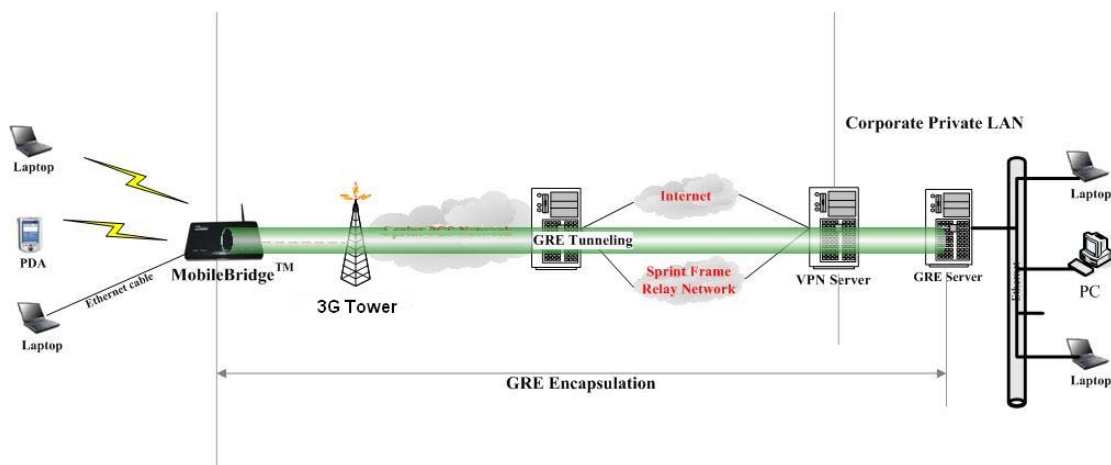


## What and why GRE

There are two cases in a network when using MB8000 for the traveling group.

1. When the users behind the MB8000 want to access the network with some network protocol other than IP protocol, such as IPX, NetBIOS, OSPF, BGP, that traffic will not be routed.
2. The users in the corporate network cannot access the users behind MB8000 reversely.

MB8000 also provide a solution to address the situations above. That is GRE tunneling.

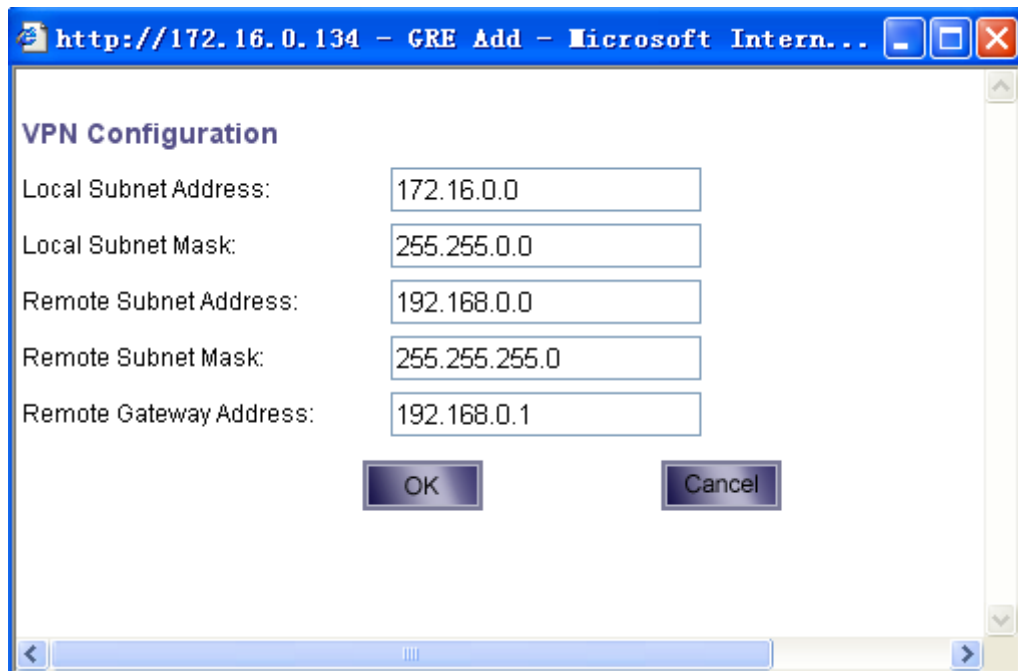


**Figure 1. GRE Tunneling**

Figure 1 depicts the network topologic for a GRE tunnel. With GRE tunneling, all of the data traffic between the MB8000 LAN and the corporate private network will be encapsulated and sent looked like transparently. Thus all network protocol traffic can be tunneled to the corporate private network, and the users in two different LAN network can reach each other. The data traffic to the corporate private network will be encapsulate with GRE, and sent through the 3G network.

## GRE Configuration

Here we assume that the subnet behind the MB8000 is 172.16.0.0/255.255.0.0, while the corporate network is 192.168.0.0/255.255.255.0, and the GRE server located in the corporate network has its IP address of 192.168.0.1. We now need to set up a GRE tunnel between MB8000 network and the corporate network by going to the "Advanced"->"GRE" page on MB8000 with a browser. Set the "Status" field to "Enable", and then click "Add" button to add a GRE tunneling rule. Figure 2 shows the settings for this tunnel.



**Figure 2. Set up a GRE tunnel.**

**Local Subnet Address:** The network behind MB8000.

**Local Subnet Mask:** The subnet mask of the network behind MB8000.

**Remote Subnet Address:** The corporate network.

**Remote Subnet Mask:** The subnet mask of the corporate network.

**Remote Gateway Address:** The IP address of the remote GRE server.

Save the settings and then reboot MB8000 via "Tools"->"Reboot" page.