

## 5.5 Parental Control

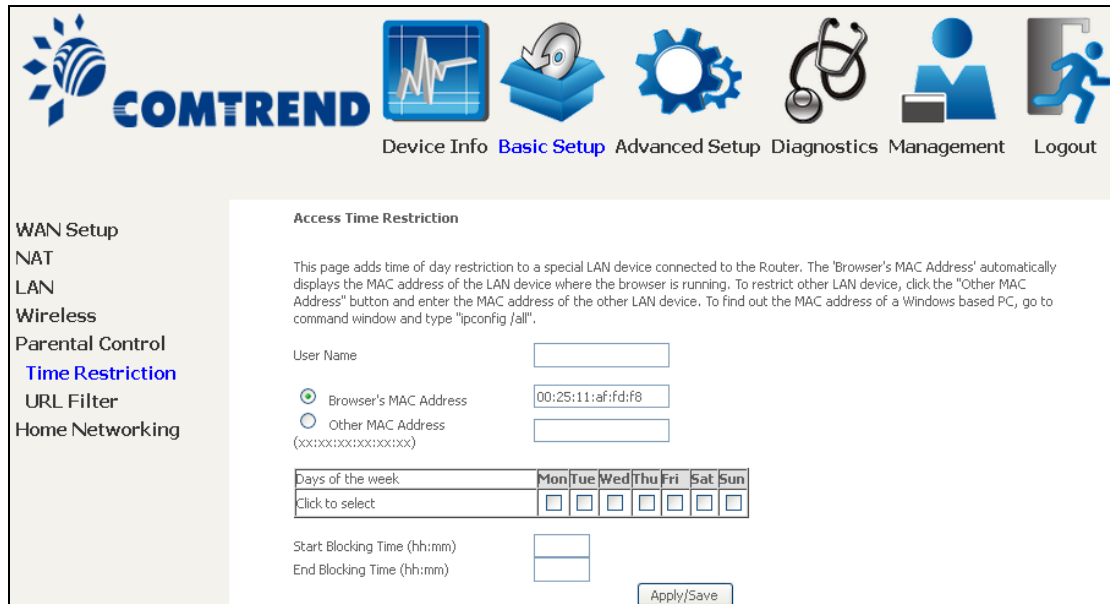
This selection provides WAN access control functionality.

### 5.5.1 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 section 8.5 [Internet Time](#), so that the scheduled times match your local time.



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




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.

## 5.5.2 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.



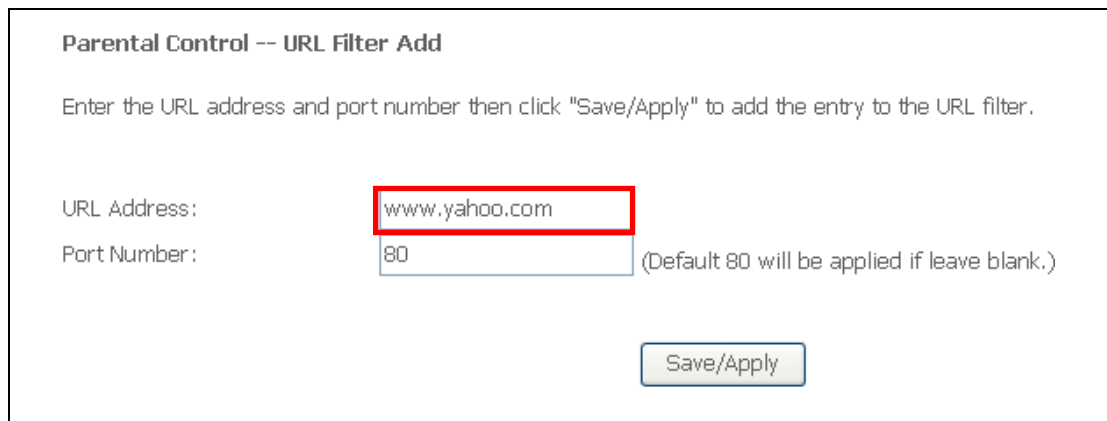
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons and labels for Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various settings: WAN Setup, NAT, LAN, Wireless, Parental Control, Time Restriction, URL Filter (highlighted), and Home Networking. The main content area is titled "URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured." Below this, a note states: "Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s)." There are two radio buttons for "URL List Type": "Exclude" (selected) and "Include". Below the radio buttons is a table with columns "Address", "Port", and "Remove". At the bottom of the table are "Add" and "Remove" buttons.

Select URL List Type: Exclude or Include.

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.

Then click **Add** to display the following screen.



The screenshot shows the "Parental Control -- URL Filter Add" screen. It contains the following text: "Enter the URL address and port number then click 'Save/Apply' to add the entry to the URL filter." Below this, there are two input fields: "URL Address:" with the value "www.yahoo.com" (highlighted with a red box) and "Port Number:" with the value "80". A note next to the port number field says "(Default 80 will be applied if leave blank.)". At the bottom right, there is a "Save/Apply" button.

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 -- A maximum 100 entries can be configured.**

URL List Type:  Exclude  Include

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

Add

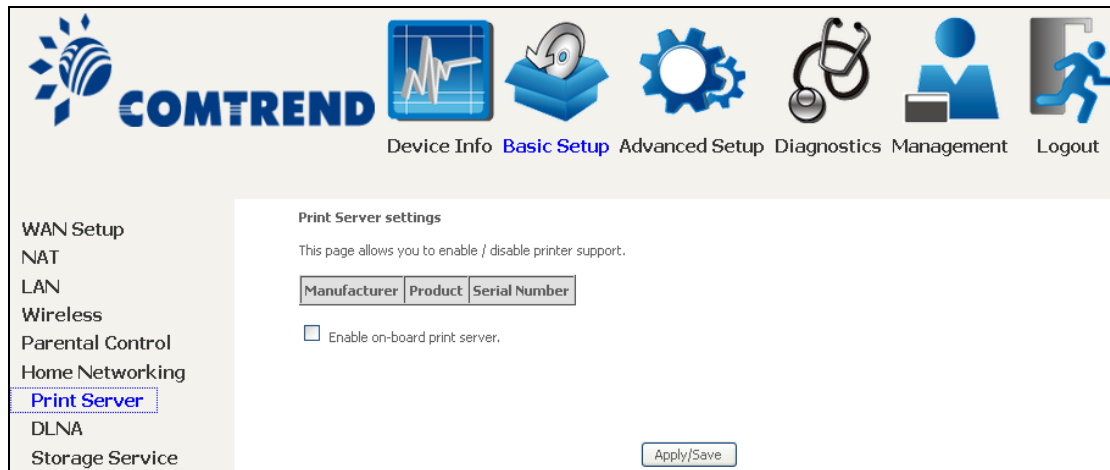
Remove

A maximum of 100 entries can be added to the URL Filter list.

## 5.6 Home networking

### 5.6.1 Print Server

This page allows you to enable or disable printer support.



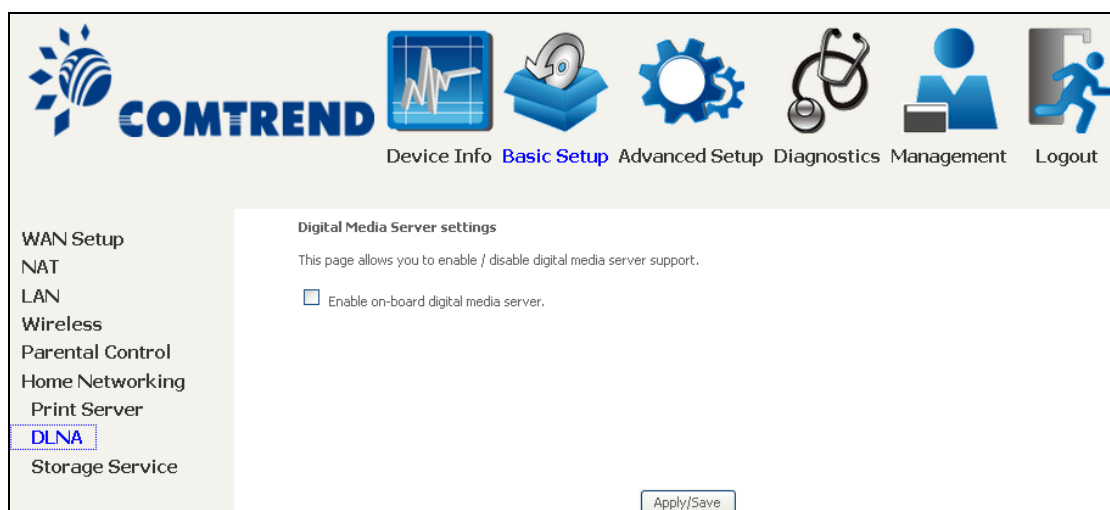
The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different settings: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with the following items: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server (highlighted), DLNA, and Storage Service. The main content area is titled "Print Server settings" and contains the following text: "This page allows you to enable / disable printer support." Below this text, there are three input fields labeled "Manufacturer", "Product", and "Serial Number". There is a checkbox labeled "Enable on-board print server." which is currently unchecked. At the bottom right of the main content area, there is an "Apply/Save" button.

