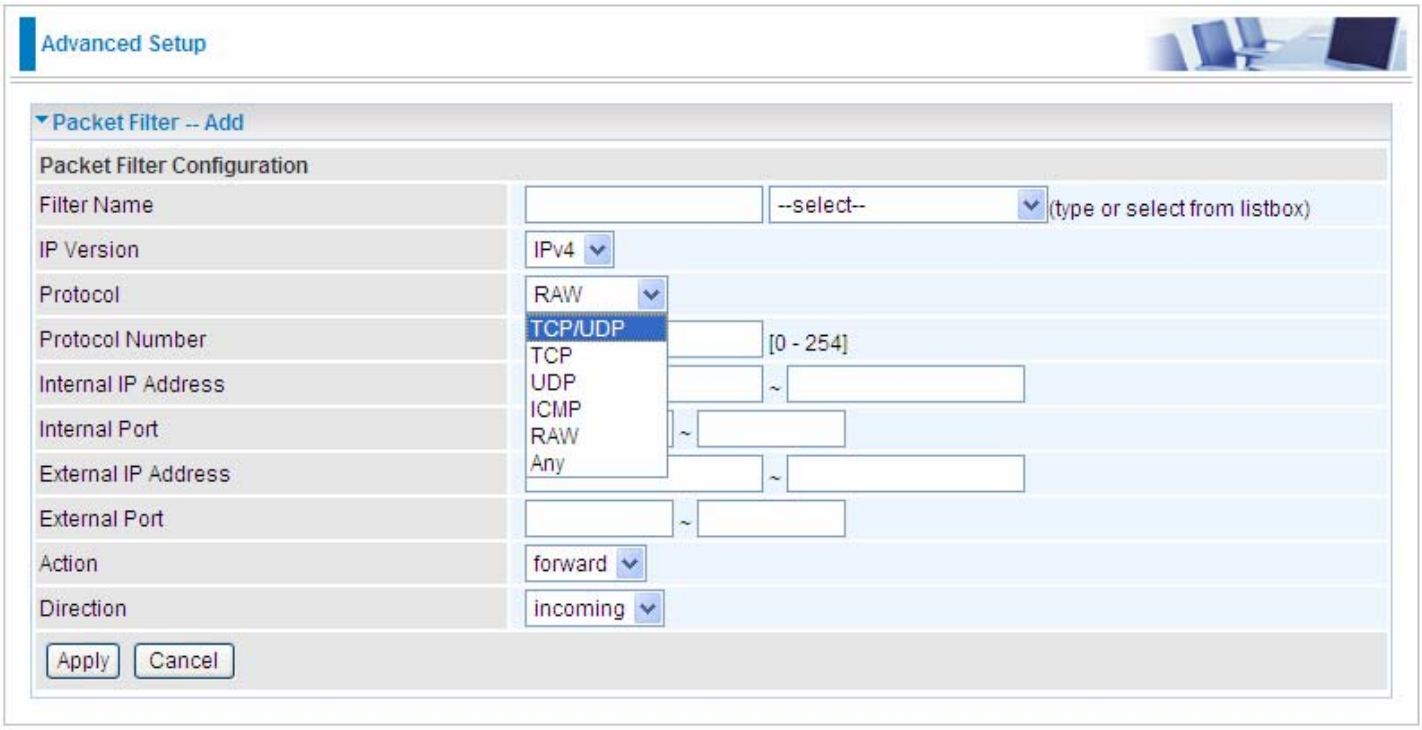
Security

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Above is the listing table. Click **Add** to add new configurations.



Filter name: a user-defined filter name or you can select from the drop-down menu the application, and leave the automatically generated name as the Filter name.

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

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/from particular IP address (es). Input the range you want to filter out. If you leave empty, it means any IP address.

Protocol: Specify the packet type (TCP/UDP，TCP, UDP, ICMP, RAW and Any) that the rule applies

to. Only when **RAW** is selected, then you can type the protocol number (0-254) to identify the protocol that you want the filter applies to. When **Any** is selected, it means the filter will applies to any protocol.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **1 ~ 65535.** It is recommended that this option be configured by an advanced user.

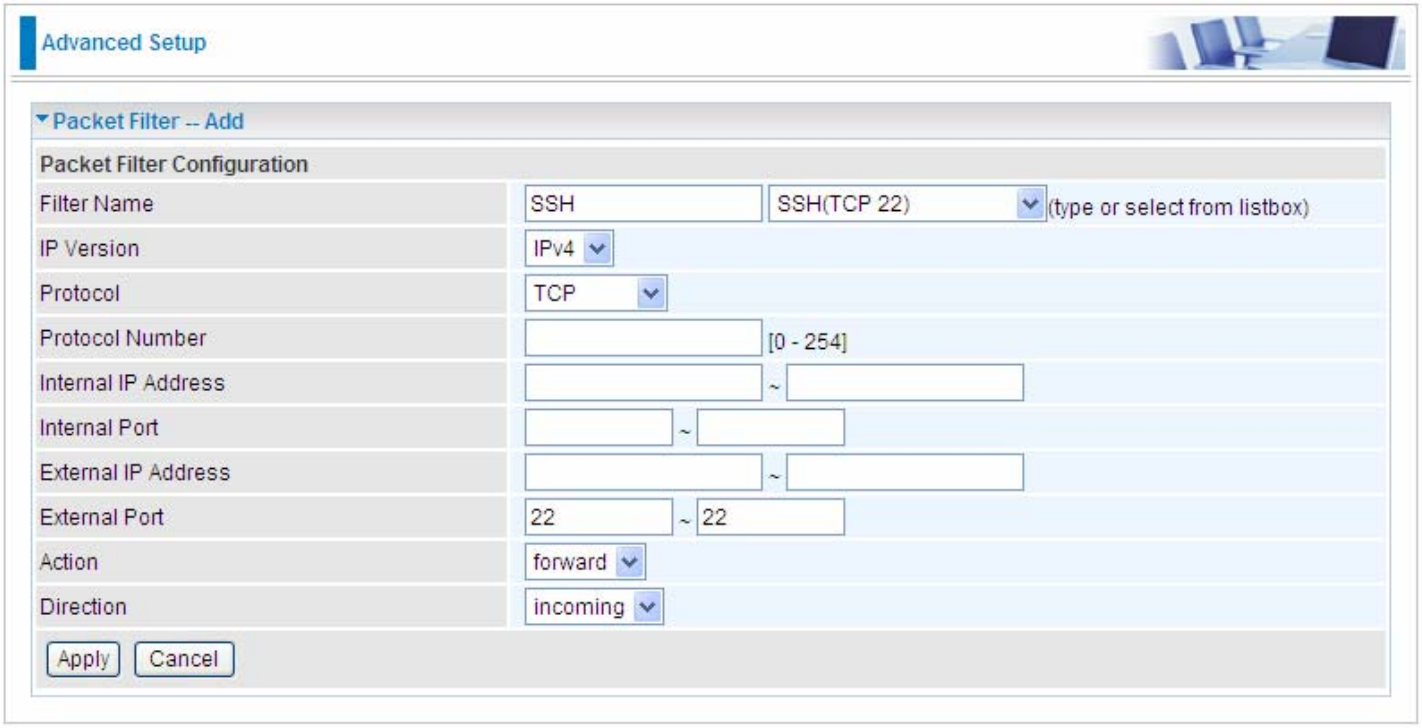
External Port: This is the Port or Port Range that defines the application. Default is set from range **1 ~ 65535.**

Action: If a packet matches this filter rule, **forward (allows the packets to pass)** or **drop (disallow the packets to pass)** this packet.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

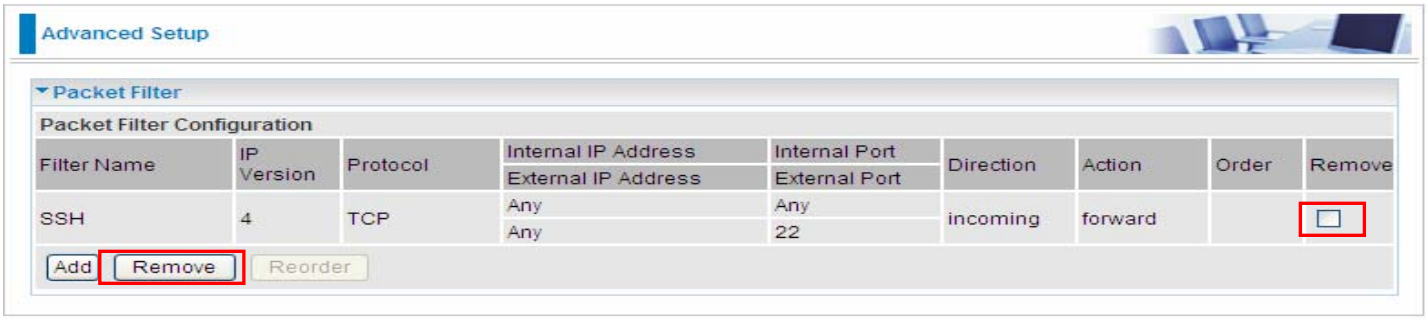
Set up

Select the application you want to filter, input the information or leave it as default according to yourself.



Press **Apply** to confirm and the item will be listed in the following table.

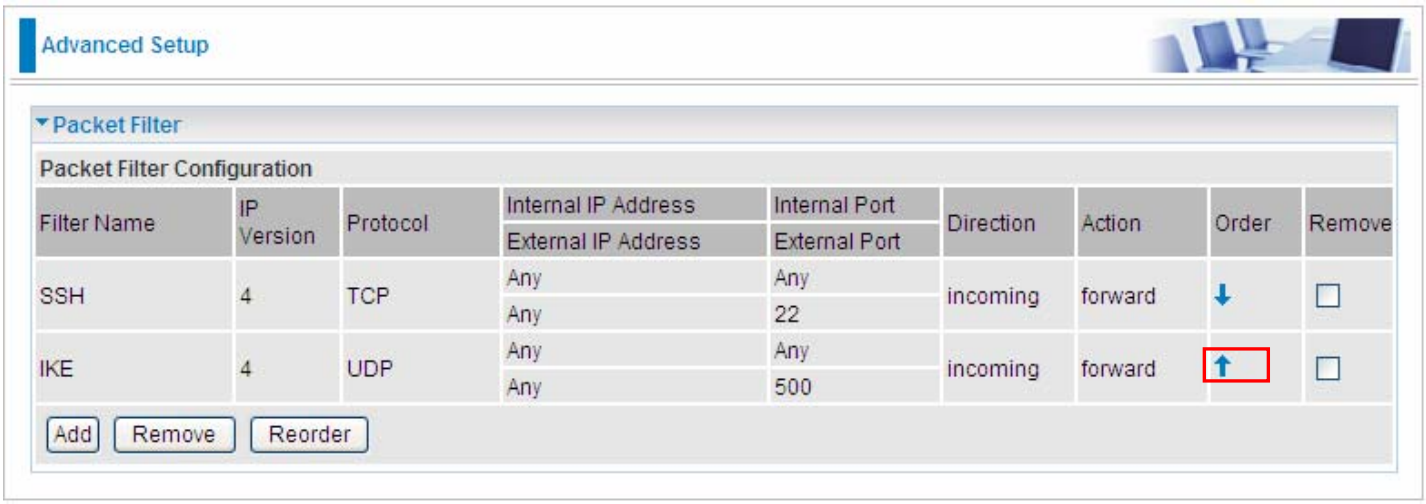
Remove



Check the checkbox, press **Remove**, the item will be removed.

Reorder

When there are more than one Filter application, you can reorder them to the priority you want. The former is prior to the latter one.



Click ↑ or ↓ to change the priority of the filter, then press Reorder to confirm.

Time Restriction

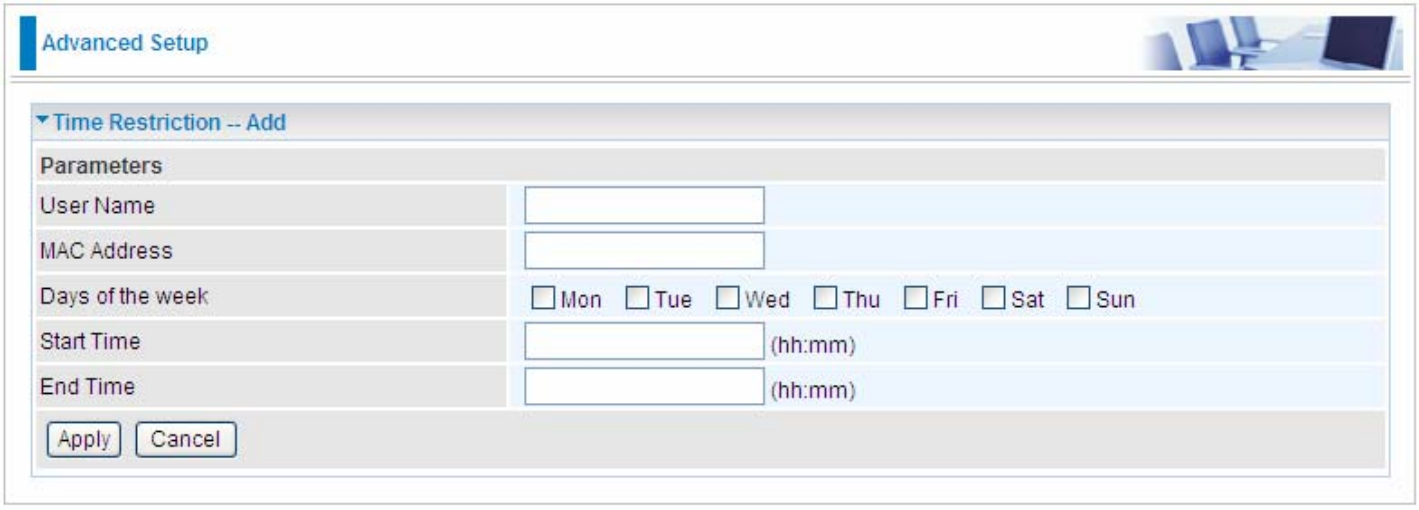
A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

Action:

- **Disable:** disable the **Time Restriction** function.
- **Allow:** allow the members in the following table to access the router.
- **Block:** block the members listed in the following table from accessing the router.

Note: here users should add the rules first, then select the wanted action.

Click **Add** to add the rules.



Username: user-defined name.

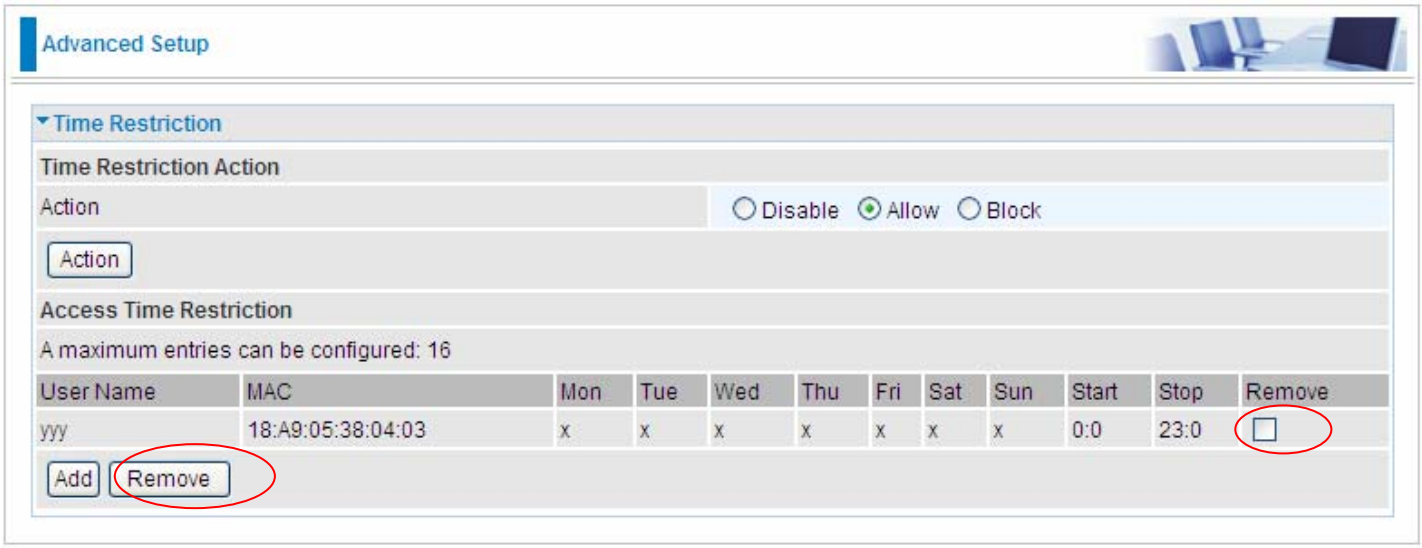
MAC Address: enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Days of the week: select the days of a week this rule takes efforts.

Start Time: enter the start time of each day in hh:mm format. Leaving it empty means 00:00.

End Time: enter the end time of each day in hh:mm format. Leaving it empty means 23:59.

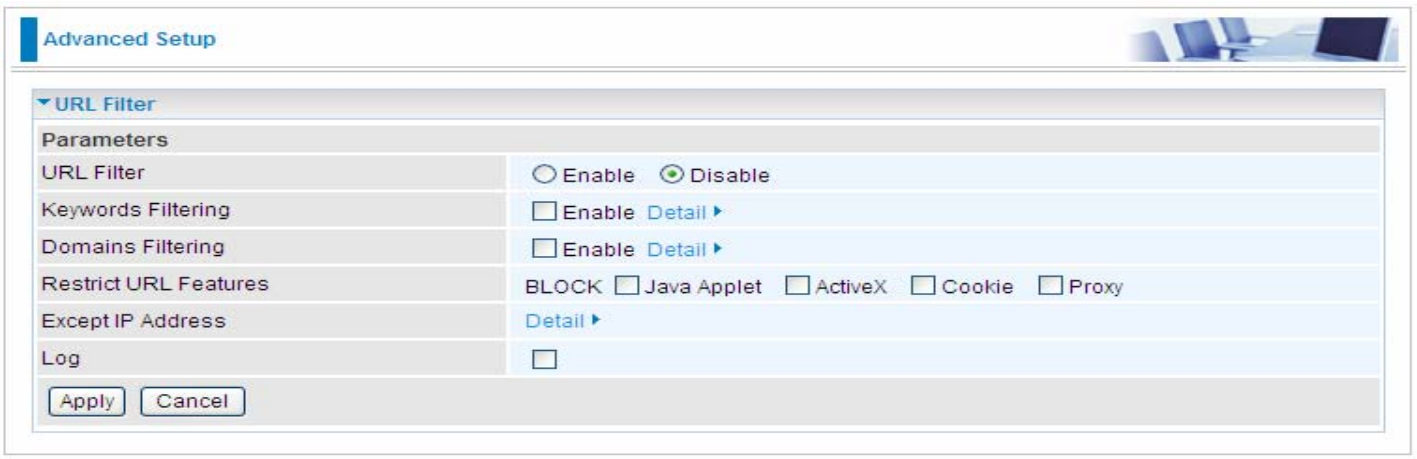
Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.



If you needn't this rule, you can check the box, press Remove, it will be OK.

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



URL Filtering: select to enable or disable URL Filtering feature.

Keywords Filtering: Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g.to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy.

Keywords Filtering

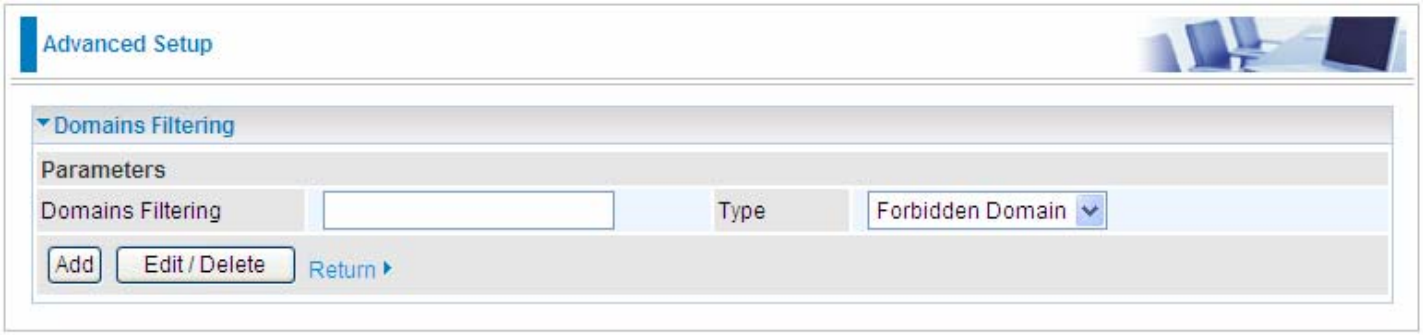
Click Detail ▸ to add the keywords.

Enter the Keyword, for example image, then click **Add.**

You can add other keyword like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domain Filtering

Click Detail to add Domains.



Domains Filtering: enter the domain you want this filter applies to.

Type: select the action this filter deals with the Domain.

- **Forbidden Domain:** the domain is the forbidden to access.
- **Trusted Domain:** the domain is trusted and allowed access.

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to **Keywords filtering.**

Exception IP Address

Click Detail to add the IP Addresses.

Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords filtering.**

At the URL Filter page, press **Apply** to confirm your settings.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.

Quality of Service: Check to activate this function and the following field will be available.

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Select Default DSCP Mark: Select the default DSCP mark from the list-box. Differentiated Services Code Point (DSCP) is the first 6 bits in the ToS byte. DSCP Mark allows users to classify the traffic of the application to be executed according to the DSCP value. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Note: Before configuring Queue config and QoS Classification section, you must enable QoS function, for the reason that the queues' activation will depend on this, the classification will also depend on this.

The corresponding IP precedence and DSCP mapping table is listed below.

IP Precedence and DSCP Mapping Table

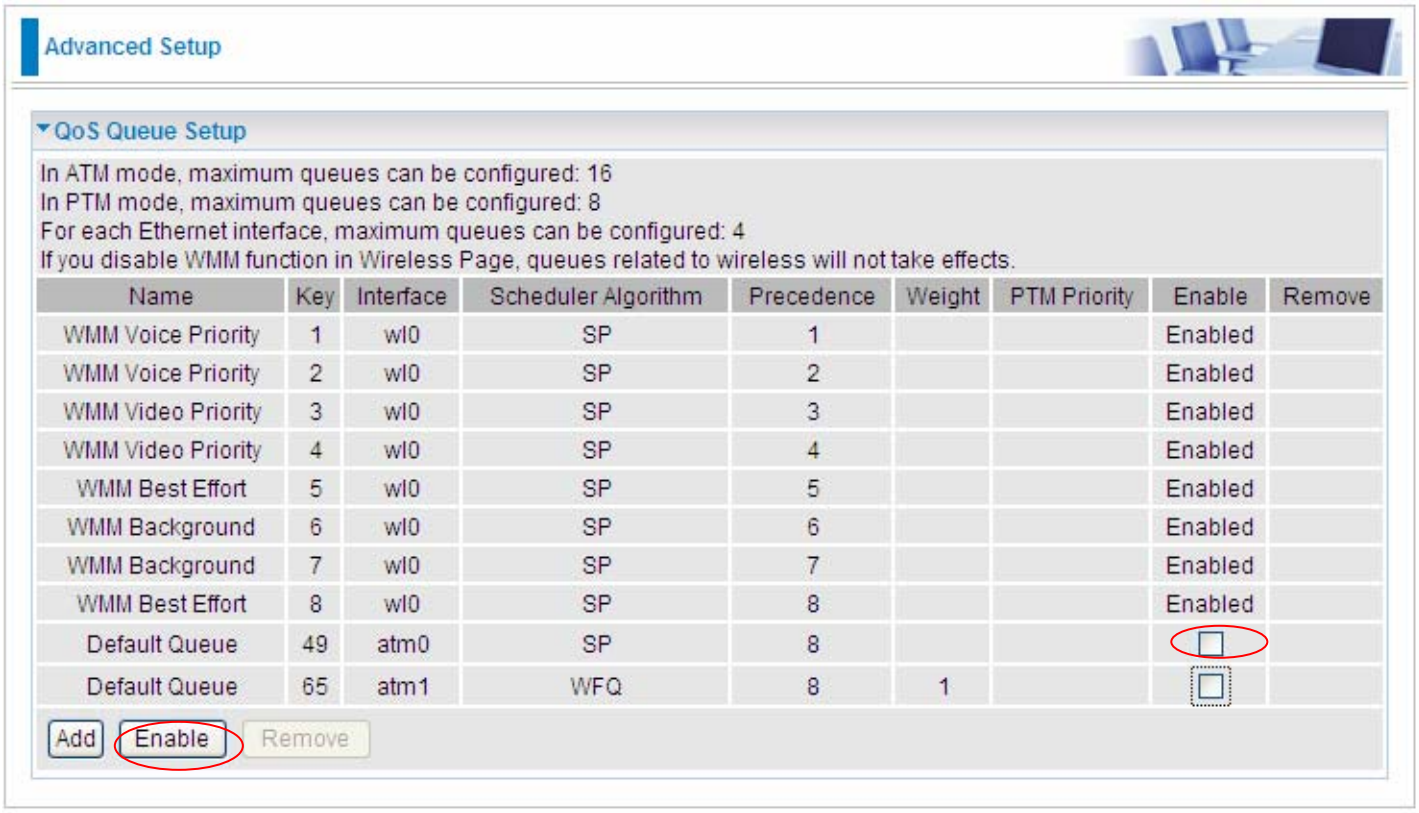
Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP indicates three kinds of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four kinds of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Click **Apply** to confirm the settings.

Queue Config

Queue is a technology of managing congestion providing precautions with the packets storing and scheduling. Queue Config allows you to configure a QoS queue entry and assign it to a specific network interface. Each queue entry set here will be used by the classfier to place ingress packets appropriately.



Note: the interface set in the **WAN**> **WAN Interface** will be list as Default Queue here, and the parameters listed above can be configured there. For detail, please turn to **WAN** > **WAN Interface** section for help. You can also add other queues to the ATM and PTM interfaces despite of the default queue.

And Wireless Service queue will be enabled by default if you enable wireless. Also if you enable virtual APs, the corresponding WMM service queues will be enabled as well.

Name: the queue name.

Key: the item number.

Interface: the queue interface.

Scheduler Algorithm: the QoS Scheduler Algorithm, SP(Strict Priority) or WFQ(Weight Fair Queuing)

Precedence: the priority identification.

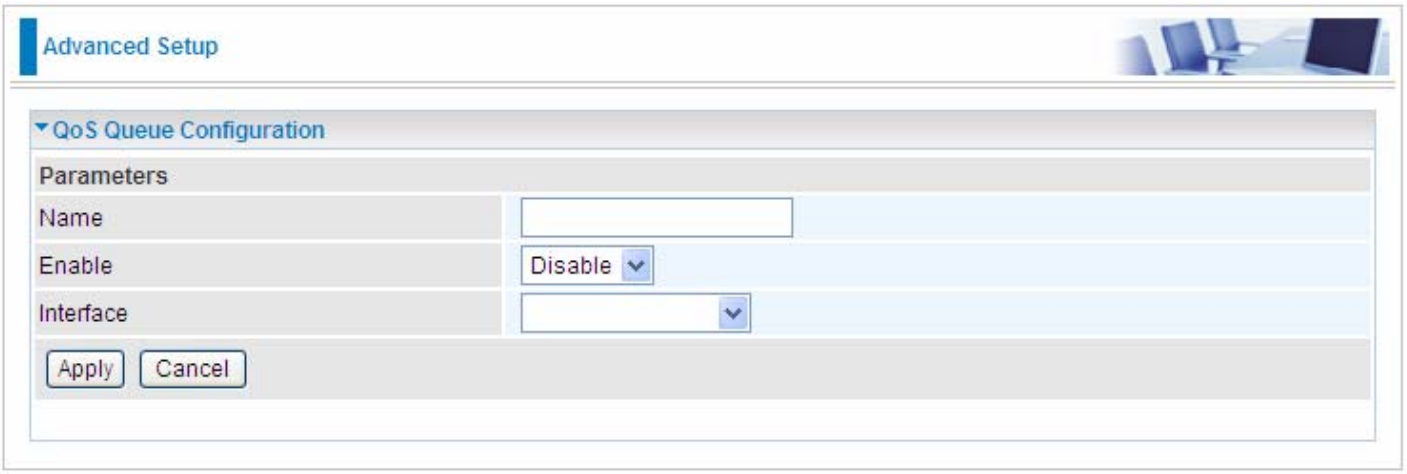
Weight: the weight value, 1-63. the highest is 63.

PTM Priority: the PTM priority, normal or high.

Enable: check the enable check-box, then press **Enable** to activate the queue. If you want to disable this queue, you can uncheck the corresponding check-box and press Enable, the queue will be disabled.

If the queue is enabled, you will see a tick, like  . Otherwise, the queue is disabled.

Click **Add** to create a queue.

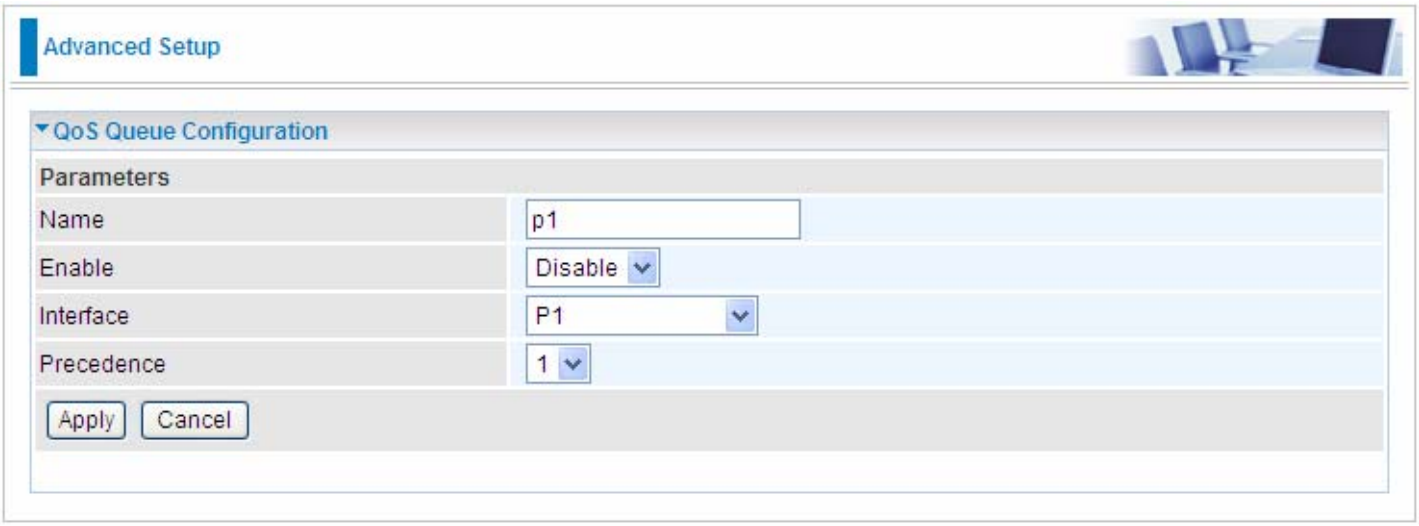


Name: Type the name of the queue.

Enable: Select whether to enable the queue.

