USER MANUAL

DAP-1150

VERSION 2.0

D-Link®

WIRELESS

Table of Contents

Package Contents

- D-Link DAP-1150 Wireless N 150 Access Point
- Power Supply
- Manual on CD
- Quick Installation Guide
- Ethernet Cable

Note: Using a power supply with a different voltage rating than the one included with the DAP-1150 will cause damage and void the warranty for this product.

System Requirements

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

Features

- **Multiple operation modes -** Can be flexibly configured to operate as an Access Point, Wireless Repeater and Router mode.

- **Faster Wireless Networking -** The DAP-1150 provides up to 150Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11b and 802.11g Devices -** The DAP-1150 is still fully compatible with the IEEE 802.11b and IEEE 802.11g standard, so it can connect with existing 802.11b and IEEE 802.11g PCI USB and Cardbus adapters.

- **Total security -** Complete set of security features including WEP encryption and WPA/WPA2 to protect network against outside intruders.

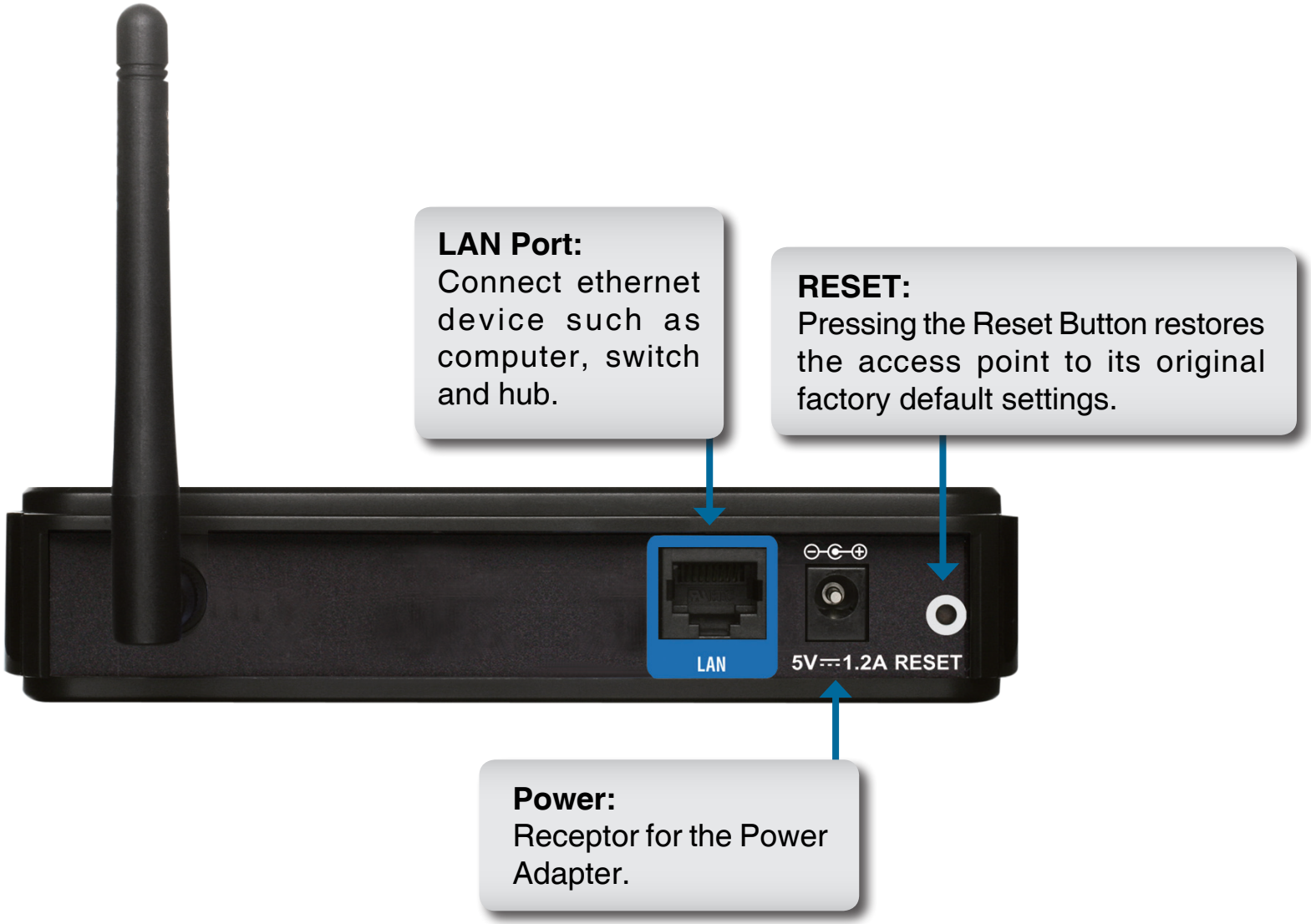
- **Connect home and soho to a wireless network -** Create a wireless network for your home and office using the D-Link DAP-1150 as an 802.11n standard Wireless Access Point. Connect this Access Point to a broadband modem and let others wirelessly access your Internet connection. Enjoy surfing the web, checking e-mail, and chatting with family and friends online.

- **Protect wireless network and data -** The DAP-1150 provides 64/128-bit WEP encryption and WPA/WPA2 security to protect your network and wireless data. In addition, it also provides MAC address filtering and the Disable SSID Broadcast function to limit outsiders' access to your home and office network.

- **Easy to install and use -** Through its easy-to-use Web-based user interface, the DAP-1150 lets you configure your AP to your specific settings within minutes.

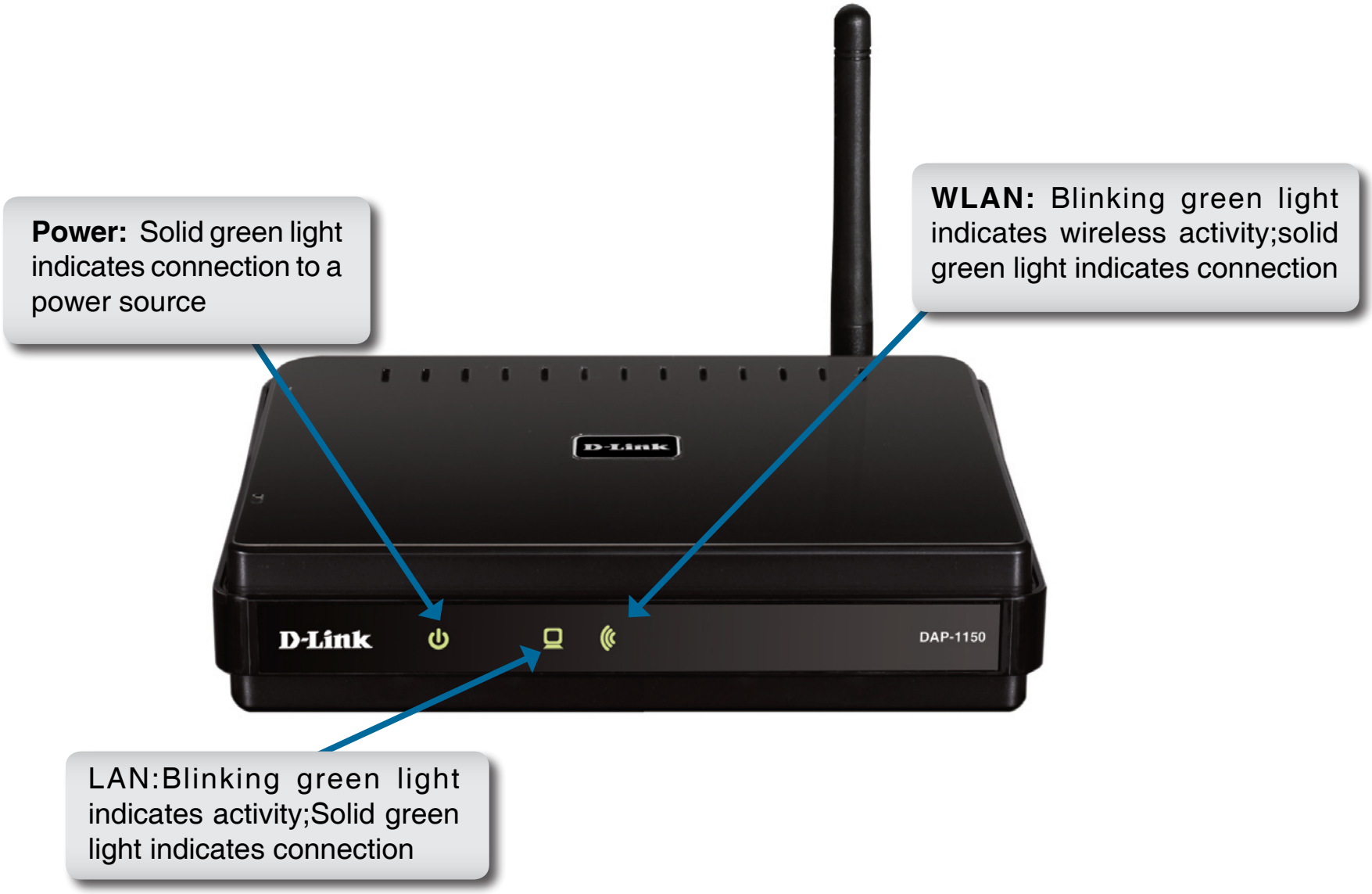
1 Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.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

Hardware Overview
Connections



Hardware Overview

LEDs



Wireless Installation Considerations

The D-Link wireless access point 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 access point 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 access points, 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.

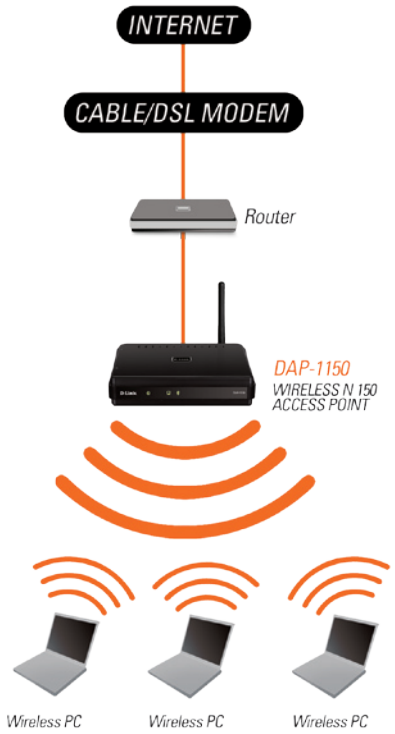
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

AP/Repeater/Router Mode

How you use your DAP-1150 will determine which mode you choose on the DAP-1150. This section will help you figure out which setting works with your setup.

Access Point Mode

In Access Point mode, the DAP-1150 acts as a central connection point for any computer (client) that has a 802.11n or backward-compatible 802.11b/g wireless network adapter and is within range of the AP. Clients must use the same SSID (wireless network name) and channel as the AP in order to connect. If wireless security is enabled on the AP, the client will need to enter a password to connect to the AP. Multiple clients can connect to the AP at the same time in Access Point mode.



Wireless PCs Using the DAP-1150 as a Central Connection Point

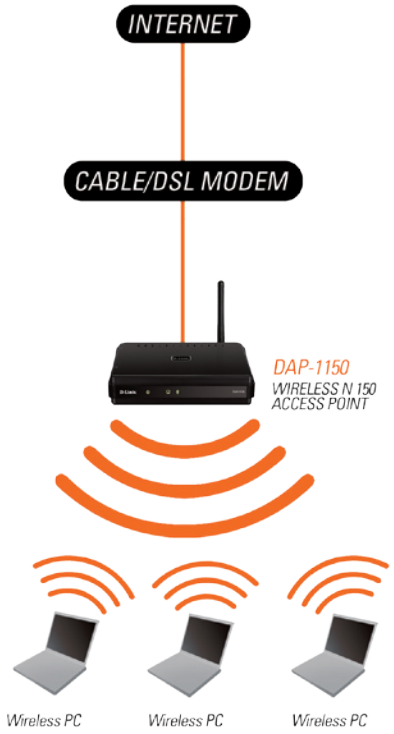
Repeater Mode

Repeater mode increases the range of your wireless network by extending the wireless coverage of another AP or wireless router. The APs and wireless router (if used) must be within range of each other. Make sure that all clients, APs, and the wireless router all use the same SSID (wireless network name) and channel.

Extending the Wireless Coverage of a Wireless Router Using the DAP-1150

Router Mode

In the Router mode, the DAP-1150 connects to a broadband modem. In this mode, the DAP-1150 also acts as a router for wireless clients on your network and provides NAT (Network Address Translation) and a DHCP server to generate IP addresses. NAT and the DHCP server allow many computers to share the same Internet connection.



When DAP-1150 operates as Router mode, the ethernet port of DAP-1150 is configured as WAN interface, you will need to connect wirelessly to the DAP-1150 to configure it. The default SSID of DAP-1150 is "dlink"

Configuration for AP Mode

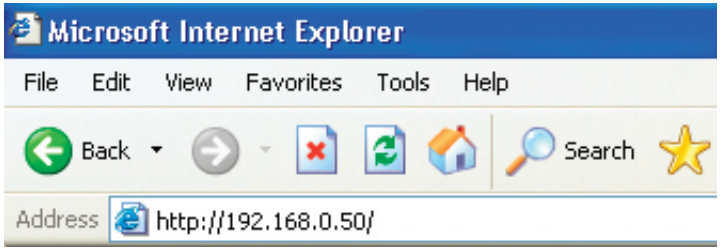
Web-based Configuration Utility

If you wish to change the default settings or optimize the performance of the DAP-1150, you may use the configuration utility that D-Link has included a configuration utility for this purpose.

After you have completed the initial installation, you can access the configuration menu, at any time, by opening the web-browser and typing in the ip address of the DAP-1150. The DAP-1150's default ip address is shown below:

1. Open the web browser

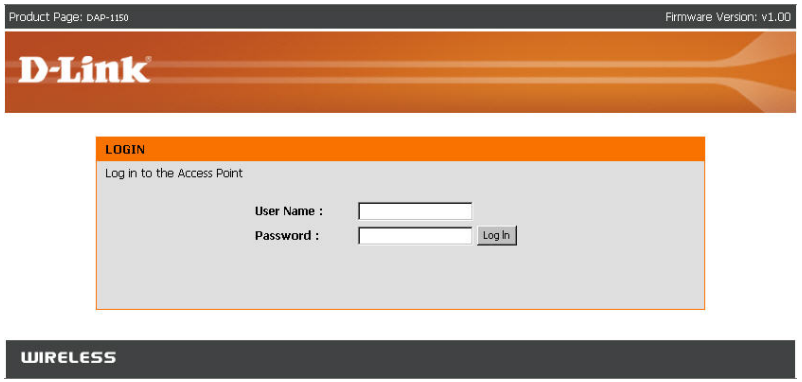
2. Type in the **ip address** of the DAP-1150.(192.168.0.50)



3. Type **admin** in the **User Name** field

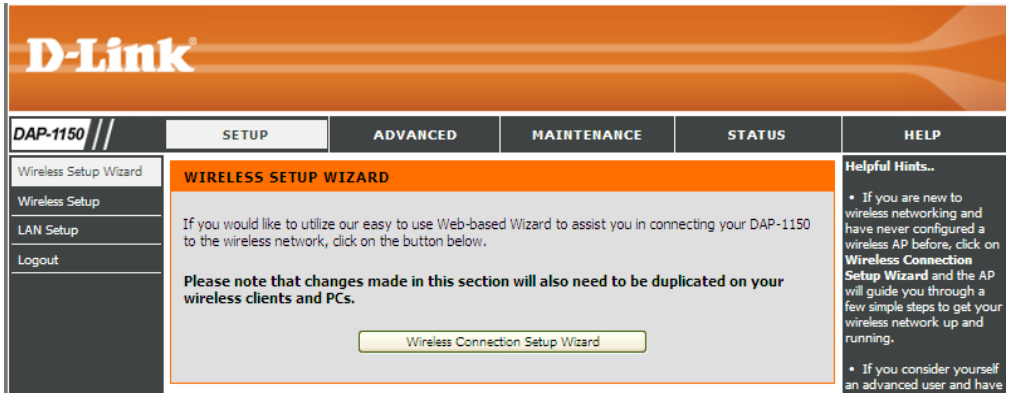
4. Leave the **Password** blank

5. Click **OK**

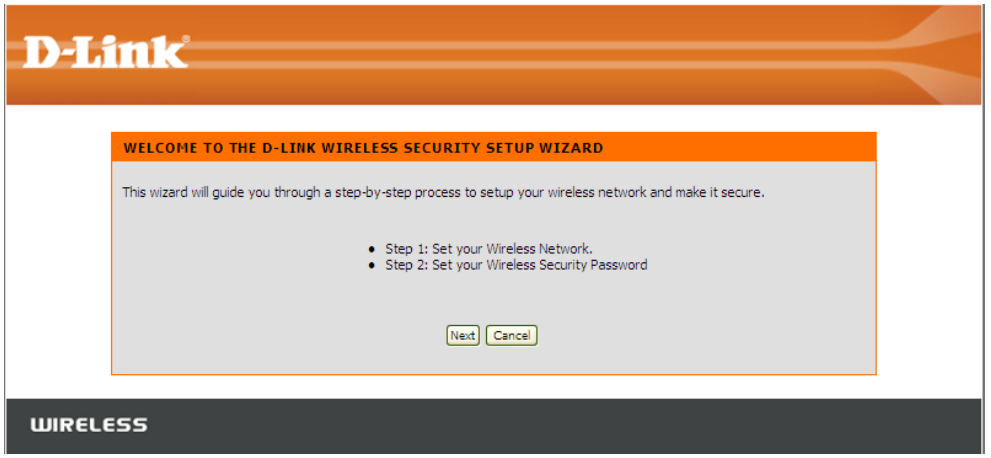


Wireless Setup Wizard

Click **Launch Wireless Setup Wizard** to quickly configure your access point.

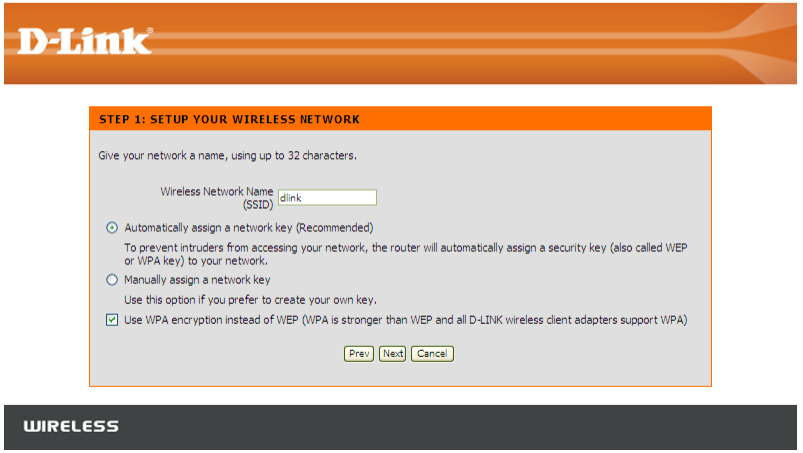


Follow the steps to configure your DAP-1150.



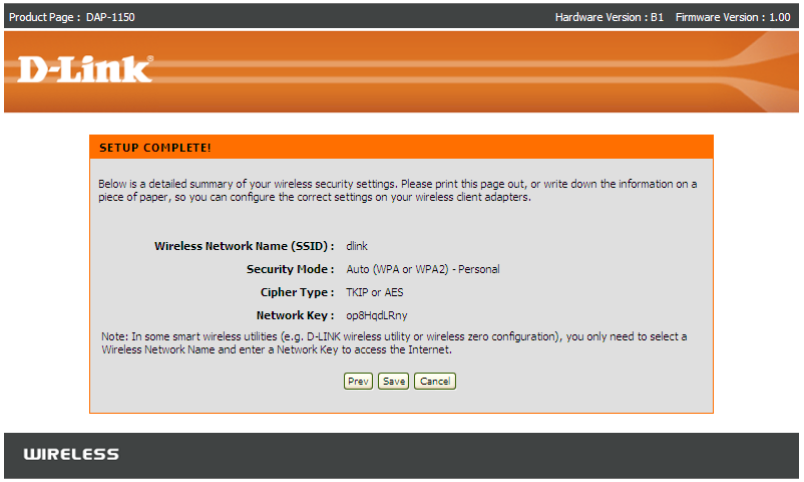
Enter a network name and choose the option to Automatically assign a network key. To Manually assign a network key, skip to page 15.

Click **Next** to continue.



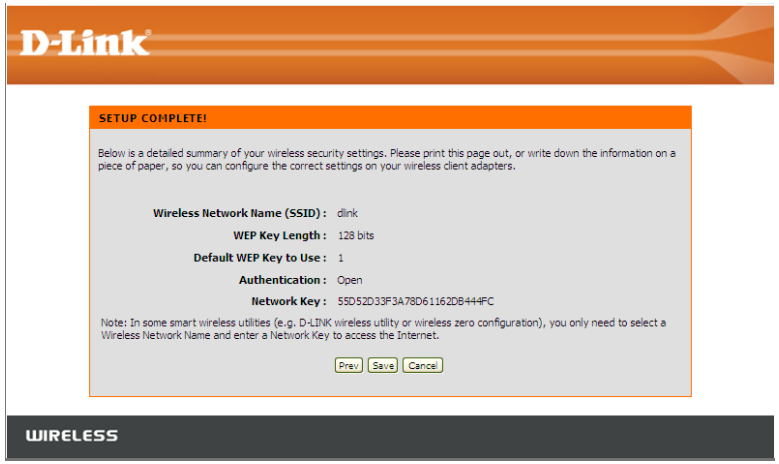
If you choose WPA-PSK encryption, the following screen will display the Network Key to be entered on your wireless clients.

Click **Save** to finish the Setup Wizard.

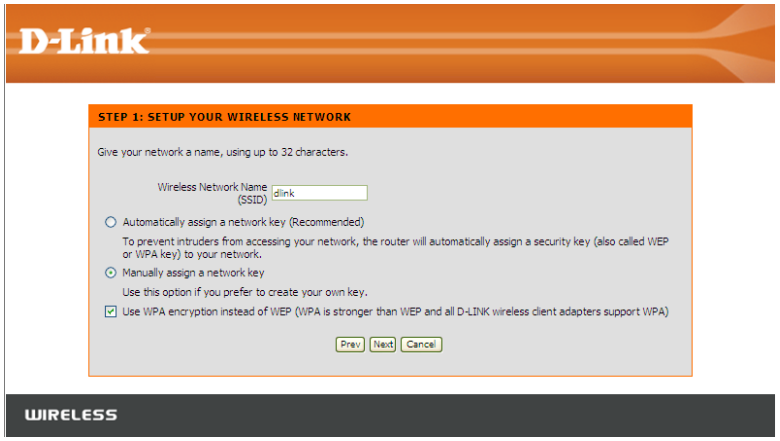


If you choose WEP encryption, the following screen will show you your Network Key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.

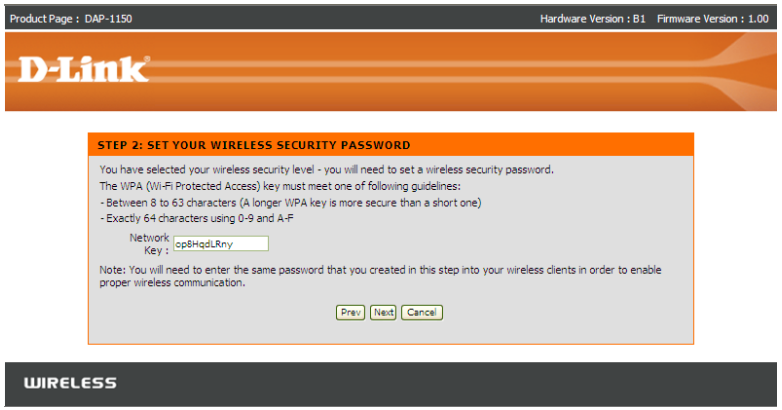


Choose Manually assign a network key to create your own key.
Click **Next** to continue.



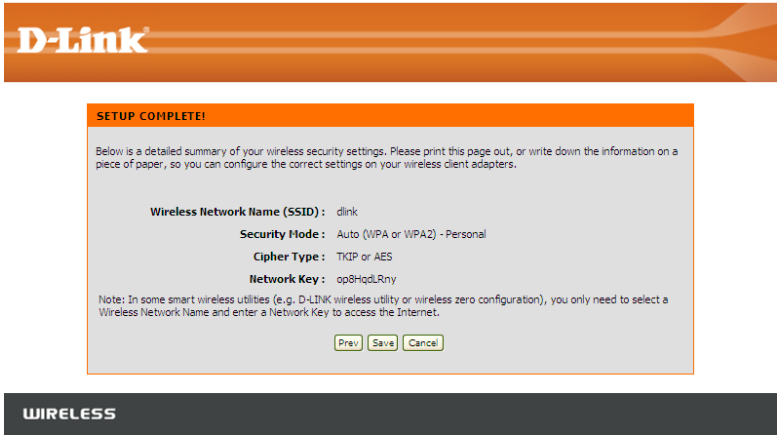
For **WPA** encryption, enter a Network Key between 8 and 63 characters long or enter exactly 64 characters using 0-9 and A-F.

Click **Next** to continue.



If you select WPA encryption, the following screen will display the network key to be entered on your wireless clients.

Click **Save** to finish the Setup Wizard.

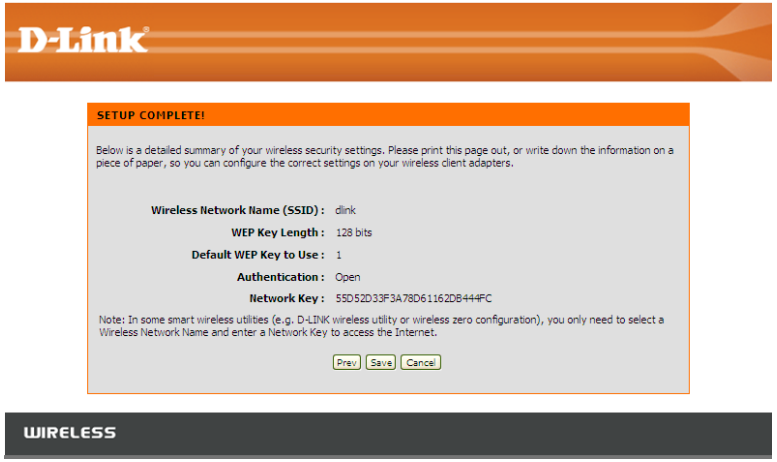


For **WEP** encryption, enter a Network Key exactly 5 or 13 characters long or exactly 10 or 26 characters using 0-9 and A-F.

