

MB8000 Network Security and Access Control

Overview

MB8000 employs almost all of the current popular WLAN security mechanisms. These include wireless-user isolation, closed system (by turning off SSID broadcasting), MAC filtering, WEP encryption, WPA-PSK (TKIP) encryption.

If you have your own RADIUS scheme deployed, you can also use IEEE 802.1x, WEB Portal, WPA and RADIUS MAC for access control.

Also, you can combine two or several of these security mechanisms for your MB8000 deployment.

1. Wireless-User Isolation

Wireless-user isolation, also known as the layer 2 isolation, is a security mechanism defined by IEEE802.11 standard. MB8000 adheres to this standard. When the layer 2 isolation is enabled, the wireless stations that associated with the access point (here is MB8000) CANNOT access each other by Wi-Fi. This provides a useful security for the users in the wireless hot spots.

To configure MB8000 to work in layer 2 isolation, you may login to its WEB page and go to "**Basic**"->"**WLAN Card**" page. And then set IBSS Relay Status field to "**Disable**". As depicted in figure 1 below:

The screenshot shows the configuration page for the 'WLAN Card'. On the left is a navigation menu with 'Basic' selected, and sub-items for 'Wireless Internet', 'Local IP Configuration', and 'WLAN Card'. The main content area is titled 'Setup - Wireless Card - Wireless Card'. It contains several configuration fields:

- Wireless Card Status: (dropdown)
- Network Name(SSID):
- Frequency Channel: (dropdown)
- Closed System Status: (dropdown)
- IBSS Relay Status: (dropdown)** (highlighted with a red circle)
- MAC Address:

At the bottom of the page are two buttons: 'OK' and 'Cancel'.

Figure 1. Layer 2 isolation.

2. Closed System

When the SSID broadcasting is turned off, your network is “closed” to the strangers. A wireless station can only associate with MB8000 with the exactly SSID. To do this on MB8000, please browse MB8000’s configuration WEB page and go to “**Basic**” -> “**WLAN Card**” page. Find “**Closed System Status**” field on this page and set it to “**Enable**” by clicking the drop list. Show as figure 2.

The screenshot shows a configuration window with a sidebar on the left containing menu items: 'Basic', 'Wireless Internet', 'Local IP Configuration', and 'WLAN Card'. The main area is titled 'Setup — Wireless Card — Wireless Card'. It contains several configuration fields:

- Wireless Card Status: Enable (dropdown)
- Network Name(SSID): Topglobal (text input)
- Frequency Channel: 3- 2.422 GHz (dropdown)
- Closed System Status: Enable (dropdown)** (highlighted with a red oval)
- IBSS Relay Status: Enable (dropdown)
- MAC Address: 00:00:00:00:00:0

At the bottom of the window are 'OK' and 'Cancel' buttons.

Figure 2. To turn off SSID broadcasting.

It is a fairly weak method for a wireless network security by just only turning off SSID broadcasting. Hackers can use 802.11 analysis tools (e.g. Airopeek or Netstumbler) to find out the SSID even through the SSID broadcasting is turned off, because the SSID is still presented in the 802.11 association request frames. The hackers just need to wait for an authentic wireless station associates with the network.

3. MAC filtering

Mb8000 offers a mechanism for MAC filtering. There is a MAC address table (so called “**MAC Access Table**”) contained in MB8000. Each entry in this table belongs to a wireless client (WLAN card). And there are two filtering policies for the wireless clients that listed on this table: **Allow** or **Deny**. When the filtering policy is set to “**Allow**”, then only the wireless clients that listed on this table can connect to MB8000 to access the Internet through this MB8000 unit. Any other wireless clients cannot gain the access authorization.

And vice versa, when the filtering policy is set to “*Deny*”, MB8000 will prevent the listed wireless clients from connecting. It is something like a “Black List” in this case.

To enable, disable MAC filtering status, or to configure the filtering policy, as well as to add, delete or edit the MAC addresses to the “*MAC Access Table*”, please browse “*Advanced*” -> “*Filters*” page.

Figure 3 shows a sample configuration on the “*Allow*” policy.

SetUp — security — Filter

MAC Access Control Status: ▾

MAC Access Control Operation Type: ▾ Filtering Policy.

MAC Access Table:

| MAC Address | Comment | EntryStatus |
|-------------------|-------------------------------|-------------|
| 00:31:5E:01:90:A8 | My own WLAN card. | Enable |
| 00:08:73:52:3E:7F | My network admin's WLAN card. | Enable |

Figure 3. A sample configuration for allowed MACs.

