

MobileBridge Gateway Series

MB9000

Wireless Cellular Data Gateway

User Guide

Version 1.03

(Firmware v2.0.4-6)

2007-06-05

Top Global USA, any modification of this product will not issue a separate notice.

All Rights Reserved.

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

Top Global declares that MB9000 (FCC ID: SUMMB9000) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A.

CONTENT

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT	2
1 INTRODUCTION	5
2 INSTALLING THE MB9000.....	6
2.1 VERIFY KIT CONTENTS.....	6
2.2 WRITE DOWN THE PRODUCT’S IDENTIFICATION	7
2.3 POWER UP THE MB9000	7
2.4 LED INDICATORS.....	8
2.5 CONNECT TO THE MB9000 UNIT.....	8
3 MANAGEMENT.....	11
3.1 OVERVIEW	11
3.2 PAGE STRUCTURE.....	13
3.2.1 <i>Shortcut</i>	13
3.3 PAGE OPERATION.....	15
3.4 CONFIGURATION PAGES DESCRIPTION.....	15
3.4.1 <i>Devices</i>	15
3.4.2 <i>Setup</i>	19
3.4.3 <i>Advanced</i>	31
3.4.4 <i>Firewall</i>	36
3.4.5 <i>VPN</i>	44
3.4.6 <i>Management</i>	48
3.4.7 <i>Diagnostics</i>	55
4 TROUBLESHOOTING	58
4.1 OVERVIEW	58
4.2 INTRODUCTION.....	58
5 DEFAULT MB9000 SETTINGS	66

FOREWORD

This section describes the objectives, audience and conventions of the Top Global MB9000 User Guide.

Objectives

This document explains the steps for initial setup and basic configuration of the MB9000. This document also provides troubleshooting information and detailed specifications.

Audience

This document is for the person installing and configuring the MB9000 for the first time. The installer should be familiar with network structures, terms and concepts.

Conventions

This document uses the following conventions to convey instructions and information:

- Tools and keywords are in boldface type.



Note

Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.



Warning

The warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Obtaining Documentation

The following sections explain how to obtain documentation from Top Global.

World Wide Web

You can access the latest Top Global documentation on the World Wide Web at the following URL: <http://www.topglobalusa.com/support1.asp>

Special comment

This device is a general Wireless router, and it can act as a WWAN router only after inserting the WWAN pc card.

1 Introduction

The MB9000 is a new 3G/4G mobile router in Top Global's MobileBridge™ family. It has two PCMCIA slots, both of them can support 3G/4G cellular cards. The MB9000 delivers Internet connectivity to PDA, Laptop/Desktop PC, and other network devices through LAN or WLAN over 3G/4G networks.

MB9000's dual-slot design of WWAN can provide excellent solutions with load balance and auto-failover features. Auto-failover feature can keep wireless network connection without interruption when one of cellular link is disconnected. Load balance feature can help users to optimize bandwidth allocation.

Flexible, easy, and on-demand Internet access using high-speed 3G/4G cellular networks (no additional requirements for software, drivers, or interfaces) make the MB9000 router an ideal solution for mission critical mobile enterprise applications.

MB9000 bridges 802.11b/g wireless networks and wired networks for LAN users, allowing them to communicate with each other. MB9000 also combines the VAP (Virtual Access Point) technology to provide multiple SSIDs for user-based authentication to offer additional security in local side.

Using the instructions in this guide to help you connect MB9000, set it up, and configure it to work.

2 Installing the MB9000

Installing the MB9000 is easy. Follow the quick steps below to power up your wireless network:

- Verify kit content
- Write down product SN and MAC
- Power up the MB9000
- LED Indicators
- Initialize the MB9000 unit

2.1 Verify Kit Contents

MB9000 kit includes the following components, similar to those depicted in Figure 2-1.

Figure2-1 MB9000 Kit Contents



1. MB9000 router (Top View)
2. Power supply
3. Ethernet cable (crossover)
4. CD
5. QIG (Quick Installation Guide)

2.2 Write Down the Product's Identification

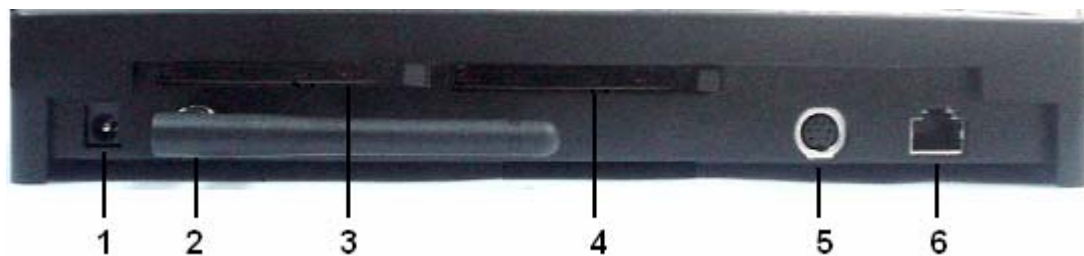
Before MB9000 installation, please write down following information on the MB9000 label:

- Serial Number
- MAC address

2.3 Power up the MB9000

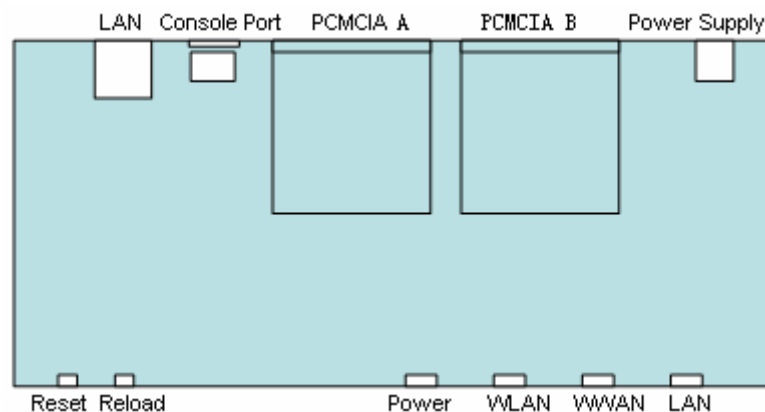
Connect the MB9000 power supply (refer to Figure 2-2).

Figure2-2 Ports description



1. Power Jack
2. WLAN Antenna
3. PC Card Slot B
4. PC Card Slot A
5. Console Port (RS232)
6. Ethernet WAN Interface (RJ45)

Figure 2-1 Top View



The MB9000 power supply accepts any input AC voltage in the range of 100-240 VAC.

2.4 LED Indicators

The following table shows the status when the MB9000 is configured successfully and running properly.

Table 2-1 Normal LED Indications

	Power	WLAN	WWAN	Ethernet LAN
Off	Power off	Disabled	Card inserted; No Internet connection	No cable
Green	Power on and normal	Enabled	Card inserted; Internet connected	100Mbps mode
Green Blink	N/A	Enabled and data transmission	Card inserted, and data transmission	100Mbps mode, and data transmission
Red	N/A	N/A	No card	10Mbps mode
Red Blink	N/A	N/A	N/A	10Mbps mode, and data transmission
Amber	System error or firmware lost	N/A	N/A	N/A
Amber Blink	System booting	N/A	Internet connecting	N/A

N/A: Not Available

2.5 Connect to the MB9000 Unit

1. There are two ways to connect your PC/laptop to MB9000:

a. Using Ethernet LAN

- 1) Verify the TCP/IP configuration of PC/laptop is set to be "Obtain IP address Automatically";
- 2) Connect your PC/laptop to LAN port of MB9000.

b. Using wireless LAN

- 1) Write down the MB9000 SN from the back label. It is the WLAN default SSID name: topglobal_SN_0;
- 2) Verify the WLAN of PC/laptop is ready to use;
- 3) Scan WLAN network, and connect to the network with the same name as MB9000's SN which you recorded in the step 1).

2. Validate that your computer has got IP address from the MB9000, then open the web browser and enter <http://172.16.0.1>. Press Enter then the MB9000 login screen appears (Figure 2-4 login window). Enter the username/password (default is public/public), and click OK, the home web page appears (Figure 2-5 home page).

Figure2-4 login window

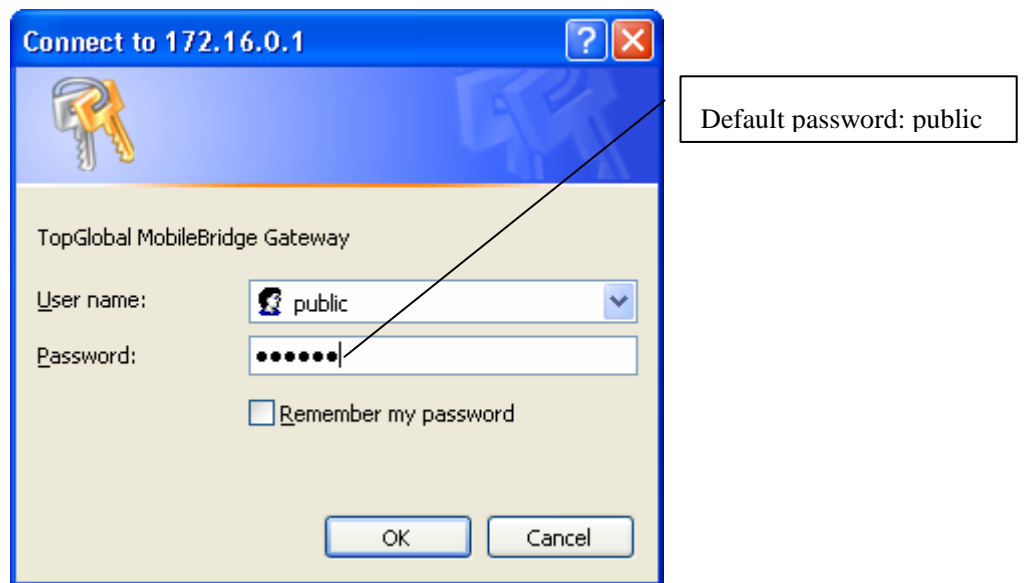




Figure2-5 home page

TOPglobal
Broadening Wireless Horizons

webGUI Configuration Wed May 23 20:48:25 2007 [【Home】](#) [【Reboot】](#)

TOPglobal
Broadening Wireless Horizons

Basic information

Product Model	MB9000-Standard
SN	MF16SG370776
Firmware Version	v2.0.4-6 Built on May 23 2007 16:43:47
Uptime	5 minutes, 6 seconds
CPU usage	 2%
Memory usage	 61% [8445952B/14069760B]

MobileBridge is © 2004-2006 by TOPGlobal. All rights reserved.