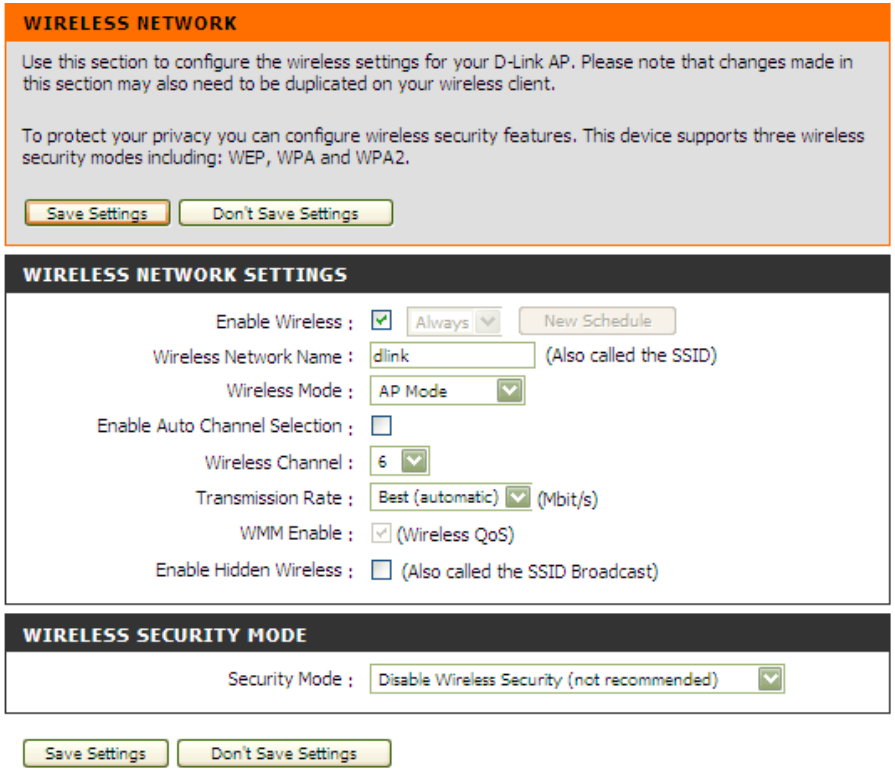
Click **Next** to continue.

If you select **WEP** encryption, the following screen will show you your network key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.



Wireless Setup



Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Wireless Mode: Select AP mode.

Enable Wireless Channel: Indicates the channel setting for the DAP-1150. By default the channel is set to *6*. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. The **Auto Channel Selection** setting can be selected to allow the DAP-1150 to choose the channel with the least amount of interference.

Transmission Rate: Use the drop-down menu to select the appropriate Transmission Rate in Mbits per second. Many users will want to use the default setting, *Best (automatic)*.

WMM Enable: Enable Wi-Fi Multimedia to enjoy basic quality of service features. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background.

Enable Hidden Wireless: Check this option if you would not like the SSID of your wireless network to be broadcasted by the DAP-1150. If this option is checked, the SSID of the DAP-1150 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DAP-1150 in order to connect to it.

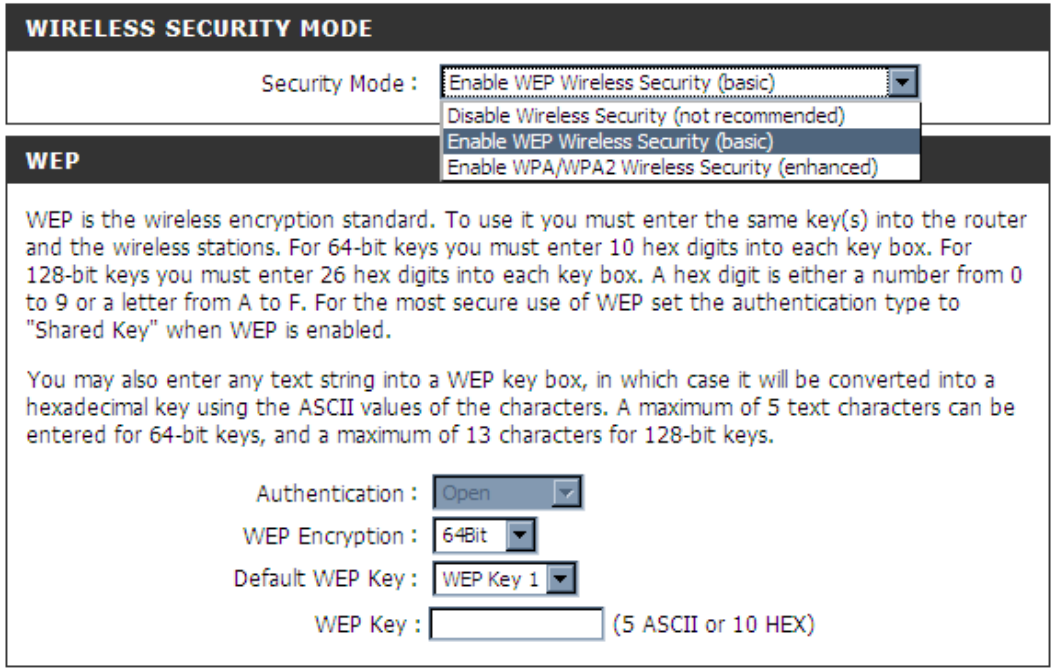
1. To enable wireless security on the AP, use the drop-down menu to select the desired option. To enable WEP, select *Enable WEP Wireless Security (basic)*.

2. Next to **Authentication**, select either *Open* or *Shared Key*. Shared Key provides greater security.

3. Select either *64Bit* or *128Bit* encryption from the drop-down menu next to **WEP Encryption**.

4. Next to **Default Key Type**, select *WEP Key 1* and enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using *Hex* or *ASCII*. *Hex* is recommended (letters A-F and numbers 0-9 are valid). In *ASCII* all numbers and letters are valid.

5. Click **Save Settings** to save your settings. If you are configuring the AP with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the AP.



NOTE:
It is recommended to enable encryption on your wireless AP before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

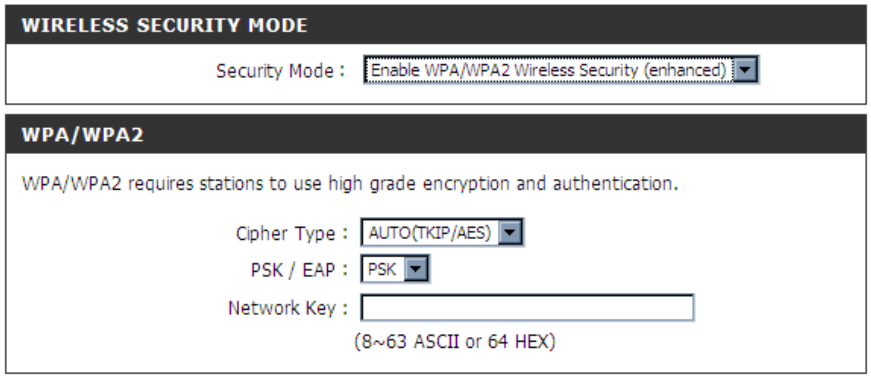
1. To enable *Enable WPA/WPA2 Wireless Security (enhanced).*

2. Next to **Cipher Type**, select *TKIP*, *AES*, or *AUTO*.

3. Next to **PSK/EAP**, select *PSK*.

4. Next to **Network Key**, enter a passphrase. The key 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.

5. Click **Save Settings** to save your settings. If you are configuring the AP with a wireless adapter, you will lose connectivity until you enable WPA/WPA2 (whichever of the three options you have selected above) on your adapter and enter the same network key as you did on the AP.



1. To enable WPA/WPA2 for a RADIUS server, next to **Security Mode**, selec or *Enable WPA/WPA2 Wireless Security (enhanced)*.

2. Next to **Cipher Type**, select *TKIP*, *AES*, or *Auto*.

3. Next to **PSK/EAP**, select *EAP*.

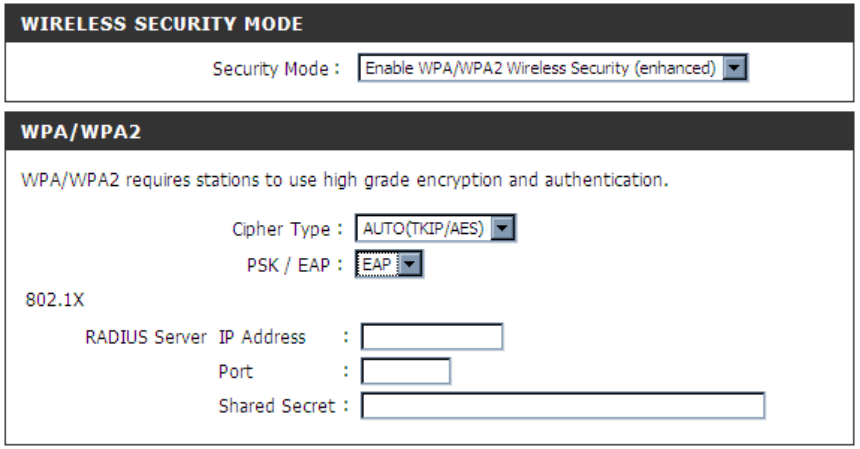
4. Next to **RADIUS Server 1** enter the **IP Address** of your RADIUS server.

5. Next to **Port**, enter the port you are using with your RADIUS server. *1812* is the default port.

6. Next to **Shared Secret**, enter the security key.

7. If you have a secondary RADIUS server, enter its IP address, port, and secret key.

8. Click **Save Settings** to save your settings.



LAN Setup

This section will allow you to change the local network settings of the AP and to configure the DHCP settings.

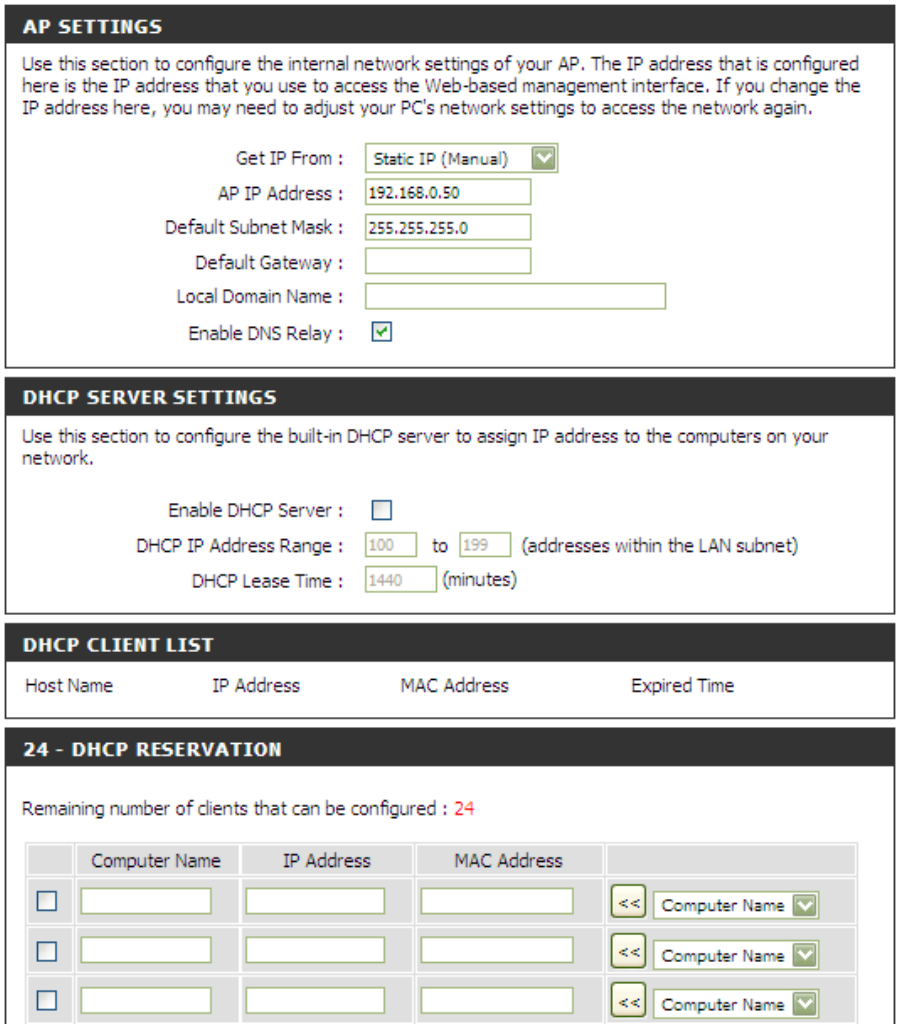
AP IP Address: Enter the IP address of the AP. The default IP address is 192.168.0.50.

If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Local Domain Name: Enter the Domain name (Optional).

Enable DNS Relay: Check the box to transfer the DNS server information from your ISP to your computers. If unchecked, your computers will use the AP for a DNS server.



Refer to the next page for DHCP information.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DAP-1150 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DAP-1150. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

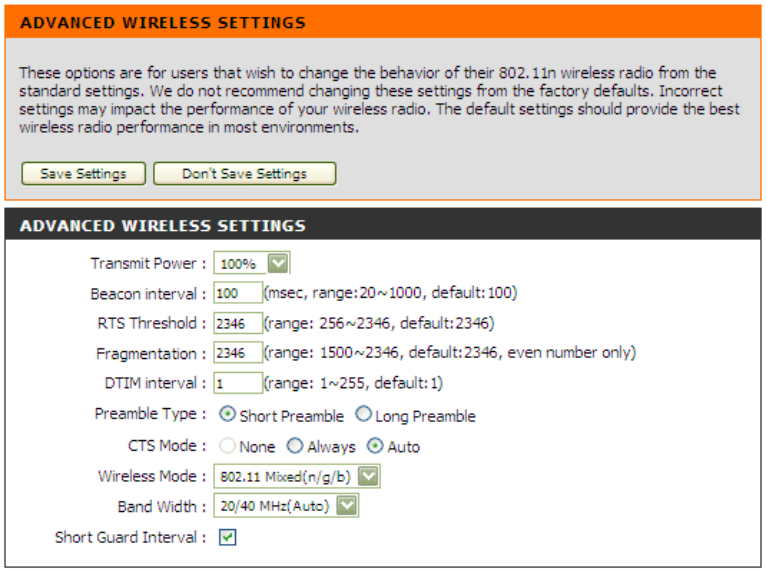
Enable DHCP Server: Check the box to enable the DHCP server on your AP. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Advanced Wireless

This window allows you to change the behavior of the 802.11n wireless radio from the standard settings. Please be aware that any changes to the factory default settings may adversely affect the behavior of your network.



Transmit Power: Set the transmit power of the antennas.

Beacon interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. *100* is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of *2346*. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. *2346* is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) *1* is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Preamble Type: Select Short or Long Preamble. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless AP and the roaming wireless network adapters. Auto is the default setting. Note: High network traffic areas should use the shorter preamble type.

CTS Mode: CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). CTS will make sure the wireless network is clear before a wireless client attempts to send wireless data. Enabling CTS will add overhead and may lower wireless through put. **None:** CTS is typically used in a pure 802.11g environment. If CTS is set to “None” in a mixed mode environment populated by 802.11b clients, wireless collisions may occur frequently. **Always:** CTS will always be used to make sure the wireless LAN is clear before sending data. **Auto:** CTS will monitor the wireless network and automatically decide whether to implement CTS based on the amount of traffic and collisions that occurs on the wireless network.

802.11 Mode: 802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11n, 802.11b, and 802.11g - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

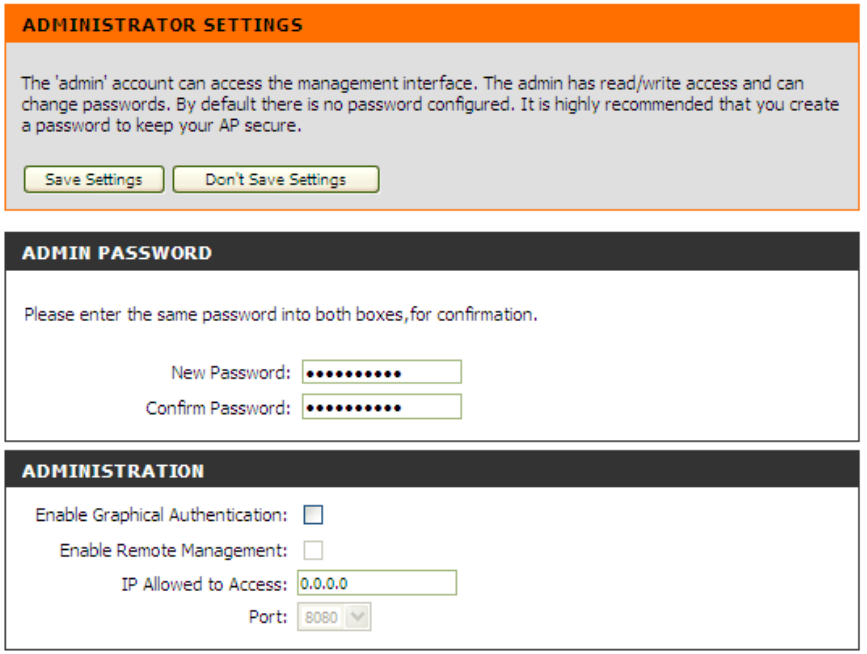
Auto 20/40: Select if you are using both 802.11n and non-802.11n wireless devices.

20MHz: Select if you are not using any 802.11n wireless clients. This is the default setting.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it’s less reliable and may create higher data loss.

Device Administration

This window will allow you to change the Administrator password. You can also enable Remote Management.



Administrator Login Name: Enter a new Login Name for the Administrator account.

Administrator Password: Enter a new password for the Administrator Login Name and then retype the new password in the Confirm Password textbox. The administrator can make changes to the settings.

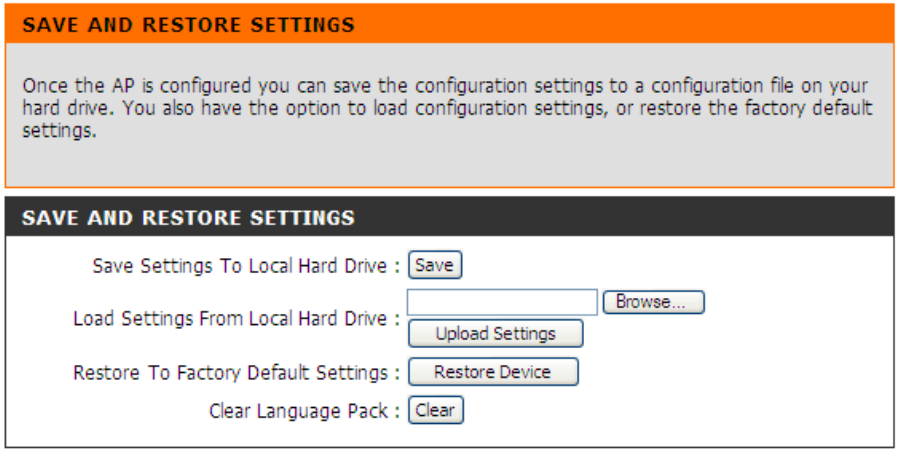
Enable Remote Management: Remote management allows the DAP-1150 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

IP Allowed to Access: The Internet IP address of the computer that has access to the AP. If you input an asterisk (*) into this field, then any computer will be able to access the AP. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port: The port number used to access the DAP-1150. For example: http://x.x.x.x:8080 whereas x.x.x.x is the LAN IP address of the DAP-1150 and *8080* is the port used for the Web-Management interface.

Save and Restore

This window allows you to save your configuration file to a hard drive, load configuration settings from a hard drive, and restore the AP's factory default settings.



Save Settings to Local Hard Drive: Use this option to save the current AP configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved AP configuration settings. First, use the **Browse** control to find a previously save file of configuration settings. Then, click the **Upload Settings** button to transfer those settings to the AP.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the AP was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current AP configuration settings, use the **Save** button above.

Clear Language Pack: Click the **Clear** button to uninstall the language pack.

Firmware Update

You can upgrade the firmware of the AP here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade: Click the **Check Now** button (or the link at the top of the window) to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Save Settings** to complete the firmware upgrade.

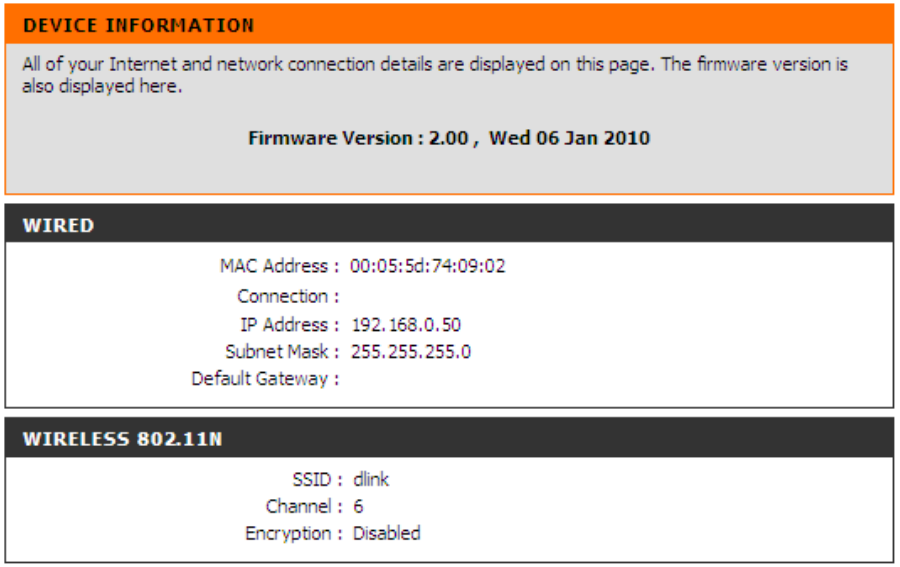
Language Pack Upgrade: To change the web configuration language, click on **Browse** to browse locate the language package upgrade file and click the **Upload** button.

Device Info

This window displays the current information for the DAP-1150. It will display the LAN, and Wireless information.

Wired: Displays the MAC address and the private (local) IP settings for the AP.

Wireless 802.11N: Displays the wireless MAC address and your wireless settings such as SSID, Channel, and Encryption status.



Log

This window allows you to view a log of activities on the AP. This is especially helpful detecting unauthorized network usage.

First Page: View the first page of the log.

Last Page: View the last page of the log.

Previous: View the previous page.

Next: View the next page.

Clear: Clear the log.

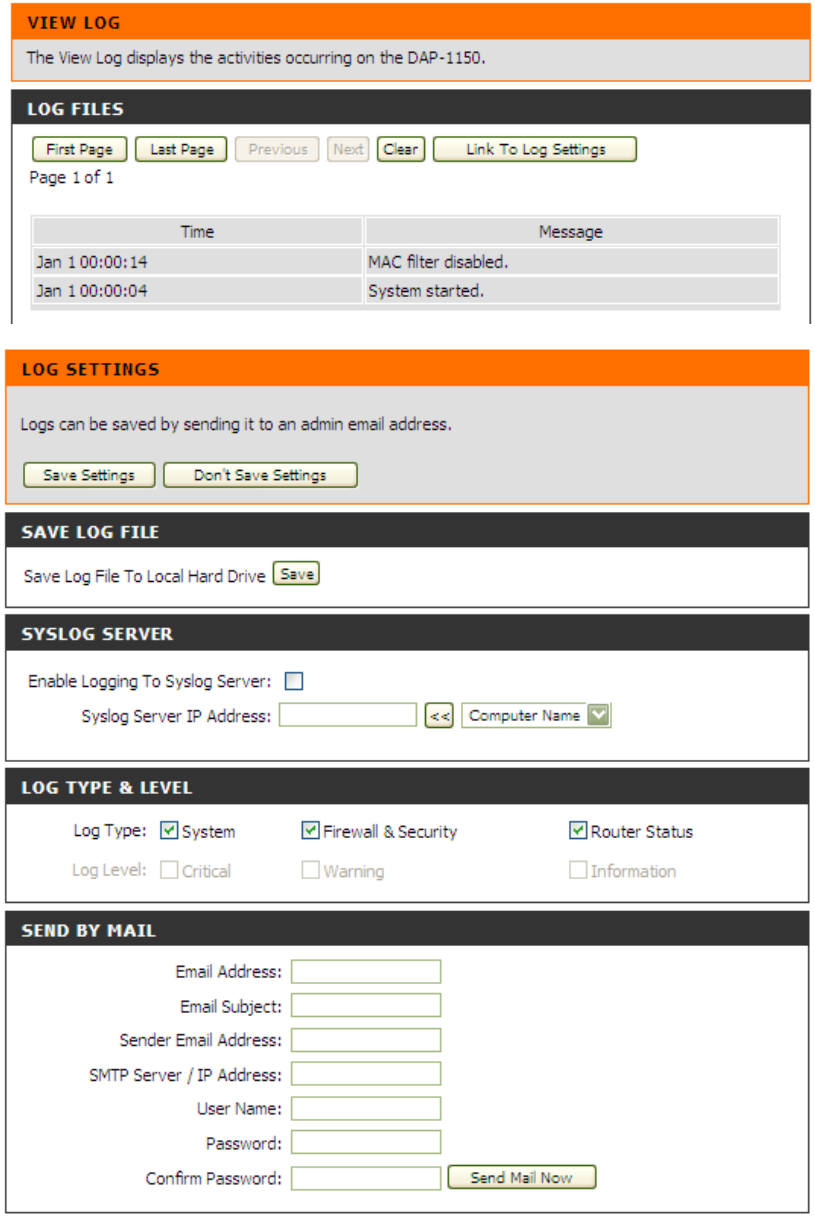
Link to Log Settings: Click this button to go directly to the Log Settings

Save Log File: Click on the Save button link on this window to save the log file to your local hard drive.

Syslog Server: Click the checkbox to save the log in the log server in the LAN side.

Log Type &Level: Click the checkbox(es) of the type of log information requested: **"System, Firewall & Security, AP Status, Critical, Warning and Information"**

Send by Mail: Enter the your SNTP server name(or IP address) and enter your mail address before sending your system log by mail.



Wireless

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

CONNECTED WIRELESS CLIENT LIST

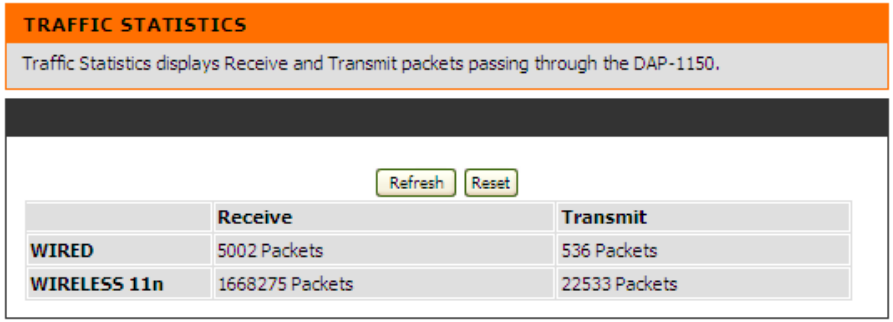
The Wireless Client table below displays Wireless clients Connected to the AP (Access Point).

