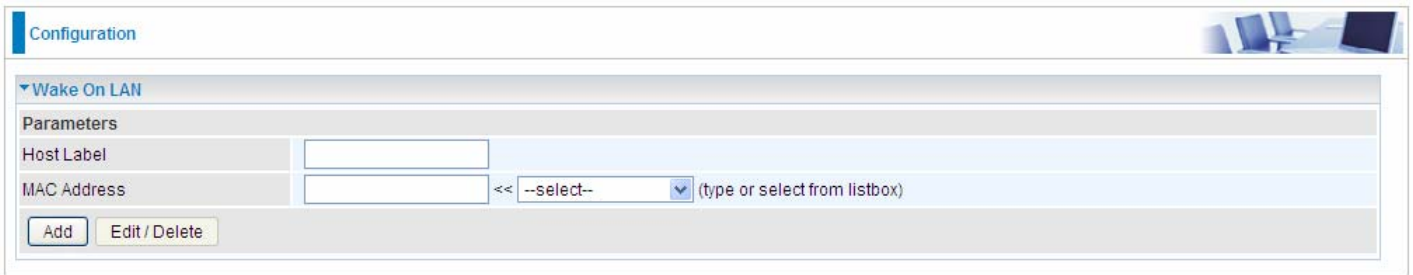


# Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



The screenshot shows a web-based configuration page for Wake On LAN. At the top, there is a 'Configuration' header. Below it, a section titled 'Wake On LAN' contains a 'Parameters' area. This area has two input fields: 'Host Label' and 'MAC Address'. The 'MAC Address' field is followed by a dropdown menu currently showing '--select--' and the text '(type or select from listbox)'. Below the input fields are two buttons: 'Add' and 'Edit / Delete'.

**Host Label:** Enter identification for the host.

**Select:** Select MAC address of the computer that you want to wake up or turn on remotely.

**Add:** After selecting, click Add then you can perform the Wake-up action.

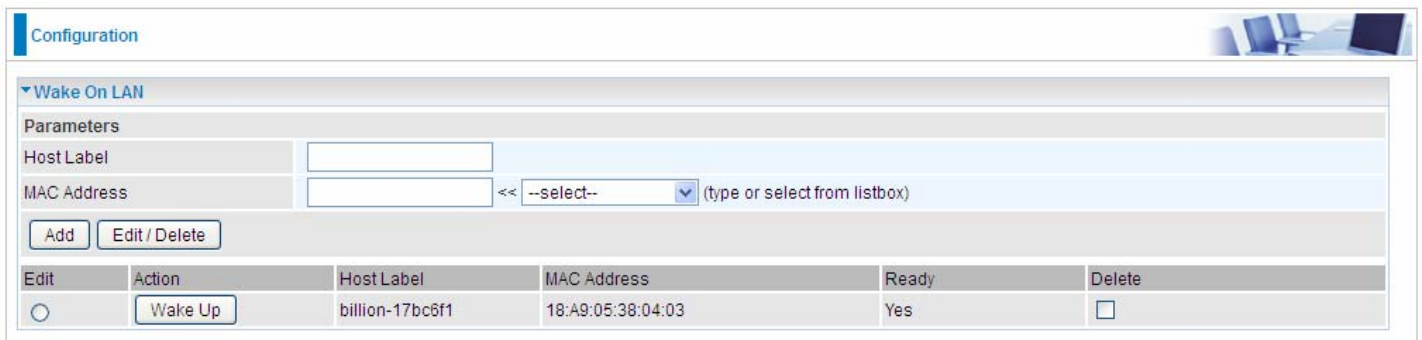
**Edit/Delete:** Click to edit or delete the selected MAC address.

**Ready:**

“Yes” indicating the remote computer is ready for your waking up.

“No” indicating the machine is not ready for your waking up.

**Delete:** Delete the selected MAC address.

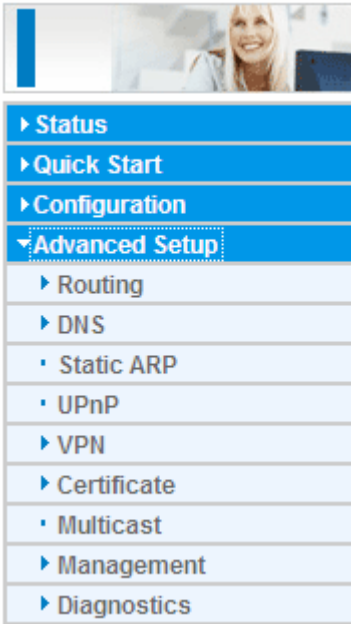


The screenshot shows the same configuration page as above, but with a table below the input fields. The table has six columns: 'Edit', 'Action', 'Host Label', 'MAC Address', 'Ready', and 'Delete'. There is one row of data in the table.

Edit	Action	Host Label	MAC Address	Ready	Delete
<input type="radio"/>	Wake Up	billion-17bc6f1	18:A9:05:38:04:03	Yes	<input type="checkbox"/>

# Advanced Setup

There are sub-items within the System section: [Routing](#), [DNS](#), [Static ARP](#), [UPnP](#), [VPN](#), [Certificate](#), [Multicast](#), [Management](#), and [Diagnostics](#).



(7800VDOX)

# Routing

## Default Gateway

Advanced Setup

▼ Default Gateway

Default Gateway Interface List

Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.



Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	-> <-	

Preferred WAN Interface As The System Default IPv6 Gateway

Selected WAN Interface: pppoe\_0\_0\_35/ppp0.1

Apply Cancel

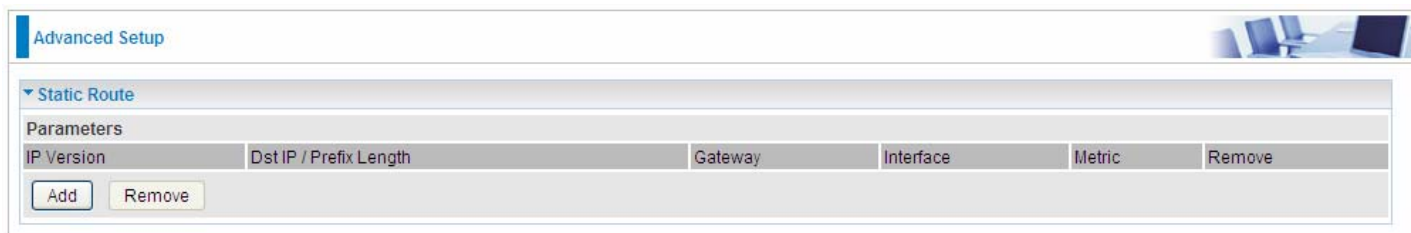
**WAN port:** Select the port this gateway applies to.

To set **Default Gateway** and **Available Routed WAN Interface**. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via  or . And select a Default IPv6 Gateway from the drop-down menu.

**Note:** Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

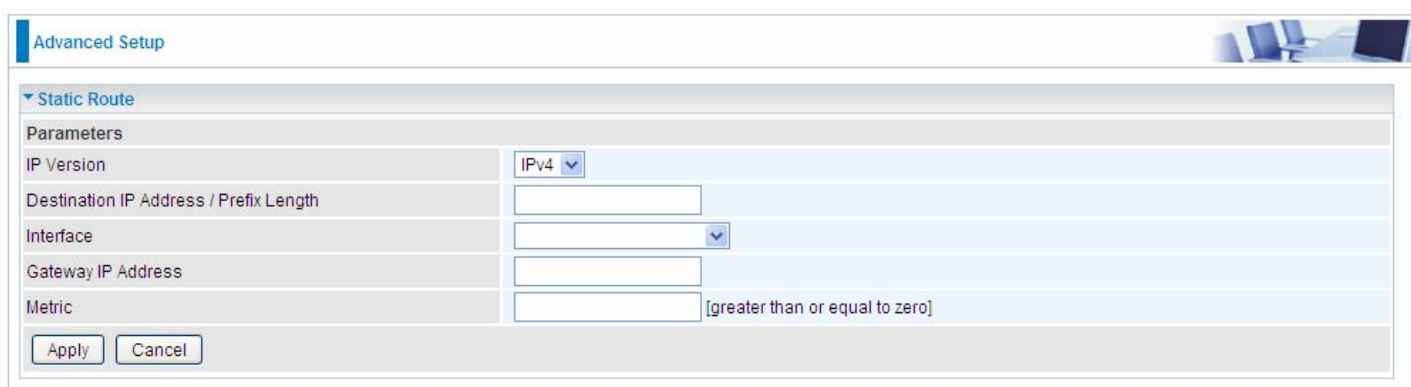
## Static Route

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.



The screenshot shows the 'Advanced Setup' interface with a 'Static Route' section. Below the section title is a table with the following columns: 'IP Version', 'Dst IP / Prefix Length', 'Gateway', 'Interface', 'Metric', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

Above is the static route listing table, click **Add** to create static routing.



The screenshot shows the 'Advanced Setup' interface with a 'Static Route' configuration form. The form has the following fields: 'IP Version' (dropdown menu set to 'IPv4'), 'Destination IP Address / Prefix Length' (text input), 'Interface' (dropdown menu), 'Gateway IP Address' (text input), and 'Metric' (text input with a note '[greater than or equal to zero]'). At the bottom are two buttons: 'Apply' and 'Cancel'.

**IP Version:** Select the IP version, IPv4 or IPv6.

**Destination IP Address / Prefix Length:** Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address, 192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.


**Interface:** Select an interface this route associated.

**Gateway IP Address:** Enter the gateway IP address.

**Metric:** Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.

Advanced Setup 

▼ Static Route

Parameters

IP Version	Dst IP/Prefix Length	Gateway	Interface	Metric	Remove
4	192.168.1.0/24		ppp0	1	<input checked="" type="checkbox"/>

## Policy Routing

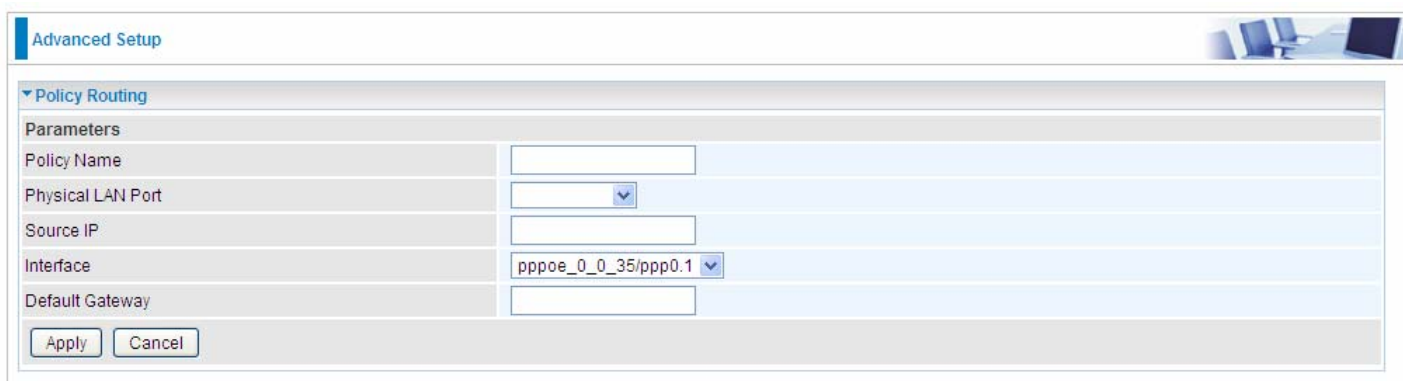
Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

The following is the policy Routing listing table.



The screenshot shows the 'Advanced Setup' interface with the 'Policy Routing' section expanded. Below the section header is a 'Parameters' table with the following columns: Policy Name, Source IP, LAN Port, WAN, Default Gateway, and Remove. At the bottom of the table are two buttons: 'Add' and 'Remove'.

Click **Add** to create a policy route.



The screenshot shows the 'Advanced Setup' interface with the 'Policy Routing' section expanded. The configuration form contains the following fields: Policy Name (text input), Physical LAN Port (dropdown menu), Source IP (text input), Interface (dropdown menu with 'pppoe\_0\_0\_35/ppp0.1' selected), and Default Gateway (text input). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

**Policy Name:** User-defined name.

**Physical LAN Port:** Select the LAN port.

**Source IP:** Enter the Host Source IP.

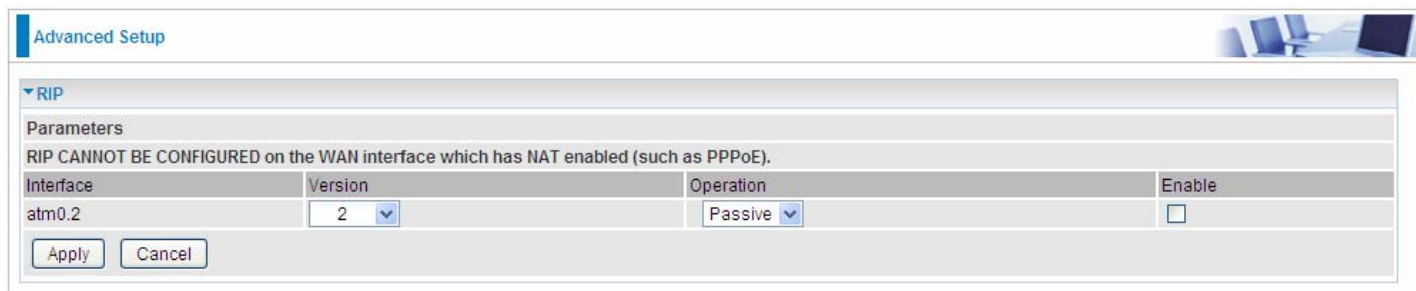
**Interface:** Select the WAN interface which you want the Source IP to access outside through.

**Default Gateway:** Enter the default gateway which you want the Source IP to access outside through.

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press **Remove** to delete it.

## RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "RIP" section, there is a "Parameters" area. A warning message states: "RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE)". Below this, a table allows configuration for the "atm0.2" interface. The table has four columns: "Interface", "Version", "Operation", and "Enable". The "Version" is set to "2" and the "Operation" is set to "Passive". The "Enable" checkbox is currently unchecked. "Apply" and "Cancel" buttons are located at the bottom left of the configuration area.

Interface	Version	Operation	Enable
atm0.2	2	Passive	<input type="checkbox"/>

**Interface:** the interface the rule applies to.

**Version:** select the RIP version, there are two versions, RIP-1 and RIP-2.

**Operation:** RIP has two operation mode.

- ① **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- ① **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

**Enable:** check the checkbox to enable RIP rule for the interface.

**Note:** RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

Click **Apply** to apply your settings.

# DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

## DNS

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

**Advanced Setup**

**DNS**

**Parameters**  
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system.  
In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.  
Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces

Selected DNS Server Interfaces	Available WAN Interfaces
ppp0.1	

Use the following Static DNS IP address

Primary DNS server:

Secondary DNS server:

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected:

Use the following Static IPv6 DNS address

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

### Obtain IPv6 DNS info from a WAN interface

**WAN Interface selected:** select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

### Use the following Static IPv6 DNS address

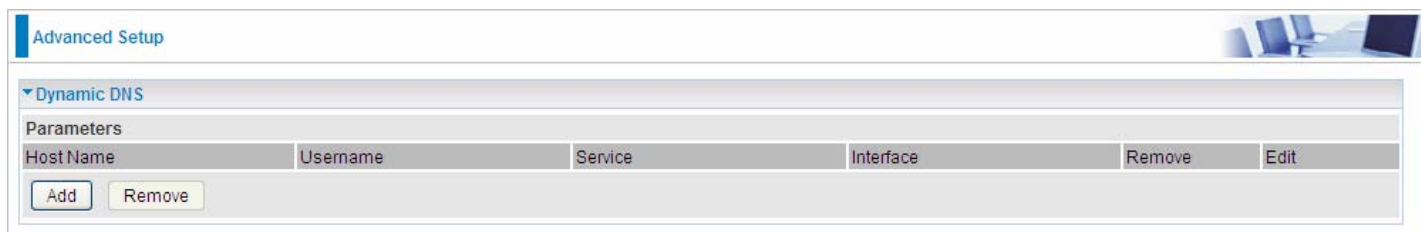
**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** type the specific primary and secondary IPv6 DNS Server address.



## Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es).



Host Name	Username	Service	Interface	Remove	Edit
-----------	----------	---------	-----------	--------	------

Click **Add** to register a WAN interface with the exact DNS.



Dynamic DNS Server:

Host Name:

Interface:

Username:

Password:

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

**Dynamic DNS Server:** Select the DDNS service you have established an account with.

**Interface:** Select the Interface that is bound to the registered Domain name.

**Host Name, Username and Password:** Enter your registered domain name and your username and password for this service.

## User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User **test** register two Dynamic Domain Names in DDNS provider <http://www.dyndns.org/>.

1. pppoe\_0\_0\_35 with DDNS: [www.hometest.com](http://www.hometest.com) using username/password test/test

Advanced Setup

Dynamic DNS -- Add

Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest.com
Interface	pppoe_0_0_35/ppp0.1
Username	test
Password	••••

Apply

Advanced Setup

Dynamic DNS

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	<input type="checkbox"/>	Edit

Add Remove

2. ipoe\_eth0 with DDNS: [www.hometest1.com](http://www.hometest1.com) using username/password test/test.

Advanced Setup

Dynamic DNS -- Add

Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest1.com
Interface	ipoe_eth0/eth0.1
Username	test
Password	••••

Apply

Advanced Setup

Dynamic DNS

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	<input type="checkbox"/>	Edit
www.hometest1.com	test	dyndns-custom	eth0.1	<input type="checkbox"/>	Edit

Add Remove

## DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



The screenshot shows a web interface for configuring DNS Proxy. The page title is "Advanced Setup". Under the "DNS Proxy" section, there are three main parameters:

Parameters	
DNS Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Host name of the Broadband Router	<input type="text" value="home.gateway"/>
Domain name of the LAN network	<input type="text" value="home.gateway"/>

At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

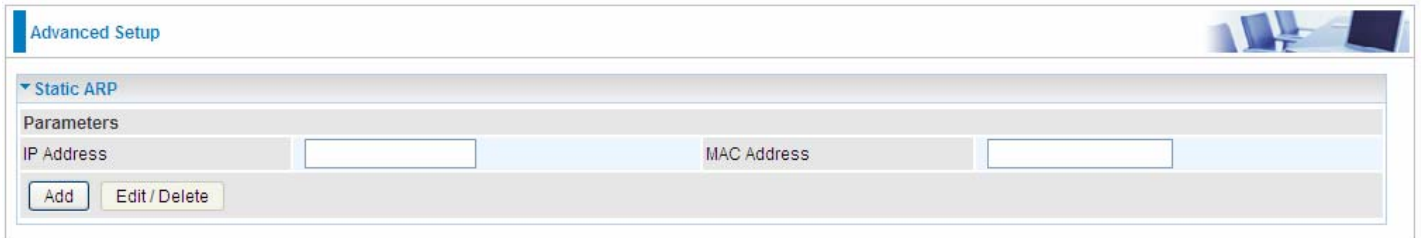
**DNS Proxy:** Select whether to enable or disable DNS Proxy function, default is enabled.

**Host name of the Broadband Router:** Enter the host name of the router. Default is home.gateway.

**Domain name of the LAN network:** Enter the domain name of the LAN network. home.gateway.

## Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.



The screenshot shows a web-based configuration interface for Static ARP. At the top, there is a tab labeled "Advanced Setup" and a small image of a computer workstation. Below this, a section titled "Static ARP" is expanded. Underneath, a "Parameters" section contains two input fields: "IP Address" and "MAC Address". Below the input fields are two buttons: "Add" and "Edit / Delete".

**IP Address:** Enter the IP of the device that the corresponding MAC address will be mapped to.

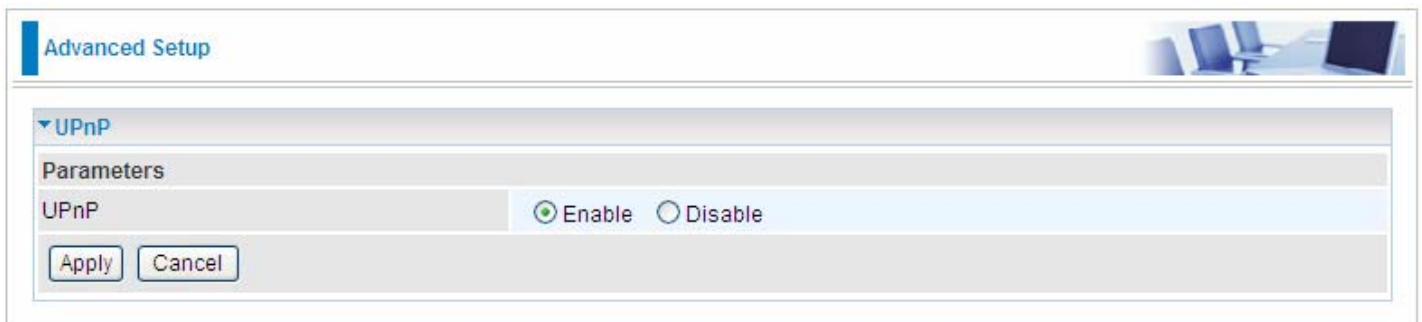
**MAC Address:** Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

## UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



### UPnP:

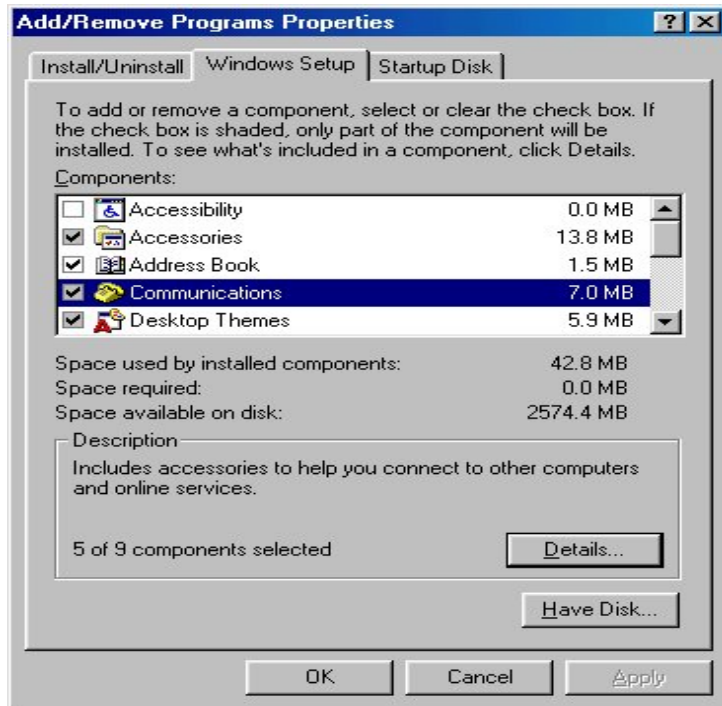
- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

## Installing UPnP in Windows Example

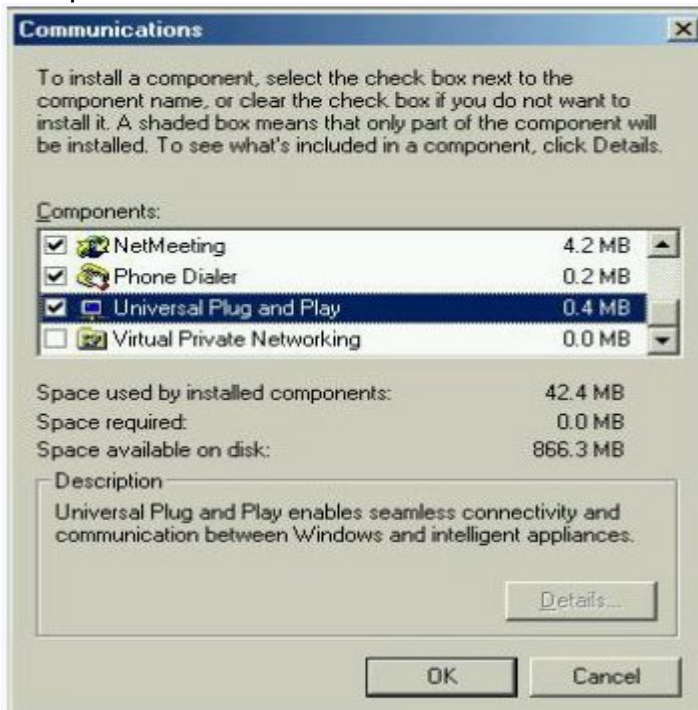
Follow the steps below to install the UPnP in Windows Me.

**Step 1:** Click Start and Control Panel. Double-click Add/Remove Programs.

**Step 2:** Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



**Step 3:** In the Communications window, select the Universal Plug and Play check box in the Components selection box.



**Step 4:** Click OK to go back to the Add/Remove Programs Properties window. Click Next.

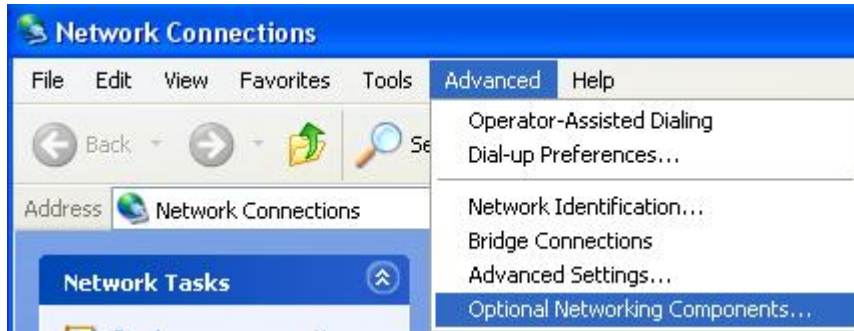
**Step 5:** Restart the computer when prompted.

**Follow the steps below to install the UPnP in Windows XP.**

**Step 1:** Click Start and Control Panel.

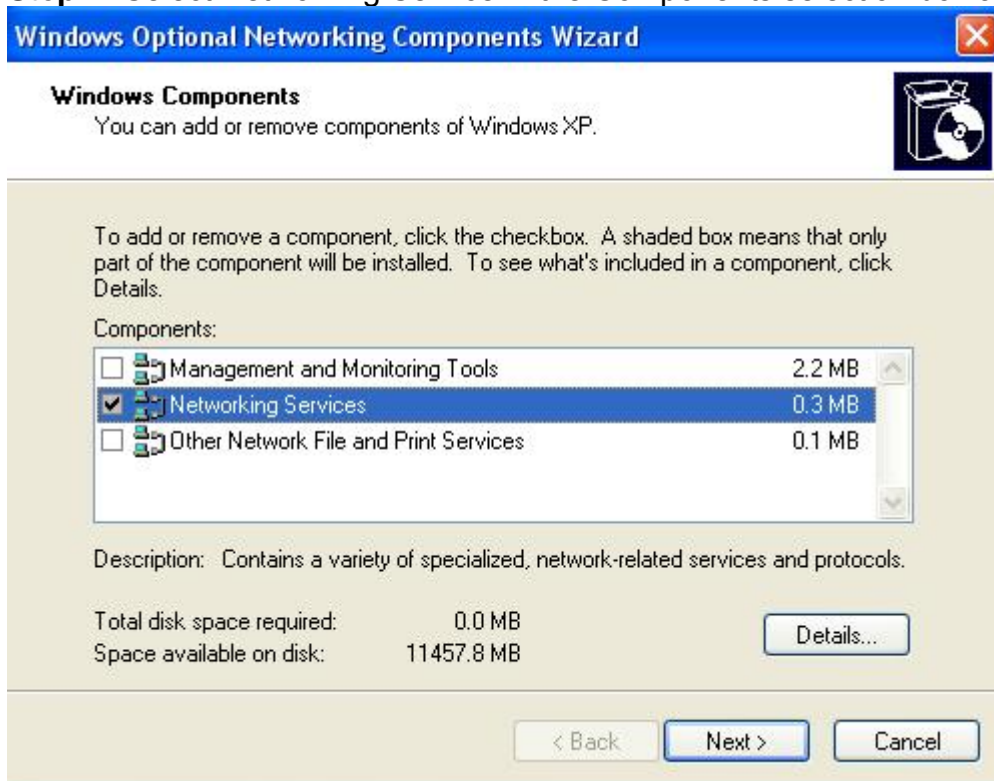
**Step 2:** Double-click Network Connections.

**Step 3:** In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ....



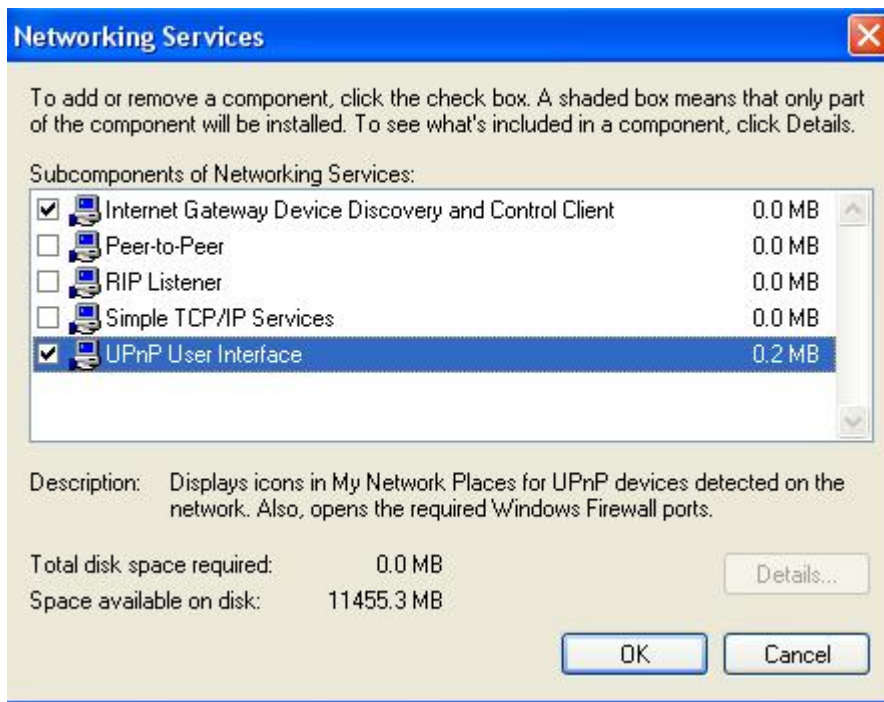
The Windows Optional Networking Components Wizard window displays.

