

## Wi-Fi Protected Access

### .A brief introduction of the legacy WLAN security and WPA

In 1999, the IEEE 802.11 Working Group proposed WEP protocol as an optional security mechanism on wireless LAN, whose goal is to provide a level of WLAN security similar to that of wired LANs by encrypting WLAN traffic data and preventing unauthorized users from connecting. Unfortunately, WEP has proven inadequate for securing wireless networks. Many security experts have identified the weakness and holes in the WEP specification, which leads WEP fatally failed to meet its design goals. The most notable papers that describe the deficiencies including "Intercepting Mobile Communications: The Insecurity of 802.11." (<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>), "Your 802.11 Wireless Networks Has No Clothes." (<http://www.cs.umd.edu/~waa/wireless.pdf>), "Weaknesses in the Key Scheduling Algorithm of RC4." ([http://downloads.securityfocus.com/library/rc4\\_ksaproc.pdf](http://downloads.securityfocus.com/library/rc4_ksaproc.pdf)).

The WLAN security issues become more and more seriously, but the WEP has been shown to have several vulnerabilities and native 802.11 authentication mechanisms are easily overcome. Wi-Fi Alliance raised WPA (Wi-Fi Protected Access) in 2003, which is derived from the IEEE 802.11i standard as an intermediate WLAN security solution that can be implementing by upgrading the firmware on the deployed WLAN devices. WPA is a specification of standard-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. It is a subset of IEEE 802.11i draft and be forward compatible with the ratified IEEE 802.11i standard. WPA utilizes the TKIP (Temporal Key Integrity Protocol) to improve data encryption, which provides a per-packet key mixing, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules and a re-keying mechanism, and these address all of WEP's known vulnerability. The IEEE 802.1X authentication infrastructure is introduced to WPA. The user authentication using 802.1X is called enterprise mode in WPA, which requires a backend authentication service such as RADIUS. For the home users, WPA also provides a home mode authentication using the Pre-Shared Key (PSK). Thus the WPA specification meets the requisites for the distinct enterprise and home users markets.

### .Top Global WPA security solution

Top Global's MobileBridge™ integrates the WLAN and 2.5/3G cell-phone network and acts as a router between those networks. With a 3G account combining, Top Global's MobileBirdge™ can be deployed as a WLAN Hot Spot any where within the 3G coverage. MB8000 is one of Top Global's MobileBridge™ serial products, which provides enterprise level WLAN security and access control, as well as the carrier-class reliability.

Top Global's MB8000 supports variety of WLAN security mechanisms including 40/128-bit WEP and TKIP (WPA) encryption for WLAN traffic data, WEP authentication and 802.1X authentication and the access control based on the 802.1X. MB8000 supports various EAP (Extensible Authentication Protocol) types including PEAP, EAP-TLS, EAP-TTLS, EAP-SIM and so on. An end-user using Microsoft Windows XP (SP2) can easily connect to MB8000 with

