

MobileBridge Gateway Series

MB5000

Wireless Cellular Data Gateway

User Guide

Version 1.1.26

(Firmware v1.1.26)

2007-06-08

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 MB5000 (FCC ID: SUMMB5000) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A.

CONTENT

CONTENT	3
1 INTRODUCTION	5
2 INSTALLING THE MB5000	6
2.1 VERIFY KIT CONTENTS.....	6
2.2 WRITE DOWN PRODUCT IDENTIFICATION.....	8
2.3 POWER ON THE MB5000	8
2.4 LED INDICATORS.....	9
2.5 INITIALIZE THE MB5000 UNIT	10
3 MANAGEMENT	15
3.1 OVERVIEW	15
3.2 PAGE STRUCTURE.....	17
3.2.1 <i>Shortcut</i>	17
3.3 PAGE OPERATION.....	19
3.4 CONFIGURATION PAGES DESCRIPTION.....	20
3.4.1 <i>System</i>	20
3.4.2 <i>Interfaces</i>	26
3.4.3 <i>Service</i>	41
3.4.4 <i>Firewall</i>	45
3.4.5 <i>Security Services</i>	51
3.4.6 <i>Tools</i>	54
3.4.7 <i>Status</i>	60
3.4.8 <i>Diagnostics</i>	62
4 TROUBLESHOOTING	65
4.1 OVERVIEW	65
4.2 INTRODUCTION	65
5 DEFAULT SETTINGS	76

FOREWORD

This section describes the objectives, audience and conventions of the Top Global MB5000 User Guide.

Objectives

This document explains the steps for initial setup and basic configuration of the MB5000. This document also provides troubleshooting information and detailed specifications.

Audience

This document is for the person installing and configuring the MB5000 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 a WWAN PC card.

1 Introduction

MB5000 is the most cost effective 3rd generation (3G) cellular solution for SMB, Small Office and Home Office (SOHO) Internet access and for Enterprise WAN back up. The products are simple to use and easily scalable. MB5000 is a 3G router based on our MobileBridge™ platform technology.

This guide will help you to know how to connect MB5000, set it up, and configure it to work.

The MB5000 comes with three different models:

- 1) The Red-Box (MB5000R), the only MB5000 model comes with built-in Wi-Fi capability

- 2) Kiosk Router (MB5000K), default DHCP/NAT enabled for always-on wireless Internet connection

- 3) Cellular Bridge (MB5000C), default in Bridge Mode, require a router or CPE to initiate PPPoE in order to establish the Internet connection.

2 Installing the MB5000

Installing the MB5000 is easy. Follow the quick steps below to power up your wireless network:

- Verify kit content;
- Write down product SN and MAC from back label;
- Power up the MB5000;
- Monitoring LED Indicators;
- Initialize the MB5000 unit

2.1 Verify Kit Contents

The MB5000 comes with three different models, only the RedBox MB5000R has built-in Wi-Fi and it is enabled by default. Wi-Fi is not available in both the Kiosk Router MB5000K and Cellular Bridge MB5000C.

1) The RedBox (MB5000R), this model comes with built-in Wi-Fi capability

2) Kiosk Router (MB5000K), DHCP/NAT is enabled by default for always-on wireless internet

3) CellBridge (MB5000C), Bridge Mode is enabled by default, which requires a router or CPE to initiate PPPoE in order to establish internet connectivity.

MB5000R kit includes the following components, similar to those depicted in Figure 2-1.

Figure2-1 MB5000R Kit Contents



MB5000R



Power Adaptor



CD



QIG For MB5000R

1. MB5000R router (Top View)
2. Power Adaptor
3. CD
4. QIG (Quick Installation Guide)

The MB5000K and MB5000C are available for OEM/ODM customers and are only intended for vertical and enterprise market. Thus they are available in bulk shipment only.

MB5000C/K kit includes the following components, similar to those depicted in Figure 2-2.

Figure2-2 **MB5000C/K Kit Contents**



1. MB5000C/K router (Top View)
2. Power Adaptor

2.2 Write Down Product Identification

Before you proceed with your MB5000 installation, please write down and keep the following MB5000 information on the MB5000 label:

- Serial Number
- MAC address

2.3 Power on the MB5000

Power on the MB5000 (refer to Figure 2-3).

Figure2-3 MB5000 Ports description



1. PC Card Slot
2. Reset Button
3. Reload Button
4. Ethernet LAN Interface (RJ45)
5. Console Port (RS232)
6. Power jack

The MB5000 power supply accepts any input AC voltage in the range of 100-240 VAC.

2.4 LED Indicators

MB5000 has four two-color LEDs to indicate the working status. The following table shows the status when the MB5000 is configured successfully and running properly.

Table 2-1 Normal LED Indications

	Power	WLAN	WWAN	Ethernet
Off	Power off	Disabled	Card inserted; No Internet connection	No cable
Green	Normal	Enabled	Card inserted; Internet connection established.	100Mbps mode
Green Blink	N/A	Enabled and data transmission	Card inserted; Internet connecting	100Mbps mode, with data transmission
Red	N/A	N/A	No card	10Mbps mode
Red Blink	N/A	N/A	N/A	10Mbps mode, with data transmission
Amber	System error	N/A	N/A	N/A
Amber Blink	System booting or Upgrading firmware	WLAN enabled with error.	N/A	N/A

2.5 Initialize the MB5000 Unit

1. Connect MB5000 with your computer, there are two ways to connect MB5000 with your computer:

- I. Connect your computer to MB5000 using an Ethernet cable or a hub and your computer is set with “Automatic IP” configuration.
- II. Alternatively, you can connect your computer to MB5000 with wireless LAN (available for MB5000R only).

- a) Enable the Wi-Fi interface in your laptop or PC. Make sure it is ready to work.
- b) Set your computer to “Automatic IP” configuration.
- c) Scan WLAN networks, and connect to the network named as the SN of MB5000,

2. Validate that your computer has got IP address from the MB5000, then open the web browser and enter <http://172.16.0.1>. Press Enter then the MB5000 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 2-5home page).

Figure2-4 login window

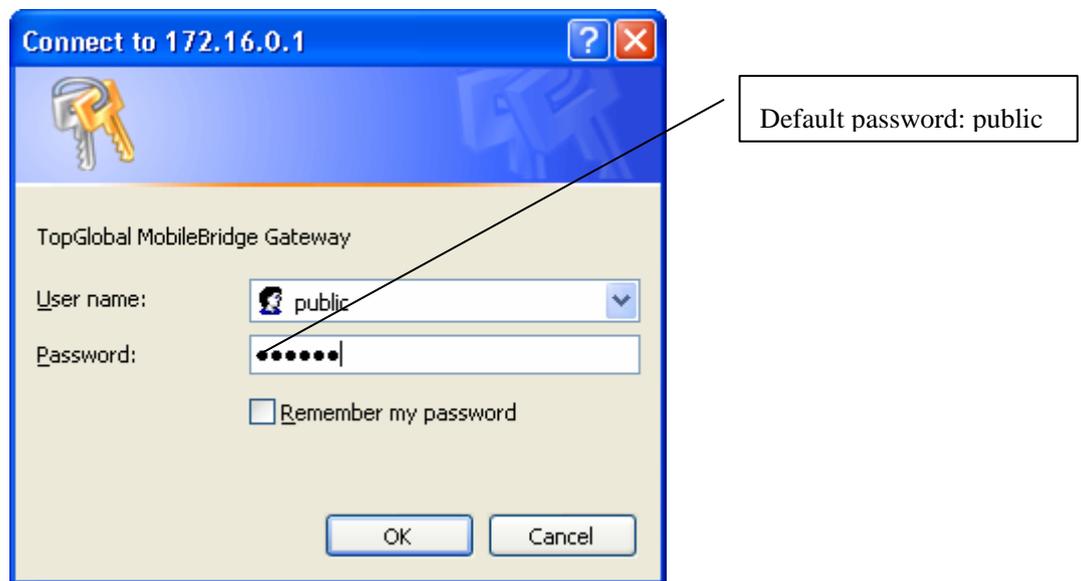


Figure2-5 home page

The screenshot shows the webGUI Configuration page for a TOP Global device. The page has a dark blue header with the TOP Global logo and the text 'Broadening Wireless Horizons'. Below the header is a navigation menu on the left with the following items: Wizard, System (Administration, Time, Firmware, Backup/Restore, Factory defaults), Interfaces (Local network, Internet access, Backup access, Wireless LAN), Services (Dynamic DNS, DHCP), Firewall (MAC Filter, Access rules, Port forwarding, DMZ), Security Services (Content Filter, Anti-Attack), Tools (PIN, PCMCIA, AT Command), and Status (Interfaces, Diagnostics). The main content area features a large TOP Global logo and a 'Basic information' table:

Basic information	
Product Model	MB5000R
SN	MA155G480115
Firmware Version	v1.1.26-1 Built on May 17 2007 13:05:35
Uptime	2 minutes, 30 seconds
WWAN Discription	Novatel Merlin C386 Card
Wireless WAN Signal Strength	
Wireless WAN Status	down Hint: wireless WAN has been set to manual mode. You can dial up/down by web page. (see the Status:Interface page)
LAN IP address	172.16.0.1

At the bottom of the page, there is a footer: MobileBridge is © 2004-2006 by TOPGlobal. All rights reserved.

