol	<input type="text" value="UDP"/>
Encryption Cipher	<input type="text" value="Blowfish CBC"/>
Hash Algorithm	<input type="text" value="SHA1"/>

Port : listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm : Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5

Advanced Options

Use LZO Compression : enable or disable use LZO compression for data transfer

Redirect default Gateway : enable or disable redirect default gateway

Allow Client to Client : enable or disable allow client to client

Allow duplicate cn : enable or disable allow duplicate cn

TUN MTU Setting : set the value of TUN MTU

TCP MSS : MSS of TCP data

TLS Cipher : TLS (Transport Layer Security) encryption standard supports

AES-128 SHA and AES-256 SHA

Client connects script : define some client script by user self

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Redirect default Gateway	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Allow Client to Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Allow duplicate cn	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
TUN MTU Setting	<input type="text" value="1500"/>	(Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/>	(Default: Disable)
TLS Cipher	<input type="text" value="Disable"/>	
Client connect script	<div></div>	

CA Cert: CA certificate

Public Server Cert	<div></div>
Private Server Key	<div></div>
DH PEM	<div></div>

Public Server Cert : server certificate
 Private Server Key : the key seted by the server
 DH PEM : PEM of the server
 Additional Config : additional configurations of the server
 CCD-Dir DEFAULT file : other file approaches
 TLS Auth Key : authority key of Transport Layer Security
 Certificate Revoke List: configure some revoke certificates

Additional Config	<div></div>
CCD-Dir DEFAULT file	<div></div>
TLS Auth Key	<div></div>
Certificate Revoke List	<div></div>

OPENVPN Client

Server IP/Name	<input type="text" value="0.0.0.0"/>	
Port	<input type="text" value="1194"/>	(Default: 1194)
Tunnel Device	<input type="text" value="TUN"/>	
Tunnel Protocol	<input type="text" value="UDP"/>	
Encryption Cipher	<input type="text" value="Blowfish CBC"/>	
Hash Algorithm	<input type="text" value="SHA1"/>	
nsCertType verification	<input type="checkbox"/>	

Server IP/Name : IP address or domain name of OPENVPN server
 Port : listen port of OPENVPN client
 Tunnel Device : TUN----Cellular Gateway mode, TAP----Bridge mode
 Tunnel Protocol : UDP and TCP protocol
 Encryption Cipher : Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC
 Hash Algorithm : Hash algorithm provides a method of quick access to data, including
 SHA1, SHA256, SHA512, MD5 nsCertType verification : support ns certificate type

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
NAT	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Bridge TAP to br0	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Local IP Address	<input type="text"/>	
TUN MTU Setting	<input type="text" value="1500"/>	(Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/>	(Default: Disable)
TLS Cipher	<input type="text" value="Disable"/>	
TLS Auth Key	<input type="text"/>	
Additional Config	<input type="text"/>	
Policy based Routing	<input type="text"/>	

Use LZO Compression : enable or disable use LZO compression for data transfer
 NAT : enable or disable NAT through function
 Bridge TAP to br0 : enable or disable bridge TAP to br0
 Local IP Address : set IP address of local OPENVPN client
 TUN MTU Setting : set MTU value of the tunnel
 TCP MSS : mss of TCP data
 TLS Cipher : TLS (Transport Layer Security) encryption standard supports AES-128
 SHA and AES-256 SHA
 TLS Auth Key : authority key of Transport Layer Security
 Additional Config : additional configurations of OPENVPN server
 Policy based Routing : input some defined routing policy

CA Cert	<input type="text"/>
Public Client Cert	<input type="text"/>
Private Client Key	<input type="text"/>

CA Cert: CA certificate
Public Client Cert: client certificate
Private Client Key: client key

3.3.4.4 IPSEC

Global settings

Global settings

Enable NAT-Traversal ☒

Debug Level None ▾

[Save](#)

Enable NAT-Traversal: Enable or disable nat traversal function

Debug Level: Enable or disable debug

Connect Status and Control

Connection status and control

Name	Type	Common Name	status	Action
Add				

Show IPSEC connection and status of current Cellular Gateway on IPSEC page.

Name : the name of IPSEC connection

Type : The type and function of current IPSEC connection

Common name: local subnet, local address, opposite end address and opposite end subnet of current connection

Status : connection status: closed, negotiating, establish

Closed : this connection does not launch a connection request to opposite end

Negotiating : this connection launches a request to opposite end, is under negotiating, the connection has not been established yet

Establish : the connection has been established, enabled to use this tunnel

Action : the action of this connection, current is to delete, edit, reconnect and enable

Delete : to delete the connection, also will delete IPSEC if IPSEC has set up

Edit : to edit the configure information of this connection, reload this connection to make the configuration effect after edit

Reconnect : this action will remove current tunnel, and re-launch tunnel establish

request **Enable:** when the connection is enabled, it will launch tunnel establish request when the system reboot or reconnect, otherwise the connection will not do it

Add : to add a new IPSEC connection

Add IPSEC connection or edit IPSEC connection

Type : to choose IPSEC mode and relevant functions in this part, supports tunnel mode

Type

Type

IPSEC role ☒ Client ☐ Server

client, tunnel mode server and transfer mode currently

Connection : this part contains basic address information of the tunnel

Connection

Connection

Name	<input type="text" value="CSS"/>	Enabled	<input checked="" type="checkbox"/>
Local WAN Interface	<input type="text" value="WAN"/>	Peer WAN address	<input type="text" value="103.141.218.182"/>
Local Subnet	<input type="text" value="10.254.0.222/32"/>	Peer subnet	<input type="text" value="172.147.0.0/22"/>
Local Id	<input type="text"/>	Peer ID	<input type="text" value="@hemabh"/>

Name : to indicate this connection name, must be unique

Enabled : If enable, the connection will send tunnel connection request when it is reboot or Re-connection, otherwise it is no need if disable

Local WAN Interface : local address of the tunnel

Remote Host Address: IP/domain name of end opposite; this option cannot fill in if using tunnel mode server

Local Subnet : IPsec local protects subnet and subnet mask, i.e., 192.168.1.0/24; this option cannot fill in if using transfer mode

Remote Subnet : IPsec opposite end protects subnet and subnet mask, i.e. 192.168.7.0/24; this option cannot fill in if using transfer mode.

Local ID : tunnel local end identification, IP and domain name are available

Peer ID : tunnel opposite end identification, IP and domain name are available

Remote ID/ Peer ID also known as match Identity.

Detection: this part contains configure information of connection detection

Detection

Enable DPD Detection ☒

Time Interval (S) Timeout (S) Action

Enable Connection Detection ☒

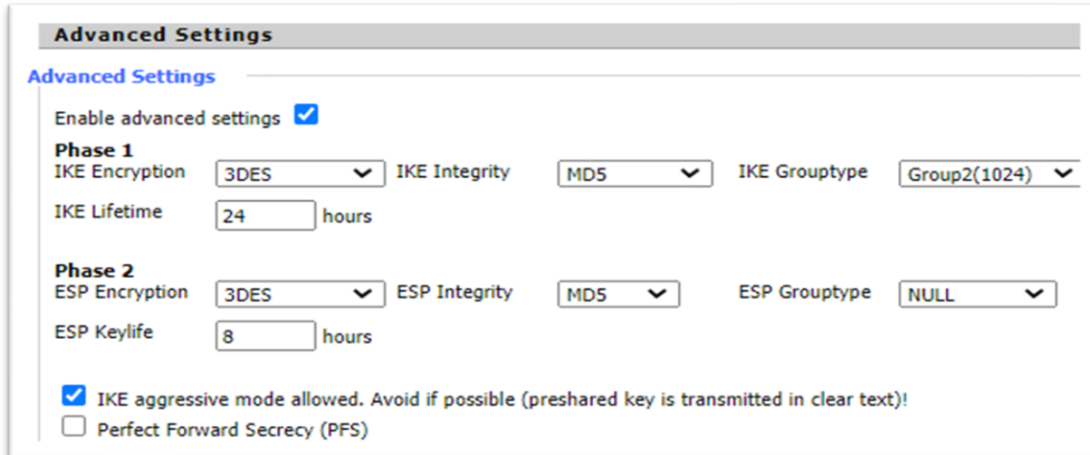
Enable DPD Detection : enable or disable this function, tick means enable

Time Interval : set time interval of connect detection (DPD)

Timeout : set the timeout of connect detection

Action : set the action of connect detection

Advanced Settings: this part contains relevant setting of IKE, ESP, negotiation mode, etc.



