



**DSA-3200**

**Wireless G Public/Private  
Gateway**

**User Manual**



(2/8/2005)

# Table of Contents

<b>1</b>	<b>Preface.....</b>	<b>4</b>
1.1	Brief Introduction to the DSA-3200 .....	4
1.2	Things to Consider .....	5
1.2.1	Audience .....	5
1.2.2	Document Convention .....	5
<b>2</b>	<b>Product Description .....</b>	<b>6</b>
2.1	Package Contents.....	6
2.2	System Requirements.....	6
2.3	Panel Function Descriptions .....	7
<b>3</b>	<b>Managing the D-Link DSA-3200.....</b>	<b>9</b>
3.1	Getting Started .....	9
3.2	System Concept.....	9
3.3	Begin Installation.....	10
<b>4</b>	<b>Web Management Interface .....</b>	<b>12</b>
4.1	Home.....	13
4.1.1	Wizard.....	14
4.1.2	System.....	15
4.1.3	WAN Configuration .....	17
4.1.4	Public LAN Configuration.....	19
4.1.5	Public WLAN Configuration .....	22
4.1.6	Private LAN Configuration .....	29
4.2	Advanced Menu .....	32
4.2.1	Authentication Policies.....	32
4.2.2	Group Configuration .....	44
4.2.3	Black List Configuration .....	47
4.2.4	On-demand User Configuration.....	49

4.2.5	Roaming Configuration .....	53
4.2.6	Additional Configuration.....	55
4.3	Tools Menu .....	59
4.3.1	Port and IP Redirect.....	60
4.3.2	Virtual Server .....	61
4.3.3	Pass Through.....	62
4.3.4	Monitor IP List .....	64
4.3.5	Free Surfing Area.....	66
4.3.6	Proxy.....	67
4.3.7	DDNS.....	68
4.3.8	Change Password .....	69
4.3.9	System Settings .....	70
4.3.10	Firmware Upgrade.....	71
4.3.11	Restart .....	72
4.4	Status .....	72
4.4.1	Device Info .....	73
4.4.2	Interface .....	75
4.4.3	Current Users.....	77
4.4.4	Traffic History .....	77
4.4.5	Notifications .....	78
4.5	Help .....	80
4.6	Confirm Functionality of User Authentication .....	81
<b>5</b>	<b>Console Interface .....</b>	<b>84</b>
5.1	Main Menu of Console interface .....	84
5.2	Console Utilities for Network Debugging .....	85
5.3	Change admin password of Console .....	87
5.4	Reload factory default of Console interface .....	87
5.5	Restart DSA-3200 .....	87
<b>6</b>	<b>Appendix - Windows TCP/IP Setup .....</b>	<b>88</b>
6.1	Setting up a PC to connect to the DSA-3200.....	88
6.1.1	TCP/IP Network Setup.....	88

6.1.2	Internet Connection Setup .....	89
6.2	Configure TCP/IP in Windows 2000.....	96
6.3	Configure TCP/IP in Windows XP.....	100
<b>7</b>	<b>Warranty .....</b>	<b>104</b>
<b>8</b>	<b>Technical Support.....</b>	<b>111</b>
<b>9</b>	<b>Registration.....</b>	<b>112</b>

# 1 Preface

## 1.1 Brief Introduction to the DSA-3200

The D-Link DSA-3200 *Airspot™* Wireless G Public/Private Gateway is an all-in-one product specially designed to manage and control a Hot Spot environment. The DSA-3200 integrates access control features and wireless network access into a single system to fulfill the basic needs of most Hot Spot venues. The DSA-3200 supports 802.11b and 802.11g wireless transmission modes simultaneously offering convenience, efficiency, and a friendly end-user experience from your Hot Spot.

### **Quick Installation, On-line Immediately**

Installation and setup of the DSA-3200 can easily be accomplished without changing the existing network architecture. Within a short time of making all of the necessary physical connections, setup of access security mechanisms can be completed through the Web-based Interface. With the DSA-3200 at the head of a network, Public LAN and WLAN users must authenticate prior to being granted access to the Internet. These users can be assigned a specific bandwidth priority and/or Firewall profile to preserve access rights and privileges between pre-defined user groups.

### **Friendly Management and Application Interfaces**

The DSA-3200 is not only easy to install, but also has a friendly management web interface. The full web-based management interface allows one to operate and maintain the system using a Java enabled web browser. Users that connect to your Hot Spot Network will automatically be redirected to the login page the first time they try to surf the web after connecting to the Public LAN or WLAN Interface of the DSA-3200.

### **Integrate an Existing User Password Database**

Often time organizations or businesses will already own and operate a specific credential database system to centralize and manage their user passwords and user

permissions on the Network. One of the more prevalent Protocols used to authenticate users is the RADIUS Protocol. With a built-in RADIUS Client the DSA-3200 can support both Local and RADIUS authentication mechanisms simultaneously, allowing one to easily incorporate an existing user password database into the *Airspot™* Hot Spot System. The DSA-3200 also provides a built-in user database, allowing dynamic account creation/deletion to coexist with the more static RADIUS database.

## **1.2 Things to Consider**

### **1.2.1 Audience**

This manual is intended for system or network administrators possessing basic networking knowledge to complete step by step instructions in this manual in order to use the DSA-3200 to centralize Network access and management. This manual attempts to explain in detail the wealth of functions the DSA-3200 supports, however there may be situations and circumstances not considered during the authoring of this document. Technical Support may only assist with the configuration of the DSA-3200 through the Web-UI or SSH, and may not troubleshoot or repair ill configured external systems or Networks.

### **1.2.2 Document Convention**

Whenever an important piece of information such as a recommendation or warning needs to be presented, said information is displayed in a box in italics similar to the recommendation below. These recommendations will for the most part be used to help in increasing the security and usability of your Hot Spot.

***Warning:*** *To Increase security, you should immediately change the Administrator's password.*

## 2 Product Description



### 2.1 Package Contents

- DSA-3200 Wireless G Public/Private Gateway
- CD-ROM (Administrator's Manual and Quick Installation Guide)
- Ethernet cable (CAT-5 UTP Crossover)
- Ethernet Cable (CAT-5 UTP Straight-through) (2)
- 2 dBi Detachable R-SMA D-Link Antenna (2)
- 5V DC, 3A Power adapter
- Null modem console cable
- Wall-mount Kit
- Rubber Feet (4)

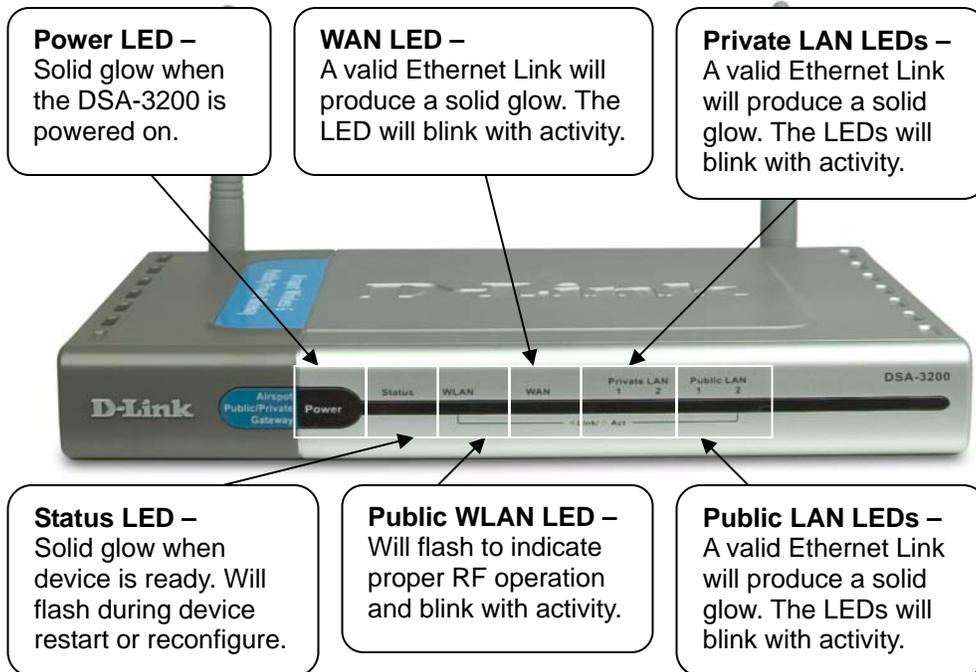
*Note: Using a power supply with a different voltage rating than the one included with the DSA-3200 will cause irreparable electrical damage and void the warranty for this product*

### 2.2 System Requirements

- Computer running Microsoft Windows, Macintosh OS, or a UNIX based OS
- An installed Ethernet adapter configured to communicate using TCP/IP.
- Internet Explorer 6.0 or Netscape Navigator 7.0 or above, with JavaScript enabled.

## 2.3 Panel Function Descriptions

### Device LED Indicators



**Power LED:** Will illuminate when the Power Supply is connected to the DSA-3200 and an appropriate AC power outlet (110VAC). If the LED does not illuminate when the device is plugged in, try a known good power outlet. If the LED still does not light with a known good outlet, please contact Technical Support for assistance.

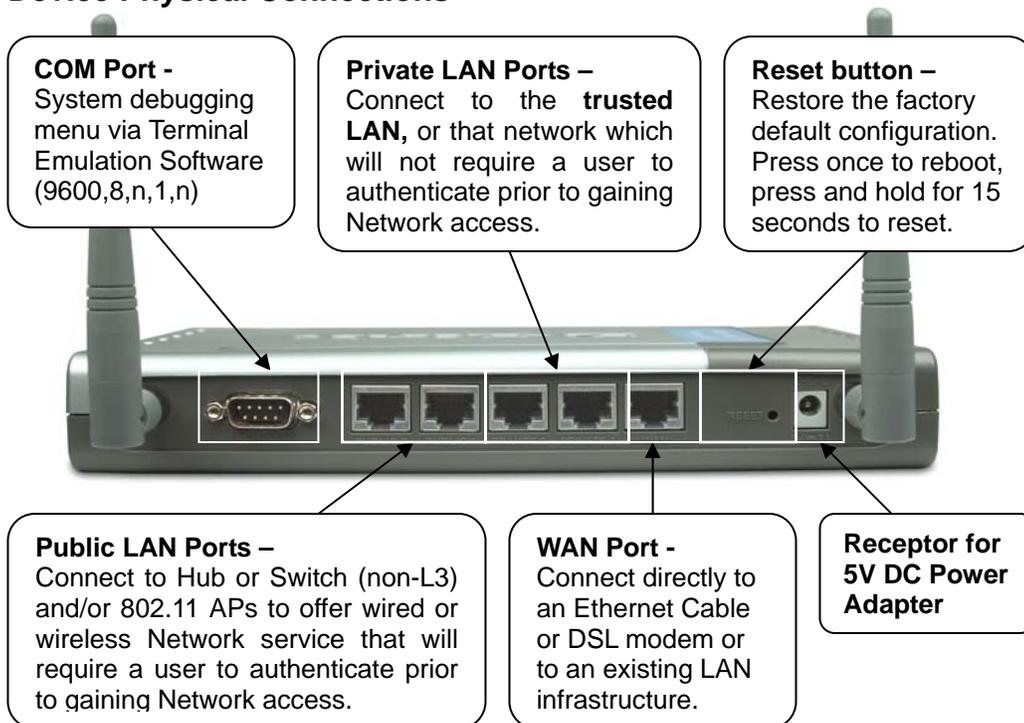
**Status LED:** A solid light indicates a functional, ready state of operation. This LED will blink during a device restart or reconfigure, then illuminate solid to indicate proper operation. If this LED continuously flashes or does not illuminate when the device is powered on, please contact Technical Support for assistance.

**Public WLAN LED:** This indicator will flash to indicate proper RF operation of the internal AP. The LED will blink rapidly with activity.

**WAN LED:** A solid light indicates a valid Ethernet Link to the WAN modem/switch. LEDs will blink to indicate WAN activity. No light indicates a no-link state (no cable or bad cable).

**Private/Public LAN LEDs:** A solid light indicates a valid Ethernet Link to a hub/switch or PC. LEDs will blink to indicate activity. No light indicates a no-link state (no cable or bad cable).