Please reference [Appendix G](#) to see the procedure for enabling the Printer Server.

### 5.6.2 DLNA

Enabling DLNA allows users to share digital media, like pictures, music and video, to other LAN devices from the digital media server.

Insert USB drive to the USB host port on the back of router. Modify media library path to the corresponding path of the USB drive and click Apply/Save to enable the DLNA media server.



The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with the following items: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA (highlighted), and Storage Service. The main content area is titled "Digital Media Server settings" and contains the following text: "This page allows you to enable / disable digital media server support." Below this text, there is a checkbox labeled "Enable on-board digital media server." which is currently unchecked. At the bottom right of the main content area, there is an "Apply/Save" button.

### 5.6.3 Storage Service

Enabling Samba service allows the user to share files on the storage device. Different levels of user access can be configured after samba security mode is enabled. This page also displays storage devices attached to USB host.

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar contains a menu with options: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA, and Storage Service (highlighted in blue). The main content area is titled 'Samba Configuration for Storage Service'. It contains two configuration options: 'Samba Service' set to 'Disable' and 'Samba Security Mode' set to 'Enable'. Below these, a text block states: 'Access to your USB storage devices via Samba is always active. You can access them in the following ways:' followed by a bullet point: 'Simply open your File Explorer and go to \\comtrend.' At the bottom of the configuration area, there is a table with columns: Volumename, FileSystem, Total Space, Free Space, and Actions.

Display after storage device attached (for your reference).

Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	30517 MB	19419 MB	Safely remove

# Chapter 6 Advanced Setup

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

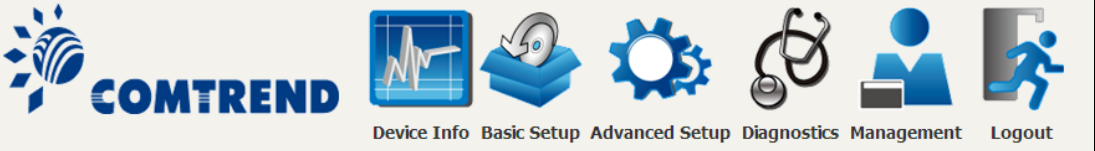


## 6.1 Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications.

A screenshot of a web interface for "COMTREND". The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. The main content area is titled "Auto-detection setup" and contains a paragraph explaining the function: "The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface when applicable. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking 'Apply/Save' will activate the auto-detect function." Below this text is a checkbox labeled "Enable auto-detect" which is currently unchecked. At the bottom right of the main content area are two buttons: "Apply/Save" and "Restart". On the left side of the screenshot, a sidebar menu lists various configuration options: Auto-Detection (highlighted), Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, and Interface Grouping.

The Auto Detection page simply provides a checkbox allowing users to enable or disable the feature. Check the checkbox to display the following configuration options.



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

**Auto-detection setup**

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.

Enable auto-detect

Auto-detection status: Waiting for DSL or Ethernet line connect

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Select a LAN-as-WAN Ethernet port for auto-detect:

Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order. A maximum 7 entries can be configured.

Select Service:

VPI[0-255]	VCI[32-65535]	Service	Option
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Default Bridge"/>	

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Enter the PPP username/password given by your service provider for PPP service detection.

**Select a LAN-as-WAN Ethernet port for auto-detect:**

Select the Ethernet Port that will be used as ETHWAN during auto-detection.

Select Service ATM ▾

VPI[0-255]	VCI[32-65535]	Service
0	32	Disable ▾
0	32	PPPoE
0	32	PPPoA
0	32	IPoE
0	32	Disable
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Default Bridge ▾

**WAN services list for ATM mode:** A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement and also reduce the detection cycle.

Select Service PTM/ETHWAN ▾

VLAN ID[0-4094]	Service
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Default Bridge ▾

**WAN services list for PTM mode:** A maximum of 7 WAN services with corresponding VLAN ID (-1 indicates no VLAN ID is required for the service) are required to be configured for ADSL/VDSL PTM mode and ETHWAN. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of the services to meet their own requirement and also reduce the detection cycle.





Click "Apply/Save" to activate the auto-detect function.

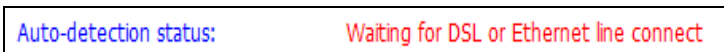
**Options for each WAN service:** These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

VPI[0-255]	VCI[32-65535]	Service	Option
0	33	PPPoE	<input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

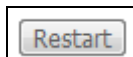
VLAN ID[0-4094]	Service	Option
8	PPPoE	<input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

### Auto Detection status and Restart

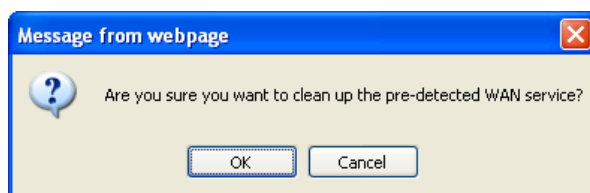
The Auto-detection status is used to display the real time status of the Auto-detection feature.



The **Restart** button is used to detect all the WAN services that are either detected by the auto-detection feature or configured manually by users.



The following window will pop up upon clicking the **Restart** button. Click the **OK** button to proceed.



### **Auto Detection notice**

**Note:** The following description concerning ETHWAN is for multiple LAN port devices only.

- 1) This feature will automatically detect one WAN service only. If customers require multiple WAN services, manual configuration is required.
- 2) If a physical ETHWAN port is detected, the Auto Detection for ETHWAN will be fixed on the physical ETHWAN port and cannot be configured for any LAN port; if the physical ETHWAN port is not detected, the Auto Detection for ETHWAN will be configured to the 4<sup>th</sup> LAN port by default and allows it to be configured for any LAN port as well.
- 3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
- 4) If none of the pre-configured services are detected, a Bridge service will be created.

## 6.2 Security

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

### 6.2.1 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, [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.



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. Below the navigation bar, there is a sidebar on the left with a menu containing: Auto-Detection, Security, IP Filtering (highlighted in blue), Outgoing, Incoming, and MAC Filtering. The main content area is titled "Outgoing IP Filtering Setup" and contains the following text: "By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters." Below this text is a table with the following columns: Filter Name, IP Version, Protocol, SrcIP/ PrefixLength, SrcPort, DstIP/ PrefixLength, DstPort, and Remove. At the bottom of the table, there are two buttons: "Add" and "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**.

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.

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  
 DSL Bonding  
 Interface Grouping  
 IP Tunnel  
 Certificate  
 Power Management  
 Multicast

**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:

Protocol:

Policy:

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 NexusLink 3112u 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.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The main content area is titled "MAC Filtering Setup". It contains the following text:

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	<input type="checkbox"/>

Below the table is a "Change Policy" button.

Choose Add or Remove to configure MAC filtering rules.

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

Below the table are "Add" and "Remove" buttons.

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.

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

Consult the table below for detailed field descriptions.

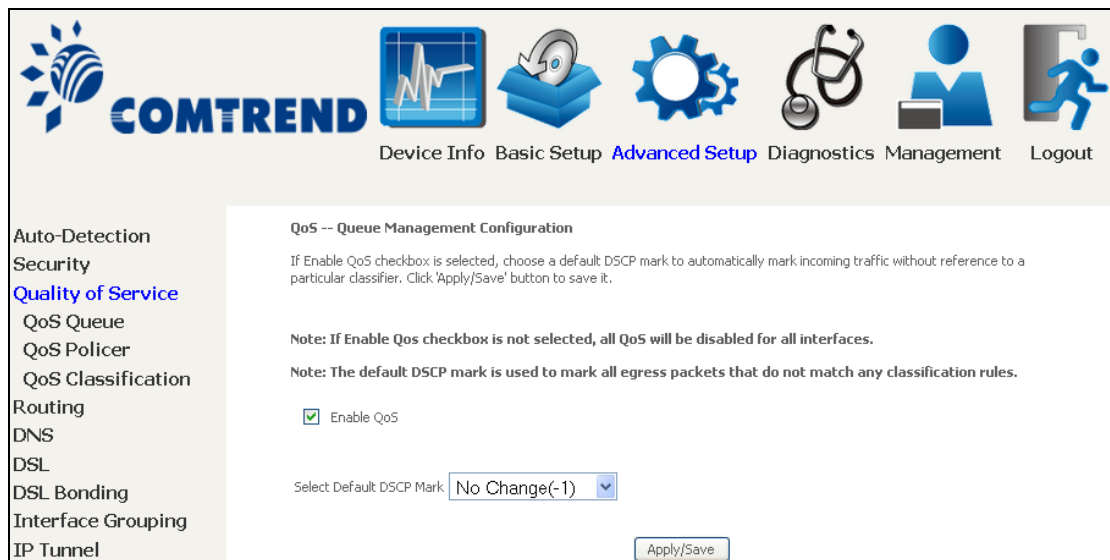
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected 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. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories: Auto-Detection, Security, **Quality of Service**, QoS Queue, QoS Policer, QoS Classification, Routing, DNS, DSL, DSL Bonding, Interface Grouping, and IP Tunnel. The main content area is titled "QoS -- Queue Management Configuration" and 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.

