

CY-SWR1100 User Manual



Wireless Router



SAFETY INFORMATION

SAFETY WARNINGS

To reduce the risk of electric shock, do not remove the cover (or back).
No user serviceable parts are inside. Refer to qualified service personnel.

	<div style="text-align: center;"> <p>CAUTION</p> <p>RISK OF ELECTRIC SHOCK DO NOT OPEN</p> </div>	
<p>This symbol indicates “dangerous voltage” inside the product that presents a risk of electric shock or personal injury.</p>	<p>Caution: To prevent electric shock, match wide blade of plug to the wide slot, fully insert.</p>	<p>This symbol indicates important instructions accompanying the product.</p>

Warning

- To reduce the risk of fire or electric shock, do not expose this appliance to rain or moisture.

Caution

- Apparatus shall not be exposed to dripping or splashing and no objects filled with liquids, such as vases, shall be placed on the apparatus.
- The Mains plug is used as a disconnect device and shall stay readily operable at any time.
- This apparatus shall always be connected to a AC outlet with a protective grounding connection.
- To disconnect the apparatus from the mains, the plug must be pulled out from the mains socket, therefore the mains plug shall be readily operable.

PRECAUTIONS

- Ensure that the AC power supply in your house complies with the identification sticker located on the back of your product.
- Install your product horizontally or vertically, on a suitable base (furniture), with enough space around it for ventilation (7.5~10cm).
- Do not place the product on amplifiers or other equipment which may become hot.
- Do not stack anything on top of the product.
- In order to disconnect the product completely from the power supply, remove the main plug from the wall outlet, especially when left unused for a long period of time.
- During thunderstorms, disconnect the AC main plug from the wall outlet. Voltage peaks due to lightning could damage the product.
- Do not expose the product to direct sunlight or other heat sources. This could lead to overheating and malfunction of the product.
- Protect the product from moisture, and excess heat or equipment creating strong magnetic or electric fields (i.e. speakers).
- Disconnect the power cable from the AC supply if the product malfunctions.
- Your product is not intended for industrial use. Use of this product is for personal use only.
- Condensation may occur if your product has been stored in cold temperatures. If transporting the product during the winter, wait approximately 2 hours until the product has reached room temperature before using.

TABLE OF CONTENTS

Safety Information	2	Knowledge Base	90
Safety Warnings	2	One Foot Connection (OFC) Method	90
Precautions	2	Connect my Samsung TV to the router using OFC	90
Getting Started	4	Plug & Access Connection Method	91
Package Contents	4	Connect my Samsung TV to the router using Plug & Access	91
System Requirements	4	Priority Quality of Service	91
About this Product	5	Wireless Basics	92
Features	5	Wireless Modes	94
Description	6	Wireless Security	94
Front View	6	What is WPA?	94
Back View	6	Networking Basics	95
Installation	7	Connect to a Wireless Network	96
Before you Begin	7	Using Windows® 7	96
Wireless Installation Considerations	7	Configuration WPS	97
Connect to Cable/DSL/Satellite Modem	7	Using Windows Vista®	100
Connect to Another Router	8	Using Windows® XP	101
Connecting to the Web UI	9	Troubleshooting	102
Router's Defaults	9	Technical Specifications	104
Connecting using the Browser	9		
Web User Interface	10		
Setup Category	11		
Internet - Wizard	12		
Internet - Manual Internet Connection	18		
Wireless Settings	27		
Network Settings	35		
Advanced Category	37		
Virtual Server	38		
Port Forwarding	39		
Application Rules	40		
Quality of Service (QoS)	41		
Network Filter	43		
Access Control	44		
Website Filter	47		
Inbound Filter	48		
Firewall Settings	49		
Routing	50		
Advanced Wireless	51		
Wi-Fi Protected Setup	53		
Advanced Network Settings	55		
Guest Zone	57		
IPv6	59		
IPv6 Firewall	72		
Tools Category	73		
Admin	74		
Time	75		
Syslog	76		
Email Settings	77		
System	78		
Firmware	79		
Dynamic DNS	80		
System Check	81		
Schedules	82		
Status Category	83		
Device Info	84		
Logs	86		
Statistics	87		
Internet Sessions	87		
Wireless	88		
IPv6	88		
Support Category	89		

GETTING STARTED

PACKAGE CONTENTS

Check for the supplied accessories below:

- Wireless 802.11n Dual Band Router
- Power Adapter with extra Power Cable
- Ethernet Cable
- CD-ROM (with installation software and manuals)
- Quick Installation Guide
- Stand
- Mounting Kit



SYSTEM REQUIREMENTS

Network Requirements:

- 10/100Mbps Ethernet LAN adapter
- 802.11a/g/n Wireless Adapter
- Ethernet-based Cable or DSL Modem

Computer Requirements:

- Window 7/Vista/XP (with SP3)
- 10/100 Ethernet LAN adapter
- CD-ROM drive

Software Requirements:

- Operating System like Microsoft Windows, Macintosh, or Linux
- Browser like Internet Explorer (6 or higher), Mozilla Firefox (3.0 or higher), Safari (3.0 or higher), or Chrome (2.0 or higher)

ABOUT THIS PRODUCT

This user's guide provides a wonderful insight into the functionality of the product called the Samsung CY-SWR1100. This guide is based on the current running firmware/software version available for this product and might touch on some new and exciting topics never seen on this product line before providing a rewarding reading experience and in the end acts as a guide when installing and maintaining this product.

FEATURES

The Samsung CY-SWR1100 wireless router is packed with a load of features. Most of these features are what is expected from an Internet Wireless router, and then there are the features that are unique to Samsung products.

- **Internet Connectivity.** In conjunction with a DSL or Cable Modem, this device can act as the Internet Gateway to your local network. Connections like, PPPoE, Static and Dynamic IP Connections, PPTP, and L2TP connection can be made.
- **Wireless LAN functionality.** This router supports the full package of what the 802.11n protocol has to offer. Other remarkable features are WMM, Automatic Fall-back, RF Output Level Control, Latest Wireless Security requirements, WPS and much more.
- **Networking.** This router is equipped with 4 10/100Mbps LAN port and 1 10/100Mbps Internet port. This device can handle a network of up to 1000 MAC addresses.
- **Multicasting.** Supports IGMPv2.
- **DHCP.** This device supports both Server and Client functionality.
- **Quality of Service.** QoS rules can be created to shape traffic based on weight or priority. IP Pools can be managed based on application port numbers.
- **Advanced Security.** The Samsung router supports also a list of security features like Network Filtering, Access Control, Website Filtering, Inbound Filtering and SPI.
- **IPv6.** One of the most attractive features of this router is the fact that not only does it support local IPv6 support, but also IPv6 Internet Connection support. This is truly an Internet Gateway ahead of it's time.
- **More.** Other features like DDNS, System Checking, Firmware Updates, Email Settings (for notification), and Schedules are also available on this device.
- **One Foot Connection.** This powerful, Samsung unique, feature allows you to connect your Samsung TV automatically to this router, using the OFC connection method.
- **Plug & Access.** This powerful, Samsung unique, feature allows you to connect this router to any Samsung wireless device easily by using USB memory stick.
- **Samsung Priority QoS.** This powerful, Samsung unique, feature will identify any Samsung networking device in your network and give it the higher wireless network traffic priority. The is perfect for video steaming to your Samsung TV.

DESCRIPTION

FRONT VIEW



1	POWER LED	A solid blue light indicates a proper connection to the power supply.
2	INTERNET LED	A solid blue light indicates the PPP negotiation has successfully completed.
3	2.4Ghz LED	A solid light indicates that the 2.4GHz wireless segment is ready. This LED blinks during wireless data transmission.
4	5Ghz LED	A solid light indicates that the 5.0GHz wireless segment is ready. This LED blinks during wireless data transmission.
5	WPS BUTTON	Press the WPS button for 1 second to initiate the WPS process. The button will flash blue while a WPS connection is being established. The button will light solid blue for 5 seconds when the device has successfully been added to the network.

BACK VIEW



1	USB PORT	The USB port can be used for WPS enabled Wireless USB adapters. One other feature this port is used for is called the Plug & Access feature.
2	LAN PORTS	The 4 x RJ-45 LAN ports can be used for 10/100Mbps LAN connections like computers.
3	INTERNET PORT	The RJ-45 Internet (WAN) port can be used for connections like a DSL/Cable modem.
4	RESET BUTTON	Pressing the Reset button restores the router to its original factory default settings.
5	POWER SWITCH	Use this switch to power on/power off the device.
6	POWER RECEPTOR	Receptor for the supplied power adapter.

INSTALLATION

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, attic or garage.

BEFORE YOU BEGIN

- Please configure the router with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.
- When running the Setup Wizard from the CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, reconnect your computer back to the modem and make sure you are online.

WIRELESS INSTALLATION CONSIDERATIONS

The wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

CONNECT TO CABLE/DSL/SATELLITE MODEM

If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter to the router and connect to an outlet or power strip.
7. Use the power switch to power on the router. Wait about 30 seconds for the router to boot.
8. Turn on your computer.

CONNECT TO ANOTHER ROUTER

If you are connecting the router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router and use the power switch to power up the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
2. Open a web browser and enter <http://192.168.0.1> and press Enter. When the login window appears, set the user name to '**admin**' and leave the password box empty. Click **Login** to continue.
3. Click on Advanced and then click Advanced Network. Uncheck the Enable UPnP checkbox. Click Save Settings to continue.
4. Click Setup and then click Network Settings. Uncheck the Enable DHCP Server checkbox. Click Save Settings to continue.
5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click Save Settings to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.
6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet (WAN) port of the router.
8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the Configuration and Wireless Security sections for more information on setting up your wireless network.

CONNECTING TO THE WEB UI

This section will help you to connect to your router's Web User Interface (Web UI) for the first time.

ROUTER'S DEFAULTS

The router's default values are as follows:

IP Address:	192.168.0.1
Username:	admin
Password:	(blank)

CONNECTING USING THE BROWSER

To connect the router's Web UI, you'll need to use your Internet Browser. Open your Internet browser, like Internet Explorer, and enter the router's default IP address in the address bar as follows.



After entering the IP address (default is 192.168.0.1), press <enter> or click on the **'Go'** option. This will open a page called the login page, which will look like this:



Enter the username and password in the spaces provided and click on the **Login** button.

WEB USER INTERFACE

This Web User Interface is divided into categories, found in the top menu, and pages, found in the left menu.

The Samsung Wireless router Web UI provides five categories to edit.

Setup:	In this category the user will be able to configure the basic features for this router to function properly on a network. Features like Internet Connectivity, Local Area Network Connectivity and Wireless Connectivity.
Advanced:	In this category the user will be able to configure the more advanced features that can be done by this router. Features like Port Forwarding, Firewall settings, Quality of Service settings and more.
Tools:	In this category the user will be able to configure features that are related to the router itself. Features like the time settings, login accounts, firmware update and more.
Status:	In this category the user will be able to view information regarding the configuration and functionality of this device. Displays like WAN, LAN and Wireless configurations, System, Firewall and Router logs, and more.
Support:	In this category the user will have access to a portal of information regarding each and every page that exists on this device. This information gives the basic description of parameter and uses for the pages.

SETUP CATEGORY

Samsung Wireless Router
Powered by **D-Link**

SETUP ADVANCED TOOLS STATUS SUPPORT

CY-SWR1100 **INTERNET CONNECTION** **HELPFUL HINTS**

INTERNET If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

WIRELESS SETTINGS

NETWORK SETTINGS

INTERNET CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new Samsung Systems Router to the Internet, click on the button below.

[Internet Connection Setup Wizard](#)

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL INTERNET CONNECTION OPTION

If you would like to configure the Internet settings of your new Samsung Router manually, then click on the button below.

[Manual Internet Connection Setup](#)

Helpful Hints...

- If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before, click **Manual Internet Connection Setup** to input all the settings manually.

COPYRIGHT © 2010 SAMSUNG ELECTRONICS CO.,LTD.
ALL RIGHTS RESERVED.

SAMSUNG

In this category the user will be able to configure the basic features for this router to function properly on a network. Features like Internet Connectivity, Local Area Network Connectivity and Wireless Connectivity.

Pages that can be configured in the **Setup** category are as follows:

Internet: On this page the user can configure the Internet settings for this router.

Wireless Settings: On this page the user can configure the Wireless settings for this router.

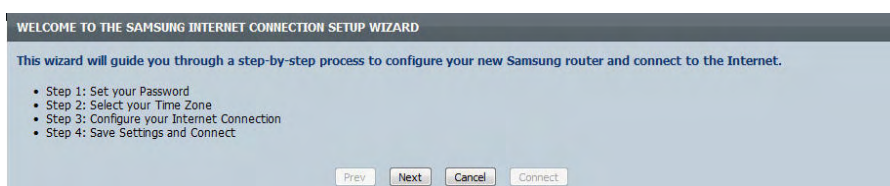
Network Settings: On this page the user can configure the Network settings for this router.

INTERNET - WIZARD

When configuring the CY-SWR1100 for the first time, we recommend that you click use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to assist user with a quick and easy method to configure the Internet Connectivity of this router.



To initiate the quick and easy Internet connection wizard, click on the **Internet Connection Setup Wizard** button. This will start a 4 step configuration process.



This wizard will guide you through a step-by-step process to configure your new Samsung router and connect to the Internet.

Step 1: In this step the user will be able to re-configure the **Login Password** for this device.

Step 2: In this step the user will be able to configure the **Time Zone** used by this device.

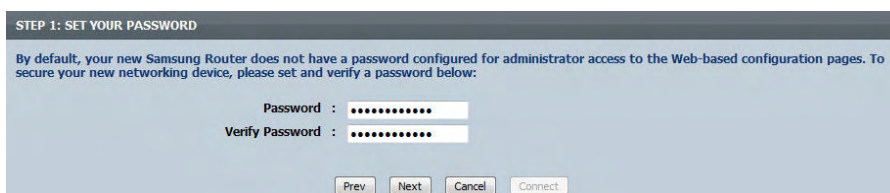
Step 3: In this step the user will be able to configure the **Internet Connectivity** of this device.

Step 4: In this step the user will be able to save the settings and initiate the connection process.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step.

Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Step 1: By default, the new Samsung Router does not have a password configured for administrator access to the Web-based configuration pages. To secure the new networking device, please set and verify a password here.



The following parameters can be configured:

Password:	Enter the new login password used here.
Verify Password:	Re-enter the new login password used here.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step.

Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Step 2: Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

The following parameters can be configured:

Time Zone:	Select the appropriate Time Zone used. This information will be used by the time-based options on this router.
-------------------	--

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Step 3: On this page the user will be able to configure the Internet Connectivity used by this device.