**Step 4:** Select Networking Service in the Components selection box and click Details.



**Step 5:** In the Networking Services window, select the Universal Plug and Play check box.

**Step 6:** Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



### Auto-discover Your UPnP-enabled Network Device

**Step 1:** Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

**Step 2:** Right-click the icon and select Properties.

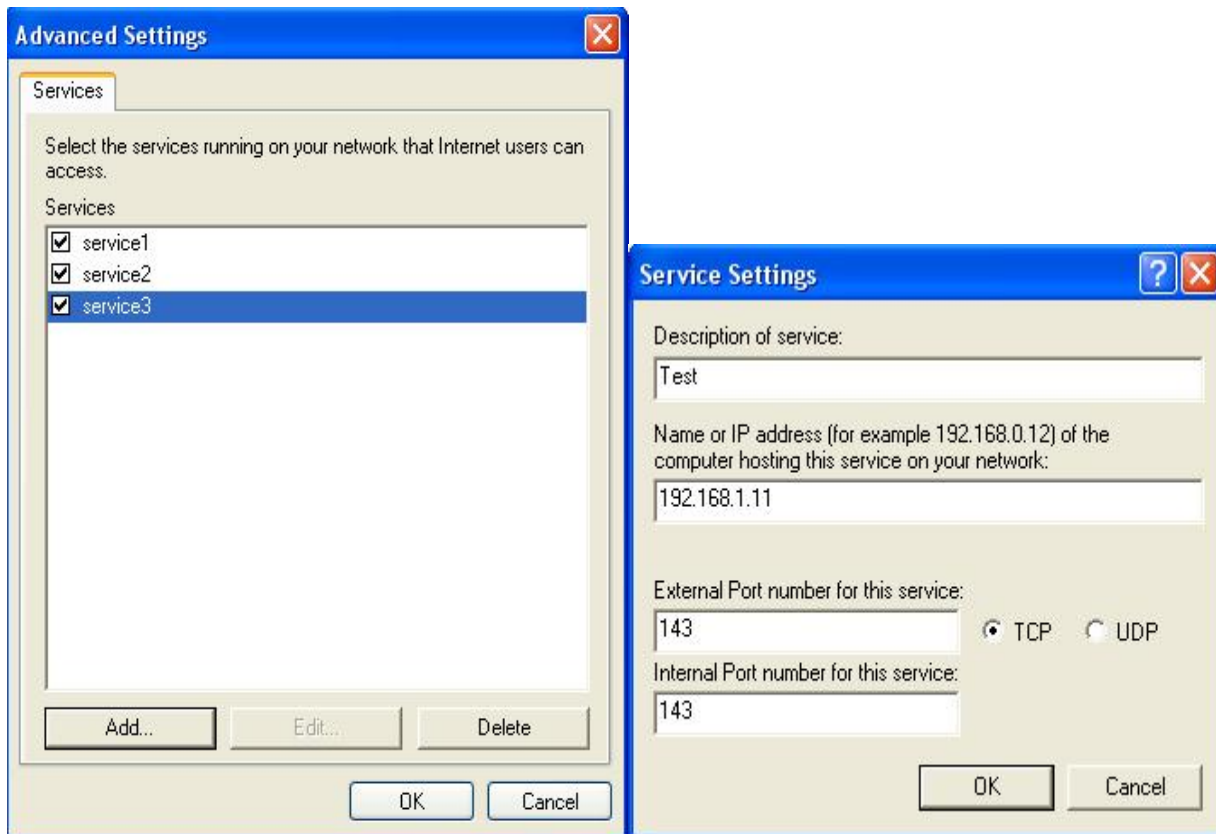




**Step 3:** In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

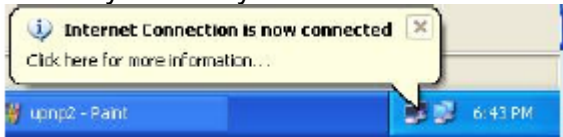


**Step 4:** You may edit or delete the port mappings or click Add to manually add port mappings.

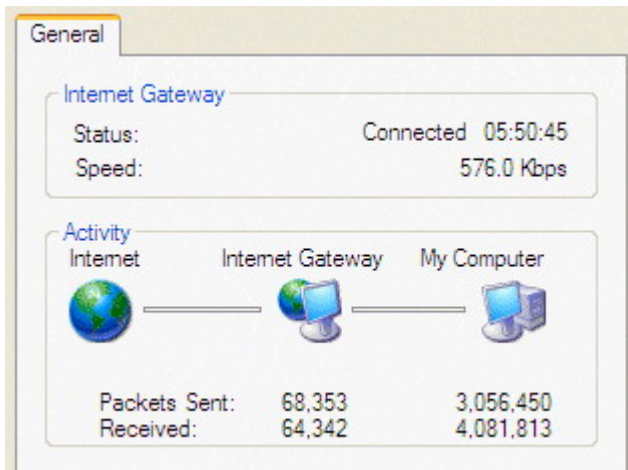


**Step 5:** Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



**Step 6:** Double-click on the icon to display your current Internet connection status.



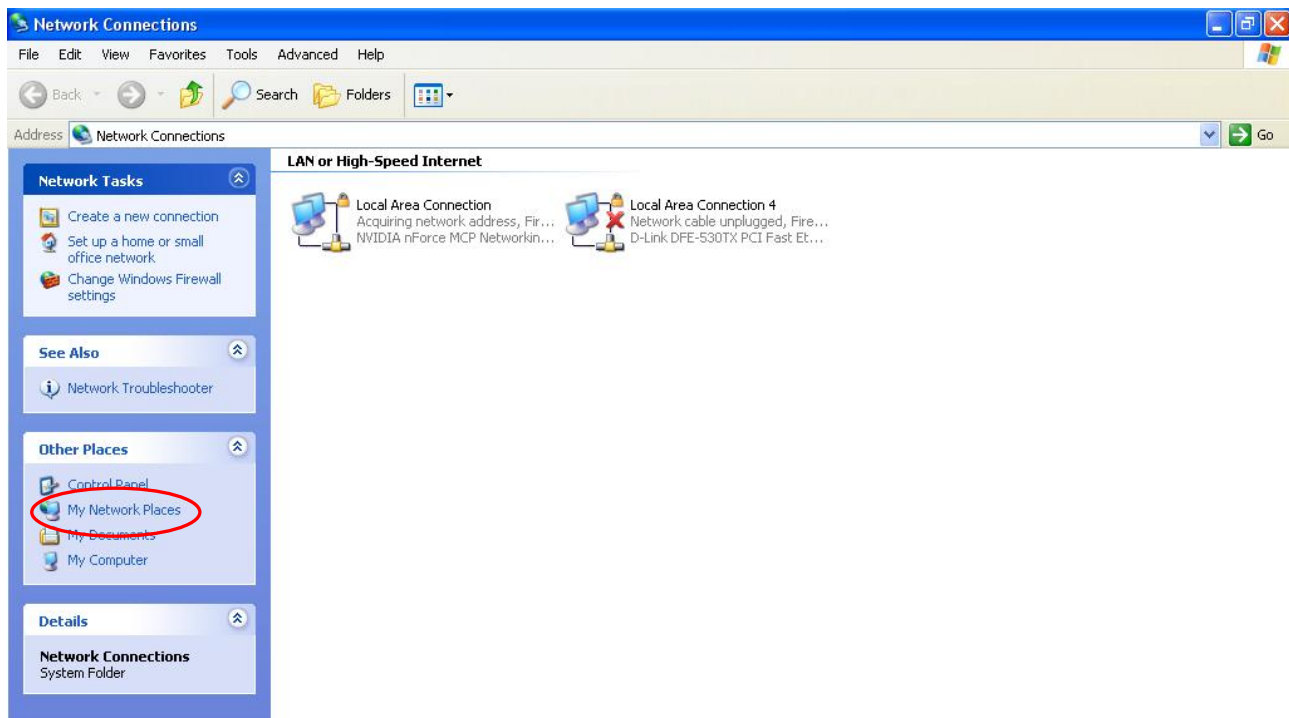
## Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7800VDP(O)X without first finding out the IP address of the router. This helps if you do not know the router's IP address. Follow the steps below to access web configuration.

**Step 1:** Click Start and then Control Panel.

**Step 2:** Double-click Network Connections.

**Step 3:** Select My Network Places under Other Places.



**Step 4:** An icon describing each UPnP-enabled device shows under Local Network.

**Step 5:** Right-click on the icon of your BiPAC 7800VDP(O)X and select Invoke. The web configuration login screen displays.

**Step 6:** Right-click on the icon of your BiPAC 7800VDP(O)X and select Properties. A properties window displays basic information about the BiPAC 7800VDP(O)X.

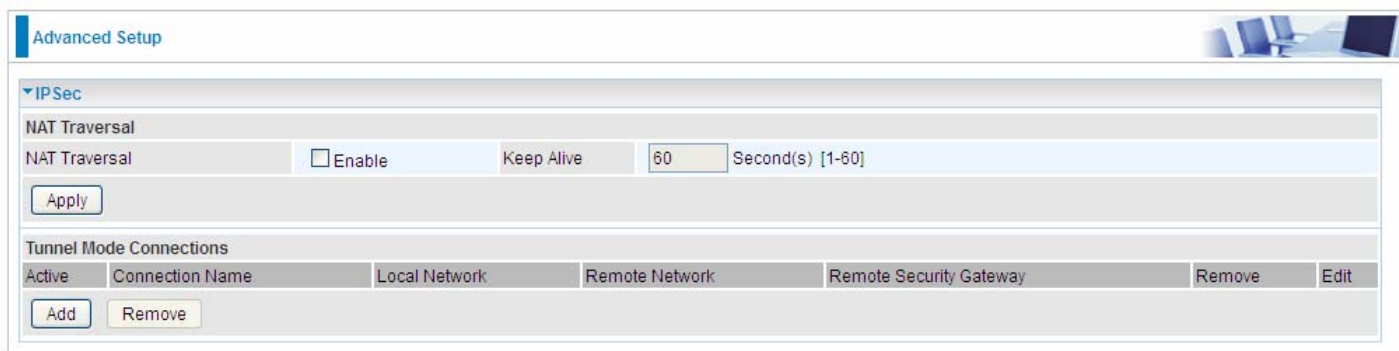
# VPN

A **virtual private network (VPN)** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

## IPSec

**Internet Protocol Security (IPsec)** is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).



The screenshot shows the 'Advanced Setup' window for IPSec configuration. It features a 'NAT Traversal' section with an 'Enable' checkbox, a 'Keep Alive' interval set to '60' seconds, and an 'Apply' button. Below this is a 'Tunnel Mode Connections' table with columns for 'Active', 'Connection Name', 'Local Network', 'Remote Network', 'Remote Security Gateway', 'Remove', and 'Edit'. There are 'Add' and 'Remove' buttons at the bottom of the table.

Active	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
--------	-----------------	---------------	----------------	-------------------------	--------	------

## NAT Traversal

**NAT Traversal:** This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

**Keep Alive:** Type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click **Apply** to save and apply your settings.

Click **Add** to create IPsec connections.

The screenshot shows the 'Advanced Setup' page for IPsec configuration. The 'IPsec' section is expanded, showing the following fields and options:

- IPsec Settings:**
  - Connection Name: [Text Input]
  - WAN Interface: Default [Dropdown]
  - IP Version: IPv4 [Dropdown]
  - Local Network: Subnet [Dropdown]
  - IP Address: [Text Input]
  - Netmask: [Text Input]
  - Remote Security Gateway: [Text Input]
  - Anonymous:
  - Remote Network: Single Address [Dropdown]
  - IP Address: [Text Input]
  - Netmask: [Text Input]
  - Key Exchange Method: IKE
  - IPsec Protocol: ESP
  - Pre-Shared Key: [Text Input]
  - Local ID Type: Default [Dropdown]
  - ID Content: [Text Input]
  - Remote ID Type: Default [Dropdown]
  - ID Content: [Text Input]
- Phase 1:**
  - Mode: Main [Dropdown]
  - Encryption Algorithm: 3DES [Dropdown]
  - Integrity Algorithm: MD5 [Dropdown]
  - DH Group: MODP1024(DH2) [Dropdown]
  - SA Lifetime: 480 Minute(s) [60-1440]
- Phase 2:**
  - Encryption Algorithm: 3DES [Dropdown]
  - Integrity Algorithm: MD5 [Dropdown]
  - DH Group: None [Dropdown]
  - IPsec Lifetime: 60 Minute(s) [60-1440]
- DPD Setting:**
  - DPD Function:  Enable  Disable
  - Detection Interval: 180 Second(s) [180-86400]
  - Idle Timeout: 5 Consecutive times [5-99]

An 'Apply' button is located at the bottom left of the configuration area.

## IPsec Settings

**Connection Name:** A given name for the connection (e.g. “connection to office”).

**WAN Interface:** Select the set used interface for the IPsec connection, when you select adsl pppoe\_0\_0\_35/ppp0.1 interface, the IPsec tunnel would transmit data via this interface to connect to the remote peer.

**IP Version:** Select the IP version base on your network framework.

**Local Network:** Set the IP address or subnet of the local network.

- ① **Single Address:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (*network-to-host*).
- ① **Subnet:** The subnet of the local network, for establishing an IPsec tunnel between a pair of security gateways (*network-to-network*)

**IP Address:** The local network address.

**Netmask:** The local network netmask.

**Remote Secure Gateway:** The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

**Anonymous:** Enable any IP to connect in.

**Remote Network:** Set the IP address or subnet of the remote network.

- ① **Single Address:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ① **Subnet:** The subnet of the local network, for establishing an IPsec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

**Key Exchange Method:** Displays key exchange method.

**Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

**Local ID Type and Remote ID Type:** When the mode of phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

**ID content:** Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

## Phase 1

**Mode:** Select IKE mode from the drop-down menu: **Main** or **Aggressive**. This IKE provides secured key generation and key management.

**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56\*3) bits as an encryption method.
- ① **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

**Integrity Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

**DH Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are 8 modes. MODP stands for Modular Exponentiation Groups.

**SA Lifetime:** Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 480 minutes (28800 seconds). A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

## Phase 2

**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

**Integrity Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

**DH Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are 8 modes. MODP stands for Modular Exponentiation Groups.

**IPSec Lifetime:** Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure

authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

## **DPD Setting**

**DPD Function:** Check **Enable** to enable the function.

**Detection Interval:** The period cycle for dead peer detection. The interval can be 180~86400 seconds.

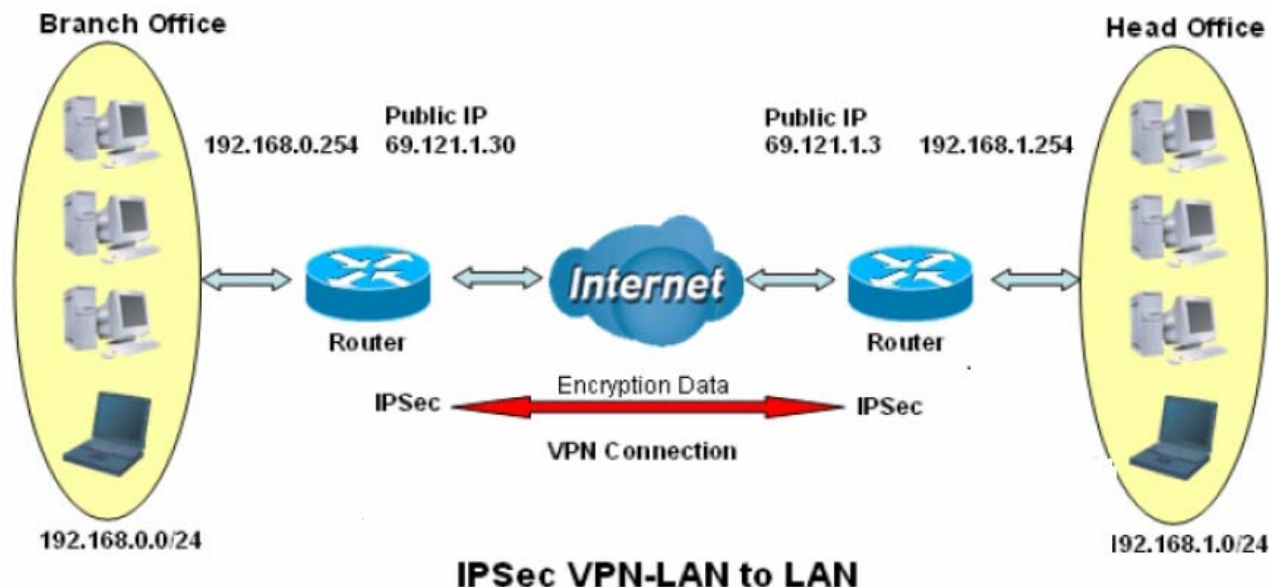
**Idle Timeout:** Auto-disconnect the IPSec connection after trying several consecutive times.

