


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection
Security
 IP Filtering
 Outgoing
 Incoming
 MAC Filtering
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version: IPv4

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	Select from the drop down menu.
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.


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection
Security
 IP Filtering
 Outgoing
 Incoming
 MAC Filtering
Quality of Service

Incoming IP Filtering Setup

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.

Filter Name	Interfaces	IP Version	Protocol	Action	ICMP Type	SrcIP / PrefixLength	SrcPort	DstIP / PrefixLength	DstPort	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**.

 **COMTREND**








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection
Security
 IP Filtering
 Outgoing
 Incoming
 MAC Filtering
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version: IPv4

Protocol:

Policy: Permit

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

☒ Select All ☒ br0/br0

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
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.

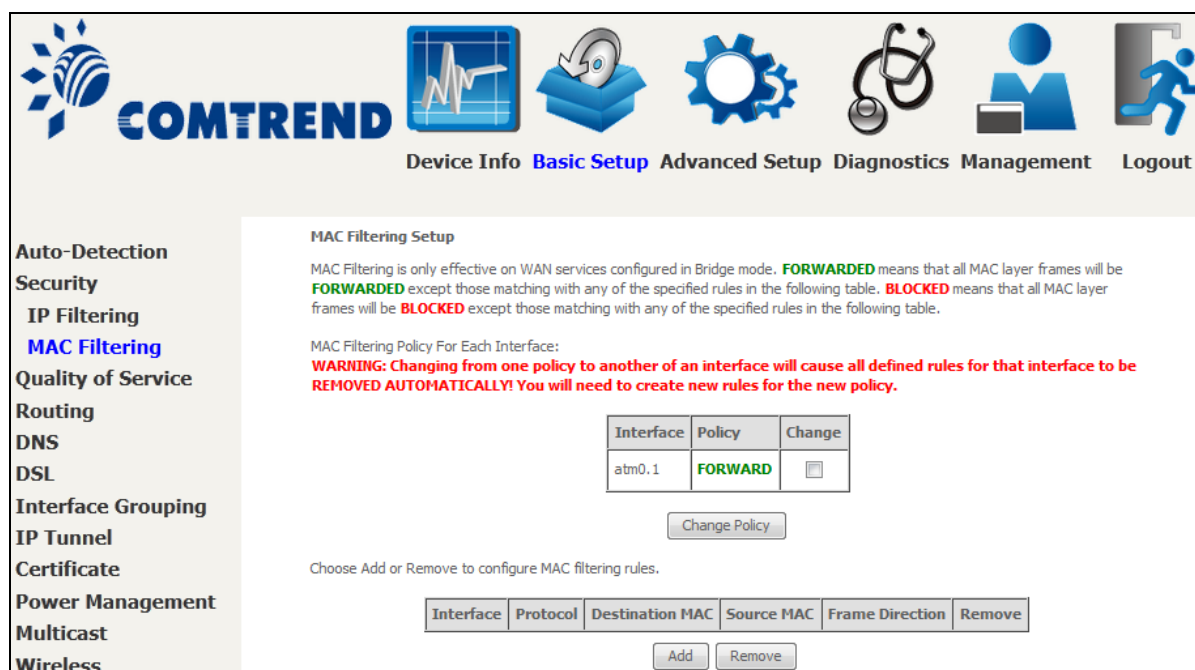
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

6.2.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use [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-5313u 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 Device Info **Basic Setup** Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
 IP Filtering
MAC Filtering
 Quality of Service
 Routing
 DNS
 DSL
 Interface Grouping
 IP Tunnel
 Certificate
 Power Management
 Multicast
 Wireless

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
atm0.1	FORWARD	

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
Add 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.

 **COMTREND**








[Device Info](#)
[Basic Setup](#)
[Advanced Setup](#)
[Diagnostics](#)
[Management](#)
[Logout](#)

Auto-Detection

Security

 IP Filtering

MAC Filtering

Quality of Service

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Click **Save/Apply** to save and activate the filter rule.

Consult the table below for detailed field descriptions.

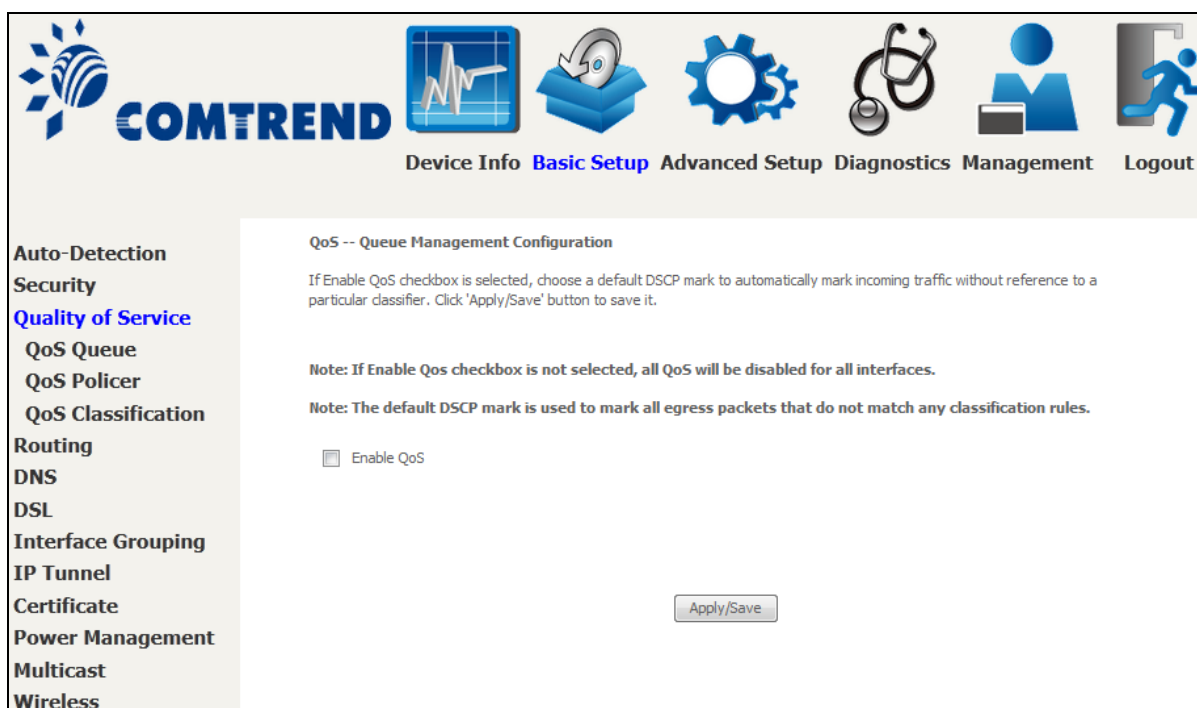
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

6.3 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).

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

Click Apply/Save to activate QoS.



The screenshot shows the COMTREND web interface with the 'Basic Setup' tab selected. The left sidebar lists various configuration categories: Auto-Detection, Security, Quality of Service (highlighted), QoS Queue, QoS Policer, QoS Classification, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled 'QoS -- Queue Management Configuration'. It contains the following text:

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

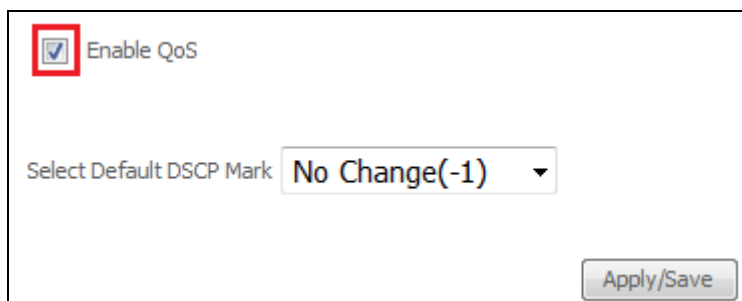
Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Below the notes, there is a checkbox labeled 'Enable QoS' which is checked. At the bottom right of the configuration area is an 'Apply/Save' button.

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.



This close-up screenshot shows the 'Enable QoS' checkbox, which is checked and highlighted with a red box. Below it is a dropdown menu labeled 'Select Default DSCP Mark' with the value 'No Change(-1)' selected. An 'Apply/Save' button is located at the bottom right of this section.

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.

6.3.1 QoS Queue Setup

Configure queues with different priorities to be used for QoS 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.


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

QoS Queue

QoS Policer

QoS Classification

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

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	Shaping Rate(bits/s)	Burst Size(bytes)	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	

Add
Enable
Remove

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

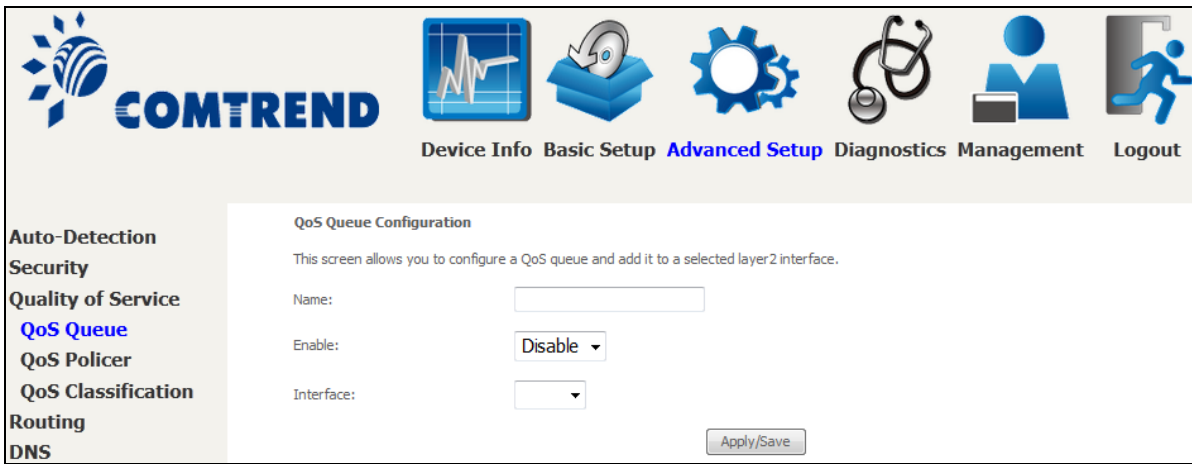
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

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 effect. 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.

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



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup (highlighted in blue), Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with the following items: Auto-Detection, Security, Quality of Service (highlighted in blue), QoS Queue (highlighted in blue), QoS Policer, QoS Classification, Routing, and DNS. The main content area is titled 'QoS Queue Configuration' and contains the following text: 'This screen allows you to configure a QoS queue and add it to a selected layer2 interface.' Below this text, there are three input fields: 'Name:' with a text box, 'Enable:' with a dropdown menu showing 'Disable', and 'Interface:' with a dropdown menu. At the bottom right of the main content area, there is an 'Apply/Save' button.

Click **Apply/Save** to apply and save the settings.

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

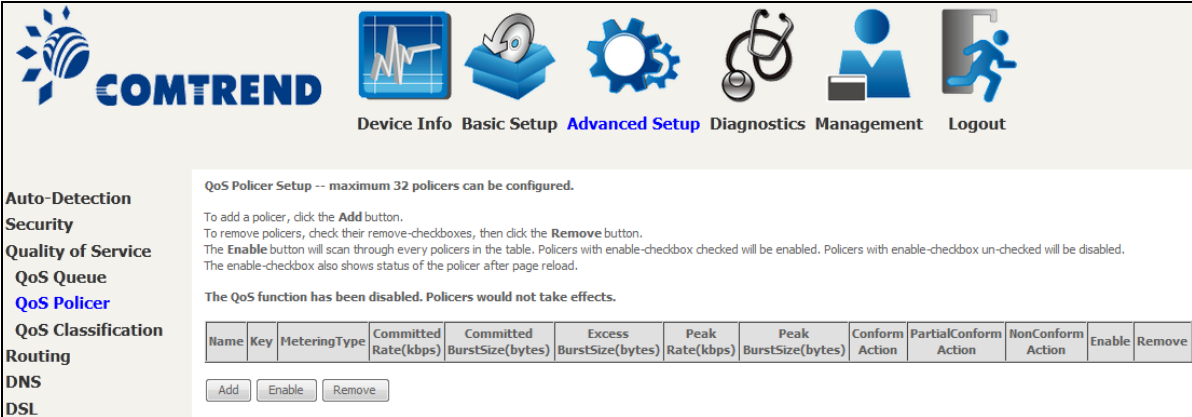
Interface: Assign the entry to a specific network interface (QoS enabled).

6.3.2 QoS Policer

To remove policers, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the policer after page reload.



COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
 QoS Queue
QoS Policer
 QoS Classification
 Routing
 DNS
 DSL

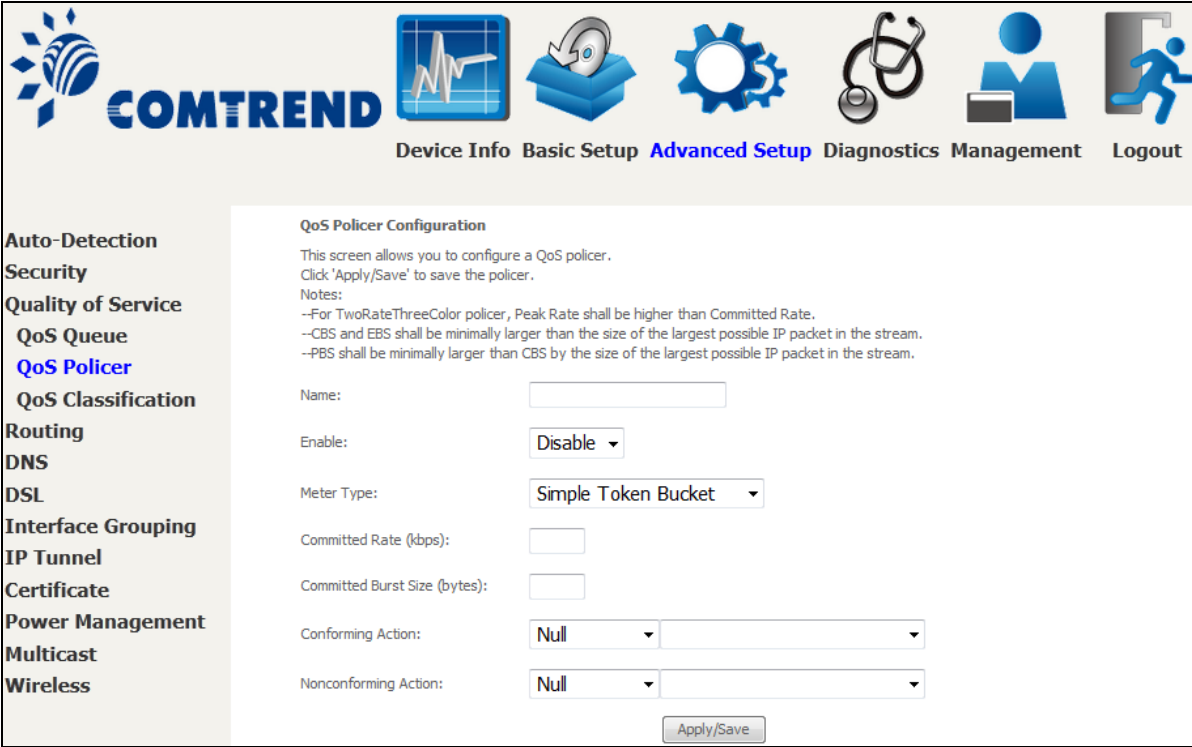
QoS Policer Setup -- maximum 32 policers can be configured.

To add a policer, click the **Add** button.
 To remove policers, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the policer after page reload.

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

Name	Key	MeteringType	Committed Rate(kbps)	Committed BurstSize(bytes)	Excess BurstSize(bytes)	Peak Rate(kbps)	Peak BurstSize(bytes)	Conform Action	PartialConform Action	NonConform Action	Enable	Remove
Add Enable Remove												

To add a policer, click the **Add** button.



COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
 QoS Queue
QoS Policer
 QoS Classification
 Routing
 DNS
 DSL
 Interface Grouping
 IP Tunnel
 Certificate
 Power Management
 Multicast
 Wireless

QoS Policer Configuration

This screen allows you to configure a QoS policer.
 Click 'Apply/Save' to save the policer.

Notes:
 --For TwoRateThreeColor policer, Peak Rate shall be higher than Committed Rate.
 --CBS and EBS shall be minimally larger than the size of the largest possible IP packet in the stream.
 --PBS shall be minimally larger than CBS by the size of the largest possible IP packet in the stream.

Name:

Enable:

Meter Type:

Committed Rate (kbps):

Committed Burst Size (bytes):

Conforming Action:

Nonconforming Action:

Click **Apply/Save** to save the policer.

Field	Description
Name	Name of this policer rule
Enable	Enable/Disable this policer rule
Meter Type	Meter type used for this policer rule
Committed Rate (kbps)	Defines the rate allowed for committed packets
Committed Burst Size (bytes)	Maximum amount of packets that can be processed by this policer
Conforming Action	Defines action to be taken if packets match this policer
Nonconforming Action	Defines actions to be taken if packets do not match this policer

6.3.3 QoS Classification

The network traffic classes are listed in the following table.


COMTREND








Auto-Detection

Security

Quality of Service

QoS Queue

QoS Policer

QoS Classification

Routing

DNS

DSL

Interface Grouping

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	Policer Key	DSCP Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
Add Enable 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:

Last

Rule Status:

Disable

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

Class Interface:

LAN

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.

Specify Class Policer:

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.

Set Rate Limit: [Kbits/s]

Apply/Save

Click **Apply/Save** to save and activate the rule.

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.
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	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.
Specify Class Policer	Packets classified into a policer will be marked based on the conforming action of the policer
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.
Set Rate Limit	The data transmission rate limit in kbps.

6.4 Routing

The following routing functions are accessed from this menu:

Default Gateway, Static Route, Policy Routing, RIP and IPv6 Static Route.

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

6.4.1 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.



COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
 Default Gateway
 Static Route
 Policy Routing
 RIP
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

Routing -- 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.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

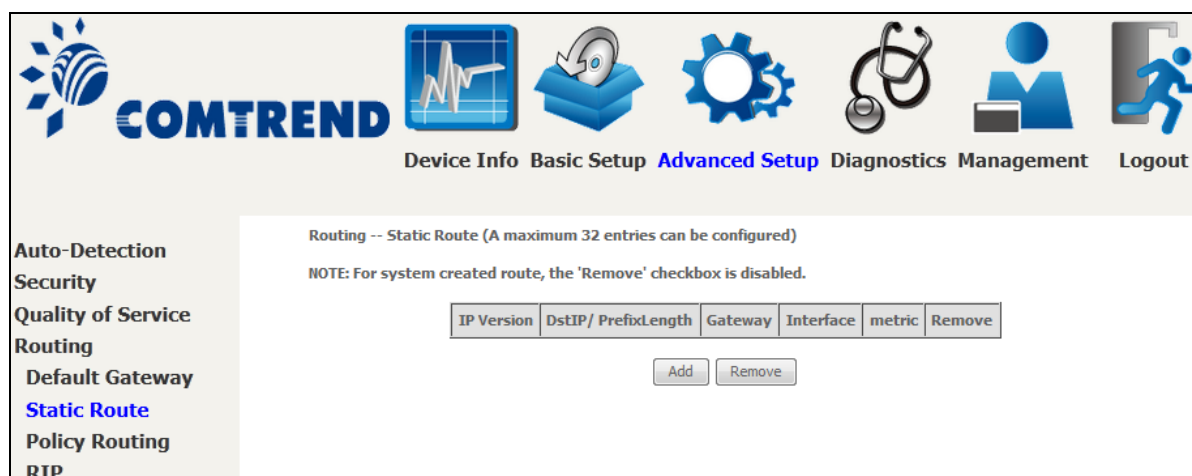
TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: NO CONFIGURED INTERFACE

Apply/Save

6.4.2 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.



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

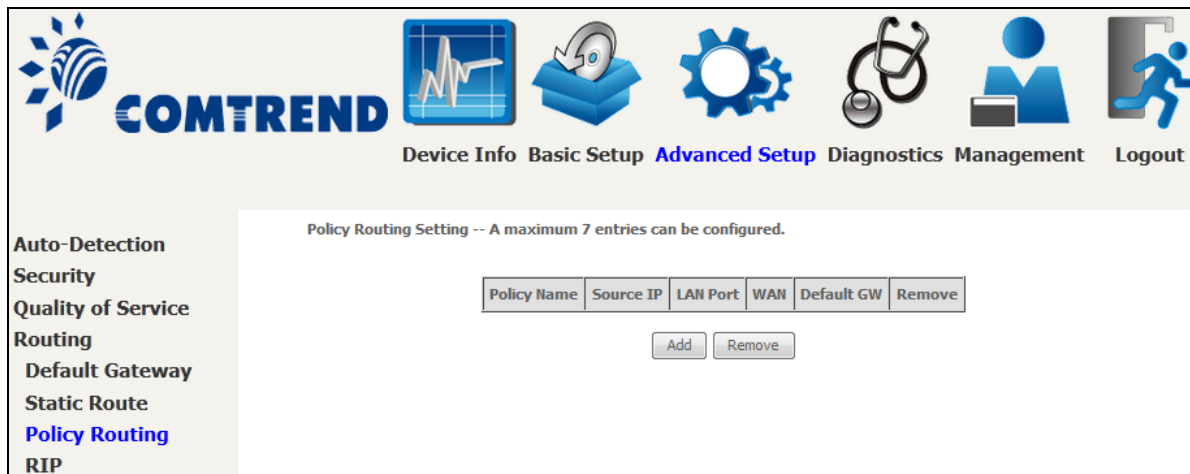


- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

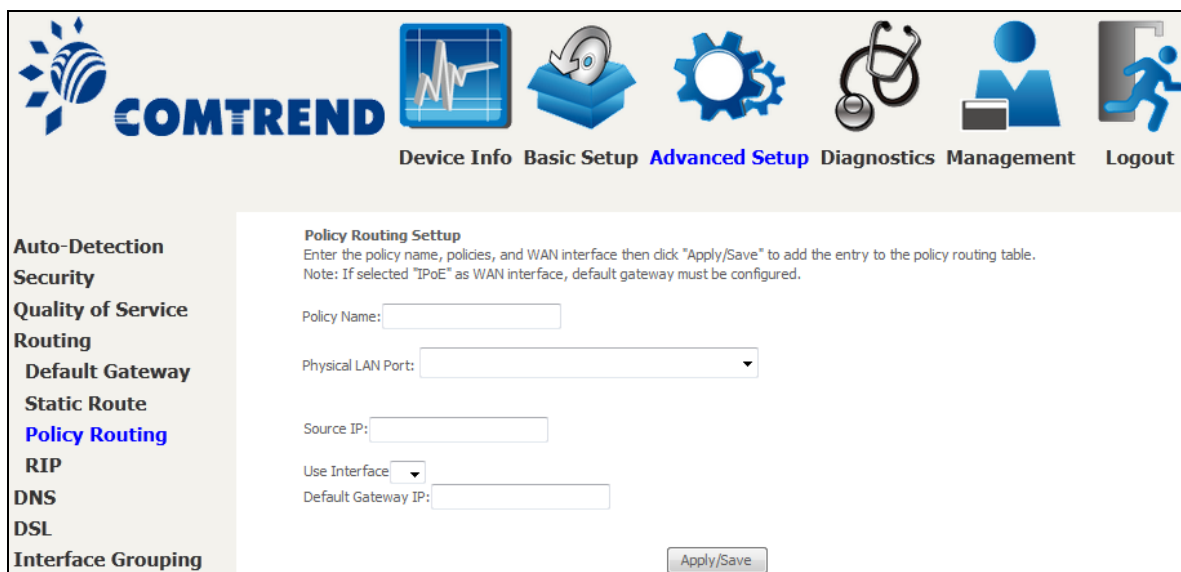
After completing the settings, click **Apply/Save** to add the entry to the routing table.

6.4.3 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.



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



Field	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway

6.4.4 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**.


COMTREND








Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection

Security

Quality of Service

Routing

Default Gateway

Static Route

Policy Routing

RIP

DNS

DSL

Interface Grouping

Routing -- RIP Configuration

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.

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.