The following parameters can be configured:

Dynamic IP Address:	Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
PPPoE	Choose this option if your Internet connection requires a PPPoE username and password to get online. Most DSL modems use this type of connection.
PPTP	Choose this option if your Internet connection requires a PPTP username and password to get online.
L2TP	Choose this option if your Internet connection requires an L2TP username and password to get online.
Static IP Address:	Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Configure your Internet Connection: Dynamic IP Address Connection

After selecting the **Dynamic IP Address** Internet connection method, the following page will appear:

The following parameters can be configured:

MAC Address:	Enter the MAC address of the Internet gateway (plugged into the Internet port of this device) here.
Clone Button:	If the configuration PC also acts as the Internet gateway, then click on the Clone Your PC's MAC Address button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC Address field blank.
Host Name:	Enter the host name used here. You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Configure your Internet Connection: PPPoE Connection

After selecting the **PPPoE** Internet connection method, the following page will appear:

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPPoE usually requires a Dynamic IP configuration.
IP Address:	Enter the PPPoE IP address used here. This option is only available if Static IP is selected.
User Name:	Enter the PPPoE account user name used here. This information is given by the ISP.
Password:	Enter the PPPoE account password used here. This information is given by the ISP.
Verify Password:	Re-enter the PPPoE account password used here.
Service Name:	This optional field enables the user to enter a service name to identify this Internet connection here.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Configure your Internet Connection: PPTP Connection

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

- DHCP Connection (Dynamic IP Address)
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (PPTP)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (L2TP)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Static IP Address Connection
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

After selecting the **PPTP** Internet connection method, the following page will appear:

SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address : (may be same as gateway)

User Name :

Password :

Verify Password :

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPTP usual requires a Dynamic IP configuration.
PPTP IP Address:	Enter the PPTP IP address used here. This option is only available if Static IP is selected.
PPTP Subnet Mask:	Enter the PPTP Subnet Mask used here.
PPTP Gateway IP Address:	Enter the PPTP Gateway IP address used here.
PPTP Server IP Address:	Enter the PPTP Server IP address used here. This is normally the same a the PPTP Gateway IP address.
User Name:	Enter the PPTP username used here.
Password:	Enter the PPTP password used here.
Verify Password:	Re-enter the PPTP password used here.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Configure your Internet Connection: L2TP Connection

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

- DHCP Connection (Dynamic IP Address)
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (PPTP)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (L2TP)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Static IP Address Connection
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

After selecting the **L2TP** Internet connection method, the following page will appear:

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usual requires a Dynamic IP configuration.
L2TP IP Address:	Enter the L2TP IP address used here. This option is only available if Static IP is selected.
L2TP Subnet Mask:	Enter the L2TP Subnet Mask used here.
L2TP Gateway IP Address:	Enter the L2TP Gateway IP address used here.
L2TP Server IP Address:	Enter the L2TP Server IP address used here. This is normally the same as the L2TP Gateway IP address.
User Name:	Enter the L2TP username used here.
Password:	Enter the L2TP password used here.
Verify Password:	Re-enter the L2TP password used here.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Configure your Internet Connection: Static IP Address Connection

After selecting the **Static IP Address** Internet connection method, the following page will appear:

The following parameters can be configured:

IP Address:	Enter the Static IP address provided by the ISP here.
Subnet Mask:	Enter the Subnet Mask provided by the ISP here.
Gateway Address:	Enter the Gateway IP address provided by the ISP here.
Primary DNS Address:	Enter the Primary DNS IP address used here.
Secondary DNS Address:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

Step 4: The Internet Connection Setup Wizard has completed. Click the **Connect** button to save your settings.

Click on the **Prev** button to return to the previous window. Click on the **Next** button to continue to the next step. Click on the **Cancel** button to discard the changes made and return to the Internet home page.

After clicking the **Connect** button to following window will appear. The device will save the settings and return to the main Internet page.

INTERNET - MANUAL INTERNET CONNECTION

On this page the user can configure the Internet Connection settings manually. To access the Manual Internet Connection page, click on the **Manual Internet Connection Setup** button.

MANUAL INTERNET CONNECTION OPTION

If you would like to configure the Internet settings of your new Samsung Router manually, then click on the button below.

[Manual Internet Connection Setup](#)

On this page there are multiple parameters that can be configured regarding the Internet Connection setup. We'll discuss them from top to bottom.

WAN

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

[Save Settings](#)

[Don't Save Settings](#)

At any given point the user can save the configurations done, on this page, by clicking on the **Save Settings** button. If you choose to discard the changes made, then click on the **Don't Save Settings** button.

Internet Connection Type: Static IP

Select Static IP from the drop-down menu if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : ▼

STATIC IP ADDRESS INTERNET CONNECTION TYPE :

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Secondary DNS Server : (optional)

MTU :

MAC Address :

The following parameters can be configured:

IP Address:	Enter the Static IP address provided by the ISP here.
Subnet Mask:	Enter the Subnet Mask provided by the ISP here.
Gateway Address:	Enter the Gateway IP address provided by the ISP here.
Primary DNS Address:	Enter the Primary DNS IP address used here.
Secondary DNS Address:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

Internet Connection Type: Dynamic IP (DHCP)

Select Dynamic IP (DHCP) from the drop-down menu to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : ▼

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Primary DNS Server :

Secondary DNS Server : (optional)

MTU :

MAC Address :

The following parameters can be configured:

Host Name:	The Host Name is optional but may be required by some ISPs. Leave blank if you are not sure.
Primary DNS Server:	Enter the Primary DNS IP address used here.
Secondary DNS Server:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

Internet Connection Type: PPPoE (Username / Password)

Select PPPoE (Username/Password) from the drop-down menu if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPPoE (Username / Password) ▼

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : Always on New Schedule

On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

DNS Mode : Receive DNS from ISP Enter DNS Manually

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1492

MAC Address :

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPPoE usually requires a Dynamic IP configuration.
IP Address:	Enter the PPPoE IP address used here. This option is only available if Static IP is selected.
Username:	Enter the PPPoE account user name used here. This information is given by the ISP.
Password:	Enter the PPPoE account password used here. This information is given by the ISP.
Verify Password:	Re-enter the PPPoE account password used here.
Service Name:	This optional field enables the user to enter a service name to identify this Internet connection here.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the On Demand , or Manual option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
DNS Mode:	This option allow the router to obtain the DNS IP addresses from the ISP, when Receive DNS from ISP is selected, or allows the user to enter DNS IP address manually, when Enter DNS Manually is selected.
Primary DNS Server:	Enter the Primary DNS IP address used here.

This page is a continue from the PPPoE Internet Connection Type:

Secondary DNS Server:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

Internet Connection Type: PPTP (Username / Password)

Select PPTP (Point-to-Point Tunneling Protocol) from the drop-down menu if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPTP (Username / Password) ▼

PPTP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on ▼

On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1400

MAC Address :

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPTP usual requires a Dynamic IP configuration.
PPTP IP Address:	Enter the PPTP IP address used here. This option is only available if Static IP is selected.
PPTP Subnet Mask:	Enter the PPTP Subnet Mask used here.
PPTP Gateway IP Address:	Enter the PPTP Gateway IP address used here.
PPTP Server IP Address:	Enter the PPTP Server IP address used here. This is normally the same a the PPTP Gateway IP address.
Username:	Enter the PPTP username used here.
Password:	Enter the PPTP password used here.
Verify Password:	Re-enter the PPTP password used here.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the On Demand , or Manual option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
Primary DNS Server:	Enter the Primary DNS IP address used here.
Secondary DNS Server:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

This page is a continue from the PPTP Internet Connection Type:

MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

Internet Connection Type: L2TP (Username / Password)

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : L2TP (Username / Password) ▼

L2TP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on ▼

On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1400

MAC Address :

The following parameters can be configured:

Address Mode:	Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usual requires a Dynamic IP configuration.
L2TP IP Address:	Enter the L2TP IP address used here. This option is only available if Static IP is selected.
L2TP Subnet Mask:	Enter the L2TP Subnet Mask used here.
L2TP Gateway IP Address:	Enter the L2TP Gateway IP address used here.
L2TP Server IP Address:	Enter the L2TP Server IP address used here. This is normally the same as the PPTP Gateway IP address.
Username:	Enter the L2TP username used here.
Password:	Enter the L2TP password used here.
Verify Password:	Re-enter the L2TP password used here.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the On Demand , or Manual option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
Primary DNS Server:	Enter the Primary DNS IP address used here.
Secondary DNS Server:	Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

This page is a continue from the L2TP Internet Connection Type:

MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

WIRELESS SETTINGS

On this page the user can configure the Wireless settings for this device. There are 3 ways to configure Wireless using this router. Firstly, the user can choose to make use for the quick and easy Wireless Connection Wizard. Secondly, the user can choose to make use Wi-Fi Protected Setup. Lastly, the user can configure the Wireless settings manually.

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Wireless Settings: Wireless Network Setup Wizard

The Wireless Network Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to configure the wireless settings of this router. It is highly recommended to customized the wireless network settings to fit into your environment and to add higher security.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Connection Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the Samsung Router.

To initiate the Wireless Network Setup Wizard click on the **Wireless Connection Setup Wizard** button.

Step 1: In this step, the user must enter a custom Wireless Network Name or SSID for the frequency band 2.4GHz and 5GHz. Enter the new SSID names in the appropriate spaces provided. Secondly the user can choose between two wireless security wizard configurations. The user can select '**Automatically assign a network key**', by which the router will automatically generate a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods; or the user can select '**Manually assign a network key**', by which the user will be prompt to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

Step 2: This step will only be available if the user selected '**Manually assign a network key**' in the previous step. Here the user can manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. If the user chooses to use the same key for both frequency bands, then select the '**Use the same Wireless Security Password**

on both **2.4GHz and 5GHz band**' option. Un-selecting this option will allow the user to manually enter a pre-shared key for both individual frequency bands. The key entered must be between 8 and 63 characters long.

Remember, this key will be used when wireless clients want to connect to this device. So please remember this key to prevent future troubleshooting.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page.

Click on the **Cancel** button to discard the changes made and return to the main wireless page.

SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Band	: 2.4GHz Band
Wireless Network Name (SSID)	: SWR1100
Security Mode	: Auto (WPA or WPA2) - Personal
Cipher Type	: TKIP and AES
Pre-Shared Key	: c339f2efa7ef638daba073a662236dbc30da0c5d62b9154bcd27a4fa5ffb8f2

Wireless Band	: 5GHz Band
Wireless Network Name (SSID)	: SWR1100_media
Security Mode	: Auto (WPA or WPA2) - Personal
Cipher Type	: TKIP and AES
Pre-Shared Key	: c339f2efa7ef638daba073a662236dbc30da0c5d62b9154bcd27a4fa5ffb8f2

Setup Complete: On this page the user can view the configuration made and verify whether they are correct.

Click on the **Prev** button to return to the previous page.

Click on the **Cancel** button to discard the changes made and return to the main wireless page.

Click on the **Save** button to accept the changes made.

After click the **Save** button the device will save the settings made and return to the main wireless page.

SAVING

The settings are being saved and are taking effect.

Please wait ...

Wireless Settings: Wi-Fi Protected Setup Wizard

If your Wireless Clients support the WPS connection method, this Wi-Fi Protected Setup Wizard can be used to initiate a wireless connection between this device and Wireless clients with a simple click of the WPS button. The Wi-Fi Protected Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to connect wireless clients to this router using the WPS method.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

Add Wireless Device with WPS

To initiate the Wi-Fi Protected Setup Wizard click on the **Add Wireless Device with WPS** button.

STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

Please select one of following configuration methods and click next to continue.

Auto Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

Manual Select this option will display the current wireless settings for you to configure the wireless device manually

Prev Next Cancel Connect

Step 1: In this step the user have two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

STEP 2: CONNECT YOUR WIRELESS DEVICE

There are two ways to add wireless device to your wireless network:
-PIN (Personal Identification Number)
-PBC (Push Button Configuration)

PIN :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Prev Next Cancel Connect

Step 2: After selecting **Auto**, the following page will appear. There are two ways to add a wireless device, that supports WPS. Firstly, there is the **Personal Identification Number (PIN)** method. Using this method will prompt the user to enter a **PIN** code. This PIN code should be identical on the wireless client. Secondly, there is the **Push Button Configuration (PBC)** method. Using this method will allow the wireless client to connect to this device by similarly pressing the PBC button on it.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

STEP 2: CONNECT YOUR WIRELESS DEVICE

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

2.4 Ghz Frequency
SSID: SWR1100
Security Mode: Auto (WPA or WPA2) - Personal
Cipher Type: TKIP and AES
Pre-shared Key: 1234567890

5 Ghz Frequency
SSID: SWR1100_media
Security Mode: Auto (WPA or WPA2) - Personal
Cipher Type: TKIP and AES
Pre-shared Key: 1234567890

Step 2: After selecting **Manual**, the following page will appear. On this page to user can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that can't use the WPS method to connect to this device.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page.

Click on the **Cancel** button to discard the changes made and return to the main wireless page.

Click on the **Wireless Status** button to navigate to the Status > Wireless page to view what wireless client are connected to this device.

Wireless Settings: Manual Wireless Network Setup

The manual wireless network setup option allows user to configure the wireless settings of this device manually. This option is for the more advanced user and includes all parameter that can be configured for wireless connectivity.

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new Samsung Systems Router manually, then click on the Manual Wireless Network Setup button below.

Manual Wireless Connection Setup

To initiate the Manual Wireless Network Setup page, click on the **Manual Wireless Connection Setup** button.

WIRELESS NETWORK

Use this section to configure the wireless settings for your Samsung router. Please note that changes made in this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

On this page the user can configure all the parameters related to the wireless connectivity of this router.

WIRELESS NETWORK SETTINGS

Wireless Band : 2.4GHz Band

Enable Wireless : Always New Schedule

Wireless Network Name : SWR1100 (Also called the SSID)

Enable Auto Channel Selection :

Wireless Channel : 1

Transmission Rate : Best (automatic) (Mbit/s)

Wireless Mode : 802.11 Mixed(n/g/b)

Band Width : 20 MHz

WMM Enable : (Wireless QoS)

Enable Hidden Wireless : (Also called the SSID Broadcast)

The following parameters can be configured:

Wireless Band:	Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 2.4GHz band.
Enable Wireless:	Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always . Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Enable Auto Channel Selection:	The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.
Wireless Channel:	By default the channel is set to 1. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.
Transmission Rate:	Select the transmit rate. It is strongly suggested to select Best (Automatic) for best performance.
Wireless Mode:	Here the user can manually select the preferred frequency band to use for this wireless network.
Band Width:	When using the 802.11n frequency band, the user have an option to choose between a 20MHz or 20/40MHz bandwidth.

WMM Enable:	WMM (Wi-Fi Multimedia) is QoS for your wireless network. Check this box to improve the quality of video and voice applications for your wireless clients. This feature is not available in 802.11n configurations.
Enabled Hidden Wireless:	Check this box if you do not want the SSID of your wireless network to be broadcasted. If the SSID is hidden, the SSID will not be seen by Site Survey utilities, so your wireless clients will have to know the SSID of your router in order to connect to it.

By default the wireless security of this router will be disabled. In this next option the user can enabled or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used. WEP or WPA/WPA2.

WIRELESS SECURITY MODE

Security Mode : ▼

Wireless Security Mode: WEP Wireless Security (basic)

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.

WIRELESS SECURITY MODE

Security Mode : ▼

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

Authentication : ▼
 WEP Encryption : ▼
 Default WEP Key : ▼
 WEP Key : (5 ASCII or 10 HEX)

The following parameters can be configured:

Authentication:	Displays that the authentication method Open System is used.
WEP Encryption:	Here the user can specify to either use a 64Bit or a 128Bit encrypted key.
Default WEP Key:	Here the WEP key number used will be displayed. The Key number used by WEP on this device can only be set to 1.
WEP Key:	Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

Wireless Security Mode: WPA/WPA2 Wireless Security (enhanced)

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option.

WIRELESS SECURITY MODE

Security Mode :

WPA/WPA2

WPA/WPA2 requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

Network Key :
(8~63 ASCII or 64 HEX)

The following parameters can be configured:

Cipher Type:	Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Auto (TKIP/AES) .
PSK/EAP:	WPA supports two authentication frameworks. Pre-Shared Key (PSK) and Extensible Authentication Protocol (EAP). PSK requires only the use of a pass-phrase (Shared Secret) for security. EAP on the other hand requires the installation of a RADIUS Server on the local network.
RADIUS Server IP Address:	When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.
Port:	When the user chooses to use the EAP authentication framework, the RADIUS server's port number can be entered here.
Shared Secret:	Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless client for them to be able to connect to the wireless network successfully.