Advanced Settings

Advanced Settings

Enable advanced settings ☒

Phase 1

IKE Encryption: 3DES IKE Integrity: MD5 IKE Group type: Group2(1024)

IKE Lifetime: 24 hours

Phase 2

ESP Encryption: 3DES ESP Integrity: MD5 ESP Group type: NULL

ESP Key life: 8 hours

☒ IKE aggressive mode allowed. Avoid if possible (preshared key is transmitted in clear text)!

☐ Perfect Forward Secrecy (PFS)

Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise It will automatic negotiation according to opposite end

IKE Encryption: IKE phased encryption mode

IKE Integrity : IKE phased integrity solution

IKE Group type : DH exchange algorithm

IKE Lifetime : set IKE lifetime, current unit is hour, the default is 0


ESP Encryption : ESP encryption type

ESP Integrity : ESP integrity solution

ESP Key life : set ESP key life, current unit is hour, the default is 0

IKE aggressive mode allowed : negotiation mode adopt aggressive mode if tick; it is main mode if non-tick

Perfect forward secrecy (PFS) : It is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised.



Authentication

☒ Use a Pre-Shared Key:

☐ Generate and use the X.509 certificate

3.3.4.5 GRE

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP) transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol VPN (Virtual Private Network).

San Telequip (P) Ltd.,
 504 & 505 Deron Heights, Baner Road
 Pune 411045, India
 Phone : +91-20-27293455, 9764027070, 8390069393
 email : info@santelequip.com



GRE Tunnel

GRE Tunnels list

Number	Name	Enable	Through	Peer Wan IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Keepalive	Retry times	Interval	Fail Action
1	fff	Yes	PPP	120.42.46.98	192.168.5.0/24	200.200.200.1	200.200.200.5	255.255.255.0	No	0	0	Hold

Refresh Close

Number: [1] [Delete]

Status: [Enable]

Name: [fff]

Through: [PPP]

Peer Wan IP Addr: [120.42.46.98]

Peer Subnet: [192.168.5.0/24] (eg:192.168.1.0/24)

Peer Tunnel IP: [200.200.200.1]

Local Tunnel IP: [200.200.200.5]

Local Netmask: [255.255.255.0]

GRE Tunnel : enable or disable GRE function
Number : Switch on/off GRE tunnel app
Status : Switch on/off someone GRE tunnel app
Name : GRE tunnel name
Through : The GRE packet transmit interface
Peer Wan IP Addr : The remote WAN address
Peer Subnet : The remote gateway local subnet, eg: 192.168.1.0/24
Peer Tunnel IP : The remote tunnel ip address
Local Tunnel IP : The local tunnel ip address
Local Netmask : Netmask of local network

Keepalive: ☒ Enable ☐ Disable

Retry times: []

Interval: []

Fail Action: [Hold]

Keepalive : Enable or disable GRE Keep alive function
Retry times : GRE keep alive detect fail retries
Interval : The time interval of GRE keeps alive packet sent
Fail Action : The action would be exec after keeping alive failed Click on “**View GRE tunnels**” keys can view the information of GRE

3.3.5 Security

3.3.5.1 Firewall

You can enable or disable the firewall, filter specific Internet data types, and prevent anonymous Internet requests, ultimately enhance network security.

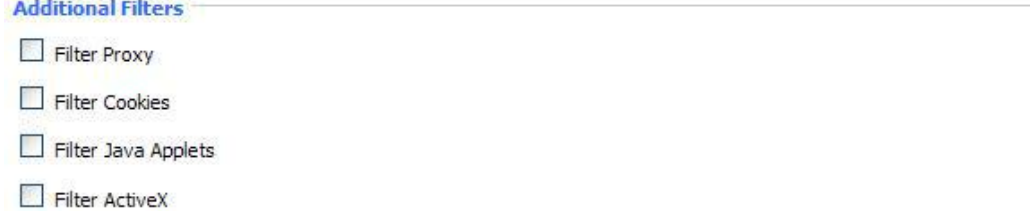
Firewall Protection



The screenshot shows a 'Firewall Protection' section with a sub-header 'SPI Firewall'. Below it, there are two radio buttons: 'Enable' (which is selected) and 'Disable'.

Firewall enhance network security and use SPI to check the packets into the network. To use firewall protection, choose to enable otherwise disabled. Only enable the SPI firewall, you can use other firewall functions: filtering proxy, block WAN requests, etc.

Additional Filters



The screenshot shows an 'Additional Filters' section with four checkboxes, all of which are currently unchecked:

- ☐ Filter Proxy
- ☐ Filter Cookies
- ☐ Filter Java Applets
- ☐ Filter ActiveX

Filter Proxy: WAN proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

Filter Cookies: Cookies are the website of data the data stored on your computer. When you interact with the site, the cookies will be used. Click the check box to enable the function Otherwise disabled.

Filter Java Applets: If refuse to Java, you may not be able to open web pages using the Java Programming. Click the check box to enable the function otherwise disabled.

Filter ActiveX: If refuse to ActiveX, you may not be able to open web pages using the ActiveX Programming. Click the check box to enable the function otherwise disabled.

Prevent WAN Request

Block WAN Requests

- ☒ Block Anonymous WAN Requests (ping)
- ☒ Filter IDENT (Port 113)
- ☒ Block WAN SNMP access

Block Anonymous WAN Requests (ping) : By selecting “Block Anonymous WAN Requests(ping)” box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled, choose to disable allow anonymous Internet requests.

Filter IDENT (Port 113) : Enable this feature can prevent port 113 from being scanned from outside. Click the check box to enable the function otherwise disabled.

Block WAN SNMP access: This feature prevents the SNMP connection requests from the WAN. After complete the changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

Impede WAN DoS/Bruteforce

Impede WAN DoS/Bruteforce

- ☐ Limit SSH Access
- ☐ Limit Telnet Access
- ☐ Limit PPTP Server Access
- ☐ Limit L2TP Server Access

Limit ssh Access: This feature limits the access request from the WAN by ssh, and per minute upto accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit PPTP Server Access: When build a PPTP Server in the Cellular Gateway, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit L2TP Server Access: When build a L2TP Server in the Cellular Gateway, this feature

limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Log Management

Log

Log

☒ Enable ☐ Disable

Log Level

High ▼

Options

Dropped

Disable ▼

Rejected

Enable ▼

Accepted

Enable ▼

The Cellular Gateway can keep logs of all incoming or outgoing traffic for your Internet connection.

Log: To keep activity logs, select Enable. To stop logging, select Disable. When select enable, the following page will appear.

Log Level: Set this to the required log level. Set Log Level higher to log more actions.

Options: When select Enable, the corresponding connection will be recorded in the journal, the disabled are not recorded.

Incoming Log: To see a temporary log of the Cellular Gateway's most recent incoming traffic, click the Incoming Log button.

Incoming Log Table			
Source IP	Protocol	Destination Port Number	Rule
		Refresh	Close

Outgoing Log: To see a temporary log of the Cellular Gateway's most recent outgoing traffic, click the Outgoing Log button.

Outgoing Log Table				
LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	119.147.32.204	UDP	8000	Accepted
192.168.1.164	112.90.86.244	UDP	8000	Accepted
192.168.1.164	119.147.45.157	UDP	8000	Accepted
192.168.1.164	183.60.49.15	UDP	8000	Accepted
192.168.1.164	183.60.16.70	UDP	8000	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted

Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

3.3.6 Access Restrictions

3.3.6.1 WAN Access

Use access restrictions, you can block or allow specific types of Internet applications. You can set specific PC-based Internet access policies. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses.

Access Policy

Policy: 1 () Delete Summary

Status: ☐ Enable ☒ Disable

Policy Name:

PCs: Edit List of clients

☐ Deny ☒ Filter

Internet access during selected days and hours.

Two options in the default policy rules: "Filter" and "reject". If select "Deny", you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter", It will block specific computers to access the specific sites at a specific time period. You can set up 10 Internet access policies filtering specific PCs access Internet services at a particular time period.

Access Policy : You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy.

Status : Enable or disable a policy.

Policy Name : You may assign a name to your policy.

