

Radius Application Notes using MB-8000

Introduction

Wireless LAN (WLAN) is now a common way to access to internet. Naturally, 3G service providers will extend offerings of data services by WLAN. Using their existing network, customer service, and billing infrastructure, MB-8000 can start their WLAN business rapidly while realizing significant cost savings and operational smoothly. Consequently network administrators have had to deal with two conflicting issues. Network administrators want to provide users with the flexibility and convenience that wireless network access offers while maintaining network security and integrity.

Generally, WLAN can provide two security features: SSID and WEP. Using the 802.11 security features certainly increases the security of the WLAN. However, these features alone do not provide a complete wireless security solution. Radius based security concerns will meet the advanced requirement for WLAN security.

Radius

Radius is a standard for AAA (Authentication, Authorization, and Accounting) service in different operator world. Security, especially controlling access to the network through the use of AAA services is essential for both voice and data. This application notes presents how MB-8000, can be deployed as a gateway between a WLAN and public network resulting in a shared authentication service using Radius protocol for both networks.

MB-8000

MB-8000 is a bridge that connects 3G and Wi-Fi network, and it is a bridge that allows 3G operators to deliver a variety of data services to a multiple and fast proliferating WLAN devices.

Comparing with shortage of killer application of 3G, many new applications are introduced by MB-8000, such as internet access, web browsing, instant messaging, video on demand, as well as any other voice, data, and video traffic.

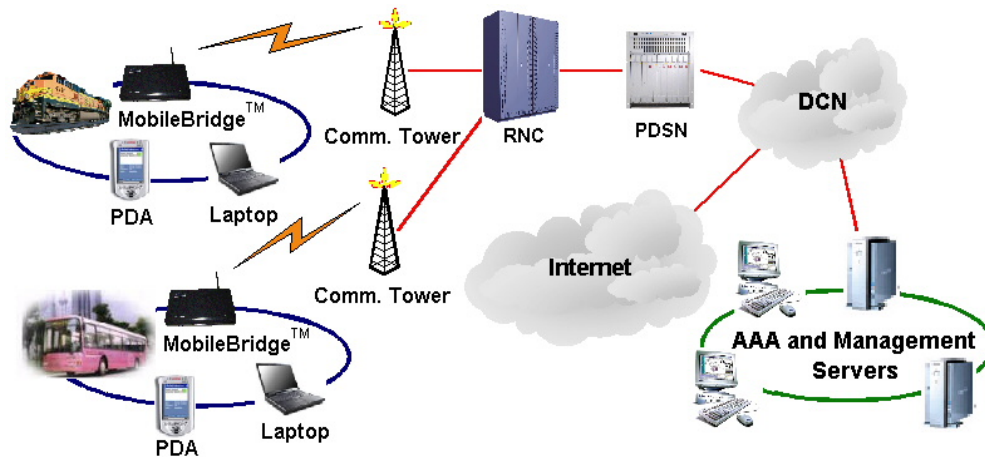
For security, TOP Global MB-8000 supports ESSID suppression, WEP (RC4) encryption, 802.1x port-based authentication and WPA. MB-8000™ offers the secure “Always on, anywhere, anytime” wireless connectivity to subscribers. It also supports VPN and gives the user maximum security.

RADIUS Client in MB-8000™ supports various accounting methods. Operators and WISPs could choose their preferred business model and accounting policies.

For Radius application MB-8000 supports RADIUS authentication and RADIUS accounting.

Application view

Generally, MobileBridge will provide secure access to network for different customers, Mobile Hotspot, ISP and enterprise, with RADIUS server, to fulfill authentication, authorization and accounting.



Typically in a Mobile Hotspot, the operator supplies internet access over 3G wireless link, while customers using Wi-Fi to connect to internet. But how can operators control users' activity of access?

It's commonly used by operators to deploy remote AAA server based on RADIUS protocol. Thus it is very important for device to support RADIUS server used in Mobile Hotspot.

MB8000, with its build-in RADIUS client, can meet this requirement conveniently. Operators just simple enable this feature and configure RADIUS server information in MB8000, and then it can be deployed in any vehicles running in 3G covering area. Customers can access internet and setup a real mobile office; of course, they will have to pass the authentication and authorization through MB8000's Wireless Wan firstly, and network traffic will be accounted by RADIUS server automatically through MB8000.

