

TopGlobal MB8000 Hotspots Solution

TopGlobal's MB8000 is a mobile/portable wireless communication gateway. It combines the best of Wi-Fi technology and 2.5G/3G mobile communication technology. WISP can deploy their wireless hotspots with MB8000 rapidly with minimal installation and maintenance.

MB8000 has many significant features which are suitable for wireless hotspots. MB8000 has a build-in RADIUS client module, which implements a widely used protocol for authentication, authorization and accounting (AAA), and MB8000 does access control according to the result of AAA.

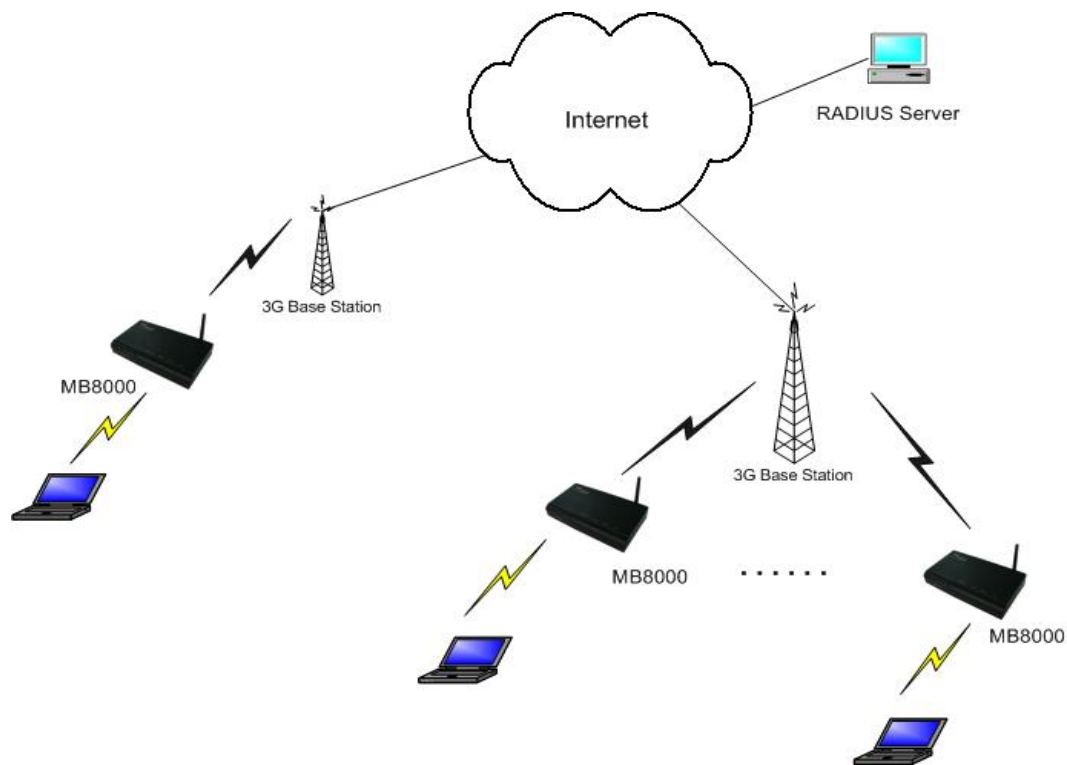
This application notes shows how to deploy a wireless hotspot rapidly with MB8000.