You can start your own configuration from here.

3 Management

3.1 Overview

MB9000 embeds a web server for web-based management. This section will show you how to visit MB9000's web pages.

1. Open your browser and enter the MB9000's IP address in the address bar.
2. Press the **ENTER** key. The MB9000 **Login** dialog box appears.

Figure 3-1 **Login Dialog Box**



Note:

Default user name: public

Default password: public

3. After you input the right username and password, the home page of MB9000 web site will appear (Figure 3-2).

Figure 3-2 MB9000's home page



Basic information	
Product Model	MB9000-Standard
SN	MF165G370776
Firmware Version	v2.0.4-6 Built on May 23 2007 16:43:47
Uptime	5 minutes, 6 seconds
CPU usage	 2%
Memory usage	 61% [8445952B/14069760B]

There are **seven** main categories on MB9000's web site:

- Devices;
- Setup;
- Advanced;
- Firewall;
- VPN;
- Management;
- Diagnostics.

The following sections will explain each of them in detail.

3.2 Page Structure

Figure 3-3 MB9000's home page

The screenshot shows the webGUI Configuration page for the MB9000. The header includes the TOP Global logo, the title 'webGUI Configuration', and the system time 'Wed May 23 20:48:25 2007' along with 'Home' and 'Reboot' buttons. The left sidebar contains a menu with categories: Devices (Basic, Status, Log), Setup (LAN, WAN), Advanced (Dynamic DNS, Qos, Route), Firewall (General, MAC Filter, IP Filter, WEB Filter, Port Forwarding), VPN (IPsec, PPTP Client), Management (System Administration, Time, Certificate, Firmware, Backup/Restore, Factory defaults), and Diagnostics. The main content area features the TOP Global logo and a 'Basic information' table:

Basic information	
Product Model	MB9000-Standard
SN	MF165G370776
Firmware Version	v2.0.4-6 Built on May 23 2007 16:43:47
Uptime	5 minutes, 6 seconds
CPU usage	<input type="text" value="2%"/>
Memory usage	<input type="text" value="61% [8445952B/14069760B]"/>

At the bottom of the page, it states: 'MobileBridge is © 2004-2006 by TOPGlobal. All rights reserved.'

The whole page consists of 3 main spaces:

- Upper title and shortcut space: display the most common used function page shortcuts. For example, the system time, the shortcut to the home page of the unit and reboot page.
- Left menu space: display main 7 categories of the function menu for MB9000.
- Right working space: display the detailed configuration pages for the function menu.

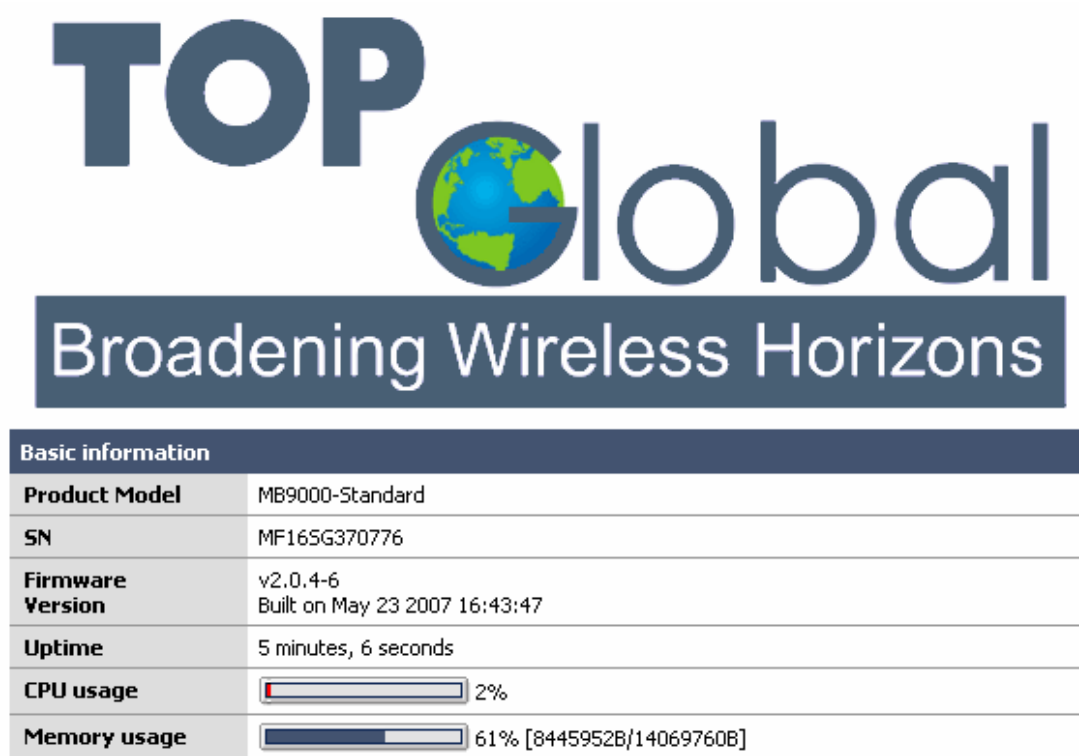
3.2.1 Shortcut

There are two main categories in this setting:

- Home
- Reboot

3.2.1.1 Home

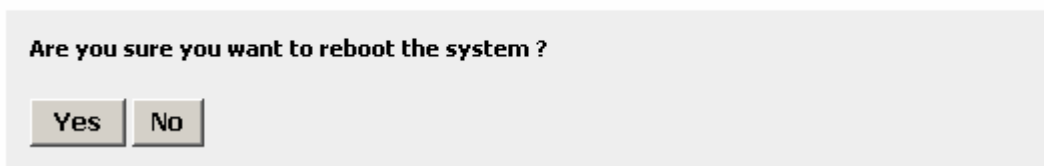
Figure 3-4 MB9000's home page



3.2.1.2 Reboot

Figure 3-5 Reboot system

Reboot system



Reboot operation will write all of the configuration changes (if any) to the flash before reboot the unit. Click “**Yes**”, the device will be rebooted. During the reboot process, the power LED will blink with amber color.



Note:

If you made any changes on this router, please DO remember to reboot it from the reboot page. If not, all the changes you made might be lost. You can

make a batch changes on the different pages before reboot the router to take the changes effect.

Figure 3-6 **Restarting page**



3.3 Page Operation

- ✓ All of the MB9000 functions can be configured and become effective by going through the following 3 steps: set up the parameters → submit → reboot;
- ✓ Once the parameters are submitted, the system will confirm the page content, and then notify the user to reboot the MB9000 to take effect.

3.4 Configuration Pages Description

3.4.1 Devices

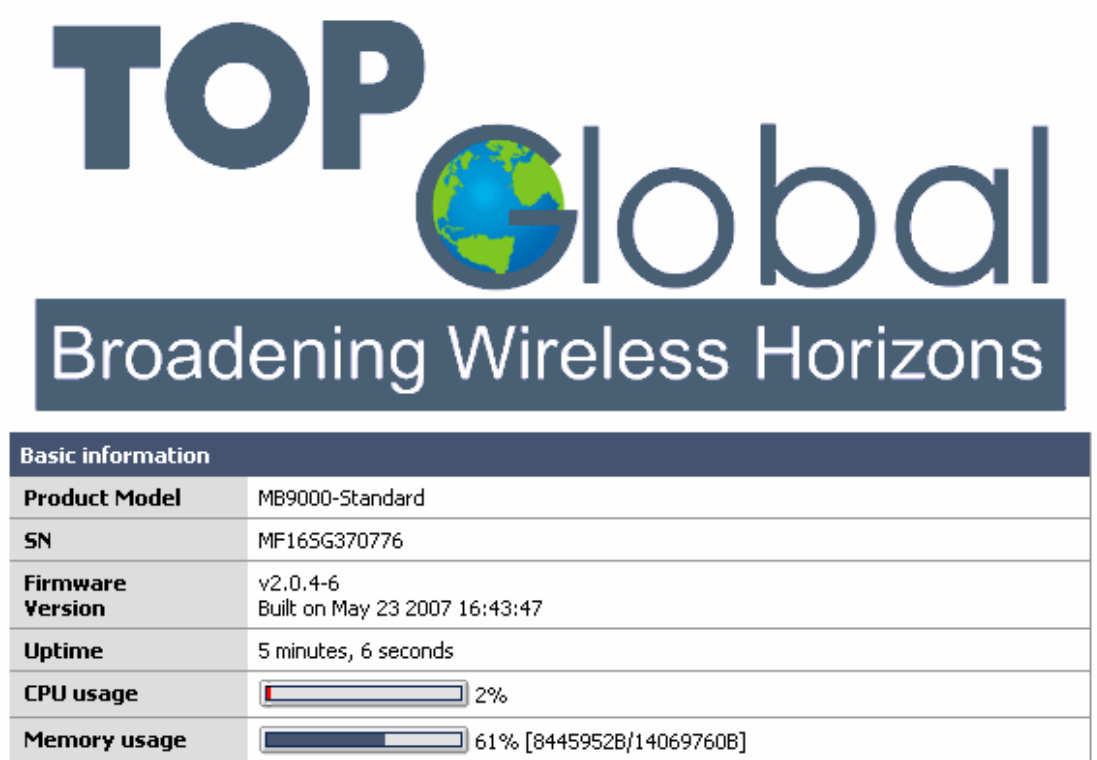
There are three main categories in this setting:

- Basic
- Status

- Log

3.4.1.1 Basic

Figure 3-7 *Basic page*



The Basic page is same to the home page. You can see some main information about the MB9000 device on this page, these including the model name, serial number (SN) of the unit, the current firmware version of the unit, the uptime since power up or the last reboot, the CPU usage, and the memory usage. Once you encounter trouble using this router and ask for help to our technical support, you need to provide the firmware version as well as the serial number.