## Device Physical Connections



**Serial COM Port:** This port serves two distinct purposes:

1. Connect to a DSA-3100P to auto-generate temporary User accounts and print detailed receipts to be given to customers. Receipts include pricing and Wi-Fi Network information (SSID, WEP, etc.)
2. Use the included Null modem cable to connect to a PC with a serial COM port in order to troubleshoot, debug, change admin password, or to restore the factory default settings without using the Web-based UI. Configure Terminal Emulation software (Hyperterminal) as follows: 9600, 8, N, 1, No flow control.

**WAN Port:** Connects to a network not managed by the DSA-3200 via an Ethernet port on most Cable or xDSL modems, or a Switch or Hub in an existing Ethernet Network.

**Public LAN Ports (1 and 2):** The Public LAN ports connect to the managed network that will require user authentication prior to granting Network Access. This Network may consist of Hubs and/or Switches (non-L3) as well as 802.11 Access Points.

**Private LAN Ports (1 and 2):** The Private LAN port is used to connect to the trusted Ethernet network that will not require authentication prior to access.

**Reset Button:** Push and release to restart, push and hold for 15s to reset defaults.

**DC Power Socket:** Connect the power supply to a wall outlet before connecting here.

## **3 Managing the D-Link DSA-3200**

### **3.1 Getting Started**

This guide will provide information and instruction for administrators of the DSA-3200 Wireless G Public/Private Gateway. This manual corresponds with the version of firmware shipped with the DSA-3200 (v 1.00). From time to time D-Link may release new firmware to add new features or improve on existing ones. These firmware upgrades can be found on the Technical Support Website <http://support.dlink.com/>. The Support Website also has plenty of great documentation in the way of FAQs and updated manuals, etc. Please take a moment to visit support.dlink.com prior to contacting Technical Support.

### **3.2 System Concept**

The DSA-3200 has the ability to allow or deny access to Network resources based on various types of credentials (IP address, MAC address, or username/password). From a single Broadband Internet connection, the DSA-3200 creates 3 separate networks using NAT, each with its own DHCP server. The WLAN RF interface is an 802.11b/g network that can be configured to either authenticate users or use WPA for enhanced wireless security. The Public LAN interface can be configured to authenticate users so it may serve as a secondary Public access network. The third Private LAN interface does not authenticate users and is intended to service the back office or an existing office network.

Authentication of users is accomplished through any Java enabled Web browser. After a user connects to one of the Public Access networks and attempts to browse the Internet, they will be redirected to a customizable login page hosted on the DSA-3200 without or without SSL encryption. A Walled Garden may be defined to allow users that have not authenticated to access those URLs specified in the Free Surf Zone. Once users authenticate successfully via the Internal Database or an external RADIUS server, the Web browser will once again be redirected to a specified URL. At this point

the user may freely browse the Internet until the account expires or their connection remains idle longer than allowed. Limits may be imposed on how long an account may be or the length of time a connection remains idle before it is terminated or even the maximum bandwidth available to the authenticated user.

The DSA-3200 manages all network data that passes through it. Users under the managed network must authenticate in order to access any network resources. User authentication is processed via the DSA-3200 Web server with or without SSL encrypted links. When a user is prompted to login, the DSA-3200 will check the user database to confirm the user's access rights. In addition to the internal User database for local and On-demand users, the DSA-3200 may query any external RADIUS Server to authenticate and authorize user credentials. If the user fails to successfully authenticate, the DSA-3200 will refuse access and continue to prompt for user log in. If the Administrator so chooses, a list of URLs may be provided for free access to users that have not yet authenticated. Once the user authenticates successfully, the DSA-3200 will grant limited access based on the group membership of the user and redirect the web-browser to the administrator defined URL.

The DSA-3200 can be configured to terminate user access if a user requests to log out or remains idle longer than the configured idle time. Limits can be placed on user session length as well as maximum bandwidth available to specific user groups.

The system is responsible for user authentication, authorization and management. The user account information is stored in the local database, or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and the palm computers.

### **3.3 Begin Installation**

Please follow the Quick Installation Guide included with the DSA-3200 to physically connect the device to the appropriate networks. The QIG also provides instructions to configure the Network interfaces of the DSA-3200 using the Setup

Wizard. Following completion of the Setup Wizard, configurations pertaining to User Authentication mechanisms, access privileges, and system management will need to be made for a fully operational Hot Spot.

Once the Setup Wizard is complete, the DSA-3200 will restart. Depending on what configurations were made, it may be necessary to login to the Web-UI again. From a PC connected to the Private LAN interface, open a Web-browser and enter <https://192.168.0.40> (the default Private LAN IP) into the address bar and hit enter. The Administrator login page should load. Enter the appropriate credentials (default username is admin password is admin) and click Enter.



The image shows the administrator login page for the D-Link DSA-3200. At the top left is the D-Link logo with the tagline "Building Networks for People". At the top right, the text reads "DSA-3200 Airspot Wireless G Public/Private Gateway". In the center, the word "Administrator" is displayed above a login form. The form contains two input fields: "User Name:" and "Password:". Below these fields are two buttons: "Enter" and "Clear".

## 4 Web Management Interface

This section gives a complete description of the Web Management Interface of the DSA-3200 on a page-by-page basis. The following table shows all configuration pages where each column represents each of the Navigation Tabs and the configuration pages available in each section.

Section	Home	Advanced	Tools	Status
<b>Web-UI Configuration Page</b>	Wizard	Authentication Policies	Port and IP Redirect	Device Info
	System	Group	Virtual Server	Interface
	WAN	Black List	Pass Through	Current Users
	Public LAN	On-demand User	Monitor IP List	Traffic History
	Wireless LAN	Roaming	Free Surfing Area	Notify
	Private LAN	Additional	Proxy	
			DDNS	
			Change Password	
			System	
			Firmware	
		Restart		

## 4.1 Home

The Home Tab consists of System and Network Specific configurations. All Interface information such as IP configuration, DHCP Server configuration, and per port Authentication features can be accessed through the Home Tab. The Home section provides the following interface configuration pages to further set up your Airspot system: **Wizard, System, WAN, Public Network, Wireless, and Private Network.** Please refer to each section for more information.



### **4.1.1 Wizard**

The Wizard will guide through the Interface setup of the DSA-3200. All that is needed is to follow the procedures and instructions as presented by the Wizard, step by step, filling in all required values. Upon completion, restart the DSA-3200 to activate any new settings.

Please refer to the Quick Installation Guide for detailed information about running the Setup Wizard.

**Setup Wizard**

The D-Link DSA-3200 Airspot Wireless G Public/Private Gateway is an Ethernet Broadband Router with access control features ideal for Wi-Fi hotspots, as well as small to medium business applications. The Setup Wizard will guide you through essential configurations to enable WAN connectivity, and Network settings pertaining to the Public LAN Interface as well as the Wireless LAN Interface. You may exit the wizard at any time without altering your previous configuration. To enable the configurations made in the wizard, follow the wizard step by step to the end and restart the DSA-3200. Keep in mind that after the Wizard is completed, User Authentication and other Advanced features will need to be configured manually in the appropriate section of this Web UI.

## 4.1.2 System

The System Information page allows configuration of items related to system management/maintenance. Any changes on this page will also require an entry for System Name as well as Succeed Page before they can be applied.

System Information	
System Name	<input type="text" value="dsa-3200.com"/> *
Admin Detail	<div style="border: 1px solid gray; padding: 2px;"> <p><b>Sorry! The service is temporarily unavailable.</b></p> <p>(It'll appear when Internet connection fail.)</p> </div>
Succeed Page	<input type="text" value="http://www.dlink.com"/> *
Remote Manage IP	<input type="text"/> (ex: 192.168.3.1 or 192.168.3.0/24)
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="checkbox"/> DoS protection for user	
User Logon SSL	<input checked="" type="radio"/> Enable <input type="radio"/> Disbale
System Time	Device Time : 2004/11/29 17:23:42 <input checked="" type="radio"/> Enable NTP NTP Server <input type="text" value="tock.usno.navy.mil"/> *(ex: tock.usno.navy.mil) Time Zone <input type="text" value="(GMT-08:00)Pacific Time(US&amp;Canada):Tijuana"/>
<input type="radio"/> Set Device Date and Time	

**System Name:** The Host Name of the DSA-3200, the default value is “DSA-3200.” This field will be used to identify the device through SNMP.

**Admin Detail:** The text in this box will be displayed when the WAN connection is lost and unauthenticated users attempt to browse the Internet. Contact information for help desk/technical representatives should be entered here so customers may inform the appropriate personnel in the event of failed WAN connectivity.

**Succeed Page:** Any URL may be entered in this field. Once a user logs in successfully he or she will be linked to this Succeed page URL automatically. The succeed page is typically set to the URL of a company website such as <http://www.dlink.com>.

**Remote Manage IP:** The DSA-3200 is able to be configured remotely through the WAN interface via HTTP, HTTPS, or SSH protocols. Access may be granted to a single IP address, a single IP Network, or any IP (0.0.0.0/32).

**SNMP:** The DSA-3200 supports SNMP v2 read-only data access. A Trap Host IP address and an SNMP community name must be specified for the DSA-3200 to be successfully managed through SNMP.

**Dos Protection for User:** The DSA-3200 protects users (when enabled) against various types of Denial of Service attacks including:

- NMAP FIN/URG/PSH
- Xmas Tree
- SYN/RST
- Ping of Death
- Null Scan
- SYN/FIN

**User Logon SSL:** When enabled users will be redirected to an HTTPS (SSL encrypted) log in page, otherwise a standard HTTP login page will be used.

**System Time:** The DSA-3200 has an NTP client to automatically synchronize the system time over the Internet from an NTP Server.

System Time	Device Time : 2004/11/29 17:23:42
	<input checked="" type="radio"/> Enable NTP
	NTP Server <input type="text" value="tock.usno.navy.mil"/> <small>*(ex. tock.usno.navy.mil)</small>
	Time
	Zone <input type="text" value="(GMT-08:00)Pacific Time(US&amp;Canada):Tijuana"/> <input type="button" value="v"/>
	<input type="radio"/> Set Device Date and Time

**Enable NTP:** Specify the IP address or domain name of an NTP server here.

**Time Zone:** Select the appropriate Time Zone of your current location from the drop down selection box (Universal Time is Greenwich Mean Time, GMT).

System Time	Device Time : 2004/11/29 17:23:42		
	<input type="radio"/> Enable NTP		
	<input checked="" type="radio"/> Set Device Date and Time		
	Year: <input type="text" value="2005"/>	Month: <input type="text" value="01"/>	Day: <input type="text" value="01"/>
	Hour: <input type="text" value="00"/>	Minute: <input type="text" value="00"/>	Second: <input type="text" value="00"/>

**Set Device Date and Time:** Manually configure the DSA-3200 system time.

### 4.1.3 WAN Configuration

The DSA-3200 supports 3 WAN types: Static IP Address, Dynamic IP Address, and PPPoE.

- **Static IP Address:** Manually specify the IP address of the WAN Port. This information will come from your ISP. IP address, Subnet Mask, Default Gateway, and Primary DNS Server fields must be completed to apply the settings.

WAN Port Configuration	
WAN Port	<input checked="" type="radio"/> Static IP Address
	IP address <input style="float: right; text-align: right; color: red; font-size: small; margin-left: 5px;" type="text" value="67.130.140.148"/> *
	Subnet mask <input style="float: right; text-align: right; color: red; font-size: small; margin-left: 5px;" type="text" value="255.255.255.0"/> *
	Default gateway <input style="float: right; text-align: right; color: red; font-size: small; margin-left: 5px;" type="text" value="67.130.140.1"/> *
	Primary DNS server <input style="float: right; text-align: right; color: red; font-size: small; margin-left: 5px;" type="text" value="192.152.81.1"/> *
	Secondary DNS server <input type="text"/>
	<input type="radio"/> Dynamic IP Address
<input type="radio"/> PPPoE Client	

- **Dynamic IP Address:** Use this configuration in situations in which a dynamic IP address is provided by the ISP (most Cable Internet connections are dynamic).