PCs : The part is used to edit client list, the strategy is only effective for the PC in the list.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Days

Everyday	Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Times

24 Hours ☒

From ☐ 0 : 00 To ☐ 0 : 00

Days : Choose the day of the week you would like your policy to be applied.
Times : Enter the time of the day you would like your policy to be applied.

Website Blocking by URL Address

<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Website Blocking by Keyword

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Website Blocking by URL Address: You can block access to certain websites by entering their URL.

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Website Blocking by Keyword: You can block access to certain website by the keywords contained in their webpage

List of clients

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC	Address
MAC 01	00:AA:BB:CC:DD:EE
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00

Enter the IP Address of the clients

IP	Address
IP 01	192.168.1.15
IP 02	192.168.1.0
IP 03	192.168.1.0
IP 04	192.168.1.0
IP 05	192.168.1.0
IP 06	192.168.1.0

Enter the IP Range of the clients

IP Range	Start	End
IP Range 01	192.168.1.19 ~ 192.168.1.30	
IP Range 02	0.0.0.0 ~ 0.0.0.0	

set up Internet access policy

Select the policy number (1-10) in the drop-down menu.

For this policy is enabled, click the radio button next to "Enable"

Enter a name in the Policy Name field.

Click the Edit List of PCs button.

On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.

Click the Apply button to save your changes.

Click the Cancel button to cancel your unsaved changes.

Click the Close button to return to the Filters screen.

If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.

Set the days when access will be filtered. Select Everyday or the appropriate days of the week. Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.

Click the Add to Policy button to save your changes and active it.

To create or edit additional policies, repeat steps 1-9.

To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the original number.

Turn off the power of the Cellular Gateway or reboot the Cellular Gateway can cause a temporary failure. After the failure of the Cellular Gateway, if cannot automatically synchronized NTP time server, you need to recalibrate to ensure the correct implementation of the relevant period control function.

3.3.6.2 URL Filter

If you want to prevent certain client access to specific network domain name, such as www.sina.com. We can achieve it through the function of URL filter.

URL filtering function



Del	Num	URL
<input type="checkbox"/>	1	www.sina.com

Discard packets conform to the following rules: only discard the matching URL address in the list.

Accept only the data packets conform to the following rules: receive only with custom rules of network address, discarded all other URL address.

3.3 6.3 Packet Filter

To block some packets getting Internet access or block some Internet packets getting local network access, you can configure filter items to block these packets. Packet Filter



Packet filter function is realized based on IP address or port of packets.

Enable Packet Filter: Enable or disable “packet filter” function

Policy: The filter rule’s policy, you can choose the following options

Discard the Following: Discard packets conform to the following rules, Accept all other packets

Only Accept the Following-- Accept only the data packets conform to the following rules,

Discard all other packets

Add Filter Rule	
Dir	OUTPUT ▼
Interface	Main WAN ▼
Pro	TCP/UDP ▼
SPorts	1 - 65535
DPorts	1 - 65535
Source IP	0 . 0 . 0 . 0 / 0
Destination IP	0 . 0 . 0 . 0 / 0

Dir

Input : packet from WAN to LAN

Output : packet from LAN to WAN

Interface : network interface

Pro : packet protocol type

Sports : packet's source port

DPorts : packet's destination port

Source IP : packet's source IP address

Destination IP: packet's destination IP address

Note: "Source Port", "Destination Port", "Source IP", "Destination IP" could not be all empty, you have to input at least one of these four parameters.

3.3.7 NAT

3.3.7.1 Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the Cellular Gateway will forward those requests to the appropriate PC. If you want to forward a whole range of ports, see [Port Range Forwarding](#).

Basic Settings

NAT Type ☐ DNAT ☐ SNAT

Protocol

Original Address * 192.168.6.1 or 192.168.6.0/24

Original Port 1-65535 or [1-65535]

Destination Address * 192.168.6.1 or 192.168.6.0/24

Destination Port 1-65535 or [1-65535]

Mapping Address Type

Mapping Address * eg 192.168.0.1

Mapping Port 1-65535 or [1-65535]

SNAT: It is a technique that translates source IP address generally when connecting from private IP address to public IP address.

SNAT							
Protocol	Original Address	Original Port	Destination Address	Destination Port	Mapping Address	Mapping Port	Operation
all	192.168.1.1				100.103.229.4		

DNAT : It's a technique that translates destination IP address generally when connecting from public IP address to private IP address. It is generally used to redirect packets destined for specific IP address or specific port on IP address, on one host simply to a different address's, mostly on different host.

Application : Enter the name of the application in the field provided.

Protocol : Chose the right protocol TCP, UDP or Both. Set this to what the application requires.

Source Net : Forward only if sender matches this ip/net (example 192.168.1.0/24).

Port from : Enter the number of the external port (the port number seen by users on the Internet).

IP Address : Enter the IP Address of the PC running the application.

Port to : Enter the number of the internal port (the port number used by the application).

Enable : Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

DNAT						
Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation	
all	10.127.0.1	8000	192.168.1.23	5000	Mod	Del
all	10.127.0.1	10000	192.168.1.23	10000	Mod	Del
all	10.127.0.1	12000	192.168.1.23	12000	Mod	Del
all	172.168.10.11	5001	192.168.1.23	5001	Mod	Del
all	10.127.0.1	8001	192.168.1.23	8000	Mod	Del

3.3.7.2 Port Range Forward

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the Cellular Gateway will forward those requests to the appropriate PC. If you only want to forward a single port, see Port Forwarding.

Forwards

Delete	Num	Application	Start	End	Protocol	IP Address	Enable
<input type="checkbox"/>	1		0	0	Both ▼	0.0.0.0	<input type="checkbox"/>

Add

Save

Apply Settings

Cancel Changes

Application : Enter the name of the application in the field provided.

Start : Enter the number of the first port of the range you want to seen by users on the Internet and forwarded to your PC.

End : Enter the number of the last port of the range you want to seen by users on the Internet and forwarded to your PC.

Protocol : Chose the right protocol TCP, UDP or Both. Set this to what the application requires.

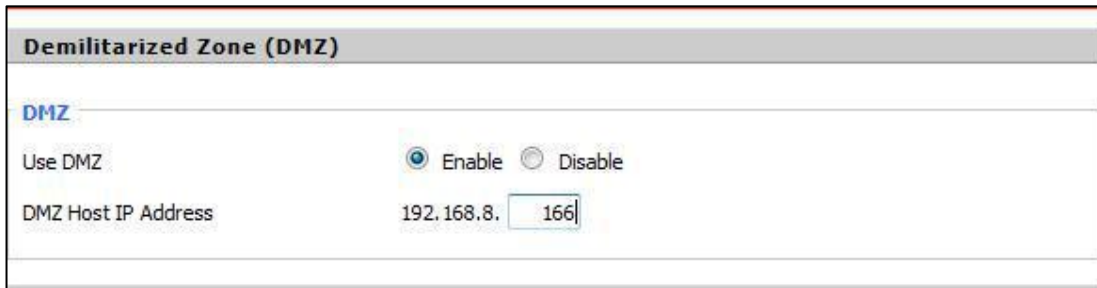
IP Address : Enter the IP Address of the PC running the application.

Enable : Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.7.3 DMZ

The DMZ (Demilitarized Zone) hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.



Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ Host IP Address: To expose one PC to the Internet, select Enable and enter the computer's IP address in the DMZ Host IP Address field. To disable the DMZ, keep the default setting : Disable

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.8 QoS Setting

3.3.8.1 Basic

Bandwidth management prioritizes the traffic on your Cellular Gateway. Interactive traffic (telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things. All of this is more or less automatic.

QoS allows control of the bandwidth allocation to different services, netmasks, MAC Addresses and the four LAN ports.