Enable QoS

Select Default DSCP Mark:

### 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.



### 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 3 queues can be configured.

**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 3 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.

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					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Voice Priority	2	wl0	2	2/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Video Priority	3	wl0	3	3/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Video Priority	4	wl0	4	4/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Best Effort	5	wl0	5	5/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Background	6	wl0	6	6/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Background	7	wl0	7	7/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Best Effort	8	wl0	8	8/SP					<input checked="" type="checkbox"/>	<input type="checkbox"/>
Default Queue	33	atm0	1	8/WRR/1	Path0				<input type="checkbox"/>	<input type="checkbox"/>

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

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

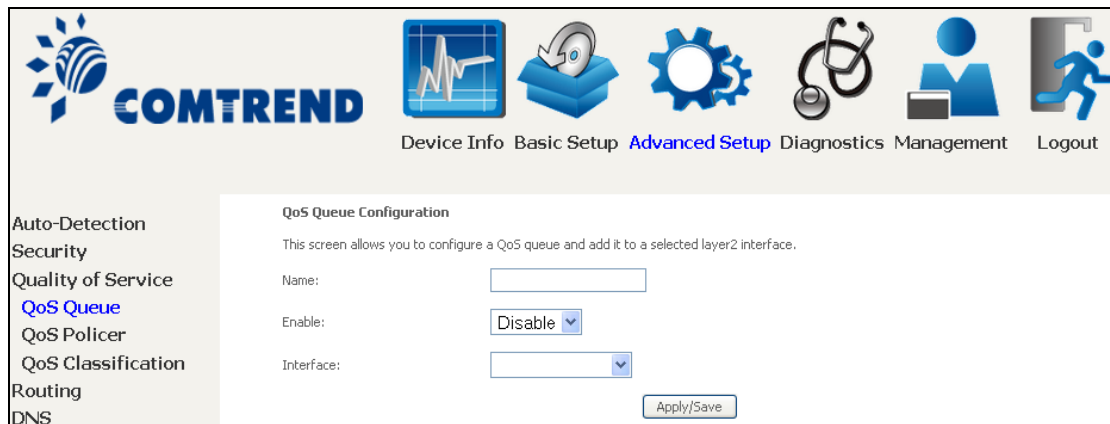
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

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 left is the Comtrend logo. To its right is a navigation bar with icons and labels: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. Below the navigation bar is a sidebar menu with the following items: Auto-Detection, Security, Quality of Service, **QoS Queue** (highlighted), 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 are three form fields: "Name:" with a text input box, "Enable:" with a dropdown menu set to "Disable", and "Interface:" with a dropdown menu. At the bottom right of the form 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

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.

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  
DSL Bonding  
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:

Apply/Save

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

<b>Field</b>	<b>Description</b>
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.

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.

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]

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.
<b>Classification Criteria</b>	
Class Interface	Select an interface (i.e. Local, eth0-4, w10)
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.
<b>Classification Results</b>	
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. Lower values have higher priority.
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.

The screenshot displays the Comtrend web interface for configuring the Default Gateway. The top navigation bar includes the Comtrend logo and icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. A left sidebar lists various configuration categories, with **Routing** expanded to show **Default Gateway** as the selected option. The main content area is titled "Routing -- Default Gateway" and contains the following elements:

- 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."
- Two empty list boxes: "Selected Default Gateway Interfaces" and "Available Routed WAN Interfaces".
- Two directional buttons: a right-pointing arrow (->) and a left-pointing arrow (<-).
- A "TODO" message: "TODO: IPv6 \*\*\*\*\* Select a preferred wan interface as the system default IPv6 gateway."
- A "Selected WAN Interface" dropdown menu currently set to "NO CONFIGURED INTERFACE".
- An "Apply/Save" button at the bottom right.

## 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.



COMTREND

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

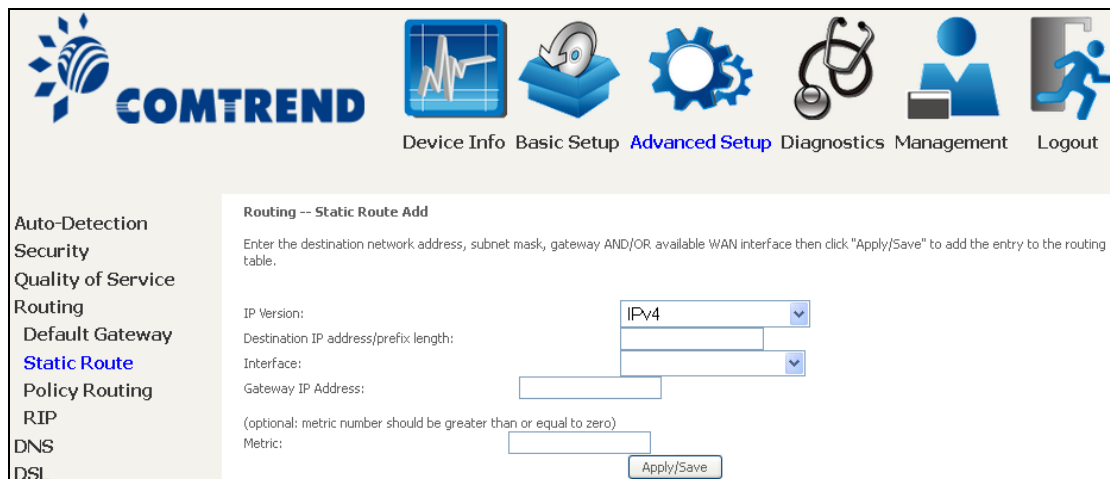
Auto-Detection  
Security  
Quality of Service  
Routing  
Default Gateway  
**Static Route**  
Policy Routing  
RIP

Routing -- Static Route (A maximum 32 entries can be configured)  
NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

Add Remove

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



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

Routing -- Static Route Add

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.

IP Version: IPv4  
Destination IP address/prefix length:  
Interface:  
Gateway IP Address:  
(optional: metric number should be greater than or equal to zero)  
Metric:  
Apply/Save

- **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.

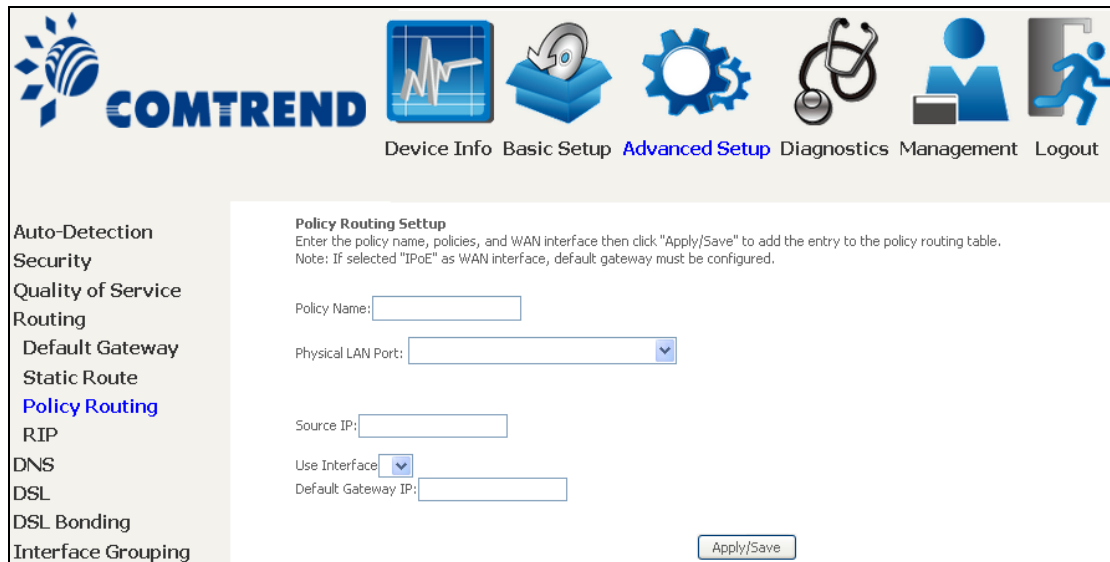


### 6.4.3 Policy Routing

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**.