3.4.1.2 Status

The **Interface** page shows the interfaces that provided by the MB9000. MB9000 names the wireless WAN slot A interface as “Interface 0”, and wireless WAN slot B interface as “Interface 1”. Figure 3-8 shows this page as an example.

Figure 3-8 **Interface page**

WAN interface#0 Wireless WAN	
Status	Up
UP Time	11 minutes, 41 seconds
IP Address	220.192.250.48
Network Mask	255.255.255.255
In/out packets	51/93(20.1KB/6.1KB)

WAN interface#1 Wireless WAN	
Status	Up
UP Time	11 minutes, 32 seconds
IP Address	220.207.74.18
Network Mask	255.255.255.255
In/out packets	69/94(22.8KB/6.5KB)

LAN interface	
Status	Link
MAC address	00:01:24:D0:9A:B6
IP address	172.16.0.1
Subnet mask	255.255.255.0
In/out packets	414/194(37.3KB/121.7KB)
In/out errors	0/0
Collisions	0

This page shows the interface type, the status, the IP address, the subnet mask, and the statistic of the incoming/outgoing packets through this interface.

3.4.1.3 Log

The **Log** page shows the system log message on the WEB page. There are 2 tabs on this page: *System* and *Settings*.

Figure 3-9 System log message

Last 50 system log entries		
1 00:00:41 (none)	dnsmasq[61]:	using nameserver 220.192.0.130#53
1 00:00:41 (none)	pluto[102]:	listening for IKE messages
1 00:00:41 (none)	pluto[102]:	adding interface ipsec0/ppp0 220.192.250.48:500
1 00:00:41 (none)	pluto[102]:	adding interface ipsec0/ppp0 220.192.250.48:4500

The System Log displays a list of the most recent activities that have taken place on MB9000. (These log messages are useful for us to check the issues response from customers. Please send with these messages to our supporters when you are looking for help from them.) The **System** tab shows the latest 50 system log messages.

Figure 3-10 Log settings

Syslog	
<input type="checkbox"/> Show log entries in reverse order (newest entries on top)	
Number of log entries to show: <input type="text" value="50"/>	
<input type="checkbox"/> Enable syslog'ing to remote syslog server	
Remote syslog server	<input type="text"/>
IP address of remote syslog server	
<input type="button" value="Submit"/>	
<p>Note: Syslog sends UDP datagrams to port 514 on the specified remote syslog server. Be sure to set syslogd on the remote server to accept syslog messages from MobileBridge.</p>	

By default, the syslog message will display on the WEB page. When the box of “**Enable syslog'ing to remote syslog server**” is checked, the system logs will be sent to the specified remote syslog server.

3.4.2 Setup

The setup configuration covers LAN configuration and WAN configuration:

- LAN
- WAN

3.4.2.1 LAN

Click the **LAN** link on the left part of the page to enter the LAN configuration page, where you can configure the related information of one Ethernet interface and four WLAN interfaces of the MB9000.

Figure 3-11 *Global page*

Global
Wi-Fi

	LANGroup#0	LANGroup#1	LANGroup#2	LANGroup#3
Ethernet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WLAN0	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WLAN1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WLAN2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WLAN3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

3.4.2.1.1 LAN Group configuration

Figure 3-12 LAN group

LanGroup		DHCP Binding	DHCP Lease
Networking			
IP address	<input type="text" value="172.16.0.1"/>	(e.g. 172.16.0.1)	
Netmask	<input type="text" value="255.255.255.0"/>	(e.g. 255.255.255.0)	
<input checked="" type="checkbox"/> Enable DHCP service			
<input type="checkbox"/> Deny unknown clients If this is checked, only the clients defined below will get DHCP leases from this server.			
Available range	172.16.0.0 - 172.16.0.255		
Range	<input type="text" value="172.16.0.2"/>	to	<input type="text" value="172.16.0.100"/>
Lease time	<input type="text" value="86400"/>	seconds This is used for clients that do not ask for a specific expiration time. The default is 86400 seconds.	
<input type="button" value="Submit"/>			
<p>Warning: After you click "Submit", you must reboot your gateway for changes to take effect. You may also have to do one or more of the following steps before you can access your gateway again:</p> <ul style="list-style-type: none"> • change the IP address of your computer • renew its DHCP lease • access the webGUI with the new IP address 			

◆ Function Summary

This configuration page is used to set the LAN group parameters. This interface is used to connect internal LAN and PCs in the LAN. This configuration page is used to configure the LAN IP address, the network mask and DHCP service of this group.

◆ Detailed Configurations

- **IP Address:** The IP Address of the LAN group.
- **Netmask:** The subnet mask of the LAN group.




You can configure the parameters for the DHCP service on this page. You can enable or disable the DHCP service on the router by check or uncheck the box of “**Enable DHCP service**”. The range of the IP address for the DHCP service to distribute can be defined in the “**Range**” field. These IP addresses should be in the same subnet with the route’s LAN IP address. The “**Lease time**” field specifies the lease time for each dynamic IP address assignment, with default 86400, in second.

3.4.2.1.2 DHCP binding

Click the **DHCP Binding** link to enter the DHCP binding configuration page. You can configure MAC and IP address binding, set up a DHCP binding table, and map the client MAC address and IP address. The DHCP Server will assign an IP address to your PC according to the configured binding table based on the MAC addresses.

Figure 3-13 **DHCP binding**



Click  to add a permanent IP address assignment rule, and click  to edit, and click  to delete an entry.

If the box of “**Deny unknown clients**” is checked, Any device holds the MAC address that are not on this table will not be able to obtain IP address from the router via DHCP service.

3.4.2.1.3 DHCP Lease Status

Click the **DHCP Lease** link to enter the page for listing DHCP clients and their IP addresses.

Figure 3-14 DHCP Lease

LanGroup		DHCP Binding	DHCP Lease	
IP address	MAC address	Hostname	Remaining-time	
172.16.0.7	00:c0:02:a4:de:d1;	tg-ws5fnlcrpe7v";	23 hours, 38 minutes, 9 seconds	

3.4.2.2 Wi-Fi

MB9000 can support multiple VAP (Virtual Access Point). Every VAP owned an independent SSID and security setting. Click the **Wi-Fi** link to enter the basic WLAN configuration interface, where you can configure the following parameters and the WLAN state list:

- **Radio:** Turn on/off the WLAN interface of MB9000.
- **Wireless Channel:** Wireless channel number, you can select a proper channel according to the country code.

Figure 3-15 Wi-Fi

Global **Wi-Fi**

Radio Turn on ▾

Wireless channel 1- 2.412 GHz ▾
If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best.

Submit

I/F	SSID	Security	Status
WLAN0	topglobal010203_0	Off	Start
WLAN1	topglobal010203_1	Off	Stop
WLAN2	topglobal010203_2	Off	Stop
WLAN3	topglobal010203_3	Off	Start

MB9000 supports four independent wireless networks (VAP interfaces), although they use the same physical hardware. For each VAP, different security settings can be applied. These VAPs can belong to different LAN groups, also same groups.

Click the **WLAN0/WLAN1/WLAN2/WLAN3** link to enter its configuration page. There are three tabs in this setting:

- Basic
- Encrypt
- Access Control List(ACL)

3.4.2.2.1 Basic

Figure 3-16 *Wireless - basic*

◆ Function Summary

This configuration page is used to set the wireless LAN basic parameters.

◆ Detailed configurations

Status: Start/Stop this interface.

Wireless Network Name (SSID): the wireless LAN network name shared among all access points in a wireless network. The SSID must be identical for all the access points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). For added security, you should change the default SSID to a unique name;

Hide SSID: When wireless clients survey the local area for wireless networks, they will detect the SSID broadcast by the Router. To broadcast MB9000's SSID, keep the default setting "Disabled". If you do not want to broadcast MB9000's SSID, then select "Enabled";

STAs isolation: If you don't want different client stations connected to the device to communicate with each other, **enable** this option;

3.4.2.2.2 Encrypt

Figure 3-17 Wi-Fi – Encrypt

The screenshot shows a web interface for configuring Wi-Fi security. At the top, there are three tabs: 'Basic', 'Encrypt' (which is active), and 'ACL'. Below the tabs, there are two main sections: 'Association' and 'Network key'. In the 'Association' section, 'Network Authentication' is set to 'open' and 'Data encryption' is set to 'Disabled'. In the 'Network key' section, there is a text input field for 'PSK(Only for WPA-PSK)', a dropdown menu for 'Key index(for transmit)' set to 'Key 1', and a red 'Hint' that reads: 'The following input must be 5 or 13 ascii characters, or 10 or 26 hexadecimal characters .'. Below the hint are four text input fields labeled 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. At the bottom of the form is a 'Submit' button.

◆ Function Summary

This configuration page is used to set wireless LAN security parameters. MB9000 supports two different types of security settings for your wireless LAN network: Wi-Fi Protected Access Pre-Shared key (WPA PSK) and Wire Equivalence Protection (WEP).