Main WAN QoS Settings

Start QoS ☐ Enable ☒ Disable

Port

Packet Scheduler

Uplink (kbps)

Downlink (kbps)

Bkup WAN QoS Settings

Start QoS ☐ Enable ☒ Disable

Port

Packet Scheduler

Uplink (kbps)

Downlink (kbps)

Uplink (kbps): In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

Downlink (kbps): In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

HTB Setting

HTB Setting

HTB Prio Setting Uplink

Priority	Band range	Band value
Premium	<input type="text" value="75 %"/> - <input type="text" value="75 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Express	<input type="text" value="15 %"/> - <input type="text" value="15 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Standard	<input type="text" value="10 %"/> - <input type="text" value="10 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Bulk	<input type="text" value="1 %"/> - <input type="text" value="1 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps

HTB Prio Setting Downlink

Priority	Band range	Band value
Premium	<input type="text" value="75 %"/> - <input type="text" value="75 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Express	<input type="text" value="15 %"/> - <input type="text" value="15 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Standard	<input type="text" value="10 %"/> - <input type="text" value="10 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps
Bulk	<input type="text" value="1 %"/> - <input type="text" value="1 %"/>	WAN : <input type="text" value="0"/> -- <input type="text" value="0"/> kbps

HTB - Hierarchical Token Bucket, it is a faster replacement for the CBQ qdisc in Linux. HTB helps in controlling the use of the outbound bandwidth on a given link. HTB allows you to use one physical link to simulate several slower links and to send different kinds of traffic on different simulated links. In both cases, you have to specify how to divide the physical link into simulated links and how to decide which simulated link to use for a given packet to be sent. In other words, HTB is useful for limiting a client's download/upload rates, thereby preventing his monopolization of the available bandwidth.

3.3.8.2 Classify Netmask Priority

Netmask Priority

Delete	IP/Mask	Priority
<input type="checkbox"/>	192.168.1.1/24	Exempt
<input type="checkbox"/>	192.168.2.3/24	Standard
<input type="checkbox"/>	192.168.3.4/32	Express
<input type="checkbox"/>	192.168.4.5/32	Bulk

... /

You may specify priority for all traffic from a given IP address or IP Range.

Mac Priority

MAC Priority

Delete	Num	MAC Address	Priority
<input type="checkbox"/>	1	00:00:00:00:00:00	Standard

:::::

You may specify priority for all traffic from a given MAC.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.9 Applications

3.3.9.1 Serial Applications

There is a console port on Cellular Gateway. Normally, this port is used to debug the Cellular Gateway. This port can also be used as a serial port. The Cellular Gateway has embedded a serial to TCP program. The data sent to the serial port is encapsulated by TCP/IP protocol stack and then is sent to the destination server. This function can work as a DTU (Data Terminal Unit).

Serial Applications

☒ Enable ☐ Disable

Baudrate: 115200

Databit: 8

Stopbit: 1

Parity: None

Flow Control: None

Protocol: TCP(DTU)

Server Address: 120.42.46.98

Server Port: 55501

Device Number: 12345678901

Device Id: 12345678

Heartbeat Interval: 60

Baudrate : The serial port's baudrate
Databit : The serial port's databit
Parity : The serial port's parity
Stopbit : The serial port's stopbit
Flow Control : The serial port's flow control type.
Enable Serial TCP Function : Enable the serial to TCP function

Protocol Type: The protocol type to transmit data.

UDP (DTU) : Data transmit with UDP protocol, work as a DTU which has application protocol and hear beat mechanism.

Pure UDP : Data transmit with standard UDP protocol.

TCP (DTU) : Data transmit with TCP protocol, work as a DTU which has application protocol and hear beat mechanism.

Pure TCP : Data transmit with standard TCP protocol; Cellular Gateway is the client.

TCP Server : Data transmit with standard TCP protocol; Cellular Gateway is the server.

TCST : Data transmit with TCP protocol, Using a custom data

Server Address: The data service center's IP Address or domain name.

Server Port : The data service center's listening port.

Device ID : The Cellular Gateway's identity ID.

Device Number : The Cellular Gateway's phone number.

Heartbeat Interval : The time interval to send heart beat packet.

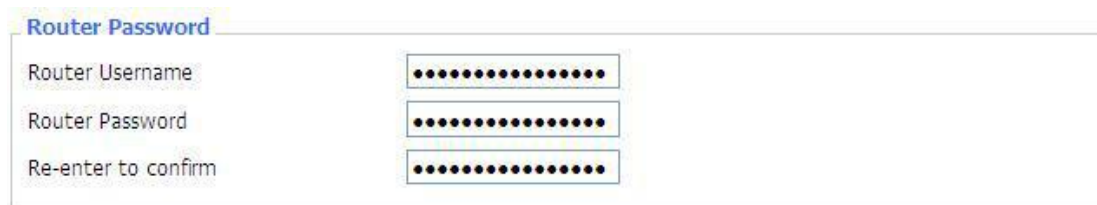
This item is valid only when you choose UDP (DTU) or TCP(DTU) protocol type

TCP Server Listen Port : This item is valid when Protocol Type is "TCP Server"
Custom Heartbeat Packet : This item is valid when Protocol Type is "TCST"
Custom Registration Packets : This item is valid when Protocol Type is "TCST"

3.3.10 Administration

3.3.10.1 Management

The Management screen allows you to change the Cellular Gateway's settings. On this page you will find most of the configurable items of the Cellular Gateway code.



The form is titled "Router Password" in blue. It contains three input fields, each with a label and a masked password field (dots). The labels are "Router Username", "Router Password", and "Re-enter to confirm".

The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

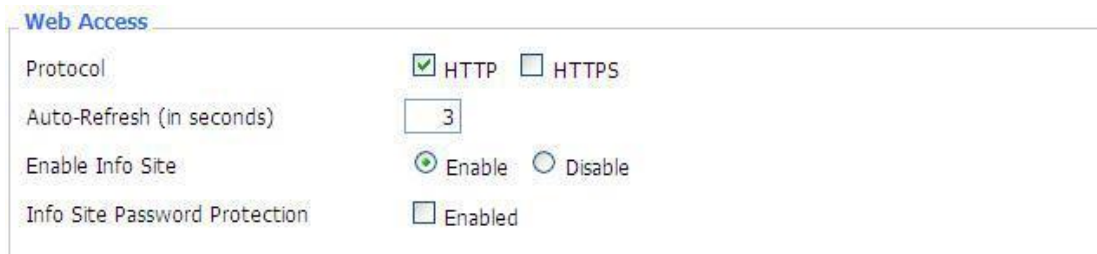
Note: Default username is root.

It is strongly recommended that you change the factory default password of the Cellular Gateway, which is admin. All users who try to access the Cellular Gateway's web-based utility or Setup Wizard will be prompted for the Cellular Gateway's password.

Web Access

This feature allows you to manage the Cellular Gateway using either HTTP protocol or the HTTPS protocol. If you choose to disable this feature, a manual reboot will be required. You can

also activate or not the Cellular Gateway information web page. It's now possible to password protect this page (same username and password than above).



The form is titled "Web Access" in blue. It contains four settings: "Protocol" with radio buttons for "HTTP" (checked) and "HTTPS"; "Auto-Refresh (in seconds)" with a text input field containing "3"; "Enable Info Site" with radio buttons for "Enable" (checked) and "Disable"; and "Info Site Password Protection" with a checkbox labeled "Enabled".

Protocol : This feature allows you to manage the Cellular Gateway using either HTTP protocol or the HTTPS protocol

Auto-Refresh : Adjusts the Web GUI automatic refresh interval. 0 disables this feature completely

Enable Info Site: Enable or disable the login system information page

Info Site Password Protection: Enable or disable the password protection feature of the system information page



Remote Access

Web GUI Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use HTTPS	<input type="checkbox"/>
Web GUI Port	<input type="text" value="8088"/> (Default: 8088, Range: 1 - 65535)
SSH Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH Remote Port	<input type="text" value="22"/> (Default: 22, Range: 1 - 65535)
Telnet Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Remote Access: This feature allows you to manage the Cellular Gateway from a remote location, via the Internet. To disable this feature, keep the default setting, Disable. To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the Cellular Gateway. You must also change the Cellular Gateway's default password to one of your own, if you haven't already.

To remotely manage the Cellular Gateway, enter `http://xxx.xxx.xxx.xxx:8080` (the x's represent the Cellular Gateway's

Internet IP address, and 8080 represents the specified port) in your web browser's address field.

You will be asked for the Cellular Gateway's password.

If you use https you need to specify the url as `https://xxx.xxx.xxx.xxx:8080` (not all firmware's does support this without rebuilding with SSL support).

SSH Management: You can also enable SSH to remotely access the Cellular Gateway by Secure Shell. Note that SSH daemon needs to be enable in Services page.

Note :

If the Remote Cellular Gateway Access feature is enabled, anyone who knows the Cellular Gateway's Internet IP address and password will be able to alter the Cellular Gateway's settings.