NUMBER OF WIRELESS CLIENTS : 4

Connect Time	MAC Address	IP Address	Mode	Rate	Signal (%)
0 days, 00:29:29	00:19:D2:AE:DE:F7	N/A	11g	54	72
0 days, 00:15:11	00:26:5E:E9:5C:1D	N/A	11g	54	100
0 days, 2:15:30	00:21:5C:39:2F:25	N/A	11n	72.2	86
0 days, 00:10:25	00:26:5E:E8:03:CC	N/A	11g	54	76

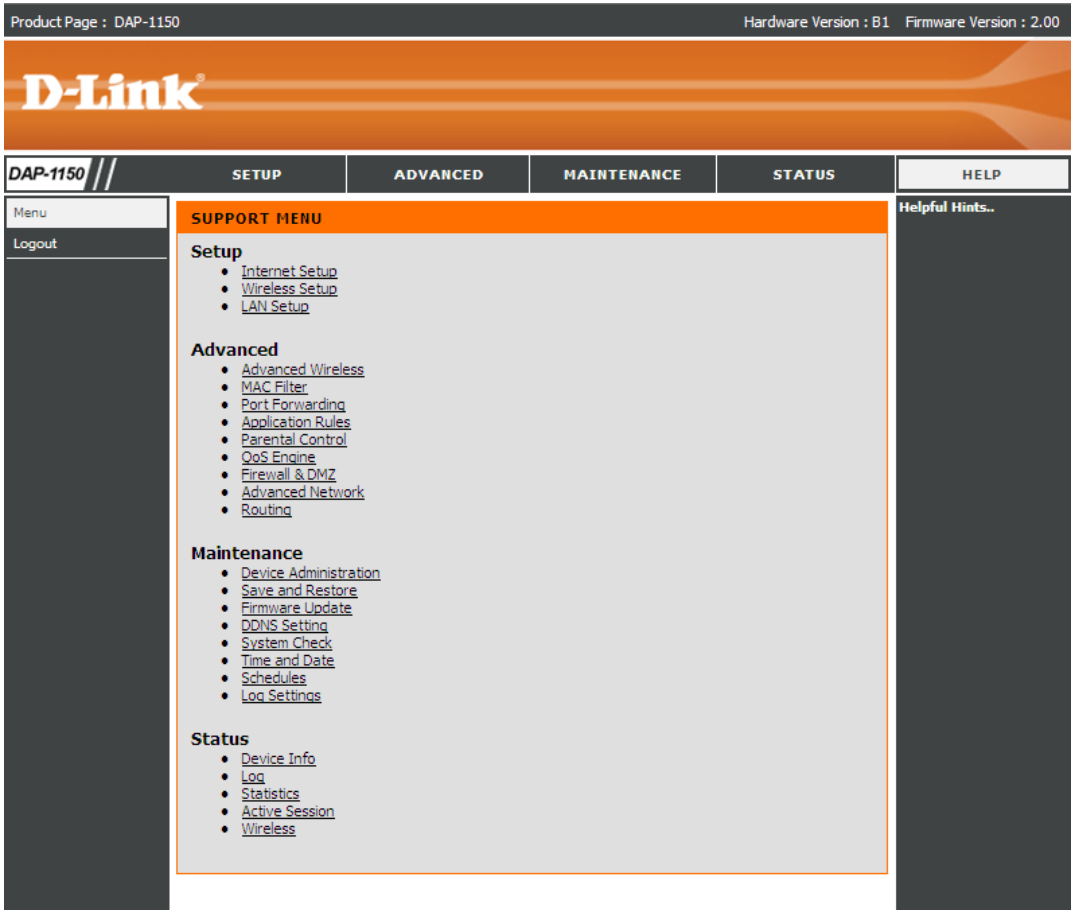
Statistics

The window below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DAP-1150 on the LAN port. The traffic counter will reset if the device is rebooted.



Help

Click the desired hyperlink to get more information about how to use the AP.



Configuration for Repeater Mode

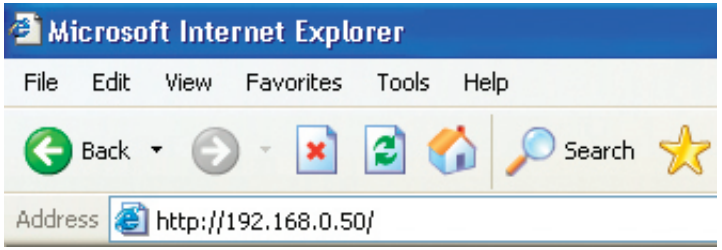
Web-based Configuration Utility

If you wish to change the default settings or optimize the performance of the DAP-1150, you may use the configuration utility that D-Link has included a configuration utility for this purpose.

After you have completed the initial installation, you can access the configuration menu, at any time, by opening the web-browser and typing in the ip address of the DAP-1150. The DAP-1150's default ip address is shown below:

1. Open the web browser

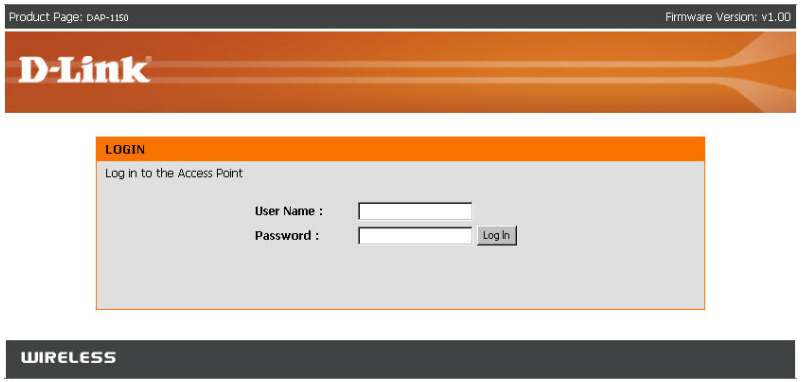
2. Type in the **ip address** of the DAP-1150.(192.168.0.50)



3. Type **admin** in the **User Name** field

4. Leave the **Password** blank

5. Click **OK**



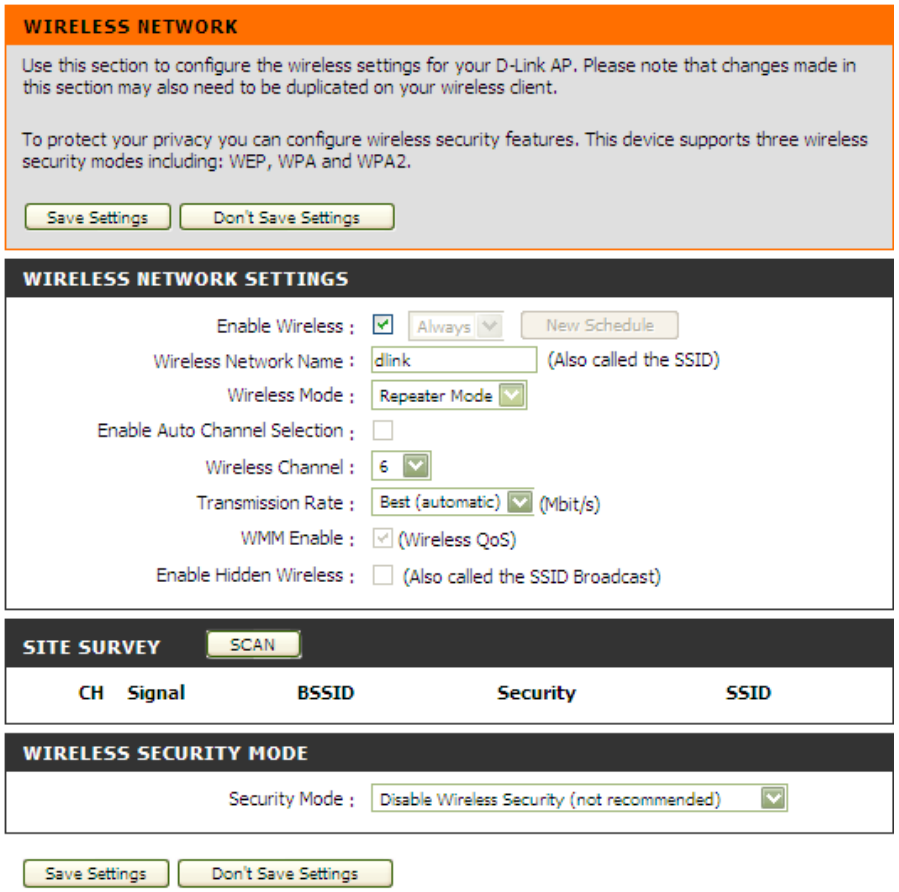
Wireless Setup

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Wireless Mode: Select Repeater mode.

Enable Wireless Channel: Indicates the channel setting for the DAP-1150. By default the channel is set to *6*. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.



Transmission Rate: Use the drop-down menu to select the appropriate Transmission Rate in Mbits per second. Many users will want to use the default setting, *Best (automatic)*.

WMM Enable: Enable Wi-Fi Multimedia to enjoy basic quality of service features. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background.

Enable Hidden Wireless: This option is unavailable in Repeater mode.

Site Survey: Click the scan button to choose the root AP from an available connection list.

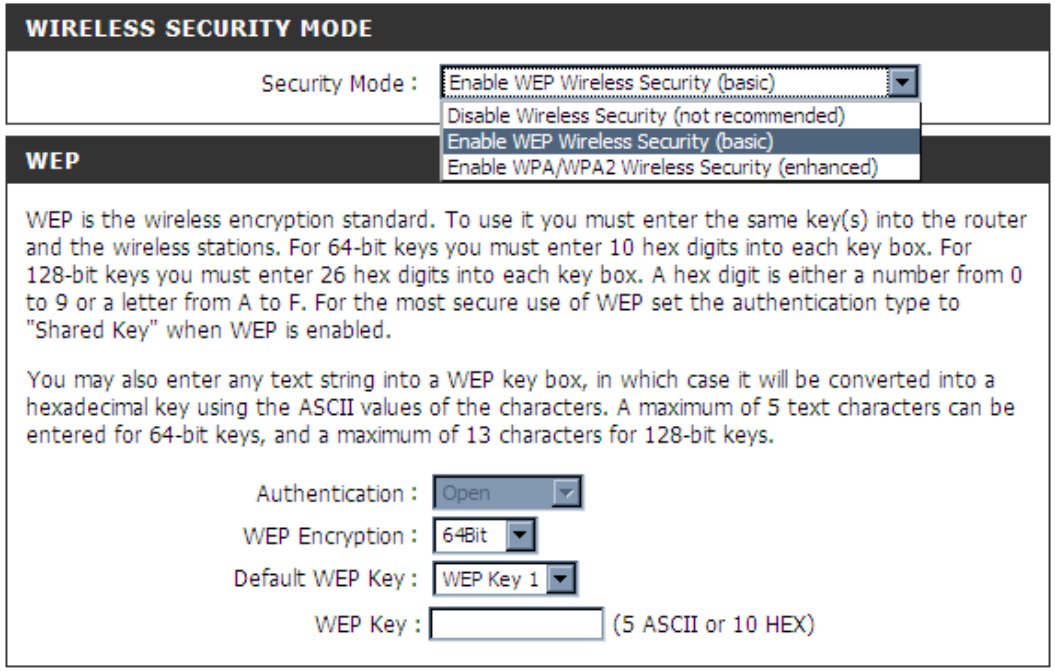
1. To enable wireless security on the AP, use the drop-down menu to select the desired option. To enable WEP, select *Enable WEP Wireless Security (basic)*.

2. Next to **Authentication**, select either *Open* or *Shared Key*. Shared Key provides greater security.

3. Select either *64Bit* or *128Bit* encryption from the drop-down menu next to **WEP Encryption**.

4. Next to **Default Key Type**, select *WEP Key 1* and enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using *Hex* or *ASCII*. *Hex* is recommended (letters A-F and numbers 0-9 are valid). In *ASCII* all numbers and letters are valid.

5. Click **Save Settings** to save your settings. If you are configuring the AP with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the AP.



NOTE:
In Repeater mode, use the same wireless security method of root AP is reguired.

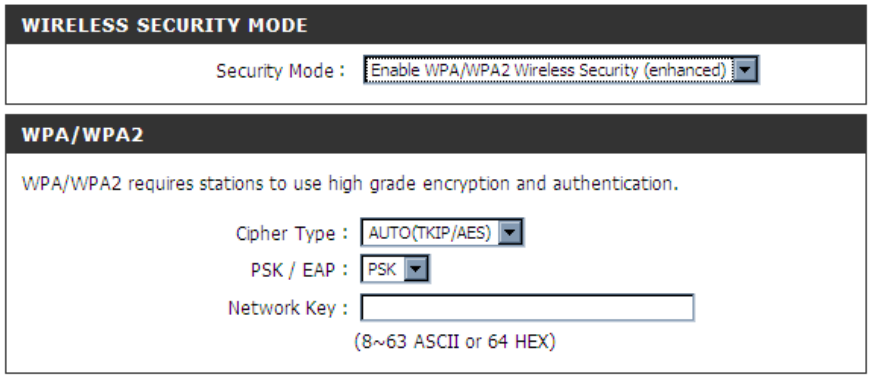
1. To enable *Enable WPA/WPA2 Wireless Security (enhanced).*

2. Next to **Cipher Type**, select *TKIP*, *AES*, or *AUTO*.

3. Next to **PSK/EAP**, select *PSK*.

4. Next to **Network Key**, enter a passphrase. The key 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.

5. Click **Save Settings** to save your settings. If you are configuring the AP with a wireless adapter, you will lose connectivity until you enable WPA/WPA2 (whichever of the three options you have selected above) on your adapter and enter the same network key as you did on the AP.



LAN Setup

This section will allow you to change the local network settings of the AP and to configure the DHCP settings.

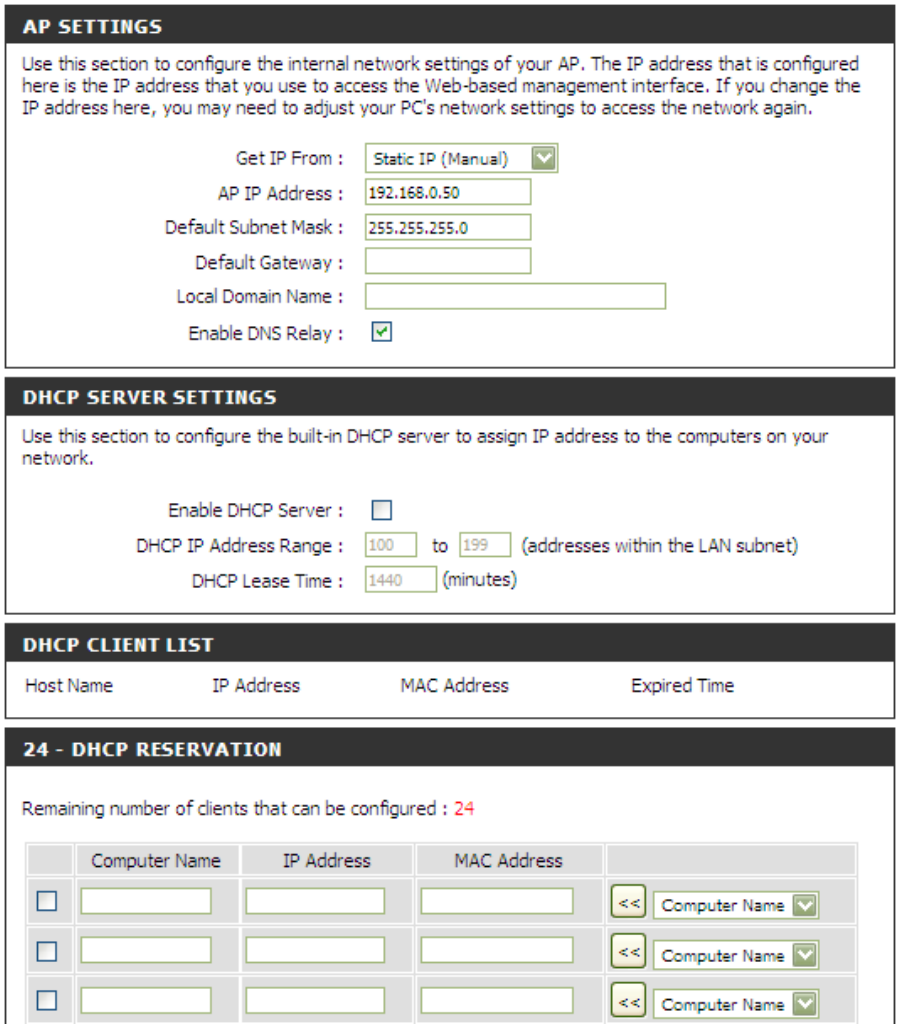
AP IP Address: Enter the IP address of the AP. The default IP address is 192.168.0.50.

If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Local Domain Name: Enter the Domain name (Optional).

Enable DNS Relay: Check the box to transfer the DNS server information from your ISP to your computers. If unchecked, your computers will use the AP for a DNS server.



Refer to the next page for DHCP information.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DAP-1150 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DAP-1150. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

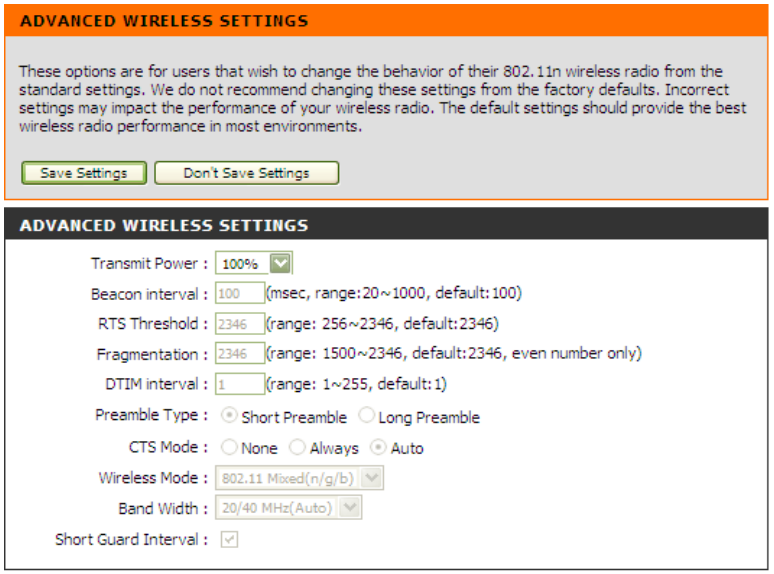
Enable DHCP Server: Check the box to enable the DHCP server on your AP. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Advanced Wireless

This window allows you to change the behavior of the 802.11n wireless radio from the standard settings. Please be aware that any changes to the factory default settings may adversely affect the behavior of your network.



Transmit Power: Set the transmit power of the antennas.

Beacon interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. *100* is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of *2346*. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. *2346* is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) *1* is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Preamble Type: Select Short or Long Preamble. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless AP and the roaming wireless network adapters. Auto is the default setting. Note: High network traffic areas should use the shorter preamble type.

CTS Mode: CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). CTS will make sure the wireless network is clear before a wireless client attempts to send wireless data. Enabling CTS will add overhead and may lower wireless through put. **None:** CTS is typically used in a pure 802.11g environment. If CTS is set to "None" in a mixed mode environment populated by 802.11b clients, wireless collisions may occur frequently. **Always:** CTS will always be used to make sure the wireless LAN is clear before sending data. **Auto:** CTS will monitor the wireless network and automatically decide whether to implement CTS based on the amount of traffic and collisions that occurs on the wireless network.

802.11 Mode: 802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11n, 802.11b, and 802.11g - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Auto 20/40: Select if you are using both 802.11n and non-802.11n wireless devices.

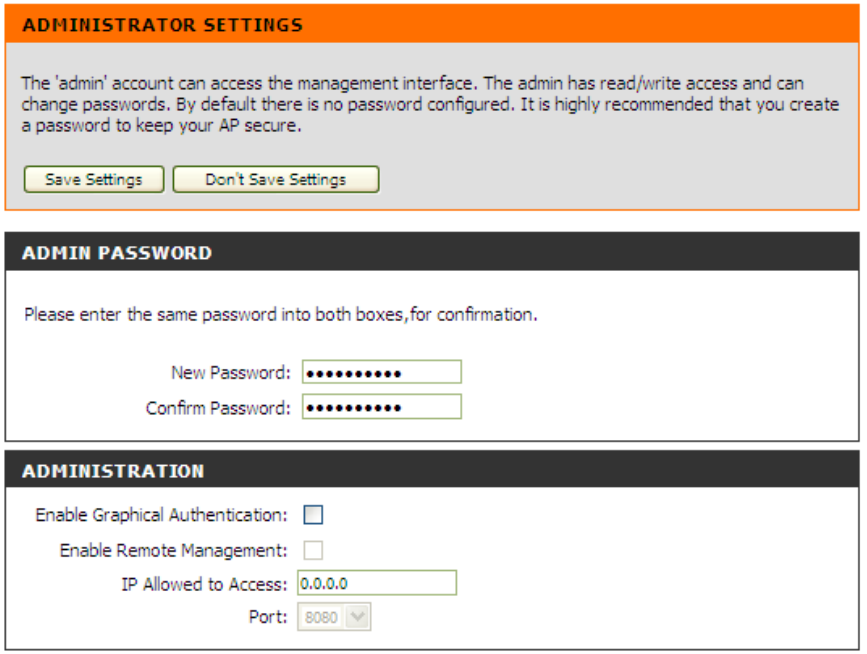
20MHz: Select if you are not using any 802.11n wireless clients. This is the default setting.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

NOTE: Some options are unavailabe in Repeater mode.

Device Administration

This window will allow you to change the Administrator password. You can also enable Remote Management.



Administrator Login Name: Enter a new Login Name for the Administrator account.

Administrator Password: Enter a new password for the Administrator Login Name and then retype the new password in the Confirm Password textbox. The administrator can make changes to the settings.

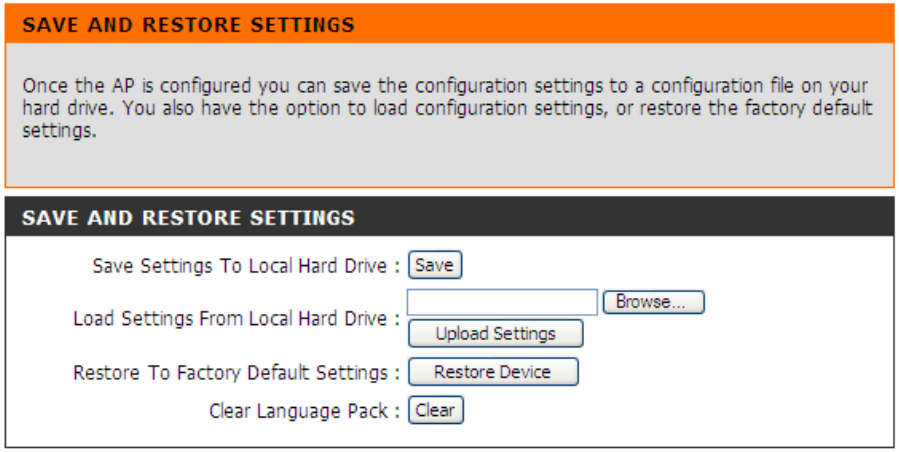
Enable Remote Management: Remote management allows the DAP-1150 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

IP Allowed to Access: The Internet IP address of the computer that has access to the AP. If you input an asterisk (*) into this field, then any computer will be able to access the AP. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port: The port number used to access the DAP-1150. For example: http://x.x.x.x:8080 whereas x.x.x.x is the LAN IP address of the DAP-1150 and *8080* is the port used for the Web-Management interface.

Save and Restore

This window allows you to save your configuration file to a hard drive, load configuration settings from a hard drive, and restore the AP's factory default settings.



Save Settings to Local Hard Drive: Use this option to save the current AP configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved AP configuration settings. First, use the **Browse** control to find a previously save file of configuration settings. Then, click the **Upload Settings** button to transfer those settings to the Router.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the AP was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current AP configuration settings, use the **Save** button above.

Clear Language Pack: Click the **Clear** button to uninstall the language pack.

Firmware Update

You can upgrade the firmware of the AP here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade: Click the **Check Now** button (or the link at the top of the window) to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

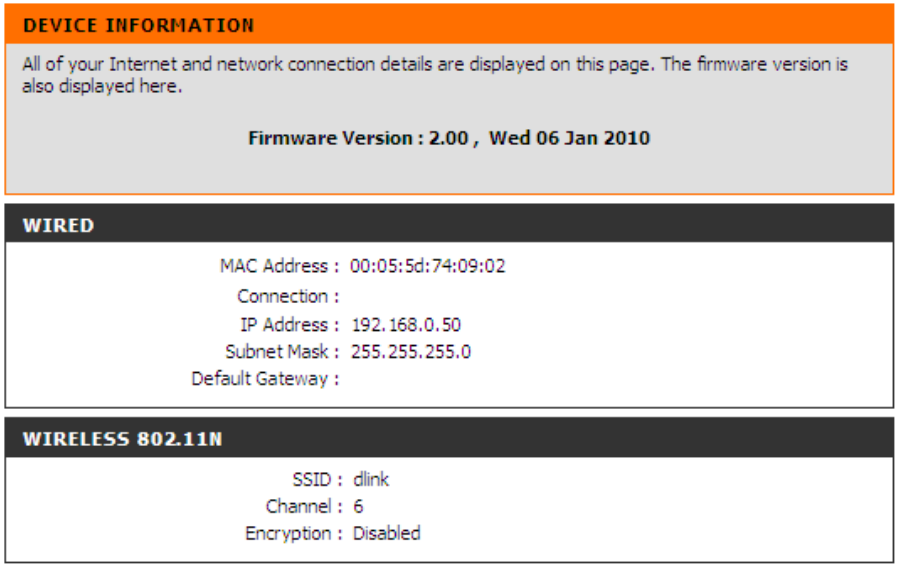
Language Pack Upgrade: To change the web configuration language, click on **Browse** to browse locate the language package upgrade file and click the **Upload** button.

Device Info

This window displays the current information for the DAP-1150. It will display the LAN, and Wireless information.

Wired: Displays the MAC address and the private (local) IP settings for the AP.

Wireless 802.11N: Displays the wireless MAC address and your wireless settings such as SSID, Channel, and Encryption status.



Log

This window allows you to view a log of activities on the AP. This is especially helpful detecting unauthorized network usage.

First Page: View the first page of the log.

Last Page: View the last page of the log.

Previous: View the previous page.

Next: View the next page.

Clear: Clear the log.

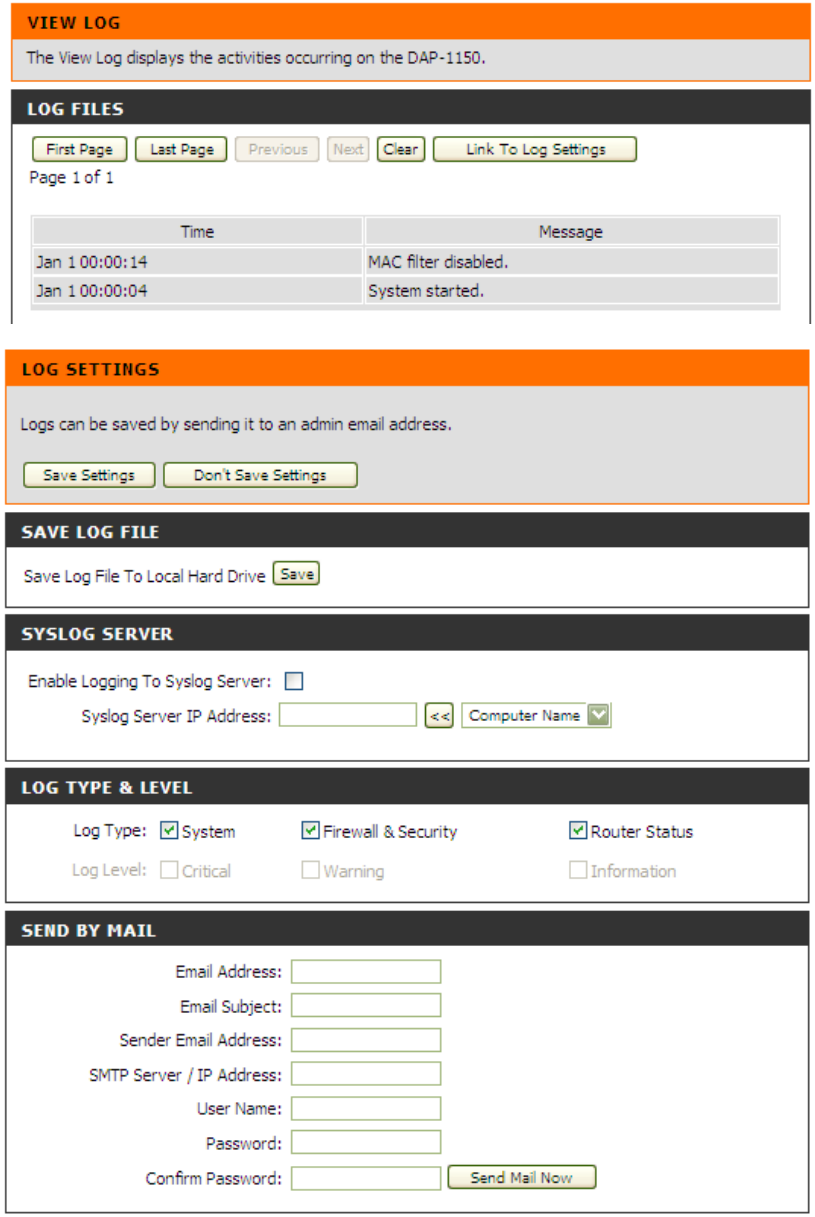
Link to Log Settings: Click this button to go directly to the Log Settings

Save Log File: Click on the Save button link on this window to save the log file to your local hard drive.

