

Web Portal Access Control

A Most Convenient Wireless Network Authentication Method

Complex WLAN Security

In recent years, the proliferation of laptop computers and PDA's has caused an increase in the range of places people perform computing. At the same time, network connectivity is becoming an increasingly integral part of computing environment. As a result, wireless network of various kinds have gained much popularity.

Meanwhile, Top Global's MobileBridge™ integrates the WLAN and 2.5/3G cell-phone network and acts as a router between those networks. MobileBridge™ can make all low-cost WLAN stations to be 2.5/3G terminals, and it brings more flexibility and convenience to the WLAN.

But with the added convenience of wireless access come new problems, not at least of which are heightened security concerns. When transmissions are broadcast over radio waves, interception and masquerading becomes trivial to anyone with a radio, and so there is a need to employ additional mechanisms to protect the communications. So security is one of the major problems for WLAN. Different from the wired network, with WLAN's radio frequencies that in clear air have a range of up to 300 meters, no one knows whether an unauthorized person has accessed the WLAN.

IEEE 802.11 contains several security features, such as MAC access table, Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA).

The MAC access table is a table contains a list of MAC address stored in an AP/AC. Only wireless station with MAC address listed in this table can access to the WLAN network. The WEP works by encrypting traffic. Under WEP, all data traffic is encrypted by a key which is 128 or 256 bits long. To access a WEP enable network, station must have pre-configured the same key as the AP's. Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements. WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption and employs 802.1X authentication with one of the standard Extensible Authentication Protocol (EAP) types available today.

However, those security mechanisms require for both complex station configuration and heavy network administration work. For example, WEP and WPA require that users know the key previously. That introduces much inconvenience for the enterprise application. Every user needs pre-configure his computer before access the network and change his configuration before connect to another network. This brings hard work for the network administration as well, and neutralizes the convenience of wireless network.

Another thing is that every user uses the same key that introduces insecurity for internal eavesdropping.

Convenience Authentication, Authorization and Accounting

No one is willing to face heavy setup process, and people always like things to be easy. Therefore, many wireless networks do not employ any security mechanism. Besides the problems mentioned before, many WLAN application deployments such as Hot Spots may encounter the authentication, authorization and accounting (AAA) issues.

How to balance the security with convenience and solve the AAA issues becomes a major issue for the wireless network.

MB8000 is one of Top Global’s MobileBridge™ serial products, which offers an ideal solution for simple security access – **Web Portal**.

Web portal is an access control method which authenticates users by requiring them to input username and password on web pages. This method needs no station configuration and minimal management of MB8000. And one user’s change about the username and password would not affect others, this minimize network administrator’s work as well.

There are 2 ways of web portal, a local one and a global one.

In the local method, MB8000 maintains a table of local users itself. Users can use the username and password in this table to access network. As the following figure 1, after laptop associate with and get IP from MB8000, it would prompt a window to require for user name and password before user connect to Internet. User can access to Internet only after providing proper username and password in the table of MB8000. This kind of authentication does not require deploying authentication server such as RADIUS. It is very suitable for the home and small enterprises. Accordingly, this scheme does not support accounting.

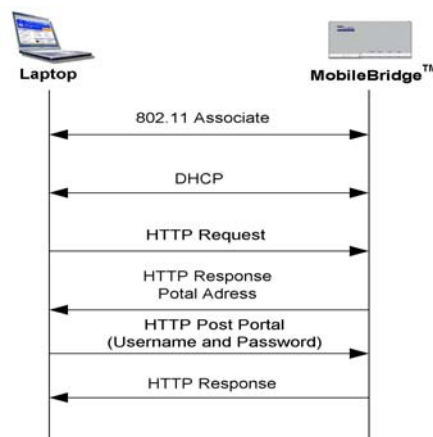


Figure 1. Local Web Portal

In the global method, network administrator needs to configure an IP address of RADIUS server to MB8000. When the end-users open their browser to browse the desired WEB sites, a popup window will gather their login credentials (username/password) and then post these information back to the MB8000. MB8000 will send those username and password, as well as the MAC address and IP address, to the pre-configured RADIUS server. The server validates those credentials and will send the result back. If the authentication success, the authenticated

users will get the authorization to connect to the Internet. In this case, if the RADIUS accounting is enabled, MB8000 will then start to send accounting requests to the RADIUS accounting server. Otherwise, the user is not a valid user and will be disconnected by MB8000.