If you want to do a quick installation, you can continue to read the content in this chapter. Otherwise, if you want to make a custom installation, please go to Chapter 3 directly.

3. Click “**Wizard**” on the home page. And click “Enter”. The “Step 1” page appears (Figure 2-6 Wizard - Basic Information).

Figure2-6 Wizard - Basic Information

Wizard: Basic Information

LAN address	<input type="text" value="172.16.0.1"/>	(e.g. 172.16.0.1)
LAN netmask	<input type="text" value="255.255.255.0"/>	(e.g. 255.255.255.0)
<input checked="" type="checkbox"/> Enable DHCP service on LAN interface		
Lease ranges from <input type="text" value="172.16.0.2"/> to <input type="text" value="172.16.0.100"/>		

Click Next to continue

You can change the IP of MB5000 or use the default values. Then click “Next”. Go to “Step 2” page (Figure 2-7 Wizard – Wireless LAN).

Figure2-7 **Wizard—Wireless LAN**

Wizard: Wireless LAN

Network name (SSID)	<input type="text" value="MA155G480115"/>
Network security	<input checked="" type="radio"/> Open network <input type="radio"/> WEP <input type="radio"/> WPA-PSK <ul style="list-style-type: none"> • Open network: Without any security, neither authentication nor encryption. • WEP: Using WEP to encrypt data under shared mode. • WPA-PSK: Using TKIP to encrypt data and authenticate peer with Pre-Shared key.
Network key	N/A

Click Next to continue

Back

Next

You can set the “Network name”, “Association Security” and related “Network Key” with the values you prefer. Then click “Next”, go to “Step 3” page (Figure 2-8 Wizard - Internet Access).

Figure2-8 **Wizard - Internet access**

Wizard: Internet access

Wireless WAN	
	<input checked="" type="checkbox"/> Enable this interface
Connect mode	<input checked="" type="radio"/> Auto <input type="radio"/> Dial on-demand <input type="radio"/> Manual <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.
Username	<input type="text" value="card"/>
Password	<input type="text" value="card"/>
Hardware descriptor	Sierra Wireless AirCard 555

Click Next to continue

Back

Next

Change “Card Status” to “Enable”, type correct “Phone Number”, “User Name” and “Password” (If you are using a GPRS/UMTS/EDGE network, you will need to input “CID”, “APN”), then click button “**Next**”, the following configuration page appears (Figure 2-9 Wizard - Finish).

Figure2-9 Wizard - Finish

Wizard: Finish

The Setup Wizard now has all the information necessary to complete your Gateway's network configuration.

If you need to change these settings in the future, you can either run the Setup Wizard again or use the sections of Setup to make individual changes.

Hostname:	MA155GFFFFFF
Local IP Address:	172.16.0.1
Local Subnet Mask:	255.255.0.0
Enable LAN DHCP:	Enabled
SSID used in wireless:	MA155G480115
Wireless security:	Open
Key for wireless:	N/A
Internet access type:	Wireless Internet access card
Enable wan interface:	Yes
Connect mode:	AUTO

Please click Submit to complete setup, and Gateway will restart automatically.

Back

Submit

Check the settings and click “Submit”, MB5000 will reboot automatically.

3 Management

3.1 Overview

MB5000 embeds a WEB server for WEB-based management. It is so-called webGUI in MB5000, as well as in this document. This section will illustrate how to visit MB5000's webGUI.

1. Open your browser and enter the MB5000's IP address in the address bar.
2. Press the **ENTER** key. The MB5000 **Login** dialog box appears.

Figure 3-1 **Login Dialog Box – English page**



Note:

Default user name: public

Default password: public

3. After you input the right username and password, the home page of MB5000 web site will appear (Figure 3-2).

Figure 3-2 MB5000's home page



Basic information	
Product Model	MB5000R
SN	MA155G480115
Firmware Version	v1.1.26-1 Built on May 17 2007 13:05:35
Uptime	12 minutes, 5 seconds
WWAN Discription	Novatel Merlin C386 Card
Wireless WAN Signal Strength	 Occur while dial-mode is set to manual
Wireless WAN Status	down Hint: wireless WAN has been set to manual mode. You can dial up/down by web page. (see the Status:Interface page)
LAN IP address	172.16.0.1

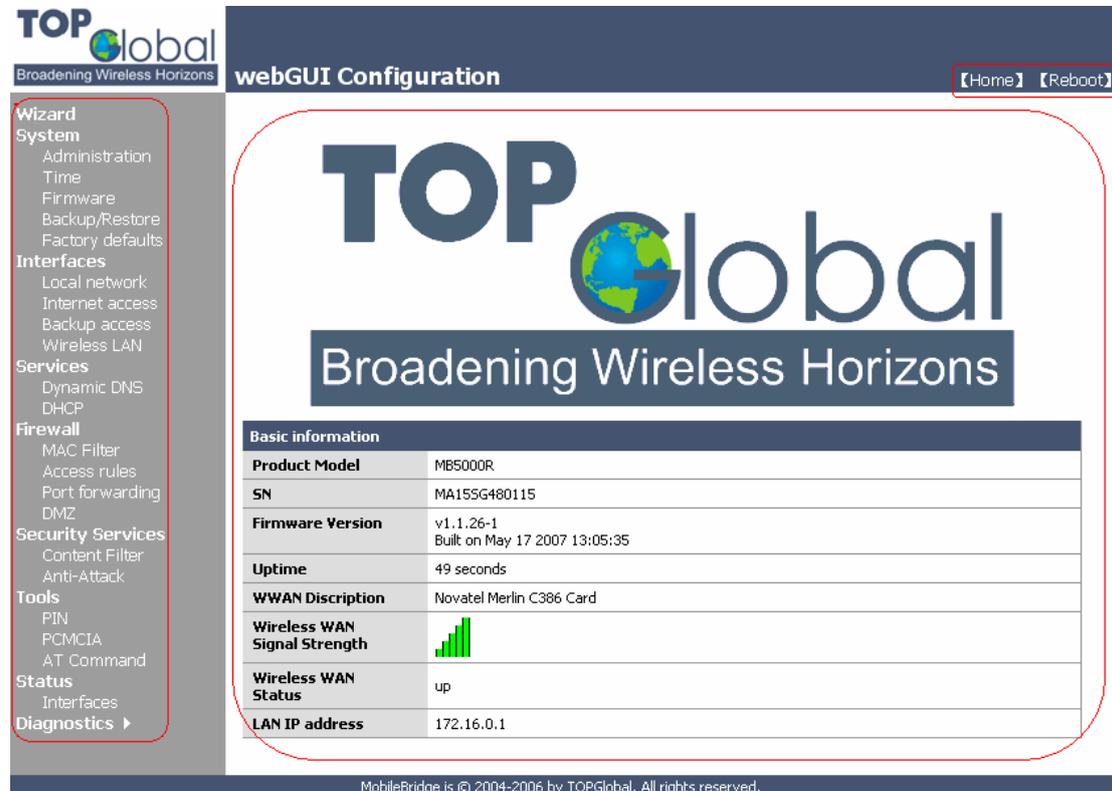
There are **nine** main categories on MB5000's web site:

- Wizard;
- System;
- Interfaces;
- Services
- Firewall;
- Security Services;
- Tools
- Status;
- Diagnostics.

The following sections will explain each of them in detail.