WAN Port Configuration	
WAN Port	<input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/> <input type="radio"/> PPPoE Client

**Renew:** Click to refresh the IP address setting, in order to obtain a different IP address.

- **PPPoE:** Use this configuration in situations where WAN connectivity is enabled through a PPPoE connection. Account Username and Password are required to successfully connect. Please verify user credentials for correctness if you are having difficulty connecting to your ISP.

WAN Port Configuration	
WAN Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input checked="" type="radio"/> PPPoE Client Username <input type="text"/> Password <input type="text"/> Dial on demand <input checked="" type="radio"/> Enable <input type="radio"/> Disable Maximum Idle Time <input type="text" value="0"/> Minutes

**Dial on Demand:** When the **Dial on Demand** function is enabled under PPPoE, the system will automatically disconnect the session after an idle time has been reached equal to the value specified here. This feature is intended for subscription plans that charge per unit time as opposed to charging for upstream and downstream connection speeds.

### 4.1.4 Public LAN Configuration

The DSA-3200 provides a public access network that is tied to the Public LAN ports on the rear of the device. The Public LAN can be configured to authenticate users as well as serve DHCP to DHCP enabled clients.

Public Port Configuration	
Public Port	IP PNP <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	User Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	IP Address <input type="text" value="192.168.1.40"/> *
	Subnet Mask <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address <input type="text" value="192.168.1.100"/> *
	End IP Address <input type="text" value="192.168.1.199"/> *
	Primary DNS Server <input type="text" value="192.152.81.1"/> *
	Secondary DNS Server <input type="text"/>
	Domain Name <input type="text" value="dlink.com"/> *
	WINS Server <input type="text"/>
	Lease Time <input type="text" value="1 Day"/> ▼
	<a href="#">Reserved IP Address List</a>

**IP PNP:** This feature enables those clients that already have Static IP information configured (IP address, Subnet Mask, Default Gateway, and DNS address) to join the Public Access Network without having to reconfigure their TCP/IP information. In order for this feature to function the user must have a default gateway and DNS address configured.

**User Authentication:** Enable or Disable user authentication to suit your Hot Spot Needs. Enabled will redirect all Public LAN users to a login page on their first web-browsing attempt. Disabled will not require authentication prior to access.

**IP Address:** Enter the desired IP address for the Public LAN interface.

**Subnet Mask:** Enter the appropriate Subnet Mask for this network.

**Related Setup for DHCP Server of Public LAN:**

The DHCP Server is optional and may be disabled or enabled at any time.

- **Disable DHCP Server:** The DSA-3200 will not dynamically configure DHCP clients on the Public LAN.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server
------------------------------	--

- **Enable DHCP Server:** The DSA-3200 will dynamically configure DHCP clients on the Public LAN. The appropriate information is needed for the DHCP server to function properly. To configure, enter: DHCP Scope Start IP Address; End IP Address; Primary DNS Server; Secondary DNS Server; Domain Name; WINS Server; Lease Time; and Reserved IP Address List.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server  DHCP Scope Start IP Address <input type="text" value="192.168.1.100"/> * End IP Address <input type="text" value="192.168.1.199"/> * Primary DNS Server <input type="text" value="192.152.81.1"/> * Secondary DNS Server <input type="text"/> Domain Name <input type="text" value="dlink.com"/> * WINS Server <input type="text"/> Lease Time <input type="text" value="1 Day"/> ▾ <a href="#">Reserved IP Address List</a>
------------------------------	--

As an option, the DSA-3200 provides a **Reserved IP Address List** for DHCP clients. This allows the reservation of specified DHCP Scope IP addresses for specified MAC addresses. Click the **Reserved IP Address List** hyperlink to configure.

Reserved IP Address List -- Public			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

(Total:40) [First](#) [Previous](#) [Next](#) [Last](#)

The Reserved IP Address List provides 40 entries. Enter the desired Reserved IP Address, client MAC address, and a short description (optional) for each reservation. After the information is completely entered, click **“Apply”** to complete the setup.

### 4.1.5 Public WLAN Configuration

The internal 802.11g Access Point serves as a secondary Public Access network. The configurations for the Wireless interface will consist of IP and DHCP selections as well as SSID, Channel, Transmission Mode, SSID Broadcast, and Layer 2 Client Isolation.

Wireless Port Configuration		
Wireless Configuration	SSID	Airspot
		<input type="checkbox"/> Sync to Ticket
	Auto Channel Selection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Channel	1
	Transmission Mode	Mixed
	SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Layer2 Client Isolation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<a href="#">Security Advance</a>		
Wireless Port	IP PNP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	IP Address	192.168.2.40 *
	Subnet Mask	255.255.255.0 *
DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server	
	DHCP Scope	
	Start IP Address	192.168.2.100 *
	End IP Address	192.168.2.199 *
	Primary DNS Server	192.152.81.1 *
	Secondary DNS Server	
	Domain Name	dlink.com *
	WINS Server	
	Lease Time	1 Day
	<a href="#">Reserved IP Address List</a>	

**SSID:** The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive and must not exceed 32 characters (any keyboard character is allowed).

**Sync to Ticket:** Checking this box will enter the SSID of the internal AP in the On-Demand User receipt SSID field.

**Auto Channel Selection:** The system will automatically select the appropriate channel based on relative noise and interference on available channels when enabled.

**Channel:** Select the appropriate channel from the list to correspond with your network settings, between 1 and 11 (North America). Channels 1, 6, and 11 tend to have the least amount of overlap in the spectrum.

**Transmission Mode:** There are 3 Wireless modes available: **802.11b** (2.4GHz, 11Mbps), **802.11g** (2.4GHz, 54Mbps) and **Mix mode** (b and g)

**SSID Broadcast:** If enabled, the SSID will be broadcast in most every 802.11 frame. Disabling this feature removes the SSID from most but not all 802.11 frames to add privacy to your wireless network. When disabled clients trying to join the Network must supply the SSID, as it most likely will not show up in normal Site Survey scans.

**Layer 2 Client Isolation:** Enabling this feature prevents wireless clients connected to the Internal AP from communicating with one another. This is to ensure the privacy and safety of all guests who use the wireless public access network.

**Security:** The Security screen is where Wired Equivalent Privacy can be enabled and configured if so desired. Click the **Security** Hyperlink.

Security	
WEP Key	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WEP Key Encryption	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits
Mode	<div style="border: 1px solid black; padding: 2px;">                     ASCII ▼                      HEX                      ASCII                 </div>
	<input type="radio"/> 2. <input type="text"/>
	<input type="radio"/> 3. <input type="text"/>
	<input type="radio"/> 4. <input type="text"/>

**WEP Key:** Choose to enable or disable WEP on the internal AP. If enabled, any user attempting to communicate on the wireless network must have the corresponding WEP key configured on their WLAN adapter.

**WEP Key Encryption:** Choose between a 64-bit (10 HEX or 5 ASCII) or 128-bit (26 HEX or 13 ASCII) WEP key.

**Mode:** Choose the key format of preference, either **HEX** (0-9, a-f) or **ASCII** (any ASCII character).

The **Advanced** menu allows fine-tuning of the RF characteristics for the internal AP. In most cases the default settings offer the best performance.

Advance	
Authentication Type	Auto ▼ (Default : Auto)
Transmission Rates	Auto ▼ (Default : Auto)
CTS Protection Mode	Disable ▼ (Default : Disable)
Basic Rates	Default ▼ (Default : Default)
Beacon Interval	100 (Default : 100, Milliseconds, Range : 20-1000)
RTS Threshold	2346 (Default : 2346, Range : 256-2346)
Fragmentation Threshold	2346 (Default : 2346, Range : 256-2346)
DTIM Interval	3 (Default : 3, Range : 1-255)

**Authentication Type:** The default value of **Auto** allows the AP to auto-detect for **Shared Key** or **Open System** Authentication types. Shared Key requires both the AP and Client to share a common WEP key (usually Key 1) before the Client can join the Network. Open Key allows any Client to associate with the AP, however if WEP is enabled the client will not be able to communicate unless the correct WEP Key is supplied.

**Transmission Rates:** The default value of **Auto** allows data rates to range from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can keep the default setting of **Auto** to have the Access Point automatically select the fastest possible data rate with an Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client.

**CTS Protection Mode:** The default setting is **Disabled**. When set to **Auto**, a protection mechanism will ensure that your Wireless-B devices will connect to the Access Point when Wireless-G devices are present. Keep in mind that the performance of your Wireless-G Network may decrease as a whole to accommodate the slower legacy client.

**Basic Rates:** The default value is **Default**. Depending on the wireless mode you have selected, a basic set of supported data rates will be selected. The default setting will ensure maximum compatibility with all devices. You may also choose to enable all data rates by selecting **ALL**. For compatibility with former Wireless-B devices, select 1-2Mbps.

**Beacon Interval:** This value indicates the frequency interval of the 802.11 Beacon Frame. The default value is 100 milliseconds. You may enter a value between 20 and 1000 milliseconds. A beacon is a packet broadcast by the Access Point to synchronize the wireless network.

**RTS Threshold:** This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor reductions are recommended.

**Fragmentation Threshold:** This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. A smaller setting means smaller packets, which will create more packets for each transmission. Only minor reductions of this value are recommended.

**DTIM Interval:** The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons to be informed they will receive broadcast and multicast messages.

Wireless Port	IP PNP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	IP Address	<input type="text" value="192.168.2.40"/> *
	Subnet Mask	<input type="text" value="255.255.255.0"/> *

**IP PNP:** Enable this feature to allow Clients configured with Static IP Addresses to be Dynamically routed to the Internet. Client reconfiguration is not necessary with this feature enabled, as long as the Client has Static values for IP Address, Subnet Mask, Default Gateway, and DNS Server Address they will be able to login to the Network and Browse the Internet without changing their IP information.

**User Authentication:** You can choose to Enable or Disable user authentication for the Wireless Interface.

**IP Address:** Enter the desired IP address for the Wireless Interface. This will be the default gateway for the Wireless Network.

**Subnet Mask:** Enter your desired Subnet Mask to determine the size of the Network the Interface may communicate with.

**Related Setup for DHCP Server of Public Wireless LAN:**

The DHCP Server is optional and may be disabled or enabled at any time.

- **Disable DHCP Server:** The DSA-3200 will not dynamically configure DHCP clients on the Public Wireless LAN.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server
------------------------------	--

- **Enable DHCP Server:** The DSA-3200 will dynamically configure DHCP clients on the Public Wireless LAN. The appropriate information is needed for the DHCP server to function properly. To configure, enter: DHCP Scope Start IP Address; End IP Address; Primary DNS Server; Secondary DNS Server; Domain Name; WINS Server; Lease Time; and Reserved IP Address List.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server  DHCP Scope Start IP Address <input type="text" value="192.168.2.100"/> * End IP Address <input type="text" value="192.168.2.199"/> * Primary DNS Server <input type="text" value="192.152.81.1"/> * Secondary DNS Server <input type="text"/> Domain Name <input type="text" value="dlink.com"/> * WINS Server <input type="text"/> Lease Time <input type="text" value="1 Day"/> ▾ <a href="#">Reserved IP Address List</a>
------------------------------	--

As an option, the DSA-3200 provides a **Reserved IP Address List** for DHCP clients. This allows the reservation of specified DHCP Scope IP addresses for specified MAC addresses. Click the **Reserved IP Address List** hyperlink to configure.

Reserved IP Address List -- Wireless			
Item	Reserved IP Address	MAC	Description
1	<input type="text" value="192.168.2.101"/>	<input type="text" value="00:0d:61:49:04:54"/>	<input type="text"/>
2	<input type="text" value="192.168.2.106"/>	<input type="text" value="00:0d:88:57:63:1f"/>	<input type="text" value="DWL-G520"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

The Reserved IP Address List provides 40 entries. Enter the desired Reserved IP Address, client MAC address, and a short description (optional) for each reservation. After the information is completely entered, click **“Apply”** to complete the setup.

## 4.1.6 Private LAN Configuration

The DSA-3200 provides a private trusted network that is tied to the Private LAN ports on the rear of the device. The Private LAN does not require user authentication prior to access. The Private LAN may be configured to serve DHCP to DHCP enabled clients.

