

5.5.4 IP Address Map

Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).

The screenshot shows the COMTREND ADSL Router web interface. The main content area is titled "NAT -- IP Address Mapping Setup". It contains a table with the following headers: Rule, Type, Local Start IP, Local End IP, Public Start IP, Public End IP, and Remove. Below the table are two buttons: "Add" and "Remove".

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP	Remove
------	------	----------------	--------------	-----------------	---------------	--------

Buttons: Add, Remove

Consult the table below for field and header descriptions.

Field/Header	Description
Rule	The number of the rule
Type	Mapping type from local to public.
Local Start IP	The beginning of the local IP
Local End IP	The ending of the local IP
Public Start IP	The beginning of the public IP
Public End IP	The ending of the public IP
Remove	Remove this rule

Click the Add button to display the following screen.

COMTREND ADSL Router

NAT -- IP Address Mapping Setup
Remaining number of entries that can be configured:32

Server Name:

Select a Service: One to One

Local Start IP	Local End IP	Public Start IP	Public End IP
	0.0.0.0		0.0.0.0

Save/Apply

Select a Service, then click the Save/Apply button.

One to One: mapping one local IP to a specific public IP

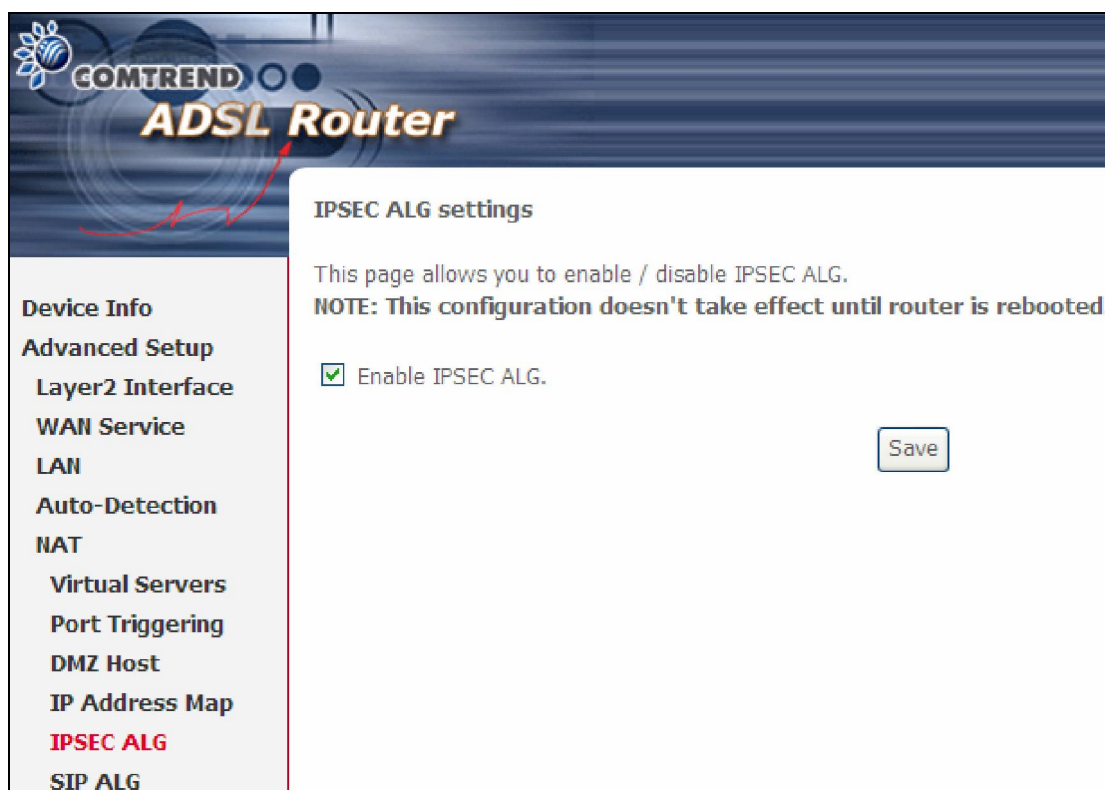
Many to One: mapping a range of local IP to a specific public IP

Many to Many(Overload): mapping a range of local IP to a different range of public IP

Many to Many(No Overload): mapping a range of local IP to a same range of public IP

5.5.5 IPSEC ALG

IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.

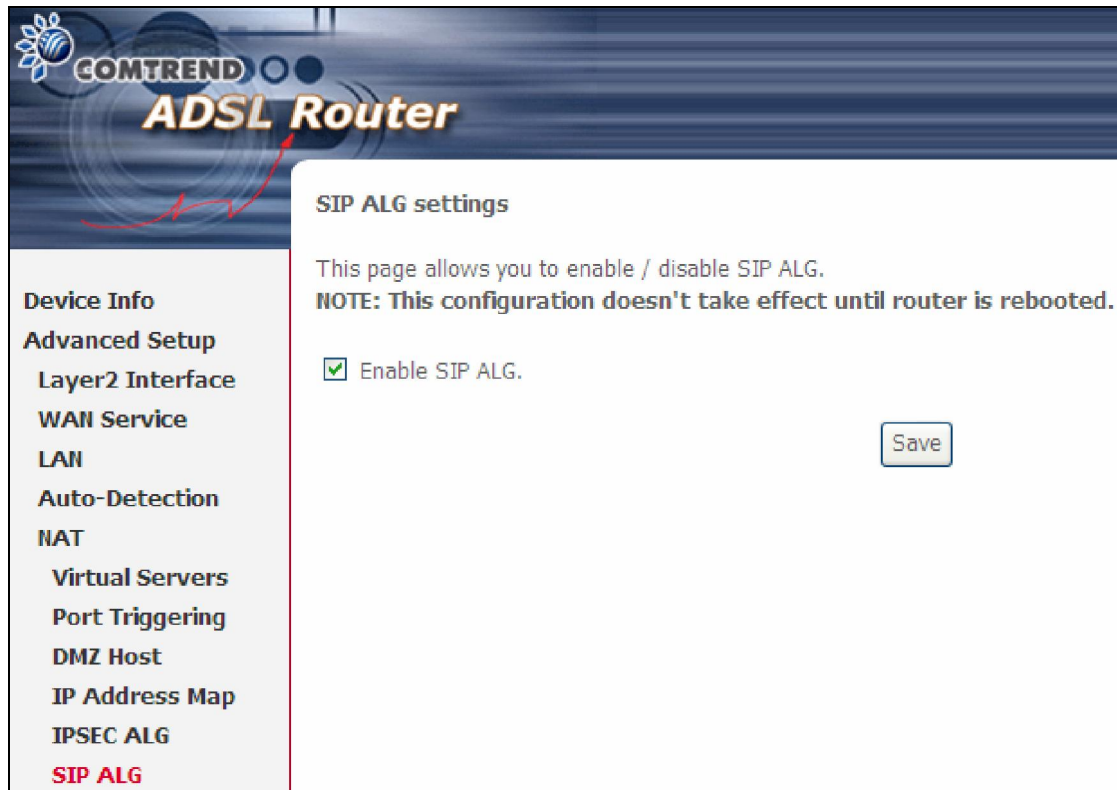


The screenshot displays the web management interface of a Comtrend ADSL Router. The top banner features the Comtrend logo and the text "ADSL Router". On the left side, there is a vertical navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, **IPSEC ALG** (highlighted in red), and SIP ALG. The main content area is titled "IPSEC ALG settings" and contains the following text: "This page allows you to enable / disable IPSEC ALG." followed by a bolded note: "NOTE: This configuration doesn't take effect until router is rebooted." Below this text is a checked checkbox labeled "Enable IPSEC ALG." and a "Save" button.

To enable IPSEC ALG, tick the checkbox and click the Save button.

5.5.6 SIP ALG

This page allows you to enable / disable SIP ALG.



The screenshot shows the configuration interface of a Comtrend ADSL Router. The top banner features the Comtrend logo and the text "ADSL Router". On the left, a vertical navigation menu lists various settings: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG, and SIP ALG (highlighted in red). The main content area is titled "SIP ALG settings" and contains the following text: "This page allows you to enable / disable SIP ALG." followed by a bolded note: "NOTE: This configuration doesn't take effect until router is rebooted." Below this, there is a checked checkbox labeled "Enable SIP ALG." and a "Save" button.

5.6 Security

To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions, with examples, please consult [Appendix A - Firewall](#).