How does MB8000 meet the requirements for a hotspot deployment

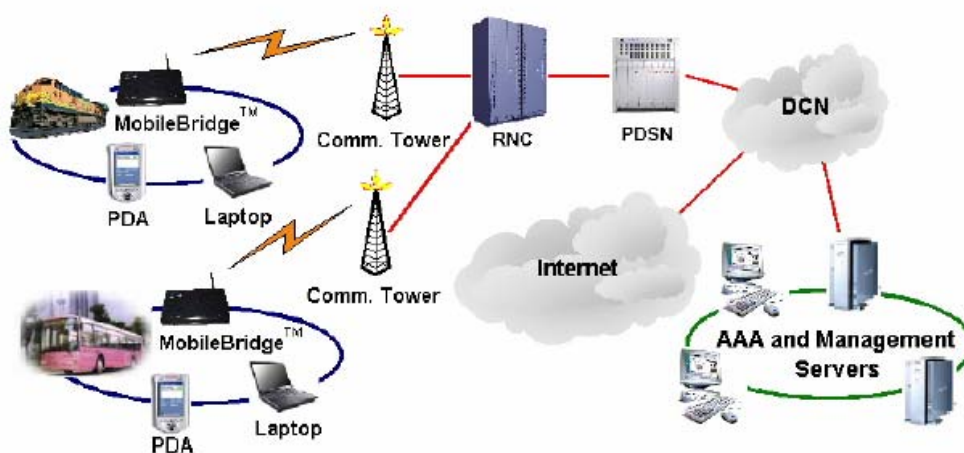
- ✓ MB8000 is configurable to run a DHCP Server or to act as a DHCP relay agent for assignment of end-user IP address. An end-user can obtain a dynamic IP address from MB8000.
- ✓ MB8000 implements RADIUS Client. When configured to enabled, it will send authentication request packets to the RADIUS Server when an access request received. The end-users can access the Internet only after pass the authentication successfully.
- ✓ MB8000 supports RADIUS MAC authentication, IEEE 802.1X and WEB Portal authentication.
 - RADIUS MAC authentication: The MAC address of the end-user's WLAN card will be regarded as a unique ID (username) to authenticate by RADIUS Server.
 - 802.1X authentication: MB8000 supports many EAP types for 802.1X authentication, such as: EAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, and so on. This needs the end-users have IEEE 802.1X supplicant installed and the RADIUS Server must support EAP authentication.
 - WEB Portal authentication: This is the most convenient method for the end-users. They don't need to install any additional software or any extra configurations on their laptops or handsets. When an end-user attempts to access the Internet, MB8000 would prompt an IE window to request for the username and password and then send an authentication request to the RADIUS Server to authenticate this user. Note that the end-user's password will never presented in the network traffic all through the procedure.
 - When using WEB Portal, MB8000 supports SSL for the HTTPs POST when the end-users post their credentials for the authentication.
 - MB8000 also can redirect the unauthenticated user's HTTP GET request to a login page hosted by a remote WEB Server. This enhances roaming agreement for the wireless ISPs.
- ✓ MB8000 supports RADIUS accounting. It will send accounting requests to the specified RADIUS accounting server when an accounting session starting and stopping, and send interim accounting requests periodically during the session.

- ✓ MB8000 provides variable data encryption to protect WLAN privacy: 40/128bit WEP encryption and WPA TKIP encryption. MB8000 is configurable to reject bad-guys from accessing the network by setting MAC address filter. And when setting InterBSS relay to disabled, the end-users in the same BSS will not be able to access each other directly. This protects the privacy of the end-users in a public wireless network.
- ✓ MB8000 can be managed concentratively by TopGlobal RCM (Remote Central Management) system, which is software that can manage and configure MB8000 in group, remotely and concentratively.
- ✓ MB8000 supports a secondary RADIUS Server as a backup in case of the primary Server be down or unavailable. Also, WISPs can deploy their RADIUS Authentication Server and RADIUS Accounting Server as two independent servers, which could be located in two places.

Application scenario1: Deploy Hotspots with TopGlobal MB8000



With TopGlobal MB8000, WISPs can deploy their hotspots and mobile hotspots rapidly with low cost. The wireless hotspots can be widely deployed in any places of 3G coverage, the airports, cafés, and gymnasiums, even in the job sites, the train, the buses and yachts.



Application scenario2: Deploy Hotspots as a member of Airpath Provider Alliance with TopGlobal MB8000

Airpath Provider Alliance (APA) is Airpath's proprietary back-end settlement and clearinghouse for tying Hot Spots into one large ubiquitous network. You may reference to <http://www.airpath.com> to get more information and business model. Deploy your hotspots and join APA, the users will come.

TopGlobal MB8000 has been approved by Airpath Approval. This means that MB8000 can be deployed and used with Airpath systems straightforward. You don't have to deploy your own AAA and billing system, nor plenty of Advertisement to attract users. Joined the APA, you may share the APA's users and clients.

MB8000 Configurations for Hotspot

You may need 3 steps to finish the configuration for hotspot.