## Examples:

### 1. LAN-to-LAN connection

Two BiPAC 7800VDOXs want to setup a secure IPSec VPN tunnel

**Note:** The IPSec Settings shall be consistent between the two routers.



#### Head Office Side:

Setup details:

Item	Function		Description
1	Connection Name	H-to-B	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Secure Gateway Address(Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	





### IPsec

#### IPSec Settings

Connection Name	H-To-B	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	<input type="checkbox"/> Anonymous			
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

#### Phase 1

Mode	Main		
Encryption Algorithm	3DES	Integrity Algorithm	MD5
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]

#### Phase 2

Encryption Algorithm	3DES	Integrity Algorithm	MD5
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]

#### DPD Setting

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]

**Branch Office Side:**

Setup details: the same operation as done in Head Office side

Item	Function		Description	
1	Connection Name	B-to-H	Give a name for IPSec connection	
2	Local Network		Branch Office network	
	Subnet			Select Subnet
	IP Address	192.168.0.0		
	Netmask	255.255.255.0		
3	Remote Secure Gateway Address(Hostname)	69.121.1.3	IP address of the Head office router (on WAN side)	
4	Remote Network		Head office network	
	Subnet			Select Subnet
	IP Address	192.168.1.0		
	Netmask	255.255.255.0		
5	Proposal		Security Plan	
	Method	ESP		
	Authentication	MD5		
	Encryption	3DES		
	Prefer Forward Security	MODP 1024(group2)		
	Pre-shared Key	123456		

**Advanced Setup**

**IPsec**

**IPSec Settings**

Connection Name	<input type="text" value="B-To-H"/>	WAN Interface	<input type="text" value="Default"/>	IP Version	<input type="text" value="IPv4"/>
Local Network	Subnet <input type="text" value="Subnet"/>	IP Address	<input type="text" value="192.168.0.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Remote Security Gateway	<input type="text" value="69.121.1.3"/>	<input type="checkbox"/> Anonymous			
Remote Network	Subnet <input type="text" value="Subnet"/>	IP Address	<input type="text" value="192.168.1.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="IKE"/>	IPsec Protocol	<input type="text" value="ESP"/>		
Pre-Shared Key	<input type="text" value="123456"/>				
Local ID Type	<input type="text" value="Default"/>	ID Content	<input type="text"/>		
Remote ID Type	<input type="text" value="Default"/>	ID Content	<input type="text"/>		

**Phase 1**

Mode	<input type="text" value="Main"/>				
Encryption Algorithm	<input type="text" value="3DES"/>	Integrity Algorithm	<input type="text" value="MD5"/>		
DH Group	<input type="text" value="MODP1024(DH2)"/>	SA Lifetime	<input type="text" value="480"/>	Minute(s) [60-1440]	

**Phase 2**

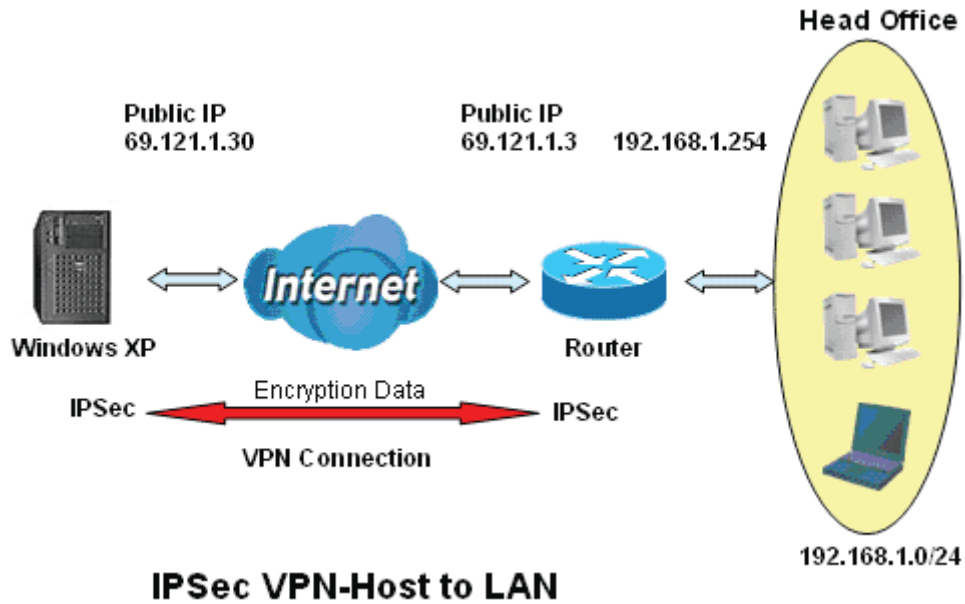
Encryption Algorithm	<input type="text" value="3DES"/>	Integrity Algorithm	<input type="text" value="MD5"/>		
DH Group	<input type="text" value="None"/>	IPSec Lifetime	<input type="text" value="60"/>	Minute(s) [60-1440]	

**DPD Setting**

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Detection Interval	<input type="text" value="180"/>	Second(s)	Idle Timeout	<input type="text" value="5"/>	Consecutive times [5-99]
	[180-86400]				

## 2. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



Item	Function		Description
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Single Address	69.121.1.30	Host
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



▼ IPsec

IPSec Settings

Connection Name	B-To-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	<input type="checkbox"/> Anonymous			
Remote Network	Single Address	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480	Minute(s) [60-1440]	

Phase 2

Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60	Minute(s) [60-1440]	

DPD Setting

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Detection Interval	180	Second(s)	Idle Timeout	5	Consecutive times [5-99]

Apply

## PPTP

The **Point-to-Point Tunneling Protocol (PPTP)** is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2 or EAP-TLS. The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2 or EAP-TLS.

**Note:** 4 sessions for Client and 4 sessions for Server respectively.

In PPTP session, users can set the basic parameters (authentication, encryption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitute the PPTP Server setting.

Parameters	
PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Interface	Default
Auth. Type	Pap or Chap
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.0
Idle Timeout	0 [0-120] Minute(s)

**PPTP Function:** Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

**WAN Interface:** Select the exact WAN interface configured for the tunnel. Select **Default** to use the now-working WAN interface for the tunnel.

**Auth. Type:** The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

**Encryption Key Length:** The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

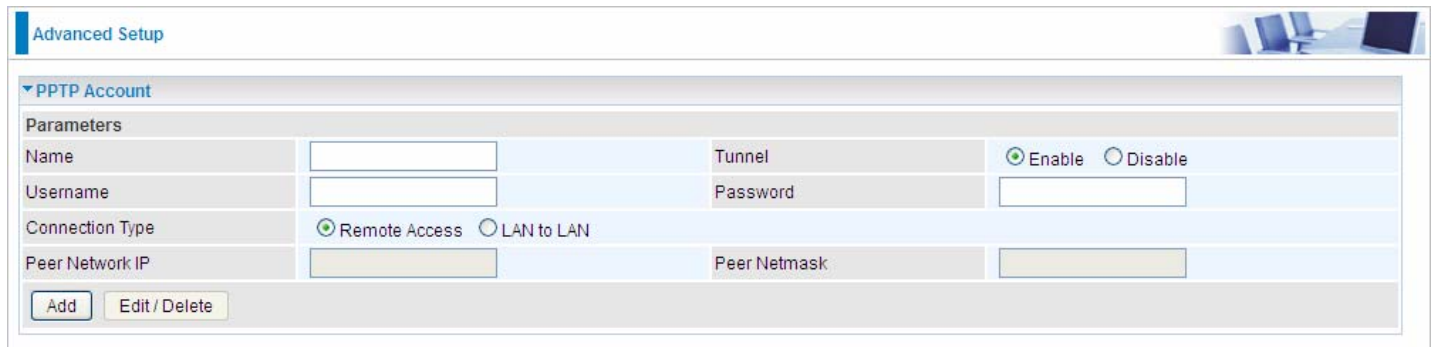
**Peer Encryption Mode:** You may select "Stateful" or "Allow Stateless and Stateful" mode. The key will be changed every 256 packets when you select Stateful mode.

**IP Addresses Assigned to Peer:** 192.168.1.x: please input the IP assigned range from 1~ 254.

**Idle Timeout:** Specify the time for remote peer to be disconnected without any activities, from 0~120 minutes.

Click **Apply** to submit your PPTP Server basic settings.

## PPTP Account



The screenshot shows a web-based configuration interface for a PPTP account. The page title is "Advanced Setup". Under the "PPTP Account" section, there is a "Parameters" table with the following fields:

Parameters	
Name	<input type="text"/>
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="password"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/>
Peer Netmask	<input type="text"/>

At the bottom of the form, there are two buttons: "Add" and "Edit / Delete".

**Connection Name:** A user-defined name for the connection.

**Tunnel:** Select **Enable** to activate the account. PPTP server is waiting for the client to connect to this account.

**Username:** Please input the username for this account.

**Password:** Please input the password for this account.

**Connection Type:** Select Remote Access for single user, Select LAN to LAN for remote gateway.

**Peer Network IP:** Please input the subnet IP for remote network.

**Peer Netmask:** Please input the Netmask for remote network.

## PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.

The screenshot shows the 'Advanced Setup' page for configuring a PPTP Client. The configuration is organized into a 'Parameters' section with the following fields and options:

Name	<input type="text"/>	WAN Interface	Default <input type="button" value="v"/>
Username	<input type="text"/>	Password	<input type="text"/>
Auth. Type	Pap or Chap <input type="button" value="v"/>	PPTP Server Address	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN	Time to Connect	<input type="radio"/> Always <input checked="" type="radio"/> Manual
Peer Network IP	<input type="text"/>	Peer Netmask	<input type="text"/>

At the bottom left of the configuration area, there are two buttons: 'Add' and 'Edit / Delete'.

**Name:** user-defined name for identification.

**WAN Interface:** Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

**Username:** Enter the username provided by your VPN Server.

**Password:** Enter the password provided by your VPN Server.

**Auth. Type:** Default is Auto if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

**PPTP Server Address:** Enter the IP address of the PPTP server.

**Connection Type:** Select Remote Access for single user, Select LAN to LAN for remote gateway.

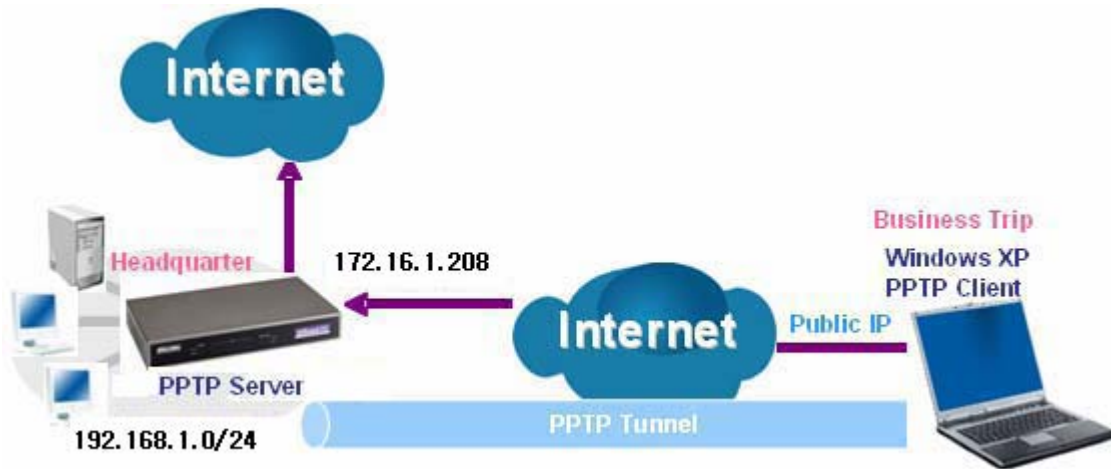
**Time to Connect:** Select Always to keep the connection always on, or Manual to connect manually any time.

**Peer Network IP:** Please input the subnet IP for Server peer.

**Peer Netmask:** Please input the Netmask for server peer.

Click **Edit/Delete** button to save your changes.

**Example: PPTP Remote Access with Windows7**  
**(Note: inside test with 172.16.1.208, just an example for illustration)**



**Server Side:**

**1. Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

Advanced Setup

▼ PPTP

Parameters

PPTP Function  Enable  Disable

WAN Interface Default

Auth. Type MS-CHAPv2

Encryption Key Length Auto

Peer Encryption Mode Only Stateless

IP Addresses Assigned to Peer start from : 192.168.1.100

Idle Timeout 10 [0-120] Minute(s)

Apply Cancel

**2: Create a PPTP Account “test”.**

Advanced Setup

▼ PPTP Account

Parameters

Name test Tunnel  Enable  Disable

Username test Password ●●●●

Connection Type  Remote Access  LAN to LAN

Peer Network IP Peer Netmask

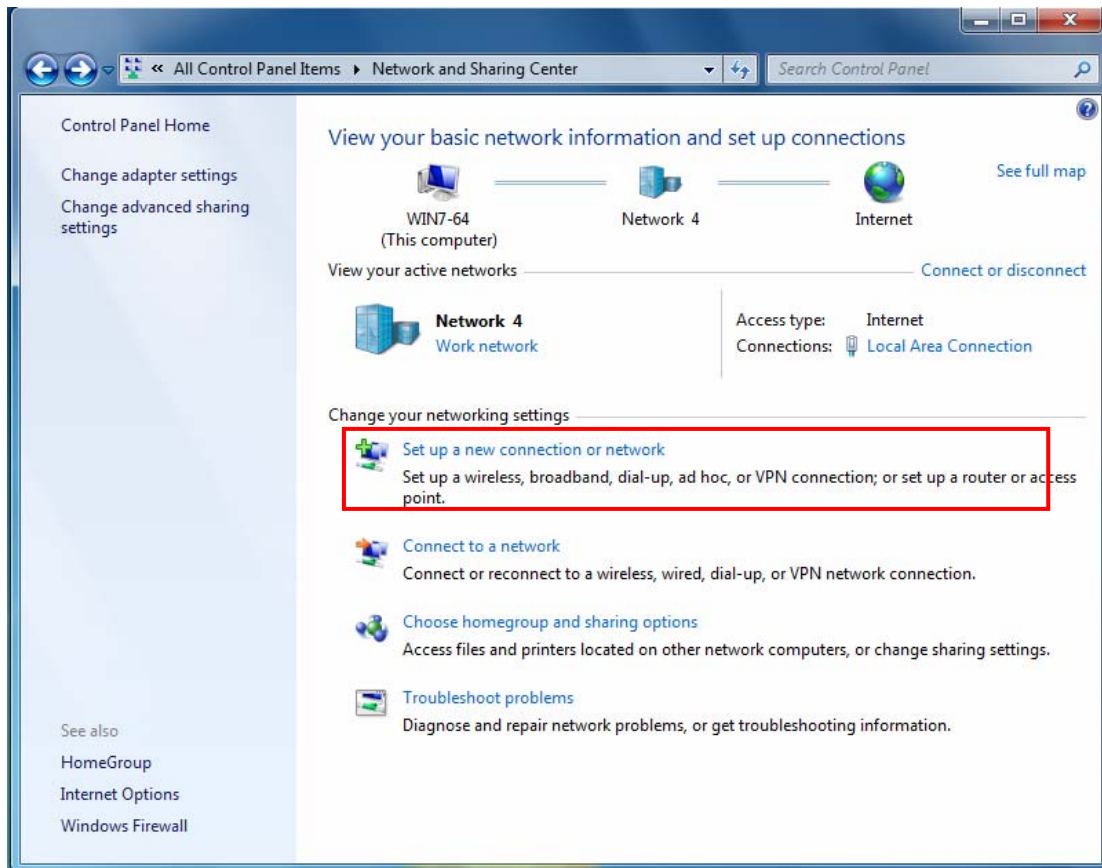
Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	test	Enable	Remote Access			<input type="checkbox"/>