5.6.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE: This function is not available when in bridge mode. Instead, [5.6.2 MAC Filtering](#) performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.

Filter Name	IP Version	Protocol	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
-------------	------------	----------	--------------------	---------	--------------------	---------	--------

To add a filter (to block some outgoing IP traffic), click the **Add** button. On the following screen, enter your filter criteria and then click **Apply/Save**.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.

The screenshot shows the 'Incoming IP Filtering Setup' page on a Comtrend ADSL Router. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, IP Filtering (with sub-items Outgoing and Incoming), and MAC Filtering. The main content area has the title 'Incoming IP Filtering Setup' and the following text: 'When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters. Choose Add or Remove to configure incoming IP filters.' Below this text is a table with the following columns: Filter Name, Interfaces, IP Version, Protocol, Action, ICMP Type, SrcIP/PrefixLength, SrcPort, DstIP/PrefixLength, DstPort, and Remove. At the bottom of the table area are two buttons: 'Add' and 'Remove'.

To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	Permit/Drop packets specified by the firewall rule.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

5.6.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use [5.6.1 IP Filtering](#) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the AR-5389 can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.

COMTREND ADSL Router

MAC Filtering Setup

MAC Filtering is only effective on WAN services configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm0.2	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.

Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface.

5.7 Parental Control

This selection provides WAN access control functionality.

5.7.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in [8.5 Internet Time](#), so that the scheduled times match your local time.

COMTREND ADSL Router

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
----------	-----	-----	-----	-----	-----	-----	-----	-----	-------	------	--------

Click **Add** to display the following screen.

COMTREND ADSL Router

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address

Days of the week

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

See below for field descriptions. Click **Apply/Save** to add a time restriction.

- User Name:** A user-defined label for this restriction.
- Browser's MAC Address:** MAC address of the PC running the browser.
- Other MAC Address:** MAC address of another LAN device.
- Days of the Week:** The days the restrictions apply.
- Start Blocking Time:** The time the restrictions start.
- End Blocking Time:** The time the restrictions end.

5.7.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

Select URL List Type: Exclude or Include. Then click **Add** to display the following screen.

Enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
www.yahoo.com	80	<input type="checkbox"/>

A maximum of 100 entries can be added to the URL Filter list.
Tick the **Exclude** radio button to deny access to the websites listed.
Tick the **Include** radio button to restrict access to only those listed websites.

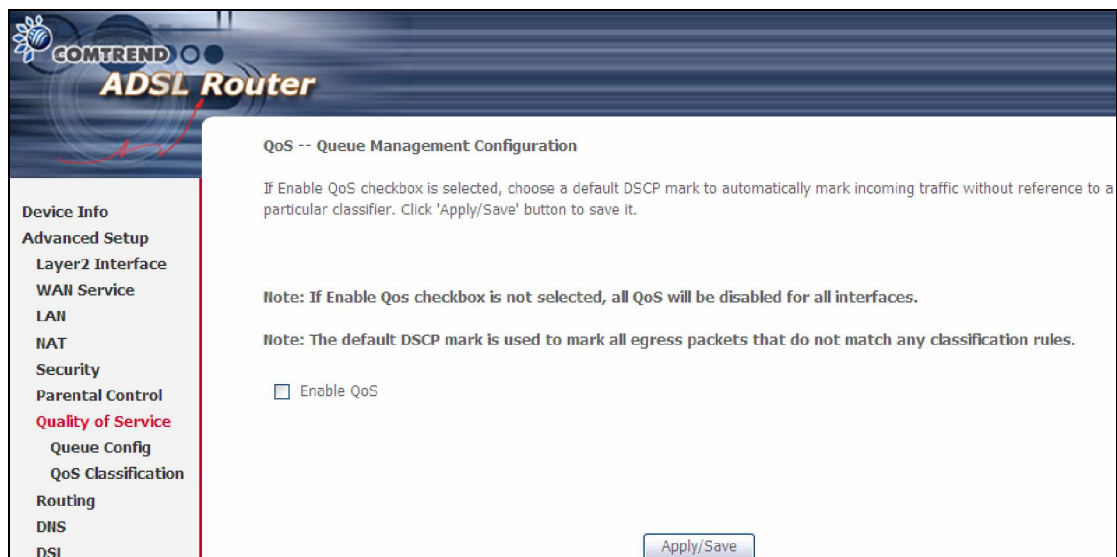
5.8 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(see [Appendix E - Connection Setup](#) for detailed PVC setup instructions).

5.8.1 Queue Management Configuration

To Enable QoS tick the checkbox and select a Default DSCP Mark.

Click **Apply/Save** to activate QoS.



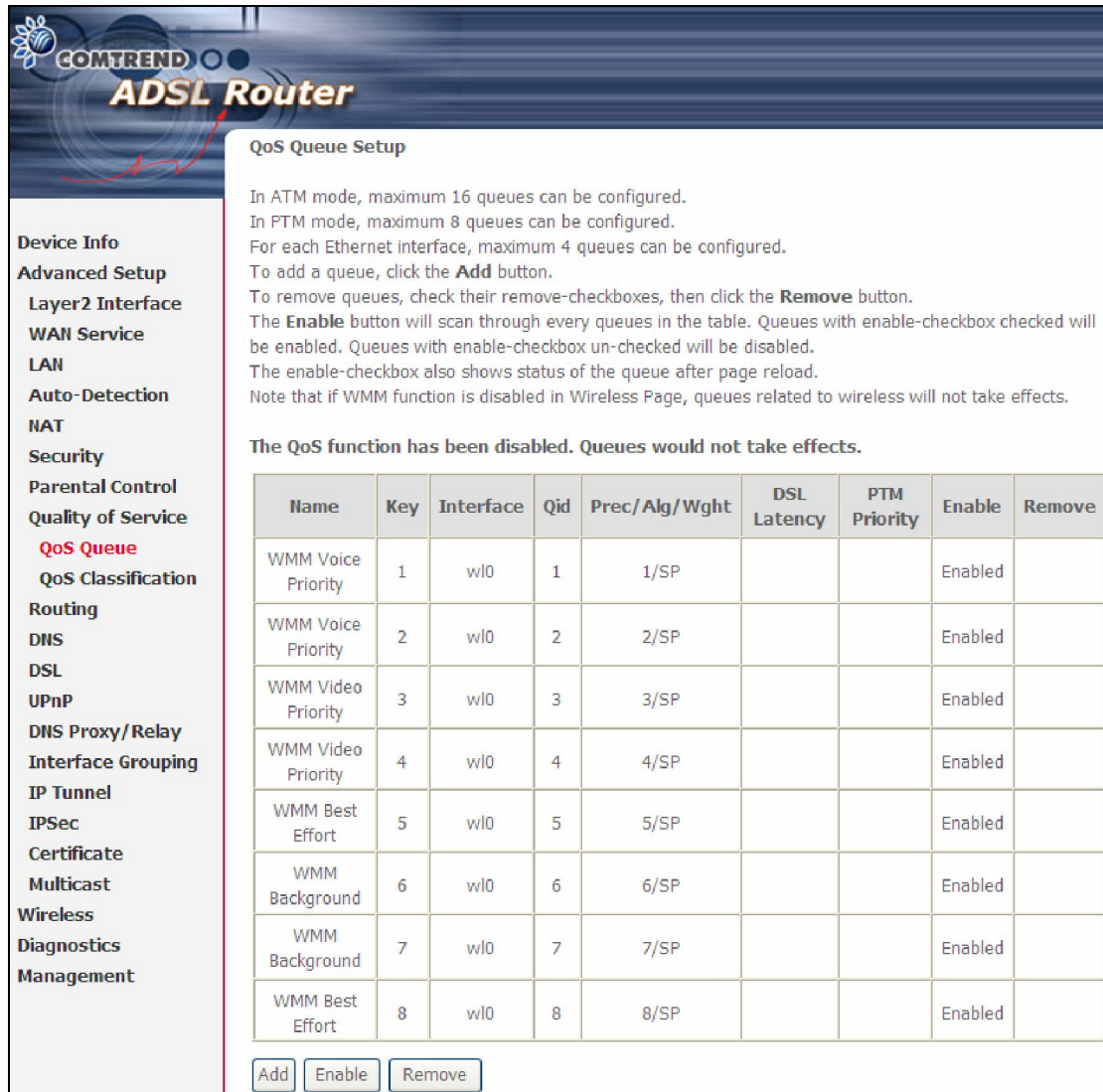
QoS and **DSCP Mark** are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

5.8.2 Queue Configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.



QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 4 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1	1/SP			Enabled	
WMM Voice Priority	2	wl0	2	2/SP			Enabled	
WMM Video Priority	3	wl0	3	3/SP			Enabled	
WMM Video Priority	4	wl0	4	4/SP			Enabled	
WMM Best Effort	5	wl0	5	5/SP			Enabled	
WMM Background	6	wl0	6	6/SP			Enabled	
WMM Background	7	wl0	7	7/SP			Enabled	
WMM Best Effort	8	wl0	8	8/SP			Enabled	

Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.