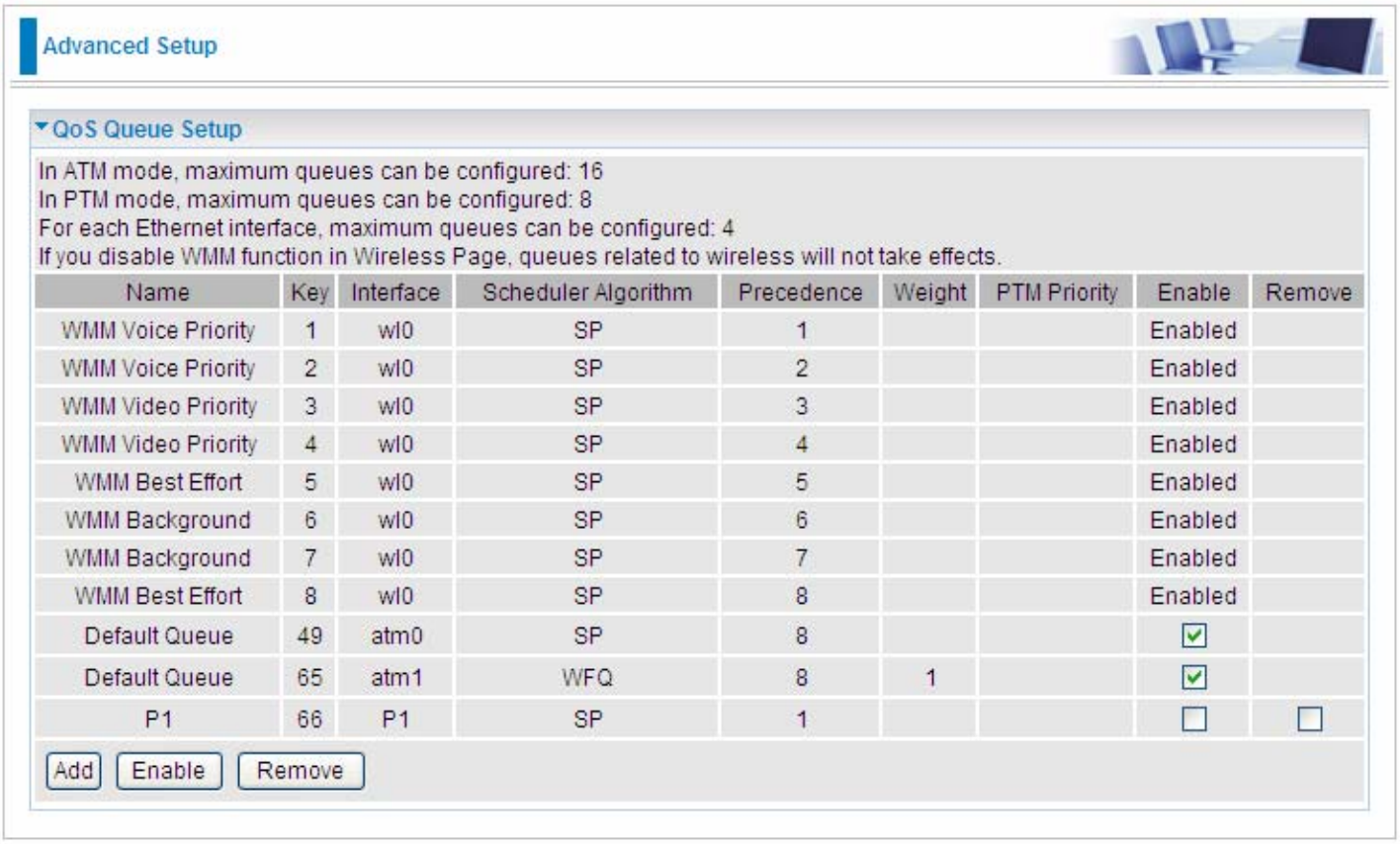
Interface: Select which interface this queue applies to.

Select interface, the following corresponding parameters will appear to let you configure, Enter the information, Click Apply to conform. Then the item will be listed in the table.



Precedence: the precedence of the queue, interface P1-P4, 4 levels from high to low are 1-4. ATM or PTM interfaces, 7 levels from high to low are 1-7, for the precedence of the default queue with the interface of SP Scheduler Algorithm is 8. Here if the interface is of WFQ Scheduler Algorithm, you should enter the weight of the queue.

Click **Apply** to save and the added queue will be listed as below.



Advanced Setup

QoS Queue Setup

In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Scheduler Algorithm	Precedence	Weight	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1			Enabled	
WMM Voice Priority	2	wl0	SP	2			Enabled	
WMM Video Priority	3	wl0	SP	3			Enabled	
WMM Video Priority	4	wl0	SP	4			Enabled	
WMM Best Effort	5	wl0	SP	5			Enabled	
WMM Background	6	wl0	SP	6			Enabled	
WMM Background	7	wl0	SP	7			Enabled	
WMM Best Effort	8	wl0	SP	8			Enabled	
Default Queue	49	atm0	SP	8			☑	
Default Queue	65	atm1	WFQ	8	1		☑	
P1	66	P1	SP	1			☐	☐

Add Enable Remove

Enable: check the enable check-box, then press **Enable** to activate the queue. If you want to disable this queue, you can uncheck the corresponding check-box and press Enable, the queue will be disabled.

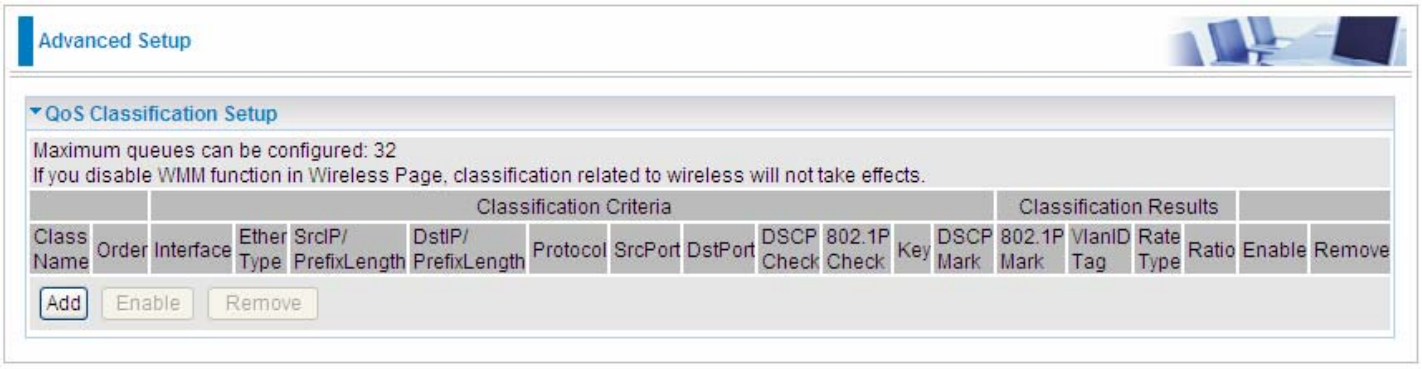
Remove: To delete the QoS rule from the table, check Remove checkbox then click **Remove button** to delete the selected item.

Note: only the queue added via the above mode can be directly removed here, the default queue can’t be removed here, if you want to remove them, remove the interface in **WAN** > **WAN Interface** section.

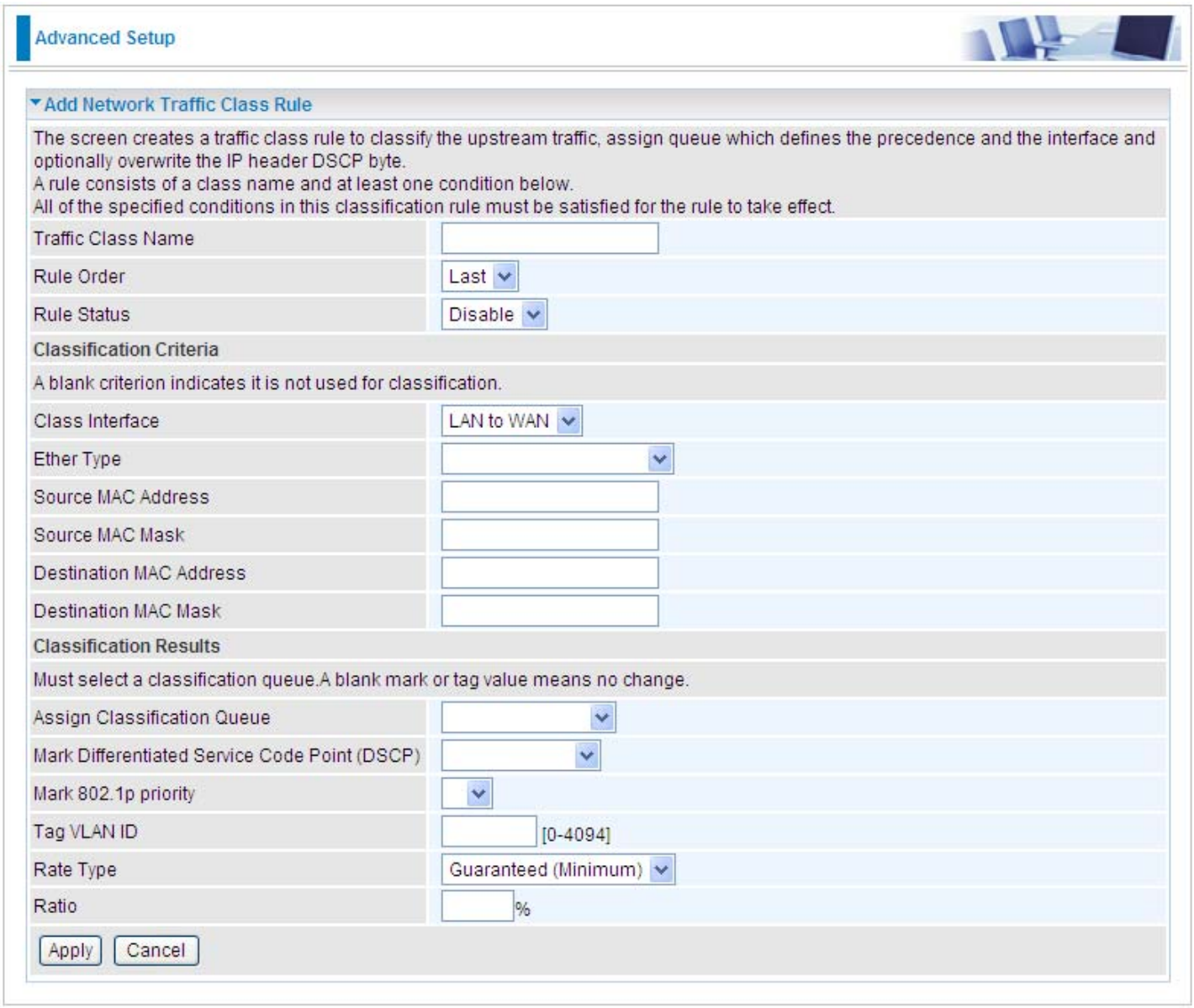
Note: In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

QoS Classification

This screen displays a packet QoS summary table and allows user to add or remove a QoS classification class. This is the main place to configure the classification, marking and queuing rules.



Click **Add** to add Network Traffic Class Rule.



The classification rule is a ‘AND’ mode, that is a rule takes effect only when all of the specified conditions must be satisfied.

Parameters

Traffic Class Name: Assign a name for this class to uniquely identify the others among multiple classes.

Rule Order: Select the priority for this class rule.

Rule Status: Select **Enable** to activate this class rule.

Specify Classification Criteria

The following parameters are to be classification rule. Enter or select appropriate parameters on the following fields. A blank criterion indicates it is not used for classification.

Class Interface: select the interface you want to be the one aspect of the classification criteria. Here ”LAN->WAN” and ”WAN->LAN” can be viewed as IP QoS, the others can be viewed as ported-based QoS, which means that control the QoS of certain port such. For example, if you select P1 port, then criteria applies to this port, that is ported-based QoS.

Entry Type: select the application type.

Source/destination MAC Address: enter the source and destination MAC address as the QoS Classification Criteria. The format should be xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Source/destination MAC Mask: MAC mask is similar to IP mask, and the format also should be xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. It is used to hide some information of the MAC address. ‘1’, means needed and ‘0’ means ignored. For example, MAC address e0:3b:4a:c2:ca:e2 and MAC mask ff:ff:ff:00:00:00, that is whatever MAC address while matches e0:3b:4a:XX:XX:XX, will be accepted.

Specify Classification Results

Enter or select appropriate parameters you want for the packets matched the above classification criteria in the following fields. You have to choose a classification queue. A blank mark or tag value means no change.

Assign Classification Queue: assign classification queue from the drop-down box. If you want to select the queue, you should make sure the specific queue is enabled in **Queue Config** section.

Mark Differentiated Service Code Point (DSCP): select the DSCP you want to be the new DSCP for the packets which matched the above classification criteria.

Mark 802.1p priority: it is a LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization. It is interoperable with IEEE 802.1Q. 802.1p has 8 kinds of priority.

Tag VLAN ID: enter the tag VLAN ID, 0-4094, used to determine the VLAN the frame belongs to.

Rate Type: You can choose Limited or Guaranteed.

Ratio: The rate percent in contrast to that on WAN interface.

Note: 802.1p/vlan tag feature be supported only when in bridge mode, DSL WAN interface.

Click Apply to confirm the settings and you will be returned to the QoS Classification page.

Enable: To disable the item, please uncheck Enable check box then click Enable button.

Remove: To delete the QoS class from the table, check Remove checkbox then click Remove button to delete the selected item.

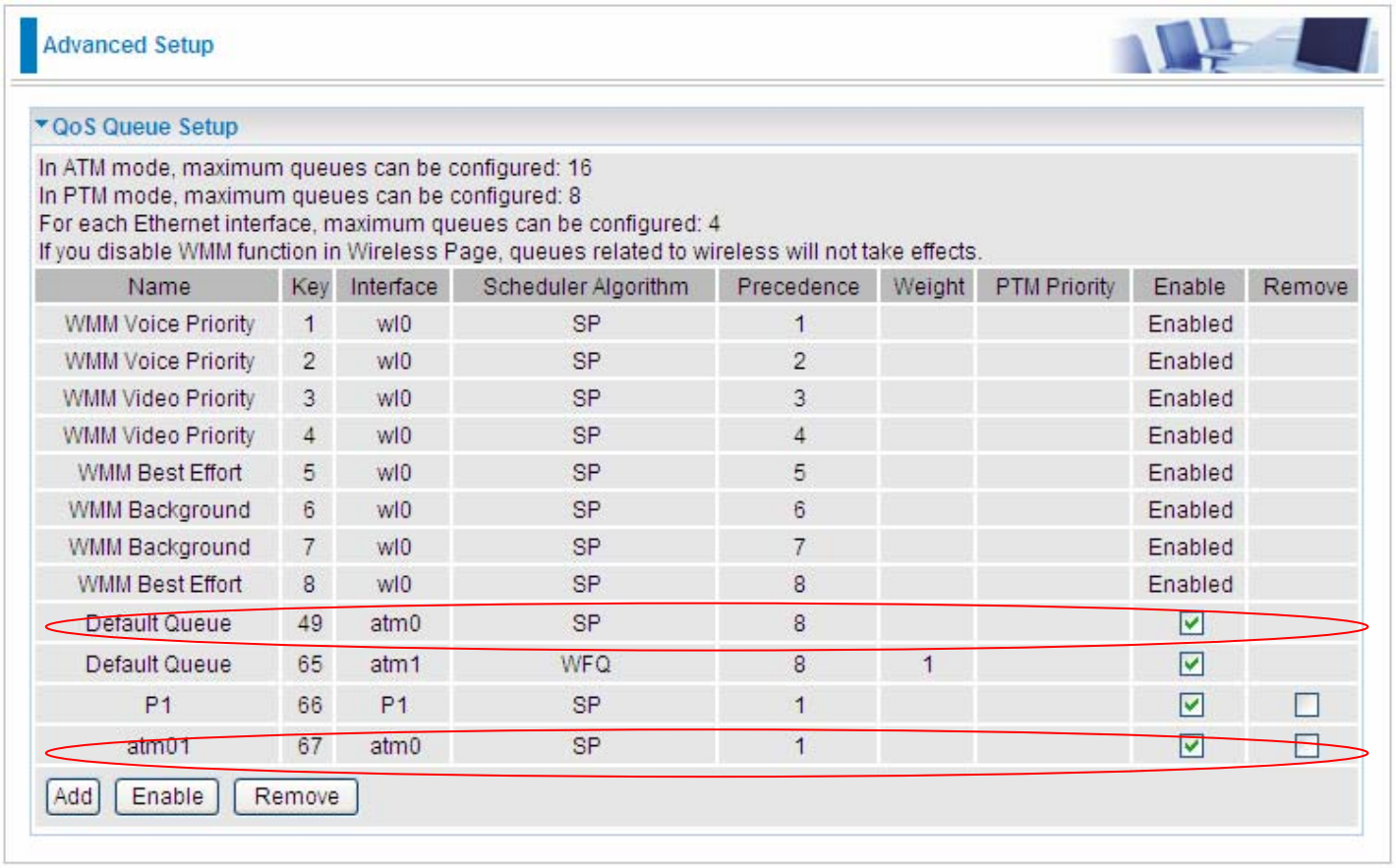
Set up a QoS Classification

IP QoS

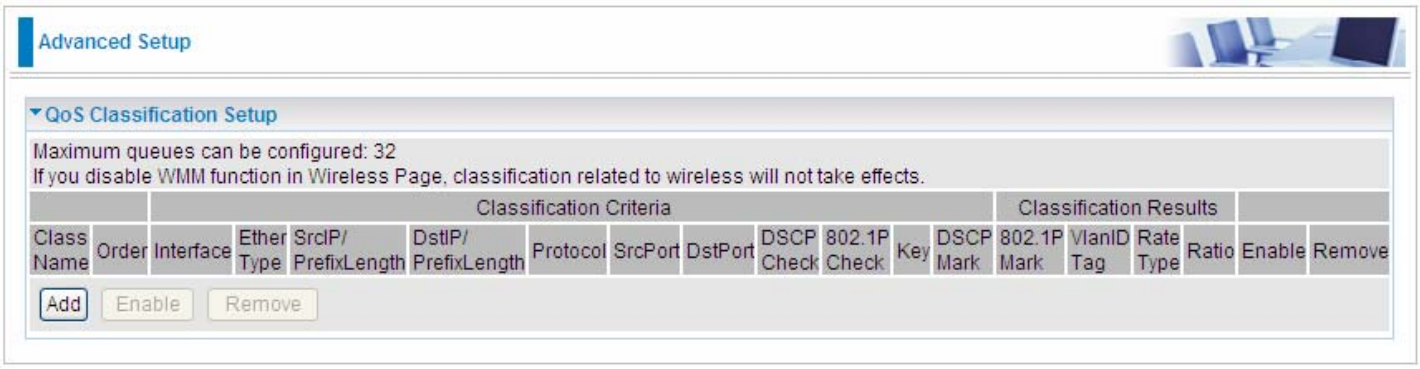
LAN to WAN IP QoS

1. It is a QoS controlling the traffic from LAN to WAN. So first make sure there is at least one WAN queue. If you have configured WAN interface and it will appeared as a default queue, you can also add other queues of the specific interface. See **Queue Config**.

Here we have a atm0 (WAN interface), the interface has a default queue and an added queue. Make sure to enable the queue.



2. In QoS Classification Setup page, Click **Add** to add a Qos Classification.



Then in the appeared Add Network Traffic Class Rule page, enter the information to set up a rule.

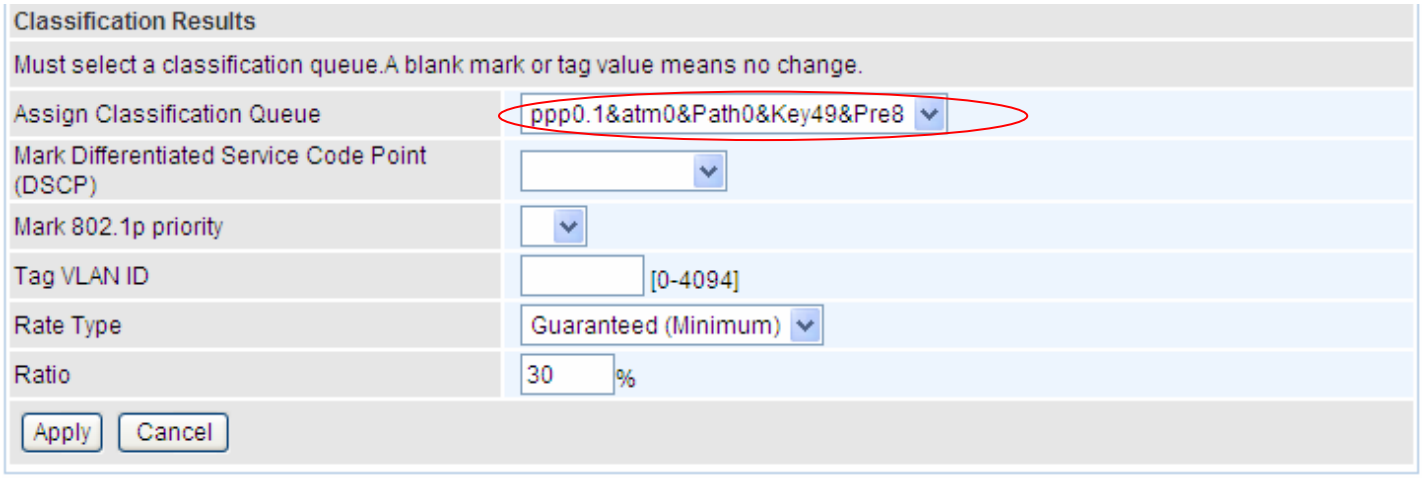
1) Specify the rule name, rule order, and rule status.

Traffic Class Name	upstream
Rule Order	Last
Rule Status	Disable

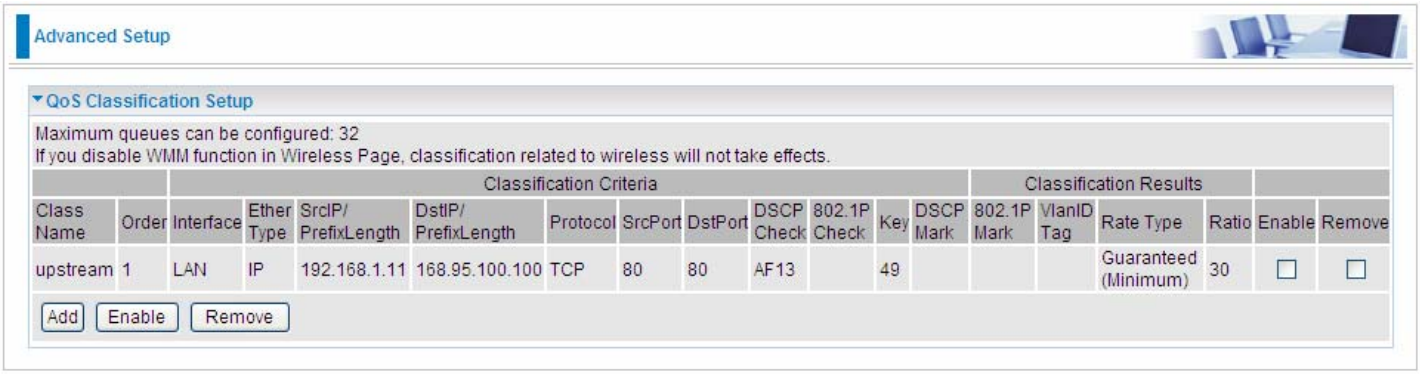
2) Specify the classification criteria. Here you can set every parameter to strictly control the specific traffic or you can set several parameters to let them be the key elements to control the traffic. A blank criterion indicates it is not used for classification.

Classification Criteria	
A blank criterion indicates it is not used for classification.	
Class Interface	LAN to WAN
Ether Type	IP (0x800)
Source MAC Address	18:A9:05:38:04:03
Source MAC Mask	ff:ff:ff:00:00:00
Destination MAC Address	e0:3b:4a:c2:ca:e2
Destination MAC Mask	ff:ff:ff:ff:ff:ff
IP Option	Source IP Address[/Mask]
Source IP Address	192.168.1.11
Destination IP Address[/Mask]	168.95.100.100
Differentiated Service Code Point (DSCP) Check	AF13(001110)
Protocol	TCP
UDP/TCP Source Port (port or port:port)	80
UDP/TCP Destination Port (port or port:port)	80

3) Specify the classification results. Here you must Assign Classification Queue. Whether the following parameters are needed is according to your needs. If you do not want to change the original information, please leave it empty. The queues listed here in the Assign Classification Queue are WAN interface queues set in Queue Config section. Select the needed queue. If you find none queues here, turn back to check whether you have configured a queue and enable it.



3. Click **Apply** to save your settings. The added rule will listed as below.



Enable: check the enable check-box, then press **Enable** to activate the rule. If you want to disable this rule, you can uncheck the corresponding check-box and press **Enable** button, the rule will be disabled.

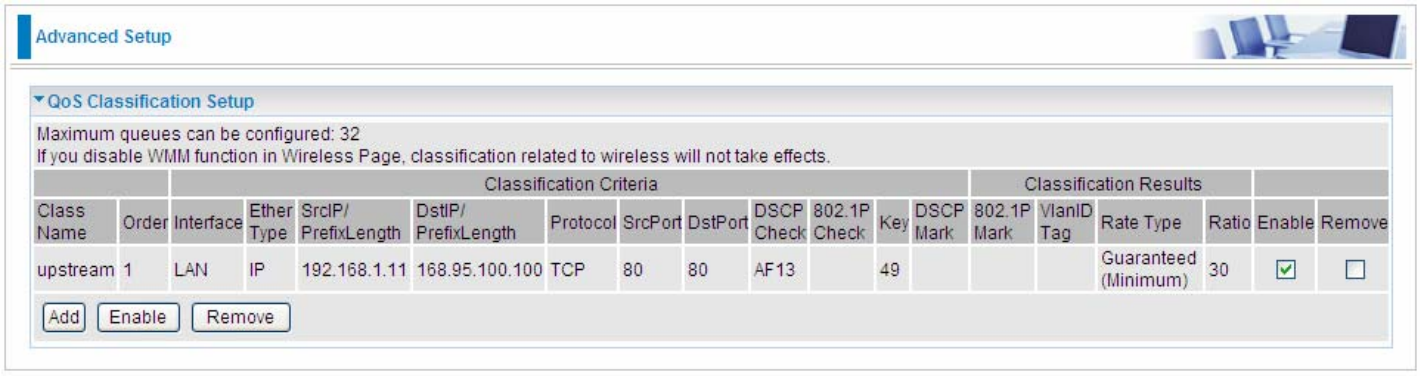
Remove: To delete the QoS class from the table, check Remove checkbox then click **Remove** button to delete the selected item.

WAN to LAN IP QoS

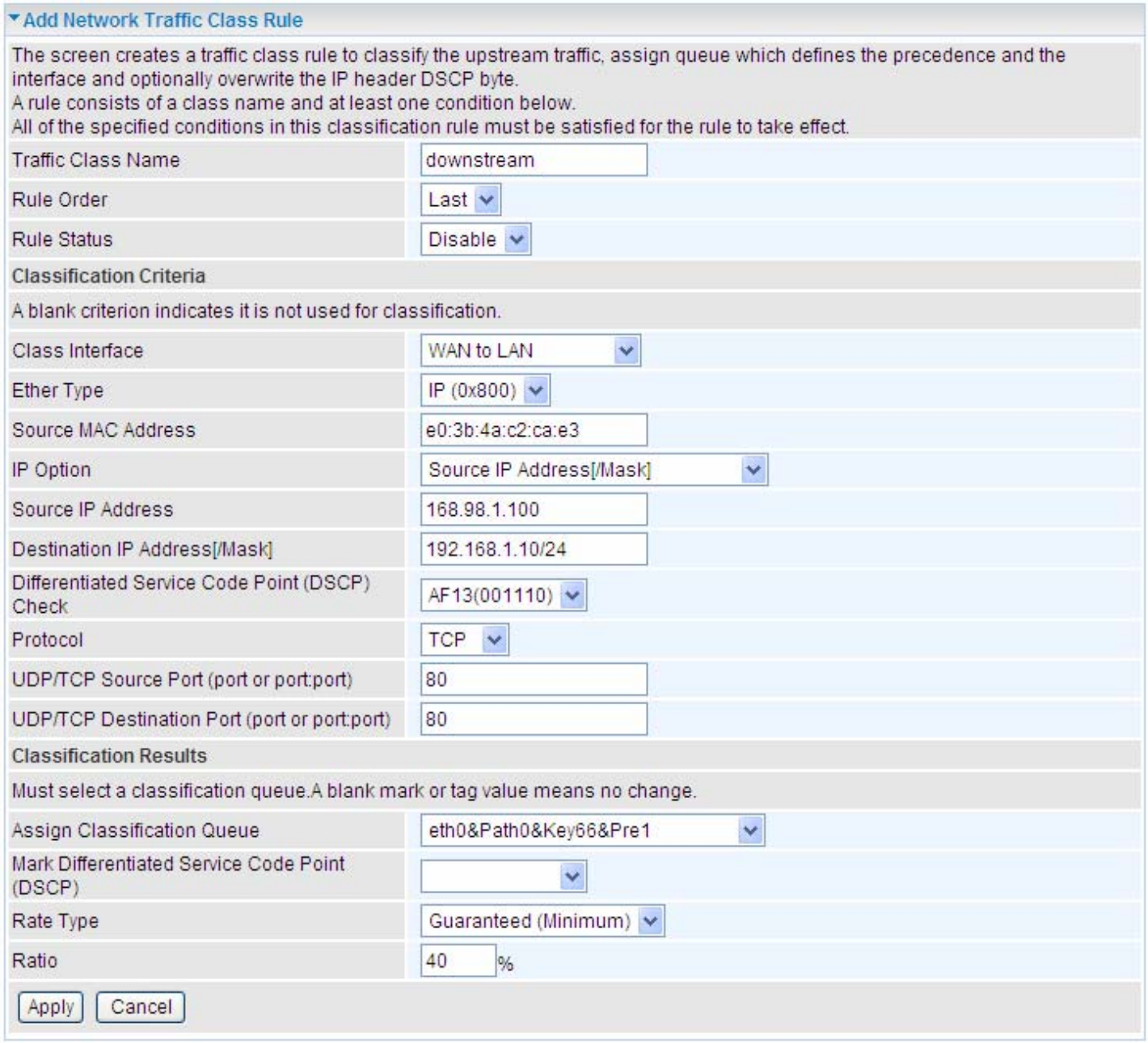
1. Here we take WAN to LAN (P1) QoS for example. Make sure there are enabled port P1 based queues here. LAN queues need your configuration. You can enable wireless to enable WMM queues by default or add P1-P4 ported based queues manually.

P1	66	P1	SP	1			☑	☐

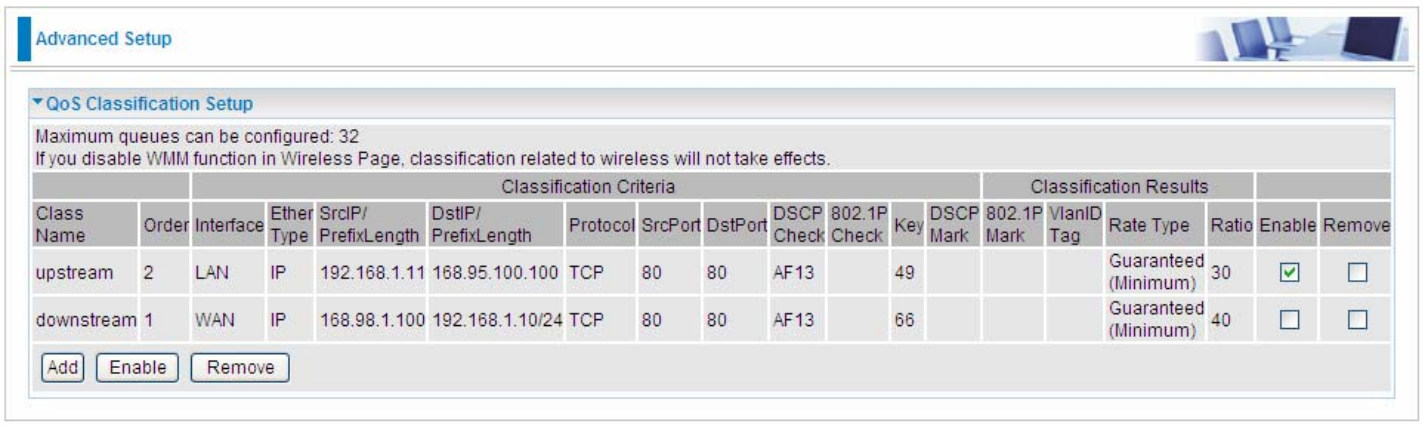
2. In QoS Classification Setup page, Click **Add** to add a Qos Classification.



Then in the Add Network Traffic Class Rule page, enter the information to set up a rule.