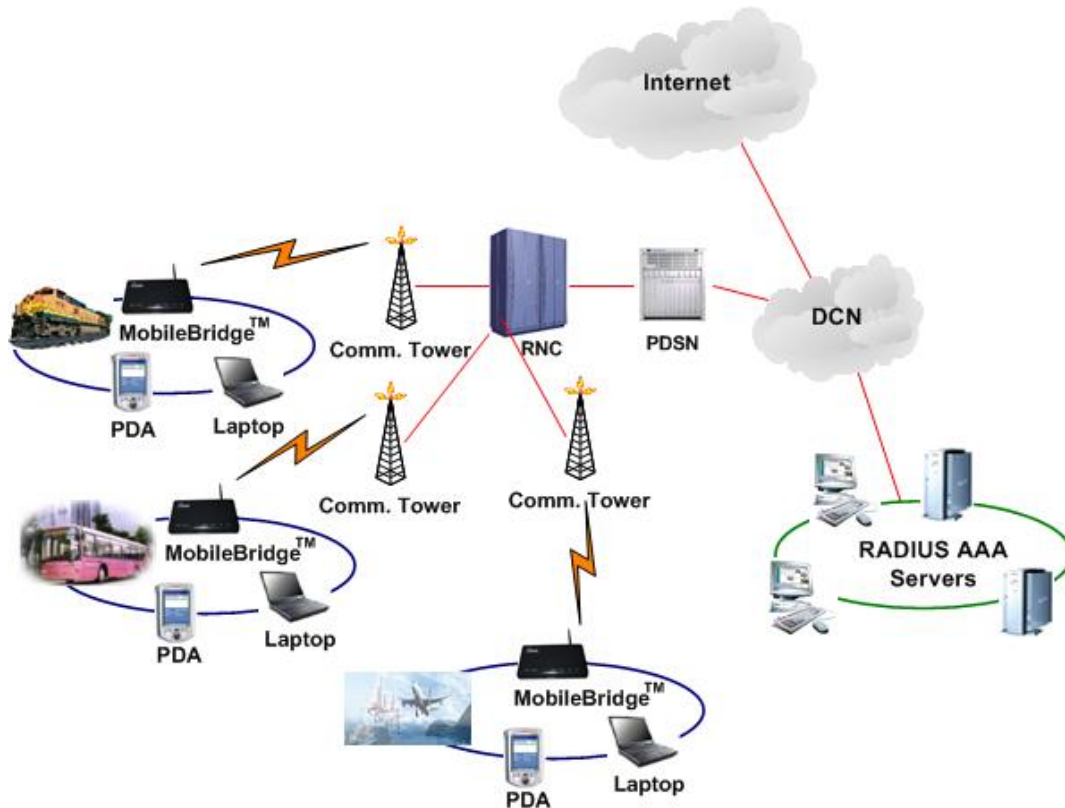
the correct credential.

MB8000 supports the WPA enterprise mode and home (PSK) mode. When operating the WPA enterprise mode, a backend RADIUS server is required.

**.MB8000 deployed for enterprises and Hot Spots**

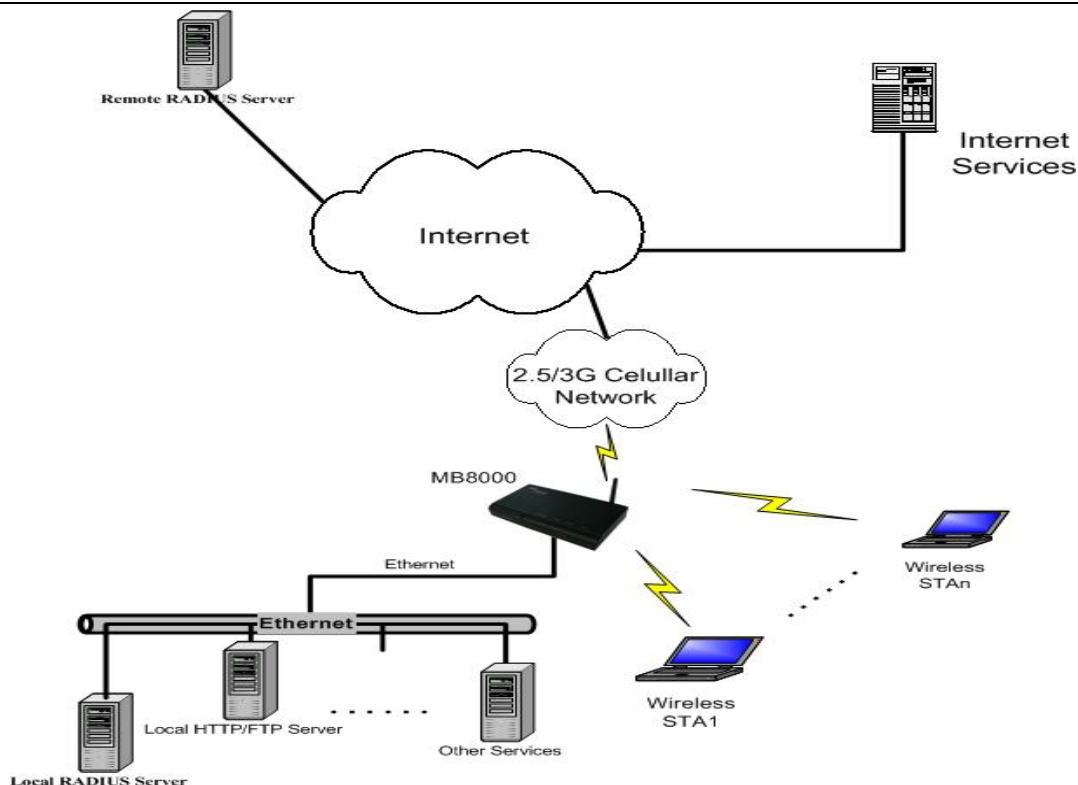
For enterprise users or Hot Spots, MB8000 can be deployed to provide a high level WLAN traffic privacy and access control when utilizing WPA with a backend RADIUS server. The RADIUS server can be deployed in a LAN that the MB8000 attached or in WAN (Internet) that MB8000 can reach.

