

# DNS

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

## DNS

**Parameters**  
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider 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 USB3G0	

Use the following Static DNS IP address

Primary DNS server:   
Secondary DNS server:

Use the IP Addresses provided by Parental Control Provider

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: pppoe\_0\_8\_35/ppp0.1

Use the following Static IPv6 DNS address

Primary IPv6 DNS server:   
Secondary IPv6 DNS server:

Apply Cancel

### ➤ IPv4

#### Three ways to set an IPv4 DNS server

- ① **Select DNS server interface from available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **User the following Static DNS IP address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Use the IP address provided by Parental Control Provider:** If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

### ➤ IPv6:

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

#### 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.

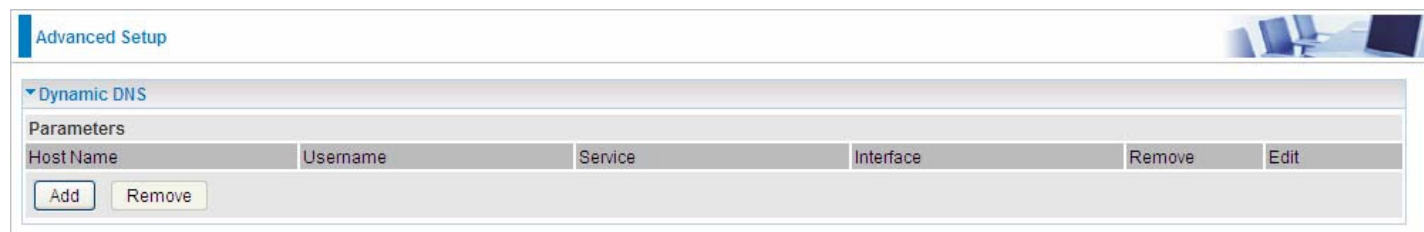
#### Use the following Static IPv6 DNS address

**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).



Advanced Setup

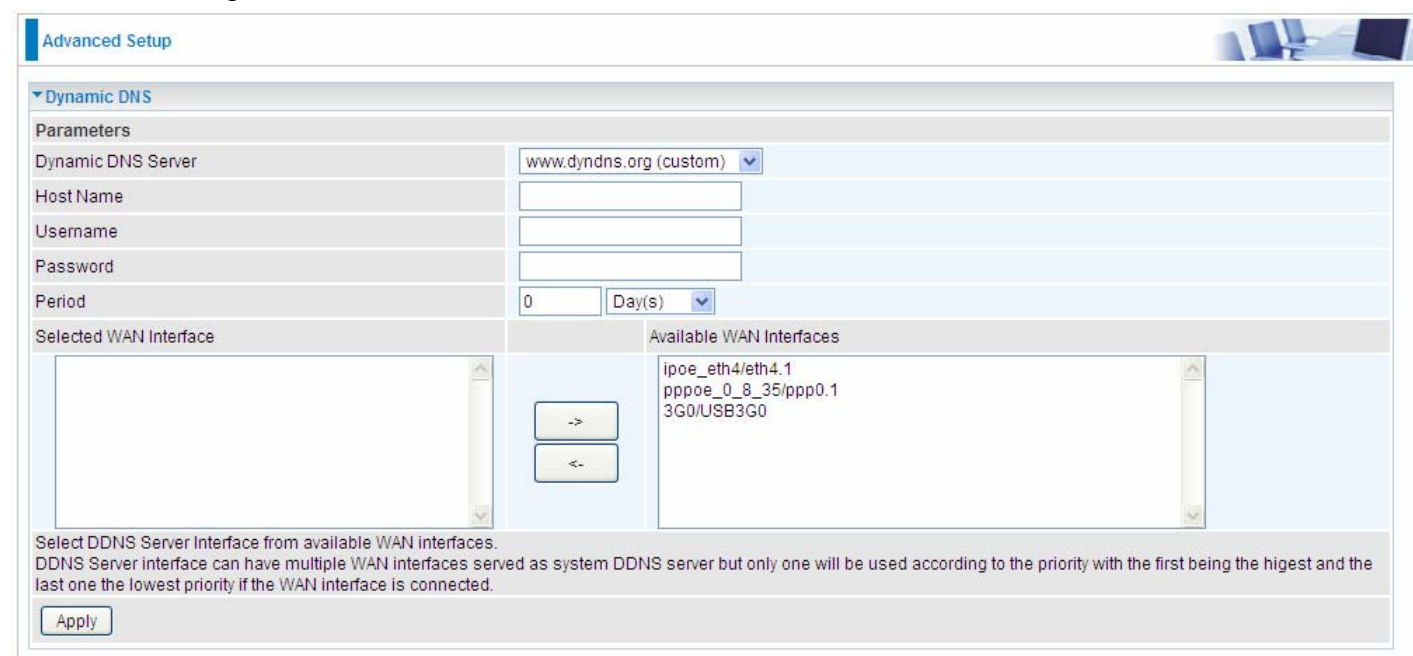
Dynamic DNS

Parameters

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

Add Remove

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



Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server:

Host Name:

Username:

Password:

Period:  Day(s)

Selected WAN Interface:

Available WAN Interfaces:

- ipoe\_eth4/eth4.1
- pppoe\_0\_8\_35/ppp0.1
- 3G0/USB3G0

Select DDNS Server interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

Apply

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.

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

**Period:** Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

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

## 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\_8\_35 with DDNS: [www.hometest.com](http://www.hometest.com) using username/password test/test

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest.com
Username	test
Password	••••
Period	25 Day(s)

Selected WAN Interface	Available WAN Interfaces
pppoe_0_8_35/ppp0.1	ipoe_eth4/eth4.1 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

Apply

Advanced Setup

Dynamic DNS

Parameters

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

Add Remove

2. ipoe\_eth4 with DDNS: [www.hometest1.com](http://www.hometest1.com) using username/password test/test.

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest1.com
Username	test
Password	••••
Period	25 Day(s)

Selected WAN Interface: ipoe\_eth4/eth4.1

Available WAN Interfaces: pppoe\_0\_8\_35/ppp0.1, 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

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	eth4.1	<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.