Telnet Management: Enable or disable remote Telnet function

Cron: The cron subsystem schedules execution of Linux commands. You'll need to use the command line or start-up scripts to actually use this.

Cron

Cron ☒ Enable ☐ Disable

Additional Cron Jobs

Language: Set up the Cellular Gateway page shows the type of language, including simplified Chinese and English.

Language Selection

Language

Device Management: Through the custom development of remote management server for the Cellular Gateway monitoring and management, parameter configuration, etc..

Device Management

Device Management ☐ Enable ☒ Disable

Remote Management Login Server: Enable or disable remote logon selection service functionality

Remote Management Login Server

Remote Management Login Server ☐ Enable ☒ Disable

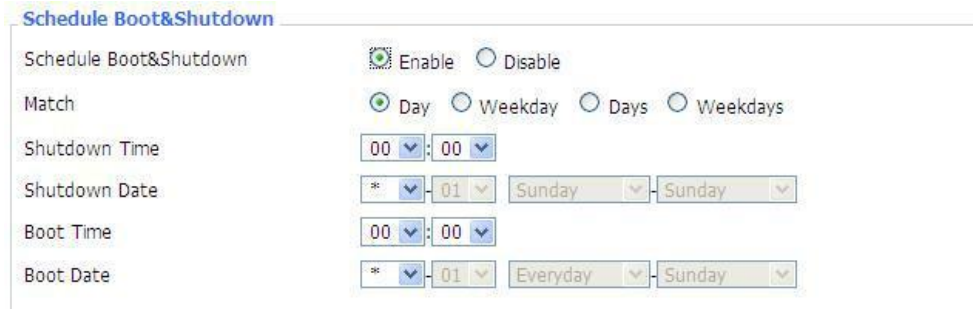
Firmware Upgrade: Enable or disable remote upgrade function

Firmware Upgrade

Firmware Upgrade ☐ Enable ☒ Disable

3.3.10.2 Keep Alive

Schedule Boot & Shutdown



Schedule Boot&Shutdown

Schedule Boot&Shutdown ☒ Enable ☐ Disable

Match ☒ Day ☐ Weekday ☐ Days ☐ Weekdays

Shutdown Time 00:00

Shutdown Date * 01 Sunday Sunday

Boot Time 00:00

Boot Date * 01 Everyday Sunday

User can set schedule boot & shutdown the Cellular Gateway

Set shutdown time, shutdown date, boot time and boot date in relevant match settings.

Schedule Reboot



Schedule Reboot

Schedule Reboot ☒ Enable ☐ Disable

Interval (in seconds) ☒ 3600

At a set Time ☐ 00:00 Sunday

You can schedule regular reboots for the Cellular Gateway:

Regularly after xxx seconds.

At a specific date time each week or every day.

Note: For date-based reboots Cron must be activated. See Management for Cron activation.

3.3.10.3 Commands

Commands: You are able to run command lines directly via the Web interface.



Command Shell

Commands

Run Commands Save Startup Save Shutdown Save Firewall Save Custom Script

Run Command : You can run command lines via the web interface. Fill the text area with your command and click Run Commands to submit.

Save Startup : You can save some command lines to be executed at startup's Cellular Gateway. Fill the text area with commands (only one command by row) and click Save Startup.

Save Shutdown : You can save some command lines to be executed at shutdown's Cellular Gateway. Fill the text area with commands (only one command by row) and click Save Shutdown.

Save Firewall : Each time the firewall is started, it can run some custom ip tables instructions. Fill the text area with firewall's instructions (only one command by row) and click Save Firewall.

Save Custom Script : Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. Fill the text area with script's instructions (only one command by row) and click Save Custom Script.

3.3.10.4 Factory Defaults



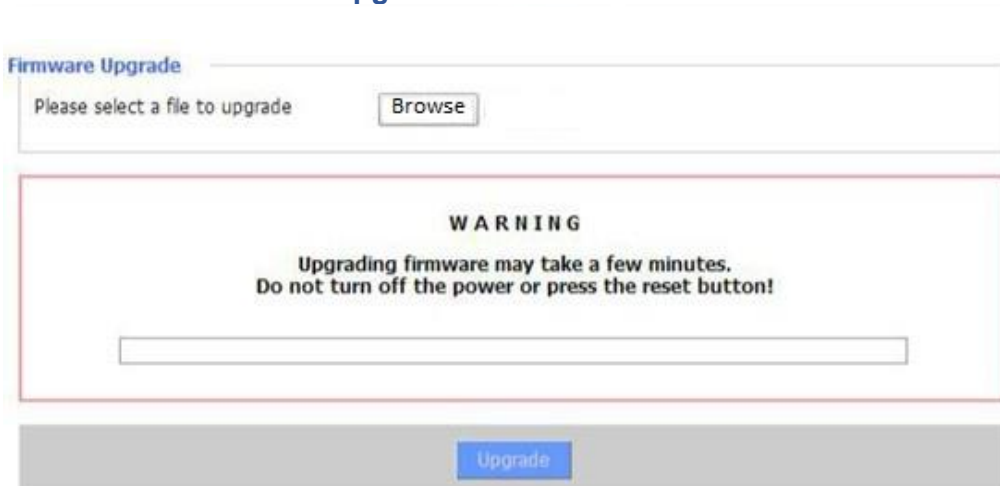
The screenshot shows a 'Factory Defaults' section with a sub-header 'Reset router settings'. Below it, there is a label 'Restore Factory Defaults' followed by two radio buttons: 'Yes' and 'No'. The 'No' radio button is selected.

Reset Cellular Gateway settings: Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

Note :

Any settings you have saved will be lost when the default settings are restored. After restoring the Cellular Gateway is accessible under the default IP address 192.168.1.1 and the default password admin.

3.3.10.5 Firmware Upgrade



The screenshot shows a 'Firmware Upgrade' section. At the top, it says 'Please select a file to upgrade' with a 'Browse' button. Below this is a large red-bordered box containing a 'WARNING' message: 'Upgrading firmware may take a few minutes. Do not turn off the power or press the reset button!'. Under the warning is a progress bar. At the bottom of the section is a blue 'Upgrade' button.

Firmware Upgrade: New firmware versions are posted can be downloaded. If the Cellular Gateway is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Note :

When you upgrade the Cellular Gateway's firmware, you lose its configuration settings, so make sure you write down the Cellular Gateway settings before you upgrade its firmware.

To upgrade the Cellular Gateway's firmware:

Download the firmware upgrade file from the website.

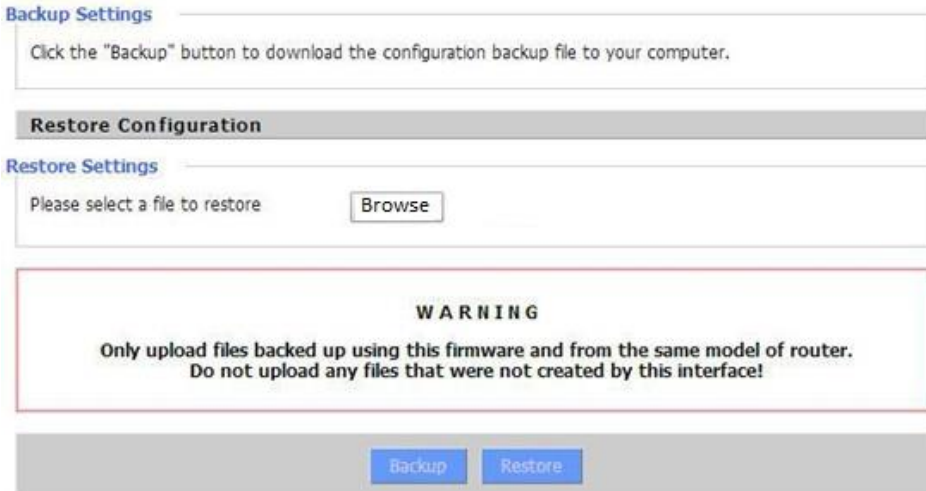
1. Click the Browse... button and chose the firmware upgrade file.
2. Click the Upgrade button and wait until the upgrade is finished.

Note:

Upgrading firmware may take a few minutes.

Do not turn off the power or press the reset button!