3.2 Page Structure

Figure 3-3 MB5000's home page



The screenshot shows the webGUI Configuration page for the MB5000. The page is divided into three main sections: a top header, a left sidebar, and a main content area. The header includes the TOP Global logo and the text 'webGUI Configuration'. The sidebar contains a navigation menu with the following categories: Wizard, System, Interfaces, Services, Firewall, Security Services, Tools, and Status. The main content area displays the TOP Global logo and a 'Basic information' table. The table contains the following data:

Basic information	
Product Model	MB5000R
SN	MA155G480115
Firmware Version	v1.1.26-1 Built on May 17 2007 13:05:35
Uptime	49 seconds
WWAN Discription	Novatel Merlin C386 Card
Wireless WAN Signal Strength	
Wireless WAN Status	up
LAN IP address	172.16.0.1

At the bottom of the page, there is a footer that reads: '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;
- Left menu space: display main 8 categories of the function menu for MB5000;
- 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 MB5000's home page

The screenshot shows the home page of the MB5000 device. At the top, there is a large logo for 'TOP Global' with the tagline 'Broadening Wireless Horizons'. Below the logo is a table titled 'Basic information' containing the following data:

Basic information	
Product Model	MB5000R
SN	MA155G480115
Firmware Version	v1.1.26-1 Built on May 17 2007 13:05:35
Uptime	48 seconds
WWAN Discription	Novatel Merlin C386 Card
Wireless WAN Signal Strength	
Wireless WAN Status	up Hint: wireless WAN has been set to manual mode. You can dial up/down by web page. (see the Status:Interface page)
LAN IP address	172.16.0.1

3.2.1.2 Reboot

Figure 3-5 Reboot system

The screenshot shows a confirmation dialog titled 'Reboot system'. The text asks: 'Are you sure you want to reboot the system?'. Below the text are two buttons: 'Yes' and 'No'.

The **Reboot** operation here will save all of the changed settings (if any) to the device before restarting the MB5000. Click the “Yes” button, the device will then reboot. During the reboot process, the power LEDs will blink with amber color for a while, and then turn green.



Note:

After configured all the parameters you need, reboot the MB5000. Then the new configurations will become effective.

Figure 3-6 *MB5000's restarting page*



3.3 Page Operation

- ✓ All of the MB5000 functions can be configured and become effective by going through the following 3 steps: page content editing → submit → reboot;
- ✓ Once every page is submitted, the system will confirm the page content, then notify the user to reboot the MB5000 to make the configuration effective;

3.4 Configuration Pages Description

3.4.1 System

There are five main categories in this setting:

- Administration
- Time
- Firmware
- Backup/Restore
- Factory defaults

3.4.1.1 Administration

Figure 3-7 Administration

System: Administration

General	
Hostname	<input type="text" value="MA155G480115"/> <small>Name of the gateway, without domain part e.g. mymb</small>
Serial Speed	<input type="text" value="115200bps"/>
ALG plugin	<input type="checkbox"/> SIP <input type="checkbox"/> H.323
Web Management Settings	
Username	<input type="text" value="public"/> <small>If you want to change the username for accessing the webGUI, enter it here.</small>
Password	<input type="password" value="....."/> <input type="password" value="....."/> (confirmation) <small>If you want to change the http password for accessing the webGUI, enter it here twice.</small>
webGUI protocol	<input checked="" type="radio"/> HTTP
webGUI port	<input type="text" value="80"/> <small>Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).</small> <input type="checkbox"/> Enable management from WAN, use port <input type="text" value="8080"/>
Advanced Management	
SNMP	<input type="checkbox"/> Enable SNMP Read-Only Community Name: <input type="text" value="public"/> ReadWrite Community Name: <input type="text" value="private"/> Trap Community Name: <input type="text" value="public"/> Trap Server : <input type="text"/> Trap interval : <input type="text" value="30"/> seconds
RCM	<input type="checkbox"/> Enable RCM RCM Server : <input type="text" value="rcm.topglobalusa.com"/> RCM Domain : <input type="text"/>

- **Host Name:** Up to 64 characters name to represent MB5000. The device default name is topglobalXXXXXX("XXXXXX" means the last 6 digits of SN)
- **Serial Speed:** When you need a backup link (for example, the v.90 modem) for MB5000, 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.
- **ALG plugin:** This technique relies on the installation of a new, enhanced Firewall/NAT - called an Application Layer Gateway. MB5000 provides two kinds of ALG plugin names SIP and H.323. When you choose either, you can plug the protocol.
- **Username:** Username for MB5000's web administration. The default username is public.
- **Password:** Password for MB5000's web administration. The default password is public.
- **webGUI Protocol:** The protocol web configuration used. HTTP is the only Current choice.
- **webGUI port:** The TCP port for HTTP. It is 80 by default. Generally, we don't suggest to modify this unless you have the knowledge about it. If you want to manage the MB5000 from the Internet, you may need to check the box for **Enable management from WAN**, and modify the TCP port number if needed.



Note:

Submit is not equal to keep the configuration information permanently in the device. User must reboot the system, and then the configuration will be saved. So if user saves the configuration, and doesn't reboot the device through the webGUI, all of the changed configurations information will be lost.

By default, MB5000 can't be configured through WAN interface for security consideration. If an user wishes to remotely configure the MB5000 through WAN interface, please check the checkbox "Enable management from WAN" to enable this feature.



Note:

Each time when the user modifies the username and password, you will be required to login again with the new username and password.

- **Enable SNMP:** It lets the administrator manage the MB5000 through the SNMP protocol. At the same time, you must specify the **Read-Only communicate Name** and **Read-Write communicate Name**, which enables the SNMP Manager to access MB5000 safely. Also, MB5000 supports sending trap information to a remote trap server to report the status of devices. To enable this function, you must specify the IP address of **Trap server** and **Trap interval**. The **Trap interval** indicates the frequency of the device for sending trap information to the server.
- **Enable RCM:** It makes MB5000 to be managed through RCM. You need to specify the RCM server's IP address or hostname and the domain. You can get this information from RCM administrator.

3.4.1.2 Time

Figure 3-8 Time

System: Time

Time	
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
Time setting	<input type="checkbox"/> Automatically synchronize with Internet time server Server <input type="text" value="207.46.130.100"/>

Submit

- **Time zone:** Current country time zone. You should check **Enable Daylight Saving Time** if implement DST(Daylight Save Time) in your country.
- **Time setting:** You can enable/disable synchronize local time with Internet time server by checking **Automatically synchronize with Internet time server**. The default value of the NTP server's IP address is 207.46.130.100, and this value can be changed as your requirement.

3.4.1.3 Firmware

Figure 3-9 Firmware

System: Firmware

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.

MB5000's firmware is upgraded through this tab. Follow these instructions:

1. Download the firmware from Top Global website www.topglobalusa.com to your host PC. You 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 then a pop up window for comparing the current version of firmware and the new version of the firmware to be upgraded will appear. Then you need to click on the OK button to confirm it.

Figure 3-10

System: Firmware

 The firmware has been uploaded and verified successfully.

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

Firmware file:

Current Version	v1.1.26-1
New Version	v1.1.26

Are you sure to upgrade the firmware?

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.



Note:

During the upgrade process, the Power LED is blinking with amber color. The device will be rebooted after the firmware upgrade is complete. After the firmware is upgraded successfully, you will need to restore all of the configurations to the factory defaults with the instructions in section 3.4.1.5 in this document.

3.4.1.4 Backup/Restore

Figure 3-11 Backup/Restore

System: Backup/restore

Backup configuration

Click this button to download the system configuration.

Download configuration

Restore configuration

Open a MobileBridge configuration file and click the button below to restore the configuration.

Note:
The gateway will reboot after restoring the configuration.

Upload configuration

Download Configurations: You can download current device configurations and save them in the local PC for later use.

Upload Configurations: You can use previous saved configurations to restore the device configuration to some previous configuration status. The process will change the current configurations with the previous one.



Note:

After upload configuration, the device will reboot automatically.

3.4.1.5 Factory Defaults

Figure 3-12 *Factory defaults*

System: Factory defaults

If you click "Yes", the gateway will be reset to factory defaults and will reboot immediately. The entire system configuration will be overwritten. The LAN IP address will be reset to 172.16.0.1, the system will be configured as a DHCP server, both the username and password will be set to 'public'.

Are you sure you want to proceed?

Click the **Yes** button to reset all configurations to their factory default values. After the firmware is upgraded, this process is needed.

3.4.2 Interfaces

There are three main categories in this setting:

- Local network
- Internet access
- Backup access
- Wireless LAN

3.4.2.1 Local Network

Figure 3-13 *Local network*

Interfaces: Local network

Static IP configuration	
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)

◆ Function Summary

The LAN interfaces are used to connect internal LAN and PCs in the LAN. The LAN interfaces include Wired LAN RJ45 interface and Wireless LAN interface. Wireless LAN interface is only available in MB5000R. MB5000K/C has no this interface.

◆ Detailed Configurations

- ✓ Static IP Configuration
 - **IP Address:** The IP Address of the LAN & WLAN on MB5000. The default IP address is 172.16.0.1.
 - **Netmask:** The subnet mask of the LAN & WLAN. The default subnet mask is 255.255.255.0.

3.4.2.2 Internet Access

Figure 3-14 MB5000's Initiating page

Interfaces: Internet access

Initiating Hardware ...



MB5000's Initiating page will appear and this page refreshes every 3 seconds. If the SIM card of your WWAN supports PIN function, it will redirect you to the **PIN:Authentication** page after the initiating process finished.