COMTREND
ADSL Router

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: ▾

Interface: ▾

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
QoS Queue
QoS Classification

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

Interface: Assign the entry to a specific network interface (QoS enabled).

5.8.3 QoS Classification

The network traffic classes are listed in the following table.

QoS Classification Setup -- maximum 32 rules can be configured.


To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

CLASSIFICATION CRITERIA													CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/Mask	DstMAC/Mask	SrcIP/PrefixLength	DstIP/PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																	

Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.



Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required): ▼

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.

Field	Description
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Specify Class Queue	Select corresponding queue to deliver outgoing traffic.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. Lower values have higher priority.

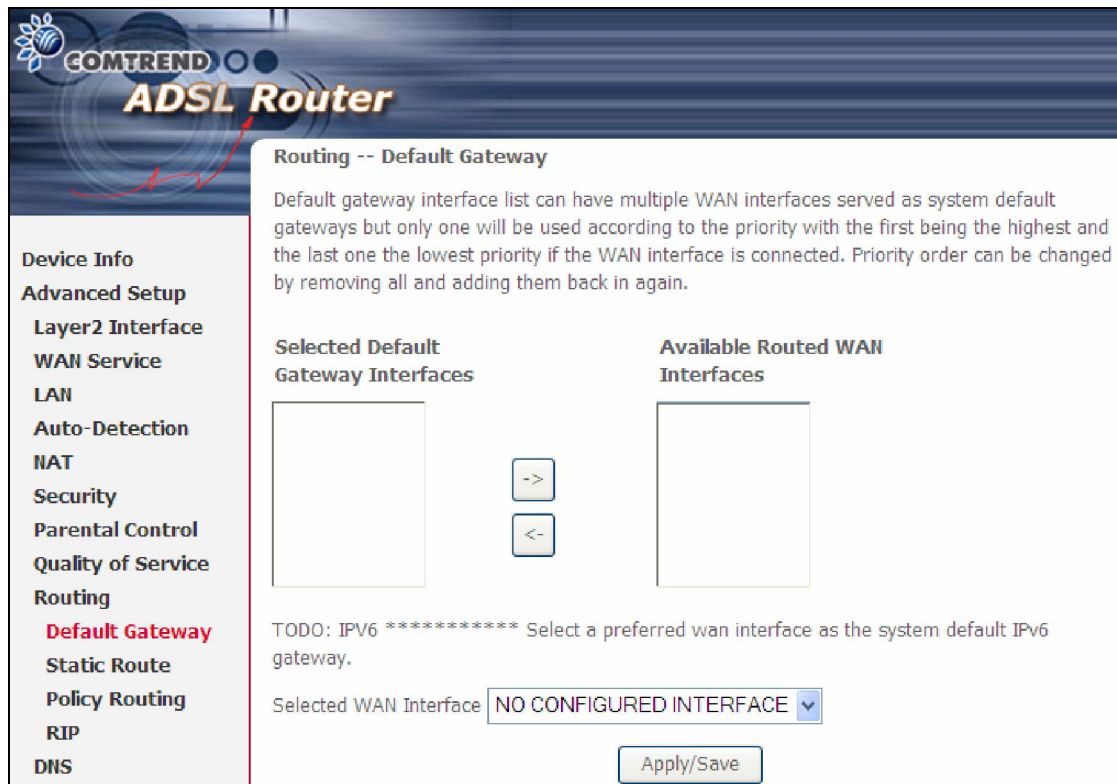
5.9 Routing

These following routing functions are accessed from this menu:
Default Gateway, Static Route, Policy Routing and RIP.

NOTE: In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

5.9.1 Default Gateway

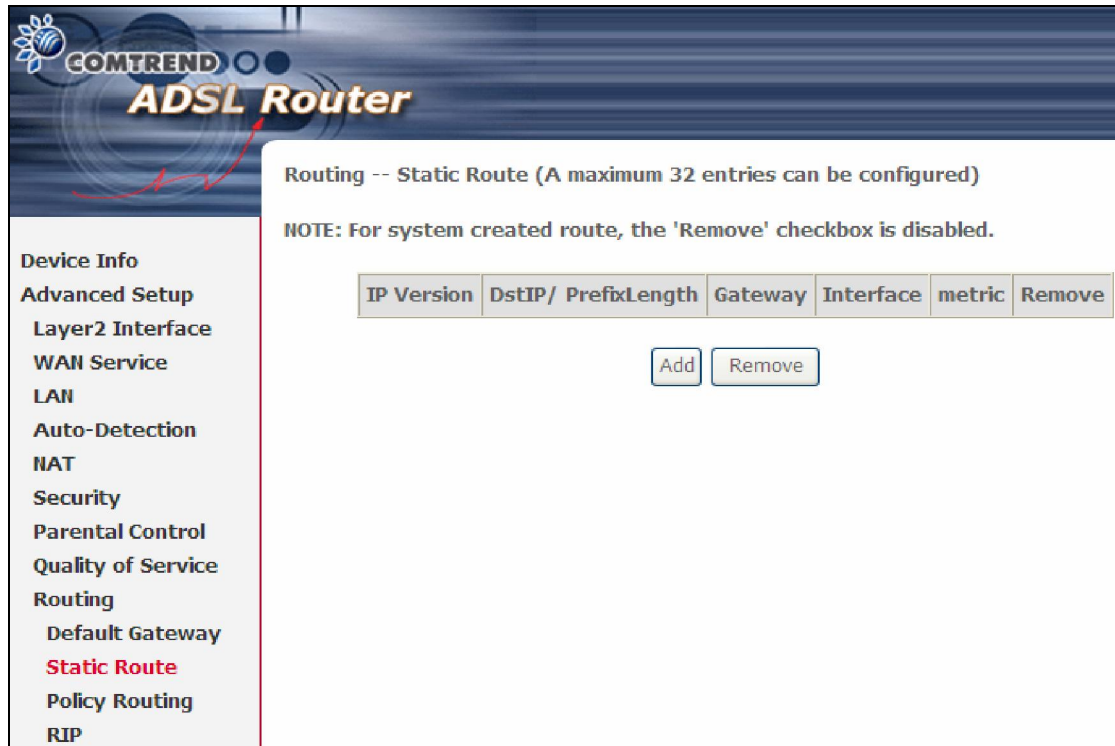
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.



The screenshot displays the web interface of a GOMTREND ADSL Router. The main title is "GOMTREND ADSL Router". The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, **Default Gateway** (highlighted in red), Static Route, Policy Routing, RIP, and DNS. The main content area is titled "Routing -- Default Gateway". It contains a descriptive paragraph: "Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again." Below this text are two empty boxes: "Selected Default Gateway Interfaces" and "Available Routed WAN Interfaces", with arrows between them for moving items. A note states: "TODO: IPV6 ***** Select a preferred wan interface as the system default IPV6 gateway." Below the note is a dropdown menu for "Selected WAN Interface" currently set to "NO CONFIGURED INTERFACE". An "Apply/Save" button is at the bottom right.