☒ Send default route

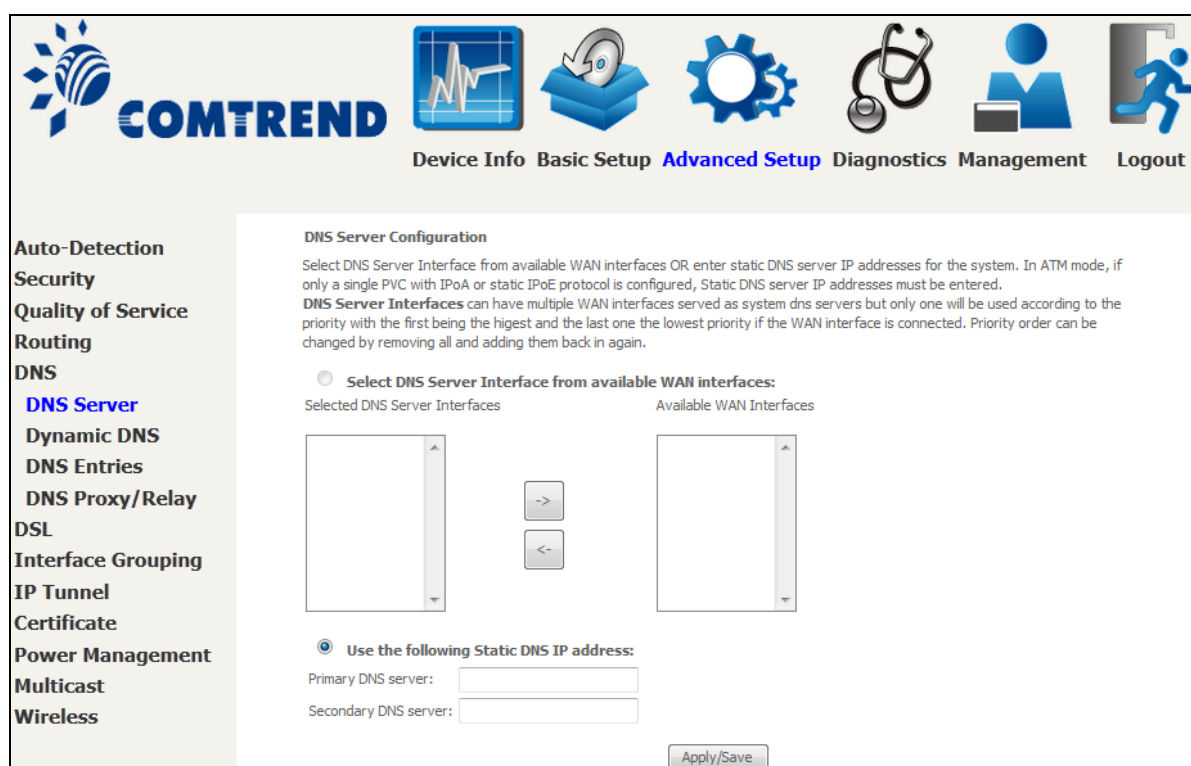
Interface	Version	Operation	Enabled
WAN Interface not exist for RIP.			

6.5 DNS

6.5.1 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.



COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

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:

Apply/Save

Click **Apply/Save** to save the new configuration.

NOTE: You must reboot the router to make the new configuration effective.

6.5.2 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-5313u to be more easily accessed from various locations on the Internet.



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



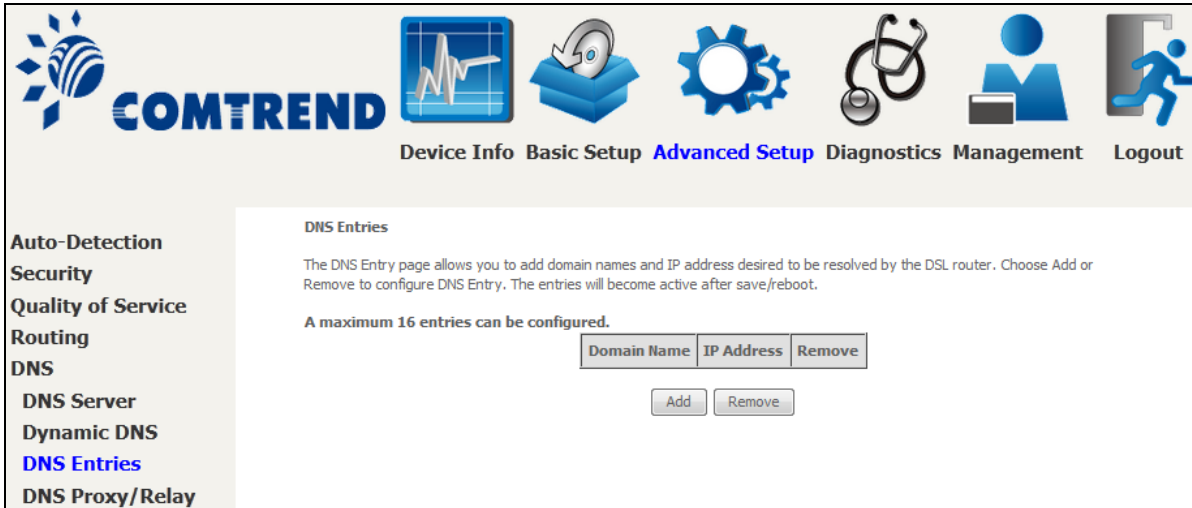
Click **Apply/Save** to save your settings.

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

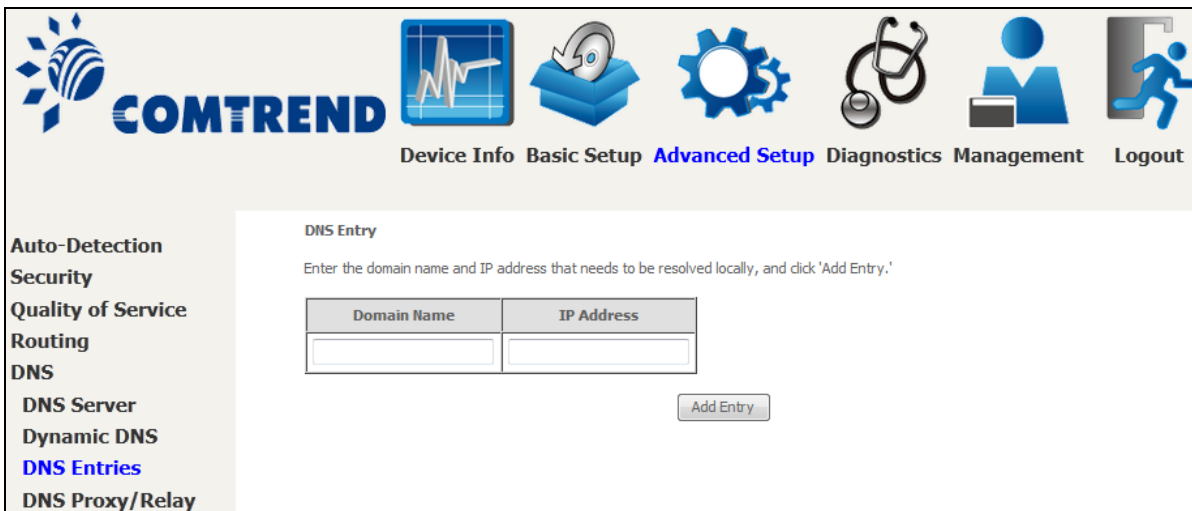
6.5.3 DNS Entries

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



The screenshot shows the COMTREND Advanced Setup page. The left sidebar contains a menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS (highlighted), DNS Server, Dynamic DNS, **DNS Entries** (selected), and DNS Proxy/Relay. The main content area is titled "DNS Entries" and contains the following text: "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." Below this text, it states "A maximum 16 entries can be configured." There is a table with two columns: "Domain Name" and "IP Address". Below the table, there are two buttons: "Add" and "Remove".

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



The screenshot shows the COMTREND Advanced Setup page. The left sidebar contains a menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS (highlighted), DNS Server, Dynamic DNS, **DNS Entries** (selected), and DNS Proxy/Relay. The main content area is titled "DNS Entry" and contains the following text: "Enter the domain name and IP address that needs to be resolved locally, and click 'Add Entry.'" Below this text, there is a form with two input fields: "Domain Name" and "IP Address". Below the form, there is a button labeled "Add Entry".

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

6.5.4 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".

 **COMTREND**
     
Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

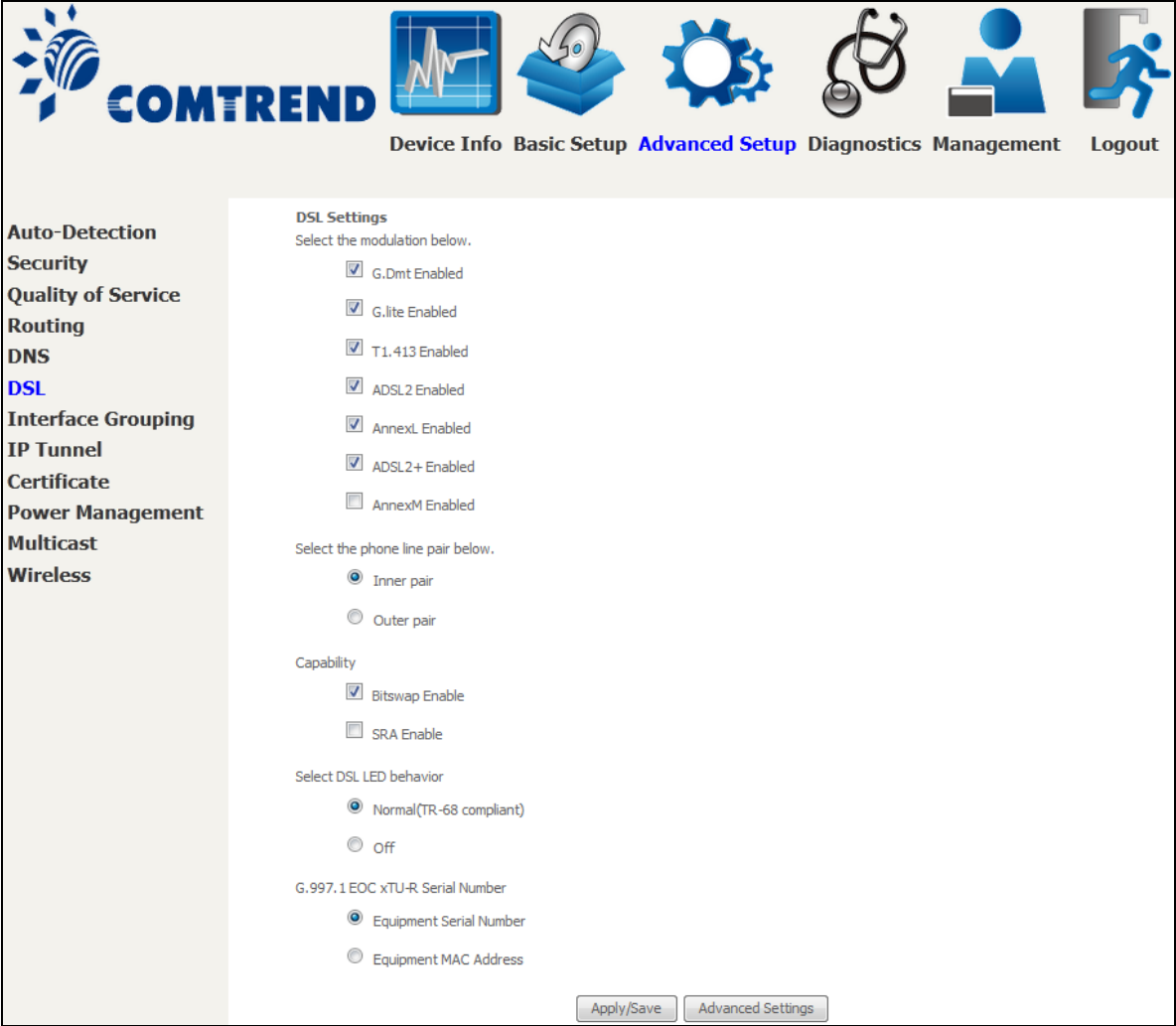
Auto-Detection
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DNS Proxy/Relay

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

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

6.6 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.

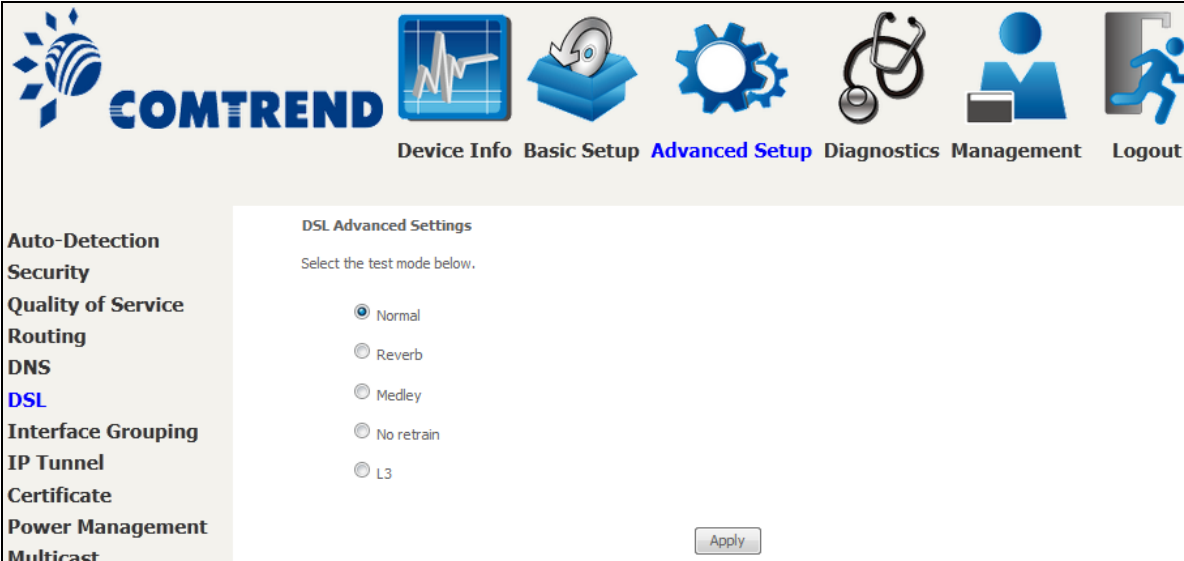


DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission 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)
Select DSL LED behavior	Normal (TR-68 compliant): Select this option for DSL LED to operate normally (See menu 2.2 LED Indicator) Off:DSL LED will always be OFF
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.



COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast

DSL Advanced Settings

Select the test mode below.

☒ Normal
☐ Reverb
☐ Medley
☐ No retrain
☐ L3

Apply

On this screen you select the required test mode, then click the **Apply** button.

Field	Description
Normal	DSL line signal is detected and sent normally
Reverb	DSL line signal is sent continuously in reverb mode
Medley	DSL line signal is sent continuously in medley mode
No Retrain	DSL line signal will always be on even when DSL line is unplugged
L3	DSL line is set in L3 power mode

6.7 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.


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

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				ETH1	
				ETH2	
				ETH3	
				ETH4	
				wlan0	

Add
Remove

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.










Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

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:

Grouped WAN Interfaces

->

<-

Available WAN Interfaces

Grouped LAN Interfaces

Available LAN Interfaces

ETH1
ETH2
ETH3
ETH4
wlan0

->

<-

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 ETH1, ETH2, ETH3, and ETH4.

The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and ETH4.
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).

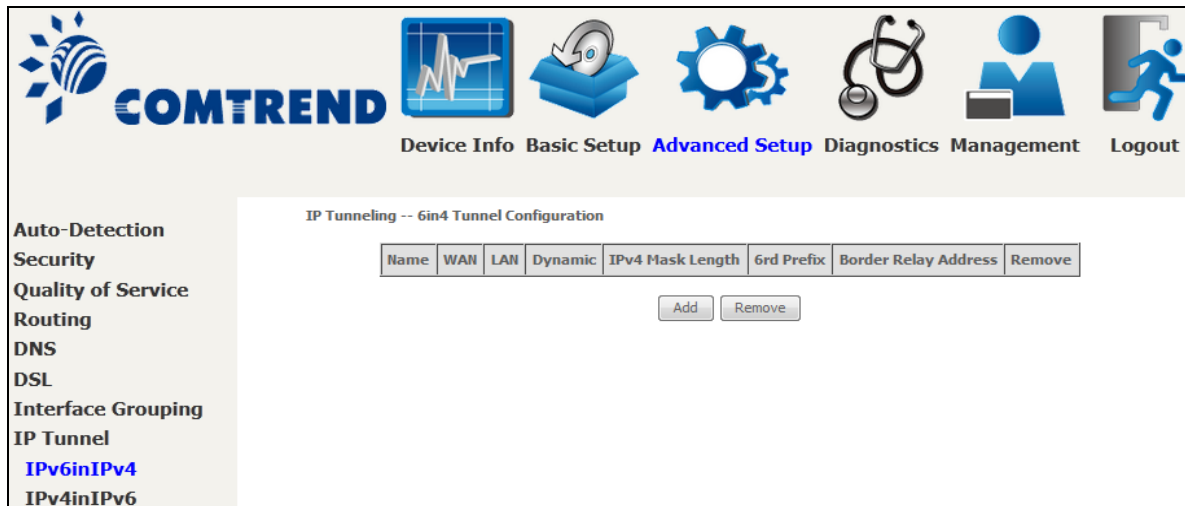
If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ETH2, ETH3, and ETH4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ETH1

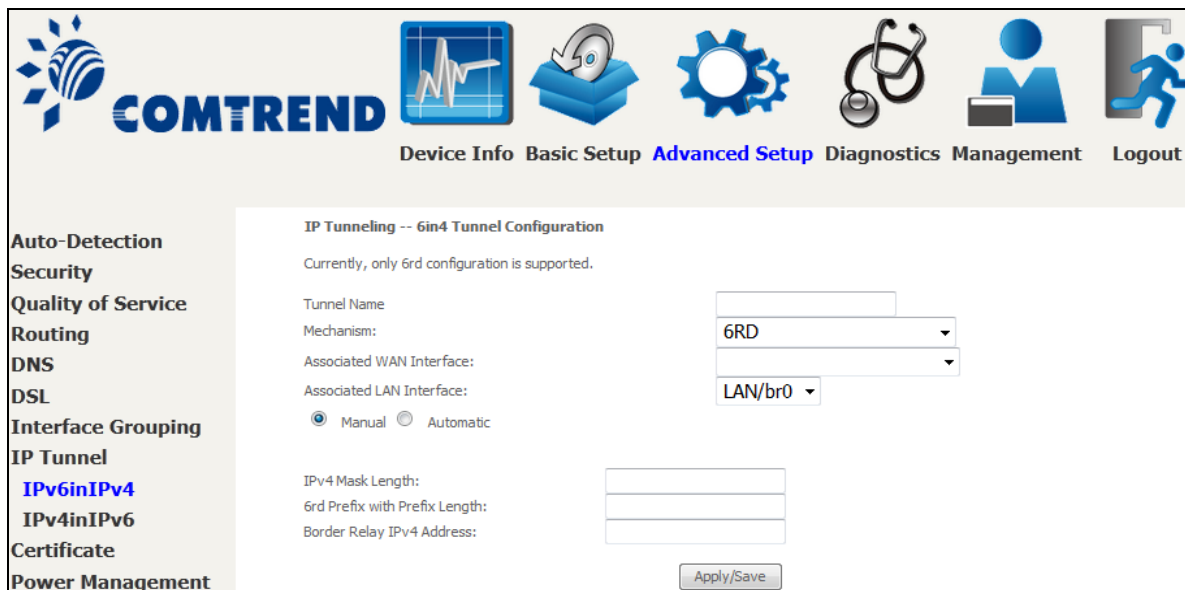
6.8 IP Tunnel

6.8.1 IPv6inIPv4

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



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



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

6.8.2 IPv4inIPv6

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

 **COMTREND**








Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
 IPv6inIPv4
 IPv4inIPv6

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove
Add Remove					

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

 **COMTREND**








Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
 IPv6inIPv4
 IPv4inIPv6

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

☒ Manual
☐ Automatic

AFTR:

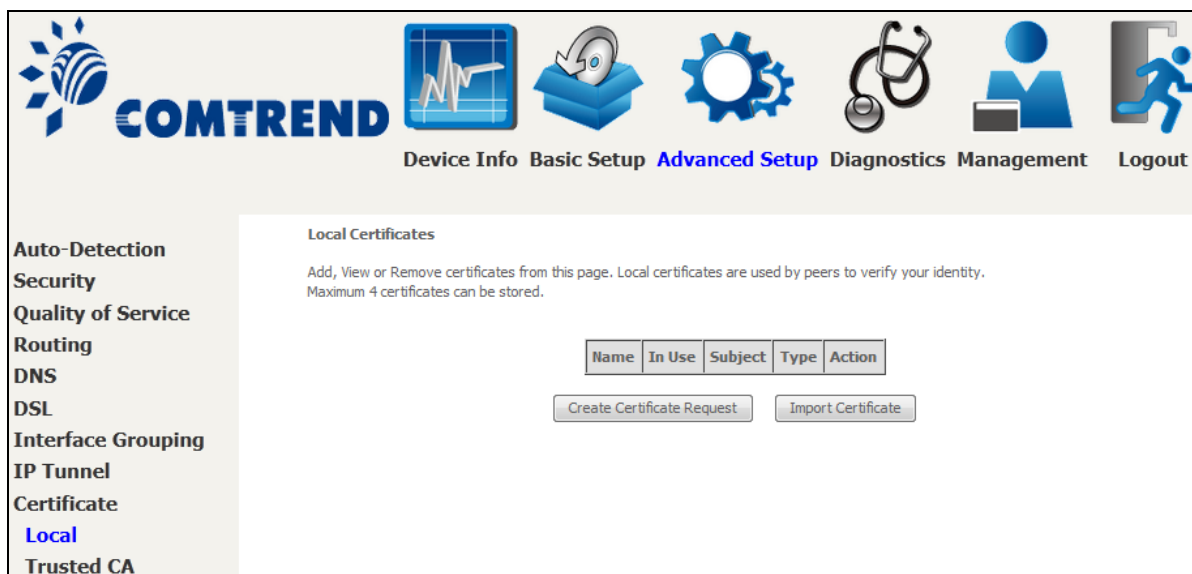
Apply/Save

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

6.9 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

6.9.1 Local



COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Local
Trusted CA

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
Create Certificate Request Import Certificate				

CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Local

Trusted CA

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

US (United States)

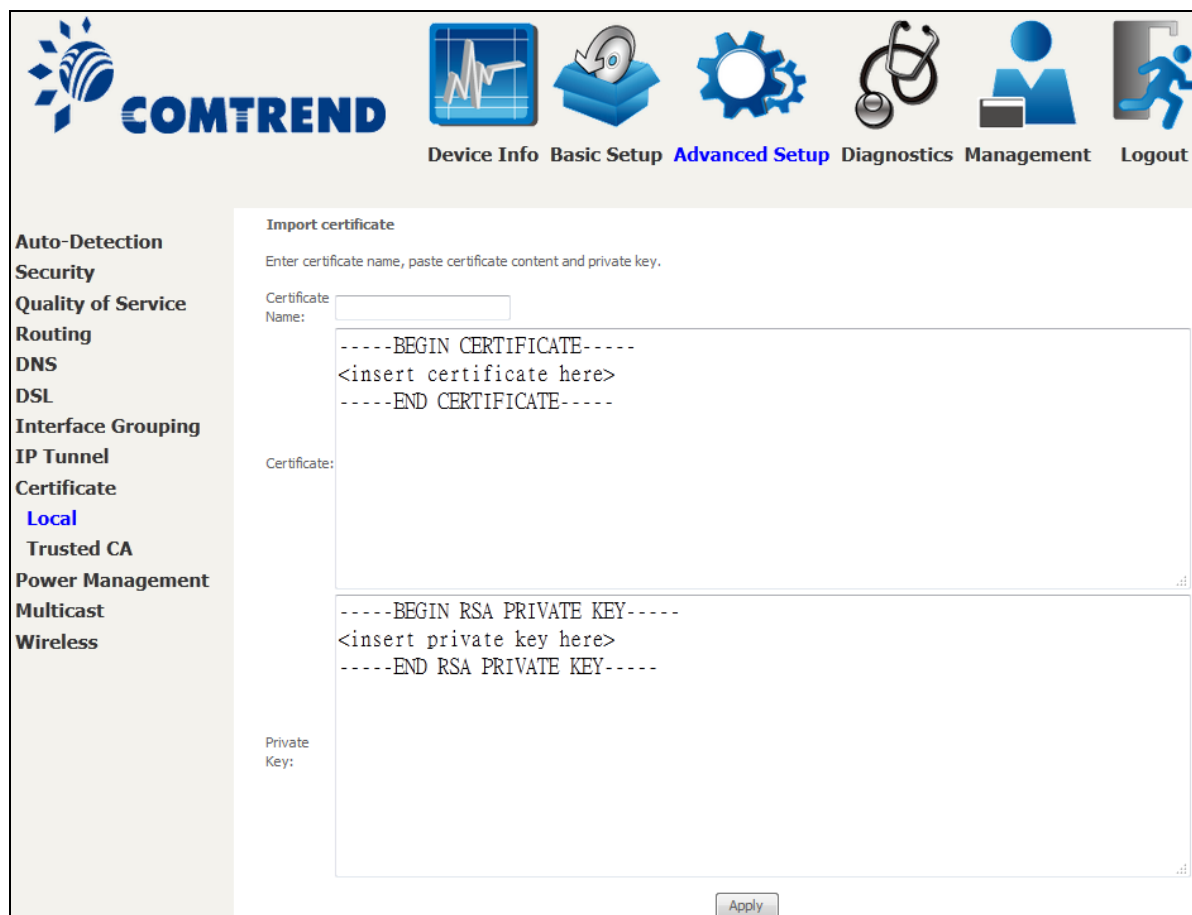
▼

The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with various configuration options: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate (highlighted), Local, Trusted CA, Power Management, Multicast, and Wireless. The main content area is titled 'Import certificate' and contains the following fields and instructions:

- Import certificate**
- Enter certificate name, paste certificate content and private key.
- Certificate Name:** A text input field.
- Certificate:** A large text area containing the following text:

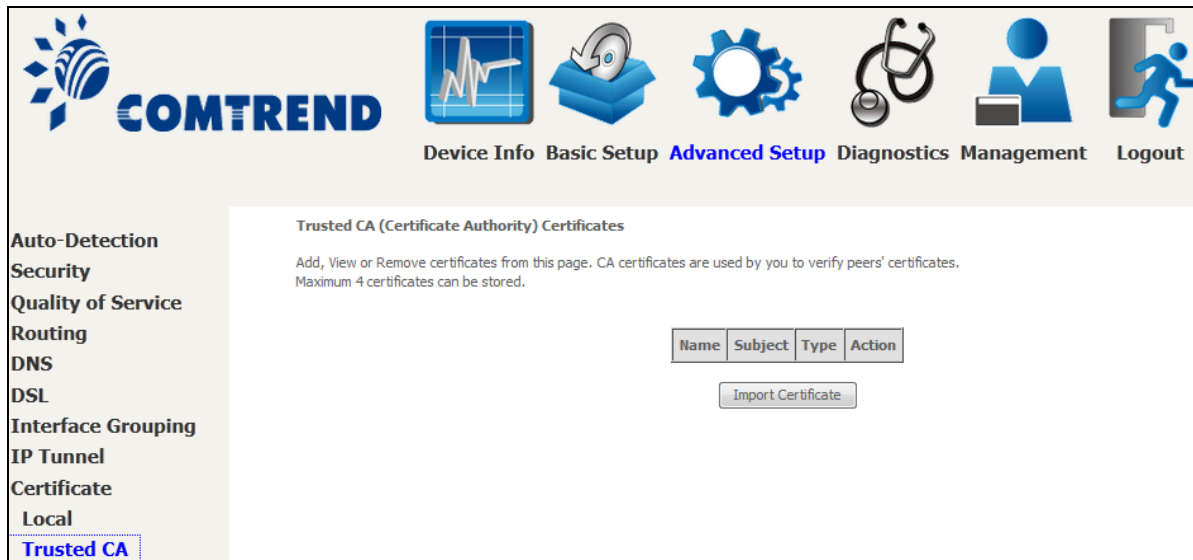
```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```
- Private Key:** A large text area containing the following text:

```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```
- Apply** button at the bottom right.

Enter a certificate name and click the **Apply** button to import the certificate and its private key.

6.9.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.



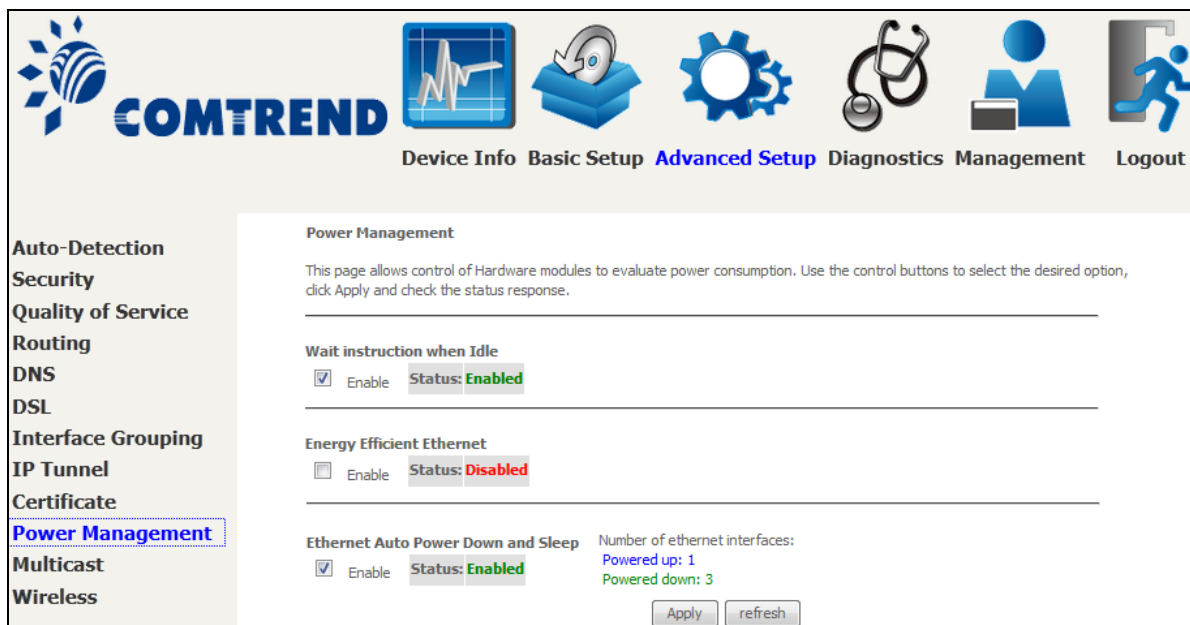
Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Enter a certificate name and click **Apply** to import the CA certificate.

6.10 Power Management

This screen allows for control of hardware modules to evaluate power consumption. Use the buttons to select the desired option, click **Apply** and check the response.



The screenshot shows the COMTREND web interface for Power Management. The top navigation bar includes links for Device Info, Basic Setup, **Advanced Setup** (selected), Diagnostics, Management, and Logout. The left sidebar lists various configuration categories, with **Power Management** highlighted. The main content area is titled 'Power Management' and contains the following settings:

- Wait instruction when Idle:** A checkbox labeled 'Enable' is checked, and the status is 'Enabled'.
- Energy Efficient Ethernet:** A checkbox labeled 'Enable' is unchecked, and the status is 'Disabled'.
- Ethernet Auto Power Down and Sleep:** A checkbox labeled 'Enable' is checked, and the status is 'Enabled'.

Below the Ethernet Auto Power Down and Sleep section, there is a summary of the number of ethernet interfaces: 'Powered up: 1' and 'Powered down: 3'. At the bottom right of the main content area, there are 'Apply' and 'refresh' buttons.

6.11 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Apply/Save**.


COMTREND








Device Info
Basic Setup
Advanced Setup
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☒
LAN to LAN (Intra LAN) Multicast Enable:	☐
Membership Join Immediate (IPTV):	☐

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv3):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	☒
LAN to LAN (Intra LAN) Multicast Enable:	☐

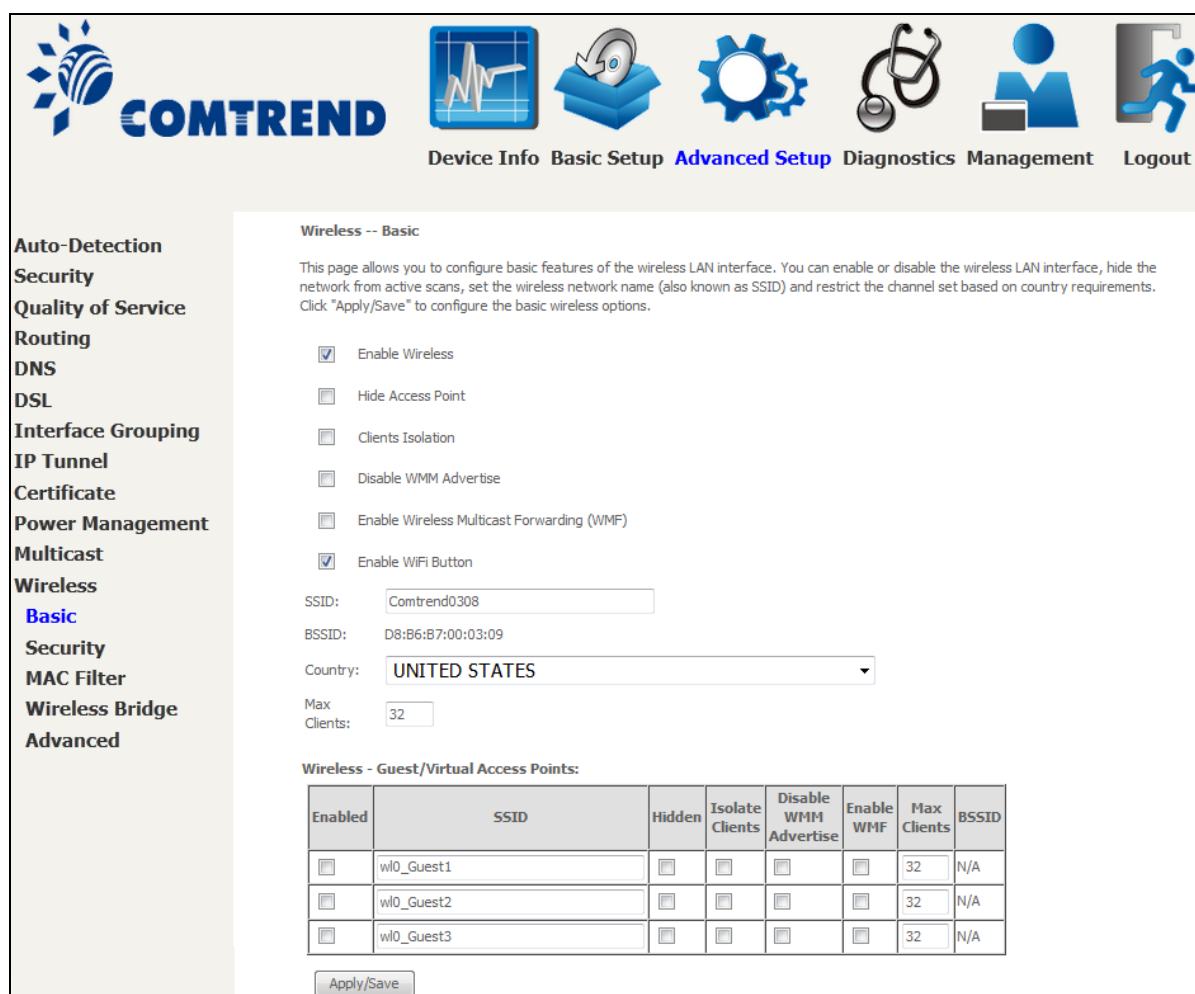
Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.

Field	Description
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.
LAN to LAN (Intra LAN) Multicast Enable	This will activate IGMP snooping for cases where multicast data source and player are all located on the LAN side.
Membership to join Immediate (IPTV)	Enable IGMP immediate join feature for multicast membership group.

6.12 Wireless

6.12.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Click **Apply/Save** to apply the selected wireless options.

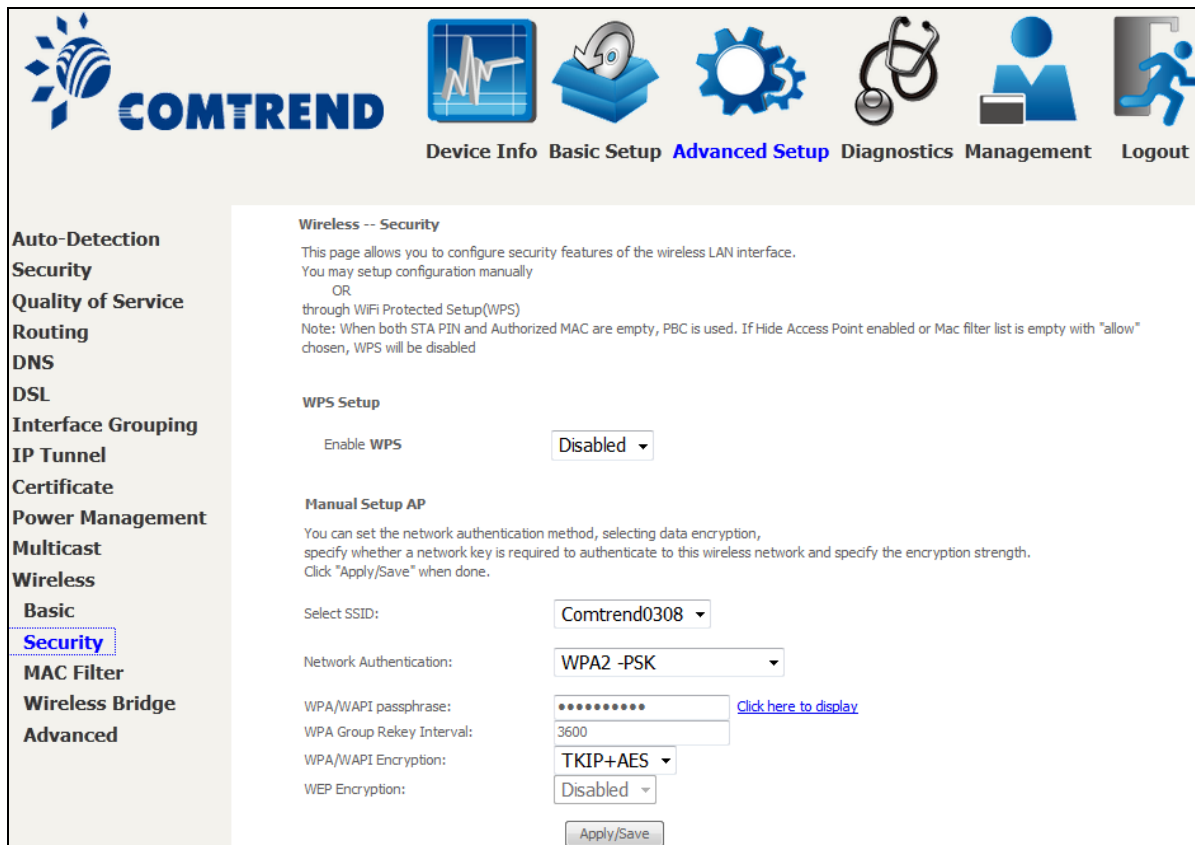
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☒ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. If the access point is hidden, it will not be listed or listed with empty SSID in the scan result of wireless stations. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.

