



# CONTENT

## **FOREWORD ..... 3**

<b>OBJECTIVES</b> .....	3
<b>AUDIENCE</b> .....	3
<b>CONVENTIONS</b> .....	3
<b>OBTAINING DOCUMENTATION</b> .....	3
<b>WORLD WIDE WEB</b> .....	3

## **1. INTRODUCTION ..... 4**

<b>1.1 OVERVIEW</b> .....	4
<b>1.2 ADVANCED FEATURES OF MOBILE BRIDGE 8000</b> .....	4
<b>1.3 NETWORK ARCHITECTURE</b> .....	4
<b>1.4 SPECIFICATION</b> .....	5

## **2. INSTALLING THE MB8000 ..... 7**

<b>2.1 OVERVIEW</b> .....	7
<b>2.2 VERIFY KIT CONTENTS</b> .....	7
<b>2.3 WRITE PRODUCT IDENTIFICATION</b> .....	8
<b>2.4 POWER UP THE MB8000</b> .....	8
<b>2.5 LED INDICATORS</b> .....	9
<b>2.6 INITIALIZE THE MB8000 UNIT</b> .....	9

## **3. MANAGEMENT ..... 13**

<b>3.1 OVERVIEW</b> .....	13
<b>3.2 MANAGEMENT OPTIONS</b> .....	13
<b>3.3 WEB-BASED MANAGEMENT INTERFACE</b> .....	13
<b>3.3.1 STATUS</b> .....	14
<b>3.3.2 BASIC</b> .....	14
<b>3.3.2.1 WIRELESS INTERNET</b> .....	15
<b>3.3.2.2 LOCAL IP CONFIGURATION</b> .....	17
<b>3.3.2.3 WLAN CARD</b> .....	19
<b>3.3.3 ADVANCED</b> .....	20
<b>3.3.3.1 PASSWORD</b> .....	20
<b>3.3.3.2 ENCRYPTION</b> .....	21

3.3.3.3 RADIUS AUTHENTICATION .....	23
3.3.3.4 RADIUS ACCOUNTING .....	26
3.3.3.5 MAC ACCESS .....	27
3.3.3.6 WEB PORTAL .....	28
3.3.3.7 NAT SETTING (IP PORT FORWARDING) .....	29
3.3.3.8 LINK INTEGRITY .....	30
<b>3.3.4 TOOLS .....</b>	<b>31</b>
3.3.4.1 DOWNLOAD & UPLOAD .....	31
3.3.4.2 REBOOT .....	32
3.3.4.3 RELOAD .....	33
<b>3.3.5 MONITOR .....</b>	<b>33</b>
3.3.5.1 WAN .....	33
3.3.5.2 ROUTER .....	33
3.3.5.3 SYSTEM LOG .....	33
3.3.5.4 LINK STATUS .....	34
<b>3.3.6 WIZARD .....</b>	<b>34</b>

## **4. SECURE SOCKET LAYER (SSL) ..... 38**

<b>4.1 OVERVIEW .....</b>	<b>38</b>
<b>4.2 INTRODUCTION TO SSL .....</b>	<b>38</b>
<b>4.3 SERVER CERTIFICATE AND PRIVATE KEY DOWNLOAD FOR MB8000 .....</b>	<b>38</b>
<b>4.4 CA CERTIFICATE DOWNLOAD FOR MB8000 .....</b>	<b>39</b>
<b>4.5 CA CERTIFICATE INSTALL FOR MB8000'S CLIENT .....</b>	<b>40</b>
<b>4.6 CA CERTIFICATE UNINSTALL FOR MB8000'S CLIENT .....</b>	<b>44</b>

## **5. TROUBLESHOOTING ..... 45**

<b>5.1 OVERVIEW .....</b>	<b>45</b>
<b>5.2 INTRODUCTION .....</b>	<b>45</b>
<b>5.3 RESET TO FACTORY DEFAULT PROCEDURE .....</b>	<b>45</b>
<b>5.4 FORCED RELOAD PROCEDURE .....</b>	<b>46</b>
<b>5.5 FIRMWARE UPGRADE PROCEDURE THROUGH WEB .....</b>	<b>46</b>
<b>5.6 SCAN TOOL UTILITY .....</b>	<b>47</b>

## **6. DEFAULT MB8000 SETTINGS ..... 51**

## **FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT ..... 52**

# Foreword

This section describes the objectives, audience and conventions of the Top Global MB8000 User Guide.

## Objectives

This document explains the steps for initial setup and basic configuration of the MB8000. This document also provides troubleshooting information and detailed specifications.

## Audience

This document is for the person installing and configuring the Top Global MB8000 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.



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

Note



**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.

Warning

## Obtaining Documentation

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

## World Wide Web

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

# 1. Introduction

## 1.1 Overview

- Advanced Features of MB8000
- Network architecture
- Specification

## 1.2 Advanced Features of Mobile Bridge 8000

MB8000 has the most state-of-the-art system architecture design based on its rich network protocol features, reliable system level performance, optimized hardware design architecture, solid wireless security algorithms, and competitive product price. It is a leading MobileBridge design in the industry.

People can access network resources anytime anywhere by using this technology. MB8000 is the first wireless product combining WLAN with GPRS/EDGE/UMTS, and CDMA 1x/EVDO.

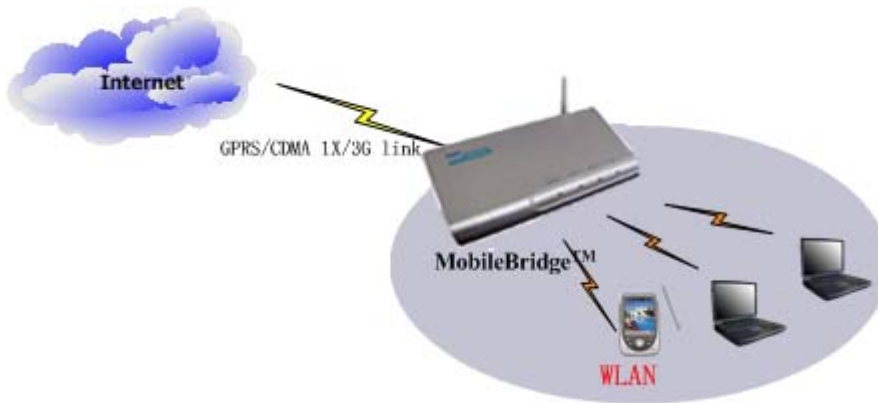
TOP Global MB8000 supports ESSID suppression, WEP (RC4) encryption, 802.1x port-based authentication and WPA. MB8000™ offers the secure “Always on, anywhere, anytime” wireless connectivity to subscribers. It also supports VPN and gives the user maximum security.

RADIUS Client in MB8000™ supports various accounting methods. Operators and WISPs could choose their preferred business model and accounting policies.

## 1.3 Network Architecture

Figure 1-1 Illustrates a typical configuration for internet access via MB8000.

Figure 1-1 **Standalone wireless network access infrastructure**



## 1.4 Specification

Table 1-1 **Mobile Bridge Specifications**

Category	Specification
<b>Hardware</b>	
Dimensions (HXWXL)	2.7 cm X 13 cm X 25.4cm 1.1 in X 5.1in X 10 in
Weight	895g(1.97 lbs)
Power	100/240 VAC high quality and worldwide safety approval
Operating	0° to 50°C (32° to 122°F) @ 20 to 90% relative humidity
Transport	-40° to 60°C (-40° to 140°F) @ 15 to 95% relative humidity (no condensation allowed)
Storage	-10° to 60°C (14° to 140°F) @ 10 to 90% relative humidity (no condensation allowed)
Ethernet interface	One 10/100 Base-T, RJ-45 female socket
Wireless interface	IEEE 802.11b, MiniPCI slots for radio NIC
PC CARD interface	One PC card slot for Wireless Wide Area Network (WWAN) including: GPRS / EDGE/ UMTS and CDMA1x / EVDO networks
Serial interface	8-Pin Female MiniDin RS232 connector
4 LEDs	Power WLAN Wireless Wide Area Network (WWAN) Ethernet Activity port (LAN)
MTBF(Mean Time Between Failures)	244,048Hrs
<b>Software</b>	
	<ul style="list-style-type: none"> <li>● Boot Loader and Power On Self Tests (POST)</li> <li>● MB8000 executable program (MB Firmware)</li> <li>● CLI compatible with generic Telnet and Terminal clients.</li> <li>● Serial port Interface is compatible with most ASCII terminal</li> </ul>

---

	<p>programs (such as HyperTerminal)</p> <ul style="list-style-type: none"><li>● HTTP Interface compatible with web browsers equivalent to Microsoft Internet Explorer 4.0 and Netscape 4.0 and higher.</li></ul>
--	--

---

## 2. Installing the MB8000

### 2.1 Overview

Installing the Top Global MB8000 is easy. Follow the quick steps below to power up your wireless network:

1. Verify kit Contents.
2. Write Down Product Identification.
3. Power up the MB8000.
4. LED Indicators
5. Installation Requirements

### 2.2 Verify Kit Contents

Your MB8000 kit includes the following components, similar to those depicted in Figure 2-1.

