

6.4.3 Policy Routing

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



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



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

6.4.4 RIP

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



COMTREND

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

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

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

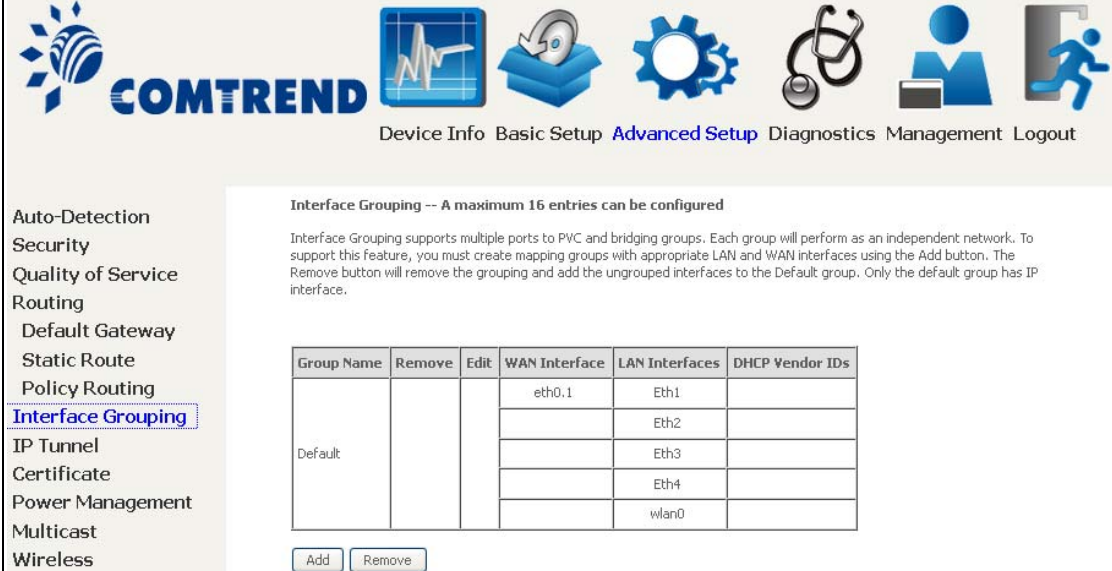
Send default route

Interface	Version	Operation	Enabled

WAN Interface not exist for RIP.

6.5 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

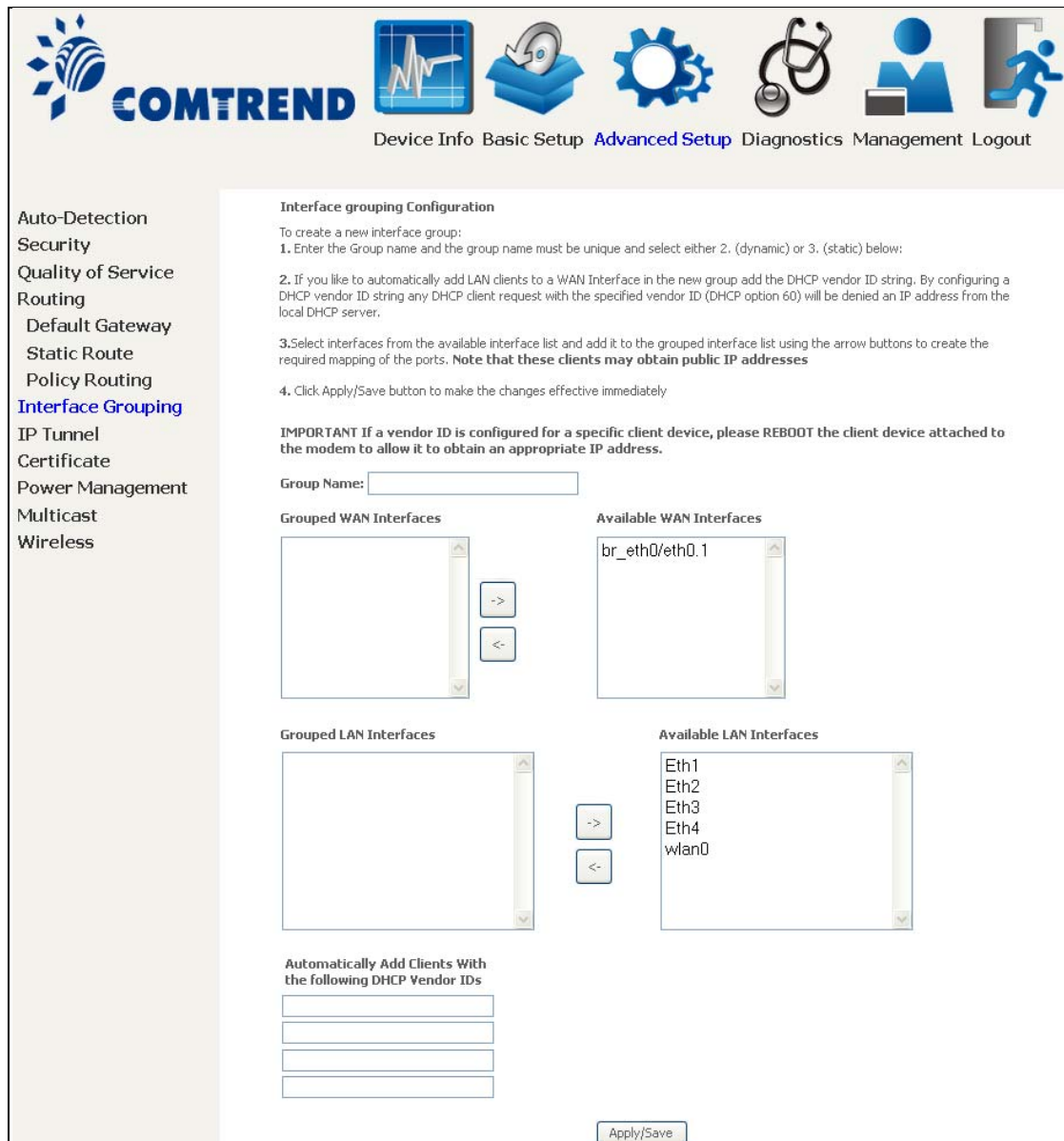
Auto-Detection
Security
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

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			eth0.1	Eth1	
				Eth2	
				Eth3	
				Eth4	
				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.



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

br_eth0/eth0.1

Grouped LAN Interfaces

Available LAN Interfaces

Eth1
Eth2
Eth3
Eth4
wlan0

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

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 2 WAN services, an IPoE and a PPPoE. IPoE is for IP set-top box (video). The LAN interfaces are ETH1, ETH2, ETH3, and ETH4.

The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and ETH4.
2. Video: ipoe_eth0. The DHCP vendor ID is "Video".



If the onboard DHCP server is running on "Default" and the remote DHCP server is running on IPoE (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 .

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

1. Default: ETH2, ETH3, and ETH4
2. Video: ipoe_eth0, and ETH1.

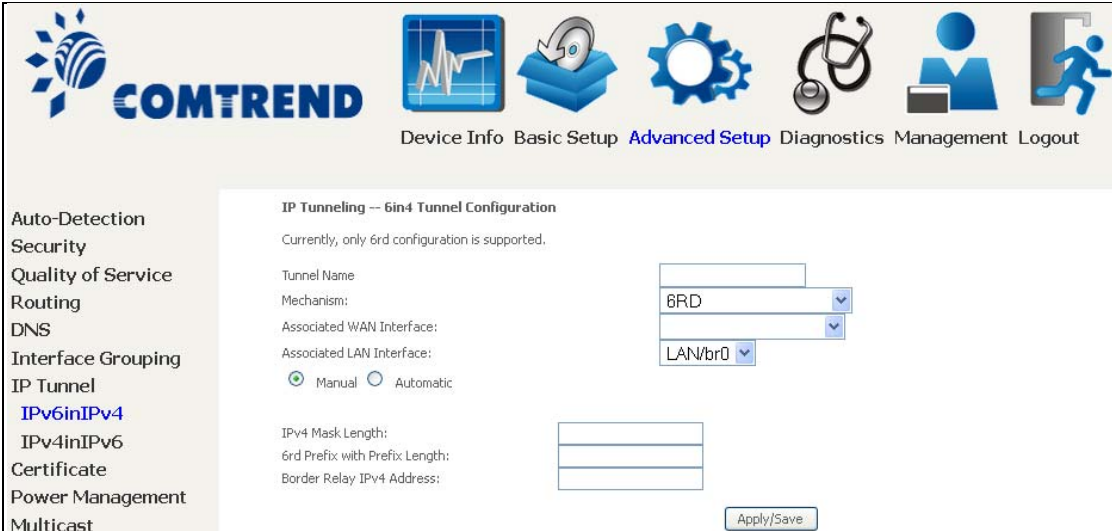
6.6 IP Tunnel

6.6.1 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

6.6.2 IPv4inIPv6

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



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

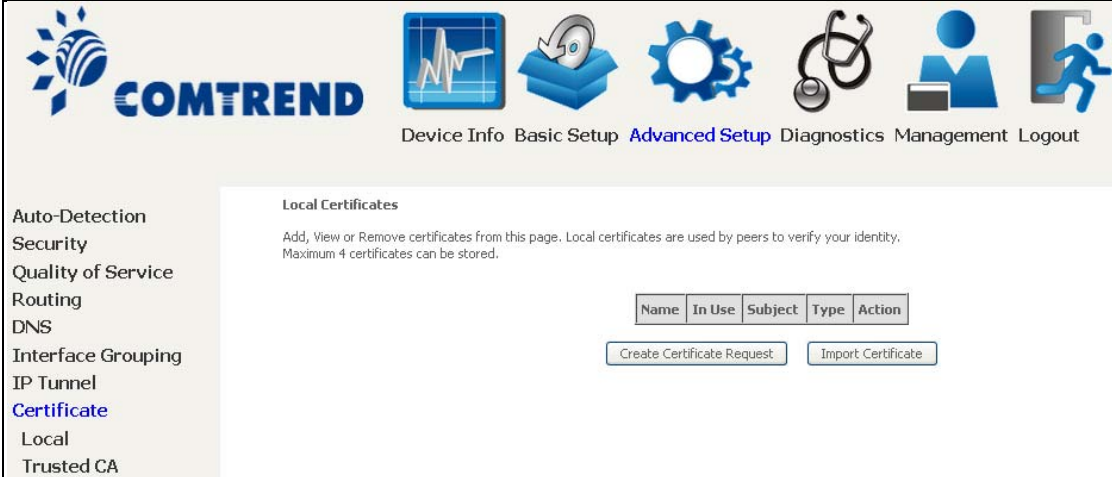


Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for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

6.7 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.

6.7.1 Local



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.

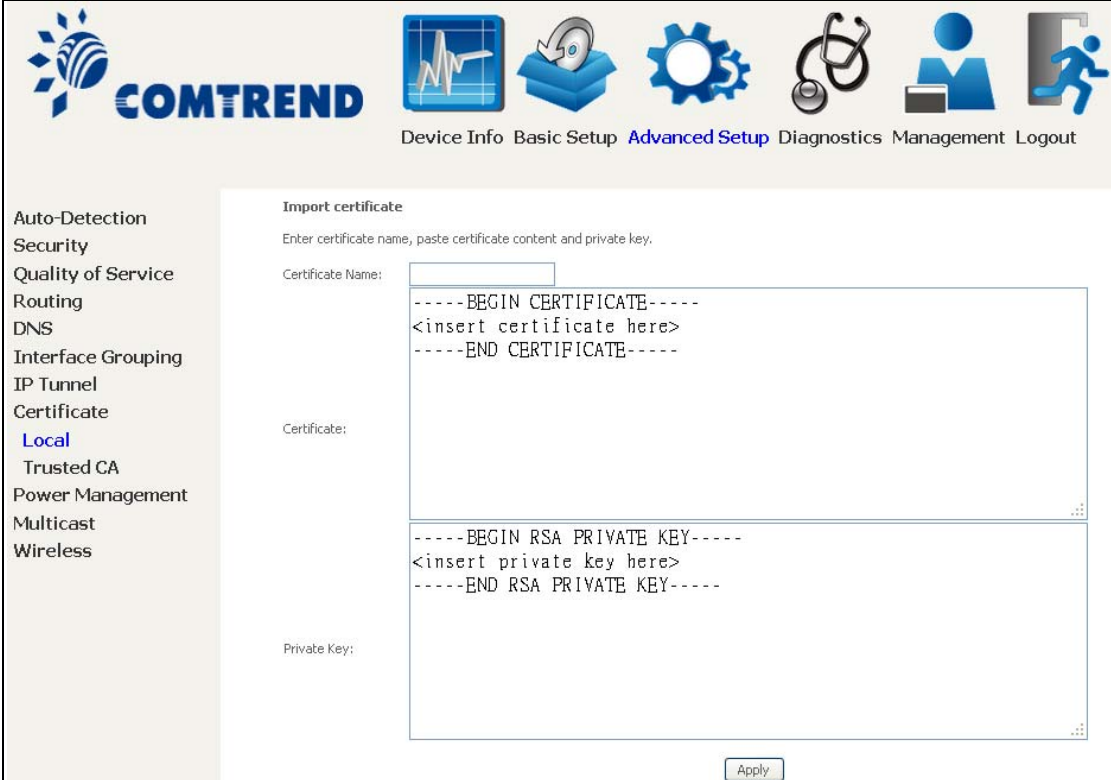


The following table is provided for your reference.

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.



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

Auto-Detection
Security
Quality of Service
Routing
DNS
Interface Grouping
IP Tunnel
Certificate
Local
Trusted CA
Power Management
Multicast
Wireless