◆ Detailed configurations

Shared: Select from the dropdown menu of **Network Authentication**, which will enable the WEP sections;

WEP: There are two levels of WEP encryption security, 64-bit and 128-bit. The bigger encryption bit number, the more secure your wireless network. However, the transmission speed is sacrificed for the higher bit level's WEP security;

Key Index (for transmit): Select WEP key (1-4) to decide which key will be used during the data transmission;

Enter the WEP Key into the appropriate Key field. All access points in your wireless network must use the same WEP key to utilize WEP encryption;

WPA Pre-Shared Key - There are two encryption options for WPA Pre-Shared Key, TKIP and AES. TKIP stands for Temporal Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes a symmetric 128-bit block data encryption. To use WPA Pre-Shared Key, enter a password in the **PSK(Only for WPA-PSK)** field between 8 and 63 characters in length.

3.4.2.2.3 Access Control List

Figure 3-18 Wireless LAN – Access Control

The screenshot shows a configuration interface for Wireless LAN Access Control. At the top, there are three tabs: 'Basic', 'Encrypt', and 'ACL', with 'ACL' being the active tab. Below the tabs, there is a section for 'Access Control Mode' with a dropdown menu currently set to 'Deny Only'. A note below the dropdown states: 'If choose **Accept Only**, only the clients defined below will get authentication from this AP. Instead when choose **Deny Only**.' Below this section is a 'Submit' button. At the bottom, there is a table with two columns: 'MAC address' and 'Description'. A plus sign icon is located at the bottom right of the table area.

◆ Function Summary

Besides assuring the communication security in Wi-Fi network through encryption and authentication, allowing or denying some special stations connection in the Wi-Fi network

is also an option to guarantee the security of the wireless network. This page configuration is used to set the station connection control to assure the wireless network security. This access control scheme is only valid to Wi-Fi client.




◆ Detailed configurations

Access Control Mode: MB9000 supports 2 types of access control modes:

Allow only: Indicates only allow the stations which MAC address listed in the table to associate with the MB9000;

Deny only: Indicates only deny the stations which MAC address listed in the table to associate with the MB9000;

Access Control List: The MAC addresses of stations which have been allowed or denied to connect to MB9000 are saved in this list box.

Click  to add a MAC address assignment rule, and click  to edit, and click  to delete an entry. The input MAC address format must be “XX:XX:XX:XX:XX:XX”.

3.4.2.3 WAN

MB9000 provides two PC card slots for Internet connection: the cellular wireless Internet connection marked with WAN0 and WAN1. You can use each of them to configure your Internet connection. Click **WAN#0/WAN#1** to enter its WAN configuration page.

Figure 3-19 *Wireless Internet access*


	I/F	Network	IP Address	Status
WAN#0	PCMCIA0	WWAN-(Sierra Wireless AirCard 555)	220.207.73.166	up
WAN#1	PCMCIA1	WWAN-(Sierra Wireless AirCard 850)	10.15.156.204	up

3.4.2.3.1 Using either WAN0 or WAN1

You can use either WAN0 or WAN1 for the Internet connection. The parameters on their configuration pages are the same. Using WAN0 for example:

Figure 3-20 **Wireless Internet access**

Enable this interface

Hardware	
Description	Novatel Merlin C386 Card
Manufactory	QUALCOMM, Incorporated
Product	Model 100
SW	F/W VER: 127 S/W VER: DP3.3.20
Signal	 96%
Dial number	<input type="text" value="#777"/>
Init string	<input type="text"/>

PPP	
Compression	<input checked="" type="checkbox"/> Disable Van Jacobson style TCP/IP header compression. <input type="checkbox"/> Disable Address/Control compression(ACCM) in both directions. <input type="checkbox"/> Disable CCP (Compression Control Protocol) negotiation. <input type="checkbox"/> Disable protocol field compression negotiation. <input type="checkbox"/> Disable asyncmap(ACCM) negotiation.
MRU	<input type="text"/> Hint: Leaving it blank means not to special MRU of PPP.
MTU	<input type="text"/> Hint: Leaving it blank means not to special MTU of PPP.
DNS	<input checked="" type="checkbox"/> Obtain DNS server address automatically
Username	<input type="text" value="card"/>
Password	<input type="text" value="card"/>

Networking	
Connect mode	Auto <input type="button" value="v"/> <ul style="list-style-type: none"> ● Auto: Automatically dial up when power up. ● Dial on-demand: Dial up when LAN data request to access Internet. ● Manual: Manually dial up by client software or from web page. ● Bridge: Bridge with LAN interface, and provide PPPOE services to LAN user. In this mode, only one user can connect Interfaces.
Keepalive	<input checked="" type="checkbox"/> Enable, and interval with <input type="text" value="15"/> seconds
Status	Down
Load Balance	Primary <input type="button" value="v"/> If choose Primary, this interface will load balance system traffic with other primary interface. If choose Secondary, this interface will be backup of other primary interface.
NAT	Enabled <input type="button" value="v"/>

There are three sections on the same page for the wireless Internet configuration: the basic WWAN option, the PPP dialing parameters and the wireless Internet network mode.

◆ Function Summary

This WAN interface of MB9000 is used to connect Internet and wireless WAN. This configuration page is used to set some basic parameters of the wireless WAN card.

◆ Detailed Configurations

If **Enable this Interface** is not checked, no other parameters in this page are available.

- **Connect mode:** Indicate which wireless WAN connection policy is used.
 - **Auto:** This option enables MB9000 to automatically make the Internet connection each time when it powers on. It keeps MB9000 always connected to the Internet, even when the connection is idle. Once the auto mode been selected, the **keepalive** will enabled and MB9000 will check the Internet connectivity periodically. If MB9000 detects the Internet connection lost on this interface, it will try to dial up automatically to re-establish the connection. The default Redial Period is 15 seconds (In other words, the Device will check the Internet connectivity every 15 seconds).
 - **Dial-on-Demand:** When Connect mode is set to Dial-On-Demand, MB9000 will disable Keepalive automatically. When Dial-on-Demand mode is selected,

other than the “**Auto**” mode, the MB9000 will not automatically dial up to the Internet after powered up, until there is data traffic outward to the Internet from its LAN users.

Figure 3-21 **Dial-On-Demand**

Connect mode

- Auto: Automatically dial up when power up.
- Dial on-demand: Dial up when LAN data request to access Internet.
- Manual: Manually dial up by client software or from web page.
- Bridge: Bridge with LAN interface, and provide PPPOE services to LAN user. In this mode, only one user can connect Interfaces.

Disconnect if no data packets sent or received for seconds

MB9000 can be configured to automatically disconnect from Internet connection after a specified period of inactivity (Max Idle Time). If the Internet connection has been terminated due to inactivity, **Dial-on-Demand** enables MB9000 to automatically re-establish the Internet connection as soon as you attempt to access the Internet again. Enter a number in seconds you want your Internet connection to last when there is no data transmission.

- **Manual:** If you choose the Manual mode, the MB9000 will not make the Internet connection when you power up the MB9000. You must manually make the Cellular connection through web configuration page. To dialup manually, please login to the MB9000’s WEB configuration page, and go to “*Networks*”->“*WAN*” page or go to “*Devices*”->“*Status*” page.
- **Keep Alive:** This can detect whether the WWAN connection is in good status. When the WWAN connection is abnormal, it will be detected and the router will try to reconnect automatically. When the system is still abnormal, modem will be restart. After consecutively restart for several (configurable) times, if the system still could not turn well, the router will reboot automatically.
- **Status:** The Status field shows whether the wireless WAN module has dialed up to the Internet.
- **User Name:** Provide a username assigned to the subscriber by the cellular mobile operator. Please consult your mobile operator for that.

- **Password:** Provide a password for your wireless Internet dialing. Also you need to consult your mobile operator for that.

-  **Note:**

If you are using a GPRS network, the parameters different from CDMA network must be configured are as shown as *Figure 3-22* and *Figure 3-23*.

Figure 3-22

Username	ISP@CINGULARGPRS.COM
Password	CINGULAR1

Figure 3-23

Phone number	*99***1#
CID	1
PDP Type	IP
APN	isp.cingular
PDP Address	0.0.0.0
Data Compress	0
Header Compress	0

- **Phone Number:** Provide a phone number for wireless WAN modem;
- **CID:** (PDP Context Identifier) A numeric parameter, which specifies a particular PDP context definition.
- **APN:** (Access Point Name) A string parameter, which is a logical name that is used to select the GGSN or the external packet data network. User may need to consult the ISP for that.
- **PDP Address:** A string parameter that identifies the MB9000 in the address space applicable to the PDP.

There may be some operators do not require the username and password for the dialing, if so, please leave them empty (NULL).

- **Description/Manufactory/Product/SW/Signal:** These will display some information about the WWAN PCMCIA card inserted.
- **Phone Number:** Provide a phone number for wireless WAN modem.
- **Init string:** Provide an initializing string for wireless WAN modem.
- **Advanced Settings for PPP dialing**

There are some advanced settings for the PPP dial up: the MTU and MRU. Leave it empty unless you are aware of these, or follow the instructions from cellular operator.

You can either specify the DNS server's IP address manually or let the router obtain that from the PPP negotiation.

3.4.2.3.2 Using both WAN0 and WAN1 (Load Balance and NAT on the Internet interfaces)

You can use both WAN0 and WAN1 to configure your Internet connection. Both of their interfaces provide NAT option and Load Balance settings.

The client devices will NOT be able to access the Internet through this interface once the "NAT" option on it is set to Disabled.

If the "Load Balance" option is set to "Primary" on one of the interfaces (wan0 or wan1) while another one set to "Secondary", the secondary link will be a backup for the primary one. In this scenario, the primary interface will provide Internet access to the client devices, while the secondary one will be standby, and once the primary Internet link goes down, the secondary one will automatically connect to the Internet and take place of the primary one. When the primary link connects well to the Internet again, the secondary will automatically shutdown the connection.