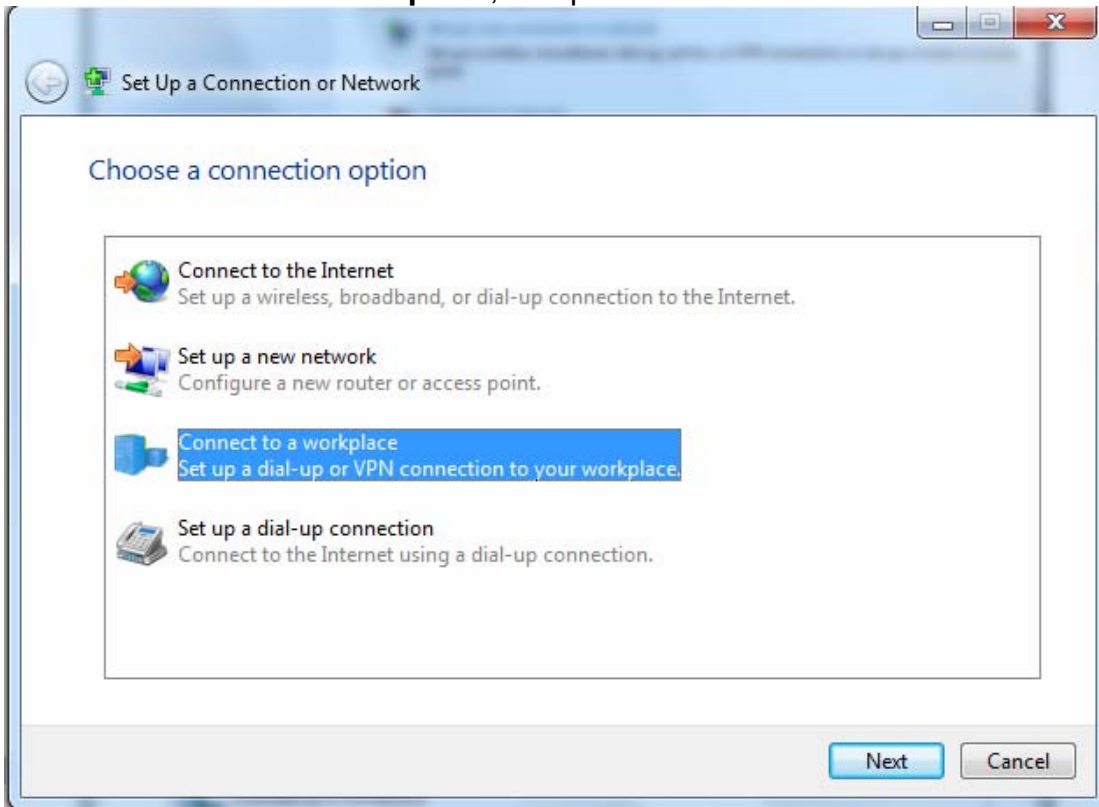


**Client Side:**

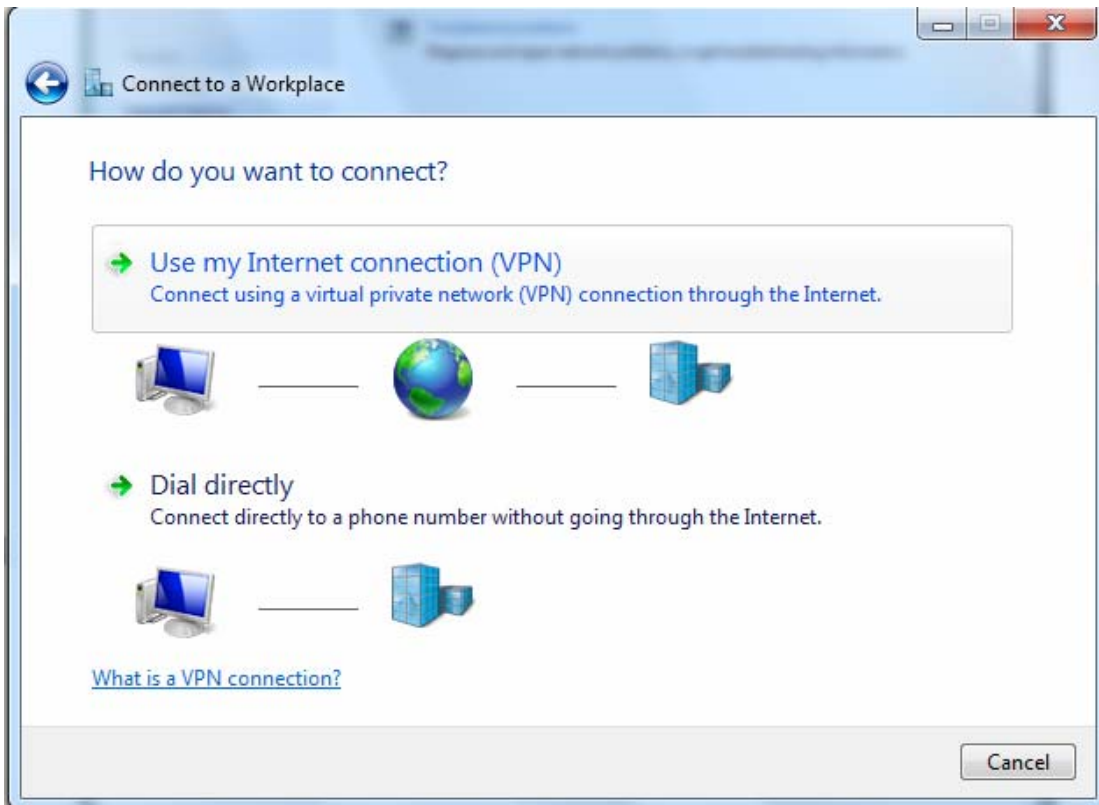
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

Use a smart card

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Next Cancel

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.208

Destination name: test

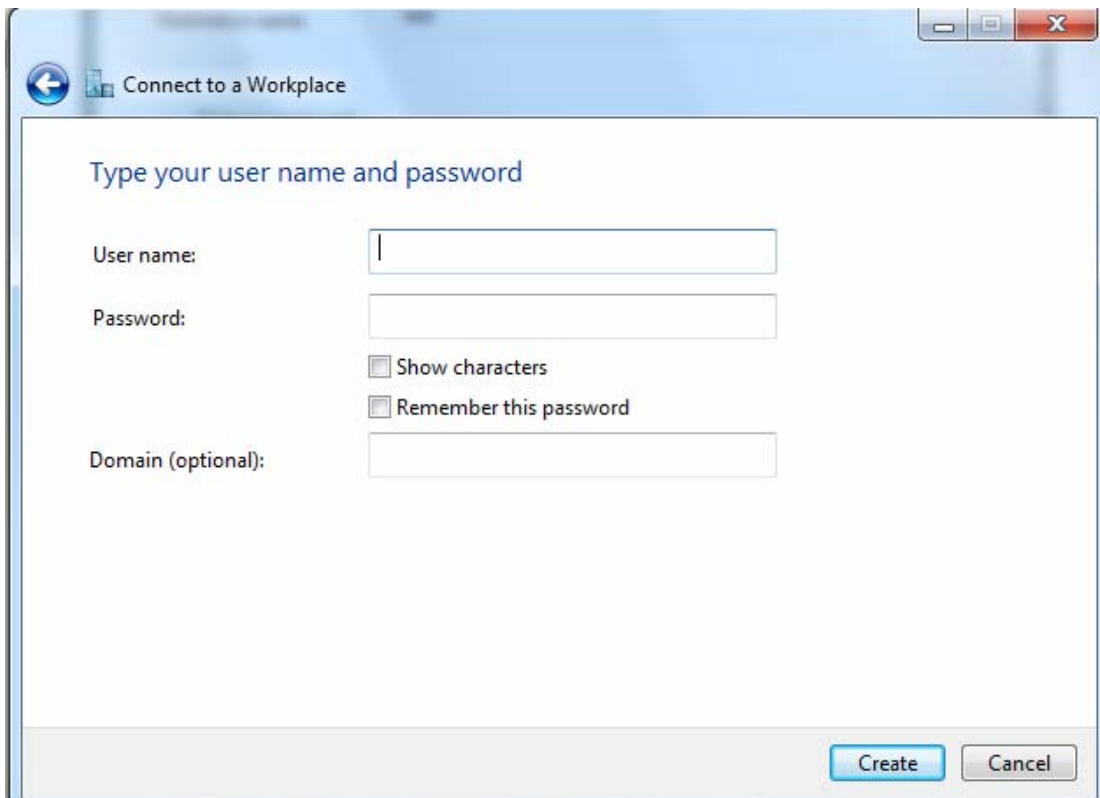
Use a smart card

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

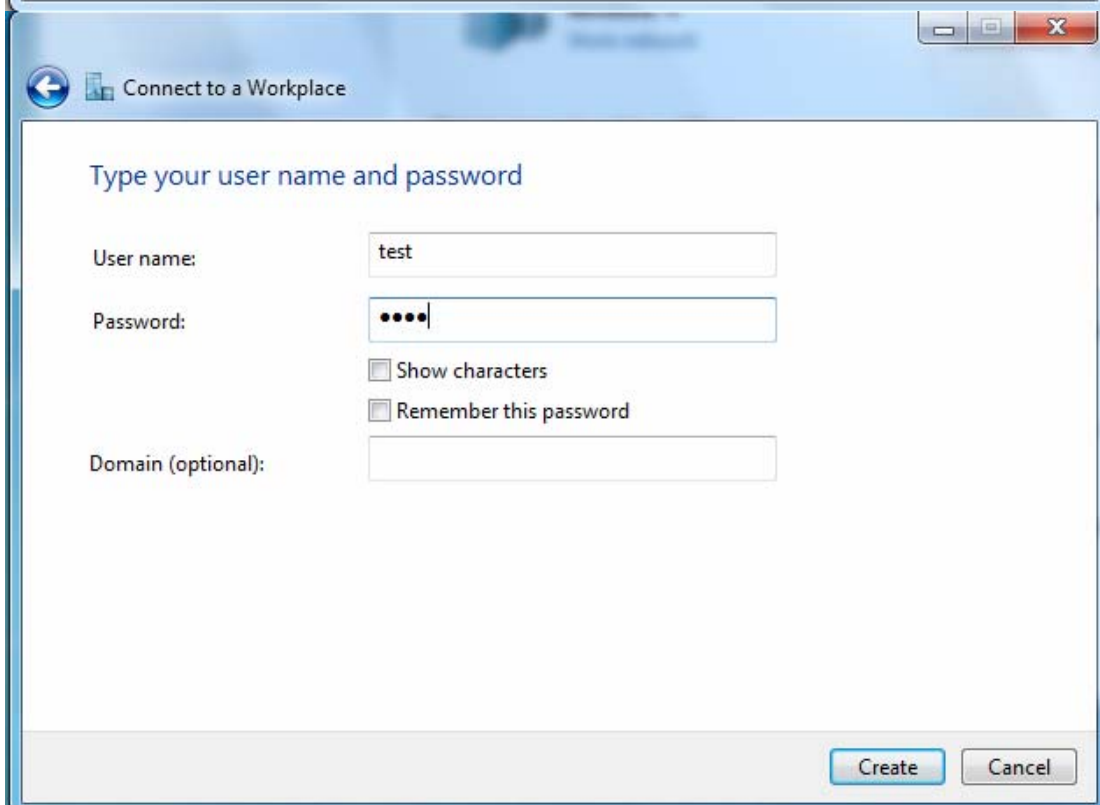
Don't connect now; just set it up so I can connect later