Import certificate
Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

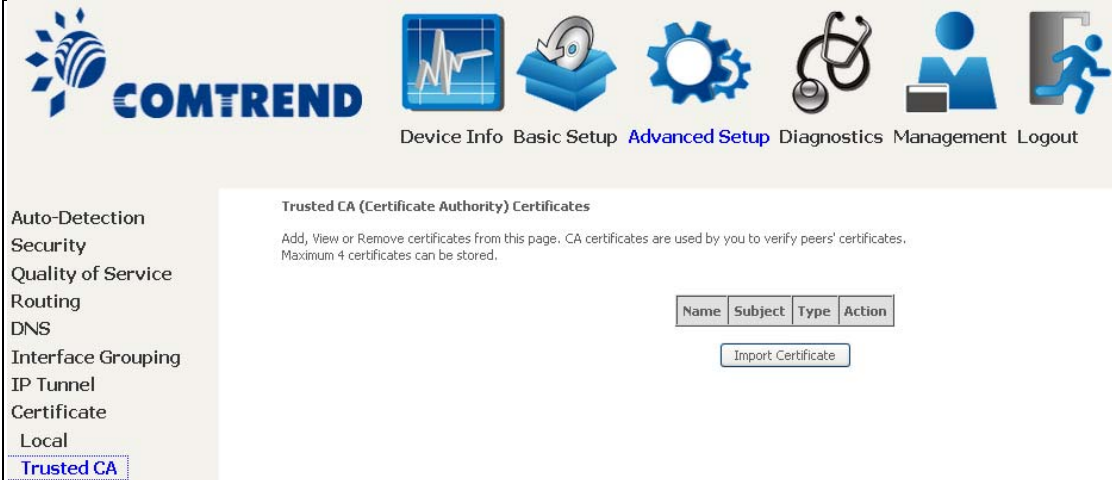
```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Apply

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

6.7.2 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.



COMTREND

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

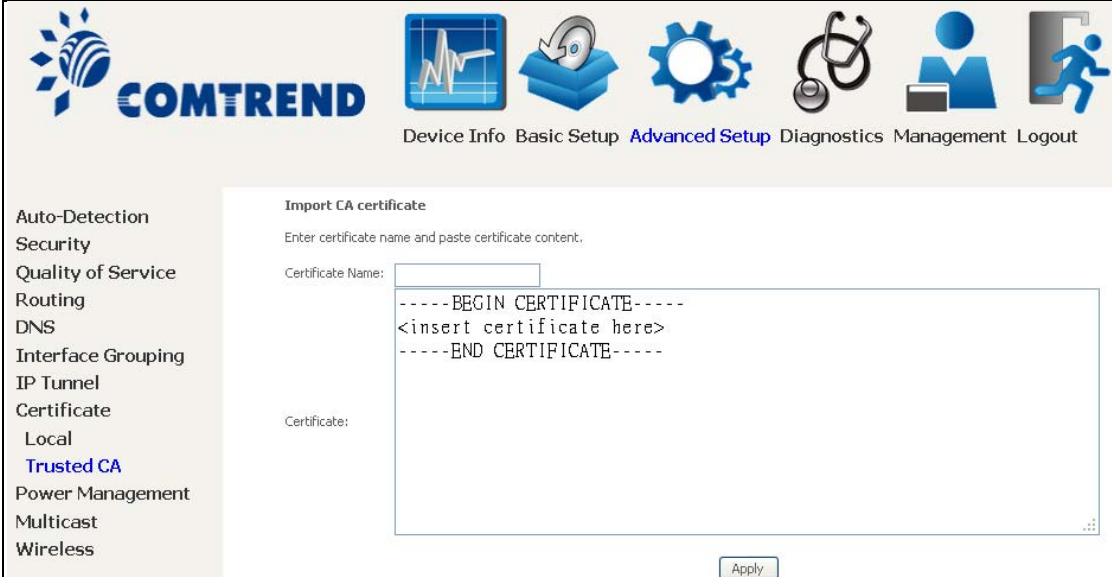
Auto-Detection
Security
Quality of Service
Routing
DNS
Interface Grouping
IP Tunnel
Certificate
Local
Trusted CA

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action
<input type="button" value="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.



COMTREND

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

Auto-Detection
Security
Quality of Service
Routing
DNS
Interface Grouping
IP Tunnel
Certificate
Local
Trusted CA
Power Management
Multicast
Wireless

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

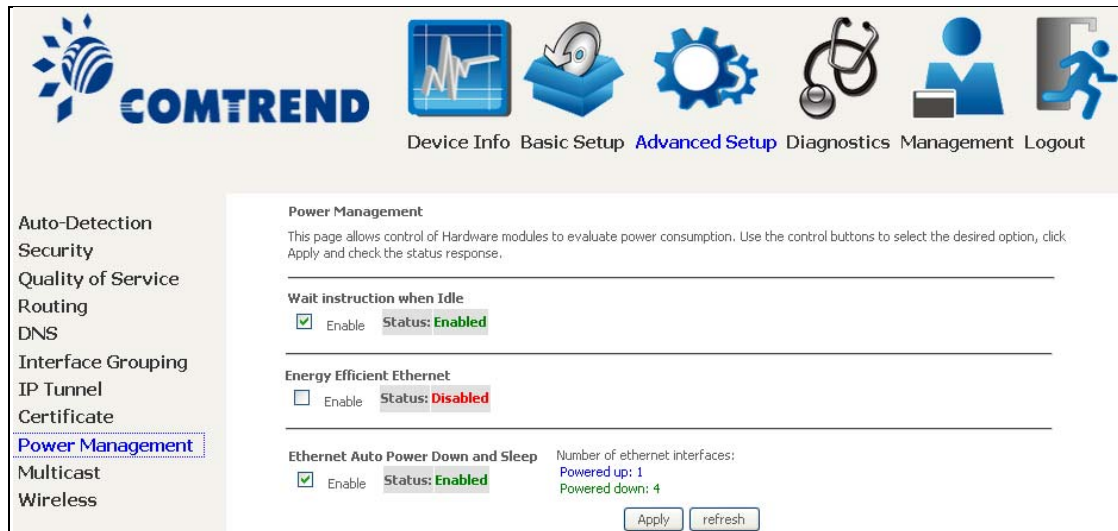
Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

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

6.8 Power Management

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



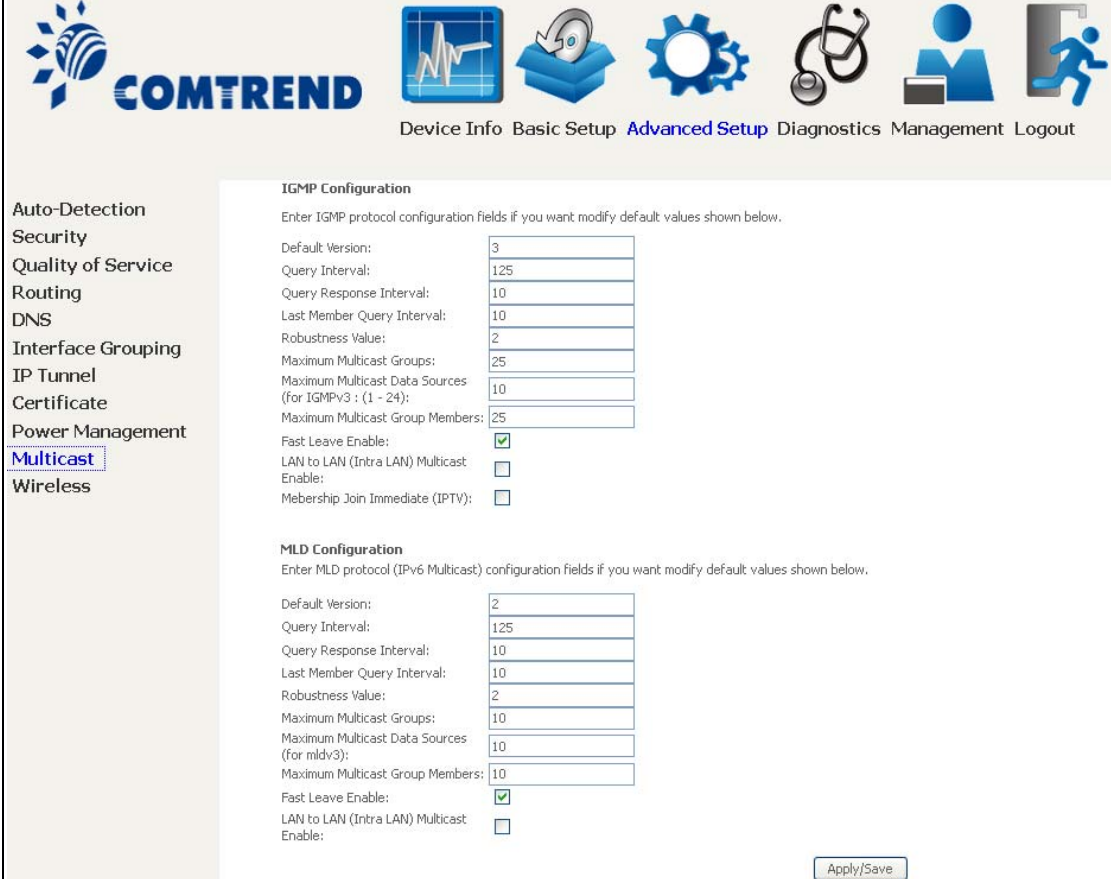
The screenshot shows the COMTREND web interface for Power Management. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The left sidebar contains a menu with items like Auto-Detection, Security, Quality of Service, Routing, DNS, Interface Grouping, IP Tunnel, Certificate, **Power Management**, Multicast, and Wireless. The main content area is titled "Power Management" and includes the following sections:

- Power Management**: A descriptive paragraph stating that the page allows control of hardware modules to evaluate power consumption and that users should use control buttons to select options, click Apply, and check the status response.
- Wait instruction when Idle**: A checkbox labeled "Enable" is checked, and the status is "Enabled".
- Energy Efficient Ethernet**: A checkbox labeled "Enable" is unchecked, and the status is "Disabled".
- Ethernet Auto Power Down and Sleep**: A checkbox labeled "Enable" is checked, and the status is "Enabled".
- Number of ethernet interfaces**: A summary showing "Powered up: 1" and "Powered down: 4".

At the bottom right of the configuration area, there are "Apply" and "refresh" buttons.

6.9 Multicast

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



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

Multicast

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

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

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

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

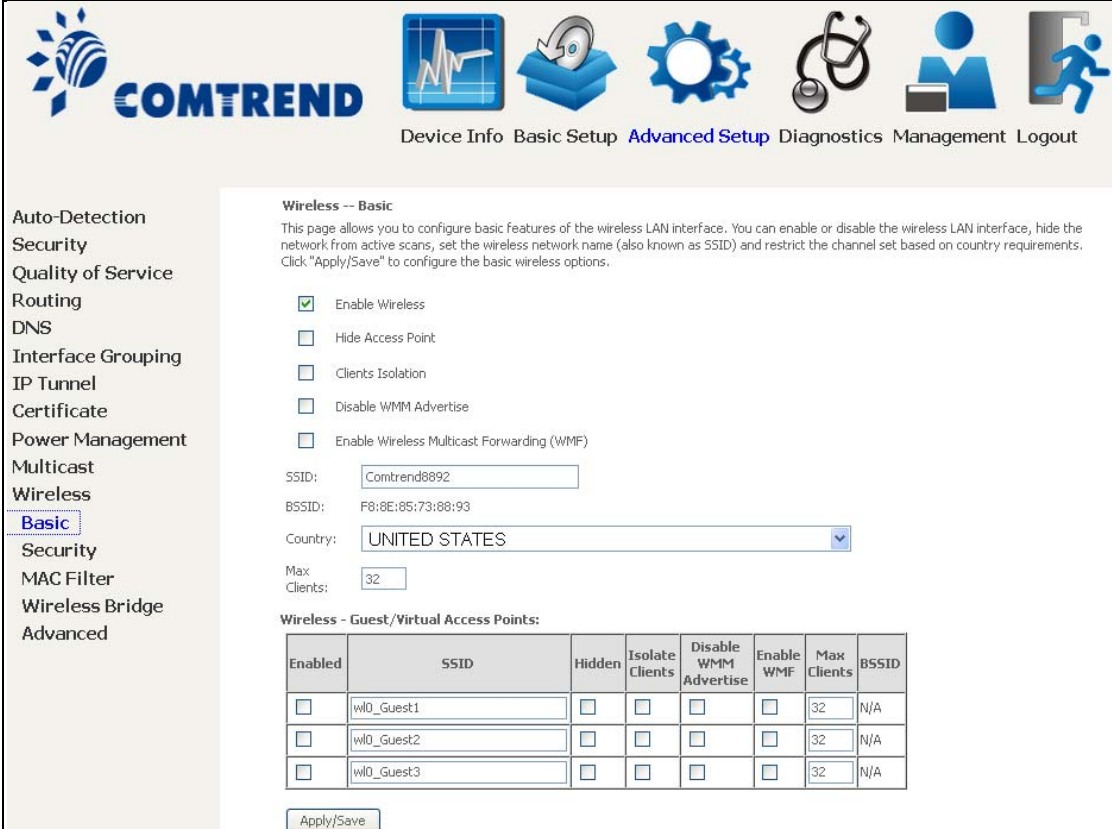
Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response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

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

6.10 Wireless

6.10.1 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) .



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

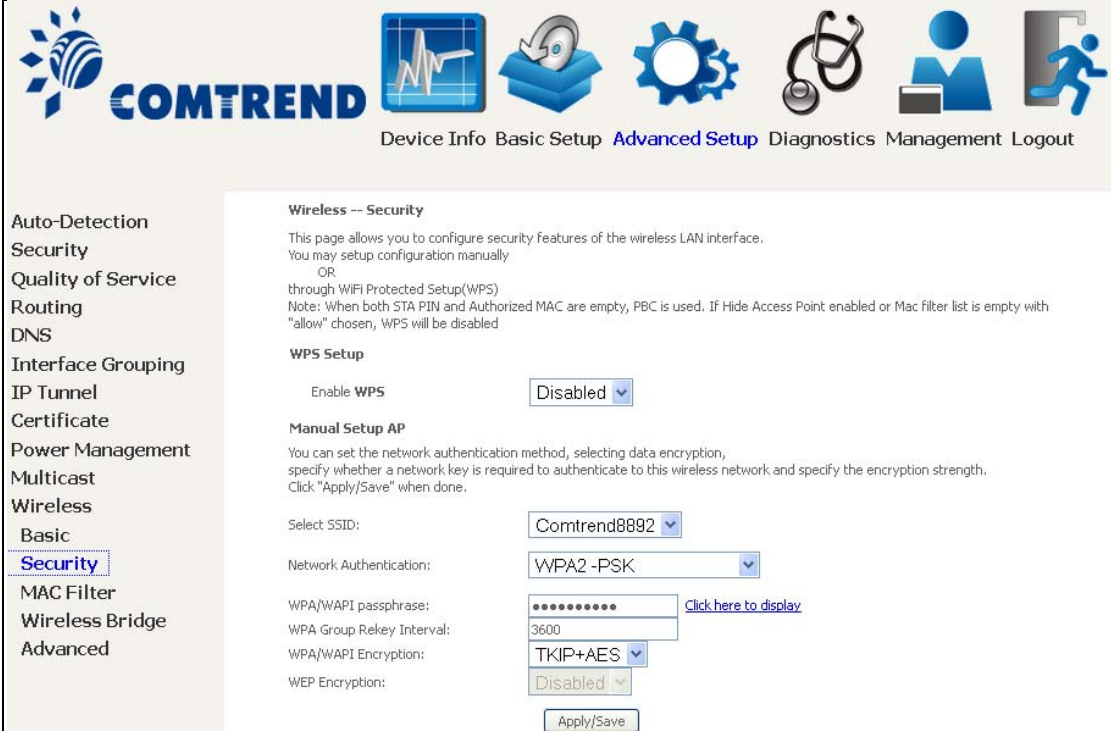
Consult the table below for descriptions of these options.

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.
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 Network Connections from the start Menu and select View Available Network Connections . 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.

Option	Description
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox <input checked="" type="checkbox"/> to enable this function.
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	US= worldwide
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 Enabled column. To hide a Guest SSID select its checkbox <input checked="" type="checkbox"/> in the Hidden column.</p> <p>Do the same for Isolate Clients and Disable WMM Advertise. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF, Max Clients and BSSID, consult the matching entries in this table.</p> <p>NOTE: Remote wireless hosts cannot scan Guest SSIDs.</p>

6.10.2 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.



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

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS)
 Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable WPS

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

Please see [6.10.3 WPS](#) for WPS setup instructions.

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 menu. 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.
Different authentication type pops up different settings requests.
Choosing 802.1X , enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key.

Also, enable WEP Encryption and select Encryption Strength.

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

Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Choosing **WPA**, you must enter WPA Group Rekey Interval.

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

Choosing **WPA-PSK**, you must enter WPA Pre-Shared Key and Group Rekey Interval.

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

6.10.3 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 WR-6891u 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 WR-6891u will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the WR-6891u.

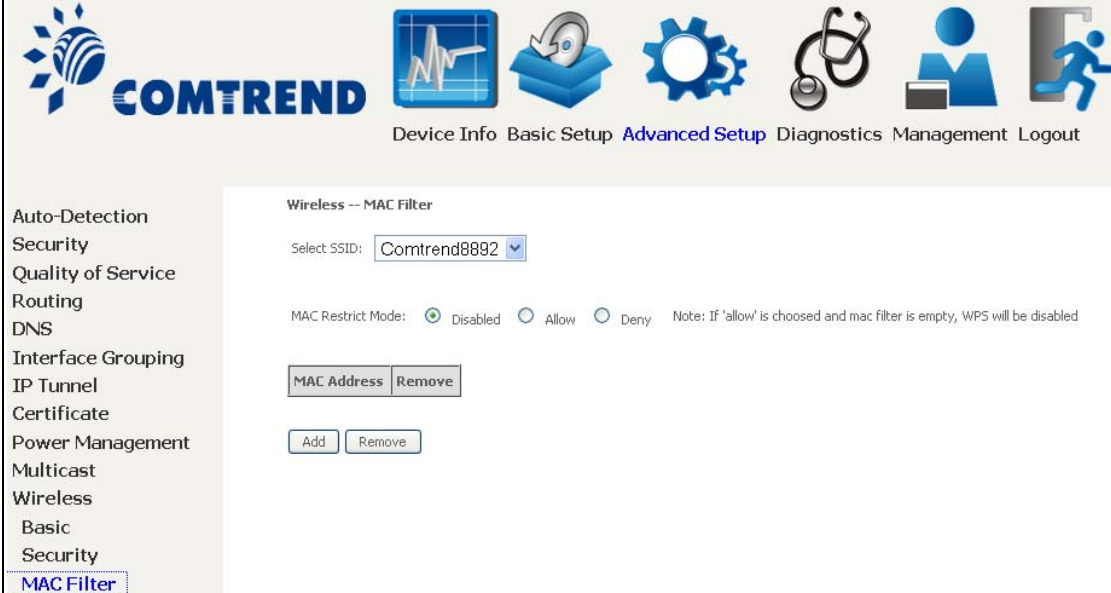