Figure 3-15 PIN:Authentication

PIN: Authenticate

Welcome to use MB5000R

PIN Code

Save PIN code

Hint:
Your PIN Code prevents unauthorized users from connecting to the Internet. If wrong PIN is inputted thrice (continually), the SIM will be locked, and you must use PUK to unlock it .

Input the correct PIN Code and click **Enter**, **Internet access** page will appear. Check the box **Save PIN Code** if you want MB5000 to save the PIN Code you enter.



Note:

Only after you pass the PIN authentication can you login the **Internet access** page or the PIN management pages. The process of how to configure PIN will be described in **3.4.6 Tools**.

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.

Figure 3-16 Internet Access

Interfaces: Internet access

Enable this interface

Hardware					
Name:	Novatel Merlin C386 Card				
Manufactory:	QUALCOMM, Incorporated				
Product:	Model 100				
SW:	F/W VER: 127 S/W VER: DP3.3.20				
Singal strength:	Good (31) Hint: Good:31-24,Normal:23-16,Poor:15-8,Bad:7-1,Invalid:0				
PIN:	<input checked="" type="checkbox"/> Automatically authenticate with the saved pincode when device startup.				
Modem:	<table border="1"> <tr> <td>Phone number</td> <td><input type="text" value="#777"/></td> </tr> <tr> <td>Init string</td> <td><input type="text"/></td> </tr> </table>	Phone number	<input type="text" value="#777"/>	Init string	<input type="text"/>
Phone 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 empty means not to special MRU of PPP.
MTU	<input type="text"/> Hint: Leaving it empty means not to special MTU of PPP.
DNS	<input checked="" type="checkbox"/> Obtain DNS server address automatically DNS Server: <input type="text"/>
Username	<input type="text" value="card"/>
Password	<input type="text" value="card"/>

Networking	
Connect mode	<input type="text" value="Auto"/> <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.(see the Status:Interface page) • Bridge with LAN: As a PPPOE modem and the device connected to LAN of MobileBridge can use PPPOE to use WWAN. • Bridge with Serial: As a lease modem and the device connected to serial port of MobileBridge can use async PPP to use WWAN.
Keepalive	<input checked="" type="checkbox"/> Enable keepalive Interval with <input type="text" value="15"/> seconds Reset Modem After redialing <input type="text" value="3"/> times. Reboot System After resetting modem <input type="text" value="3"/> times.

◆ Function Summary

The WAN interface of MB5000 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:** Indicates which wireless WAN connection policy is used.
 - **Auto:** MB5000 will connect to the Internet automatically when it is powered up. It keeps MB5000 always connected to the Internet, even when the connection is idle.
 - **Dial-On-Demand:** When Connect mode is set to Dial-On-Demand, MB5000 will disable Keepalive automatically.

Figure 3-17 **Dial-On-Demand**

Connect mode	Dial on-demand <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.(see the Status:Interface page) ● Bridge with LAN: As a PPPOE modem and the device connected to LAN of MobileBridge can use PPPOE to use WWAN. ● Bridge with Serial: As a lease modem and the device connected to serial port of MobileBridge can use async PPP to use WWAN. Disconnect if no data packets sent or received for <input type="text" value="300"/> seconds
---------------------	--

MB5000 can be configured to 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 MB5000 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 MB5000 will not make the internet connection when you power up the MB5000. You must manually make the Cellular connection using the web configuration page.

- **Bridged with LAN:** When this type is selected, the MB5000 acts as a modem between the cellular network and client device (PC or handheld or others) which attached to the MB5000 by Wi-Fi or wired-Ethernet. By this mode, the MB5000 only supports one client device. The MB5000 will initiate the PCMCIA card after startup and be ready for the client device to dial up to the cellular network using PPPoE. User needs to configure the right username and password in the PPPoE client. For the CDMA 1X/EVDO data card, username/password should be card/card; for the WCDMA/HSDPA data card, username/password will be different from different cellular Operators, please check with your cellular service provider.

Connect mode	Bridged with LAN <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.(see the Status:Interface page) ● Bridge with LAN: As a PPPOE modem and the device connected to LAN of MobileBridge can use PPPOE to use WWAN. ● Bridge with Serial: As a lease modem and the device connected to serial port of MobileBridge can use async PPP to use WWAN.
---------------------	---

- Bridged with Serial:** When this type selected, the MB5000 acts as a modem between the cellular network and the serial port. You can attach a DTE device such as Cisco router or PC with the serial cable, and then initiate a PPP procedure on the client device.

Note: MB5000 can connect the 3G modem automatically when received a PPP connection request from a DTE device and disconnect it when received a PPP termination. This mode also support auto disconnect like dial on demand. Make sure the MB5000's serial speed is match with the modem. (refer to "3.4.1.1 administration" of this guide for the detail about how to set the serial speed)

Connect mode	Bridged with Serial ▼ <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.(see the Status:Interface page) Bridge with LAN: As a PPPOE modem and the device connected to LAN of MobileBridge can use PPPOE to use WWAN. Bridge with Serial: As a lease modem and the device connected to serial port of MobileBridge can use async PPP to use WWAN. <p style="text-align: right;">Disconnect if no data packets sent or received for <input type="text" value="300"/> seconds</p>
---------------------	---

- Keepalive:** This can detect whether the WWAN connection is in good status. When the WWAN connection is abnormal, keepalive module will detect it if keepalive is enabled 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. Check the box to enable the Keep-Alive feature. If the Keep-Alive is enabled, MB5000 will detect the Internet connection health periodically with the interval specified. Once it detects the Internet connection goes down, it will try to connect again. It will try to re-connect several times (3 times by default). If all of the attempts fail, MB5000 will reset the 3G data card modem. If still no help, MB5000 will reboot itself after several attempts (3 times by default) fail.

Keepalive	<input checked="" type="checkbox"/> Enable keepalive Interval with <input type="text" value="15"/> seconds Reset Modem After redialing <input type="text" value="3"/> times. Reboot System After resetting modem <input type="text" value="3"/> times.
------------------	---

- 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 the wireless WAN card connects to a GRPS network, it is different from the type of the CDMA. The parameters to be configured are as shown as *Figure 3-18* and *Figure 3-19*.

Figure 3-18 An example username and password setting for Cingular GPRS network

Username	ISP@CINGULARGPRS.COM
Password	CINGULAR1

This is the type of the CDMA wireless wan card to configure:

Figure 3-19

Username	card
Password	card

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

- **Card model:** When a cellular PC Card is inserted into the MB5000 correctly, it will automatically detect the WAN card type. If the 3G data card is supported and recognized by the MB5000, the name and model of the wireless WAN card will be listed here. Please contact Top Global for a list of all supported 3G data cards.
- **Signal strength:** Indicates the current cellular network's signal strength. Value 31 is the best signal strength indication. The less value, the worse signal strength. If this value is 0, you do not have a signal, please check the wireless WAN card carefully to make sure it is inserted correctly and you may need to call your mobile operator to make sure your area is covered within their network;
- **Modem:** If **Enable custom parameters** is checked, the parameters to be configured are as shown as *Figure 3-20*.

Figure 3-20

Modem: Customize

Phone number	#777
Init string	AT&F

Phone Number: Provide a phone number for wireless WAN modem;

Init string: Provide an initializing string for wireless WAN modem.

If the wireless card type is GPRS, UMTS or EDGE, more parameters are to be configured.

Shown as follows:

Figure 3-21 **Wireless - basic**

Modem: Customize

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.
- **PDP Address:** A string parameter that identifies the MB5000 in the address space applicable to the PDP.

● **Advanced Settings for PPP dialing**

MRU	<input type="text"/> Hint: Leaving it empty means not to special MRU of PPP.
MTU	<input type="text"/> Hint: Leaving it empty means not to special MTU of PPP.
DNS	<input checked="" type="checkbox"/> Obtain DNS server address automatically DNS Server: <input type="text"/>

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 your operator.

