D-Link®
Building Networks for People

DWL-3150

Release 1.00

802.11g Wirless Bridge

User Manual

Business Class Networking

Table of Contents

Product Overview 4
Package Contents 4
Minimum System Requirements 4
Introduction 5
Features 7

Wireless Installation Considerations 8

Three Operational Modes 9

Using the Configuration Menu 10

Home > Basic Settings 11
Wireless Bridge 11
No Security 12
Open System (64 Bits or 128 Bits) 13
Shared Key (64 Bits or 128 Bits) 14
WPA & WPA2 Personal 15
Wireless Workgroup Bridge 16
No Security 17
Open System (64 Bits or 128 Bits) 18
Shared Key (64 Bits or 128 Bits) 19
Wireless WAN 20
Wireless WAN > DHCP Client 22
No Security 22
Open System (64 Bits or 128 Bits) 23
Shared Key (64 Bits or 128 Bits) 24
WPA & WPA2 Personal 25
WPA & WPA2 Enterprise 26
Wireless WAN > Static IP 27
No Security 28
Open System (64 Bits or 128 Bits) 29
Shared Key (64 Bits or 128 Bits) 30
WPA & WPA2 Personal 31
WPA & WPA2 Enterprise 32
LAN 33

Home > Advanced Settings 35
Performance 35
Virtual Server 37
Port Forwarding 38
Application Rules 39
Firewall 40
Advanced Network 41
DDNS 42
Schedule 43
Filters 44
Network Filter 44
Website Filter 45

Home > Status 46
Device Information 46
Wireless Information 47

Statistics 48
Log 49
View Log 49
Log Settings 50

Tool 51
Administrator Settings 51
Firmware Upgrade 52
Configuration File Upload and Download 53
NTP Settings 54

Configuration 55
Save and Activate 55

System 56
System Settings 56
System Information 57

Wireless Basics 58

Networking Basics 63
Check your IP Address 63
Statically Assign an IP Address 64

Contacting Technical Support 65

GNU/Linux GPL 66
GNU General Public License 67

Warranty 73

Registration 78

Package Contents

- D-Link DWL-3150 802.11g Wireless Bridge
- Install Guide
- Manual, Install Guide, and warranty on CD
- Ethernet (CAT5-UTP/Straight-Through) Cable
- Power Adapter

If any of the above items are missing, please contact your reseller.

Minimum System Requirements

- Computers with Windows®, Macintosh, or Linux-based operating systems with an installed Ethernet Adapter.
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.

Introduction

At up to fifteen times the speed* of previous wireless devices you can work faster and more efficiently, increasing productivity. With the DWL-3150, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are able to move across the network quickly.

Inclusion of all three standards (802.11b and 802.11g) means that the DWL-3150 is versatile enough to allow connection to almost any 802.11 network or device.

The DWL-3150 is capable of operating in one of 3 different modes to meet your wireless networking needs. The DWL-3150 can operate as a Wireless Bridge, a Wireless Workgroup Bridge, or a Wireless WAN.

An ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, trade shows and special events, the DWL-3150 provides data transfers at up to 54Mbps* when used with other D-Link Air Premier® or Air Premier AG® products (The 802.11g standard is backwards compatible with 802.11b devices).

WPA is offered in two flavors: Enterprise (used for corporations), and Personal (used for home users).

WPA-Personal and WPA2-Personal is directed at home users who do not have the server based equipment required for user authentication. The method of authentication is similar to WEP because you define a “Pre-Shared Key” on the wireless router/AP. Once the pre-shared key is confirmed and satisfied on both the client and access point, then access is granted. The encryption method used is referred to as the Temporal Key Integrity Protocol (TKIP), which offers per-packet dynamic hashing. It also includes an integrity checking feature which ensures that the packets were not tampered with during wireless transmission. WPA2-Personal is far superior to WPA-Personal, because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

WPA-Enterprise and WPA2-Enterprise is ideal for businesses that have existing security infrastructures in place. Management and security implementation can now be centralized on a server participating on the network. Utilizing 802.1x with a RADIUS (Remote Authentication Dial-in User Service) server, a network administrator can define a list of authorized users who can access the wireless LAN. When attempting to access a wireless LAN with either WPA-Enterprise or WPA2-Enterprise configured, the new client will be challenged with a username and password. If the new client is authorized by the administration, and enters the correct username and password, then access is granted. In a scenario where an employee leaves the company, the network administrator can remove the employee from the authorized list and not have to worry about the network being compromised by a former employee. WPA2-Enterprise is far superior to WPA-Enterprise, because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

Features

- **3 Different Operation modes** - Capable of operating in one of three different operation modes to meet your wireless networking requirements: Wireless Bridge, Wireless Workgroup Bridge, or Wireless WAN.
- Faster wireless networking speeds up to 54Mbps*.
- **Compatible with 802.11b and 802.11g Devices** that is fully compatible with the IEEE 802.11b and 802.11g standards, the DWL-3150 can connect with existing 802.11b- or 802.11g-compliant wireless network adapter cards.
- **Compatible with the 802.11b standard** to provide a wireless data rate of up to 11Mbps - that means you can migrate your system to the 802.11g standard on your own schedule without sacrificing connectivity.
- **Better security with WPA** - The DWL-3150 can securely connect wireless clients on the network using WPA (Wi-Fi Protected Access) providing a much higher level of security for your data and communications than has previously been available.
- Utilizes **OFDM** technology (Orthogonal Frequency Division Multiplexing).
- Operates in the 2.437GHz frequency range for an 802.11b and 802.11g network.
- **Web-based interface** for managing and configuring.

*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

Wireless Installation Considerations

The D-Link 802.11g Wireless Bridge 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 D-Link adapter 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 in not in use.

Three Operational Modes

Operation Mode (Only supports 1 mode at a time)	Function
Wireless Bridge	This enables any device behind the DWL-3150 that connects to the Wireless LAN.
Wireless Workgroup Bridge	Wirelessly Connects Multi Netrworks.
Wireless WAN	The WISP (Wireless Internet Service Provider) subscriber can share the WISP connection without the need of an extra router.

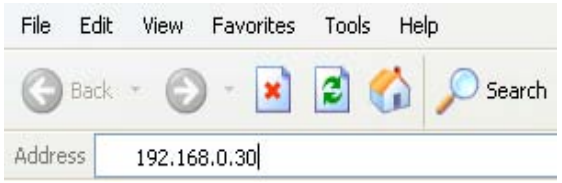
Using the Configuration Menu

To configure the DWL-3150, use a computer which is connected to the DWL-3150 with an Ethernet cable (see the *Network Layout* diagram).

First, disable the ***Access the Internet using a proxy server*** function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.

Start your web browser program (Internet Explorer, Netscape Navigator).

Type the IP address and http port of the DWL-3150 in the address field (http://192.168.0.30) and press **Enter**. Make sure that the IP addresses of the DWL-3150 and your computer are in the same subnet.



After the connection is established, you will see the user identification window as shown.

Note: *If you have changed the default IP address assigned to the DWL-3150, make sure to enter the correct IP address.*

- Type **admin** in the **User Name** field
- Leave the **Password** field blank
- Click **OK**

Note: If you have changed the password, make sure to enter the correct password.

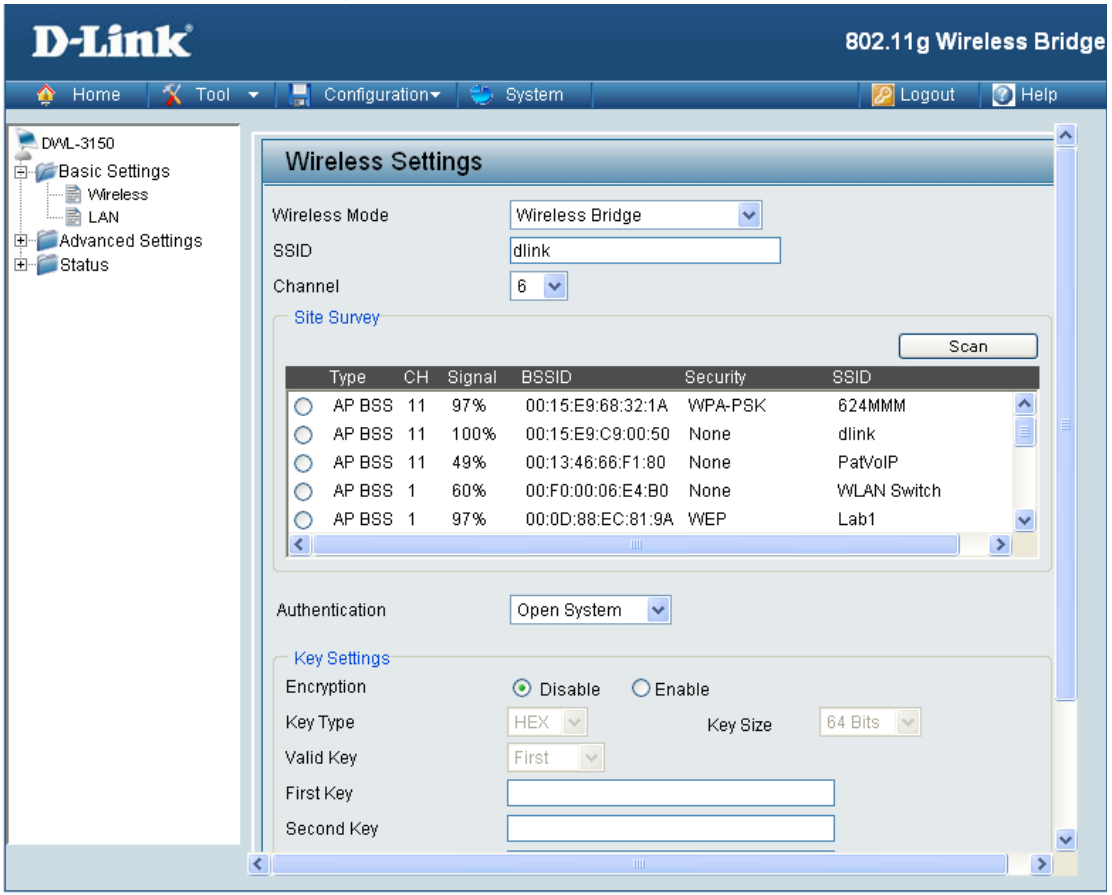
Home > Basic Settings
Wireless Bridge

Wireless Mode: Wireless Bridge - Wirelessly connects Ethernet devices, and provides immediate connection for Ethernet devices without the need for any drivers.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The factory default setting is “dlink”. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Channel: Indicates the channel setting for the DWL-3150. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

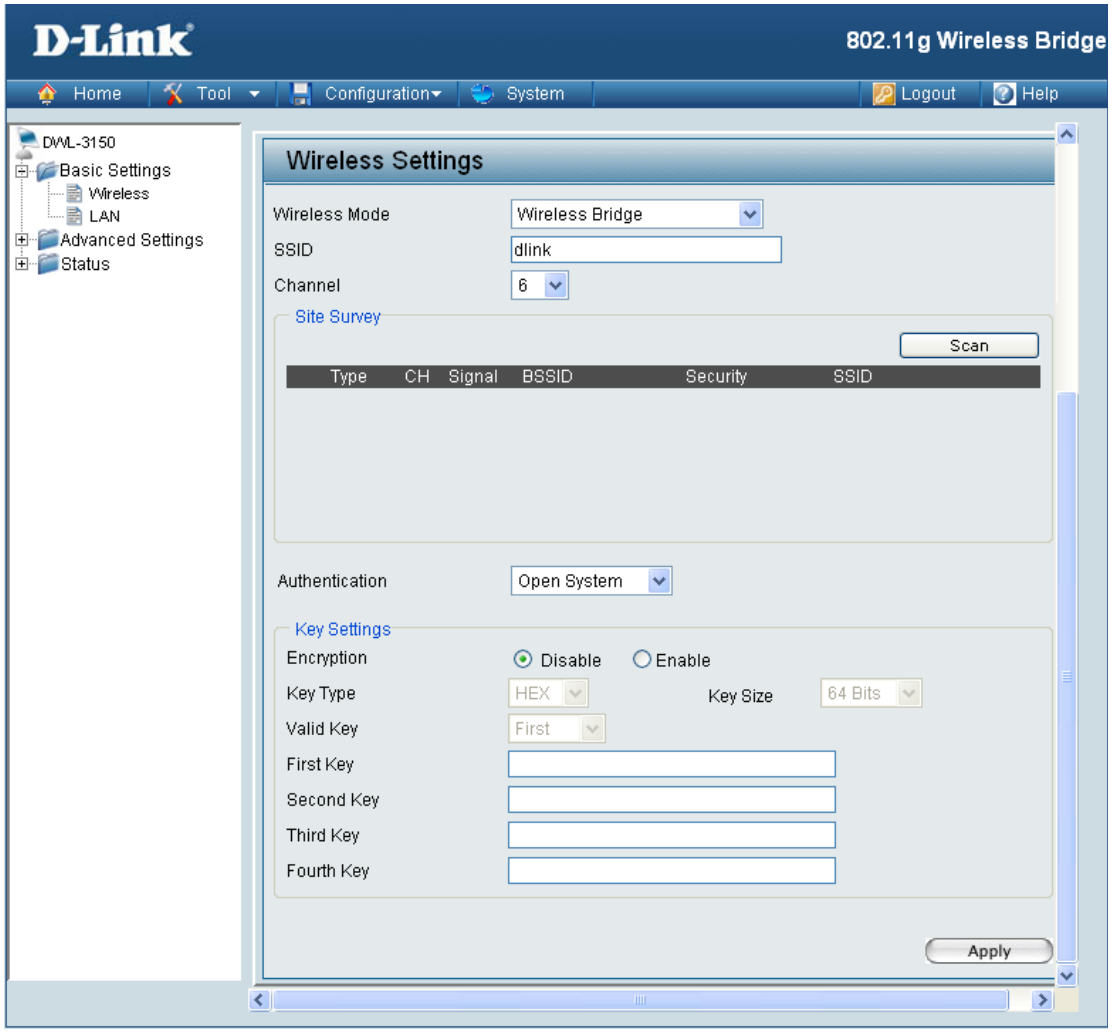
Authentication: For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to “Open System”.



No Security

Authentication: For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

Encryption: Select Disabled to disable WEP encryption.



Open System (64 Bits or 128 Bits)

Authentication: For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

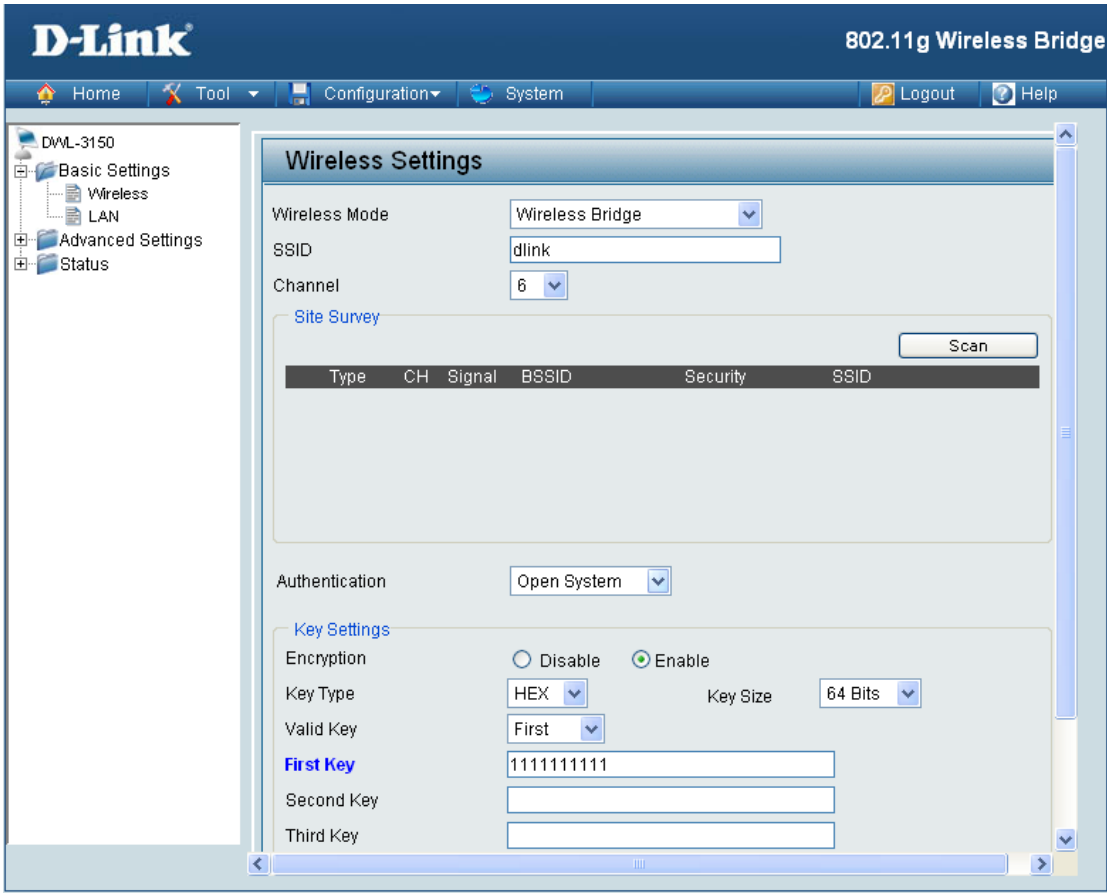
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Keys: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Shared Key (64 Bits or 128 Bits)

Authentication: For Shared Key authentication, the bridge cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

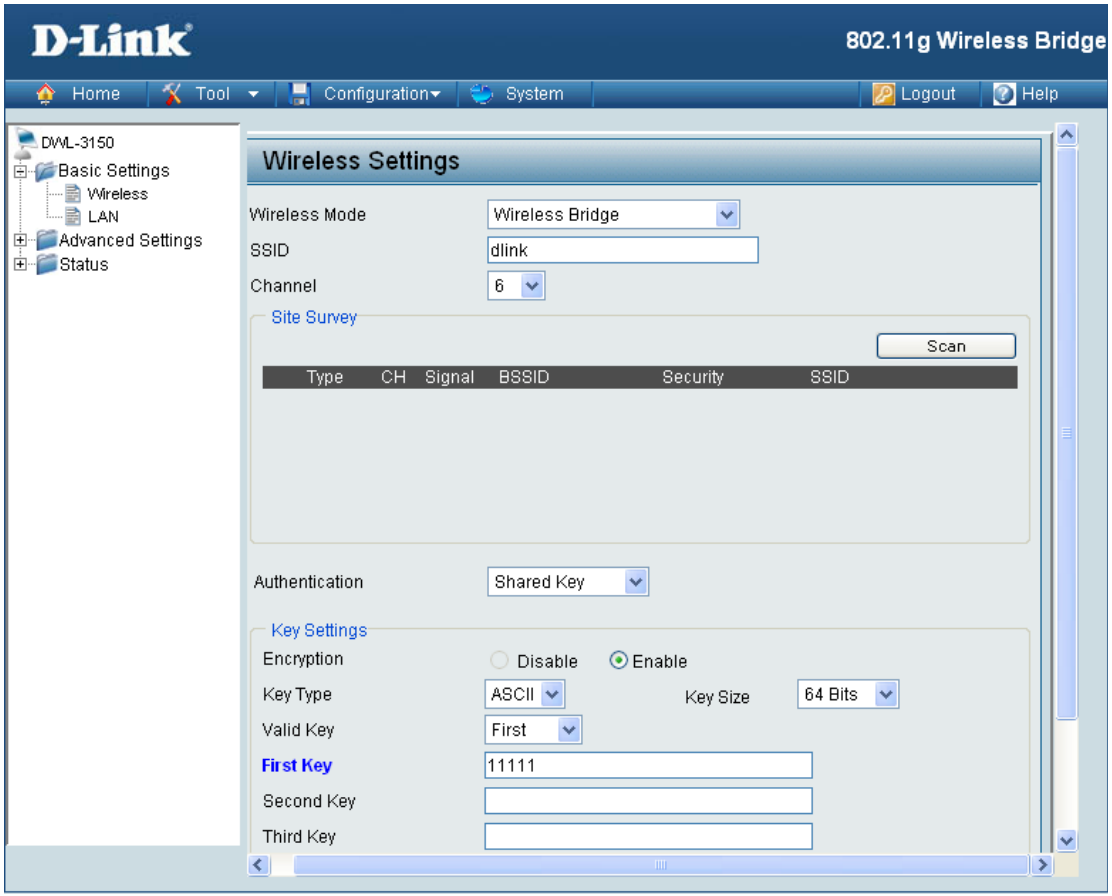
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Keys: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

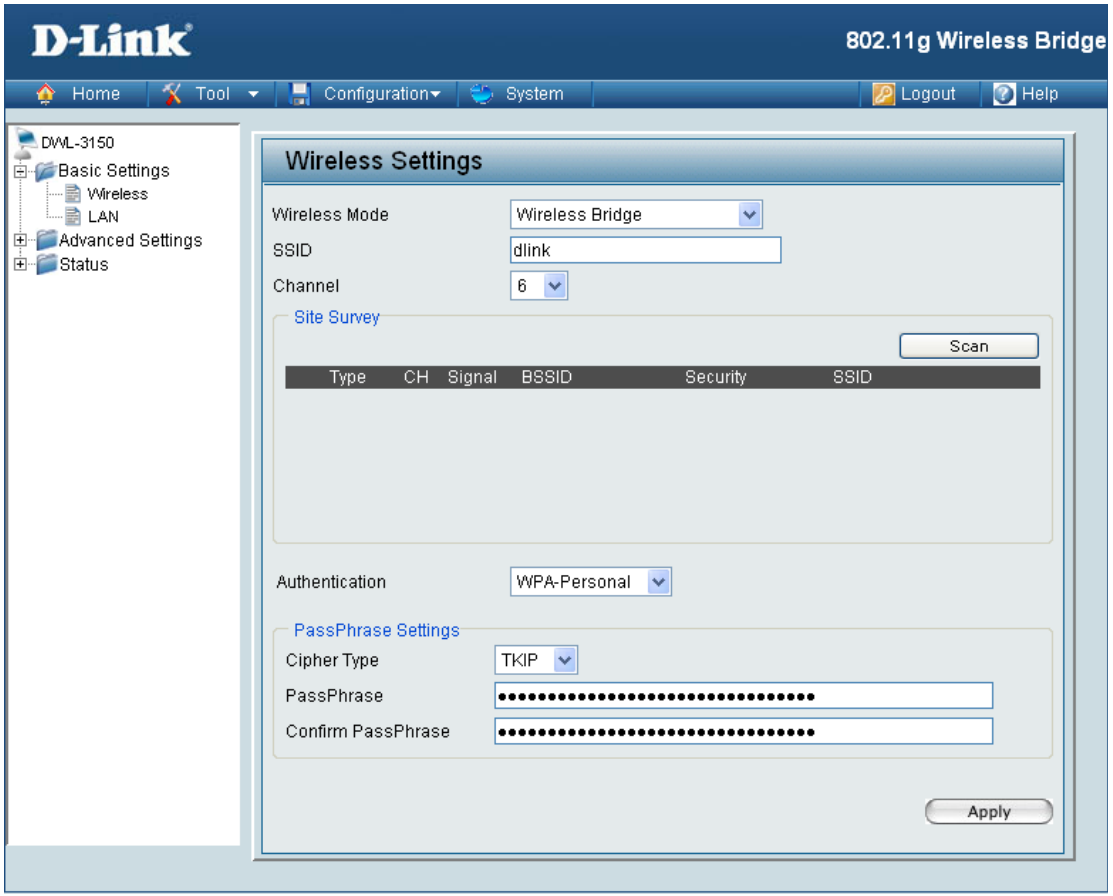
WPA & WPA2 Personal

Authentication: Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA and WPA2 uses different algorithm. Auto allows both WPA and WPA2.