NOTES: Your client may or may not have the ability to provide security settings to the WR-6891u. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

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

6.10.4 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.

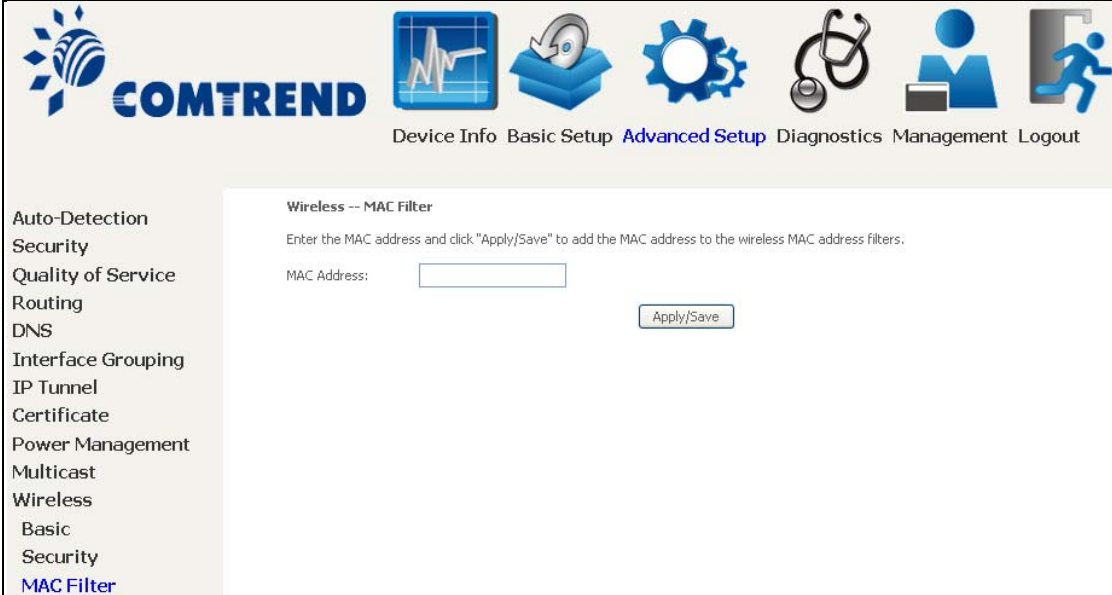


The screenshot shows the COMTREND router's web interface. The top navigation bar includes: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The left sidebar lists various settings categories, with **MAC Filter** selected under the Security section. The main content area is titled "Wireless -- MAC Filter" and contains the following configuration options:

- Select SSID:** A drop-down menu currently showing "Comtrend8892".
- MAC Restrict Mode:** Three radio buttons: Disabled, Allow, and Deny. A note states: "Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled".
- MAC Address Table:** A table with two columns: "MAC Address" and "Remove".
- Buttons:** "Add" and "Remove" buttons are located below the table.

Option	Description
Select SSID	Select the wireless network name from the drop-down menu. 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.

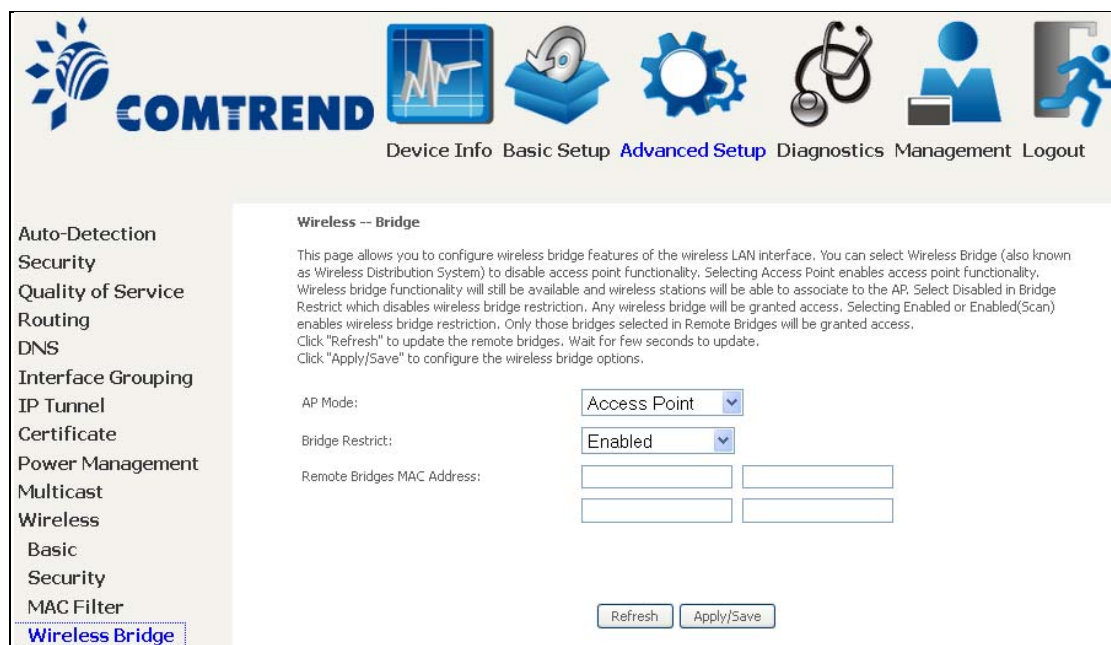


The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, Basic, Security, and **MAC Filter** (highlighted). The main content area is titled "Wireless -- MAC Filter" and contains the following text: "Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters." Below this text, there is a label "MAC Address:" followed by an empty text input box. To the right of the input box is a button labeled "Apply/Save".

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

6.10.5 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:

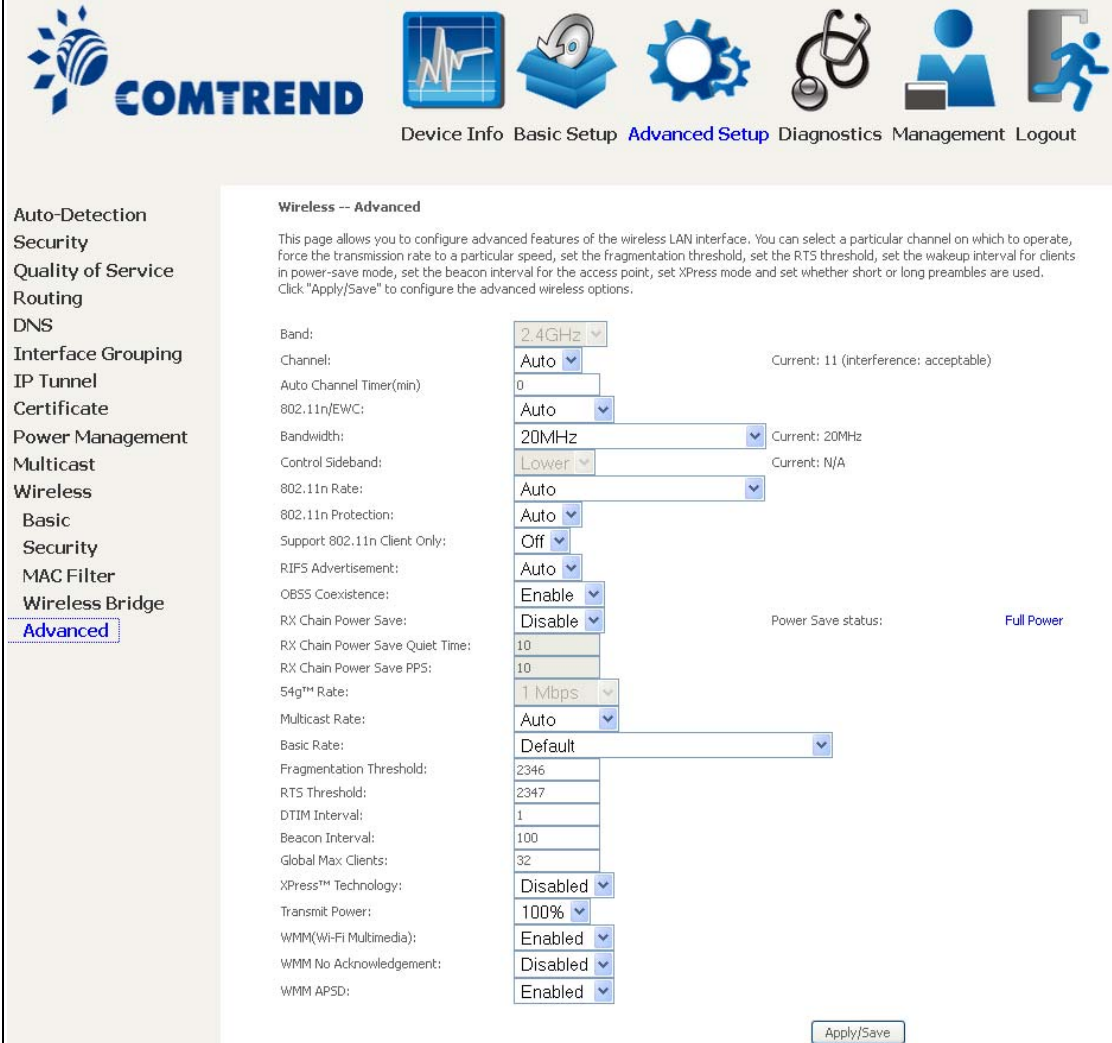
Remote Bridges MAC Address:

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

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

6.10.6 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.



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

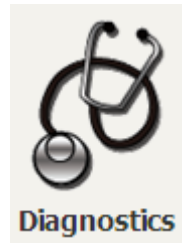
Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.

Field	Description
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.
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.

Field	Description
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.

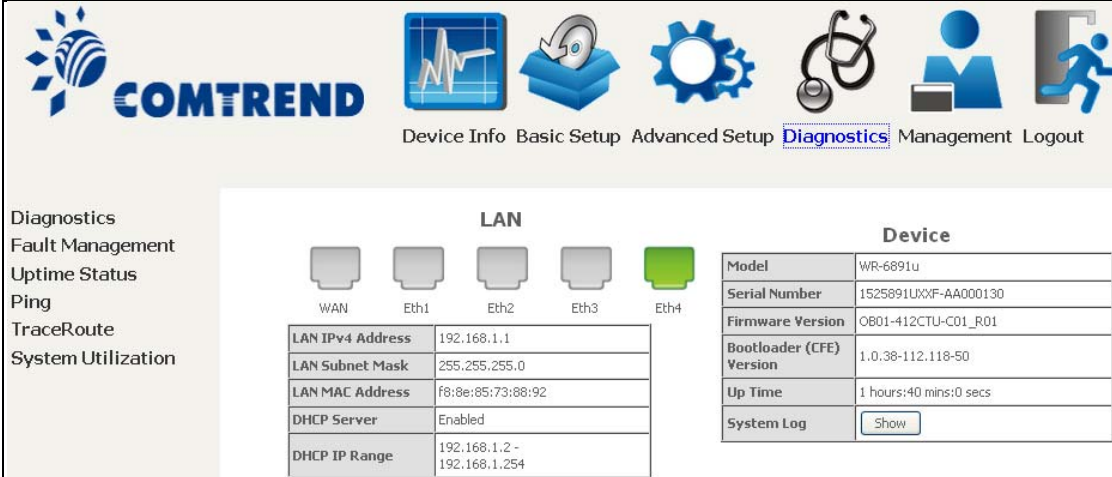
Chapter 7 Diagnostics

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



7.1 Diagnostics – Individual Tests

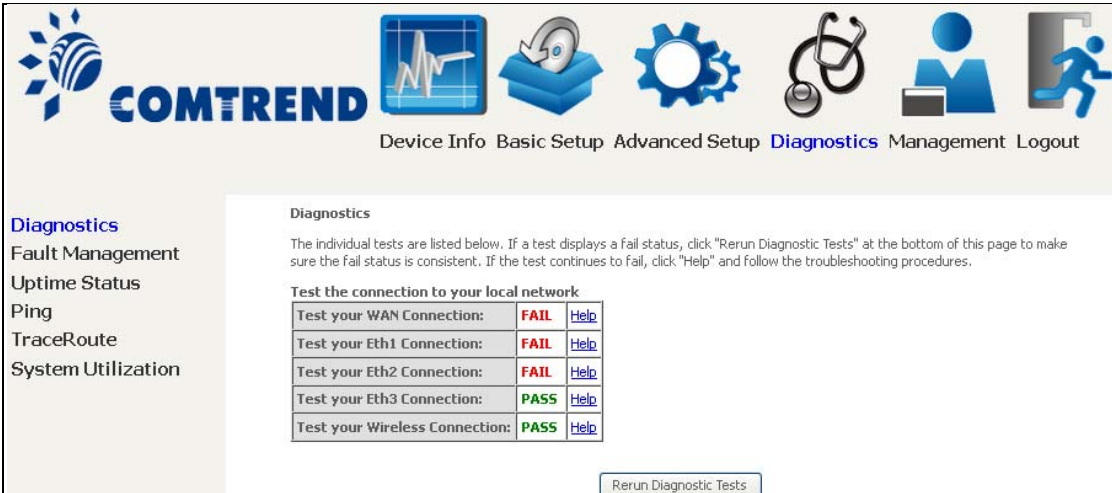
The first Diagnostics screen is a dashboard that shows overall connection status.



LAN	
WAN	
Eth1	
Eth2	
Eth3	
Eth4	
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:9e:85:73:88:92
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254

Device	
Model	WR-6891u
Serial Number	1525891UXXF-AA000130
Firmware Version	0801-412CTU-C01_R01
Bootloader (CFE) Version	1.0.38-112.118-50
Up Time	1 hours:40 mins:0 secs
System Log	Show

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




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 WAN Connection:	FAIL	Help
Test your Eth1 Connection:	FAIL	Help
Test your Eth2 Connection:	FAIL	Help
Test your Eth3 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

[Rerun Diagnostic Tests](#)

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 Logout

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 1 hours:45 mins:2 secs

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=0.459 ms
 64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.331 ms
 64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.325 ms
 64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.508 ms

--- 192.168.1.1 ping statistics ---
 4 packets transmitted, 4 packets received, 0% packet loss
 round-trip min/avg/max = 0.325/0.405/0.508 ms

7.5 Trace Route

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



The screenshot displays the COMTREND web interface. At the top, there is a navigation menu with icons and labels for: Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted), Management, and Logout. On the left side, a sidebar menu lists: Diagnostics, Fault Management, Uptime Status, Ping, and **TraceRoute** (highlighted). 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 field labeled "TraceRoute IP Address / Hostname:" with an empty input box and a "TraceRoute" button. At the bottom of the main area, there is a sample command and its output: "traceroute 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) 0.723 ms".

7.6 System Utilization



COMTREND

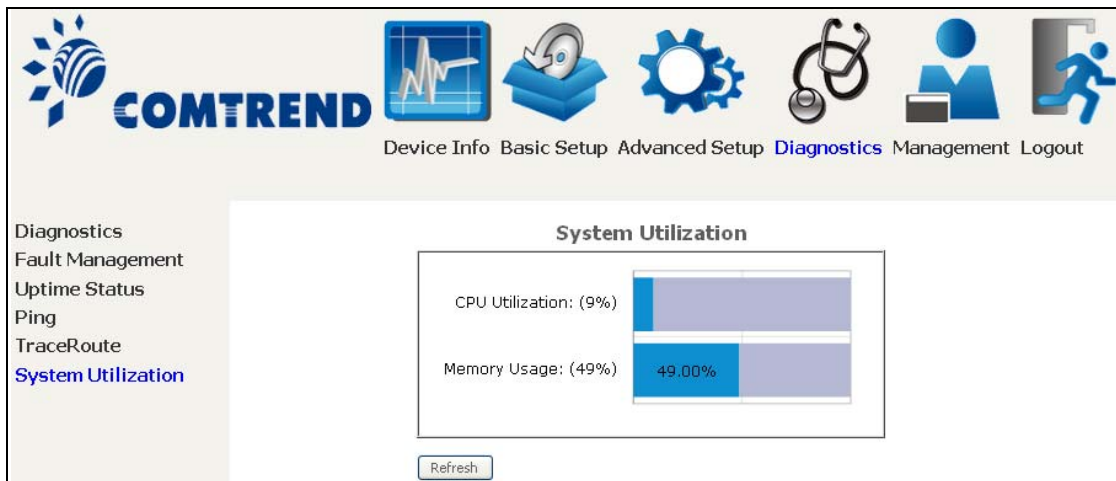
Device Info Basic Setup Advanced Setup **Diagnostics** Management Logout

Diagnostics
Fault Management
Uptime Status
Ping
TraceRoute
System Utilization

System Utilization

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

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


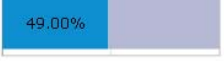


COMTREND

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

Diagnostics
Fault Management
Uptime Status
Ping
TraceRoute
System Utilization

System Utilization

CPU Utilization: (9%)	
Memory Usage: (49%)	

Chapter 8 Management

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



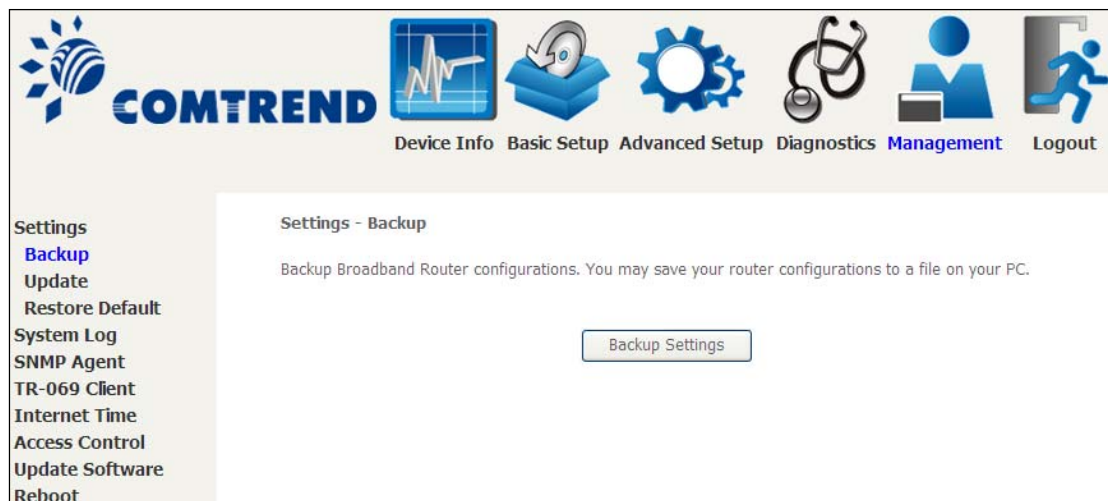