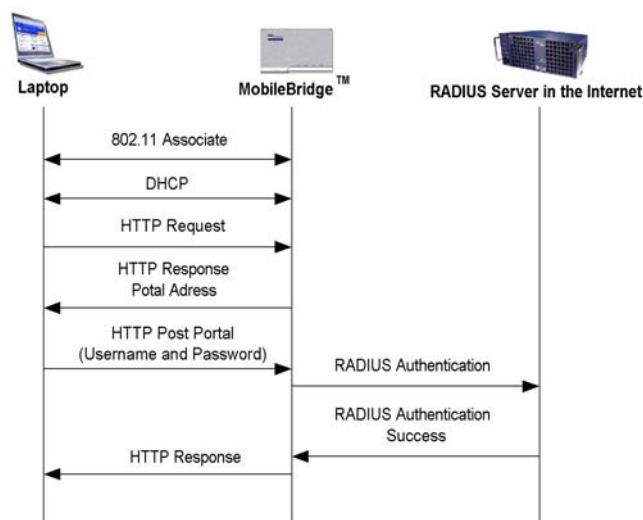


Figure 2. Global Web Portal

More Advantages of Web Portal

As mentioned in previous section, web portal is a most convenient method for wireless user authentication. Besides that, web portal also provides a way to start the accounting. MB8000 adheres to the RADIUS RFC standards. The accounting begins right after RADIUS authentication success and ends after user close the web portal window. Also web portal can be used for logging out idle user. User idles more than pre specified time would be automatically logout by MB8000. The idle timeout can be either specified on the WEB configuration page as default to all users, or by RADIUS server for each single user. Besides that, the RADIUS server can also specify a session time to timeout the authenticated user. When the session timeout or idle timeout occurs, MB8000 will send an ACCT-STOP request to the RADIUS Server to stop the accounting session, and will also take back the network access authorization for that user, thus the user will not be able to access the Internet unless he gains another authorized session.

When using WEB Portal to take the user access control, the WLAN security scheme such as WEP encryption and WPA-PSK can also be combined with it. For more details on WEP encryption and WPA-PSK, you may reference to the user guide of MB8000.

The user's password will never be presented on the network in plain text, while it has been hidden by the algorithm of MD5. MB8000 WEB Portal provides SSL (https) method to encrypt the user's credential. This will protect the username and password privacy in furthest.

Application Scenario 1: WEB Portal based on the local user database

Here shows an application scenario for MB8000 WEB Portal. In this scenario, the

authentication is based on the local user database resident in MB8000 itself. It doesn't need any extra backend authentication server. As shown in the figure 3 below, the network administrator only need to deploy the MB8000 device with a 3G wireless WAN card (PCMCIA), and set the WEB Portal status to "Enable" in MB8000. Users can access the Internet through the MB8000 only after they pass the authentication and gain the authorization.