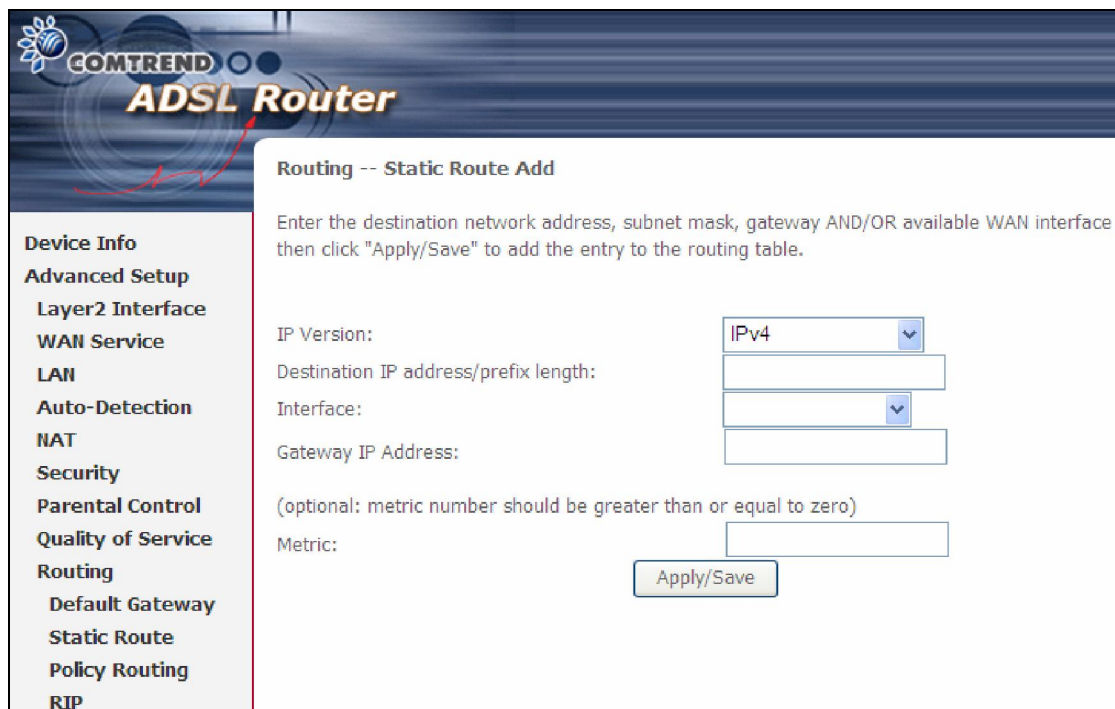
5.9.2 Static Route

This option allows for the configuration of static routes by destination IP. Click **Add** to create a static route or click **Remove** to delete a static route.



The screenshot shows the COMTREND ADSL Router configuration page. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing (highlighted), Default Gateway, Static Route (highlighted in red), Policy Routing, and RIP. The main content area is titled "Routing -- Static Route (A maximum 32 entries can be configured)". Below the title is a note: "NOTE: For system created route, the 'Remove' checkbox is disabled." A table with the following headers is displayed: IP Version, DstIP/ PrefixLength, Gateway, Interface, metric, and Remove. Below the table are two buttons: "Add" and "Remove".

After clicking **Add** the following screen will display.



The screenshot shows the COMTREND ADSL Router configuration page with the "Routing -- Static Route Add" form. The left sidebar is the same as in the previous screenshot. The main content area has the title "Routing -- Static Route Add" and a note: "Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table." The form contains the following fields: "IP Version:" with a dropdown menu set to "IPv4"; "Destination IP address/prefix length:" with a text input field; "Interface:" with a dropdown menu; "Gateway IP Address:" with a text input field; and "Metric:" with a text input field. Below the "Metric" field is a note: "(optional: metric number should be greater than or equal to zero)". At the bottom of the form is an "Apply/Save" button.

Input the Destination IP Address, select the interface type, Input the Gateway IP, (and the Metric number if required). Then, click **Apply/Save** to add an entry to the routing table.

5.9.3 Policy Routing

This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.

COMTREND ADSL Router

Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
-------------	-----------	----------	-----	------------	--------

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP

On the following screen, complete the form and click **Apply/Save** to create a policy.

COMTREND ADSL Router

Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

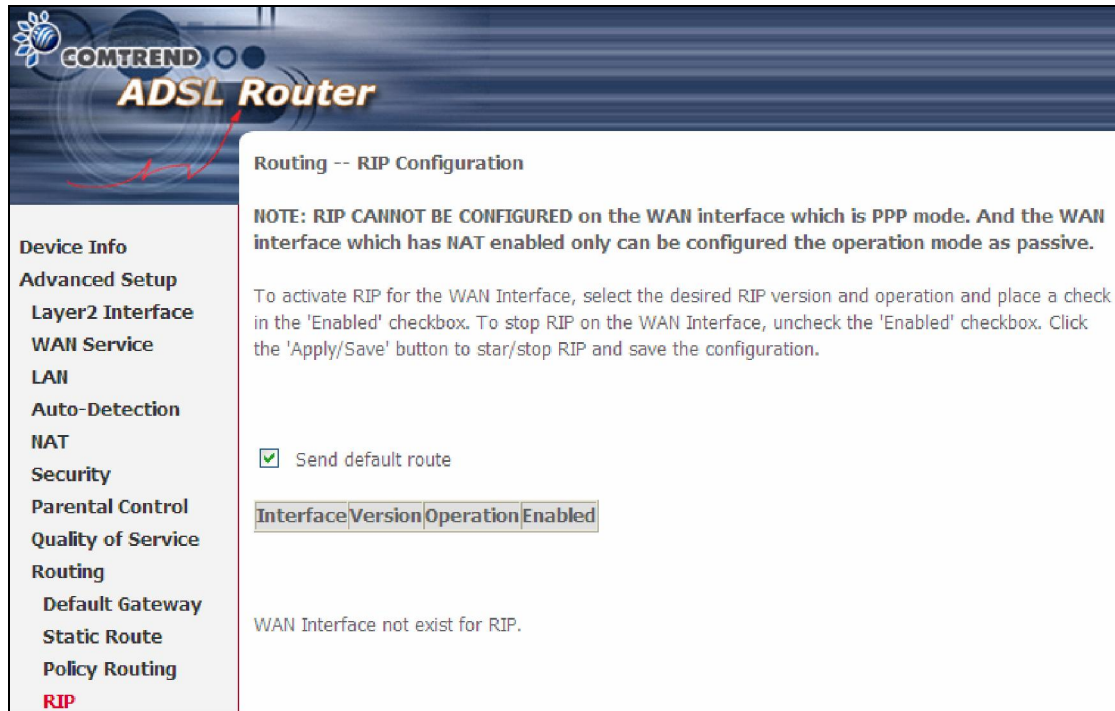
Use Interface

Default Gateway IP:

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP

5.9.4 RIP

To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox for at least one WAN interface before clicking **Save/Apply**.



The screenshot shows the configuration interface for a COMTREND ADSL Router. The page title is "COMTREND ADSL Router". The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, Default Gateway, Static Route, Policy Routing, and RIP (highlighted in red). The main content area is titled "Routing -- RIP Configuration". It contains a note: "NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive." Below the note is a paragraph: "To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration." There is a checkbox labeled "Send default route" which is checked. Below this is a table with the following header: "Interface|Version|Operation|Enabled". The table body is empty. At the bottom of the main content area, it says "WAN Interface not exist for RIP."

5.10 DNS

5.10.1 DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

DNS Server Configuration

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

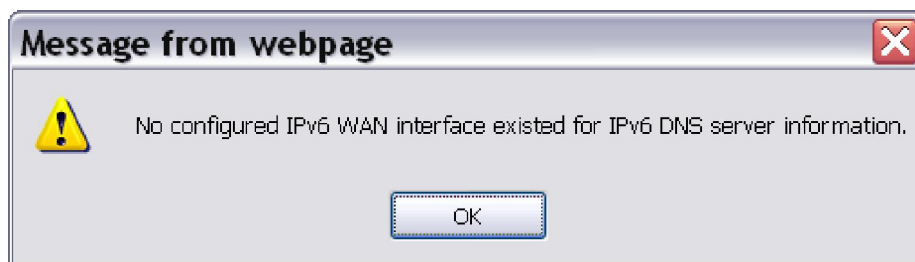
Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