When both of the two interfaces were set to "Primary", the MB9000 will balance the data traffic between them.

3.4.3 Advanced

There are three main categories in this setting:

- Dynamic DNS

- QoS
- Route

3.4.3.1 Dynamic DNS

Figure 3-24 DDNS configuration page

Network: Dynamic DNS

Enable Dynamic DNS update when WAN up

Provider	DynDNS.org ▾
Interface	wan0 ▾
Username	<input type="text"/>
Password	<input type="text"/>
Domain Name	<input type="text"/>
Wildcard	<input type="checkbox"/> Enable
Online	

MB9000 supports dynamic DNS (DDNS). The default status for DDNS is disabled. By far, MB9000 only supports dyndns.org, which provided by www.dyndns.com. To use this feature, you should obtain your own domain name from the provider (dyndns.com). Every time the WAN IP changed which interface you selected, the router will register the new public IP address obtained from the PPP negotiation to the provider.



3.4.3.2QoS

This section indicates the features of the QoS provided by the MB9000. The MB9000 QoS enables complex networks to control and predictably service a variety of networked applications and traffic types. Fundamentally, QoS enables you to provide better service to certain applications. This is done by either raising the priority of a flow or limiting the

priority of another flow.

Figure 3-25 QoS Rule list

Bandwidth: QoS Rule

LAN Hosts	Application	Priority	Enable	Configure
172.16.0.2	FTP(TCP)	High	<input checked="" type="checkbox"/>	 

Add

Note:
the first rule that matches a packet will be executed.
The following match patterns are not shown in the list above: IP packet length, TCP flags.



To add a QoS rule, you just need to click **Add** button and then you will see a pop-up window show as figure 3-26. Follow the instructions in this screen to add a new QoS rule to the MB9000, see the following figure. You can also set the rules status to enable or disable by check the box of "Enable". Or edit the content of a rule entry by click , as well as delete it by click . After you added one or more entries, or made any changes on the existed entries, you will need to reboot system from the reboot page to take them effect and save the settings to flash.

Figure 3-26 Add QoS Rules

Bandwidth: QoS Rule

LAN hosts	Address: Host <input type="text"/> / <input type="text"/>
Application	Protocol: ALL <input type="text"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here. Port: (other) <input type="text"/> Hint: use the string such as "port1,ports:porte" to specify multiple ports or ports range.
Priority	High <input type="text"/> Choose a pipe or queue where packets that match this rule should be sent.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

Submit

3.4.3.3 Route

3.4.3.3.1 Static Route

MB9000 supports user defined static route. Figure 3-27 shows a sample static route status.

Figure 3-27 **Static Route**

Network: Static Route

The screenshot shows a web interface for configuring static routes. At the top left is an 'Apply Change' button. Below it is a table with the following columns: 'Interface', 'Network', 'Gateway', 'Enable', and 'Configure'. At the bottom right of the table area is an 'Add' button.



To add a static route rule, you just need to click the “Add” button and then you will see a pop-up window show as figure 3-28. You can also set the rules status to enable or disable by check the box of “Enable”. Or edit the content of a rule entry by click , as well as delete it by click . After you added one or more entries, or made any changes on the existed entries, you will need to click the “Apply Changes” button to take them effect and reboot from the reboot page to save the settings to flash.

Figure 3-28 **Static Route**

The screenshot shows a pop-up window for adding a static route. It has four main sections: 'Destination' with an 'Address:' label and a dropdown menu containing an asterisk (*); 'Nexthop' with a text input field; 'Interface' with a dropdown menu; and a 'Submit' button at the bottom.

To add a new entry, this pop-up window will appear. The **Interface** is to tell the router through which interface should the outgoing packets go for the specified destination. There are totally 6 options: LANGroup0, LANGroup1, LANGroup2, LANGroup3, WAN0,

and WAN1. The “**Nexthop**” field indicates the router that the next hop for the specified network/host. You can configure the destination address to in the “**Destination**” field. Here the “*” means any IP address, same as 0.0.0.0/0.0.0.0, in this case, the IP address in the **Nexthop** field will be the default gateway for the router. When “**Host**” in the “**Destination**” field is selected, it means that the destination is a single host’s IP address, same as Host_IP/255.255.255.255. When the “**Network**” is selected, you need to configure the IP address of the destination network as well as its subnet length in the drop-down list. Before you configure the rules for the static route, you should be aware clearly about the route.

3.4.3.3.2 RIP

Figure 3-29 RIP configuration page

Static Route	RIP	OSPF
<input type="checkbox"/> Enable RIP Dynamic Route		
Interface	LANGroup0	
Version	v2	
Update Timer		
Invalid Timer		
<input type="button" value="Submit"/>		
<p>Warning: After you click "Submit", you must reboot your gateway for changes to take effect. You may also have to do one or more of the following steps before you can access your gateway again:</p>		

Check the “**Enable RIP Protocol**” box to enable RIP or uncheck it to disable. You can select “**V1**”, “**V2**”, or “**V1 and V2**” in the “**Version**” field. The “**Update Timer**” indicates how long the router should update the RIP information, and the “**Invalid Timer**” field indicates that how long the router should age the RIP information, all in second.

3.4.3.3.3 OSPF

Figure 3-30 OSPF configuration page

Check the “**Enable OSPF Protocol**” box to enable OSPF or uncheck it to disable.

Fill in the “**Pass Phrase**” to setup the OSPF security.

3.4.4 Firewall

There are five main categories in this setting:

- General
- MAC Filter
- IP Filter
- WEB Filter
- Port forwarding

3.4.4.1 General

Click the **General** link on the left part of the interface to enter the firewall by-level control

page, where the user can configure the firewall security level and whether to enable the status packet check accelerating function.

Figure 3-31 **General**

Level	<input type="radio"/> High	Default Inbound Policy: Reject Default OutBound Policy: Reject Anti-attack: Enabled SPI: Enabled Others filter settings will override above policy.
	<input type="radio"/> Middle	Default Inbound Policy: Reject Default OutBound Policy: Accept Anti-attack: Disabled SPI: Enabled Others filter settings will override above policy.
	<input checked="" type="radio"/> Low	Default Inbound Policy: Accept Default OutBound Policy: Accept Anti-attack: Disabled SPI: Disabled Others filter settings will override above policy.
	<input type="radio"/> None	Default Inbound Policy: Accept Default OutBound Policy: Accept Anti-attack: Disabled SPI: Disabled Others filter settings will be disabled.
	<input type="radio"/> Customize	Default Inbound Policy: <input type="text" value="Accept"/> Default OutBound Policy: <input type="text" value="Accept"/> Anti-attack: <input type="text" value="Enabled"/> SPI: <input type="text" value="Enabled"/> MAC Filter: <input type="text" value="Enabled"/> IP Filter: <input type="text" value="Enabled"/> WEB Filter: <input type="text" value="Enabled"/>
Max Single Host Conn.	<input type="text" value="0"/> (0 - 128 , 0 for nolimit)	
<input type="button" value="Submit"/>		

High: The firewall level is high. In this case, bilateral access of the inner network and outer network is denied, and the anti-attack, SPI function is also enabled.

Medium: The firewall level is medium. In this case, the inner network is allowed to access the outer network and the anti-attack function is also disabled, the external access is denied and the SPI function is also enabled.

Low: The firewall level is low. In this case, all the access of the inner network and outer network is allowed.

None: The firewall level is low. In this case, all the access of the inner network and outer network is allowed, and none of the filtering rules takes effect.

Customize: User can customize the firewall settings.

Max Single Host Conn.: This field indicates that how many TCP connections that a single client device can establish through the router in maximum, 0 for no limitation.

3.4.4.2 MAC Filter

Figure 3-32 MAC Filtering table

The screenshot shows a web-based configuration interface for MAC filtering. At the top, there is a 'Mode' dropdown menu currently set to 'Allow'. Below this is a 'Submit' button. Underneath the button is a table with two columns: 'Hw Address' and 'Desc'. The table is currently empty. In the bottom right corner of the table area, there is a blue circular icon with a plus sign, indicating that new entries can be added.

◆ Function Summary

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length). MAC Filter can control the hosts in LAN to allow or deny their Internet access based on their MAC addresses.

◆ Detailed Configurations

- **MAC Filter Mode:**
 - ◆ Allow means only the hosts with the MAC address in the list can access the Internet.
 - ◆ Deny means only the hosts with the MAC address in the list can't access the Internet.



Note:

Both MAC Filter and Wireless LAN MAC Access Control List can realize the access

control based on MAC addresses, but they are different: MAC filter controls the access to the Internet however Wireless LAN Access Control List controls the access to the MB9000 via Wireless LAN.

3.4.4.3 IP Filter

Figure 3-33 IP Filtering table



◆ Function Summary

Access Rules is one of the most important functions of MB9000's firewall.

◆ Detailed Configurations

The access rules of the firewall in MB9000 have many access rule items. You can maintain these rules with the operations of: Add, Delete, Move up, Move down, Apply.

- **Enable Checkbox:** You can enable or disable a rule by checking or unchecking this checkbox;
- **Move up, Move down:** The sequence of the rules in the list is very important for the firewall. When the firewall deals with a data packet, it will check the rules from top to bottom sequentially and execute the first rule which matches the character of this packet. So please pay attention to the sequence when you are using multiple rules;
- **Apply Change:** Click the **Apply Change** button to validate the change immediately. No reboot is required here;
- **Add:** Click the **Add** button, a pop-up window for inputting an access rule will appear:

Figure 3-34 IP Filtering definition

General		Schedule
Action	Block	
Service	Custom Protocol: TCP Port Range: -	
Source	Interface: All LANGroup Address: * /	
Destination	Interface: WANO Address: * /	
Description	<input type="text"/> You may enter a description here for your reference (not parsed).	
<input type="button" value="Submit"/>		

Each rule consists of the following parameters:

Action: You have two options here: Block or Pass. Block means the data packet which matches this rule will be blocked by firewall; Pass means the data packet which matches this rule will be passed by firewall;

Service: You can customize a service or select the defined services from the dropdown list to configure the rules.