3.3.10.6 Backup



The screenshot shows a web interface for configuration management. At the top, under 'Backup Settings', there is a text box with the instruction: 'Click the "Backup" button to download the configuration backup file to your computer.' Below this is a 'Restore Configuration' section. Under 'Restore Settings', there is a text box saying 'Please select a file to restore' with a 'Browse' button next to it. A large red-bordered box contains a 'WARNING' message: 'Only upload files backed up using this firmware and from the same model of router. Do not upload any files that were not created by this interface!'. At the bottom, there are two buttons: 'Backup' and 'Restore'.

Backup Settings You may backup your current configuration in case you need to reset the Cellular Gateway back to its factory default settings. Click the Backup button to back up your current configuration.

Restore Settings : Click the Browse button to browse for a configuration file that is currently saved on your PC. Click the Restore button to overwrite all current configurations with the ones in the configuration file.

Note :

Only restore configurations with files backed up using the same firmware and the same model of Cellular Gateway.

3.3.11 Status

3.3.11.1 Cellular Gateway

Cellular Gateway Name: name of the Cellular Gateway, setting basic setting to modify

System

Router Name	GSF9364
Router Model	GSF9364
Firmware Version	v2.1.0 (Jun 3 2021 14:48:05) std - build 5293M
MAC Address	<u>54:D0:B4:0C:33:FA</u>
SN	FD4180303140
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Sun, 15 Aug 2021 16:25:18
Uptime	34 min

Cellular Gateway Model : model of the Cellular Gateway, unavailable to modify

Firmware Version : software version information

MAC Address : MAC address of WAN, setting Clone MAC Address to modify

Host Name : host name of the Cellular Gateway, setting basic setting to modify

WAN Domain Name : domain name of WAN, setting basic setting to modify

LAN Domain Name : domain name of LAN, unavailable to modify

Current Time : local time of the system

Uptime : operating uptime as long as the system is powered on

Memory

Total Available	28880 kB / 32768 kB	88%
Free	12436 kB / 28880 kB	43%
Used	16444 kB / 28880 kB	57%
Buffers	1660 kB / 16444 kB	10%
Cached	5708 kB / 16444 kB	35%
Active	963 kB / 16444 kB	6%
Inactive	1118 kB / 16444 kB	7%

Total Available : the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free : free memory, the Cellular Gateway will reboot if the memory is less than 500kB

Used : used memory, total available memory minus free memory

Buffers : used memory for buffers,

Cached : the memory used by high-speed cache memory

Active : active use of buffer or cache memory page file size

Inactive: not often used in a buffer or cache memory page file size

Serial Applications

Status	Disabled
--------	----------

Serial Applications: Status of serial

Network

IP Filter Maximum Ports	4096
Active IP Connections	43 <div style="width: 1%;"></div> 1%

IP Filter Maximum Ports: preset is 4096, available to re-management

Active IP Connections: real time monitor active IP connections of the system, click to see the table as blow:

Active IP Connections 53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED
31	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT

Active IP Connections : total active IP connections

Protocol : connection protocol

Timeouts : connection timeouts, unit is second

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Source Address : source IP address
Remote Address : remote IP address
Service Name : connecting service port
Status : displayed status

3.3.11.2 WAN

Connection Type Automatic Configuration - DHCP
Connection Uptime Not available

Connection Type: disabled, static IP, automatic configuration-DHCP, 3G Link 1, 3G Link 2
Connection Uptime: connecting uptime; If disconnect, display Not available

IP Address 0.0.0.0
Subnet Mask 0.0.0.0
Gateway 0.0.0.0
DNS 1
DNS 2
DNS 3

IP Address: IP address of Cellular Gateway WAN
Subnet Mask: subnet mask of Cellular Gateway WAN
Gateway: the gateway of Cellular Gateway WAN
DNS1, DNS2, DNS3: DNS1/DNS2/DNS3 of Cellular Gateway WAN

Remaining Lease Time 0 days 23:38:43
DHCP Release DHCP Renew


Remaining Lease Time: remaining lease time of IP address in DHCP way
DHCP Release: release DHCP address
DHCP Renew: renew IP address in DHCP way, default is 1 day

Login Status Disconnected Connect

Login Status: connection status of WAN
Disconnection: disconnect
Connection: connect

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Module Type ANYDATA-EVDO MODULE

Signal Status -51 dBm
Network CDMA/HDR

Module Type: module type in 3G/UMTS way
Signal Status: signal intensity of the module in 3G/UMTS way
Network: network type of the module in 3G/UMTS way



Total Flow: flow from power-off last time until now statistics, download and upload direction
Monthly Flow: the flow of a month, unit is MB
Last Month: the flow of last month
Next Month: the flow of next month

Data Administration

[Backup](#) [Restore](#) [Delete](#)

Backup: backup data administration

Restore: restore data administration

Delete: delete data administration

3.3.11.3 BKUP WAN

Connection Type: disabled, static IP, automatic configuration-DHCP, 3G Link 1, 3G Link 2

Connection Uptime: connecting uptime; If disconnect, display Not available

Connection Type	Automatic Configuration - DHCP
Connection Uptime	Not available

IP Address : IP address of Cellular Gateway WAN

Subnet Mask : subnet mask of Cellular Gateway WAN

Gateway : the gateway of Cellular Gateway WAN

DNS1, DNS2, DNS3 : DNS1/DNS2/DNS3 of Cellular Gateway WAN

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

Remaining Lease Time: remaining lease time of IP address in DHCP way

DHCP Release: release DHCP address

DHCP Renew: renew IP address in DHCP way, default is 1 day

Remaining Lease Time	0 days 23:38:43
----------------------	-----------------

[DHCP Release](#) [DHCP Renew](#)

Login Status: connection status of WAN

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Disconnection: disconnect

Connection: connect

Login Status

Disconnected

Connect

Module Type: module type in 3G/UMTS way

Signal Status: signal intensity of the module in 3G/UMTS way

Network: network type of the module in 3G/UMTS way

Module Type

ANYDATA-EVDO MODULE



Signal Status

-51 dBm

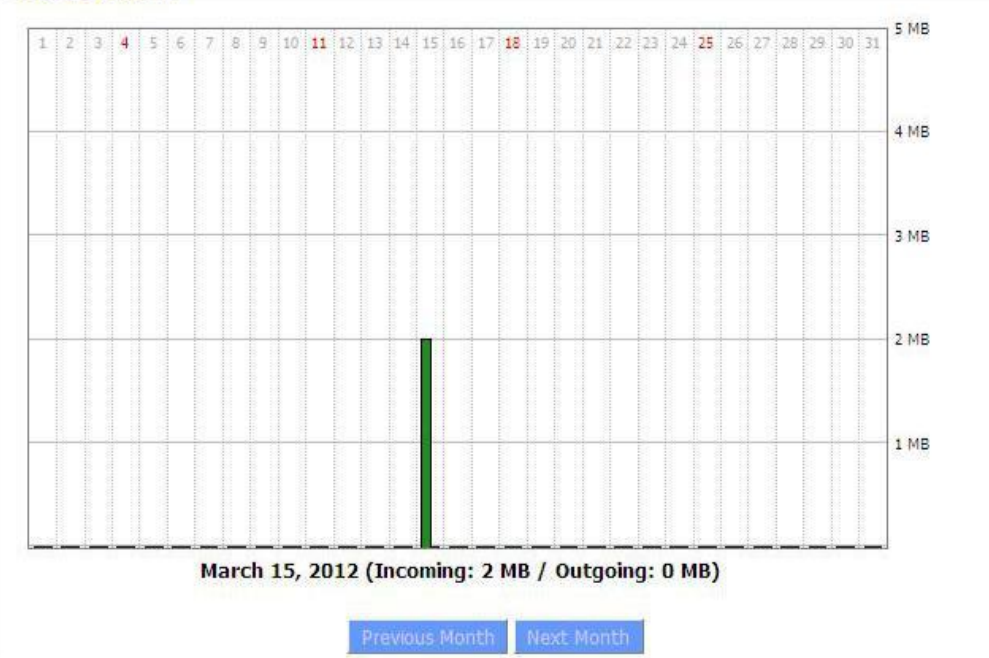
Network

CDMA/HDR

Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month



Total Flow : flow from power-off last time until now statistics, download and upload direction

Monthly Flow : the flow of a month, unit is MB

Last Month : the flow of last month

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



Next Month : the flow of next month
Backup: backup data administration
Restore: restore data administration
Delete: delete data administration