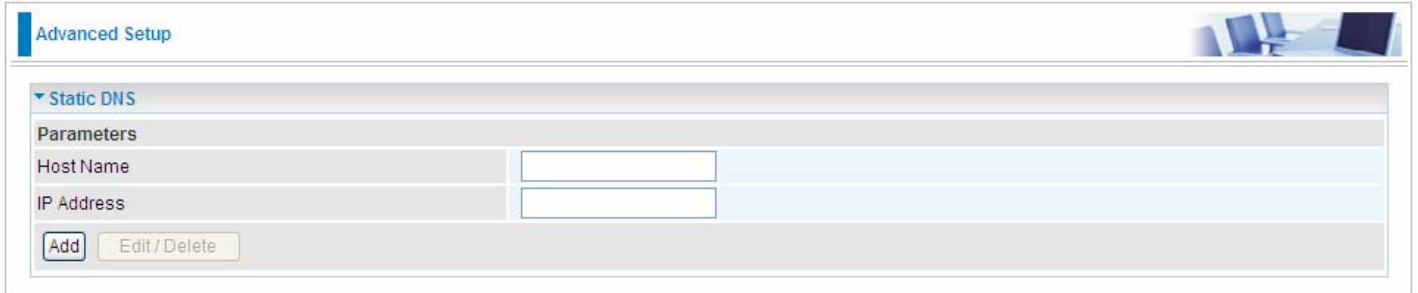
**Host name of the Broadband Router:** Enter the host name of the router. Default is home.gateway.

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

## Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



The screenshot shows a web interface for 'Advanced Setup'. Under the 'Static DNS' section, there is a 'Parameters' table with two rows: 'Host Name' and 'IP Address', each with an empty text input field. Below the table are two buttons: 'Add' and 'Edit/Delete'.

Parameters	
Host Name	<input type="text"/>
IP Address	<input type="text"/>

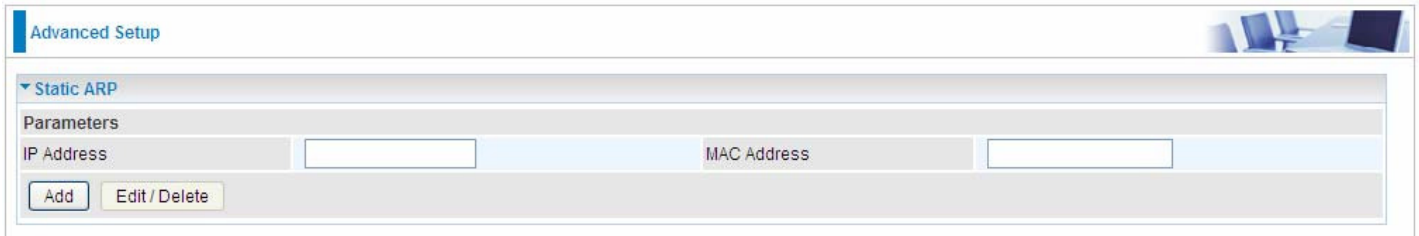
**Host Name:** Type the domain name (host name) for the specific IP .

**IP Address:** Type the IP address bound to the set host name above.

Click **Add** to save your settings.

## 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, there is a "Parameters" section with 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.

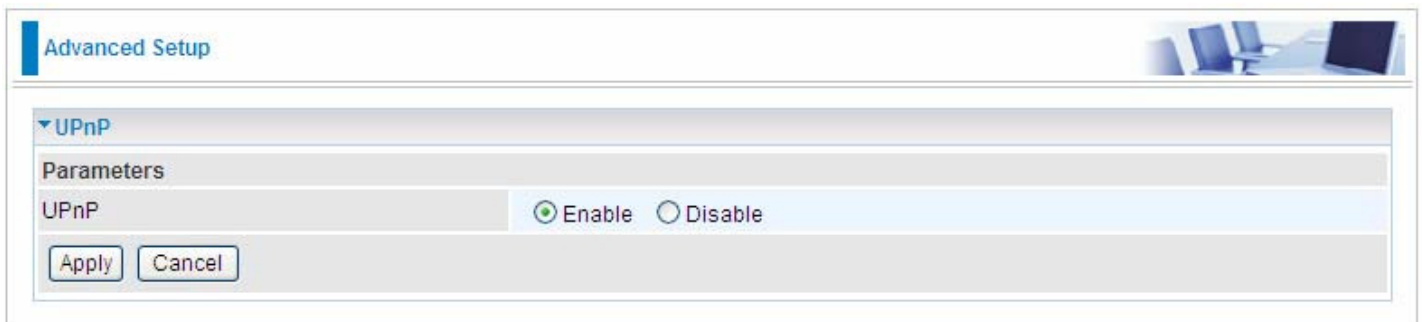
Click **Add** to confirm the settings.



## 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:

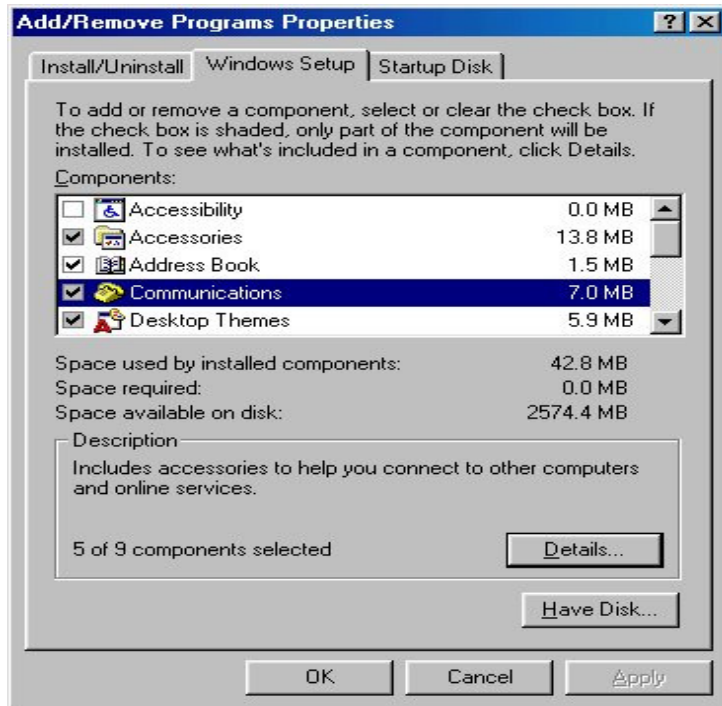
- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

## Installing UPnP in Windows Example

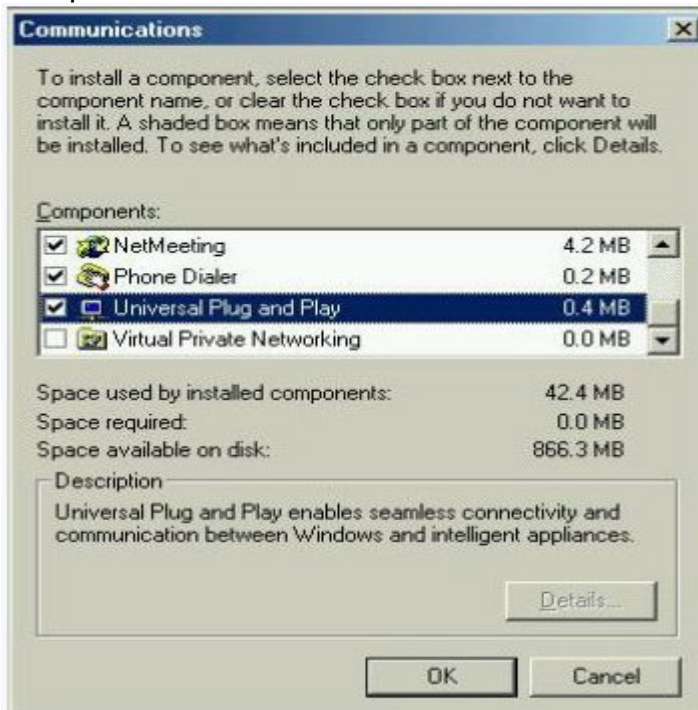
Follow the steps below to install the UPnP in Windows Me.