The screenshot shows the Comtrend web interface for configuring RIP. The navigation menu on the left includes: Auto-Detection, Security, Quality of Service, Routing (selected), Default Gateway, Static Route, Policy Routing, RIP, DNS, DSL, and DSL Bonding. The main content area is titled "Routing -- RIP Configuration" and contains the following text:

**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
atm0.1	2	Passive	<input type="checkbox"/>

Apply/Save

## 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.

The screenshot shows the Comtrend web interface for DNS Server Configuration. At the top, there is a navigation bar with icons and labels for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various configuration options, with **DNS Server** highlighted. The main content area is titled "DNS Server Configuration" and contains the following text: "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."

Below the text, there are two radio buttons for configuration options:

- Select DNS Server Interface from available WAN interfaces:

This option includes two columns of scrollable lists: "Selected DNS Server Interfaces" and "Available WAN Interfaces". Between these lists are two buttons: "->" and "<-" for moving items between the lists.

The second radio button is selected:

- Use the following Static DNS IP address:

Below this, there are two input fields for "Primary DNS server:" and "Secondary DNS server:". At the bottom right of the configuration area is an "Apply/Save" button.

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 NexusLink 3112u 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.

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 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
-------------	------------	--------

Add Remove

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

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 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"/>

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".



The screenshot displays the Comtrend web management interface. At the top, the Comtrend logo is on the left, and navigation icons for Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout are on the right. A left sidebar lists menu items: Auto-Detection, Security, Quality of Service, Routing, DNS, DNS Server, Dynamic DNS, DNS Entries, and DNS Proxy/Relay (highlighted). 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:

- Enable DNS Relay

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

## 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

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
VDSL2	Downstream: 100 Mbps      Upstream: 60 Mbps
Options	Description
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
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.

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The 'Advanced Setup' icon is active. On the left side, there is a vertical menu with options: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL (highlighted in blue), DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, and Multicast. The main content area is titled 'DSL Advanced Settings' and contains the text 'Select the test mode below.' followed by five radio button options: 'Normal' (selected), 'Reverb', 'Medley', 'No retrain', and 'L3'. An 'Apply' button is located at the bottom right of the settings area.

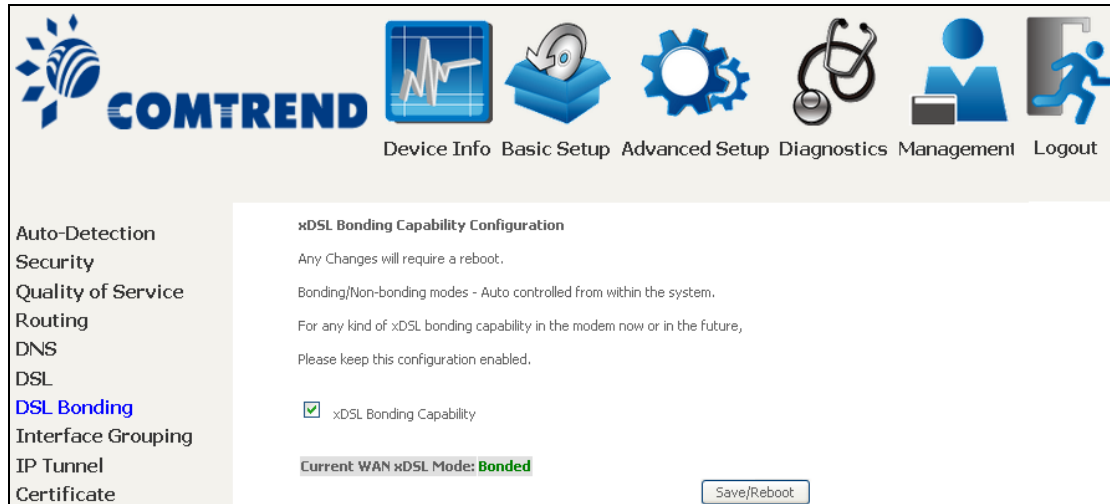
On this screen you select the required test mode, then click the **Apply** button.

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 DSL Bonding

This screen displays the current status of DSL bonding mode. Bonding status is detected automatically.



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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DSL  
**DSL Bonding**  
Interface Grouping  
IP Tunnel  
Certificate

**xDSL Bonding Capability Configuration**  
Any Changes will require a reboot.  
Bonding/Non-bonding modes - Auto controlled from within the system.  
For any kind of xDSL bonding capability in the modem now or in the future,  
Please keep this configuration enabled.

xDSL Bonding Capability

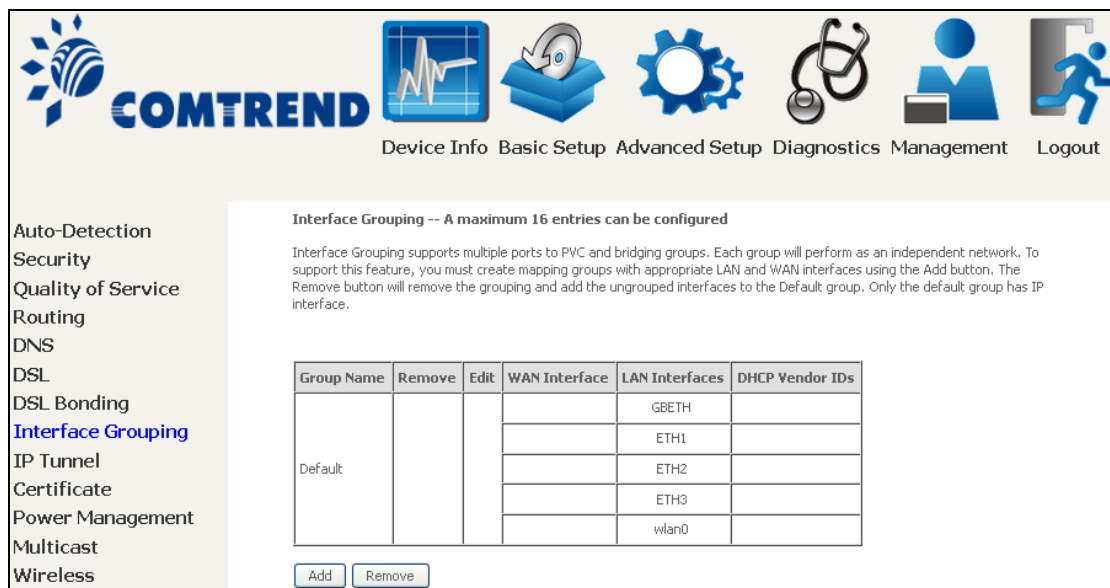
Current WAN xDSL Mode: **Bonded**

Save/Reboot

NOTE: This configuration doesn't take effect until router is rebooted.

## 6.8 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  
DSL Bonding  
**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				GBETH	
				ETH1	
				ETH2	
				ETH3	
				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**

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

**Auto-Detection**  
**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
**DSL**  
**DSL Bonding**  
**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**

GBETH  
 ETH1  
 ETH2  
 ETH3  
 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 GBETH.

The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and GBETH.
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 GBETH
2. Video: nas\_0\_36, nas\_0\_37, nas\_0\_38, and ETH1.

## 6.9 IP Tunnel

### 6.9.1 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

## 6.9.2 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  
DSL Bonding  
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  
DSL Bonding  
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:

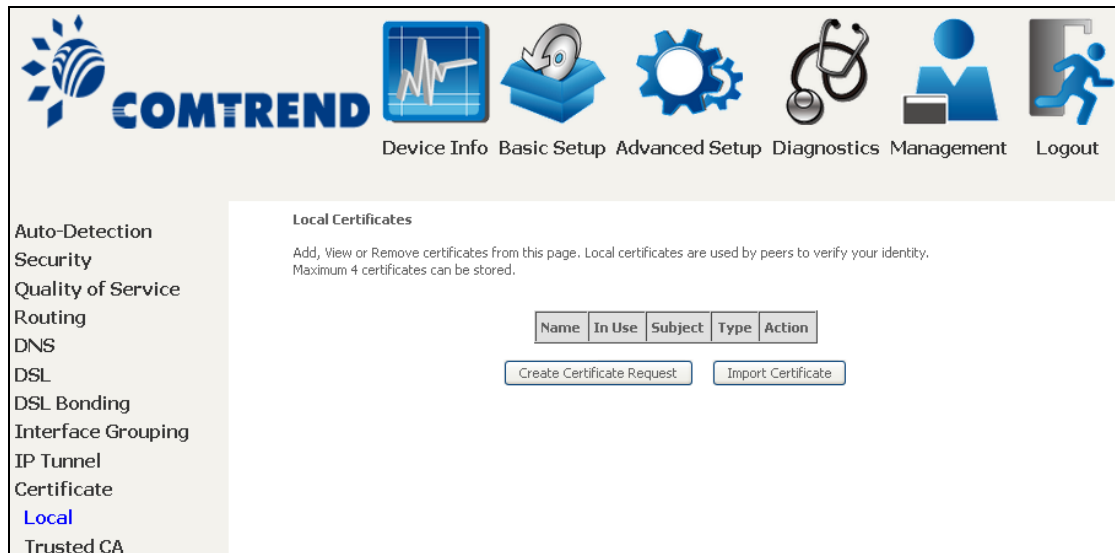
Apply/Save

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

## 6.10 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.

### 6.10.1 Local

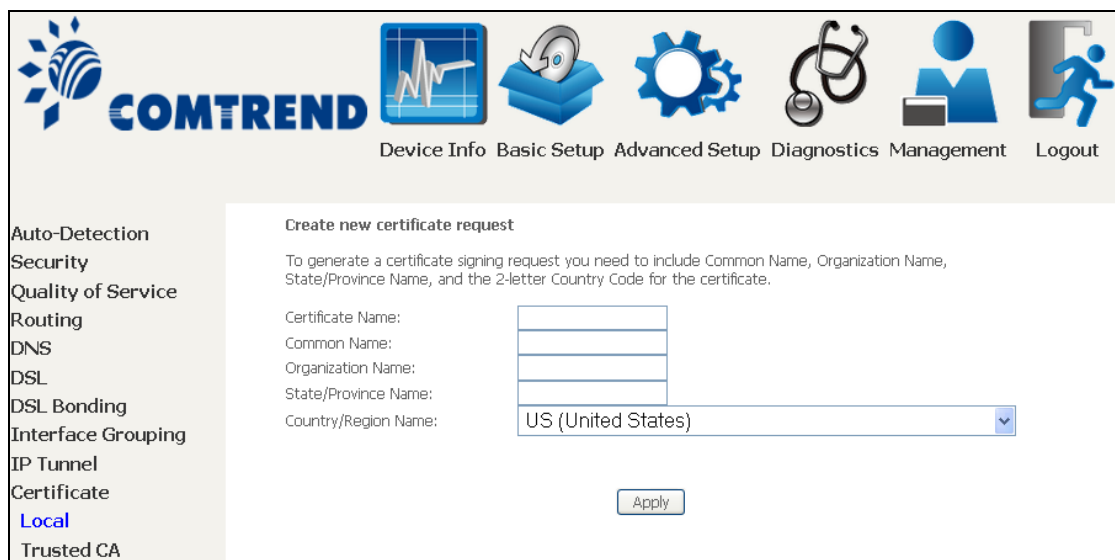


The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various configuration options, with 'Certificate' selected and 'Local' highlighted. The main content area is titled 'Local Certificates' and contains the following text: 'Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.' Below this text is a table with columns: Name, In Use, Subject, Type, and Action. At the bottom of the table are two buttons: 'Create Certificate Request' and '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.



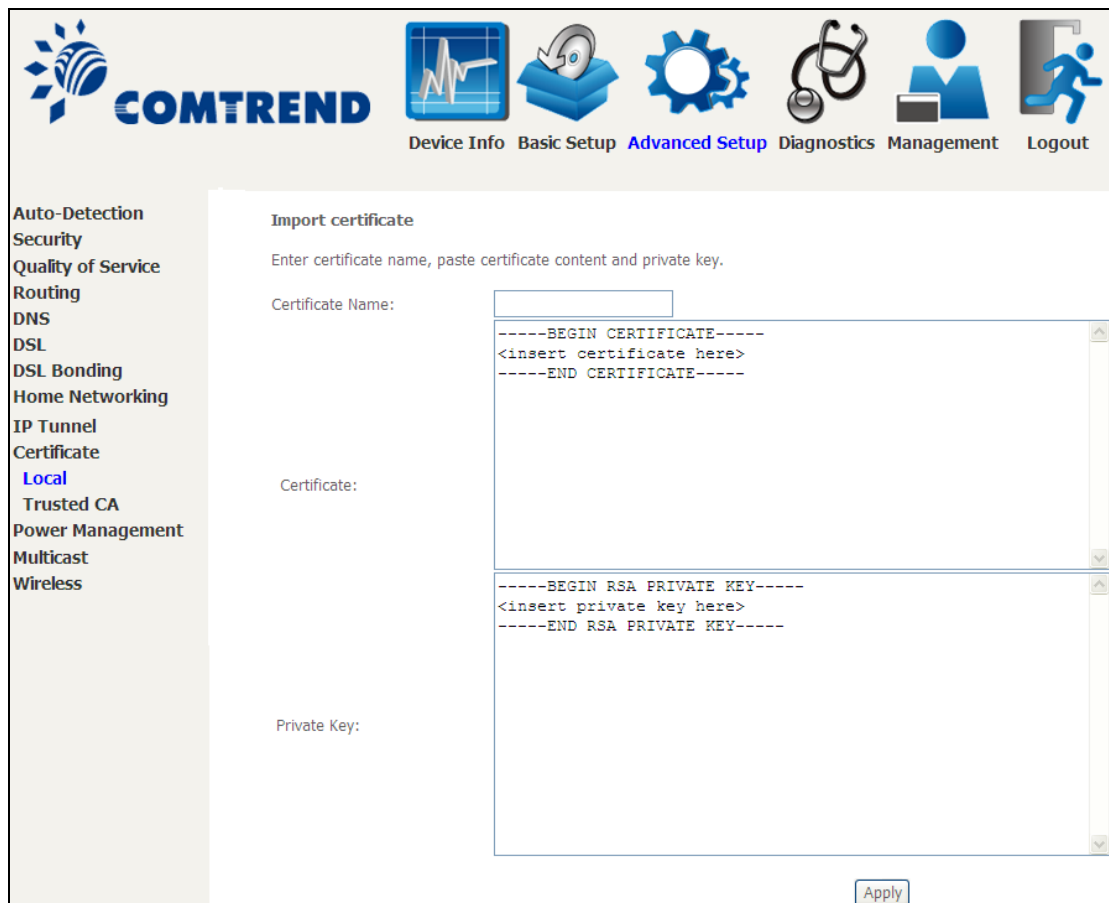
The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various configuration options, with 'Certificate' selected and 'Local' highlighted. The main content area is titled 'Create new certificate request' and contains the following text: '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.' Below this text are four input fields: 'Certificate Name:', 'Common Name:', 'Organization Name:', and 'State/Province Name:'. The 'Country/Region Name:' field is a dropdown menu with 'US (United States)' selected. At the bottom of the form is an 'Apply' button.

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.



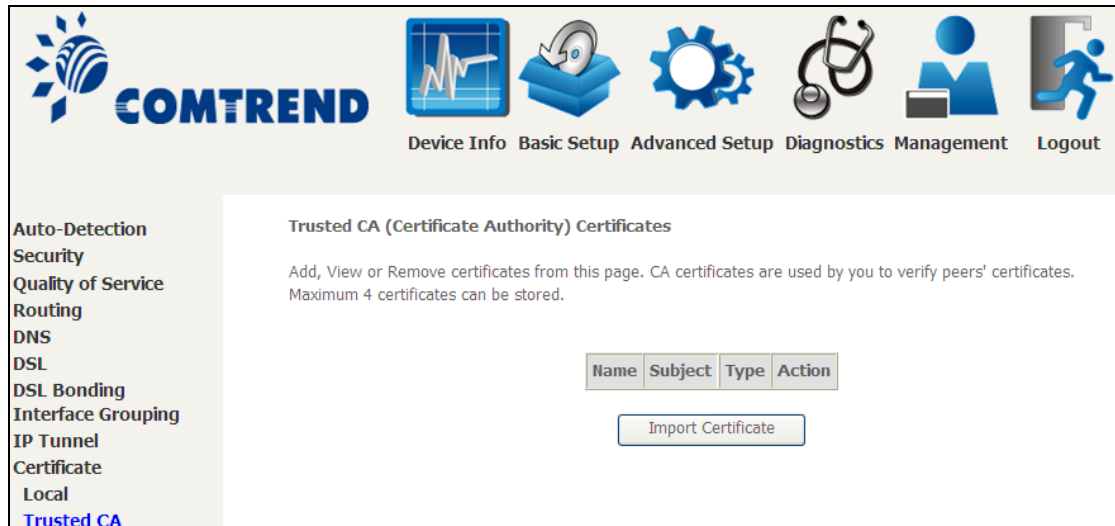
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons and labels for 'Device Info', 'Basic Setup', 'Advanced Setup', 'Diagnostics', 'Management', and 'Logout'. The 'Advanced Setup' option is highlighted. On the left side, there is a vertical menu with various configuration categories, including 'Certificate' which is currently selected. The main content area is titled 'Import certificate' and contains the following text: 'Enter certificate name, paste certificate content and private key.' Below this, there are three input fields: 'Certificate Name' (a small text box), 'Certificate' (a large text area containing the placeholder text: '-----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----'), and 'Private Key' (a large text area containing the placeholder text: '-----BEGIN RSA PRIVATE KEY-----<br><insert private key here><br>-----END RSA PRIVATE KEY-----'). At the bottom right of the form, there is an 'Apply' button.