WPA/WPA2

WPA/WPA2 requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

RADIUS Server IP Address :

Port :

Shared Secret :

The next section will allow the user to configure all the parameters regarding the **5GHz** frequency band.

WIRELESS NETWORK SETTINGS

Wireless Band : 5GHz Band

Enable Wireless : Always New Schedule

Wireless Network Name : SWR1100_media (Also called the SSID)

Enable Auto Channel Selection :

Wireless Channel : 36

Transmission Rate : Best (automatic) (Mbit/s)

Wireless Mode : 802.11 Mixed(a/n)

Band Width : 20/40 MHz(Auto)

WMM Enable : (Wireless QoS)

Enable Hidden Wireless : (Also called the SSID Broadcast)

The following parameters can be configured:

Wireless Band:	Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 5GHz band.
Enable Wireless:	Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always . Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Enable Auto Channel Selection:	The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.
Wireless Channel:	By default the channel is set to 36. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.
Transmission Rate:	Select the transmit rate. It is strongly suggested to select Best (Automatic) for best performance.
Wireless Mode:	Here the user can manually select the preferred frequency band to use for this wireless network.
Band Width:	When using the 802.11n frequency band, the user have an option to choose between a 20MHz or 20/40MHz bandwidth.
WMM Enable:	WMM (Wi-Fi Multimedia) is QoS for your wireless network. Check this box to improve the quality of video and voice applications for your wireless clients. This feature is not available in 802.11n configurations.
Enabled Hidden Wireless:	Check this box if you do not want the SSID of your wireless network to be broadcasted. If the SSID is hidden, the SSID will not be seen by Site Survey utilities, so your wireless clients will have to know the SSID of your router in order to connect to it.

By default the wireless security of this router will be disabled. In this next option the user can enabled or disable wireless security for the frequency band 5GHz. These settings are identical to what we've discussed for the 2.4GHz security earlier.

WIRELESS SECURITY MODE

Security Mode : Disable Wireless Security (not recommended)

Save Settings Don't Save Settings

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

NETWORK SETTINGS

On this page the user can configure the internal network settings of the router and also able to configure the built-in DHCP server to assign IP addresses to computers on the network. The IP address that is configured here is the IP address that is used to access the Web-based management interface. If you change the IP address in this section, you may need to adjust your PC's network settings to access the network again.

NETWORK SETTINGS

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP addresses to computers on your network. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address in this section, you may need to adjust your PC's network settings to access the network again.

Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.

Save Settings Don't Save Settings

In this next section the user can configure the router settings of this device.

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.0.1
 Default Subnet Mask : 255.255.255.0
 Host Name : samsungrouter
 Local Domain Name : (optional)
 Enable DNS Relay :

The following parameters can be configured:

Router IP Address:	Enter the IP address of the router. The default IP address is 192.168.0.1. If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.
Default Subnet Mask:	Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
Host Name:	Enter a Host Name to identify this device.
Local Domain Name:	Enter the Domain name (Optional).
Enable DNS Relay:	Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. This device has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the router. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

At the bottom of the page, click on the **Save Settings** button to accept the changes made. Click on the **Don't Save Settings** button to discard the changes made.

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)

DHCP Lease Time : 10080 (minutes)

The following parameters can be configured:

Enable DHCP Server:	Check this box to enable the DHCP server on your router. Uncheck to disable this function.
DHCP IP Address Range:	Enter the starting and ending IP addresses for the DHCP server's IP assignment.
DHCP Lease Time:	The length of time for the IP address lease. Enter the Lease time in minutes.



Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

In the **DHCP Reservation List** a list of DHCP clients, which MAC address that have been locked to specific IP addresses in the DHCP pool, will be displayed.

DHCP RESERVATIONS LIST

Host Name	IP Address	MAC Address	Expired Time
-----------	------------	-------------	--------------

In the '**Number of Dynamic DHCP Clients**' section, all the active DHCP clients will be displayed.

NUMBER OF DYNAMIC DHCP CLIENTS

Host Name	IP Address	MAC Address	Expired Time
-----------	------------	-------------	--------------

In the **DHCP Reservation** section, the user can configure reserved IP address to selective DHCP clients, by entering their MAC addresses in the list along with the appropriate IP address.

25 - DHCP RESERVATION

Remaining number of rules that can be created: 25

	Computer Name	IP Address	MAC Address	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾

The following parameters can be configured:

Checkbox:	Check this box to enable the reservation.
Computer Name:	Enter the computer name. Alternatively, select a computer that currently has a DHCP lease from the drop down menu and click << to automatically populate the Computer Name, IP Address, and MAC Address fields.
IP Address:	Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.
MAC Address:	Enter the MAC address of the computer or device.

ADVANCED CATEGORY

Samsung Wireless Router
Powered by D-Link

SETUP **ADVANCED** TOOLS STATUS SUPPORT

CY-SWR1100 **VIRTUAL SERVER** HELPFUL HINTS

VIRTUAL SERVER
The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

32 - VIRTUAL SERVERS LIST
Remaining number of rules that can be created: 32

	Name	Application name	Port	Traffic Type	Schedule	Inbound Filter
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol All	Schedule Always	Inbound Filter Allow All
	IP Address	<< Computer Name	Private			
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol All	Schedule Always	Inbound Filter Allow All
	IP Address	<< Computer Name	Private			
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol All	Schedule Always	Inbound Filter Allow All
	IP Address	<< Computer Name	Private			
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol All	Schedule Always	Inbound Filter Allow All
	IP Address	<< Computer Name	Private			

Helpful Hints...

- Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.
- You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.
- Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the [Tools -> Schedules](#) screen and create a new schedule.

In this category the user will be able to configure the more advanced features that can be done by this router. Features like Port Forwarding, Firewall settings, Quality of Service settings and more.

Pages that can be configured in the **Advanced** category are as follows:

Virtual Server: On this page that user can configure Virtual Server policies related to this router.

Port Forwarding: On this page the user will be able to forward a list of ports to an internal IP address.

Application Rules: On this page, the user can create a set of application rules.

QoS: The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

Network Filter: On this page the user can configure network filtering rules.

Access Control: On this page the user can configure access control rules.

Website Filter: On this page the user can configure website and domain filtering rules.

Inbound Filter: On this page the user can configure Inbound Firewall Filtering rules.

Firewall Settings: On this page the user can configure some basic Firewall settings.

Routing: On this page the your can setup multiple routing profiles and rules.

Advanced Wireless: On this page the user can configure more advanced wireless properties.

Guest Zone: On this page the user can create and maintain guest zone for wireless access.

IPv6: On this page the user can configure the IPv6 connectivity of this device.

IPv6 Firewall: On this page the user can configure the IPv6 Firewall properties for this device.

VIRTUAL SERVER

This router can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network). The router's firewall feature filters out unrecognized packets to protect the LAN network so all computers networked with the router are invisible to the outside world. The user can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the router redirects the external service request to the appropriate server within the LAN network. The router is also capable of port-redirection, meaning that incoming traffic to a particular port may be redirected to a different port on the server computer.

VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

On this page, the user can open external access to single ports.

32 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 32

	Name	Application name	Port	Traffic Type	Schedule
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol	Schedule
	IP Address	<< Computer Name	Private	All	Always
					Inbound Filter
					Allow All
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol	Schedule
	IP Address	<< Computer Name	Private	All	Always
					Inbound Filter
					Allow All
<input type="checkbox"/>	<input type="text"/>	<< Application name	Public	Protocol	Schedule
	IP Address	<< Computer Name	Private	All	Always
					Inbound Filter
					Allow All

The following parameters can be configured:

Checkbox:	Check the box on the left side to enable the Virtual Server rule.
Name:	Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.
IP Address:	Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the Computer Name drop-down menu. Select your computer and click <<.
Port (Public/Private):	Enter the port that you want to open next to Public Port and Private Port. The public and private ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.
Traffic Type:	Select TCP, UDP, or All from the Protocol drop-down menu.
Schedule:	Use the drop-down menu to schedule the time that the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

PORT FORWARDING

On this page the user will be able to forward a list of ports to an internal IP address.

PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in the format, Port Ranges (100-150). This option is only applicable to the INTERNET session.

The following section allows the user to configure the port forwarding rules.

32 -- PORT FORWARDING RULES

Remaining number of rules that can be created: 32

			Ports to Open	
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	TCP <input type="text"/>	Schedule Always ▼
	IP Address <input type="text"/>	<< Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	TCP <input type="text"/>	Schedule Always ▼
	IP Address <input type="text"/>	<< Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	TCP <input type="text"/>	Schedule Always ▼
	IP Address <input type="text"/>	<< Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼

The following parameters can be configured:

Checkbox:	Tick the checkbox on the left side to enable the Port Forwarding rule.
Name:	Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.
IP Address:	Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the Computer Name drop-down menu. Select your computer and click <<.
Ports to Open (TCP/UDP):	Enter the external port number in the appropriate space provided. If the port number is TCP then enter the number in the TCP space, and if the port number is UDP then enter it in the UDP space.
Schedule:	Use the drop-down menu to schedule the time that the Port Forwarding rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.
Inbound Filter:	Select the inbound filter rule here. Options to choose from are Allow All , Deny All , and any other custom rule created.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

APPLICATION RULES

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the router. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

APPLICATION RULES

The Application Rules option is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on an outgoing "Trigger" port or port range. Special Application rules apply to all computers on your internal network.

On this page, the user can create a set of application rules.

32 -- APPLICATION RULES

Remaining number of rules that can be created: 32

		Port	Traffic Type	Schedule
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Trigger <input type="text"/> Firewall <input type="text"/>	Protocol All Schedule Always
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Trigger <input type="text"/> Firewall <input type="text"/>	Protocol All Schedule Always
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Trigger <input type="text"/> Firewall <input type="text"/>	Protocol All Schedule Always

The following parameters can be configured:

Checkbox:	Check the box on the left side to enable the Application Rule.
Name:	Enter a name for the rule. You may select a predefined application from the Application drop-down menu and click <<.
Application:	Displays a list of predefined application to use in the rules.
Port (Trigger):	This is the port used to trigger the application. It can be either a single port or a range of ports.
Port (Firewall):	This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.
Protocol:	Select the protocol of the firewall port (TCP, UDP, or All).
Schedule:	The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

QUALITY OF SERVICE (QoS)

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

QOS SETTINGS

QoS rules can be used to control traffic.

Smart QoS improves VoIP voice quality or streaming by ensuring your VoIP or streaming traffic is prioritized over other network traffic, such as FTP or Web.

QOS SETUP

Enable QoS :

Uplink Speed : 2048 kbps <<

Downlink Speed : 8192 kbps <<

Queue Type : Strict Priority Queue Weight Fair Queue

Queue ID	Queue Priority	Queue Weight
1	Highest	<input type="text"/> %
2	Higher	<input type="text"/> %
3	Normal	<input type="text"/> %
4	Best Effort(default)	<input type="text"/> %

The following parameters can be configured:

Enable QoS:	This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.
Uplink Speed:	The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com .
Downlink Speed:	The speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as www.dslreports.com .
Queue Type:	Here the user can specify the queue type used. When choosing the option Strict Priority Queue , the router will apply QoS based on the internal specification for the queue ID's listed. When choosing the option Weight Fair Queue , the router will apply QoS based on the user defined percentage in the Queue Weight column.
Queue ID:	In this column the Queue ID used will be displayed.
Queue Priority:	In this column the Queue Priority used will be displayed.
Queue Weight:	After choosing to use the Weight Fair Queue option, under Queue Type, the user will be able to manual enter the Queue Weight for each individual Queue ID.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

After specifying the QoS framework used, in the QoS setup section, the user can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.

32 -- CLASSIFICATION RULES

Remaining number of rules that can be created:

<input type="checkbox"/>	Name <input type="text"/>	Priority Highest ▼	Protocol <input type="text"/> << ALL ▼
	Local IP Range <input type="text"/> to <input type="text"/>		Application Port <input type="text"/>
	Remote IP Range <input type="text"/> to <input type="text"/>		<< ALL ▼
<input type="checkbox"/>	Name <input type="text"/>	Priority Highest ▼	Protocol <input type="text"/> << ALL ▼
	Local IP Range <input type="text"/> to <input type="text"/>		Application Port <input type="text"/>
	Remote IP Range <input type="text"/> to <input type="text"/>		<< ALL ▼
<input type="checkbox"/>	Name <input type="text"/>	Priority Highest ▼	Protocol <input type="text"/> << ALL ▼
	Local IP Range <input type="text"/> to <input type="text"/>		Application Port <input type="text"/>
	Remote IP Range <input type="text"/> to <input type="text"/>		<< ALL ▼

The following parameters can be configured:

Checkbox:	Tick this option to enable the rule specified.
Name:	Enter a custom name for the rule being created here. This name is used for identification.
Priority:	Select the appropriate priority requirement from the drop-down menu that will be applied to this rule. Option to choose from are Highest , Higher , Normal , and Best Effort .
Protocol:	Select the protocol used for the application for in the drop-down menu and it will automatically place it in the Protocol field.
Local IP Range:	Enter the local IP range used here. This is the IP range of you Local Area Network. The Router's IP cannot be included in this range.
Remote IP Range:	Enter the remote IP range used here. This is the IP range of the public network from the Internet Port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.
Application Port:	Enter the application port number used here.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

NETWORK FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

In the **MAC Filtering Rules** section, the user can create and edit Network filter rules. This maximum amount of rules that can be created are 24 rules.

24 -- MAC FILTERING RULES

Configure MAC Filtering below:

Remaining number of rules that can be created: 24

	MAC Address		DHCP Client List	Schedule
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name	Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name	Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name	Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name	Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name	Always <input type="button" value="New Schedule"/>

The following parameters can be configured:

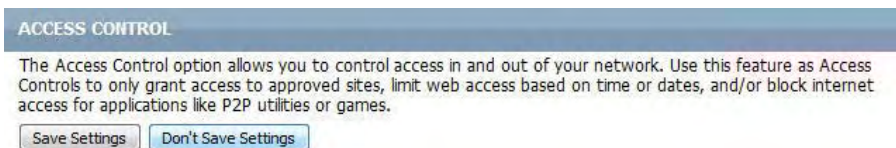
Configure MAC Filtering:	Select Turn MAC Filtering OFF , Turn MAC Filtering ON and ALLOW computers listed to access the network, or Turn MAC Filtering ON and DENY computers listed to access the network from the drop-down menu.
Checkbox:	Check the box on the left side to enable the Network Filter.
MAC Address:	Enter the MAC address you would like to use in this filtering rule.
DHCP Client List:	Select a DHCP client from the Computer Name drop-down menu and click << to copy that MAC Address.
Schedule:	The schedule of time when the Network Filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.



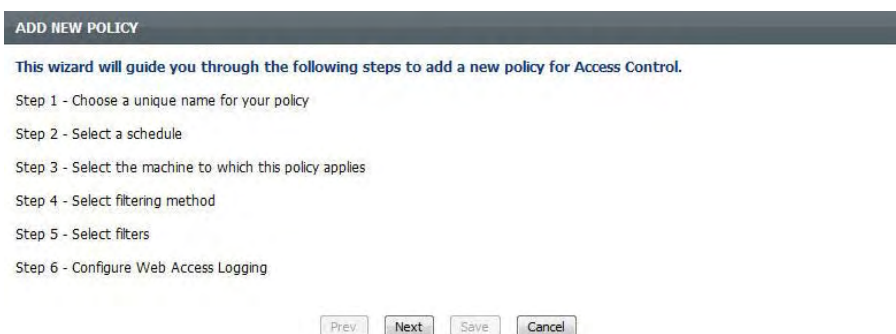
In **Access Control** section the user can enable the access control feature and add new access control policies.



