SMCBR18VPN Router Installation Instructions

Part 1 | Basic Configuration of Your Broadband VPN Router

Before you attempt to log into the web-based Administration, please verify the following.
1. Your browser is configured properly (see below).
2. Disable any firewall or security software that may be running.
3. Confirm that you have a good link LED where your computer is plugged into the Router.
If you don't have a link light, then try another cable until you get a good link.

1.1 | Browser Configuration

Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.
You will also need to verify that the HTTP Proxy feature of your web browser is disabled. This is so that your web browser will be able to view the Router configuration pages. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer 5 or above (For Windows)

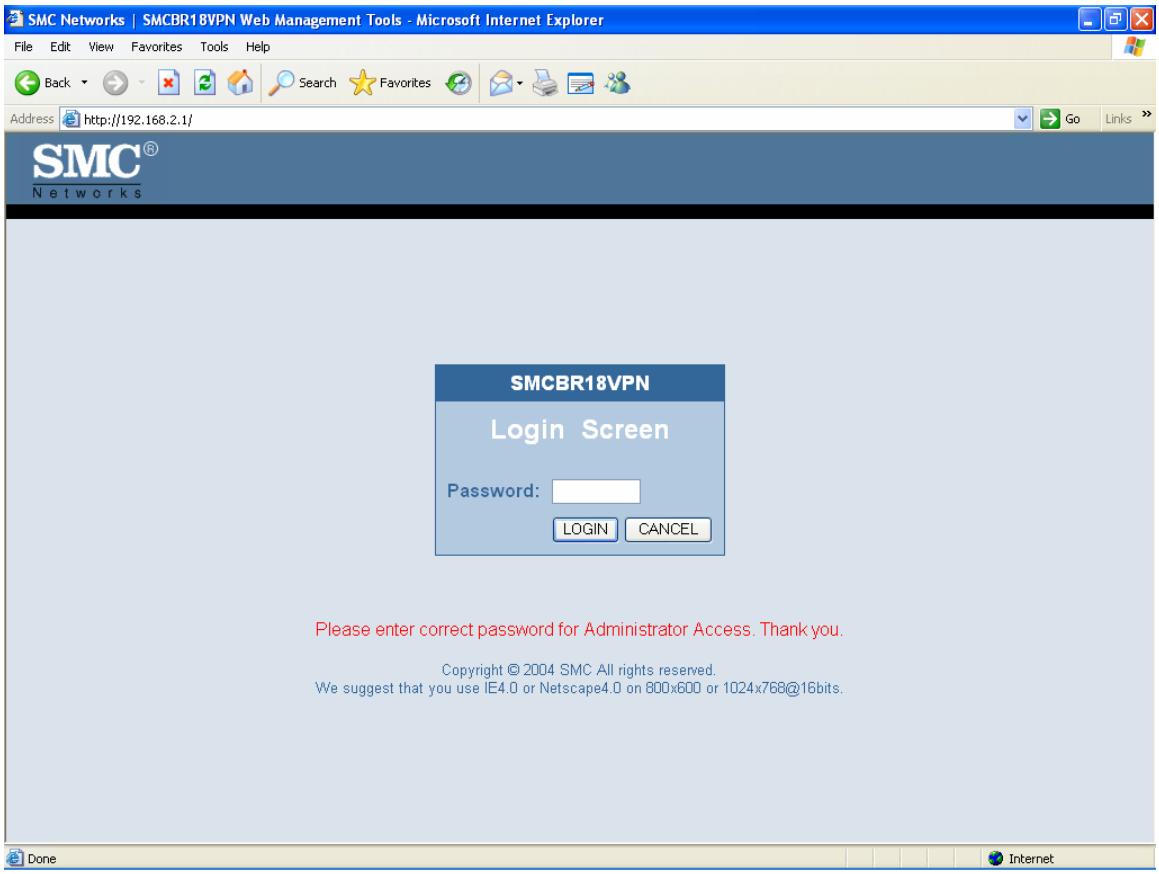
1. Open Internet Explorer. Click Tools, and then select Internet Options.
2. In the Internet Options window, click the Connections tab.
3. Click the LAN Settings button.
4. Clear the "Use a proxy server for your LAN" checkbox and click OK to save these LAN settings changes.
5. Click OK again to close the Internet Options window.

Netscape 7.2 or Mozilla

1. Open the Netscape browser.
2. Click the Edit drop down menu and select Preferences.
3. Double click to expand the "advanced" option on the preference category list.
4. Click Proxies.
5. Click the radio button "Direct Connection to the Internet".
6. Click OK to save.