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



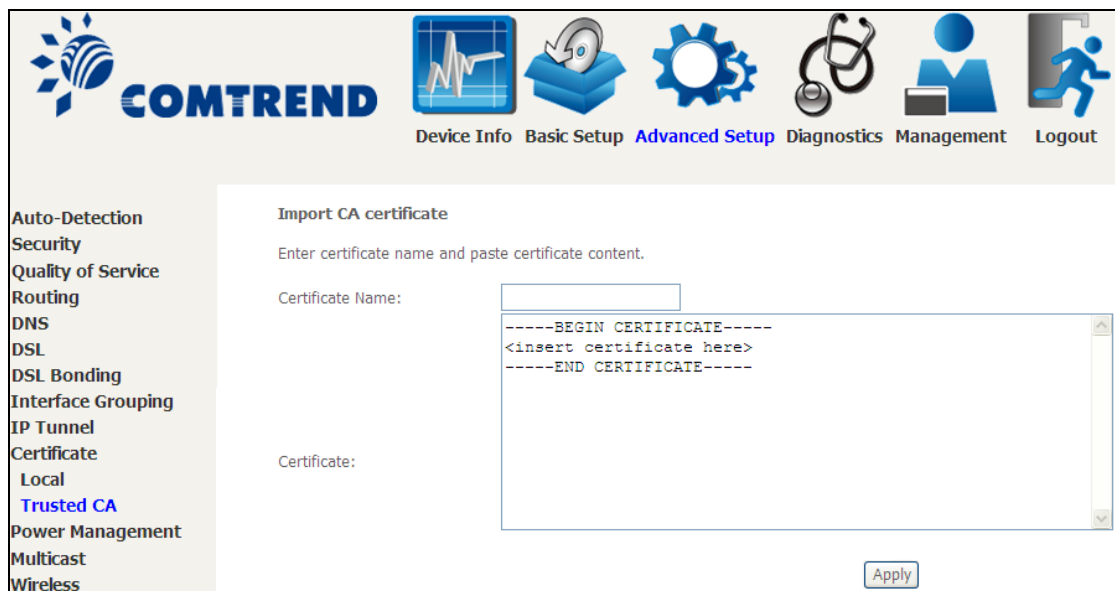
## 6.10.2 Trusted CA

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.



The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of menu items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Local, and Trusted CA (which is highlighted in blue). The main content area is titled "Trusted CA (Certificate Authority) Certificates". It contains the following text: "Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored." Below this text is a table with four columns: Name, Subject, Type, and Action. Below the table is a button labeled "Import Certificate".

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.



The screenshot shows the Comtrend web interface with the "Advanced Setup" menu item highlighted in the navigation bar. The sidebar on the left now includes "Power Management", "Multicast", and "Wireless" at the bottom. The main content area is titled "Import CA certificate". It contains the following text: "Enter certificate name and paste certificate content." Below this text is a form with two fields: "Certificate Name:" and "Certificate:". The "Certificate:" field is a large text area containing the following text: "-----BEGIN CERTIFICATE-----", "<insert certificate here>", and "-----END CERTIFICATE-----". Below the form is a button labeled "Apply".

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

## 6.11 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. At the top, there is a navigation bar with the COMTREND logo and icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar contains a list of menu items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management (highlighted in blue), Multicast, and Wireless. The main content area is titled "Power Management" and contains the following text: "This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response." Below this text are three sections: "Wait instruction when Idle" with a checked checkbox and "Status: Enabled"; "Energy Efficient Ethernet" with an unchecked checkbox and "Status: Disabled"; and "Ethernet Auto Power Down and Sleep" with a checked checkbox and "Status: Enabled". To the right of the "Ethernet Auto Power Down and Sleep" section, it says "Number of ethernet interfaces: Powered up: 1, Powered down: 3". At the bottom right of the main content area are "Apply" and "refresh" buttons.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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

**Power Management**

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

Wait instruction when Idle

Enable Status: **Enabled**

Energy Efficient Ethernet

Enable Status: **Disabled**

Ethernet Auto Power Down and Sleep Number of ethernet interfaces:  
 Enable Status: **Enabled** Powered up: 1  
Powered down: 3

Apply refresh

## 6.12 Multicast

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

The screenshot shows the COMTREND web interface with a navigation menu on the left and a main configuration area. The navigation menu includes: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, **Multicast**, and Wireless. The main area is titled 'IGMP Configuration' and contains the following fields:

- 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):

Below the IGMP configuration is the 'MLD Configuration' section with the following fields:

- 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:

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

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.

Field	Description
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.
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.

## 6.13 Wireless

### 6.13.1 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.

**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. 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 configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)
- Enable WiFi Button

SSID:

BSSID:

Country:

Max Clients:

**Wireless - Guest/Virtual Access Points:**

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

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

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox <input checked="" type="checkbox"/> that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.

Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open <b>Network Connections</b> from the <b>start</b> Menu and select <b>View Available Network Connections</b> . If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
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 <input checked="" type="checkbox"/> to enable this function.
Enable WiFi Button	Select the checkbox <input checked="" type="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	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	<p>This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes <input checked="" type="checkbox"/> in the <b>Enabled</b> column. To hide a Guest SSID select its checkbox <input checked="" type="checkbox"/> in the <b>Hidden</b> column.</p> <p>Do the same for <b>Isolate Clients</b> and <b>Disable WMM Advertise</b>. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for <b>Enable WMF</b>, <b>Max Clients</b> and <b>BSSID</b>, consult the matching entries in this table.</p> <p><b>NOTE:</b> Remote wireless hosts cannot scan Guest SSIDs.</p>

## 6.13.2 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 interface for configuring wireless security. The top navigation bar includes the Comtrend logo and icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories, with 'Security' highlighted. The main content area is titled 'Wireless -- Security' and contains the following sections:

- Wireless -- Security**: A descriptive paragraph stating that this page allows for configuring security features of the wireless LAN interface, either manually or through WiFi Protected Setup (WPS). A note specifies that WPS will be disabled if both STA PIN and Authorized MAC are empty, or if Hide Access Point is enabled or Mac filter list is empty with "allow" chosen.
- WPS Setup**: A section with a single configuration item: 'Enable WPS' set to a dropdown menu showing 'Disabled'.
- Manual Setup AP**: A section explaining that users can set the network authentication method, data encryption, and whether a network key is required. It instructs users to click 'Apply/Save' when done.
- Configuration Fields**:
  - 'Select SSID': A dropdown menu showing 'Comtrend3D8D'.
  - 'Network Authentication': A dropdown menu showing 'WPA2-PSK'.
  - 'WPA/WAPI passphrase': A text input field with masked characters (dots) and a link 'Click here to display'.
  - 'WPA Group Rekey Interval': A text input field containing '3600'.
  - 'WPA/WAPI Encryption': A dropdown menu showing 'TKIP+AES'.
  - 'WEP Encryption': A dropdown menu showing 'Disabled'.
- Apply/Save**: A button at the bottom of the configuration area.

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	<input type="button" value="v"/>
WPA/WAPI passphrase:	●●●●●●●●●●●●●●	<a href="#">Click here to display</a>
WPA Group Rekey Interval:	3600	
WPA/WAPI Encryption:	TKIP+AES	<input type="button" value="v"/>
WEP Encryption:	Disabled	<input type="button" value="v"/>
<input type="button" value="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.

### 6.13.3 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 NexusLink 3112u 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.

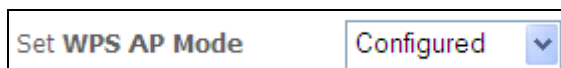
To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

#### I. Setup

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



**Step 2:** Set the WPS AP Mode. **Configured** is used when the NexusLink 3112u will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the NexusLink 3112u.