Syslog Server: Click the checkbox to save the log in the log server in the LAN side.

Log Type &Level: Click the checkbox(es) of the type of log information requested: **"System, Firewall & Security, AP Status, Critical, Warning and Information"**

Send by Mail: Enter the your SNTP server name(or IP address) and enter your mail address before sending your system log by mail.



Wireless

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

CONNECTED WIRELESS CLIENT LIST

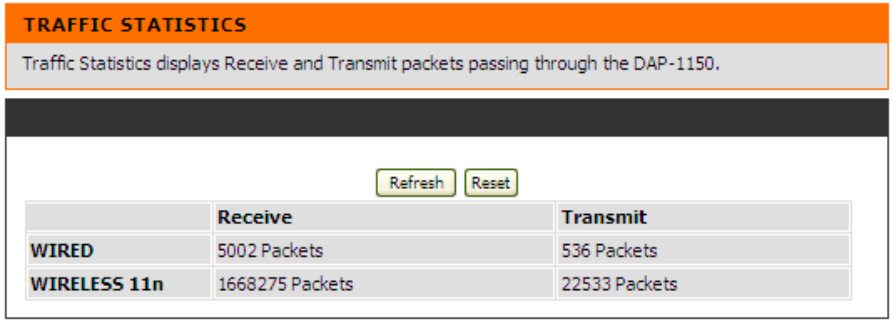
The Wireless Client table below displays Wireless clients Connected to the AP (Access Point).

NUMBER OF WIRELESS CLIENTS : 4

Connect Time	MAC Address	IP Address	Mode	Rate	Signal (%)
0 days, 00:29:29	00:19:D2:AE:DE:F7	N/A	11g	54	72
0 days, 00:15:11	00:26:5E:E9:5C:1D	N/A	11g	54	100
0 days, 2:15:30	00:21:5C:39:2F:25	N/A	11n	72.2	86
0 days, 00:10:25	00:26:5E:E8:03:CC	N/A	11g	54	76

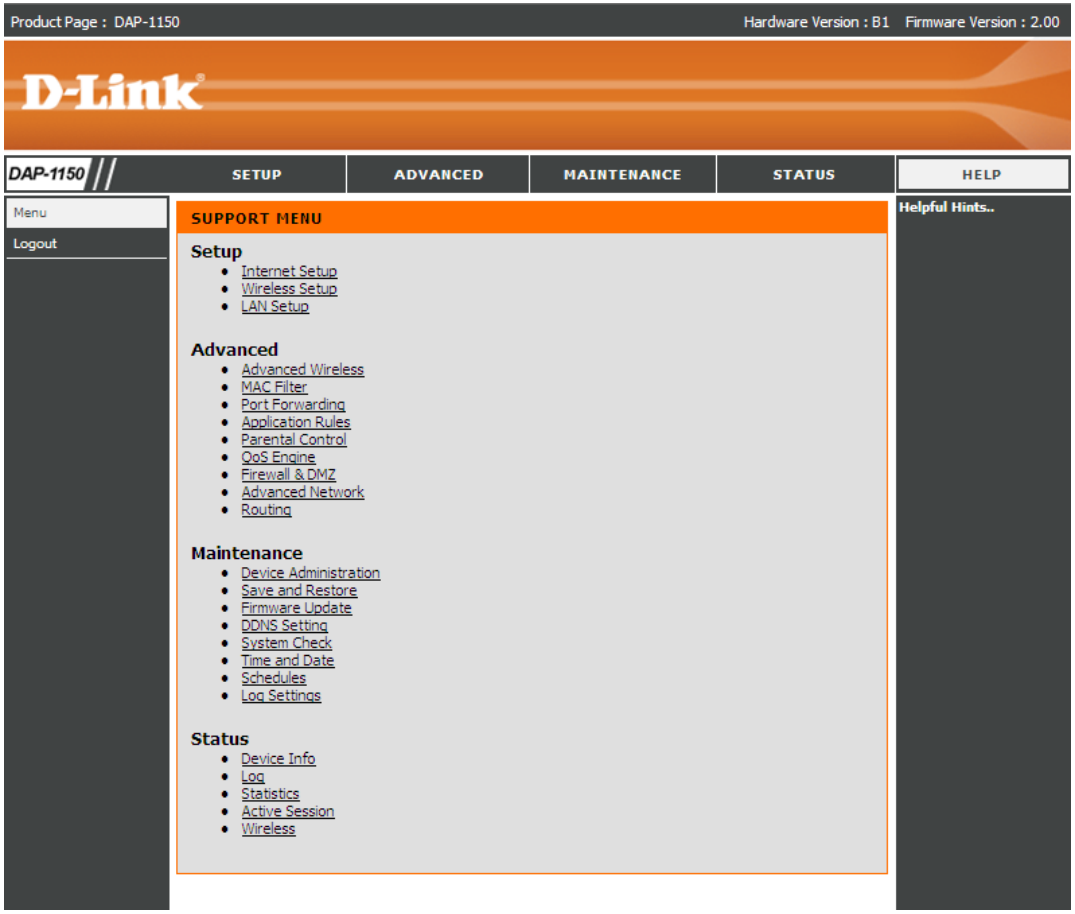
Statistics

The window below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DAP-1150 on the LAN port. The traffic counter will reset if the device is rebooted.



Help

Click the desired hyperlink to get more information about how to use the AP.



Configuration for Router Mode

Web-based Configuration Utility

If you wish to change the default settings or optimize the performance of the DAP-1150, you may use the configuration utility that D-Link has included a configuration utility for this purpose.

After you have completed the initial installation, you can access the configuration menu, at any time, by opening the web-browser and typing in the ip address of the DAP-1150. The DAP-1150's default ip address is shown below:

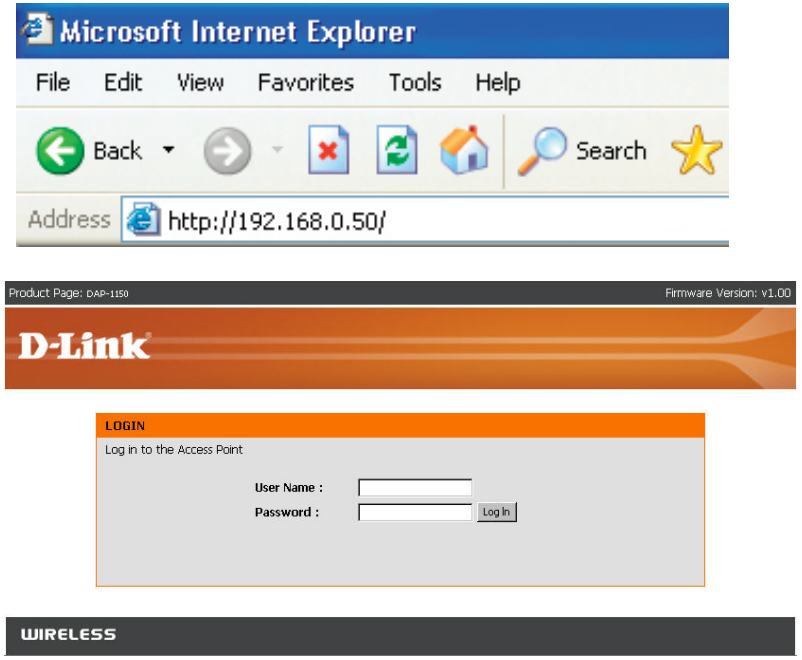
1. Open the web browser

2. Type in the **ip address** of the DAP-1150.(192.168.0.50)

3. Type **admin** in the **User Name** field

4. Leave the **Password** blank

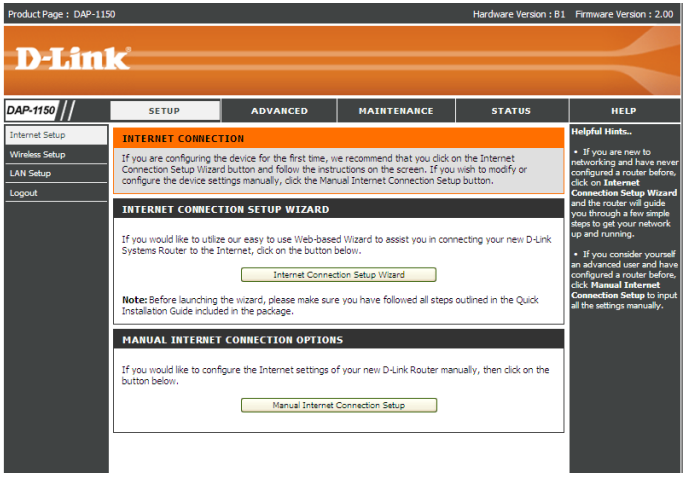
5. Click **OK**



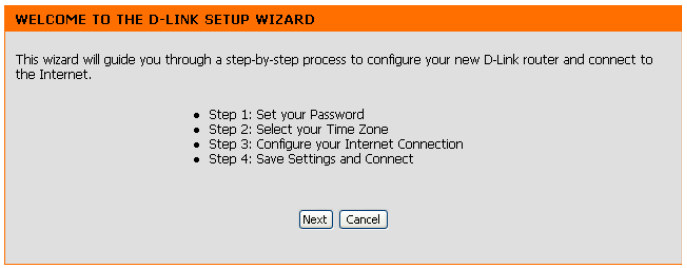
Note. **When DAP-1150 operates as Router mode, the ethernet port of DAP-1150 is configured as WAN interface, you will need to connect wirelessly to the DAP-1150 to configure it. The default SSID of DAP-1150 is "dlink".**

Setup Wizard

You may run the setup wizard from the opening Internet Setup window to quickly set up your router. Click **Internet Connection Setup Wizard**, you will be directed to the first window of the wizard.

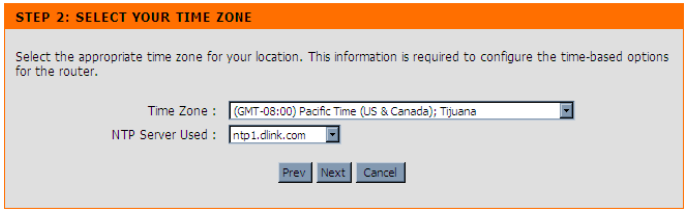


Click **Next** to continue.

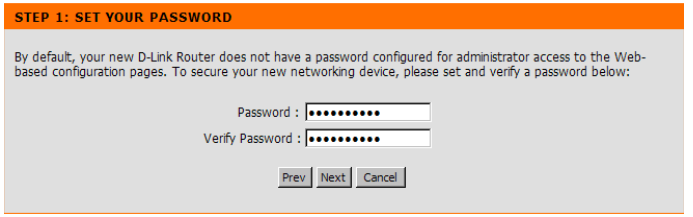


Create a new password and then click **Next** to continue.

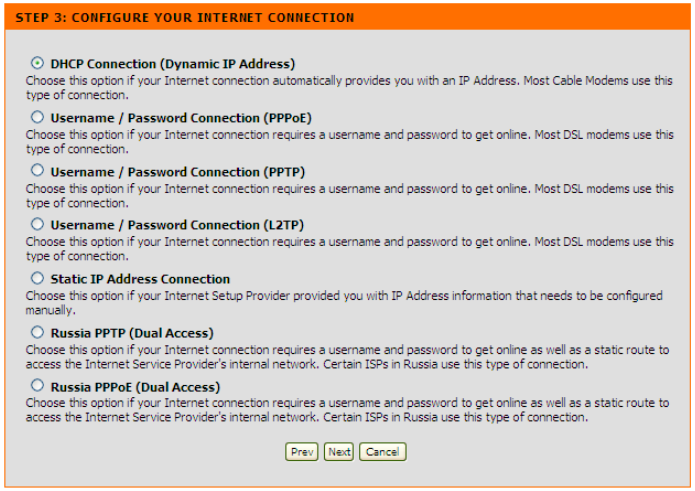
Select your time zone and NTP-server from the drop-down menu and then click **Next** to continue.



If you want to change the admin account password, enter a new password and click **Next**.

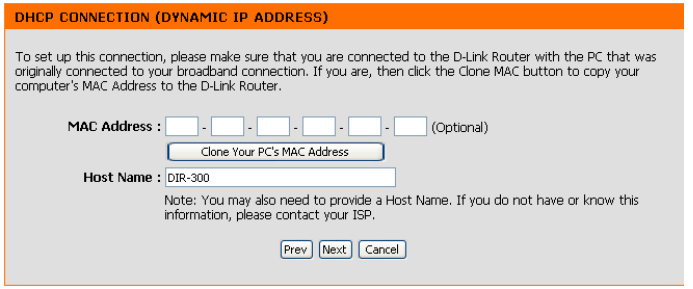


Select the type of Internet connection you use and then click **Next** to continue.

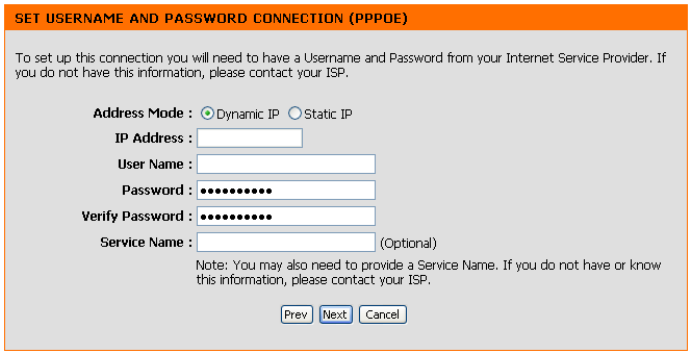


If you selected Dynamic, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click **Clone Your PC's MAC Address** and then click **Next** to continue.

The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.



If you selected PPPoE, enter your PPPoE username and password. Click **Next** to continue.

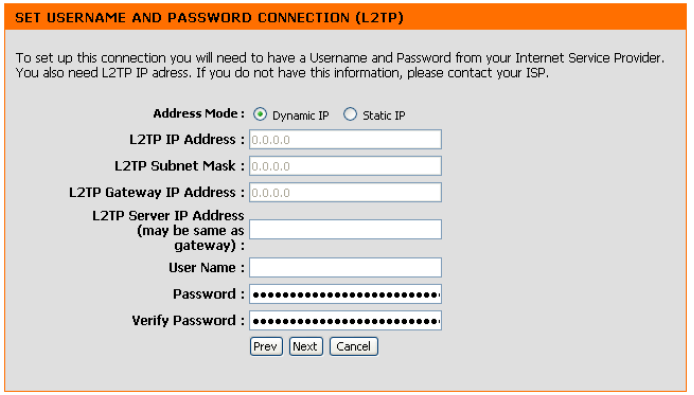


Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

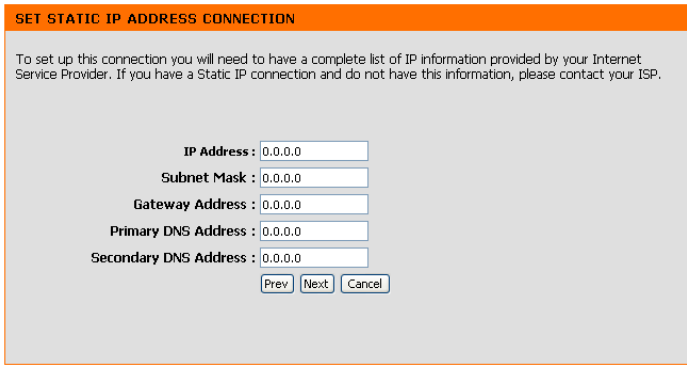
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*

If you selected PPTP, enter your PPTP username and password. Click **Next** to continue.

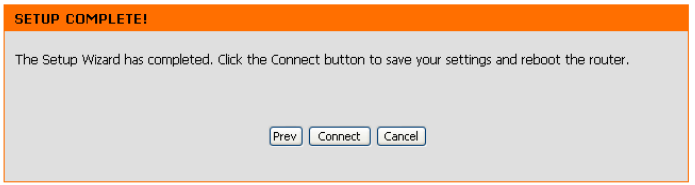
If you selected L2TP, enter your L2TP username and password. Click **Next** to continue.



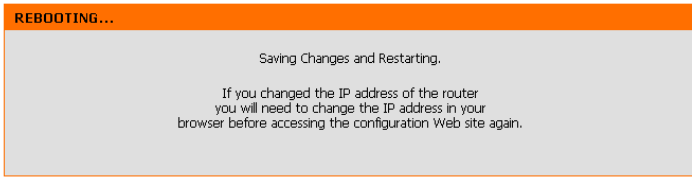
If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.



Click **Connect** to save your settings.

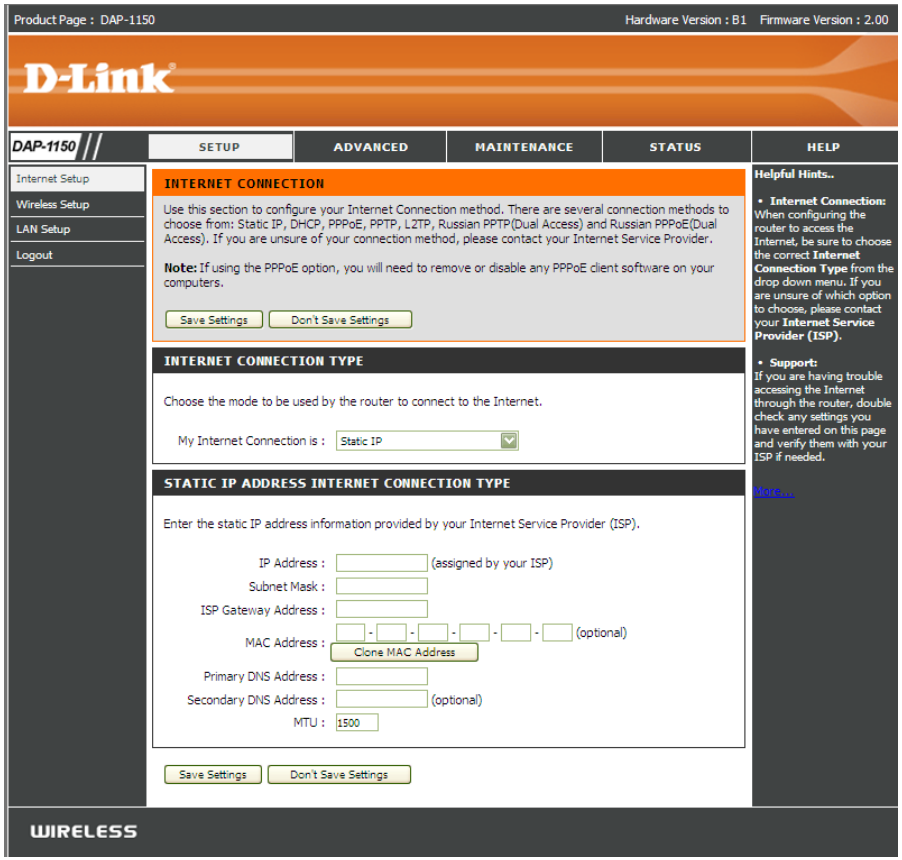


Please allow 1-2 minutes for rebooting. When the router has finished rebooting, the opening window will be displayed.



Internet Setup
Static (assigned by ISP)

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



IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

ISP Gateway Address: Enter the Gateway assigned by your ISP.

MAC Address: The default MAC Address is set to the WAN's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

Clone MAC Address: The default MAC address is set to the WAN's physical interface MAC address on the Broadband Router. You can use the **Clone MAC Address** button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with the MAC address of the router. It is not recommended that you change the default MAC address unless required by your ISP.

Primary DNS Address: Enter the Primary DNS server IP address assigned by your ISP.

Secondary DNS Address: This is optional.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. *1492* is the default MTU.

Internet Setup
Dynamic

To manually set up the Internet connection, click the **Manual Internet Connection Setup** button on the Router's opening window.

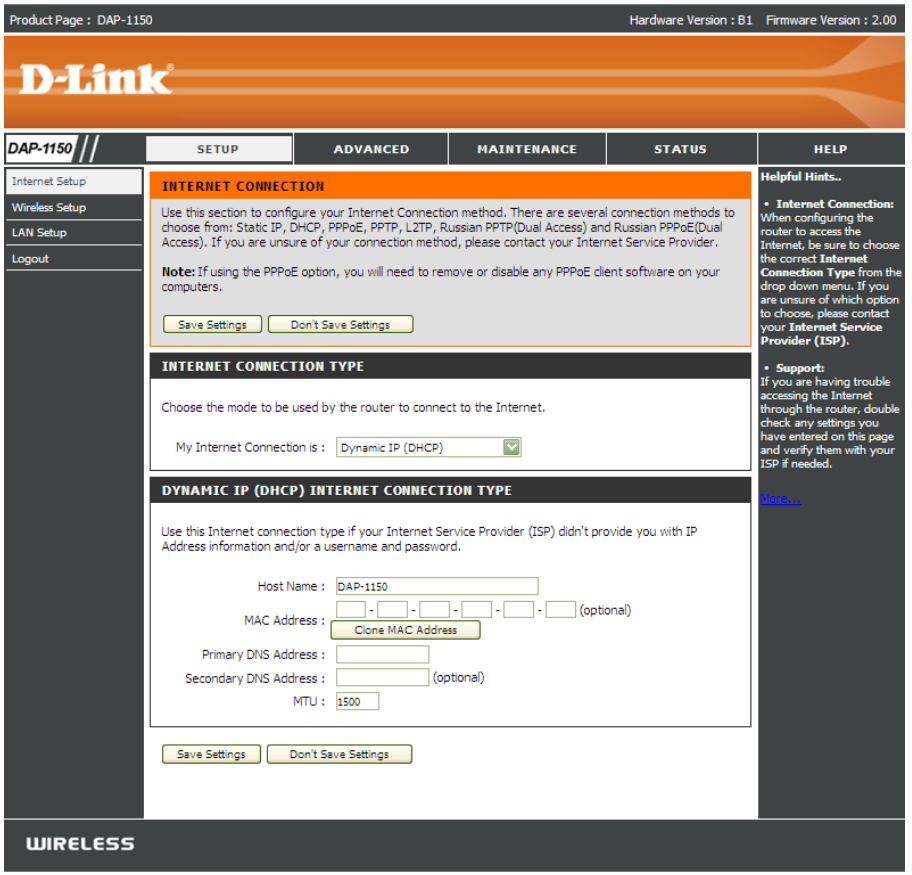
Access Point Mode: Checking this box disables NAT and turns the Router into an Access Point only.

Host Name: The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.

MAC Address: The default MAC Address is set to the WAN's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

Clone MAC Address: The default MAC address is set to the WAN's physical interface MAC address on the Broadband Router. You can use the "Clone MAC Address" button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with the MAC address of the router. It is not recommended that you change the default MAC address unless required by your ISP.

Primary / Secondary DNS Addresses: Enter the DNS (Domain Name Server) server IP address assigned by your ISP.



MTU: Maximum Transmission Unit - You may need to change the MTU for optimal performance with your specific ISP.

Internet Setup
PPPoE

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

PPPoE: Select **Dynamic** (most common) or **Static**. Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

User Name: Enter your PPPoE user name.

Password: Enter your PPPoE password and then retype the password in the next box.

Service Name: Enter the ISP Service Name (optional).

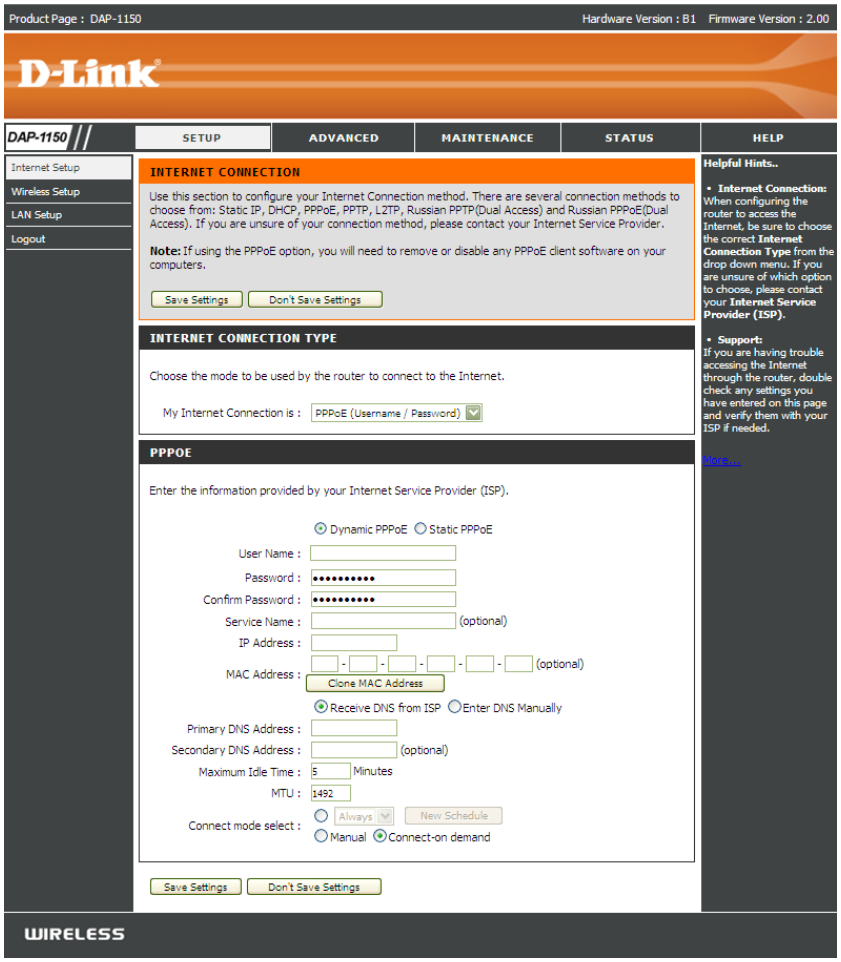
IP Address: Enter the IP address (Static PPPoE only).

DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

MTU: Maximum Transmission Unit - You may need to change the MTU for optimal performance with your specific ISP. *1492* is the default MTU.

Connection Mode Select: Select either **Always-on**, **Manual**, or **Connect-on demand**.



Internet Setup
PPTP

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

PPTP: Select **Dynamic** (most common) or **Static**. Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

IP Address: Enter the IP address (Static PPTP only).

Subnet Mask: Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

Gateway: Enter the Gateway IP Address provided by your ISP.

DNS: The DNS server information will be supplied by your ISP (Internet Service Provider.)

Server IP: Enter the Server IP provided by your ISP (optional).