1.2 | Web Management

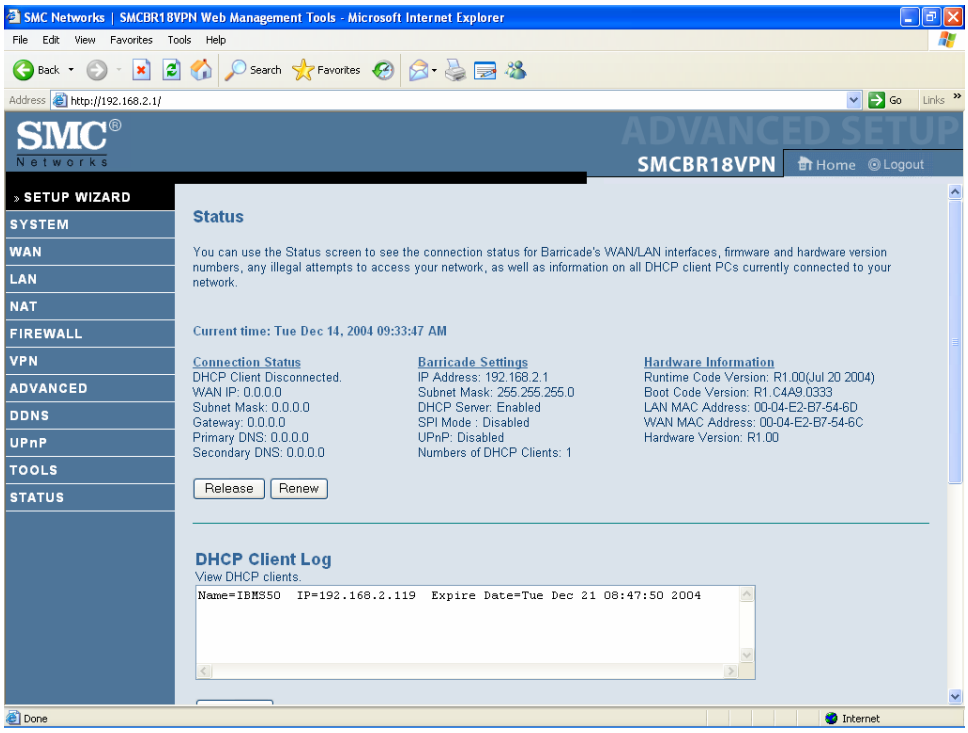
To access the Router's management interface, enter the Router IP address in your web browser http://192.168.2.1.



To log on as an administrator, enter the system password (default password is **smcadmin**) and click the **LOGIN** button. If you typed the password correctly, the
left panel of the Web user interface changes to the administrator configuration mode as shown in the following figures.

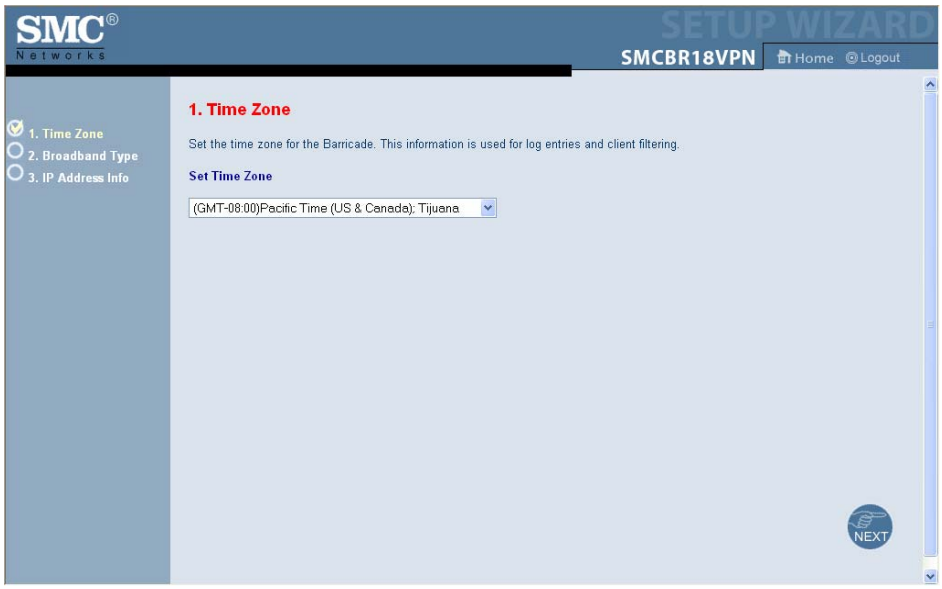
1.3 | Setup Wizard

Note: Select "Setup Wizard at the top left of the navigation panel in order to start you through the basic configuration screens.