Figure 2-1 *MB8000 Kits Contents*



1. MB8000 Main Unit (Top View)
2. Power supply
3. MB8000 Mounting Rack (Back View, optional and can be purchased separately)
4. CD
5. Cross-over cable
6. User manual
7. QIG (Quick Installation Guide)



**Note:**

When shipped from the factory, a Mini-PCI Card has been built into MB8000. Mini PCI Card is a wireless network card with integrated radio modules and antennas (2.4 GHz). The card complies with the IEEE 802.11b and Wi-Fi™ standards.

## 2.3 Write Product Identification

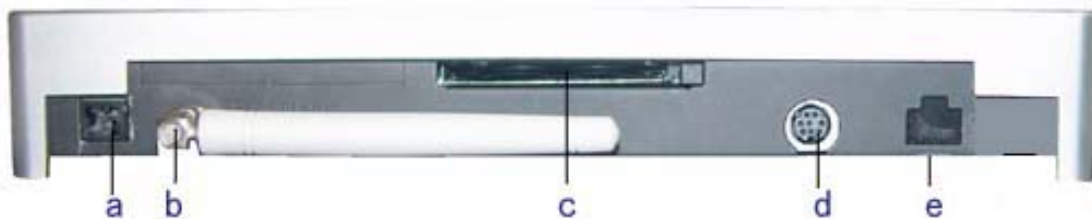
Before you proceed with your MB8000 installation, please write down and keep the following MB8000 information.

- Serial Number
- MAC address

## 2.4 Power up the MB8000

Connect the power supply. (See Figure 2-2).

Figure 2-2 *Ports description*



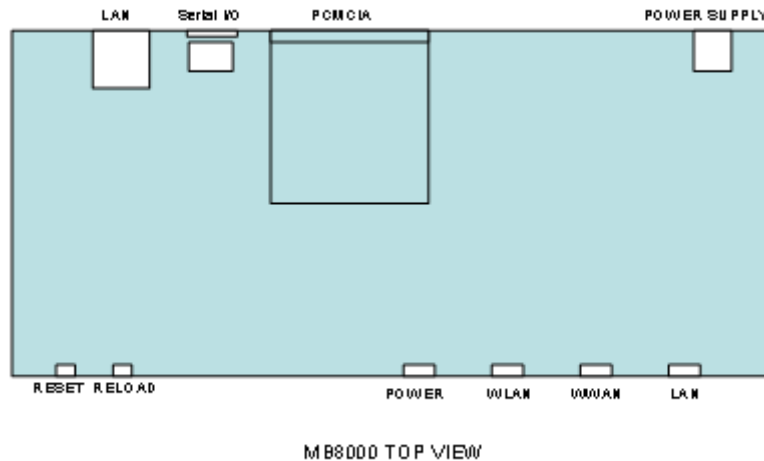
- a. Power
- b. WLAN Antenna
- c. PC CARD
- d. Serial Port
- e. Ethernet Interface(LAN)



**Note:**

MB8000 reserves another hole between port d and port e for extended Ethernet interface, please make sure you use port e for your Ethernet LAN.

Figure 2-3 *MB8000 Top View*



The MB8000 power supply accepts any input AC voltage in the range of 100-240 VAC.

## 2.5 LED Indicators

MB8000 has four two-color LEDs to indicate the working status. The follow table shows the status when the MB8000 is configured successfully and running properly.

Table 2-1 **Normal LED Indications (Use WWAN to Connect to Internet and No WAN)**

Power	WLAN	WWAN	LAN
Green when MB8000 is ready. Red if an error occurs. For example, corrupt firmware.	Green Blink if WLAN is transferring data.	Green blink if WWAN is transferring data. Red if WWAN is in error status.	Green blink if LAN is transferring data.

## 2.6 Initialize the MB8000 Unit

1. Connect MB8000 with your computer, there are two ways to connect MB8000 with your computer:

- I. Connect your computer to MB8000 using a “Cross-over” Ethernet cable or a

- hub and your computer is set with “Automatic IP” configuration.
- II. Alternatively, you can connect your computer to MB8000 with wireless LAN.
    - a) Install a 802.11b wireless LAN PC card in a laptop or other computer, including the driver and the Client Manager Application software if available. If you are using a Centrino laptop, the wireless LAN module is already embedded. There is no need to install extra wireless LANPC card.
    - b) Configure the wireless LAN card to match the network name and encryption key of wireless LAN card installed in the MB8000. The default network name is “mbnet”, and “Automatic IP” configuration is also needed.
  2. Validate that your computer has got IP address from the MB8000, then open the web browser and enter <http://172.16.0.1>. Press Enter then the MB8000 login screen appears. Enter the username/password (default is public/public), and click OK, the web configuration screen appears.

Figure 2-4 *login window*

The screenshot shows a standard Windows-style dialog box titled "Enter Network Password". The background is light gray. At the top left, there is a yellow key icon with a blue eye. To its right, the text "Please type your user name and password." is displayed. Below this, the "Site:" field is populated with "172.16.0.1" and the "Realm:" field is populated with "mbnet". There are two empty text input boxes, one for "User Name" and one for "Password". At the bottom left, there is a checkbox with the label "Save this password in your password list", which is currently unchecked. At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 2-5 **Home Page**

**System Status:**

System Status	
Local IP Address:	172.16.0.1
Local IP Mask:	255.255.0.0
Wireless WAN IP Address:	220.207.81.86
System Description:	MB-8000 v2.02(00003) SN: MB04TG010226
WLAN Card States:	Existence
WLAN Card Style:	Intersil wireless card
Wireless Internet Card States:	CDMA
Wireless Internet Card Style:	Sierra Air Card 555
Cable LAN States:	100M full
WLAN Name(SSID):	mbnet
UpTime:	0 days, 1:11:04 (hr:min:sec)

Wizard >>

Customize <<

Show wireless internet card signal strength:

Refresh

Strength:

excellent

**System Logs:**

System logs is the asynchronous information, used by agent to report some important events to the network management station. Each log identifies a specific severity level.

System Logs			
Index	Description	Severity	Time Stamp
1	Cold started	informational	00 days 00:00:00
2	Link up	informational	00 days 00:00:01
3	Link up	informational	00 days 00:01:55
4	modem: command = ATZ	informational	00 days 00:01:55

There are two buttons on the home page: Wizard and Customize. Alternatively, you can configure your MB by using them. If you are using the Wizard to configure the MB8000, please continue with the remaining part of this section. If you are using Customize to configure the MB8000, please jump to the section 3.

**3. Change the Dialing Up parameters of WWAN card if needed**

Click button “**Wizard**” on the home page. The following configuration page appears (use CDMA 1x/EVDO for example).

Figure 2-6 **Wizard--Wireless Wan**

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 2-7 **Wizard--Wireless connect**

Click button “**Connect**” and wait a moment, a page will appear to tell you the results.

Figure 2-8 **Wizard -connection result**

Congratulations! Now you can access internet through MB.

## 3. Management

### 3.1 Overview

- Management Options
- Web-based Management Interface

### 3.2 Management Options

Top Global MB8000 provides web-based interface for system management.

### 3.3 Web-based Management Interface

MB8000 embeds a web server for web-based management. This section will show you how to visit MB8000's web site.

1. Open your browser and enter the MB8000's IP address in the address bar.
2. Press the **ENTER** key. The MB8000 **Login** dialog box appears.

Figure 3-1 **Login Dialog Box**



**Note:**

Default user name: public

Default password: public

3. After you have input the right username and password, the home page of MB8000 web site will be displayed (Figure 3-2).

Figure 3-2 *MB8000's home page*

**System Status:**

System Status	
Local IP Address:	172.16.0.1
Local IP Mask:	255.255.0.0
Wireless WAN IP Address:	220.207.81.86
System Description:	MB-8000 v2.02(00003) SN: MB04TG010226
WLAN Card States:	Existence
WLAN Card Style:	Intersil wireless card
Wireless Internet Card States:	CDMA
Wireless Internet Card Style:	Sierra Air Card 555
Cable LAN States:	100M full
WLAN Name(SSID):	mbnet
UpTime:	0 days, 1:11:04 (hr:min:sec)

Wizard >>

Customize <<

Show wireless internet card signal strength:

Refresh

Strength:  
*excellent*

**System Logs:**

System logs is the asynchronous information, used by agent to report some important events to the network management station. Each log identifies a specific severity level.