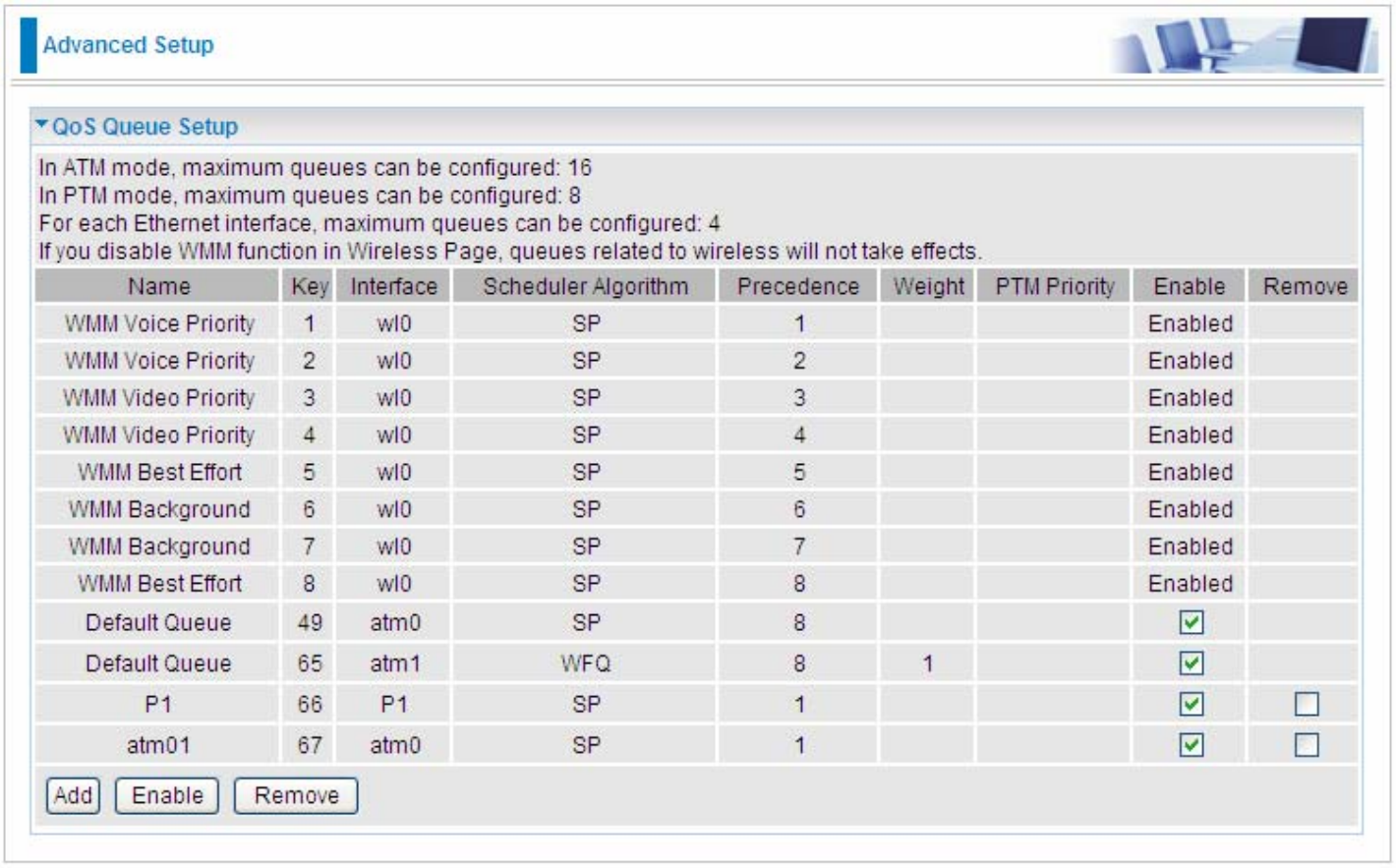
3. Click **Apply** to save your settings. The added rule will be listed as below.



Port-based QoS

Take port P1 to WAN QoS for example.

1. First make sure there is at least a WAN queue and it is enabled.



Advanced Setup

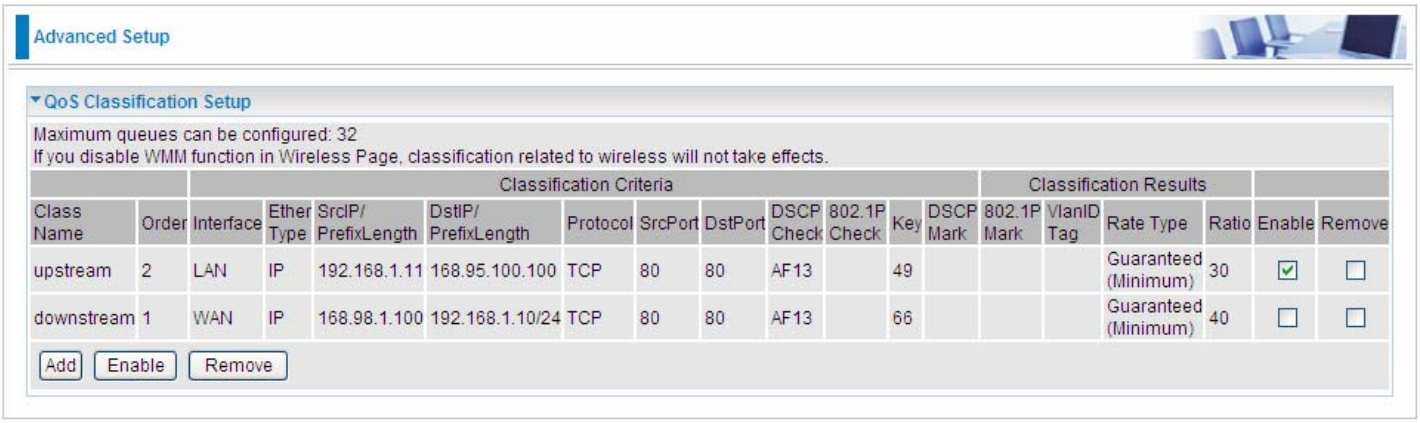
QoS Queue Setup

In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Scheduler Algorithm	Precedence	Weight	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1			Enabled	
WMM Voice Priority	2	wl0	SP	2			Enabled	
WMM Video Priority	3	wl0	SP	3			Enabled	
WMM Video Priority	4	wl0	SP	4			Enabled	
WMM Best Effort	5	wl0	SP	5			Enabled	
WMM Background	6	wl0	SP	6			Enabled	
WMM Background	7	wl0	SP	7			Enabled	
WMM Best Effort	8	wl0	SP	8			Enabled	
Default Queue	49	atm0	SP	8			☑	
Default Queue	65	atm1	WFQ	8	1		☑	
P1	66	P1	SP	1			☑	☐
atm01	67	atm0	SP	1			☑	☐

Add Enable Remove

2. In QoS Classification Setup page, Click **Add** to add a QoS Classification.



Advanced Setup

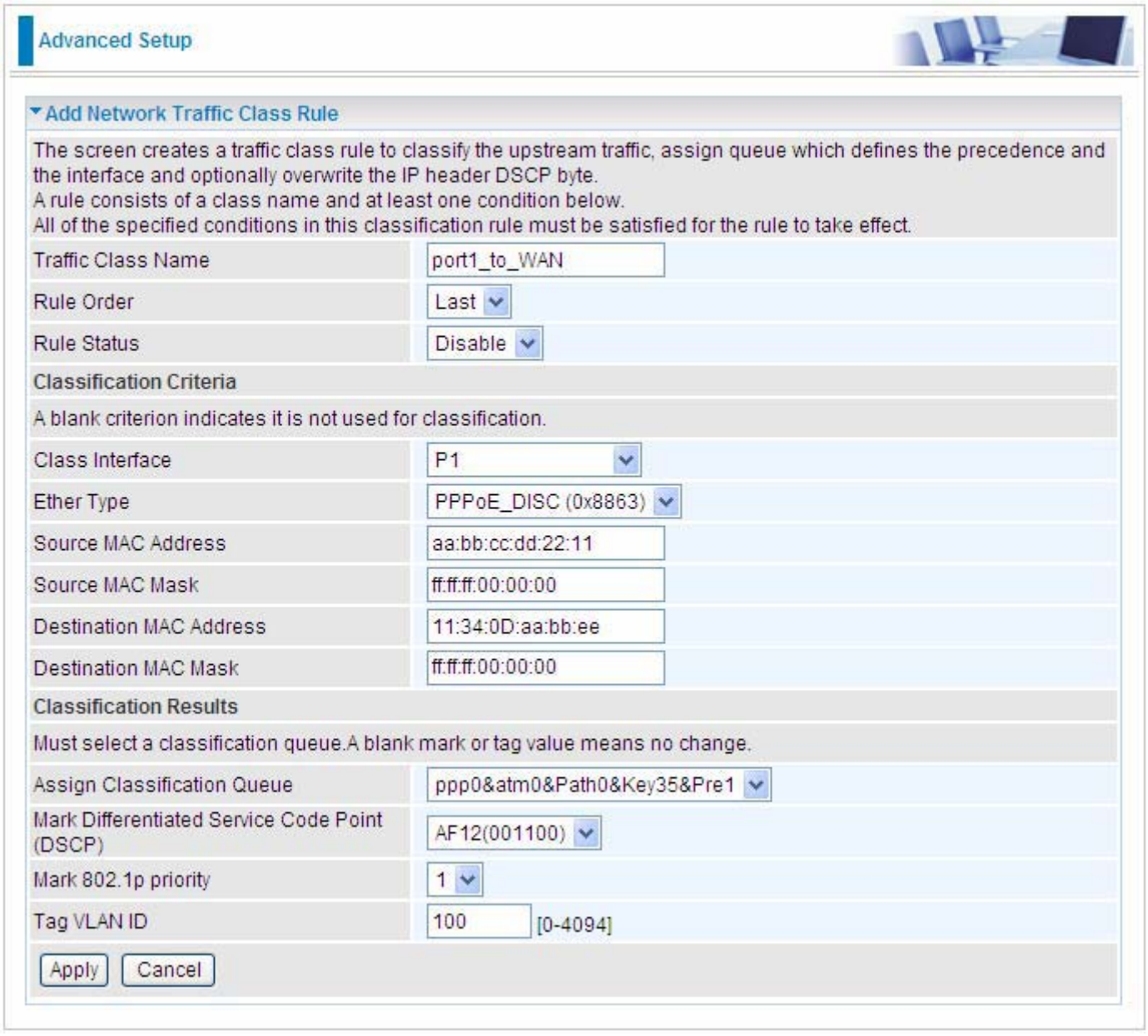
QoS Classification Setup

Maximum queues can be configured: 32
If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

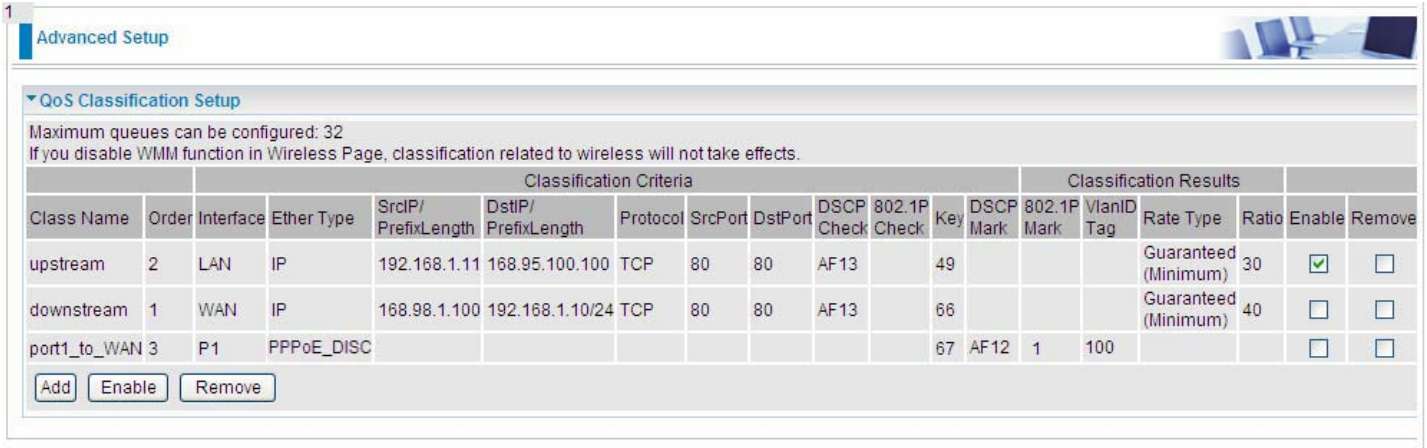
	Classification Criteria											Classification Results					
Class Name	Order	Interface	Ether Type	SrcIP/ PrefixLength	DstIP/ PrefixLength	Protocol	SrcPort	DstPort	DSCP Check	802.1P Check	Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Type	Ratio	Enable	Remove
upstream	2	LAN	IP	192.168.1.11	168.95.100.100	TCP	80	80	AF13		49				Guaranteed (Minimum)	30	☑	☐
downstream	1	WAN	IP	168.98.1.100	192.168.1.10/24	TCP	80	80	AF13		66				Guaranteed (Minimum)	40	☐	☐

Add Enable Remove

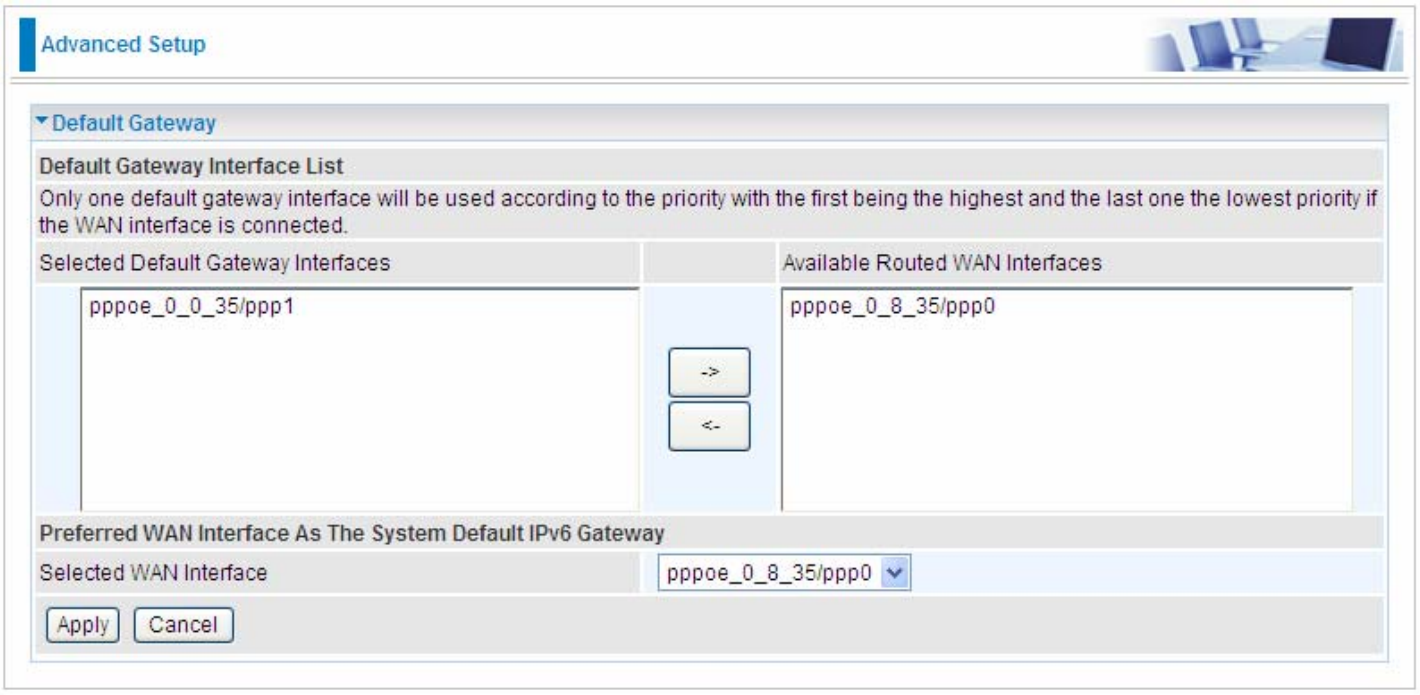
Then in the Add Network Traffic Class Rule page, enter the information to set up a rule to your needs. To Assign Classification queue, select the needed WAN queue.



3. Click **Apply** to save your settings and the added rule will be listed as below.



Default Gateway

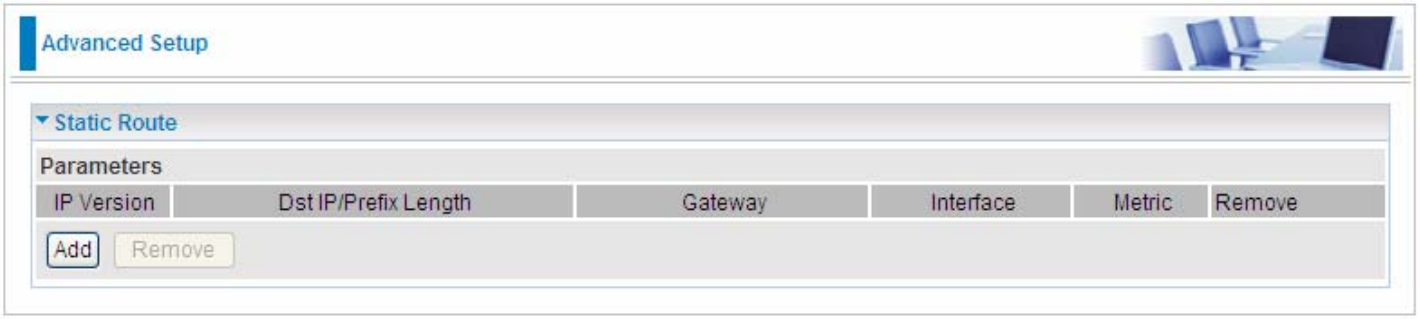


To set default gateway and Available Routed WAN Interface. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via -> or <- . And select a Default IPv6 Gateway from the drop-down menu.

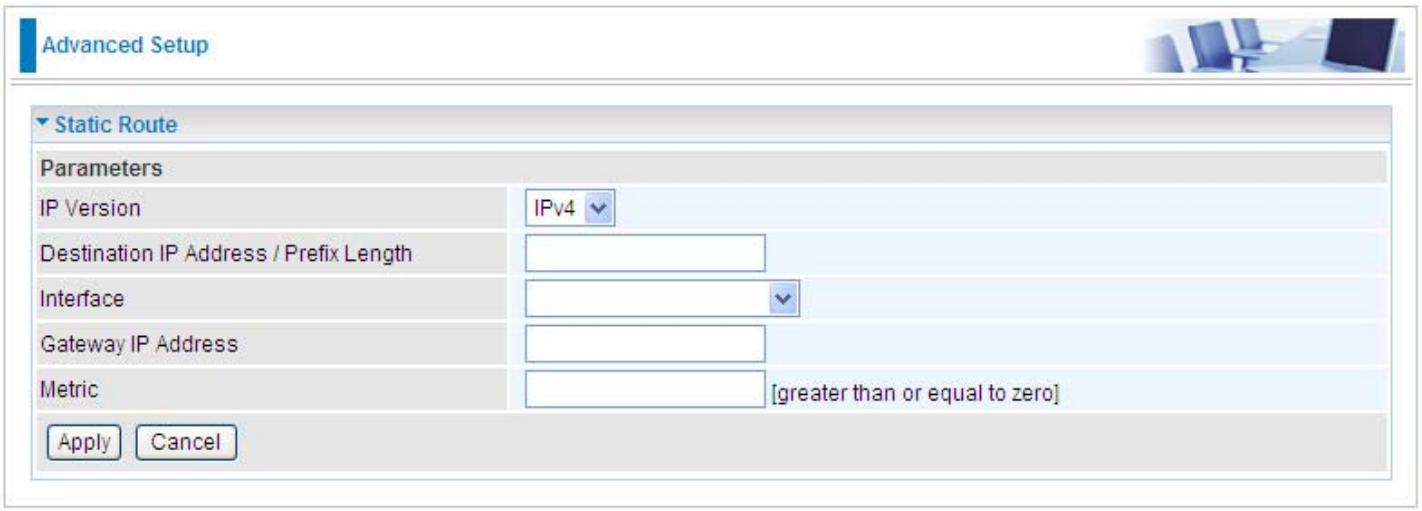
Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

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



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



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.

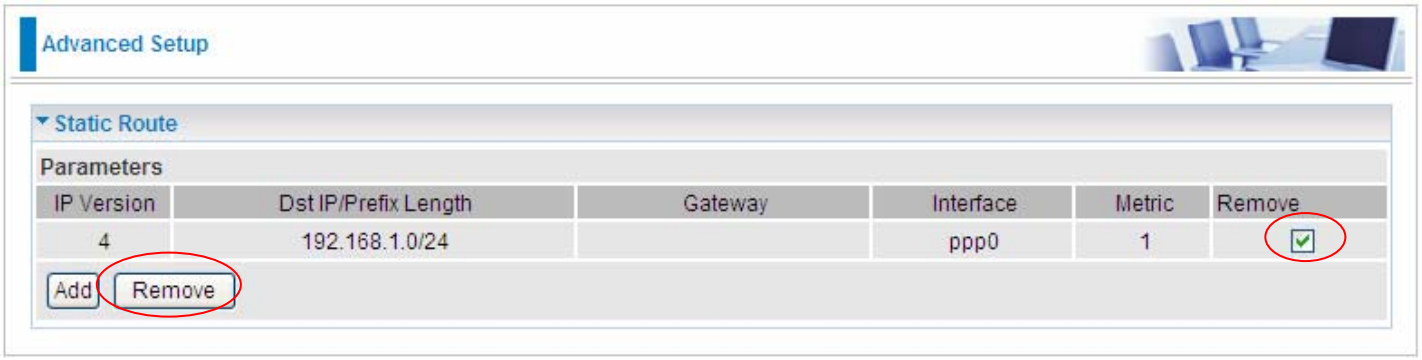
Interface: select an interface this route associated.

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.



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.

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

Policy Name: user-defined name.

Physical LAN Port: select the LAN port.

Source IP: enter the Host Source IP.

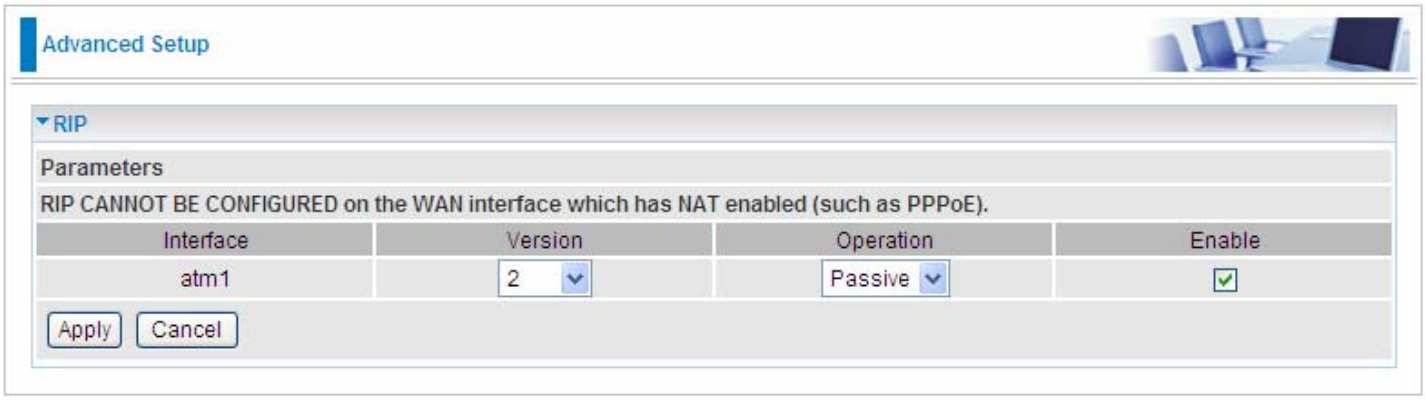
Interface: select the WAN interface which you want the Source IP to access outside through.

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.



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.

- **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- **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 not be configured on the WAN interface which has NAT enabled (such as PPPoE).

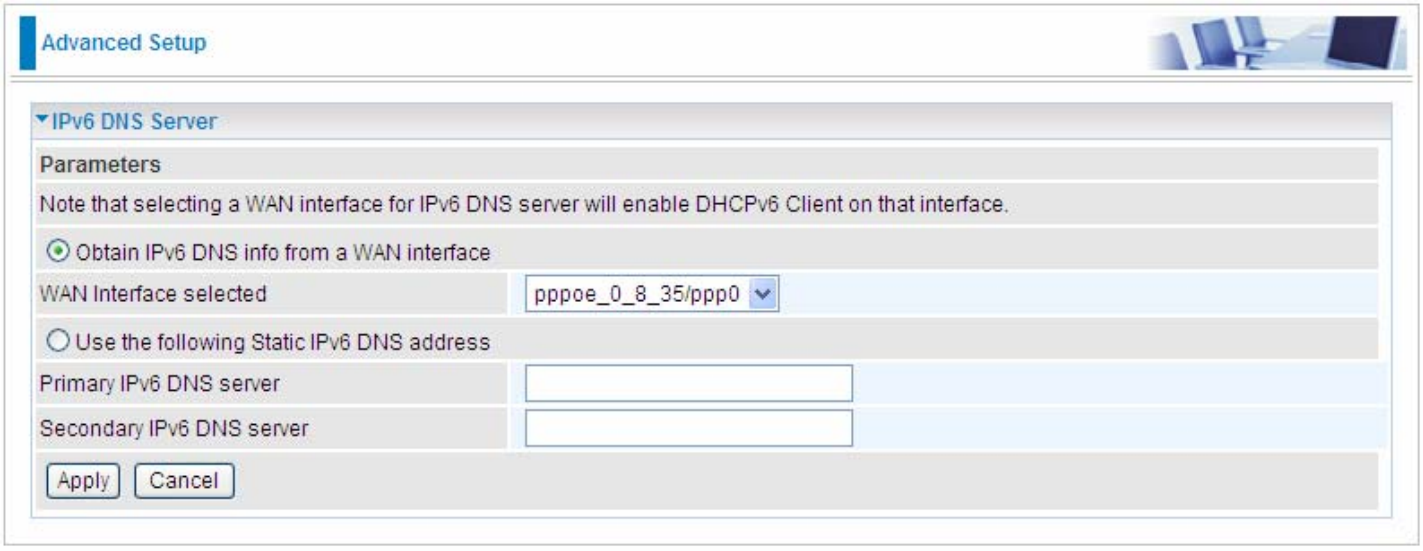
Click **Apply** to apply your settings.

DNS

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

IPv6 DNS Server

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

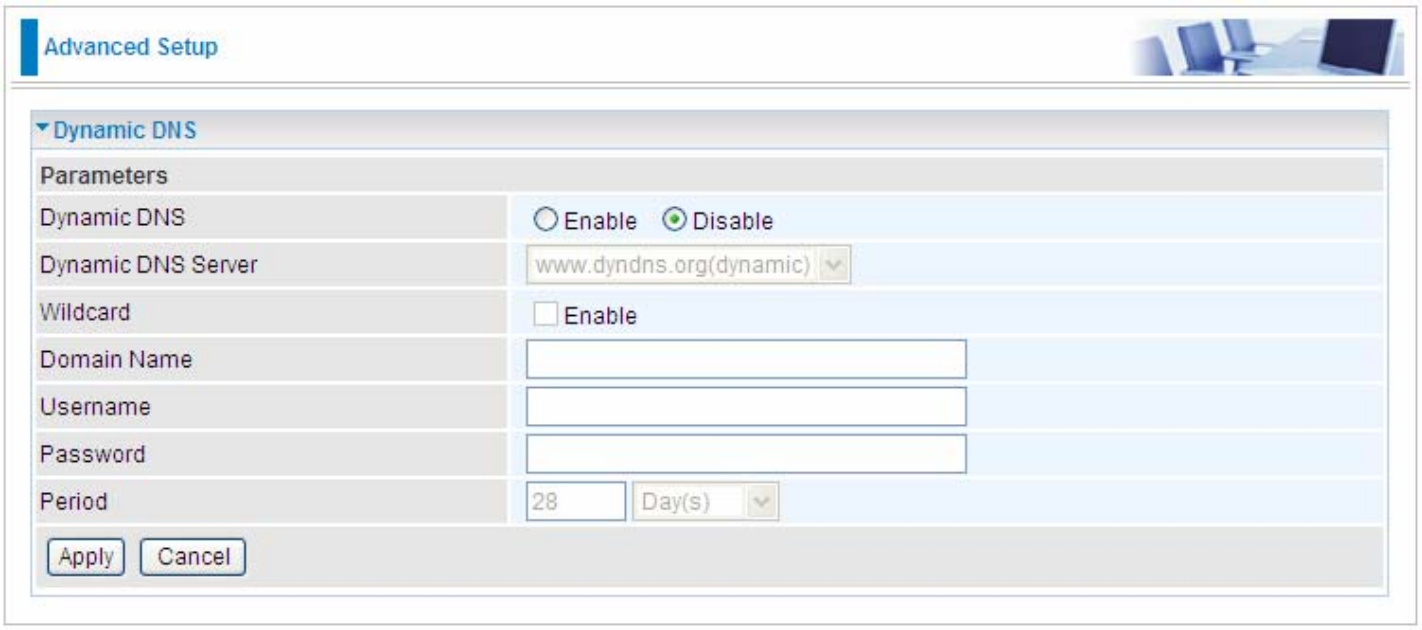
WAN Interface selected: select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

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 fromtime to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



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:

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required.

Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

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

Domain 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

DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.

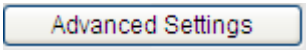
Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, ”ADSL2+”, “AnnexM” that user can select for this connection.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- **Bitswap Enable:** Allows bitswaping function.
- **SRA Enable:** Allows seamless rate adaptation.

Click Apply to confirm the settings.

Click  to future configure DSL.

Select the Test Mode, or leave it as default.

Tone Selection: suggesting you to leave it as default or let it configured by an advanced user.

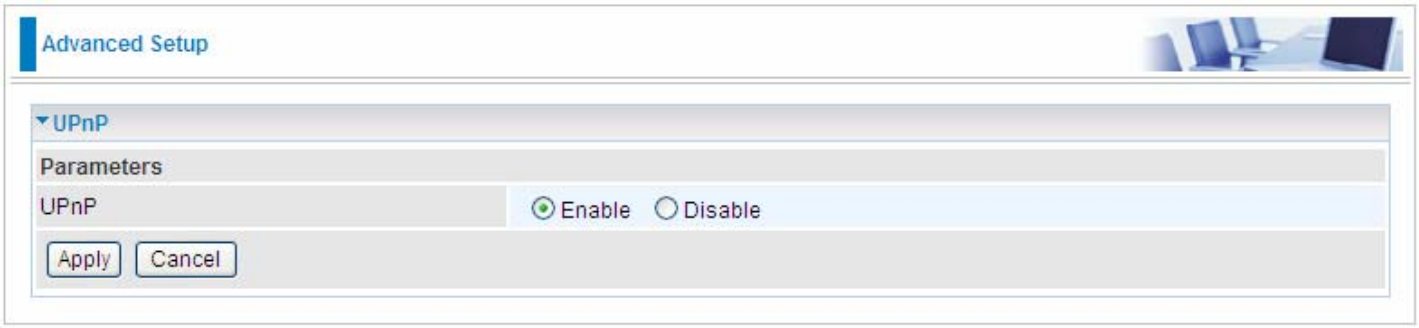
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream。

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.