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

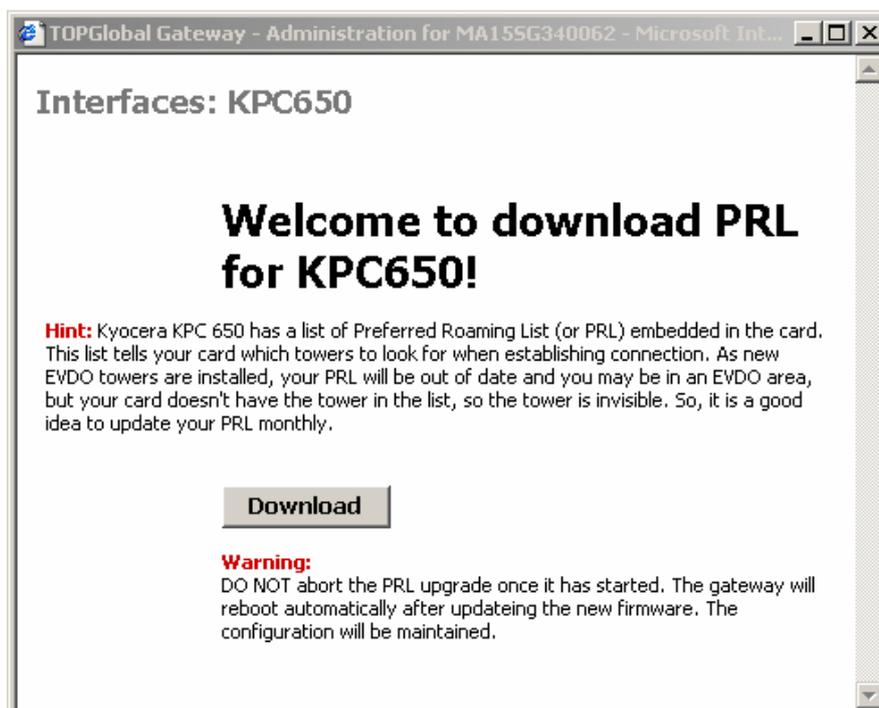
- **PIN:** This function appears only when the SIM card of your WWAN card supports PIN function.

If **Automatically authenticate with the saved PIN code when device startup** is checked, MB5000 will save the PIN code automatically and you needn't to input the PIN again next time you startup MB5000.

Aware that this function can only be effective when you have already saved the PIN.

- **Download PRL:** The first time when you use a KPC650 data card, you may need to activate it and download the latest PRL (Preferred Roaming List) step by step. The PRL contains the latest addition of EVDO sites and can enable you to roam and use these new sites:

1. Change the **connect mode** to **Manual** on the Internet access page of MB5000, then reboot the system to make this change become effective. So that MB5000 will not start to dial-up when startup.
2. Click "**download PRL**" button on the Internet access page. The following page will pop-up.



3. Click “**download**” button on the Internet access page. There will be a result page return to show whether this process is success or failure.
4. Reboot the MB5000 if it has download PRL successfully.

3.4.2.3 Backup access

Figure 3-22 Backup access

Interfaces: Backup access

Enable Backup interface

ISP Dial Number	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

The 3G Phoebus MB5000 supports v.90 modem for the WAN backup link. When the WWAN is unavailable or is down, the backup link will automatically dial up.

ISP Dial Number. The dialing number to dial up to the ISP’s network. You may contact your ISP for that.

Username: The username for authentication during the PPP negotiation period.

Password: The password for authentication during the PPP negotiation period.

Note:

The backup link requires a special cable to connect MB5000 and the V.90 modem. You may contact the retailers or Top Global sales to obtain that.

3.4.2.4 Wireless LAN

There are three main tabs in this setting:

- Basic
- Advanced
- Access Control

3.4.2.4.1 Basic

Figure 3-23 Wireless - basic

Interfaces: Wireless LAN Basic **Advanced** Access Control

Enable wireless LAN radio

Network name (SSID)	<input type="text" value="MA15SGFFFFFF"/> <input checked="" type="checkbox"/> Enable broadcast SSID .
Wireless channel	<input type="text" value="6- 2.437 GHz"/>
Network mode	<input type="text" value="Mixed"/> <ul style="list-style-type: none"> Mixed: both 802.11g and 802.11b mode wireless stations will be allowed on the network. g-only: this ensures that 802.11g mode wireless stations will connect at high speed, but 802.11b mode wireless stations will be unable to connect at all. b-only: 802.11g mode wireless stations will be unavailable.
STAs isolation	<input type="text" value="Disabled"/> <p>When enabled, STAs associated with the MobileBridge will not be able to communicate with each other.</p>
MAX associations	<input type="text" value="128"/>

◆ Function Summary

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

◆ Detailed configurations

Enable Wireless radio: If this box is not checked, no other parameters in this page are available;

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;

Enable SSID Broadcast: When wireless clients survey the local area for wireless networks, they will detect the SSID broadcast by the Router. To broadcast MB5000's SSID, keep the default setting checked. If you do not want to broadcast MB5000's SSID, then select Disable;

Wireless Channel: Select the appropriate channel from the list provided to correspond with your network settings. All client devices in your wireless network must be broadcast on the same channel in order to function correctly;

Network Mode: From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-g and Wireless-b devices in your network, you can keep the default setting as **Mix**. If you have only Wireless-g devices, select **g-Only**. If you have only Wireless-b devices, select **b-Only**;

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

Max associations: The number of maximum client stations allowed to associate with the MB5000.

3.4.2.4.2 Advanced

Figure 3-24 Wireless – advanced

Interfaces: Wireless LAN

Basic
Advanced
Access Control

Association

Network Authentication	<input type="text" value="Open"/>
Data encryption	<input type="text" value="Disabled"/>

Network key

PSK(Only for WPA-PSK)	<input type="text"/>
Key index(for transmit)	<input type="text" value="Key 1"/>
Hint: The following input must be 5 or 13 ascii characters, or 10 or 26 hexadecimal characters .	
Key 1	<input type="text"/>
Key 2	<input type="text"/>
Key 3	<input type="text"/>
Key 4	<input type="text"/>

◆ Function Summary

This configuration page is used to set wireless LAN security parameters. MB5000 supports two different types of security settings for your wireless LAN network: Wi-Fi Protected Access (WPA) Pre-Shared key (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.

You can also configure the MB5000 as other security mode to be compatible for other station security settings. Such as:

Mode 1: no security, no authentication

Network Authentication: OPEN

Data Encryption: Disabled

Mode 2: enable security, no authentication

Network Authentication: OPEN

Data Encryption: WEP

Mode 3: no security, enable authentication

Network Authentication: Shared

Data Encryption: Disabled

Disable: Indicates no access control function, allow all of the stations connect to MB5000;

Allow: Indicates only allow the stations which have the MAC addresses listed in the table to access the MB5000;

Deny: Indicates only deny the stations which have the MAC addresses listed in the table to access the MB5000;

Stations connected: In order to add the ACL conveniently, the MAC addresses of stations which have been already connected to MB5000 appear in this domain. Click the **Refresh** button, this list will be updated.

Access Control List: The MAC addresses of stations which have been allowed or denied to connect to MB5000 are saved in this list box.

There are 2 methods to input the MAC address: one is to select the station item in the Station Connected list, then click **Add**; the other is to input the station MAC address through MAC address edit box on the page (below the ACL), the input MAC address format must be XX:XX:XX:XX:XX:XX.



Note:

Don't forget to click **Save** button to save the settings.

3.4.3 Service

There are two main categories in this setting:

- Dynamic DNS
- DHCP

3.4.3.1 Dynamic DNS

Figure 3-26 Dynamic DNS

Network: Dynamic DNS

Enable Dynamic DNS update when WAN up

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

MB5000 supports dynamic DNS (DDNS). The default status for DDNS is disabled. By far, MB5000 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 wireless WAN's IP changed, the router will register the new public IP address obtained from the PPP negotiation to the provider.

3.4.3.2 DHCP

Figure 3-27 DHCP

Enable DHCP service

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.	

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

MAC address	IP address	Description
172.16.0.108	00:11:50:10:D3:82	

⊖ ⊗
⊕

■ DHCP Configuration

This setting is used to configure MB5000's Dynamic Host Configuration Protocol (DHCP) server function. MB5000 can be used as a DHCP server for the internal LAN network. The DHCP server automatically assigns an IP address to each computer in the LAN network. If you choose to enable MB5000's DHCP server option, you must configure all of PCs in the LAN network to connect to this DHCP server (MB5000), and make sure there is no other DHCP server on your network.

DHCP is enabled by factory default. If there is already a DHCP server in the LAN network or a DHCP server is not necessary for the LAN network, the **Enable DHCP Server on LAN Interface** can be un-checked. (Other DHCP features will be disabled).

- **Range:** Enter the values for start IP address and end IP address, the default start IP address is 172.16.0.2 and the default end IP address is 172.16.0.100.
- **Lease Time:** The amount of time in second a network user will be allowed to connect to MB5000 with their current dynamic IP address got from the DHCP server. When the time is up, the user will be automatically assigned a new dynamic IP address. The default is 86400 seconds, which means one day.



Note:

When the DHCP server's IP address range is set, it must be assured that there is no other device in the network to use the IP address located in this address range, such as printer server, file server, etc. Otherwise there is a risk for address conflict.

■ Advanced settings

✓ **Static IP address assignment for DHCP clients:**

You can specify the static IP address for the known DHCP clients. The router will assign the IP address you configured on the list to these clients.