**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.

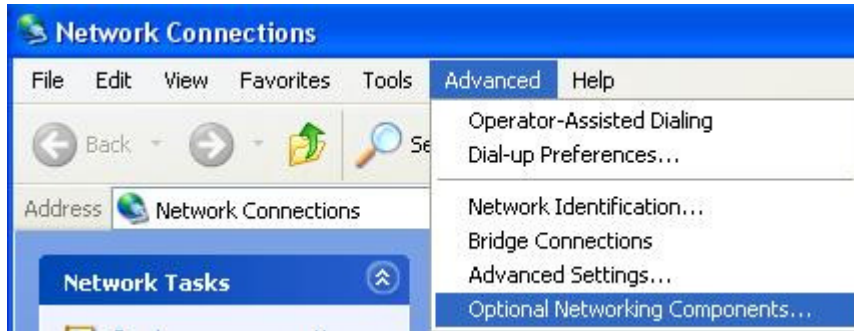
**Step 5:** Restart the computer when prompted.

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

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

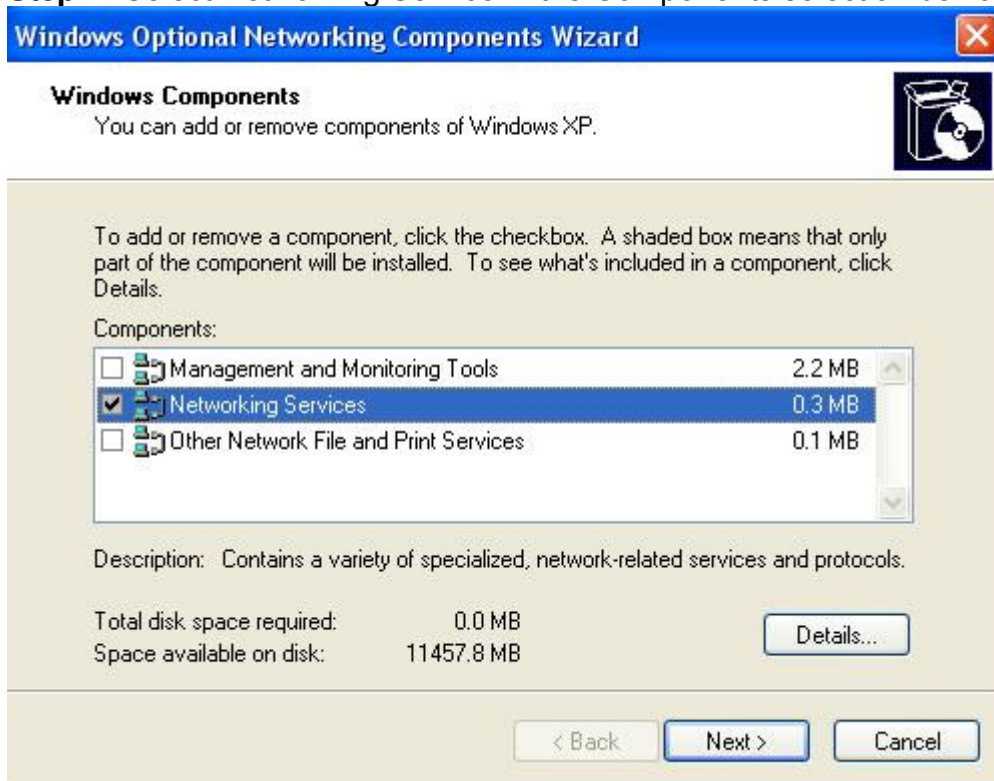
**Step 2:** Double-click Network Connections.

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



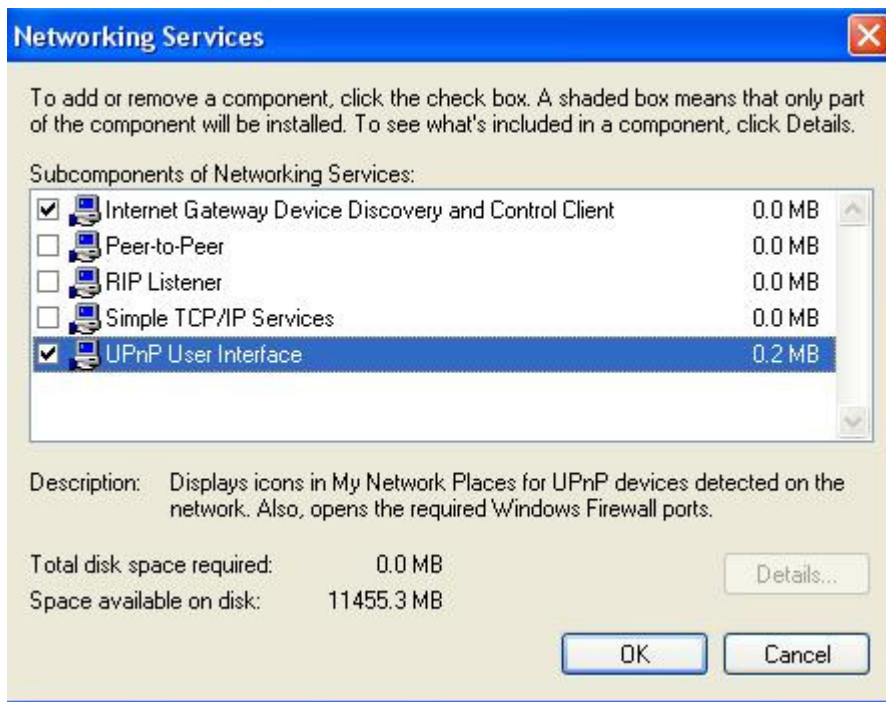
The Windows Optional Networking Components Wizard window displays.