The following parameters can be configured:

Enable Access Control:	Tick this option to enable the Access Control feature.
Add Policy:	Click on this button to add a new Access Control Policy.

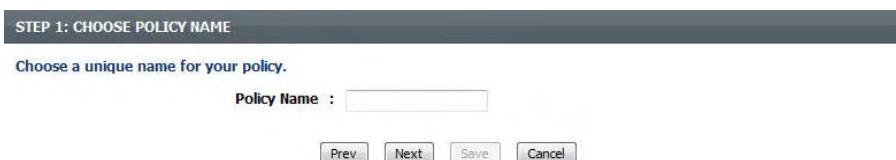
After clicking on the **Add Policy** button, the add policy wizard will guide you through the step-by-step process in adding a new policy. The first window explains the process.



Click on the **Next** button to continue to the next window.

Click on the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 1: In the first step, the user can enter the policy name used.



The following parameters can be configured:

Policy Name:	Enter the new policy name used for this rule here.
---------------------	--

Click on the **Prev** button to return to the previous window.

Click on the **Next** button to continue to the next window.

Click on the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 2: In the second step, the user can configure the schedule settings for this rule.

STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

always ▾

Details : always

Prev Next Save Cancel

The following parameters can be configured:

Details:	Select the appropriate predefined schedule rule to apply to this rule from the drop-down menu.
-----------------	--

Click on the **Prev** button to return to the previous window.

Click on the **Next** button to continue to the next window.

Click on the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 3: In the third step, the user can configure the address type and IP address of the machines used in this rule.

STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy.



Address Type : IP MAC Other Machines

IP Address : 192.168.0.150 << Computer Name ▾

Machine Address : << Computer Name ▾



Clone Your PC's MAC Address

Update Cancel

Machine		
192.168.0.150		

Prev Next Save Cancel

The following parameters can be configured:

Address Type:	Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy.
IP Address:	After selecting the IP address type, the user can enter the IP address of the machines used in this rule here. Alternatively, the user can select a Computer from the Computer Name list.
Machine Address:	After selecting the MAC address type, the user can enter the MAC address of the machine used in this rule here. Alternatively, the user can select a Computer from the Computer Name list.
Add:	Click on this button to add the machine to the list.
Update:	After clicking the  option, the user will be able to update the machine information.
Delete:	If the user chooses to remove a machine from the list, click on the  icon.

Click on the **Prev** button to return to the previous window.

Click on the **Next** button to continue to the next window.

Click on the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 4: In the fourth step, the user can select the filtering method used for this rule.

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method : Log Web Access Only Block All Access Block Some Access

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method : Log Web Access Only Block All Access Block Some Access

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method : Log Web Access Only Block All Access Block Some Access

Apply Web Filter :

Apply Advanced Port Filters :

The following parameters can be configured:



Method:	Here the user can select the filtering method used. Options to choose from are ' Log Web Access Only ', ' Block All Access ', and ' Block Some Access '.
Apply Web Filter:	After selecting the ' Block Some Access ' option, the user will be able to select this option. Selecting this option will allow the web filter access control feature to be applied to this rule.
Apply Advance Port Filters:	After selecting the ' Block Some Access ' option, the user will be able to select this option. Selecting this option will allow the advanced port filters access control feature to be applied to this rule.

Click on the **Prev** button to return to the previous window.



Click on the **Next** button to continue to the next window.

Click on the **Cancel** button to discard the changes made and return to the main Access Control window.

Click on the **Save** button to accept the changes made and return to the main Access Control window.

In the Policy Table section a list on access control rules will be displayed. To edit a specific rule, click on the  icon. To remove a specific rule, click on the  icon.

POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule		
<input checked="" type="checkbox"/>	policyname	192.168.0.150	Log Web Access Only	Yes	always		

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

WEBSITE FILTER

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network.

WEBSITE FILTER

The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network.

Website Filter is used to allow or deny computers on your network from accessing specific web sites by keywords or specific Domain Names. Select '**ALLOW computers access to ONLY these sites**' in order only allow computers on your network to access the specified URLs and Domain Names. '**DENY computers access to ONLY these sites**' in order deny computers on your network to access the specified URLs and Domain Names.

40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites ▼

Website URL/Domain	

The following parameters can be configured:

Website URL/Domain:	Enter the URL or Domain name that you want to allow or block here. An example of an URL is: http://www.facebook.com/ An example of a domain name is: facebook.com
----------------------------	---

Click on the **Clear the list below...** button to remove all the entries from the spaces in the list.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features. The user can add new Inbound filter rule in the next section.

ADD INBOUND FILTER RULE



Name :

Action : **Allow** ▼





Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255

The following parameters can be configured:

Name:	The user can enter a custom name for the inbound filter rule here.
Action:	Select an action that will take place when this rule is initiated. Options to choose from are Allow and Deny .
Enable:	Tick this option to enable the specified IP range for this rule.
Remote IP Start:	Enter the remote starting IP address here in the range.
Remote IP End:	Enter the remote ending IP address here in the range.
Add:	Click this button to add the new inbound filter rule.
Cancel:	Click this button to discard the new inbound filter rule.

In the **Inbound Filter List** section, the user can view a list of the inbound filter rules already created. To edit a specific rule, click on the appropriate  icon. To delete a specific rule, click on the  icon.

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range		
rule1	allow	192.168.69.1-192.168.69.254		

FIREWALL SETTINGS

A firewall protects your network from the outside world. The router offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

FIREWALL & DMZ SETTINGS

Firewall rules can be used to allow or deny traffic passing through the router. You can specify a single port by utilizing the input box at the top or a range of ports by utilizing both input boxes.

DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

Save Settings Don't Save Settings

Firewall rules can be used to allow or deny traffic passing through the router. You can specify a single port by utilizing the input box at the top or a range of ports by utilizing both input boxes. DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

FIREWALL SETTINGS

Enable SPI :

The following parameters can be configured:

Enable SPI:	Check the Enable SPI box to enable the SPI (Stateful Packet Inspection, also known as dynamic packet filtering) feature. Enabling SPI helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.
--------------------	--

In the **DMZ Host** section, the user will be able to configure the DMZ settings for this router.

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ :

DMZ IP Address : <<

Computer Name

Save Settings Don't Save Settings

The following parameters can be configured:

Enable DMZ:	Tick this option to enable the DMZ feature.
DMZ IP Address:	Enter the IP address of the computer on the LAN that you want to have unrestricted Internet communication in the DMZ IP address field. To specify an existing DHCP client, use the Computer Name drop-down to select the computer that you want to make a DMZ host. If selecting a computer that is a DHCP client, be sure to make a static reservation in the Setup > Network Settings page so that the IP address of the DMZ machine does not change.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

ROUTING

The Routing option is an advanced method of customizing specific routes of data through your network.

ROUTING

The Routing option allows you to define static routes to specific destinations.

In the **Static Routing** section, the user can configure routing rules used by this router. The maximum amount of rules that can be configured is 32.

32 -- STATIC ROUTING

Remaining number of rules that can be created: **32**

	Interface	Destination	Subnet Mask	Gateway
<input type="checkbox"/>	WAN (192.168.69.56) ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	WAN (192.168.69.56) ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	WAN (192.168.69.56) ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	WAN (192.168.69.56) ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	WAN (192.168.69.56) ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following parameters can be configured:

Checkbox:	To enable a route, check the box that is on the left side of the route.
Interface:	Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the Router.
Destination:	Enter the IP address of the packets that will take this route.
Subnet Mask:	Enter the subnet mask to specify the subnet of the IP packets that will take this route.
Gateway:	Enter the next hop that will be taken if this route is used.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

ADVANCED WIRELESS

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

Save Settings Don't Save Settings

In the next section, the user can configure the more advanced wireless settings for the **2.4GHz frequency** band.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band

Transmit Power : 100%

Beacon interval : 100 (msec, range: 20~1000, default: 100)

RTS Threshold : 2346 (range: 256~2346, default: 2346)

Fragmentation : 2346 (range: 1500~2346, default: 2346, even number only)

DTIM interval : 1 (range: 1~255, default: 1)

Preamble Type : Short Preamble Long Preamble

Short Guard Interval :

The following parameters can be configured:

Wireless Band:	Here the user can view the wireless frequency band being configured. In the case 2.4GHz .
Transmit Power:	This option sets the transmit power of the antennas.
Beacon Interval:	Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.
RTS Threshold:	Here the user can enter the RTS threshold value used. This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.
Fragmentation:	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
DTIM Interval:	Here the user can enter the DTIM Interval value. Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default settings is 1.
Preamble Type:	Use the radio buttons to specify whether the Router should use the Short Preamble or Long Preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters.
Short Guard Interval:	Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

In the next section, the user can configure the more advanced wireless settings for the **5GHz frequency** band.

ADVANCED WIRELESS SETTINGS

Wireless Band : 5GHz Band

Transmit Power : 100% ▾

Beacon interval : 100 (msec, range: 20~1000, default: 100)

RTS Threshold : 2346 (range: 256~2346, default: 2346)

Fragmentation : 2346 (range: 1500~2346, default: 2346, even number only)

DTIM interval : 1 (range: 1~255, default: 1)

Preamble Type : Short Preamble Long Preamble

Short Guard Interval :

The following parameters can be configured:

Wireless Band:	Here the user can view the wireless frequency band being configured. In the case 5GHz .
Transmit Power:	This option sets the transmit power of the antennas.
Beacon Interval:	Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.
RTS Threshold:	Here the user can enter the RTS threshold value used. This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.
Fragmentation:	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
DTIM Interval:	Here the user can enter the DTIM Interval value. Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default settings is 1.
Preamble Type:	Use the radio buttons to specify whether the Router should use the Short Preamble or Long Preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters.
Short Guard Interval:	Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on “Don't Save Settings” button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

In the Wi-Fi Protected Setup section, the user can enable the WPS feature of this router.

WI-FI PROTECTED SETUP

Enable :

WiFi Protected Setup : Enabled / Configured

The following parameters can be configured:

Enable:	Tick this option to enable the Wi-Fi Protected Setup feature.
Wi-Fi Protected Setup:	This parameter displays the WPS setup status.
Reset to Unconfigured:	Click this button disable the WPS feature used on this router.

In the **PIN Settings** section, the user not only will be able to view the PIN code, but will also be able to reset the PIN to default or to generate a new PIN code. A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

PIN SETTINGS

PIN : 12345670

The following parameters can be configured:

PIN:	Shows the current value of the router's PIN.
Reset PIN to Default:	Click this button to restore the default PIN of the router.
Generate New PIN:	Click this button to create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.

ADD WIRELESS STATION

Click the **Connect your Wireless Device** button to start Wireless Connection Setup Wizard. This wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

ADVANCED NETWORK SETTINGS

This section contains settings which can change the way the router handles certain types of traffic. We recommend that you not change any of these settings unless you are already familiar with them or have been instructed to change them by one of our support personnel.

ADVANCED NETWORK SETTINGS

These options are for users that wish to change the LAN settings. We do not recommend changing these settings from factory default. Changing these settings may affect the behavior of your network.

Save Settings Don't Save Settings

UPnP:

UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The device is a UPnP enabled router, meaning it will work with other UPnP devices/software. If you do not want to use the UPnP functionality, it can be disabled by selecting "Disabled".

UPNP

Universal Plug and Play(UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP :

The following parameters can be configured:

Enable UPnP:	Tick this option to enable the UPnP feature of the router.
---------------------	--

WAN Ping:

When you Enable WAN Ping response, you are causing the public WAN (Wide Area Network) IP address on the device to respond to ping commands sent by Internet users. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

WAN PING

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Response :

The following parameters can be configured:

Enable WAN Ping:	Tick this option to enable the WAN Ping Response option of the router.
-------------------------	--

WAN Port Speed:

This allows you to select the speed of the WAN interface of the router: Choose 100Mbps, 10Mbps, or 10/100Mbps Auto.

WAN PORT SPEED

WAN Port Speed : Auto 10/100/1000Mbps ▼

The following parameters can be configured:

WAN Port Speed:	You may set the port speed of the Internet port to 10Mbps, 100Mbps, or auto. Some older cable or DSL modems may require you to set the port speed to 10Mbps.
------------------------	--

Multicast Streams:

This section enables the user to allow Multicast traffic to pass from the Internet to your network more efficiently.

MULTICAST STREAMS

Enable Multicast Streams :

Wireless Enhance Mode :

Save Settings

Don't Save Settings

The following parameters can be configured:

Enable Multicast Streams:	Enable this option if you are receiving video on demand type of service from the Internet. The router uses the IGMP protocol to support efficient multicasting transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.
Wireless Enhance Mode:	Check the Wireless Enhance Mode box to enable the router to forward all multicast streams from the Internet to the wireless station using a unicast stream. This feature helps improve the quality of multimedia applications for wireless users.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

GUEST ZONE

On this page, the user will be able to configure the Guest Zone, settings. The guest zone provide a separate network zone for guest to access Internet.

GUEST ZONE SELECTION

Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.

In the Guest Zone section below, the user will be able to enable the routing function between guest zones.

GUEST ZONE

Enable Routing Between Zones :

The following parameters can be configured:

Enable Routing:	Tick this option to enable routing between guest zones.
------------------------	---

In the following section, the user will be able to configure the Guest Zone Wireless Network settings used by the **2.4GHz** frequency band.

SESSION 2.4 GHZ

Enable Guest Zone : Always

Wireless Band : 2.4GHz Band

Wireless Network Name : SWR1100+ (Also called the SSID)

Security Mode : Disable Wireless Security (not recommended)

The following parameters can be configured:

Enable Guest Zone:	Tick this option to enable the Guest Zone feature for the frequency band 2.4GHz. Use the drop-down menu to schedule the time that the Firewall rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.
Wireless Band:	Displays the frequency band used.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Security Mode:	The security mode enables the user to configure wireless security for this wireless guest zone. For more information about wireless security, refer to the Wireless Settings page.

In the following section, the user will be able to configure the Guest Zone Wireless Network settings used by the **5GHz** frequency band.

SESSION 5 GHZ

Enable Guest Zone : Always New Schedule

Wireless Band : 5GHz Band

Wireless Network Name : SWR1100_media+ (Also called the SSID)

Security Mode : Disable Wireless Security (not recommended)

Save Settings
Don't Save Settings

The following parameters can be configured:

Enable Guest Zone:	Tick this option to enable the Guest Zone feature for the frequency band 5GHz. Use the drop-down menu to schedule the time that the Firewall rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.
Wireless Band:	Displays the frequency band used.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Security Mode:	The security mode enables the user to configure wireless security for this wireless guest zone. For more information about wireless security, refer to the Wireless Settings page.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6

On this page the user can configure the mode that the Router will use to access an IPv6 Internet connection.

IPv6

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider.

There are several connection types to choose from: Link-local, Static IPv6, DHCPv6, Stateless Auto-Configuration, PPPoE, IPv6 over IPv4 Tunnel and 6to4. If you are unsure of your connection method, please contact your IPv6 ISP.



Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

IPv6 Connection Type: Static IPv6

In the following section we'll discuss the parameters that can be configured when setting up an Static IPv6 connection. This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all this information.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

WAN IPv6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

IPv6 Address :
 Subnet Prefix Length :
 Default Gateway :
 Primary DNS Server :
 Secondary DNS Server :

The following parameters can be configured:

IPv6 Address:	Enter the WAN IPv6 address for the router here.
Subnet Prefix Length:	Enter the WAN subnet prefix length value used here.
Default Gateway:	Enter the WAN default gateway IPv6 address used here.
Primary DNS Server:	Enter the WAN primary DNS Server address used here.
Secondary DNS Server:	Enter the WAN secondary DNS Server address used here.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64
 LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

LAN IPv6 Address:	Enter the LAN (local) IPv6 address for the router here.
Link-Local Address:	Displays the Router's LAN Link-Local Address here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

Save Settings

Don't Save Settings

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : :00 3

IPv6 Address Range (End) : :00 16

IPv6 Address Lifetime : (minutes)

Save Settings

Don't Save Settings

The following parameters can be configured:

Enable Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: Auto-Configuration (Stateless/DHCPv6)

In the following section we'll discuss the parameters that can be configured when setting up an Auto-Configuration (Stateless/DHCPv6) connection. This is a method of connection where the ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the IPv6 Internet.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

IPv6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

Obtain IPv6 DNS Servers automatically

Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

The following parameters can be configured:

Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

Enable DHCP-PD :

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

Enable DHCP PD:	Select this option to enable DHCP PD.
LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

Save Settings

Don't Save Settings

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : ::00 3

IPv6 Address Range (End) : ::00 16

IPv6 Address Lifetime : (minutes)

Save Settings

Don't Save Settings

The following parameters can be configured:

Enable Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: PPPoE

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection to IPv6 Internet. DSL providers typically use this option. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the IPv6 Internet. The supported authentication protocols are PAP and CHAP.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

PPPoE Session : Share with IPv4 Create a new one

Username :

Password :

Verify Password :

Service Name : (optional)

MTU : (bytes)

The following parameters can be configured:

PPPoE Session:	Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.
Username:	Enter the PPPoE username used here. This information is obtainable from the ISP.
Password:	Enter the PPPoE password used here. This information is obtainable from the ISP.
Verify Password:	Re-enter the PPPoE password used here.
Service Name:	Enter the service name for this connection here. This option is optional.
MTU:	Enter the MTU value used here. The default value is 1492.

IPv6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

Obtain IPv6 DNS Servers automatically

Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

The following parameters can be configured:

Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

Enable DHCP-PD :

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

Enable DHCP PD:	Select this option to enable DHCP PD.
LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : ::00 3

IPv6 Address Range (End) : ::00 16

IPv6 Address Lifetime : (minutes)

The following parameters can be configured:

Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: IPv6 in IPv4 Tunnel

In section to the user can configure the IPv6 connection to run in IPv4 Tunnel mode. IPv6 over IPv4 tunneling encapsulates IPv6 packets in IPv4 packets so that IPv6 packets can be sent over an IPv4 infrastructure.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

IPv6 OVER IPv4 TUNNEL SETTINGS

Enter the IPv6 over IPv4 Tunnel information provided by your Tunnel Broker.

Remote IPv4 Address :
 Remote IPv6 Address :
 Local IPv4 Address :
 Local IPv6 Address :
 Subnet Prefix Length :

The following parameters can be configured:

Remote IPv4 Address:	Enter the remote IPv4 address used here.
Remote IPv6 Address:	Enter the remote IPv6 address used here.
Local IPv4 Address:	Enter the local IPv4 address used here.
Local IPv6 Address:	Enter the local IPv6 address used here.
Subnet Prefix Length:	Enter the Subnet prefix length value used here.

IPv6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

Obtain IPv6 DNS Servers automatically
 Use the following IPv6 DNS Servers
 Primary DNS Server :
 Secondary DNS Server :

The following parameters can be configured:

Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

LAN IPv6 Address : /64
 LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local:	Displays the LAN IPv6 Link-Local address used here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

Save Settings

Don't Save Settings

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : ::00 3

IPv6 Address Range (End) : ::00 16

IPv6 Address Lifetime : (minutes)

Save Settings

Don't Save Settings

The following parameters can be configured:

Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: 6to4

In this section the user can configure the IPv6 6to4 connection settings. 6to4 is an IPv6 address assignment and automatic tunneling technology that used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

WAN IPv6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

6to4 Address :

6to4 Relay :

Primary DNS Server :

Secondary DNS Server :

The following parameters can be configured:

6to4 Address:	Here the 6to4 configured address will be displayed.
6to4 Relay:	Enter the 6to4 relay address used here.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

Save Settings

Don't Save Settings

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : ::00 3

IPv6 Address Range (End) : ::00 16

IPv6 Address Lifetime : (minutes)

Save Settings

Don't Save Settings

The following parameters can be configured:

Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: 6rd

In this section the user can configure the IPv6 6rd connection settings.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

WAN IPv6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

6rd IPv6 Prefix : /

IPv4 Address : Mask Length :

Assigned IPv6 Prefix :

6rd Border Relay IPv4 Address :

Primary DNS Server :

Secondary DNS Server :

The following parameters can be configured:

6rd IPv6 Prefix:	Enter the 6rd IPv6 address and prefix value used here.
IPv4 Address:	Enter the IPv4 address used here.
Mask Length:	Enter the IPv4 mask length used here.
Assigned IPv6 Prefix:	Displays the IPv6 assigned prefix value here.
6rd Border Relay IPv4 Address:	Enter the 6rd border relay IPv4 address used here.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address uses here.

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : (minutes)

Save Settings

Don't Save Settings

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful(DHCPv6)

IPv6 Address Range (Start) : ::00 3

IPv6 Address Range (End) : ::00 16

IPv6 Address Lifetime : (minutes)

Save Settings

Don't Save Settings

The following parameters can be configured:

Auto-Configuration:	The user can tick this option to enable the auto-configuration feature.
Auto-Configuration Type:	The user can select the auto-configuration type used here. Options to choose from are Stateless or Stateful (DHCPv6) .
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to Stateless . Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to Stateful . Enter the start IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to Stateful . Enter the end IPv6 Address for the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to Stateful . Enter the IPv6 Address Lifetime (in minutes).

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: Link-Local Only

The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is :

The following parameters can be configured:

My IPv6 Connection is:	Select the appropriate IPv6 Connection Type used for this configuration here.
-------------------------------	---

LAN IPv6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface.

LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64

The following parameters can be configured:

LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.
-------------------------------------	---

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

IPv6 FIREWALL

On this page the user can configure the IPv6 firewall settings. The firewall settings section is an advance feature that is used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

IPv6 FIREWALL

The firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

Save Settings Don't Save Settings

In the IPv6 Firewall rules section the user can create, enable and disable IPv6 firewall rules used by this device.

32 -- IPv6 FIREWALL RULES

Remaining number of rules that can be created: 32

Configure IPv6 Filtering below:

Turn IPv6 Filtering OFF

<input type="checkbox"/>	Name	Schedule	
		Always	
Source	Interface	IP Address Range	Protocol
		-	ALL
Dest	Interface	IP Address Range	Port Range
		-	
<input type="checkbox"/>	Name	Schedule	
		Always	
Source	Interface	IP Address Range	Protocol
		-	ALL
Dest	Interface	IP Address Range	Port Range
		-	

Save Settings Don't Save Settings

The following parameters can be configured:

Configure IPv6 Filtering:	This option defines the behaviour of all the IPv6 firewall rules created. Option to choose from are 'Turn IPv6 Filtering OFF' , 'Turn IPv6 Filtering ON and ALLOW rules listed' , and 'Turn IPv6 Filtering ON and DENY rules listed' . Select the appropriate option used here.
Checkbox:	Tick this option to used the firewall rules created.
Name:	Enter a custom firewall rule name here. This name is used for identification.
Source Interface:	Select the appropriate source interface used here.
Destination Interface:	Select the appropriate destination interface used here.
Schedule:	Select a time schedule that will be applied to this rules here.
IP Address Range:	Enter the IPv6 address range used here.
Protocol:	Select the protocol used for this rule here. Options to choose from are ALL , TCP , UDP , and ICMP .
Port Range:	Enter the port range used for this rule here.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

TOOLS CATEGORY

Samsung Wireless Router
Powered by **D-Link**

SETUP ADVANCED **TOOLS** STATUS SUPPORT

CY-SWR1100 **ADMINISTRATOR SETTINGS** **HELPFUL HINTS**

ADMIN
The 'admin' account can access the management interface. The admin has read/write access and can change password.
By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD
Please enter the same password into both boxes, for confirmation.
Password :
Verify Password :

ADMINISTRATION
Enable Graphical Authentication :
Enable Remote Management :
Remote Admin Port :
Remote Admin Inbound Filter :
Details :

Helpful Hints...
• For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the router in case they are forgotten.

COPYRIGHT © 2010 SAMSUNG ELECTRONICS CO.,LTD.
ALL RIGHTS RESERVED.

SAMSUNG

In this category the user will be able to configure features that are related to the router itself. Features like the time settings, login accounts, firmware update and more.

Pages that can be configured in the **Tools** category are as follows:

Administration: On this page the user can configure a new password as well as remote administration settings for this device.

Time: On this page the user can configure the time and date settings for this router.

System Log: On this page the user can view and configure the system log.

Email Settings: On this page the user can configure the email settings for this router.

System: On this page the user can reboot, reset, backup and restore this router.

Firmware: On this page the user can perform a firmware upgrade on this router. Also uploadable from this page is the language packs.

Dynamic DNS: On this page the user can configure the DDNS settings for this router.

System Check: On this page the user can perform a system check (using Ping) for this router.

Schedules: On this page the user can create and maintain time schedules for this router.

ADMIN

This page will allow you to change the Administrator password and configure the authentication settings. This window also allows you to enable Remote Management, via the Internet.

ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface. The admin has read/write access and can change password.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

In the **Admin Password** section, the user can change the login password used for this device.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :

Verify Password :

The following parameters can be configured:

Password:	Enter the new login password used here.
Verify Password:	Re-enter the new login password here.

ADMINISTRATION

Enable Graphical Authentication :


Enable Remote Management :

Remote Admin Port :

Remote Admin Inbound Filter :

Details :

The following parameters can be configured:

Enable Graphical Authentication:	<p>Tick this option to enable the graphical image confirmation when the user login to the web configuration. Example:</p> 
Enable Remote Management:	Tick this option to enable remote management. This option will enable the router to be accessible from the Internet port.
Remote Admin Port:	Enter the remote administration port number used here. Sometimes services like an internal webserver will occupy the port number 80. In this option the user can change the remote administration port to 8080 for example.
Remote Admin Inbound Filter:	Select the appropriate remote admin inbound filter behaviour here. Options to choose from are Allow All and Deny All .
Details:	Enter the remote admin inbound filter detail description used here.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

TIME

The Time window allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

TIME AND DATE CONFIGURATION

Time : 2010/12/16 11:20:21

Time Zone : (GMT+08:00) Taipei

Enable Daylight Saving :

The following parameters can be configured:

Time:	Here will be displayed the current time configuration running on this device.
Time Zone:	Select the appropriate time zone used on this device here.
Enable Daylight Saving:	Check this box if the country your are located in uses Daylight Saving time. Enter a start date and an end date for daylight saving time.
Sync. your computer's time settings:	Click this button to synchronize the router's system clock to the management computer's time settings.

AUTOMATIC TIME AND DATE CONFIGURATION

Automatically synchronize with Internet time server

NTP Server Used :

The following parameters can be configured:

Automatically synchro- nize:	NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Tick this option to enable automatic time and date synchronizing.
NTP Server Used:	Select the appropriate time server used here. The interval at which the router will communicate with the NTP server is set to 7 days.
Update Now:	After selecting the appropriate time server and enabling the automatic synchronization option, click on this button to update the current time and date of the router.

SET THE TIME AND DATE MANUALLY

Year
 Month
 Day

Hour
 Minute
 Second

The following parameters can be configured:

Set Manually:	Here the user can manually configure the date and time used by this device. Options to configure are Year, Month, Day, Hour, Minute, and Second.
----------------------	---

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

SYSLOG

The Syslog options allow you to send log information to a System Log Server.

SYSLOG

The SysLog options allow you to send log information to a Syslog Server.

SYSLOG SETTINGS

Enable Logging To SysLog Server :

Syslog Server IP Address : << Computer Name ▾

The following parameters can be configured:

Enable Logging:	Tick this option to enable the Syslog feature.
Syslog Server IP Address:	Enter the Syslog Server IP address used here.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

EMAIL SETTINGS

The Email feature can be used to send the system log files and router alert messages to your email address.

EMAIL SETTINGS

The Email feature can be used to send the system log files, router alert messages.

EMAIL SETTINGS

From Email Address :

To Email Address :

Email Subject :

SMTP Server Address :

Account Name :

Password :

Verify Password :

The following parameters can be configured:

From Email Address:	This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.
To Email Address:	Enter the email address where you want the email sent.
Email Subject:	Enter the text that you want to appear in the subject line of the e-mail that is sent.
SMTP Server Address:	Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.
Account Name:	Enter your account for sending email.
Password:	Enter the password associated with the account.
Verify Password:	Re-enter the password associated with the account here.
Send Mail Now:	Click this button to send a test email from the Router to verify that the email settings have been configured correctly.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

SYSTEM

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

SAVE AND RESTORE SETTINGS

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings.

SAVE AND RESTORE SETTINGS

Save Settings To Local Hard Drive :

Load Settings From Local Hard Drive :

Restore To Factory Default Settings :

Reboot The Device :

Clear Language Pack :

The following parameters can be configured:

Save Settings To Local Hard Drive:	Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. A file dialog will appear, allowing you to select a location and file name for the settings.
Load Settings From Local Hard Drive:	Use this option to load previously saved router configuration settings. First, use the Browse option to find a previously saved file of configuration settings. Then, click the Upload Settings button below to transfer those settings to the router.
Restore To Factory Default Settings:	This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.
Reboot The Device:	Click to reboot the router.
Clear Language Pack:	If you previously installed a language pack and want to revert all the menus on the Router interface back to the default language settings, click the Clear button.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

FIRMWARE

Use the Firmware window to upgrade the firmware of the Router and install language packs. If you plan to install new firmware, make sure the firmware you want to use is on the local hard drive of the computer. If you want to install a new language pack, make sure that you have the language pack available. Please check the support site for firmware updates. You can download firmware upgrades to your hard drive from the support site.

FIRMWARE UPDATE

There may be new firmware for your router to improve functionality and performance.

[Click here to check for an upgrade on our support site.](#)

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the router. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

In the **Firmware Information** section the user can view the **Current Firmware Version** number running on this device, the **Current Firmware Date** of this same firmware version running on this device, and a button to click that will **Check Online Now for Latest Firmware Version**.

FIRMWARE INFORMATION

Current Firmware Version : 1.00

Current Firmware Date : Fri 10 Dec 2010

Check Online Now for Latest :
Firmware Version

In the **Firmware Upgrade** section the user can physically upgrade the firmware of this device clicking on the **Browse** button and navigating to the firmware file, saved on the local hard drive. After locating the file, click on the **Upload** button to initiate the firmware upgrade.



Note: Some firmware upgrades will reset the configuration, of the device, to factory defaults. Be sure to save the current configuration first before any firmware update.



Note: Always update the firmware of this device using the **wired** connection. Never upgrade the firmware using a wireless connection.

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

In the **Language Pack Upgrade** section, the user can change the router's language pack by clicking on the **Browse** button and navigating to the language pack, downloaded to the computer. After navigating to the language pack file, click on the **Upload** button to initiate the language pack upload and configuration.