1. Click  to add a new entry for the static IP assignment.

Services: DHCP

IP Address	<input type="text" value="172.16.0.109"/>
HW Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/>
Description	<input type="text" value="Sample"/> You may enter a description here for your reference (not parsed).

You should NOT assign the IP address within the *Range* field configured on the main DHCP page in order to avoiding the IP address confliction.

2. Click  to edit an existing entry.

3. Click  to delete an existing entry.
 4. Save the configuration and reboot to take them effect by clicking the *Reboot* button on the web page.
- ✓ **Deny unknown clients:**
- With this box checked the wired and wireless clients that NOT on the static IP assignment list will not be able to obtain the IP address from the router by DHCP request.

3.4.4 Firewall

There are four main categories in this setting:

- MAC Filter
- Access rules
- Port forwarding
- DMZ

3.4.4.1 MAC Filter

Figure 3-28 MAC Filter

Mode

MAC Filter Mode

Disable
 Allow
 Deny

- Disable: Disable MAC Filter.
- Allow: Only allow MACs within the MAC List.
- Deny: Only deny MACs within the MAC list.

MAC Filter List

ARP Cache	Actions	MAC Filter List (MFL)
<div style="border: 1px solid #ccc; min-height: 40px; margin-bottom: 5px;">00:D0:B7:91:B5:05</div> <div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Refresh"/></div>	<input type="button" value="Add >>"/>	<div style="border: 1px solid #ccc; min-height: 40px; margin-bottom: 5px;">00:D0:B7:91:B5:05</div> <div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Remove"/></div> <div style="display: flex; justify-content: space-between; align-items: center;"> <input style="width: 80%; border: 1px solid #ccc;" type="text"/> <input type="button" value="New"/> </div> <p style="font-size: small; margin-top: 5px;">e.g. 12:23:45:78:9a:bc</p>

◆ 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:**
 - ◆ Disable means no MAC Filter is implemented
 - ◆ 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.

- **ARP Cache:** MB5000 collects the MAC address information of all the hosts that communicated with MB5000 and displays the information here. You can easily add the MAC addresses you select to the MAC Filter List by click the **Add** button. You can refresh the ARP cache by click the **Refresh** button.
- **Access Control List:** This is the MAC address list of all the selected hosts. You can add items with two methods: Select from the ARP Cache or type the MAC address manually in the MAC address edit box on the lower right hand side.



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 MB5000 via Wireless LAN.

3.4.4.2 Access rules

Figure 3-29 Access Rules

Firewall: Access Rules

Apply Change

Action when no rules matched: Block Pass

Source	Destination	Service	Action	Enable	Configure
--------	-------------	---------	--------	--------	-----------

Add Defaults

◆ Function Summary

Access Rules is one of the most important functions of MB5000's firewall. Access Rules utilize stateful package filter technology. All the access rules in firewall are set here.

◆ Detailed Configurations

The access rules of the firewall in MB5000 have many access rule items. You can maintain these rules with the operations of: Add, Delete, Move up, Move down, Apply.

- **Default Policy:** Factory default rules;
- **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 3-30 Access Rules

Firewall: Access Rules

Action	Block <input type="button" value="v"/>
Service	Custom <input type="button" value="v"/> Protocol: TCP <input type="button" value="v"/> Port Range: <input type="text"/> - <input type="text"/>
Source	Interface: LAN <input type="button" value="v"/> Address: Host <input type="button" value="v"/> <input type="text"/> / <input type="button" value="v"/>
Destination	Interface: WAN <input type="button" value="v"/> Address: Host <input type="button" value="v"/> <input type="text"/> / <input type="button" value="v"/>
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

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

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

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

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

3.4.4.3 Port forwarding

Figure 3-31 Port forwarding

Firewall: Port Forwarding

Apply Change

Interface	Protocol	Ext. port	NAT ip	Int. port	Enable	Configure

Add Defaults

◆ 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 MB5000 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 3-32 **Port forwarding**

Firewall: 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="TCP/UDP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> 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. <i>172.16.0.3</i>
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	<input type="checkbox"/> 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 MB5000 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. Possible protocols are: TCP, UDP, TCP/UDP;

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

NAT 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 MB5000 will enable this forward automatically;

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

3.4.4.4 DMZ

Figure 3-33 DMZ

Firewall: DMZ

Enable DMZ

LAN Host

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

When *DMZ* is enabled, you should assign a LAN host's IP address to MB5000. Then MB5000 will forward all incoming traffic from the WWAN interface to this client host. It will be useful when you want to access a client host of LAN from Internet. .

- LAN Host: Client's IP address.

3.4.5 Security Services

There are two main categories in this setting:

- Content Filter
- Anti-Attack

3.4.5.1 Content Filter

Figure 3-34 **Content Filter**

Security Services: Content Filter

Apply filter and Restrict Web Features on: LAN

Content Filter

Configure

Restrict WEB Features

ActiveX Java Cookies Access to HTTP proxy Servers

Don't block Java/ActiveX/Cookies to Trusted Domain sites

Trusted Domains

Trusted Domain

Edit

Delete

DeleteAll

Submit

◆ Function Summary

Content Filter is an advance security feature; it can filter the HTTP sessions according to the contents.

◆ Detailed Configurations

Content Filter includes URL filter list and WEB features restriction. The default configuration of content filter is off. You can enable it by check the box “*Apply filter and Restrict Web Features on*: LAN”, then click the button **Submit**

- **Configure:** Click the button **Configure** to define the URL filter list:

Figure 3-35 **URL Filter**

Security Services: Filter

- Enable Allowed/Forbidden Domains
- Disable all web traffic except for Allowed Domains

Allowed Domains	Move	Forbidden Domains
	<input type="button" value="<<"/> <input type="button" value=">>"/>	
<input type="button" value="Delete"/> <input type="button" value="DeleteAll"/> <input type="text"/> <input type="button" value="Edit"/>		<input type="button" value="Delete"/> <input type="button" value="DeleteAll"/> <input type="text"/> <input type="button" value="Edit"/>
<input type="button" value="Submit"/>		

Enable Allowed/Forbidden Domains: Indicates enable URL Filter or not;

Disable All web traffic expect for Allowed Domains: Indicates URL Filter mode. URL Filter has two modes: Allow means to allow the URL in the Allowed Domains only; Forbidden means to forbid the URL in the Forbidden Domains only. Checking this checkbox means the “allow” mode is adopted.

3.4.5.2 Anti-Attack

Figure 3-36 Anti-Attack

Security Services: Anti-Attack

Enable Anti-Attack

Denial of Service (DoS)	<input checked="" type="checkbox"/> Ping of Death <input checked="" type="checkbox"/> Land <input checked="" type="checkbox"/> Smurf <input checked="" type="checkbox"/> SYN Flood <input checked="" type="checkbox"/> Fraggle
Stateful Packet Inspect (SPI)	<input checked="" type="checkbox"/> Enable
IP Spoofing	<input type="checkbox"/> Enable

Submit

◆ Function Summary

Anti-Attack function can block the attack from LAN/WAN and the stateful packet inspect (SPI). MB5000 can block the following attacks:

DoS: Ping of Death, Land, Smurf, SYN Flood, Fraggle;

IP Spoofing.

◆ Detailed Configurations

Enable Anti-Attack: Check this checkbox to enable the Anti-Attack function. Select the attack you want to block after you enabled the Anti-Attack function.

3.4.6 Tools

There are three main categories in this setting:

- PIN
- PCMCIA
- AT command



Note:

Before you setup PIN, please make sure the Wireless WAN is disabled; otherwise it may cause input errors. Notice that every time you change the configuration of PIN, you must reboot the devices to make it become effective.

3.4.6.1 PIN

There are three main tabs in this setting:

- Enable/Disable
- Change PIN
- Renew PIN

3.4.6.1.1 Enable/Disable

Figure 3-37 *Enable/Disable*

Tools: PIN

Enable/Disable
Change PIN
Renew PIN

Enable/Disable PIN	
Current Status	Disabled
PIN Code	<input style="width: 100%;" type="text"/>

Enable

Hint:
Your PIN Code prevents unauthorized users from connecting to the Internet. If wrong PIN is inputted thrice(continually), the SIM will be locked, and you must use PUK to unlock it .

◆ Function Summary

This configuration page is set to Enable/Disable the function of PIN protection.

◆ Detailed Configurations

The PIN Code can prevent the unauthorized user from connecting to the Internet.

Put the Pin Code in and click **Enable** button to enable this function. The default Pin Code is 1234, and the PIN Code must be 4 characters long.

3.4.6.1.2 Change PIN

Figure 3-38 Change PIN

Tools: PIN **Enable/Disable** **Change PIN** **Renew PIN**

Change PIN

PIN Code	<input type="text"/>
New PIN Code	<input type="text"/>
	<input type="text"/> (confirmation)

Change

Hint:
Your PIN Code prevents unauthorized users from connecting to the Internet. If wrong PIN input thrice(continually), the SIM will be locked, and you must use PUK to unlock it .