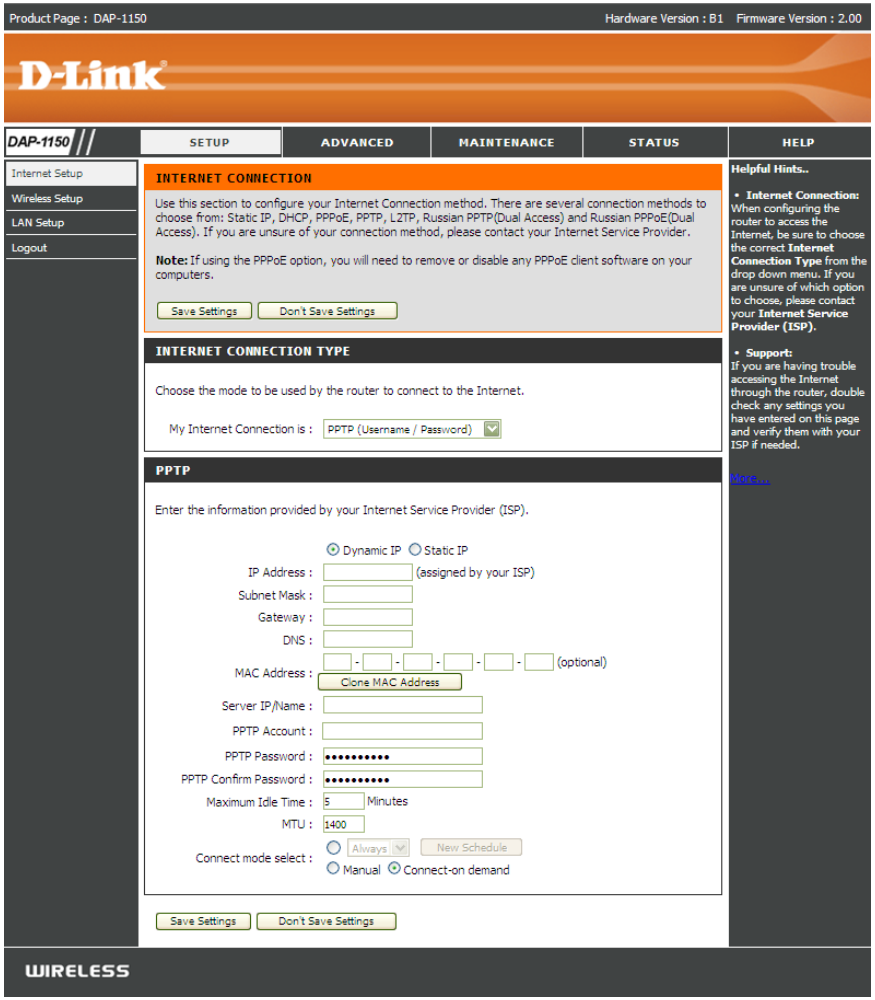
PPTP Account: Enter your PPTP account name.

PPTP Password: Enter your PPTP password and then retype the password in the next box.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

MTU: Maximum Transmission Unit - You may need to change the MTU for optimal performance.

Connect Mode: Select either Always-on, Manual, or Connect-on demand.



Internet Setup
L2TP

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

L2TP: Select **Dynamic** (most common) or **Static**. Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

IP Address: Enter the IP address (Static L2TP only).

Subnet Mask: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

Gateway: Enter the Gateway IP Address provided by your ISP.

DNS: The DNS server information will be supplied by your ISP (Internet Service Provider.)

Server IP: Enter the Server IP provided by your ISP (optional).

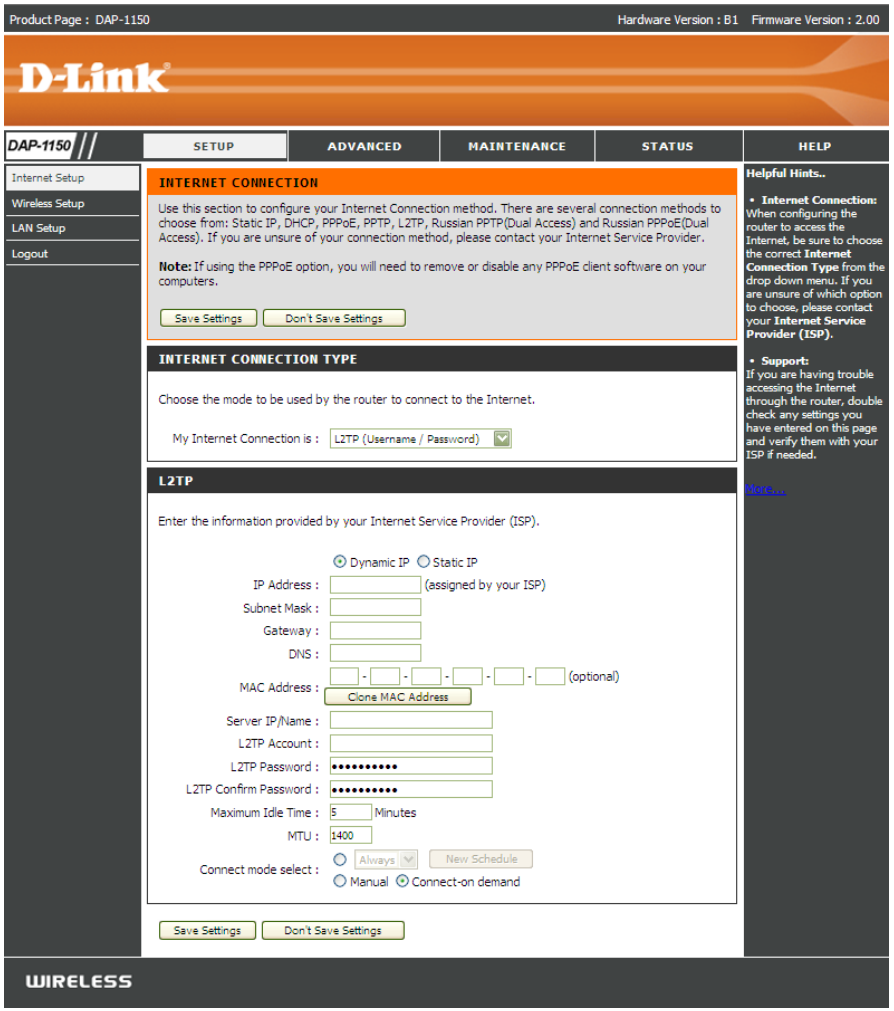
L2TP Account: Enter your L2TP account name.

L2TP Password: Enter your L2TP password and then retype the password in the next box.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

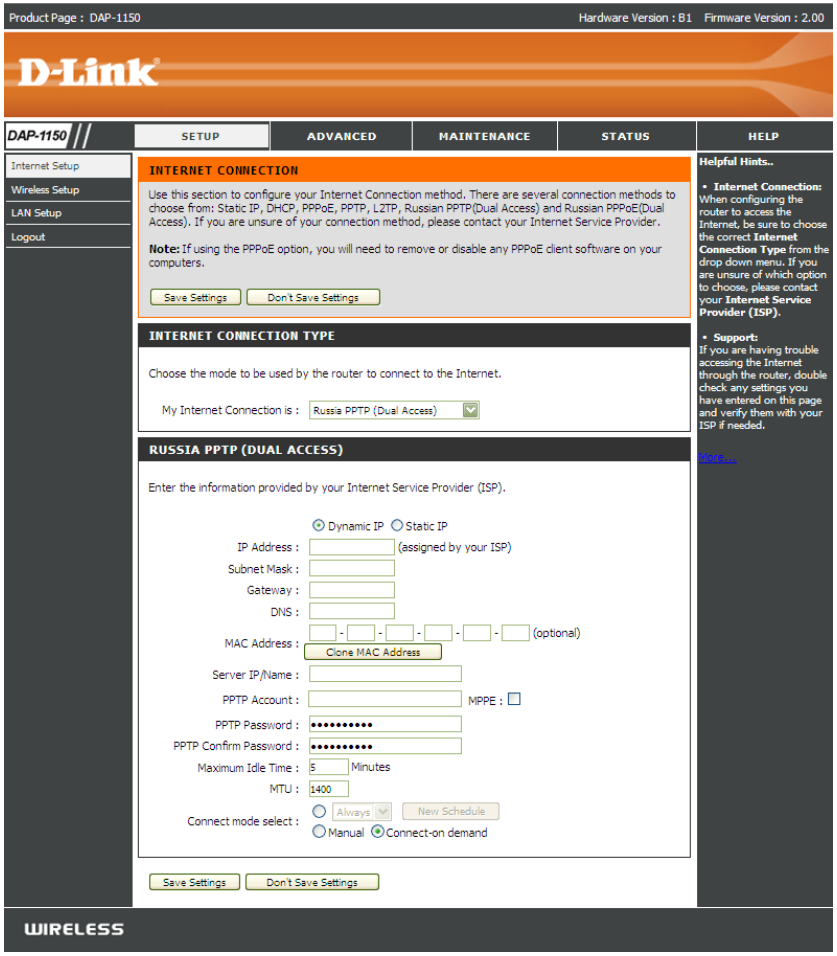
MTU: Maximum Transmission Unit - You may need to change the MTU for optimal performance with your specific ISP.

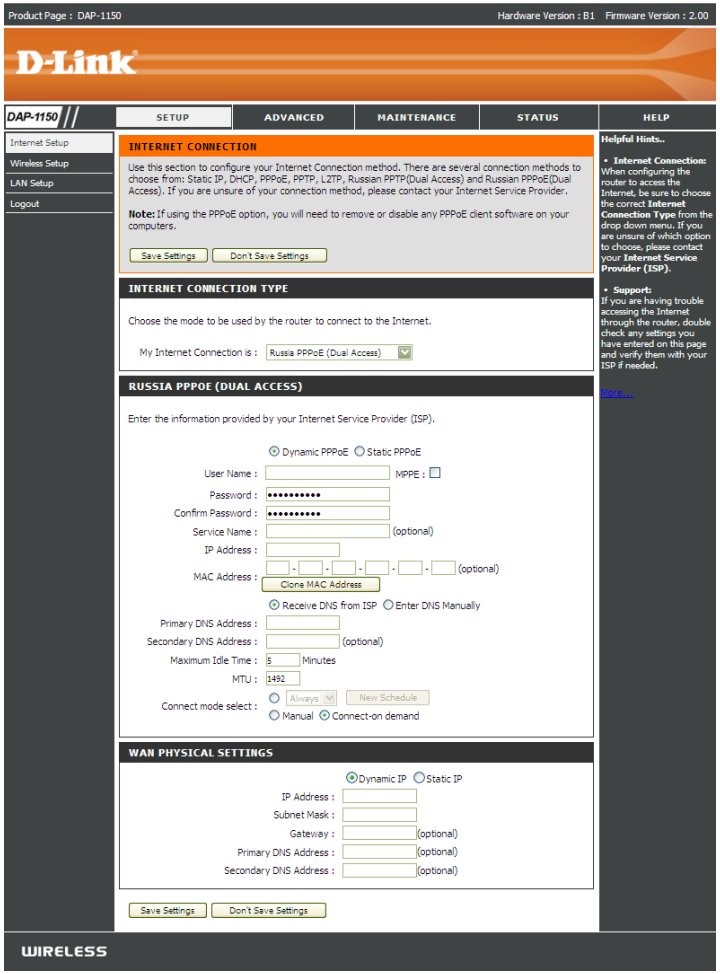
Connect Mode: Select either Always-on, Manual, or Connect-on demand.



Internet Setup
Dual Access (for Russia only)

There are two main steps to configure a Dual Access Internet connection for Russia. First, configure a PPPoE connection (as previously described for PPPoE connections), and add the physical WAN IP settings as instructed from the ISP. Second, configure a PPTP connection (as previously described for PPTP connections). In addition, the second step also includes an option to use a MAC address that will always be associated with the connection. The MAC address is entered manually or copied from the computer.





Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Enable Wireless Channel: Indicates the channel setting for the DAP-1150. By default the channel is set to *6*. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. The **Auto Channel Selection** setting can be selected to allow the DAP-1150 to choose the channel with the least amount of interference.

Transmission Rate: Use the drop-down menu to select the appropriate Transmission Rate in Mbits per second. Many users will want to use the default setting, *Best (automatic)*.

WMM Enable: Enable Wi-Fi Multimedia to enjoy basic quality of service features. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background.

Enable Hidden Wireless: Check this option if you would not like the SSID of your wireless network to be broadcasted by the DAP-1150. If this option is checked, the SSID of the DAP-1150 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DAP-1150 in order to connect to it.

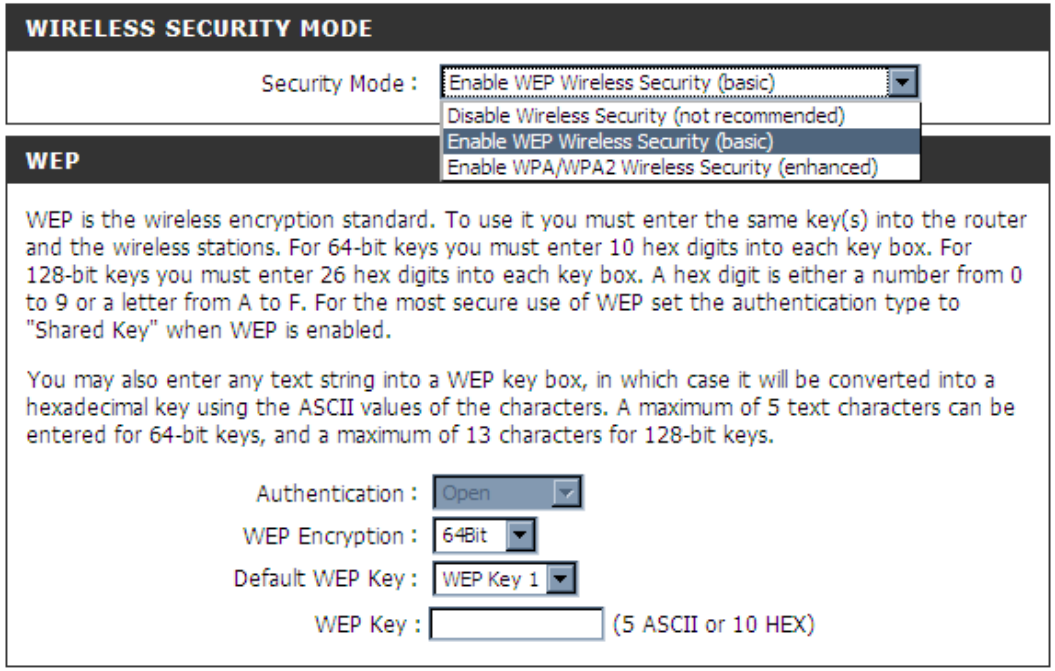
1. To enable wireless security on the Router, use the drop-down menu to select the desired option. To enable WEP, select *Enable WEP Wireless Security (basic)*.

2. Next to **Authentication**, select either *Open* or *Shared Key*. Shared Key provides greater security.

3. Select either *64Bit* or *128Bit* encryption from the drop-down menu next to **WEP Encryption**.

4. Next to **Default Key Type**, select *WEP Key 1* and enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using *Hex* or *ASCII*. *Hex* is recommended (letters A-F and numbers 0-9 are valid). In *ASCII* all numbers and letters are valid.

5. Click **Save Settings** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the Router.



NOTE:
It is recommended to enable encryption on your wireless Router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

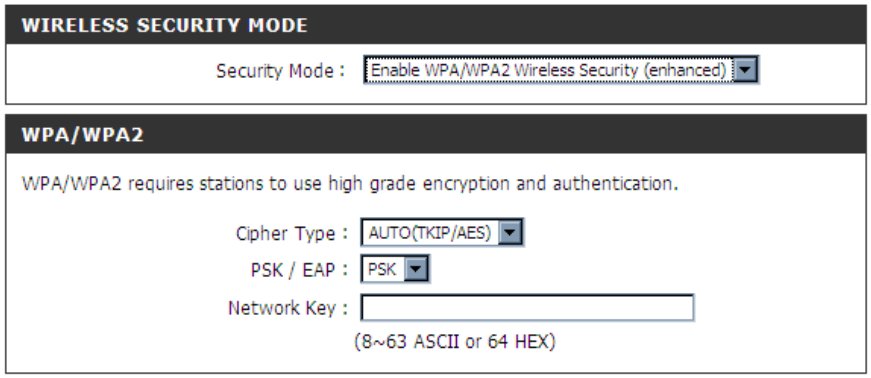
1. To enable *Enable WPA/WPA2 Wireless Security (enhanced).*

2. Next to **Cipher Type**, select *TKIP*, *AES*, or *AUTO*.

3. Next to **PSK/EAP**, select *PSK*.

4. Next to **Network Key**, enter a passphrase. The key 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.

5. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA/WPA2 (whichever of the three options you have selected above) on your adapter and enter the same network key as you did on the router.



1. To enable WPA/WPA2 for a RADIUS server, next to **Security Mode**, selec or *Enable WPA/WPA2 Wireless Security (enhanced)*.

2. Next to **Cipher Type**, select *TKIP*, *AES*, or *Auto*.

3. Next to **PSK/EAP**, select *EAP*.

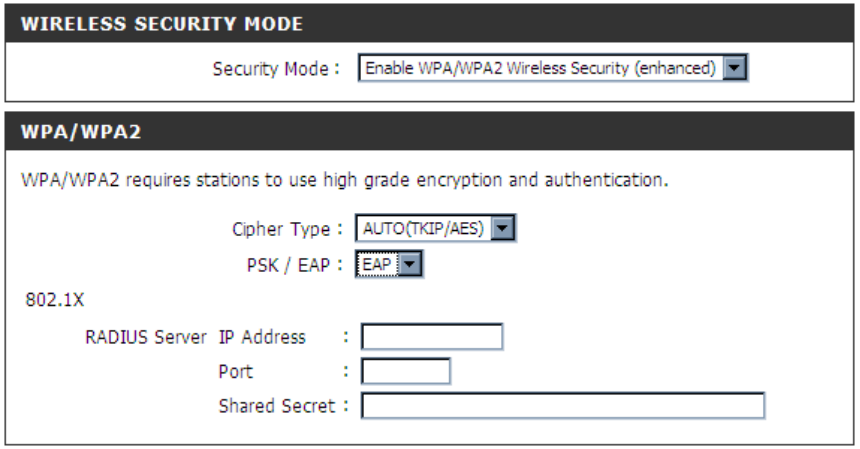
4. Next to **RADIUS Server 1** enter the **IP Address** of your RADIUS server.

5. Next to **Port**, enter the port you are using with your RADIUS server. *1812* is the default port.

6. Next to **Shared Secret**, enter the security key.

7. If you have a secondary RADIUS server, enter its IP address, port, and secret key.

8. Click **Save Settings** to save your settings.



LAN Setup

This section will allow you to change the local network settings of the router and to configure the DHCP settings.

Router IP Address: Enter the IP address of the router. The default IP address is 192.168.0.50.

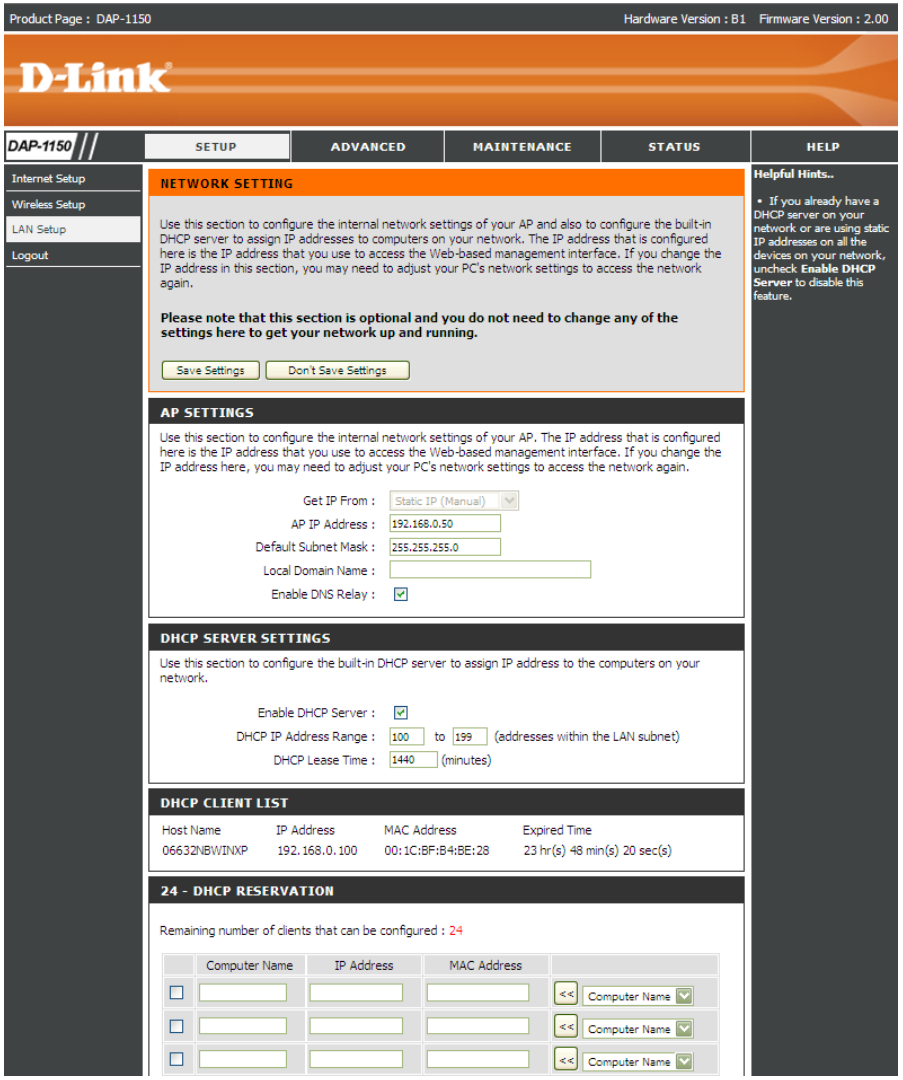
If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Local Domain Name: Enter the Domain name (Optional).

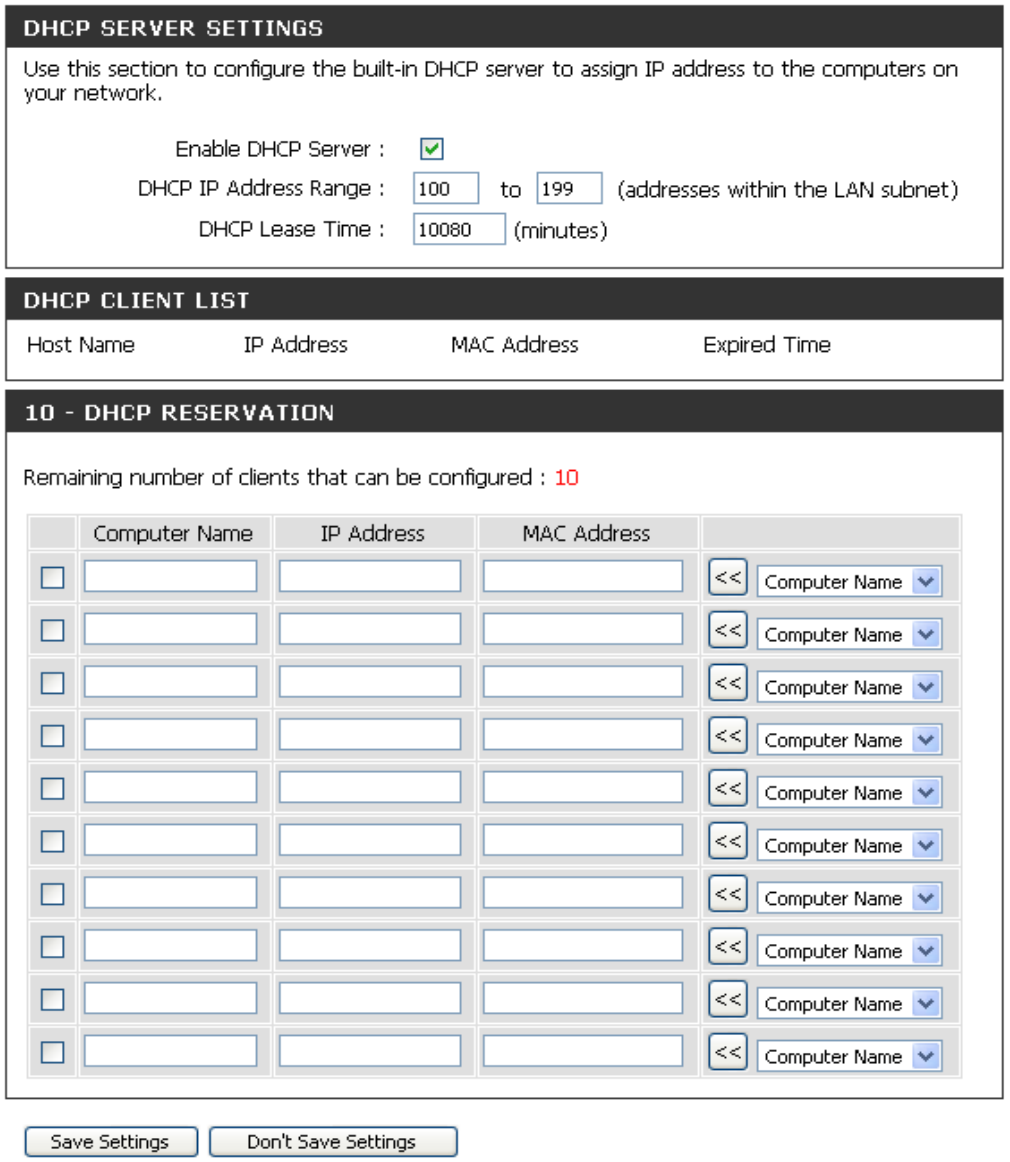
Enable DNS Relay: Check the box to transfer the DNS server information from your ISP to your computers. If unchecked, your computers will use the router for a DNS server.

Refer to the next page for DHCP information.



DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DAP-1150 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DAP-1150. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.



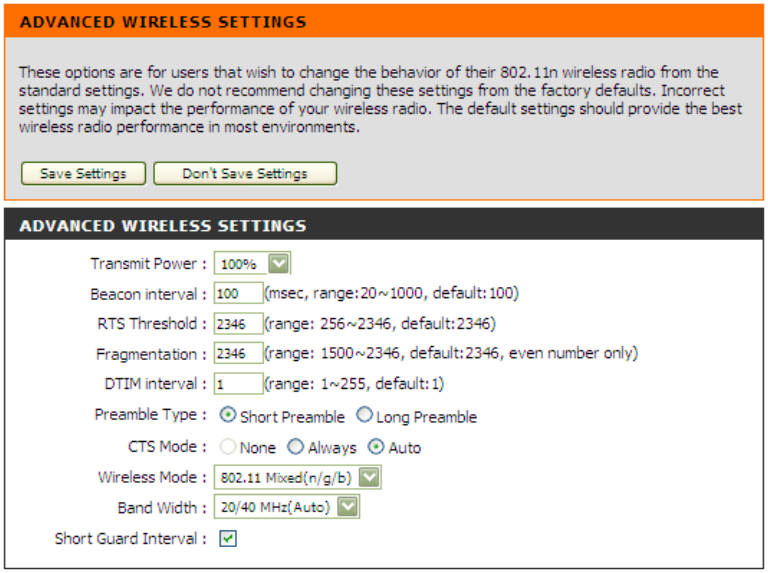
Enable DHCP Server: Check the box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Advanced Wireless

This window allows you to change the behavior of the 802.11g wireless radio from the standard settings. Please be aware that any changes to the factory default settings may adversely affect the behavior of your network.



Transmit Power: Set the transmit power of the antennas.

Beacon interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. *100* is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of *2346*. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. *2346* is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) *1* is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Preamble Type: Select Short or Long Preamble. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters. Auto is the default setting. Note: High network traffic areas should use the shorter preamble type.

CTS Mode: CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). CTS will make sure the wireless network is clear before a wireless client attempts to send wireless data. Enabling CTS will add overhead and may lower wireless through put. **None:** CTS is typically used in a pure 802.11g environment. If CTS is set to “None” in a mixed mode environment populated by 802.11b clients, wireless collisions may occur frequently. **Always:** CTS will always be used to make sure the wireless LAN is clear before sending data. **Auto:** CTS will monitor the wireless network and automatically decide whether to implement CTS based on the amount of traffic and collisions that occurs on the wireless network.

802.11 Mode: 802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11n, 802.11b, and 802.11g - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Auto 20/40: Select if you are using both 802.11n and non-802.11n wireless devices.

20MHz: Select if you are not using any 802.11n wireless clients. This is the default setting.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it’s less reliable and may create higher data loss.