Option	Description
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox ☒ to enable this function.
Enable WiFi Button	Select the checkbox ☒ to enable the WiFi button.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	Local regulations limit channel range: US/Canada = 1-11.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☒ in the Enabled column. To hide a Guest SSID select its checkbox ☒ in the Hidden column. Do the same for Isolate Clients and Disable WMM Advertise. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF, Max Clients and BSSID, consult the matching entries in this table. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

6.12.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



The screenshot shows the Comtrend Web User Interface. At the top, there is a navigation bar with icons and labels: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. On the left, a sidebar menu lists various configuration categories: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, Basic, **Security** (highlighted), MAC Filter, Wireless Bridge, and Advanced. The main content area is titled "Wireless -- Security". It contains the following sections:

- Wireless -- Security**: A paragraph stating, "This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS). Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS will be disabled."
- WPS Setup**: A section with "Enable WPS" set to a "Disabled" dropdown menu.
- Manual Setup AP**: A section with instructions: "You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Apply/Save' when done." It includes the following fields:
 - Select SSID: A dropdown menu showing "Comtrend0308".
 - Network Authentication: A dropdown menu showing "WPA2 -PSK".
 - WPA/WAPI passphrase: A text field with masked characters (dots) and a link "Click here to display".
 - WPA Group Rekey Interval: A text field showing "3600".
 - WPA/WAPI Encryption: A dropdown menu showing "TKIP+AES".
 - WEP Encryption: A dropdown menu showing "Disabled".

At the bottom of the main content area is an "Apply/Save" button.

Click **Apply/Save** to implement new configuration settings.

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

Network Authentication:	802.1X ▾
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled ▾
Encryption Strength:	128-bit ▾
Current Network Key:	2 ▾
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

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

Apply/Save

The settings for WPA authentication are shown below.

Network Authentication:	WPA ▾
WPA Group Rekey Interval:	3600
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	TKIP+AES ▾
WEP Encryption:	Disabled ▾

Apply/Save

The settings for WPA-PSK authentication are shown next.

Network Authentication:	WPA-PSK ▾
WPA/WAPI passphrase:	•••••••• Click here to display
WPA Group Rekey Interval:	3600
WPA/WAPI Encryption:	TKIP+AES ▾
WEP Encryption:	Disabled ▾

Apply/Save

WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.12.3 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The AR-5313u has a WPS button on the device.

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



NOTE: WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

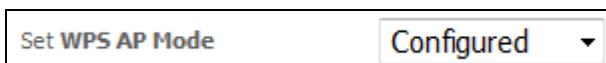
To configure security settings with WPS, follow the procedures below.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.

A screenshot of a web interface for WPS Setup. It shows a label 'WPS Setup' in blue. Below it is a label 'Enable WPS' and a dropdown menu currently set to 'Enabled' with a downward arrow.

Step 2: Set the WPS AP Mode. **Configured** is used when the AR-5313u will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the AR-5313u.

A screenshot of a web interface for setting WPS AP Mode. It shows a label 'Set WPS AP Mode' and a dropdown menu currently set to 'Configured' with a downward arrow.

NOTES: Your client may or may not have the ability to provide security settings to the AR-5313u. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

IIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

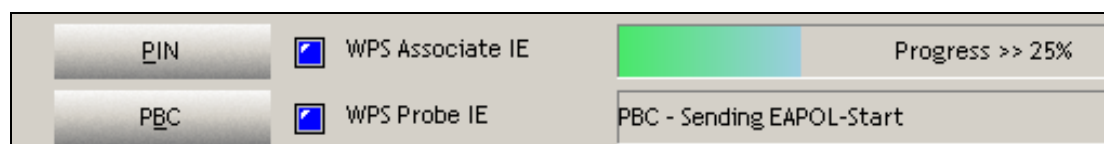
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 4, return to Step 3.

Step 3: Press WPS button

Press the WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Step 4: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



IIb. WPS – PIN CONFIGURATION

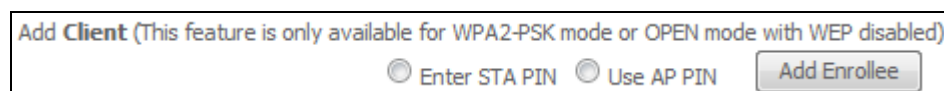
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

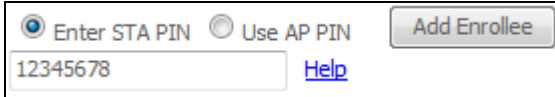
NOTE: Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

Step 5: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

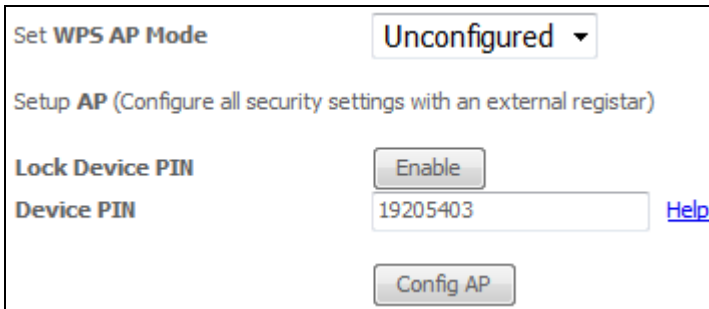
A - For Configured mode, click the Add Enrollee button.



Enter STA PIN: a Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be inputted at representing the network, usually the Access Point of the network.

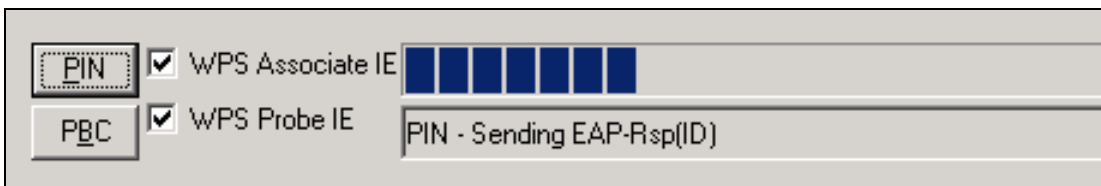


B - For **Unconfigured** mode, click the **Config AP** button.



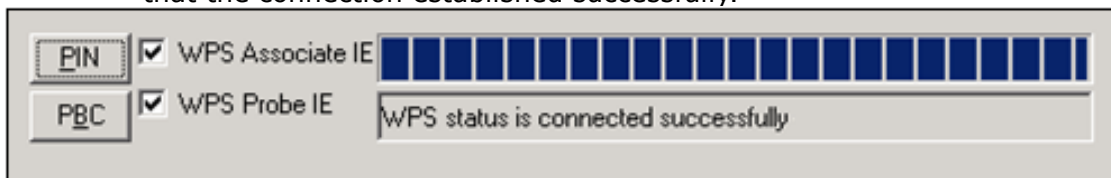
Step 6: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

The figure below provides an example of a WPS client PIN function in-progress.



III. CHECK CONNECTION

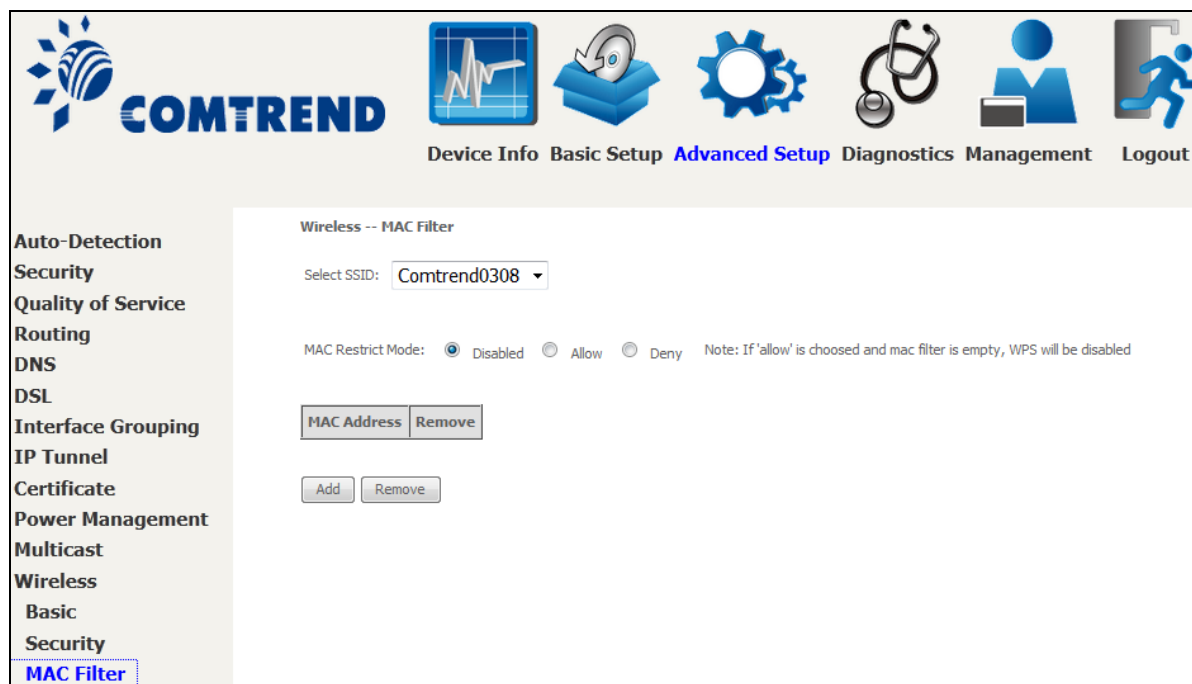
Step 7: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

6.12.4 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.



Option	Description
Select SSID	Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.

 **COMTREND**
     
Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

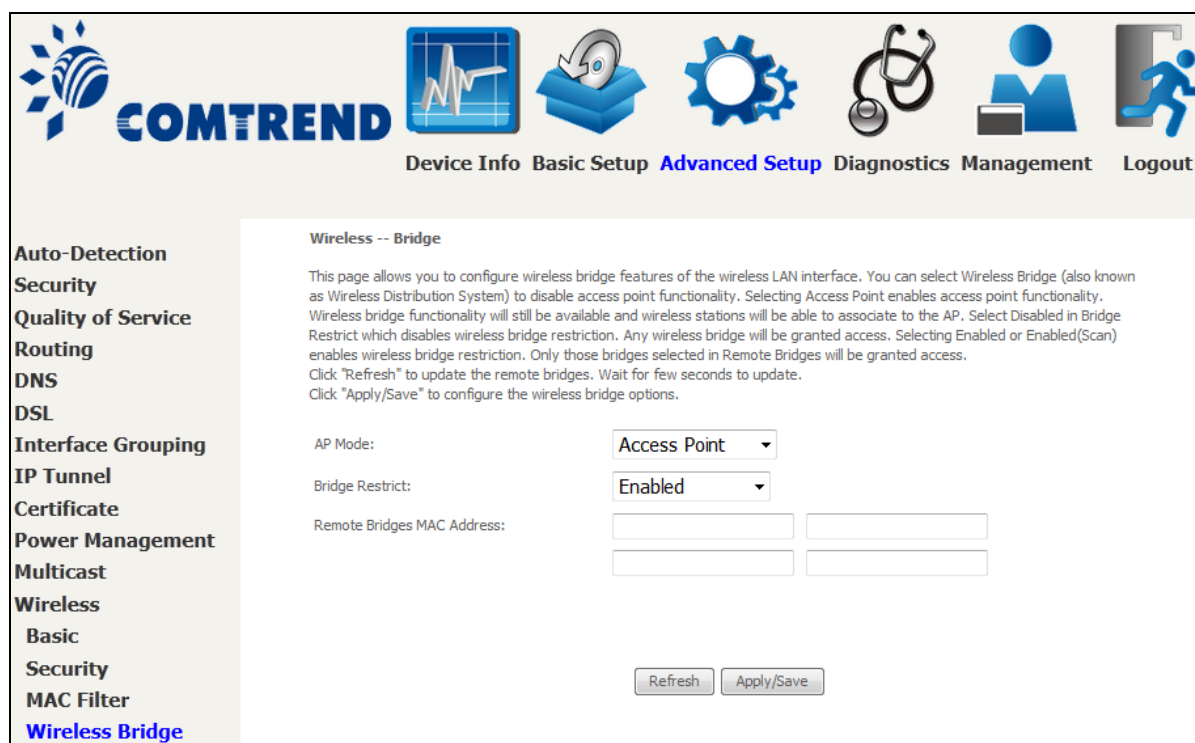
Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless
 Basic
 Security
 MAC Filter

Wireless -- MAC Filter
Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.
MAC Address:

Enter the MAC address in the box provided and click **Apply/Save**.