◆ Function Summary

This configuration page is set to change the PIN code.

◆ Detailed Configurations

Put in the former Pin Code and new one twice, click the **Change** button. Notice that if wrong PIN Code was put in thrice (continually), the SIM will be locked.

3.4.6.1.3 Renew PIN

Figure 3-39 Renew PIN

Tools: PIN Enable/Disable Change PIN Renew PIN

Renew PIN	
PUK Code	<input type="text"/>
New PIN Code	<input type="text"/>

Renew

Hint:
Your PIN Code prevents unauthorized users from connecting to the Internet. If wrong PIN input thrice(continually), the SIM will be locked, and you must use PUK to unlock it .

◆ Function Summary

This configuration page is set to renew PIN Code when the SIM is locked.

◆ Detailed Configurations

Put in the PUK and new PIN Code, click **Renew** button, then the PIN Code will be unlocked and the former PIN Code is changed to a new one.

Aware if you disable PIN, you can't change or renew PIN and error messages will appear.

Figure 3-40

Tools: PIN
Enable/Disable
Change PIN
Renew PIN

The following input errors were detected:

- **Your SIM card has disabled PIN protection.**

Change PIN

PIN Code	<input type="text"/>
New PIN Code	<input type="text"/>
	<input type="text"/> (confirmation)

Change

Hint:
Your PIN Code prevents unauthorized users from connecting to the Internet. If wrong PIN input thrice(continually), the SIM will be locked, and you must use PUK to unlock it .

3.4.6.2 PCMCIA

Figure 3-41 PCMCIA

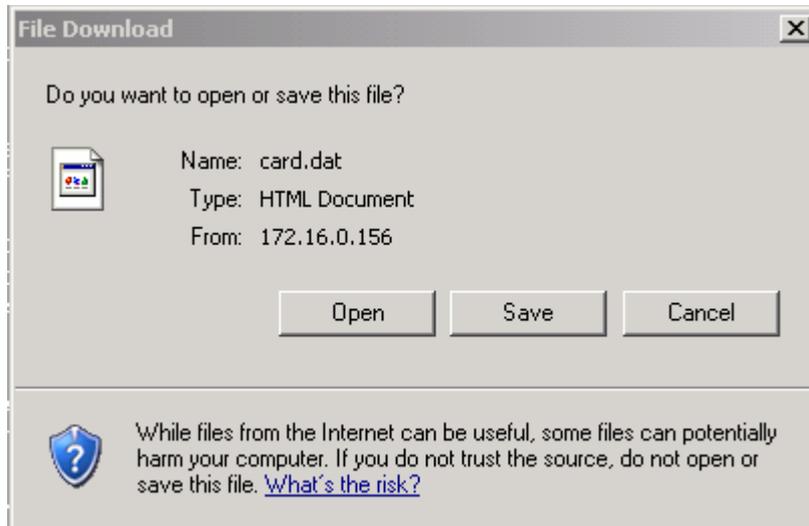
Tools: PCMCIA

Status	Socket 0: 5V 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

export

PCMCIA page displays the hardware information of the wireless WAN card. Click the **export** button, the File Download will appear (Figure 3-42).

Figure 3-42



Then click the **Save** button, you can export the hardware information to local host.

3.4.6.3AT Command

Figure 3-43 AT Command

Tools: AT Command

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

AT Command function is provided to the advanced users to diagnostic the wireless WAN card or the V.90 modem connected by the serial cable. Select a target device from the drop-down menu in the **Port** field. Input the AT commands in the “**Command**” field. Click the **Execute** button to send the AT commands to the target and then the result will be seen in the **Output** filed.



Note:

1. The AT commands CANNOT be sent to the target device before you make it disconnected from the Internet.
2. You should be aware clearly about the AT commands before you do that.

3.4.7 Status

There is one category in this setting:

- Interfaces

3.4.7.1 Interfaces

This tab displays the current information of LAN interface, as well as the WAN interface.

Figure 3-44 **Interfaces**

Status: Interfaces

WAN interface#0 Wireless WAN	
Status	Down
UP Time	0 seconds
IP Address	0.0.0.0
Network Mask	0.0.0.0
In/out packets	0/0(0/0)

WAN interface#1 Dialer on V.90 Modem	
Status	Down
UP Time	0 seconds
IP Address	0.0.0.0
Network Mask	0.0.0.0
In/out packets	0/0(0/0)

LAN interface	
Status	Up
MAC address	00:0B:89:10:00:76
IP address	172.16.0.1
Subnet mask	255.255.255.0
In/out packets	2544/1101(298.1KB/612.7KB)
In/out errors	0/0
Collisions	0

◆ Function Summary

The interfaces' status displays all the network interfaces information of MB5000. You can also do the dial up and hang off WAN connection here.

◆ Detailed information:

WAN Interface#0: This block shows the information of Wireless WAN data card inserted in MB5000. The **Status** field shows whether the wireless WAN card has dialed up to the Internet. Or if no data card exists, it will inform “*No data card was found.*”. When a data card is inserted and the “**Connect Mode**” on the “**Internet Access**” page is set to “**Manual**”, the information about this interface will be displayed as below:

WAN interface#0 Wireless WAN	
Status	Down <input type="button" value="Connect"/>
UP Time	0 seconds
IP Address	0.0.0.0
Network Mask	0.0.0.0
In/out packets	0/0(0/0)

The status field shows the current status of the cellular wireless WAN card. Users can click the button **Connect/Disconnect** to do dial up and hang off.

The **Up Time** field shows how long in second that this interface has been connected to the Internet since last dialing up.

The **IP Address** field and the **Network Mask** field shows the IP address and the subnet mask that the interface obtained from the PPP dialing negotiation.

The “**In/out packets**” field shows how many packets have been passed through this interface since the last dialing up.

WAN interface#1: This block shows the information on the interface of the serial modem. The meaning for each field is same as the former ones.

LAN interface: This block shows the information on the LAN interface.

3.4.8 Diagnostics

There are two main categories in this setting:

- System logs
- DHCP leases

3.4.8.1 System Logs

There are two main tabs in this setting:

- Logs of System
- Settings

3.4.8.1.1 System Log

Figure 3-45 System logs

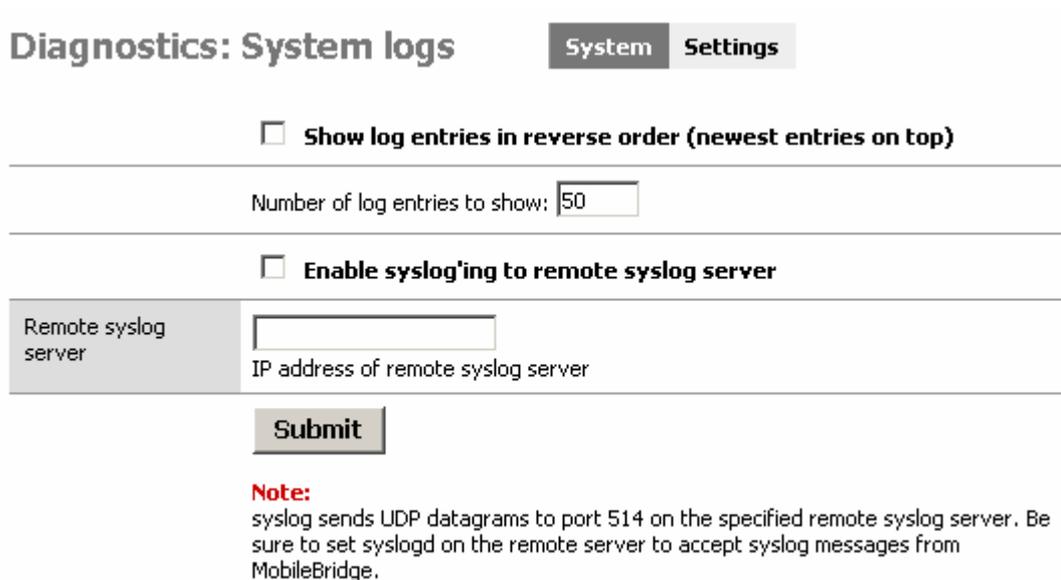
Diagnostics: System logs	
	System Settings
Last 50 system log entries	
Jan 1 00:00:01	syslogd started: BusyBox v0.60.0 (2006.01.04-10:53+0000)
Jan 1 00:00:01	cardmgr[14]: watching 1 socket
Jan 1 00:00:01	cardmgr[16]: socket 0: Sierra Wireless AirCard 555
Jan 1 00:00:01	cardmgr[16]: executing: 'modprobe serial_cs 2>&1'
Jan 1 00:00:02	udhcpd: udhcp server (v0.9.8) started
Jan 1 00:00:02	dnsmasq[37]: started, version 1.10 cachesize 150
Jan 1 00:00:02	dnsmasq[37]: failed to drop root privs
Jan 1 00:00:02	dnsmasq[37]: cleared cache
Jan 1 00:00:02	dnsmasq[37]: reading /tmp/resolv.conf
Jan 1 00:02:30	pppd[97]: pppd 2.4.1 started by root, uid 0
Jan 1 00:02:30	pppd[97]: Serial connection established.
Jan 1 00:02:30	pppd[97]: Using interface ppp0
Jan 1 00:02:35	pppd[97]: Remote message: ^@
Jan 1 00:02:35	pppd[97]: local IP address 220.207.75.175
Jan 1 00:02:36	dnsmasq[37]: cleared cache
Jan 1 00:02:46	pppd[97]: Received bad configure-nak/rej: 12 06 00 00 00 01
Jan 1 00:02:50	pppd[97]: Hangup (SIGHUP)
Jan 1 00:02:50	pppd[97]: Connection terminated.
Jan 1 00:02:50	dnsmasq[37]: cleared cache
Jan 1 00:02:54	pppd[97]: Serial link disconnected.