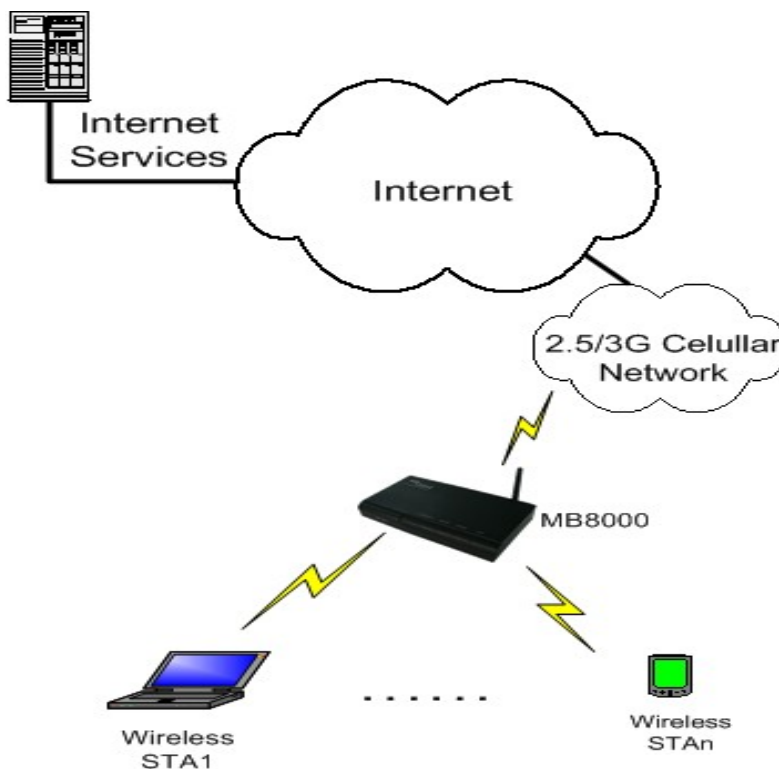


Figure 3. Local user based WEB Portal access control

To enable the WEB Portal access control and use local user database for authentication, the administrator should login to the MB8000 WEB configuration page and go to "Advanced" -> "Web Portal" page, which is shown in figure 4.

Setup — **security** — Web Portal

Web Portal Status:

AliveTimeouts:

Local User Base Status:

User Base Table:

User Name	Entry Status
<i>test</i>	<i>Enable</i>
<i>testtc</i>	<i>Enable</i>
<i>test2</i>	<i>Enable</i>
<i>test3</i>	<i>Enable</i>
<i>test4</i>	<i>Enable</i>
<i>test5</i>	<i>Enable</i>
<i>test6</i>	<i>Enable</i>
<i>test7</i>	<i>Enable</i>
<i>test8</i>	<i>Enable</i>
<i>test9</i>	<i>Enable</i>

Figure 4. WEB Portal setting page

Set “Web Portal Status” to “Enable” to enable WEB Portal access control. The “AliveTimeouts” is the default idle timeout period (in second) for all users. When a user idles more than this period, he will be logout. Importantly, to use the local user database for WEB Portal authentication, the “Local User Base Status” should be set to “Enable”. A default user table is contained in the MB8000. There are 10 entries in the default local user table, with status set to enable as default. The default password for these users is same as the username. The administrator can add new entries or edit these entries.

Application Scenario 2: WEB Portal based on RADIUS server in LAN

Top Global’s MB8000 also support WEB Portal authentication based on the RADIUS architecture. The RADIUS server can be deployed in a LAN to which MB8000 attached by the RJ-45 (10/100 Base-T) Ethernet port on the panel. The MB8000 and the RADIUS server should be in the same subnet. Figure 5 shows a typical network TOPO for this scenario.