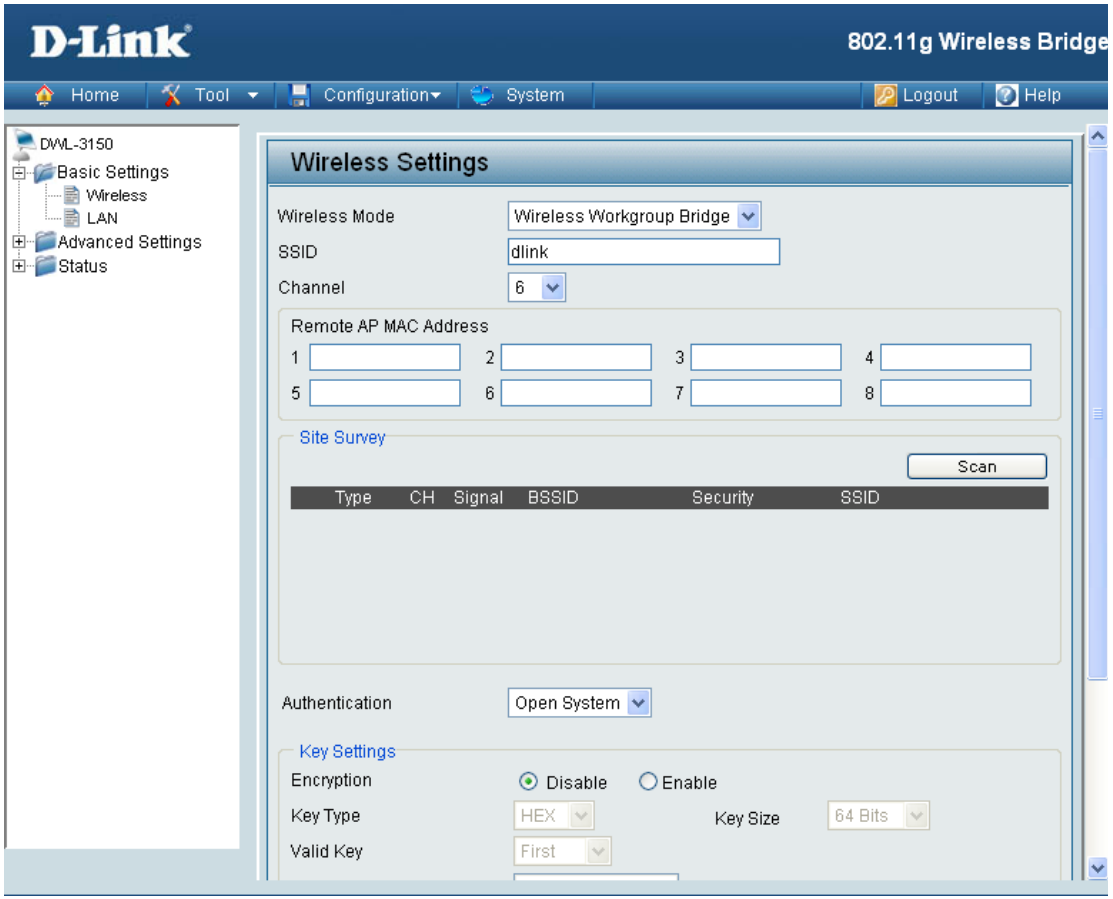
Cipher Type: Select TKIP or AES from the pull-down menu.

PassPhrase: Enter a passphrase. The passphrase is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.

Confirm PassPhrase: Re-enter the passphrase once more for confirmation.



Wireless Workgroup Bridge



Wireless Mode: Wireless Workgroup Bridge - Wirelessly connects multiple wireless networks while still functioning as a wireless access point.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The factory default setting is “dlink”. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Channel: Indicates the channel setting for the DWL-3150. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Remote AP MAC Address: Enter up to eight Remote Bridge MAC Addresses.

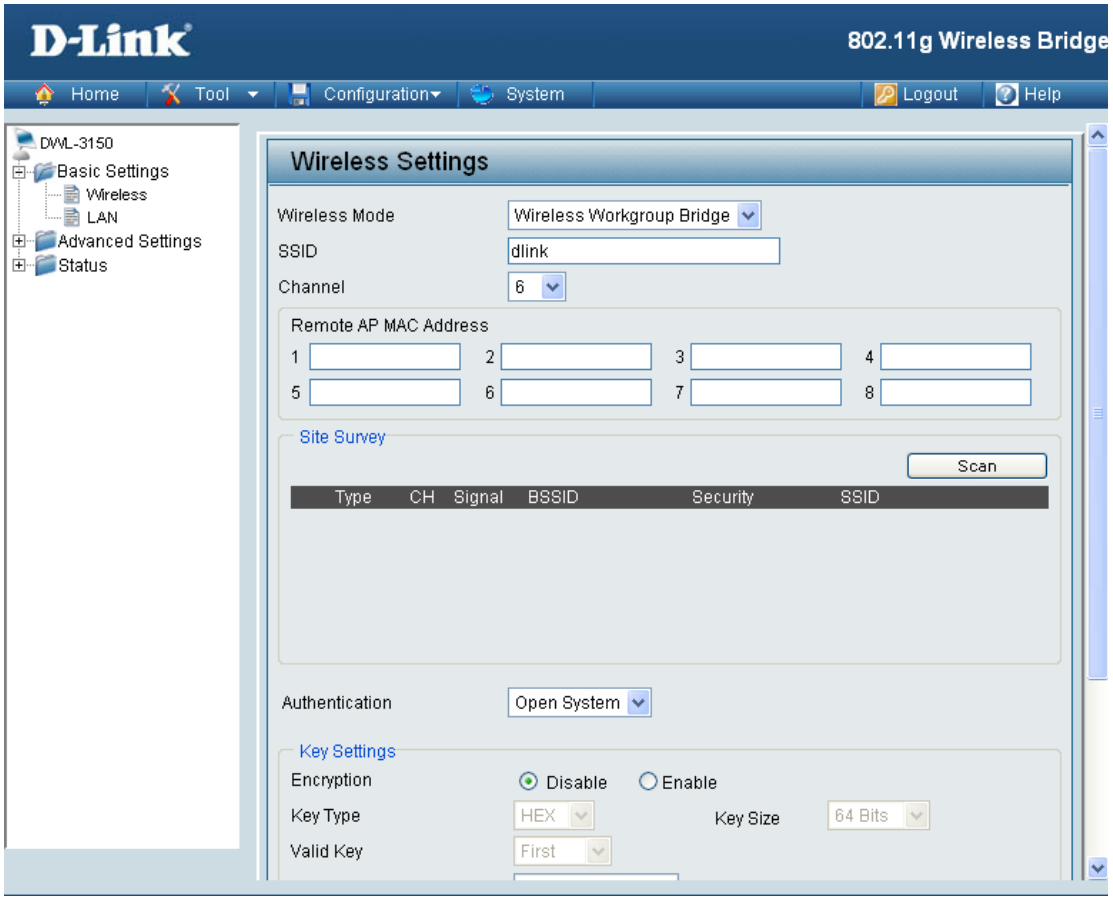
Site Survey: Select your network.

Authentication: For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to “Open System”.

No Security

Authentication: No Security is selected.

Encryption: Disabled.



Open System (64 Bits or 128 Bits)

Authentication: For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

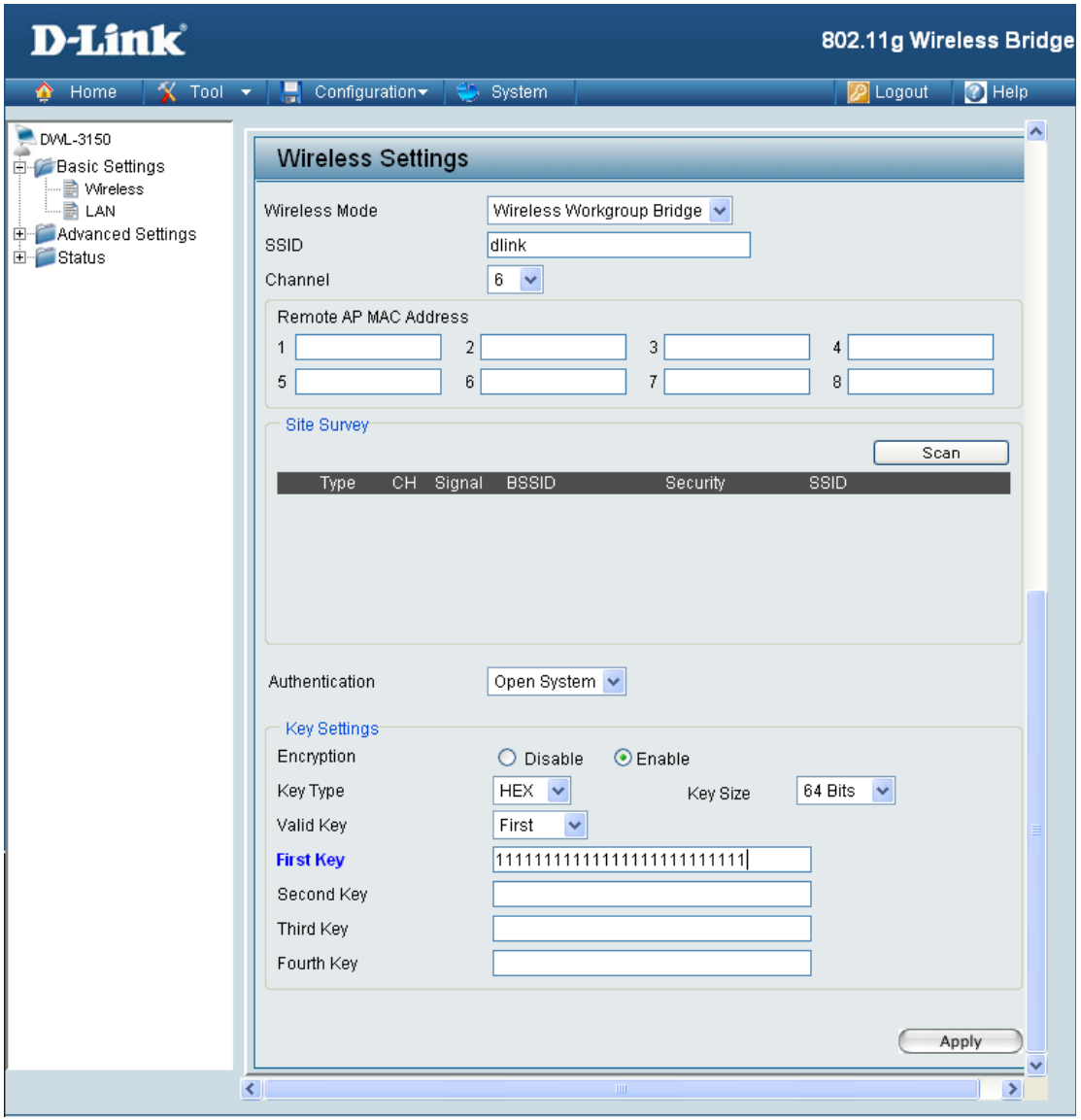
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Shared Key (64 Bits or 128 Bits)

Authentication: For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

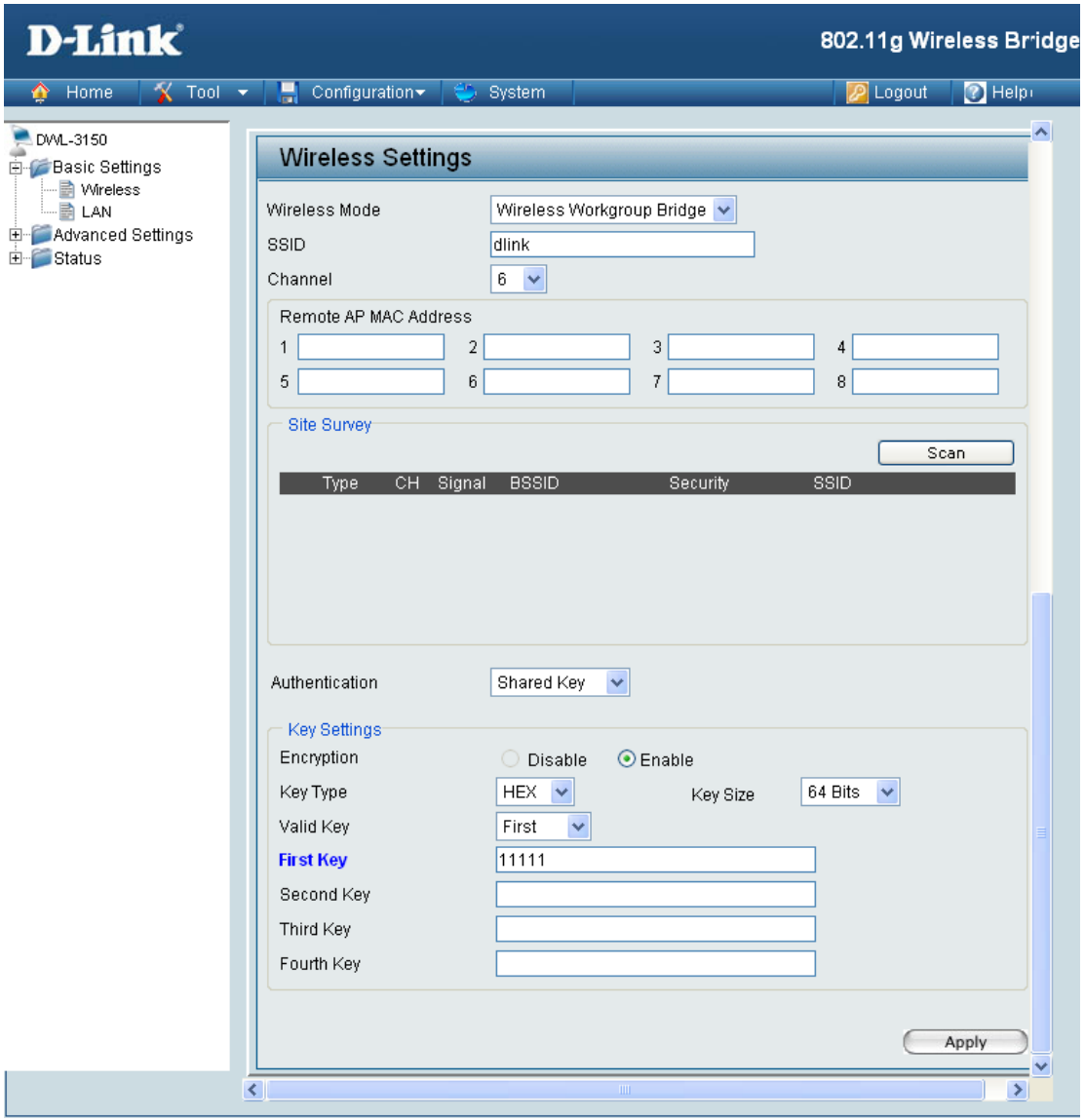
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



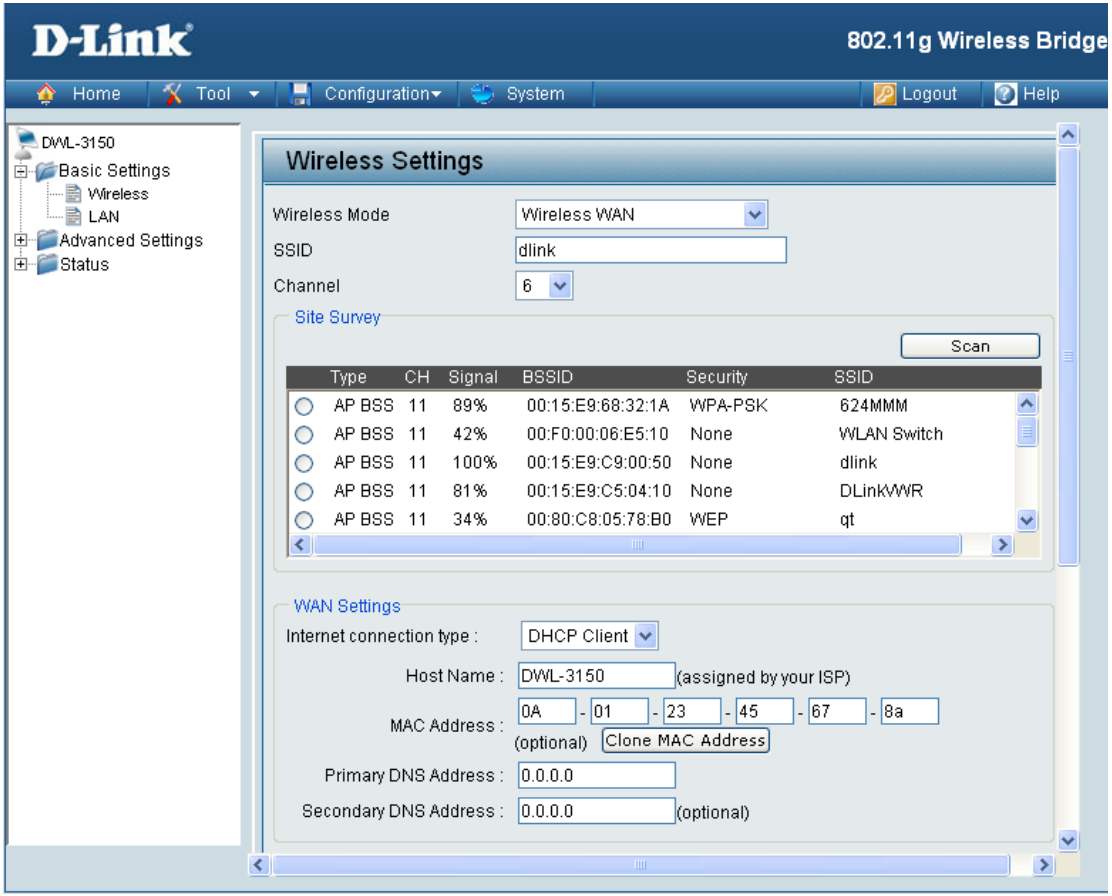
Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Wireless WAN

Wireless Mode: Wireless WAN - In this mode, the DWL-3150 will behave just the same as the Wireless Bridge mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WISP (Wireless Internet Service Provider) subscriber can share the WISP connection without the need for extra router.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless ISP. The factory default setting is “dlink”. The SSID can be easily changed to connect to an existing wireless network.

Channel: Indicates the channel setting for the DWL-3150. The Channel can be changed to fit the channel setting for an existing wireless network.