Step1. Choose and configure the authentication scheme:

You may choose one of the following 3 authentication scheme:

- 1) Configure to RADIUS MAC: Login to the MB8000's configuration page, go to "Advanced"->"RADIUS Authentication" page, and set the "RADIUS MAC Access Control Status" to "Enable".
- 2) Configure to 802.1X authentication: Go to the "Advanced"->"Encryption" page, and set the "Network Authentication" to "NonWPA-802dot1XOnly", or "WPA". We strongly suggest that "WPA" be selected.
- 3) Configure to WEB Portal: Go to the "Advanced"->"WEB Portal" page, and set the "WEB Portal Status" to "Enable".

Step2. Configure the RADIUS settings:

1) Go to "Advanced"->"RADIUS Authentication" page, according to the network TOPO, you need to select one interface for the MB8000 communicating with the RADIUS Server. If the RADIUS Server is connected with MB8000 in a wired-LAN, you may set this value to "LAN" in

the “Interface” field, else “WAN” might be selected.

2) Configure the primary RADIUS authentication server for user authentication. The “Server Status” field MUST set to “Enable”, and then fill in the IP address and shared secret.

RADIUS Server:	Server 1
Server Status:	Enable
IP Address:	0.0.0.0
Destination Port:	1812
Response Time (sec):	3
Shared Secret:	*****
Confirm Shared Secret:	*****
Maximum Retransmissions:	3

If you have a secondary RADIUS authentication server, you may fill in the settings just as the primary one.

3) Configure the primary RADIUS accounting server for accounting. The “Server Status” field MUST set to “Enable”, and then fill in the IP address and shared secret.

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:	*****

If you have a secondary RADIUS accounting server, you may fill in the settings just as the primary one.

Step3. Configure the WLAN data encryption scheme:

You might decide the WLAN data encryption scheme according to your hotspot’s operation. You can choose a non-encryption network or WEP encryption or TKIP encryption.

- 1) Non-encryption network: Go to the “Advanced”->“Encryption” page, and set the “Network Authentication” field to “Open”, make sure that “Data Encryption” field be set to “Disable” as following settings:

Setup — **security** — Encryption

Network Authentication:	Open
Data Encryption:	Disable
Key Length:	40 bit
Deny Non-Encrypted Data:	Disable

- 2) 40/128bit WEP encryption: The following figure shows typical 40bit WEP encryption

settings. You can set 128bit WEP encryption if needed.

SetUp — **security** — Encryption

Network Authentication:

Data Encryption:

Key Length:

Deny Non-Encrypted Data:

The **Encryption Key** needs to be 40 bits or 104 bits depending on the **Key Length** configuration above. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Encryption Key1:

Encryption Key2:

Encryption Key3:

Encryption Key4:

Encrypt Data Transmissions Using:

- 3) TKIP encryption: Set “Network Authentication” field to “WPA” or “WPA-PSK”, TKIP encryption scheme will be automatically selected.

Annex: RADIUS Attributes that MB8000 supports

RADIUS Attributes	Auth Request	Auth Reply	Accounting Request	
[1]User-Name	✓		✓	
[2]User-Password	✓			
[4]NAS-IP-Address	✓		✓	
[6]Service-Type	✓			
[8]Framed-IP-Address	✓		✓	
[18]Reply-Message		✓		
[24]State	✓	✓		
[25]Class		✓	✓	
[27]Session-Timeout		✓		
[28]Idle-Timeout		✓		
[30]Called-Station-ID	✓		✓	
[31]Calling-Station-ID	✓		✓	
[32]NAS-ID	✓		✓	
[40]Acct-Status-Type			✓	1 - Start, 2 - Stop, 3 - Interim Update
[41]Acct-Delay-Time			✓	
[42]Acct-Input-Octets			✓	
[43]Acct-Output-Octets			✓	
[44]Acct-Session-ID	✓	✓	✓	
[46]Acct-Session-Time			✓	

[47]Acct-Input-Packets			✓	
[48]Acct-Output-Packets			✓	
[49]Acct-Terminate-Case			✓	
[61]NAS-Port-Type	✓		✓	15 - Ethernet, 19 - 802.11
[85]Acct-interim-Interval		✓		