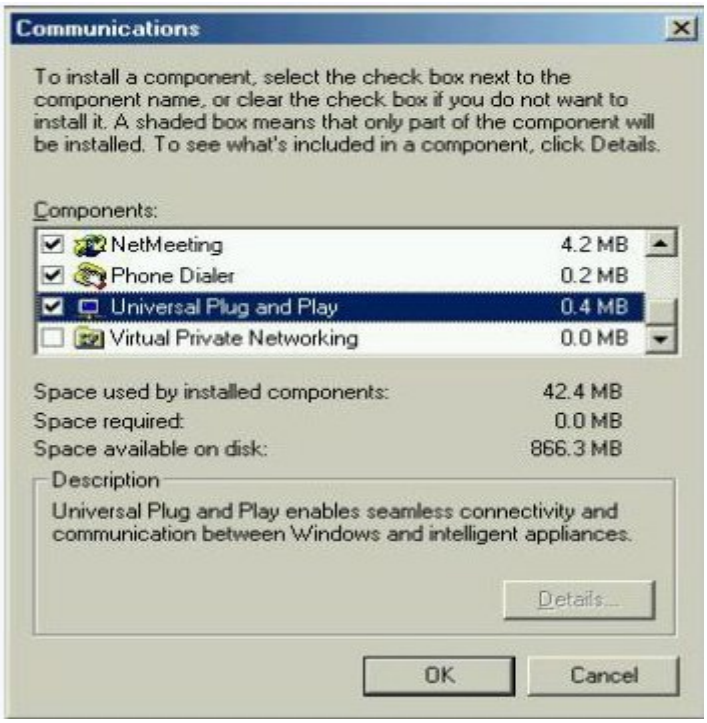
UPnP:

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

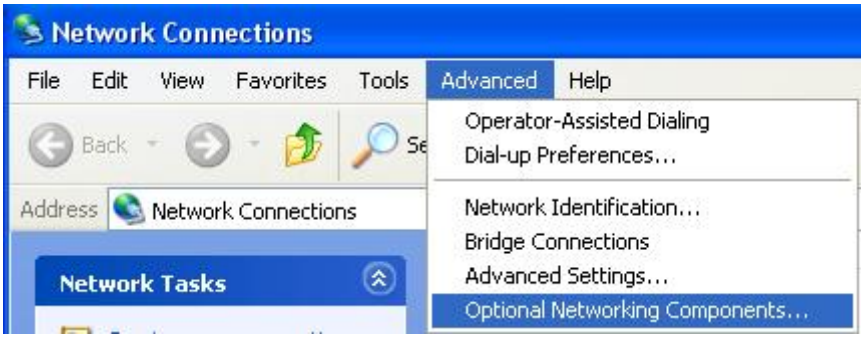
Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.
Step 5: Restart the computer when prompted.

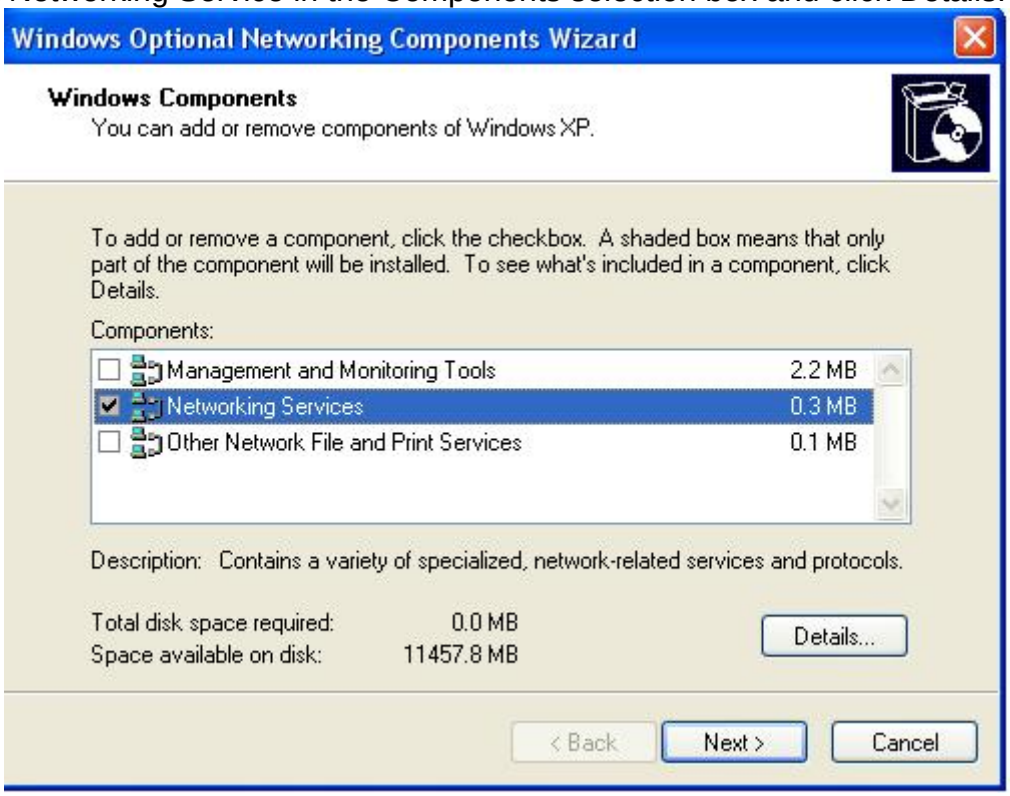
Follow the steps below to install the UPnP in Windows XP.

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 ….

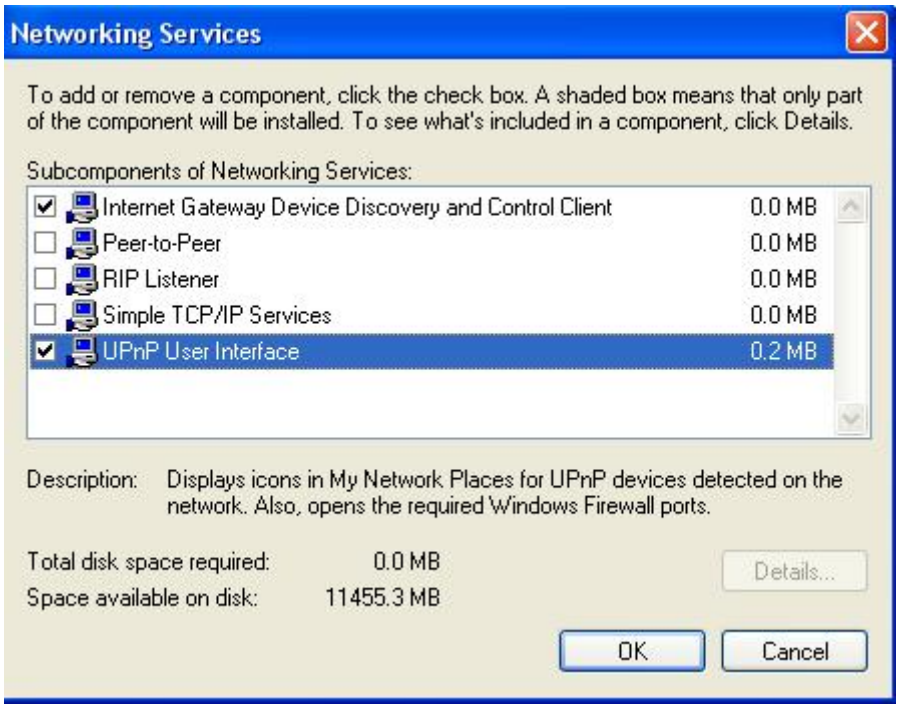


The Windows Optional Networking Components Wizard window displays.

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

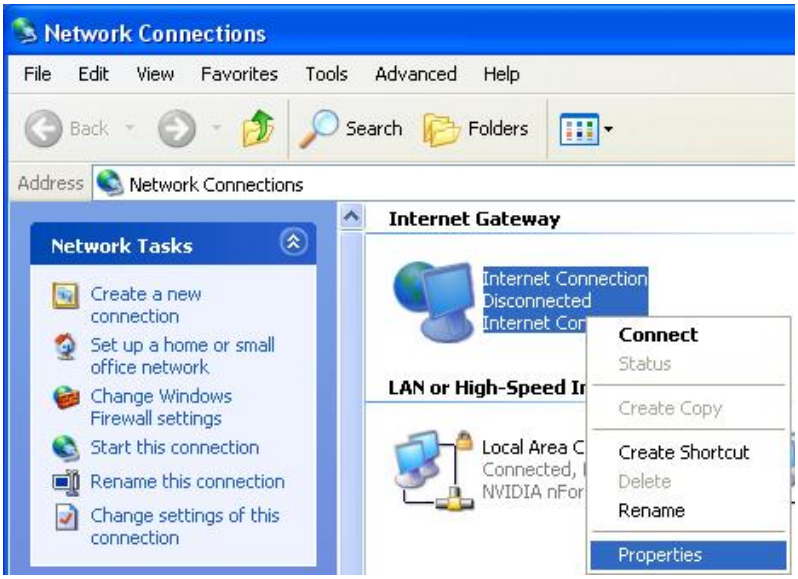


Step 5: In the Networking Services window, select the Universal Plug and Play check box.
Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.

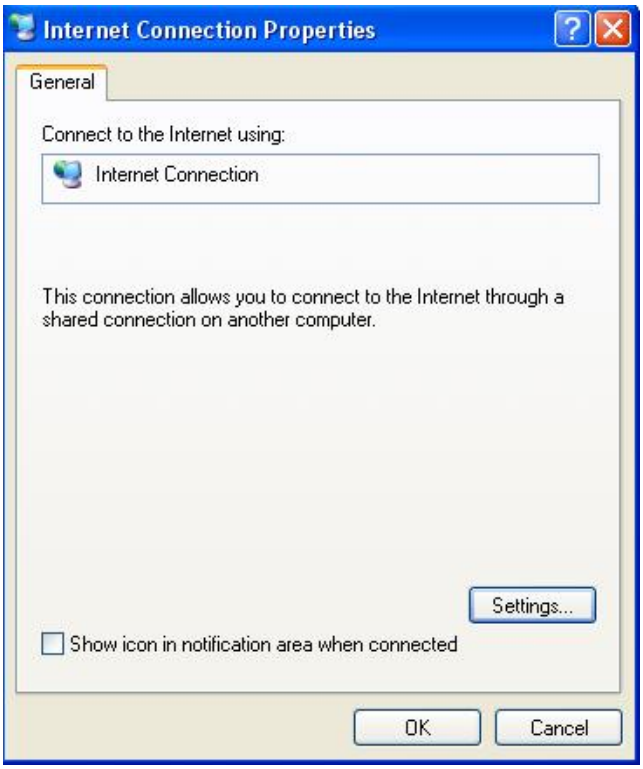


Auto-discover Your UPnP-enabled Network Device

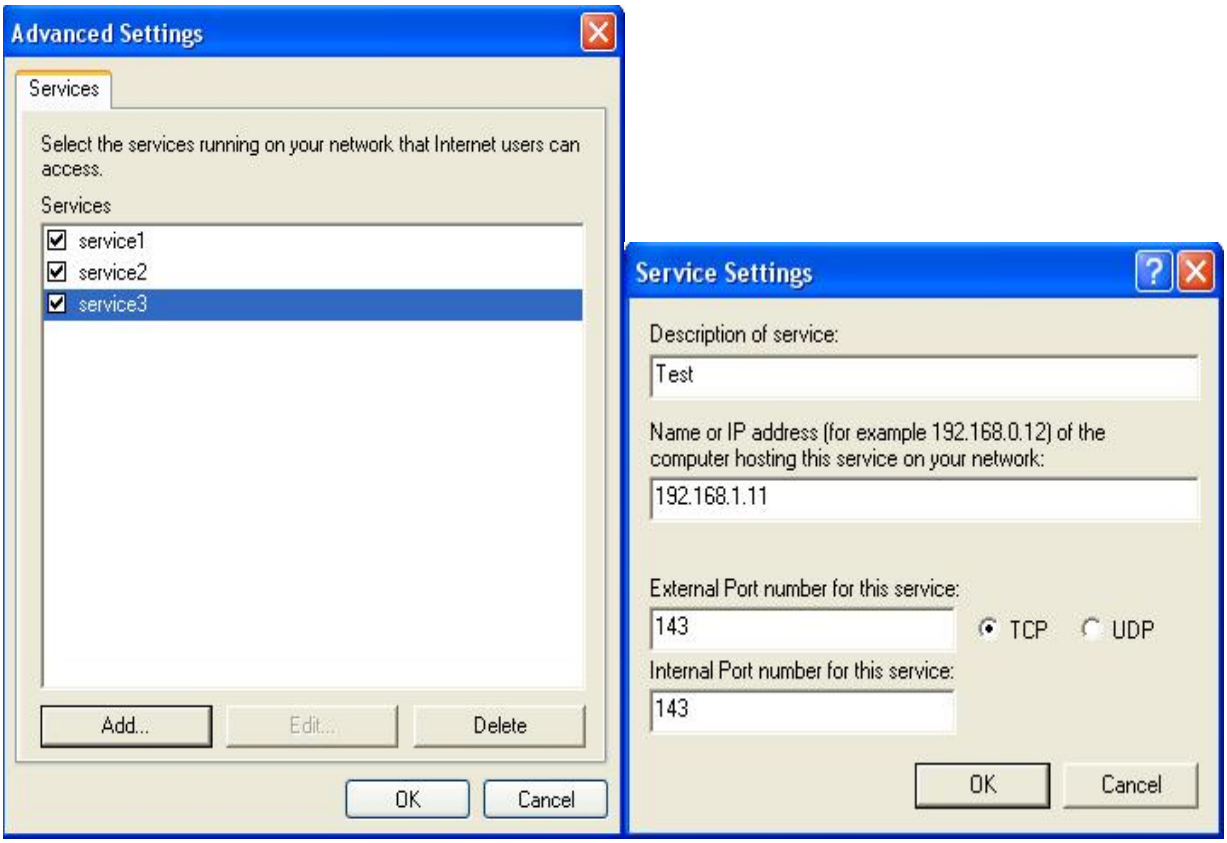
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.
Step 2: Right-click the icon and select Properties.



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

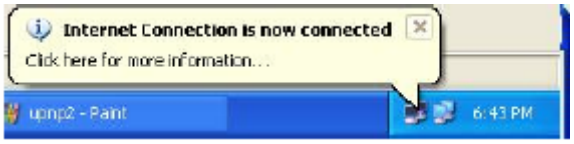


Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.

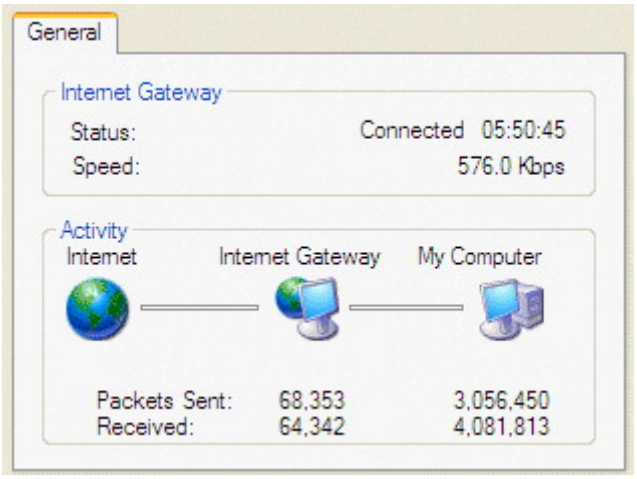


Step 5: Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



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



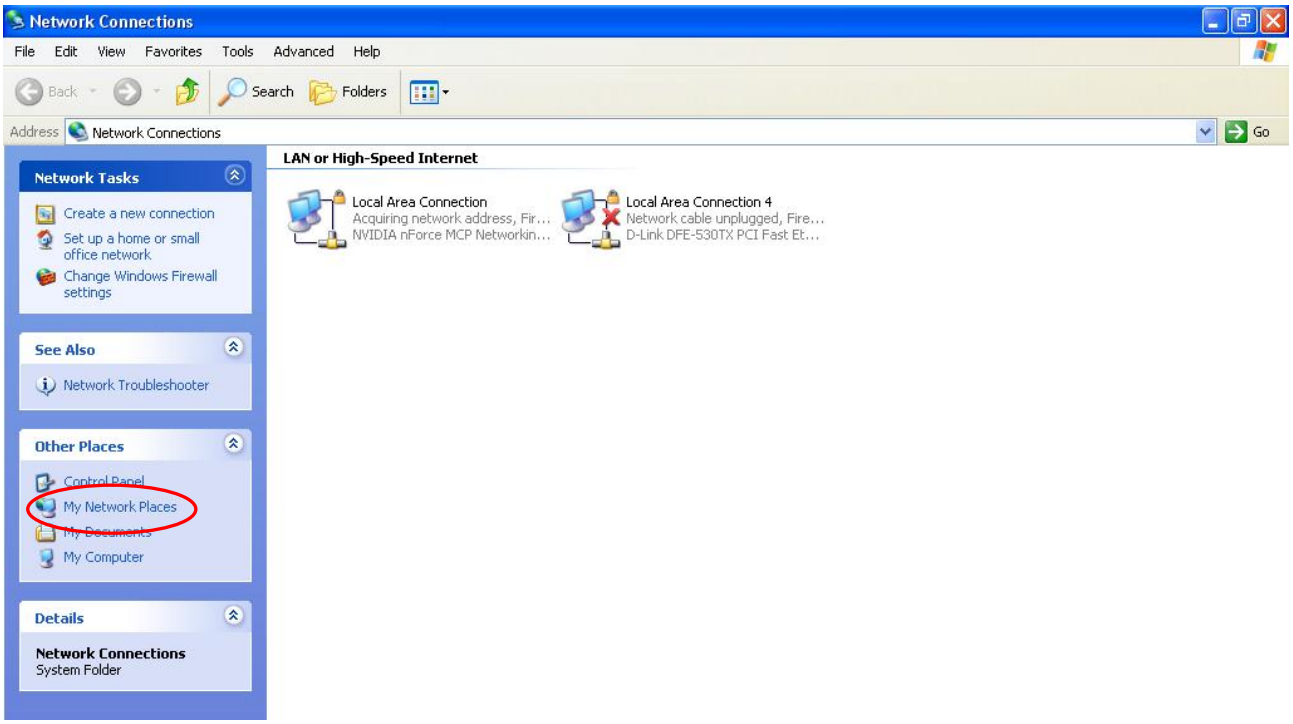
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7800NEXL 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.



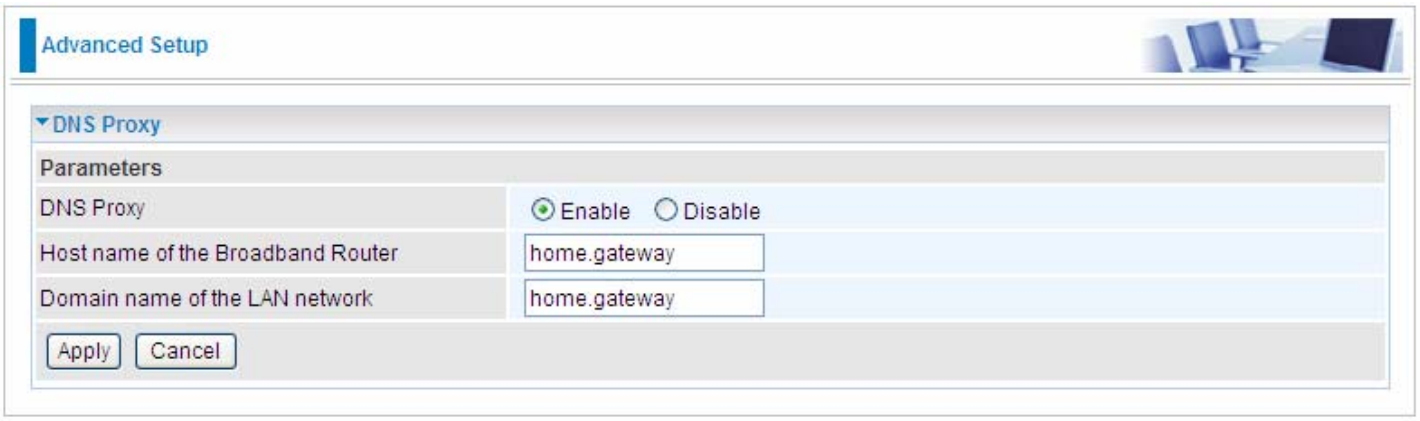
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7800NEXL and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7800NEXL and select Properties. A properties window displays basic information about the BiPAC 7800NEXL.

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.



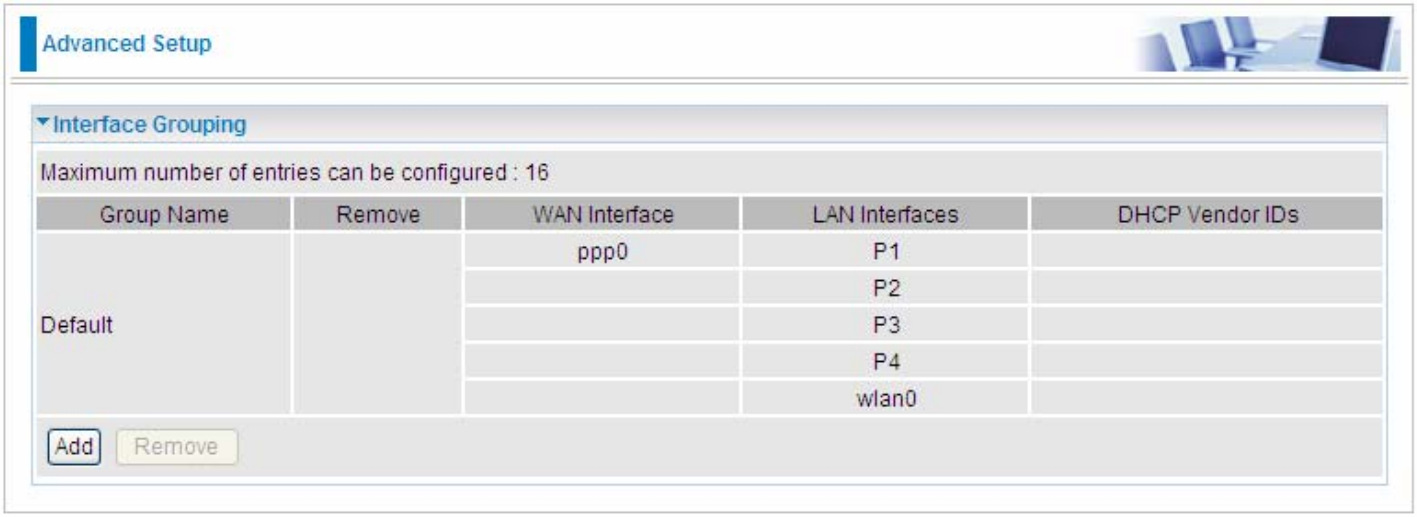
DNS Proxy: select whether to enable or disable DNS Proxy function, default is enabled.

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

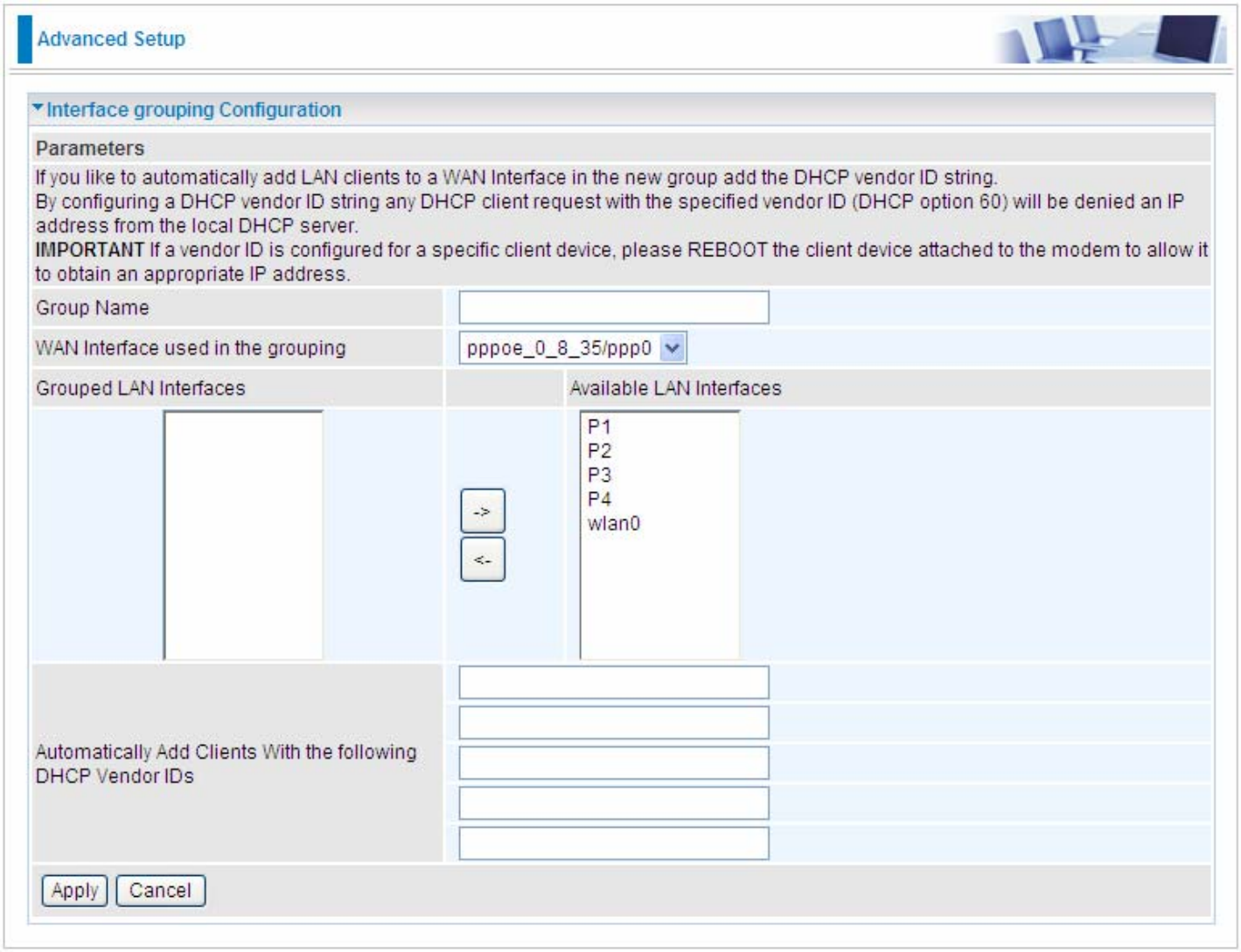
Domain name of the LAN network: enter the domain name of the LAN network. home.gateway.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.



Click **Add** to add groups. But note that the maximum number can be 16.



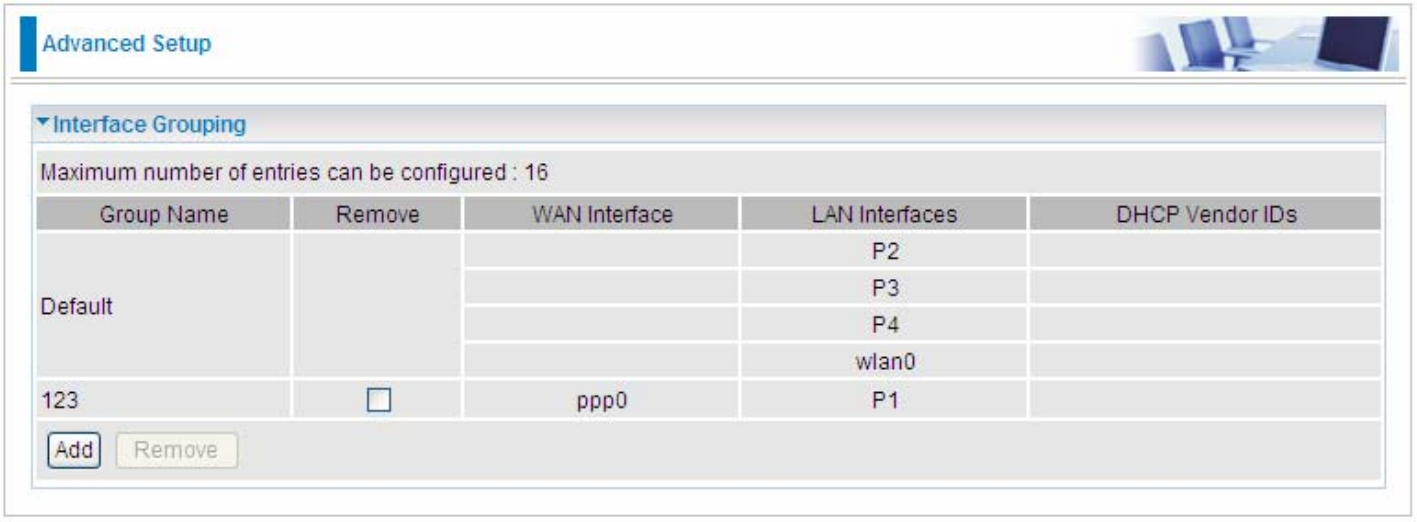
Group Name: type a group name.

WAN interface used in the grouping: select from the drop-down box the WAN interface you want to applied in the group.

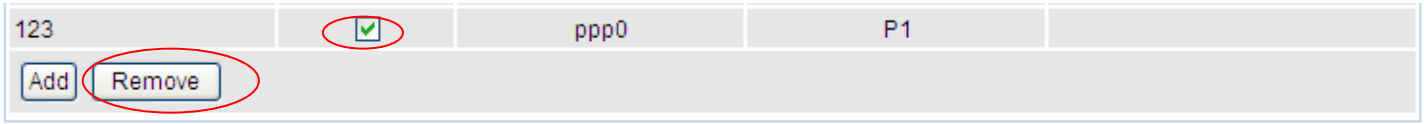
Grouped LAN Interfaces: select the LAN interfaces you want to group as a single group from **Available LAN Interfaces**.

Automatically Add Clients With following DHCP Vendor IDs: enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.



If you want to remove the group, check the box as the following and press **Remove**.



Note: If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

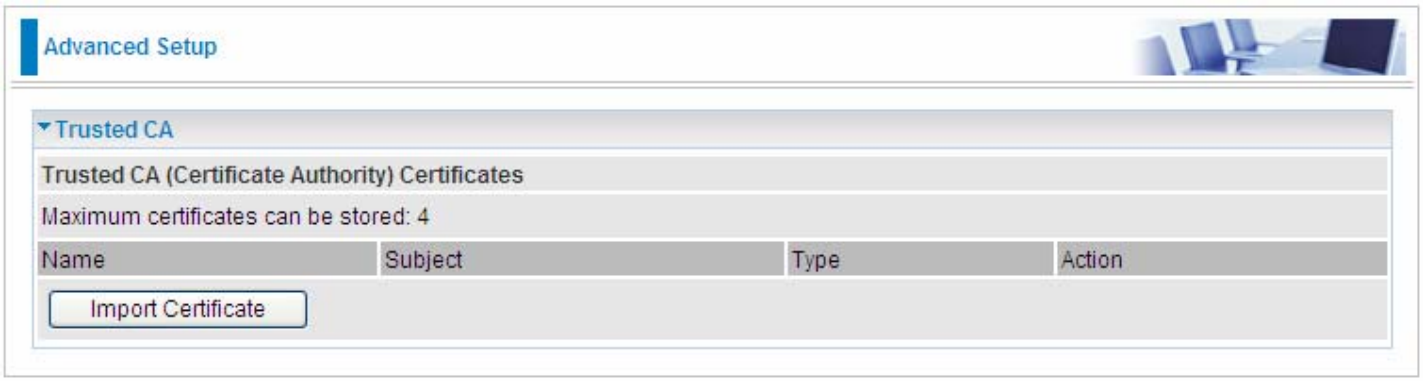
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

Certificate

This feature is used for TR069 ACS Server authentication of the device used 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.



Certificate Name: the certificate identification name.

Subject: the certificate subject.