**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.

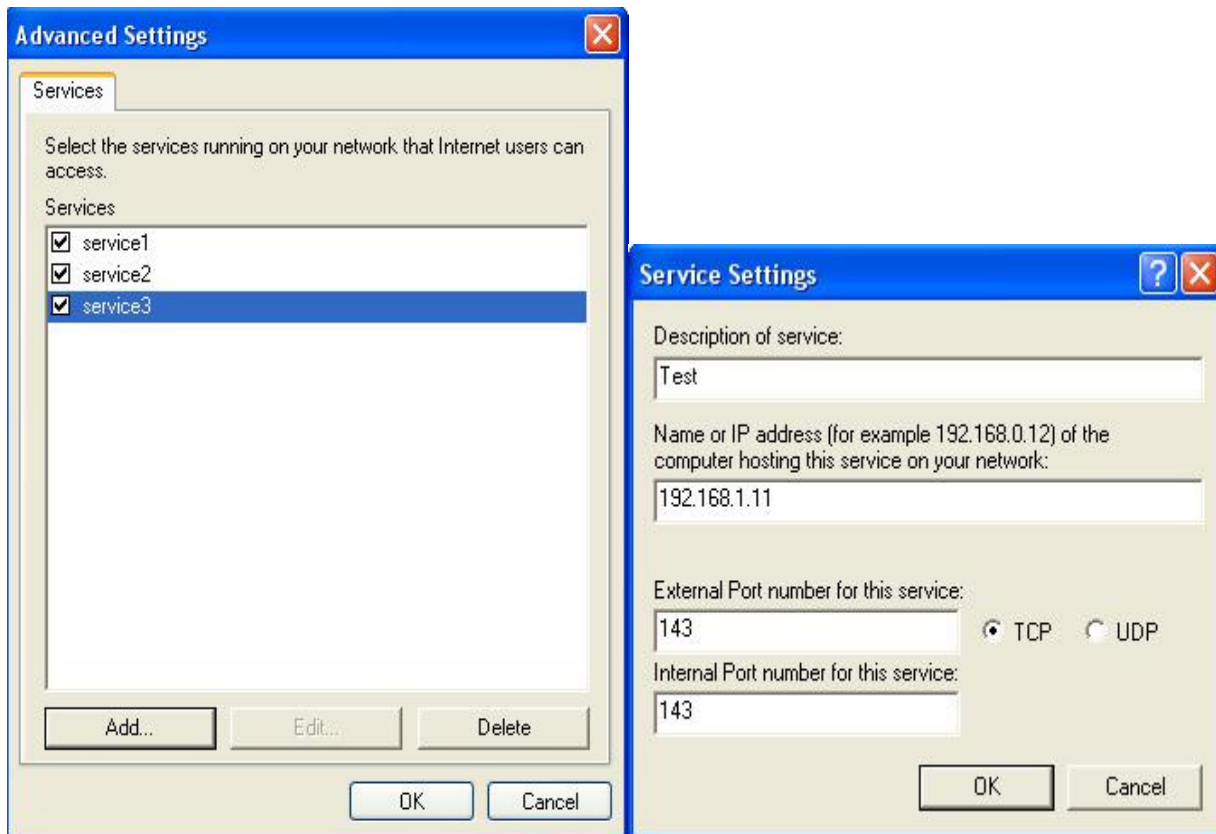
**Step 2:** Right-click the icon and select Properties.



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

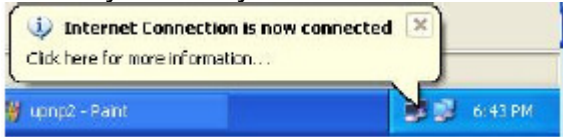


**Step 4:** You may edit or delete the port mappings or click Add to manually add port mappings.

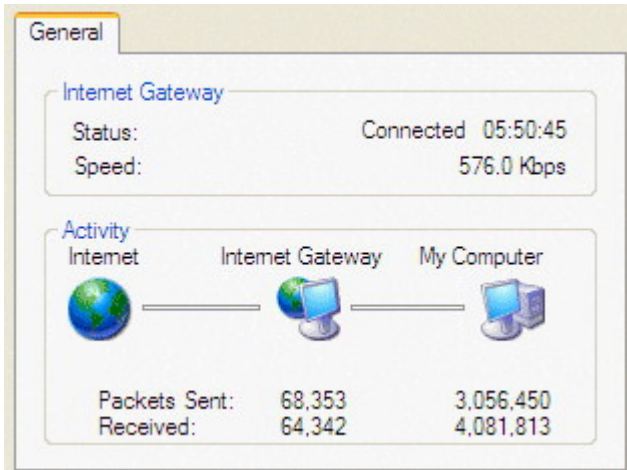


**Step 5:** Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



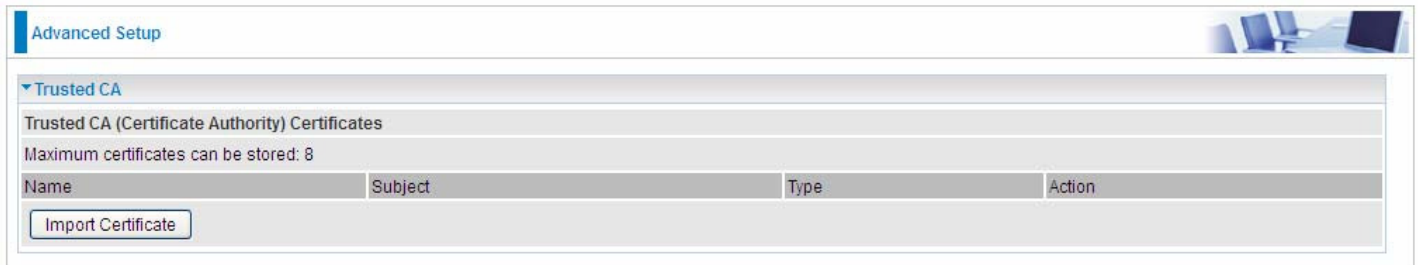
**Step 6:** Double-click on the icon to display your current Internet connection status.