◆ Function Summary

The System Log displays a list of the most recent activities that have taken place on MB5000. The **System** tab shows the latest 50 system log entries.

3.4.8.1.2 Settings

Figure 3-46 System log settings



Diagnostics: System logs System Settings

Show log entries in reverse order (newest entries on top)

Number of log entries to show:

Enable syslog'ing to remote syslog server

Remote syslog server

IP address of remote syslog server

Submit

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.

◆ Function Summary

You can configure the Log method here. MB5000 can display the Syslog entries in the Web GUI; it can also send the Syslog entries to a remote syslog server. To send the Syslog to the syslog server, you need to check the “*Enable sysloging to remote syslog server*” checkbox and assign the IP address of remote syslog server in the bottom box.

3.4.8.2DHCP leases

Figure 3-47 *DHCP leases*

Diagnostics: DHCP leases

IP address	MAC address	Hostname	Remaining-time
171.16.0.2	00:90:4B:C2:1F:54	Jerry-W2K	23 hours, 59 minutes, 56 seconds

Function Summary

This tab shows the information of MB5000's DHCP server.

4 Troubleshooting

4.1 Overview

- Introduction
- Reset to Factory Default procedure
- Force Reload 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 MB5000 setup. The most common installation problems are related to the IP address. For example, without the TFTP server IP address, you will not be able to download firmware to MB5000.

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 forgotten, you will need to reset the MB5000 to default values. The **Reset to Factory Default** procedure resets the MB5000 configuration settings, but does not change the current firmware. The **Forced Reload** procedure will erase the current firmware and configurations, please use it with caution when you need to download new software.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration values, including the MB5000 IP Address, Subnet Mask, and so on. The current MB5000 Software will not be erased. This

procedure may be required if the password is forgotten or the configurations are forgotten.

Power on MB5000 and wait for at least 1 minute till the device boots up and work in a stable 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 MB5000, the factory default network values are restored. Please refer Table 6-1 for the factory default value.



Warning:

If you press and hold the **RELOAD** button for more than 10 seconds immediately after the MB5000 is power on or reset, the MB5000 will enter into Force Reload Procedure. The software in the MB5000 will be erased. You will have to download software into MB5000 to make it work again.

Forced Reload Procedure

Use this procedure to force the MB5000 back to default network configuration values and download new MB5000 software. This procedure may be required when the current MB5000 software is missing, corrupted or needs to be upgraded.

Download procedure

1. Prepare you TFTP server. TFTP server is a computer with TFTP server software running. TFTP server can be freely downloaded from www.solarwinds.net. You can also search other TFTP servers from Internet if you like.
2. To download the MB5000 Software, you will need an Ethernet connected to the computer on which the TFTP server resides. This can be any computer on the LAN, or connected to the MB5000's "LAN" port with a "crossover" Ethernet cable.
3. After force reload, MB5000's IP will be set to 172.16.0.1 by default, and MB5000 will login the TFTP server with IP address "172.16.0.2" to download software named "firmware.bin" by default. So please change the IP address of TFTP server to 172.16.0.2, and change the MB5000 software name to **firmware.bin**, put it in the directory of TFTP server root.

4. After finishing this preparation, power on the MB5000.
5. Press the **RESET** button.
6. Press and hold the **RELOAD** button for about 10 seconds immediately after you press and release the **RESET** button until the POWER LED turns amber and the WWAN LED turns off. Result: The MB5000 deletes the current MB5000 software and Configuration files. Then MB5000 will download the software you have prepared in step 3. Observe what the TFTP displays and you should see downloading activity begins after a few seconds.
7. After finish this procedure, MB5000 will reboot automatically and you can see the POWER LED turns amber and blinks.
8. MB5000 will be configured to the factory default value. 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 MB5000 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**

System: Firmware

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.

MB5000'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 MB5000. 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 MB5000’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 MB5000.
- e. Enter the Subnet Mask, 255.255.0.0.
- f. Enter the Default Gateway, 172.16.0.1 (MB5000'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. In the 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 MB5000.
- 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 MB5000.
- 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 press the Enter key. The WAN IP Address can be found on the Status screen of MB5000’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 MB5000.
- 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 MB5000. 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 MB5000 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 directly connection to the Internet.

Frequently Asked Questions

What is the maximum number of IP addresses that MB5000 will support?

MB5000 will support up to 253 IP addresses.

Is IPSec Pass-Through supported by MB5000?

Yes, it is a built-in feature that MB5000 automatically enables.

Does MB5000 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 MB5000 to be used with low cost Internet accounts. The user may have many private addresses behind this single address provided by the ISP.

Does MB5000 support any operating system other than Windows 98, Windows Millennium, Windows 2000, or Windows XP?

Yes.

Does MB5000 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 MB5000.

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 MB5000 support?

MB5000 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 MB5000. 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 directly connection to the Internet.

Does MB5000 pass PPTP packets or actively route PPTP sessions?

MB5000 allows PPTP packets to pass through.

Is MB5000 cross-platform compatible?

Any platform that supports Ethernet and TCP/IP is compatible with MB5000.

Can MB5000 act as my DHCP server?

Yes. MB5000 has DHCP server software built-in.

What is the IEEE 802.11g standard?

It is one of the IEEE standards for wireless networks. The 802.11g standards allow wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standards. The 802.11g standards state a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz. The 802.11g is downward compatible with 802.11b.

What IEEE 802.11b features are supported?

MB5000 supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP or WPA) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is WPA-PSK?

WPA-PSK means Wi-Fi Protected Access - Pre-Shared Key. It is an enhanced wireless encryption standards defined by the Wi-Fi Alliances.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same making it a valuable identifier for the network.

How do I reset MB5000 to factory default?

When MB5000 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 MB5000 to its default settings.

How do I deal with signal loss issue?

The range of Wi-Fi network offered by MB5000 depends much on real environment. Every obstacle placed between MB5000 and your PC will create wireless signal loss. Lead glass, metal, concrete floors, water and walls will decrease the signal strength much. You can try using different Wi-Fi channel, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.

WEP or WPA-PSK is probably enabled on MB5000, but not on your wireless client. Verify that the same keys are being used on all nodes of your wireless network.

How many channels/frequencies are available with MB5000?

There are eleven available channels, ranging from 1 to 11 (in North America).

5 Default Settings

The following tables lists the settings defined at the factory for all MB5000 units, and provides a place to enter the values for your system if you have changed them.

Table 6-1 **MB5000R 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)	topglobalXXXXXX("XXX XXX" means the last 6 digits of SN)	
Frequency Channel	6	
Wireless LAN Status	Enabled	
DHCP Server Status	Enabled	
DHCP Lease Range	172.16.0.2-172.16.0.100	
TFTP Server IP Address	172.16.0.2	
TFTP File Name	firmware.bin	
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

Table 6-2 **MB5000C 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)	N/A	
Frequency Channel	N/A	
Wireless LAN Status	N/A	
DHCP Server Status	Enabled	
DHCP Lease Range	172.16.0.2-172.16.0.100	
TFTP Server IP Address	172.16.0.2	
TFTP File Name	firmware.bin	
Http Username	public	
Http Password	public	

Wireless WAN default setting:	Dial mode	Bridged with PPPoE
	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

Table 6-3 **MB5000K 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)	N/A	
Frequency Channel	N/A	
Wireless LAN Status	N/A	
DHCP Server Status	Enabled	
DHCP Lease Range	172.16.0.2-172.16.0.100	
TFTP Server IP Address	172.16.0.2	
TFTP File Name	firmware.bin	
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