Next Cancel

5. Input the account (**user name** and **password**) and press **Create**.

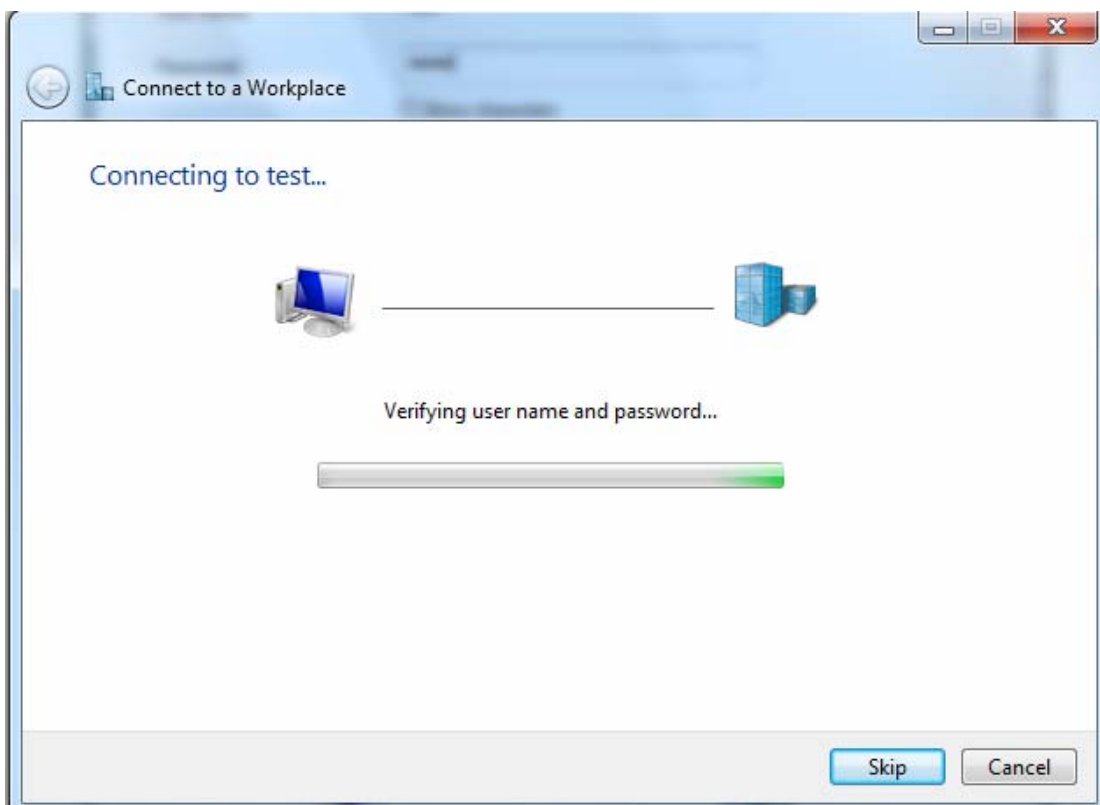
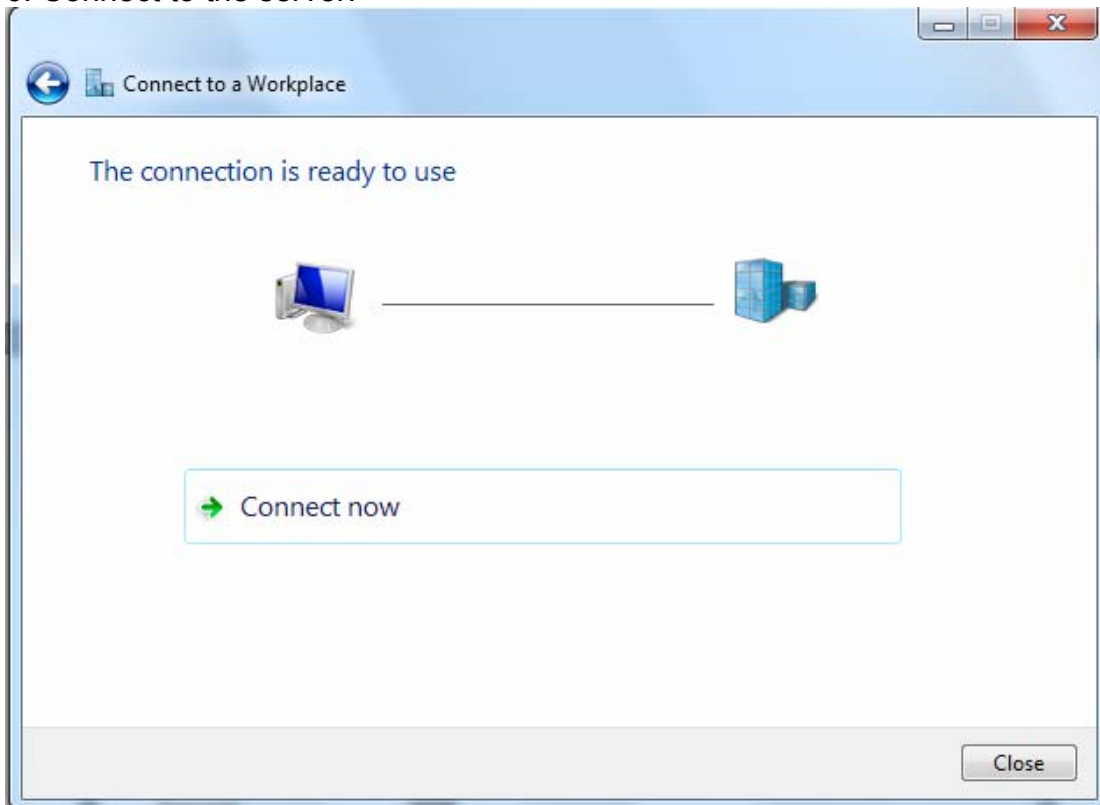


The screenshot shows a dialog box titled "Connect to a Workplace". The main heading is "Type your user name and password". There are four input fields: "User name:", "Password:", "Domain (optional):", and a checkbox area. The "User name" field is empty. The "Password" field is empty. The "Domain (optional)" field is empty. The checkbox area contains two options: "Show characters" and "Remember this password", both of which are unchecked. At the bottom right, there are two buttons: "Create" and "Cancel".

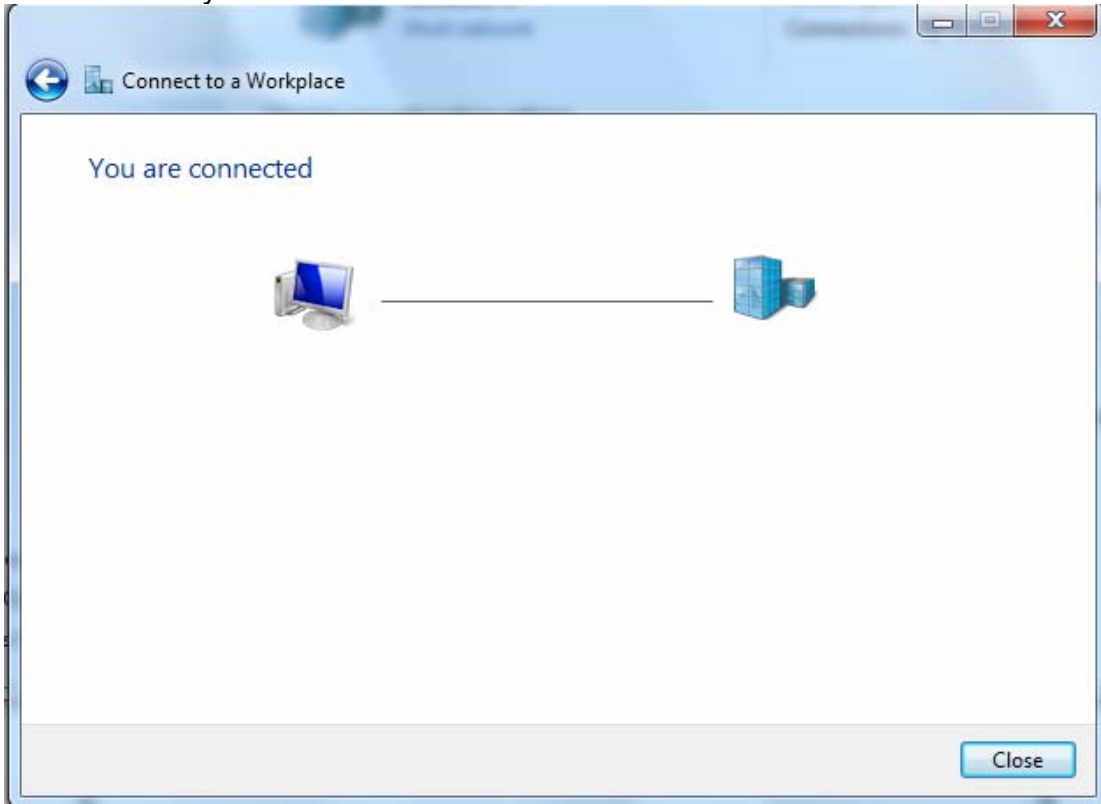


The screenshot shows the same "Connect to a Workplace" dialog box. The "User name" field now contains the text "test". The "Password" field contains four black dots, indicating a masked password. The "Domain (optional)" field remains empty. The checkbox area remains unchanged with "Show characters" and "Remember this password" unchecked. The "Create" and "Cancel" buttons are still present at the bottom right.

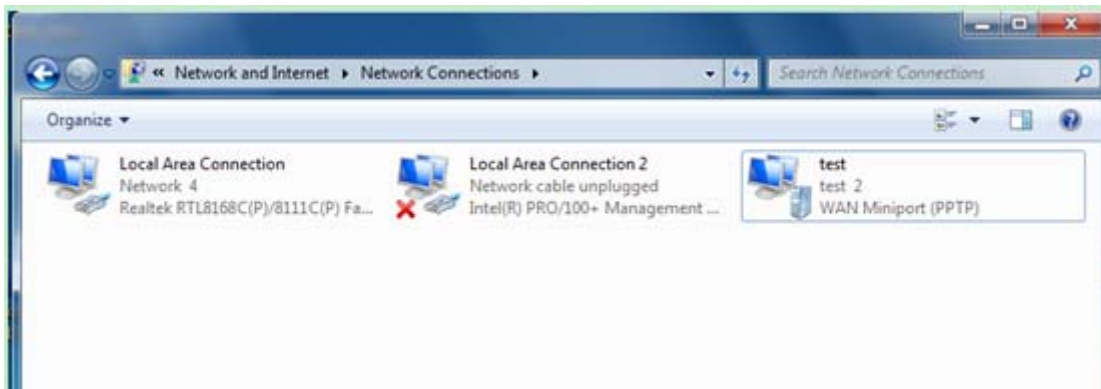
6. Connect to the server.

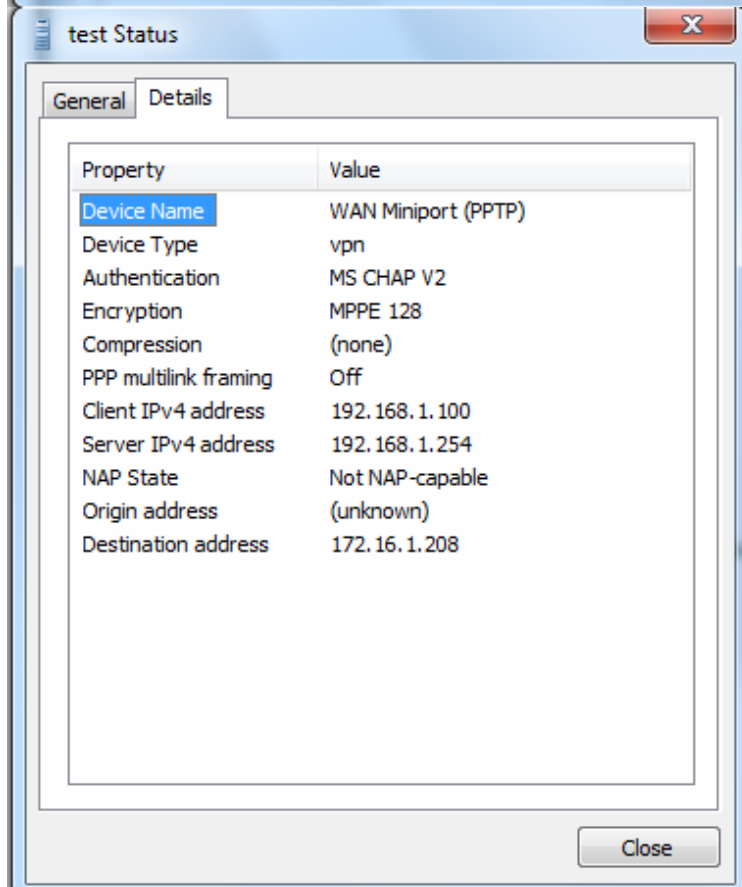
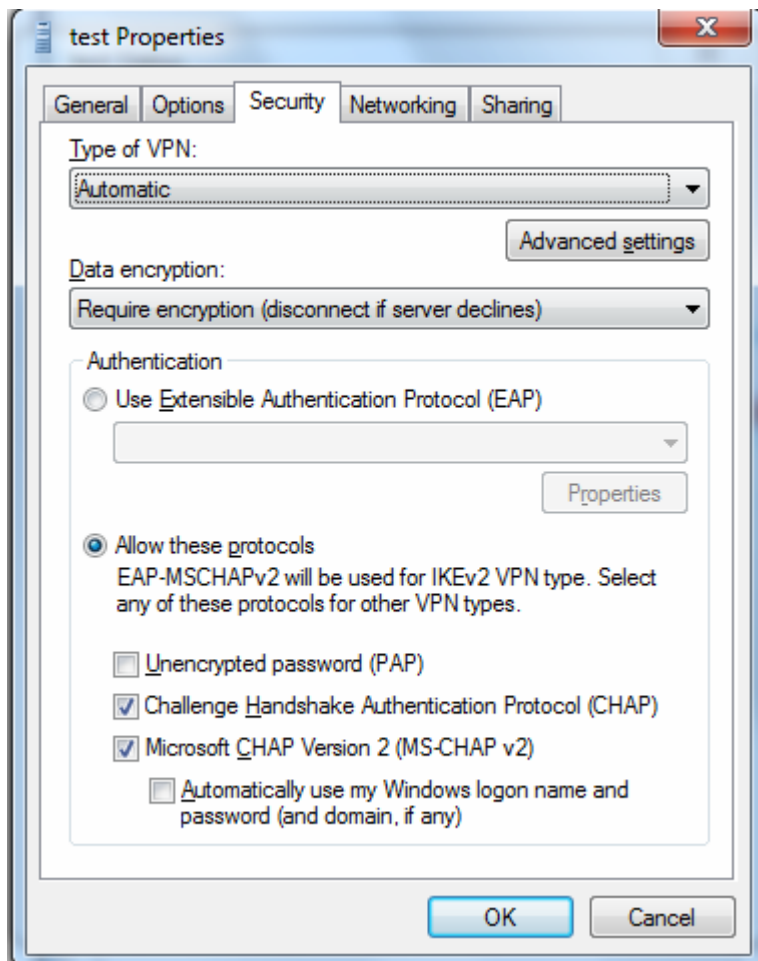


7. Successfully connected.



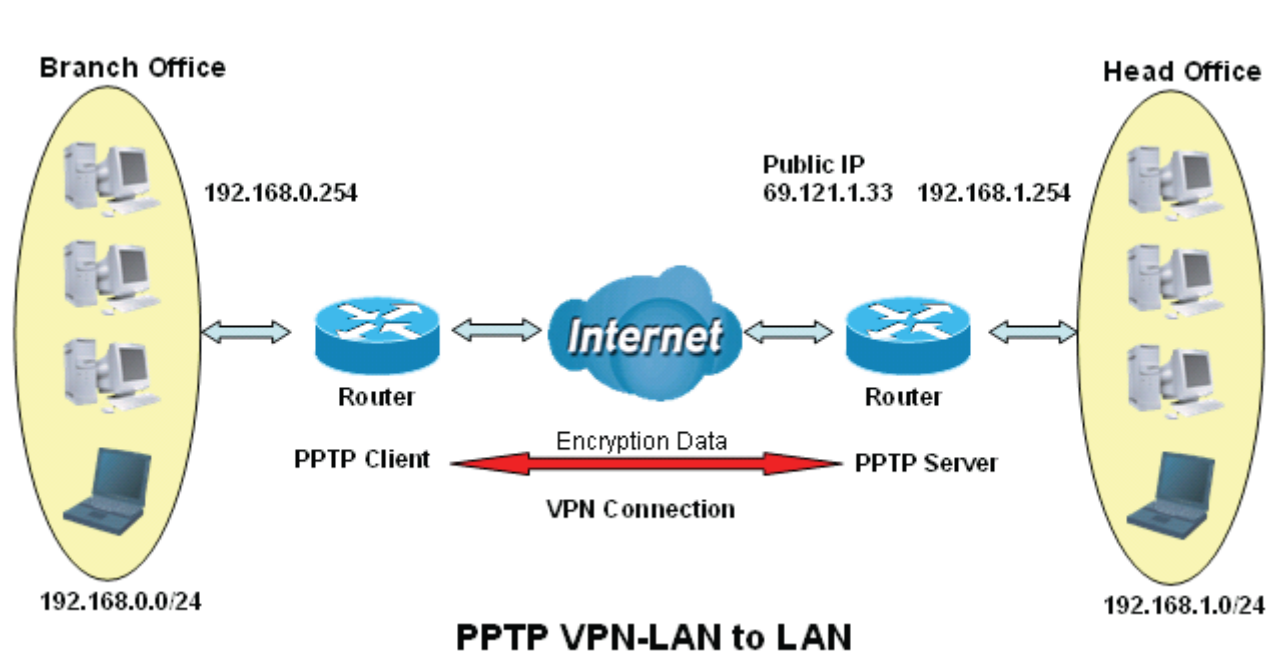
**PS:** You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "Properties" to change the security parameters (if the connection fails, users can go here to change the settings)





## Example: Configuring a LAN-to-LAN PPTP VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.



### Server side: Head Office

Advanced Setup

**PPTP**

Parameters

PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.100
Idle Timeout	10 [0-120] Minute(s)

Apply Cancel

The above is the commonly setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then account the PPTP Account.