LANGUAGE PACK UPGRADE

Upload :

Always keep a close lookout on the local vendor's website for new firmware upgrades and language packs.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

DYNAMIC DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your host name to connect to your game server no matter what your IP address is.

[Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.](http://www.DLinkDDNS.com)

DYNAMIC DNS SETTINGS

Enable DDNS :

Server Address :

Host Name :

User Account :

Password :

The following parameters can be configured:

Enable DDNS:	Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.
Server Address:	Choose your DDNS provider from the drop down menu.
Host Name:	Enter the Host Name that you registered with your DDNS service provider.
User Account:	Enter the Username for your DDNS account.
Password:	Enter the Password for your DDNS account.
DDNS Account Testing:	Click this button to verify that the DDNS account user name and password have been entered correctly.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

SYSTEM CHECK

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host.

PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

In the **Ping Test** section the user can test the Internet connectivity by entering in a **host name** or the **IP address** that you want to ping (Packet Internet Groper) and click on the **Ping** button. The status of your Ping attempt will be displayed in the **Ping Result** box.

PING TEST

Host Name or IP Address :

In the **IPv6 Ping Test** section the user can test the Internet connectivity by entering in a **host name** or the **IPv6 address** that you want to ping (Packet Internet Groper) and click on the **Ping** button. The status of your Ping attempt will be displayed in the **Ping Result** box.

IPV6 PING TEST

Host Name or IPv6 Address :

In the **Ping Result** section the results of the attempted ping will be displayed.

PING RESULT

Enter a host name or IP address above and click 'Ping'

PING RESULT

No response from 192.168.69.2

PING RESULT

192.168.69.1 is alive!

PING RESULT

google.com is alive!

SCHEDULES

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

SCHEDULES

The Schedule configuration option is used to manage schedule rules for "WAN", "Wireless", "Virtual Server", "Port Forwarding", "Applications", "Network Filter", "Website Filter" and "Firewall".

10 -- ADD SCHEDULE RULE

Name :

Day(s) : All Week Select Day(s)
 Sun Mon Tue Wed Thu Fri Sat

All Day - 24 hrs :

Start Time : 0 : 0 AM (hour:minute, 12 hour time)



End Time : 11 : 59 PM (hour:minute, 12 hour time)

The following parameters can be configured:





Name:	Enter the custom name for the new schedule rule here. This name is used for identification.
Day(s):	To use every day in the week for this rule, select the All Week option. To use only selected days for this rule, select the Select Day(s) option and tick the appropriate days used for this rule.
All Day - 24 hrs:	To enable this rule to run 24 hours instead of only a certain part of the day, tick this option.
Start Time:	If the All Day option is not selected, the user can enter the starting time here.
End Time:	If the All Day option is not selected, the user can enter the ending time here.

Click on the **Add** button to add this new rule to the schedule rules list.

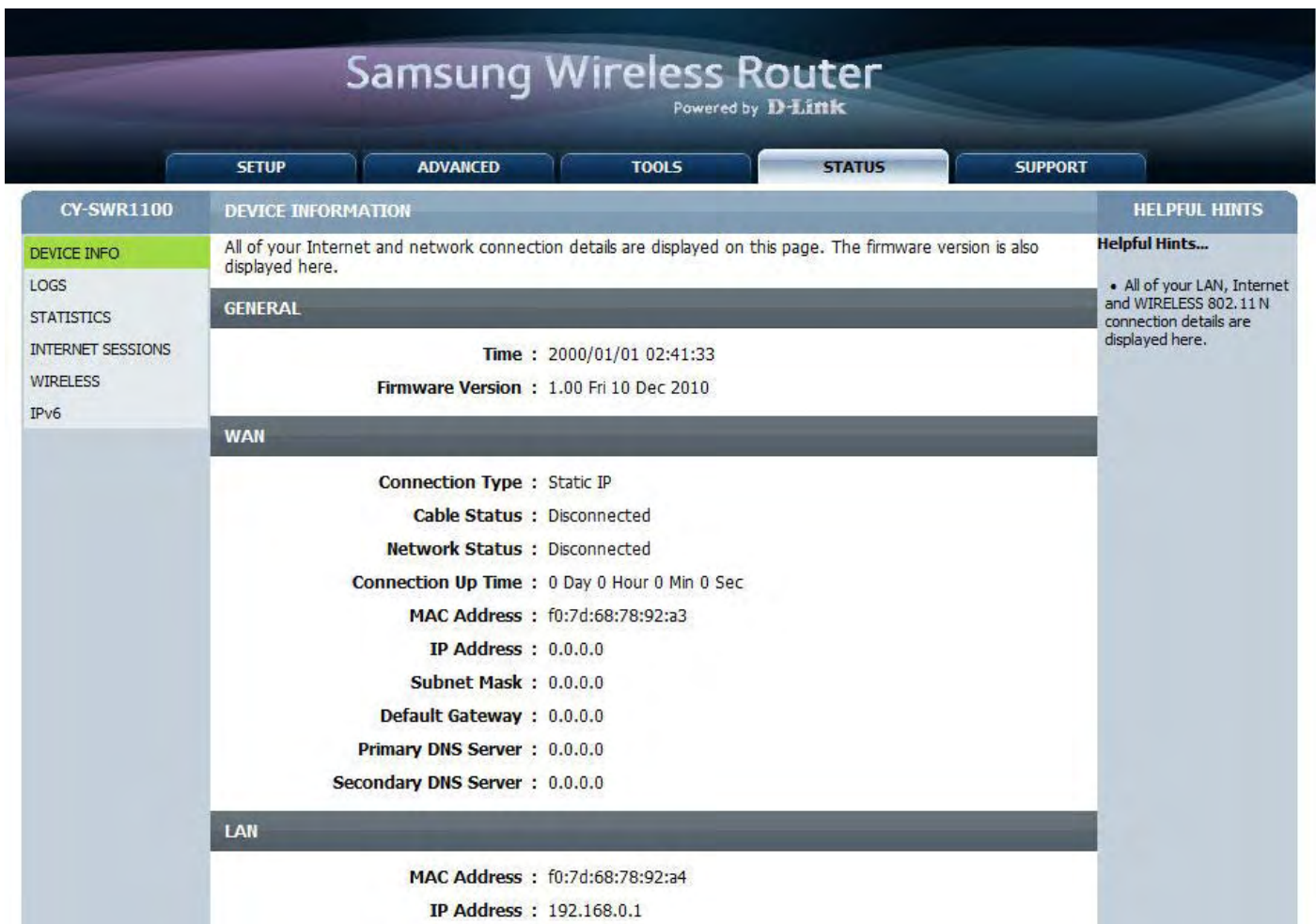
Click on the **Cancel** button to discard the information and cancel the rule addition.

In the **Schedule Rules List** section, the user can view the available schedule rules created. To edit an existing rule, click on the  icon of the specific entry, To remove an existing rule, click on the  icon of the specific entry.

SCHEDULE RULES LIST

Name	Day(s)	Time Frame		
rule1	SUN,MON,TUE,WED,THU,FRI,SAT	0:00 ~ 23:59		

STATUS CATEGORY



Samsung Wireless Router
Powered by **D-Link**

SETUP ADVANCED TOOLS **STATUS** SUPPORT

CY-SWR1100 **DEVICE INFORMATION** **HELPFUL HINTS**

DEVICE INFO All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

LOGS

STATISTICS

INTERNET SESSIONS

WIRELESS

IPv6

GENERAL

Time : 2000/01/01 02:41:33

Firmware Version : 1.00 Fri 10 Dec 2010

WAN

Connection Type : Static IP

Cable Status : Disconnected

Network Status : Disconnected

Connection Up Time : 0 Day 0 Hour 0 Min 0 Sec

MAC Address : f0:7d:68:78:92:a3

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Default Gateway : 0.0.0.0

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

LAN

MAC Address : f0:7d:68:78:92:a4

IP Address : 192.168.0.1

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.

In this category the user will be able to view information regarding the configuration and functionality of this device. Displays like WAN, LAN and Wireless configurations, System, Firewall and Router logs, and more.

Pages that can be configured in the **Status** category are as follows:

Device Information: This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information.

Logs: The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Statistics: Here you can view the amount of packets that pass through the router on both the WAN, LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.

Internet Sessions: The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

Wireless: The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

IPv6: The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

DEVICE INFO

This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

In the **General** section, information about the time and firmware is being displayed.

GENERAL

Time : 2010/12/16 11:26:50

Firmware Version : 1.00 Wed 01 Dec 2010

In the **WAN** section, information about the Internet connection is being displayed.

WAN

Connection Type : Static IP

Cable Status : Disconnected

Network Status : Disconnected

Connection Up Time : 0 Day 0 Hour 0 Min 0 Sec

MAC Address : f0:7d:68:78:92:a3

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Default Gateway : 0.0.0.0

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

In the **LAN** section, information about the Local Area Network configuration is being displayed.

LAN

MAC Address : f0:7d:68:78:92:a4

IP Address : 192.168.0.1

Subnet Mask : 255.255.255.0

DHCP Server : Enabled

In the **Wireless LAN** section, information about the **2.4GHz** Wireless Local Area Network configuration is being displayed.

WIRELESS LAN

Wireless Radio : Enabled

MAC Address : f0:7d:68:78:92:a2

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Channel Width : 20MHz

Channel : 1

Wi-Fi Protected Setup : Enabled/Configured

Network Name (SSID) : SWR1100

Security : WPA/WPA2-PSK

GUESTZONE settings

Network Name (SSID) : SWR1100+

Security : Disabled

In the **Wireless LAN2** section, information about the **5GHz** Wireless Local Area Network configuration is being displayed.

WIRELESS LAN2

Wireless Radio : Enabled

MAC Address : f0:7d:68:78:92:a4

802.11 Mode : Mixed 802.11n and 802.11a

Channel Width : 20/40MHz

Wi-Fi Protected Setup : Enabled/Configured

Channel : 36

Network Name (SSID) : SWR1100_media

Security : WPA/WPA2-PSK

GUESTZONE settings

Network Name (SSID) : SWR1100_media+

Security : Disabled

Logs

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

VIEW LOG

The View Log displays the activities occurring on the CY-SWR1100.

SAVE LOG FILE

Save Log File To Local Hard Drive.

The following parameters can be configured:

Save Log File:	Click the Save button save the Router's log entries to a log file on your computer.
-----------------------	--

LOG TYPE & LEVEL

Log Type: System Firewall & Security Router Status

Log Level: Critical Warning Information

The following parameters can be configured:

Log Type:	Use the radio buttons to select the types of messages that you want to display from the log. System, Firewall & Security, and Router Status messages can be selected.
Log Level:	There are three levels of message importance: Critical, Warning, and Information. Select the levels that you want displayed in the log.

LOG FILES

Page 1 of 1

Time	Message
Thu Dec 16 11:12:09 2010	Web login success from 192.168.0.150
Thu Dec 16 11:12:03 2010	Web logout from 192.168.0.150
Thu Dec 16 10:28:53 2010	Web login success from 192.168.0.150
Thu Dec 16 10:20:30 2010	Web login success from 192.168.0.150
Thu Dec 16 10:20:26 2010	Web login failure from 192.168.0.150
Thu Dec 16 10:20:23 2010	Web login failure from 192.168.0.150

The following parameters can be configured:

First - Last Page:	Use these buttons to navigate to the first or last page of the router logs.
Previous - Next:	Use these buttons to navigate to the next or previous page of the router logs.
Clear:	Click on this button to clear all the contents from the log.
Link to Email Log Settings:	Click this button to open the Email Settings screen so that you can change the Email configuration for sending logs.

STATISTICS

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the router on both the WAN, LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.

TRAFFIC STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

TRAFFIC STATISTICS

	Receive	Transmit
Internet	0 Packets	4 Packets
LAN	3384 Packets	2617 Packets
WIRELESS 2.4G	326508 Packets	13467 Packets
WIRELESS 5G	N/A	N/A

Click on the **Refresh** button to refresh the display page.

Click on the **Reset** button to clear all the statistic information for all the fields displayed.

INTERNET SESSIONS

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

INTERNET SESSIONS

This page displays Source and Destination sessions passing through the device.

NAPT SESSIONS

TCP Sessions : 1

UDP Sessions : 0

Total : 1

NAPT ACTIVE SESSIONS

IP Address	TCP Sessions	UDP Sessions
192.168.0.150	1	0

WIRELESS

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

CONNECTED WIRELESS CLIENT LIST

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

In the **Number of Wireless Clients - 2.4GHz Band** section a list of 2.4GHz active wireless clients will be displayed.

NUMBER OF WIRELESS CLIENTS - 2.4GHZ BAND : 1

SSID	MAC Address	IP Address	Mode	Rate (Mbps)
SWR1100	40:D3:2D:D7:82:F0	192.168.0.100	11g	54

In the **Number of Wireless Clients - 5GHz Band** section a list of 5GHz active wireless clients will be displayed.

NUMBER OF WIRELESS CLIENTS - 5GHZ BAND : 0

SSID	MAC Address	IP Address	Mode	Rate (Mbps)
------	-------------	------------	------	-------------

IPv6

The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

IPv6 NETWORK INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

IPv6 CONNECTION INFORMATION

IPv6 Connection Type : LL
Network Status : Disconnected
WAN IPv6 Address :
IPv6 Default Gateway :
LAN IPv6 Address : /
LAN IPv6 Link-Local Address : fe80::f27d:68ff:fe78:92a4 /64
Primary DNS Server : 0::0
Secondary DNS Server : 0::0

SUPPORT CATEGORY

Samsung Wireless Router
Powered by **D-Link**

SETUP ADVANCED TOOLS STATUS **SUPPORT**

CY-SWR1100 **SUPPORT MENU**

MENU

- [Setup](#)
- [Advanced](#)
- [Tools](#)
- [Status](#)

SETUP HELP

- [Internet](#)
- [Wireless Settings](#)
- [Network Settings](#)

ADVANCED HELP

- [Virtual Server](#)
- [Port Forwarding](#)
- [Application Rules](#)
- [QoS Engine](#)
- [Network Filter](#)
- [Website Filter](#)
- [Firewall Settings](#)
- [Routing](#)
- [Advanced Wireless](#)
- [Wi-Fi Protected Setup](#)
- [Advanced Network](#)
- [IPv6](#)

TOOLS HELP

- [Device Administration](#)
- [Time](#)
- [Email Settings](#)
- [System](#)
- [Firmware](#)

In this category the user will have access to a portal of information regarding each and every page that exists on this device. This information gives the basic description of parameter and uses for the pages.