System Logs			
Index	Description	Severity	Time Stamp
1	Cold started	informational	00 days 00:00:00
2	Link up	informational	00 days 00:00:01
3	Link up	informational	00 days 00:01:55
4	modem: command = ATZ	informational	00 days 00:01:55

There are three main categories of MB8000's web site: **status**, **wizard** and **customize**. The following section will explain each of them in detail.

**3.3.1 Status**

View your system information in status area.

The **status** area includes two sub-areas: **system status** and **system logs**.

- **System status** provides system level information, including the MB8000's IP address and contact information.
- **System logs** report some important events to the network management stations. Each trap identifies a specific severity level.

For more information about system traps, refer to "Troubleshooting" of the user guide.

**3.3.2 Basic**

**Basic** part includes the most primary configurations for MB8000.

There are three main categories of basic settings:

- Wireless Internet
- Local IP Configuration
- WLAN Card

### 3.3.2.1 Wireless Internet

1. Configuration varies by wireless card. As Figure 3-3 shows, the wireless card's type is CDMA.

Figure 3-3 *wireless Internet*

- Card status: Enable or Disable the wireless card status, the default value is Disabled.
- Connect Type: Indicates the wireless card's type: CDMA, EVDO, GPRS, or UMTS.
- Phone Number: this parameter is used to provide a phone number for modem.
- User Name: this parameter is used to provide a user name for modem.
- Password: this parameter is used to provide a password for modem.
- Remote IP Negotiation: Enable or disable MB to negotiate with service provider to get peer IP address.
- Primary DNS Negotiation: Enable or disable MB to negotiate with service provider to get primary DNS address.
- Secondary DNS Negotiation: Enable or disable MB to negotiate with service provider to get secondary DNS address.
- Connect: connect to Internet.

- Disconnect: disconnect to Internet.
- Submit: submit and save the parameters.

2. If wireless card type is GPRS or UMTS, the parameters to be configured are shown as follows. (Figure 3-4) Check in the checkbox to show the advanced configuration of the card. (Figure 3-5)

Figure 3-4 *wireless Internet*

<input type="button" value="Connect"/>	<input type="button" value="Submit"/>
Card Status:	<input type="text" value="Disable"/>
Connection Type:	<b>GPRS</b>
PhoneNumber:	<input type="text" value="*99***1#"/>
UserName:	<input type="text" value="vxTarget"/>
Password:	<input type="text" value="*****"/>
APN:	<input type="text" value="cmnet"/>
CID:	<input type="text" value="1"/>
PDP Address:	<input type="text" value="0.0.0.0"/>
Data Compression:	<input type="text" value="0"/>
Head Compression:	<input type="text" value="0"/>
Remote IP Negotiation:	<input type="text" value="Enable"/>
Primary DNS Negotiation:	<input type="text" value="Enable"/>
Secondary DNS Negotiation:	<input type="text" value="Enable"/>
LOCALWAN IP Negotiation:	<input type="text" value="Enable"/>
Static IP Address:	<input type="text" value="192.168.1.254"/>
Advanced: <input type="checkbox"/>	

- 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.
- CID: (PDP Context Identifier) a numeric parameter, which specifies a particular PDP context definition.
- PDP Address: A string parameter that identifies the MB in the address space applicable to the PDP.
- LOCAL WAN IP Negotiation: Enable or disable MB to negotiate with service provider to get WAN IP address.
- Static IP Address: When LOCAL WAN IP Negotiation is disabled, MB will use Static IP Address as PDP address.

## Advanced

Figure 3-5 *wireless Internet-Advanced*

Advanced:

Precedence:

Delay:

Reliability:

Peak throughput:

Mean throughput:

- Precedence: is a numeric parameter that specifies the precedence class.
- Delay: is a numeric parameter that specifies the delay class.
- Reliability: is a numeric parameter that specifies the reliability class.
- Peak throughput: is a numeric parameter that specifies the peak class.
- Mean throughput: is a numeric parameter that specifies the mean class.

3. If no card is inserted, the page will prompt you that there is novalid wireless WAN card.

Figure 3-6 *No card*



### 3.3.2.2 Local IP Configuration

#### IP Configuration

- Local IP Address: This parameter represents the IP Address of the LAN & WLAN. The default IP address is 172.16.0.1.
- Local IP Mask: This parameter represents the subnet mask of the wireless LAN & WLAN. The default subnet mask is 255.255.0.0.

Figure 3-7 **IP configuration**

### IP Configuration

Local Network settings allow you to share a single internet address among all of the local wired and wireless clients of the Gateway as well as distribute internet addresses dynamically to clients connecting to the Gateway.

Local IP Address:

Local IP Mask:

### DHCP Server

- **DHCP Server Status:** This parameter indicates whether the DHCP server is enabled or disabled in MB8000. If DHCP is disabled, each client device must be manually configured.
- **Start IP Address:** The start IP address for the DHCP IP address pool.
- **Width of IP Address:** The width of DHCP IP address pool.
- **Default Lease Time:** The default lease time in seconds for the IP address assigned by the DHCP server to the DHCP client.
- **Maximum Lease Time:** The maximum lease time in seconds for the IP address assigned by the DHCP server to the DHCP client.

Figure 3-8 **DHCP Server**

### DHCP Server

DHCP server status just on the local network. Each client device must be manually configured with a unique, static Internet (IP) address if this option is disabled.

DHCP Server Status:

Start IP Address:

Width of IP Address:

Default Lease Time:

Maximum Lease Time:

### DNS Configure

DNS Relay, also called DNS Redirect or DNS Proxy, allows clients on the local network to use the gateway as their primary DNS server. In this way, all DNS queries from clients are sent to MB8000 and then automatically forwarded to your ISP's DNS servers by MB8000. This allows clients to always be able to use the gateway as their DNS server regardless of changes in DNS server that your ISP may make in the future.

- **DNS Relay Status:** This parameter indicates whether DNS relay is enabled or disabled.
- **Primary DNS IP Address:** This parameter represents the IP address of the primary DNS server.
- **Secondary DNS IP Address:** This parameter represents the IP address of the secondary DNS server.

Figure 3-9 **DNS Relay Configuration**

### DNS Configuration

DNS Relay, also sometimes called DNS Redirect or DNS Proxy, allows clients on the local network to use the Gateway as their primary DNS server. All DNS queries are then automatically forwarded to your ISP's DNS servers for resolution. This allows clients to always be able to use the Gateway as their DNS server regardless of any DNS server changes that your ISP may make in the future.

DNS Relay Status:	<input type="text" value="Enable"/>
Primary DNS IP Address:	<input type="text" value="220.192.0.130"/>
Secondary DNS IP Address:	<input type="text" value="220.106.196.115"/>

### 3.3.2.3 WLAN Card

- Wireless card status: This parameter indicates whether wireless card is enabled or disabled.
- Network Name: Network name for each mini-PCI Card. This is the same name with the one used by Client Manager Software.
- Frequency Channel: The desired frequency channel for card. Ensure that the nearby devices do not use it.
- Closed System: A closed system means that only clients who know the MB8000's network name can access MB8000's wireless network. When this parameter is set to **Enable**, MB8000 will not broadcast MB8000's network name. When this parameter is set to **Disable**, MB8000 will broadcast MB8000's network name so client can scan the name.
- IBSS Relay Status: This parameter indicates whether IBSS Relay Status is enabled or disabled.
- MAC Address: Show the WLAN card's MAC address.

Figure 3-10 **Wireless Card**

**Basic**

- Wireless Internet
- Local IP Configuration
- WLAN Card

**Setup - Wireless Card - Wireless Card**

Wireless Card Status:

Network Name (SSID):

Frequency Channel:

Closed System Status:

IBSS Relay Status:

MAC Address: 00:90:4b:8b:59:fd

### 3.3.3 Advanced

- Password
- Encryption
- Radius Authentication
- Radius Accounting
- MAC Access
- Web Portal
- NAT
- Link Integrity

#### 3.3.3.1 Password

- Http Password: User name and password for MB8000's web administration.
- Telnet Password: User name and password for MB8000's telnet server.
- SNMP Password: User name and password for MB8000's SNMP agent.