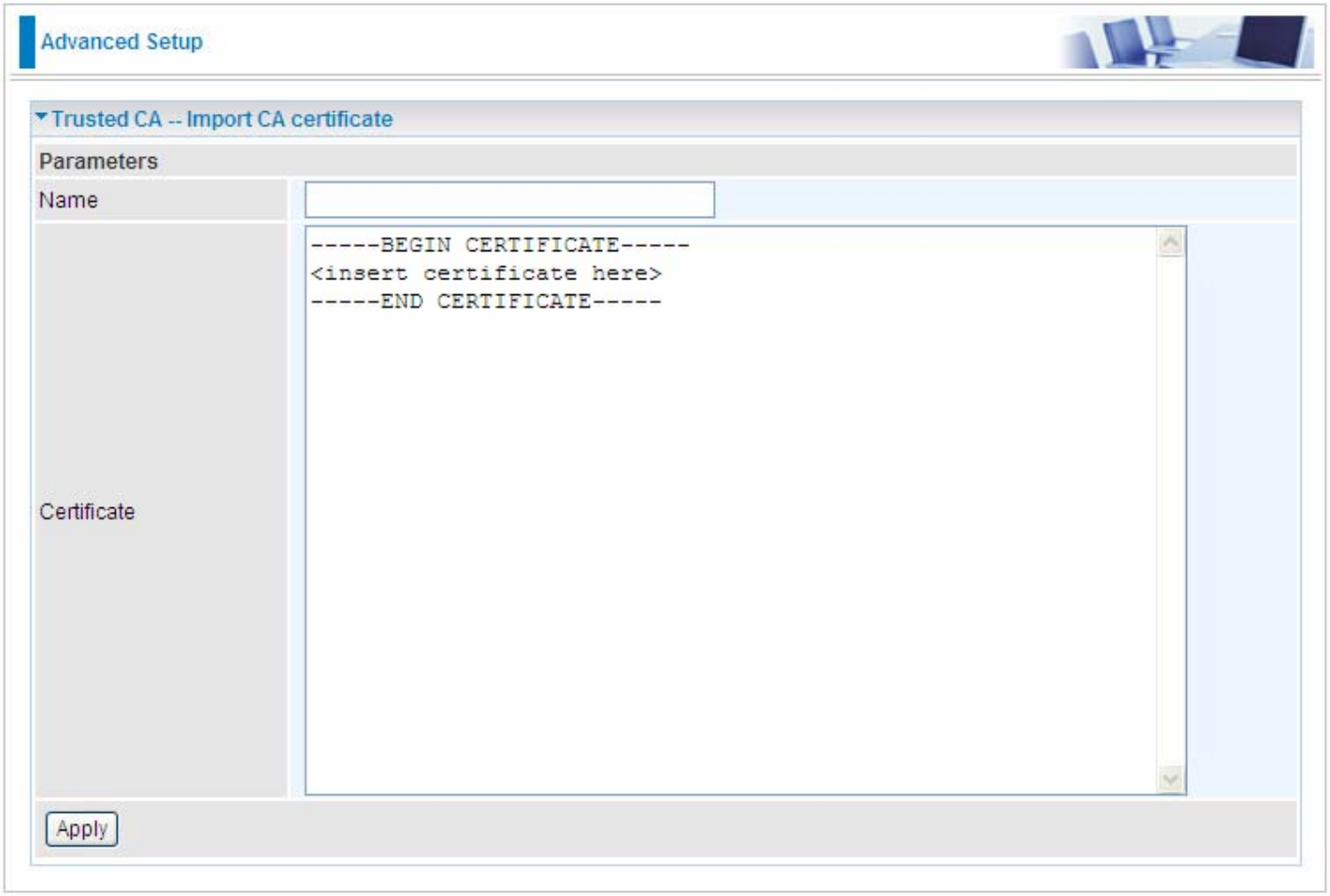
Type: the certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

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

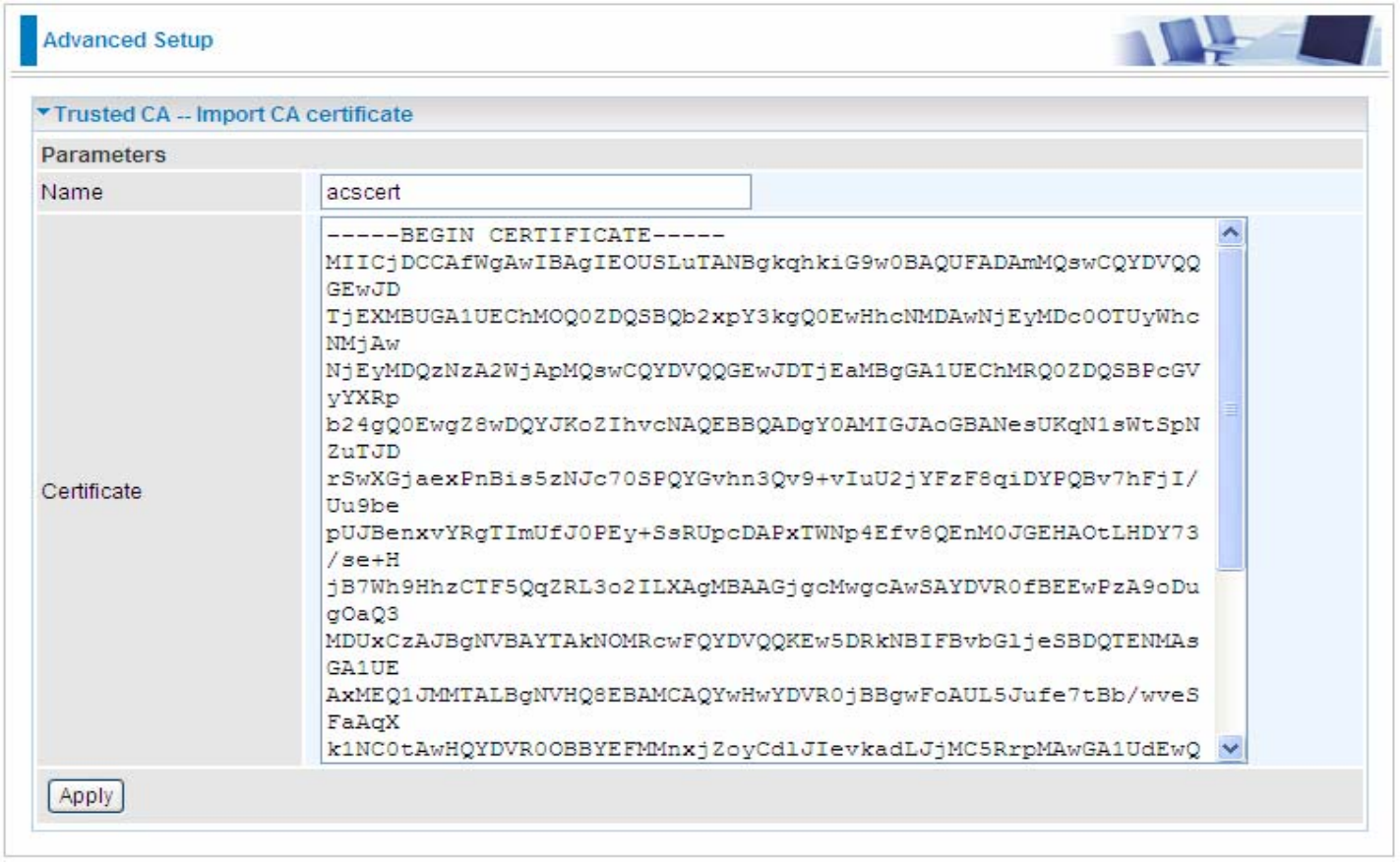
Action:

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

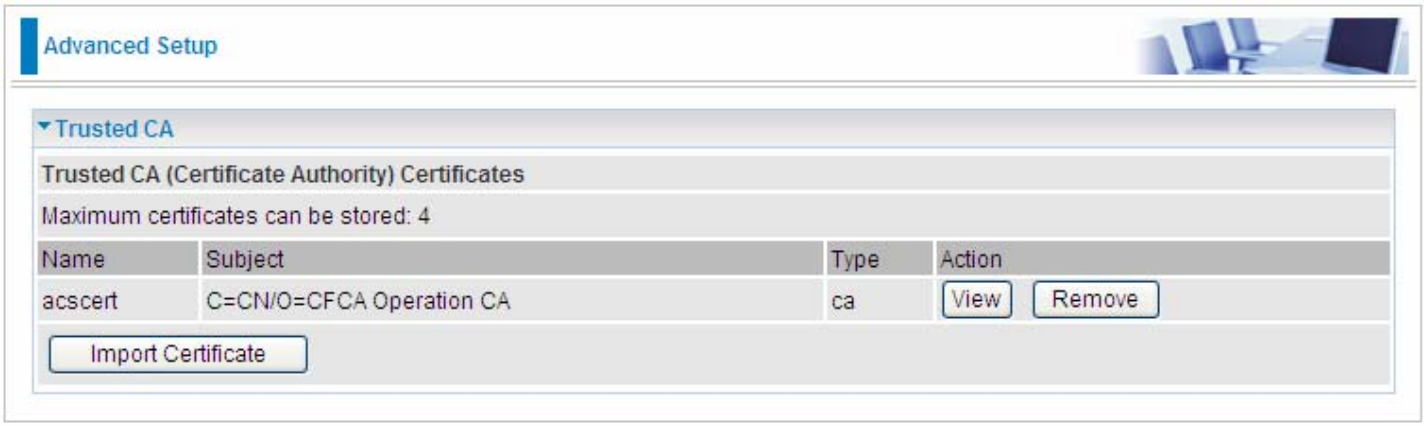
Click **Import Certificate** button to import your certificate.



Enter the certificate name and insert the certificate.



Click Apply to confirm your settings.

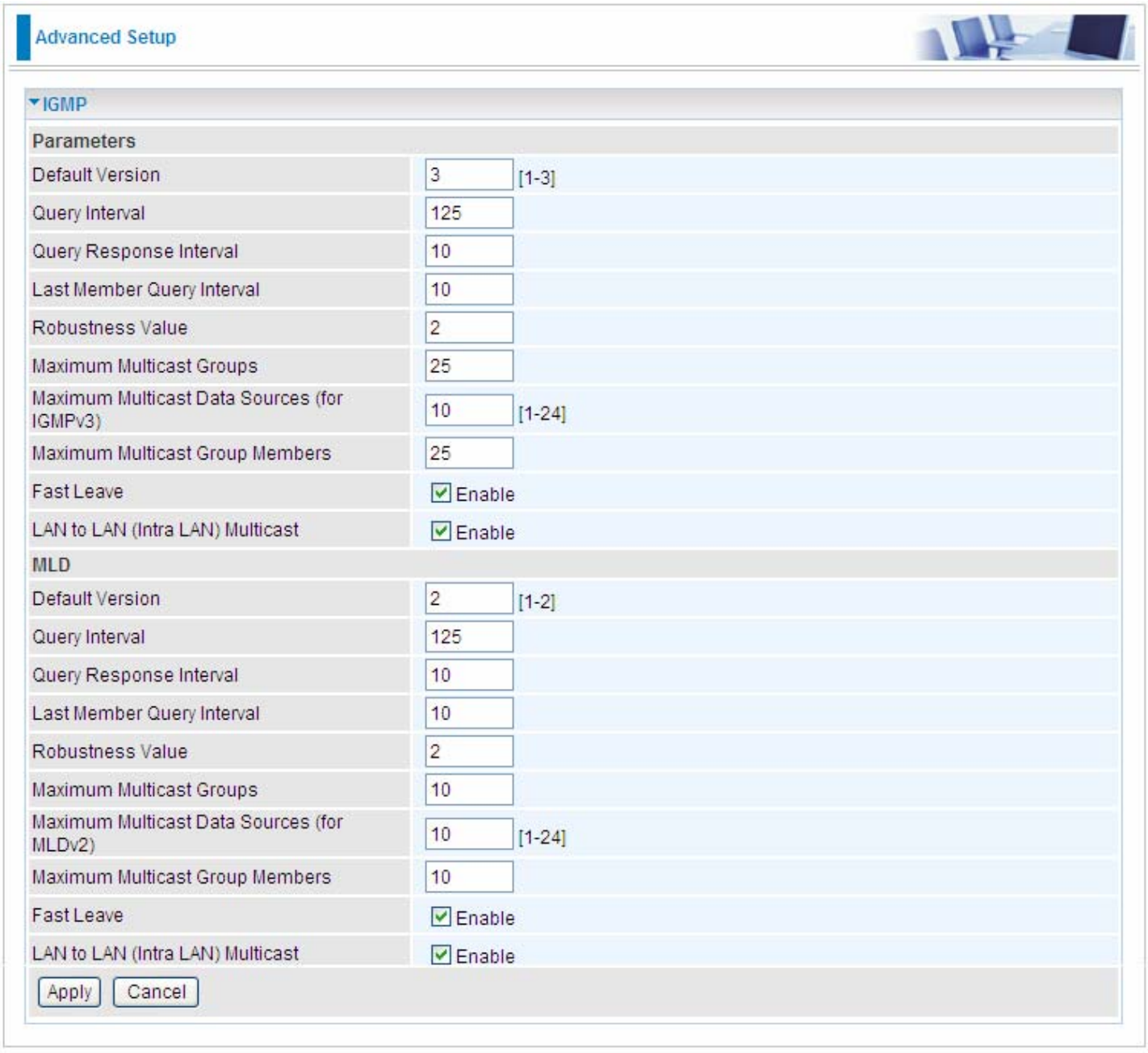


Multicast

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** 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.



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.

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.

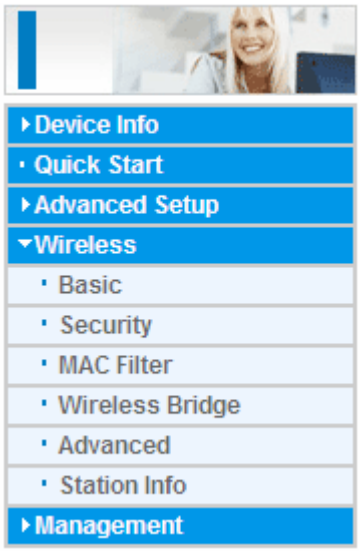
Fast leave: check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

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.

Wireless

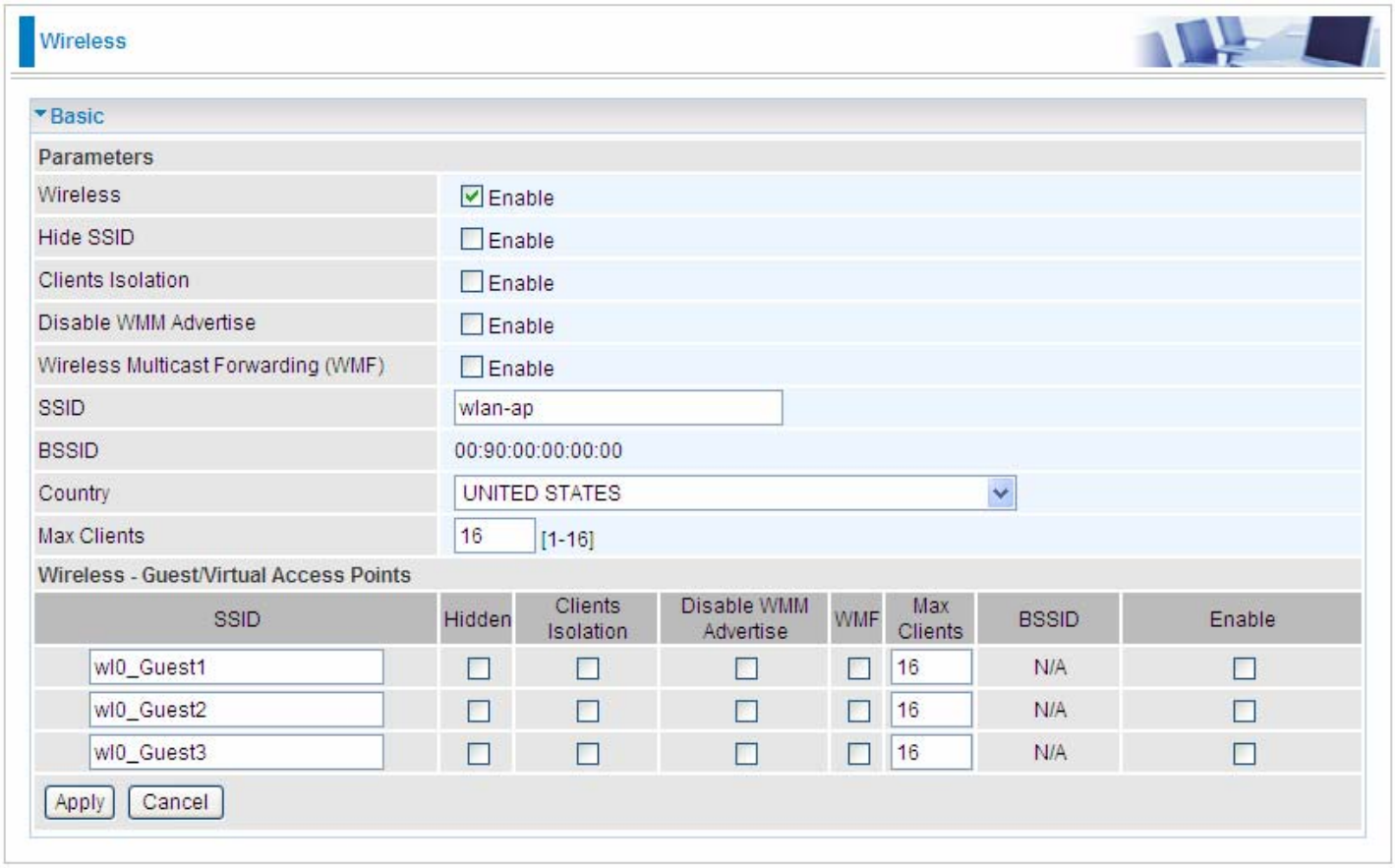
This section provides you ways to configure wireless access. When you click this item, the column will expand to display the sub-items that will lead you to configure your router.

Basic, **Secturity**, **MAC Filter**, **Wireless Bridge**, **Advanced** and **Station Info** are included here.



Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.



Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not excess 32 characters.

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to the area where you want to device used.

Max Clients: enter the number of max clients the wireless network can supports,1-16.

Max-Guest/virtual Access points: A "Virtual Access Point" is a logical entity that exists within a

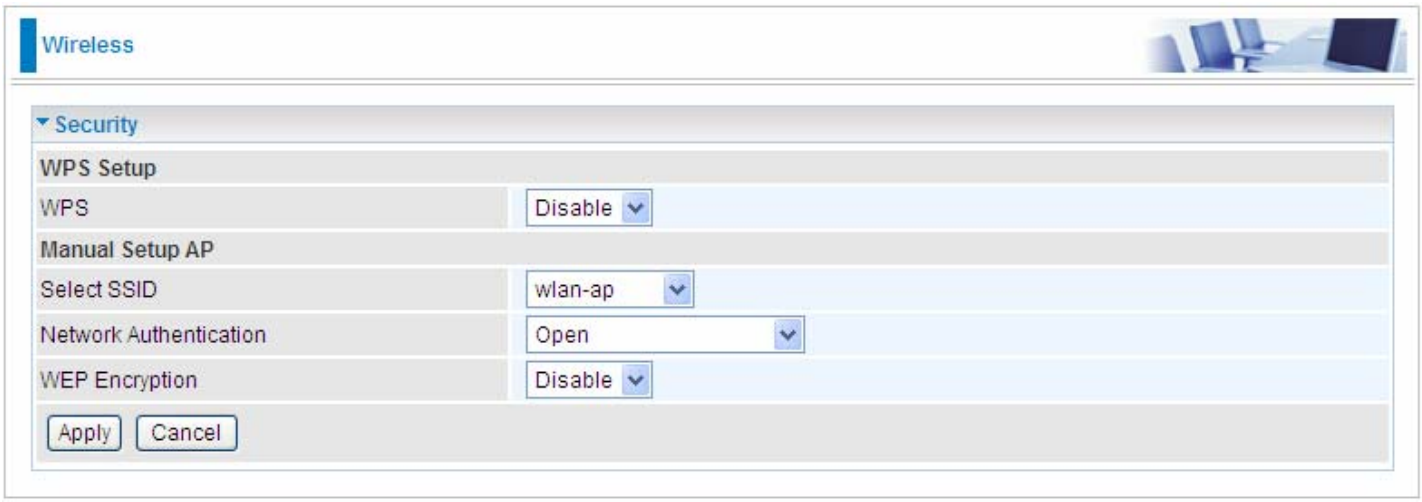
physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless network.

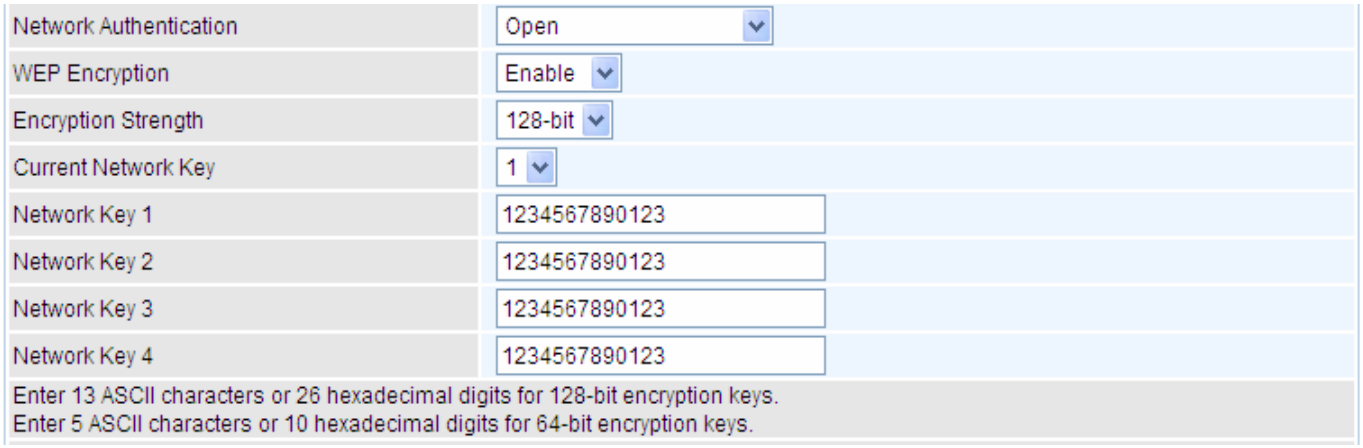


Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

ⓘ **Open**



WEP Encryption: select to enable or disable WEP Encryption. Here select Enable.

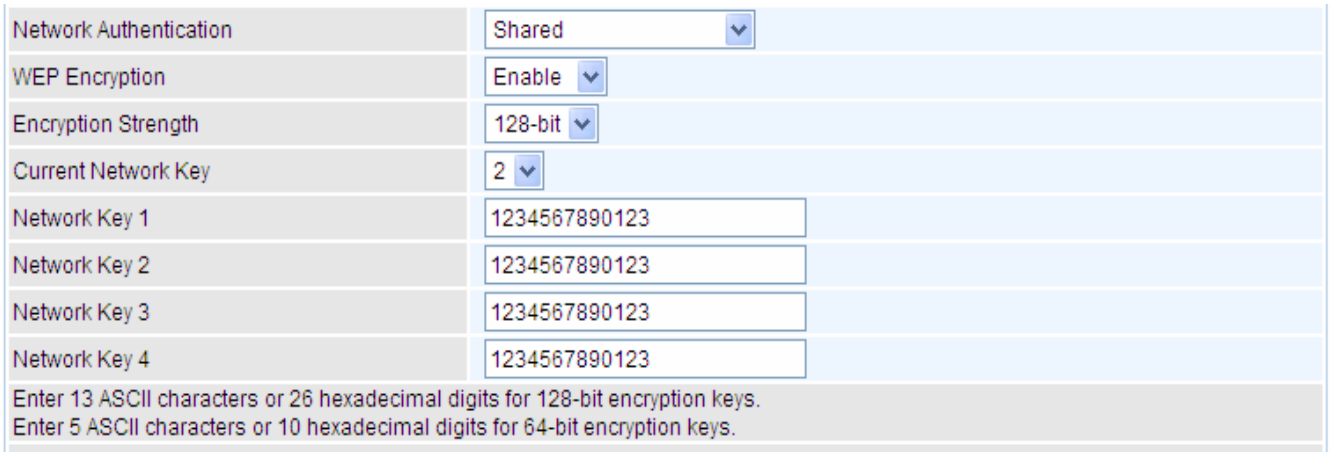
Encryption Strength: select the strength, 128-bit or 64-bit.

Current Network Key: select the one to be the current network key. Please refer to key 1- 4 below.

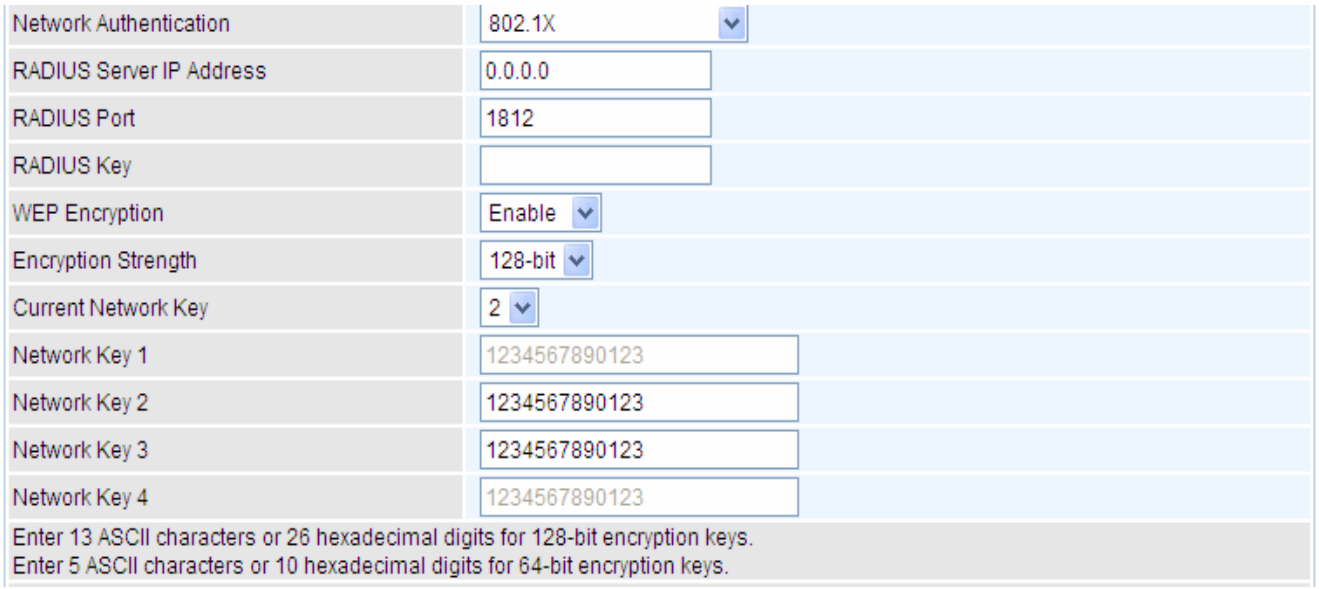
Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ Shared

It is similar to network authentication ‘Open’. But here the WEP Encryption must be enabled.



ⓘ 802.1x



RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

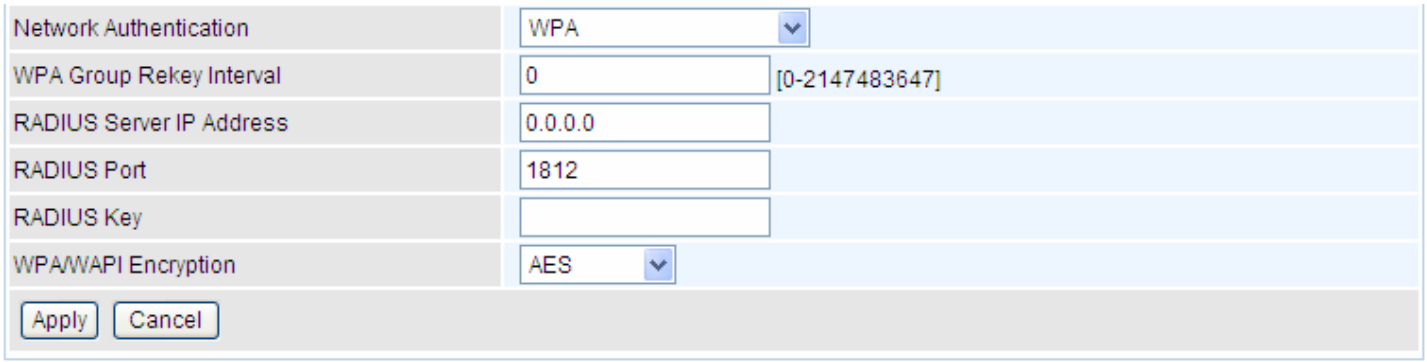
RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ WPA



WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

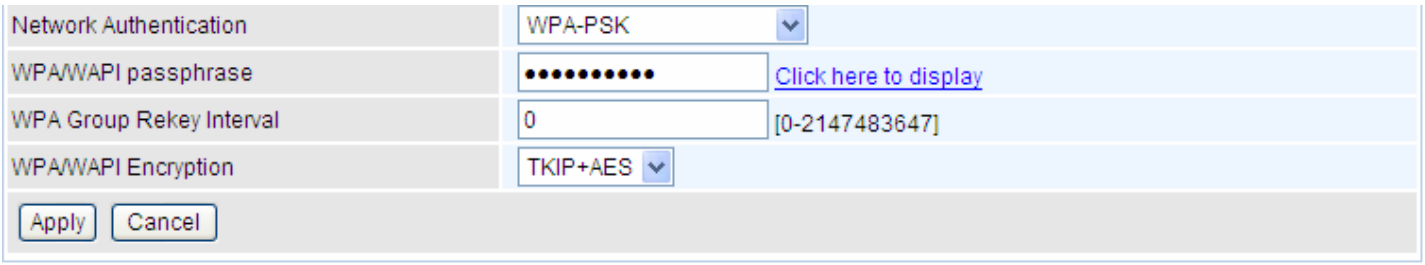
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA-PSK / WPA2-PSK

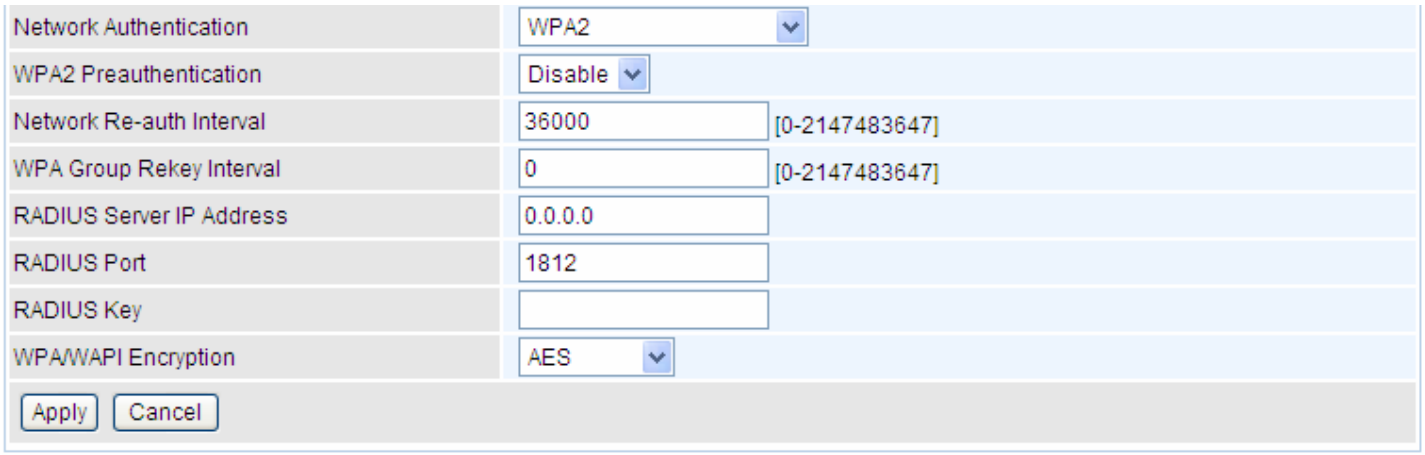


WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA2



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with

preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

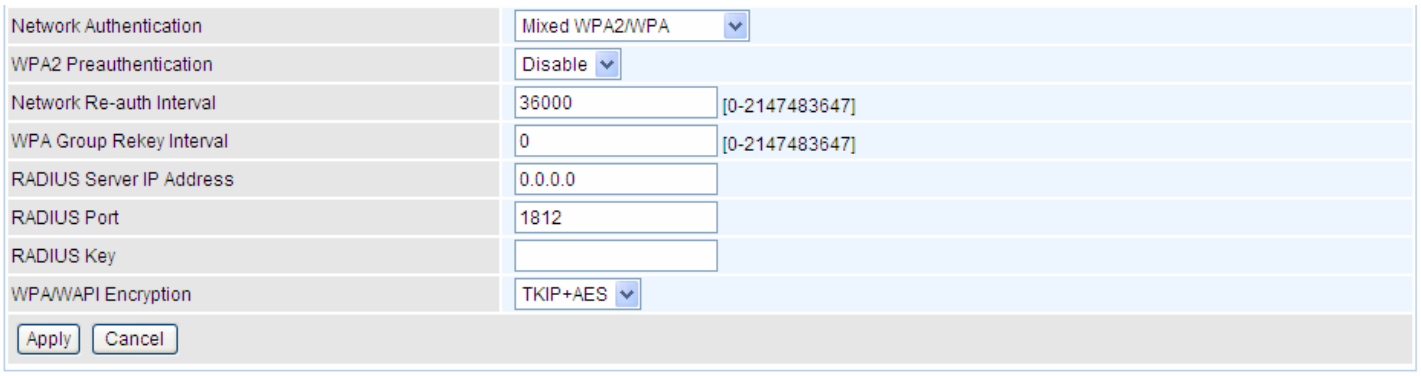
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. The unit is second.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