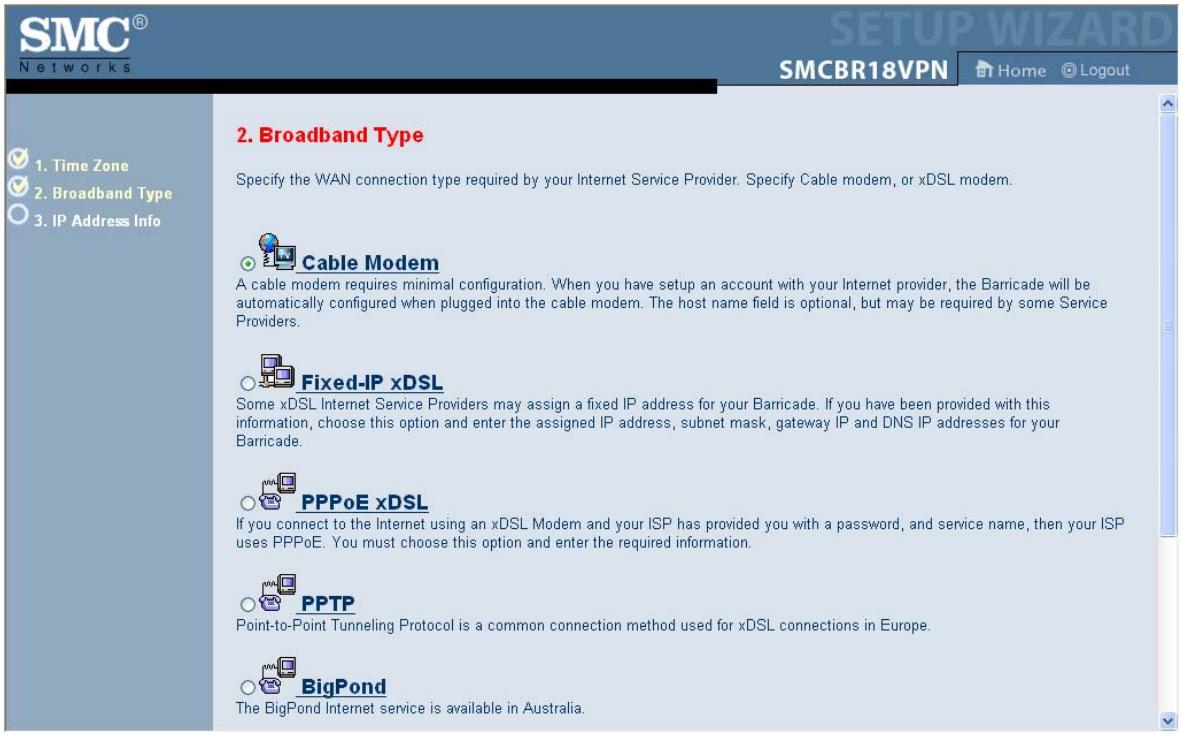


1.4 | Time Zone

The first item is Time Zone. For accurate timing of client filtering and log events, you need to set the time zone. Select your time zone from the drop-down list. Click "NEXT to navigate to the next screen.



Select your Broadband Type and follow the appropriate section below.

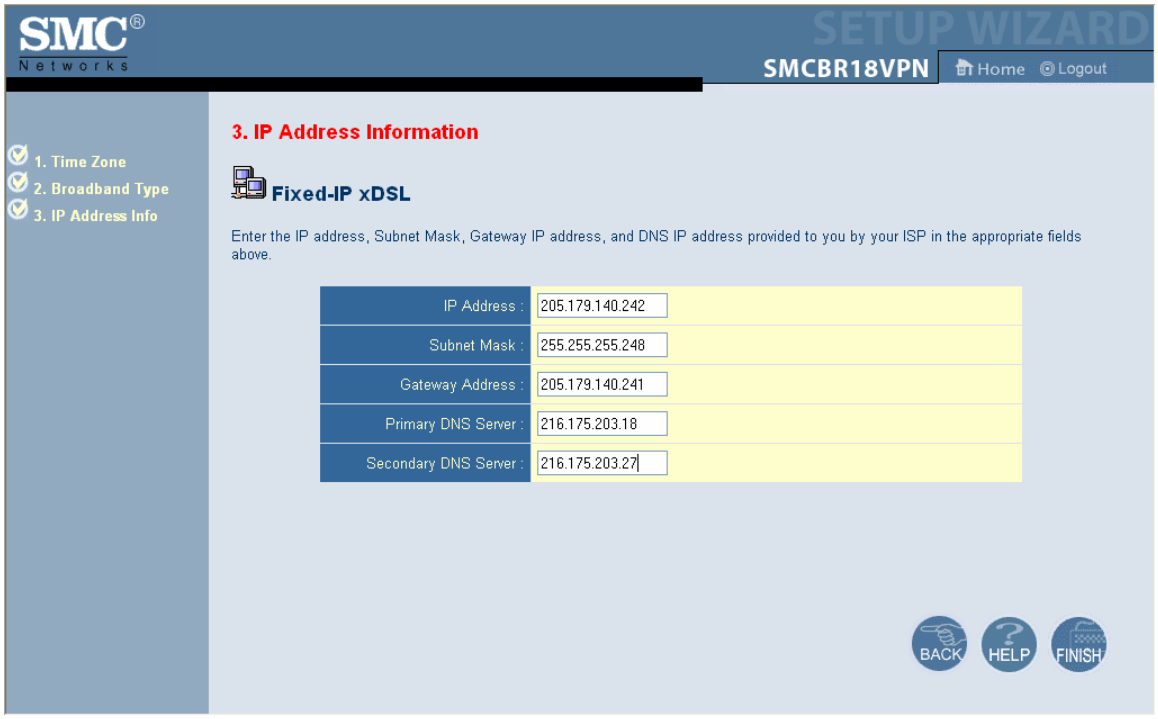


1.5 Cable Modem (Dynamic IP /xDSL)

The cable modem option allows you to configure a host name and MAC Address. The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Router. Use this address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of an Ethernet card as an identifier when first setting up your broadband account, only connect the PC with the registered MAC address to the Router and click the Clone MAC Address button. This will replace the current Router MAC address with the already registered Ethernet card MAC address. If you are unsure of which PC was originally set up by the broadband technician, call your ISP and request that they register a new MAC address for your account. Register the default MAC address of the Router. Click "FINISH" in order to save the configuration information.