Figure 3-11 **Password**

### 3.3.3.2 Encryption

Encryption configuration defines what security protocol to be adopted in WLAN. Available security protocol in MB8000 includes 802.1x, WPA and 128-bit WEP.

- Network Authentication:

Open:

Shared:

802.1x Only (Non-WPA):

802.1x and WEP (Non-WPA):

WPA:

WPA-PSK:

This parameter sets the authentication mode.

“**Open**” means setting the authentication mode to open-system authentication. Under this mode, stations can associate to the MB freely.

“**Shared**” means setting the authentication mode to shared-secret authentication. Under this mode, stations can associate to the MB with the proper WEP keys.

“**802.1x Only (Non-WPA)**” means that the MB uses IEEE 802.1x to perform the authentication. Stations which failed to the 802.1x authentication will be denied to access the MB.

“**802.1x and WEP (Non-WPA)**” means that the stations which success in either the WEP authentication or 802.1x authentication will be allowed to access the MB.

“**WPA**” means that the MB uses WPA with the backend authentication sever to authenticate the station

“**WPA Pre-Shared Key**” means that the MB uses WPA authentication with the Pre-Shared Key to authenticate the users. To use WPA PSK mode, you should configure as following:

1. Set "Network Authentication" to "WPA-PSK";
2. Set "Data Encryption" to "TKIP";

3. Set "Deny Non-Encryption Data" to "Disable";
4. Set "WPA Pre-Shared Key" with a pass-phrase (min 8 max 63 characters);

- Data Encryption:

This parameter sets the data encryption type.

“**Disabled**” means that no encryption is used in the traffic between the MB and the stations.

“**WEP**” means that the traffic data is encrypted by WEP.

“**TKIP**” means that TKIP is used in the traffic.

- Key length: There are two options you can select to decide the WEP key length.
- Encryption Key: These parameters are used as WEP key.
- Deny Non-Encrypted Data:

**Disabled:**

**Enabled:**

This parameter sets whether to deny the data that is not being encrypted.

- Encrypt Data Transmissions Using: Indicates which WEP key ID is selected to use to encrypt the outgoing data.
- 802.1x Re-Authentication Interval:

The 802.1x Re-Authentication Interval field is an integer, which indicates that how long the 802.1x authenticator will issue a re-authentication request in second. The minimal is 60, and the default value will be 600.



**Note:**

The range of this value is from 60 to 65535.

- WPA Group Key Renewal:  
This field is an integer, which indicates that the interval of TKIP key to renew. The minimal is 30.
- WPA Pre-Shared Key(passphrase):  
The WPA Pre-Shared Key field, which is to be filled with WPA-PSK, it's a string of “pass-phrase”, whose length ranges from 8 to 63 octets.

Figure 3-12 **Encryption**

### 3.3.3.3 Radius Authentication

A RADIUS server is one that contains central user databases which identify which user is allowed to access the wireless network. The information for primary RADIUS server is mandatory if RADIUS is enabled. The information for backup RADIUS server is optional.

- **RADIUS MAC Access Control Status:** This parameter indicates whether user authentication by RADIUS is enabled or disabled.
- **Interface:** The network interface that will be used for communicating with RADIUS server.
- **Authentication Lifetime (minutes):** The time before when auto re-authentication will be performed. The default value is 15 minutes.
- **Server Status:** The status of RADIUS server.
- **IP Address:** The IP address of RADIUS server.
- **Destination Port:** The listen port of RADIUS server. The default value is 1812.
- **Response Time (sec):** The maximum time to wait for the authentication response from RADIUS server.
- **Shared Secret:** Shared secret between RADIUS server and MB8000.
- **Maximum retransmissions:** The maximum number of times when an authentication may be retransmitted.

Figure 3-13 **Radius Authentication Configurations**

**Setup** — **security** — Radius Authentication

---

**Authentication**

RADIUS MAC Access Control Status:

Authentication Lifetime (minutes):

---

Interface:

---

RADIUS Server: *Server 1*

Server Status:

IP Address:

Destination Port:

Response Time (sec):

Shared Secret:

Confirm Shared Secret:

Maximum Retransmissions:

---

RADIUS Server: *Server 2*

Server Status:

IP Address:

Destination Port:

Response Time (sec):

Shared Secret:

Confirm Shared Secret:

Maximum Retransmissions:

---



**Note:**

For RADIUS authentication interface, there are two options to be selected:

---**LAN**: see Figure3-14 for the proper connection.

---**WWAN**: see Figure3-15 for the proper connection.

Figure 3-14 **Radius by LAN**

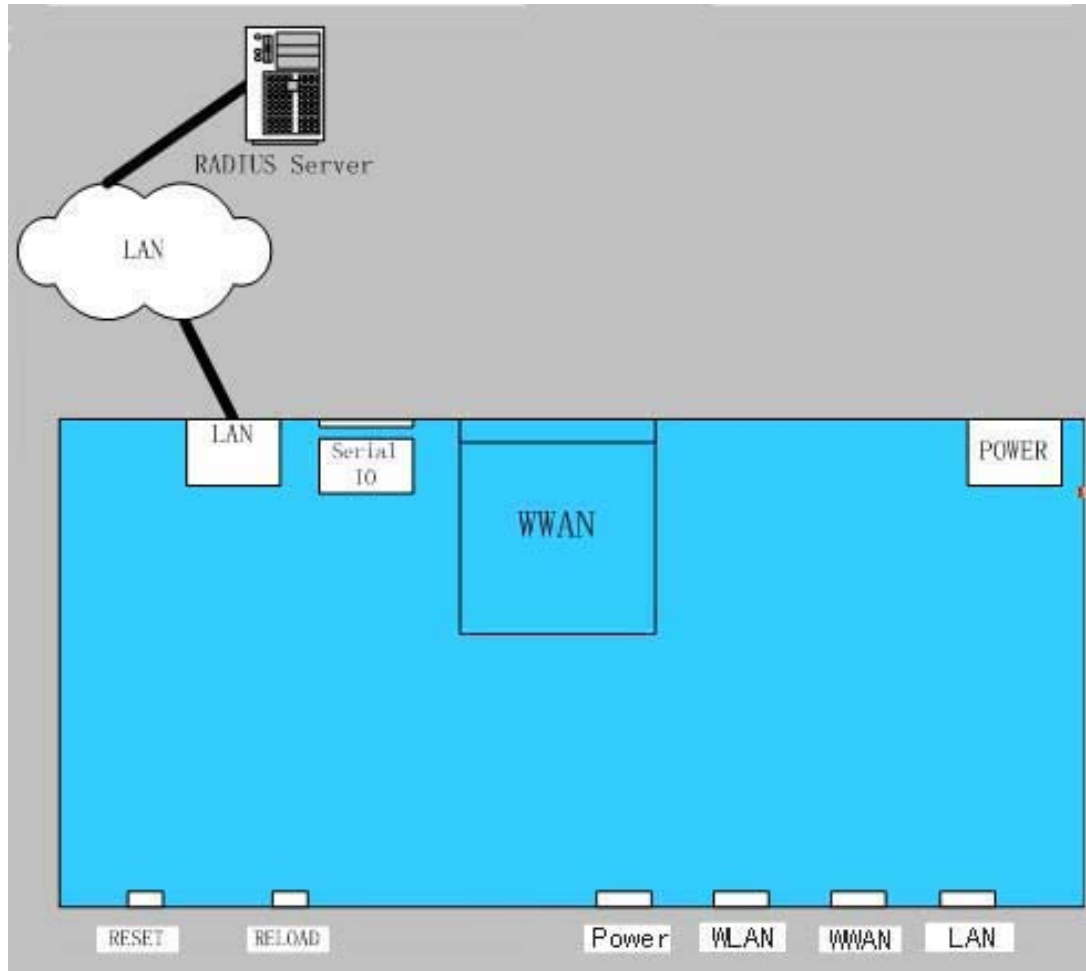
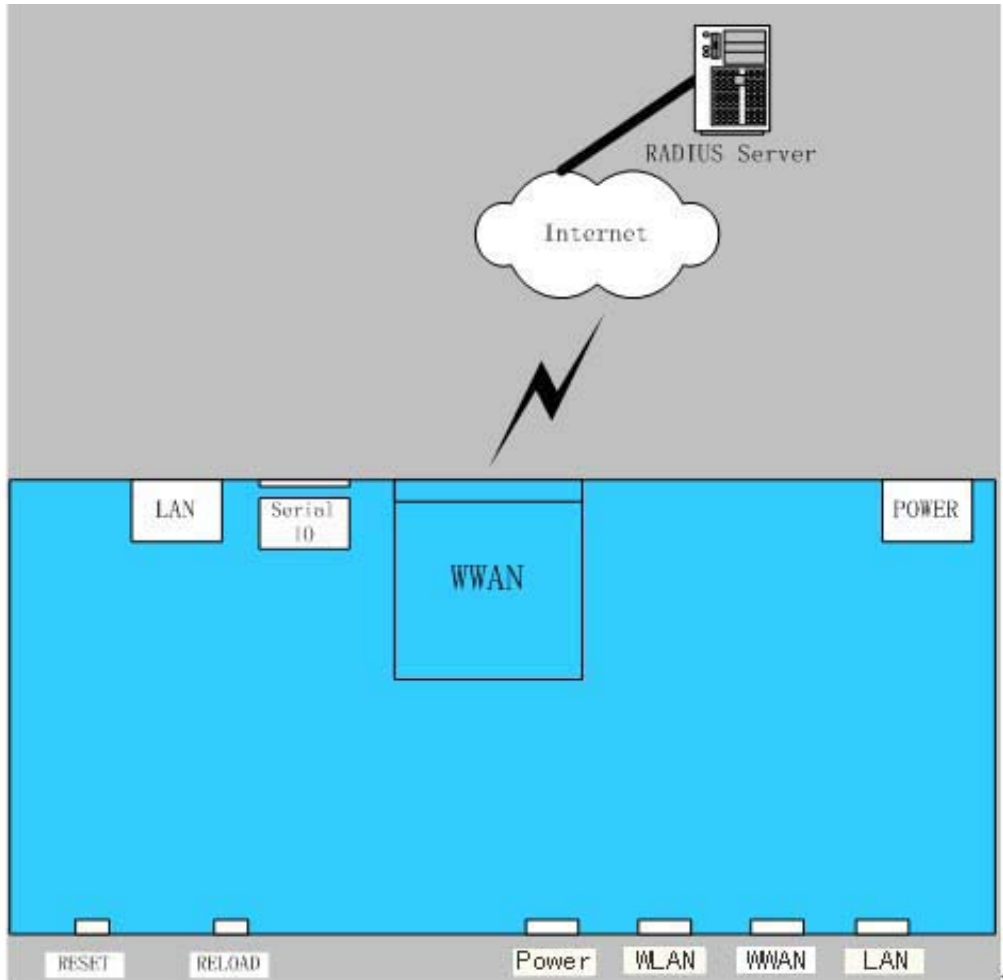