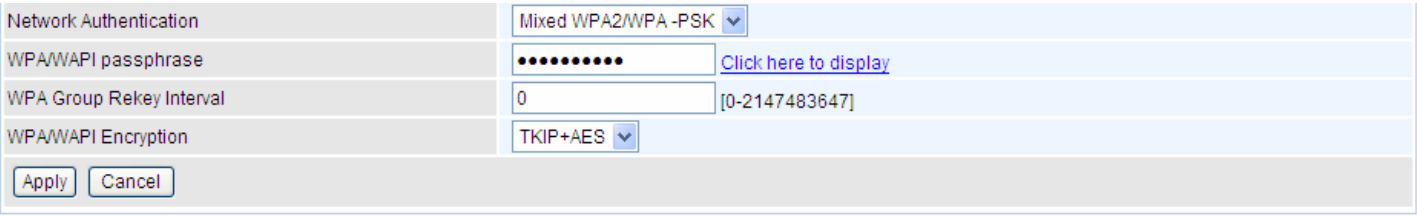
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA-PSk



WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

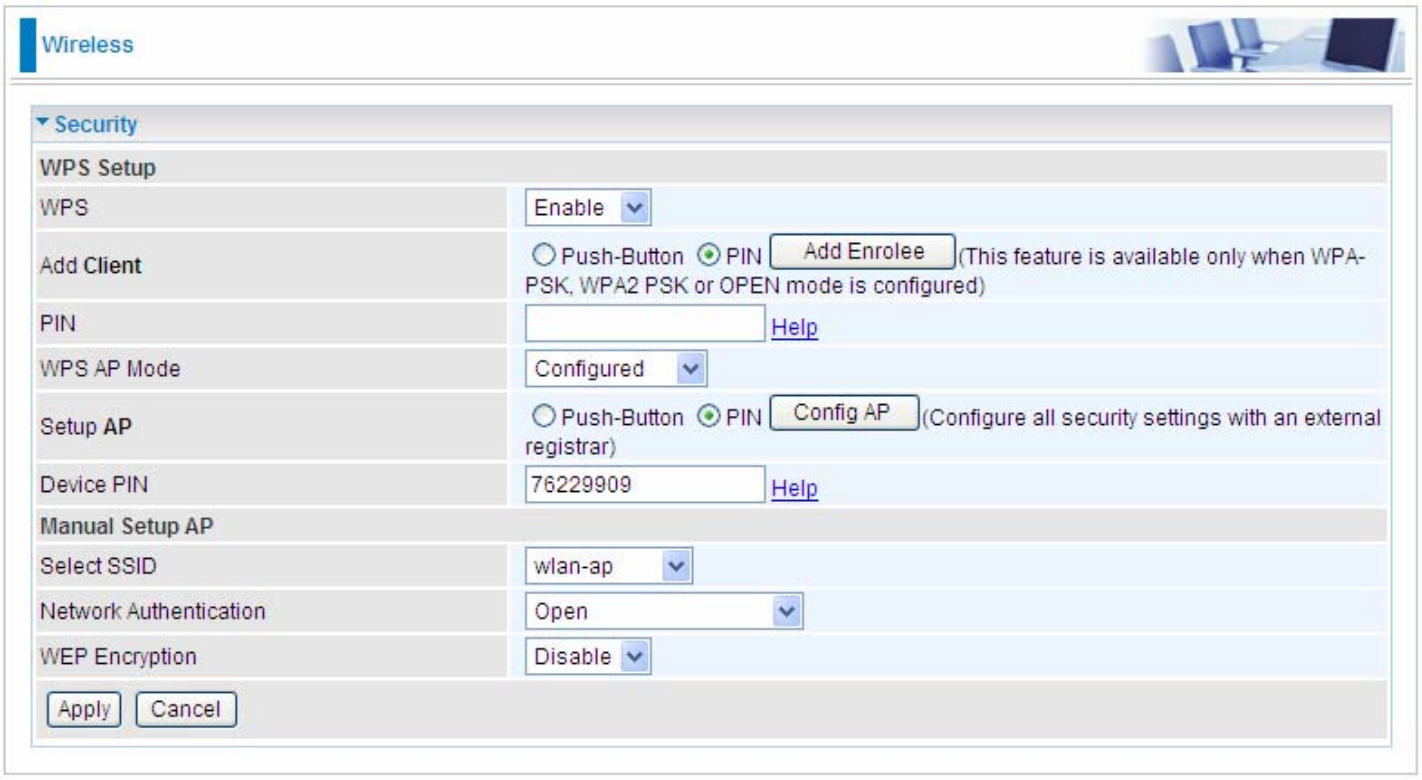
WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure Ap setting.This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.

WPS: select enable to enable WPS function. As you see, WPS can only be available when WPA-PSK, WPA2 PSK or OPEN mode is configured.

Note: here wireless can be configured as Registrar and Enrolee mode respectively. When AP is configured as Registrar, you should select Configured in the WPS AP Mode below, and default WPS AP Mode is Configured. When AP is configured as Enrolee, the WPS AP Mode below should changed to Unconfigured. Follow the following steps.

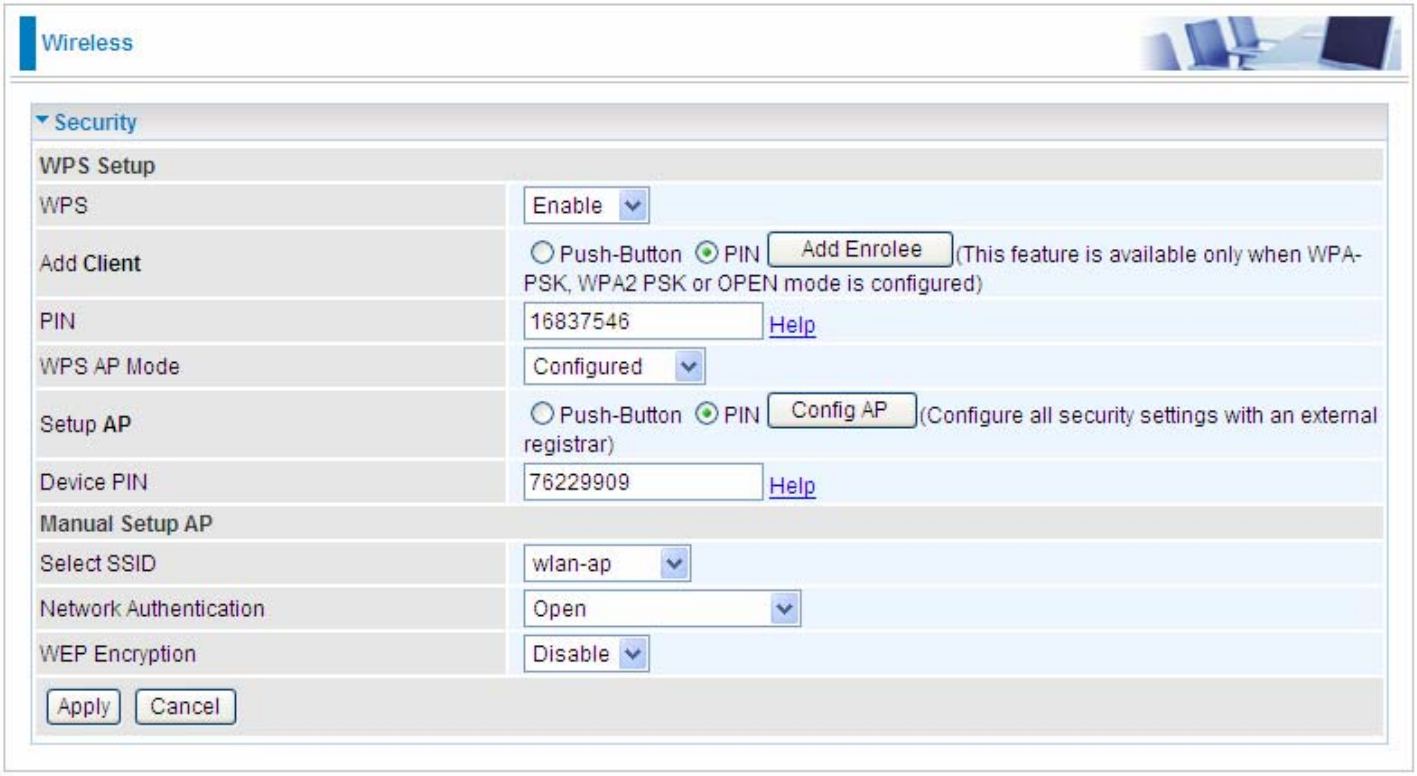


Configure AP as Registrar

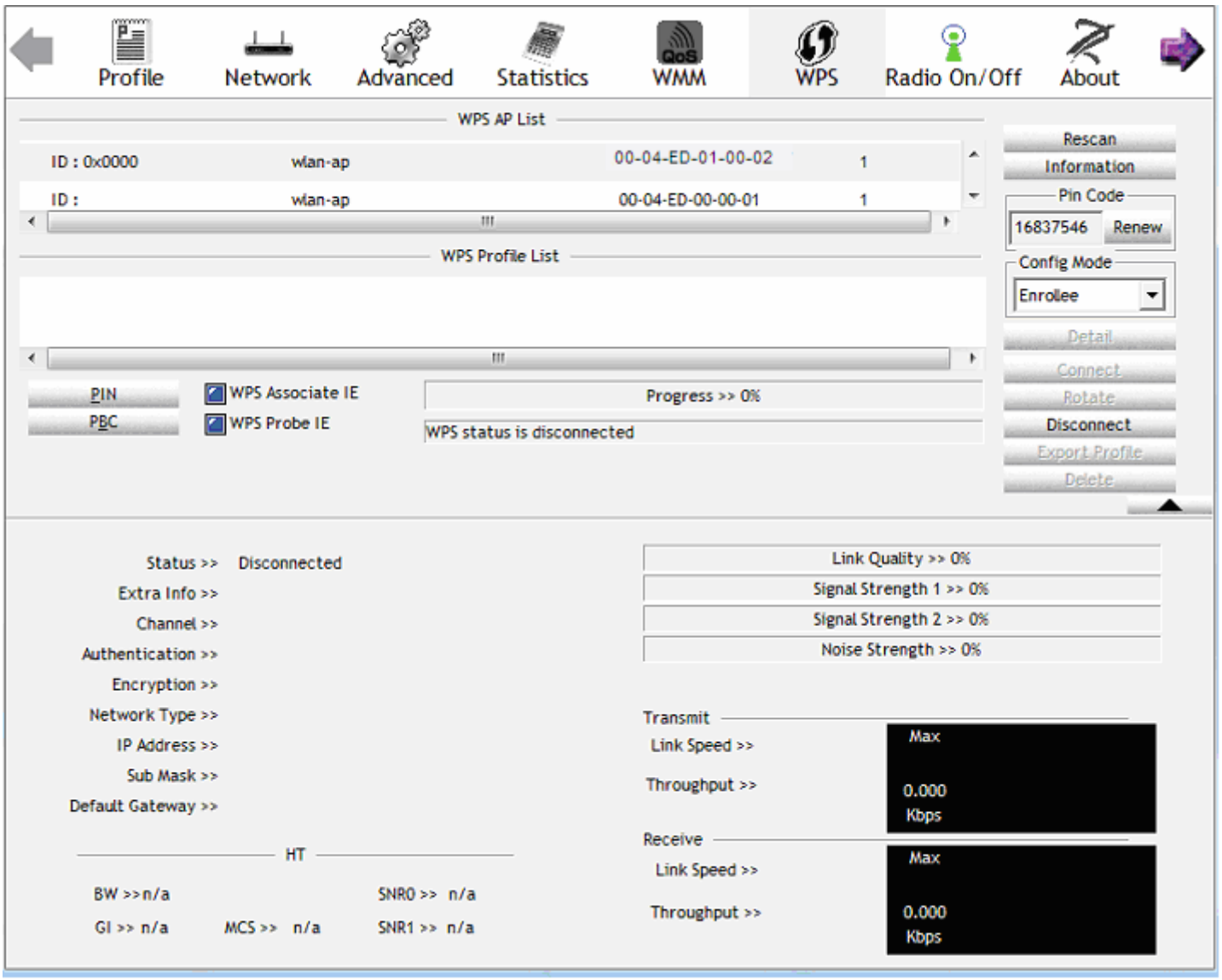
Add Enrollee with PIN method

1. select radio button ‘PIN’.
2. Input PIN from Enrollee Station (16837546 in this example). Help: it is to help users to understand PIN.

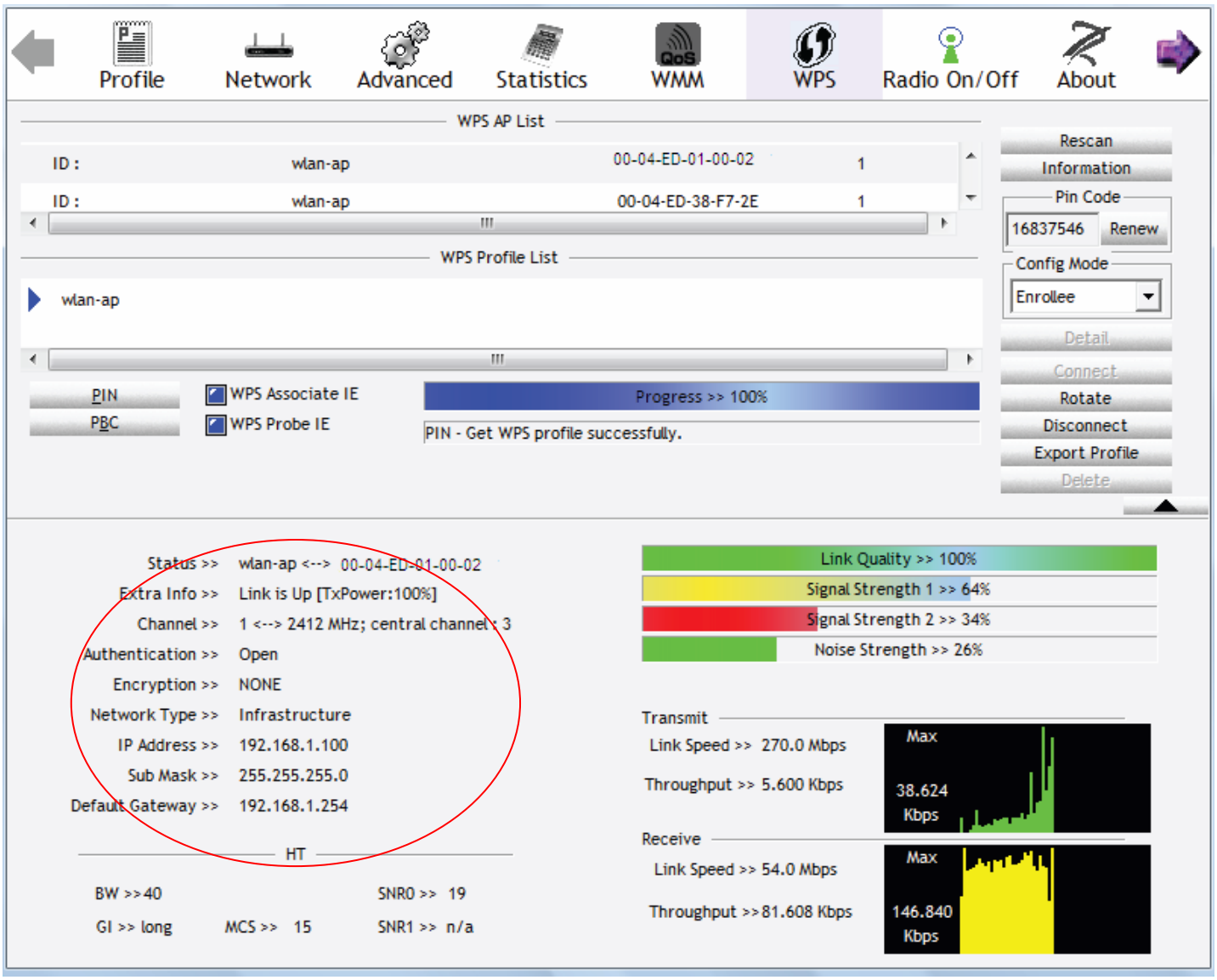
3.Click Add Enrolee.



3. Operate Station to start WPS Adding Enrollee. Launch the wireless client's WPS utility (eg.Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



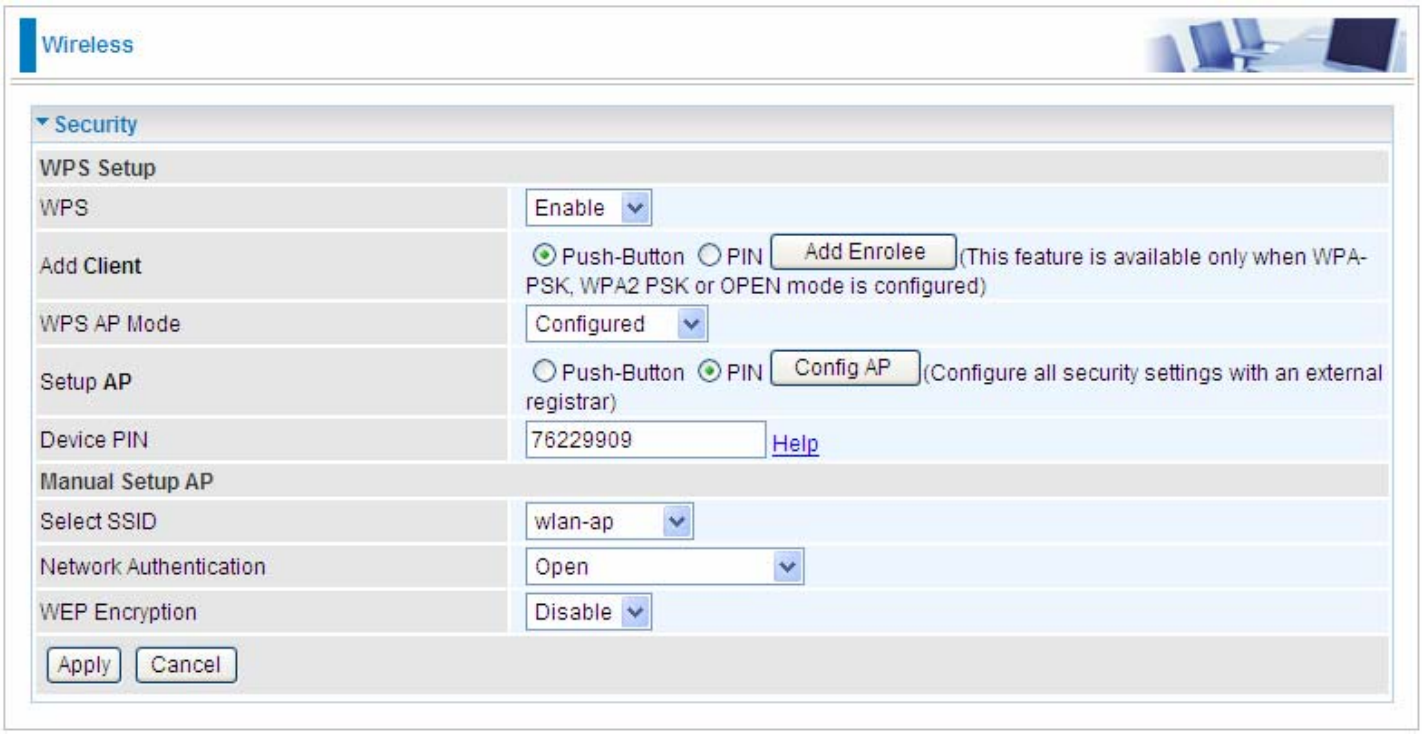
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.



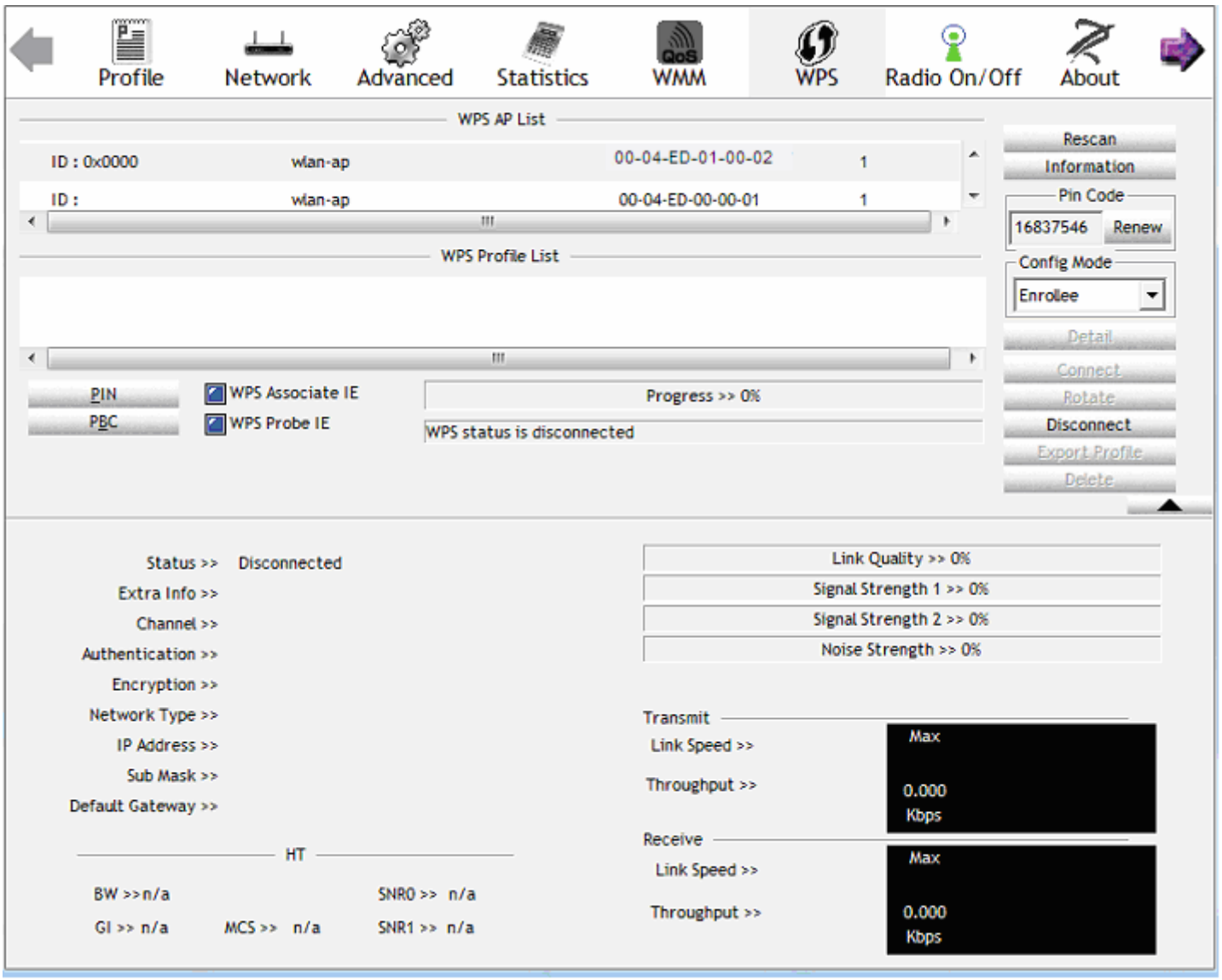
You can check the message in the red ellipse with the security parameters you set, here we all use the default.

Add Enrollee with PBC Method

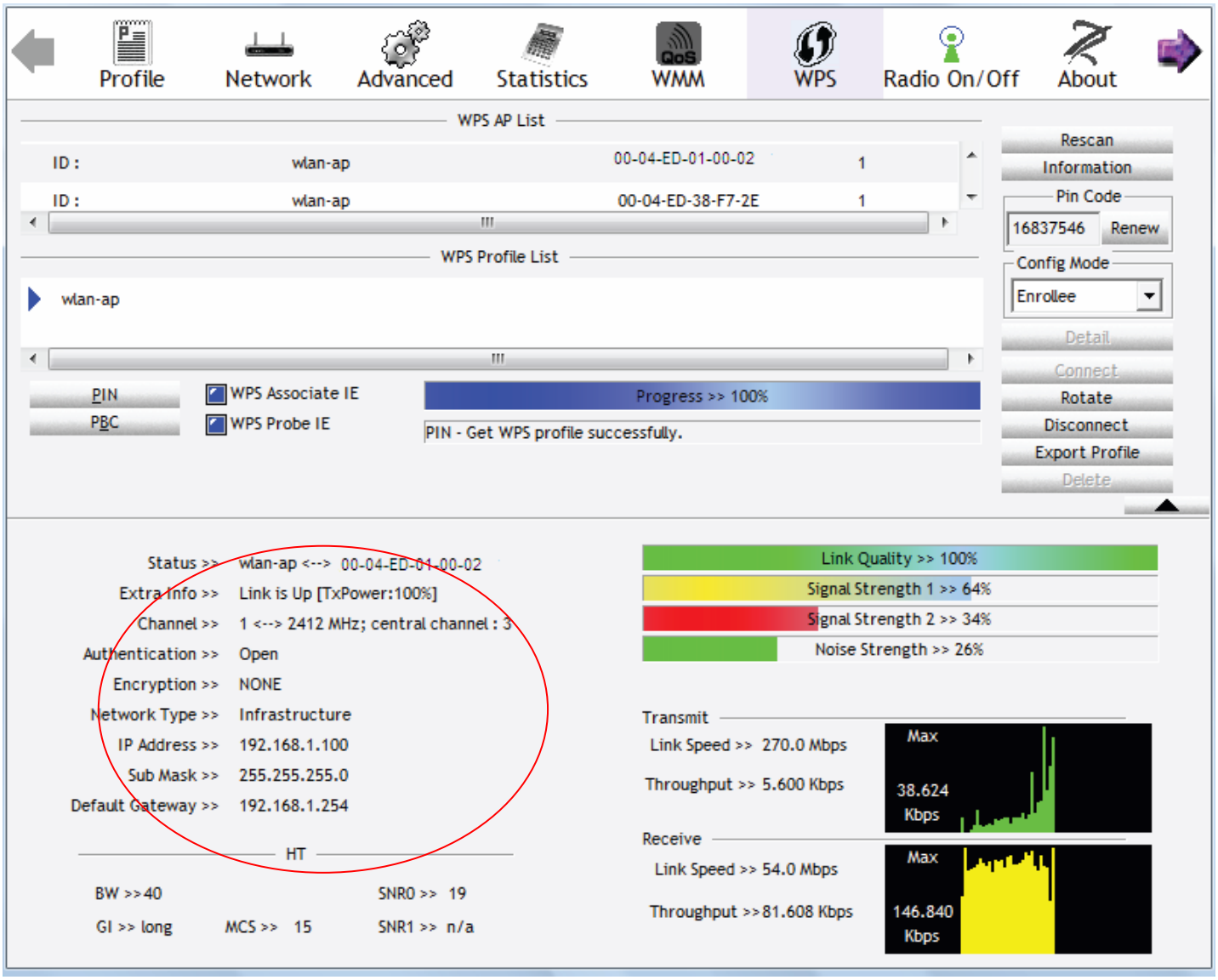
1. Select radio button “Push-Button” and Click Add Enrolee Or Press the physical button on router.