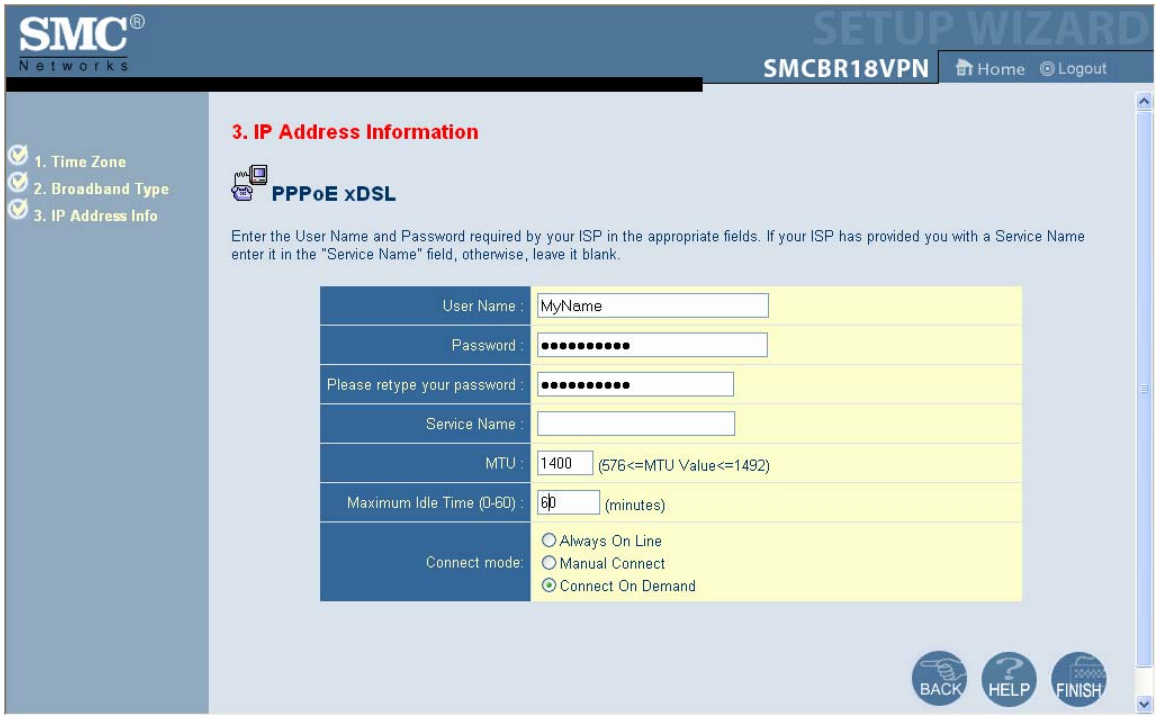
1.6 Fixed-IP xDSL

Some xDSL Internet Service Providers may assign a fixed (static) IP address. If you have been provided with this information, choose this option and enter the assigned IP address, gateway IP address, DNS IP addresses, and subnet mask. Click "FINISH" in order to save the configuration information.



1.7 PPPoE xDSL

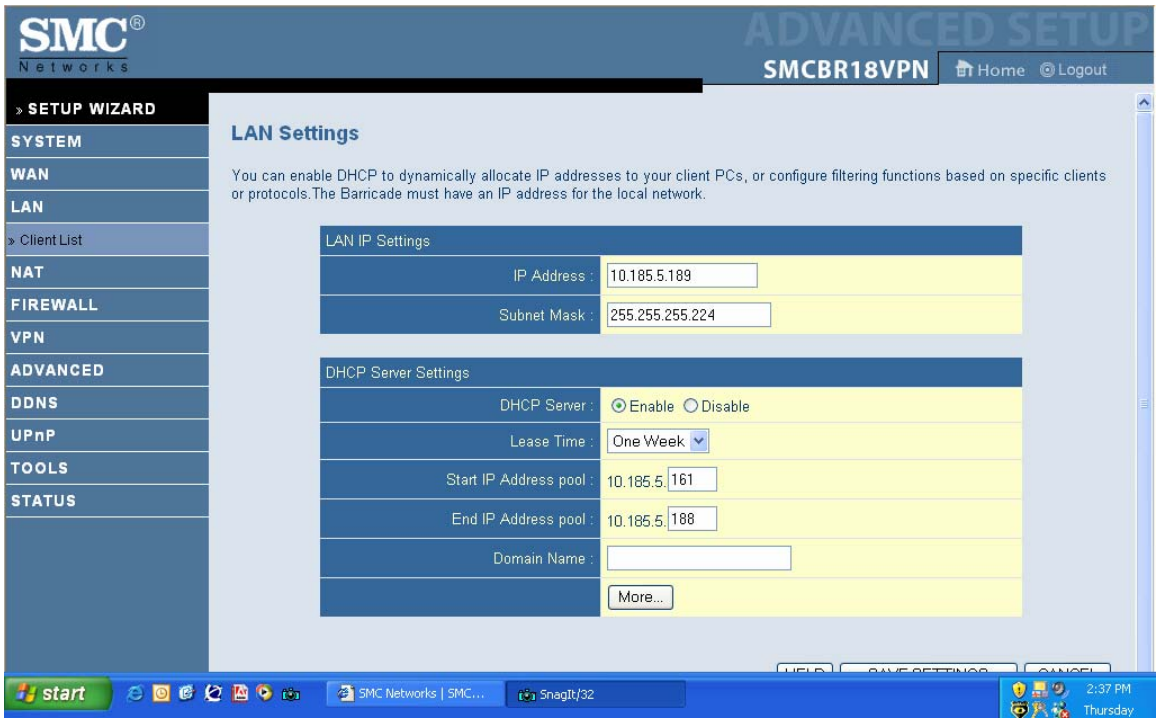
Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Leave the Maximum Transmission Unit (MTU) at the default value unless you have a particular reason to change it. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10) Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again. Click "FINISH" in order to save the configuration information.