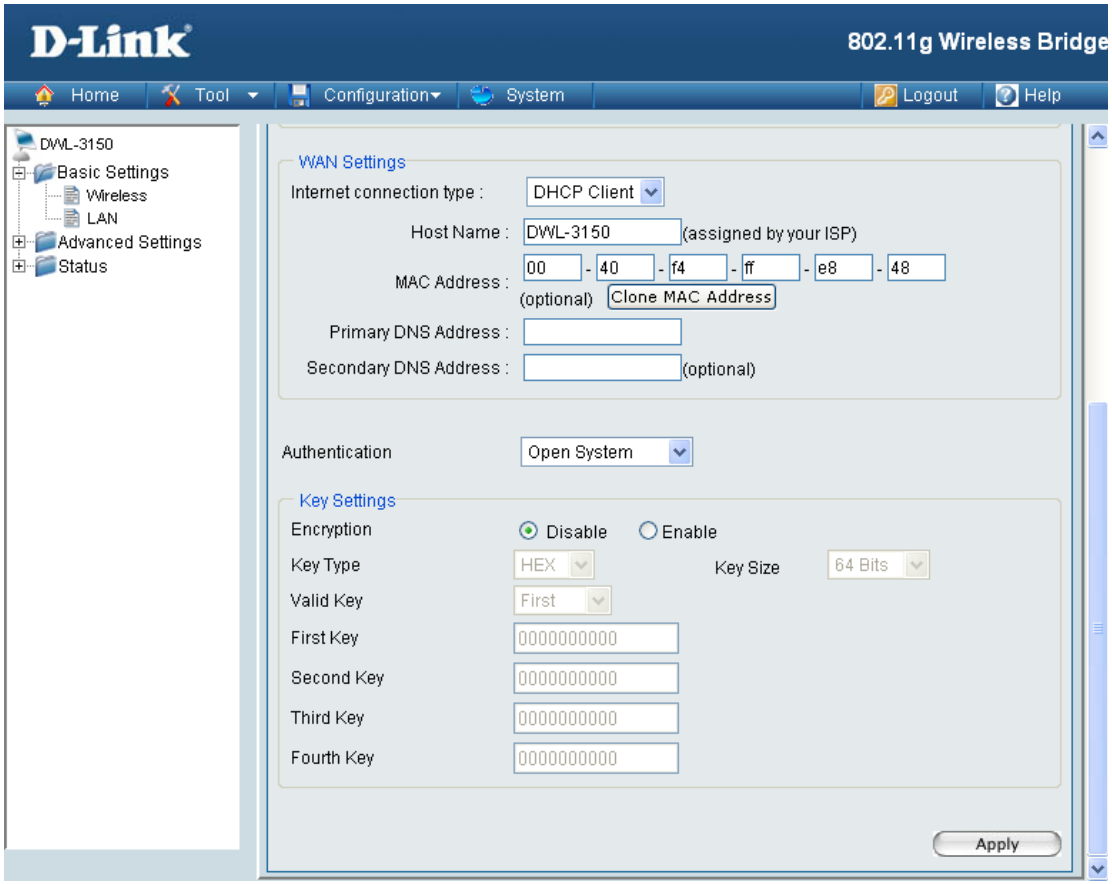
Internet Connection Type:	Choose DHCP to obtain an IP Address automatically from a DHCP server in your network. This is allows the DWL-3150 to obtain the DHCP address from WISP.
Host Name:	The Hostname of the network device you are configuring DHCP Reservation for.
MAC Address:	Enter the MAC address of the network device you are configuring a DHCP Reservation for.
Clone MAC Address:	Copy the MAC address of the network device you are configuring a DHCP Reservation for.
Primary DNS Server:	Enter your primary DNS IP address.
Secondary DNS Server:	Enter your secondary DNS IP address.

Wireless WAN > DHCP Client

No Security

Authentication: For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected.

Encryption: Select Disable if you choose to not have security.



Open System (64 Bits or 128 Bits)

Authentication: For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

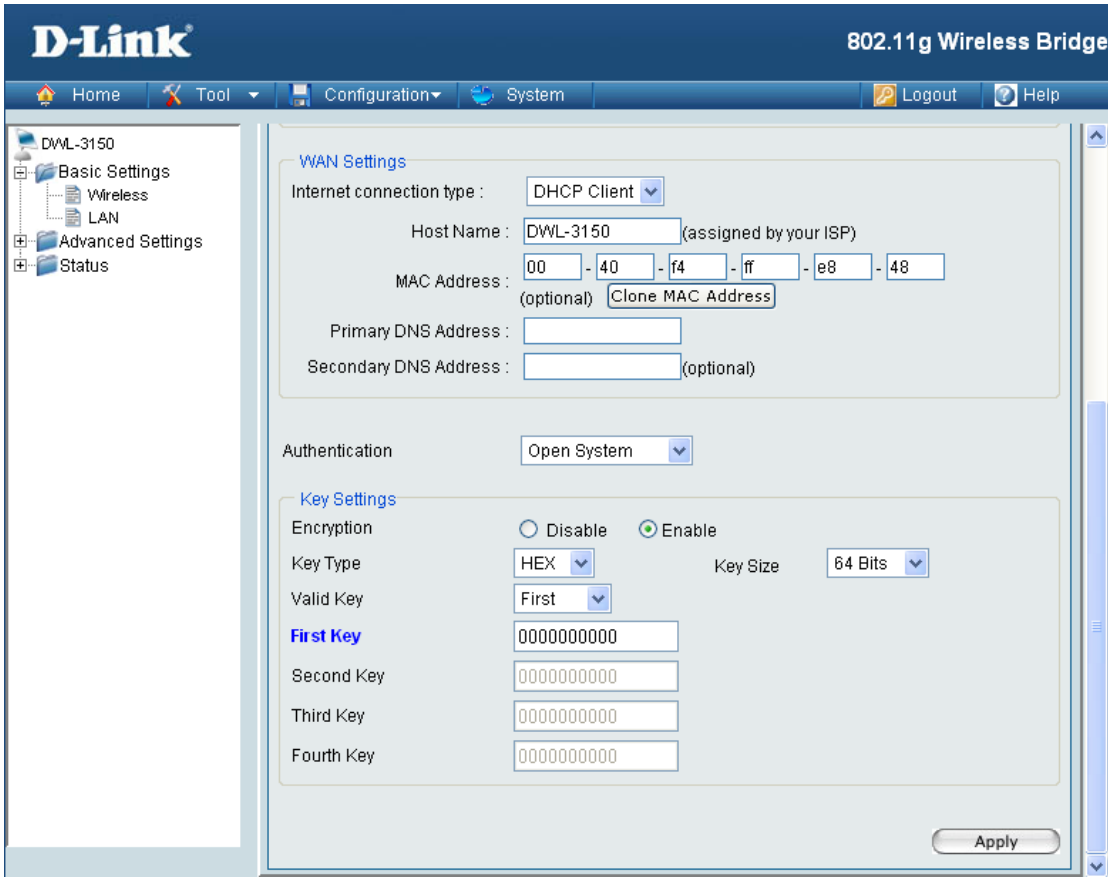
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Shared Key (64 Bits or 128 Bits)

Authentication: For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

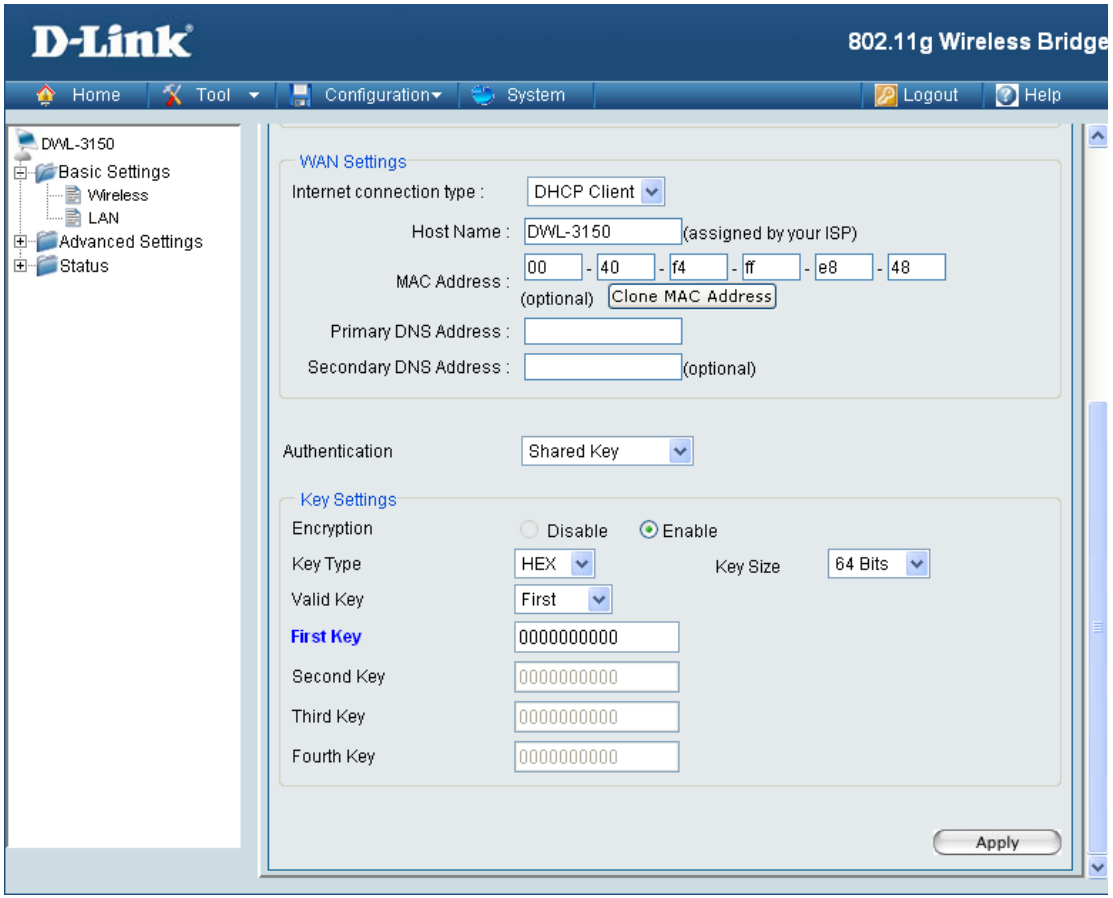
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

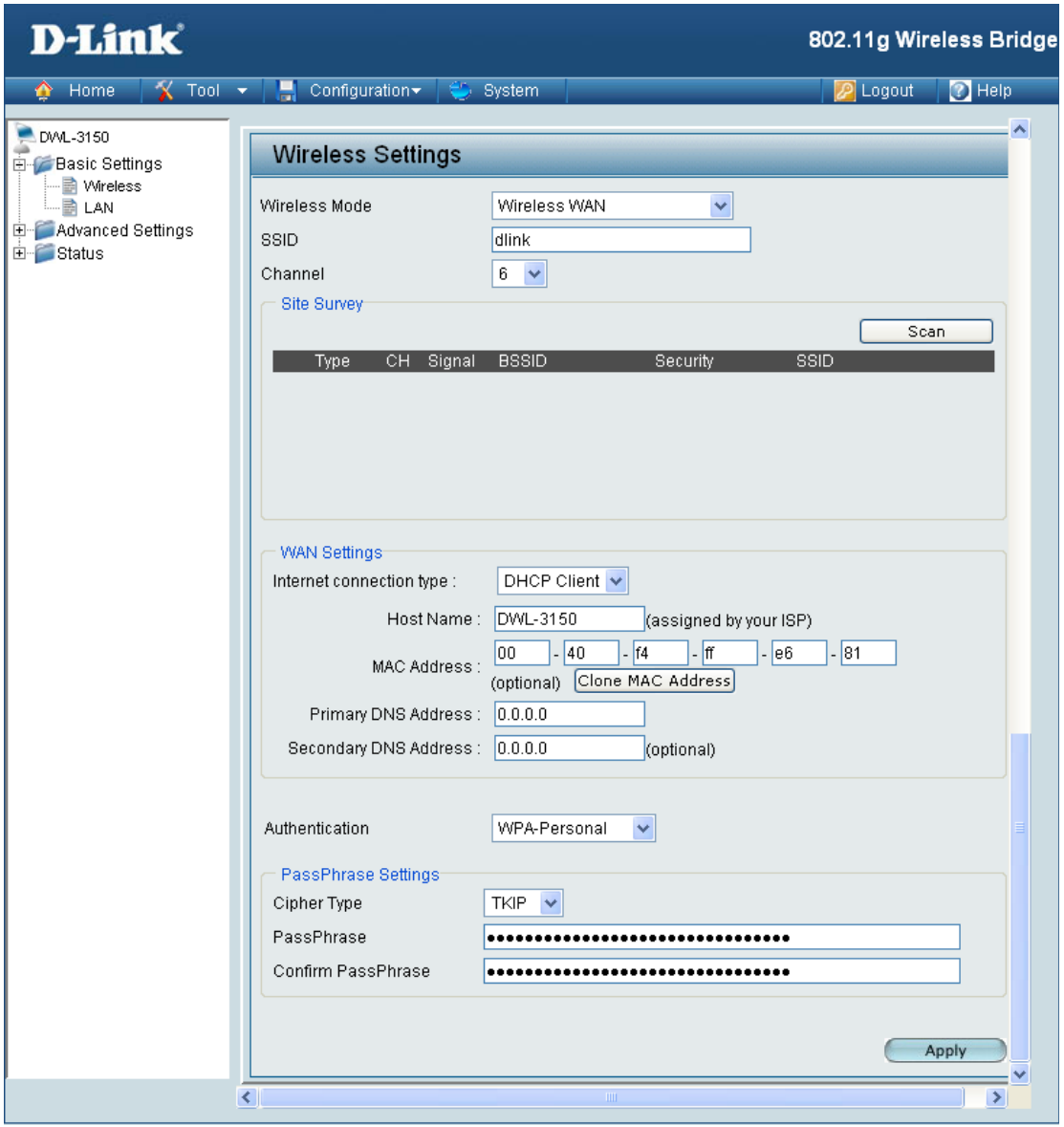
WPA & WPA2 Personal

Authentication: Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA and WPA2 uses different algorithm.

Cipher Type: Select TKIP or AES from the pull-down menu.

PassPhrase: Enter a passphrase. The passphrase is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.

Confirm PassPhrase: Re-enter the passphrase once more for confirmation.



WPA & WPA2 Enterprise

Authentication: Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

EAP Type: Select TLS, TTLS or PEAP from the pull-down menu.

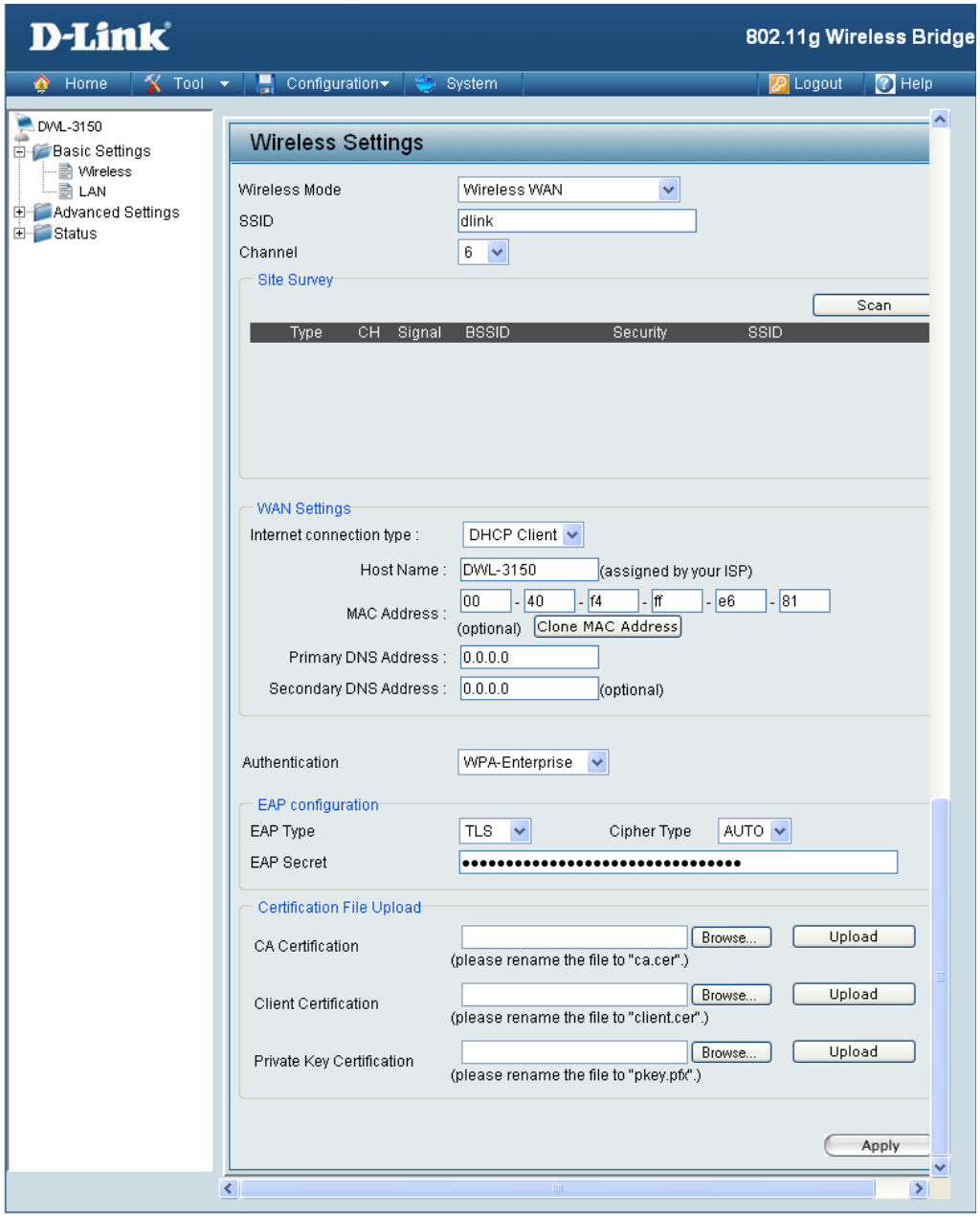
Cipher Type: Select TKIP or AES from the pull-down menu.

EAP Secret: Client and server authenticate each other using digital certificates. Client generates a pre-master secret key by encrypting a random number with the server's public key and sends it to the server.

CA Certification: Certificate Authority (Ex: Microsoft Certification, Bank Cerification…etc).

Client Certification: Client Authentication (Ex: The cerification from Radius Server use in client device).

Private Key Certification: EAP private key data use in wireless connection.



Wireless WAN > Static IP

Internet Connection Type: Choose Static IP if you have a static IP subscription from WISP.

IP Address: Enter the initial IP address to be assigned by the DHCP server.

Subnet Mask: Enter the subnet mask.

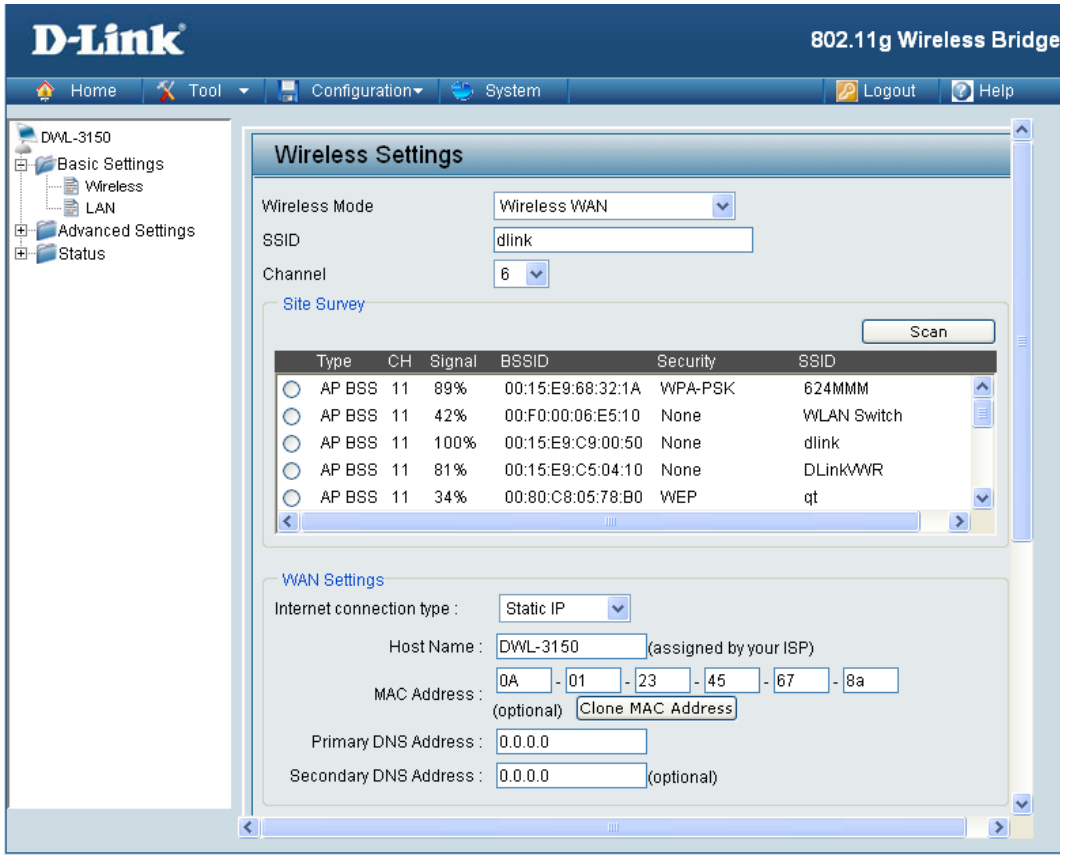
ISP Gateway Address: Enter the gateway IP address, typically a router.

MAC Address: Enter the MAC address of the network device you are configuring a DHCP Reservation for.

Clone MAC Address: Copy the MAC address of the network device you are configuring a DHCP Reservation for.

Primary DNS Server: Enter your primary DNS IP address.