Data Administration

Backup Restore Delete

3.3.11.4 LAN

LAN Status

MAC Address	00:0C:43:30:52:77
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

MAC Address: MAC Address of the LAN port Ethernet

IP Address : IP Address of the LAN port

Subnet Mask : Subnet Mask of the LAN port

Gateway : Gateway of the LAN port

Local DNS : DNS of the LAN port

Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.1.120	10:78:D2:98:C9:46	57	1%

Host Name : host name of LAN client

IP Address : IP address of the client

MAC Address: MAC address of the client

Conn. Count : connection count caused by the client

Ratio : the ratio of 4096 connection




Dynamic Host Configuration Protocol

DHCP Status

DHCP Server	Enabled
DHCP Daemon	uDHCPd
Start IP Address	192.168.1.100
End IP Address	192.168.1.149
Client Lease Time	1440 minutes

DHCP Server : enable or disable the Cellular Gateway work as a DHCP server
DHCP Daemon: the agreement allocated using DHCP including DNSMasq and uDHCPd
Starting IP Address : the starting IP Address of the DHCP server's Address pool
Ending IP Address : the ending IP Address of the DHCP server's Address pool
Client Lease Time : the lease time of DHCP client

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC-201011161332	192.168.1.142	00:21:5C:33:4D:29	1 day 00:00:00	
jack-lincw	192.168.1.117	44:37:E6:3F:45:54	1 day 00:00:00	
*	192.168.1.149	00:0C:E7:00:00:00	1 day 00:00:00	

Host Name : host name of LAN client
IP Address : IP address of the client
MAC Address : MAC address of the client
Expires : the expiry the client rents the IP address

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

Interface : the interface assigned by dial-up system
User Name : user name of PPPoE client
Local IP : IP address assigned by PPPoE client
Delete : click to delete PPPoE client

Connected L2TP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: the interface assigned by dial-up system
Local IP: tunnel IP address of local L2TP
Remote IP: tunnel IP address of L2TP server
Delete: click to disconnect L2TP

Connected L2TP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.50.2	120.42.46.98	

Interface: the interface assigned by dial-up system

San Telequip (P) Ltd.,
 504 & 505 Deron Heights, Baner Road
 Pune 411045, India
 Phone : +91-20-27293455, 9764027070, 8390069393
 email : info@santelequip.com



User Name: user name of the client
Local IP: tunnel IP address of L2TP client
Remote IP: IP address of L2TP client
Delete: click to delete L2TP client

Interface: the interface assigned by dial-up system

Connected PPTP Server			
Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Local IP: tunnel IP address of local PPTP
Remote IP: tunnel IP address of PPTP server
Delete: click to disconnect PPTP

Connected PPTP Clients				
Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.5.1	120.42.46.98	

Interface : the interface assigned by dial-up system
User Name : user name of the client
Local IP : tunnel IP address of PPTP client
Remote IP : IP address of PPTP client
Delete : click to delete PPTP client

3.3.11.5 Wireless

Wireless Status	
MAC Address	00:0C:43:30:52:79
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	San Telequip
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s
Encryption - Interface wl0	Disabled
PPTP Status	Disconnected

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



MAC Address : MAC address of wireless client
Radio : display whether radio is on or not
Mode : wireless mode
Network : wireless network mode
SSID : wireless network name
Channel : wireless network channel
TX Power : reflection power of wireless network
Rate : reflection rate of wireless network
Encryption-Interface w10 : enable or disable Encryption-Interface w10
PPTP Status : show wireless pptp status

Wireless Packet Info

Received (RX)	91125 OK, no error	100%
Transmitted (TX)	11957 OK, no error	100%

Received (RX) : received data packet
Transmitted (TX) : transmitted data packet

Wireless Nodes

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address : MAC address of wireless client
Interface : interface of wireless client
Uptime : connecting uptime of wireless client
TX Rate : transmit rate of wireless client
RX Rate : receive rate of wireless client
Signal : the signal of wireless client
Noise : the noise of wireless client
SNR : the signal to noise ratio of wireless client
Signal Quality : signal quality of wireless client

San Telequip (P) Ltd.,
 504 & 505 Deron Heights, Baner Road
 Pune 411045, India
 Phone : +91-20-27293455, 9764027070, 8390069393
 email : info@santelequip.com



Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Rssi	Noise	beacon	Open	dtim	Rate	Join Site
tzt-3g	Unknown	00:aa:bb:cc:dd:14	2	-5	-95	0	No	0	54(b/g)	Join
four-faith	Unknown	00:0c:43:30:52:79	6	-24	-95	0	No	0	300(b/g/n)	Join
ff-old	AP	00:13:10:09:56:92	6	-55	-95	0	No	0	54(b/g)	Join

[Refresh](#)[Close](#)

Neighbor's Wireless Network: display other networks nearby

SSID : the name of wireless network nearby

Mode : operating mode of wireless network nearby

MAC Address: MAC address of the wireless nearby

Channel : the channel of the wireless nearby

Rssi : signal intensity of the wireless nearby

Noise : the noise of the wireless nearby

Beacon : signal beacon of the wireless nearby

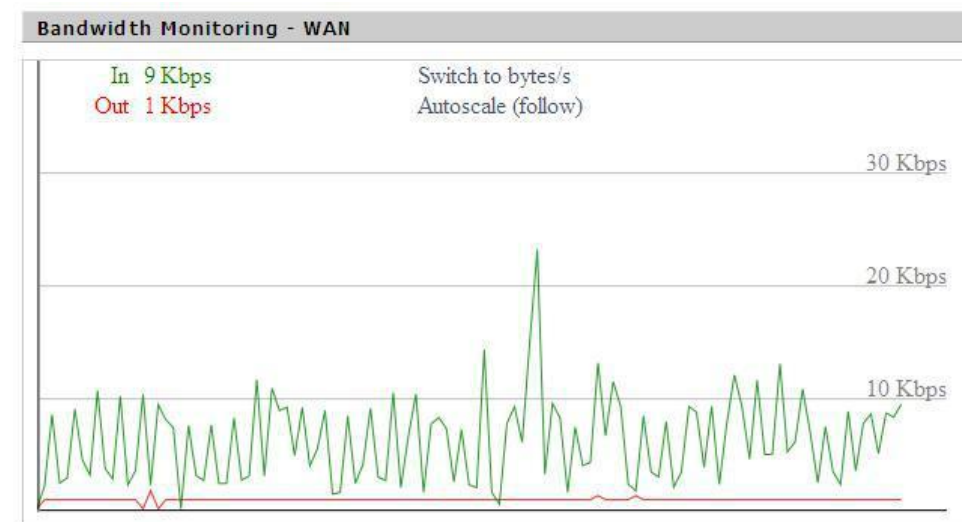
Open : the wireless nearby is open or not