2. Operate Station to start WPS Adding Enrollee. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.



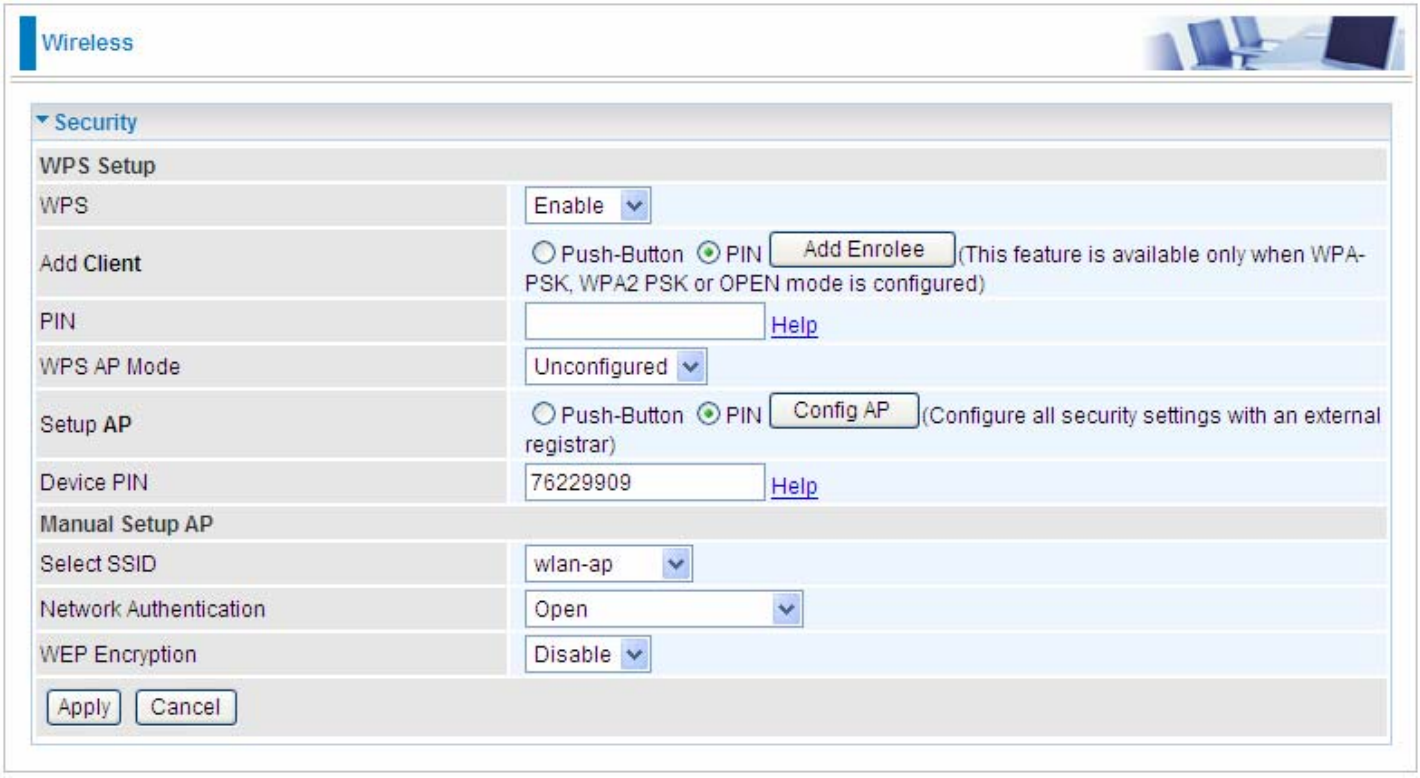
3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



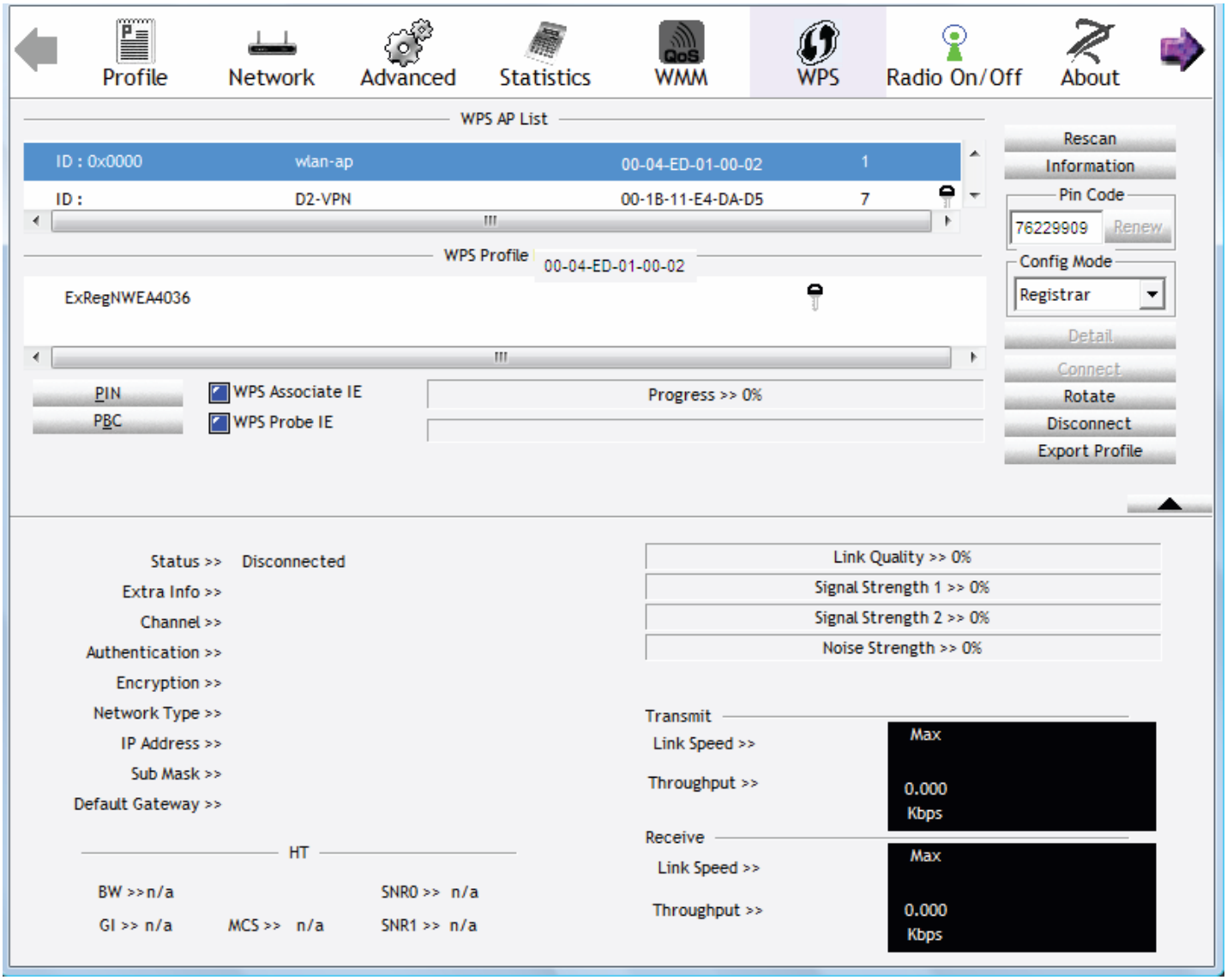
Configure AP as Enrollee

Add Registrar with PIN Method

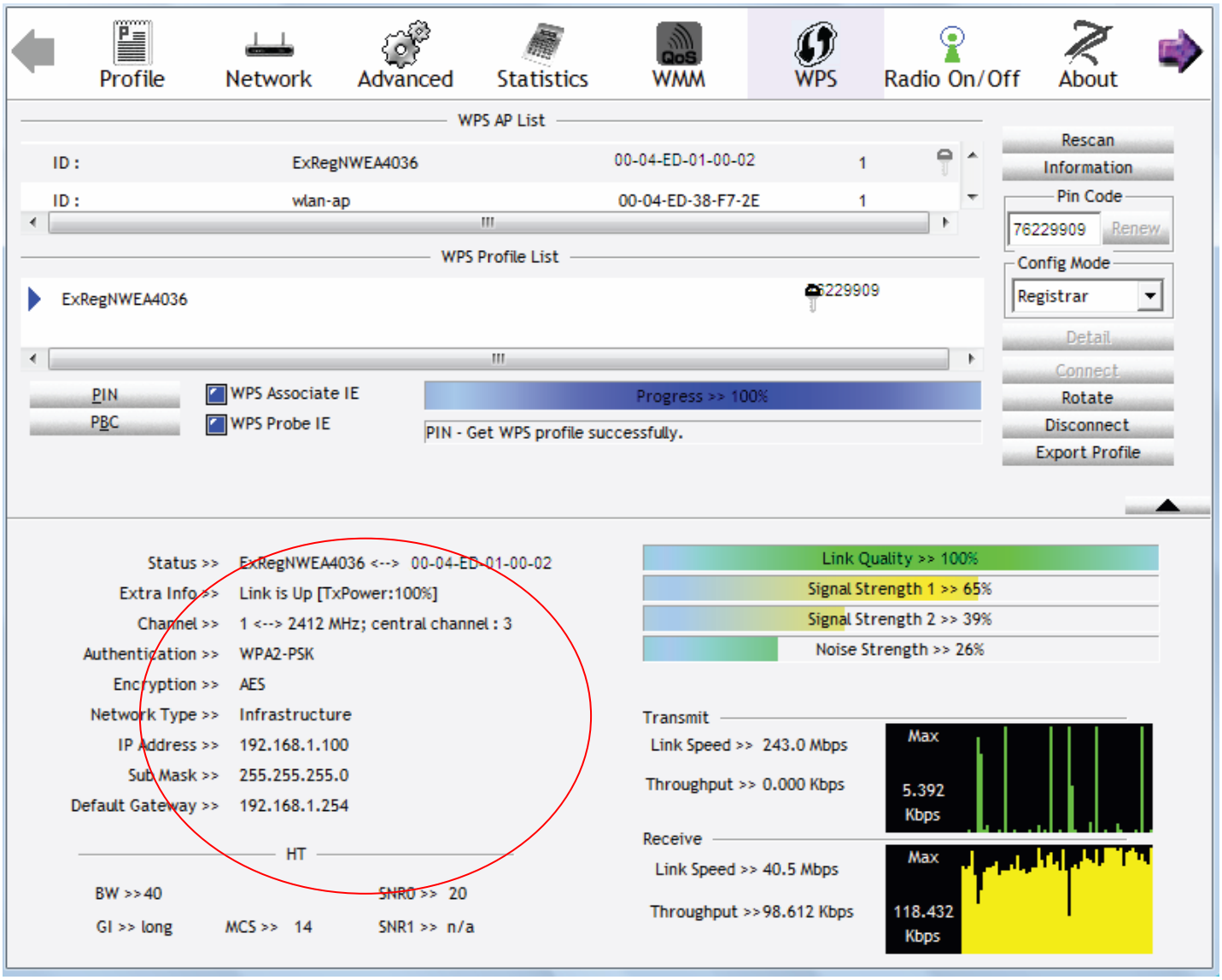
1. Set AP to “Unconfigured Mode” and Click “Config AP” button.



2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number (76229909 for example) in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

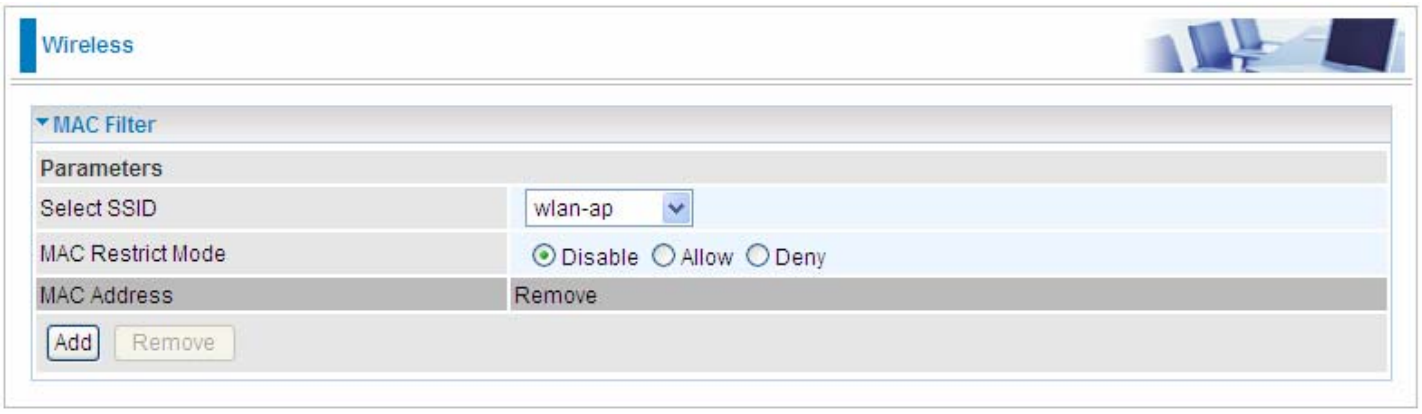


3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

MAC Filter

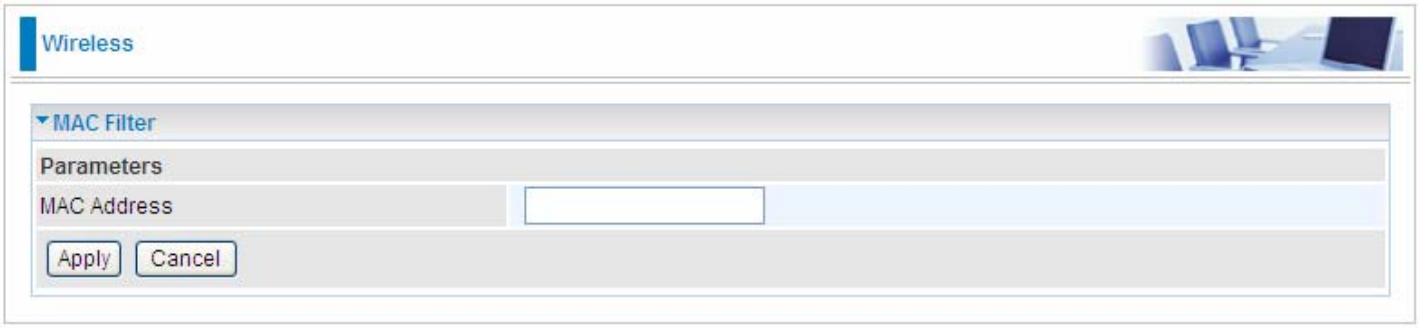


Select SSID: select the SSID you want this filter applies to.

MAC Restrict Mode:

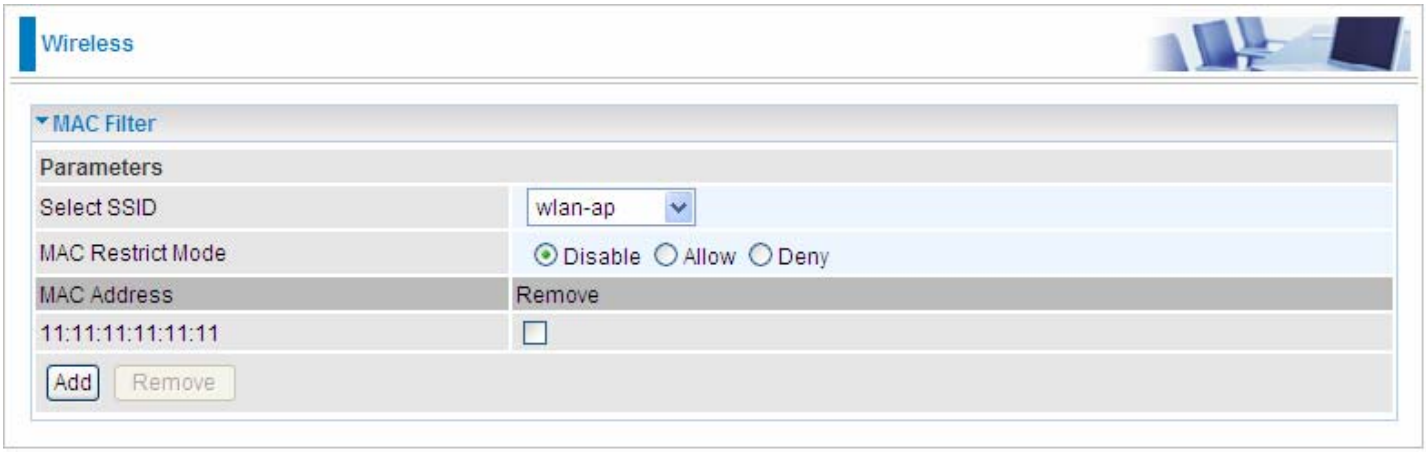
- **Disable:** disable the MAC Filter function.
- **Allow**: allow the hosts with the following listed MACs to access the wireless network.
- **Deny**: deny the hosts with the following listed MACs to access the wireless network.

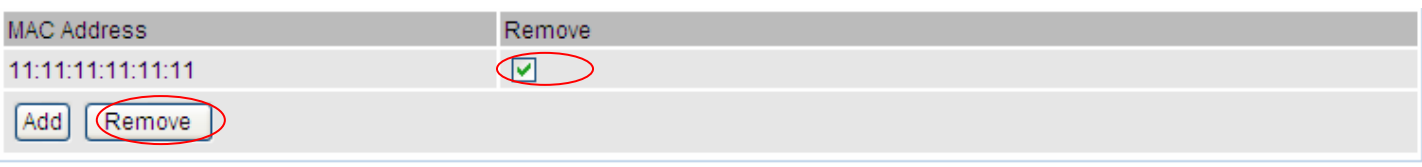
Click **Add** to add the MACs.



MAC Address: enter the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click **Apply** to apply your settings and the item will be listed below.



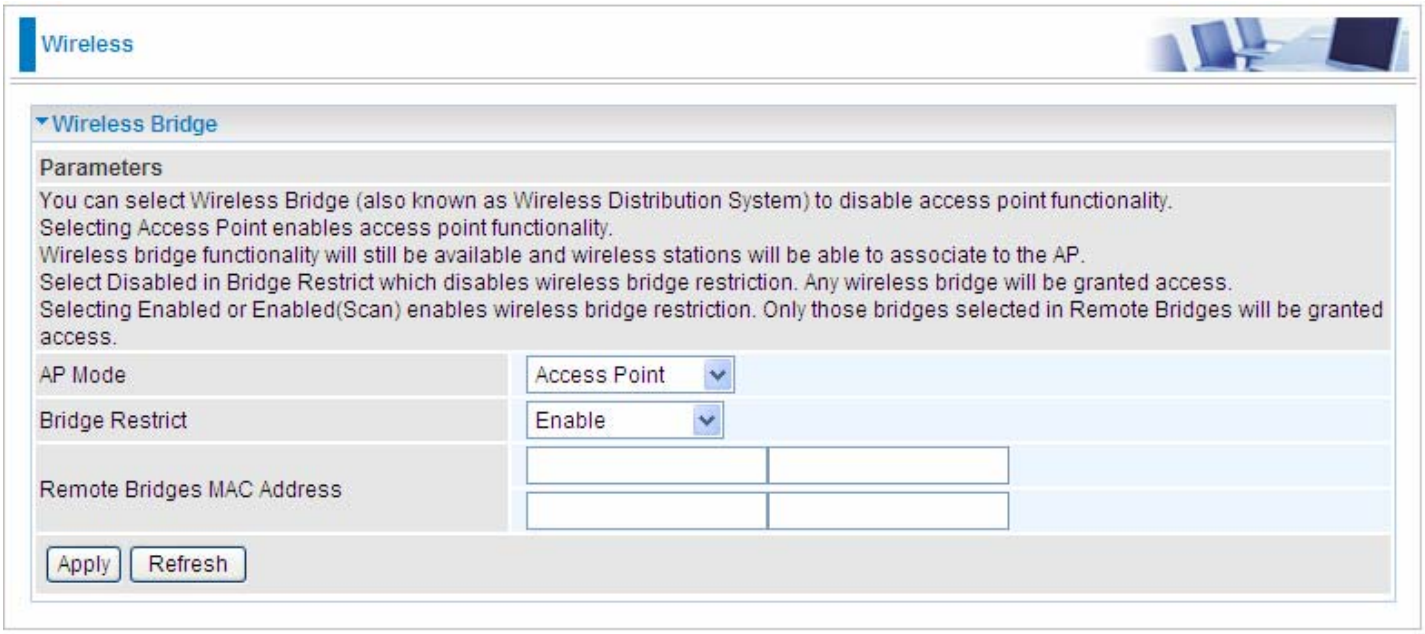


If you need not the rules, check the remove checkbox and press **Remove** to delete it.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, simply define the peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Here you can select to decide what role the AP servers as, AP or wireless bridge (WDS).



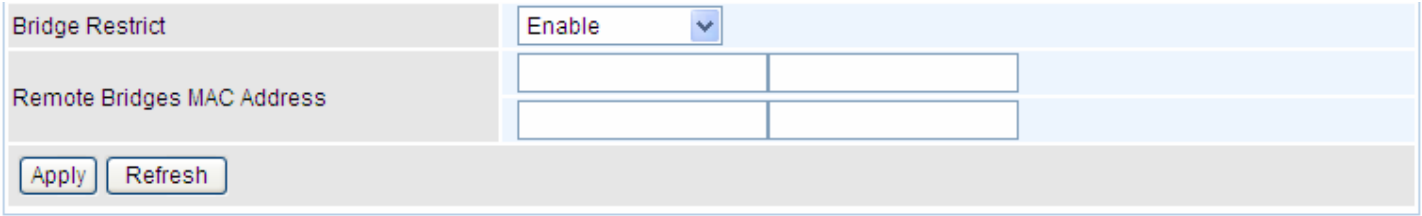
AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- **Access Point**: the gateway communicates with both clients and bridges.
- **Wireless Bridge**: the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

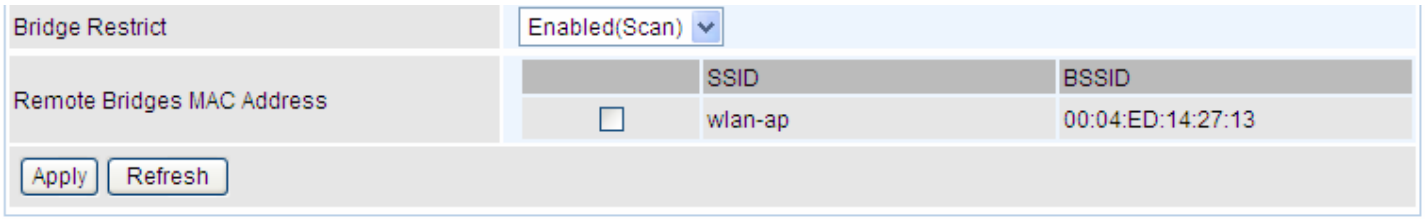
Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

- **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.



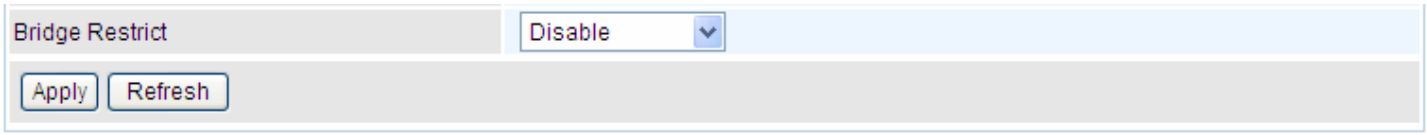
Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

ⓘ **Enabled (Scan):** to enable wireless bridge restriction. Only those been scanned the gateway can communicate with.



Remote Bridge MAC Address: select the remote bridge MAC addresses.

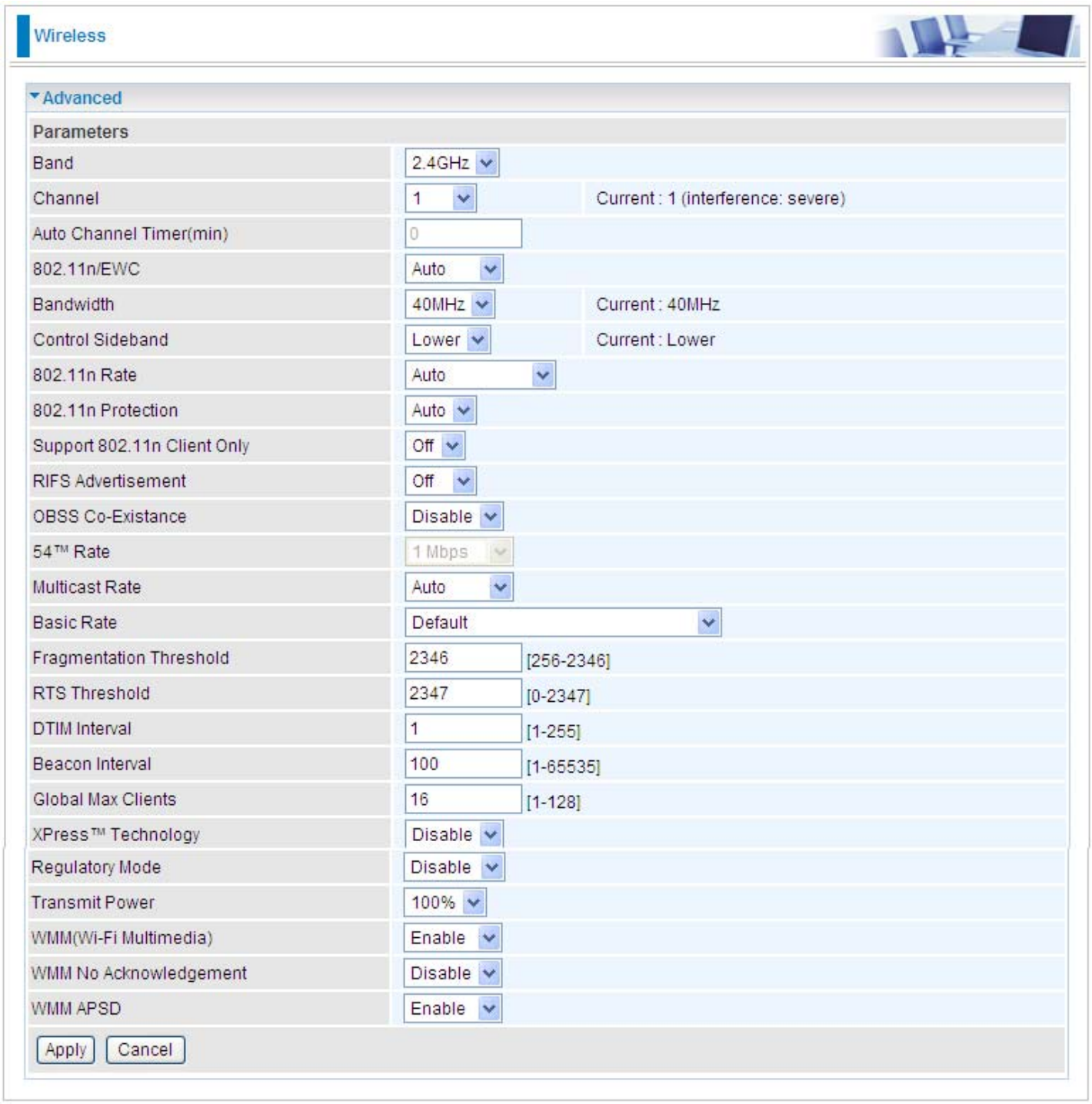
ⓘ **Disable:** Does not restrict the gateway to communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.



Click **Apply** to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.



Band: select frequency band. Here 2.4GHZ.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

Auto Channel Timer(min): the auto channel times length it takes to scan in minutes. Only available for auto channel mode.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: It allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximized throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option is to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existance: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a certain kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Regulatory Mode: select to deny any regulatory mode. There are two regulatory modes:

802.11h: The standard solves interference problems with e.g. satellites and radar using the same 5 GHz band as 802.11a or 802.11n dual-band access points.

802.11d: This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.
This means that manufacturers don't need to make country specific products.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view the information about the wireless clients.

MAC Address: the MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access**.**

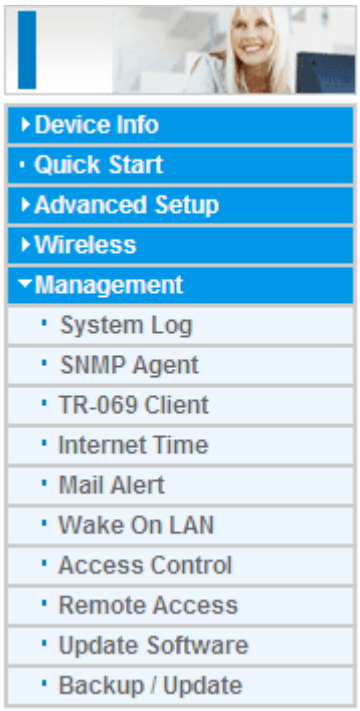
SSID: show the current SSID of the client.

Interface: to show which interface the wireless client is connected to.

Refresh: to get the latest information.

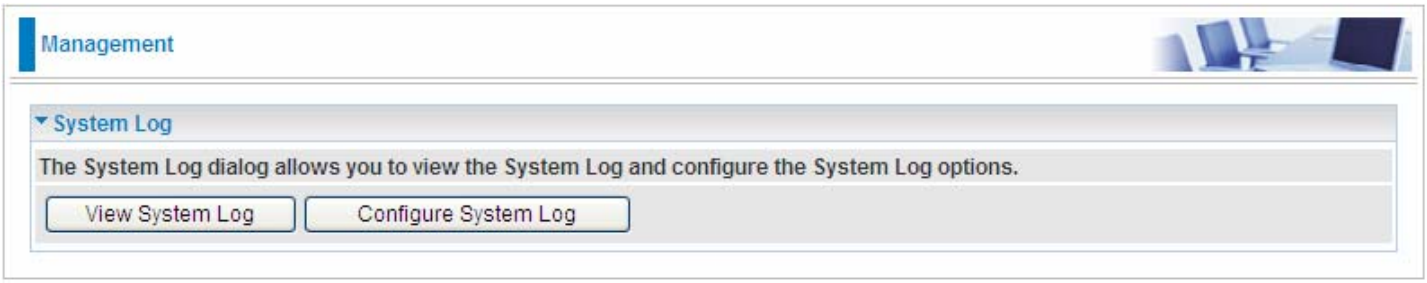
Management

There are 9 items within the System section: **System Log**, **SNMP Agent**, **TR-069 Client, Internet Time**, **Mail Alert, Wake on LAN, Access Control, Remote Access**, **Update Software** and **Backup/Update.**

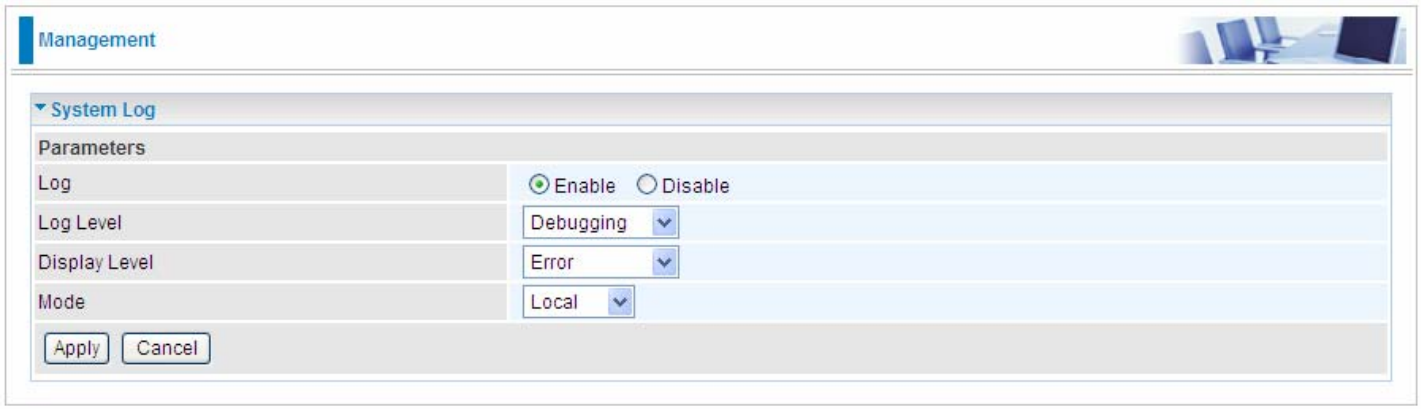


System Log

To let users view or configure System Log.



Click Configure System Log to configure the log.



Log: enable or disable this function.

Log level: select your log level. The log level allows you to configure which types of events are loged. There are eight log levels from high to low are displayed below:

- **Emergency** = system is unusable (these appear in red in the log)
- **Alert** = action must be taken immediately (pale red)
- **Critical** = critical conditions (orange)
- **Error** = error conditions (yellow)
- **Warning** = warning conditions (green)
- **Notice** = normal but significant conditions (blue)
- **Informational** = information events (white)
- **Debugging** = debug-level messages (dark grey on cream)

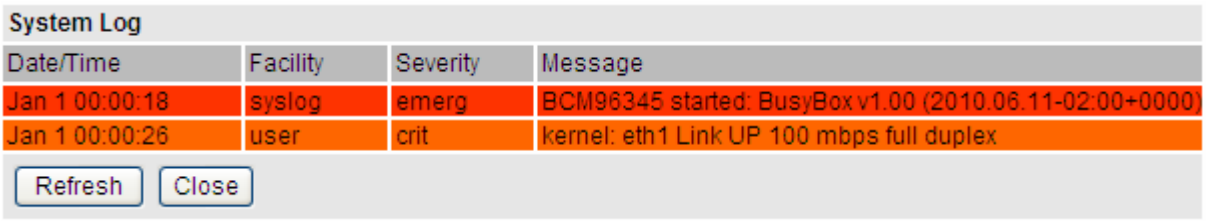
The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: select the mode the system log adopted. Three modes: local, Remote and Both.

- **Local**: select this mode to store the logs in the router's local memory.
- **Remote**: select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- **Both**: logs stored adopting above two ways.

Click View System Log to see the System log of this router. The logs will be listed as configured above. Click **refresh** to get the latest information.



Click **Apply** to save your settings.

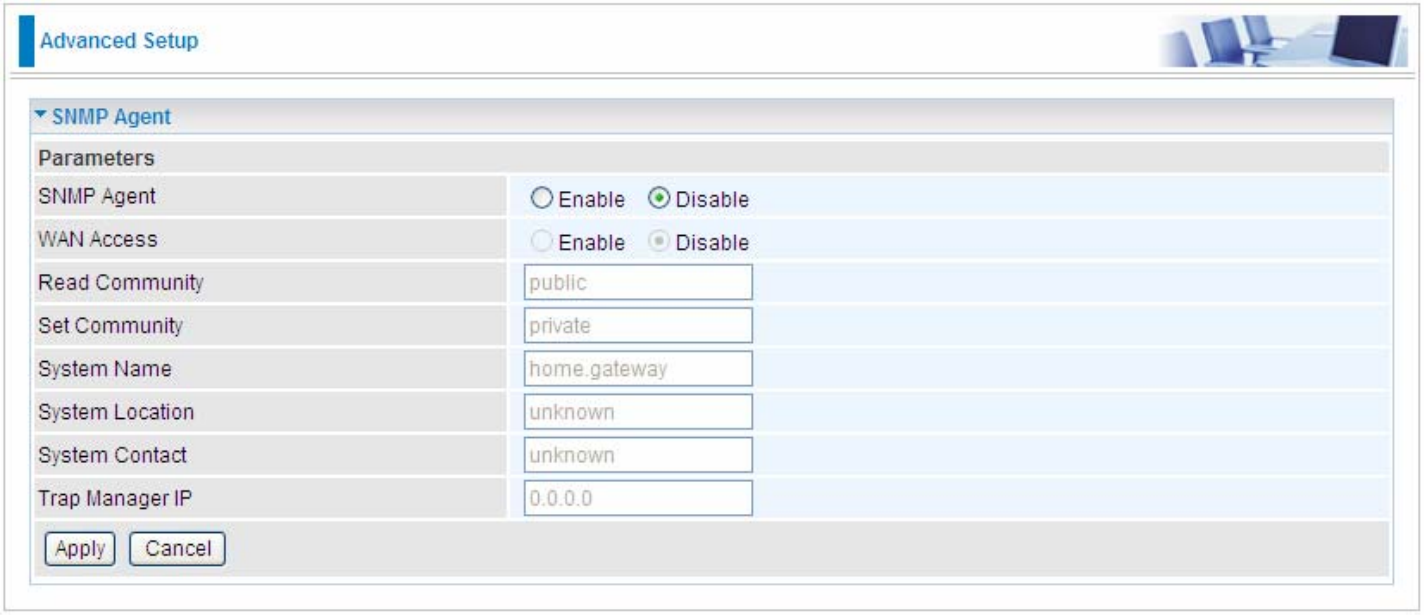
SNMP Agent

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 the server, is to use 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.