1.8 | Advanced Setup – LAN

Click on "LAN" on the left side of the screen in order to validate the LAN settings.

This is the local IP address of the router. All networked computers must use the LAN IP address of the router as their default Gateway. **The addresses you need to use are the addresses supplied by Galileo International.** Typically in the Range of 10.185.X.X for the U.S.
Once the LAN IP address has been assigned the next address space will be part of the dynamic IP address pool. The IP address for the FPM/GPM workstation will be Static.
Do not include the address of the router in the client address pool.
Also remember to configure your client PCs for dynamic IP address allocation with the exception of the FPM/GPM workstation.
Click "SAVE SETTINGS" in order to save the configuration information.



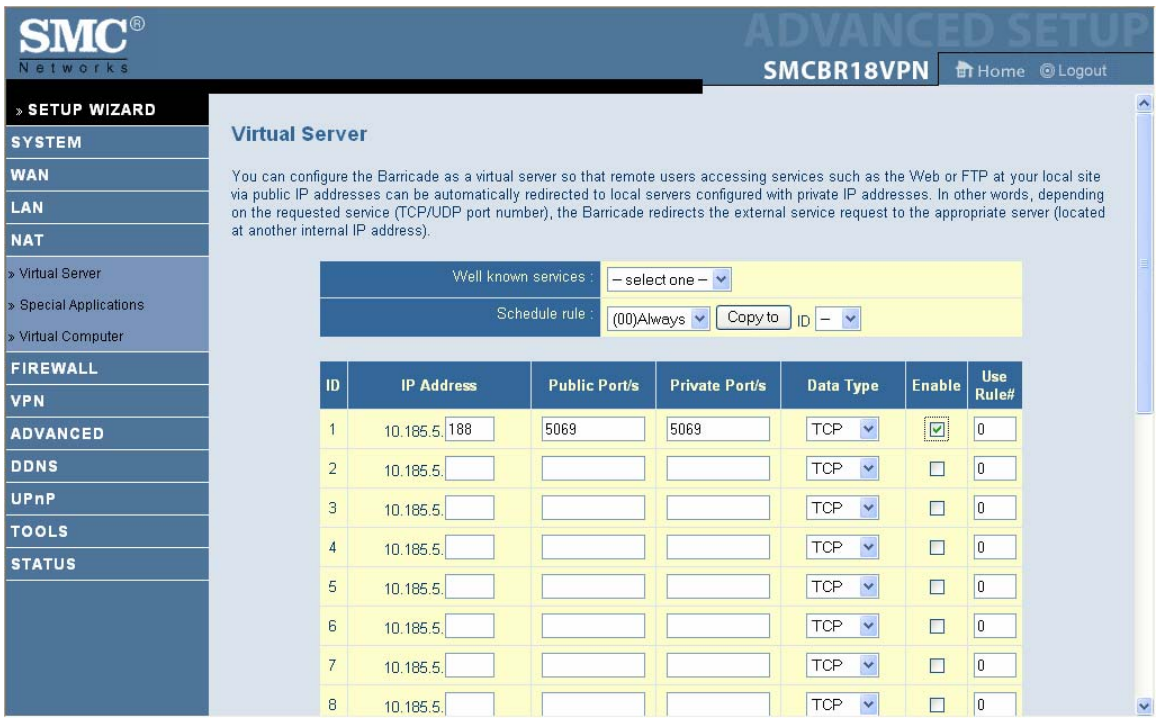
1.9 | Virtual Server

The firewall of the router filters out unrecognized packets to protect your intranet. This means that all network hosts are invisible to the outside world. However, some of the hosts can be made accessible by enabling the Virtual Server mapping. A virtual server is defined as a Service Port. All requests to this port will be redirected to the computer specified by the Server IP.

The virtual server must be initiated for the FPM/GPM workstation. You must add in the **Static IP address** that is reserved for the FPM/GPM workstation in order to allow for the incoming Wakeup message to be handled properly. This inbound message is TCP on Port 5069.The following is only an example. The real addressing will be assigned by Galileo International.

FPM/GPM Workstation IP Address = 10.185.5.188
FPM/GPM Workstation Subnet Mask = 255.255.255.224
FPM/GPM Workstation Default Gateway = 10.185.5.161

Click "SAVE SETTINGS" in order to save the configuration information.



Note: At this point of the configuration you should have internet connectivity. You can test your Internet access before proceeding to the next step.