The Management menu has the following maintenance functions and processes:

8.1 Settings

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

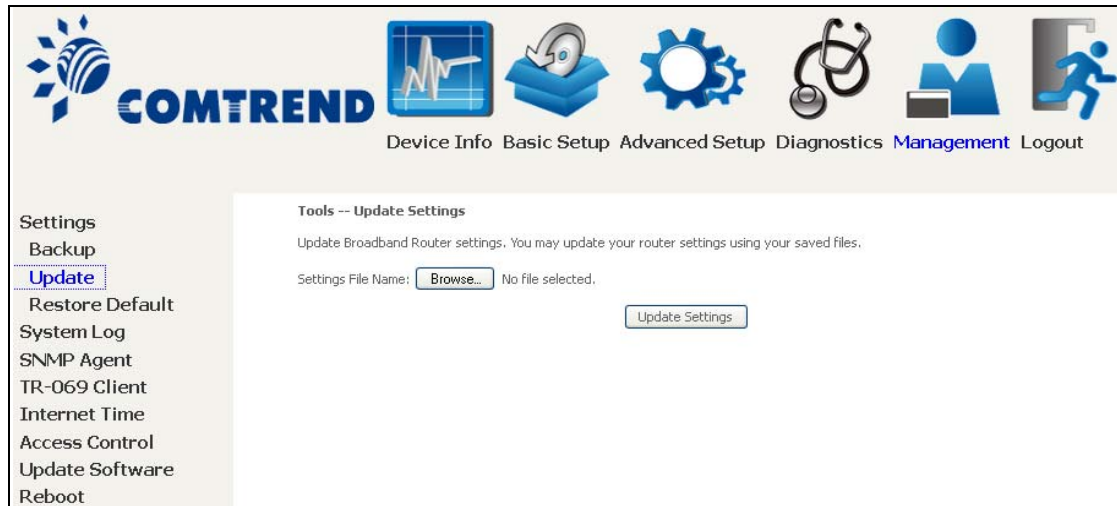
8.1.1 Backup Settings

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.



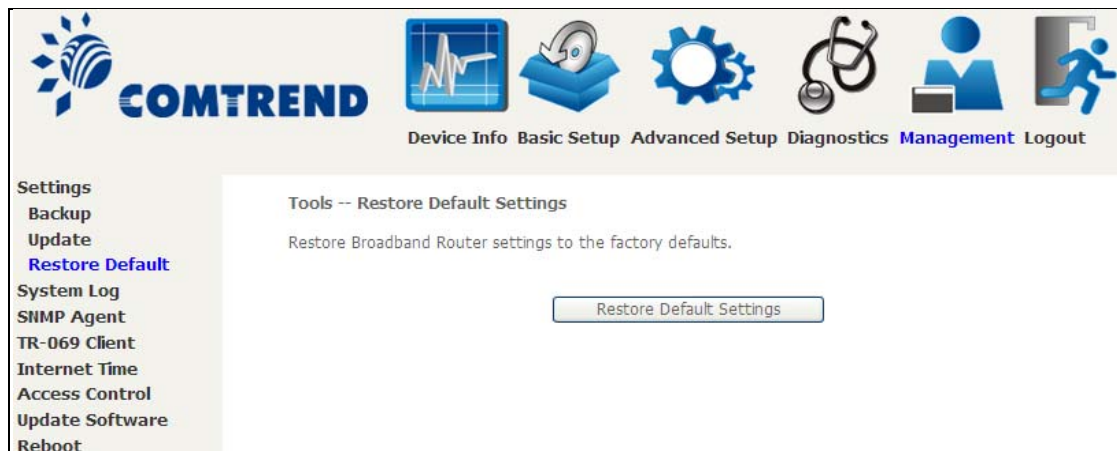
8.1.2 Update Settings

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.

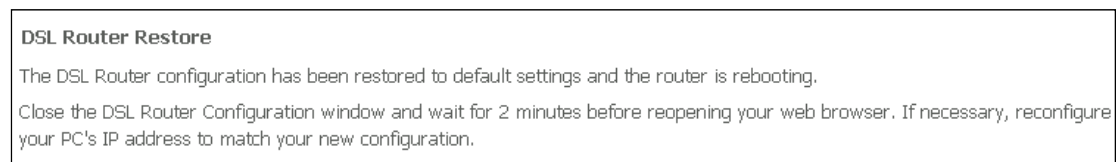


8.1.3 Restore Default

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 WR-6891u 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

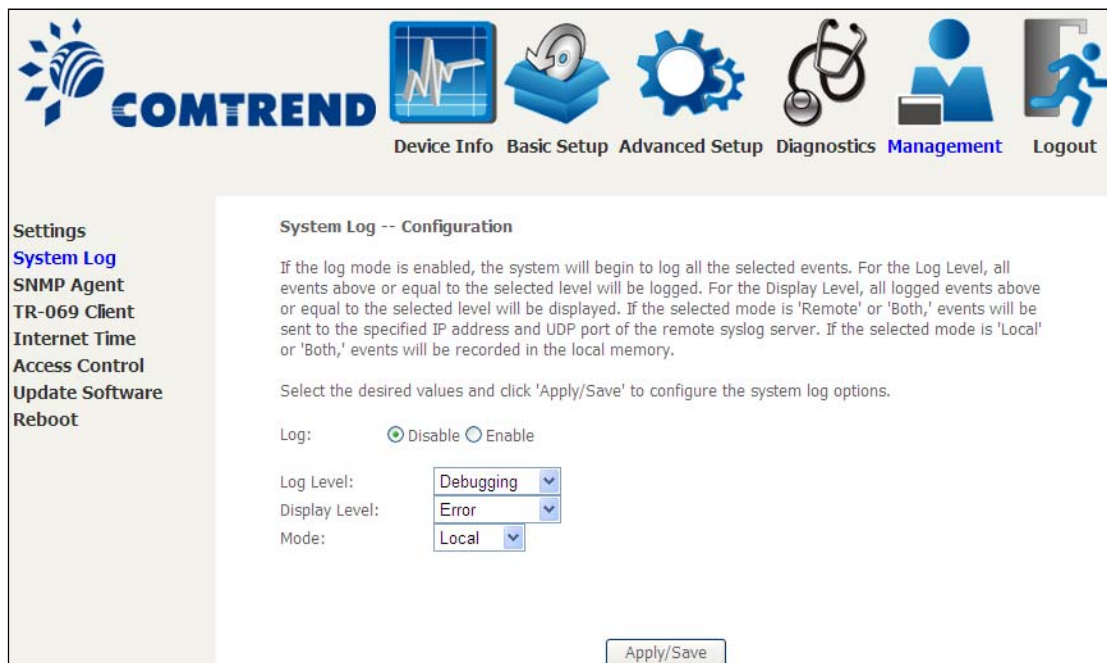
This function allows a system log to be kept and viewed upon request.

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 Enable radio button and then click Apply/Save .

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 WR-6891u 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"> • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages <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 View System Log 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.

8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.



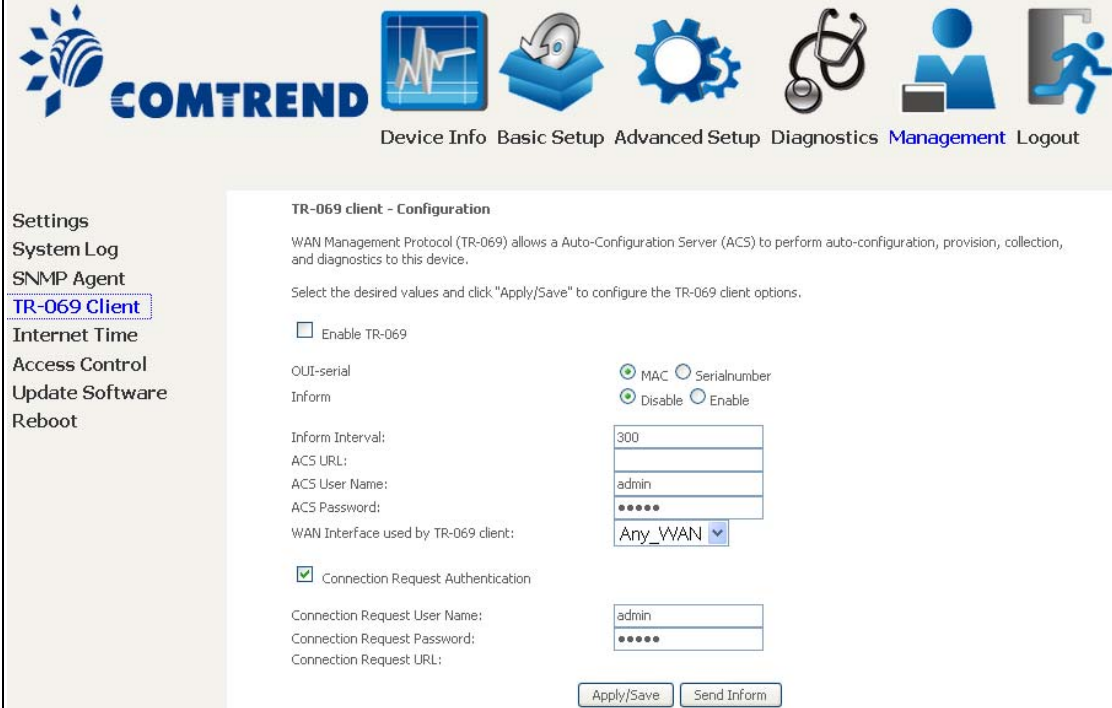
The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (highlighted), and Logout. Below the navigation bar, the main content area is titled "SNMP - Configuration". It contains a brief description of SNMP and instructions to select values and click "Apply". The configuration options include:

- SNMP Agent: Disable Enable
- Read Community: public
- Set Community: private
- System Name: Comtrend
- System Location: unknown
- System Contact: unknown
- Trap Manager IP: 0.0.0.0

A "Save/Apply" button is located at the bottom right of the configuration area. On the left side of the interface, there is a sidebar menu with the following items: Settings, System Log, **SNMP Agent** (highlighted), TR-069 Client, Internet Time, Access Control, Update Software, and Reboot.

8.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.



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

Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Reboot

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Enable TR-069

OUI-serial MAC Serialnumber
Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

The table below is provided for ease of reference.

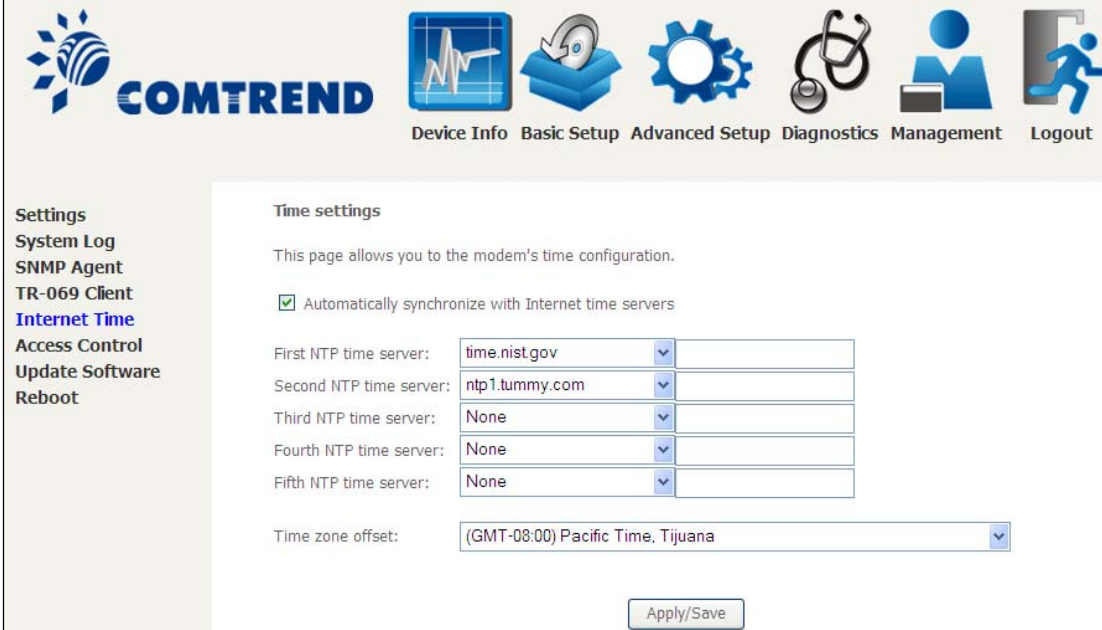
Option	Description
Enable TR-069	Tick the checkbox <input checked="" type="checkbox"/> to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with ACS or select serial number to use router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.

Option	Description
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Connection Request	
Authentication	Tick the checkbox <input checked="" type="checkbox"/> to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to router.

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.

8.5 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox , choose your preferred time server(s), select the correct time zone offset, and click **Save/Apply**.



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 items: Settings, System Log, SNMP Agent, TR-069 Client, **Internet Time**, Access Control, Update Software, and Reboot. The main content area is titled "Time settings" and contains the following configuration options:

- Automatically synchronize with Internet time servers
- First NTP time server:
- Second NTP time server:
- Third NTP time server:
- Fourth NTP time server:
- Fifth NTP time server:
- Time zone offset:

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

NOTE: Internet Time must be activated to use [5.5 Parental Control](#). In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.


8.6 Access Control







8.6.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the WR-6891u is controlled through the following user accounts:

- The root account has unrestricted access to view and change the configuration of your Broadband router.
- The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.
- The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.
- The apuser account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure wireless settings.

Use the fields to update passwords for the accounts, add/remove accounts (max of 5 accounts) as well as adjust their specific privileges.



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Settings

System Log

SNMP Agent

TR-069 Client

Internet Time

Access Control

Accounts

Service Access

IP Address

Update Software

Reboot

Access Control -- Accounts/Passwords

By default, access to your Broadband router is controlled through three user accounts: root,support,and user.

The root account has unrestricted access to view and change the configuration of your Broadband router.

The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.

The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.

Use the fields below to update passwords for the accounts, add/remove accounts (max of 5 accounts). Note: Passwords may be as long as 16 characters but must not contain a space.

Select an account:

Create an account:

Old Password:

New Password:

Confirm Password:

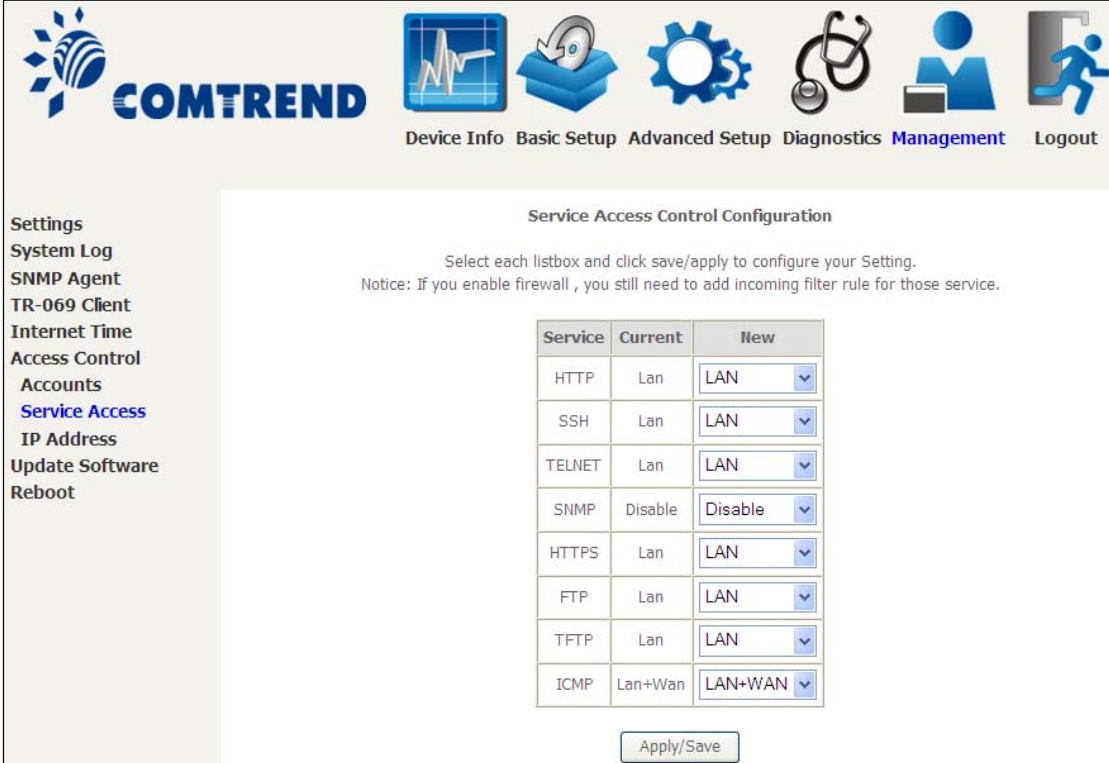
Use the fields below to enable/disable accounts as well as adjust their specific privileges.