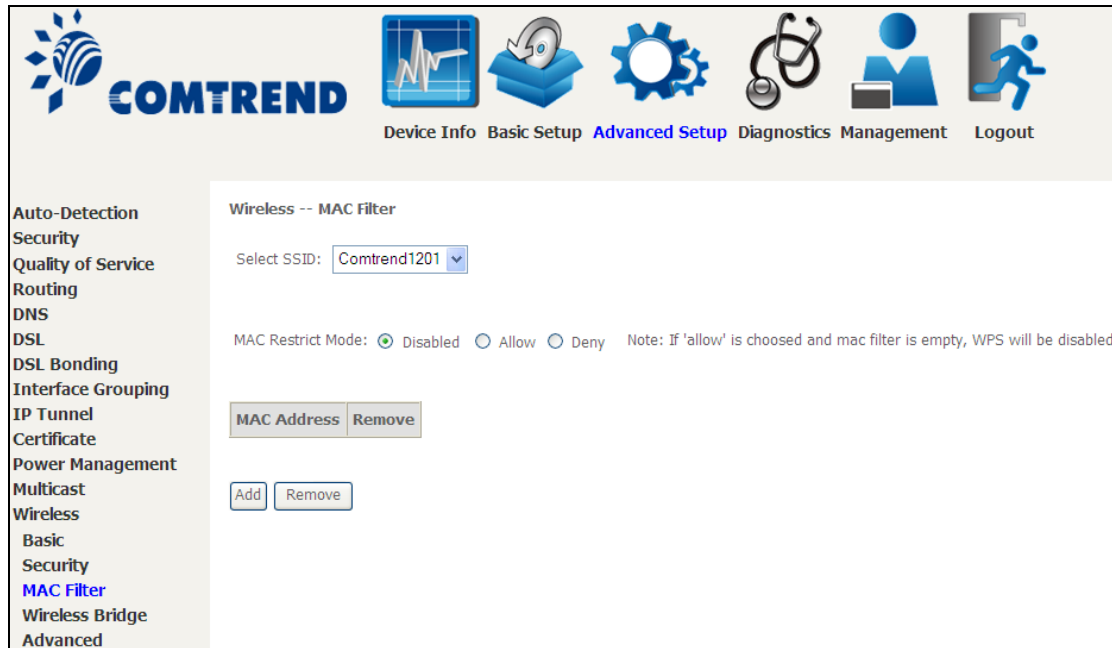


**NOTES:** Your client may or may not have the ability to provide security settings to the NexusLink 3112u. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

In addition, using Windows 7, you can add an external registrar using the **Config AP** button ([Appendix F - WPS OPERATION](#) has detailed instructions).


### 6.13.4 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.



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

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

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

Apply/Save

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

## 6.13.5 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

**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:

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

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

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

## 6.13.6 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 Advanced Setup interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left, a sidebar lists various configuration categories, with **Advanced** selected under the Wireless section. The main content area is titled "Wireless -- Advanced" and contains a descriptive paragraph and a list of configuration parameters.

**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](#)

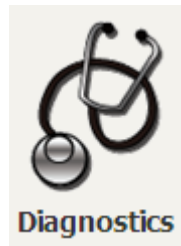
<b>Field</b>	<b>Description</b>
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 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.

<b>Field</b>	<b>Description</b>
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.

The screenshot shows the COMTREND Diagnostics dashboard. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics (highlighted), Management, and Logout. On the left side, there is a menu with options: Diagnostics, Fault Management, Uptime Status, Ping, TraceRoute, and System Utilization. The main content area is divided into two sections: LAN and Device.

**LAN**

GBETH ETH1 ETH2 ETH3

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:b3:3d:8d
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254

**Device**

Model	NexusLink 3112u
Serial Number	13B3112UXXF-AA000095
Firmware Version	WA31-412CTU-C03_R01.A2pvbF039j.d25c
Bootloader (CFE) Version	1.0.38-112.118-19
Up Time	46 mins:40 secs
System Log	<input type="button" value="Show"/>

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

The screenshot shows the COMTREND Diagnostics screen with the Diagnostics menu item highlighted in the left sidebar. The main content area displays the following information:

**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 GBETH Connection:	FAIL	<a href="#">Help</a>
Test your ETH1 Connection:	FAIL	<a href="#">Help</a>
Test your ETH2 Connection:	FAIL	<a href="#">Help</a>
Test your ETH3 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

## 7.2 Fault Management

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.

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

**Diagnostics**  
Fault Management  
**Uptime Status**  
Ping  
TraceRoute  
System Utilization

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

**System Up Time** 25 mins:20 secs

DSL Group:

**DSL Up Time** Not Connected

ClearAll

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.

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

**Diagnostics**  
Fault Management  
Uptime Status  
**Ping**  
TraceRoute  
System Utilization

### Ping

Send ICMP ECHO\_REQUEST packets to network hosts.

Ping IP Address / Hostname:  Ping

PING 192.168.1.1 (192.168.1.1): 56 data bytes  
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.471 ms  
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.349 ms  
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.347 ms  
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.347 ms

--- 192.168.1.1 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max = 0.347/0.378/0.471 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.



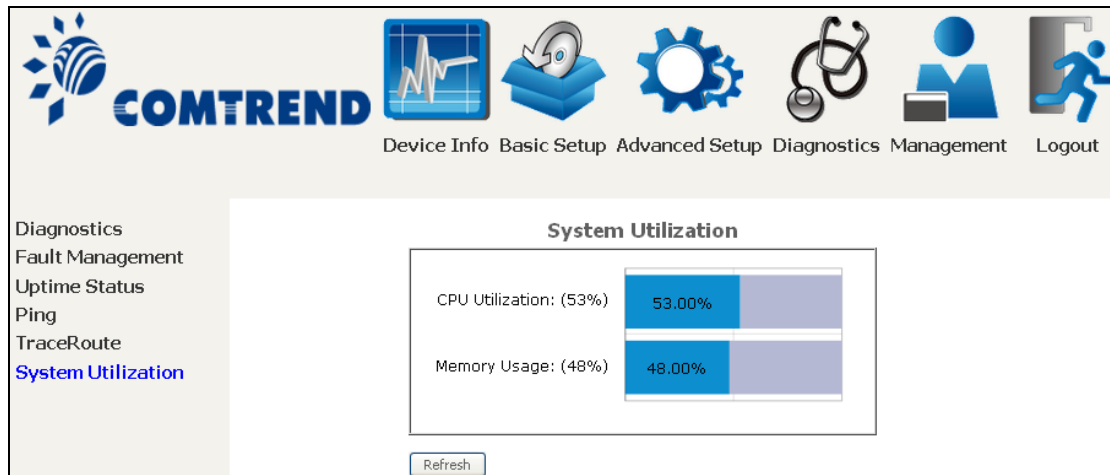
The screenshot displays the Comtrend web interface. At the top, the Comtrend logo is on the left, and a navigation menu is on the right with icons and labels: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side of the main content area, there is a vertical 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 is a form with the label "TraceRoute IP Address / Hostname:" followed by an empty text input field and a "TraceRoute" button. At the bottom of the main content area, there is a sample output: "tracert to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets" followed by "1 192.168.1.1 (192.168.1.1) 0.416 ms".

## 7.6 System Utilization



The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, and Management. The Diagnostics menu is expanded, showing options like Fault Management, Uptime Status, Ping, TraceRoute, and System Utilization (which is highlighted). The main content area is titled "System Utilization" and contains the following text: "Click 'Start' button to initialize CPU and Memory utilization calculation. Please wait 10 seconds for the test to run." Below this text is a "Start" button.

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



The screenshot shows the Comtrend web interface after the test has completed. The navigation bar is the same, but now includes a "Logout" icon. The Diagnostics menu is still expanded. The main content area is titled "System Utilization" and displays two horizontal bar charts. The first chart shows "CPU Utilization: (53%)" with a blue bar representing 53.00%. The second chart shows "Memory Usage: (48%)" with a blue bar representing 48.00%. Below the charts is a "Refresh" button.