Part 2 | VPN Tunnel Configuration of Your Broadband VPN Router (IPSec)

2.0 General Information

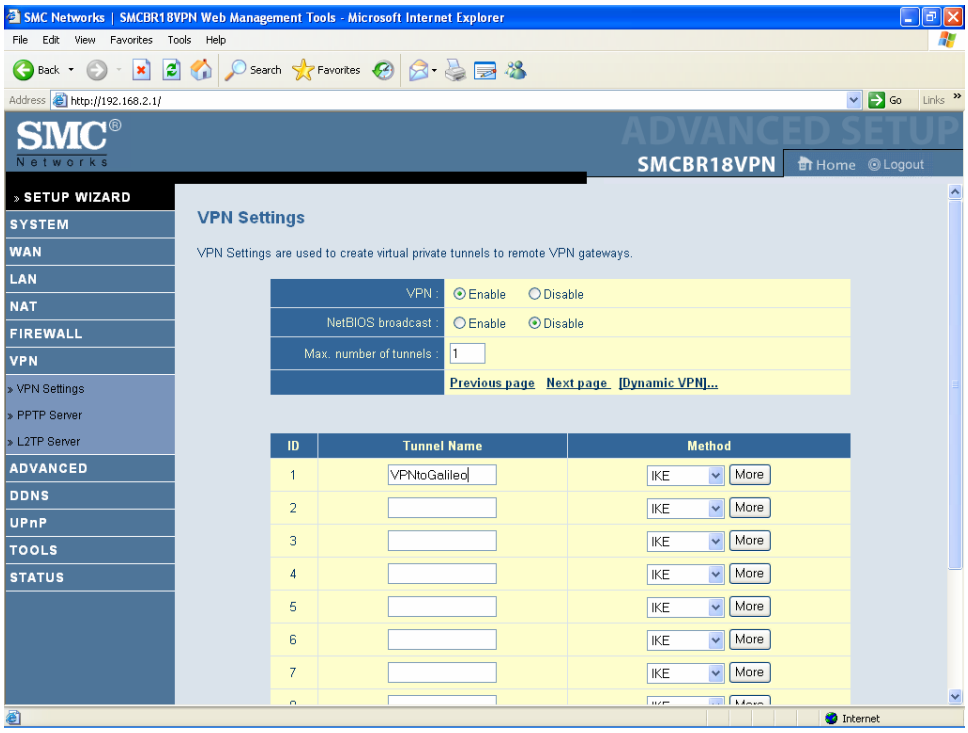
VPN settings are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information, by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

- VPN: VPN protects network information from intruders.

2.1 Basic Setup

Click on VPN Settings" on the left side of the screen in order to configure the VPN tunnel information.

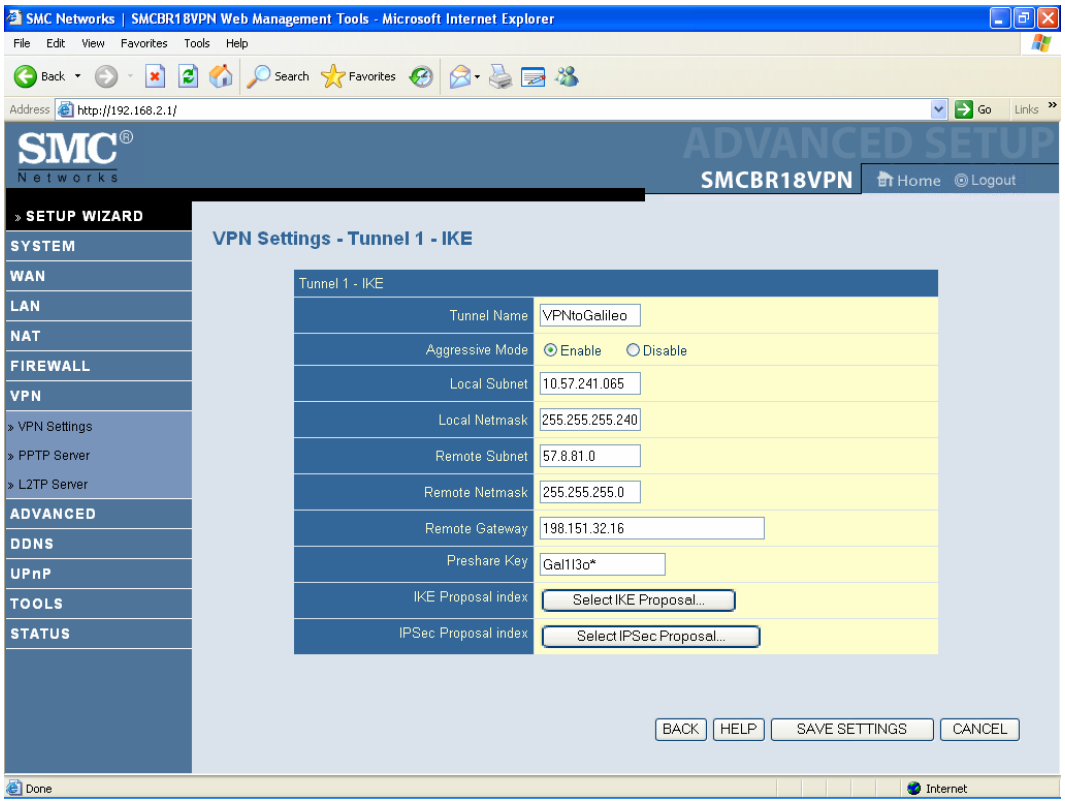
- Enable: Select "Enable" to allow the VPN Setting to be initialized.
- Max. Number of Tunnels: Set the number of tunnels that are allowed to be in operation simultaneously. This will generally be 1 unless there are other VPN endpoints that need access to this site.
- Tunnel name: Lists the monitored tunnel. (ex. VPNtoGalileo)
- Method: IPSec VPN supports two kinds of key-exchange methods: manual key exchange and the automatic key exchange. Galileo uses the IKE method that performs an automatic Internet key exchange. The system managers of both end gateways only need to set the same preshared key. The preshared key will be obtained from Galileo as needed for configuration.