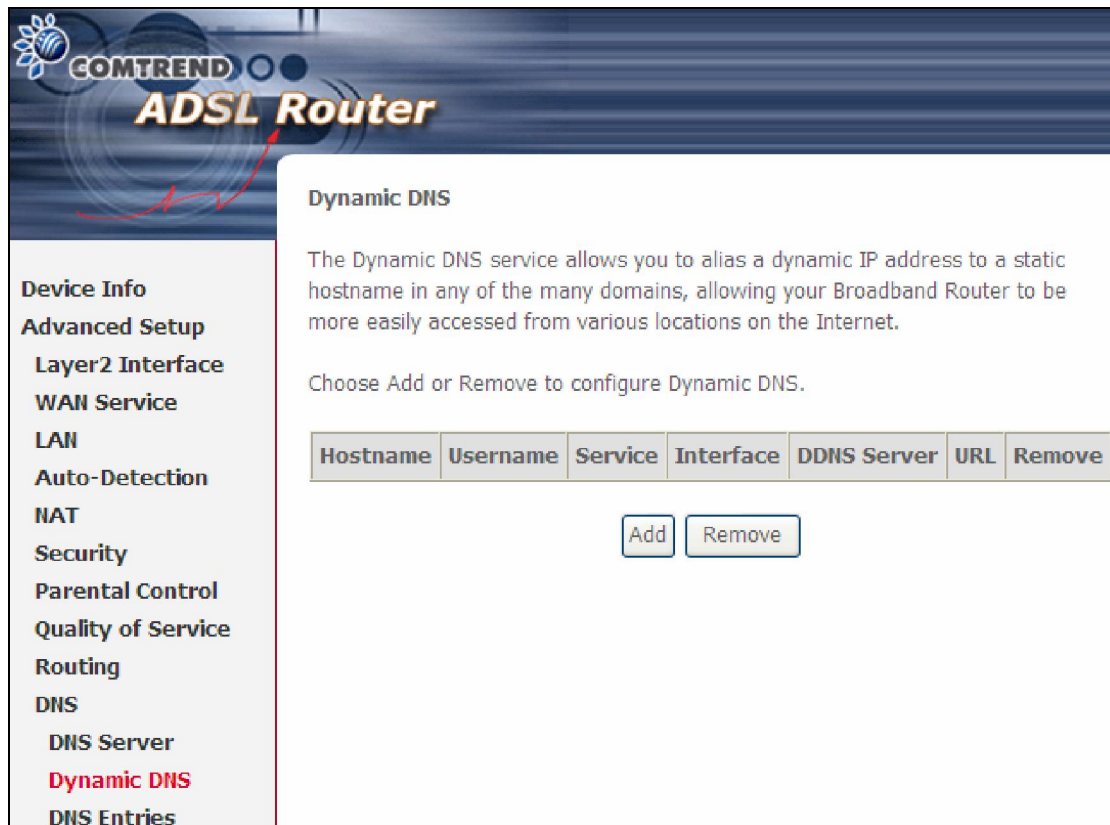
Secondary DNS server:



If is no IPv6 WAN interface is configured, a warning message system will pop up when accessing DNS Server.

5.10.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the AR-5389 to be more easily accessed from various locations on the Internet.



The screenshot shows the web interface of a COMTREND ADSL Router. The top banner features the COMTREND logo and the text "ADSL Router". On the left is a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DNS Server, Dynamic DNS (highlighted in red), and DNS Entries. The main content area is titled "Dynamic DNS" and contains the following text: "The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet." Below this is the instruction: "Choose Add or Remove to configure Dynamic DNS." A table with the following headers is present: Hostname, Username, Service, Interface, DDNS Server, URL, and Remove. Below the table are two buttons: "Add" and "Remove".

To add a dynamic DNS service, click **Add**. The following screen will display.

Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

5.10.3 DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router.

COMTREND ADSL Router

DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router. Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.

A maximum 16 entries can be configured.

Domain Name	IP Address	Remove
-------------	------------	--------

Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.

COMTREND ADSL Router

DNS Entry

Enter the domain name and IP address that needs to be resolved locally, and click 'Add Entry.'

Domain Name	IP Address
<input type="text"/>	<input type="text"/>

Enter the domain name and IP address that needs to be resolved locally, and click the **Add Entry** button.

5.11 DSL

The DSL Settings screen allows for the selection of DSL modulation modes. For optimum performance, the modes selected should match those of your ISP.

The screenshot shows the DSL Settings page of a GOMTREND ADSL Router. The page has a left-hand navigation menu and a main content area. The navigation menu includes: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Print Server, DLNA, Storage Service, Interface Grouping, IP Tunnel, IPSec, Certificate, Multicast, Wireless, Diagnostics, and Management. The main content area is titled 'DSL Settings' and contains the following sections:

- Select the modulation below.**
 - G.Dmt Enabled
 - G.lite Enabled
 - T1.413 Enabled
 - ADSL2 Enabled
 - AnnexL Enabled
 - ADSL2+ Enabled
 - AnnexM Enabled
- Select the phone line pair below.**
 - Inner pair
 - Outer pair
- Capability**
 - Bitswap Enable
 - SRA Enable
- Select DSL LED behavior**
 - Normal(TR-68 compliant)
 - Off
- G.997.1 EOC xTU-R Serial Number**
 - Equipment Serial Number
 - Equipment MAC Address

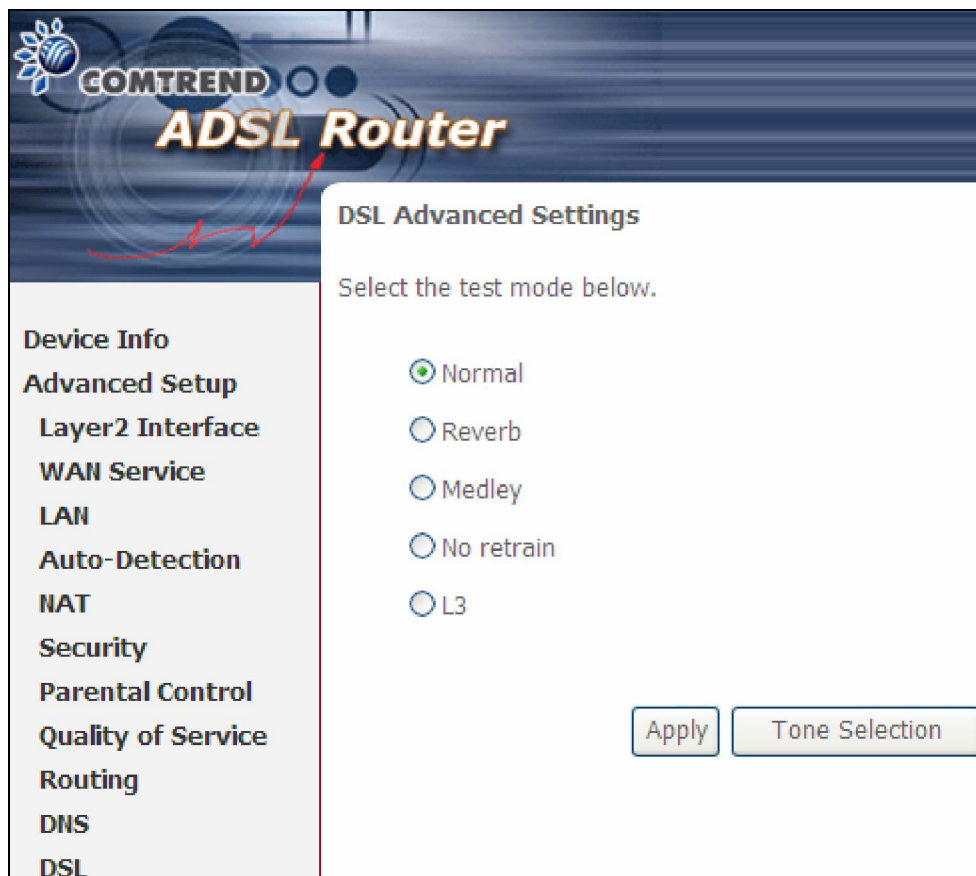
At the bottom right of the page, there are two buttons: 'Apply/Save' and 'Advanced Settings'.

