

Web Portal Security Access

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).

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.

For example, John, Mike, Tom, William are working together in an office which is under WLAN coverage, and Jim is the network administrator. Jim set same password for all computers. One day, a new employee, George comes to this office. Jim set the shared password in George's computer, only after that George could access the WLAN network. However, one day John quits his job, and his password needs to be expired for security reason. And because every person shares same password, so Jim needs to change the password in everyone's computers and AP.

This is just for a small office. If there are more people here, Jim needs to do more works in every computer. Oh, pity Jim!

Convenience Security Authentication

No one is willing to face heavy password setup and change works, and people always like things to be easy. Therefore, many wireless networks do not employ any security mechanism. But as mentioned before, those networks may encounter severe network security problem.

How to balance the security with convenience becomes a major issue for the wireless network.

Top Global’s MobilrBridge™ offers an ideal solution for simple security access – **Web Portal**.

Web portal is an authentication 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 MobilrBridge™. 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 global one.

In the local method, the network administrator maintains a table in MobilrBridge™. A user can use username and password in this table to access network. As the following figure 1, after laptop associate with and get IP from MobilrBridge™, it would prompt a window require for the user name and password before the user

connect to Internet. The user can access to Internet only after inserting proper username and password in the table of MobilrBridge™.

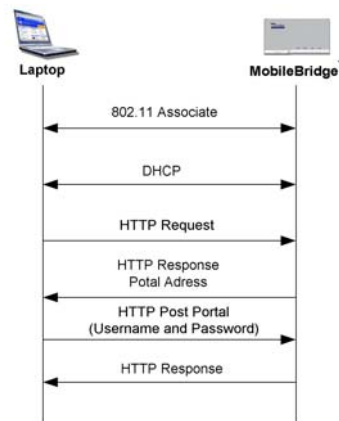


Figure 1. Local Web Portal

In the global method, the network administrator needs to configure a IP address of RADIUS server of MobilrBridge™. After the user insert username and password in prompted window, MobilrBridge™ will send those username and password to the RADIUS server. The server would check whether those username and password are valid and will send the result back. If the authentication success, the user can connect to the Internet. Otherwise, the user is not a valid user and will be disconnected by MobilrBridge™.

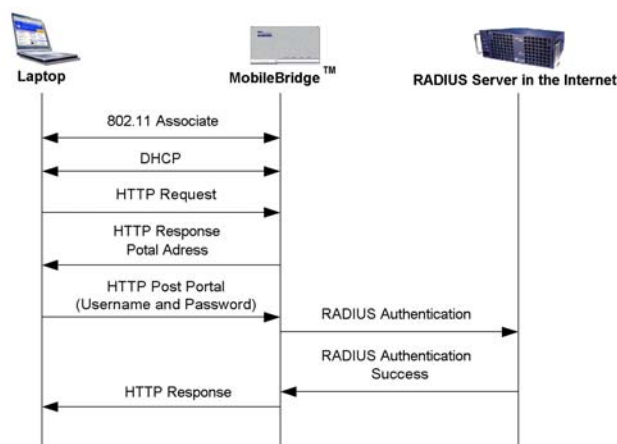


Figure 2. Global Web Portal

More Advantages of Web Portal

As mentioned in previous section, web portal is a most convenient method for wireless user authentication. Beside that, web portal also provide a way to start the accounting. 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 disconnected from Internet by MobilrBridge™, but they can also connect to other customer stations under the WLAN coverage.

To Use Web Portal In MB8000

As a member of MobilrBridge™ family, MB8000 can be configured to enable web portal function as well.

To make this function available, the user needs to login to the MobilrBridge™ as an administrator, and push the customize button in the default page. Then select **Web Portal** in the left menu and the user will see the following picture:

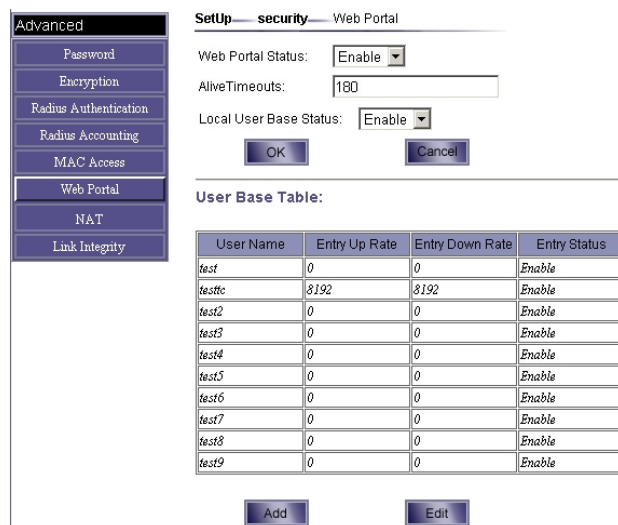


Figure 3. Web Portal Configuration Page

At first, the user needs to set the “Web Portal Status” to “Enable”, and specify the “Alive Timeouts” to idle seconds permitted by MobilrBridge™. The user can select between the local web portal and global web portal by enable or disable the “Local User Base Status”. If user chooses local web portal method, the following User Base Table is used for username and password storage. The user can add, edit, and delete entries in this table. If the user chooses global web portal, MobilrBridge™ will not store username and password in itself.

After enabling web portal, the following window will popup while a new user want to connect to the Internet, the



Figure 4. Web Portal Configuration Page

user can only connect Internet after insert valid username and password in this window.

Application Example

At last, let us back to the previous example.

If that office uses MobilrBridge™ and enables Web Portal, all complex setup and change works become much easier. Jim only needs to set up different usernames and passwords for every one in the MobilrBridge™.

When George joins to the office, Jim only needs to add a new entry in the User Base Table and tells George his username and password. After inserting username and password in the pop-up window, George can connect to Internet.

After John's quit, Jim only needs to delete John's entry in the User Base Table and no need to change every computer's configuration in the office.

Obviously, all works for the administrator and all employees are much easier than before. That is what Web Portal brings to you.



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.chinatopglobal.com/>