# Certificate

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

## Trusted CA



**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-----  
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQ  
GEwJD  
TjEXMBUGA1UEChMOQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc  
NMjAw  
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV  
yYXRp  
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN  
ZuTJD  
rSwXGjaexPnBie5zNjc70SPQYgVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/  
Uu9be  
pUJBenxvYRgTImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73  
/se+H  
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu  
gOaQ3  
MDUxCzAJBgNVBAYTAKNOMRcwFQYDVQQKEw5DRkNBIFBvbG1jeSBBDQITENMA  
GA1UE  
AxMEQ1JMMTALBgNVHQ8EBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS  
FaAqX  
k1NC0tAwHQYDVRO0BBYEFMMnxjZoyCdlJIEvkadLJjMC5RrpMAwGA1UdEwQ
```

Apply



Click Apply to confirm your settings.

**Advanced Setup**

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 8

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	
<b>Multicast</b>	
Multicast Precedence	Disable [lower value, higher priority]
<b>IGMP</b>	
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
<b>MLD</b>	
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
[Apply] [Cancel]	

## IGMP

**Multicast Precedence:** It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

**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.

## 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.

# Management

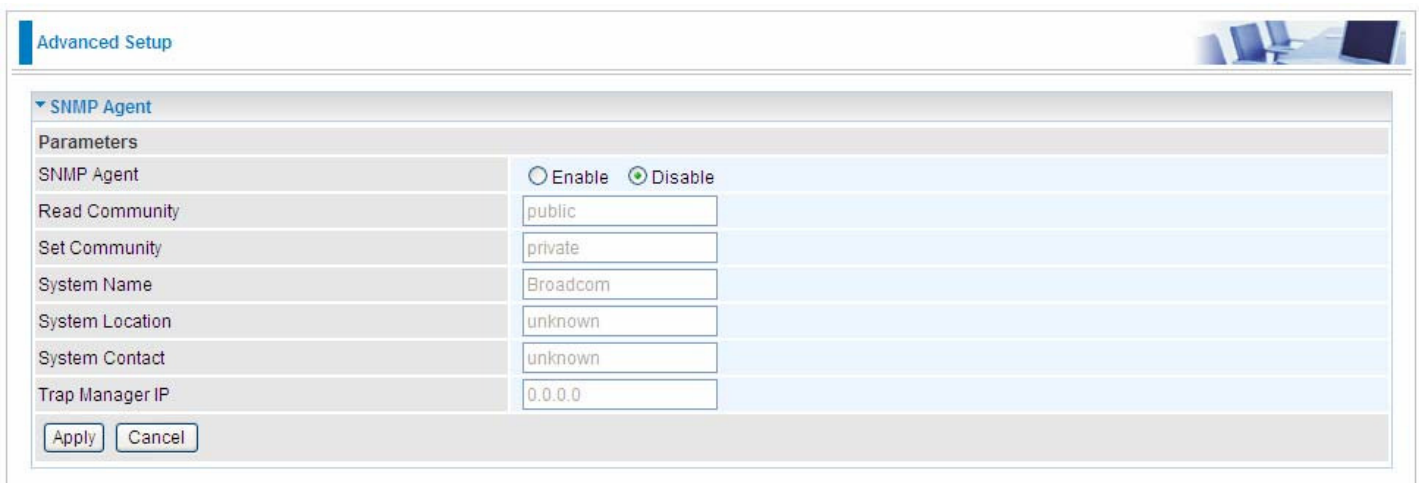
## SNMP Agent

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. 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 provide 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.

Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform Interval	870 [1-2147483647]
ACS URL	http://cpe.bectechnologi
ACS User Name	testcpe
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	conexant
Connection Request Password	.....
Connection Request URL	http://[2001:b011:7009:0805:25ca:c0d7:5b7a:1267]:30005/

Apply 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.

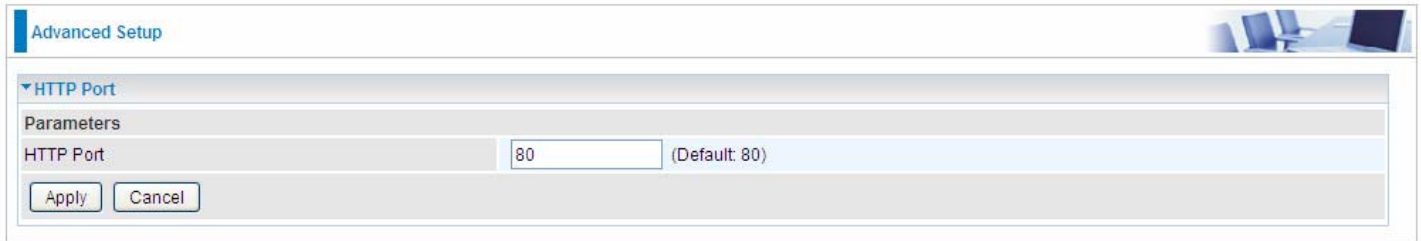
**Connection Request URL:** Automatically match the URL for ACS server to make connection request.

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

Click **Apply** to apply your settings.

## HTTP Port

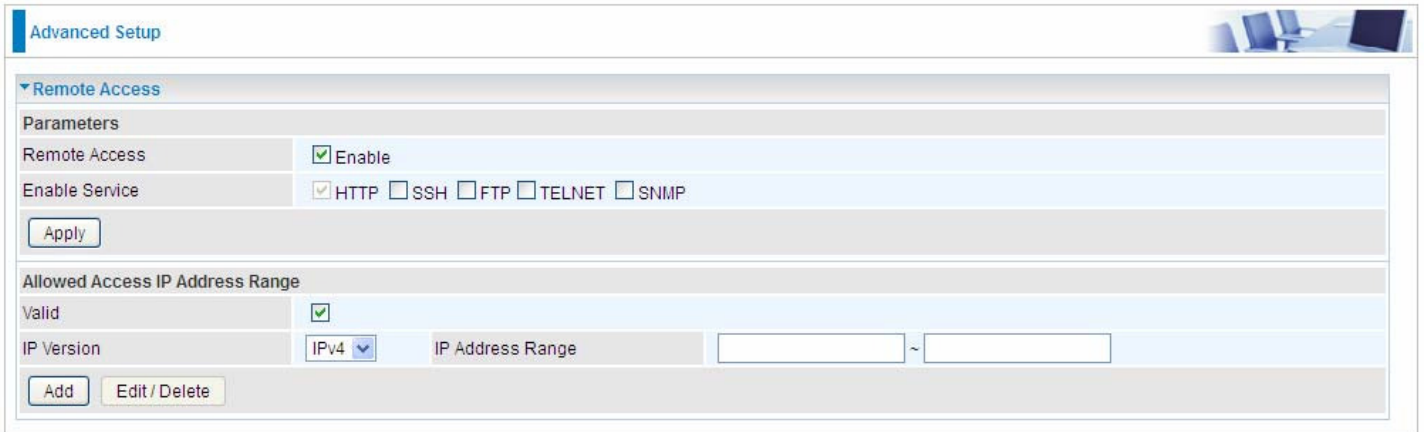
The device equips user to change the embedded web server accessing port. Default is 80.



The screenshot shows a web interface for 'Advanced Setup'. At the top right, there is a small image of a computer workstation. Below the title bar, a section titled 'HTTP Port' is expanded. Underneath, a 'Parameters' section contains a single configuration item: 'HTTP Port' with a text input field containing the value '80' and a label '(Default: 80)'. At the bottom of this section, there are two buttons: 'Apply' and 'Cancel'.