MAC Filter

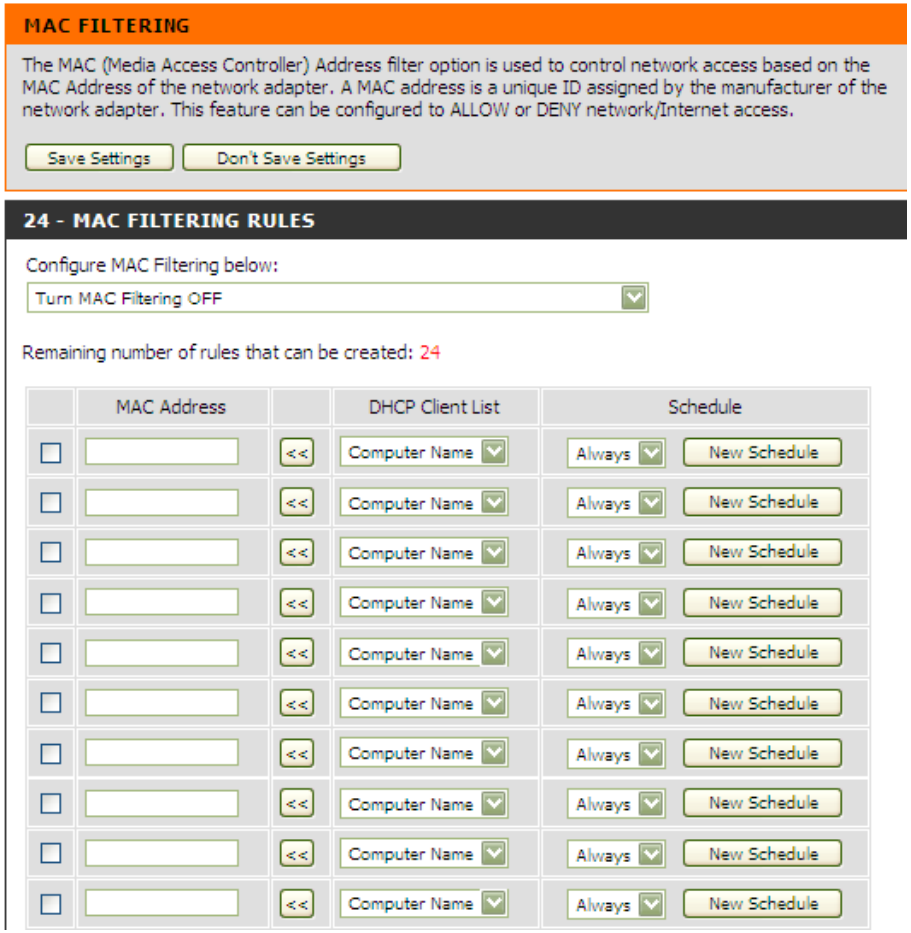
Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Internet via Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

Configure MAC Filter: Select *Turn MAC Filtering OFF*, *Turn MAC Filtering ON and ALLOW computers listed to access the network*, or *Turn MAC Filtering ON and DENY computers listed to access the network*.

MAC Address: Enter the MAC address you would like to filter. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

DHCP Client List: Select a DHCP client from the drop-down menu and click the arrow to copy that MAC Address.

Schedule: The schedule of time when the network filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.



Port Forwarding

This will allow you to open a single port or a range of ports.

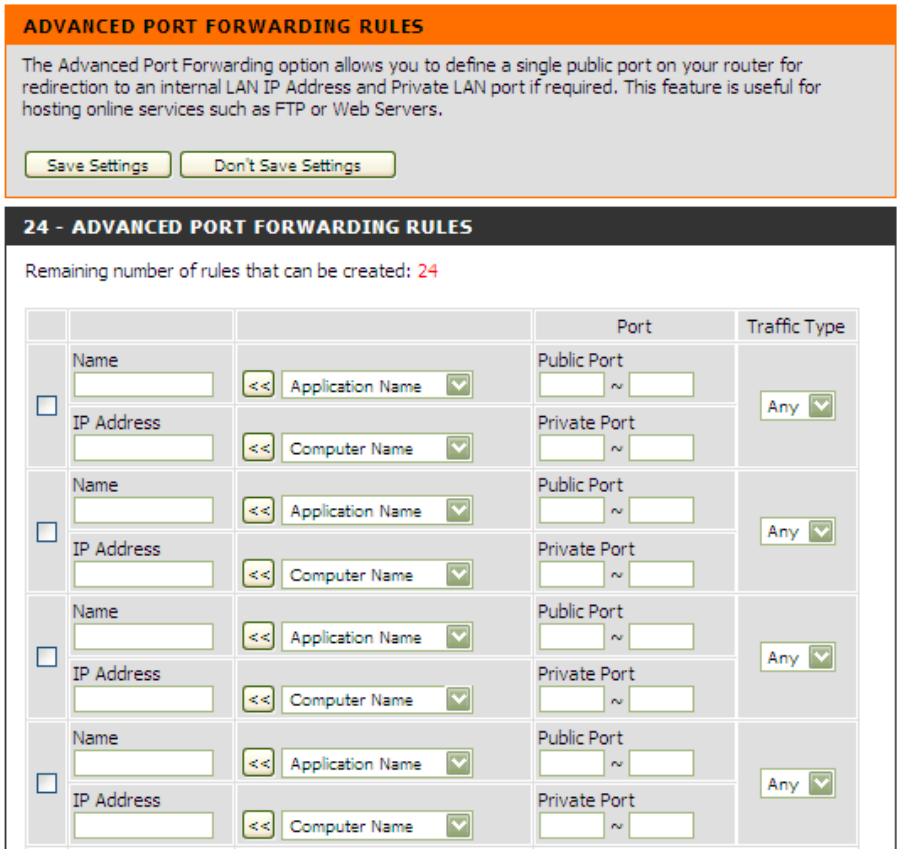
Rule: Check the box to enabled the rule.

Name: Enter a name for the rule.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to.

Start Port/ End Port: Enter the port or ports that you want to open. If you want to open one port, enter the same port in both boxes.

Traffic Type: Select *TCP*, *UDP*, or *Any*



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DAP-1150.

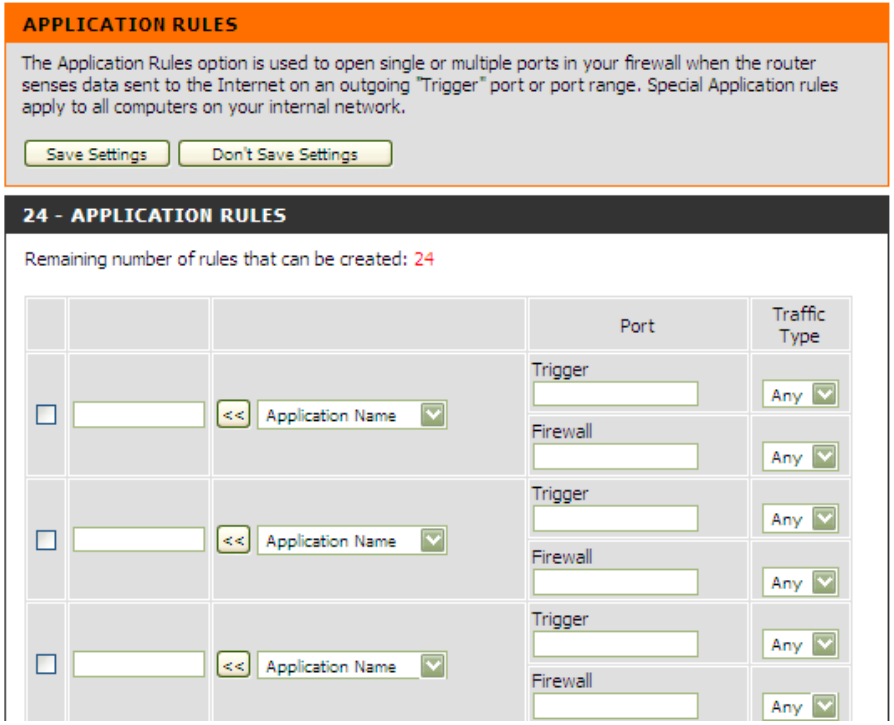
Rule: Check the box to enable the rule.

Name: Enter a name for the rule.

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

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: Select *TCP*, *UDP*, or *Any*.



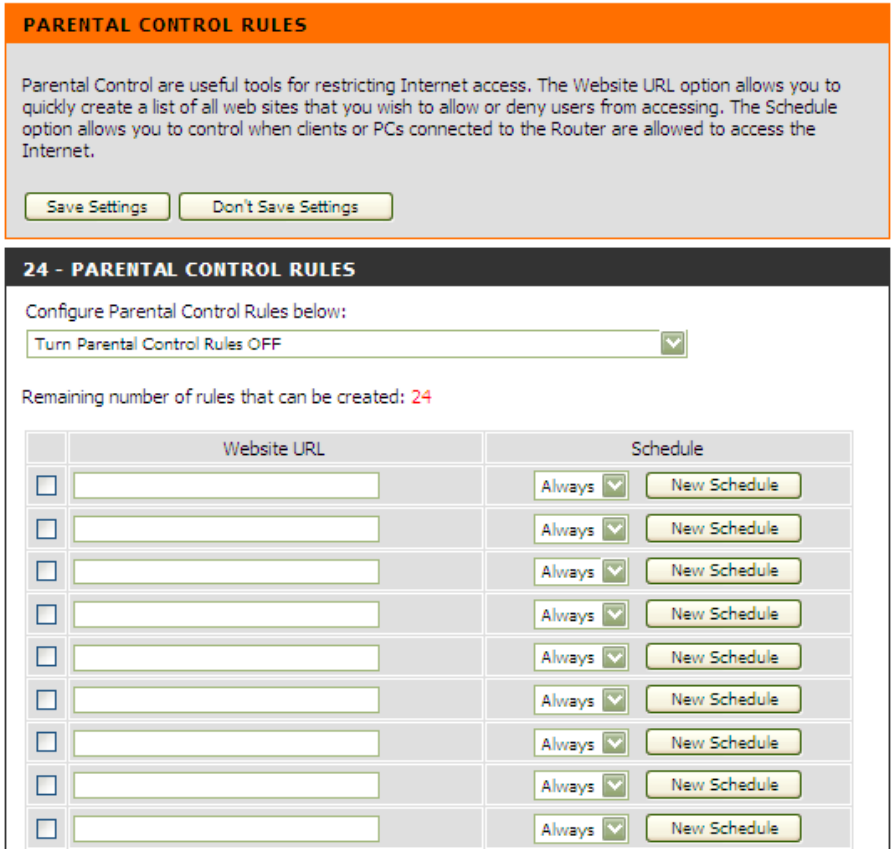
Parental Control

This feature allows you to create a list of websites that you want to either allow or deny users access.

Configure Parental Control: Select *Turn Parental Control OFF*, *Turn Parental Control ON and ALLOW computers access to ONLY these sites*, or *Turn Parental Control ON and DENY computers access to ONLY these sites*.

Website URL: Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked.

Schedule: The schedule of time when the parental control filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.



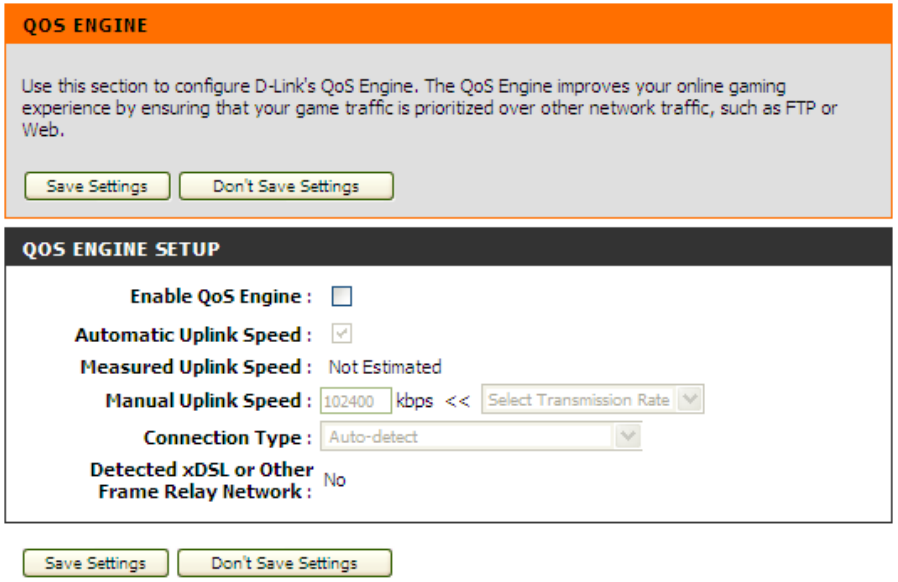
QoS Engine

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

Enable QOS: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Uplink Speed: This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

Measured Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.



Connection Type: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the Internet settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL: When Connection Type is set to automatic, the automatically detected connection type is displayed here.

Firewall & DMZ

This section will allow you to set up a DMZ host and to set up firewall rules.

If you have a client PC that cannot run Internet applications properly from behind the DAP-1150, then you can set the client up for unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

Enable SPI: Check this to enable SPI.

Enable DMZ Host: Check this box to enable DMZ.

DMZ IP Address: Enter the IP address of the computer you would like to open all ports to.

Name: Choose a name for the firewall rule.

Action: Select to *Allow* or *Deny* transport of the data packets according to the criteria defined in the rule.

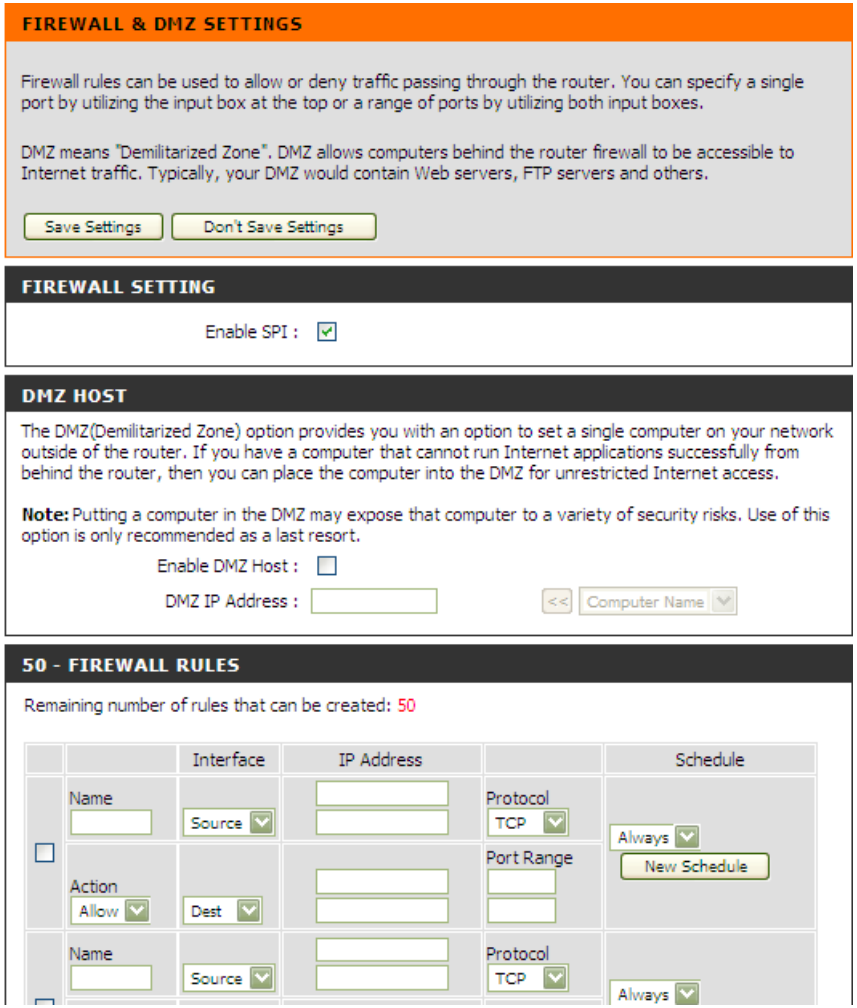
Source/Dest: The Source/Destination is the TCP/UDP port on either the LAN or WAN side.

Schedule: Click **New Schedule** to access the Schedules window. See **Maintenance>Schedules** for more information.

IP Address: Enter a beginning and ending IP address.

Protocol: Select the transport protocol that will be used for the filter rule.

Port Range: Enter the desired port range for the filter rule.



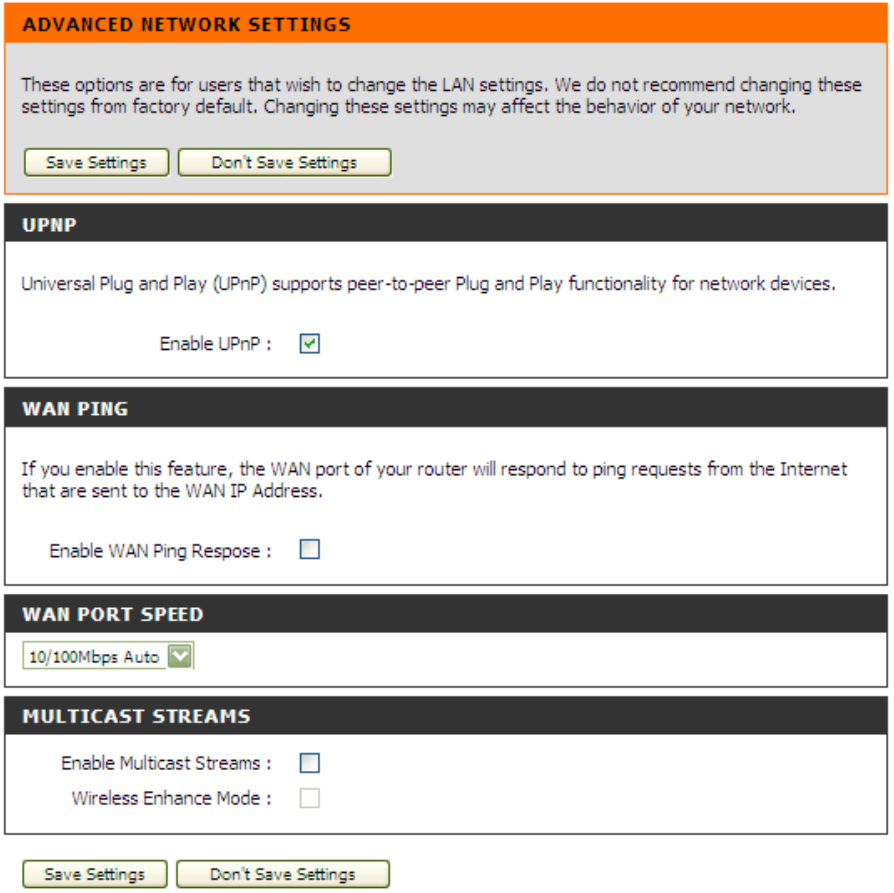
Advanced Network

This window allows you to change the LAN settings. Please be aware that any changes to the factory default settings may affect the behavior of your network.

Enable UPnP: To use the Universal Plug and Play (UPnP™) feature tick this checkbox. UPNP provides compatibility with networking equipment, software and peripherals.

Enable WAN Ping Respond: Unchecking the box will not allow the DAP-1150 to respond to Pings. Blocking the Ping may provide some extra security from hackers. Tick this checkbox to allow the WAN port to be “Pinged”.

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



Routing

This option allows you to define fixed routes to defined destinations.

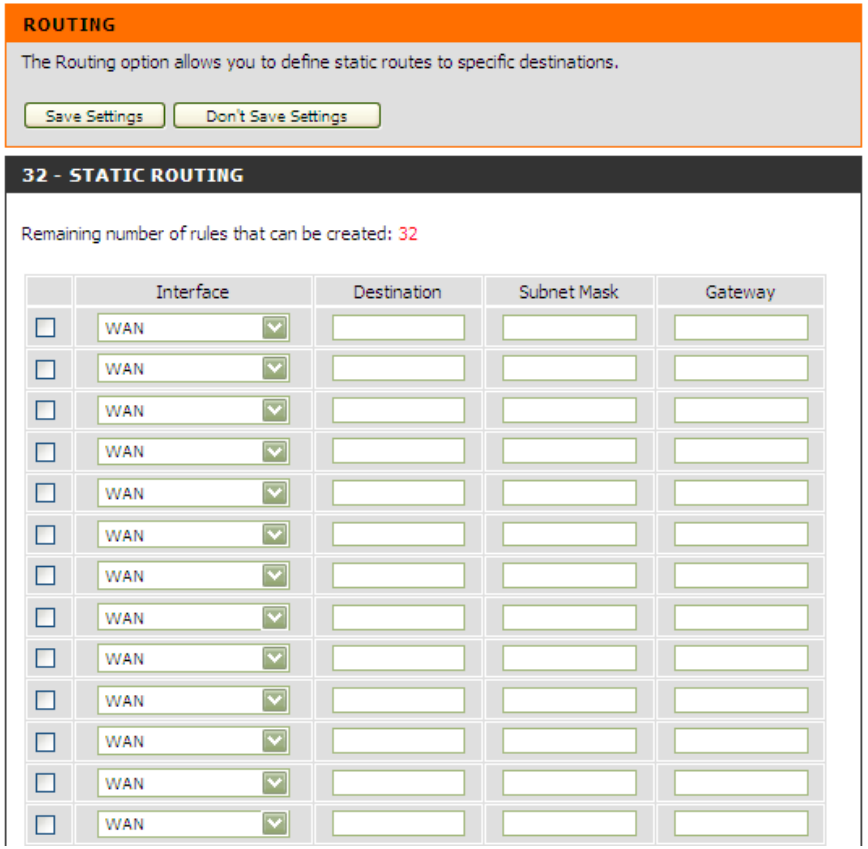
Enable: Tick this checkbox to enable or disable fixed routes to defined destinations.

Interface: Use the drop-down menu to choose the *WAN or WAN (Physical Port)* Interface the IP packet must use to transit out of the Router.

Destination: The IP address of the packets that will take this route.

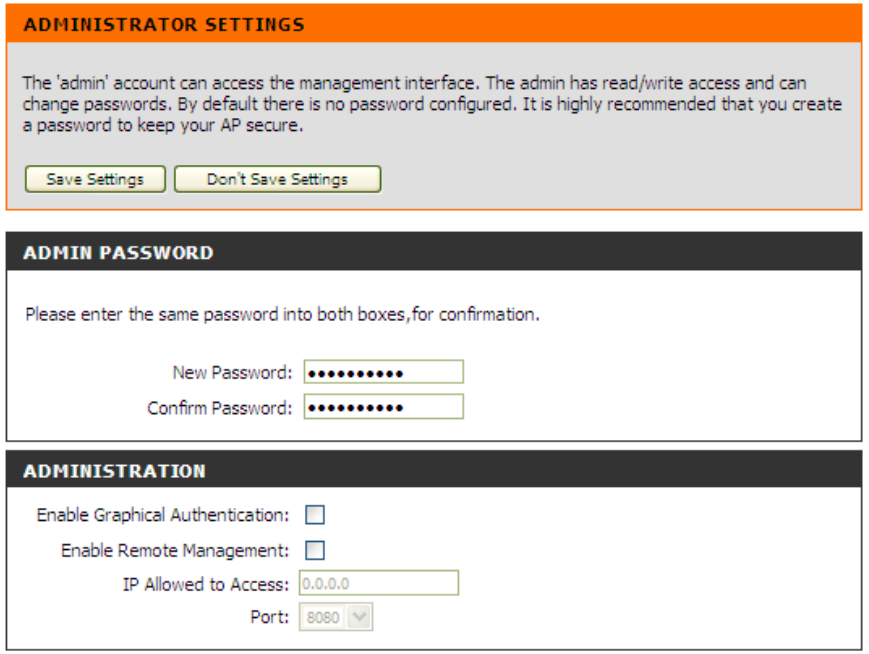
Subnet Mask: The subnet of the IP address of the packets that will take this route.

Gateway: Specifies the next hop to be taken if this route is used.



Device Administration

This window will allow you to change the Administrator password. You can also enable Remote Management.



Administrator Login Name: Enter a new Login Name for the Administrator account.

Administrator Password: Enter a new password for the Administrator Login Name and then retype the new password in the Confirm Password textbox. The administrator can make changes to the settings.

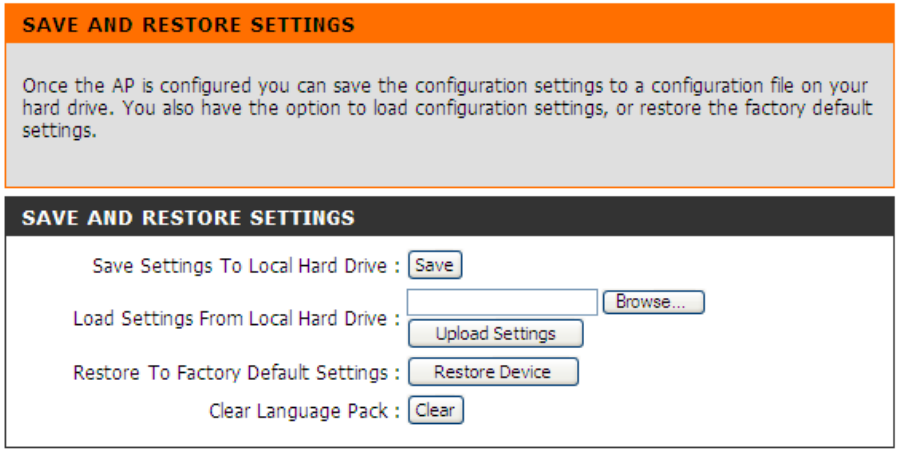
Enable Remote Management: Remote management allows the DAP-1150 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

IP Allowed to Access: The Internet IP address of the computer that has access to the Broadband Router. If you input an asterisk (*) into this field, then any computer will be able to access the Router. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port: The port number used to access the DAP-1150. For example: http://x.x.x.x:8080 whereas x.x.x.x is the WAN IP address of the DAP-1150 and *8080* is the port used for the Web-Management interface.

Save and Restore

This window allows you to save your configuration file to a hard drive, load configuration settings from a hard drive, and restore the Router's factory default settings.



Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the **Browse** control to find a previously save file of configuration settings. Then, click the **Upload Settings** button to transfer those settings to the Router.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the **Save** button above.