SNMP Agent: enable or disable SNMP Agent.

WAN Access: enable or disable WAN access which allows PCs in WAN side read or set the SNMP related MIB pamareters.

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.

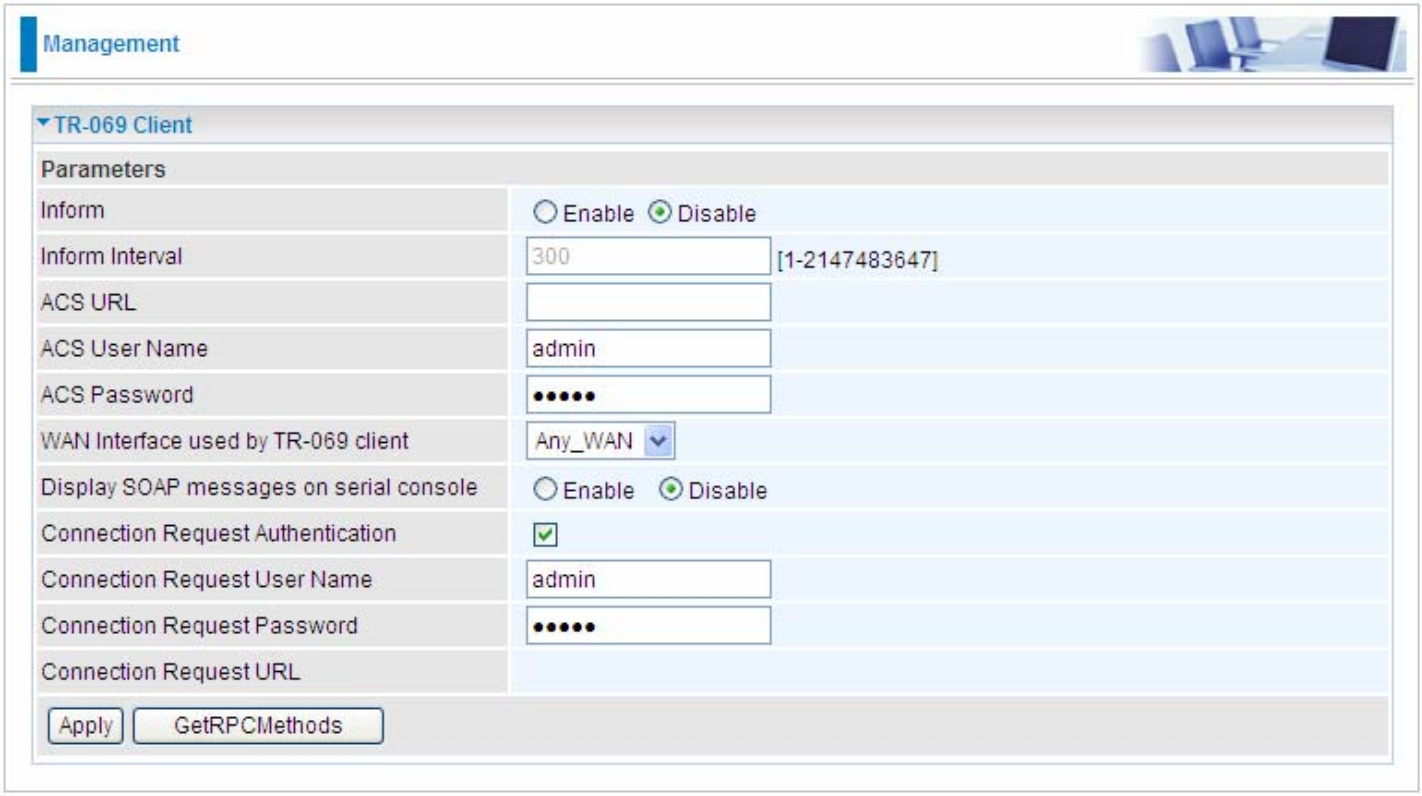
System Contact: user-defined contact message.

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. 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.



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.

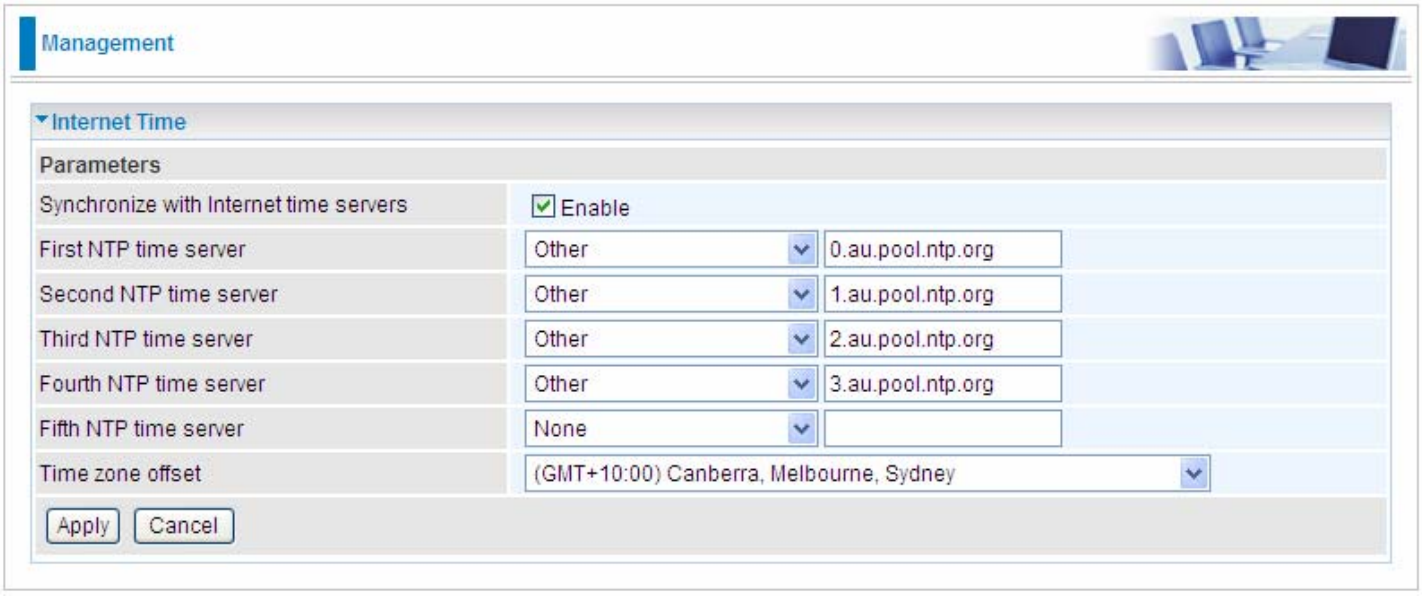
GetRPCMethods： supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



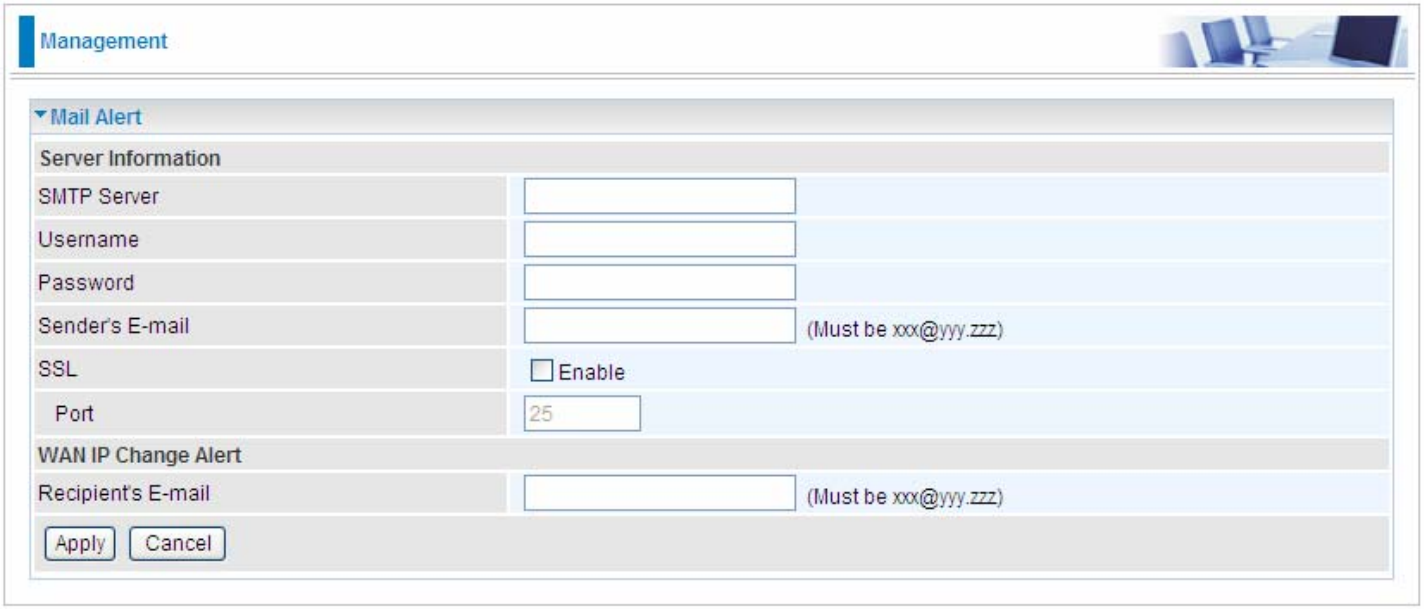
Choose the NTP time server from the drop-down menu, If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to apply your settings.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnels alerted of any unexpected events that might have occured to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

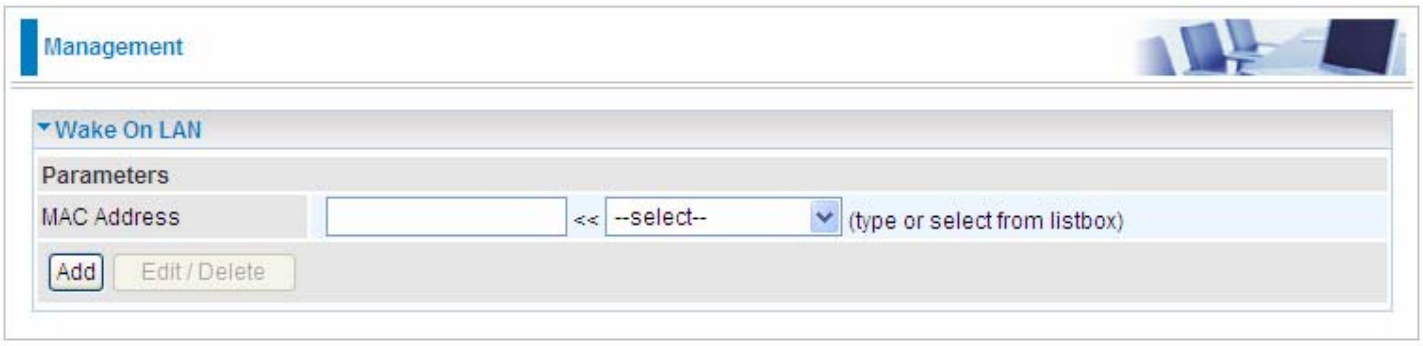
SSL: check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once an WAN IP change has been detected.

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.



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.

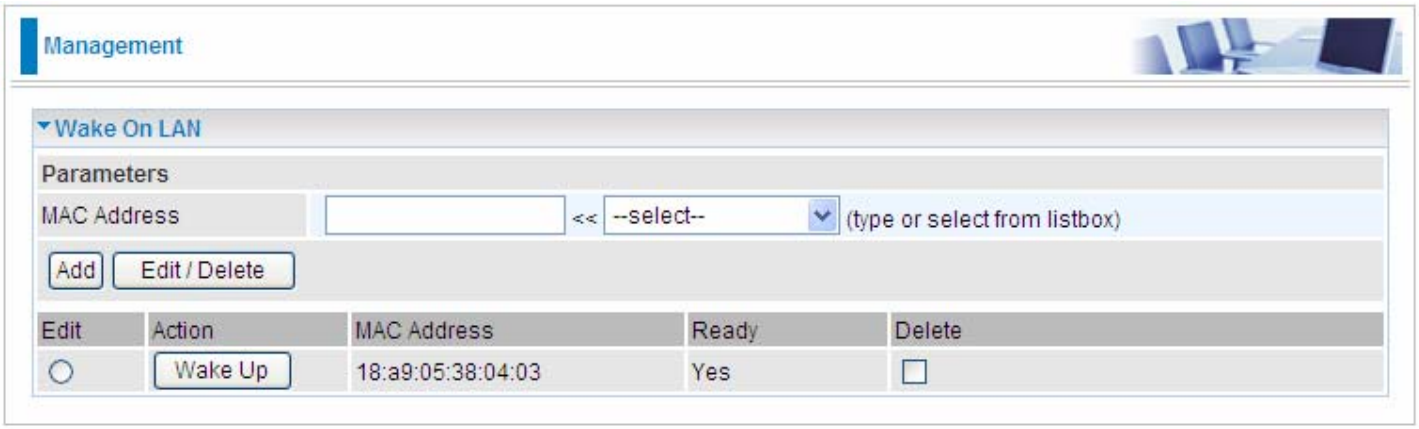
Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

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

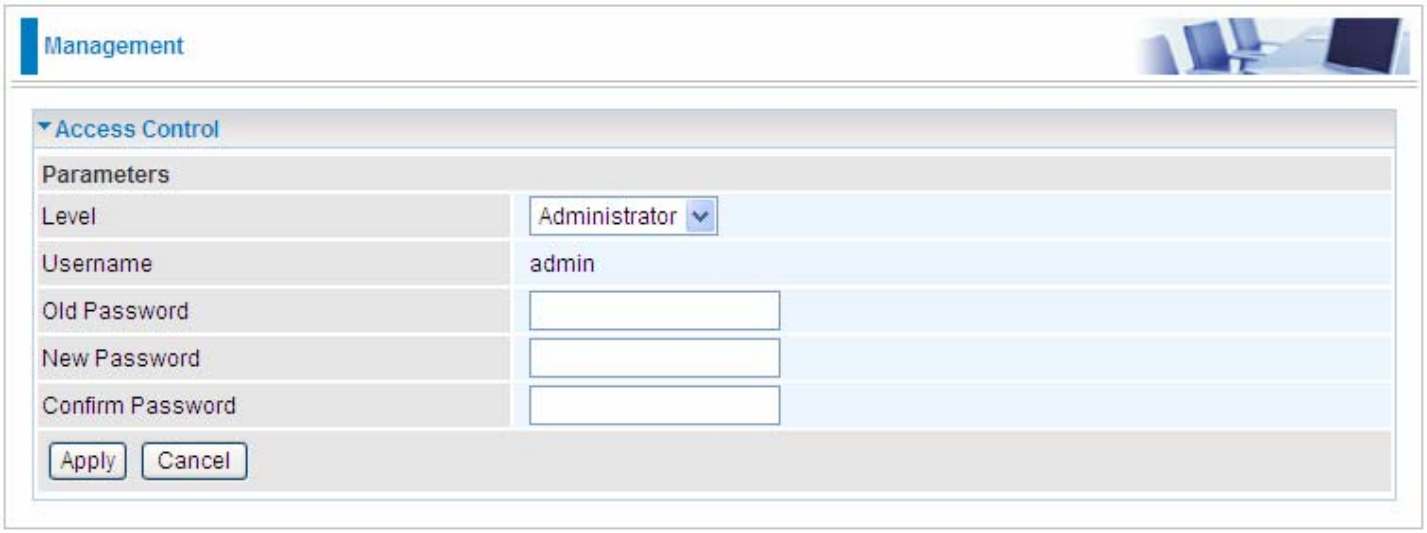
"No" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.



Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.



Level: select which level you want to change password to. There are three default levels.

- **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- **Remote:** username for the remote user to login, corresponding default username and password are support and support respectively.
- **Local:** username for the general user, corresponding default username password are user and user respectivley.

Username: the default username for each user level.

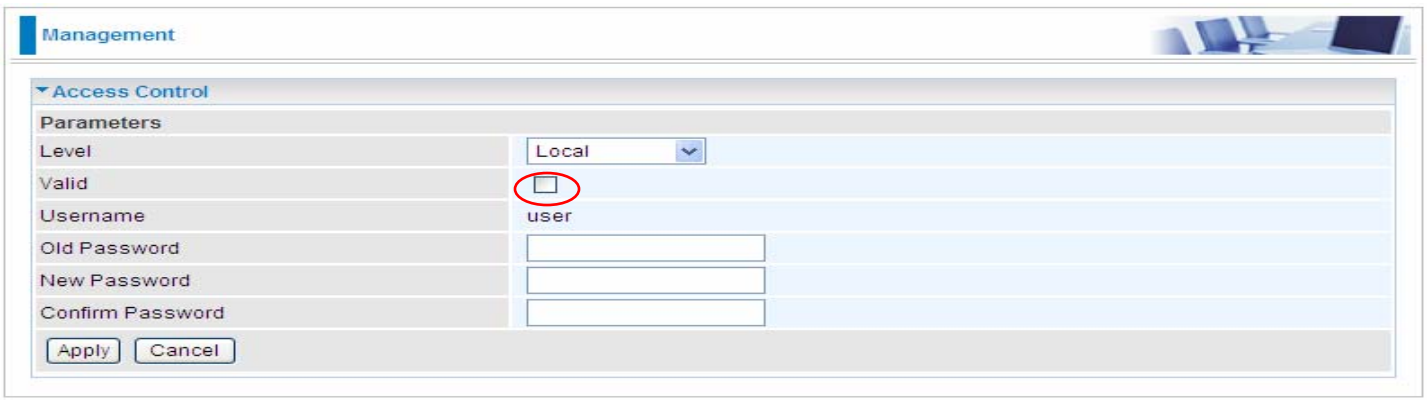
Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

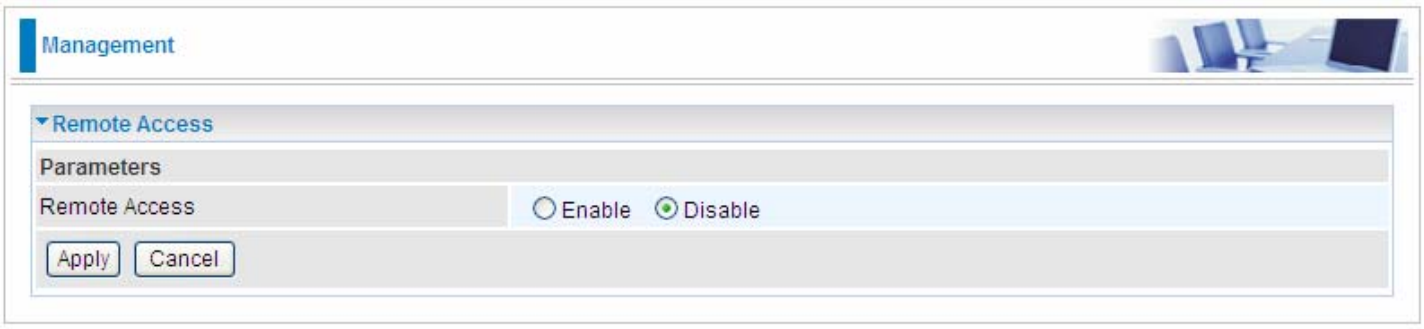
Click **Apply** to apply your new settings.

Note: by default the other two users of level Local and level Remote, thus user and support, are not available, if you want to use the two accounts, check **Valid** and set their passwords.



Remote Access

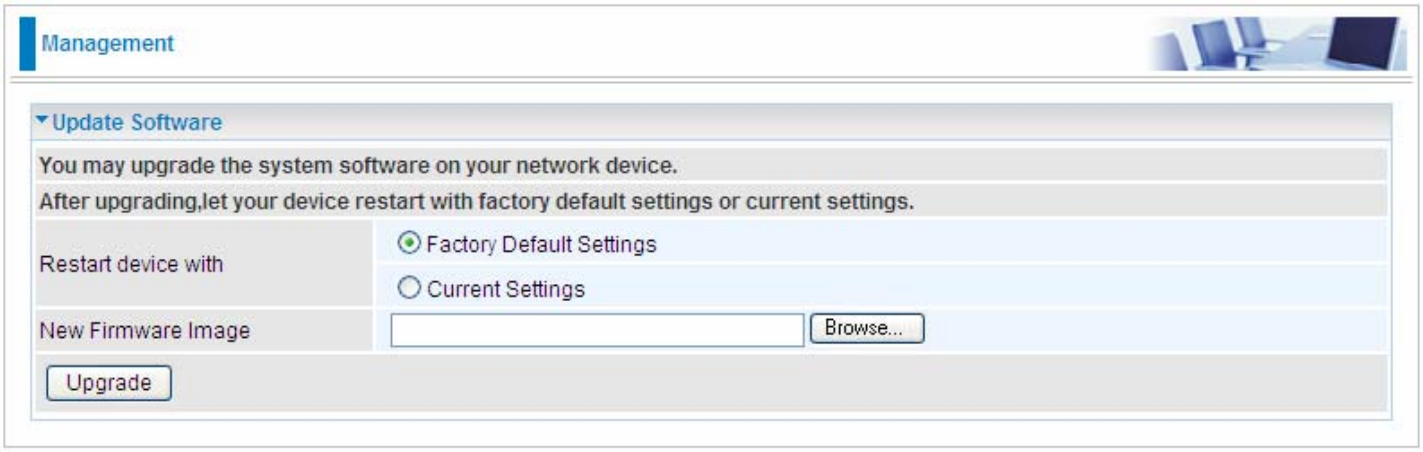
It is to allow remote access to the router to view or configure.



Remote: Select to enable or disable Remote Access functionality.

Update Software

Software upgrading lets you experience the new and integral function of your router.



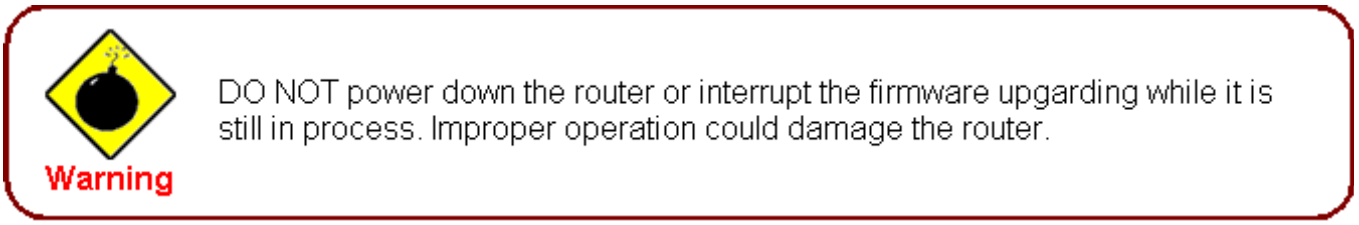
Restart device with:

- **Factory Default Settings:** Restart the device with factory default settings automatically when finished upgrading.
- **Current Settings:** Restart the device with the current settings automatically when finished upgrading.

Your router's "firmware" is the software that allows it to operate and provides all its functionality.

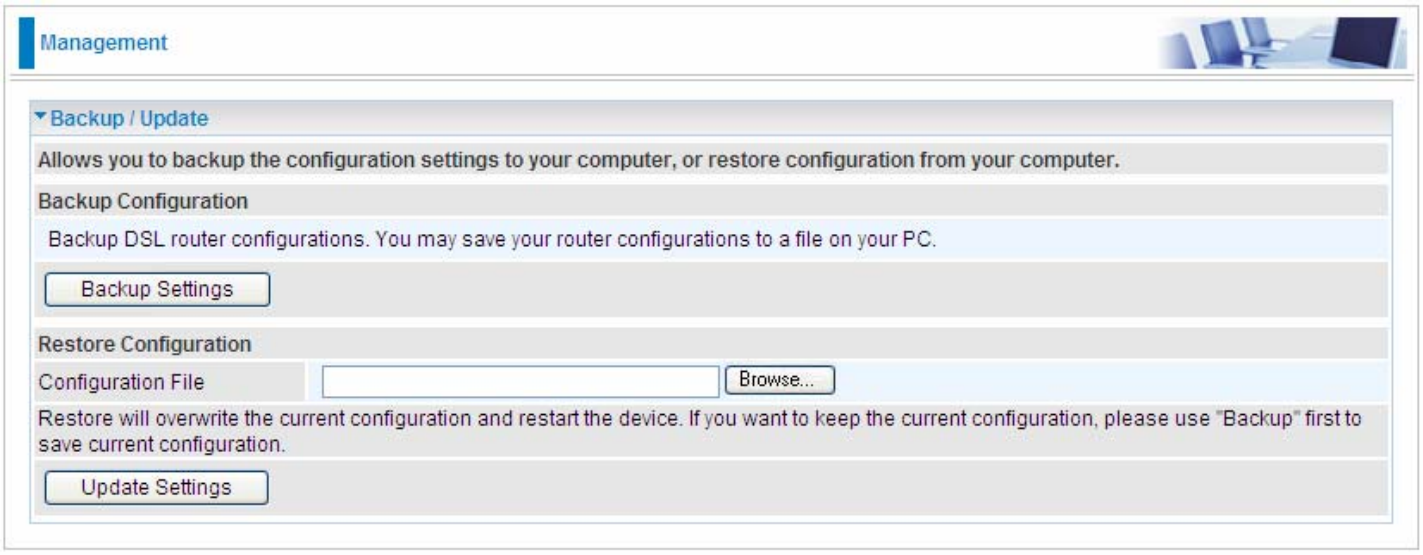
Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click **Upgrade** to update the firmware in your router.



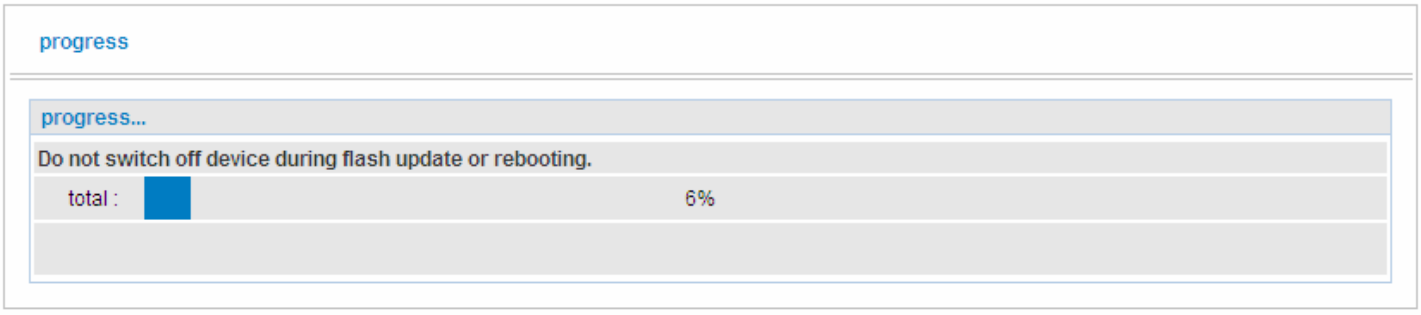
Backup / Update

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.



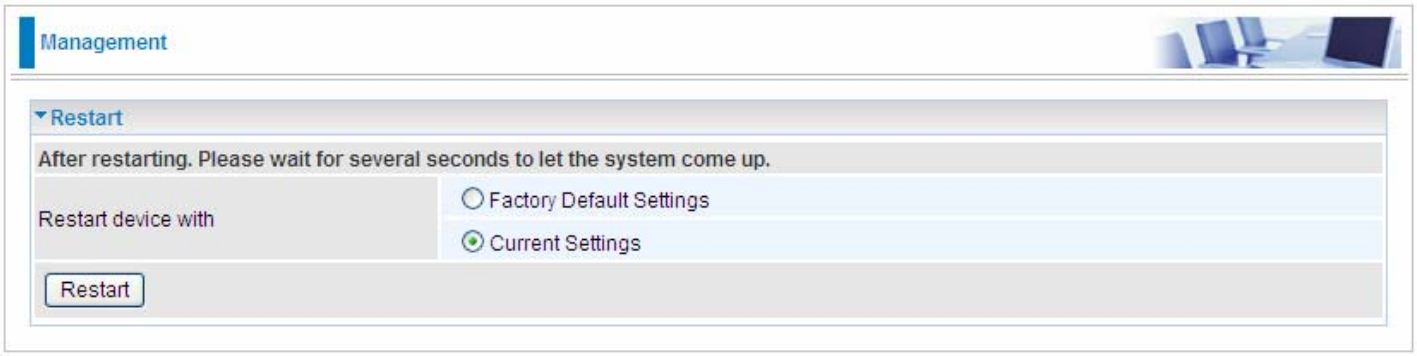
Click **Backup Settings**, a window appears, click save , then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open.** Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.

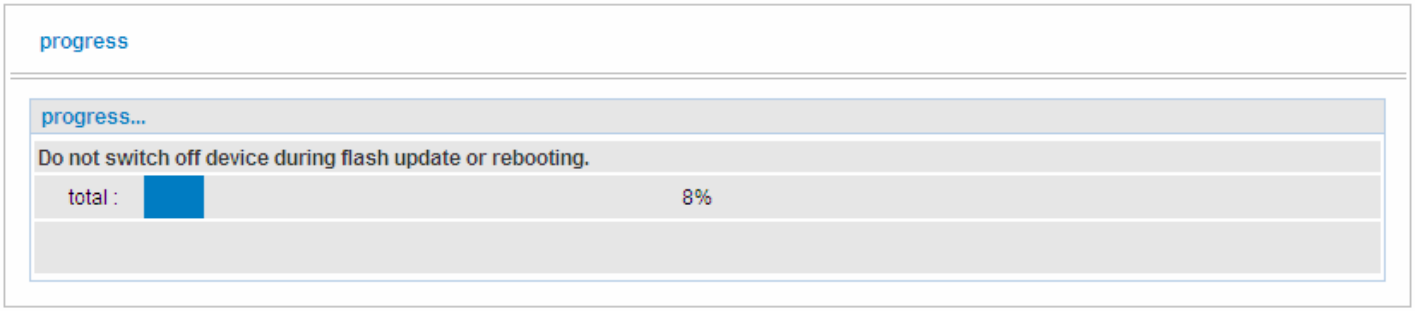


Restart

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



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.



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
None of the LEDs is on when you turn on the router	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.
You have forgotten your login username or password	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
Frequent loss of ADSL line sync (disconnections)	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
Cannot PING any PC on LAN	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

FCC statement in the User's Manual (for class B)
"Federal Communication Commission (FCC) 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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. There is not guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio and television reception, which can be determined by turning on and off, 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 the receiver
- Connect the equipment into a outlet on a circuit different from that to which the received is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

1. The device complies with Part 15 of the FCC rules. Operations is subject to the following two conditions:
   (1) The device may not cause harmful interference, and
   (2) this device must accept any interference received, including interference that may cause undesired operation.

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

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOT:
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.

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.