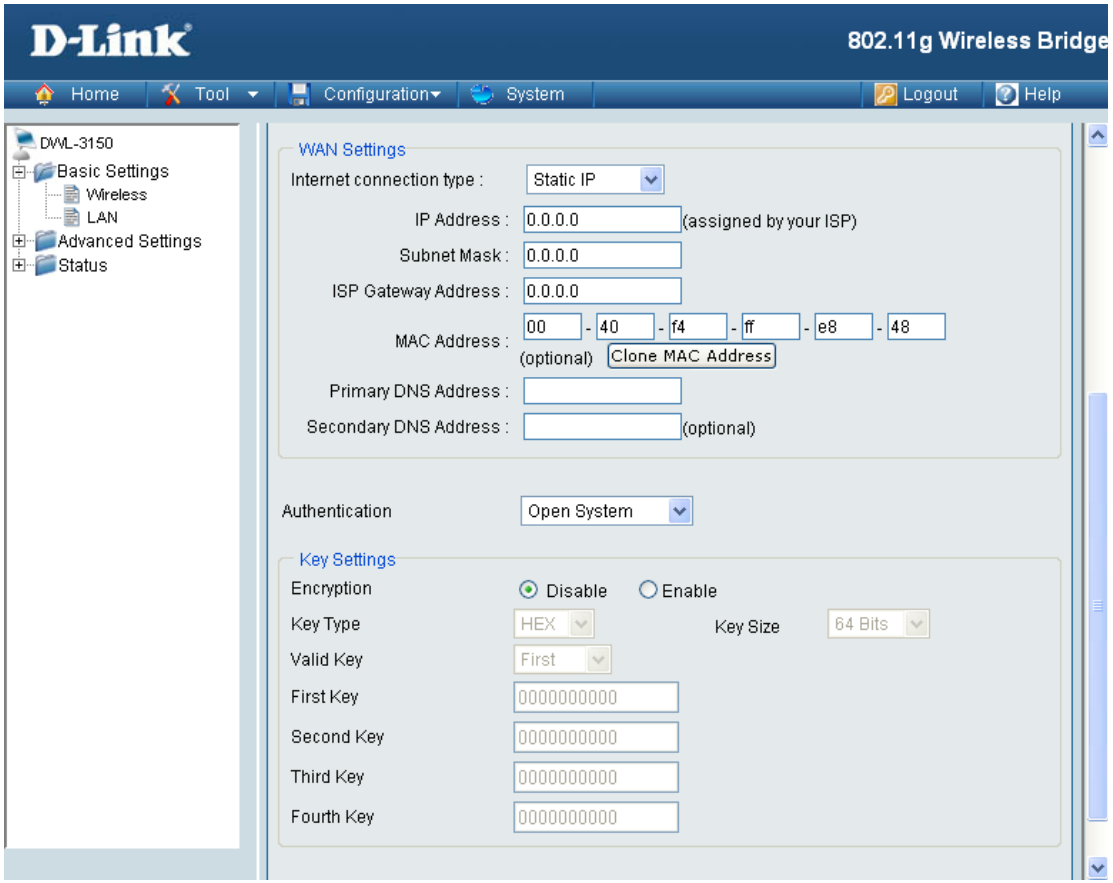
Secondary DNS Server: Enter your secondary DNS IP address.



No Security

Authentication: For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected.

Encryption: Select Disable if you choose to not have security.



Open System (64 Bits or 128 Bits)

Authentication: For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

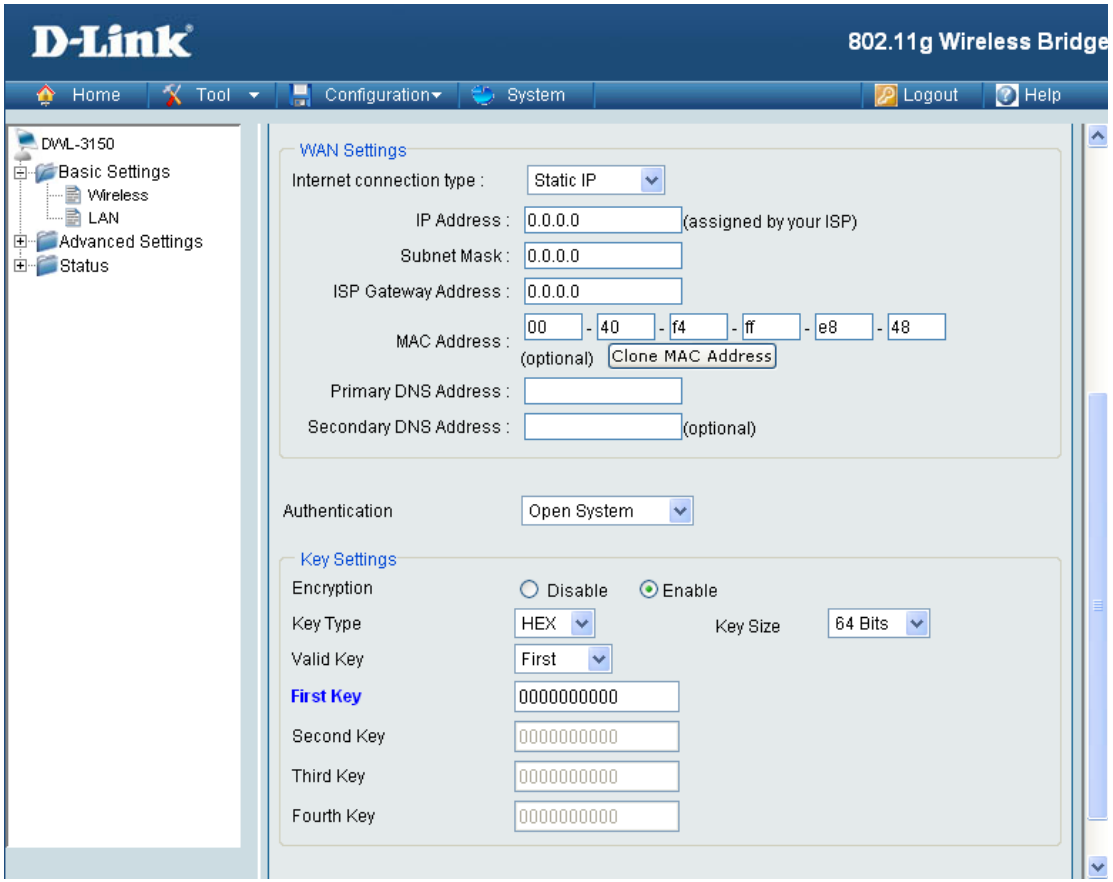
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Shared Key (64 Bits or 128 Bits)

Authentication: For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

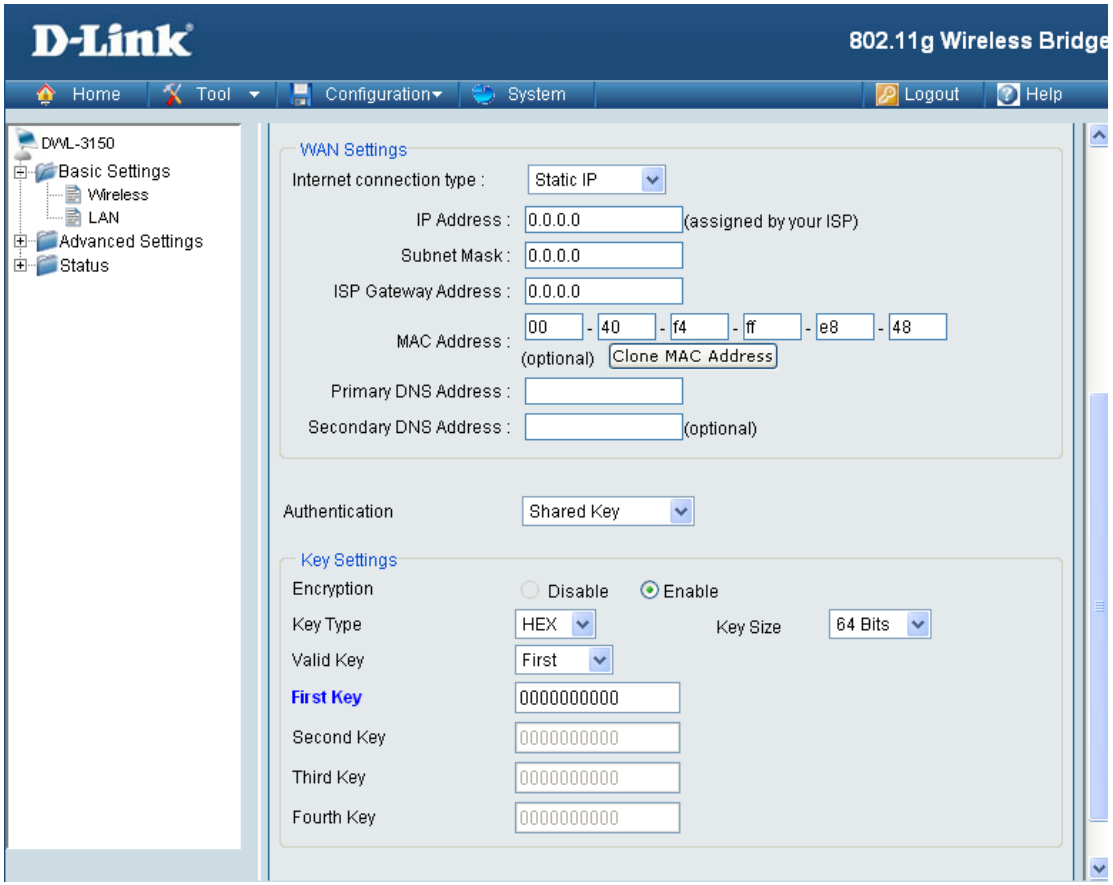
Encryption: Select Enabled to enable WEP encryption.

Key Type: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

Valid Key: Select the 1st through the 4th key to be the active key.

First through Fourth Key: Input up to four keys for encryption. You will select one of these keys in the valid key field.



Note: *Hexadecimal digits consist of the numbers 0-9 and the letters A-F.*
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

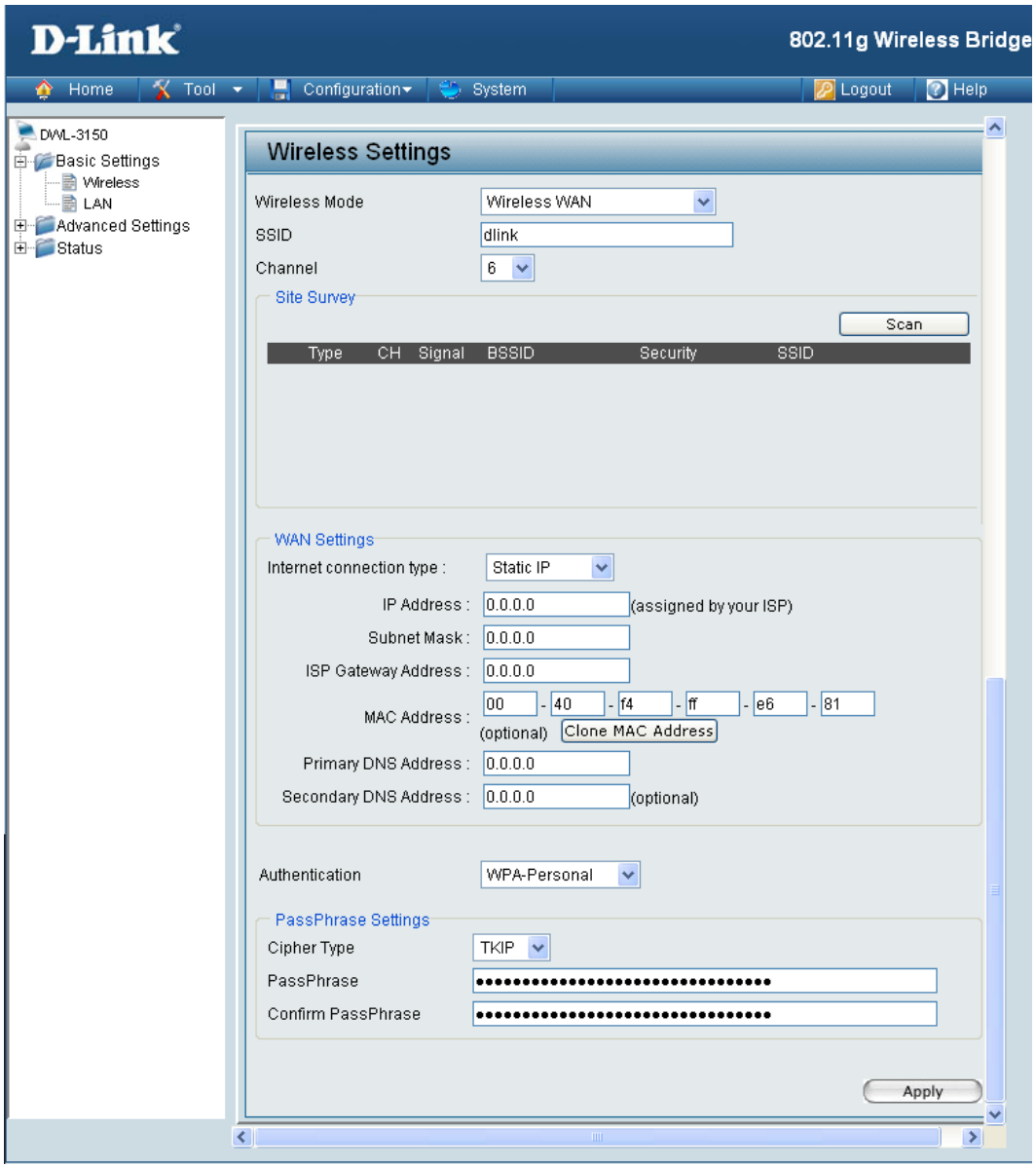
WPA & WPA2 Personal

Authentication: Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

Cipher Type: Select TKIP or AES from the pull-down menu.

PassPhrase: Enter a passphrase. The passphrase is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.

Confirm PassPhrase: Re-enter the passphrase once more for confirmation.



WPA & WPA2 Enterprise

Authentication: Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

EAP Type: Select TLS, TTLS or PEAP from the pull-down menu.

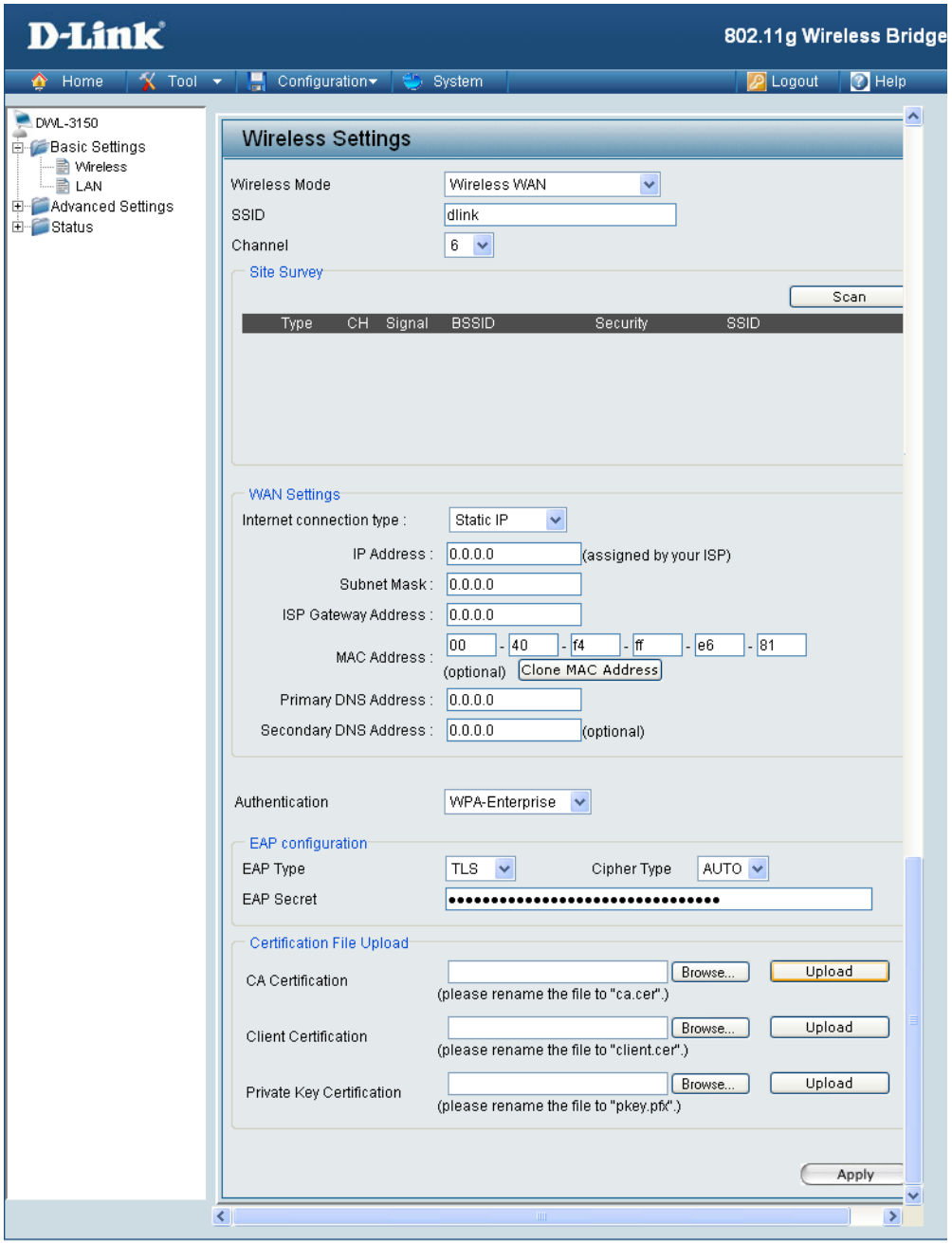
Cipher Type: Select TKIP or AES from the pull-down menu.

EAP Secret: Client and server authenticate each other using digital certificates. Client generates a pre-master secret key by encrypting a random number with the server's public key and sends it to the server.

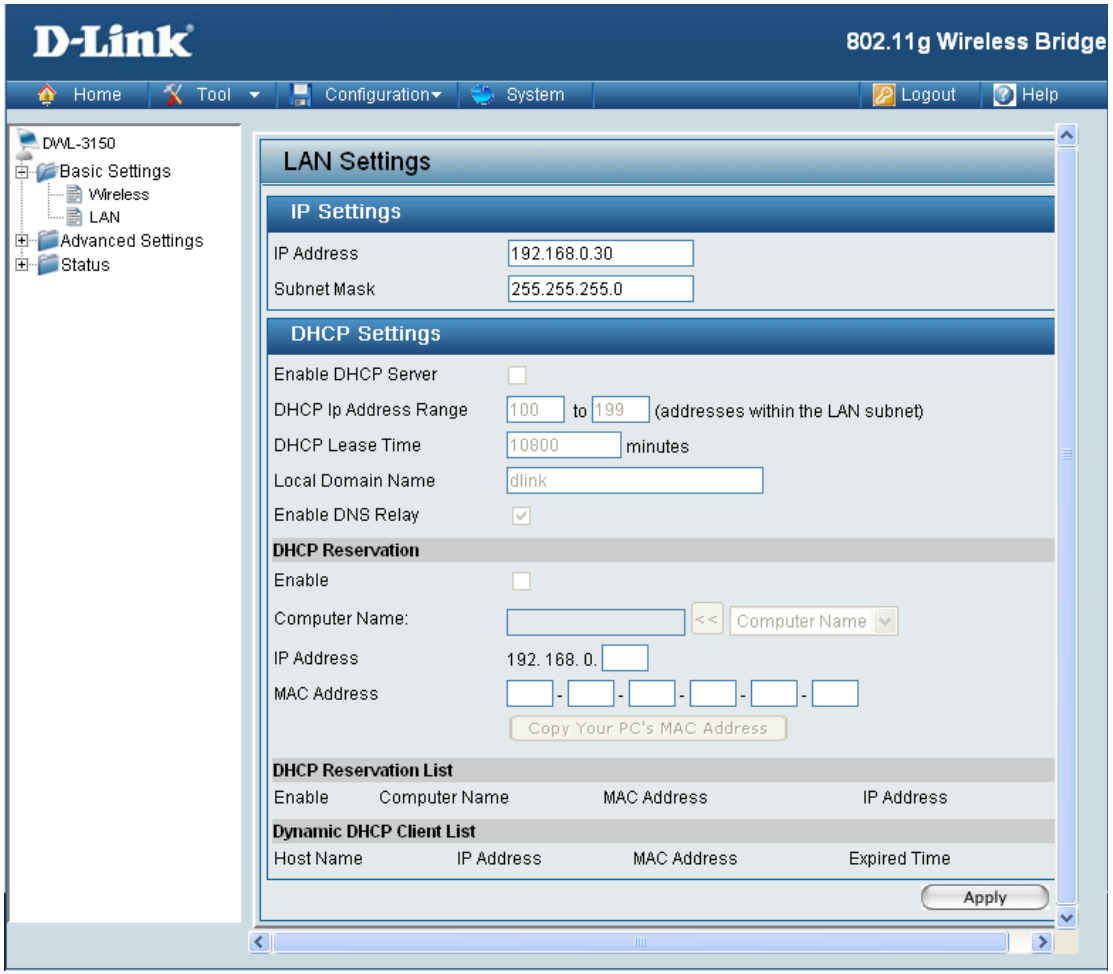
CA Certification: Certificate Authority (Ex: Microsoft Certification, Bank Cerification...etc). Upload the Client certificate for client recognition.

Client Certification: Client Authentication (Ex: The cerification from Radius Server use in client device).

Private Key Certification: EAP private key data use in wireless connection.



LAN



IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Enable DHCP Server: DHCP stands for Dynamic Host Control Protocol. The DHCP server assigns IP addresses to devices on the network that request them. These devices must be set to “Obtain the IP address automatically”. By default, the DHCP Server is enabled on the DWL-3150. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP IP Address Range: The starting and ending IP address for the DHCP server’s IP assignment.