Feature	root	support	user	apuser
Account access	Both	<input type="button" value="None"/>	<input type="button" value="None"/>	<input type="button" value="None"/>
Add/Remove WAN	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wireless - Basic	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wireless - Advanced	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LAN Settings	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Port Mapping	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAT Settings	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Update Software	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Quality of Service	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management Settings	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced Setup	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: Passwords may be as long as 16 characters but must not contain a space. Click **Save/Apply** to continue.

8.6.2 Service Access

The Services option limits or opens the access services over the LAN or WAN. These access services available are: FTP, HTTP, ICMP, SNMP, TELNET and TFTP. Enable a service by selecting its dropdown listbox. Click **APPLY/SAVE** to activate.



COMTREND

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

Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Accounts
Service Access
IP Address
Update Software
Reboot

Service Access Control Configuration

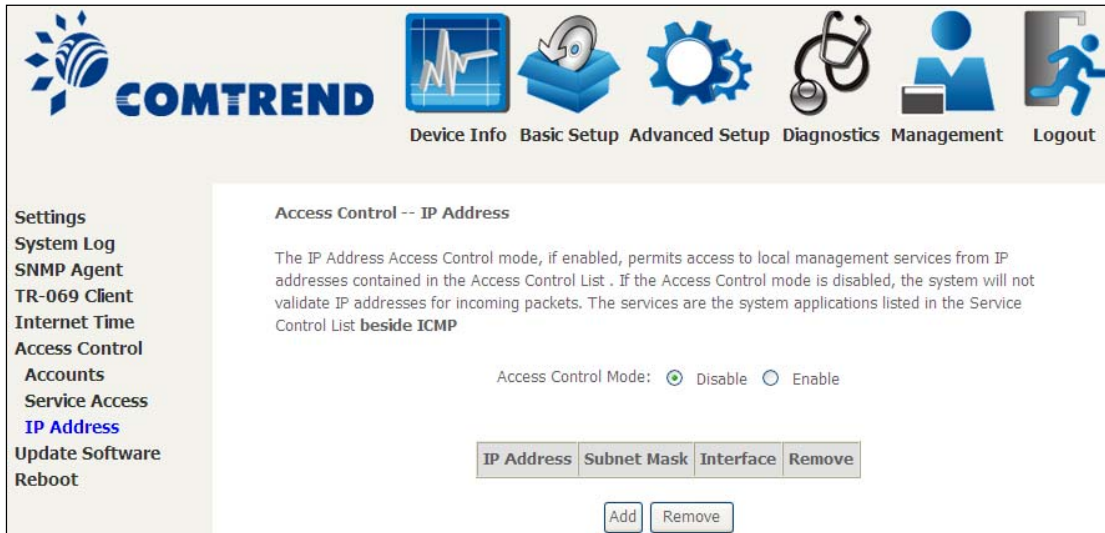
Select each listbox and click save/apply to configure your Setting.
Notice: If you enable firewall , you still need to add incoming filter rule for those service.

Service	Current	New
HTTP	Lan	LAN
SSH	Lan	LAN
TELNET	Lan	LAN
SNMP	Disable	Disable
HTTPS	Lan	LAN
FTP	Lan	LAN
TFTP	Lan	LAN
ICMP	Lan+Wan	LAN+WAN

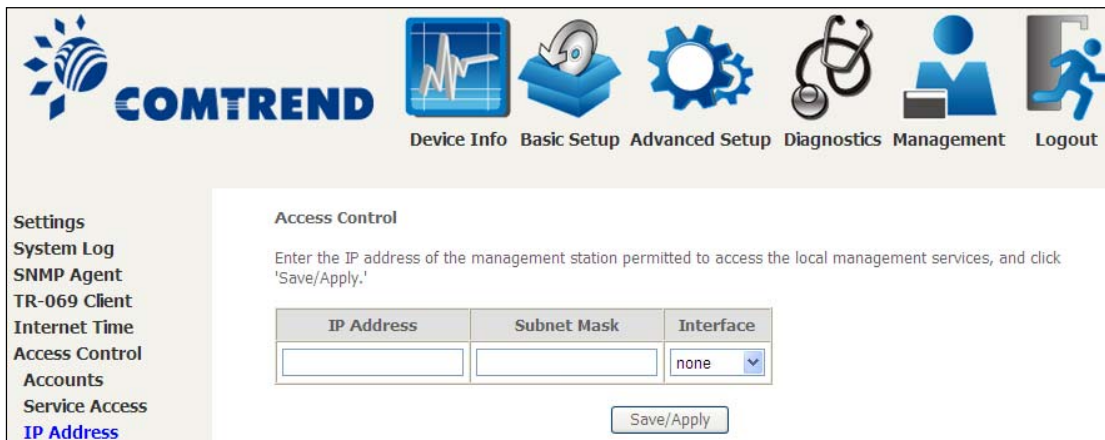
Apply/Save

8.6.3 IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List **beside ICMP**.



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



Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.


IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.

8.7 Update Software

This option allows for firmware upgrades from a locally stored file.



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

Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Reboot

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Configuration:

Software File Name: No file selected.

STEP 1: Obtain an updated software image file from your ISP.

STEP 2: Select the configuration from the drop-down menu.

Configuration options:

No change – upgrade software directly.

Erase current config – If the router has save_default configuration, this option will erase the current configuration and restore to save_default configuration after software upgrade.

Erase All – Router will be restored to factory default configuration after software upgrade.

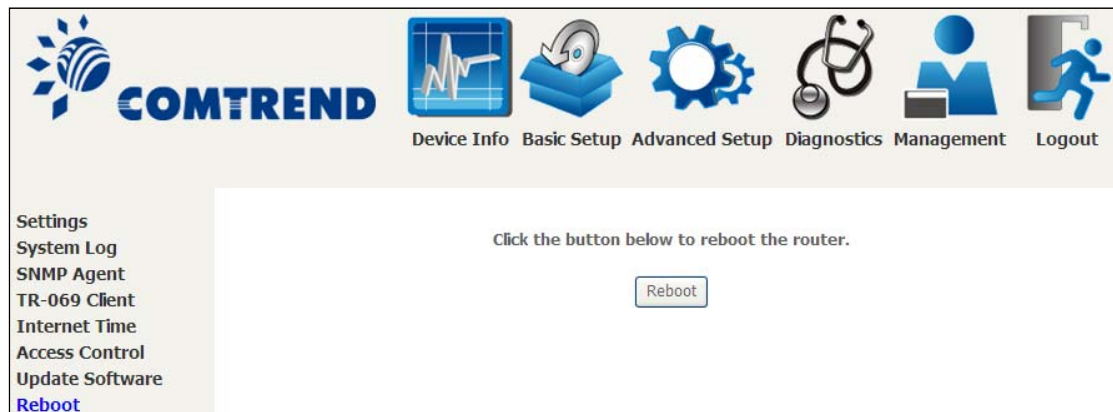
STEP 3: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 4: Click the **Update Software** button once to upload and install the file.

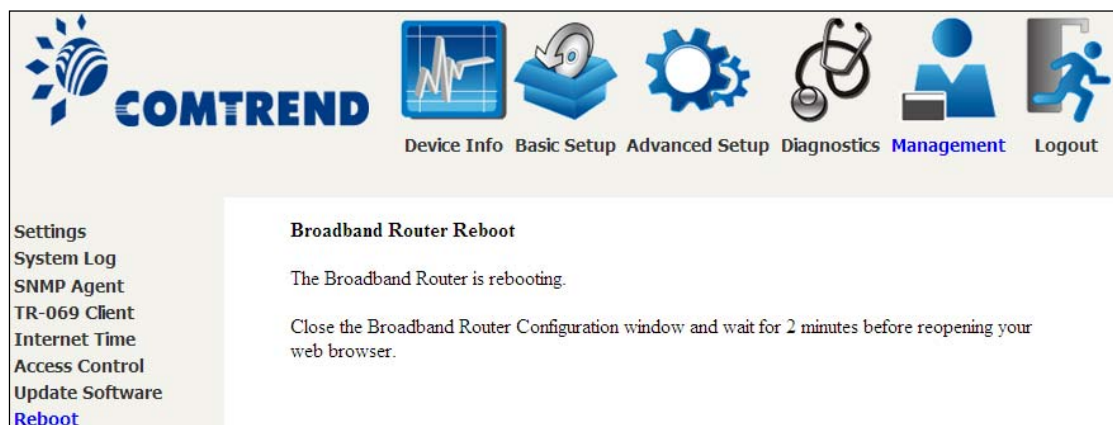
NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Information](#) screen with the firmware version installed, to confirm the installation was successful.

8.8 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.



NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

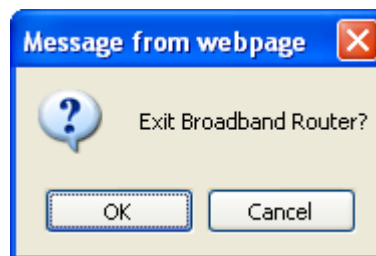


Chapter 9 Logout

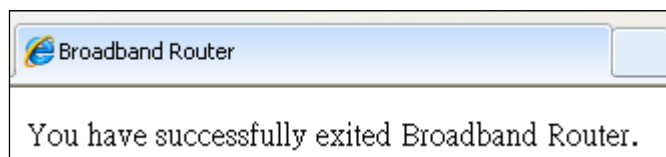
To log out from the device simply click the following icon located at the top of your screen.



When the following window pops up, click the **OK** button to exit the router.



Upon successful exit, the following message will be displayed.



Appendix A - Firewall

STATEFUL PACKET INSPECTION

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER

These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER

Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:

Filter Name	:	Out_Filter1
Protocol	:	TCP
Source IP address	:	192.168.1.45
Source Subnet Mask	:	255.255.255.0
Source Port	:	80
Dest. IP Address	:	NA
Dest. Subnet Mask	:	NA
Dest. Port	:	NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:

Filter Name	:	Out_Filter2
Protocol	:	UDP
Source IP Address	:	192.168.1.45
Source Subnet Mask	:	255.255.255.0
Source Port	:	5060:6060
Dest. IP Address	:	172.16.13.4
Dest. Subnet Mask	:	255.255.255.0
Dest. Port	:	6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER

Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the WR-6891u , as per chosen days of the week and the chosen times.

Example:

User Name	: FilterJohn
Browser's MAC Address	: 00:25:46:78:63:21
Days of the Week	: Mon, Wed, Fri
Start Blocking Time	: 14:00
End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

Signals for ETHERNET WAN port (10/1001000Base-T)

Pin	Signal name	Signal definition
1	TRD+(0)	Transmit/Receive data 0 (positive lead)
2	TRD-(0)	Transmit/Receive data 0 (negative lead)
3	TRD+(1)	Transmit/Receive data 1 (positive lead)
4	TRD+(2)	Transmit/Receive data 2 (positive lead)
5	TRD-(2)	Transmit/Receive data 2 (negative lead)
6	TRD-(1)	Transmit/Receive data 1 (negative lead)
7	TRD+(3)	Transmit/Receive data 3 (positive lead)
8	TRD-(3)	Transmit/Receive data 3 (negative lead)

Appendix C – Specifications

Hardware Interface