Metric	Value
CPU Utilization: (53%)	53.00%
Memory Usage: (48%)	48.00%

# Chapter 8 Management

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



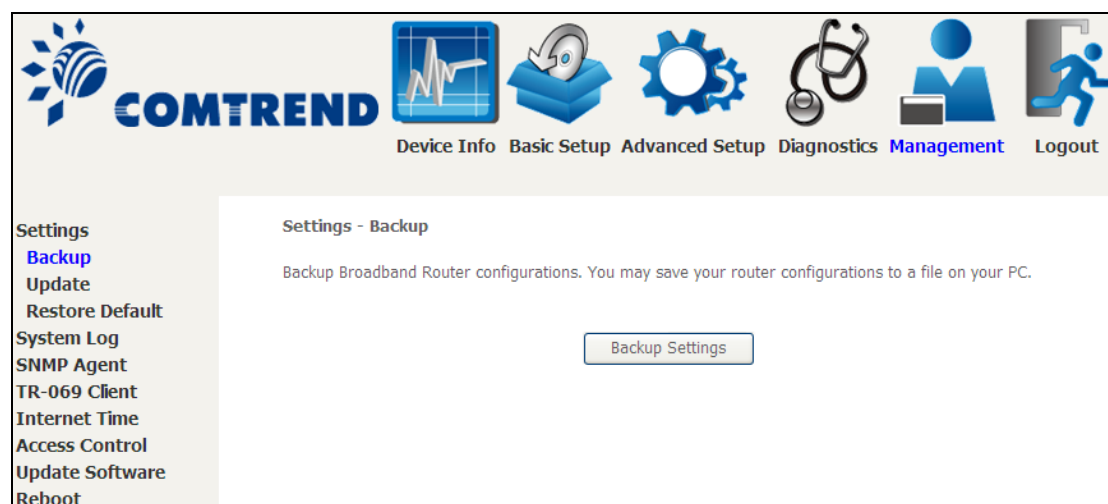
The Management menu has the following maintenance functions and processes:

## 8.1 Settings

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

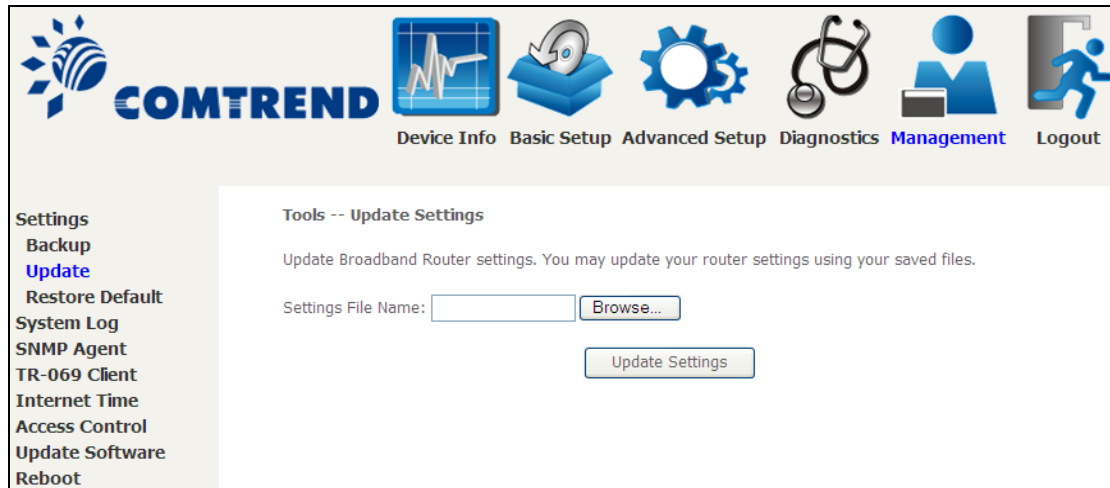
### 8.1.1 Backup Settings

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.



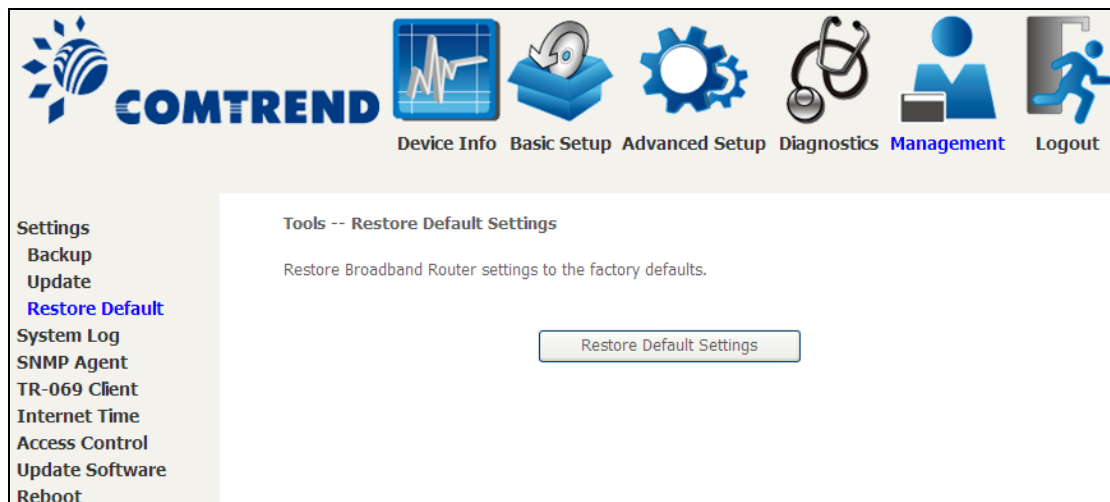
### 8.1.2 Update Settings

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

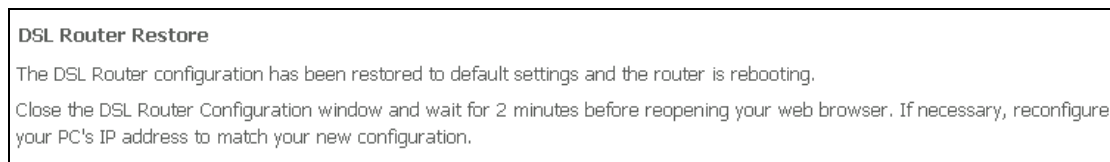


### 8.1.3 Restore Default

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



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



Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

**NOTE:** This entry has the same effect as the **Reset** button. The NexusLink 3112u board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the boot loader will erase the configuration data saved in flash memory.

## 8.2 System Log

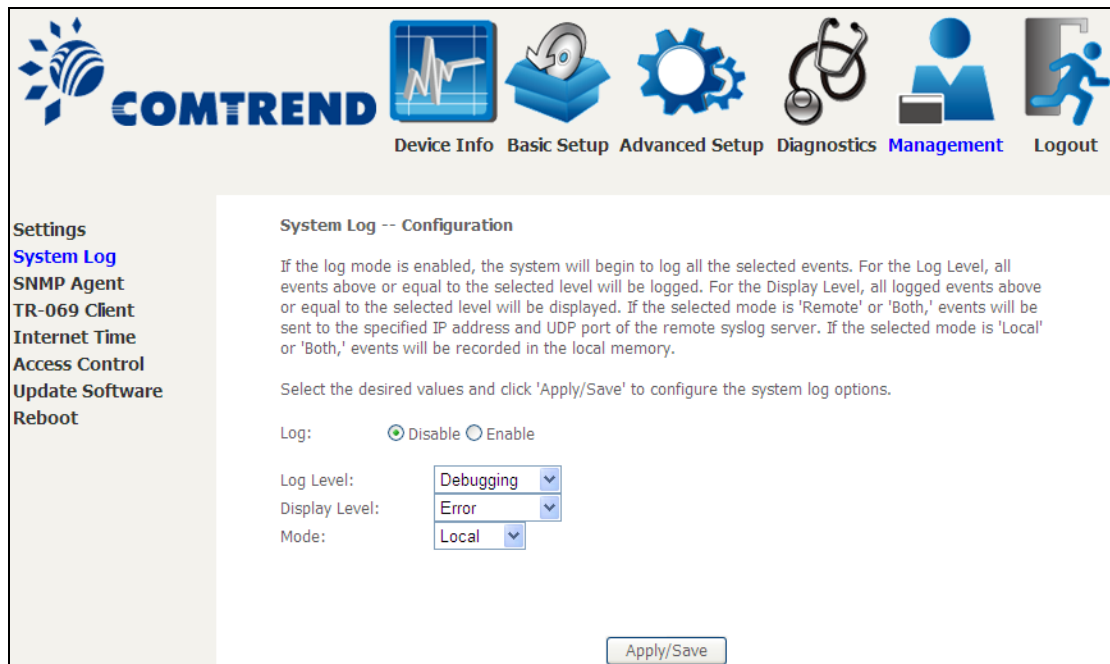
This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

**STEP 1:** Click **Configure System Log**, as shown below (circled in **Red**).



**STEP 2:** Select desired options and click **Apply/Save**.



Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the <b>Enable</b> radio button and then click <b>Apply/Save</b> .



Option	Description
Log Level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the NexusLink 3112u SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> <li>• Emergency = system is unusable</li> <li>• Alert = action must be taken immediately</li> <li>• Critical = critical conditions</li> <li>• Error = Error conditions</li> <li>• Warning = normal but significant condition</li> <li>• Notice= normal but insignificant condition</li> <li>• Informational= provides information for reference</li> <li>• Debugging = debug-level messages</li> </ul> <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	<p>Allows the user to select the logged events and displays on the <b>View System Log</b> window for events of this level and above to the highest Emergency level.</p>
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

**STEP 3:** Click **View System Log**. The results are displayed as follows.

System Log			
Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.