There are three settings that must be configured to enable IKE for a dedicated tunnel:

- Basic Setup. The tunnel name is equal to the name you configured.
- IKE proposal: Click this button to setup a set of frequently used IKE proposals for the dedicated tunnel.
- IPSec proposal: Click this button to setup a set of frequently used IPSec proposals for the dedicated tunnel.

2.1 Basic Setup



- Local Subnet: The subnet of the local VPN gateway's LAN site. The subnet can be a host, a partial subnet, or the whole subnet of the local gateway's LAN site.

- Local netmask: The local netmask combined with the local subnet forms a subnet domain.

- Remote subnet: The subnet of a remote VPN gateway's LAN site. The subnet can be a host, a partial subnet, or the whole subnet of the remote gateway's LAN site.

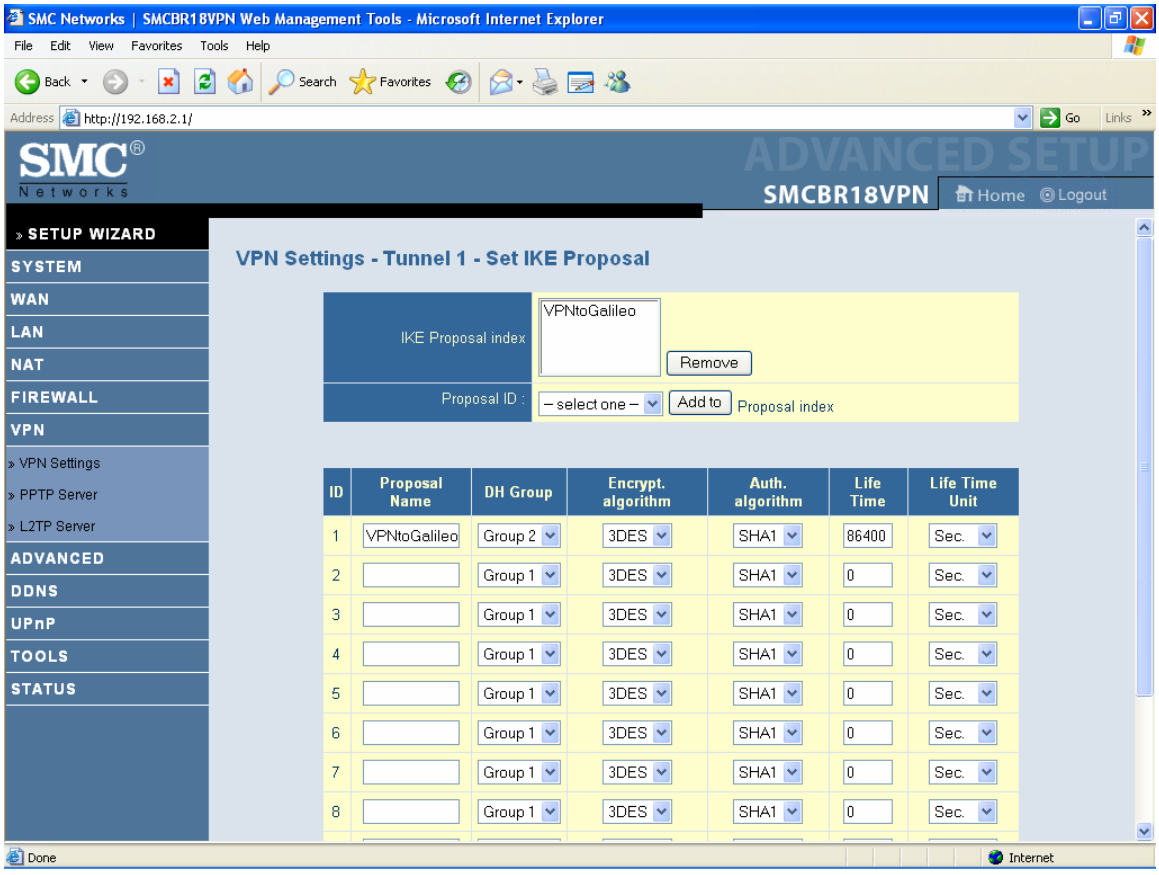
- Remote netmask: The remote netmask combined with the remote subnet forms a subnet domain.

- Remote gateway: The IP address of the remote gateway.

- Pre-shared key: The first key that supports the IKE mechanism of both VPN gateways to negotiate further security keys. The pre-shared key must be the same for both end gateways.

2.2 IKE Proposal Setup

Click "Select IKE Proposal" in order to configure the IKE proposal information.