Private LAN Configuration	
Private LAN	IP Address <input type="text" value="192.168.0.40"/> * Subnet Mask <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server  DHCP Scope Start IP Address <input type="text" value="192.168.0.100"/> * End IP Address <input type="text" value="192.168.0.199"/> * Primary DNS Server <input type="text" value="192.152.81.1"/> * Secondary DNS Server <input type="text"/> Domain Name <input type="text" value="dlink.com"/> * WINS IP Address <input type="text"/> Lease Time <input type="text" value="1 Day"/> ▾ <a href="#">Reserved IP Address List</a>

**IP Address:** Enter the desired IP address for the Private LAN Interface. This will be the default gateway for the Private Network.

**Subnet Mask:** Enter your desired Subnet Mask to determine the size of the Network the Interface may communicate with.

**Related Setup for DHCP Server of Private LAN:**

The DHCP Server is optional and may be disabled or enabled at any time.

**Disable DHCP Server:** The DSA-3200 will not dynamically configure DHCP clients on the Public Wireless LAN.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server
------------------------------	--

- **Enable DHCP Server:** The DSA-3200 will dynamically configure DHCP clients on the Private LAN. The appropriate information is needed for the DHCP server to function properly. To configure, enter: DHCP Scope Start IP Address; End IP Address; Primary DNS Server; Secondary DNS Server; Domain Name; WINS Server; Lease Time; and Reserved IP Address List.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server  DHCP Scope Start IP Address <input type="text" value="192.168.1.100"/> * End IP Address <input type="text" value="192.168.1.199"/> * Primary DNS Server <input type="text" value="192.152.81.1"/> * Secondary DNS Server <input type="text"/> Domain Name <input type="text" value="dlink.com"/> * WINS Server <input type="text"/> Lease Time <input type="text" value="1 Day"/> ▾ <a href="#">Reserved IP Address List</a>
------------------------------	--

As an option, the DSA-3200 provides a **Reserved IP Address List** for DHCP clients. This allows the reservation of specified DHCP Scope IP addresses for specified MAC addresses. Click the **Reserved IP Address List** hyperlink to configure.

Reserved IP Address List -- Private LAN			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

(Total:40) [First](#) [Previous](#) [Next](#) [Last](#)

The Reserved IP Address List provides 40 entries. Enter the desired Reserved IP Address, client MAC address, and a short description (optional) for each reservation. After the information is completely entered, click “**Apply**” to complete the setup.

## **4.2 Advanced Menu**

The configuration pages presented in the Advanced Menu are intended to assist with setup of User Authentication and more specific Hot Spot features. Options may be configured in any of the following Interface Pages: **Authentication Policies, Group, Black List, On-demand User, Roaming** and **Additional**. Refer to each section below for more detailed information regarding functions and configurations.

### **4.2.1 Authentication Policies**

The DSA-3200 provides a familiar D-Link interface designed to enable easy and quick setup to get your Wi-Fi Hot Spot up and operational. The DSA-3200 provides 2 simultaneous user authentication policies to allow Hot Spot users to be authenticated through the Internal User Database or through an External RADIUS server at the same time. An Administrator may adopt different Authentication methods according to each management setup. Each management setup has at most 20 management rules to go with the group configuration, so that the management on general users is diversified and flexible. An Administrator may select the desired management set up via the pull-down menu. As an alternative to User based authentication, Layer 2 Authentication is also possible in the form of 802.1x or WPA.

Default Policy	
Policy Name	Policy_1
Policies Configuration	
Select Policy	1:Policy_1 <input type="checkbox"/> Set as default: <input checked="" type="checkbox"/>
Policy Name	Policy_1 * (User authenticates as username@policyname)
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	1 : Blacklist1
Authentication Server	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS <b>Local Users List</b> Assign to Group: 1:Group1
Layer 2 Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> 802.1x <input type="radio"/> WPA w/802.1x <input type="radio"/> WPA-PSK

**Default Policy:** This Authentication method will be used to authenticate all users that do not specify an authentication policy during login (*user@policy1*).

**Policy Name:** Friendly name used to identify the policy based on the Administrator's preference.

**Policies Configuration:** Authentication Policy parameter configuration.

**Select Policy:** The DSA-3200 provides 2 separate Authentication policies for flexibility. Select the Authentication policy to be configured from the pull-down menu.

**Set as Default:** Check the Checkbox to assign the default Authentication policy accordingly. This Authentication method will be used to authenticate all users that do not specify an authentication policy during login (*user@policy1*).

**Policy Name:** Friendly name for the Authentication policy will also be used during user login as a username postfix to differentiate the authentication method used to authenticate the user.

**Policy Status:** The Administrator has the option of disabling or enabling each authentication policy independently, allowing a single policy to serve all public access networks. Disabled authentication policies will not be used to authenticate users.

**Warning:** The Policy Name cannot use the following system defined words: GRIC, MAC, or IP. It is recommended that a useful name be assigned to each policy.

Black List Profile	<input type="text" value="None"/>
Authentication Server	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS <b>Local Users List</b> Assign to Group: <input type="text" value="1:Group1"/>
Layer 2 Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> 802.1x <input type="radio"/> WPA w/802.1x <input type="radio"/> WPA-PSK

**Black List Profile:** Select from a previously defined user blacklist profile to block the specified users from being able to authenticate using this authentication policy.

**Authentication Server:** Select the server that will perform user authentication functionalities for the selected Authentication Method: Local User Database or external RADIUS Server.

**Assign to Group:** Assign all users that authenticate using this Authentication Method to the specified User group selected from the pull-down menu.

**Two Authentication Mechanisms:**

**1. Local**

The user’s account information is stored in DSA-3200. If you need to manage any user accounts, click the **Local Users List** hyperlink on the Authentication Server interface to enter the Account Management Interface.

Users List				
Username	Password	MAC	Group	Del All
			Remark	
<a href="#">ADMIN</a>	AMDIN	01:23:45:67:89:AB	Group1	<a href="#">Delete</a>

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#)

**User List:** The user list provides a complete view of existing user accounts as shown above. The information displayed includes Username, Password, MAC (not necessary), Group ID, and Administrative Remarks. An Administrator may delete or search user information via this management interface. One may also use the “**Delete All**” function to delete all local user accounts. To edit the content of an individual user account, click the Username hyperlink of the desired user account to enter the **Edit User** Interface. Clicking the “**Refresh**” button will show the most updated data.

Add User					
Item	Username	Password	MAC (XX:XX:XX:XX:XX:XX)	Group	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	None ▾	<input type="text"/>

**Add User:** Click “**Add Users**” on the **User List** to enter the **Add User** interface, and key in the appropriate information such as username, password (required), MAC, and Remark (not required). Click on the “**Apply**” button to complete the addition.

User '**Todd**' has been added!  
User '**Matt**' has been added!  
User '**David**' has been added!  
User '**Emily**' has been added!

### Edit User

Username  \*

Password  \*

MAC

Group  ▼

Remark

**Edit Account:** Click the desired username that you want to modify from the **User List** to enter the User Account Interface, and then key in your desired information such as username and password (compulsory), MAC, and Remark (optional). Then, click **“Apply”** to complete the modification.

**Note:** The format of each line is "ID, Password, MAC, Group, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will be replaced by the new ones.

**Upload User Account**

File Name	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Submit"/>		

**Upload User:** Click **“Upload User”** to enter the Upload User Accounts interface. Click the browser button to select the text file for the user account. Then click **“Submit”** to complete the upload. The format of the uploading file is text file, and Each line represents a User Account, **Format→Username, Password, MAC, Group, Remark**, each parameter is separated by a comma, and no space is allowed between MAC, Group and Remark but the comma is still needed. The Group parameter should be 0, 1 or 2. 0 means “None”, 1 means “Group1” and 2 means “Group2.” Group 1 and Group 2 is user defined in **Advanced → Group → Group name**. When you uploading, make sure that there is no duplicate account in the text file and in the embedded database. Otherwise, no account will be generated.

Users List				
Username	Password	MAC	Group	Remark
test	test		1	

**Download**

**Download User:** Click “**Download User**” in the **User List** to enter the Download User Accounts interface, and the system will directly list all created user accounts, and show a hyperlink for the download at the bottom of the screen. Move the cursor of the mouse to such hyperlink and press the right button of the mouse to save as new file. Then, you can list the user accounts and load them into your computer.

## 2. RADIUS

The RADIUS client in the DSA-3200 allows user accounts to be authenticated using an external RADIUS server as an alternative to storing the user accounts locally on the DSA-3200. Configure both the Primary and Secondary server information as necessary to ensure all RADIUS authentication requests are properly handled.

Authentication Server	<input type="radio"/> Local <input checked="" type="radio"/> RADIUS	
	<b>Primary RADIUS Server</b>	
	802.1x Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Trans Full Name	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Server IP	<input type="text"/> *
	Authentication Port	<input type="text"/> *(Default:1812)
	Accounting Port	<input type="text"/> *(Default:1813)
	Secret Key	<input type="text"/> *
	Accounting Service	Disabled ▾
	Authentication Method	PAP ▾
	<b>Secondary RADIUS Server</b>	
	Server IP	<input type="text"/>
	Authentication Port	<input type="text"/>
	Accounting Port	<input type="text"/>
	Secret Key	<input type="text"/>
Accounting Service	Disabled ▾	
Authentication Method	CHAP ▾	
Assign to Group:	1:Group1 ▾	

**802.1X Authentication:** Select to enable 802.1x as needed. The Switch or AP connected to the DSA-3200 must also support 802.1x protocol for this feature to work properly.

**Trans Full Name:** Select whether or not the DSA-3200 will transfer the entire username or a partial username to the RADIUS server for authentication.

**Enable:** ID and postfix will transfer to RADIUS server for authentication.

**Disable:** Only ID will transfer to RADIUS server for authentication.

**Server IP:** Enter the appropriate IP Address or Fully Qualified Domain Name of the RADIUS server to be used to authenticate user accounts.

**Authentication Port:** The TCP Port that will be used to authenticate users through the RADIUS server.

**Accounting Port:** The TCP Port that will be used to communicate accounting information to the RADIUS server.

**Secret Key:** This shared secret should be configured on both the RADIUS server and RADIUS client (DSA-3200). The shared secret assures only the RADIUS server and client can decipher each message.

**Accounting Service:** Enabling this feature tells the DSA-3200 to report account usage statistics to the RADIUS server for each authenticated user that is connected to the DSA-3200.

**Authentication Method:** Choose between CHAP or PAP as the authentication protocol between the RADIUS Server and Client. In general CHAP is more secure.

**Layer 2 Authentications:**

- **Disable:** All authentications will be performed at Layer 3, after the client has already joined the network.

Layer 2 Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> 802.1x <input type="radio"/> WPA w/802.1x <input type="radio"/> WPA-PSK
---------------------------	--

- **802.1x:** Clients will be unable to join the network until they have been granted access via successful completion of the 802.1x authentication and accounting mechanism.

**Policies Configuration**

Disable  802.1x  WPA w/802.1x  WPA-PSK

Layer 2 Authentication

Authentication Server IP: 10.1.1.1 \*

Authentication Port: 1812 \*(Default:1812)

Secret Key: 1234 \*

Accounting Service: Enabled

Accounting Server IP: 10.1.1.2 \*

Accounting Port: 1813 \*(Default:1813)

Secret Key: 1234 \*

Assign to Group: 2:Group 2

**Authentication Server IP:** IP address or FQDN of the server performing User Authentication Services (can consist of username/password, TLS, etc.).

**Authentication Port:** The TCP Port that will be used to authenticate users through the Authentication server.

**Secret Key (Authentication Server):** This shared secret should be configured on both the Authentication server and Authenticator client (DSA-3200). The shared secret assures only the Authentication server and client can decipher each message.

**Accounting Service:** Click to enable the accounting service.

**Accounting Server IP:** Enter the appropriate IP Address or Fully Qualified Domain Name of the Authentication server to be used to authenticate potential users.

**Accounting Port:** The TCP Port that will be used to communicate accounting information to the Accounting server.

**Secret Key (Accounting Server):** This shared secret should be configured on both the Accounting server and Accounting client (DSA-3200).