Dtim : delivery traffic indication message of the wireless nearby

Rate : speed rate of the wireless nearby

Join Site : click to join wireless network nearby

3.3.11.6 Bandwidth





Bandwidth Monitoring-LAN Graph

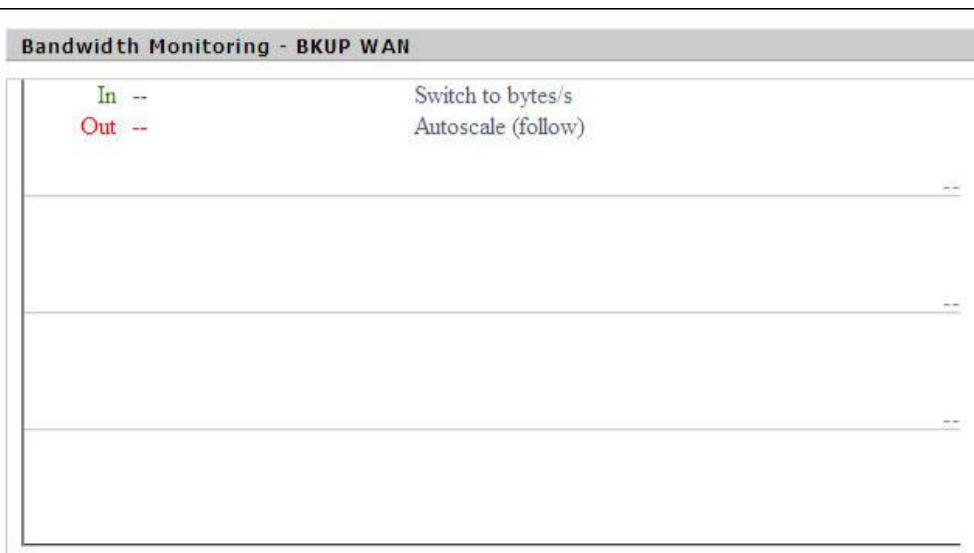
abscissa axis: time

vertical axis: speed rate

Bandwidth Monitoring-WAN Graph

abscissa axis: time

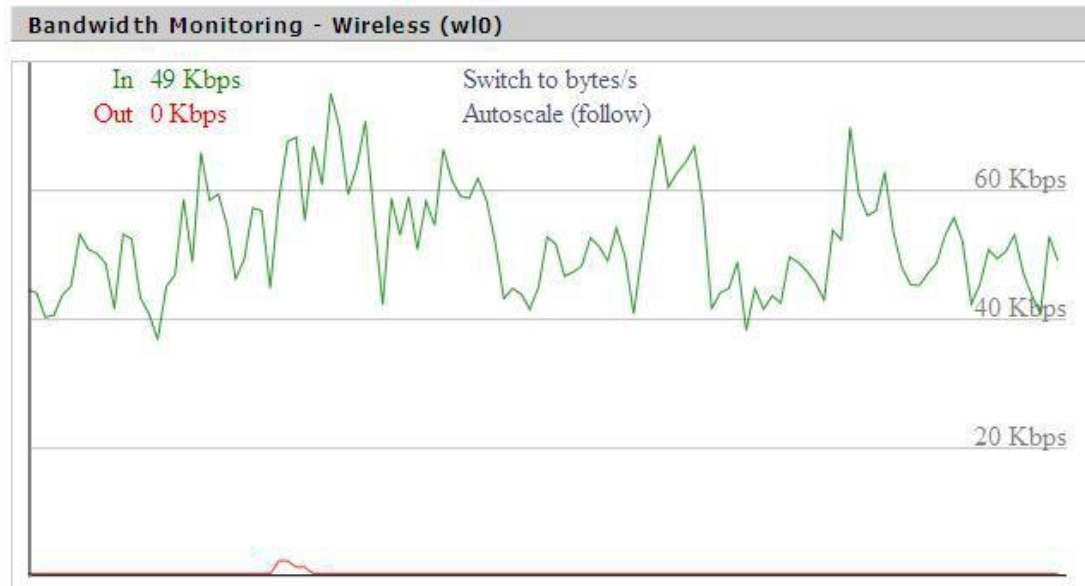
vertical axis: speed rate



Bandwidth Monitoring-BKUP WAN Graph

abscissa axis: time

vertical axis: speed rate



Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

3.3.11.7 Sys-Info

Router	
Router Name	Router
Router Model	Router
LAN MAC	<u>00:0C:43:30:52:77</u>
WAN MAC	<u>00:0C:43:30:52:78</u>
Wireless MAC	<u>00:0C:43:30:52:79</u>
WAN IP	27.149.86.163
BKUP WAN IP	0.0.0.0
LAN IP	192.168.1.1

Cellular Gateway Name : the name of the Cellular Gateway

Cellular Gateway Model : the model of the Cellular Gateway

LAN MAC : MAC address of LAN port

WAN MAC : MAC address of WAN port

Wireless MAC : MAC address of the wireless

WAN IP : IP address of Main WAN port
BKUP WAN IP : IP address of bkup WAN port
LAN IP : IP address of LAN port

Wireless	
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	four-faith
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s

Radio : display whether radio is on or not
Mode : wireless mode
Network : wireless network mode
SSID : wireless network name
Channel : wireless network channel
TX Power : reflection power of wireless network
Rate : reflection rate of wireless network

Wireless Packet Info	
Received (RX)	6982 OK, no error
Transmitted (TX)	1498 OK, no error

Received (RX): received data packet
Transmitted (TX): transmitted data packet

Wireless							
Clients							
MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR
- None -							

MAC Address: MAC address of wireless client
Interface : interface of wireless client
Uptime : connecting uptime of wireless client

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



TX Rate : transmit rate of wireless client
RX Rate : receive rate of wireless client
Signal : the signal of wireless client
Noise : the noise of wireless client
SNR : the signal to noise ratio of wireless client
Signal Quality: signal quality of wireless client

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Disabled

DHCP Server : enabled or disabled
ff-radauth : enabled or disabled
USB Support : enabled or disabled

Memory

Total Available	28.2 MB / 32.0 MB
Free	11.2 MB / 28.2 MB
Used	17.0 MB / 28.2 MB
Buffers	1.8 MB / 17.0 MB
Cached	6.3 MB / 17.0 MB
Active	1.5 MB / 17.0 MB
Inactive	0.8 MB / 17.0 MB

Total Available : the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)
Free : free memory, the Cellular Gateway will reboot if the memory is less than 500kB
Used : used memory, total available memory minus free memory
Buffers : used memory for buffers, total available memory minus allocated memory
Cached : the memory used by high-speed cache memory
Active : Active use of buffer or cache memory page file size
Inactive : Not often used in a buffer or cache memory page file size

San Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 9764027070, 8390069393
email : info@santelequip.com



DHCP			
DHCP Clients			
Host Name	IP Address	MAC Address	Expires
*	192.168.1.143	xx:xx:xx:xx:DD:45	1 day 00:00:00
four-488e1df5fa	192.168.1.125	xx:xx:xx:xx:D8:F7	1 day 00:00:00
Mycenae-PC	192.168.1.116	xx:xx:xx:xx:5E:30	1 day 00:00:00

Host Name: host name of LAN client

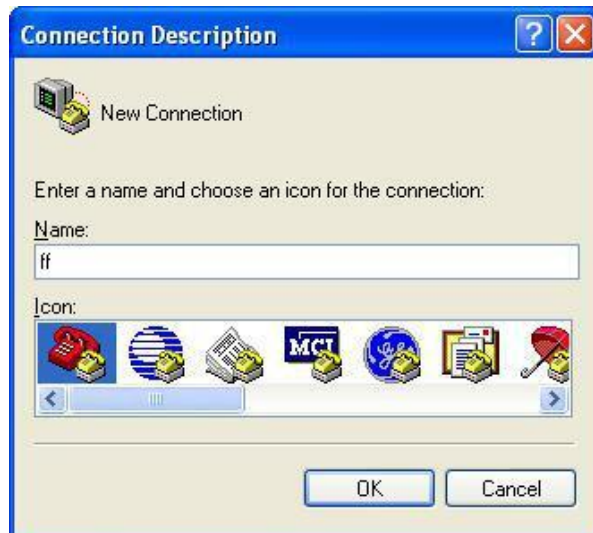
IP Address: IP address of the client

MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

Chapter 4 Appendix

The following steps describe how to setup Windows XP Hyper Terminal.
Press "Start", "Programs", "Accessories", "Communications", "Hyper Terminal"

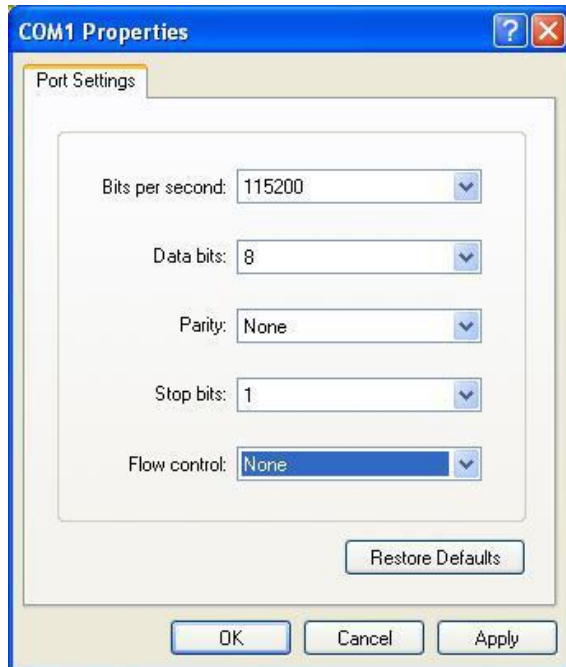


Input connection name, choose "OK"



Choose the correct COM port which connects to modem, choose "OK"

Configure the Serial port parameters as following, choose "OK"



Bits per second: 115200
Data bits : 8
Parity : None
Stop bits : 1
Flow control : None