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates	
ADSL2+	Downstream: 24 Mbps	Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps	Upstream: 3.5 Mbps
Options	Description	
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)	
Bitswap Enable	Enables adaptive handshaking functionality	

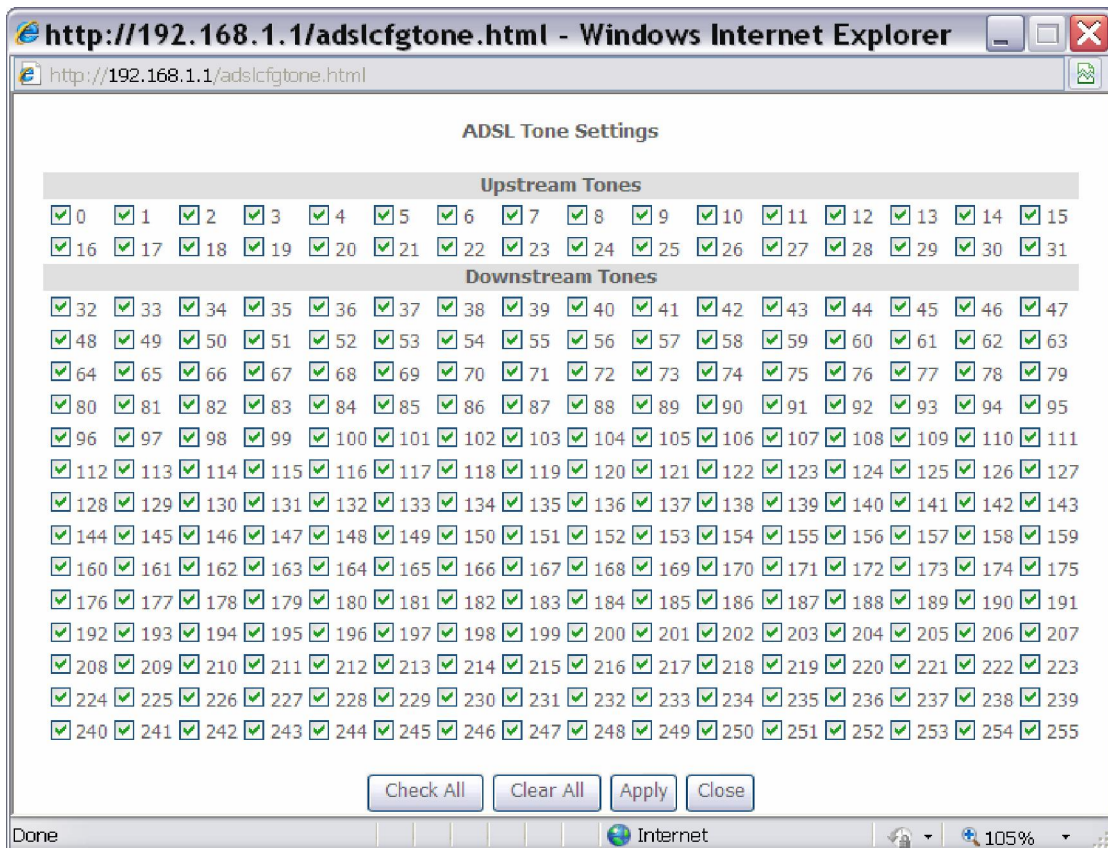
DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
SRA Enable	Enables Seamless Rate Adaptation (SRA)
DSL LED behavior	Normal (TR-68 compliant) – DSL LED blink/on/off following TR-68 standard Off – always turn off DSL LED
G997.1 EOC xTU-R Serial Number	Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options. On the following screen you can select a test mode or modify tones by clicking **Tone Selection**. Click **Apply** to implement these settings and return to the previous screen.

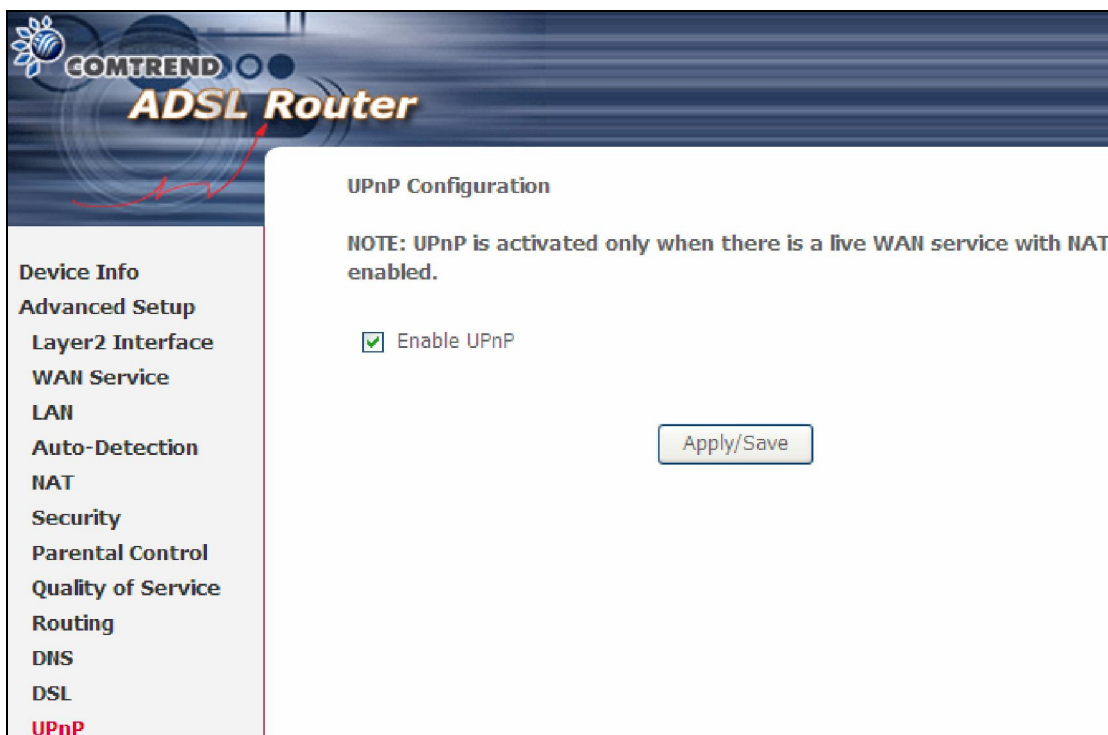


On this screen you select the tones you want activated, then click **Apply** and **Close**.



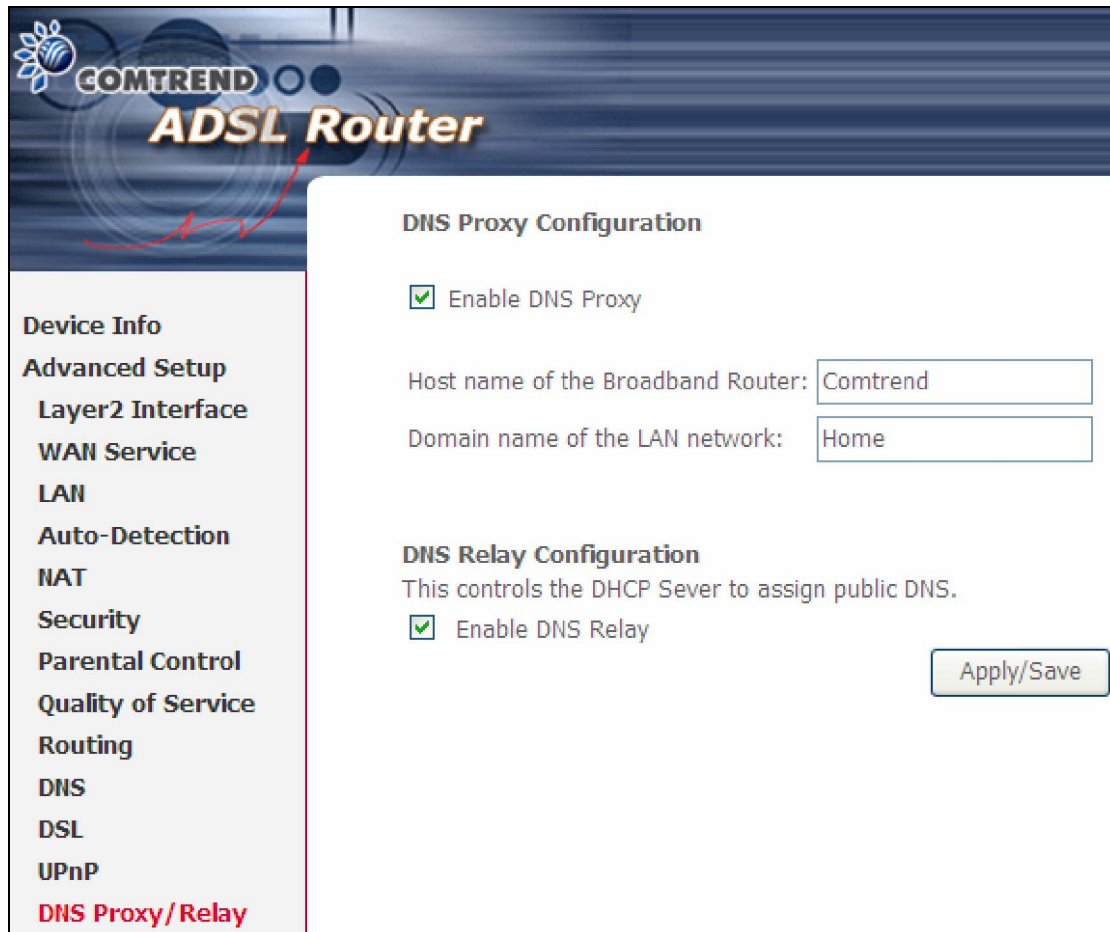
5.12 UPnP

Select the checkbox provided and click **Apply/Save** to enable UPnP protocol.