**Assign to Group:** Users that are authenticated through 802.1x will be assigned the permissions of the selected group.

*Caution: Layer 2 authentication mechanisms override any Layer 3 (local user or RADIUS) mechanisms already configured making them null and void.*

- **WPA w/802.1x:** Also known as WPA-EAP, this is a wireless extension of 802.1x Port Based Authentication.

The screenshot shows the 'Policies Configuration' window for 'Layer 2 Authentication'. At the top, there are four radio buttons: 'Disable', '802.1x', 'WPA w/802.1x' (which is selected), and 'WPA-PSK'. Below this, there are several configuration fields:

- Authentication Server IP:** A text box containing '10.1.1.1' with a red asterisk to its right.
- Authentication Port:** A text box containing '1812' with a red asterisk and the text '\*(Default:1812)' to its right.
- Secret Key:** A text box containing '1234' with a red asterisk to its right.
- Accounting Service:** A dropdown menu with 'Enabled' selected.
- Accounting Server IP:** A text box containing '10.1.1.2' with a red asterisk to its right.
- Accounting Port:** A text box containing '1813' with a red asterisk and the text '\*(Default:1813)' to its right.
- Secret Key:** A text box containing '1234' with a red asterisk to its right.
- Assign to Group:** A dropdown menu with '2:Group 2' selected.
- Group Re-key Time:** A text box containing '100' with a red asterisk and the text 'sec (0~6000)' to its right.

**Group Re-key Time:** Time interval for re-keying broadcast/multicast keys in seconds.

- **WPA-PSK:** Supports WPA-Personal, only requiring users to provide a PSK.

Policies Configuration	
Layer 2 Authentication	<input type="radio"/> Disable <input type="radio"/> 802.1x <input type="radio"/> WPA w/802.1x <input checked="" type="radio"/> WPA-PSK
	Group Re-key Time <input type="text" value="100"/> * sec (0~6000)
	<input type="radio"/> Passphrase <input type="text"/>
	<input checked="" type="radio"/> PSK <input type="text"/>
	Assign to Group <input type="text" value="2:Group 2"/>

**PSK (Pre Shared Key):** This key should be a random sequence of Hexadecimal characters (upper or lowercase letters and numbers) 64 Characters in length.

**Pass-phrase:** Alternatively the Administrator may choose a pass-phrase that will be used to generate the Pre-Shared Key making user configurations much more manageable. Enter anywhere from 8 to 63 Alphanumeric characters (including symbols and white space) to be used by clients to join the network.

## 4.2.2 Group Configuration

The DSA-3200 provides the ability to configure 2 separate user groups enabling separate permissions to be assigned to the same user pool. Each user group may be assigned a specific Firewall profile, time schedule profile, and/or bandwidth maximum. These permissions will apply to all users assigned to the corresponding group number.

Group Configuration	
Select Group	1:Group1 <input type="button" value="v"/>
Group Name	Group1
<b>Select Group Profile</b>	
Firewall Profile	1: Firewall 1 <input type="button" value="v"/> <a href="#">Edit</a>
Schedule Profile	1: Schedule 1 <input type="button" value="v"/> <a href="#">Edit</a>
Bandwidth	Unlimited <input type="button" value="v"/>

**Group Name:** Friendly name to help identify the privileges of the associated user.

**Firewall Profile:** A specific firewall profile may be assigned to a user group to allow differentiated access privileges between groups. Click the Edit Hyperlink to manage the Firewall Profiles after all other changes have been applied.

**Schedule Profile:** A specific Schedule profile may be assigned to a user group to allow differentiated timed access privileges between groups. Click the Edit Hyperlink to manage the Schedule Profiles after all other changes have been applied.

**Bandwidth:** Select the maximum Bandwidth that the corresponding user group will be able to utilize. Keep in mind that this configures the Ceiling Bandwidth.

### ■ Firewall Profiles - Edit

The DSA-3200 provides a single Global and 2 custom firewall profiles. The Global policy will affect all users, whereas the other policies will only affect those user groups to which they are assigned.

Firewall Profiles						
Select Profile: Global:Global						
Profile Name: Global						
Filter Rule Item	Active	Action	Name	Source	Protocol	MAC
				Destination		
1	<input checked="" type="checkbox"/>	Pass	allow_http	ANY	TCP	
				ANY		
2	<input checked="" type="checkbox"/>	Pass	allow_ftp	255.255.255.255/32	TCP	00:04:B5:E6:12:D2
				255.255.255.255/32		
3	<input checked="" type="checkbox"/>	Pass	allow_icmp	ANY	ICMP	
				ANY		
4	<input checked="" type="checkbox"/>	Pass	allow_ssh	ANY	TCP	
				ANY		
5	<input checked="" type="checkbox"/>	Pass	allow_telnet	192.168.1.171/32	TCP	
				ANY		
6	<input checked="" type="checkbox"/>	Pass	allow_Public	ANY	ALL	
				ANY		
7	<input checked="" type="checkbox"/>	Pass	allow_Private	ANY	ALL	
				ANY		
8	<input type="checkbox"/>	Pass	pass_WLAN	ANY	ALL	
				ANY		
9	<input checked="" type="checkbox"/>	Block	block_1PC	255.255.255.255/32	ALL	00:04:23:2B:E6:62
				255.255.255.255/32		
10	<input checked="" type="checkbox"/>	Block	block_all	ANY	ALL	
				ANY		

**Filter Rule Item:** The filter rules obey Top Down evaluation to determine the permission of a transmission from the source address to the target address or examine whether there is a data loss. Click the **Index Number** for rule specific configurations.

Edit Filter Rule					
Rule Item: 1					
Rule Name: <input type="text"/>				<input type="checkbox"/> Enable this Rule	
Action : <input type="text" value="Block"/>		Protocol <input type="text" value="ALL"/>			
Source MAC Address: <input type="text"/> (For Specific MAC Address Filter)					
	Interface	IP	Subnet Mask	Start Port	End Port
Source	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="WAN"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>

**Rule Name:** Friendly name given to identify the rule and its intended action.

**Enable this Rule:** Such rule will be effective when selected.

**Action:** The basic behavior of the rule. If the rule parameters match, this action will be taken.

**Pass :** The packet passes successfully.

**Block :** The packet is blocked and dropped.

**Protocol:** Provides three common protocols: TCP, UDP, and ICMP. The All option will not discriminate based on packet protocol (protocols other than 1, 6, or 17).

**Source MAC:** MAC Address of the Transmission Source. Leave blank to specify any.

**Source (Destination) Interface:** Source (Destination) Interface includes 5 choices: WAN, Wireless LAN, Public LAN, Private LAN, or ALL.

**Source (Destination) IP Address:** IP address of Transmission Source (Destination).

**Source (Destination) Subnet Mask:** Subnet Mask of Source (Destination).

**Source (Destination) Start Port:** Start Port of Source (Destination).

**Source (Destination) End Port:** End Port of Source (Destination).

■ **Login Schedule Profiles - Edit**

User login schedules may be configured to allow/disallow access during the specified periods of time. Times corresponding to checkboxes will be enabled, unchecked boxes indicate a disable or blocked status.

Login Schedule Profile							
Select Profile:	1:Schedule 1						
Profile Name:	Schedule 1 <input checked="" type="radio"/> Enable <input type="radio"/> Disable						
hour	SUN	MON	TUE	WED	THU	FRI	SAT
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

### 4.2.3 Black List Configuration

The DSA-3200 provides a black list function to block specified users from accessing Network resources. Administrator can add to, delete from, or edit a specific black list. Each blacklist may have at most 40 users. Users in the blacklist will be denied access upon authentication attempt.

Black List Configuration		
Select Black List :	1:Blacklist 1 ▾	
Name	Blacklist 1	
User	Remark	<input type="button" value="Delete"/>

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#)

**[Add User to List](#)**

Click “**Add User to List**” to access the **Add Users to Blacklist** Menu.

Add Users to Blacklist : Blacklist 1		
No	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Enter the username you wish to block and a remark, click “**Apply.**”

To return to the **Black List Configuration**, click “**Prev.**”

Black List Configuration		
Select Black List : 1:Blacklist 1		
Name	Blacklist 1	
User	Remark	Delete
Blacklist_test		<input checked="" type="checkbox"/>

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#)

#### Add User to List

To delete a user from the black list, select the appropriate delete check box and click the “Delete” button.

*Caution: After you delete a user, no message or request of confirmation will appear.*

## 4.2.4 On-demand User Configuration

**On-demand user:** When a DSA-3100P is connected to the DSA-3200’s console port, 2000 On-demand user accounts are made available. By default, the On-demand user database is empty. Each time one presses the Printer’s Print button, an On-demand user will be created and stored in the DSA-3200 while at the same time a receipt is printed out with the user credentials and Wireless Network Information (SSID, WEP).

On-demand User Configuration	
Store Name	DSA-3200 (e.g.: DSA-3200. Max: 8 char)
Receipt Header	Welcome! (e.g.: Welcome!)
Receipt Footer	Thank You! (e.g.: Thank You!)
Printer Baud Rate	9600
Assign To Group	2:Group 2
WLAN ESSID	Airspot (e.g.: Airspot)
WEP Key	wepkeytest

[On-demand Users List](#) [Billing Configuration](#) [Upload On-demand User](#)

Field	Description
<b>Store Name</b>	You can specify the prefix for each automatically generated user name up to a maximum of 8 characters, for example: D-Link.
<b>Receipt Header</b>	You can configure the receipt's header in this filed.
<b>Receipt Footer</b>	You can configure the receipt's footer in this filed.
<b>Printer Baud Rate</b>	You may specify the COM port baud rate to support other printers. The Default value is 9600.
<b>Assign to Group</b>	You can assign on-demand users to a pre-determined group.
<b>WLAN ESSID</b>	You can specify the AP's ESSID in this filed.
<b>WEP Key</b>	You can specify the AP's WEP key in WEP Key filed.

- **On-demand User List:** A list of all On-demand user accounts configured in the DSA-3200.

**On-demand Users List**

Username	Password	Remain Time Quota	Status	Expire Time	<input type="button" value="Delete All"/>
(Total:0) <a href="#">First</a> <a href="#">Previous</a> <a href="#">Next</a> <a href="#">Last</a>					

To delete specific users accounts, click on the checkbox next to those user accounts and click the **Delete** button. To delete all user accounts, click **Delete All**.

- Billing Configuration:** The DSA-3200 provides 10 separate On-Demand User billing profiles. The default profile will be used when the DSA-3100P is connected to the DSA-3200.

Billing Configuration					
Button	Status	Time Quota	Account Expire Date	Validity Duration	Price
1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	2 hrs 0 mins	3 days	5 days	\$20
2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
6	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	
0	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	hrs mins	days	days	

**Status:** Enable/Disable this billing rule. When using the DSA-3100P enable only one Billing Configuration Profile.

**Account Expire Day:** The number of days after generation during which the account will be valid. After the specified number of days, any inactivated account will be automatically expired

**Validity Duration:** In the case where a user has activated his or her account the account will be valid for the number of days specified here.

**Price:** Administrator assigned Price for online access.

■ **Upload On-demand User:**

**Note1: The format of each line is "ID, Password, type, Session length, Activation deadline, Validity duration" without the quotes. There must be no space between the fields and commas. When adding user accounts by uploading a file, any existing account in the embedded database that has the same user name as the one defined in the uploaded file will not be replaced by the new one.**

**Note2: The value of type for sessional user is 0. The unit of session length is second. ID and Password must be in upper case.**

Upload On-demand User Account	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

**File Name:** Key in the path or browse to the file that contains the on-demand user information (format as described in Note 1). The unit of Activation deadline and Validity duration entries are measured in days.

## 4.2.5 Roaming Configuration

The DSA-3200 has the capability to allow GRIC and Airpath Wireless Users access to the Hot Spot by using their existing user credentials. Service from either GRIC or Airpath Wireless is required before the DSA-3200 can authenticate such users. Once the appropriate service is obtained, gather the information provided by the appropriate Wireless Access Provider to complete the DSA-3200 configuration.