- **Protocol:** This parameter indicates which protocol will implement this service. Possible protocols are: TCP, UDP, TCP/UDP;
- **Port range:** This parameter indicates which port or port range will implement this service. If only one port will implement this service, type this port in both boxes. If several ports will implement this service, type the start port in the left box and the end port in the right box.

Source: This parameter indicates the IP address range of data source;

Destination: This parameter indicates the IP address range of destination;

Service: This parameter indicates the service type of this rule. The possible type includes the system default services and user defined services;

Description (optional): Type your comments for this rule here.

User can also configure the period of time when a rule is available.

Figure 3-35 *IP Filtering Schedule*

General	Schedule
Time	Start: <input type="text" value="00"/> : <input type="text" value="00"/> End: <input type="text" value="23"/> : <input type="text" value="59"/>
List of days	<input checked="" type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday

3.4.4.4 WEB Filter

Click the **Web Filter** link on the left part of the WEB page to enter the Web Filter page, which consists of the Filtering Rule used to set rule respectively and filter HTTP request for the Web server by any client.

Figure 3-36 **Web Filtering table**

Restricted WEB Feature	<input type="checkbox"/> ActiveX <input type="checkbox"/> Java <input type="checkbox"/> Cookies <input type="checkbox"/> Access to HTTP proxy Servers
Blocked Hosts	<div style="border: 1px solid gray; height: 80px; width: 100%;"></div> <p>Specify a list of Hosts Keywords separated by spaces</p>
Blocked URLs	<div style="border: 1px solid gray; height: 80px; width: 100%;"></div> <p>Specify a list of URLs Keywords separated by spaces</p>
<input type="button" value="Submit"/>	

3.4.4.5 Port forwarding

Figure 3-37 **Port forwarding**

Firewall: Port Forwarding

Interface	Protocol	Ext. port	NAT ip	Int. port	Enable	Configure
<input type="button" value="Add"/>						

◆ Function Summary

This feature allows you to forward incoming traffic on certain ports in order to access servers behind the NAT. This feature can let you setup a web server, mail server, FTP server, DNS, etc on your LAN so it can be accessed from the Internet.

◆ Detailed Configurations

The port forwarding table in MB9000 consists of many port forwarding items.

- **Enable Checkbox:** You can enable or disable a port forwarding item by checking or unchecking this checkbox;
- **Move up, Move down:** Re-arrange the order of each item in the list;
- **Apply Change:** Click the **Apply Change** button to validate the change immediately. No reboot is needed here;
- **Add:** Click the **Add** button, a pop-up window for inputting port forwarding item will appear:

Figure 3-38 Port forwarding

Interface	<input type="text" value="WAN"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	<input type="text" value="ALL"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
External port	<input type="text" value="(other)"/> Start <input type="text"/> - End <input type="text"/> Specify the port on the firewall's external address for this mapping.
NAT IP	<input type="text"/> Enter the internal IP address of the server on which you want to map the ports. e.g. 172.16.0.3
Local port	<input type="text" value="(other)"/> Start <input type="text"/> - End <input type="text"/> Specify the port on the machine with the IP address entered above.
Auto forward	Enable Hint: specify if auto add one access rule for allow this packet to forward .
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

Each item consists of the following parameters:

Interface: This parameter indicates which interface of MB9000 will implement this port forwarding rule. In most cases the interface should be WAN;

Protocol: This parameter indicates which protocol will implement this port forwarding rule;

External port: This parameter indicates the port for public access;

NAP IP: This parameter indicates the IP address of the internal host which wants to provide service for the outside;

Local port: This parameter indicates the port of internal service;

Auto forward: This parameter will be Enable always, which means MB9000 will enable this forward automatically;

Description (optional): Type your comments for this rule here.

3.4.5 VPN

There are two main categories in this setting:

- IPsec
- PPTP Client

3.4.5.1 IPsec

Figure 3-39 IPsec VPN Configuration

The screenshot shows the 'General' tab of the IPsec VPN configuration interface. It includes a 'Connection' sub-tab. The 'Enable VPN Service' checkbox is unchecked. The 'Tunnel Mode' section has 'Net-To-Net' selected with a radio button, and 'Host-To-Net' is unselected. The 'IPSEC Services' status is shown as 'Stopped' in red text. A 'Submit' button is located at the bottom of the configuration area.

The screenshot shows the 'Connection' sub-tab of the IPsec VPN configuration interface. It features an 'Apply Change' button at the top. Below it is a table with columns for 'Local net', 'Remote net', 'Interface', 'Remote gw', 'Status', 'Enable', and 'Configure'. An 'Add' button is positioned at the bottom right of the table area.

Local net	Remote net	Interface	Remote gw	Status	Enable	Configure
Add						

◆ Function Summary

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

◆ Detailed Configurations

- **Tunnel mode:** Tunnel mode encapsulates the entire IP packet to transmit it securely. A Tunnel mode is required for gateway services to provide access to internal systems. Tunnel mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. Tunnel mode is required for client to client or host to client communications.
- **Add:** Click the **Add** button, a pop-up window for inputting a tunnel item will appear:

General	Manual Key	Auto Key
Interface	wan0 ▾ Select the interface for the local endpoint of this tunnel.	
Local subnet	[] / 24 ▾	
Remote subnet	[] / 24 ▾	
Remote gateway	[] Enter the public IP address of the remote gateway	
Protocol	<input type="checkbox"/> AH <input checked="" type="checkbox"/> ESP <input type="checkbox"/> Compress ESP is encryption, AH is authentication only.	
Encryption algorithms	3DES ▾ Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card.	
HMAC algorithms	SHA1 ▾	
Keying Mode	Automatic(IKE) ▾ Automatic Keying is more secure, but more complex.	
Description	[] You may enter a description here for your reference (not parsed).	

Select **Manual Key** to display the manual VPN rule setup screen.

General	Manual Key	Auto Key
ESP Key	<input type="text"/>	(for encrypt)
	<input type="text"/>	(for authenticate)
AH Key	<input type="text"/>	
SPI	<input type="text"/>	(inbound)
	<input type="text"/>	(outbound)

Select **Auto Key** to display the auto VPN rule setup screen.

General	Manual Key	Auto Key
Auto-establish	<input type="checkbox"/> Automatically establish this tunnel Set this option to automatically re-establish this tunnel after reboots/reconfigures. If this is not set, the tunnel is established by manual.	
Negotiation mode	<input type="text" value="main"/> Aggressive is faster, but less secure.	
Encryption algorithm	<input type="text" value="3DES"/> Must match the setting chosen on the remote side.	
Hash algorithm	<input type="text" value="SHA1"/> Must match the setting chosen on the remote side.	
DH key group	<input type="text" value="2"/> <i>2 = 1024 bit, 5 = 1536 bit</i> Must match the setting chosen on the remote side.	
Authentication method	<input type="text" value="Pre-shared key"/> Must match the setting chosen on the remote side.	
DPD option	<input type="text" value="Enabled"/> Set this option to check peer live or dead after building tunnel. Set the delay to <input type="text" value="10"/> seconds between Dead Peer Detection (RFC 3706) keepalives. Declare the peer dead and remove the SA after <input type="text" value="30"/> seconds with no response and no traffic.	
Pre-Shared Key	<input type="text"/>	
PFS	<input type="text" value="off"/> with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier.	
IKE Lifetime	<input type="text"/> seconds	
IPSEC Lifetime	<input type="text"/> seconds	

3.4.5.2 PPTP Client

Figure 3-40 PPTP Client Configuration

Enable this interface

Interface	<input type="text" value="WAN0"/> Select the interface for the local endpoint of this tunnel.
User Name	<input type="text"/>
User Password	<input type="password"/>
Remote Server	<input type="text"/> (e.g. pptpserver.mycompany.com/201.32.44.1)
Accessed Network	<input type="text"/> / <input type="text" value="24"/>
Connect mode	<input type="text" value="Auto"/>
Status	down
IP Address	0.0.0.0

Warning:
After you click "Submit", you must reboot your gateway for changes to take effect. You may also have to do one or more of the following steps before you can access your gateway again:

- change the IP address of your computer
- renew its DHCP lease
- access the webGUI with the new IP address

◆ Function Summary

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

Check the “**Enable this interface**” box to enable PPTP or uncheck it to disable.

◆ Detailed Configurations

- **Interface:** Select the interface (wan0/wan1/wan2) to creating tunnel with server.
- **User Name:** Type the user name given to you by server.
- **Password:** Type the password associated with the User Name above.
- **Remote Server:** Type the IP address of the PPTP server.
- **Accessed Network:** Enter the private network IP address behind server which

you want to visit.

- **Connect mode:** To choose a connection policy be used.
- **Status:** Indicate the connection status.
- **IP Address:** Display the IP address after PPTP connection established.

3.4.6 Management

There are seven main categories in this setting:

- System
- Administration
- Time
- Certificate
- Firmware
- Backup/Restore
- Factory Defaults

3.4.6.1 System

Figure 3-41 System

Hostname	<input type="text" value="topglobal_MF165G370776"/> Name of the gateway, without domain part e.g. mymb
Serial Speed	<input type="text" value="115200bps"/>
Serial used for	<input type="text" value="Debug"/>
DNS servers	<input type="text"/> <input type="text"/> IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients
ALG plugin	<input type="checkbox"/> SIP <input type="checkbox"/> H.323

- **Host Name:** Up to 64 characters name to represent MB9000 device. The default name: topglobal_SN.
- **Serial Speed:** When you need a backup link (for example, the v.90 modem) for MB9000, you might need to configure the serial speed for the modem. There are totally 6 options for the serial speed (bps): 115200, 57600, 38400, 19200, 9600, and 4800. You may need to reference to the user guide of the modem to configure the right speed.
- **Serial used for:** Select a serial used mode.
- **DNS servers:** Use DNS (Domain Name System) to map a domain name to its corresponding IP address.
- **ALG Plug-in:** This technique relies on the installation of a new, enhanced Firewall/NAT - called an Application Layer Gateway. MB9000 provides two kinds of ALG Plug-in names SIP and H.323. When you choose either, you can plug the protocol.