## 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, 'Remote Access' is checked 'Enable'. Under 'Enable Service', 'HTTP' is checked, while 'SSH', 'FTP', 'TELNET', and 'SNMP' are unchecked. An 'Apply' button is present. Below, the 'Allowed Access IP Address Range' section has 'Valid' checked. The 'IP Version' is set to 'IPv4', and there are two empty input fields for the IP address range, separated by a tilde (~). 'Add' and 'Edit / Delete' buttons are at the bottom.

**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.

**Enable Service:** Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"**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**.

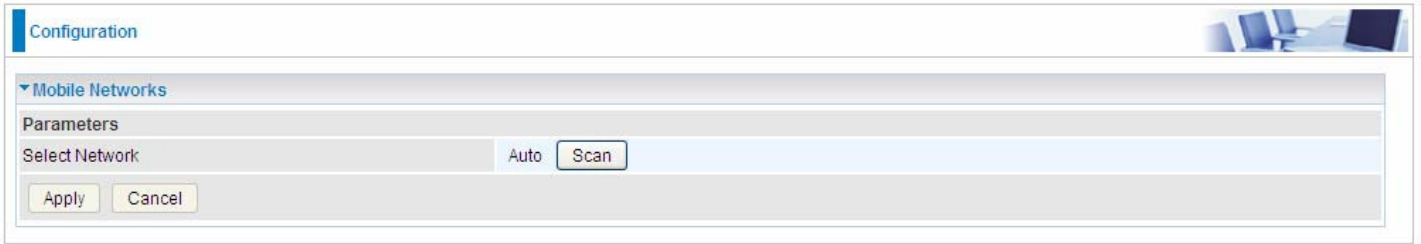
### 2. Remote Access enabled:

- 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.



## Mobile Networks

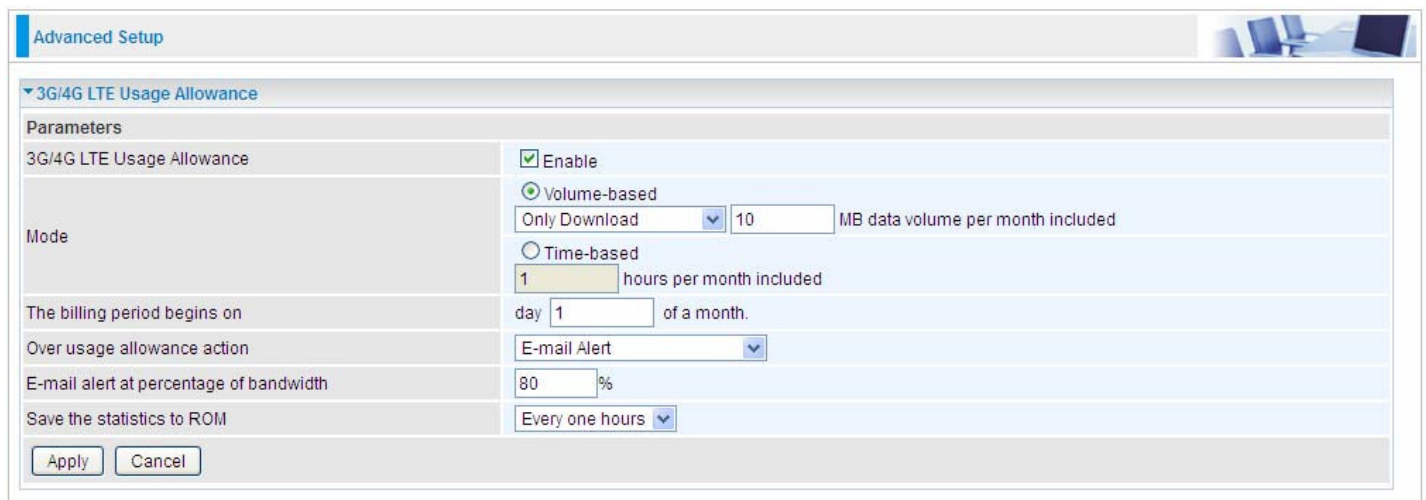
User can press **Scan** to discover available 3G/4G LTE mobile network.



The screenshot shows a web-based configuration interface. At the top left, there is a blue header bar with the word "Configuration" in white. To the right of the header is a small image of a computer workstation. Below the header, there is a section titled "Mobile Networks" with a downward-pointing arrow. Underneath this section is a "Parameters" area. The "Select Network" field is currently set to "Auto". To the right of this field are two buttons: "Auto" and "Scan". The "Scan" button is highlighted with a light blue background. At the bottom of the parameters area, there are two buttons: "Apply" and "Cancel".

## 3G/4G LTE Usage Allowance

3G/4G LTE usage allowance is designated for users to monitor and control the 3G flow usage. 8920NXL-600's 3G/4G LTE usage allowance offers exact control settings for each SIM card.



The screenshot shows the 'Advanced Setup' window for '3G/4G LTE Usage Allowance'. The 'Parameters' section includes:

- 3G/4G LTE Usage Allowance:**  Enable
- Mode:**  Volume-based (Only Download) 10 MB data volume per month included;  Time-based 1 hours per month included
- The billing period begins on:** day 1 of a month.
- Over usage allowance action:** E-mail Alert
- E-mail alert at percentage of bandwidth:** 80%
- Save the statistics to ROM:** Every one hours

Buttons: Apply, Cancel

**3G/LTE Usage Allowance:** Enable to monitor 3G/4G LTE usage.

**Mode:** include Volume-based and Time-based control.

- ① **Volume-based** include “only Download”, “only Upload” and “Download and Upload” to limit the flow.
- ① **Time-based** control the flow by providing specific hours per month.

**The billing period begins on:** The beginning day of billing each month.

**Over usage allowance action:** What to do when the flow is over usage allowance, the available methods are “E-mail Alert”, “Email Alert and Disconnect” and “Disconnect”.


**E-mail alert at percentage of bandwidth:** When the used bandwidth exceeds the set proportion, the system will send email to alert.

**Save the statistics to ROM:** To save the statistics to ROM system.

## 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

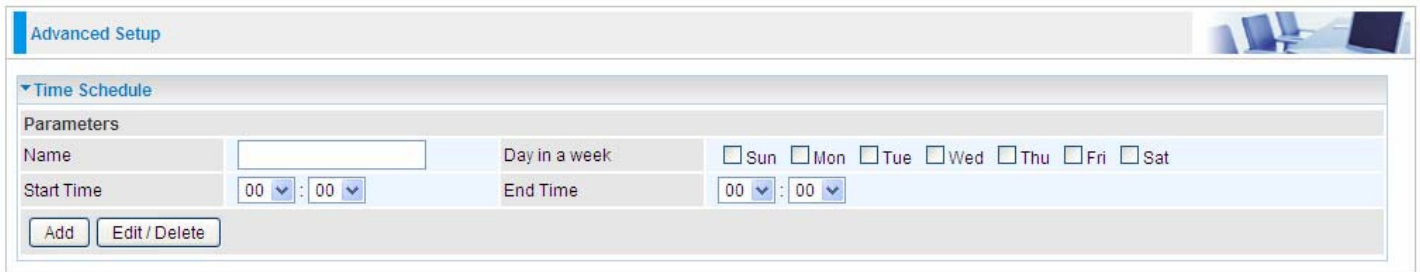