Roaming Configuration	
GRIC	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Server IP <input type="text"/> * Authentication Port <input type="text"/> * Accounting Port <input type="text"/> * Secret Key <input type="text"/> * Accounting Service <input type="text" value="Disabled"/> ▾ Authentication Method <input type="text" value="PAP"/> ▾ Default Group <input type="text" value="1:Group1"/> ▾
Airpath	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Airpath Server <a href="#">Free Surfing Area</a> Device name <input type="text" value="dsa3200"/> * Server IP <input type="text" value="63.166.40.7"/> * Authentication Port <input type="text" value="1812"/> * Accounting Port <input type="text" value="1813"/> * Secret Key <input type="text" value="dlinktest"/> * Accounting Service <input type="text" value="Enabled"/> ▾ Authentication Method <input type="text" value="CHAP"/> ▾ Default Group <input type="text" value="1:Group1"/> ▾ <a href="#">Upload Certificate</a>

GoRemote users will be authenticated via a secure web page hosted on the DSA-3200 while Airpath Wireless users have the option of redirection to AirpathWireless's secure login page via the internally hosted login page.

■ **GRIC Roaming: GoRemote will provide all required information**

Below is a GRIC example:

**DSA-3200 Authentication Port IP address:** 192.168.1.254

**Username:** xyz, and his **IP address:** 192.168.1.100

**Password:** xyz

**MAC address:** 01:23:45:67:89:ab

The gric.shtml example should look like this:

**`https://192.168.1.254/loginpages/gric.shtml?uname=xyz&uip=192.168.1.100&upwd=xyz&umac=01:23:45:67:89:ab`**

As an alternative, a user may also use the internally hosted login page by specifying [username@GRIC](#) on ID field and the appropriate password.

■ **Airpath Roaming: Airpath Wireless will provide all required information**

The DSA-3200 Administrator must have a roaming user agreement with Airpath Wireless in order to use this feature. Users who registered Airpath Wireless's service may login to the local public network via roaming. Within the system default login page, users are provided with a link redirected to Airpath's login page. The URL of the login page or more generally all of Airpath Wireless IP space must be configured in the Free Surfing Area for this function to work.

## 4.2.6 Additional Configuration

Additional Configuration	
User Control	Logout Timer : <input type="text" value="10"/> Min(s) (1 - 1440)
Friendly	<input type="checkbox"/> Login <input type="text" value="12 Hours"/> <input type="checkbox"/> Logout
Internet Connection Detection	http:// <input type="text"/>
Upload File	<a href="#">Upload Login Page</a> <a href="#">Upload Logout Page</a> <a href="#">Upload Certificate</a>
POP3 Message	<a href="#">Edit Mail Message</a>

**User Control:** This applies to all users.

**Logout Timer :** If a user has idled and not used the network for the specified amount of time the DSA-3200 will automatically log out the user. The logout time is specified in minutes, having values ranging from 1~1440. Default is 10 minutes.

**Friendly:** The DSA-3200 provides features to increase the user-friendliness of the experience.

**Login:** After you select this function, the login page will automatically obtain the username and password from a previous login. The login page will be dismissed and the user will no longer need to enter a username and password to login. The username and password for login will be saved for **12 hours**.

**Logout:** Following a successful login, a small window will appear that shows the user's information and provides them with a logout button for ease of logout. With friendly logout enabled a warning message will appear when the user attempts to close this window. When disabled, the window will close and users must manually logout by browsing to 1.1.1.1.

**Internet connection detection:** DSA-3200 detects if the Internet connection is

functioning properly by accessing a predetermined URL (or IP address).

**URL or IP address:** this predetermined URL will be used as a target address for the DSA-3200 to check the Internet connection.

**Upload File:** The internal Login and Logout pages, as well as the SSL certificate may be replaced with user files.

■ **Upload Login page**

The Login page may be customized to suit any particular application. The coding for this page should be HTML and include the code in the box below. To upload, enter the filename and path of the customized Login page in the appropriate field, or browse and select the file. To recover the factory default login interface, click the **“Use Default Page”** button. After the upload is complete, click the **“Preview”** button at the bottom of this page to preview your user-defined login page.

Upload Login Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	<input type="button" value="Use Default Page"/>

The following HTML code must be included to provide a channel for the user to key in a username and a password.

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

### ■ Upload Logout Page

The Login page may be customized to suit any particular application. The coding for this page should be HTML and include the code in the box below. To upload, enter the filename and path of the customized Login page in the appropriate field, or browse and select the file. To recover the factory default login interface, click the “**Use Default Page**” button. After the upload is complete, click the “**Preview**” button at the bottom of this page to preview your user-defined login page.

Upload Logout Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	<input type="button" value="Use Default Page"/>

The following HTML code must be included to provide a channel for the user to key in a username and a password.

```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

### ■ Upload Image

If either custom login or logout page includes a graphic file, the HTML code of the graphic file path must be included in said page. In the **Upload Image** section, navigate to the **Upload Image File** box and key in the path and file name of such graphic file or browse to select the file. The maximum total size of all graphic files is 512K.