3.4.6.2 Administration

Figure 3-42 Administration-Basic

Basic	
Username	<input type="text" value="public"/> If you want to change the username for accessing the webGUI, enter it here.
Password	<input type="password" value="....."/> <input type="password" value="....."/> (confirmation) If you want to change the http password for accessing the webGUI, enter it here twice.
webGUI protocol	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
webGUI port	<input type="text" value="80"/> Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS). <input type="checkbox"/> Enable management from WAN, use port <input type="text" value="8080"/>
<input type="button" value="Submit"/>	

- **Username:** Username for MB9000's web administration. The default username is public.
- **Password:** Password for MB9000's web administration. The default password is public.



Note:

Each time when the user modifies the username and password, the system will request the user to re-authenticate the new user name and password.

- **WebGUI Protocol:** The protocol web configuration used. You can select HTTP or HTTPS to browse the WEB page on the router.
- **WebGUI port:** The service port for HTTP. User normally need not modify this value. If you want to allow someone else to manage the MB9000 from WAN, you can check **Enable management from WAN**, and modify the port value according to your needs. Normally, MB9000 can't be configured through WAN interface for the security consideration. If user wishes to remotely configure the MB9000 through WAN interface, there is one box to select to enable this feature.



Note:

Submit is not equal to keep the configuration information permanently in the device. Users must reboot the system, the configuration will be saved. So if user saves the configuration, and doesn't reboot the device through web page, the configuration information will be lost.

3.4.6.3 Time

Figure 3-43 Time

Current Time	Thu May 10 20:56:16 2007
Time zone	<input type="text" value="(GMT-05:00) Eastern Time (USA, Canada)"/> Select the location closest to you <input type="checkbox"/> Enable Daylight Saving Time
NTP setting	<input checked="" type="checkbox"/> Automatically synchronize with Internet time server Primary Server <input type="text" value="pool.ntp.org"/> Second Server <input type="text" value="time.nist.gov"/> Third Server <input type="text" value="time.windows.com"/>
<input type="button" value="Submit"/>	

- **Current Time:** Current time of the system.
- **Time zone:** Current country time zone. You should check **Enable Daylight Saving Time** if implement DST (Daylight Save Time) in your country.
- **NTP setting:** You can enable/disable synchronize local time with Internet time server by checking **automatically synchronize with Internet time server**.

3.4.6.4 Certificate

Figure 3-44 **Certificate information**

	Owner	Issuer
<input checked="" type="radio"/>	Web-GUI	C=US, ST=CA, O=TopGlobal USA Ltd, CN=MobileBridge
<input type="radio"/>	VPN	N/A

You can use this screen to view in-detail certificate information and import a new one for Web-GUI or VPN or renew a certificate. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 3-45 **Certificate information**

System: Certificate

Certificate Information	
Version	1 (0x0)
Serial Number	0 (0x0)
Signature Algorith	md5WithRSAEncryption
Issuer	C=US, ST=CA, O=TopGlobal USA Ltd, CN=MobileBridge
Validity From	Jan 1 00:00:10 1970 GMT
Validity To	Jan 1 00:00:10 1971 GMT
Subject	C=US, ST=CA, O=TopGlobal USA Ltd, CN=MobileBridge
Public Key	RSA Public Key: (1024 bit)

Click **Import** to open the Certificate Import screen. Follow the instructions in this screen import a new certificate to the MB9000, see the following figure.

Figure 3-46 **Certificate import**

Certificate	<input type="text"/> Paste a signed PKCS7/X509 certificate in PEM format here.
Key	<input type="text"/> Paste a signed PrivateKey in PEM format here.

3.4.6.5 Firmware

If you have downloaded the firmware from our WEB site and stored it in your local computer, you can upgrade the firmware from the local host.

Figure 3-47 **Local Upgrade**

Local Upgrade

Choose the firmware file to be uploaded.
Click "Upgrade firmware" to start the upgrade process.

Firmware file:

Warning:
DO NOT abort the firmware upgrade once it has started. The gateway will reboot automatically after storing the new firmware. The configuration will be maintained.

MB9000's firmware can be upgraded through this tab. Follow these instructions:

1. Download the firmware from Top Global website www.topglobalusa.com to your host PC. User can also get technical support from Top Global USA, Inc. by email or phone.

2. Enter the location of the firmware file or click the **Browse** button to find the file. Click the **Upgrade Firmware** button to upgrade the firmware.

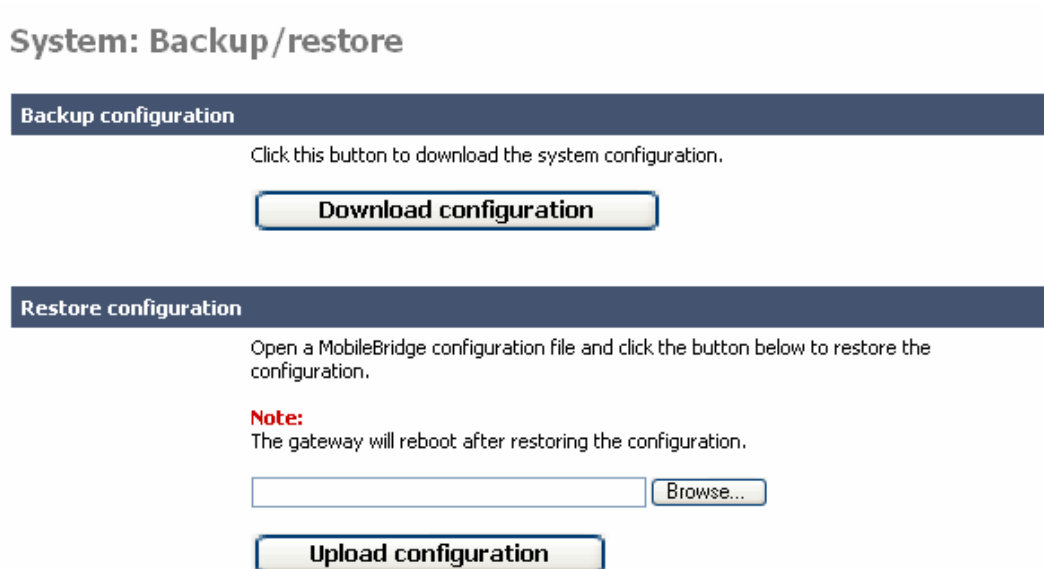


Note:

Don't interrupt the upgrade process, the device will be rebooted after the firmware upgrade is complete.

3.4.6.6 Backup/Restore

Figure 3-48 Backup/Restore



Download Configurations: User can download current device configurations and save them in the local PC for later uploading and restoring.

Upload Configurations: User can use previous saved configurations to restore the device configuration to the previous configuration status. Note that this function will erase the current configuration.

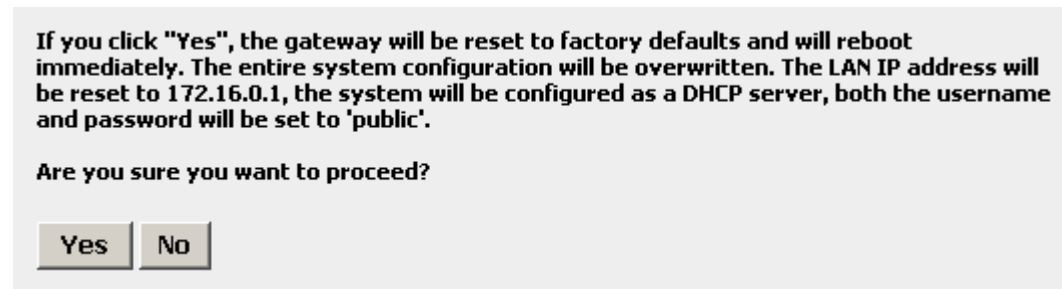


Note:

After uploading configuration finished, the device will reboot itself automatically.

3.4.6.7 Factory defaults

Figure 3-49 Reload to the Factory Defaults



Click the **Yes** button to reset all configurations to their factory default values. All of the current configured parameters will be lost after the router is reloaded to the factory defaults, so, you'd better backup them by following the instructions in 3.4.6.6.

3.4.7 Diagnostics

There are three categories in this setting:

- Ping
- PCMCIA
- AT Command

The tools in this block offer interfaces for the advanced users to diagnostic the network connection.

3.4.7.1 Ping

Figure 3-50 *ping*

Diagnostics: Ping

Host	<input type="text"/>
Size	<input type="text" value="64"/>
Count	<input type="text" value="1"/> ▼
<input type="button" value="Ping"/>	

Ping is one of the most useful network debugging tools. It can test whether a given host is reachable through network. With this tool, you can test if the router has connected to the Internet. You can fill in destination host by its domain name or IP address in the “**Host**” field. The specified host should be routed on the Internet. The “**Size**” field specifies the packet length to send to the host. The “**Count**” field specifies how many packets the router should send.