First of all, you need to enable the MAC filtering by selecting “*Enable*” on the drop list for “*MAC Access Control Status*” field, and then set the filtering policy to “*Allow*”. Click “*OK*” to save the changes, and then click “*Add*” to add a new MAC address to the “*MAC Access Table*”. You can also edit or delete an existed entry by clicking “*Edit*”. To delete an entry from the table, please “*Edit*” and then set the “*EntryStatus*” to “*Deleted*”. As depicted in figure 4.

| MAC Address | Comment | EntryStatus |
|--|--|--|
| <input type="text" value="00:31:5E:01:90:A8"/> | <input type="text" value="My own WLAN card."/> | <input type="button" value="Enable"/> ▾ |
| <input type="text" value="00:08:73:52:3E:7F"/> | <input type="text" value="My network admin's WLAN card."/> | <input type="button" value="Deleted"/> ▾ |

Figure 4. To delete an MAC address entry.

Figure 5 shows a sample configuration on the “*Deny*” policy.

SetUp — security — Filter

MAC Access Control Status:

MAC Access Control Operation Type: *Filtering Policy*

MAC Access Table:

| MAC Address | Comment | EntryStatus |
|-------------------|--------------------|-------------|
| 00:31:5E:01:90:A8 | This is a bad guy. | Enable |
| 00:08:73:52:3E:7F | Also a bad guy. | Enable |

Figure 5. A sample configuration for denied MACs.

It is a fairly good scheme to apply MAC filtering on a small wireless network for small companies or SOHO users. But when more and more users are added or more MB8000s are deployed, it is a nightmare for the network administrator to maintain such a table for MAC addresses. Because he must manually add a new MAC entry to the table on each MB8000 once a new user is added or delete one when a user leaves or his wireless card lost. MB8000 provides a centralized MAC filtering mechanism to address this issue, which is so-called RADIUS MAC authentication in MB8000. Please reference to “[Application Note for RADIUS MAC.pdf](#)” for more detail.

4. WEP Encryption

WEP (Wired Equivalent Privacy) is introduced to IEEE 802.11 networks, which encrypts the payload in the 802.11 frames. The WEP key is also used to authenticate a wireless station which tries to associate with the access point (here it means MB8000). When WEP key is used to authenticate the wireless station, only the wireless stations with the exactly WEP keys can associate with the access point. Thus the strangers will be kept out.

The WEP encryption is supposed to keep hackers or eavesdroppers from viewing sensitive emails, usernames and passwords, etc. It was proven that a person can easily decode WEP-Encrypted information after monitoring an active network for less than one day and then he can access your network also. As an expert in WLAN security, Top Global does not advise you rely on WEP for protecting your sensitive information. However, WEP security mechanism is better than no encryption at all, especially for the people who just want to keep out the passive eavesdroppers.

To configure WEP security mechanism on MB8000, please reference to “**Application Note for MB8000 WEP Encryption.pdf**” for more detail.

5. WPA and WPA-PSK

As we already known, WEP is inadequate for securing wireless network. WPA (Wi-Fi Protected Access) is raised by Wi-Fi Alliance in 2003 to address to the security issues on wireless network. WPA utilizes TKIP (Temporal Key Integrity Protocol) on data encryption to address to the WEP's vulnerability. And also, IEEE 802.1X is introduced to WPA for the enterprise users who have their authentication server (such as RADIUS) deployed. With 802.1X, TLS/TTLS/PEAP can be used for authentication. For the small firm or home/SOHO users, WPA defines a brief mode without authentication server deployment. In this mode, a Pre-Shared Key (PSK) is used to authenticate users.

With WPA deployed, users can connect to the wireless network only after they pass the IEEE802.1X authentication with their credentials. And with WPA-PSK, only the users who owes the exactly PSK could be able to connect to the wireless network.

What's more, Microsoft Windows XP with SP2 offers official standard WPA/WPA-PSK client software, so the users needn't install any extra software on their computers.

Top Global MB8000 adheres to WPA specification to enhance the security on WLAN. And WPA/WPA-PSK is recommended by Top Global, especially for the enterprise users. Please reference to “**Application Note for MB8000 WPA.pdf**” for more detail configuration.

6. WEB Portal

WPA and WPA-PSK is a wonderful solution for the wireless network security. But for the Wi-Fi hot spots deployment, it may lead to a lot of inconvenience for the hot spot users, as well as a lot of requests for technical support from their customers. MB8000 also provides a mechanism for access control, which is “WEB Portal”.

With WEB Portal deployed, a user cannot access the Internet through MB8000 before he passes the authentication. When an unauthenticated user tries to browse the Internet, he will be redirected to a login page. He MUST input his proper username and the password to pass the authentication.

For the small firm without RADIUS service deployed, MB8000 provides a local user table on itself. The administrator can add, edit or delete user entries on this table. When a user tries to login with his username and password, MB8000 will look up this table to verify that. For the operators and ISPs with RADIUS service deployed, MB8000 adheres to the RADIUS protocol for user authentication as well as accounting. In this case, the username and password will be authenticated by the remote RADIUS server.

For detail configuration, please reference to “**Application Note for WEB Portal.pdf**”.



TOP Global Technology Ltd.

ADDR: 21072 Bake Parkway Suite 106

Lake Forest, CA 92630

TEL: 949-586-7046

FAX: 949-380-4128

<http://www.topglobalusa.com/>