```

```

After a graphic file is uploaded, the second section called **Existing Image Files** will list the graphic files stored on the DSA-3200. You can select or delete any graphic file, and the system will show the used space of the graphic file in the third section.

Existing Image Files :
------------------------

After the web page and graphic files are uploaded, you can click **“Preview”** at the bottom of this page to preview your custom login/logout interface.

Total Capacity: 512 K	
Now Used: 0 K	
<b>Upload Image Files</b>	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

[Preview](#)

■ **Upload Certificate**

The DSA-3200 provides administrators the ability to upload their own SSL Certificate to increase compatibility with Wireless Provider Systems or to integrate seamlessly with a company's own Certificate Authority.

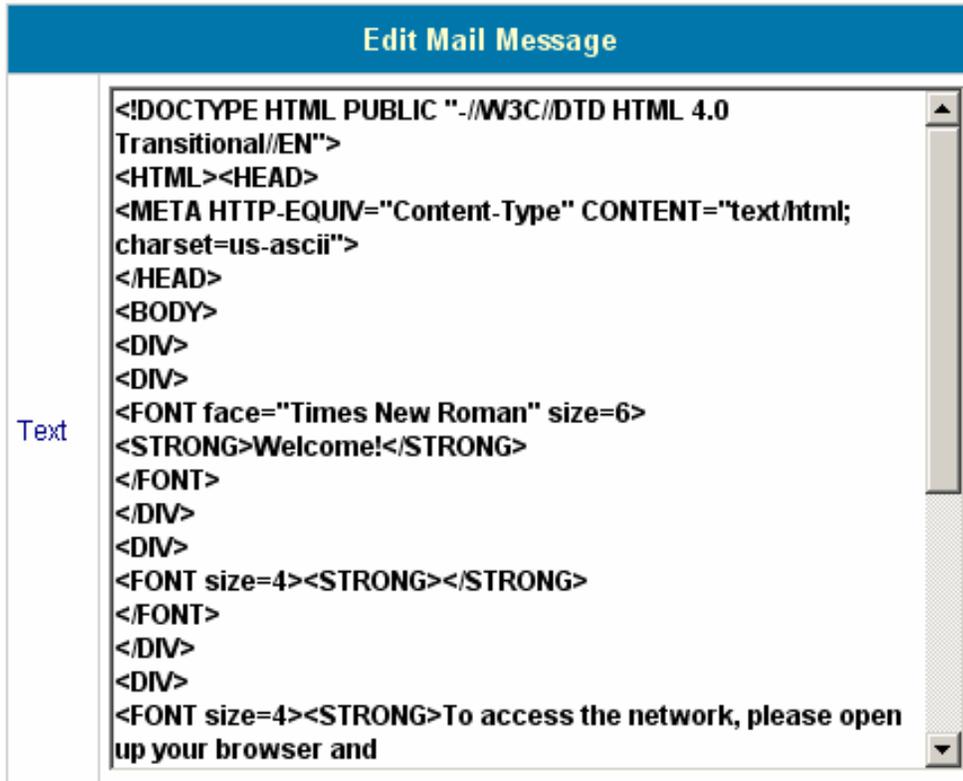
<b>Upload Private Key</b>	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

<b>Upload Customer Certification</b>	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

<input type="button" value="Submit"/>	<input type="button" value="Use Default CA"/>
---------------------------------------	---

### ■ POP3 Message

The DSA-3200 provides a mechanism to alert users that have not signed in and are trying to access Mail resources. The DSA-3200 will deliver an e-mail to the user's inbox. Customize the message to your liking.



## 4.3 Tools Menu

Several functions are provided to control individual aspects of network transmissions, including **Port and IP Redirect**, **Virtual Server**, **Pass Through**, **Monitor IP List**, **Free Surfing Area**, **Proxy**, **DDNS**, **Change Password**, **System**, **Firmware**, and **Restart**.

### 4.3.1 Port and IP Redirect

When a user attempts to connect to a destination defined in the Port and IP Redirect section, the connection packet will be converted to the corresponding defined destination. You may define at most 40 entries to achieve the redirect feature. To convert queries on a specific port, leave the Destination IP blank and only enter the Destination port. In this case all queries on the specified port will be redirected to the defined Translate IP Destination. These settings will be effective immediately after you click “Apply”.

Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

### 4.3.2 Virtual Server

The Administrator may define at most 40 virtual server entries to allow computers on the WAN Network or beyond to access the specified LAN resources. According to the different services provided, the network service can be provided on a TCP or UDP port, or both. Applications that require both Protocols on the same port will require 2 entries. These settings will be effective immediately after you click “Apply”.

Virtual Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

### 4.3.3 Pass Through

#### ■ Pass Through IP Address List

There may be situations where computers on the Public Access Network need Internet Access but cannot provide username and password for authentication. For example, if a server has been put on the managed network and said server requires Internet access; configure the IP address in the following section. The DSA-3200 allows at most 100 Privileged IP addresses. These settings will take effect immediately after you click “Apply”.

**Warning:** *Permitting certain IP addresses to have network access rights without going through the standard authentication process may pose a security risk.*

Pass Through IP Address List		
Item	IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total:100) [First](#) [Prev](#) [Next](#) [Last](#)

■ **Pass Through MAC Address List**

In addition to permitting specific IP addresses to have “free” network access rights without authenticating, the DSA-3200 also provides the ability to do so according to a MAC address. This system permits at most 100 Privileged MAC addresses to have network access rights without going through user authentication. The format of the MAC address is **XX:XX:XX:XX:XX:XX**. These settings will be effective immediately after you click “**Apply**”.

**Warning:** *Permitting certain MAC addresses to have network access rights without going through the standard authentication process may pose a security risk.*

Pass Through MAC Address List		
Item	MAC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total:100) [First](#) [Prev](#) [Next](#) [Last](#)

**Note:** To allow PCs the ability to access WAN resources through the Public Interface without authenticating when User Authentication is enabled, specify the IP address for statically configured PCs or the MAC address for DHCP clients. IP and MAC authentication are separate, only one or the other is required to authenticate.

### 4.3.4 Monitor IP List

The system will use ICMP messages on a customized interval (1, 2, 4, 6, 12 hours and 1 day) to monitor and control the status of IP addresses on the list. If the monitored IP address does not exist or does not respond, the system will send out an e-mail to the Administrator once every 30 minutes, such as: 1:00, 1:30, 2:00, 2:30, and 3:00 until the problem is fixed.

Admin Email	
Send From	<input type="text"/>
Send To	<input type="text"/>
Interval	1 Hour <input type="button" value="v"/>
SMTP Server	<input type="text"/>
Auth Method	PLAIN <input type="button" value="v"/>
Account Name	<input type="text"/>
Password	<input type="text"/>

NONE  
PLAIN  
LOGIN  
CRAM-MD5  
NTLMv1

**Send From:** The email address of the party responsible for monitoring IP addresses.

**Send To:** The email address of the intended recipient of the Admin messages.

**Interval:** The time interval time for dispatching of warning or instruction messages.

**SMTP Server:** The IP address/domain name of your ISP's SMTP server.

**Auto Method:** 5 authentication methods are provided: None, PLAIN, LOGIN, CRAM-MD5 and NTLMv1. Contact your ISP for further information.

**Account Name:** Account name registered with the SMTP server.

**Password:** Account password.

**Monitor IP list:** The list of IP addresses to be monitored.

Monitor IP List			
Item	IP Address	Item	IP Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

**Monitor**

Click "**Monitor**" to view all monitored IP. A maximum of 40 IP address for monitoring is allowed.

**Monitor:** Show monitor IP status.

Monitor IP result		
No.	IP	Result

### 4.3.5 Free Surfing Area

This system allows users to login to certain websites before passing through the Public LAN. You only need to enter the IP address (or Domain Name) of these websites into the Walled Garden List. You can enter up to 20 addresses into this list. This function lets you provide some free service to users. For example, you can provide a brief introduction of the local site, and facilities and path guide on a website, by listing the address of the website in the Walled Garden. Even users having no network access rights can link to any website in the Walled Garden to browse the pages located in the specified domain. This function can be used to provide users a free chance to experience the network service. The customer may experience the actual network service without any preparation in advance. These settings will be effective immediately after you click “**Apply**”.

Free Surfing Area			
Item	Address	Item	Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

### 4.3.6 Proxy

**Internal Proxy Server:** The DSA-3200 has a built-in web proxy server, if you active this function, end users may specify the DSA-3200 as a proxy server, no need to enter the IP address and Port.

**External Proxy Server:** As a basis of the security management features of the DSA-3200, only ports 80 and 443 are allowed (for redirection to login page). In the case that a Proxy Server already exists in your network environment, the Proxy Server IP address and Port of communication must be configured in the DSA-3200 for proper operation. These settings will be effective immediately after you click “**Apply**”.

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

### 4.3.7 DDNS

The DSA-3200 provides the ability to use a Dynamic DNS provider service to assign a host name to the WAN interface even in the event of a Dynamic WAN connection. The DSA-3200 provides support for most popular Dynamic DNS Provider Systems, allowing seamless translation of a dynamic WAN IP address to a domain name.

Dynamic DNS	
DDNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Provider	DynDNS.org(Dynamic) ▼
Host name	DynDNS.org(Dynamic)
Username / E-mail	DynDNS.org(Custom)
Password / Key	DynDNS.org(Static)
	dhs.org
	myip.us
	no-ip.com
	3322.org(Dynamic)
	3322.org(Static)
	zoneedit.com

**DDNS:** Enable activates the Dynamic DNS Update service on the DSA-3200.

**DNS provider:** Select the appropriate provider from the predefined list. Most of these services are offered free of charge.

**Host name:** Enter the hostname that was registered with the selected provider.

**Username / E-mail:** Enter the username or e-mail address that was registered with the selected provider.

**Password / Key:** Enter the password or shared key that was registered with the selected provider.

### 4.3.8 Change Password

To change the Administrator's password, please key in the existing admin Password in the appropriate field, followed by the new password entered twice for verification.

Change Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
New Password (confirm)	<input type="text"/>

**Caution:** *If you lost or forgot the Administrator's Password, you can still change the Administrator's password through the text mode management interface on the serial COM port.*

### 4.3.9 System Settings

The Systems Settings Page provides the ability to back up the current configuration to the local HDD, restore the configuration from the local HDD, and/or reset the device to factory default settings.

System Settings	
Create Backup Image	<input type="button" value="Create"/>
Restore Settings From File	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Restore"/>
Reset to Factory Default	<input type="button" value="Reset"/>

**Create Backup Image:** Generate the backup (image) file. Click on the Hyperlink to download to the local HDD.

**Restore Settings From File:** Load a configuration file from the HDD by entering the filename and path or Browse to the appropriate location on the local HDD.

**Reset to Factory Default:** Restore to the factory default settings of the DSA-3200.

### 4.3.10 Firmware Upgrade

One may upgrade the DSA-3200 firmware with any later version code obtained from D-Link Systems, Inc. Support Site.

[DSA-3200 Support Page](#)

Firmware Upgrade	
Current Version	0.02B1
File Name	<input type="text"/> <input type="button" value="Browse..."/>

**Warning:** *Firmware upgrade may cause user data loss. Please refer to the version description or release notes to see if there is any limitation before upgrading your firmware.*

Click "**Browse**" to browse the local HDD for the appropriate firmware file. Upon locating the appropriate firmware image file, click "**Submit**" and the browser will upload the firmware file to the DSA-3200. Once the upload procedure has begun do not disconnect power or attempt to access the DSA-3200 through another interface. Doing so might interrupt the upgrade process rendering the flash image useless.

You must restart the system before the upgrade firmware is effective. If you have modified any device settings, remember to save the setting before restarting the system.

**Warning:** *Please restart the system through the management interface. Do not turn off the system directly and then turn on the power again. Doing so may damage the upgraded firmware.*

### 4.3.11 Restart

This function allows you to safely restart the DSA-3200. The restart procedure takes approximately three minutes. If you need to remove power from the DSA-3200 it is recommended to restart the DSA-3200 through this interface and remove power after the status light is solidly lit.

Do you want to **restart** DSA-3200?

YES NO

**Caution:** *All online users connected to the system will be disconnected during the system restart.*

## 4.4 Status

The Status Section provides system information concerning device configuration and user activity/usage statistics. The following configuration pages are explained in detail in the following sections: **Device Info**, **Interface**, **Current Users**, **Traffic History** and **Notify**.

## 4.4.1 Device Info

This section provides information regarding the current running version of code in addition to management and essential systems configurations.

System Status		
	Current Firmware Version	0.02B1
	System Name	dsa-3200.com
	Admin Info	Sorry! The service is temporarily unavailable.
	Succeed Page	http://www.dlink.com
	External Syslog Server	N/A:N/A
	Proxy Server	Disabled
	Internet Connection Status	Disabled
Manage	Remote Manage IP	0.0.0.0/0.0.0.0
	SNMP	Disabled
History	Retain Days	3 Days
	Email To	N/A
Time	External Time Server	tock.usno.navy.mil
	Date Time(GMT+0:00)	Wed, 01 Dec 2004 09:30:41 -0800
User	Idle Logout Timer	10 Min(s)
DNS	Primary DNS Server	192.152.81.1
	Secondary DNS Server	4.2.2.2
Friendly	Login	Disabled
	Logout	Disabled

Item		Description
<b>Current Firmware Version</b>		The firmware version currently used by DSA-3200
<b>System Name</b>		System name, and the default is DSA-3200
<b>Admin Info</b>		Administrator's related information will be shown on the login screen when a user has a connection problem.
<b>Succeed Page</b>		The starting web page after a user logs on successfully.
<b>External SYSLog Server</b>		IP address and port number of external SYSLog Server
<b>Proxy Server</b>		Proxy Server enabled or disabled.
<b>Internet Connection Status</b>		When the <b>WAN</b> connection is abnormal ( <b>Internet Connection Detection</b> ), all on-line users that open a new browser will see Internet Connection Failure Info.
<b>Manage</b>	<b>Remote Manage IP</b>	May be a specific IP address or IP Network enabled to manage the DSA-3200 through the WAN port.
	<b>SNMP</b>	Enable or disable SNMP management function
<b>History</b>	<b>Retain Days</b>	Max Number of days the user History will be stored
	<b>Email To</b>	Send the history to this email address.
<b>Time</b>	<b>External Time Server</b>	The DSA-3200 uses NTP to obtain the latest and most accurate time reading available.
	<b>Date Time</b>	The system time is local time.
<b>User</b>	<b>Idle Logout Timer</b>	Max number of minutes a user can be idle before logout
<b>DNS</b>	<b>Primary DNS</b>	Primary DNS Server IP Address
	<b>Secondary DNS</b>	Secondary DNS Server IP Address
<b>Friendly</b>	<b>Login</b>	User must click " <b>Login</b> " to execute the login procedure. " <b>Enabled</b> " Indicates that after the first login users will not need to supply username and password again.