Figure 3-15 *Radius by WAN*



### 3.3.3.4 Radius Accounting

- Server Status: The status of RADIUS server.
- IP Address: The IP address of RADIUS server.
- Destination Port: The listening port of RADIUS server. The default value is 1813.
- Response Time (sec): The maximum time to wait for the response from RADIUS server.



**Note:**

The range of this value is from 1 to 10.

- Shared Secret: This is the shared key between RADIUS server and MB8000.
- Accounting Interim Update Interval: This parameter indicates the Interim update interval of the accounting.
- Maximum retransmissions: The maximum number of times that an accounting may be retransmitted.



**Note:**

The range of this value is from 1 to 4.

Figure 3-16 **Radius Accounting**

<b>Accounting</b>	
Accounting Server:	Server 1
Server Status:	Enable ▾
IP Address:	0.0.0.0
Destination Port:	1813
Response Time (sec):	3
Maximum Retransmissions:	3
Accounting Interim Update Interval(sec):	60
Shared Secret:	*****
Confirm Shared Secret:	*****
<hr/>	
Accounting Server:	Server 2
Server Status:	Enable ▾
IP Address:	0.0.0.0
Destination Port:	1813
Response Time (sec):	3
Maximum Retransmissions:	3
Accounting Interim Update Interval(sec):	60
Shared Secret:	*****
Confirm Shared Secret:	*****

### 3.3.3.5 MAC access

The MAC access section allows you to add, edit or delete users who can access MB8000. Users are identified by their MAC address.

- **Access control Status:** This parameter indicates whether access control by MAC address is enabled or disabled.
- **Access control Operation Type:** Choose between **Allow** and **Deny**. This determines how the stations identified in MAC Access Table is filtered.

#### Add an Entry to the MAC Access Control Table

1. Click the Add button in the MAC Access Control table.
2. Enter the MAC Address of the client station.
3. Add comment (optional).
4. This entries is automatically enabled.

#### Disable or Delete an Entry in the MAC Access Control Table

1. Click the Edit button in the MAC Access Control Table.
2. Select the MAC Address you want to disable or delete
3. Click OK

Figure 3-17 **MAC Access**

**MAC Access control**

Access Control Status:

Access Control Operation Type:

---

MAC Address	Comment	EntryStatus
01:02:03:04:05:06		Enable
01:02:03:04:05:07	111111	Enable

### 3.3.3.6 Web Portal

Web portal is an authentication method which authenticates users by requiring them to input user name and password on web pages.

#### Web Portal

Figure 3-18 **Web Portal**

Advanced

Password

Encryption

Radius Authentication

Radius Accounting

MAC Access

**Web Portal**

NAT

Link Integrity

**Setup** — **security** — Web Portal

Web Portal Status:

AliveTimeouts:

Local User Base Status:

---

**User Base Table:**

User Name	Entry Up Rate	Entry Down Rate	Entry Status
test	0	0	Enable
testtc	8192	8192	Enable
test2	0	0	Enable
test3	0	0	Enable
test4	0	0	Enable
test5	0	0	Enable
test6	0	0	Enable
test7	0	0	Enable
test8	0	0	Enable
test9	0	0	Enable

- Web Portal Status: This parameter indicates whether web portal is enabled or disabled.
- Alive Timeouts (Seconds): The idle time, user idle more than this time will be automatically logout by MB8000.

### Local User Base Setting

The local user base section allows you to add, edit or delete items which are used to validate the Web Portal local authentication.

- Local User Base Status: This parameter indicates whether local user authentication is enabled or disabled.

### Add an Entry to the Local User Base

- Click the Add button in the Local User Base table.
- Enter the user name and password for each user.
- Enter entry up-rate and down-rate for each user for the sake of flow control.

### Disable or Delete an Entry in the Local User Base Table

1. Click the Edit button in the Local User Base Table.
2. Select the user entry you want to disable or delete
3. Choose “Disable” or “Delete” in the user’s entry status.
4. Click OK

### 3.3.3.7 NAT Setting (IP Port Forwarding)

To make the internal machine's service available to the outside, we need to use port forwarding on the gateway server. It is assigning a port on the gateway to accept all connections and forward it to the internal machines port where the service is listening. For MB8000, the port range is from 30001~65535.

For example:

Let xxx.xxx.xxx.xxx be the IP address of the gateway server connected to the internet and 172.16.0.100 be the IP address of the internal machine. And you want to run a web server on 172.16.0.100 on port 80 which should be available to the outside internet. We can forward the port 50000 on xxx.xxx.xxx.xxx to port 80 of 172.16.0.100

Source: xxx.xxx.xxx.xxx:50000 -- forwarded to -> 172.16.0.100:80

There are two NAT tables in this configuration for inputting items for “IP port forwarding”. In the default settings, the two tables are empty. Click on “Add” and “Edit” button can pop up windows for editing the tables.

Figure 3-19 *IP port Forwarding Table*

Setup — NAT — NAT

NAT Status:

---

**TCP:**

Nat Local IP Address	Nat Local Port Number	Nat Global Port Number
172.16.0.100	80	50000
172.16.0.100	21	50001

---

**UDP:**

Nat Local IP Address	Nat Local Port Number	Nat Global Port Number
----------------------	-----------------------	------------------------

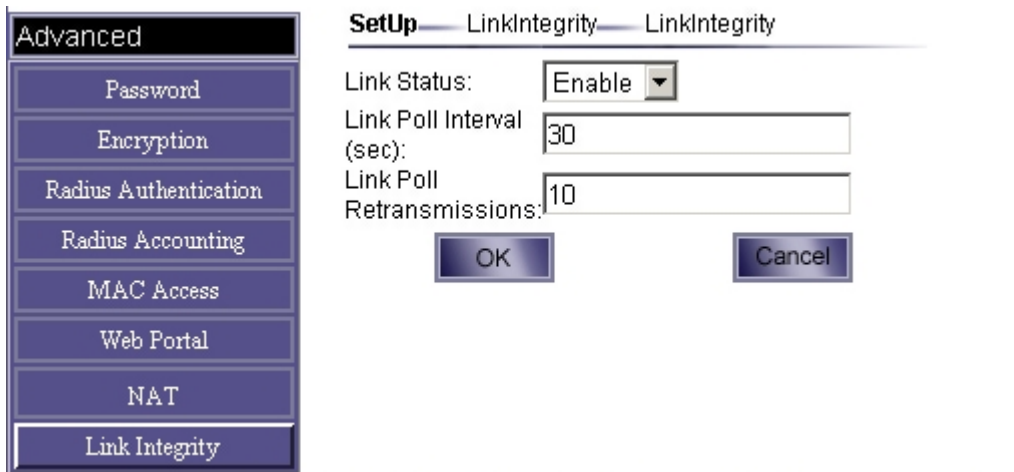
- **Add an Entry to the NAT Control Table**
  1. Click the “Add” button in the TCP or UDP table.
  2. Enter the NAT Local IP Address of the client station.
  3. Enter the NAT Local Port Number of the client station.
  4. Enter NAT Global Port Number.
  5. Add a comment as needed. Entries are automatically enabled.
- **Disable or Delete an Entry in NAT Control Table**
  1. Click the Edit button in the TCP or UDP Table.
  2. Select the entry you want to disable or delete
  3. click OK

### 3.3.3.8 Link Integrity

This function is used to verify the link status of WWAN. If the link of WWAN is down, WWAN LED will become orange and WWAN will try to reconnect.