Top Global’s MB8000 can be used to deploy Wi-Fi Hot Spots easily and rapidly, especially deployed in the mobile Hot Spots such as on the train, the bus, the yacht, and so on.



**Figure 1. MB8000 deployment in the Hot Spots**

The figure 2 shows a typical network TOPO for the deployment.



**Figure 2. A typical MB8000 deployment for enterprise**

**. Configure MB8000 to work in WPA mode**

To configure MB8000 to operate in WPA mode, you may login to its WEB configuration interface and go to the "Advanced" -> "Encryption" page, set "WPA" in the "Network Authentication" field, as figure 3 shows.

**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:

802.1x Re-Authentication Interval:

WPA Group Key Renewal:

WPA Pre-Shared Key(8-63 characters):

**Figure 3. WPA configuration**

When WPA selected, MB8000 will utilize the "TKIP" encryption automatically. WPA needs to

renew the group keys the multicast/broadcast packets periodically, the “*WPA Group Key Renewal*” field indicates this interval, and the default value is 300 seconds. MB8000 may utilize 802.1X re-authentication to renew the user’s login session and re-negotiate the encryption keys periodically, and the “*802.1x Re-Authentication Interval*” field indicates the interval in the figure3.

When using WPA, you should also specify a RADIUS server for MB8000 for the authentication by going to the “*Advanced*” -> “*RADIUS Authentication*” page, which is shown in figure 4.

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

RADIUS MAC Access Control Status:	Disable ▾
Authentication Lifetime (minutes):	15
Interface:	LAN ▾
RADIUS Server:	Server 1
Server Status:	Disable ▾
IP Address:	0.0.0.0
Destination Port:	1812
Response Time (sec):	3
Shared Secret:	*****
Confirm Shared Secret:	*****
Maximum Retransmissions:	3
RADIUS Server:	Server 2
Server Status:	Disable ▾
IP Address:	0.0.0.0
Destination Port:	1812
Response Time (sec):	3
Shared Secret:	*****
Confirm Shared Secret:	*****
Maximum Retransmissions:	3

**Figure 4. Settings for RADIUS authentication**

Set the “*Interface*” to “*LAN*” if the RADIUS server is located in a LAN which MB8000 attaches by its RJ-45, else “*WAN*” should be selected. 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 “*Server2*” 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. And so does the MB8000 RADIUS accounting.

To configure MB8000 accounting, you may need to go to “*Advanced*” -> “*Radius Accounting*” page, as shown in figure 5.

**Setup** — **security** — Radius Accounting

Accounting Server:	Server1
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:	Server2
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 5. 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.