3.4.7.2 PCMCIA

Figure 3-51 PCMCIA

Status	Socket 0: 5V 16-bit PC Card function 0: [ready] Socket 1: 3.3V 16-bit PC Card function 0: [ready]
CIS	Socket 0: dev_info no_info attr_dev_info EEPROM 250ns, 512b manfid 0x0192, 0xa555 funcid serial_port vers_1 7.0, "Sierra Wireless", "AirCard 555", "A555", "Rev 1" config base 0x0700 mask 0x0073 last_index 0x03 cftable_entry 0x20 [default] io 0x03f8-0x03ff [lines=3] [8bit] [range] irq mask 0x3fbc [level] cftable_entry 0x21 io 0x02f8-0x02ff [lines=3] [8bit] [range] cftable_entry 0x22 io 0x03e8-0x03ef [lines=3] [8bit] [range] cftable_entry 0x23 io 0x02e8

This page shows the information about the PCMCIA card (the cellular data card that you plugged into the router).

3.4.7.3 AT Command

Figure 3-52 AT Command

Port	Serial ▾
Command	<input type="text"/>
Output	<input type="text"/>

You can input some AT commands to test the serial port here.

4 Troubleshooting

4.1 Overview

- Introduction
- Reset to Factory Default procedure
- Firmware Upgrade Procedure through Web
- Common Problems and solutions
- Frequently Asked Questions
- LED Indication status

4.2 Introduction

This section helps you to locate problems related to MB9000 setup. The most common installation problems are related to the IP address.

IP address management is critical and we suggest you to create a chart to document and validate the IP addresses of your system.

If the password is lost or forgotten, you will need to reset the MB9000 to default values. The **Reset to Factory Default** procedure resets the MB9000 configuration settings, but does not change the current firmware.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration, including the MB9000 IP Address, Subnet Mask, and so on. The current MB9000 Software will not be erased. This procedure may be required if the password is forgotten or the configurations are forgotten.

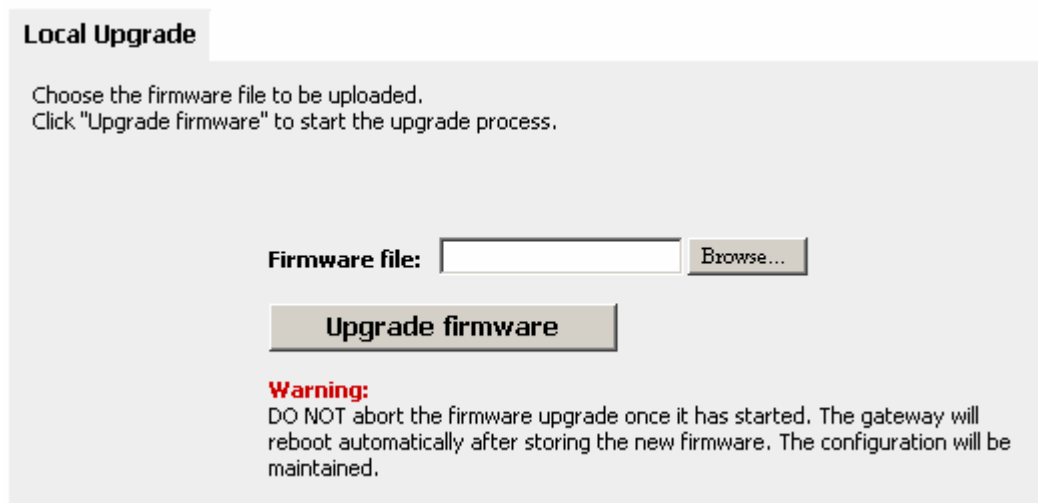
When MB9000 is working in normal status, **press and holds the RELOAD button for about**

20 seconds, until all the indicator lights change to amber. Then release **RELOAD** button, and press reset button to reboot MB9000, the factory default network values are restored. Please refer Table 6-1 for the factory default value.

Firmware Upgrade Procedure through Web

Use this procedure to upgrade the newest version firmware for MB9000 through Web interface on user client. This procedure may be necessary when a new version of firmware is released (Figure 4-1).

Figure 4-1 **Firmware upgrade**



MB9000's firmware is upgraded through **Firmware** tab. Follow these instructions:

1. Download the firmware from Top Global's website at www.topglobalusa.com to your host PC.
2. Enter the location of the firmware file or click the **Browse** button to find the file.
3. Then, click the **Upgrade Firmware** button to upgrade the firmware.

Common Problems and Solutions

1. How to set a static IP address on a PC?

You can assign a static IP address to a PC by performing the following steps:

• **For Windows 98 and Me:**

- a. Click Start, Settings, and Control Panel. Double-click Network.
- b. In "The following network components are installed" box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter

installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it then click the Properties button.

- c. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computers on the network connected to MB9000. Make sure that each IP address is unique for each PC or network device.
- d. Click the Gateway tab, and in the New Gateway prompt, enter 172.16.0.1, which is the MB9000's default IP address. Click the Add button to accept the entry.
- e. Click the DNS tab, and make sure the DNS Enabled option is selected. Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
- f. Click the OK button in the TCP/IP properties window, and click Close or the OK button for the Network window.
- g. Restart the computer when asked.

• ***For Windows 2000:***

- a. Click Start, Settings, and Control Panel. Double-click Network and Dial-Up connections.
- b. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
- c. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the Properties button. Select Use the following IP address option.
- d. Enter a unique IP address that is not used by any other computer on the network connected to MB9000.
- e. Enter the Subnet Mask, 255.255.0.0.
- f. Enter the Default Gateway, 172.16.0.1 (MB9000's default IP address).
- g. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.

- h. Click the OK button in the Internet Protocol (TCP/IP) Properties window, and click the OK button in the Local Area Connection Properties window.
- i. Restart the computer if asked.

• **For Windows XP:**

The following instructions assume you are running Windows XP with the default interface.

If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

- a. Click Start and Control Panel.
- b. Click the Network and Internet Connections icon and then the Network Connections icon.
- c. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
- d. This connection uses the following items box, highlight Internet Protocol (TCP/IP). Click the Properties button.
- e. Enter a unique IP address that is not used by any other computers on the network connected to MB9000.
- f. Enter the Subnet Mask, 255.255.0.0.
- g. Enter the Default Gateway, 172.16.0.1 (Router's default IP address).
- h. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
- i. Click the OK button in the Internet Protocol (TCP/IP) Properties window. Click the OK button in the Local Area Connection Properties window.

2. How to test my Internet connection?

a. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Make sure Obtain IP address automatically is selected in the settings.

b. Open a command prompt.

For Windows 98 and Me:

- Click Start and Run. In the Open field, type “command”. Press the Enter key or click the OK button.

For Windows 2000 and XP:

- Click **Start** and **Run**. In the Open field, type “cmd”. Press the **Enter** key or click the **OK** button. In the command prompt, type “ping 172.16.0.1” and press the **Enter** key.
- If you get a reply, the computer is communicating with MB9000.
- If you do NOT get a reply, please check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

c. In the command prompt, type ping followed by your WWAN IP address and presses the Enter key. The WAN IP Address can be found on the Status screen of MB9000’s web-based utility. For example, if WWAN IP address is 1.2.3.4, you should enter ping 1.2.3.4 and press the Enter key.

- If you get a reply, the computer is connected to MB9000.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

d. In the command prompt, type ping www.yahoo.com and press the Enter key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. When I enter a URL or IP address, I get a time-out error or I am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation’s IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check MB9000. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

- If MB9000 is configured correctly, check your Internet connection (WWAN card) to see if it is working correctly.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to direct connection to the Internet.

Frequently Asked Questions

What is the maximum number of IP addresses that MB9000 will support?

MB9000 will support up to 253 IP addresses.

Is IPSec Pass-Through supported by MB9000?

Yes, it is a built-in feature that MB9000 automatically enables.

Does MB9000 support IPX or AppleTalk?

No. TCP/IP is the only protocol supported.

What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet.

Furthermore, NAT allows MB9000 to be used with low cost Internet accounts. The user may have many private addresses behind this single address provided by the ISP.

Does MB9000 support any operating system other than Windows 98, Windows Millennium, Windows 2000, or Windows XP?

Yes.

Does MB9000 support ICQ send file?

Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind MB9000.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?

It depends on which network game or what kind of game server you are using. It will work if the game server supports multi-user with one public IP address.

Which browsers does MB9000 support?

MB9000 supports Internet Explorer 4.0, Netscape 4.0, Mozilla and Safari which mainly used in Macintosh.

I am not able to get the web configuration screen for MB9000. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to direct connection to the Internet.

Does MB9000 pass PPTP packets or actively route PPTP sessions?

MB9000 allows PPTP packets to pass through.

Is MB9000 cross-platform compatible?

Any platform that supports Ethernet and TCP/IP is compatible with MB9000.

Can MB9000 act as my DHCP server?

Yes. MB9000 has DHCP server software built-in.

How do I reset MB9000 to factory default?

When MB9000 is working in normal status, press and hold the **RELOAD** button for about 20 seconds, until all the indicator lights turn off. Then release **RELOAD** button, press the **RESET** button to set up the device again. This will reset MB9000 to its default settings.

How can I get support?

Please send mail to support@topglobalusa.com to contact us. Our supporter will reply to you as soon as possible. Otherwise, you'd better to send mail with more detailed description of the issue you meet, including the firmware version and system log messages.

5 Default MB9000 Settings

The following table lists the settings defined at the factory for all MB9000 units, and provides a place to enter the values for your system if you have changed them.

Table 5-1 **Default Setting**

Item	Default Value	My System Value
Local IP Address	172.16.0.1	
Local IP Mask	255.255.255.0	
Network Name(SSID)	topglobal_SN_0	
Frequency Channel	1	
DHCP Server Status	Enabled	
DHCP Lease Range	172.16.0.2-172.16.0.100	
Http Username	public	
Http Password	public	

Wireless WAN default setting:	Dial mode	Auto
	Keepalive	Enable
	username	"card" for CDMA/EVDO network. "ISP@CINGULARGPRS.COM" for GPRS/EDGE/UMTS/HSDPA network.
	password	"card" FOR CDMA/EVDO network, "CINGULAR1" for GPRS/EDGE/UMTS/HSDPA network