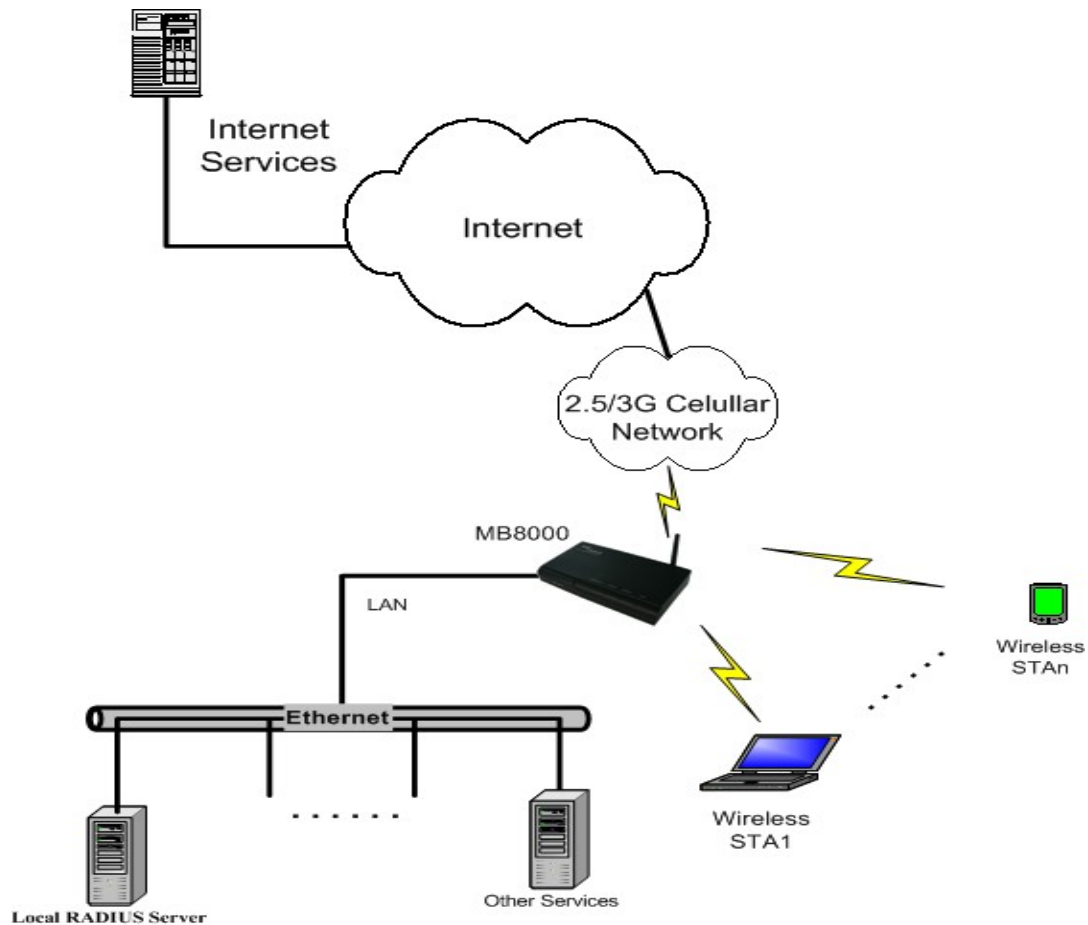


Figure 5. WEB Portal based on the RADIUS server in LAN

The administrator may need to enable WEB Portal access control by logon MB8000's WEB configuration page and go to "Advanced" -> "Web Portal" page (refer to figure 4). The default idle timeout configured in the "AliveTimeouts" field may be replaced by the value in the RADIUS attribute of "[28] Idle-Timeout" if available. The "Local User Base Status" is optional. When a user's credential is provided, MB8000 will firstly look up the local user database to validate the credential if it is enabled. And MB8000 will forward the credential to the remote RADIUS server if the local authentication fails, for example, the username or password is invalid.

You may contact the administrator of the RADIUS server to get some information such as the IP address, the UDP port for the incoming authentication requests and accounting requests, and obtain the shared secret between the RADIUS server and the RADIUS client (MB8000 in this case).

You may also need to go to "Advanced" -> "Radius Authentication" page to configure RADIUS server for MB8000, which is shown in figure 6.