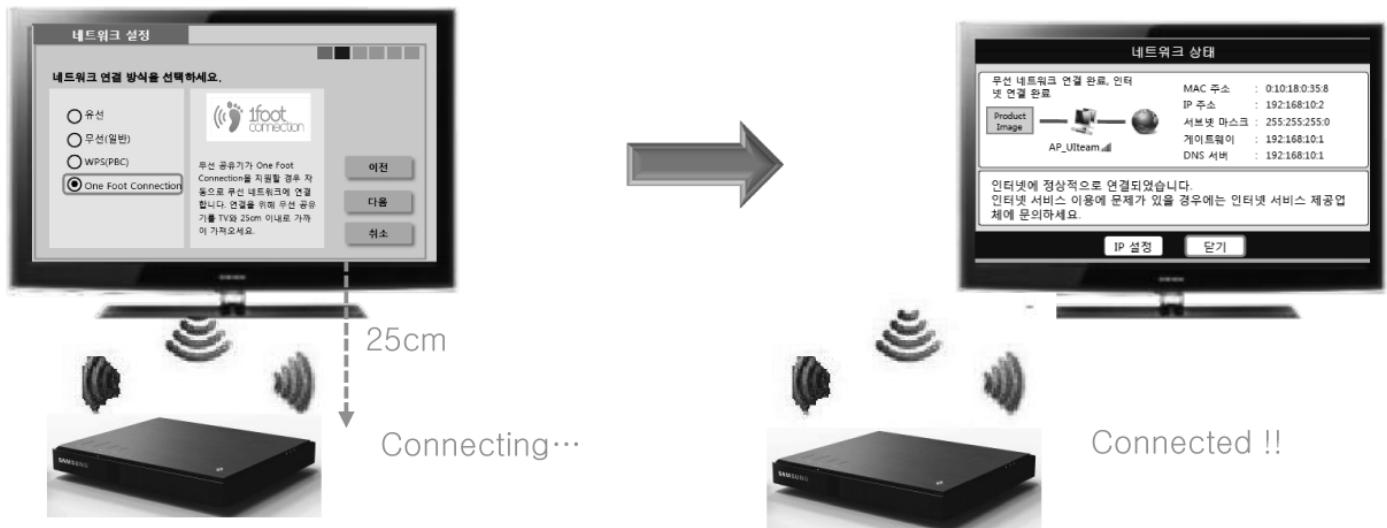
KNOWLEDGE BASE

ONE FOOT CONNECTION (OFC) METHOD

The CY-SWR1100 supports a unique feature called the One Foot Connection method. This feature allows a user to configure their Samsung TV to connect to this router in a very unique and easy way. For this feature to work, the Samsung TV must also support the OFC feature.



CONNECT MY SAMSUNG TV TO THE ROUTER USING OFC.



Step 1: Turn on the power for both devices, the TV and the Router.

Step 2: Navigate to the **Network Settings**, of the TV, using the remote and select the **One Foot Connection** option.

Step 3: Place the CY-SWR1100 approximately 1 foot away from the Wireless Adapter of the TV, while both units are powered ON.

Wait until the connection has been established automatically.

Step 4: When a successful connection is done, a message will appear on the TV, stating that the Network Settings is done.

Place the router back to the desired location in your home.

If the OFC connection failed, a fail message will appear on the TV screen. When this happens restart the Router and the TV and try the connection again by moving the router a little closer to the TV.



Note: When you want to change your wireless network settings on the router and then want to re-configure the wireless connection between the router and the TV, this procedure can be done again from **Step 1**.

PLUG & ACCESS CONNECTION METHOD

The CY-SWR1100 supports another unique feature called the Plug & Access Connection method. This feature allows a user to configure their Samsung TV to connect to this router, wirelessly, using a Flash Memory Stick to transfer the wireless settings, used on the router, to the Samsung TV. This feature will only work between Samsung devices that support the Plug & Access connection method.



CONNECT MY SAMSUNG TV TO THE ROUTER USING PLUG & ACCESS.



Step 1: Turn on the power for both devices, the TV and the Router.

Step 2: Insert a Flash Memory Stick into the USB port, found on the back panel of the CY-SWR1100.

Step 3: The router will identify that Flash Memory Stick and start the wireless configuration settings transfer automatically. The WPS light will start to flicker when data is being written. After the transfer has been completed, the WPS light will shine solid.

Step 4: Remove the Flash Memory Stick from the router and insert it into the USB port of the Samsung TV.

Step 5: When a successful wireless connection configuration is done, a message will appear on the TV, stating that the Network Settings is done.



Note: If the Plug & Access wireless connection configuration failed, a fail message will appear on the TV screen. When this happens restart the Router and the TV and try the connection again from Step 1.



Note: When you want to change your wireless network settings on the router and then want to re-configure the wireless connection between the router and the TV, this procedure can be done again from Step 1.



PRIORITY QUALITY OF SERVICE

The CY-SWR1100 supports another unique feature called the Priority Quality of Service (QoS) feature. This feature will recognize any Samsung wireless networking device, connected to the router, and automatically initiate the built-in priority QoS feature. After initiation the router will give higher wireless network priority to this device.

This is a remarkable feature, especially when a Samsung TV needs to stream High Definition (HD) video and audio content from the Internet for display. This feature is one of the most important aspects of this router and is only used between Samsung devices.

WIRELESS BASICS

Wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

How does Wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, we have a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a Wireless Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

WIRELESS MODES

There are basically two modes of networking:

- Infrastructure – All wireless clients will connect to an access point or wireless router.
- Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

WIRELESS SECURITY

This section will show you the different levels of security you can use to protect your data from intruders. The router offers wireless security options like WPA/WPA2 PSK/EAP.

WHAT IS WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

NETWORKING BASICS

Check your IP address

After you install your new network or wireless adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type cmd and click OK. (Windows® 7/Vista® users type cmd in the Start Search box.) At the prompt, type ipconfig and press Enter.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some fire-wall software programs may block a DHCP request on newly installed adapters.

```

Administrator: C:\Windows\system32\cmd.exe
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::912e:7e75:5d2c:aef%11
    IPv4 Address. . . . . : 192.168.69.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.69.1

Tunnel adapter isatap.{B2B1AEE6-C39F-447B-8462-50015D054EC6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 9:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001::8:d137:9e76:f8:351d:3f57:ba69
    Link-local IPv6 Address . . . . . : fe80::f8:351d:3f57:ba69%18
    Default Gateway . . . . . : 
  
```

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

- Windows® 7 - Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Setting.
- Windows Vista® - Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.
- Windows® XP - Click on Start > Control Panel > Network Connections.
- Windows® 2000 - From the desktop, right-click My Network Places > Properties.

Step 2

Right-click on the Local Area Connection which represents your network adapter and select Properties.

Step 3

Highlight Internet Protocol (TCP/IP) and click Properties.

Step 4

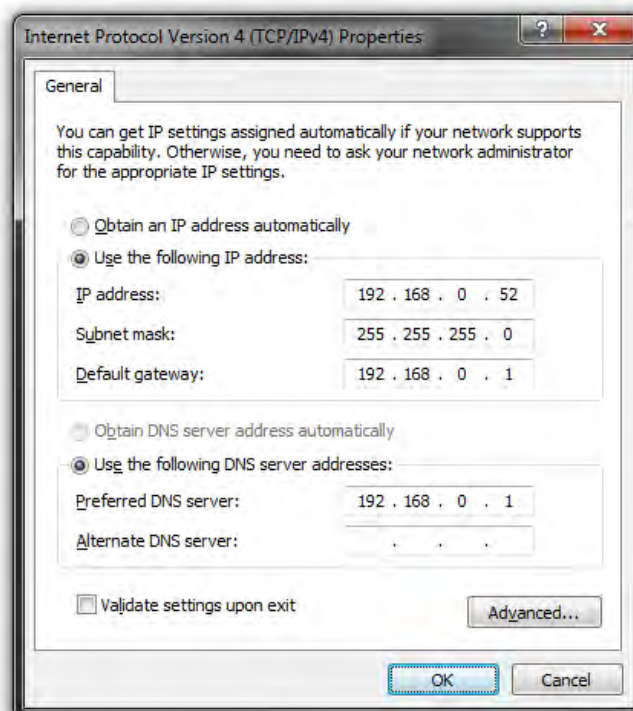
Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click OK twice to save your settings.



CONNECT TO A WIRELESS NETWORK

USING WINDOWS® 7

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

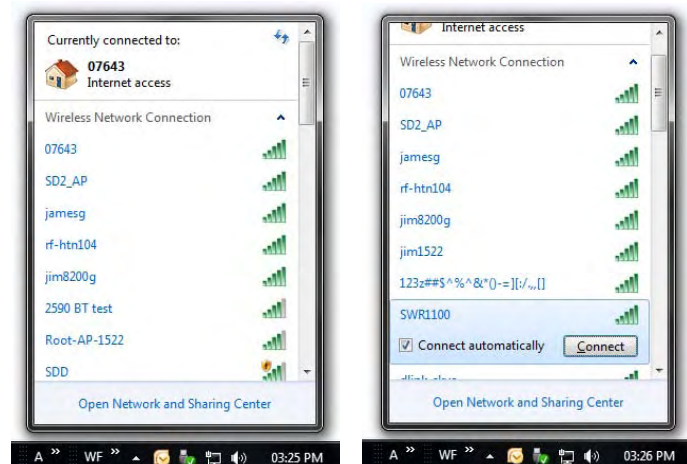
1. Click on the wireless icon in your system tray (lower-right corner).



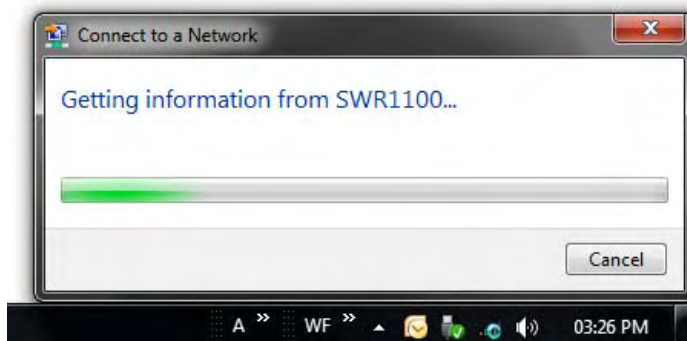
2. The utility will display any available wireless networks in your area.

3. Highlight the wireless network (SSID) you would like to connect to and click the Connect button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and click Connect. You can also connect by pushing the WPS button on the router.

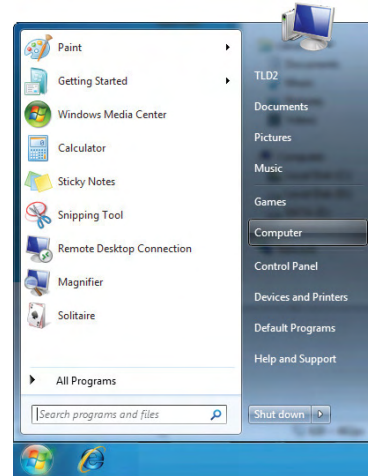
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



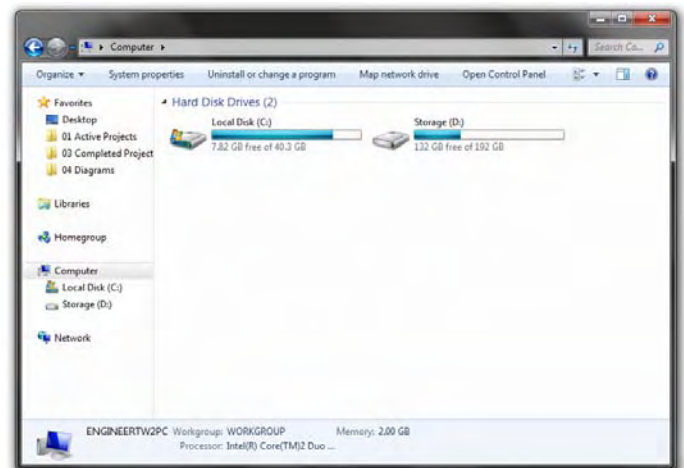
CONFIGURATION WPS

The WPS feature of the router can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature of the router:

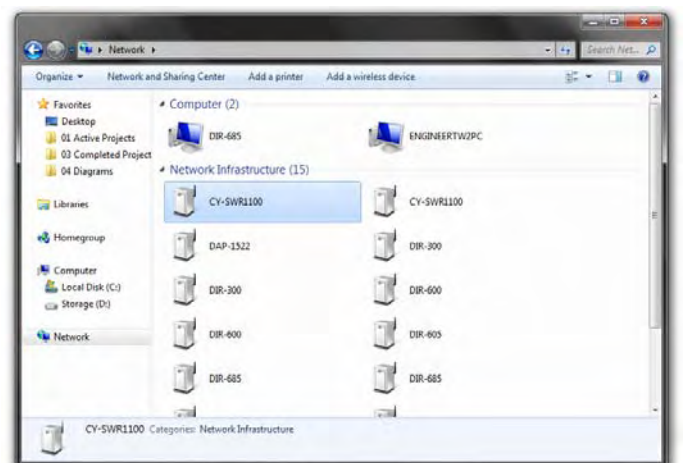
1. Click the Start button and select Computer from the Start menu.



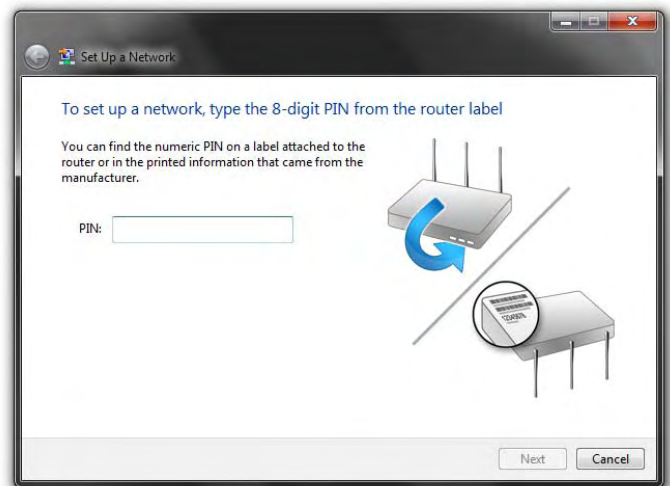
2. Click the Network option.



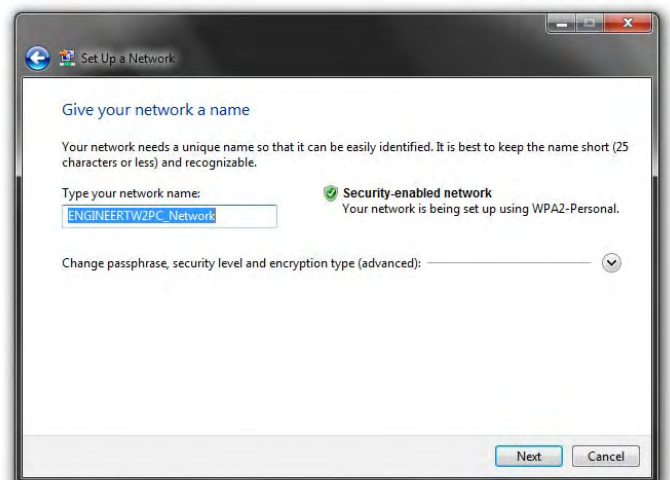
3. Double-click the Router.



4. Input the WPS PIN number and click Next.

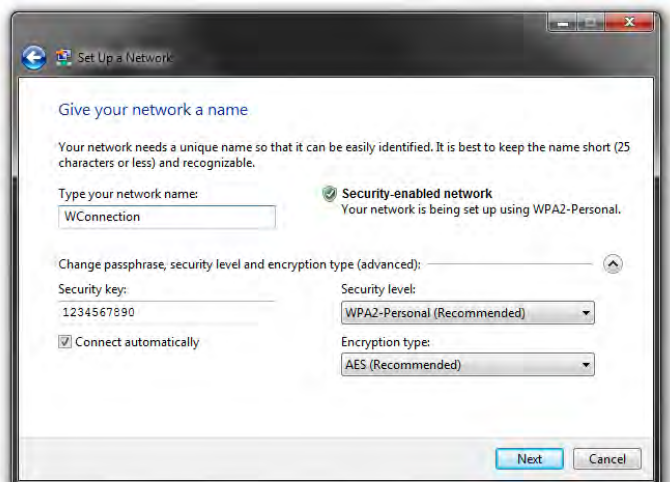


5. Type a name to identify the network.



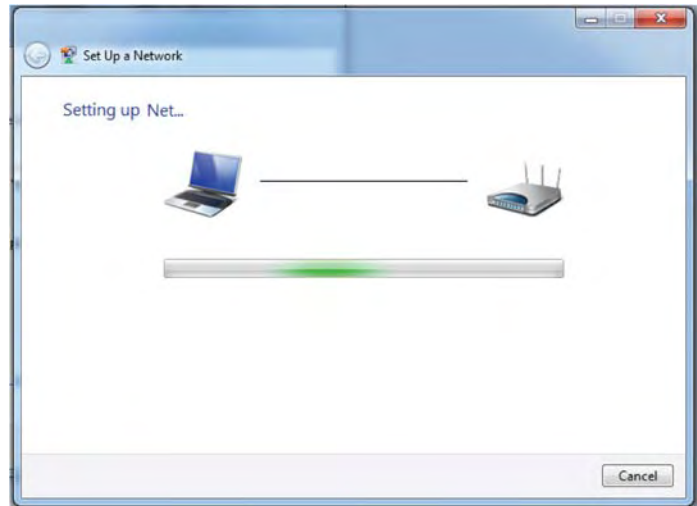
6. To configure advanced settings, click on the drop-down icon.