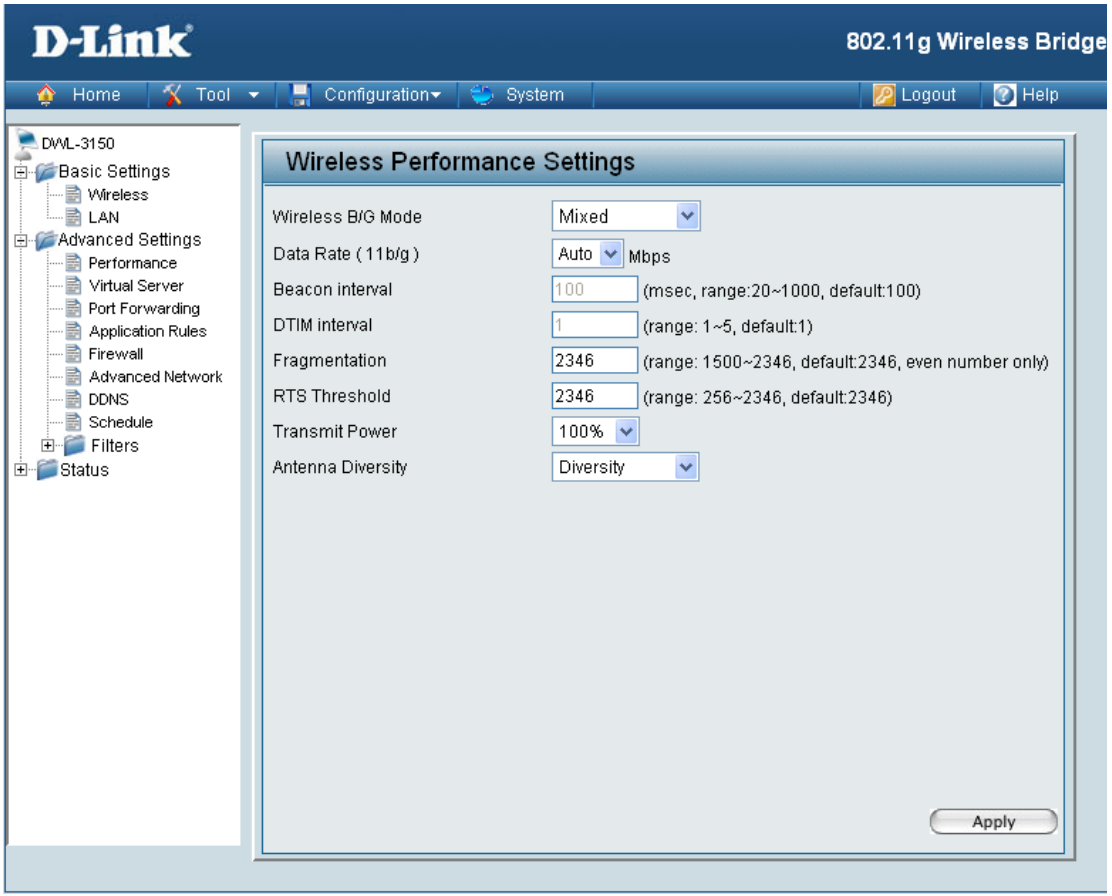
DHCP Lease Time: The Lease Time is the period of time before the DHCP server will assign new IP addresses.

Local Domain Name: Enter the domain name, if applicable. (An example of a domain name is: www.dlink.com.)

Enable DNS Relay: When DNS Relay is enabled, DHCP clients of the router will be assigned the router’s LAN IP address as their DNS server. All DNS requests that the router receives will be forwarded to your ISPs DNS servers. When DNS relay is disabled, all DHCP clients of the router will be assigned the ISP DNS server.

Enable DHCP Reservation:	DHCP Reservations allow the router to assign the same IP address to a specific device on your network. The specified device will get the same DHCP IP address information every time it is turned on or requests an IP address. No other computer on your network will receive the specified static DHCP address. DHCP Reservations are very helpful when used for server computers on your network that are hosting applications such as Web and FTP. Select Enabled to configure a DHCP Reservation. If you wish to disable this DHCP Reservation at a later date, click the edit icon next to the entry in the DHCP Reservation List, select the Disabled radio button, and then click Save Settings. Client computers with DHCP Reservations will have their information displayed in the DHCP Reservations List. The table will show the Host Name, IP Address, MAC Address, and Expired Time of the DHCP lease for each client computer.
Computer Name:	The Hostname of the network device you are configuring DHCP Reservation for.
IP Address:	Enter the last octet of the IP address that you are configuring the network device to always obtain.
MAC Address:	Enter the MAC address of the network device you are configuring a DHCP Reservation for.
DHCP Reservation List:	This is a list of the computers or other devices for which you have created reserved DHCP entries. You can enable and disable entries with the Enabled checkbox. A DHCP Reservation entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the “DHCP Reservations” section is activated for editing.
Dynamic DHCP Client List:	In this section you can see what LAN devices are currently leasing IP addresses.

Home > Advanced Settings Performance



Wireless B/G Mode: Select **Mixed**, **11g Only**, or **11b Only**.

Data Rate (11b/g): A pull-down menu to select the maximum wireless signal rate for the selected device(s).

Beacon Interval: Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of **100** is recommended.

DTIM Interval: DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages.

Fragmentation: This sets the fragmentation threshold (specified in bytes). Packets exceeding the value set here will be fragmented. The default is **2346**.

RTS Threshold: The RTS value should not be changed unless you encounter inconsistent data flow. The default value is **2346**.

Transmit Power: Choose **full**, **half (-3dB)**, **quarter (-6dB)**, **eighth (-9dB)**, **minimum power.**

Antenna Diversity: The DWL-3150 supports 2.4GHz radio with two antennas. Radio is connected to each antenna and supports auto diversity mode by default. This means that the access point will auto switch to the antenna with better RSSI value.

Diversity: The DWL-3150 will auto switch to the antenna with better RSSI value.

Left Antenna: The AP will not switch antenna and the radio will use the left antenna (when facing the AP) to transmit and receive packets.

Right Antenna: AP won't switch antenna and the radio will use the right antenna (when facing the AP) to transmit and receive packets.

Virtual Server

Name: The name for the service being provided by the device on your LAN that uses the ports being opened.

IP Address: The server computer on the LAN network that the specified ports will be opened to.

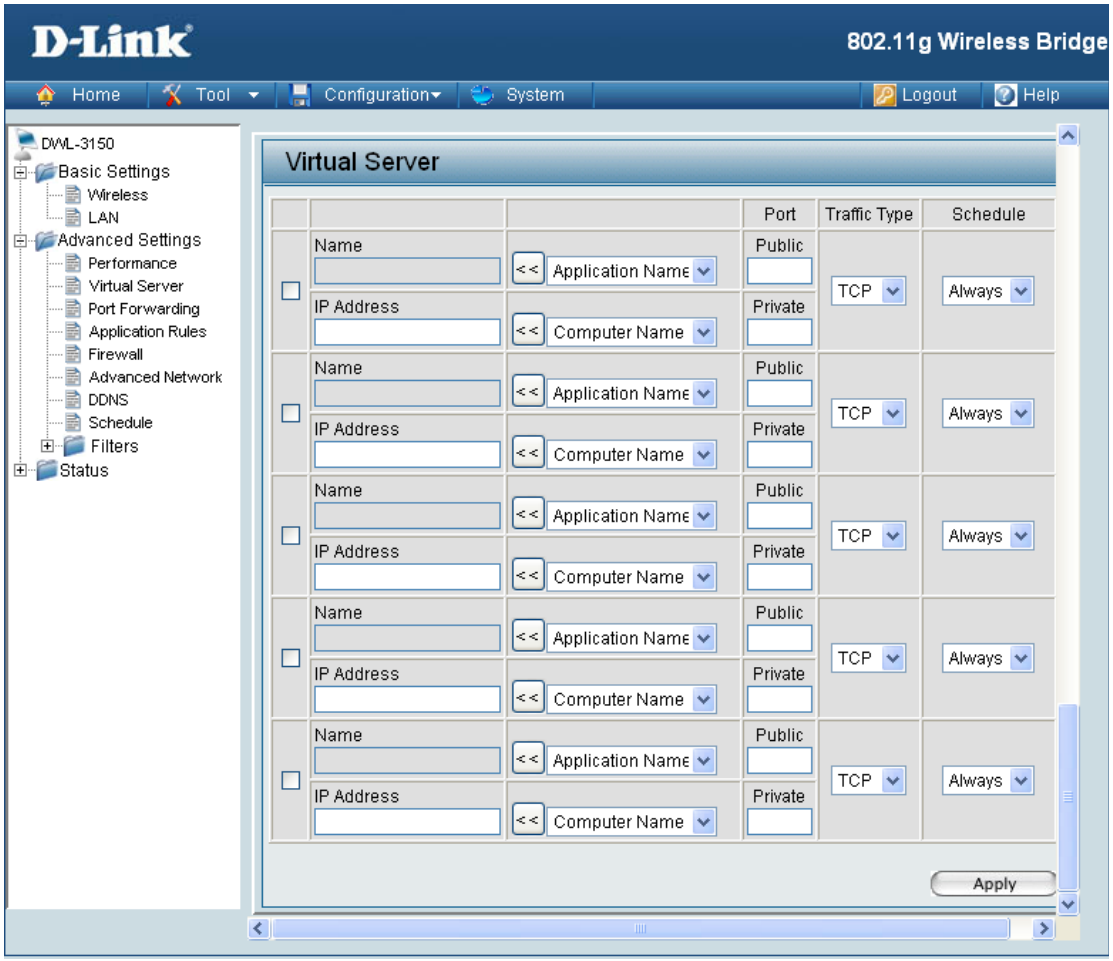
Application Name: This contains a list of pre-defined services.

Computer Name: This contains a list of the devices on your network, which have obtained an IP Address from the router.

Public Port: The port number that users on the Internet will use to access the defined service.

Private Port: The port number of the service being hosted by the server computer on the LAN.

Traffic Type: The protocol used by the service the device on your LAN is providing.



Schedule: The schedule of time when the Virtual Server Rule will be active. Schedules can be defined on the Tools>Schedules page

Port Forwarding

Name: The name for the service being provided by the device on your LAN that uses the ports being opened.

IP Address: The server computer on the LAN network that the specified ports will be opened to.

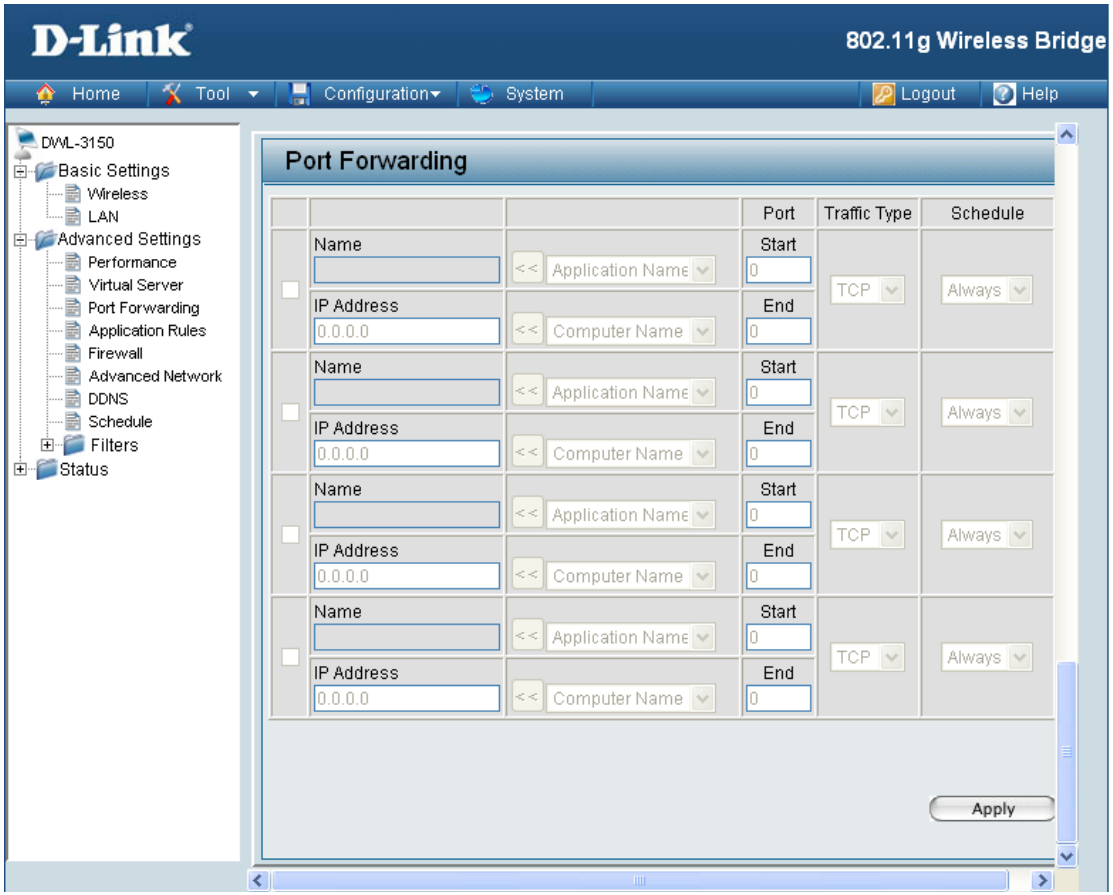
Application Name: This contains a list of pre-defined services.

Computer Name: This contains a list of the devices on your network that have obtained an IP Address from the router.

Port Start and End: The port number that users on the Internet will use to access the defined service.

Traffic Type: The protocol used by the service the device on your LAN is providing.

Schedule: The schedule of time when the Virtual Server Rule will be active. Schedules can be defined on the Tools > Schedules page.



Application Rules

Name: This is the name referencing the application.

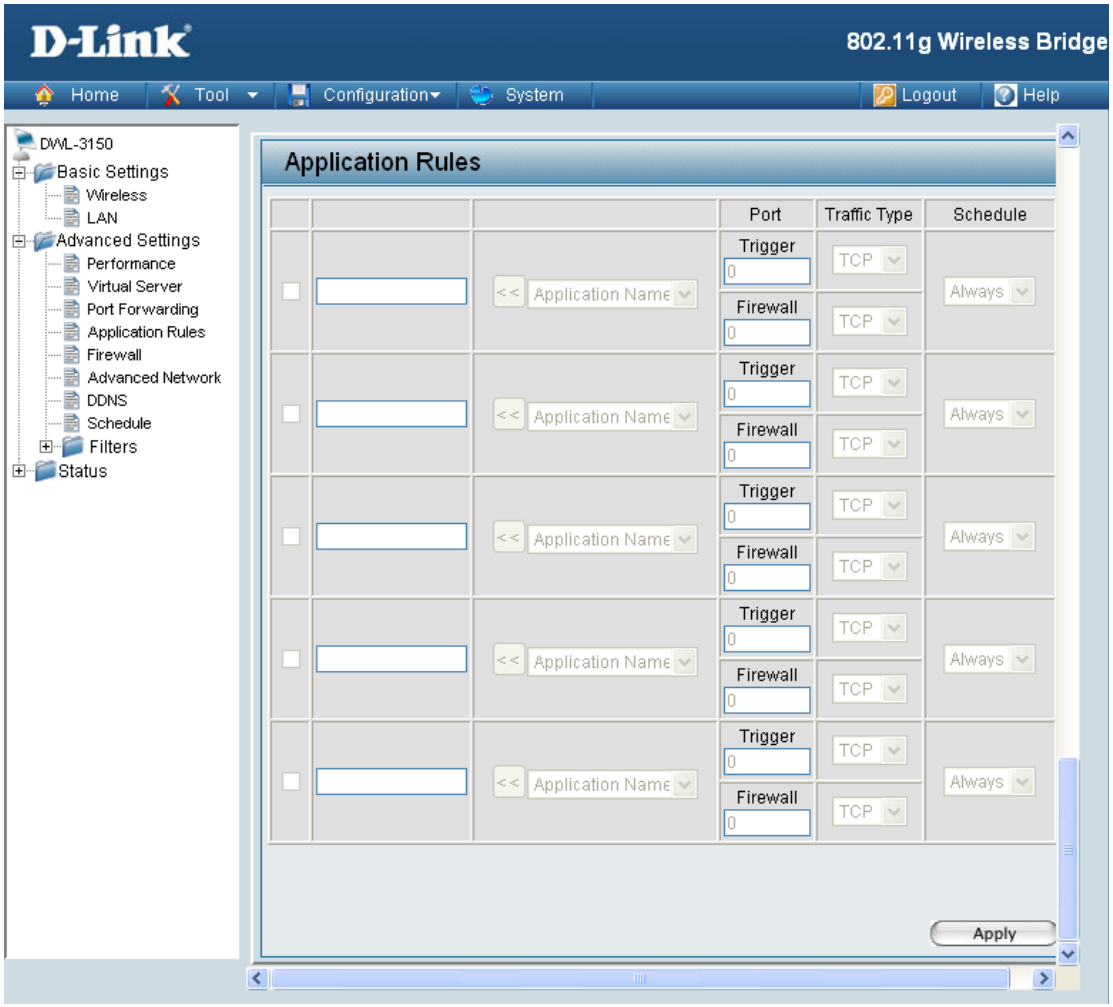
Trigger Port: This is the port used to trigger the application. It can be either a single port or a range of ports.

Traffic Type: This is the protocol used to trigger the application.

Firewall Port: This is the port number on the WAN 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.

Traffic Type: This is the protocol used for the application.

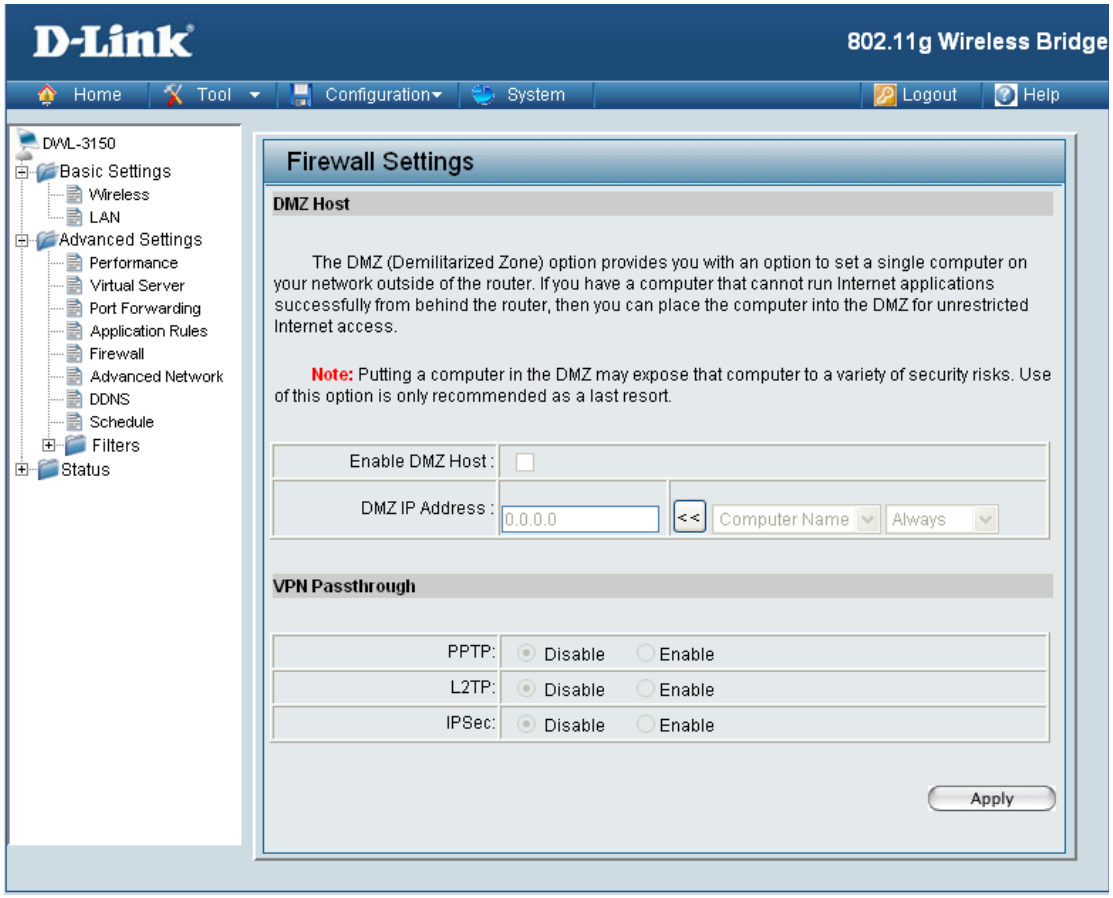
Schedule: The schedule of time when the Application Rule will be active. Schedules can be defined on the Tools > Schedules page.



Firewall

DMZ: Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

VPN Passthrough: The device supports VPN (Virtual Private Network) passthrough for PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security). Once VPN passthrough is enabled, there is no need to create any Virtual Server or Port Forwarding entries in order for outbound VPN sessions to establish properly. Multiple VPN connections can be made through the device. This is useful when you have many VPN clients on the Local Area Network.