- Link Integrity Status: This parameter is used to enable or disable the link integrity functionality.
- Link Poll Interval: This parameter is used to set the poll interval (in milliseconds) for the link integrity check.
- Link Poll Retransmissions: This parameter is used to set the number of retransmissions for the link integrity check.

Figure 3-20 *Link Integrity*



### 3.3.4 Tools

**Tools** provide functionalities including files downloading/uploading, MB8000 rebooting or reloading control.

#### 3.3.4.1 Download & Upload

Download and upload tools enable files downloading or uploading between MB8000 and TFTP server. TFTP server could be a computer with TFTP server software. TFTP server can be freely downloaded from [www.solarwinds.net](http://www.solarwinds.net). You can also search other free TFTP server in the internet.

Files downloadable includes configuration file (Config), MB Image(Img), logon web page(BspBl), server certificate file(ServerCert), server private key file(PrivateKey) and Certificate Authority certificate file(CAcert).

Files up loadable includes configure file (Config).



**Note:**

1) A TFTP server must be running and configured to point to the directory containing the target file. If you don't have a TFTP server installed on your system, install the TFTP server first.

2) Before you can download or upload file successfully, you must make sure that the physical connection was exited between the TFTP server and the corresponding interface in the same subnet.

— **Server IP Address.** The IP address of TFTP server.

- **File Name.** Name of the target file.
- **File Type.** Type of the target file. Possible file type includes:
  - **Config.** Configuration file containing information such as system name and contact name.
  - **Img.** MB Image (executable program).
  - **ServerCert.** Server certificate file(.pem file).
  - **PrivateKey.** Server private key file(.pem file).
  - **Cacert.** Certificate Authority certificate file(.cer file).
- **File Operation.** File operation type including **Download**, **Upload** or **Download & Reboot**. Download means from computer to MB8000. Upload means from MB8000 to computer. You should reboot the MB8000 after downloading files.

Figure 3-21 **Download & Upload**

**TFTP Information**

Server IP Address:

File Name:

File Type:  Server Key Password:

File Operation:

### 3.3.4.2 Reboot

**Reboot** operation saves configuration changes (if any) before resetting the MB8000 (this function can also be accomplished by holding down the Reset button). Set the time to Reboot as zero will cause an immediate reboot.



**Note:**

After configured all the parameters you need, reboot the MB8000. All the configuration will become effective.

Figure 3-22 **Reboot**

**Tools**

- Download/Upload
- Reboot
- Reload

Setup — **Tools** — Reboot

Please enter the time (in seconds) to reboot:

### 3.3.4.3 Reload

**Reload** operation restores the MB8000 configuration to factory default values. The MB8000 may also be reloaded from the **RELOAD** button on indicator side of the unit. Press and hold the **RELOAD** button for more than 30 seconds, until all the indicator lights turn off. Then release **RELOAD** button, press the **RESET** button to set up the device again. Since this will reset the current MB8000 IP address, a new IP address must be assigned. For more information, please refer to “Initialization”.



**Warning:**

If you press and hold the **RELOAD** button for more than 15 seconds immediately after the MB8000 is power on or reset, the MB8000 will enter into Force Reload Procedure. The software in the MB8000 will be erased. You will have to download software into MB8000 to make it work again. For more information, please refer to “Force Reload Procedure”.

### 3.3.5 Monitor

**Monitor** provides tools including link activity test, WAN interface monitoring and router table monitoring.

There are three sub-areas of monitor:

- Wan
- Router
- System Log
- Link status

#### 3.3.5.1 Wan

WAN interface monitoring tool shows whether WAN interface works normally or not .If the address is valid; the interface works normally, otherwise abnormally.

#### 3.3.5.2 Router

Router shows the route table of MB8000.

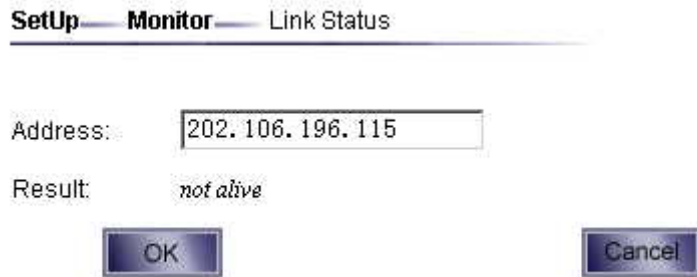
#### 3.3.5.3 System Log

Show system log information.

### 3.3.5.4 Link Status

Link tests whether a link is active by pinging the target IP address. Depending on whether the target IP address is available, the result will show *alive* or *not alive*

Figure 3-23 *Link status*



### 3.3.6 Wizard

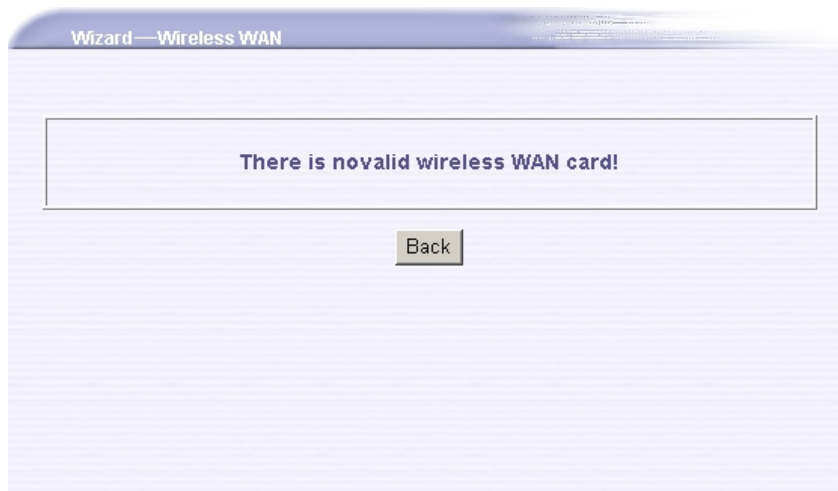
The Setup Wizard will guide you step-by-step to configure your MB8000 for use with your wired WAN and wireless WAN.

**Step1.** Configure your wireless internet card in the first step.

When you click on the “Wizard” Button, the first page will show your different wireless internet configuration page according to your card.

1. If no card has been inserted into the slot or MB can not identify the card, the following information will be prompted.

Figure 3-24 *No card*



2. If you are using CDMA EVDO card, then this page (figure 3- 25) will be shown to you:

Figure 3-25 **CDMA**

Wizard—Wireless WAN

Card Status:

Connection Type: CDMA

PhoneNumber:

UserName:

Password:

3. If you are using GPRS UMTS card, then this page (figure-26) will be shown to you :

Figure 3-26 **GPRS**

Wizard—Wireless WAN

Card Status:

Connection Type: GPRS

PhoneNumber:

UserName:

Password:

APN:

CID:

Finish the configuration of the wireless internet, click on “Next”, to the next step.

**Step2. Connect**

Click on “Connect” button. If you have already connected to the wireless Internet when you first reboot the MB, then you will be prompted not to connect again. Otherwise, you will wait for about 1 minute until MB8000 has finished dialing-up.

Figure 3-27 **Connected**



**Step3. Result**

Finally, MB will give the connection result. If MB failed to establish connection with the Internet, there will be some possible reasons given by MB. You can refer to the reasons when checking your card and your configurations.