RJ-45 X 4 for LAN GB Ports, RJ-45 X 1 for WAN GB Port, (10/100/1000 BaseT auto-sense), Reset Button X 1, WPS/WiFi on/off button x1, Power Switch X 1, Wi-Fi Antennas X 2, USB Host X 1

Gigabit Ethernet WAN

10/100/1000 Mbps
RJ45 connector

LAN Interface

Standard..... IEEE 802.3, IEEE 802.3u
MDI/MDX support..... Yes
Multiple Subnets on LAN

Wireless Interface

Standard IEEE802.11b/g
Encryption..... 64/128-bit Wired Equivalent Privacy (WEP)
Channels..... 11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate Up to 300Mbps
WPA Yes
WPA2 Yes
IEEE 802.1x Yes

Management

Compliant with TR-069/TR-098/TR-111/TR-143 remote management protocols, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

Bridge Functions

Transparent bridging and learning..... Yes
VLAN support Yes
Spanning Tree Algorithm Yes
IGMP Proxy Yes

Routing Functions

Static route, RIP v1/v2, DHCP Server/Client/Relay, DNS Proxy, ARP, RARP, SNTP

Security Functions

Authentication protocols: PAP, CHAP
Packet and MAC address filtering, IPSec termination, Three level login including local admin, local user and remote technical support access

QoS

Packet level QoS classification rules,
IP TOS/Precedence,
802.1p marking,
DiffServ DSCP marking
Src/dest MAC addresses classification

Application Layer Gateway

FTP, SIP, H.323, RTSP, L2TP, Yahoo messenger, ICQ, RealPlayer, Net2Phone,
NetMeeting, MSN, X-box, Microsoft DirectX games

Power Supply Input: 100 - 240 Vac
Output: 12 Vdc / 1A

Environment Condition

Operating temperature..... 0 ~ 40 degrees Celsius
Relative humidity 5 ~ 95% (non-condensing)

Dimensions 206 mm (W) x 46 mm (H) x 160 mm (D)

Kit Weight

(1*WR-6891u, 1*RJ14 cable, 2*RJ45 cable, 1*power adapter) = 0.6 kg

NOTE: Specifications are subject to change without notice
--

Appendix D - SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: `ssh -l root 192.168.1.1`

For WAN access, type: `ssh -l support WAN IP address`

To access the router using the Windows "putty" ssh client

For LAN access, type: `putty -ssh -l root 192.168.1.1`

For WAN access, type: `putty -ssh -l support WAN IP address`

NOTE: The WAN IP address can be found on the Device Info → WAN screen

Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

- 1 - Setup a Layer 2 Interface
- 2 - Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

E1 ~ Layer 2 Interface

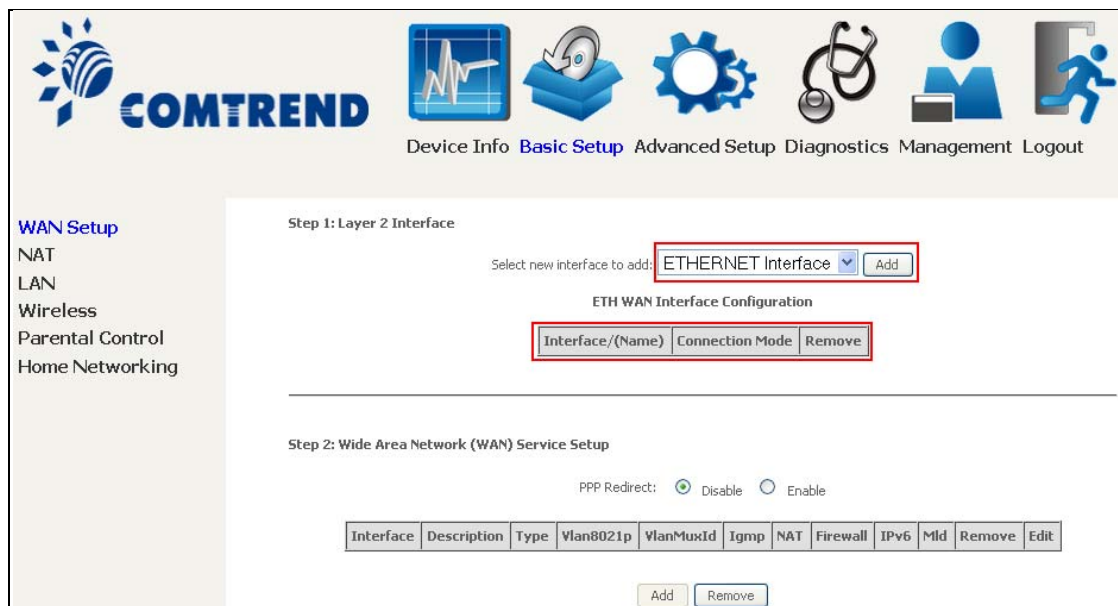
Every layer2 interface operates in Multi-Service Connection (VLAN MUX) mode, which supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces.

ETHERNET Interfaces

Follow these procedures to configure a PTM interface.



STEP 1: Go to Basic Setup → WAN Setup → Select ETHERNET Interface from the drop-down menu.



This table is provided here for ease of reference.

Heading	Description
Interface/ (Name)	WAN interface name.
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface.
Remove	Select interfaces to remove.

STEP 2: Click **Add** to proceed to the next screen.

ETH WAN Configuration

This screen allows you to configure a ETH port

Full Gigabit WAN Interfaces (GMAC): eth0

Select a ETH port:

eth0/WAN ▾

STEP 3: Select an Ethernet port and Click **Apply/Save** to confirm your choices.

On the next screen, check that the ETHERNET interface is added to the list.

ETH WAN Interface Configuration		
Interface/(Name)	Connection Mode	Remove
eth0/WAN	VlanMuxMode	<input type="button" value="Remove"/>

Note: A new parameter will be added to the screen:

Step 1: Layer 2 Interface

Select new interface to add: ETHERNET Interface ▾

Select WAN media type to apply: Auto ▾

ETH WAN Interface Configuration

Interface/(Name)	Connection Mode	Remove
eth0/WAN	VlanMuxMode	<input type="button" value="Remove"/>

Select WAN media type to apply: Select from the drop-down menu and click the **Apply** button.

E2 ~ WAN Connections

The WR-6891u supports one WAN connection for each interface, up to a maximum of 16 connections.

To setup a WAN connection follow these instructions.

Note: Before you start, it is necessary to select the WAN media type from the drop-down menu and click the **Apply** button.

Step 1: Layer 2 Interface

Select new interface to add:

Select WAN media type to apply:

ETH WAN Interface Configuration

Interface/(Name)	Connection Mode	Remove
eth0/WAN	VlanMuxMode	<input type="button" value="Remove"/>



STEP 1: Go to Basic Setup  → WAN Setup.

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: Disable Enable

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
										<input type="button" value="Add"/>	<input type="button" value="Remove"/>

Note:

PPP Redirect: if enabled (i.e. the enable radio button is selected) the function would make an ISP Login Failed window pop up (shown below) if the user logged in with an invalid PPP password while trying to surfing the web.

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

STEP 2: Click **Add** to create a WAN connection. The following screen will display.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

eth0/WAN ▾

STEP 3: Choose a layer 2 interface from the drop-down menu and click **Next**. The WAN Service Configuration screen will display as shown below.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
 For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:
 ▾

NOTE: The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.