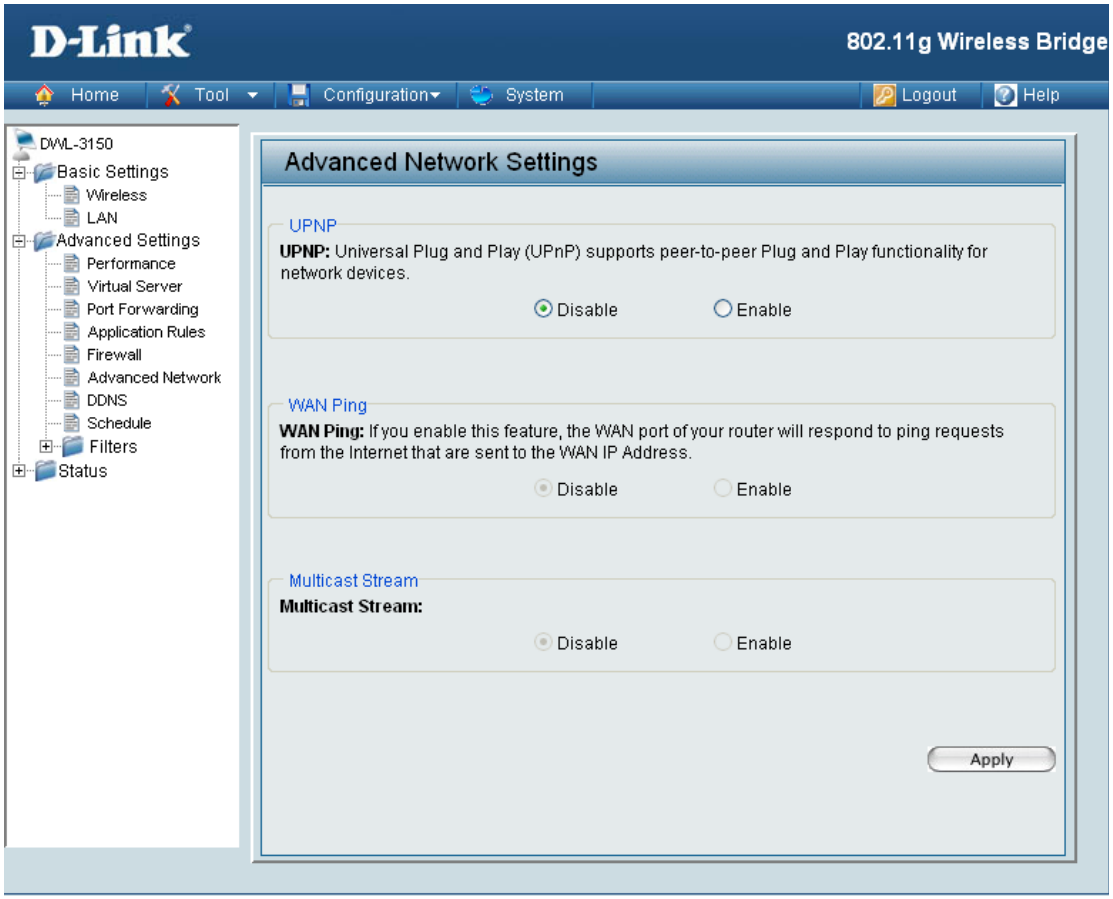


Advanced Network

UPnP: UPnP is short for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The DWL-3150 is an UPnP enabled device, 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 “Disable”.

WAN Ping: When you Enable WAN Ping respond, 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.

Multicast Stream: Enable this option to allow Multicast traffic to pass from the Internet to your network more efficiently.



DDNS

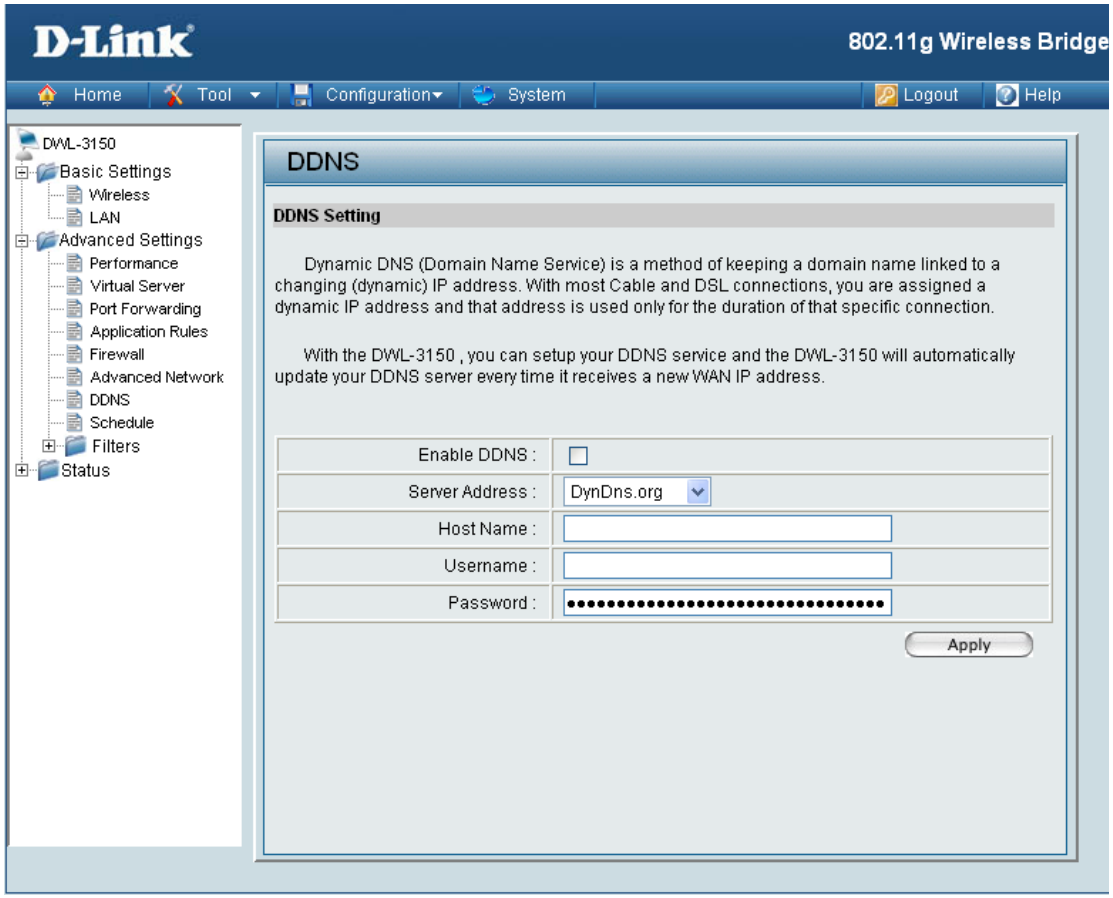
Enable DDNS: Dynamic DNS (Domain Name Service) is a method of keeping a domain name linked to a changing (dynamic) IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the DWL-3150, you can setup your DDNS service, in which the DWL-3150 will automatically update your DDNS server every time it receives a new WAN IP address.

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

Username: Enter the username for your DDNS account.

Password: Enter the password for your DDNS account



Schedule

Name: The name of the schedule being defined.

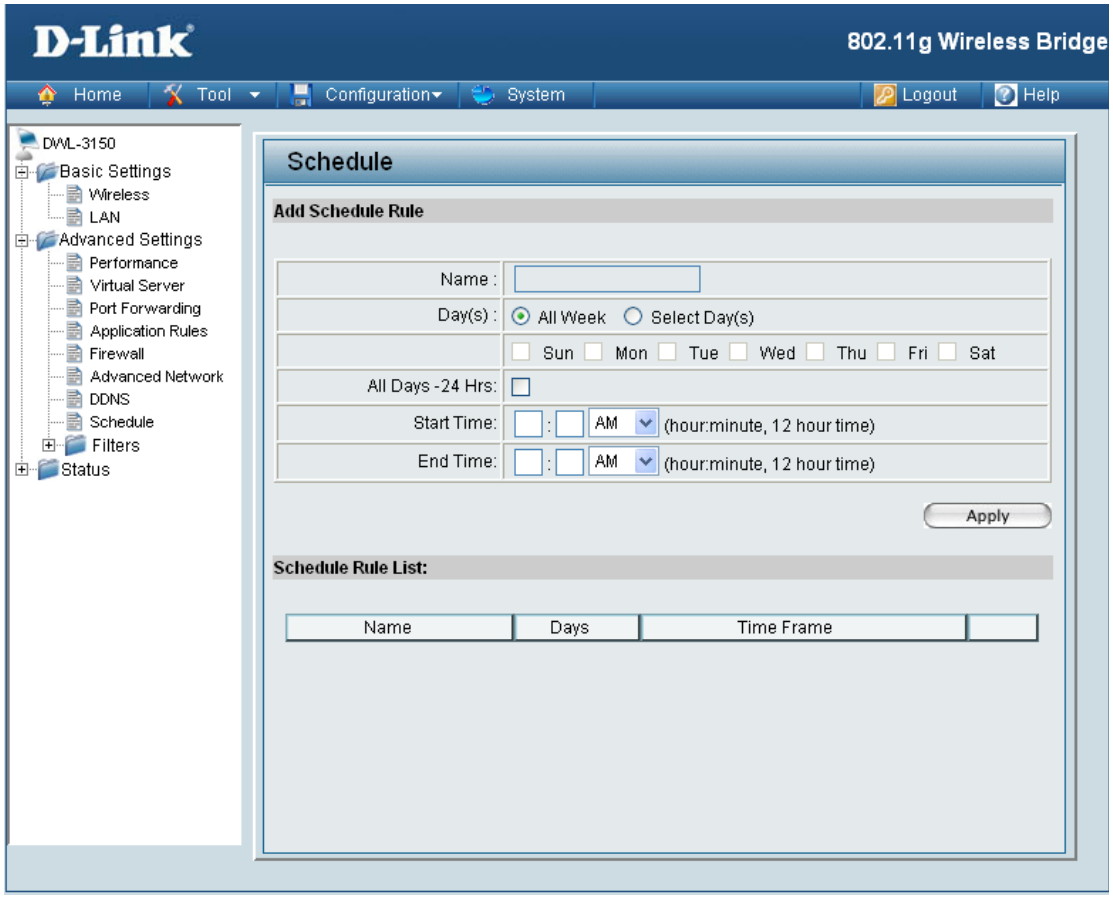
Day(s): Select a day, range of days, or select the All Week checkbox to have this schedule apply every day.

All Days - 24 Hrs: Check this box to have the schedule active the entire 24 hours on the days specified.

Start Time: Select the time at which you would like the schedule being defined to become active.

End Time: Select the time at which you would like the schedule being defined to become inactive

Schedule Rule List: This displays all the schedules that have been defined



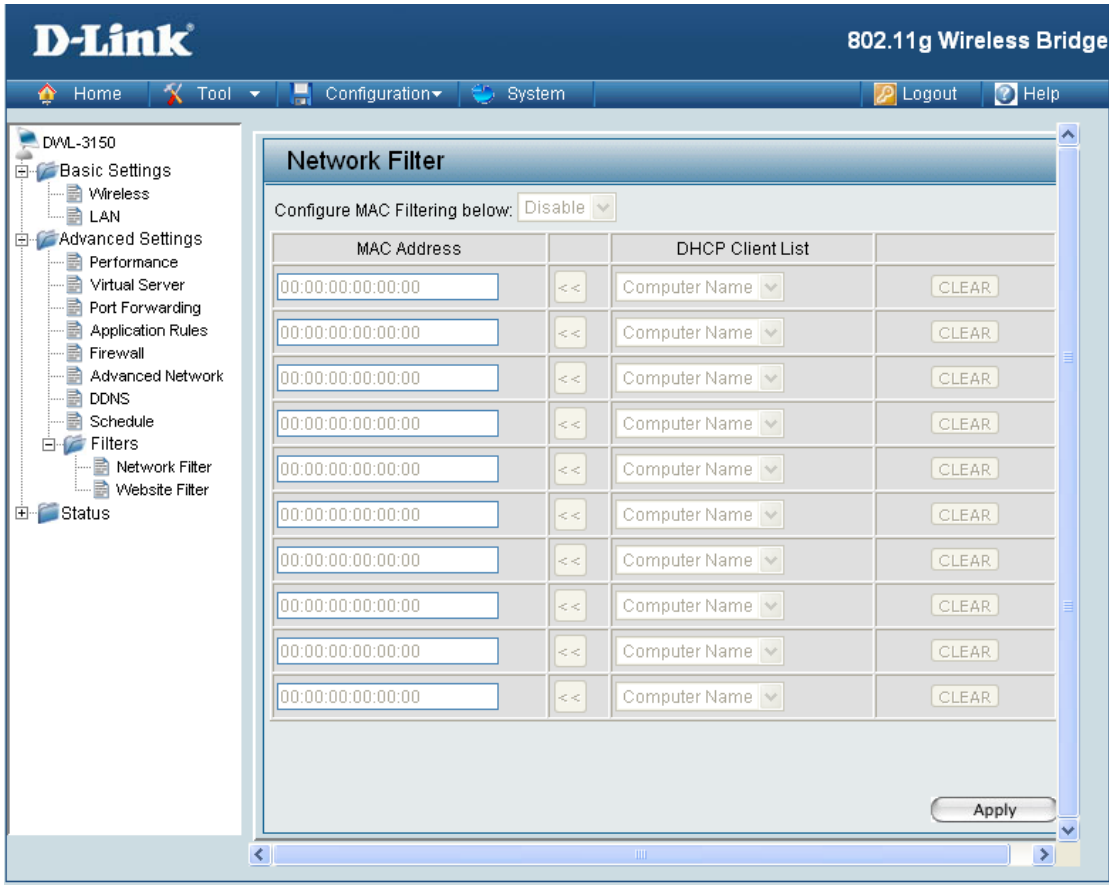
Filters

Network Filter

Configure MAC Filtering Below: Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the unit.

Select “Turn MAC Filtering ON and ALLOW computers with MAC address listed below to access the network” if you only want selected computers to have network access and all other computers not to have network access.

Select “Turn MAC Filtering ON and DENY computers with MAC address listed below to access the network” if you want all computers to have network access except those computers in the list.



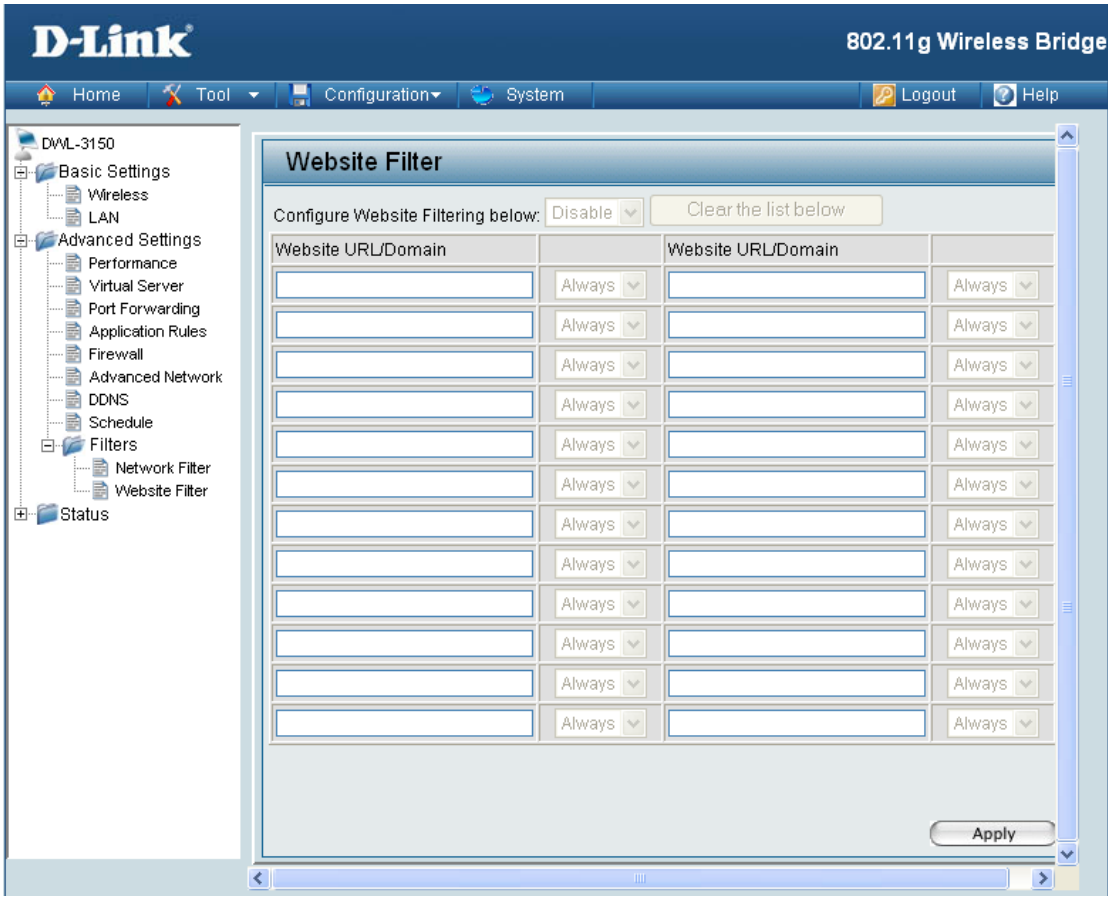
MAC 3Address: The MAC address of the network device to be added to the MAC Filter List.

DHCP Client List: DHCP clients will have their hostname in the Computer Name drop down menu. You can select the client computer you want to add to the MAC Filter List and click arrow button. This will automatically add that computer’s MAC address to the appropriate field.

Clear: This will remove the MAC Address on the corresponding line from the MAC Filtering table.

Website Filter

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



Example 1:

If you wanted to block LAN users from any website containing a URL pertaining to shopping, you would need to select “Turn Website Filtering ON and DENY” computers access to ONLY these sites, and then enter “shopping” into the Website Filtering Rules list. Sites like these will be denied access to LAN users because they contain the keyword in the URL.

- http://shopping.yahoo.com
- http://www.msn.com/search/shopping-spree.html

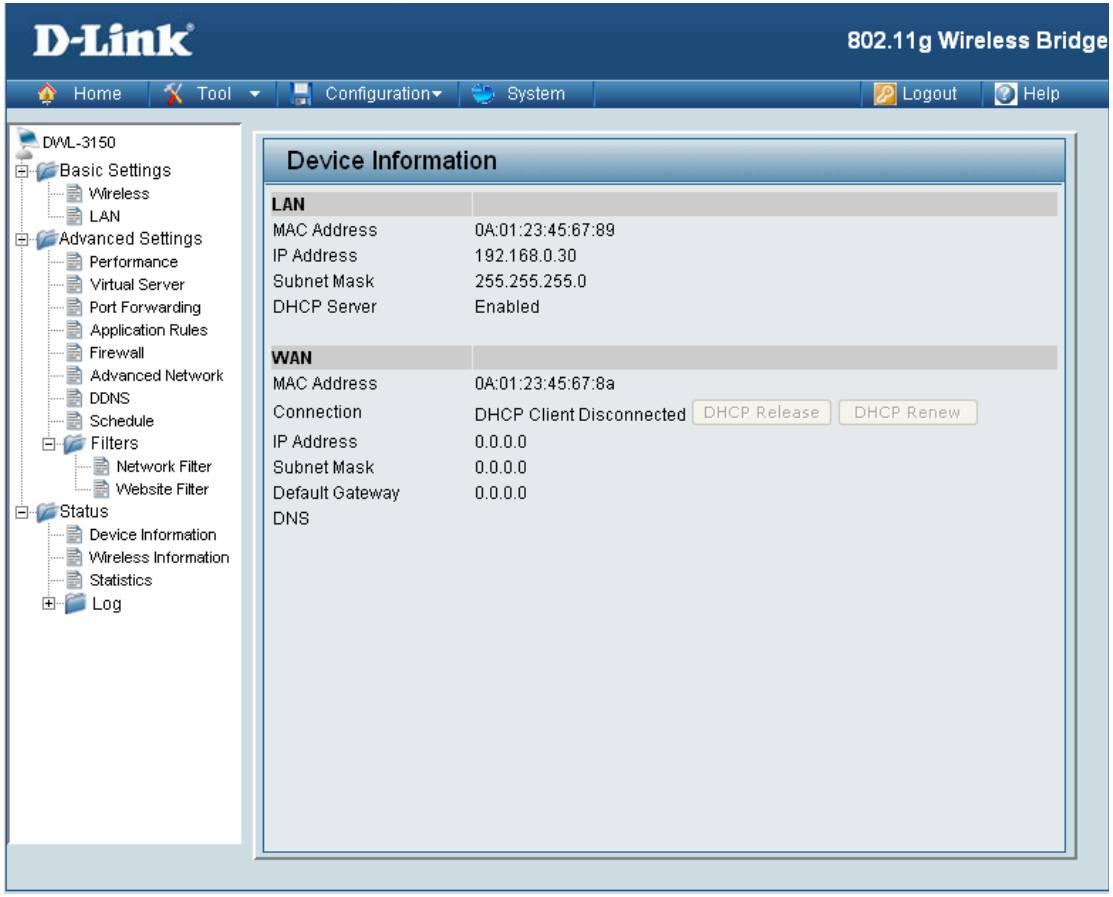
Example 2: If you want your children to only access particular sites, you would then choose “Turn Website Filtering ON and ALLOW computers access to ONLY these sites and then enter in the domains you want your children to have access to.