Figure 3-28 **Failed**

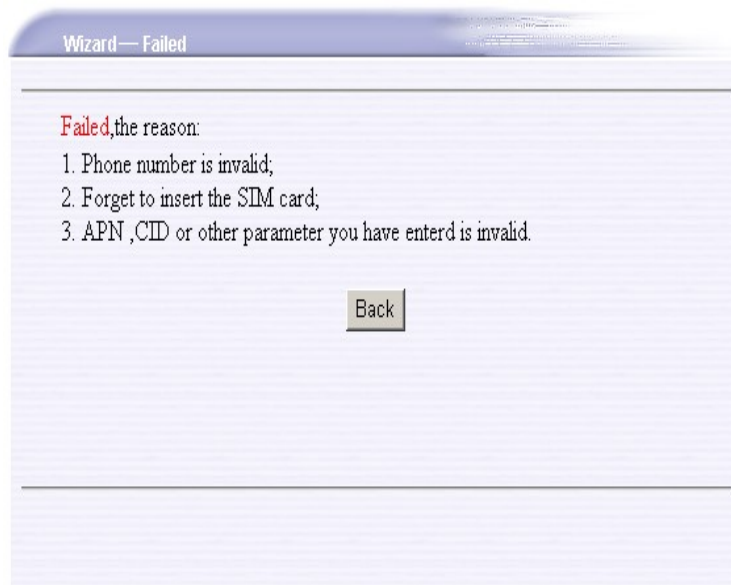


Figure 3-29 **Successful**



## 4. Secure Socket Layer (SSL)

### 4.1 Overview

- Introduction to SSL
- Server certificate and private key download for MB8000
- CA certificate download for MB8000
- CA certificate install for MB8000's client
- CA certificate uninstall for MB8000's client

### 4.2 Introduction to SSL

MB8000 supports SSL capability to provide secure network connections. By authenticating server before connecting to it, man-in-the-middle attack can be avoided. SSL also provides data encryption and integrity check.

Server authentication is based on server's certificate. Certificate is a digital identity card and it's issued by CA (certificate Authority). CA certificate is necessary to verify the validity of other certificates which issued by it. Therefore it's required that server should be issued a valid certificate from some CA which is trusted by user.

SSL is presented for login by web to launch a secure login with SSL. For user, what's need is simply type in <https://> in the web browser.( But if you haven't installed the CA certificate on your local system, you should install it at first, or you will always see an "untrustworthy root certificate" prompt every time you login. To install or uninstall CA certificate in user's local system, please refer to the "CA certificate install" and "CA certificate uninstall" topics for more information). For administrator of MB8000, it's required to download the server certificate file, server private key file and CA certificate file into MB8000 respectively. Please refer to the "server certificate download for MB800" and "CA certificate download for MB8000" topics for more information.

### 4.3 Server Certificate and Private Key Download for MB8000

The following steps will guide you how to download server certificate file and private key file from TFTP server to MB8000.

**Step1.** Applying for a server certificate and private key from a third party Certificate Authority.



**Note:**

Currently only .pem file is supported. Certificate and private key file in pem format can be generated with openssl software. Don't store certificate and private key in one file. Store them separately.

**Step2.** Downloading server certificate file and private key file into MB8000 respectively. Open page <http://172.16.0.1/download.htm>, configuring as the following example:

- Server IP Address:172.16.0.2
- File name: server-cert.pem
- File Type: ServerCert
- File operation: Download

Then press OK to download certificate file.

Open page <http://172.16.0.1/download.htm>, configuring as the following example:

- Server IP Address: 172.16.0.2
- File name: server-key.pem
- File Type: PrivateKey
- File operation: Download
- Server key password: topglobal(default value)

Then press OK button to download private key file.



**Note:**

Server key password is used to protect server-key.pem file from being read by others. Keep this item as blank if no password provided.

## 4.4 CA Certificate Download for MB8000

The following steps will guide you how to download CA certificate file from TFTP server to MB-8020.

Ensure the TFTP sever is running and configured to point to the folder containing the CACert to be downloaded.

Open page <http://172.16.0.1/download.htm>, configuring as the following example:

- Server IP Address: 172.16.0.2
- File name: cacert.cer
- File Type: CACert
- File operation: Download

Then press OK to download certificate file.

## 4.5 CA Certificate Install for MB8000's Client

The following steps will show you how to install the CA certificate in user's local system:

- Step1.** Choose "To install the CA certificate" on the test.htm page (Figure 4-1).
- Step2.** Click "open" button in the file download dialog box (Figure 4-2).
- Step3.** Choose "install certificate" of the Certificate dialog box (Figure 4-3), it will guide you into the certificate installation wizard.
- Step4.** Choose "Next" of the certificate import wizard 1 (Figure 4-4).
- Step5.** Choose "automatically select the certificate store based on the type of certificate" of the certificate import wizard 2 (Figure 4-5).
- Step6.** Choose "finish" of the certificate import wizard 3 (Figure 4-6).
- Step7.** Read the content of the certificate and make sure it can be trusted (warning: an untrusted CA would bring you great threat!) choose "yes" in the root certificate store page (Figure 4-7) to actually install the certificate.
- Step8.** Certificate installation is finished (Figure 4-8).

Figure 4-1 ***Install the CA certificate***

---

**Before you can access the internet successfully, you must login with your account and password. We provide you two ways to login:**

---

### **1.Login without SSL connection**

To login without SSL connection, please click [here](#).

---

### **2.Login with SSL connection**

When you login with SSL(Secure Socket Layer) connection, your password will be protected with cipher text, and you can be assure that you're connecting to the legal web site. But before you can successfully login with secure connection, you'll have to install the CA certificate on you local system first.

To install the CA certificate, click [here](#).

To login with secure connection, click [here](#).

Figure 4-2 **File download dialog box**



Figure 4-3 **Certificate dialog box**



Figure 4-4 **Certificate import wizard 1**



Figure 4-5 **Certificate import wizard 2**



Figure 4-6 *Certificate import wizard 3*



Figure 4-7 *Root certificate store*



Figure 4-8 *Certificate import wizard 4*



## 4.6 CA Certificate Uninstall for MB8000's Client

To uninstall the CA certificate from user's local system, simply refers to "internet options->content->certificates->trusted root certification", and remove the certificate you just installed.

# 5. Troubleshooting

## 5.1 Overview

- Introduction
- Reset to Factory Default procedure
- Force Reload Procedure
- Scanning Tool Utility
- LED Indications

## 5.2 Introduction

This section helps you to locate problems related to MB8000 setup. The most common installation problems relate to the IP address. For example, without the TFTP server IP address, you will not be able to download the MB Image to the MB8000.

IP address management is fundamental. It is suggested that you 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 MB8000 to default values. The **Reset to Factory Default** procedure resets configuration settings, but does not change the current MB software. The **Forced Reload** procedure will erase the current MB software, please use it when you need to download new software.

It is useful to set up the serial port and use your terminal emulator to monitor MB8000 activity. Serial port setup is described in “Troubleshooting”.

## 5.3 Reset to Factory Default Procedure

Use this procedure to reset the network configuration values, including the MB8000 IP Address, Subnet Mask, and so on. The current MB8000 Software will not be deleted. This procedure may be required if the password is forgotten or the configurations are forgotten.

When MB8000 is working in normal status, press and holds the **RELOAD** button for more than 30 seconds, until all the indicator lights turn off. Then release **RELOAD** button, press the **RESET** button to set up the device again. 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 15 seconds immediately after the MB8000 is power on or reset, the MB8000 will enter into Force Reload Procedure. The software in the MB8000 will be erased. You will have to download software into MB8000 to make it work again.

## 5.4 Forced Reload Procedure

Use this procedure to force the MB8000 back to default network configuration values and download new MB8000 software. This procedure may be required when the current MB8000 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](http://www.solarwinds.net). You can also search other TFTP servers from the Internet if you like.
2. To download the MB8000 Software, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN, or connected to the MB8000's "LAN" port with a "crossover" Ethernet cable.
3. After force reload, MB8000's IP will be set to 10.0.0.1 by default, and MB8000 will login the TFTP server with IP address "10.0.0.2" to download software named "filename" by default. So please change the IP address of TFTP server to 10.0.0.2, and change the MB8000 software name to FILENAME, put it in the directory of TFTP server root.
4. After finishing this preparation, power up the MB8000.
5. Press the RESET button.
6. Press and hold the RELOAD button for about 15 seconds immediately after you press and release the RESET button until the POWER LED turns amber. Result: The MB8000 deletes the current MB8000 software and Configuration files. Then MB8000 will download the software you have prepared in the step 3. Observe the TFTP display and you should see downloading activity begin after a few seconds.
7. MB8000 will be configured to the factory default value. Please refer Table 6-1 for the factory default value.