**. Configure MB8000 to work in WPA-PSK mode**

For the home users or small business networks that have no RADIUS server deployment, the WPA-PSK mode may be used. To configure MB8000 to work in the WPA-PSK mode, you may go to the “Advanced” -> “Encryption” page, and set the “Network Authentication” field to “WPA-PSK”, as figure 6 shows.

**Setup** — **security** — Encryption

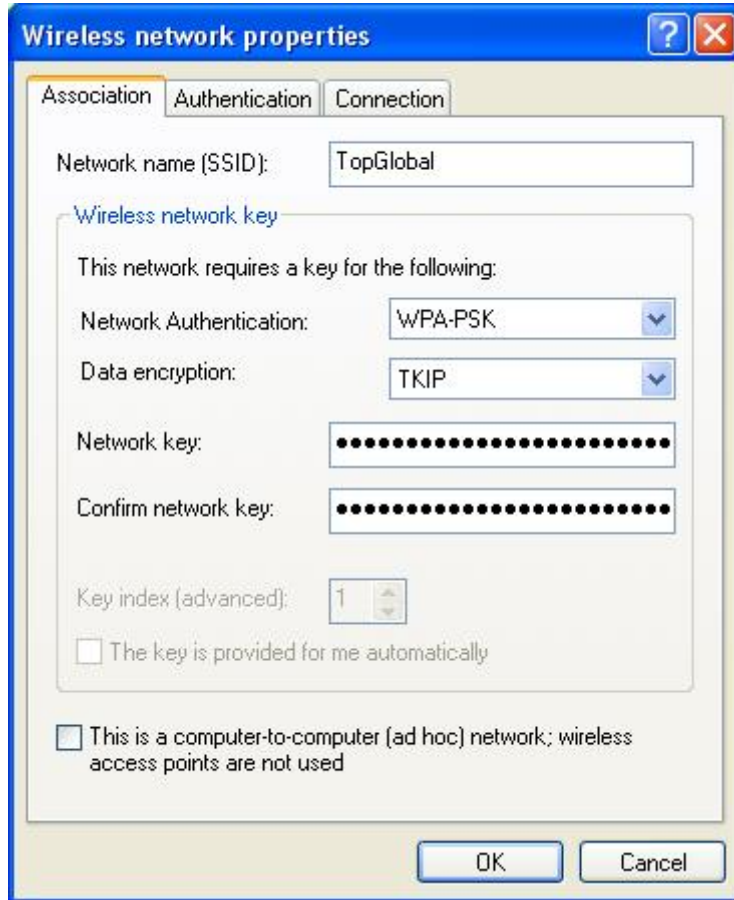
Network Authentication:	<input type="text" value="WPA-PSK"/>
Data Encryption:	<input type="text" value="TKIP"/>
Key Length:	<input type="text" value="40 bit"/>
Deny Non-Encrypted Data:	<input type="text" value="Disable"/>

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:	<input type="text"/>
Encryption Key2:	<input type="text"/>
Encryption Key3:	<input type="text"/>
Encryption Key4:	<input type="text"/>
Encrypt Data Transmissions Using:	<input type="text" value="Key 1"/>
802.1x Re-Authentication Interval:	<input type="text" value="600"/>
WPA Group Key Renewal :	<input type="text" value="300"/>
WPA Pre-Shared Key(8-63 characters):	<input type="text"/>

**Figure 6. WPA-PSK configuration**

When configured to “WPA-PSK” mode, you should fill the pre-shared key (so-called passphrase) in the “WPA Pre-Shared Key” field, 8 to 63 in length, which is shared between MB8000 and the end-users. The end-users should also configure this passphrase as the network key in the **Wireless Network Properties** dialog box in the Microsoft Windows XP (with SP2), as figure 7 shows.



**Figure 7. Example of WPA configuration for Windows XP with SP2**

For more information about the WPA, you may reference to the “Wi-Fi Protected Access (WPA)” section in [“IEEE 802.11 Wireless LAN Security with Microsoft Windows XP”](#).



**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/>

---