Setup — **security** — Radius Authentication

RADIUS MAC Access Control Status:	<input type="text" value="Disable"/>
Authentication Lifetime (minutes):	<input type="text" value="15"/>
Interface:	<input type="text" value="LAN"/>
RADIUS Server:	<i>Server 1</i>
Server Status:	<input type="text" value="Disable"/>
IP Address:	<input type="text" value="0.0.0.0"/>
Destination Port:	<input type="text" value="1812"/>
Response Time (sec):	<input type="text" value="3"/>
Shared Secret:	<input type="text" value="*****"/>
Confirm Shared Secret:	<input type="text" value="*****"/>
Maximum Retransmissions:	<input type="text" value="3"/>
RADIUS Server:	<i>Server 2</i>
Server Status:	<input type="text" value="Disable"/>
IP Address:	<input type="text" value="0.0.0.0"/>
Destination Port:	<input type="text" value="1812"/>
Response Time (sec):	<input type="text" value="3"/>
Shared Secret:	<input type="text" value="*****"/>
Confirm Shared Secret:	<input type="text" value="*****"/>
Maximum Retransmissions:	<input type="text" value="3"/>

Figure 6. Settings for RADIUS authentication

Set the “*Interface*” to “*LAN*” and set “*Server Status*” to “*Enable*” and fill the IP address of RADIUS server in “*IP Address*” field. Fill the UDP port in the “*Destination Port*” field. The “*Response Time*” indicates how long in second the MB8000 should wait to resend the authentication request packet if there’s no authentication response from the RADIUS server. The “*Maximum Retransmissions*” specifies how many times the MB8000 should retransmit the authentication request packet before MB8000 regards the RADIUS server is down. If a secondary authentication server is available, you may configure it as “*Server 2*” in this page.

MB8000 supports a failover scheme for RADIUS authentication and accounting. It takes the first RADIUS server as the primary server, and the second as a secondary one. When the primary server is down, MB8000 will try the secondary one, so a round-robin algorithm is performed. So does the MB8000 RADIUS accounting.

To configure MB8000 accounting, you may need to go to “*Advanced*” -> “*Radius Accounting*” page, as shown in figure 7.

Setup — **security** — Radius Accounting

Accounting Server:	<i>Server 1</i>
Server Status:	Disable ▾
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:	*****
Accounting Server:	<i>Server 2</i>
Server Status:	Disable ▾
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:	*****

Figure 7. Settings for RADIUS accounting

Set the “Accounting Server” to “Enable”. The “Accounting Interim Update Interval” specifies how often the MB8000 should send an accounting interim update request to the RADIUS accounting server. And this value may be replaced by the RADIUS attribute “[85] Acct-Interim-Interval” if available. If there is a secondary accounting server is available, you may configure it for MB8000. The RADIUS accounting in MB8000 plays the same rule as authentication between the primary server and the secondary one.

Note: The RADIUS authentication servers and the accounting servers may be same, or different.

Application Scenario 3: WEB Portal based on RADIUS server in WAN

As well as deployed in a LAN with Ethernet cable, RADIUS server also can be deployed on the Internet (WAN). When the RADIUS server is located on the Internet, the totally configurations in MB8000 is same as that of in a LAN, while with the “Interface” field set to “WAN” in “Radius Authentication” page. Figure 8 shows the typical network TOPO for this case.