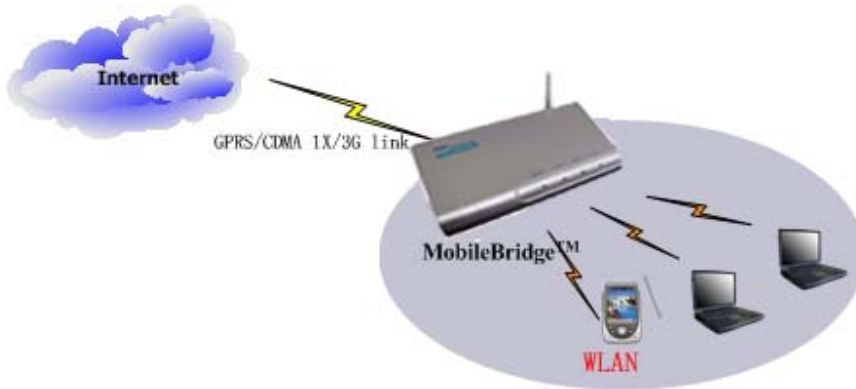
What you need in your Mobile HotSpot?

MB8000, 3G account and public AAA server. In fact, operators will use their old public AAA server just if that's a standard RADIUS server. They need only MB8000 and 3G account, then a Mobile HotSpot will be deployed easily.

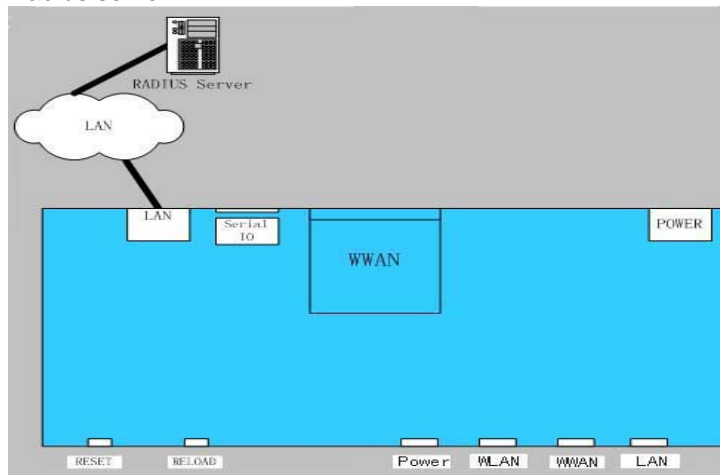
Application structure

Below is a typical application structure for MB8000 in HotSpot.

Figure 1 *MB-8000 network access infrastructure*

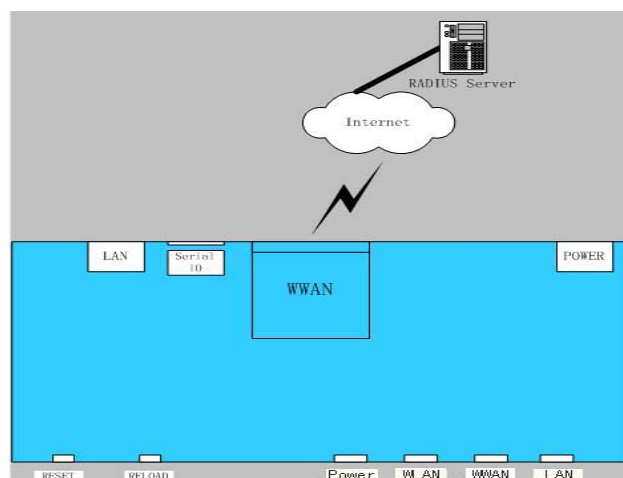


To implement Radius application over MB-8000, we can set up two kinds of infrastructure to support a Radius server.



RADIUS by LAN

In this infrastructure, RADIUS server connects MB-8000 by LAN, local users can access to public network with local LAN server authentication.



RADIUS by WWAN

In this infrastructure, RADIUS server connects MB-8000 by WWAN, 3G operators' air link, local users over WLAN can access to public network with WWAN RADIUS server authentication.

Configuration of MB-8000 to support Radius

MB-8000 supports 2 kinds of RADIUS application: MAC-RADIUS authentication, 802.1x based RADIUS authentication.

To have RADIUS authentication, we need to configure those basic information in MB-8000 first:

- 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.
- Shared Secret: This is the shared key between RADIUS server and MB-8000.
- 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.

MAC-RADIUS

The MAC-RADIUS authentication allows you to control user access by users' 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 are filtered.

To enable MAC-RADIUS

- ◆ Configure "MAC-RADIUS" enabled
- ◆ Add MAC-address
- ◆ Configure RADIUS enabled and basic RADIUS information

802.1X

MB-8000 supports 3 kinds of 802.1x infrastructure as below:

"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 (802.1x default enabled)" means when you select WPA for security, 802.1x infrastructure will be selected by MB-8000 automatically.

To enable 802.1x-RADIUS application in MB-8000

- ◆ Select one method from MB-8000 security encryption
- ◆ Configure correspond parameter for 802.1x
- ◆ Configure RADIUS enabled and basic RADIUS information

WLAN client configuration

To have 802.1x-RADIUS application works, the WLAN client must support 802.1x first as below, (“The key is provided for me automatically” must be selected):