- Disney.com
- Cartoons.com

Home > Status
Device Information

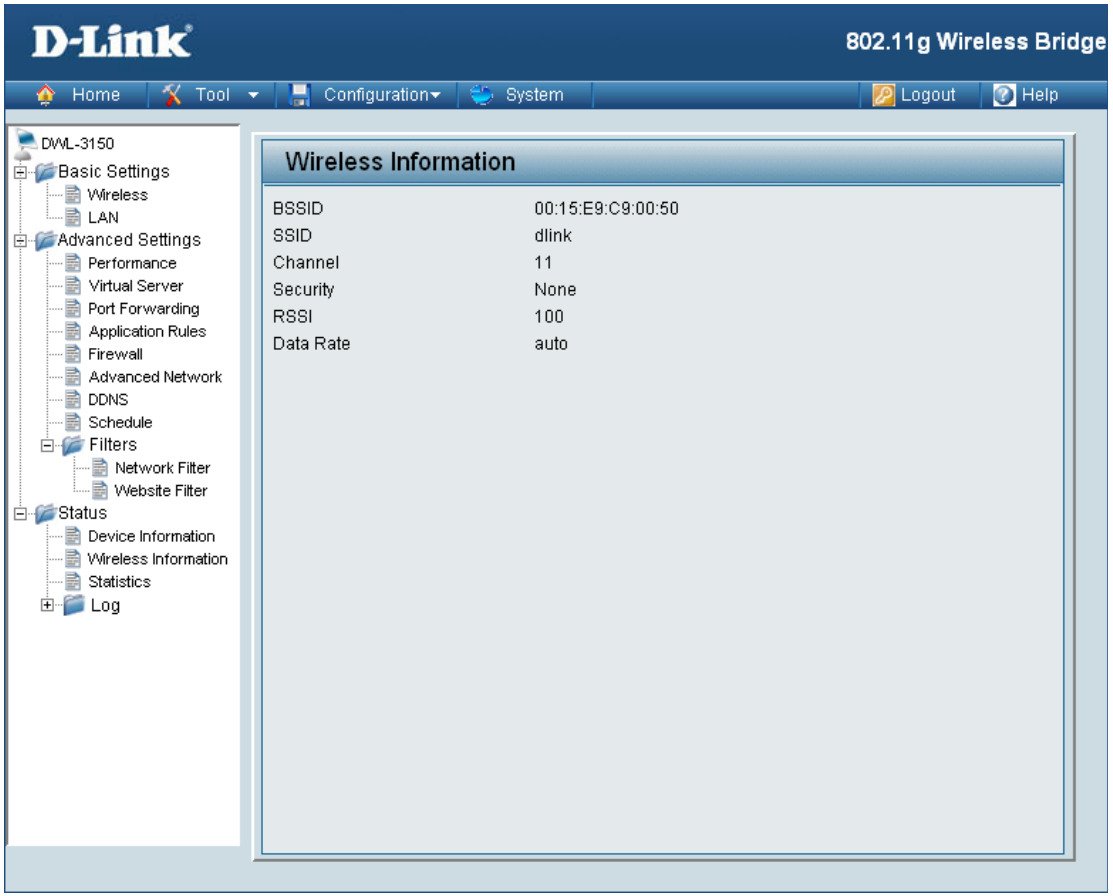
LAN (Local Area Network) - This displays the MAC Address of the Ethernet LAN interface, the IP Address and Subnet Mask of the LAN interface, and whether or not the router's built-in DHCP server is Enabled or Disabled.

WAN (Wide Area Network) - This displays the MAC Address of the WAN interface, as well as the IP Address, Subnet Mask, Default Gateway, and DNS server information that the DWL-3150 has obtained from your ISP. It will also display the connection type (Dynamic, Static, or PPPoE) that is used establish a connection with your ISP. If the router is configured for Dynamic, then there will be buttons for releasing and renewing the IP Address assigned to the WAN interface. If the router is configured for PPPoE, there will be buttons for connecting and disconnecting the PPPoE session.



Wireless Information

This displays the SSID, Channel, and whether or not Encryption is enabled on the Wireless interface.

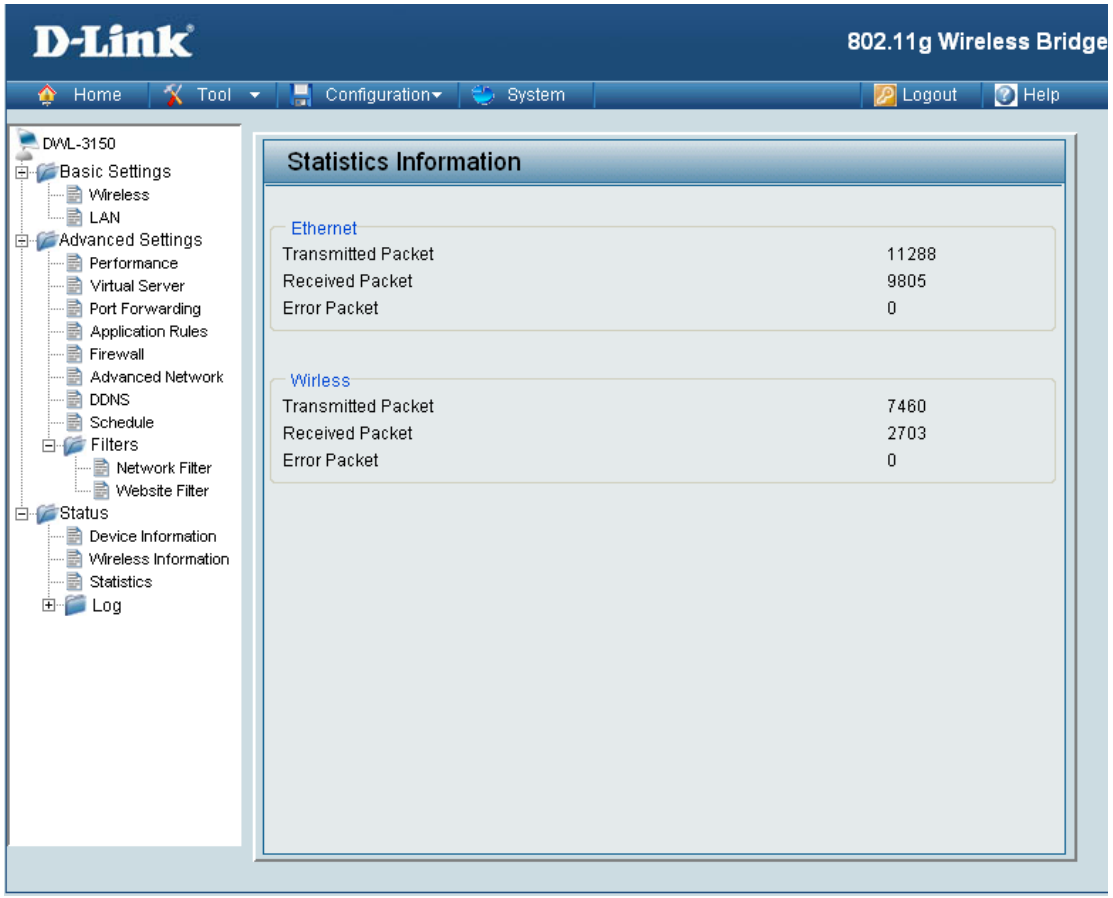


Statistics

The DWL-3150 keeps statistic of the data traffic that it handles. You are able to view the amount of packets that the device has received and transmitted on the Wireless WAN, LAN, and Wireless interfaces.

Refresh: Click this button to update the counters.

Reset: Click this button to clear the counters. The traffic counter will reset when the device is rebooted.



Log

View Log

The DWL-3150 keeps a running log of events and activities occurring on it at all times. The log will display up to 500 recent logs. Newer log activities will overwrite the older logs. You can save the log files or have them emailed to you by clicking on the Log Settings button. This is recommended as the logs are cleared every time the router is rebooted.

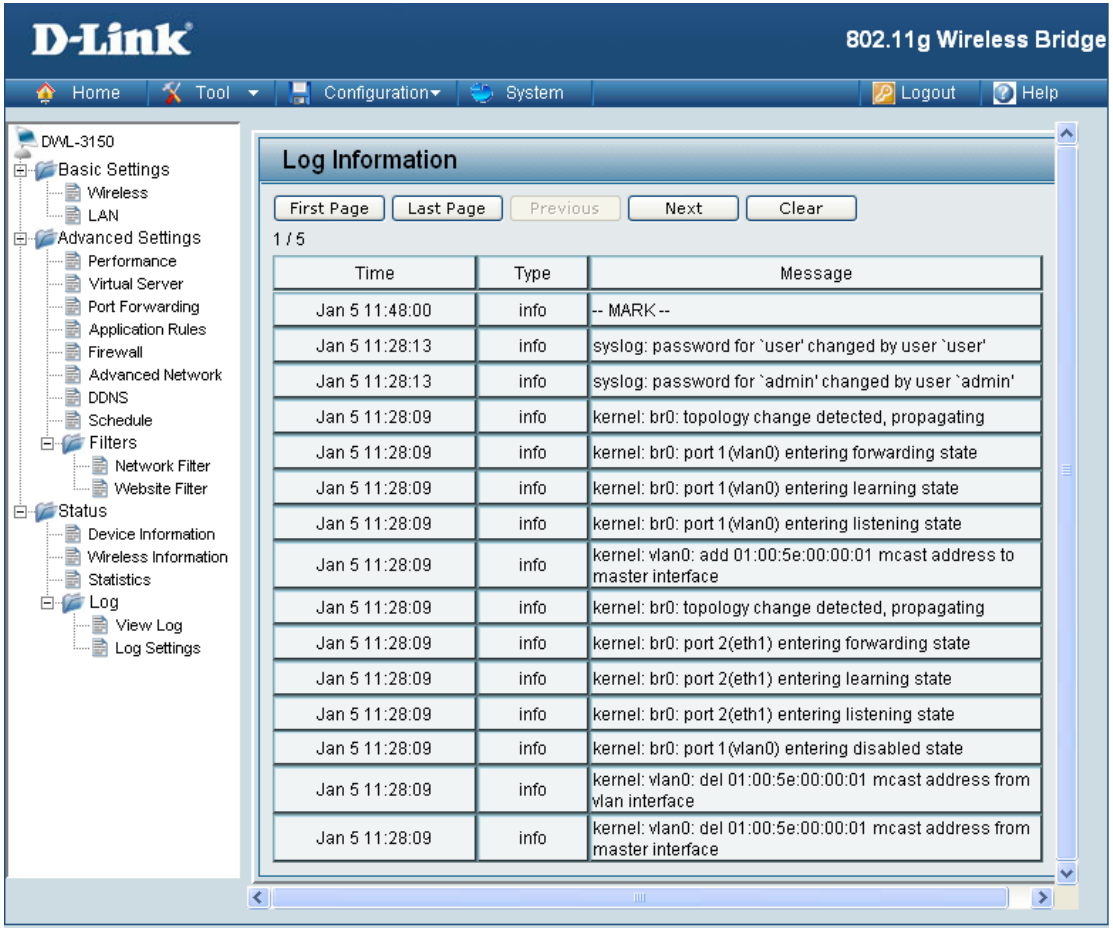
First Page: Click this button to go to the first page of the log.

Last Page: Click this button to go to the last page of the log.

Previous: Moves back one log page.

Next: Moves forward one log page.

Clear: Clears the logs completely.



Log Settings

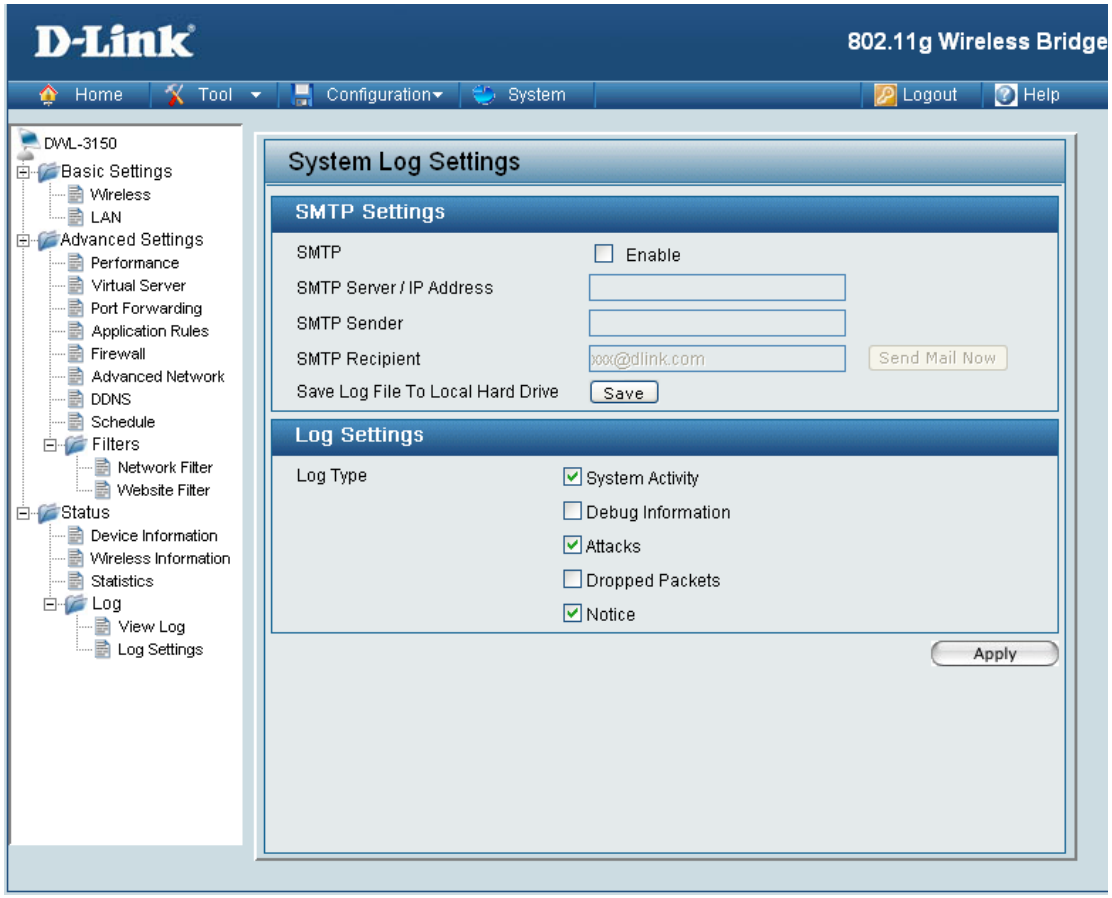
SMTP Server/IP Address: The address of the SMTP (Simple Mail Transfer Protocol) server that will be used to send the logs.

SMTP Sender: The email address the logs will be sent from.

SMTP Recipient: The email address the logs will be sent to. Click on Send Mail Now to send the email.

Save Log File to Local Hard Drive: Click this button to save the log entries to a text file.

Log Type: Select the type of information you would like the DWL-3150 to log.



Tool
Administrator Settings

Limit Administrator IP: Enter an IP address that will be allowed for the administrator to login. Enter the 2nd IP address that will be allowed for the administrator to login.

User Name: You can customize user name as an administrator of DWL-3150. The default username is “admin” with no password configured.

Old Password: Enter the old password.

New Password: Enter a password in this filed. The password is case-sensitive. “A” is a different character than “a.” The length should be between 0 and 12 characters.

Confirm New Password: Type the password again to confirm it.

Console Settings Status: Enable or disable console.

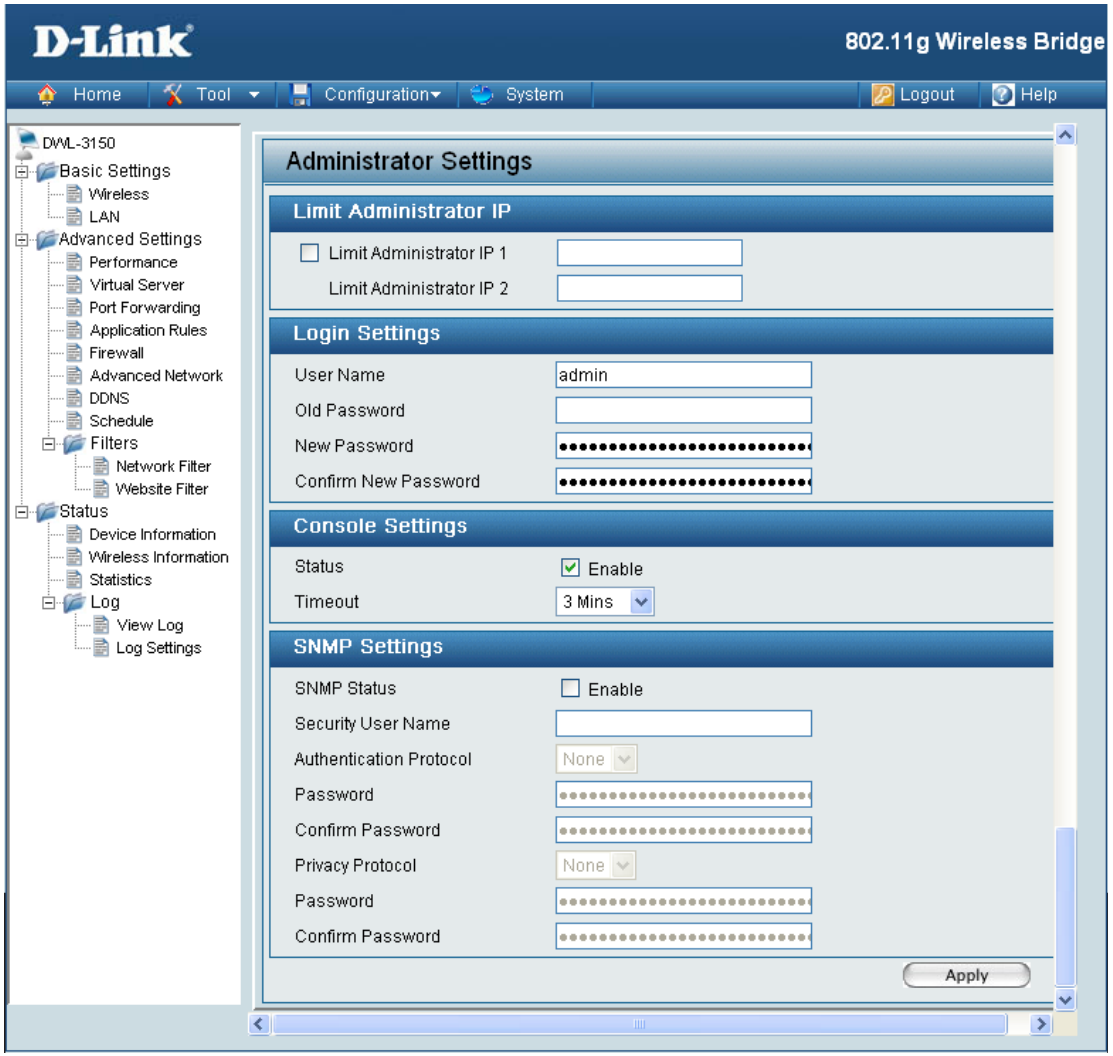
Timeout: Select the time out period.

SNMP Status: Enable or disable SNMP.

Security User Name: Enter the security user name.

Authentication Protocol: Choose MD5 or SHA1.

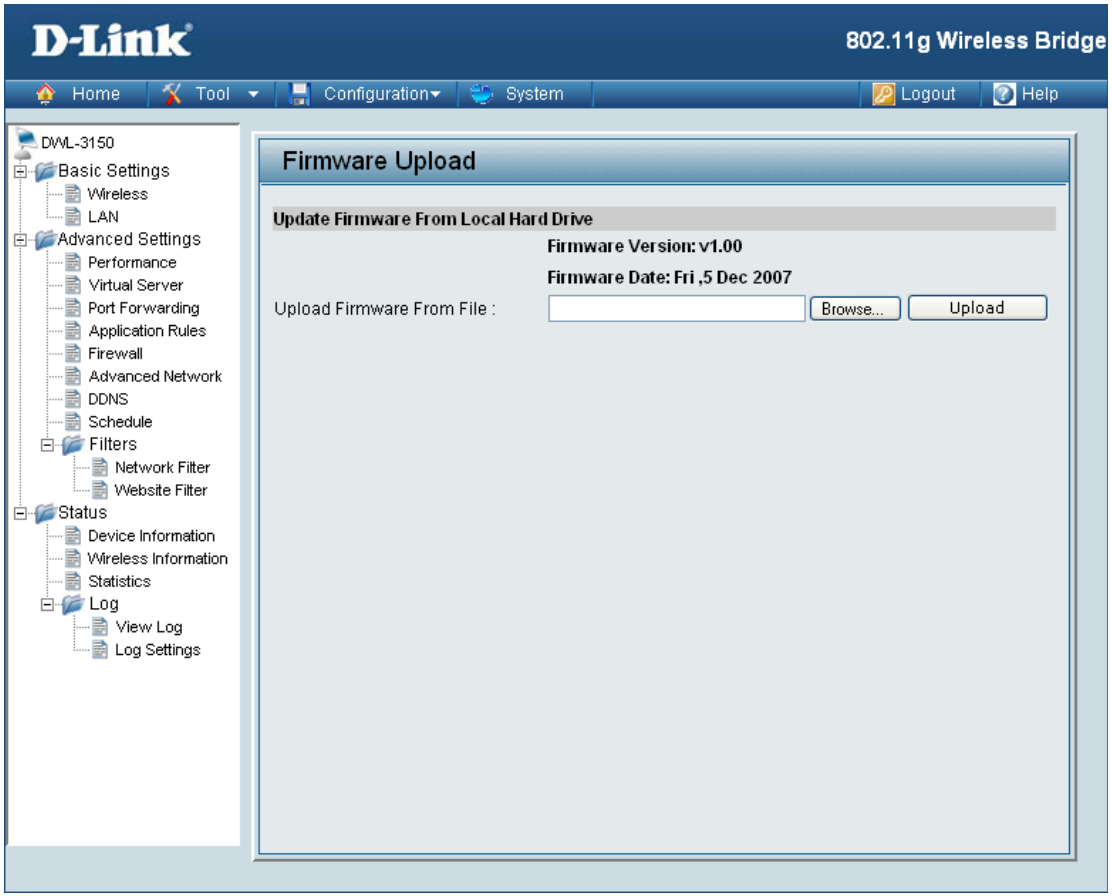
Privacy Protocol: Choose DES or AES.