Enter 802.1P Priority [0-7]:	-1
Enter 802.1Q VLAN ID [0-4094]:	-1

STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

- (1) For [PPP over ETHERNET \(PPPoE\)](#), go to page 139.
- (2) For [IP over ETHERNET \(IPoE\)](#), go to page 144.
- (3) For [Bridging](#), go to page 148.

The subsections that follow continue the WAN service setup procedure.

E2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox at the bottom of this screen.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

The settings shown above are described below.

PPP SETTINGS

The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The WR-6891u can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text" value="0"/>

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in [section 3.2](#).

FIXED MTU

Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The WR-6891u supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

NO MULTICAST VLAN FILTER

Tick the checkbox to Enable/Disable multicast VLAN filter.

Enable WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 3: Choose an interface to be the default gateway.

Routing -- Default Gateway

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	

Click **Next** to continue or click **Back** to return to the previous step.

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 a static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Configuration

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

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

After clicking **Apply/Save**, the new service should appear on the main screen.

E2.2 IP over ETHERNET (IPoE)

STEP 1: *Select the IP over Ethernet radio button and click **Next**.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

WAN interface with base MAC.
Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

NOTE: If IPv6 networking is enabled, an additional set of instructions, radio buttons, and text entry boxes will appear at the bottom of the screen. These configuration options are quite similar to those for IPv4 networks.

Click **Next** to continue or click **Back** to return to the previous step.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox . Click **Next** to continue or click **Back** to return to the previous step.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should not be selected, so as to free up system resources for improved performance.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

Enable WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

Routing -- Default Gateway

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

<p>Selected Default Gateway Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;">eth0.1</div>	<div style="border: 1px solid gray; padding: 5px; width: 30px; margin: 5px auto;">-></div> <div style="border: 1px solid gray; padding: 5px; width: 30px; margin: 5px auto;"><-</div>	<p>Available Routed WAN Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;"></div>
<div style="display: flex; justify-content: center; gap: 20px;"> <div style="border: 1px solid gray; padding: 5px 15px;">Back</div> <div style="border: 1px solid gray; padding: 5px 15px;">Next</div> </div>		

STEP 4: To choose an interface to be the default gateway.

Click **Next** to continue or click **Back** to return to the previous step.

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;">eth0.1</div>	<div style="border: 1px solid gray; padding: 5px; width: 30px; margin: 5px auto;">-></div> <div style="border: 1px solid gray; padding: 5px; width: 30px; margin: 5px auto;"><-</div>	<p>Available WAN Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;"></div>
<p><input type="radio"/> Use the following Static DNS IP address:</p> <p>Primary DNS server: <input style="width: 150px;" type="text"/></p> <p>Secondary DNS server: <input style="width: 150px;" type="text"/></p>		
<div style="display: flex; justify-content: center; gap: 20px;"> <div style="border: 1px solid gray; padding: 5px 15px;">Back</div> <div style="border: 1px solid gray; padding: 5px 15px;">Next</div> </div>		

STEP 5: 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 a static IPoE protocol is configured, Static DNS server IP addresses must be entered.

If IPv6 is enabled, an additional set of options will be shown.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: ▼

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

After clicking **Apply/Save**, the new service should appear on the main screen.

E2.3 Bridging

NOTE: This connection type is not available on the Ethernet WAN interface.

STEP 1: *Select the Bridging radio button and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
 For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

After clicking **Apply/Save**, the new service should appear on the main screen.

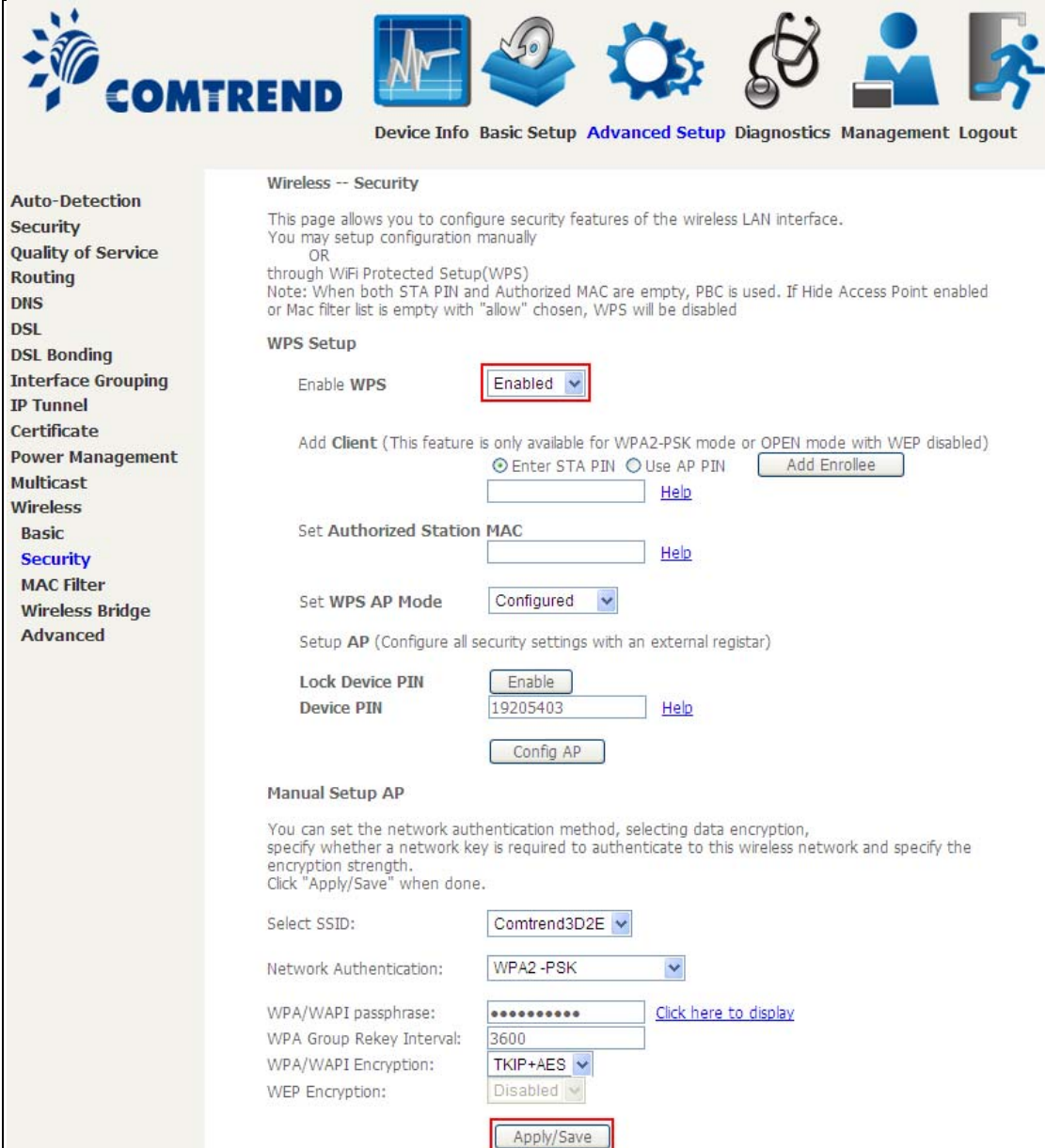
NOTE: If this bridge connection is your only WAN service, the WR-6891u will be inaccessible for remote management or technical support from the WAN.

Appendix F - WPS OPERATION

This Section shows the basic AP WPS Operation procedure.

F1 Add Enrollee with Pin Method

- 1) Go to Advanced Setup → Wireless → Security.
- 2) Select **Enabled** from the Enable WPS dropdown menu.
- 3) Click the **Apply/Save** button at the bottom of the screen.