5.13 DNS Proxy/Relay

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Home".



The screenshot shows the configuration interface for a Comtrend ADSL Router. The page title is "COMTREND ADSL Router". On the left is a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, and DNS Proxy/Relay (highlighted in red). The main content area is titled "DNS Proxy Configuration" and includes the following settings:

- Enable DNS Proxy
- Host name of the Broadband Router:
- Domain name of the LAN network:

Below this is the "DNS Relay Configuration" section, which includes:

- This controls the DHCP Server to assign public DNS.
- Enable DNS Relay

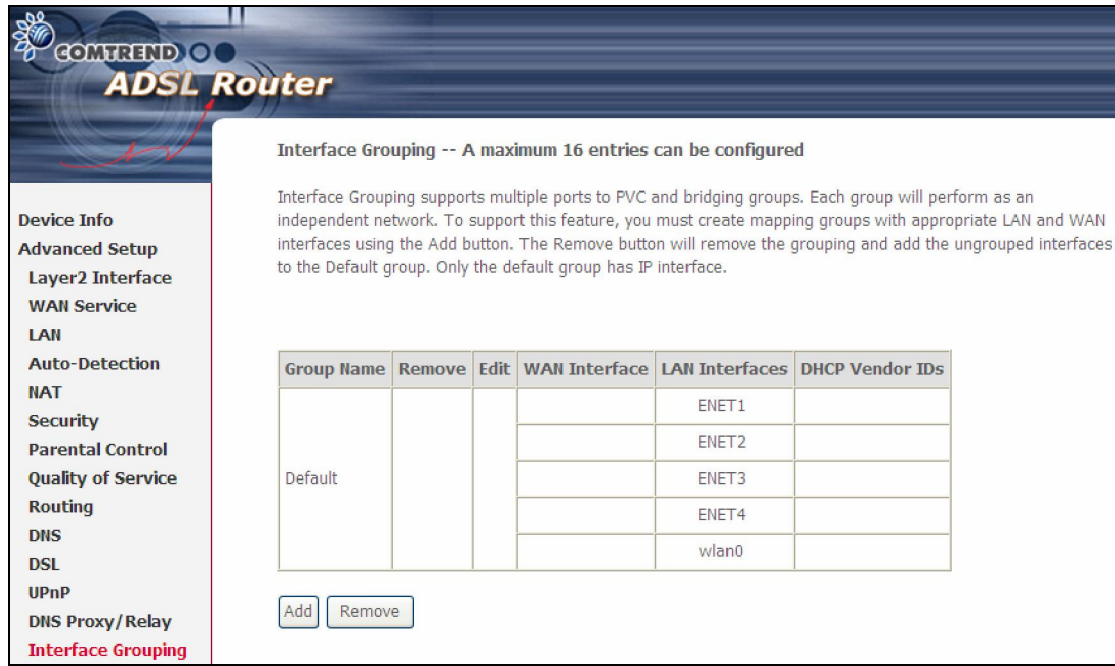
An "Apply/Save" button is located at the bottom right of the configuration area.

DNS Relay

When DNS Relay is enabled, the router will play a role as DNS server that send request to ISP DNS server and cache the information for later access. When DNS relay is disabled, the computer will pull information from ISP DNS server.

5.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.



Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	Edit	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default				ENET1	
				ENET2	
				ENET3	
				ENET4	
				wlan0	

To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.

COMTREND ADSL Router

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. 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.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

IMPORTANT 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.

Group Name:

<p>Grouped WAN Interfaces</p> <div style="border: 1px solid black; height: 80px; width: 100%;"></div>	<p>-></p> <p><-</p>	<p>Available WAN Interfaces</p> <div style="border: 1px solid black; height: 80px; width: 100%;"></div>
<p>Grouped LAN Interfaces</p> <div style="border: 1px solid black; height: 80px; width: 100%;"></div>	<p>-></p> <p><-</p>	<p>Available LAN Interfaces</p> <div style="border: 1px solid black; padding: 5px;"> <p>ENET1</p> <p>ENET2</p> <p>ENET3</p> <p>ENET4</p> <p>wlan0</p> </div>

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

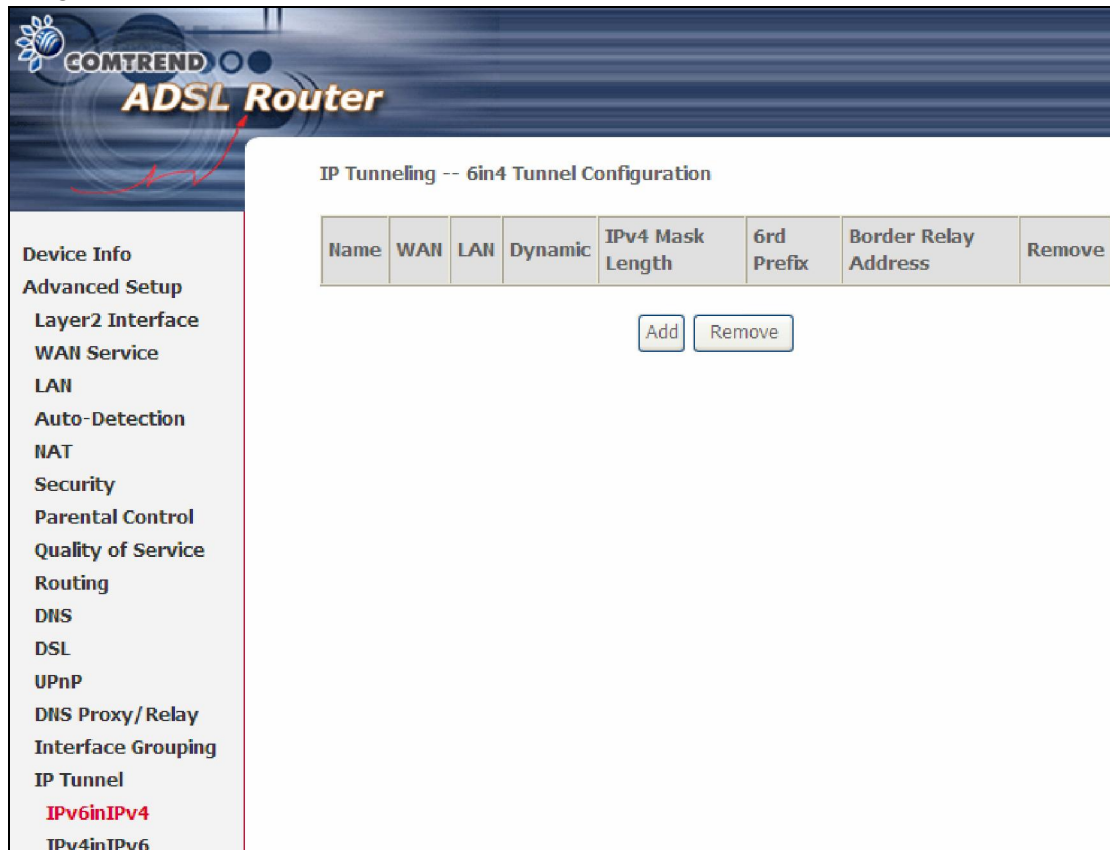
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ENET2, ENET3, and ENET4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

5.15 IP Tunnel

5.15.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.



The screenshot shows the Comtrend ADSL Router web interface. The main title is "COMTREND ADSL Router". The page is titled "IP Tunneling -- 6in4 Tunnel Configuration". On the left is a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Interface Grouping, IP Tunnel, **IPv6inIPv4**, and IPv4inIPv6. The main content area contains a table with the following columns: Name, WAN, LAN, Dynamic, IPv4 Mask Length, 6rd Prefix, Border Relay Address, and Remove. Below the table are two buttons: "Add" and "Remove".

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
------	-----	-----	---------	------------------	------------	----------------------	--------

Click the **Add** button to display the following.