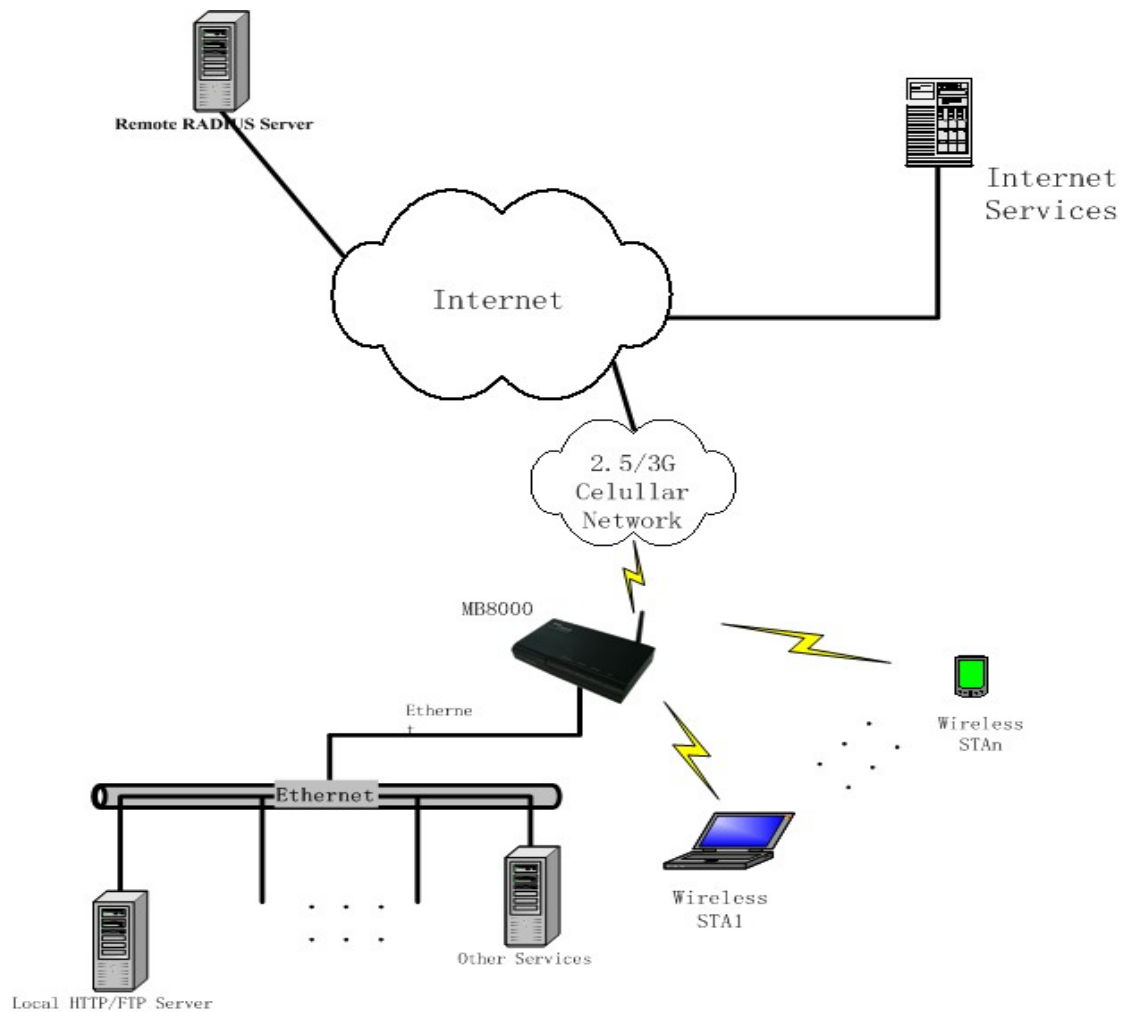


Figure 5. WEB Portal based on the RADIUS server in WAN

Manipulation on the RADIUS server

The RADIUS server needs to validate the RADIUS client who sends the incoming RADIUS request packet. It will look up the RADIUS client from its RADIUS client table by the IP address of the incoming RADIUS request packet. If the RADIUS client is not in the table or the shared secret is mismatch, the RADIUS server will discard the incoming request packet silently. So, to use the RADIUS service, the administrator should add the RADIUS client (here MB8000) to the RADIUS server, including the IP address and the shared secret. The IP address of RADIUS client should be set to the LAN's IP address of MB8000 if "LAN" is selected in the "Radius Authentication" page. Vice versa, the WAN IP address that MB8000 obtains from the dialing up procedure instead if "WAN" is selected. The administrator also needs to add user credentials to the RADIUS server for authentication and accounting.



TOP Global Technology Ltd.

ADDR : 8/F REWARD BUILDING, No.203 Wangjing Li Ze
Zhongyuan, Chaoyang District, Beijing. 100102,China

TEL: +86-010-64390528

FAX: +86-010-64392901

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