Firmware Upgrade

Upload Firmware From File:

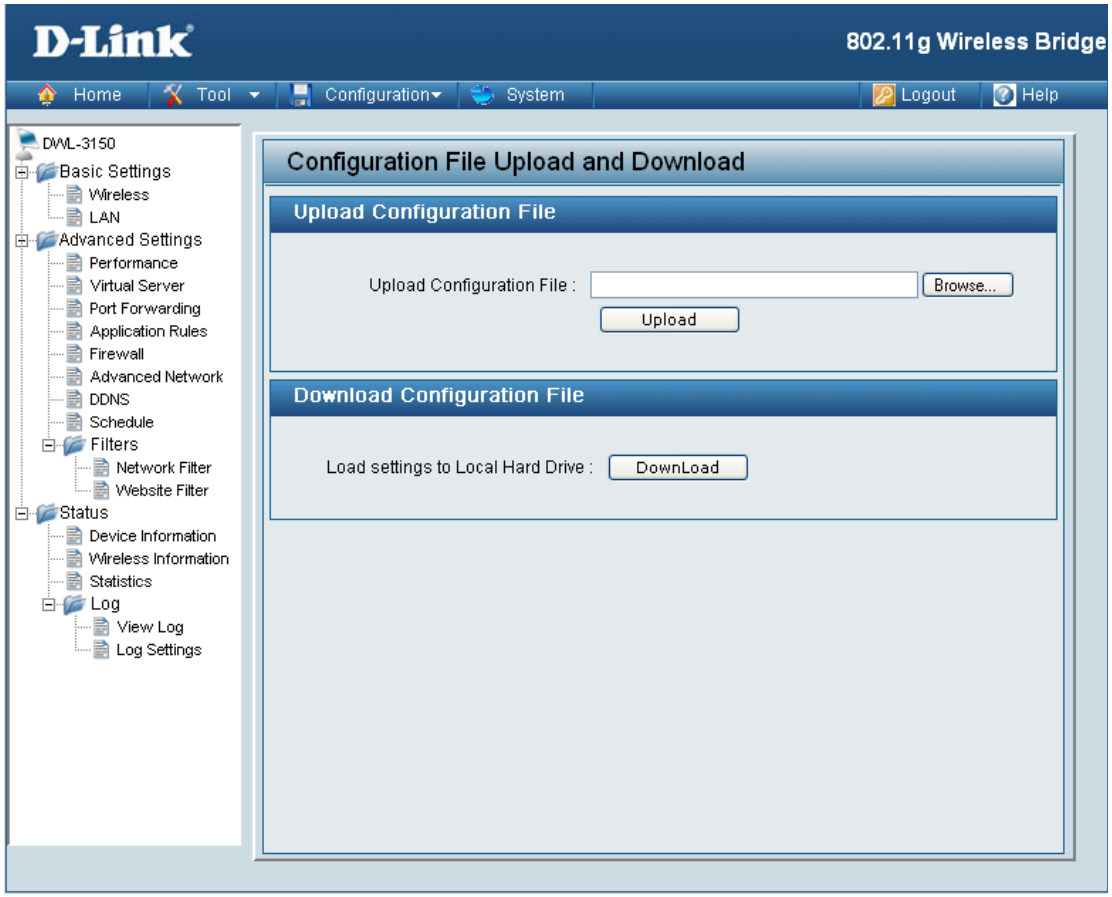
You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on Browse to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade. Please check the D-Link support site for firmware updates at http://support.dlink.com/.



Configuration File Upload and Download

Upload Configuration File: Browse to the saved configuration file you have in local drive and click open and upload to update the configuration.

Load Settings to Local Hard Drive: Click download to save the current configuration file to your local disk. Note that if you save one configuration with administrator's password now, after reset your, and then update to this saved configuration file, the password will be gone.



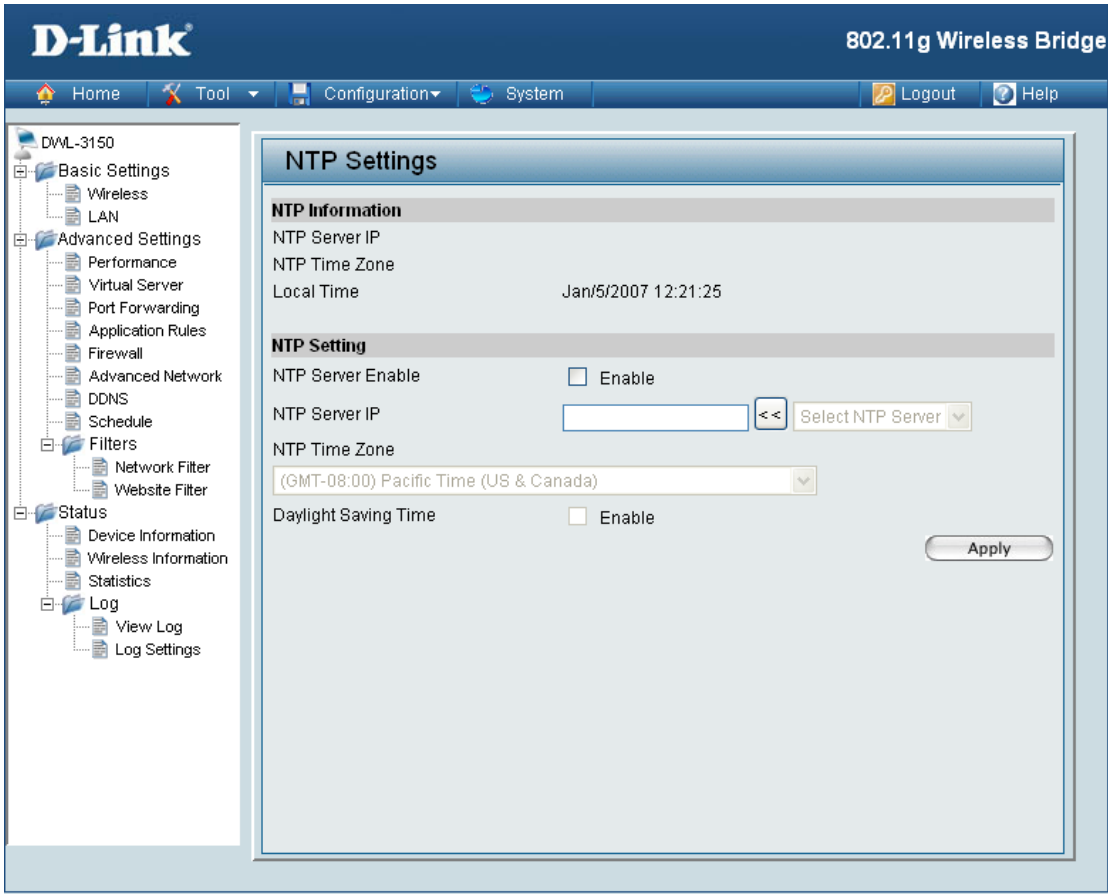
NTP Settings

NTP Information: Displays the current NTP settings.

NTP Server IP: Enter the NTP server IP, or choose from the drop-down menu.

NTP Time Zone: Select your time zone from the drop-down menu.

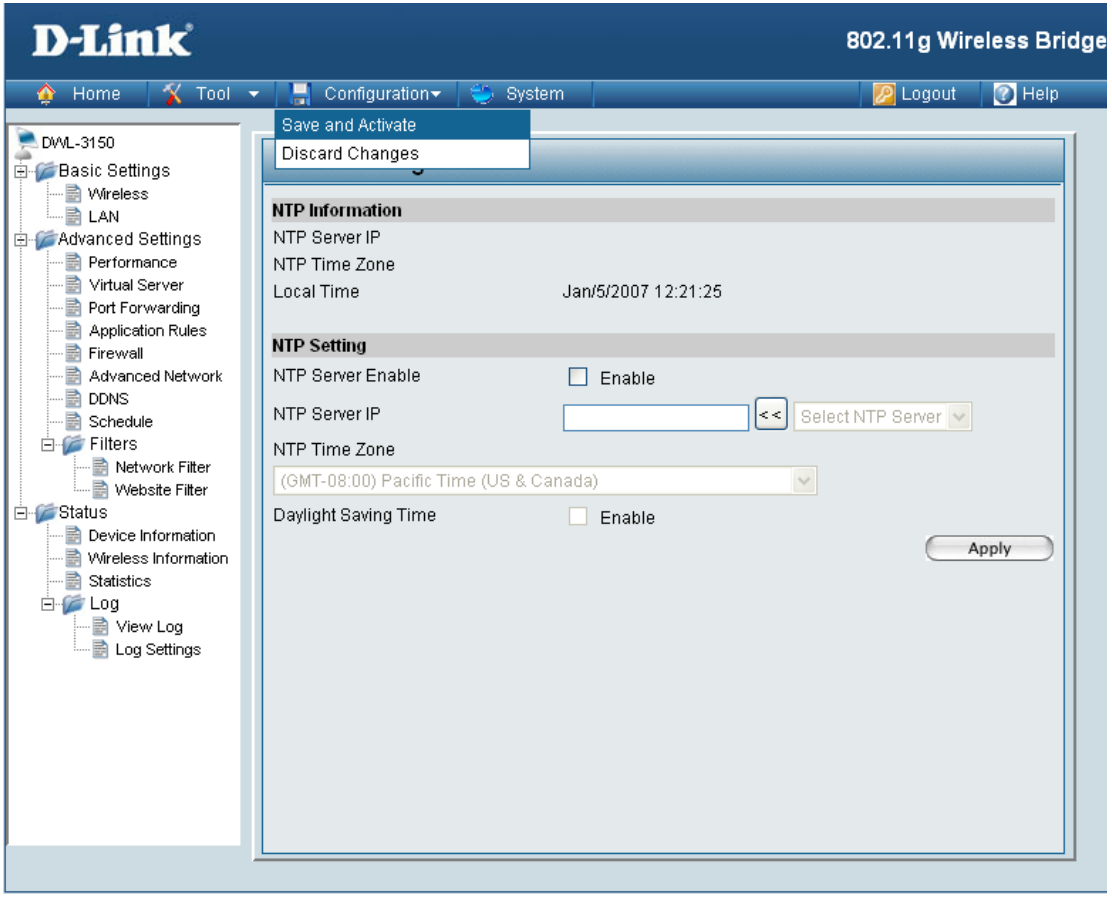
Daylight Saving Time: Check the box to enable daylight savings time.



Configuration
Save and Activate

Clicking Save and Activate will save and activate all changes made to the configuration and reboot the system.

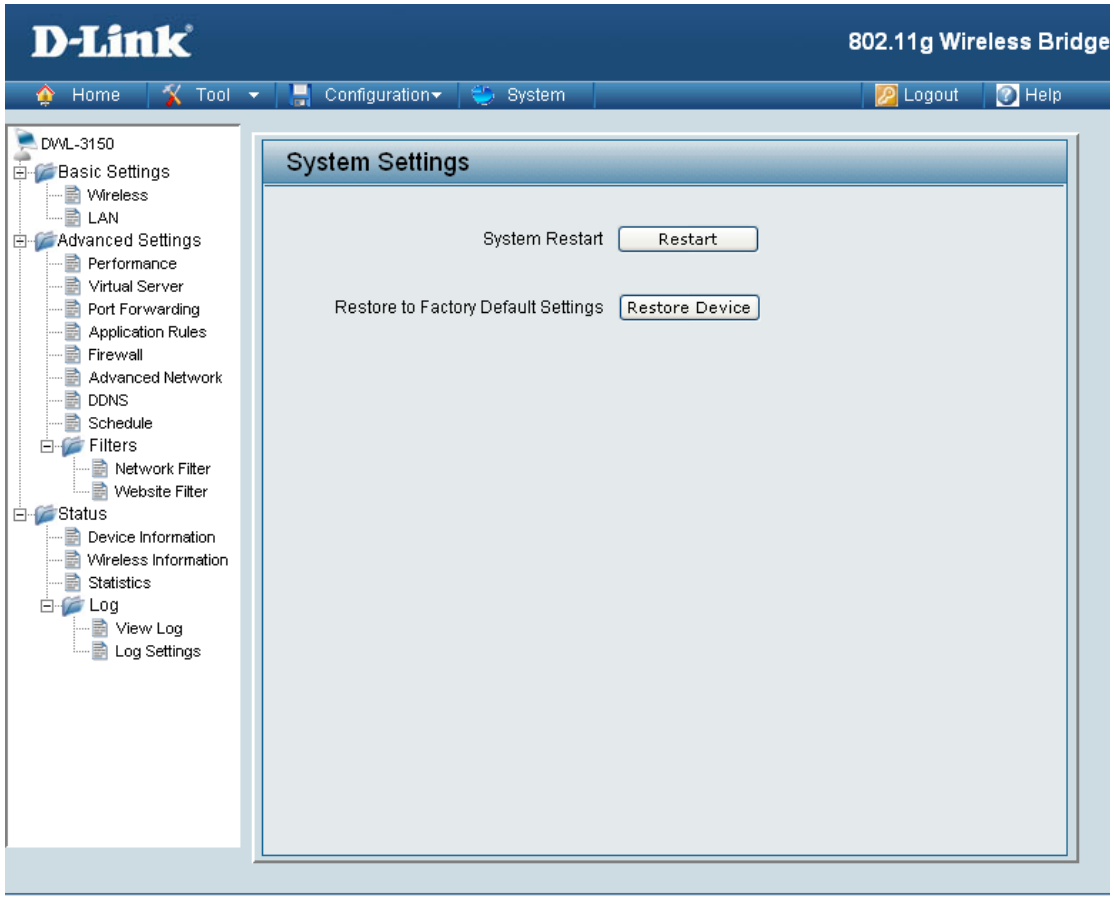
Clicking Discard Changes will discard all changes made to the configuration.



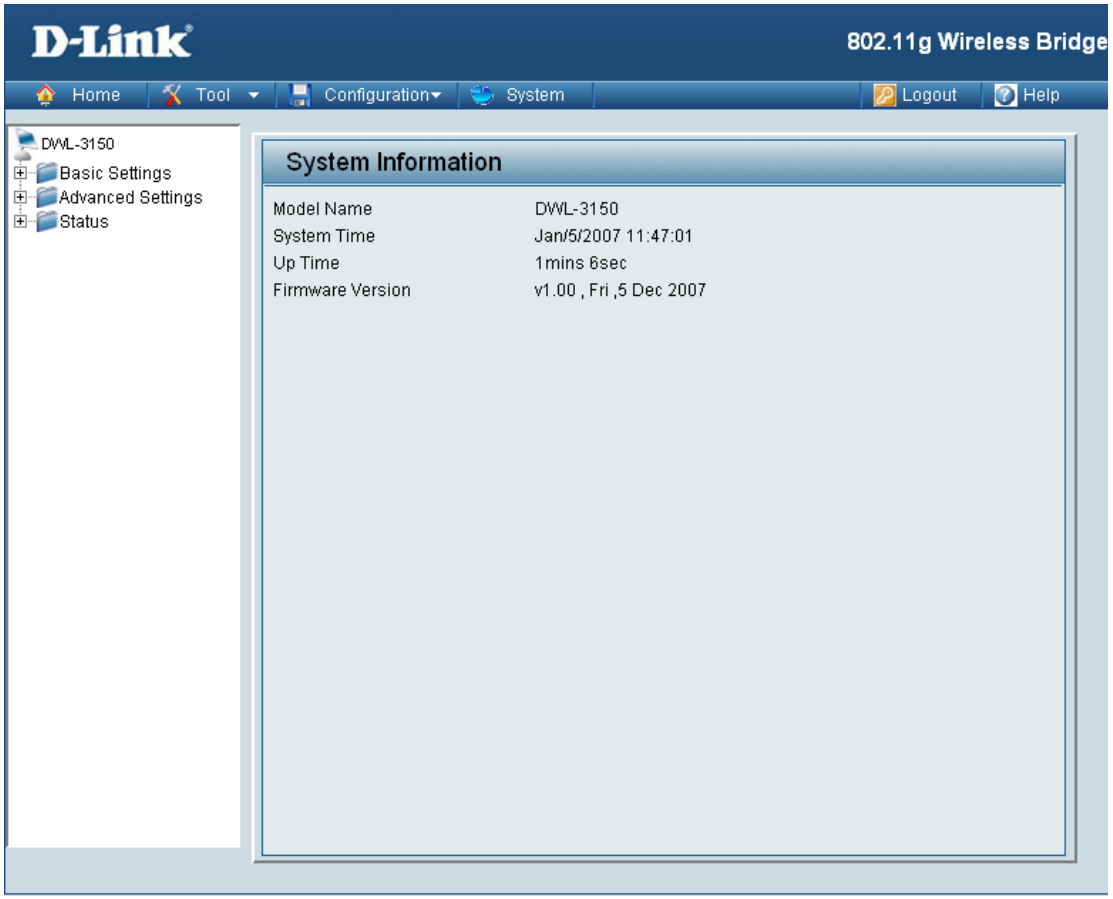
System
System Settings

System Restart: Click on to apply settings and restart.

Restore to Factory Default Settings: Click on Restore to reset to factory default settings.



System Information



Wireless Basics

D-Link 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 D-Link 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 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 infrastructures have proven to be beneficial for many users.

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

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phones work, through radio signals that transmit data from 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, 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.

Who uses wireless?

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

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and 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 the 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. A wireless connection in a public place is usually called a "hotspot".

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

A 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 the 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 the product manual for detailed information on how to set security 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 WNA-1330 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.

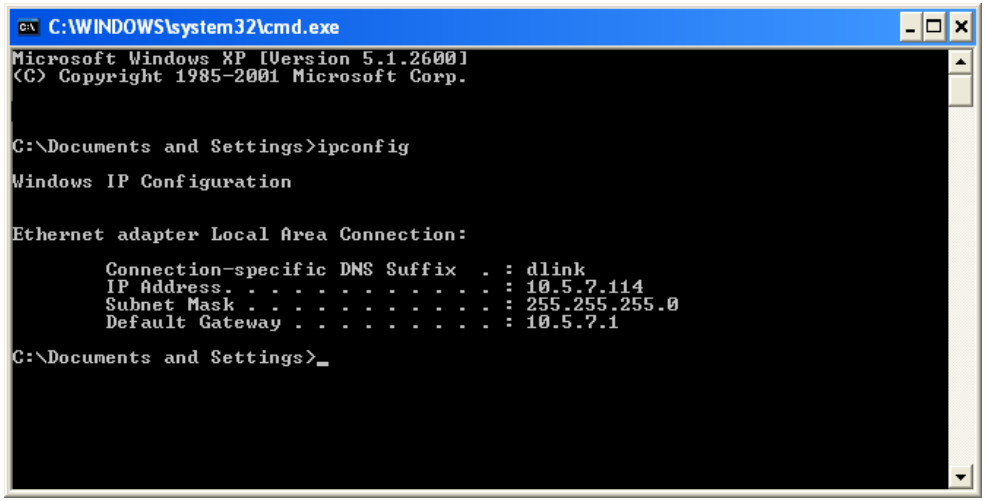
Networking Basics

Check your IP Address

After you install your new D-Link 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**.

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 firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

Statically Assign an IP Address

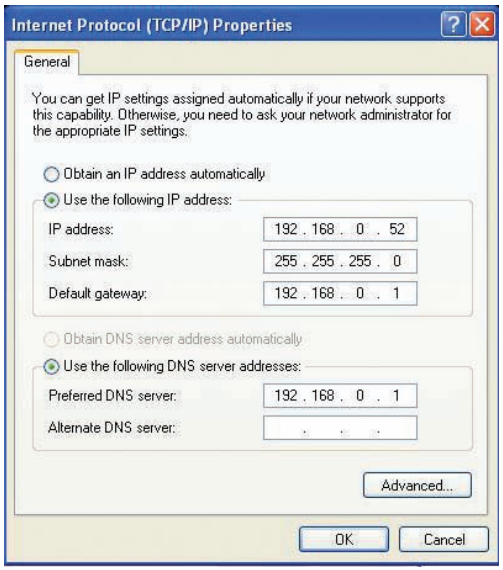
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1
Windows® 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 D-Link 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.

Contacting Technical Support

You can find software updates and user documentation on the D-Link website.

U.S. and Canadian customers can contact D-Link technical support through our web site, or by phone.

Tech Support for customers within the United States:
D-Link Technical Support over the Telephone:
(877) 453-5465

D-Link Technical Support over the Internet:
http://support.dlink.com

Tech Support for customers within Canada:
D-Link Technical Support over the Telephone:
(800) 361-5265

D-Link Technical Support over the Internet:
http://support.dlink.com

GNU/Linux GPL

- “GPL Software” means GPL software licensed to you under the GNU General Public License as published by the Free Software Foundation (GPL). A copy of the GPL is included below.

- “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements included in the materials relating to such software. Open Source Software is composed of individual software components, each of which has its own copyright and its own applicable license conditions. The Open Source Software licenses can be found in the **gpl.pdf** file, other materials accompanying the software package, the documentation or corresponding source files available from http://support.dlink.com/GPL.asp.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:

(1) copyright the software, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that hat they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

   Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. DLink will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:
Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright 2006-2007 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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.

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.

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.

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.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

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 harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
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.
This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

The Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.
Cet appareil numerique de la class [B] respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

Registration

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
February 8, 2007