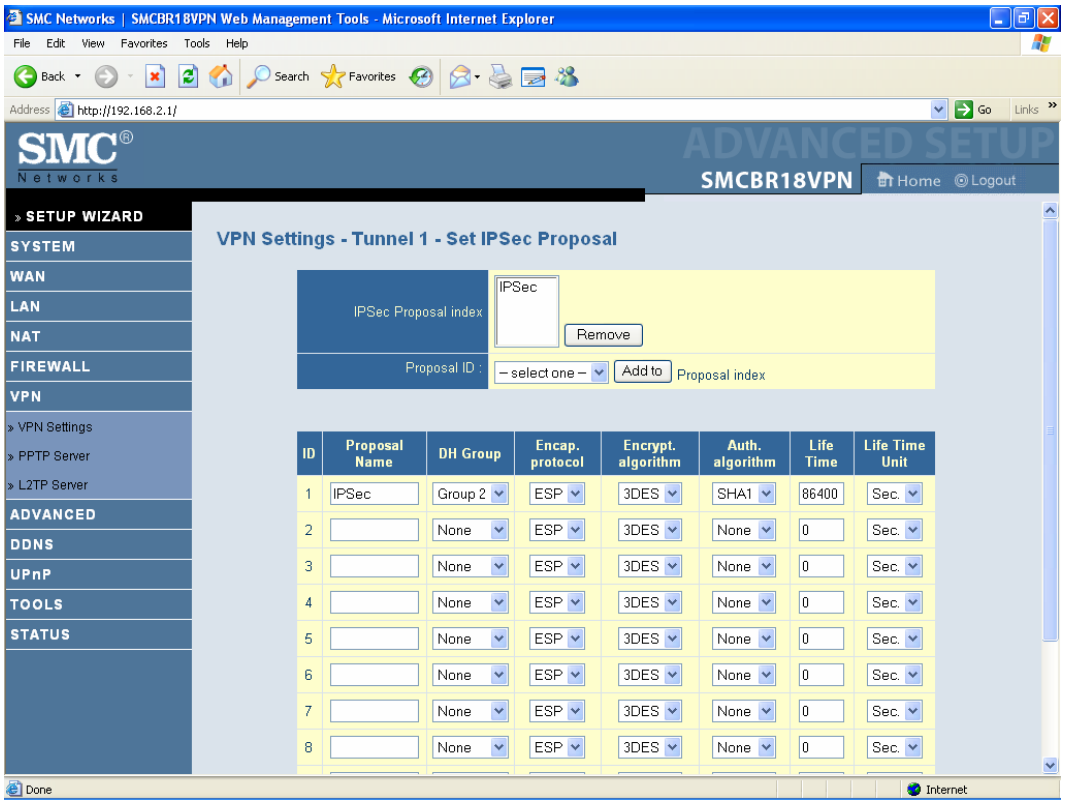
- IKE Proposal index: A list of selected proposal indexes from the IKE proposal pool. The selected activity is performed when you select a proposal ID and click the Add to button next to the Proposal ID roll-down list. A maximum of four indexes can be selected from the proposal pool for the dedicated tunnel.
- Proposal Name: The proposal name indicates which IKE proposal will be monitored.

- DH Group - Select "Group 2" (MODP1024)
- Encryption algorithm – Select "3DES"
- Authentication algorithm – Select " SHA1"
- Life Time: The unit of Life time is based on the value of the life time unit, which can be seconds or KB. The value of the unit is seconds, the value of life time represents the life time of the dedicated VPN tunnel between both end gateways. Its value can range from 300 to 172,800 seconds. Use the value 86400 for Galileo.

- Life Time Unit: The life time unit can be set to seconds or KB.
- Proposal ID: The identifier of the IKE proposal can be selected for adding a corresponding proposal to the dedicated tunnel.
- "Add to" button: Click this button to add the selected proposal, shown in the proposal ID field of the IKE Proposal index list.

2.3 IPSec Proposal Setup

You must return to the VPN Settings screen by selecting "VPN Settings" at the left of the screen . Then Select "More" in order to create the IPSec proposal information.



- Proposal Name: The proposal name indicates which IPSec proposal will be monitored. The first character of the name with the value of 0x00 stands for the IPSec proposal that is not available.
- DH Group – Select "Group 2" (MODP1024)
- Encapsulation protocol – Select "ESP"
- Encryption algorithm – Select "3DES"
- Authentication algorithm – Select "SHA1"
- Life Time: The unit of Life time is based on the value of the life time unit, which can be seconds or KB. The value of the unit is seconds, the value of life time represents the life time of the dedicated VPN tunnel between both end gateways. Its value can range from 300 to 172,800 seconds. Use the value of 86400 for Galileo.
- Life Time Unit: The life time unit should be set to seconds.
- Proposal ID: The identifier of the IPSec proposal can be selected for adding a corresponding proposal to the dedicated tunnel. A total of ten proposals can be set in the proposal pool. A maximum of four proposals from the pool can be applied to the dedicated tunnel.
- "Add to" button: Click this button to add the selected proposal, shown in the proposal ID field of the IPSec Proposal index list. The proposal shown in the index list will be used in phase 2 of the IPSec negotiation for getting the IPSec SA of the dedicated tunnel.

Select "SAVE SETTINGS" at the bottom of the screen in order to save this configuration information.