6.12.5 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WIFI interface. See the table beneath for detailed explanations of the various options.



COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless
 Basic
 Security
 MAC Filter
Wireless Bridge

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

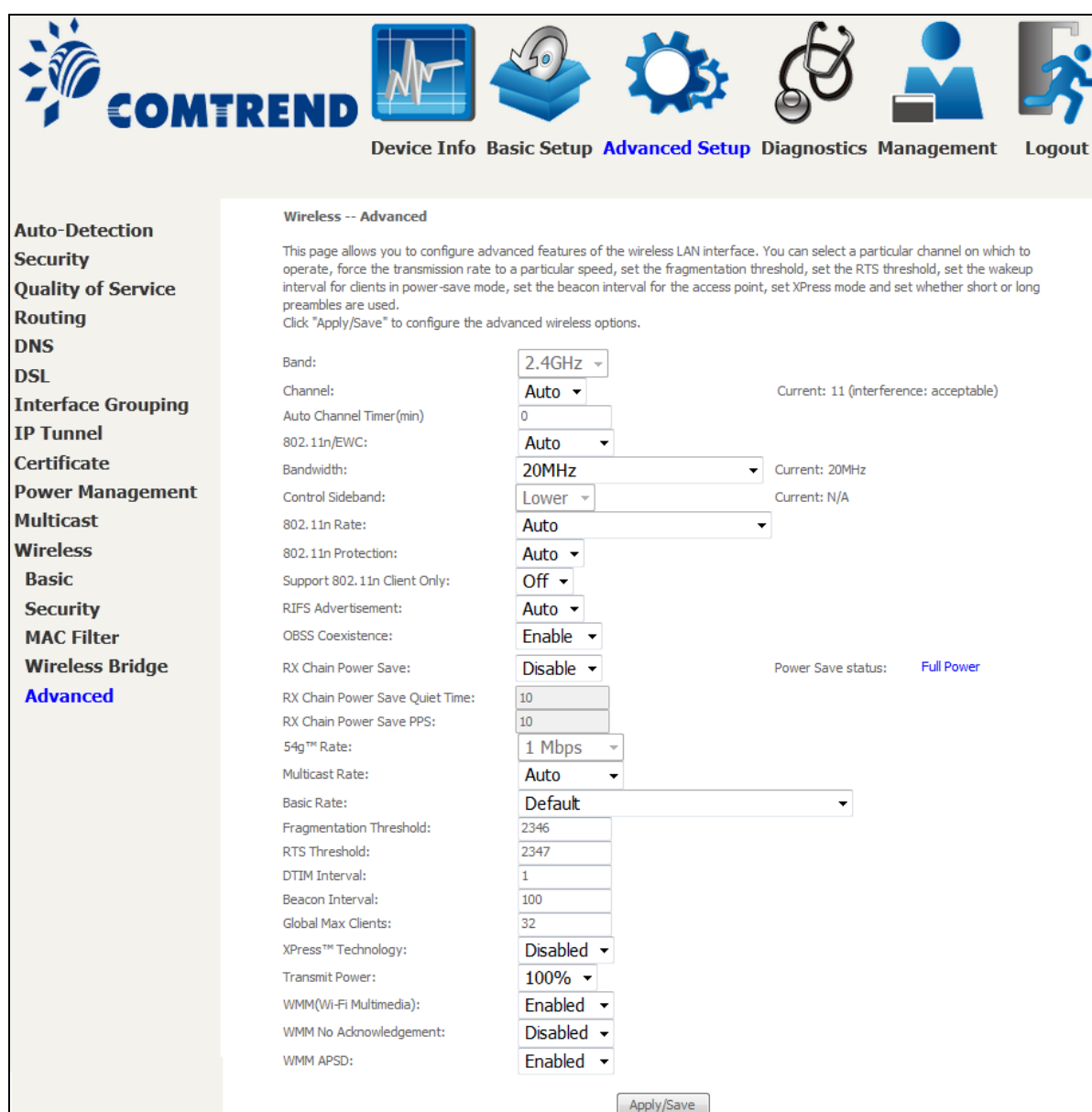
Remote Bridges MAC Address:

Click **Apply/Save** to implement new configuration settings.

Feature	Description
AP Mode	Selecting Wireless Bridge (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

6.12.6 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Apply/Save** to set new advanced wireless options.



The screenshot shows the COMTREND web interface with the 'Advanced Setup' tab selected. The left sidebar contains a menu with options: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, Basic, Security, MAC Filter, Wireless Bridge, and Advanced (highlighted in blue). The main content area is titled 'Wireless -- Advanced' and contains a description of the page's purpose. Below the description is a list of configuration parameters, each with a dropdown menu or input field. The parameters are: Band (2.4GHz), Channel (Auto), Auto Channel Timer (min) (0), 802.11n/EWC (Auto), Bandwidth (20MHz), Control Sideband (Lower), 802.11n Rate (Auto), 802.11n Protection (Auto), Support 802.11n Client Only (Off), RIFS Advertisement (Auto), OBSS Coexistence (Enable), RX Chain Power Save (Disable), RX Chain Power Save Quiet Time (10), RX Chain Power Save PPS (10), 54g™ Rate (1 Mbps), Multicast Rate (Auto), Basic Rate (Default), Fragmentation Threshold (2346), RTS Threshold (2347), DTIM Interval (1), Beacon Interval (100), Global Max Clients (32), XPress™ Technology (Disabled), Transmit Power (100%), WMM(Wi-Fi Multimedia) (Enabled), WMM No Acknowledgement (Disabled), and WMM APSD (Enabled). The 'Power Save status' is shown as 'Full Power'. An 'Apply/Save' button is located at the bottom right of the configuration area.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	Auto	Current: 11 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz	Current: 20MHz
Control Sideband:	Lower	Current: N/A
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Auto	
OBSS Coexistence:	Enable	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	32	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Apply/Save

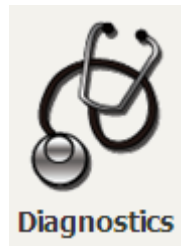
Consult the table below for detailed parameter descriptions.

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20MHz or 40MHz bandwidth. 40MHz bandwidth uses two adjacent 20MHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40MHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g client's access to the router.
RIFS Advertisement	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in 802.11a or g.
OBSS Co-Existence	Co-existence between 20 MHz AND 40 MHz overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.

Field	Description
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a 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 milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

Chapter 7 Diagnostics

You can reach this page by clicking on the following icon located at the top of the screen.



7.1 Diagnostics – Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.

 **COMTREND**








Device Info Basic Setup Advanced Setup **Diagnostics** Management Logout

Diagnostics
Fault Management
Uptime Status
Ping
TraceRoute
System Utilization

LAN






ETH1

ETH2

ETH3

ETH4

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:00:03:08
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254

Device

Model	AR-5313u
Serial Number	1555313UXXF-AA000006
Firmware Version	SE31-412CTU-C01_R01.A2pG039k.d25f
Bootloader (CFE) Version	1.0.38-112.118-46
Up Time	58 mins:35 secs
System Log	Show

Click the Diagnostics Menu item on the left side of the screen to display the individual connections.

 **COMTREND**








Device Info Basic Setup Advanced Setup **Diagnostics** Management Logout

Diagnostics
Fault Management
Uptime Status
Ping
TraceRoute
System Utilization

Diagnostics

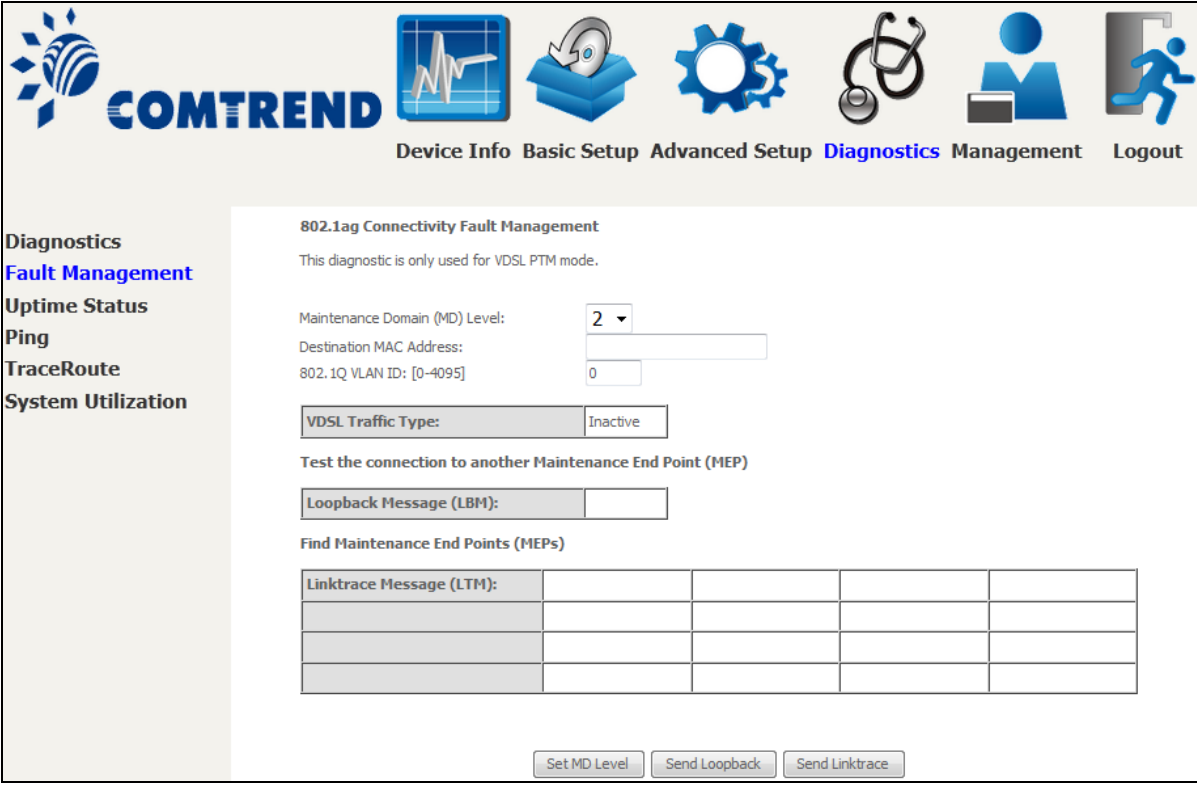
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ETH1 Connection:	FAIL	Help
Test your ETH2 Connection:	FAIL	Help
Test your ETH3 Connection:	PASS	Help
Test your ETH4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

[Rerun Diagnostic Tests](#)

7.2 Fault Management



802.1ag Connectivity Fault Management

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

Set MD Level Send Loopback Send Linktrace

Item	Description
Maintenance Domain (MD) Level	Management space on the network, the larger the domain, the higher the level value
Destination MAC Address	Destination MAC address for sending the loopback message
802.1Q VLAN ID: [0-4095]	802.1Q VLAN used in VDSL PTM mode

Set MD Level

Save the Maintenance domain level.