## 5.5 Firmware Upgrade Procedure through Web

Use this procedure to upgrade the newest version firmware for MB8000 through Web interface on user client. This procedure may be necessary when a new version firmware is released.

1. Prepare you TFTP server. TFTP server can be one computer with TFTP server software running. The TFTP server can be freely downloaded from [www.solarwinds.net](http://www.solarwinds.net) or you can use the one on attached CD. You can also search

- other TFTP servers from the Internet if you like.
2. To download the new version MB8000 firmware to MB, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN, or connected to the MB8000's "LAN" port with a "crossover" Ethernet cable attached in the MB8000 package.
  3. Refer to part 3.3.4.1 "Download & Upload" in this document, set the IP Address of the TFTP server (it is the IP address of the computer where the TFTP server resides, this IP address must be in the same subnet as IP address of MB8000 itself).
  4. Set the File Name you want to download on TFTP server.
  5. Change the File Type to Img.
  6. Change the File Operation to Download or Download&reboot.
  7. Click OK.
  8. The firmware will begin to be downloaded into MB8000.



**Warning:**

You shall reboot the MB8000 by yourself after the firmware has been downloaded into MB8000, if the File Operation you select is "Download".

## 5.6 Scan Tool utility

Use Scan Tool to initialize units and download image files for any unit connected to the LAN subnet. If your MB8000 is in normal status, you can set the IP Address and IP mask of MB8000. If your MB8000 is under the condition of Force Reload (See 5.4), you can set IP Address and mask, TFTP Server Address, TFTP filename. The **Scan Tool.exe** application is included on the installation CD-ROM.

**NOTE:**

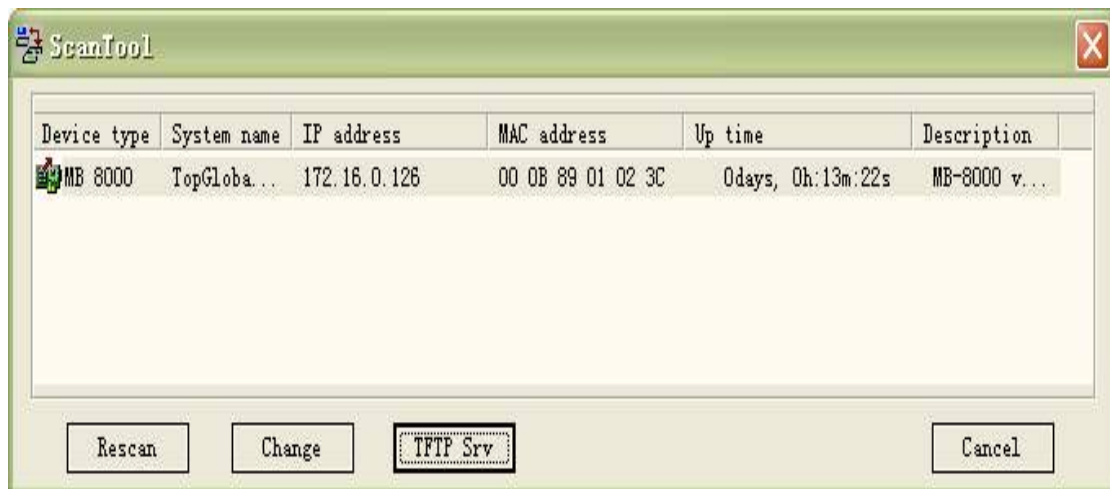
Scan Tool is very useful because units can be installed without prior bench initialization. To track units, you must record the MAC Address and physical location of each unit during installation. Since Scan Tool identifies each unit by its MAC Address, you can install multiple units simultaneously and initialize them from Scan Tool.

Use the following procedure to open Scan Tool and set MB8000 network parameters. You should have the MB8000 unit(s) and your computer connected to the same LAN subnet.

1. Install the MB8000 hardware and connect the unit(s) to the LAN.
2. Power up, reboot, or reset the MB8000.
3. Open Scan Tool. Result: Scan Tool scans the subnet and locates all MB8000 units.

The Scan Tool **Main** screen appears, similar to the example below, which shows a single unit in the factory default state.

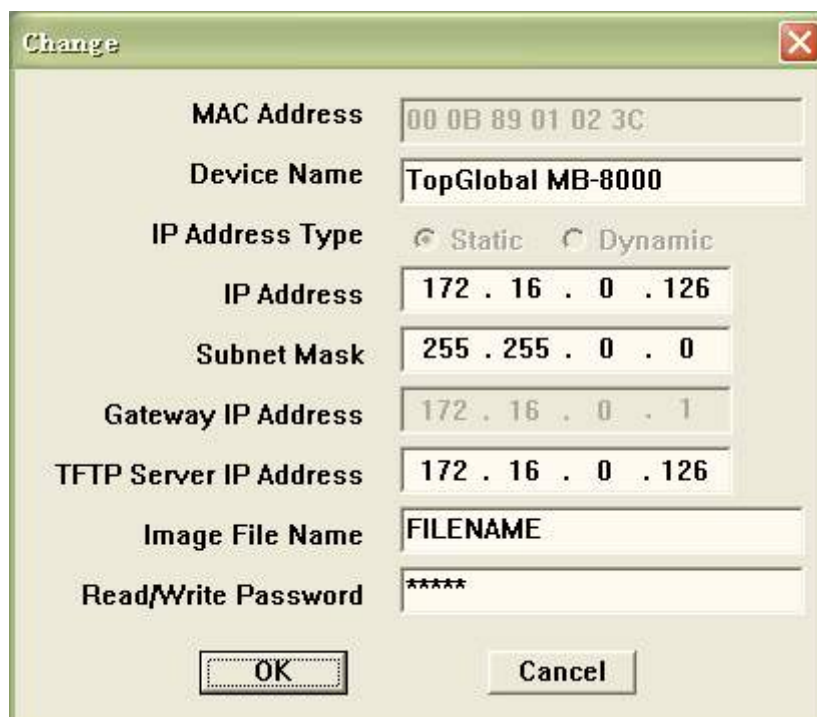
Figure 5-1 **Scan Tool**



To re-scan the network and update the display after changing values, click the **Rescan** button.

To change values or download an MB Image, select the desired unit, and then click the **Change** button. Result: the Scan Tool **Change** screen appears, similar to the following example. Our example shows a unit with factory default settings.

Figure 5-2 **Change**



You may perform the following operations.

- **MAC Address.** This read-only field displays the MAC Address of the selected unit.
- **Name.** Enter the System Name of the unit. This is typically descriptive text, such as “Main Lobby”.
- **IP Address Type.** This read-only field displays the type by which you gained the IP Address.
- **IP Address.** Enter the IP Address.
- **Subnet Mask.** Enter the Subnet Mask.
- **Gateway IP Address.** This read-only field shows the default IP Address of the Gateway.
- **TFTP Server IP Address.** If you wish to download a new MB Image file, then enter the IP Address of the TFTP server.
- **Image File Name.** If you wish to download a new MB Image file, then enter file name.
- **Read/Write Password.** Enter the read/write password. The default password is “public”.

To reboot the unit to make the changes effective, verify the entered values and then click the **OK** button. Result: The unit will reboot and the new values will be in effect.

To cancel the operation and return to the Scan Tool **Main** screen, click the **Cancel** button.



**Note:**

If you wish to download a new MB Image file, you must run a TFTP Server. Tftpd32.exe is a free product and is included on the installation CD-ROM. To launch this TFTP Server, please click the **TFTP Srv** button.

Figure 5-3 **TFTP Server**





## 6. Default MB8000 Settings

The following table lists the settings defined at the factory for all MB8000 units, and provides a place to enter values for your system.

Table 6-1 **Default Setting**

Item	Default Value	My System Value
Local IP Address	172.16.0.1	
Local IP Mask	255.255.0.0	
Network Name(SSID)	mbnet	
Frequency Channel	3	
DHCP Server Status	Enabled	
TFTP Server IP Address	10.0.0.2	
TFTP File Name	FILENAME	
Http Username	Public	
Http Password	Public	
CLI Password	Public	
Wireless	phone number	"#777"
WAN default setting:	username	"card"
	password	"card"
	Init string	"AT&F"

## Federal Communication Commission Interference Statement

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.
- (2) This device must accept any interference received, including interference that may cause undesired operation.



**Note:**

This equipment has been tested and found to comply with the limit of 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 or more 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.