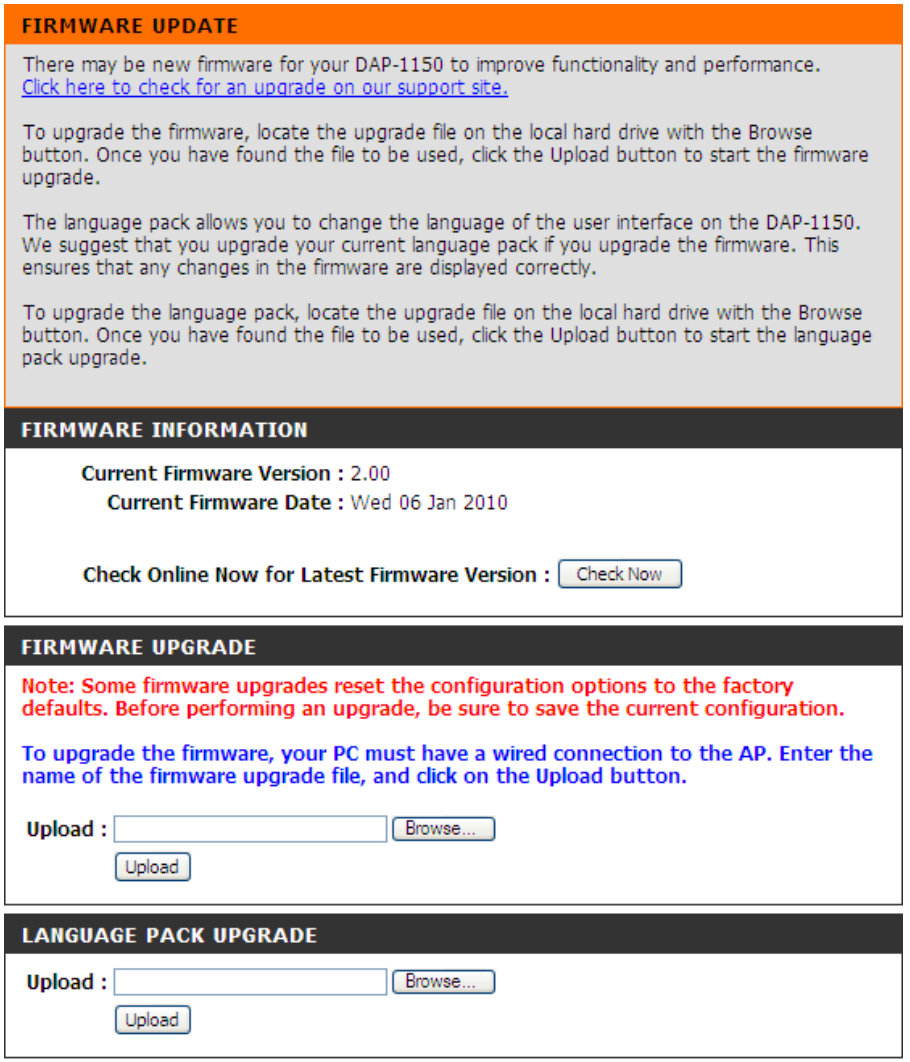
Reboots: Click the **Reboots** button on the left side of the window to restart the Router.

Firmware Update

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade: Click the **Check Now** button (or the link at the top of the window) to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Save Settings** to complete the firmware upgrade.



DDNS Setting

The router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form “hostname.dyndns.org”. Many ISPs assign public IP addresses using DHCP, this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

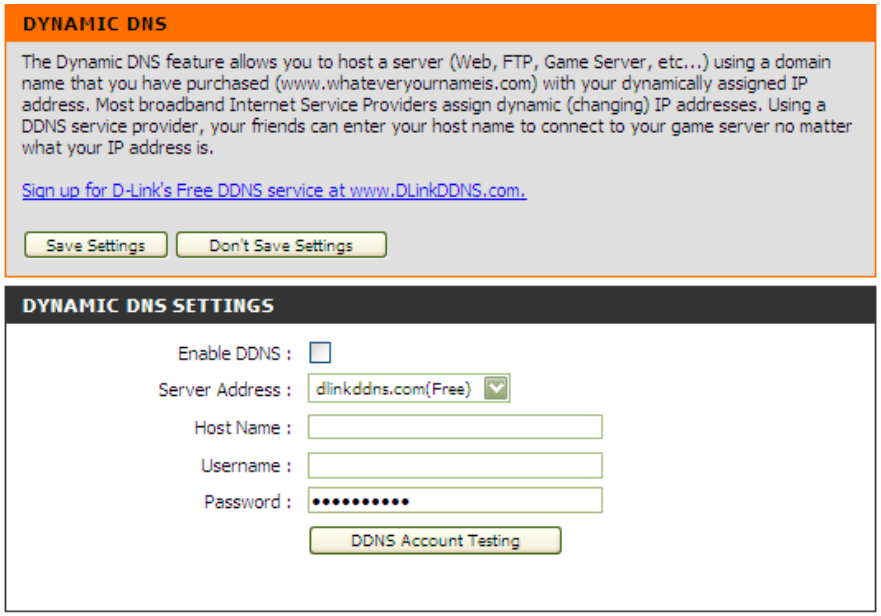
Enable DDNS: Tick the Enable DDNS checkbox to enable support for DDNS.

Server Address: Select one of the DDNS registration organizations form those listed in the pull-down menu. Available servers include *dlinkddns.com(Free)*, *DynDns.org(Custom)*, *Dyn.Dns.org(free)*, and *Dyn.Dns.org(Static)*.

Host Name: Enter the host name of the DDNS server.

Username: Enter the username given to you by your DDNS server.

Password: Enter the password or key given to you by your DDNS server.

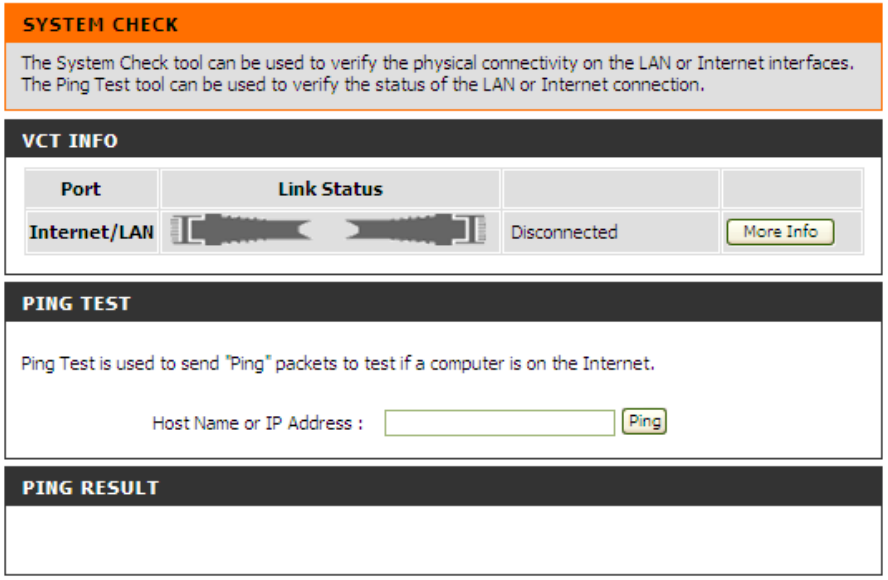


System Check

This tool is used to verify the physical connectivity on both the LAN and the WAN interfaces. The Ping Test can be used to test the status of the Internet.

Virtual Cable Tester (VCT) Info: VCT is an advanced feature that integrates a LAN cable tester on every Ethernet port on the router. Through the graphical user interface (GUI), VCT can be used to remotely diagnose and report cable faults such as opens, shorts, swaps, and impedance mismatch. This feature significantly reduces service calls and returns by allowing users to easily troubleshoot their cable connections.

Ping Test: The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click **Ping**.



Time and Date

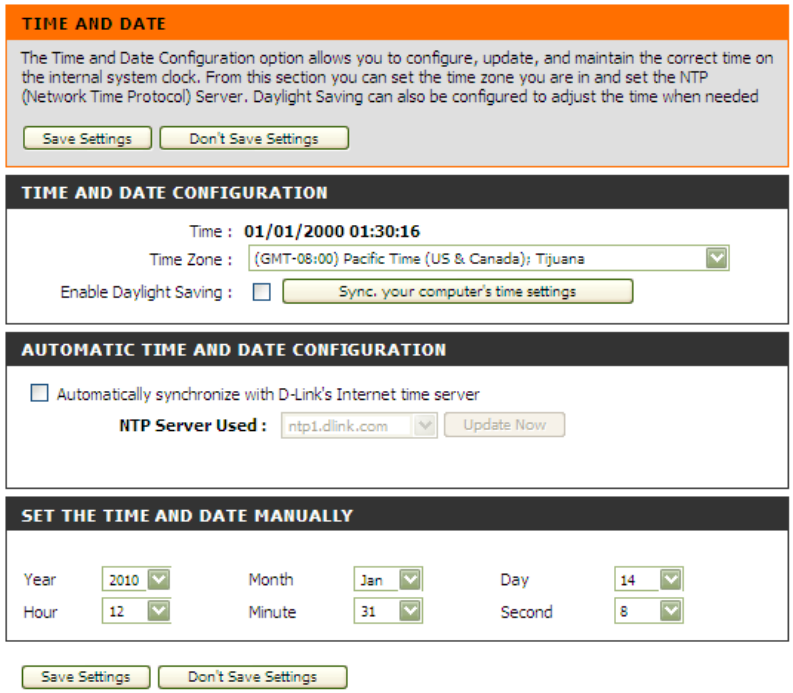
This section will allow you to configure, update, and maintain the correct time on the internal system clock.

Time Zone: Select the Time Zone from the drop-down menu.

Enable Daylight Saving: Ticking this checkbox enables Daylight Saving time. Click **Sync. your computer's time settings** to copy your PC's time settings.

NTP Server Used: Tick the "Automatically synchronize with D-Link's Internet time server" checkbox and then use the drop-down menu to select an NTP Server. NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers.

Manual: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second. Click **Save Settings**.



Schedules

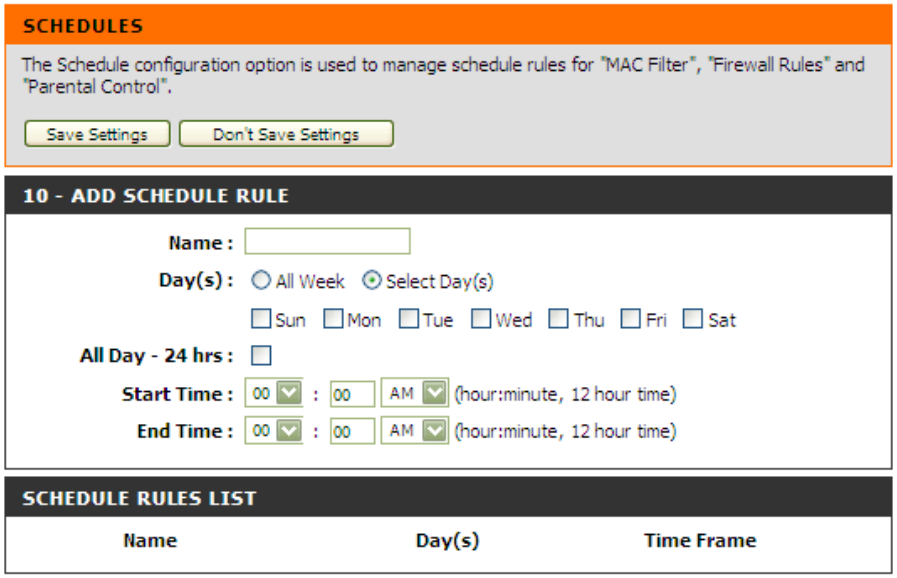
The Router allows the user the ability to manage schedule rules for various firewall and parental control features on this window. Once you have finished configuring the new schedule rule, click the **Save Settings** button at the top of the window.

Name: Enter a name for the new schedule rule.

Day(s): Choose the desired day(s), either All Week or Select Days. If the latter is selected, please use the checkboxes directly below to specify the individual days.

All Day - 24 hrs: Tick this check box if the new schedule rule applies to the full 24-hour period.

Start Time/ End Time: If the new schedule rule does not apply to the full 24-hour period, untick the previous checkbox and then enter a specific beginning and ending time.



Log Settings

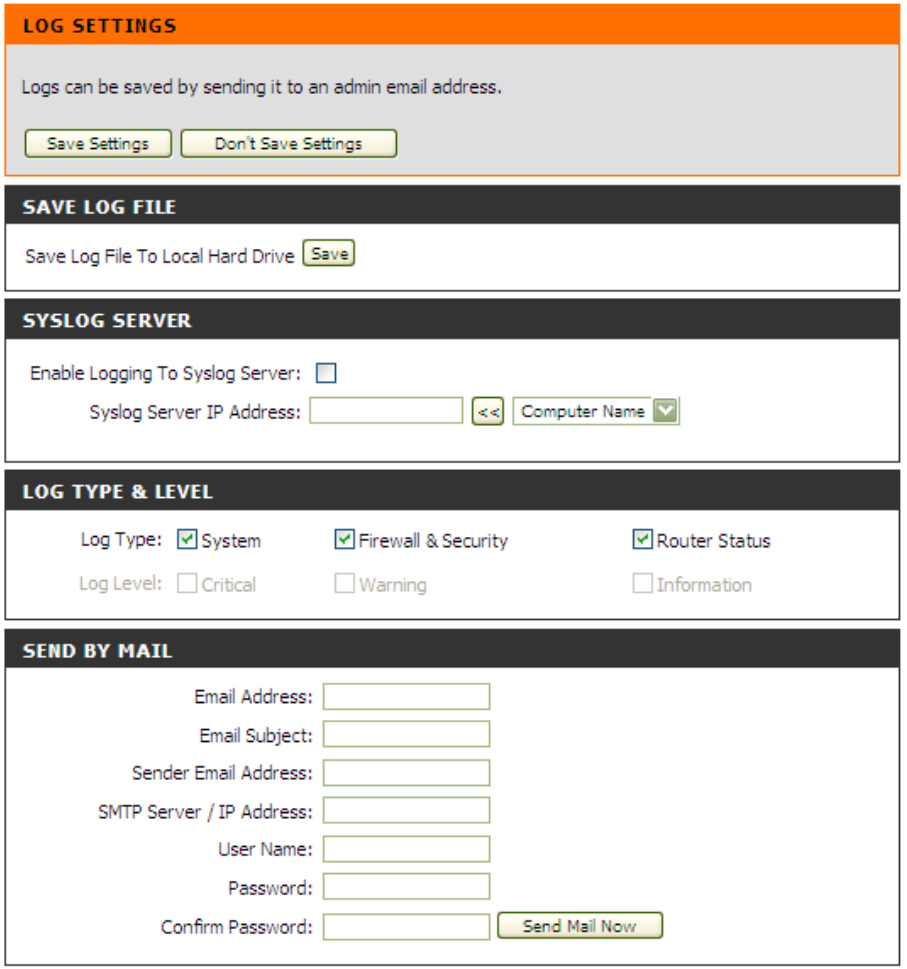
The system log displays chronological event log data specified by the router user. You may also save a simple text file containing the log to your computer. Click the **Save** button and follow the prompts to save the file.

Save Log File: Click on the **Save** button link on this window to save the log file to your local hard drive.

Syslog Server: click the checkbox to save the log in the log server in the LAN side.

Log Type & Level: Click the checkbox(es) of the type of log information requested: **"System, Firewall & Security, Router Status, Critical, Warning and Information"**

Send by Mail: Enter the your SNTP server name(or IP address) and enter your mail address before sending your system log by mail.



Device Info

This window displays the current information for the DAP-1150. It will display the LAN, WAN, and Wireless information.

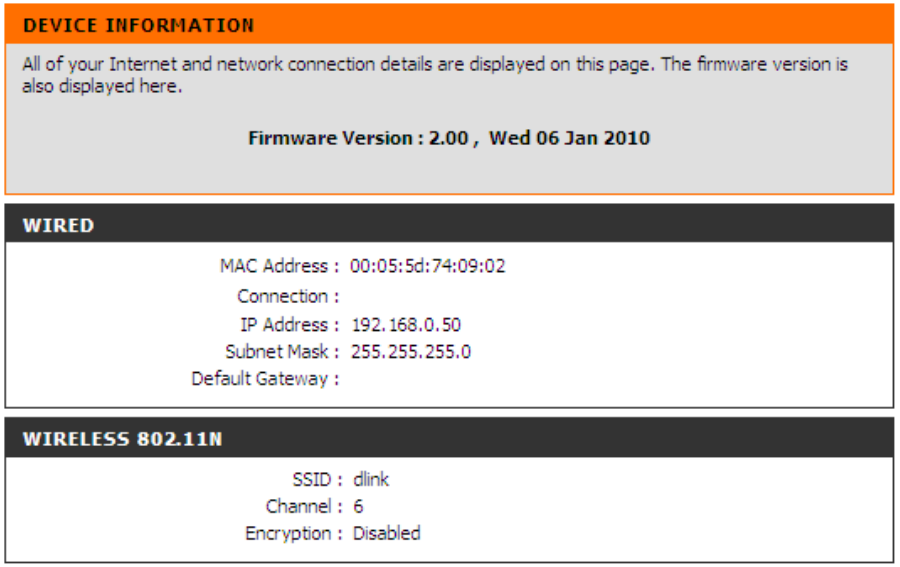
If your WAN connection is set up for a Dynamic IP address then a **DHCP Release** button and a **DHCP Renew** button will be displayed. Use **DHCP Release** to disconnect from your ISP and use **DHCP Renew** to connect to your ISP.

If your WAN connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

LAN: Displays the MAC address and the private (local) IP settings for the router.

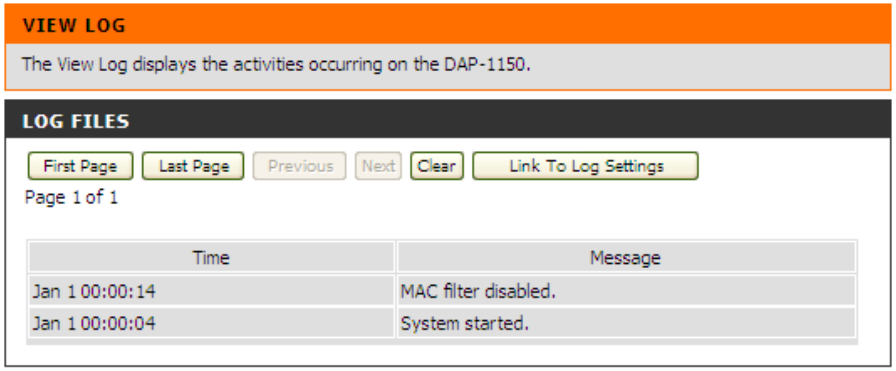
WAN: Displays the MAC address and the public IP settings for the router.

Wireless 802.11N: Displays the wireless MAC address and your wireless settings such as SSID, Channel, and Encryption status.



Log

This window allows you to view a log of activities on the Router. This is especially helpful detecting unauthorized network usage.



First Page: View the first page of the log.

Last Page: View the last page of the log.

Previous: View the previous page.

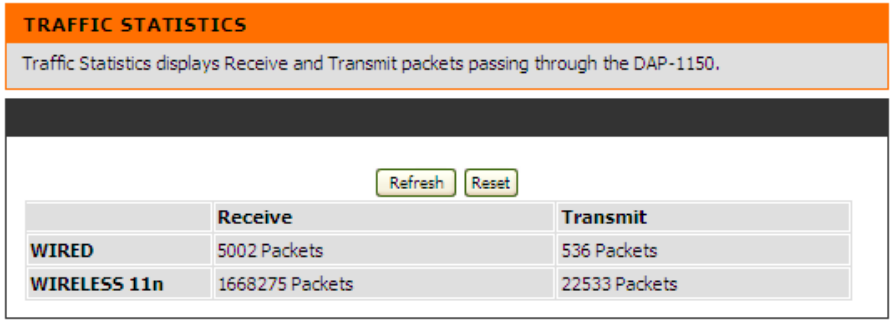
Next: View the next page.

Clear: Clear the log.

Link to Log Settings: Click this button to go directly to the Log Settings window (**Maintenance** > **Log Settings**).

Statistics

The window below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DAP-1150 on both the WAN and the LAN ports. The traffic counter will reset if the device is rebooted.



Active Session

The NAPT Active Session table displays a list of all active conversations between WAN computers and LAN computers.

Wireless

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

CONNECTED WIRELESS CLIENT LIST

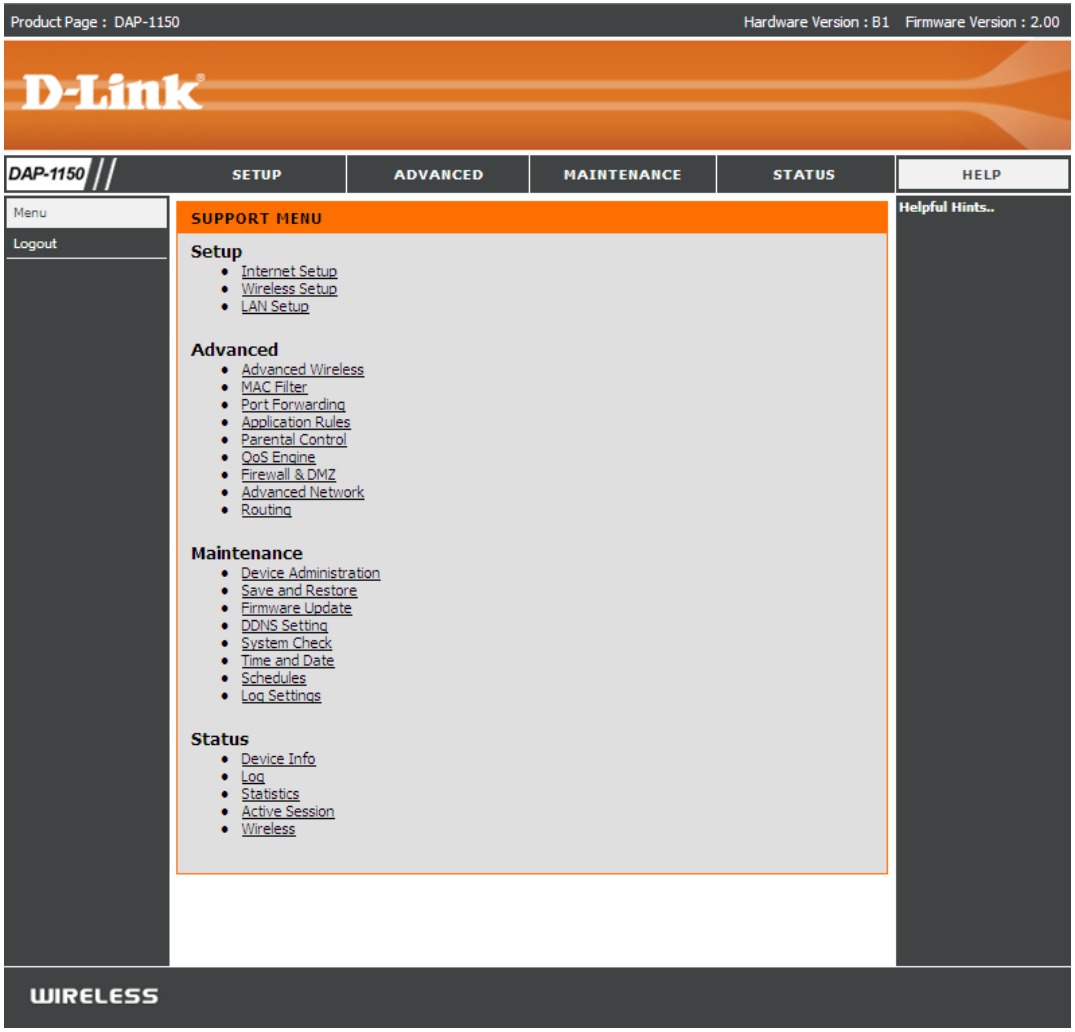
The Wireless Client table below displays Wireless clients Connected to the AP (Access Point).

NUMBER OF WIRELESS CLIENTS : 4

Connect Time	MAC Address	IP Address	Mode	Rate	Signal (%)
0 days, 00:29:29	00:19:D2:AE:DE:F7	N/A	11g	54	72
0 days, 00:15:11	00:26:5E:E9:5C:1D	N/A	11g	54	100
0 days, 2:15:30	00:21:5C:39:2F:25	N/A	11n	72.2	86
0 days, 00:10:25	00:26:5E:E8:03:CC	N/A	11g	54	76

Help

Click the desired hyperlink to get more information about how to use the Router.



Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-1150 offers the following types of security:

- WPA-Personal (Pre-Shared Key)
- WPA2-Personal (Pre-Shared Key 2)
- WPA2-Auto-Personal
- WEP (Wired Equivalent Privacy)
- WPA-Enterprise (Extensible Authentication Protocol)
- WPA2-Enterprise (Extensible Authentication Protocol 2)
- WPA2-Auto-Enterprise (Extensible Authentication Protocol 2 Auto)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

Configure WEP

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Settings** on the left side.

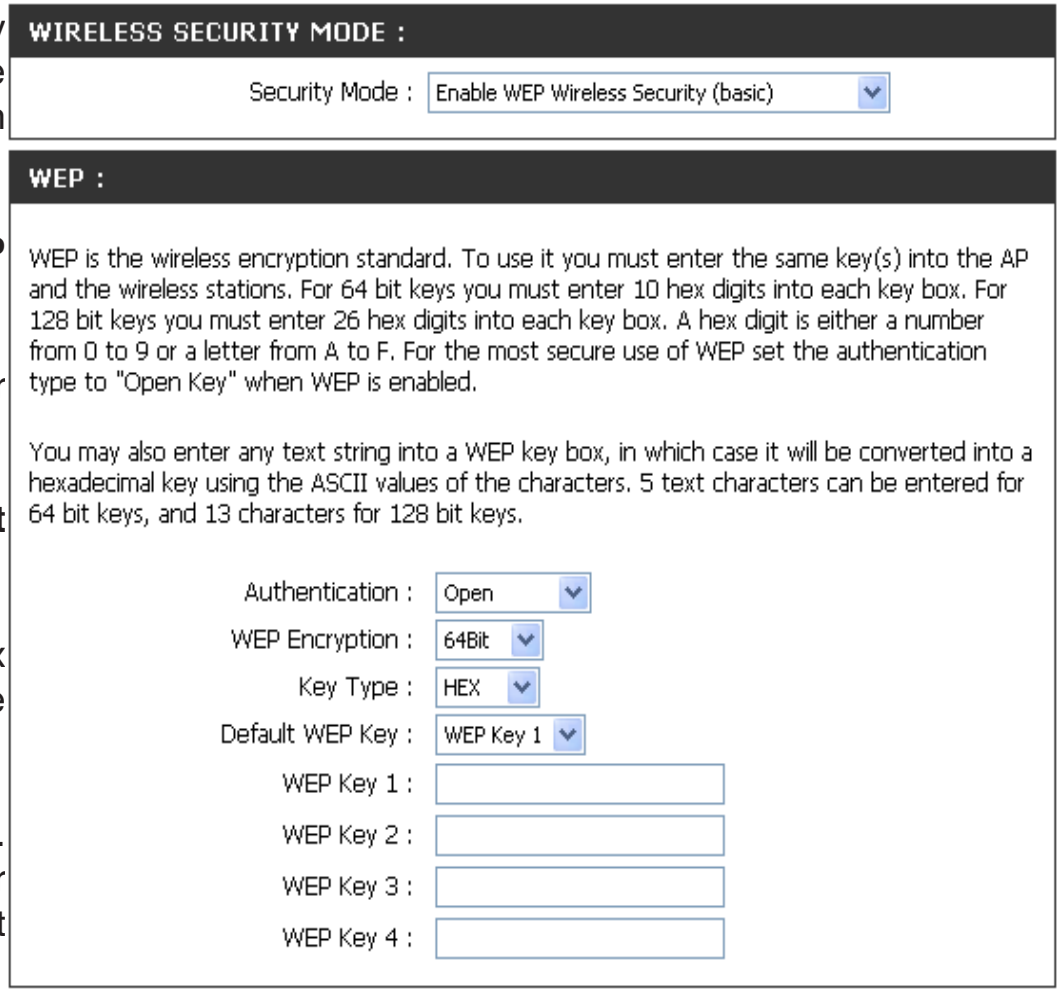
2. Next to Security Mode, select **Enable WEP Security**.

3. Next to Authentication, select **Shared Key** or **Open**.

4. Next to WEP Encryption, select **64-bit** or **128-bit** encryption.

5. Next to Key Type, select either **Hex** or **ASCII**.Hex (recommended) - Letters A-F and numbers 0-9 are valid. ASCII - All numbers and letters are valid.

6. Next to Key 1, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.



7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the access point.

What is WPA?

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

There are 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature ensures that the keys haven't been tampered with.