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
 Basic
Security
 MAC Filter
 Wireless Bridge
 Advanced

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
 You may setup configuration manually
 OR
 through WiFi Protected Setup(WPS)
 Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable WPS **Enabled**

Add Client (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)
 Enter STA PIN Use AP PIN
 [Help](#)

Set Authorized Station MAC
 [Help](#)

Set WPS AP Mode **Configured**

Setup AP (Configure all security settings with an external registrar)

Lock Device PIN
 Device PIN [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
 Click "Apply/Save" when done.

Select SSID: **Comtrend3D2E**

Network Authentication: **WPA2-PSK**

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption: **TKIP+AES**

WEP Encryption: **Disabled**

- 4) When the screen refreshes select the Radio button "Enter STA Pin"
- 5) Input Pin from Enrollee Station (15624697 in this example)

6) Click "Add Enrollee"

Add **Client** (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)

Enter STA PIN Use AP PIN Add Enrollee

 [Help](#)

7) Operate Station to start WPS Adding Enrollee.

F2 Add Enrollee with PBC Method

1) Press the WPS button on the front of the device to activate WPS PBC operation.

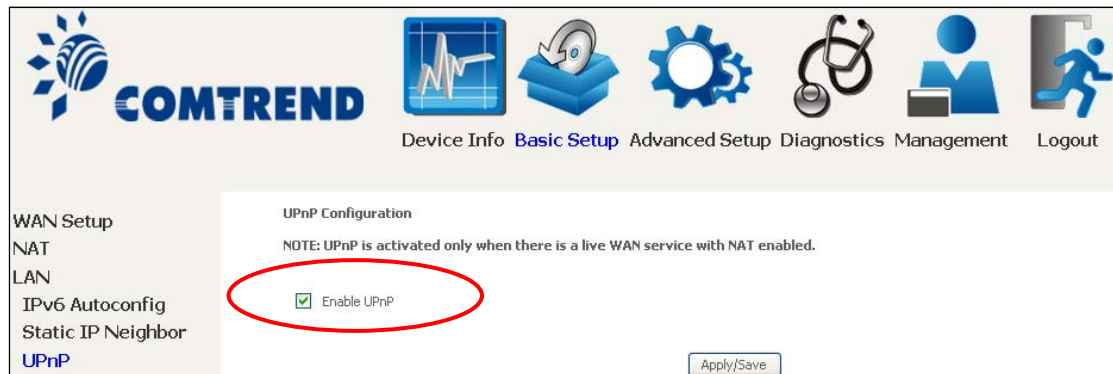


2) Operate Station (your dongle for example) to start WPS Adding Enrollee.

F3 – Configure WPS External Registrar

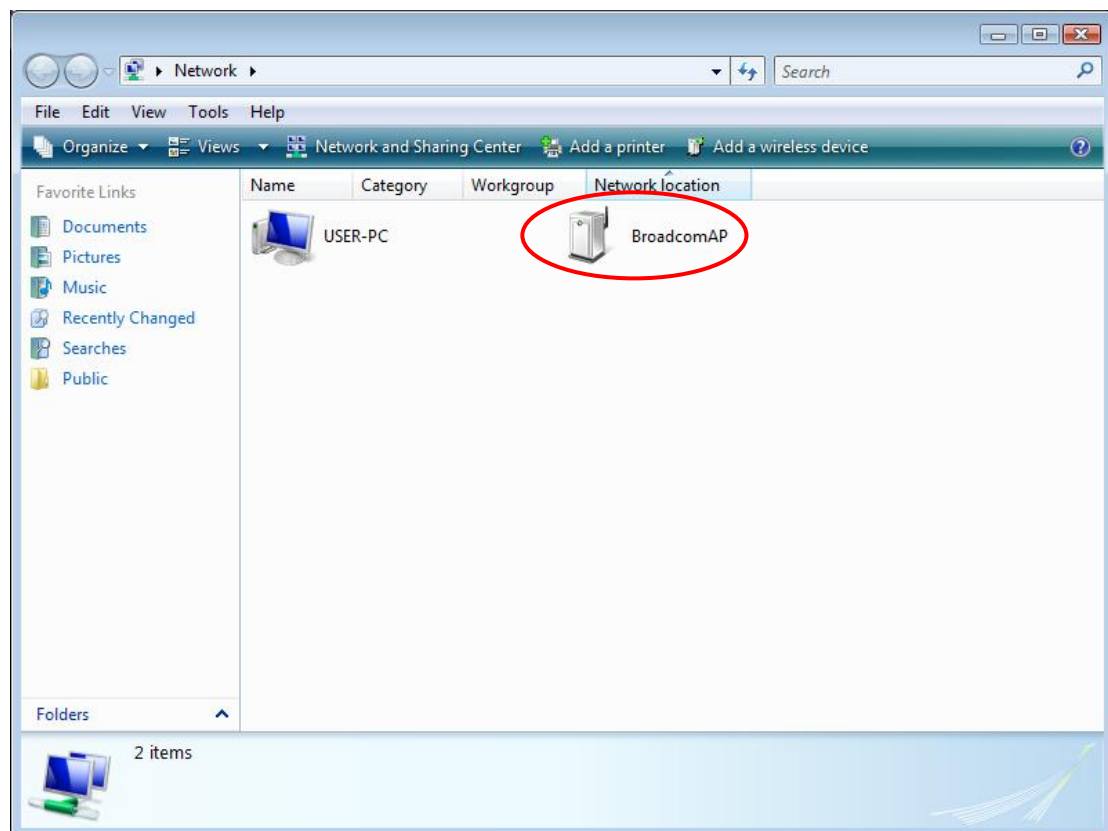
Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows 7 operating system:

Step 1: Enable UPnP on the Advanced Setup → LAN screen in the WUI.

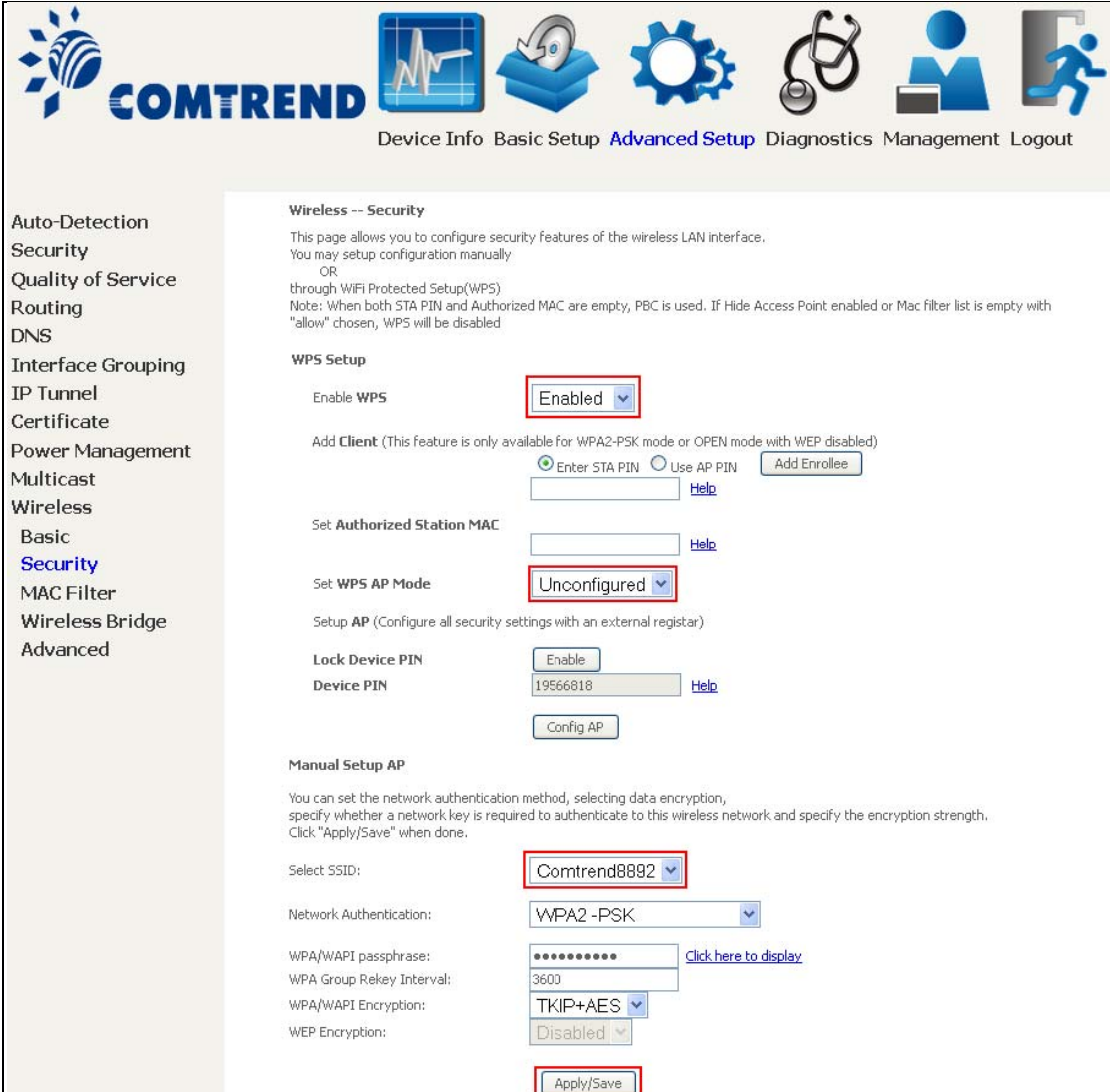


NOTE: A PVC must exist to see this option.

Step 2: Open the Network folder and look for the BroadcomAP icon.



Step 3: On the Wireless → Security screen, enable WSC by selecting **Enabled** from the drop down list box and set the WPS AP Mode to Unconfigured.



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

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

Wireless -- Security
This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable WPS **Enabled** ▾

Add Client (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)
 Enter STA PIN Use AP PIN
 [Help](#)

Set Authorized Station MAC [Help](#)

Set WPS AP Mode **Unconfigured** ▾

Setup AP (Configure all security settings with an external registrar)

Lock Device PIN
Device PIN [Help](#)

Manual Setup AP
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: **Comtrend8892** ▾

Network Authentication: WPA2 -PSK ▾

WPA/WAPI passphrase: [Click here to display](#)

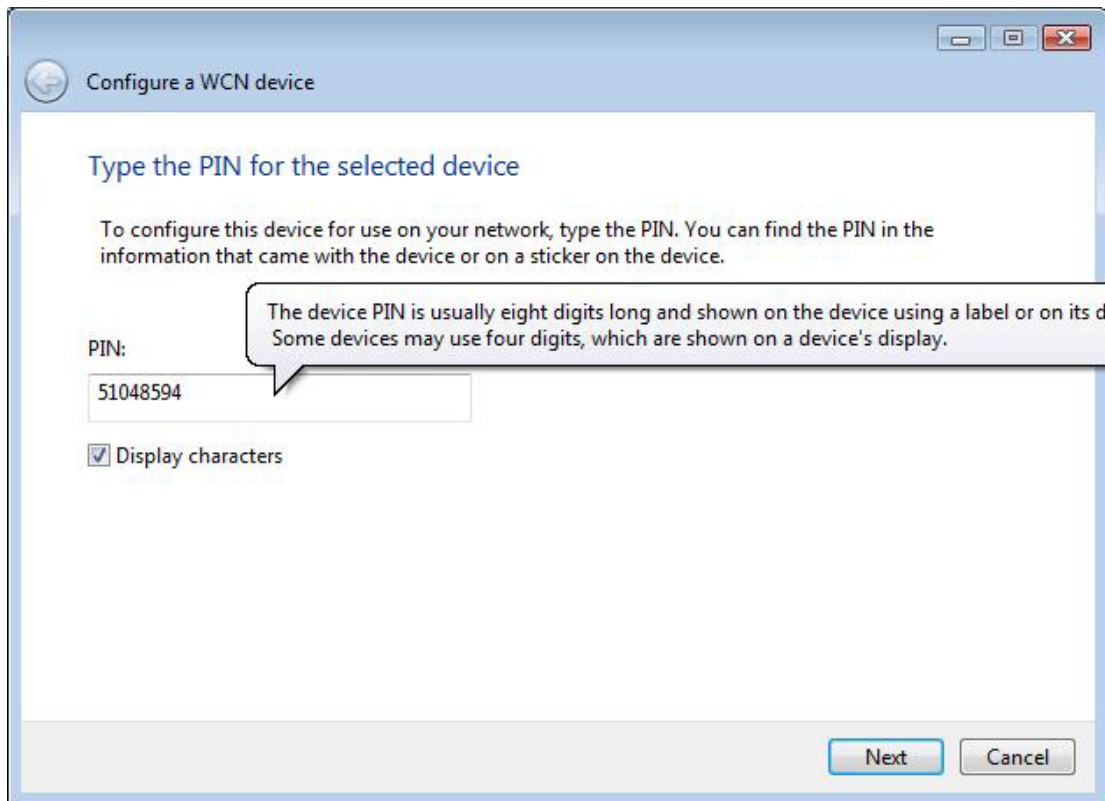
WPA Group Rekey Interval:

WPA/WAPI Encryption: TKIP+AES ▾

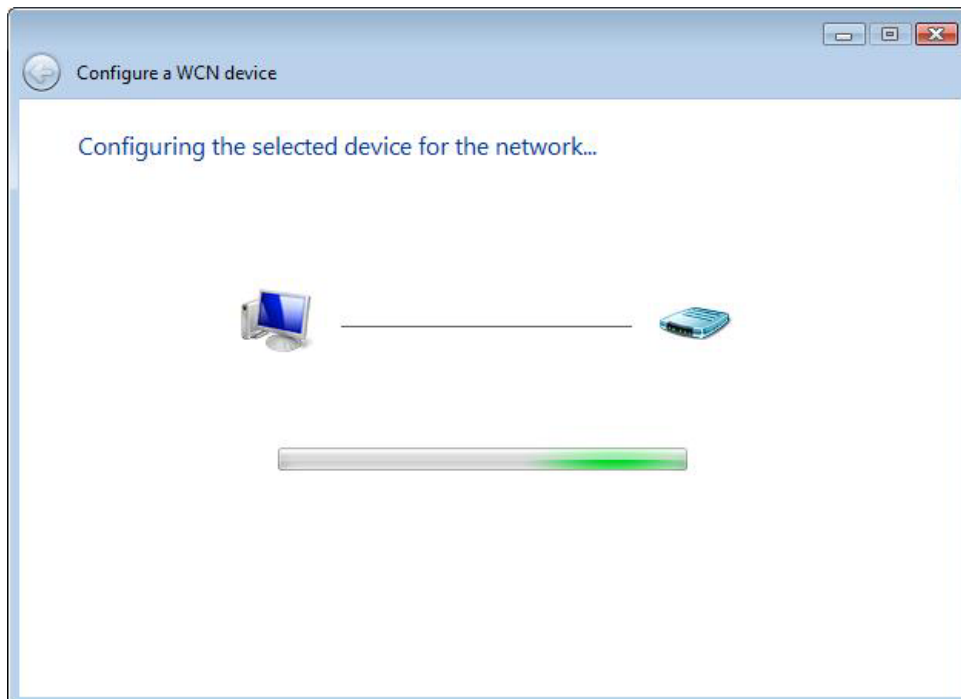
WEP Encryption: Disabled ▾

Step 4: Click the **Apply/Save** button at the bottom of the screen. The screen will go blank while the router applies the new Wireless settings.

Step 5: Now return to the Network folder and click the BroadcomAP icon. A dialog box will appear asking for the Device PIN number. Enter the Device PIN as shown on the Wireless → Security screen. Click **Next**.



Step 6: Windows 7 will attempt to configure the wireless security settings.



Step 7: If successful, the security settings will match those in Windows 7.

Appendix G - Printer Server

These steps explain the procedure for enabling the Printer Server.

NOTE: This function only applies to models with an USB host port.

STEP 1: Enable Print Server from Web User Interface. Select Enable on-board print server checkbox and enter Printer name and Make and model

NOTE: The **Printer name** can be any text string up to 40 characters.
The **Make and model** can be any text string up to 128 characters.

Print Server settings

This page allows you to enable / disable printer support.

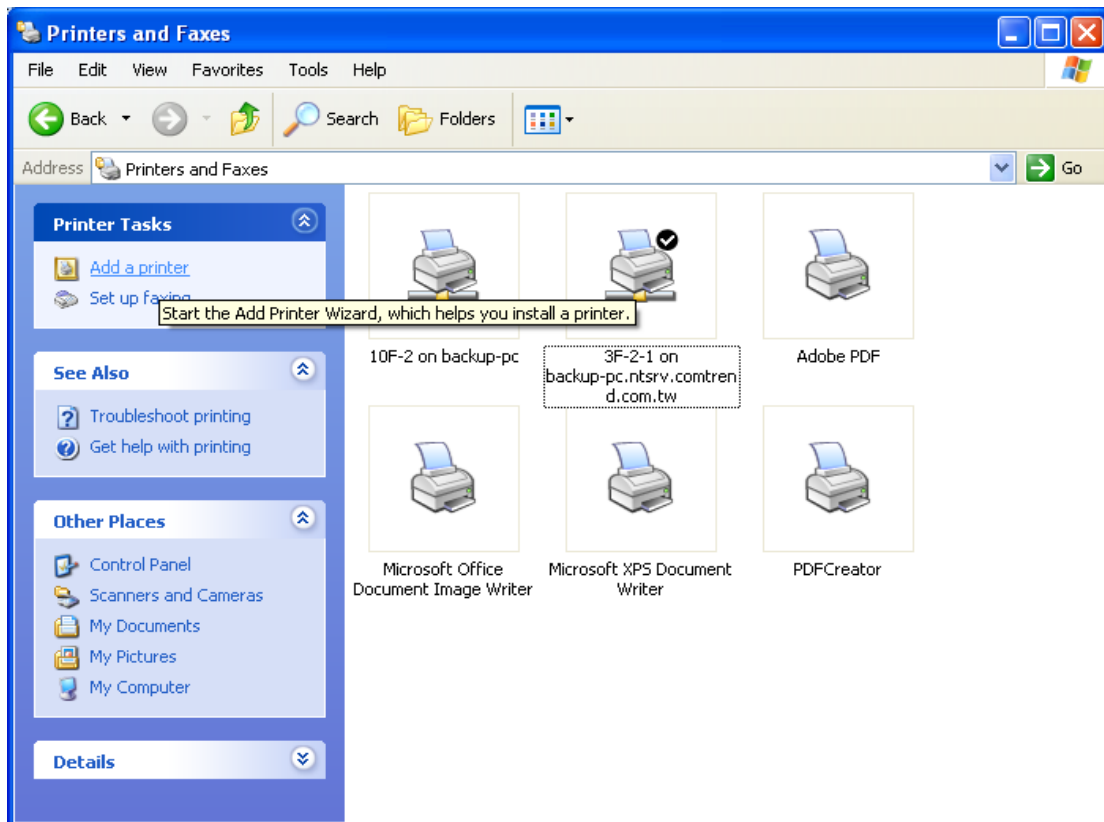
Manufacturer	Product	Serial Number
--------------	---------	---------------

Enable on-board print server.

Printer name

Make and model

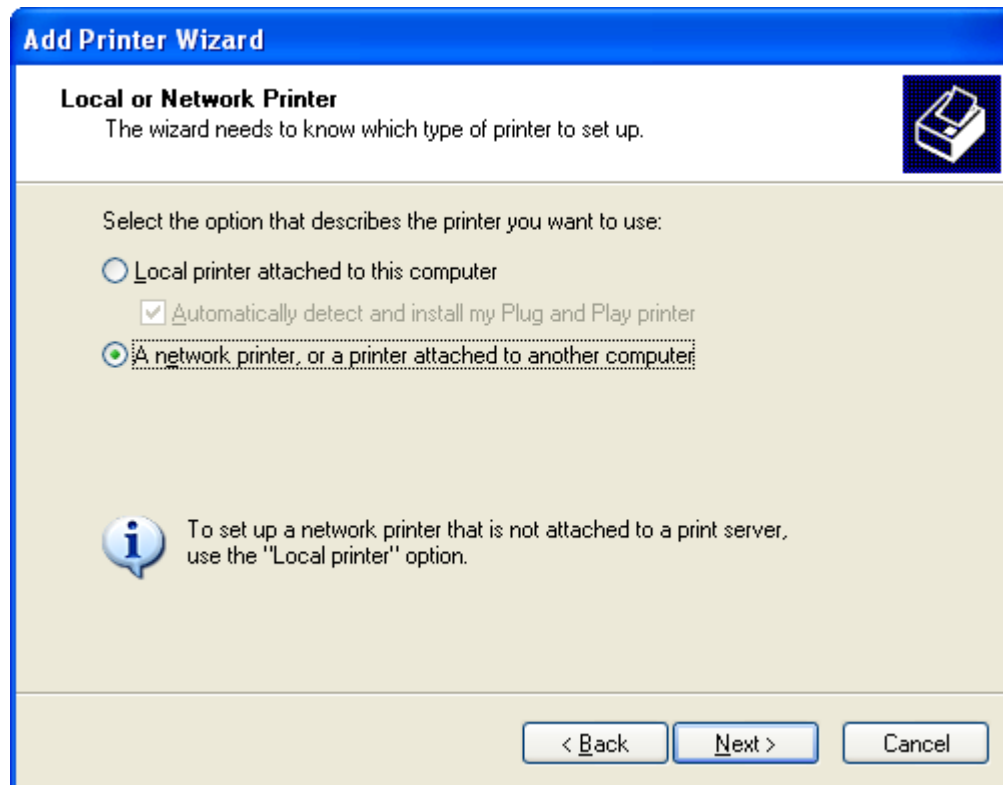
STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



STEP 3: Click **Next** to continue when you see the dialog box below.

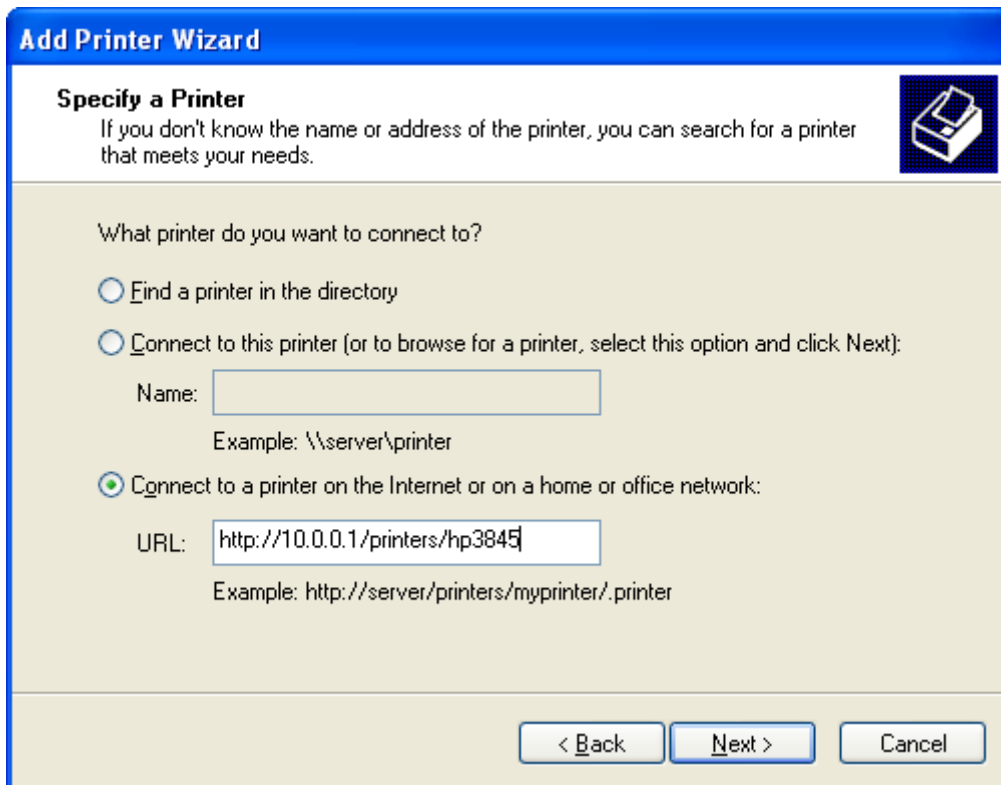


STEP 4: Select **Network Printer** and click **Next**.



STEP 5: Select **Connect to a printer on the Internet** and enter your printer link. (e.g. <http://192.168.1.1:631/printers/hp3845>) and click **Next**.

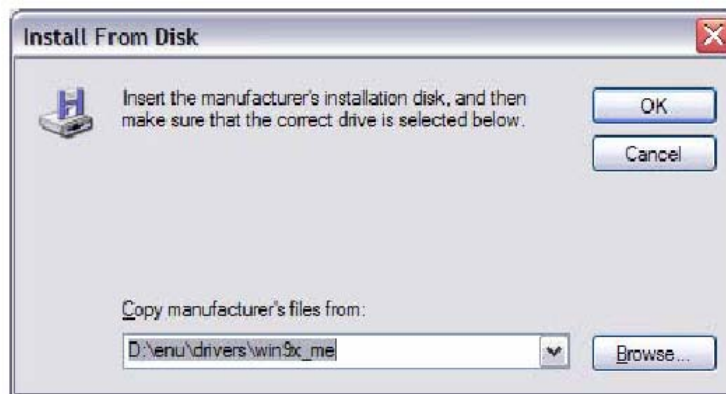
NOTE: The printer name must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.



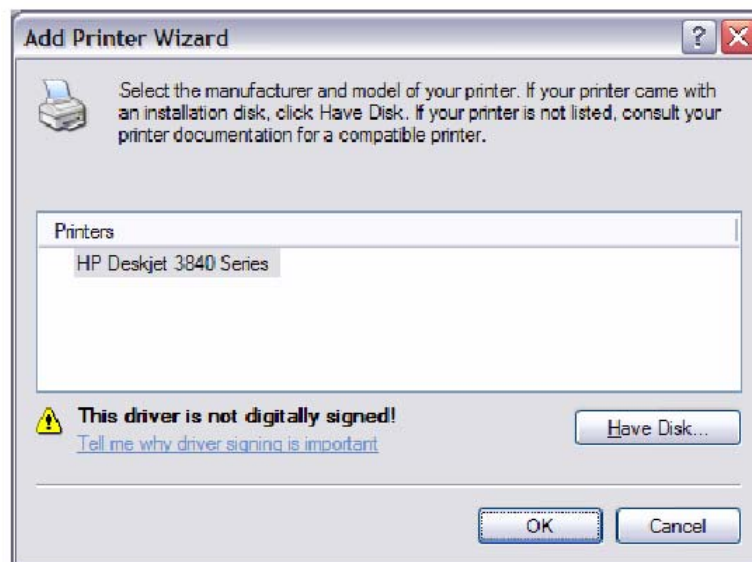
STEP 6: Click **Have Disk** and insert the printer driver CD.



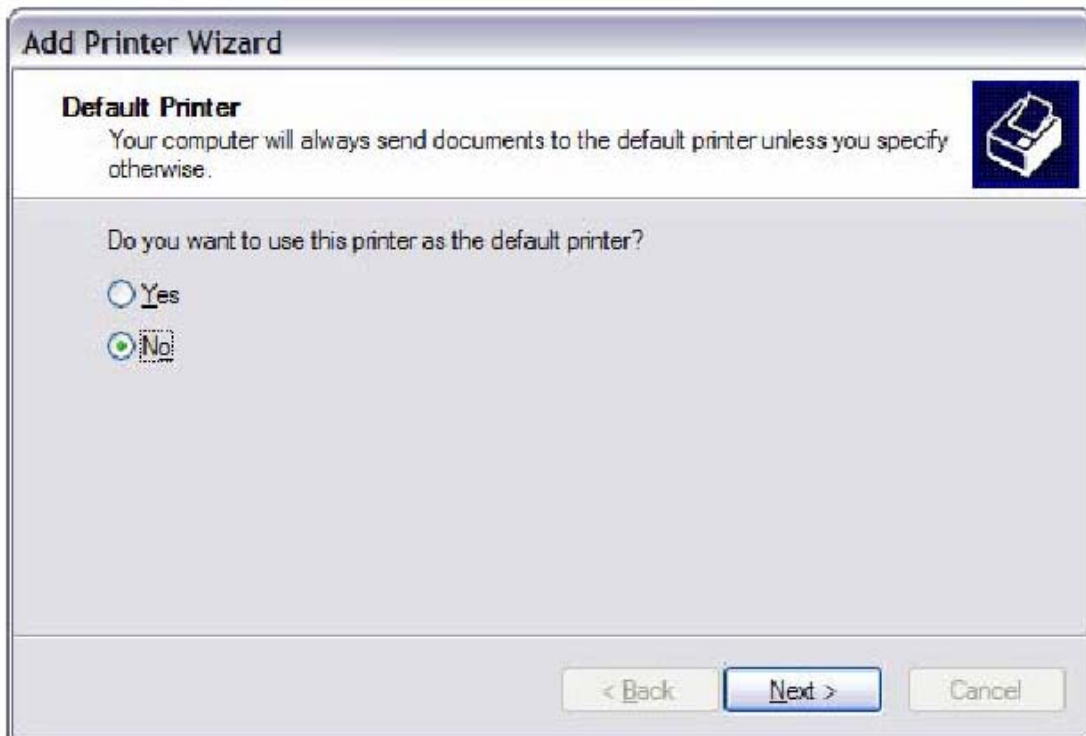
STEP 7: Select driver file directory on CD-ROM and click **OK**.



STEP 8: Once the printer name appears, click **OK**.



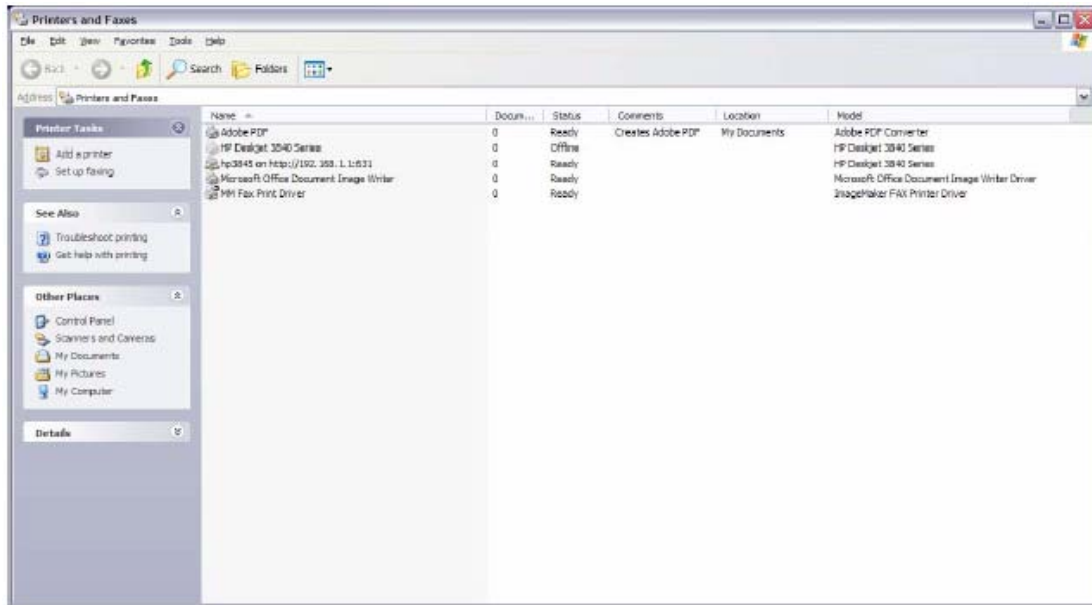
STEP 9: Choose **Yes** or **No** for default printer setting and click **Next**.



STEP 10: Click Finish.



STEP 11: Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.



FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on , the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cmbetween the radiator & your body

<p>FCC Caution: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.</p>
--