COMTREND ADSL Router

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

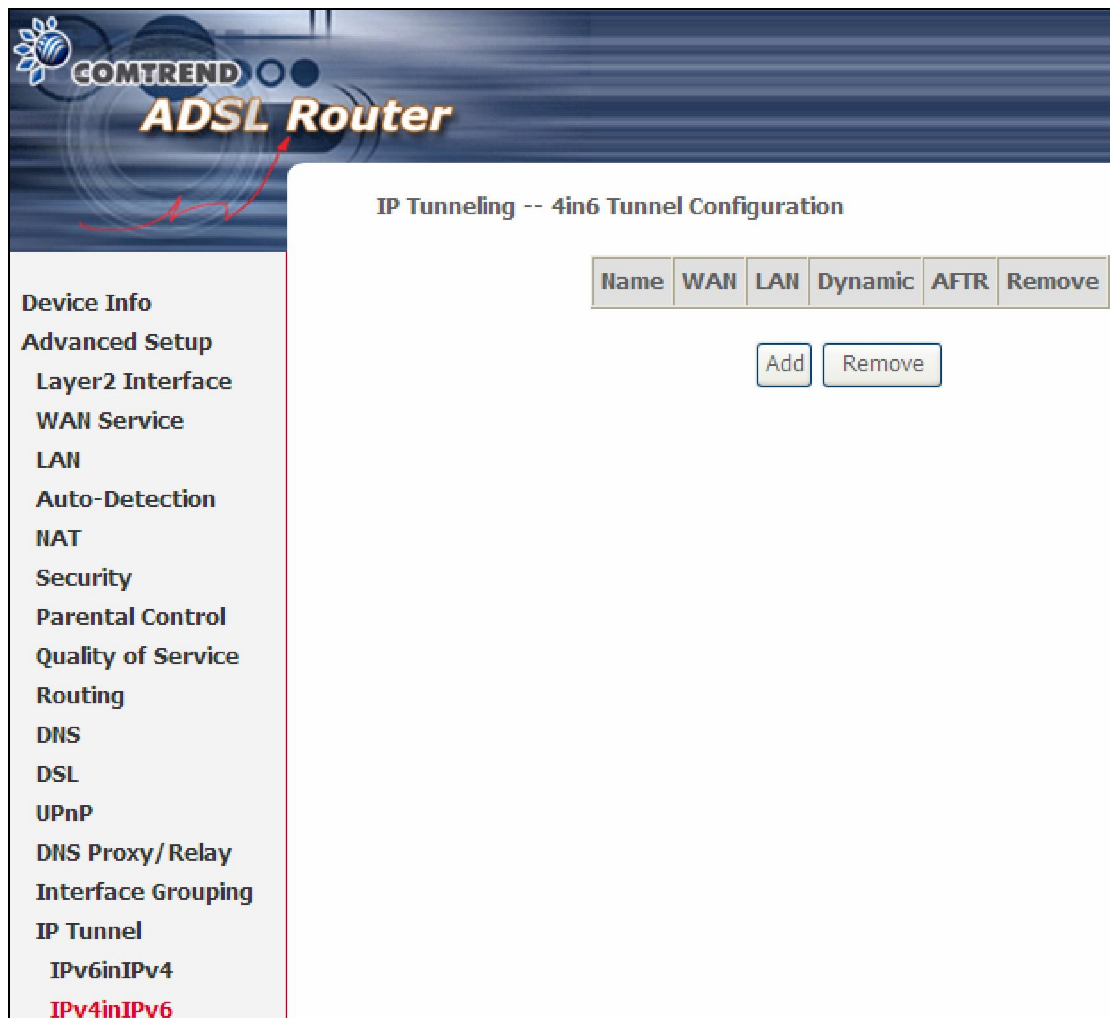
Border Relay IPv4 Address:

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
 IPv6inIPv4
 IPv4inIPv6

Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used for the IPv4 interface
6rd Prefix with Prefix Length	Prefix and prefix length used for the IPv6 interface
Border Relay IPv4 Address	Input the IPv4 address of the other device

5.15.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.



The screenshot shows the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and the text "ADSL Router". The main content area is titled "IP Tunneling -- 4in6 Tunnel Configuration". Below the title is a table with the following columns: Name, WAN, LAN, Dynamic, AFTR, and Remove. Below the table are two buttons: "Add" and "Remove". On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Interface Grouping, IP Tunnel, IPv6inIPv4, and IPv4inIPv6 (highlighted in red).

Name	WAN	LAN	Dynamic	AFTR	Remove
------	-----	-----	---------	------	--------

[Add](#) [Remove](#)

- Device Info
- Advanced Setup
- Layer2 Interface
- WAN Service
- LAN
- Auto-Detection
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnP
- DNS Proxy/Relay
- Interface Grouping
- IP Tunnel
- IPv6inIPv4
- IPv4inIPv6**

Click the **Add** button to display the following.

COMTREND ADSL Router

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual Automatic

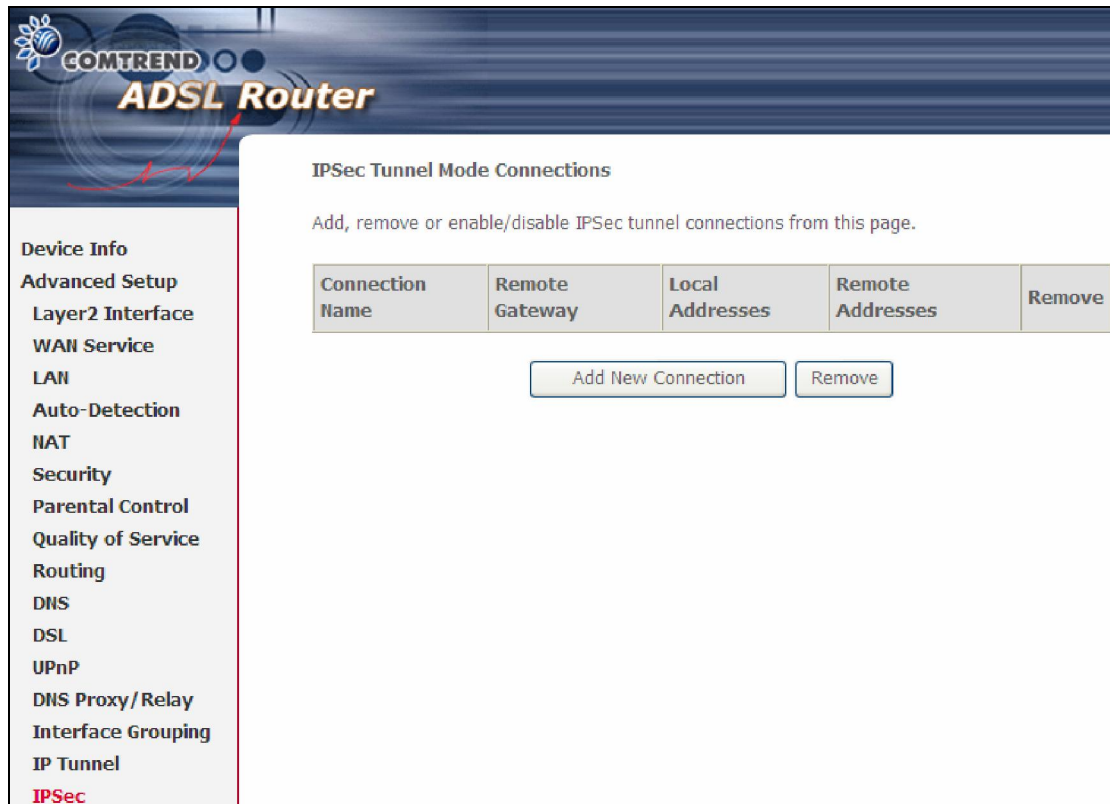
AFTR:

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
 IPv6inIPv4
 IPv4inIPv6

Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router

5.16 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page.



The screenshot shows the web interface of a COMTREND ADSL Router. The main heading is "IPSec Tunnel Mode Connections". Below the heading, there is a text instruction: "Add, remove or enable/disable IPSec tunnel connections from this page." A table with five columns is displayed: "Connection Name", "Remote Gateway", "Local Addresses", "Remote Addresses", and "Remove". Below the table, there are two buttons: "Add New Connection" and "Remove". On the left side of the interface, there is a navigation menu with the following items: "Device Info", "Advanced Setup", "Layer2 Interface", "WAN Service", "LAN", "Auto-Detection", "NAT", "Security", "Parental Control", "Quality of Service", "Routing", "DNS", "DSL", "UPnP", "DNS Proxy/Relay", "Interface Grouping", "IP Tunnel", and "IPSec" (which is highlighted in red).

Click **Add New Connection** to add a new IPSec termination rule.

The following screen will display.

IPsec Connection Name	User-defined label
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Remote IPsec Gateway Address	The location of the Remote IPsec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.