Click Next to continue.



7. The following window appears while the Router is being configured.

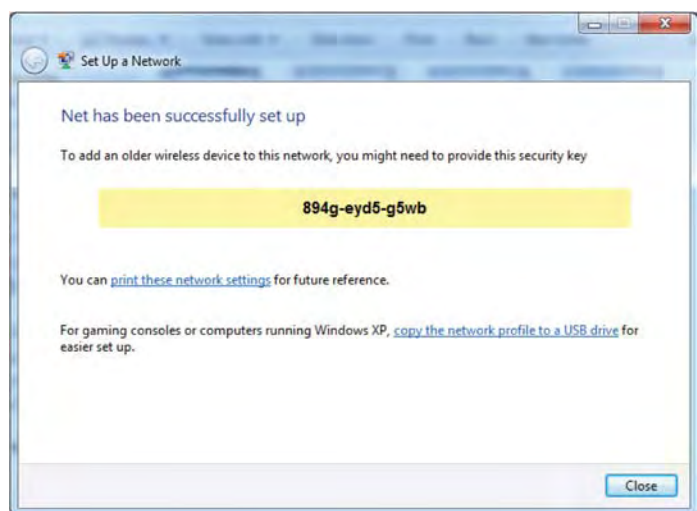
Wait for the configuration to complete.



8. The following window informs you that WPS on the CY-SWR1100 has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click Close to complete WPS setup.

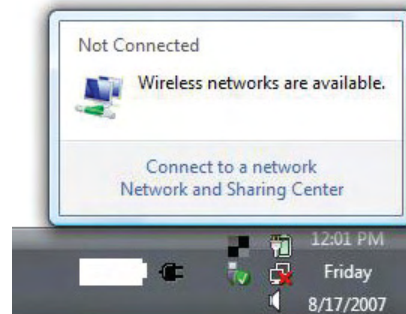


USING WINDOWS VISTA®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility or right-click on the wireless computer icon in your system tray (lower-right corner next to the time).

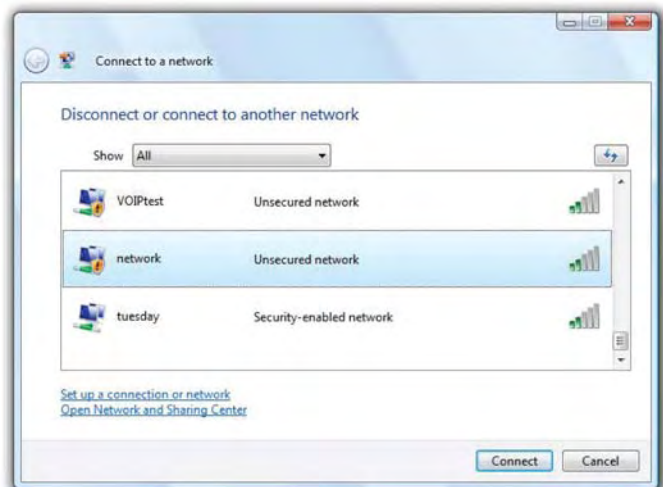
Select **Connect to a network**.



The utility will display any available wireless networks in your area.

Click on a network (displayed using the SSID) and click the **Connect** button.

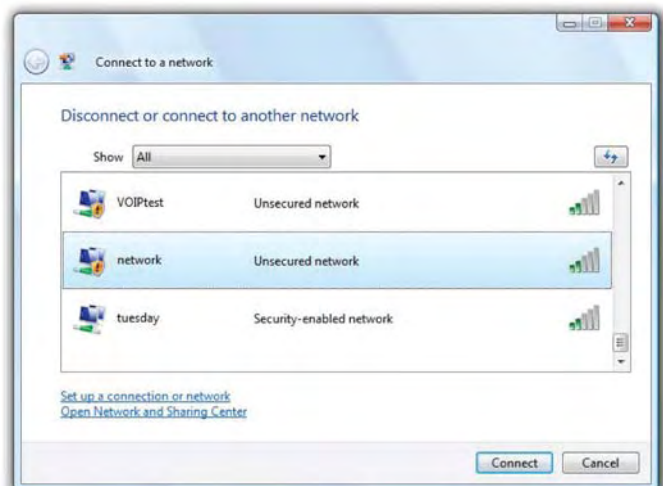
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



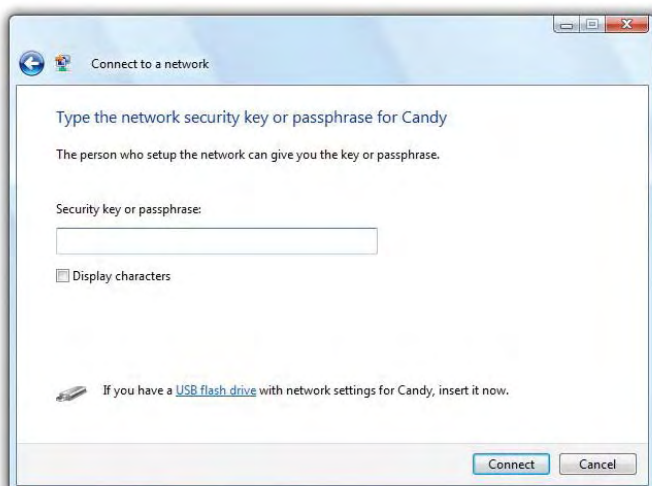
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase that is on your router and click **Connect**.



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

USING WINDOWS® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility or right-click on the wireless computer icon in your system tray (lower right corner next to the time). Select View Available Wireless Networks.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

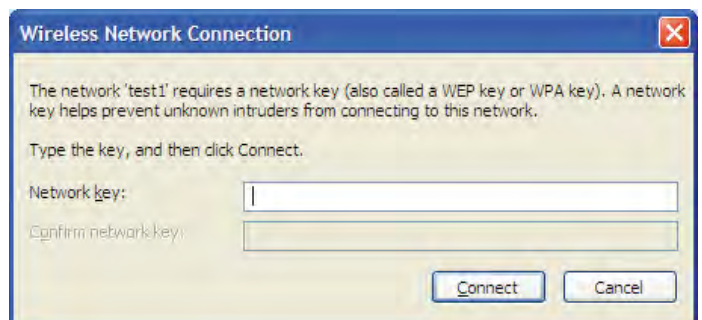
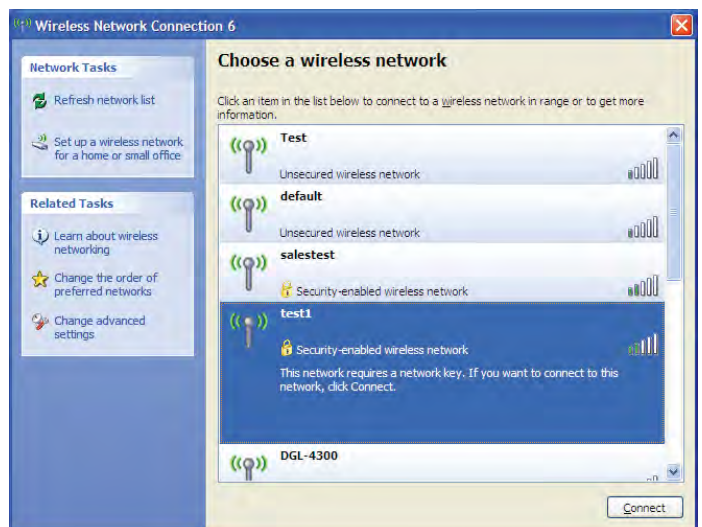
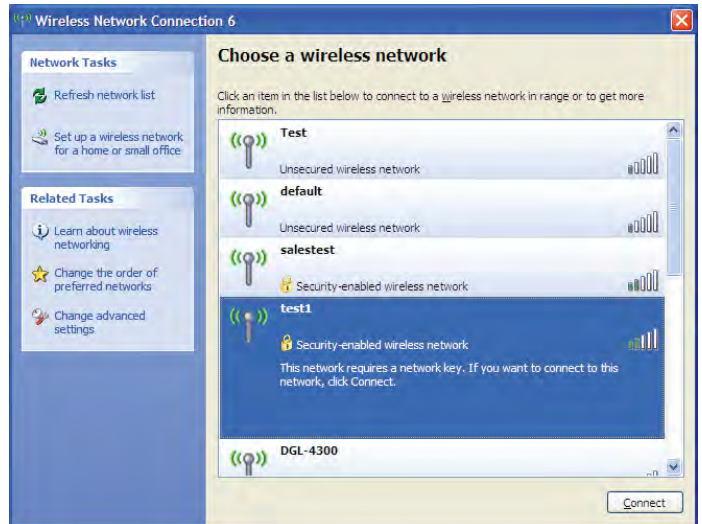
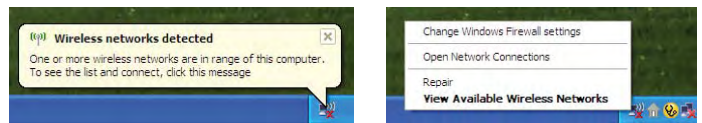
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select View Available Wireless Networks.

2. Highlight the wireless network (SSID) you would like to connect to and click Connect.

3. The Wireless Network Connection box will appear. Enter the WPA-PSK passphrase and click Connect.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



TROUBLESHOOTING

This chapter provides solutions to problems that can occur during the installation and operation of the router. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screen captures on your computer will look similar to the following examples.

Why can't I access the web-based configuration utility?

When entering the IP address of the router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

Make sure you have an updated Java-enabled web browser. We recommend the following:

- Microsoft Internet Explorer® 6.0 and higher
- Mozilla Firefox 3.0 and higher
- Google™ Chrome 2.0 and higher
- Apple Safari 3.0 and higher

Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Configure your Internet settings:

- Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.
- Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.
- Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.
- Close your web browser (if open) and open it.

Access the web management. Open your web browser and enter the IP address of your router in the address bar. This should open the login page for your web management.

If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is admin and leave the password box empty.

Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hot-mail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.



Note: AOL DSL+ users must use MTU of 1400.

- Click on Start and then click Run.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press Enter (or click OK).
- Once the window opens, you'll need to do a special ping. Use the following syntax: ping [url] [-f] [-l] [MTU value]

Example: ping yahoo.com -f -l 1472

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [98.137.149.56] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 98.137.149.56:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [98.137.149.56] with 1472 bytes of data:
Reply from 98.137.149.56: bytes=1472 time=164ms TTL=46
Reply from 98.137.149.56: bytes=1472 time=163ms TTL=46
Reply from 98.137.149.56: bytes=1472 time=165ms TTL=46
Reply from 98.137.149.56: bytes=1472 time=172ms TTL=46

Ping statistics for 98.137.149.56:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 163ms, Maximum = 172ms, Average = 166ms
C:\>_
```

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click OK.
- Enter your username (admin) and password (blank by default). Click OK to enter the web configuration page for the device.
- Click on Setup and then click Manual Configure.
- To change the MTU enter the number in the MTU field and click Save Settings to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

TECHNICAL SPECIFICATIONS

Hardware Specifications

WAN Interface:

- 1 x 10/100/1000Mbps WAN - Auto MDI/MDIX

LAN Interface:

- 4 x 10/100/1000Mbps PC Port - Auto MDI/MDIX

Wireless Interface:

- 802.11a/b/g/n (Simultaneous)

Status LEDs:

- Power, WAN, Wireless(2.4GHz/5GHz), WPS, LAN, USB

Temperature:

- Operating: 14 ~ 140°F (-10 ~ 60°C)
- Storing: -40 ~ 158°F (-40 ~ 70°C)

Operating Voltage:

- Input: 100~240V, 50~60Hz
- Output: DC12V, 2A

Software Specifications

NAT:

- PNAT

Protocols:

- HTTP, DHCP, PPPoE, PPTP, L2TP

Application Protocol:

- H323, MSN, BattleNet, etc

QoS:

- TV Priority QoS

Function Control:

- PC-based Console management

Wireless Connection:

- One Foot Connection, Plug & Access

Wireless Specifications:

Standards:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Wireless Frequency Range:

- 2.4GHz (2.4GHz ~ 2.4835GHz for USA/ Canada/ Taiwan)
- 5GHz (5.15GHz ~ 5.25GHz, 5.725GHz ~ 5.850GHz for USA/ Canada)
(5.25GHz ~ 5.35GHz, 5.725GHz ~ 5.850GHz for Taiwan)

MIMO:

- 2Tx and 2Rx

Wireless Bandwidth Rate:

- IEEE 802.11b : 1, 2, 5.5, 11Mbps
- IEEE 802.11g : 6, 9, 12, 18, 24, 36, 48, 54Mbps
- IEEE 802.11a : 6, 9, 12, 18, 24, 36, 48, 54Mbps
- IEEE 802.11n : MAX 300Mbps(with HT40MHz)

RF Output Power:

- TBD

Modulation:

- OFDM(BPSK, QPSK, 16QAM, 64QAM), DSSS(BPSK, DQPSK, CCK)

Wireless Security:

- 64/128bit WEP
- WPA-PSK
- WPA2-PSK
- WPAPSK/WPA2PSK
- WPS(PIN & PBC)

Compatibility

LED TV:

- D5000 Series and above

LCD TV:

- D550 Series

PDP TV:

- D550 Series and above

Warranty

Period:

- 2 years

Dimension

Set Size:

- 167 x 83 x 140mm (WxDxH)(mm)

Package:

- 274 x 68 x 208mm (WxDxH)(mm)

Weight

Product Weight:

- TBD

Package Weight:

- TBD

Accessory

Contents:

- Installation CD
- Quick Install Guide
- Power Adaptor with Power Cord
- LAN Cable
- Stand
- Mounting Kit

Federal Communication Commission 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 instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does 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 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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

Caution:

- (i) the device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain 4.24dBm permitted (for devices in the band 5725-5850 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

NOTE IMPORTANTE: (Pour l'utilisation des appareils portables)

Déclaration d'exposition aux radiations:

Le produit est conforme aux limites d'exposition pour les appareils portables RF pour les Etats-Unis et le Canada établies pour un environnement non contrôlé.

Le produit est sûr pour un fonctionnement tel que décrit dans ce manuel. La réduction aux expositions RF peut être augmentée si l'appareil peut être conservé aussi loin que possible du corps de l'utilisateur ou que le dispositif est réglé sur la puissance de sortie la plus faible si une telle fonction est disponible.

以下警語適用台灣地區

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在5.25-5.35 GHz頻帶內操作之無線資訊傳輸設備，限於室內使用。