Advanced Setup

**PPTP Account**

Parameters

Name	HO	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test	Password	.....
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN		
Peer Network IP	192.168.0.0	Peer Netmask	255.255.255.0

Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>



## Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.

Advanced Setup

▼ PPTP Client

Parameters

Name	BO	WAN Interface	Default
Username	test	Password	••••
Auth. Type	MS-CHAPv2	PPTP Server Address	69.121.1.3
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN	Time to Connect	<input type="radio"/> Always <input checked="" type="radio"/> Manual
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	<input type="checkbox"/>

**Note:** users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

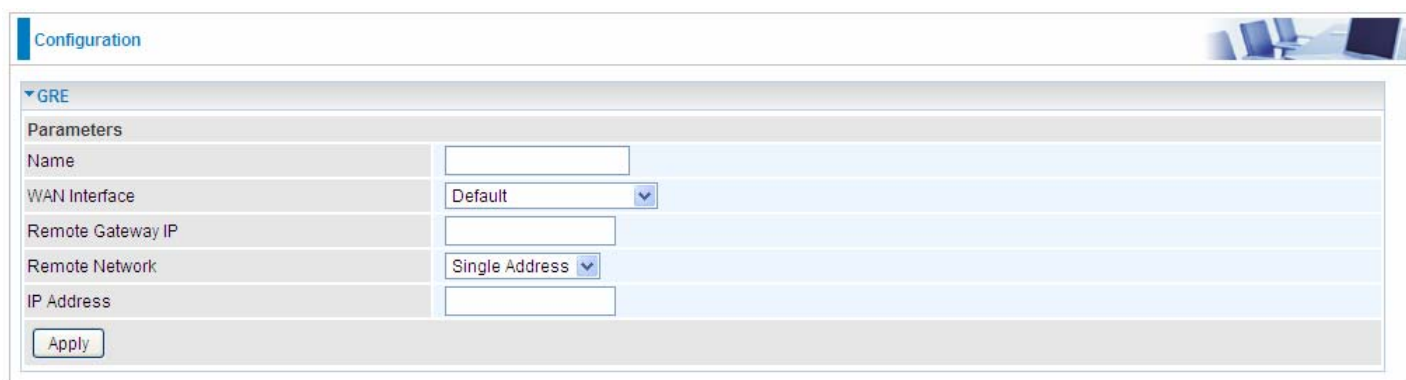
## GRE

**Generic Routing Encapsulation (GRE)** is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an Internet Protocol (IP) network. And the common use can be GRE over IPsec.



The screenshot shows a configuration window titled "Configuration" with a "GRE" section. Below the section header is a table titled "GRE Connections". The table has columns for "Active", "Default Gateway", "Name", "Remote Gateway IP", "Remote Network", "Remove", and "Edit". Below the table are two buttons: "Add" and "Remove".

Click **Add** to set up new GRE tunnels.



The screenshot shows the "GRE Parameters" configuration form. It includes the following fields and controls:

- Name:** A text input field.
- WAN Interface:** A dropdown menu with "Default" selected.
- Remote Gateway IP:** A text input field.
- Remote Network:** A dropdown menu with "Single Address" selected.
- IP Address:** A text input field.

An "Apply" button is located at the bottom left of the form.

**Name:** User-defined identification.

**WAN Interface:** Select the exact WAN interface configured for the tunnel as the source tunnel IP. Select Default to use the now-working WAN interface for the tunnel.

**Remote Gateway IP:** Set the destination IP for the tunnel.

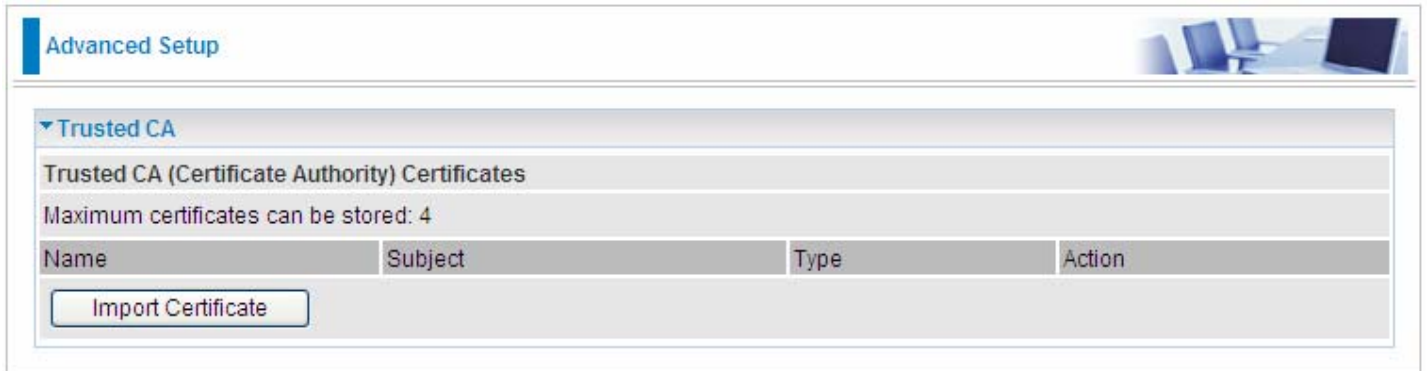
**Remote Network:** Select the peer topology, Single address (client) or Subnet.

**IP Address:** Set the IP address if the peer is a client. If the peer is a subnet, please enter the IP and netmask.

# Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate doesn't match the authorized certificate of the ACS Server, the device will have no access to the server.

## Trusted CA



**Certificate Name:** The certificate identification name.

**Subject:** The certificate subject.

**Type:** The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

**Action:**

- View: view the certificate.
- Remove: remove the certificate.

Click **Import Certificate** button to import your certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name	<input type="text"/>
------	----------------------

Certificate

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Apply

Enter the certificate name and insert the certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters


Name	acscert
------	---------

Certificate

```
-----BEGIN CERTIFICATE-----  
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQG  
GEwJD  
TjEXMBUGA1UEChMOQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc  
NMjAw  
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV  
yYXRp  
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN  
ZuTJD  
rSwXGjaexPnBie5zNJc70SPQYgVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/  
Uu9be  
pUJBenxvYRgTImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73  
/se+H  
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu  
gOaQ3  
MDUxCzAJBgNVBAYTAKNOMRcwFQYDVQQKEw5DRkNBIFBvbG1jeSBBDQITENMA  
GA1UE  
AxMEQ1JMMTALBgNVHQ8EBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS  
FaAqX  
k1NC0tAwHQYDVRO0BBYEFMMnxjZoyCdlJIEvkdLJjMC5RrpMAwGA1UdEwQ
```

Apply

Click Apply to confirm your settings.

**Advanced Setup** 

▼ **Trusted CA**

**Trusted CA (Certificate Authority) Certificates**

Maximum certificates can be stored: 4

Name	Subject	Type	Action
acscert	C=CN/O=CFCA Operation CA	ca	<a href="#">View</a> <a href="#">Remove</a>

[Import Certificate](#)

# Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol**, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

**Advanced Setup**

**IGMP**

Parameters	
Default Version	3 [1-3]
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	25
Maximum Multicast Data Sources (for IGMPv3)	10 [1-24]
Maximum Multicast Group Members	25
Fast Leave	<input checked="" type="checkbox"/> Enable
LAN to LAN (Intra LAN) Multicast	<input type="checkbox"/> Enable
Mebership Join Immediate (IPTV)	<input type="checkbox"/>

**MLD**

Default Version	2 [1-2]
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	10
Maximum Multicast Data Sources (for MLDv2)	10 [1-24]
Maximum Multicast Group Members	10
Fast Leave	<input checked="" type="checkbox"/> Enable
LAN to LAN (Intra LAN) Multicast	<input checked="" type="checkbox"/> Enable

Apply Cancel

## IGMP

**Default Version:** Enter the supported IGMP version, 1-3, default is IGMP v3.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

**Query Response Interval:** Enter the response interval time (sec).

**Last Member Query Interval:** Enter the interval time (sec) the multicast router query the specified

group after it has received leave message.

**Robustness Value:** Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

**Maximum Multicast Groups:** Enter the Maximum Multicast Groups.

**Maximum Multicast Data Sources( for IGMP v3):** Enter the Maximum Multicast Data Sources,1-24.

**Maximum Multicast Group Members:** Enter the Maximum Multicast Group Members.

**Fast leave:** Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

**LAN to LAN (Intra LAN) Multicast:** Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

**Membership Join Immediate (IPTV):** When a host joins a multicast session, it sends unsolicited join report to its upstream router immediately. The Startup Query Interval has been set to 1/4 of the General Query value to enable the faster join at startup.

## MLD

**Default Version:** Enter the supported MLD version, 1-2, default is MLDv2.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

**Query Response Interval:** Enter the response interval time (sec).

**Last Member Query Interval:** Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

**Robustness Value:** Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

**Maximum Multicast Groups:** Enter the Maximum Multicast Groups.

**Maximum Multicast Data Sources( for MLDv2):** Enter the Maximum Multicast Data Sources,1-24.

**Maximum Multicast Group Members:** Enter the Maximum Multicast Group Members.

**Fast leave:** Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

**LAN to LAN (Intra LAN) Multicast:** Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

# Management

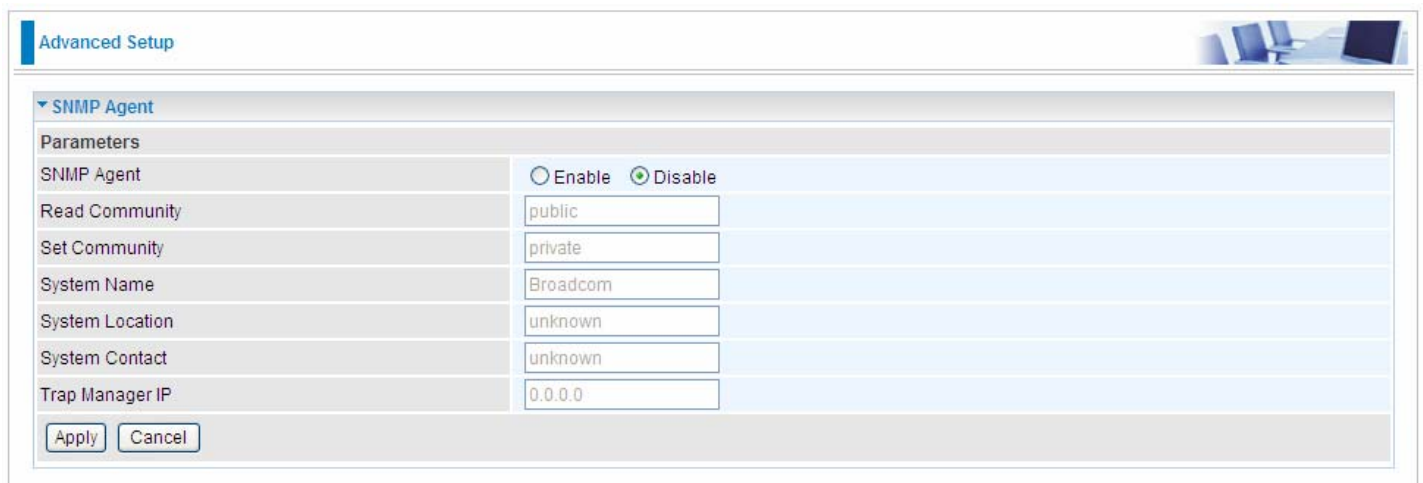
## SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager, SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest, GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



The screenshot shows the 'Advanced Setup' page for the SNMP Agent configuration. The page has a blue header with the text 'Advanced Setup' and a small image of a server rack on the right. Below the header, there is a section titled 'SNMP Agent' with a dropdown arrow. Underneath, there is a 'Parameters' section with a table of configuration options. The 'SNMP Agent' option is set to 'Disable' (indicated by a checked radio button). Other parameters include 'Read Community' (public), 'Set Community' (private), 'System Name' (Broadcom), 'System Location' (unknown), 'System Contact' (unknown), and 'Trap Manager IP' (0.0.0.0). At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

Parameters	
SNMP Agent	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Read Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
System Name	<input type="text" value="Broadcom"/>
System Location	<input type="text" value="unknown"/>
System Contact	<input type="text" value="unknown"/>
Trap Manager IP	<input type="text" value="0.0.0.0"/>

**SNMP Agent:** enable or disable SNMP Agent.

**Read Community:** Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

**Set Community:** Type the Set Community, which is the authentication for incoming Set requests from the management station.

**System Name:** here it refers to your router.

**System Location:** user-defined location.

**System Contact:** user-defined contact message.

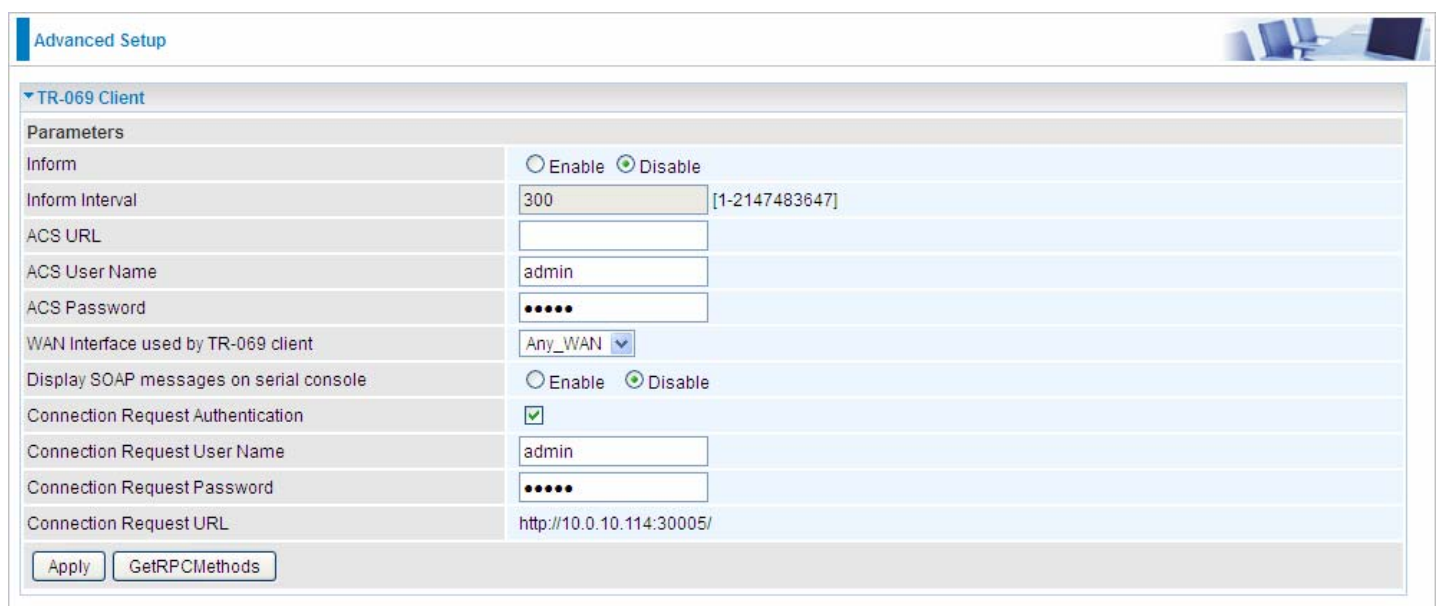
**Trap manager IP:** enter the IP address of the server receiving the trap sent by SNMP agent.



## TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



The screenshot shows the 'Advanced Setup' page for the 'TR-069 Client'. The page is titled 'Advanced Setup' and has a small image of a computer monitor in the top right corner. The main content is a form with the following fields and options:

Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform Interval	300 [1-2147483647]
ACS URL	
ACS User Name	admin
ACS Password	•••••
WAN Interface used by TR-069 client	Any_WAN
Display SOAP messages on serial console	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request User Name	admin
Connection Request Password	•••••
Connection Request URL	http://10.0.10.114:30005/

At the bottom of the form, there are two buttons: 'Apply' and 'GetRPCMethods'.

**Inform:** select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

**Inform Interval:** Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

**ACS URL:** Enter the ACS server login name.

**ACS User Name:** Specify the ACS User Name for ACS authentication to the connection from CPE.

**ACS password:** Enter the ACS server login password.

**WAN interface used by TR-069:** select the interface used by TR-069.

**Display SOAP message on serial console:** select whether to display SOAP message on serial console.

**Connection Request Authentication:** Check to enable connection request authentication feature.

**Connection Request User Name:** Enter the username for ACS server to make connection request.

**Connection Request User Password:** Enter the password for ACS server to make connection request.

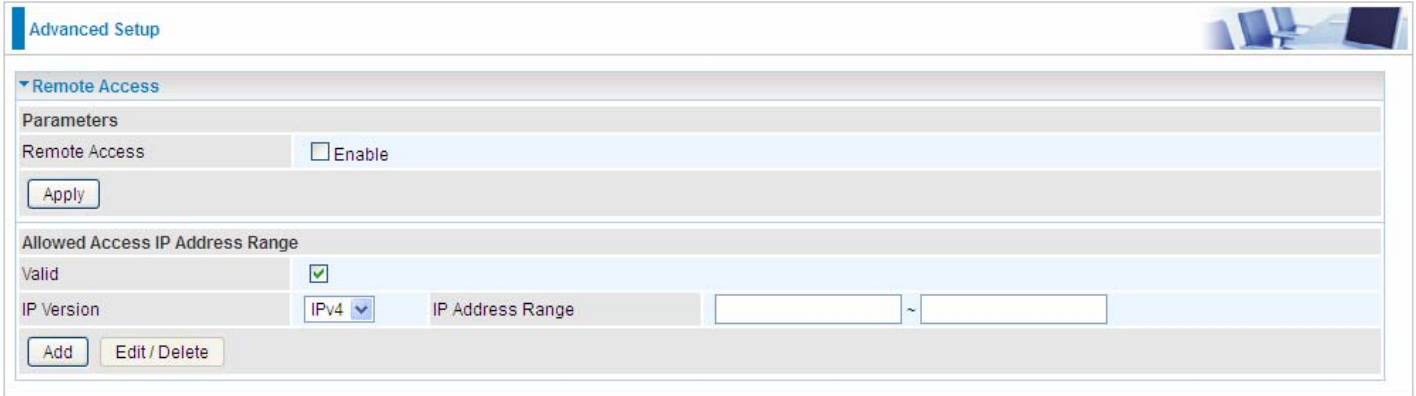
**Connection Request URL:** Automatically match the URL for ACS server to make connection request.

**GetRPCMethods:** Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

## Remote Access

It is to allow remote access to the router to view or configure.



The screenshot shows the 'Advanced Setup' page for 'Remote Access'. Under the 'Parameters' section, there is a checkbox for 'Remote Access' which is currently unchecked. An 'Apply' button is located below this section. The 'Allowed Access IP Address Range' section contains a 'Valid' checkbox which is checked. Below it, there is a dropdown menu for 'IP Version' set to 'IPv4', followed by an 'IP Address Range' field with two input boxes separated by a tilde (~). At the bottom of this section are 'Add' and 'Edit / Delete' buttons.

**Remote Access:** Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

“**Allowed Access IP Address Range**” was used to restrict which IP address could login to access system web GUI.

**Valid:** Enable/Disable Allowed Access IP Address Range

**IP Address Range:** Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click **Add** to add an IP Range to allow remote access.

**Note: 1.** If user wants to grant remote access to IPs, first enable **Remote Access**.

### 2. Remote Access enabled:

- 1) Enable **Valid** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.
- 2) Disable **Valid** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.
- 3) No listing of IP range is to allow any IP(s) to remote access the router.

## Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.



Advanced Setup

Power Management

Parameters

Parameter	Enable	Status	Value
MIPS CPU Clock divider when Idle	<input checked="" type="checkbox"/> Enable	Status	Enabled
Wait instruction when Idle	<input checked="" type="checkbox"/> Enable	Status	Enabled
DRAM Self Refresh	<input checked="" type="checkbox"/> Enable	Status	Enabled
Ethernet Auto Power Down	<input checked="" type="checkbox"/> Enable	Status	Enabled
Adaptive Voltage Scaling	<input checked="" type="checkbox"/> Enable	Status	Enabled

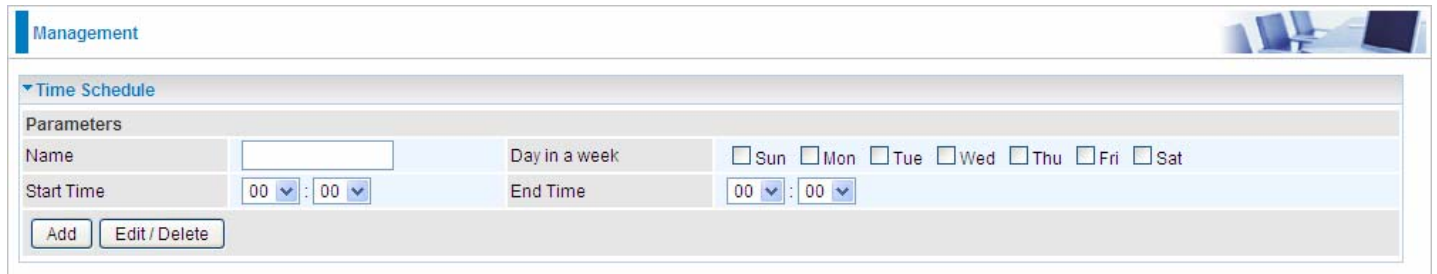
Number of ethernet interfaces in:  
Full power mode: 1  
Low power mode: 3

Apply Refresh

## Time Schedule

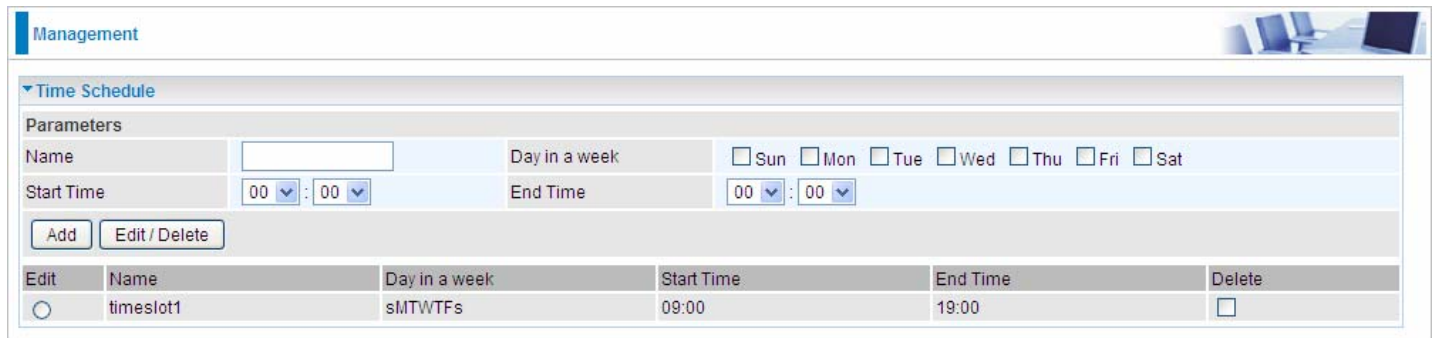
The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Internet Times** for details. Your router time should correspond



The screenshot shows the 'Management' interface with a 'Time Schedule' section. Under 'Parameters', there are fields for 'Name', 'Start Time', and 'End Time', each with dropdown menus for hours and minutes. A 'Day in a week' section contains checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. 'Add' and 'Edit / Delete' buttons are located below the form.

For example, user can add a timeslot named "timeslot1" features a period from 9:00 of Monday to 19:00 of Friday.



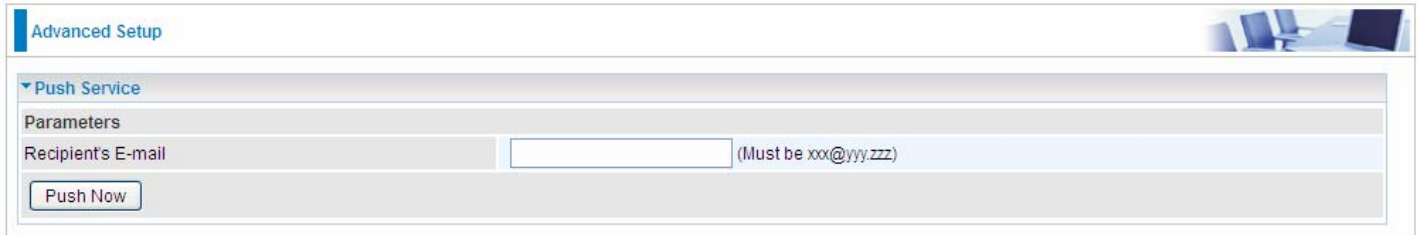
The screenshot shows the 'Management' interface with the 'Time Schedule' section. Below the 'Parameters' form, there is a table with the following data:

Edit	Name	Day in a week	Start Time	End Time	Delete
<input type="radio"/>	timeslot1	sMTWTFs	09:00	19:00	<input type="checkbox"/>

# Diagnostics

## Push Service

With push service, the system can send email messages with consumption data and system information.




The screenshot shows a web interface for 'Advanced Setup'. Under the 'Push Service' section, there is a 'Parameters' area. It contains a text input field labeled 'Recipient's E-mail' with a placeholder '(Must be xxx@yyy.zzz)'. Below the input field is a button labeled 'Push Now'.

**Recipient's E-mail:** Enter the destination mail address. The email is used to receive **system log** , **system configuration**, **security log** sent by the device when the **Push Now** button is pressed (information sent only when pressing the button ), but the mail address is not remembered.

**Note:** Please first set correct the SMTP server parameters in [Mail Alert](#).

## Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection. Click **Help** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

Diagnosics --- pppoe\_0\_8\_35 

▼ Test the connection to your local network		
Test LAN Connection ( P3 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P2 )	PASS	<a href="#">Help</a>
Test LAN Connection ( P1 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P4/EWAN )	FAIL	<a href="#">Help</a>
Test your Wireless Connection	PASSPASS	<a href="#">Help</a>
▼ Test the connection to your DSL service provider		
Test xDSL Synchronization	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping	PASS	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping	PASS	<a href="#">Help</a>
▼ Test the connection to your Internet service provider		
Test PPP server connection	PASS	<a href="#">Help</a>
Test authentication with ISP	PASS	<a href="#">Help</a>
Test the assigned IP address	PASS	<a href="#">Help</a>
Ping default gateway	PASS	<a href="#">Help</a>
Ping primary Domain Name Server	FAIL	<a href="#">Help</a>

## Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) is a standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Fault Management is to uniquely test the VDSL PTM connection; Push service

Advanced Setup

802.1ag Connectivity Fault Management

Parameters

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level: 2

Destination MAC Address: [Empty]

802.1Q VLAN ID: 0 [0-4095]

VDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM)

Find Maintenance End Points (MEPs)

Linktrace Message (LTM)

Set MD Level Send Loopback Send Linktrace

**Maintenance Domain (MD) Level:** Maintenance Domains (MDs) are management spaces on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchal relationship exists between domains based on levels. The larger the domain, the higher the level value.


**Maintenance End Point:** Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

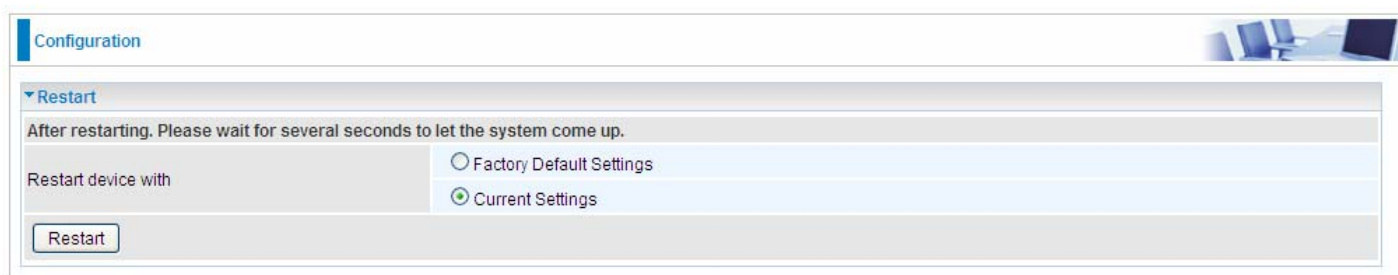
**Link Trace:** Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

**Loop-back:** Loop-back messages otherwise known as MaC ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loopback to successive MIPs can determine the location of a fault. Sending a high volume of Loopback Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loopback to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.



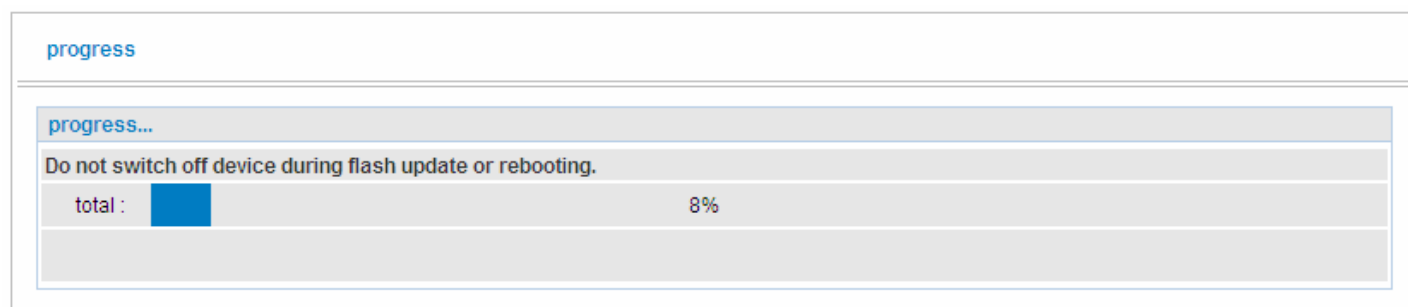
# Restart

This section lets you restart your router if necessary. Click  **Restart** in the low right corner of each configuration page.



The screenshot shows a configuration page with a 'Configuration' header. Below it is a 'Restart' section. The text reads: 'After restarting. Please wait for several seconds to let the system come up.' There are two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. A 'Restart' button is located at the bottom left of the section.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.



The screenshot shows a progress bar with the text 'progress' at the top. Below it is a 'progress...' section. The text reads: 'Do not switch off device during flash update or rebooting.' There is a progress bar with a blue fill and the text 'total : 8%' next to it.

# Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

## Problems with the router

Problem	Suggested Action
<b>None of the LEDs is on when you turn on the router</b>	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
<b>You have forgotten your login username or password</b>	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

## Problems with WAN interface

Problem	Suggested Action
<b>Frequent loss of ADSL line sync (disconnections)</b>	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

## Problem with LAN interface

Problem	Suggested Action
<b>Cannot PING any PC on LAN</b>	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

# Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

## Contact Billion

### Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### **FCC Caution**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

### **Co-location statement**

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

### **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.