- User authentication, which is generally missing in WEP, is done through the Extensible Authentication Protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

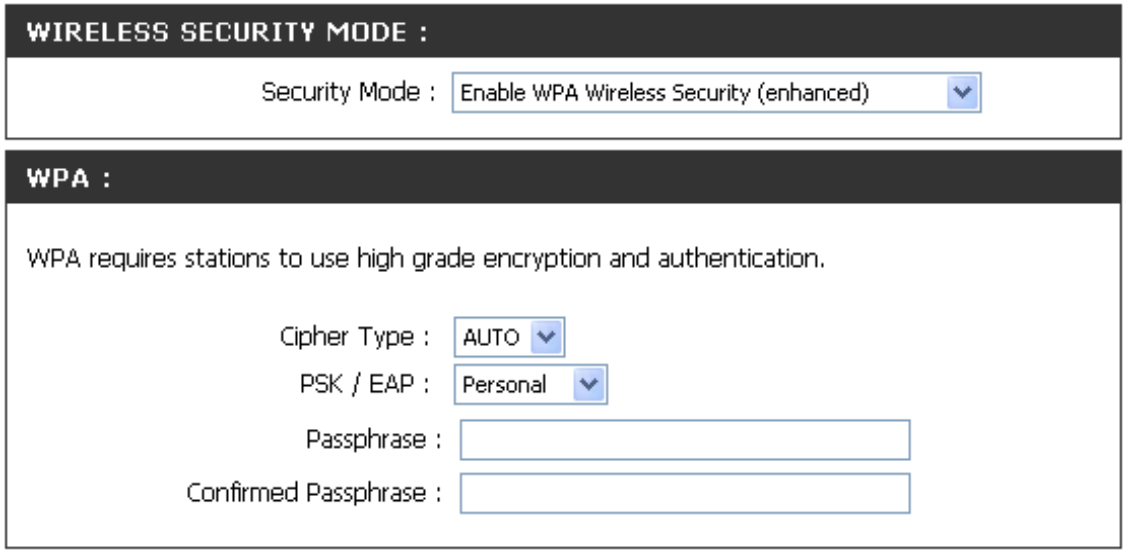
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

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

WPA2-Auto-PSK/WPA2-Auto-EAP accepts wireless clients that use WPA or WPA2. Authentication is sill necessary.

Configure WPA-PSK, WPA2-PSK, and WPA2-Auto-PSK (Personal)

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.



1. Log into the web-based configuration utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Settings** on the left side.

2. Next to Security Mode, select **Enable WPA Wireless Security**, **Enable WPA2 Wireless Security**, or **Enable WPA2-Auto Wireless Security**.

3. Next to Cipher Mode, select **TKIP, AES,** or **Auto**.

4. Next to PSK / EAP, select **Personal**.

5. Next to Passphrase, enter a key (passphrase). The key 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. Enter the passphrase again next to Confirmed Passphrase.

7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-Personal, WPA2-Personal, or WPA2-Auto-Personal on your adapter and enter the same passphrase as you did on the access point.

Configure WPA-EAP, WPA2-EAP, and WPA2-Auto-EAP (Enterprise)

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Settings** on the left side.

2. Next to Security Mode, select **Enable WPA Wireless Security**, **Enable WPA2 Wireless Security**, or **Enable WPA2-Auto Wireless Security**.

3. Next to Cipher Mode, select **TKIP, AES,** or **Auto**.

4. Next to Personal / Enterprise, select **Enterprise**.

5. Next to RADIUS Server enter the IP Address of your RADIUS server.

6. Next to Port, enter the port you are using with your RADIUS server. 1812 is the default port.

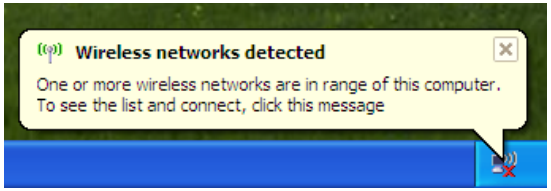
7. Next to Shared Secret, enter the security key.

8. Click **Save Settings** to save your settings.

Connect to a Wireless Network Using Windows® XP

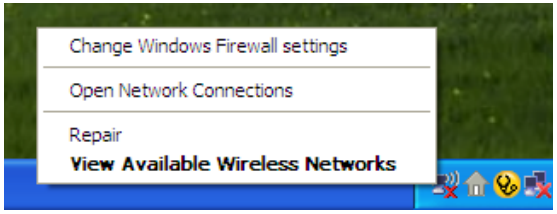
Windows® XP users can use the built-in wireless utility (Zero Configuration Utility) to connect to a wireless network. The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help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

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.



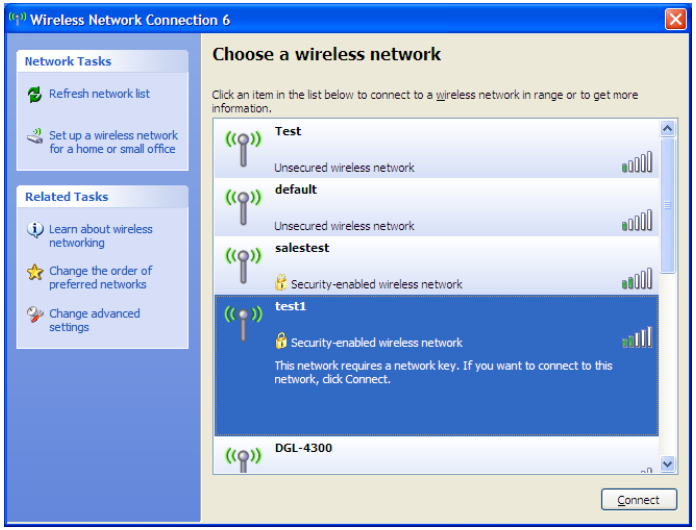
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.



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

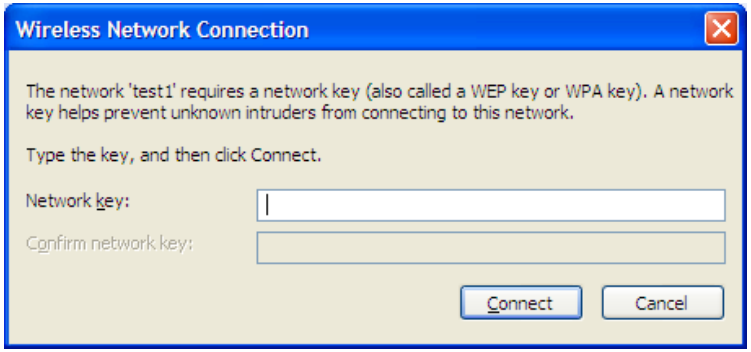
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



Configure WEP/WPA-PSK

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

Follow the steps on the previous page to connect to a wireless network using Windows® XP. After you highlight a network and click **Connect**, the **Wireless Network Connection** box will appear if the network requires authentication. Enter the same WEP or WPA-PSK key that is on your access point and click **Connect**.

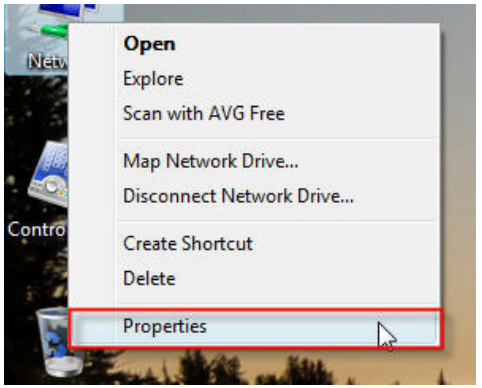


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP or WPA-PSK settings are correct. The WEP or WPA-PSK key must be exactly the same as on the wireless access point.

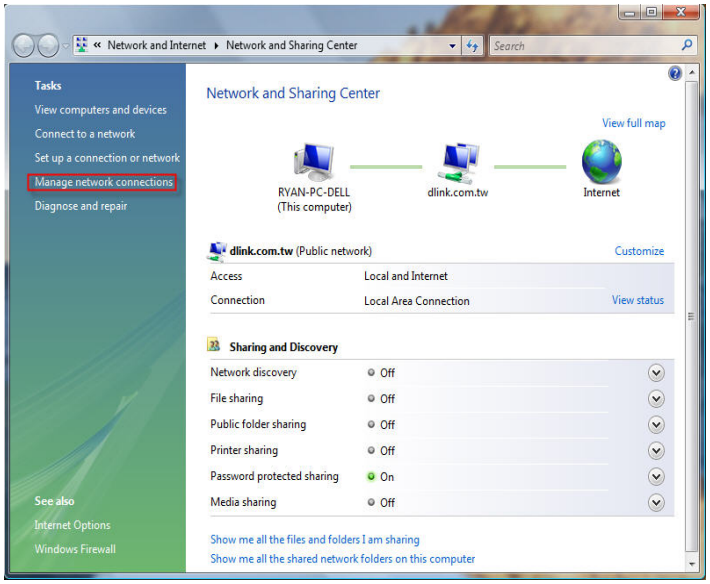
Using Windows® Vista (Secured Network)

The following are step-by-step directions to connect to a secured wireless network using Windows® Vista.

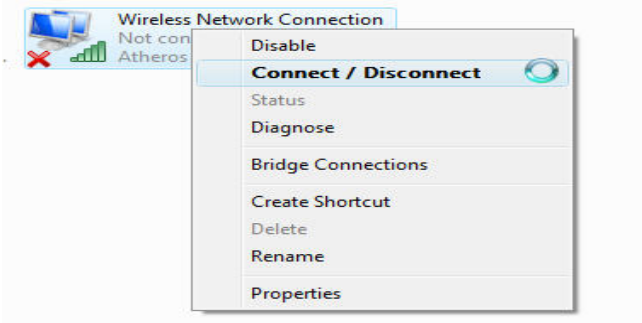
1. Right-click on **Network** and click on **Properties**.



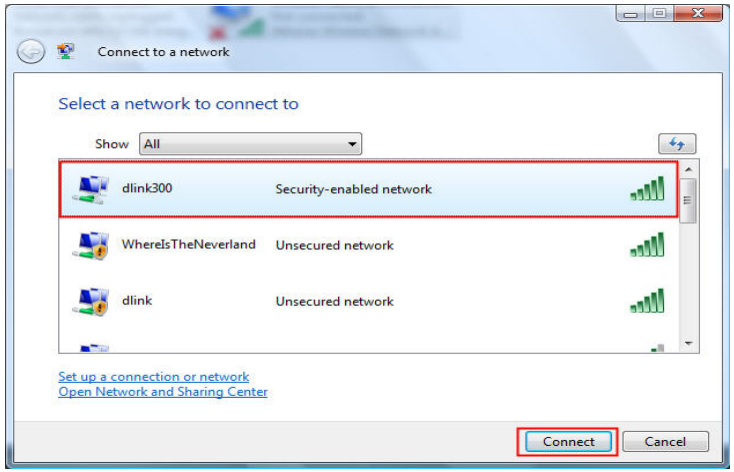
2. Click the **Manage network connections** link in the **Network and Sharing Center** window.



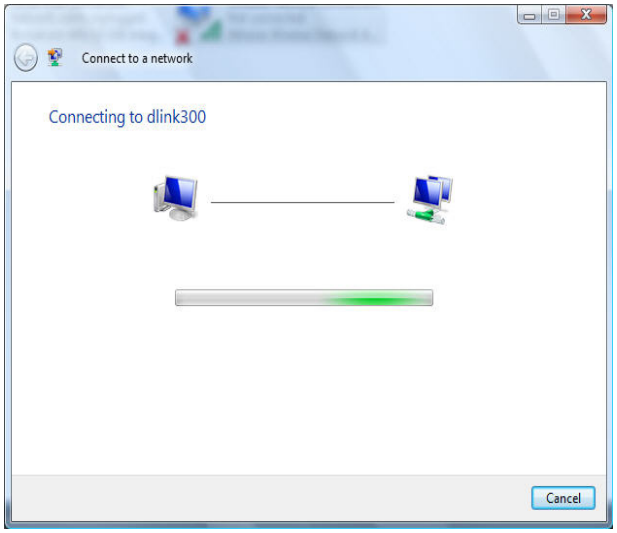
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



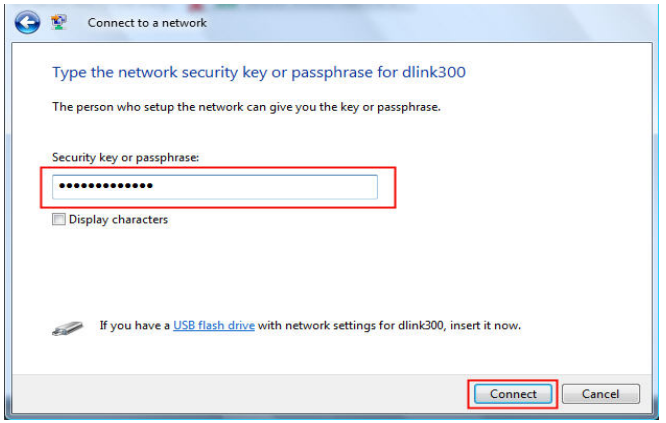
4. Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



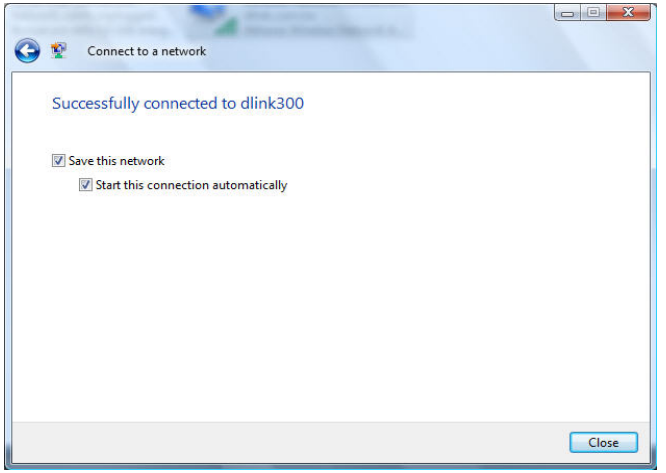
5. The following window displays connection progress.



6. Enter the network security key or passphrase for the AP in the textbox provided in the **Type the network security key or passphrase for [SSID name]** window. When you are finished, click the **Connect** button.



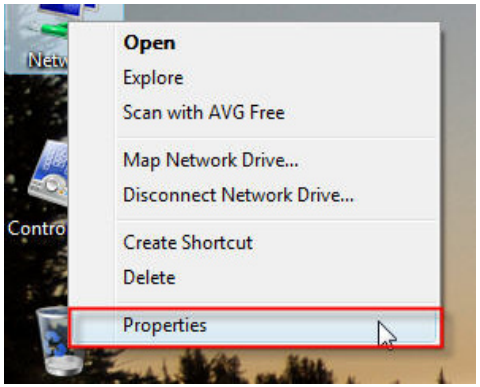
7. The following **Successfully connected to [SSID name]** window is displayed. Choose to save this network and/or start this new connection automatically. When you are finished, click the **Close** button.



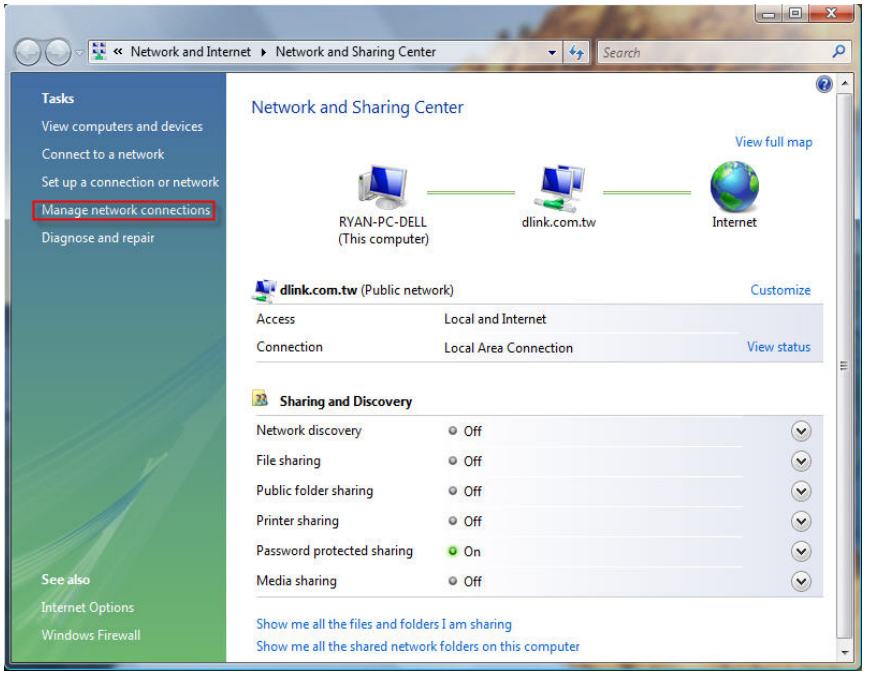
Using Windows® Vista (Unsecured Network)

The following are step-by-step directions to set up a wireless connection on an unsecured network using Windows® Vista.

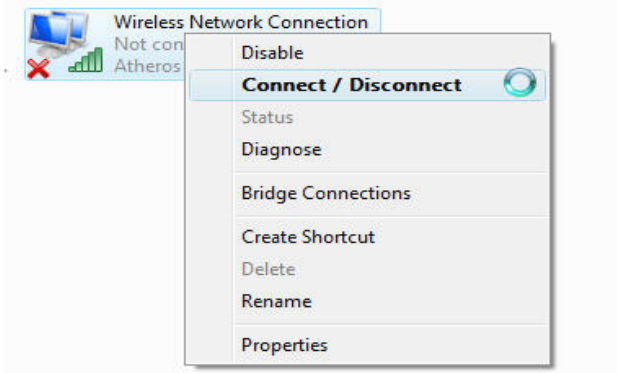
1. Right-click on **Network** and click on **Properties**.



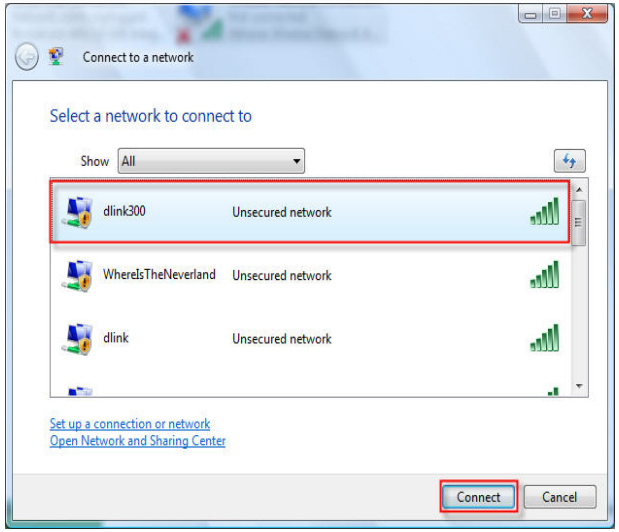
2. Go to the **Network and Sharing Center** window and click the **Manage Network Connections** link.



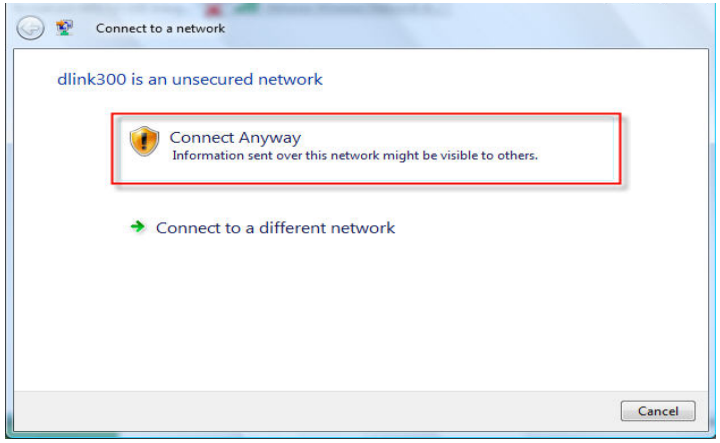
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



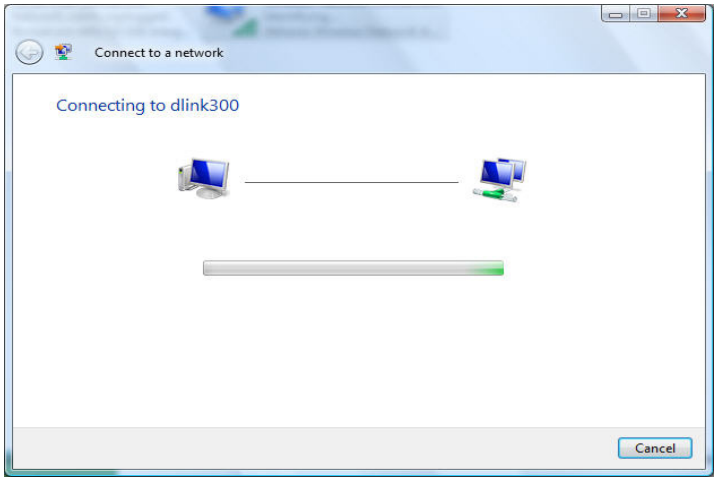
4. Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



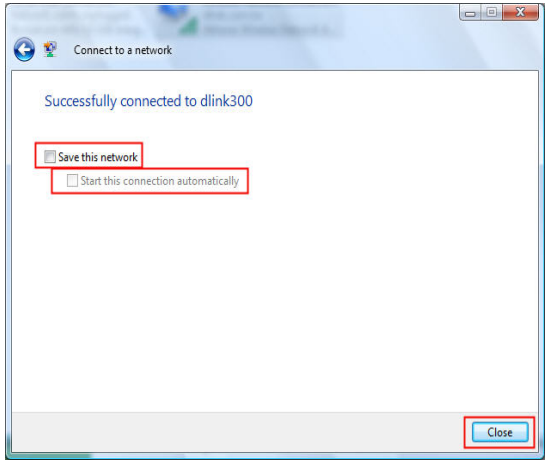
5. Confirm that you still want to connect on the following **Network Connection Status** window by clicking on **Connect Anyway**.



6. The following **Connect to a network** wizard window displays the connection progress.



7. The following **Successfully connected to [SSID name]** window is displayed. Choose to save this network and/or start this new connection automatically. When you are finished, click the **Close** button.



Wireless Basics

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

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

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

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

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio waves 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 a worldwide leader and an 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 a cordless phone works- using radio signals to transmit data from one point to another. However, 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: a Wireless Local Area Network (WLAN) and a Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a WLAN, 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 AP, the signal can travel up to 300 feet. With an outdoor AP the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPANs. Bluetooth devices in WPANs operate in a range up to 30 feet away.

The speed and wireless operation range of a WPAN is less than of a WLAN, but it excels in its efficient consumption of power. WPANs are ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, at home and in the office.

Home

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

Small Office and Home Office (SOHO)

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

Where is wireless used?

Wireless technology is quickly expanding beyond home and office use. The freedom of mobility it offers is becoming so popular that more and more public facilities are now providing wireless access to attract people. Public places that offer wireless access is usually called a “hotspot”.

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like airports, hotels, coffee shops, libraries, restaurants, and convention centers.

A wireless network is relatively 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 Access Point

Make sure you place the router/access point in a central 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 and 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 will significantly reduce any interference that the appliances might cause if operating on the same frequency.

Security

Don't let your next-door neighbors or unwanted intruders connect to your wireless network. Secure your wireless network by turning on the WEP or WPA security feature on the access point. Refer to the section "Wireless Security" in this manual for detailed information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.

- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

An Infrastructure network contains an AP or a wireless router. All the wireless devices, or clients, will connect to the wireless router or the AP.

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.

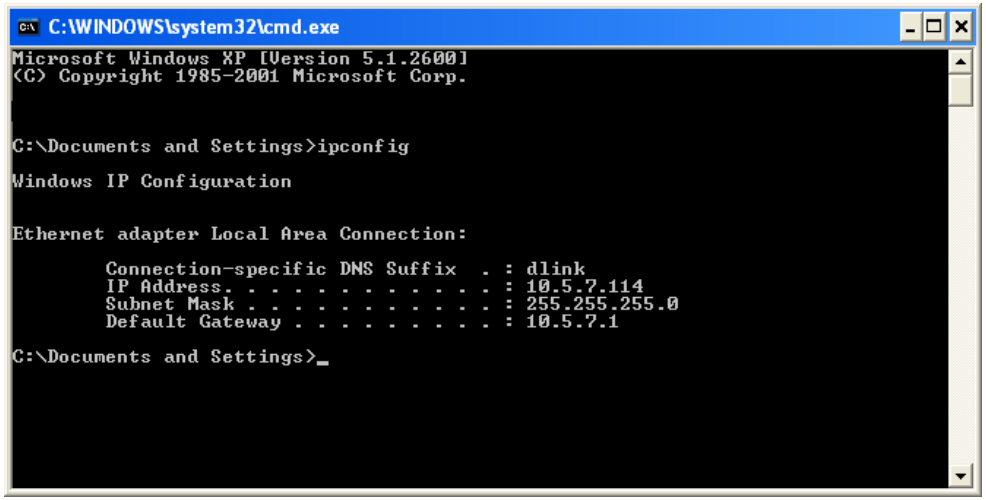
Networking Basics

Check your IP address

After you install your network 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 in a hotel, coffee shop, airport, or another public place, please contact an employee or administrator to verify their wireless network settings.

Statically Assign an IP address

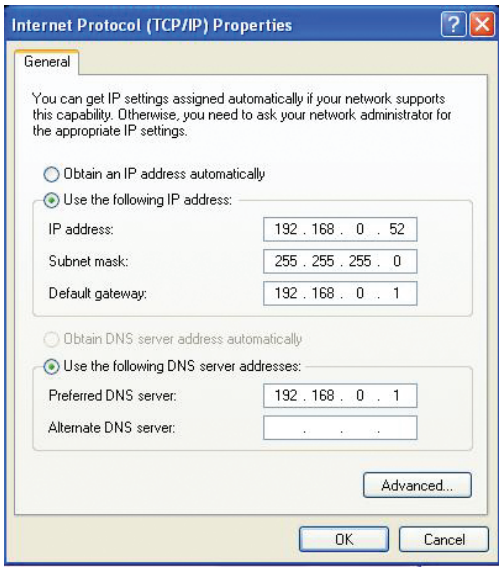
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

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 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.

Technical Specifications

NETWORK STANDARDS
- 802.11n
- 802.11g
- 802.11b
- 802.3/802.3u 10BASE-T/100BASE-TX Ethernet

DEVICE INTERFACES
- 802.11n wireless LAN
- One 10/100BASE-TX Ethernet LAN port

OPERATING FREQUENCY
2.4 to 2.4835 GHz

OPERATING CHANNELS
- ETSI: 13

RADIO & MODULATION SCHEMES
DQPSK, DBPSK, CCK, OFDM

OPERATION MODES
- Access Point
- Repeater
- Router

ANTENNA
2dBi Gain detachable omni-directional antenna with RP-SMA connector

RECEIVE SENSITIVITY
SECURITY
- 64/128-bit WEP data encryption
- WPA-PSK, WPA2-PSK
- WPA-EAP, WPA2-EAP
- TKIP, AES
- SSID broadcast disable function

QUALITY OF SERVICE (QoS)
Wi-Fi Multimedia (WMM)

DEVICE MANAGEMENT
- Web-based management through Internet Explorer v.6 or later, Netscape Navigator v.6 or later or other Java-enabled browser

Diagnostic LED
- Power
- WLAN
- LAN

POWER INPUT
5VDC 1.2A
External power adapter

DIMENSIONS
147 (W) x 113.2 (D) x 31.5(H) mm

WEIGHT
193grams

OPERATING TEMPERATURE
0 to 40 C

STORAGE TEMPERATURE
-20 to 65 C

OPERATING HUMIDITY
10% to 90% non-condensing

STORAGE HUMIDITY
5% to 95% non-condensing

D-Link®

Building Networks for People

Version 2.00

2010/01/15