Parameters

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
Energy Efficient Ethernet	<input checked="" type="checkbox"/> Enable	Status	Enabled
Ethernet Auto Power Down and Sleep	<input checked="" type="checkbox"/> Enable	Status	Enabled Number of ethernet interfaces in: Powered up: 1 Powered down: 4
Adaptive Voltage Scaling	<input checked="" type="checkbox"/> Enable	Status	Enabled

## 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 Time](#) for details. Your router time should synchronize with NTP server.



Advanced Setup

Time Schedule

Parameters

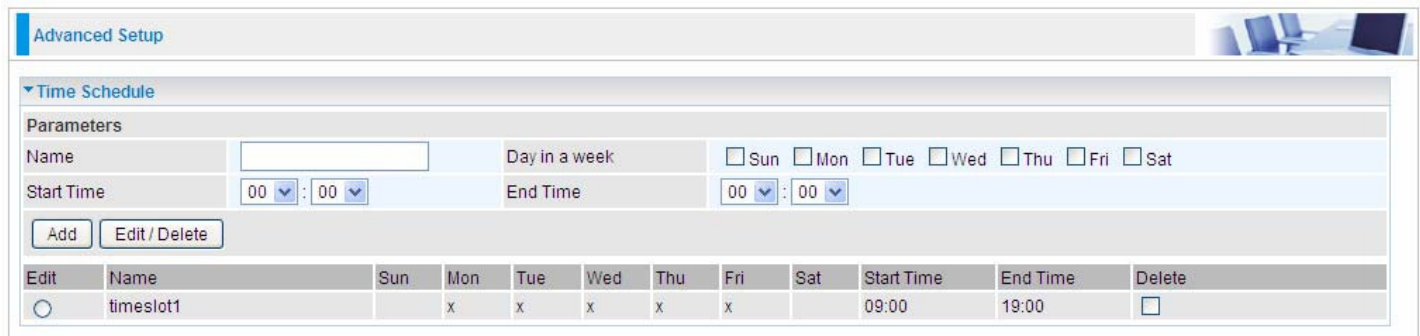
Name:

Day in a week:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Start Time: 00 : 00

End Time: 00 : 00

For example, user can add a timeslot named "timeslot1" features a period of 9:00-19:00 on every weekday.



Advanced Setup

Time Schedule

Parameters

Name:

Day in a week:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

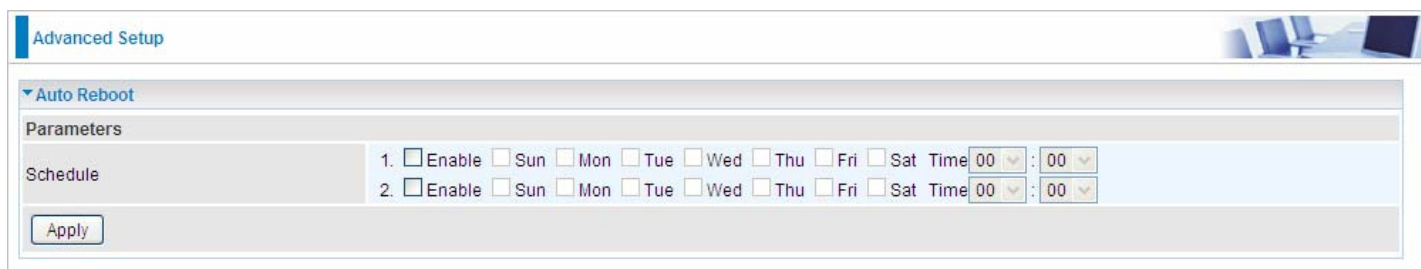
Start Time: 00 : 00

End Time: 00 : 00

Edit	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Delete
<input type="radio"/>	timeslot1		x	x	x	x	x		09:00	19:00	<input type="checkbox"/>

## Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.



Advanced Setup

Auto Reboot

Parameters

Schedule

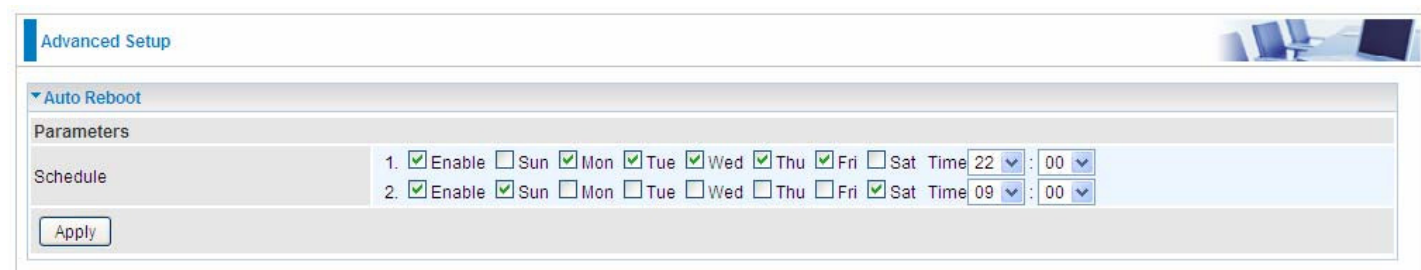
1.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 00 : 00

2.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 00 : 00

Apply

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:



Advanced Setup

Auto Reboot

Parameters

Schedule

1.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 22 : 00

2.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 09 : 00

Apply

# Diagnostics

## Diagnostics Tools

BiPAC 8920NXL-600 offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.

The screenshot shows the 'Advanced Setup' interface for the BiPAC 8920NXL-600. Under the 'Diagnostics Tools' section, there are two main test configurations:

- Ping Test:** Includes a 'Destination Host' text field, a 'Source Address' section with a selected 'Interface' radio button and an 'IP Address' radio button, and a 'Ping Test' button.
- Trace route Test:** Includes a 'Destination Host' text field, a 'Source Address' section with a selected 'Interface' radio button and an 'IP Address' radio button, a 'Max TTL value' field set to 16 (range [2-30]), a 'Wait time' field set to 3 seconds (range [2-999]), and a 'Trace route Test' button.