Send Loopback

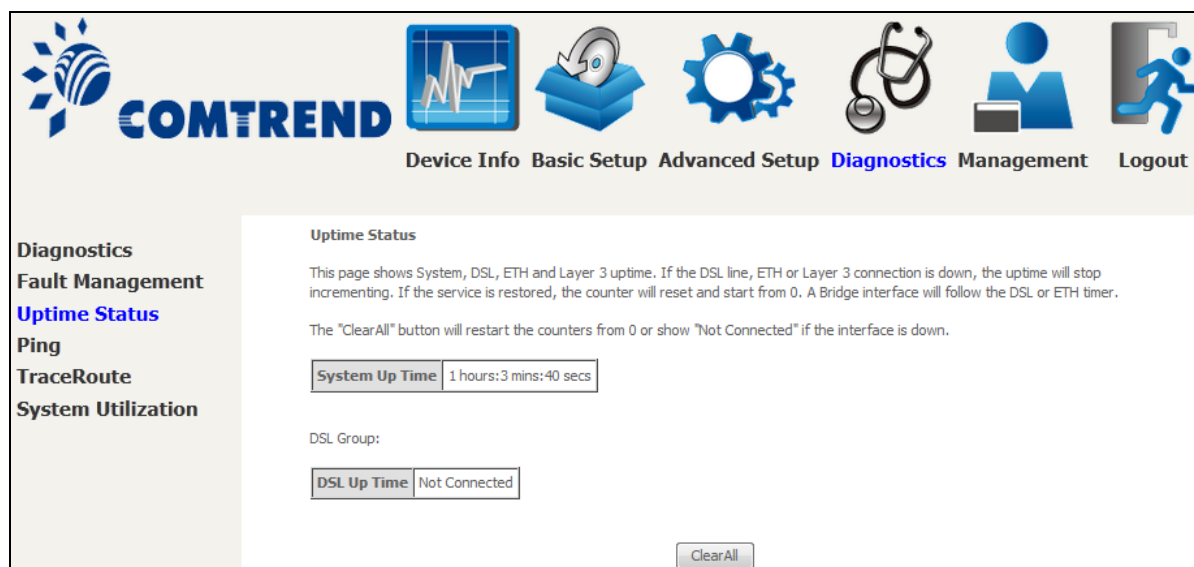
Send loopback message to destination MAC address.

Send Linktrace

Send traceroute message to destination MAC address.

7.3 Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.



The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted), Management, and Logout. The left sidebar lists: Diagnostics, Fault Management, **Uptime Status** (highlighted), Ping, TraceRoute, and System Utilization. The main content area is titled "Uptime Status" and contains the following text:

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

System Up Time	1 hours:3 mins:40 secs
----------------	------------------------

DSL Group:

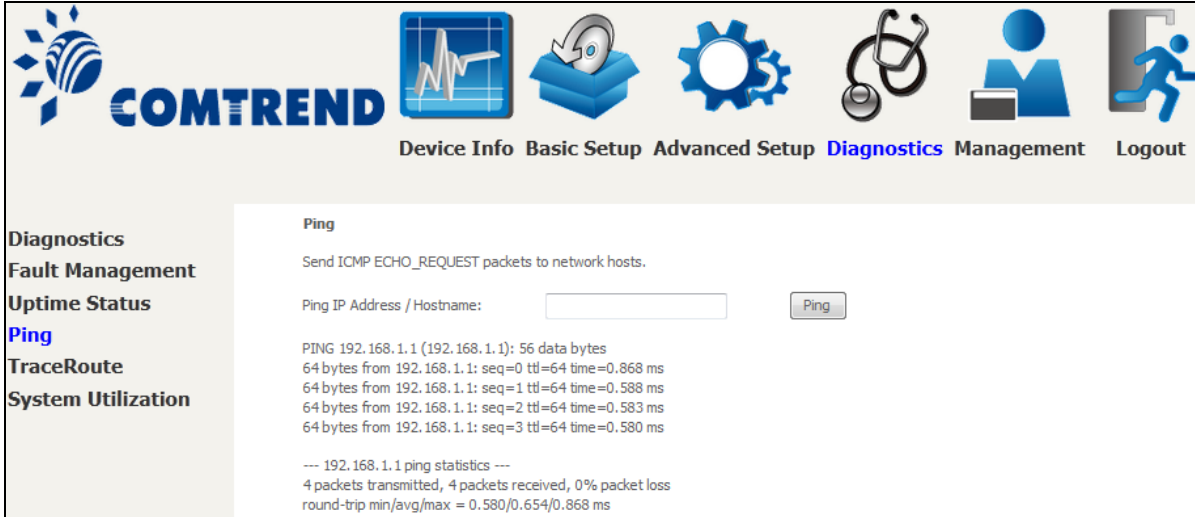
DSL Up Time	Not Connected
-------------	---------------

At the bottom right of the main content area is a "ClearAll" button.

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

7.4 Ping

Input the IP address/hostname and click the **Ping** button to execute ping diagnostic test to send the ICMP request to the specified host.



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted), Management, and Logout. On the left side, there is a sidebar menu with the following items: Diagnostics, Fault Management, Uptime Status, **Ping** (highlighted), TraceRoute, and System Utilization. The main content area is titled "Ping" and contains the following text:

Send ICMP ECHO_REQUEST packets to network hosts.

Ping IP Address / Hostname:

PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.868 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.588 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.583 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.580 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.580/0.654/0.868 ms

7.5 Trace Route

Input the IP address/hostname and click the **TraceRoute** button to execute the trace route diagnostic test to send the ICMP packets to the specified host.



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted in blue), Management, and Logout. On the left side, there is a sidebar menu with the following items: Diagnostics, Fault Management, Uptime Status, Ping, **TraceRoute** (highlighted in blue), and System Utilization. The main content area is titled "TraceRoute" and contains the following text: "Trace the route ip packets follow going to 'host'." Below this, there is a label "TraceRoute IP Address / Hostname:" followed by a text input field and a "TraceRoute" button. At the bottom of the main content area, there is a sample output of a traceroute command: "traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets" and "1 192.168.1.1 (192.168.1.1) 1.179 ms".

7.6 System Utilization

 **COMTREND**








[Device Info](#)
[Basic Setup](#)
[Advanced Setup](#)
[Diagnostics](#)
[Management](#)
[Logout](#)

[Diagnostics](#)
[Fault Management](#)
[Uptime Status](#)
[Ping](#)
[TraceRoute](#)
[System Utilization](#)

System Utilization

Click "Start" button to initialize CPU and Memory utilization calculation.
Please wait 10 seconds for the test to run.

Click "Start" button to initialize CPU and Memory utilization calculation.
Please wait 10 seconds for the test to run.

 **COMTREND**








[Device Info](#)
[Basic Setup](#)
[Advanced Setup](#)
[Diagnostics](#)
[Management](#)
[Logout](#)

[Diagnostics](#)
[Fault Management](#)
[Uptime Status](#)
[Ping](#)
[TraceRoute](#)
[System Utilization](#)

System Utilization

CPU Utilization: (100%)	100.00%
Memory Usage: (78%)	78.00%

Chapter 8 Management

You can reach this page by clicking on the following icon located at the top of the screen.



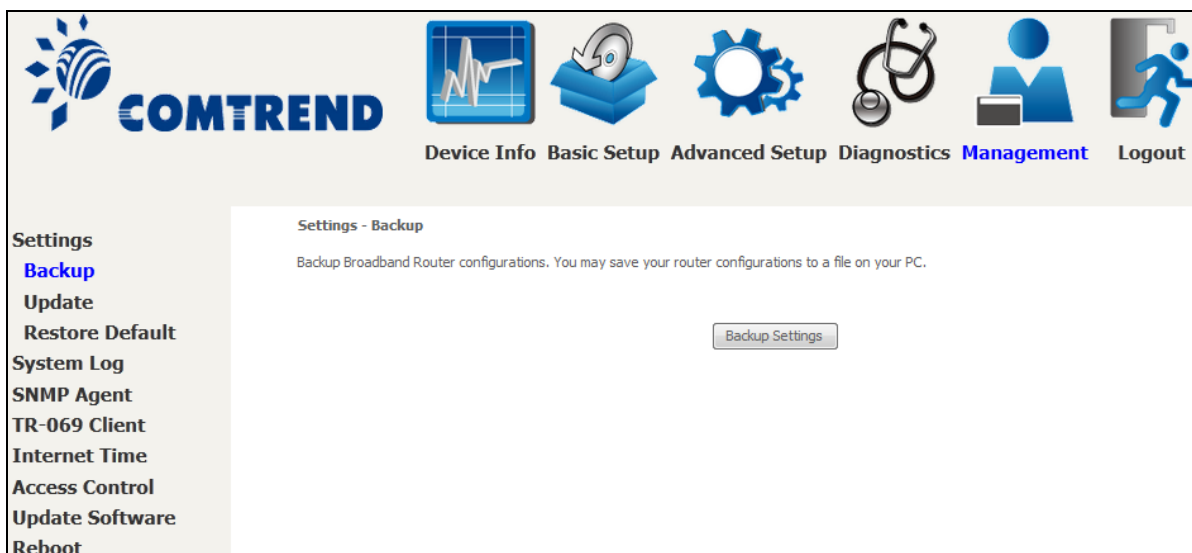
The Management menu has the following maintenance functions and processes:

8.1 Settings

This includes [Backup Settings](#), [Update Settings](#), and [Restore Default](#) screens.

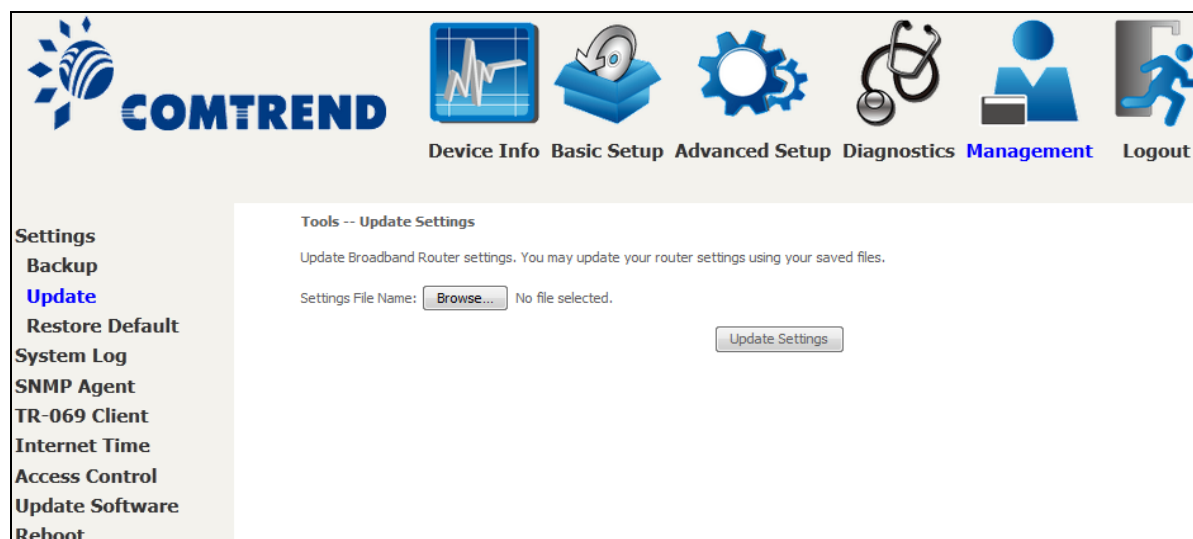
8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



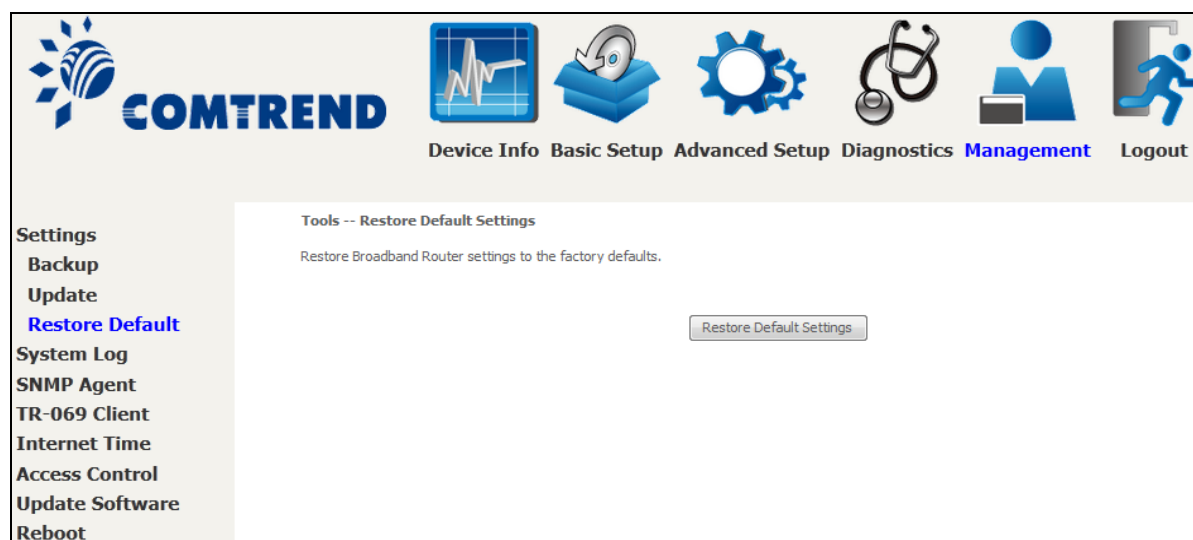
8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Press **Browse...** to search for the file, or enter the file name (including folder path) in the **File Name** box, and then click **Update Settings** to recover settings.



8.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.

Broadband Router Restore

The Broadband Router configuration has been restored to default settings and the router is rebooting.

Close the Broadband Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.