**Ping Test:** to verify the connectivity between source and destination.

**Destination Host:** Enter the destination host (IP, domain name) to be checked for connectivity.

**Source Address:** Select or set the source address to test the connectivity from the source to the destination.

**Ping Test:** Press this button to proceed ping test.

**Trace route Test:** to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

**Destination Host:** Set the destination host (IP, domain name) to be traced.

**Source Address:** Select or set the source address to trace the route from the source to the destination.

**Max TTL value:** Set the max Time to live (TTL) value.

**Wait time:** Set waiting time for each response in seconds.

## Example: Ping www.google.com

**Advanced Setup**

**Diagnostics Tools**

**Ping Test**

Destination Host:

Source Address:  Interface   IP Address

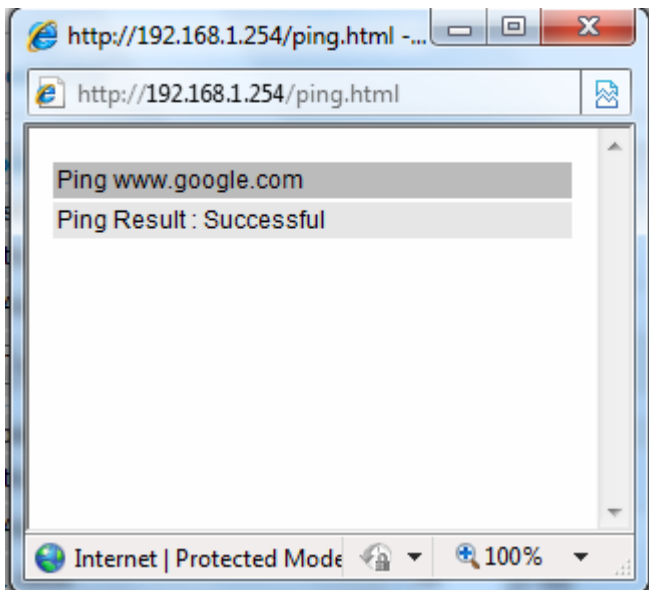
**Trace route Test**

Destination Host:

Source Address:  Interface   IP Address

Max TTL value:  [2-30]

Wait time:  seconds [2-999]



## Example: "trace" www.google.com

**Advanced Setup**

**▼ Diagnostics Tools**

**Ping Test**

Destination Host:

Source Address:  Interface   IP Address

**Trace route Test**

Destination Host:

Source Address:  Interface   IP Address

Max TTL value:  [2-30]

Wait time:  seconds [2-999]

http://192.168.1.254/tracert.html - Windows Intern...

http://192.168.1.254/tracert.html

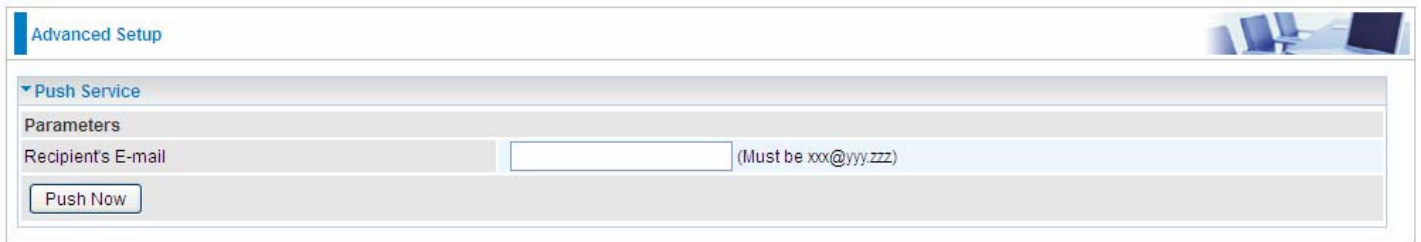
Trace www.google.com

No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	**
13	173.194.72.147	79.753 ms



## Push Service

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




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

**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.

Advanced Setup 

▼ Test the connection to your local network --- pppoe\_0\_0\_33

Test LAN Connection ( P1 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P2 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P3 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P4 )	PASS	<a href="#">Help</a>
Test LAN Connection ( P5/EWAN )	FAIL	<a href="#">Help</a>
Test your Wireless Connection	FAIL	<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	FAIL	<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 PTM connection; Push service

Advanced Setup

### 802.1ag Connectivity Fault Management

Parameters

This diagnostic is only used for xDSL PTM mode.

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: 0 [0-4095]

xDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM)

Find Maintenance End Points (MEPs)

MEP Name	IP Address	MAC Address	Level

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.

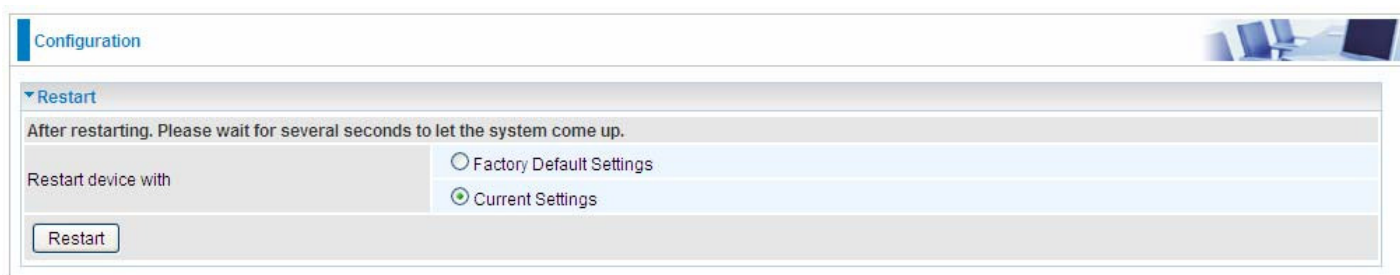
**Maintenance End Point:** Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

**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 Loop-back to successive MIPs can determine the location of a fault. Sending a high volume of Loop-back Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loop-back to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

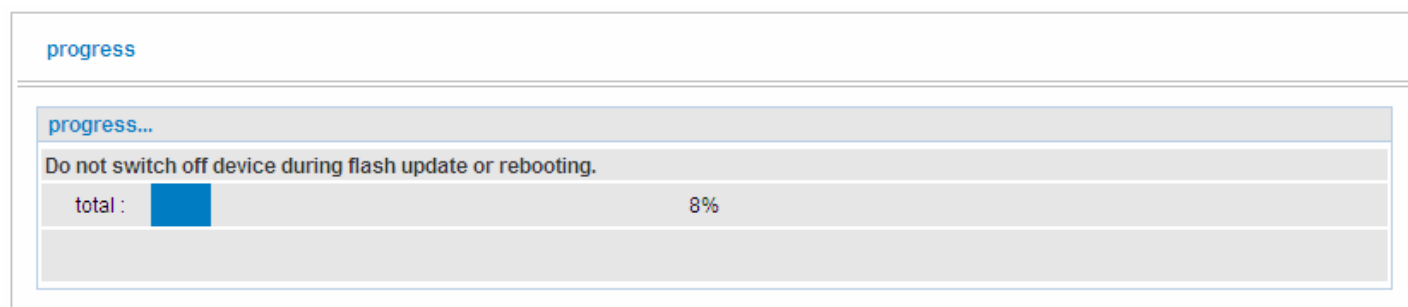
# Restart

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 XP, Windows Vista, Windows 7 and Windows 8 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.