	<b>Logout</b>	Upon user login, a small window will show the user's information and provide a logout button. " <b>Disable</b> " indicates that closing the small window will not prompt the user for logout verification.

## 4.4.2 Interface

This section provides Interface status for the following interfaces: **WAN port**, **Wireless port**, **Public** and **Private LAN Port**.

Interface Status		
WAN	MAC Address	00:0F:3D:84:B3:BC
	IP Address	67.130.140.152
	Subnet Mask	255.255.255.0
Wireless	Mode	NAT
	MAC Address	00:0D:88:E6:E7:A5
	IP Address	192.168.2.40
	Subnet Mask	255.255.255.0
	ESSID	Airspot
	Channel	N/A
	Encryption Function	Disabled
Wireless DHCP Server	Status	Disabled
Public	Mode	NAT
	MAC Address	00:0F:3D:84:B3:BB
	IP Address	192.168.1.40
	Subnet Mask	255.255.255.0
Public DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.100
	End IP Address	192.168.1.199
	Lease Time	1440 Min(s)
Private	Mode	NAT
	MAC Address	00:0F:3D:84:B3:BA
	IP Address	192.168.0.40
	Subnet Mask	255.255.255.0
Private DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.0.100
	End IP Address	192.168.0.199
	Lease Time	1440 Min(s)

Item		Description
WAN	MAC Address	The MAC address of the WAN port
	IP Address	The IP address of the WAN port
	Subnet Mask	The Subnet Mask of the WAN port
Wireless	Mode	Wireless port mode: NAT mode
	MAC Address	The MAC address of the Wireless port
	IP Address	The IP address of the Wireless port
	Subnet Mask	The Subnet Mask of the Wireless port
	ESSID	The ESSID of the Wireless port
	Channel	The Channel of Wireless
	Encryption Function	Encryption function of wireless
Wireless DHCP Server	Status	Enable/disable DHCP server
Public LAN	Mode	Public LAN mode: NAT mode
	MAC Address	The MAC address of the Public LAN
	IP Address	The IP address of the Public LAN
	Subnet Mask	The Subnet Mask of the Public LAN
Public DHCP Server	Status	Enable/disable DHCP server on Public LAN
	WINS IP Address	Set the WINS server IP on DHCP server
	Start IP Address	Starting IP Address in DHCP IP range
	End IP address	End IP address in DHCP IP range
	Lease Time	The lease time of IP Address
Private	Mode	Private LAN port mode: NAT mode
	MAC Address	The MAC address of the Private LAN port
	IP Address	The IP address of the Private LAN port
	Subnet Mask	The Subnet Mask of the Private LAN port
Private DHCP Server	Status	Enable/disable DHCP server
	WINS IP Address	Set the WINS server IP on DHCP Server
	Start IP Address	Starting IP Address in DHCP IP range
	End IP address	End IP Address in DHCP IP range
	Lease Time	The lease time of the IP address

### 4.4.3 Current Users

In this function, you can obtain particular information pertaining to each online user including **Username**, **IP Address**, **MAC Address**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out**, **Idle Time** and **Logout**. To force a user logout, simply click the **Logout** hyperlink next to the online user's name.

Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Logout
	IP	MAC	Pkts Out	Bytes Out		

### 4.4.4 Traffic History

One may browse the billing history of stored by the DSA-3200 through this section. The history of each day will be saved independently. This system will save the history in the DRAM for no more than 3 days.

Traffic History	
Date	Size (Byte)
<a href="#">2004-09-02</a>	65
<a href="#">2004-09-03</a>	65

**Caution:** Since the history is saved in DRAM, if you need to restart the DSA-3200 and want to keep the history, manually duplicate the history by saving to HDD.

If you have entered the Administrator's e-mail address in the Notification configuration, then the system will automatically send out the history of the previous day to the specified e-mail address.

The first line of the history file is the title; the actual history starts from the second line. Each line includes a record, and each record consists of 10 fields **Date**, **Type**, **Name**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out**, and **Bytes Out** to show the history of each user.

Traffic History (2004-11-30)									
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	

### 4.4.5 Notifications

The DSA-3200 will save the billing history in the internal DRAM for up to 3 days. If you wish to automatically send the history to your email address, please enter your e-mail address in the receiver field.

Notify Configuration	
History Email	Sender E-mail: <input type="text"/>
	Receiver E-mail: <input type="text"/>
	SMTP Server: <input type="text"/>
	Auth Method: <input type="text" value="NONE"/>
	Interval: <input type="text" value="1 Hour"/>
Syslog To	IP: <input type="text"/> Port: <input type="text"/>

1 Hour  
2 Hours  
4 Hours  
6 Hours  
12 Hours  
1 Day

**Sender E-mail:** The email address of the administrator responsible for maintaining the DSA-3200 (in some cases this must be a valid e-mail address as supplied by ISP).

**Receiver E-mail:** The email address of the intended History recipient.

**SMTP Server:** The IP address or Fully Qualified domain name of ISP SMTP Server.

**Auth Method:** Choose one of 5 types of SMTP extended authentication methods: None, PLAIN, LOGIN, CRAM-MD5 and NTLMv1. Please contact your ISP or SMTP server administrator for more information on their Authentication Methods.

**Account Name:** Account name registered with the SMTP server.

**Password:** Account password.

**Interval:** The Interval column specifies the interval for sending history e-mails. If you choose one day, then the history mail will be sent to you once a day.

**SYSLog To:** Specify the IP address and Port (default is 514) of the SYSLog server.

## 4.5 Help

The Help section provides on-line instructions for operating the DSA-3200.



**Home**   **Advanced**   **Tools**   **Status**   **Help**

### Welcome to administration system

The administration system allows you to set various networking parameters, enable and customize network services, manage user accounts and monitor user status. Administration functions are separated into six categories: **Home**, **Advanced**, **Tools** and **Status**. Each of them is described briefly below.

**Home:** This section relates to system configuration, include Wizard, System, WAN , Public Network, Wireless and, Private Network.

**Advanced:** This section contains user management options, includes Authentication methods, Group policy, Black list, On-demand users profile, Roaming and Additional setting for user login control.

**Tools:** This section includes most of System Configuration. Port and IP Redirect, Virtual Server, Pass Through, Monitor IP, Free Surfing Area, Proxy, DDNS, Change Password, System, Firmware and Restart.

**Status:** This part provides administrator with Device Information, Interface Status and Current Users Status. It also allowed administrator monitor Traffic History. With Notify, history data can be assigned mail to/from specific receiver/sender by configurable interval.

## 4.6 Confirm Functionality of User Authentication

If all the previous steps were properly completed, we should be able to connect to a public LAN port to experience the managed network access environment. First, connect an Ethernet enabled PC configured to support TCP/IP to the network via a Public LAN port. After a dynamic IP address is obtained on the PC, open an Internet browser and surf to any website. The default login webpage will appear in the Internet browser.



The screenshot shows the user login interface for the DSA-3200 gateway. At the top left is the D-Link logo with the tagline "Building Networks for People". To the right, it says "DSA-3200 Airspot Wireless G Public/Private Gateway". The main content area is titled "User Login" and contains a form with two input fields: "User Name:" and "Password:". Below the fields are three buttons: "Enter", "Clear", and "Remaining".

Enter in a previously created username/password in the appropriate fields. Click the “Enter” button.

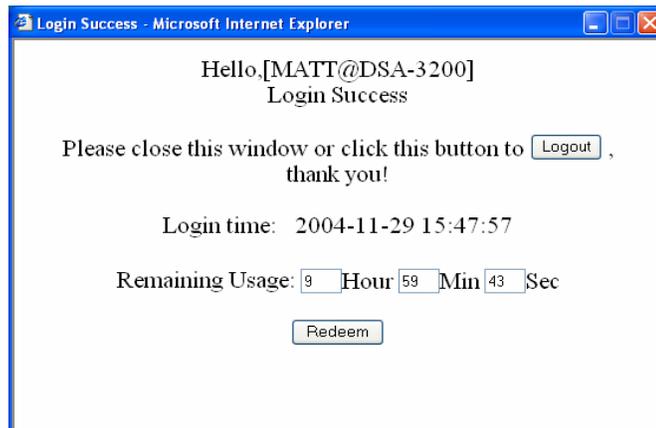
The “Remaining” button will display the remaining account balance for On-Demand users only. If a user that is not an on-demand user clicks this button, the following error window will appear.



If the user logs in successfully, the DSA-3200 is properly configured to service Hot Spot guests. This user may now browse any webpage on the Internet.



The following screen is the login successful page for an on-demand user. In this case, there is an extra function “**Redeem**” that can be used to add credit from the current account to a new account if the remaining usage is considered to be insufficient.



*Attention: The maximum session time/data transfer is 24305 days/2003Mbyte. If the redeem amount exceeds this number, the system will automatically reject the*

After a user has paid the redeem cost at the counter, he/she should get another username and password. Key in this information in the appropriate window, the system will merge the two accounts and put together the available usage.

A rectangular form with a blue border and a light gray background. It contains two text input fields. The first field is labeled "Username:" in blue text. The second field is labeled "Password:" in blue text. Below the password field is a button labeled "Remaining" in blue text.

This window will show the remaining hours or data size for user's online access.

A rectangular display window with a blue border and a light gray background. It shows four input fields for time: "Day", "Hour", "Min", and "Sec", each with a blue label. Below these is another input field for data size, labeled "Mbps" in blue text.

## 5 Console Interface

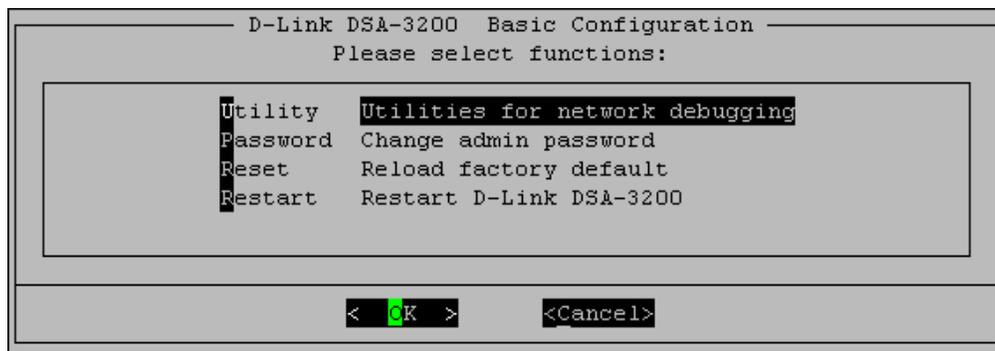
The DB-9 interface of DSA-3200 provides two functions:

1. The DSA-3200 provides a COM interface for the administrator to handle different problems and situations that may occur during operation. To connect to the **COM** interface of the DSA-3200, use the included null modem cable. The terminal simulation program that you use (i.e. Hyperterminal) should be configured as **9600 baud, 8 data bits, Parity None, Stop Bits 1, Flow Control None**. The main console menu is a basic interface using interactive dialog boxes. Please use the arrow keys on the keyboard to browse the menu and press the **“Enter”** key to select specific menus and confirm entered values.
2. The DSA-3200’s COM port can alternatively be used as a printer interface to connect a thermal line ticket printer like the DSA-3100P.

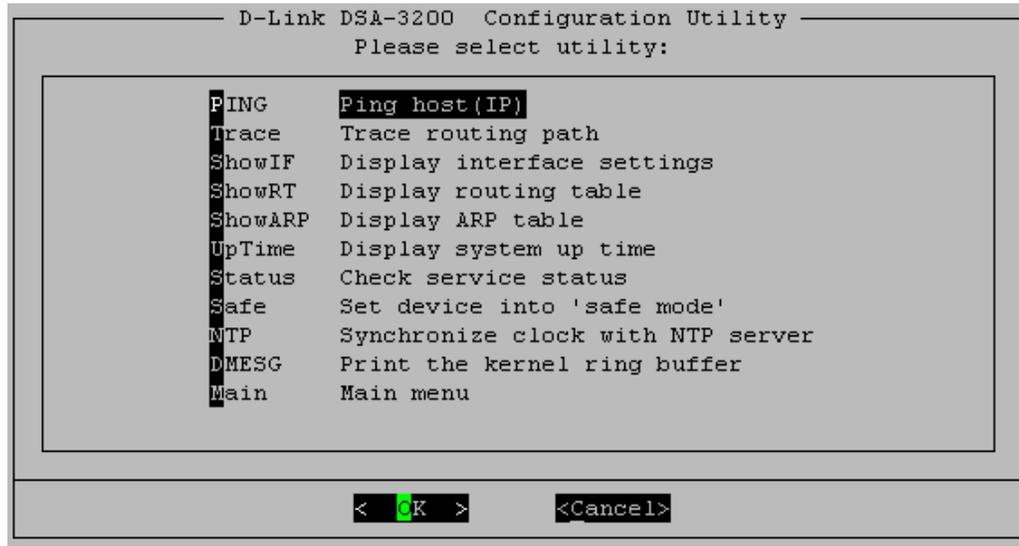
**Warning:** These two functions cannot be used at the same time.

### 5.1 Main Menu of Console interface

Once you properly connect to the serial port of the DSA-3200, the console welcome screen should appear automatically. If the welcome screen fails to appear in the terminal simulation program automatically, please try to press the **“Down”** arrow or **“Enter”** key to display the welcome screen. If you are still unable to see the welcome screen or the main menu of the console, please check the connection of the Null modem cable, verify COM port settings and setup of the terminal simulation program.



## 5.2 Console Utilities for Network Debugging



The DSA-3200 console interface provides several utilities to assist the Administrator in controlling the system conditions and to assist with debugging. The utilities are described as follows:

1. Ping host (IP): By sending ICMP echo request, the on-line condition to a specific target can be tested.
2. Trace routing path: Trace and inquire the routing path to a specific target.
3. Display interface settings: Displays information of each network interface including the MAC address, IP address, and Netmask.
4. Display the routing table: The internal routing table of the DSA-3200 is displayed to assist the confirmation of successful setup of Static Routes on the DSA-3200.
5. Display ARP table: The internal ARP table of the DSA-3200 is displayed.
6. Display system up time: The system live time (time since last system start) of the DSA-3200 is displayed.

7. Check service status: The current execution status of each service on the DSA-3200 is checked.
  
8. Set device into "**safe mode**": If administrator is unable to use Web Management Interface on the browser when the DSA-3200 unexpectedly fails. Administrator can choose this utility and set DSA-3200 into safe mode to be able to manage this device with a web browser again using the WAN port.
  
9. Synchronize clock with NTP server: Immediately check and correct the clock through the NTP protocol by querying an NTP server. Since the DSA-3200 does not support manual configuration for its internal clock, the internal clock must be reset and maintained using NTP.
  
10. Print the kernel ring buffer. Display detailed information to be given to technical support during any unexpected/unexplained occurrence. Capture the output in a file or screen shot for ease of delivery to Technical Support.
  
11. Main menu. Return to main menu.

## **5.3 Change admin password of Console**

In addition to supporting the console management interface through the COM interface using a null modem cable, the DSA-3200 also supports remote access via SSH. When using a null modem cable to connect to the DSA-3200 console, one does not need to enter the administrator's password to enter the console management interface. In the case where SSH is used to connect the DSA-3200, the default username is "**admin**" and the default password is also "**admin**". These credentials are the same as those for the Web management interface.

When connected through the COM port locally, one is able to change the DSA-3200 administrator's password without having to remember the original password. This function is also available through the Web interface and the remote SSH interface.

**Caution:** *Although it does not require a password for connection via the serial port, the same management interface can be accessed via SSH. For heightened security, we recommend an immediate change of the DSA-3200 Admin password after login to the system for the first time.*

## **5.4 Reload factory default of Console interface**

This function will reset the system configuration to factory defaults.

## **5.5 Restart DSA-3200**

This function will reboot the DSA-3200. Please allow 1.5 to 2 minutes for a complete restart.

## **6 Appendix - Windows TCP/IP Setup**

If you have not changed the factory default settings of the DSA-3200 or Windows 2000/XP TCP/IP Configuration, it is not necessary to make any modification here. With the factory default settings, the DSA-3200 will automatically assign an appropriate IP address (and related information) to each PC after the PC has been booted.

### **6.1 Setting up a PC to connect to the DSA-3200**

After the DSA-3200 is installed, the following must be set up for the PC within the Public LAN and Private LAN sections:

- TCP/IP Network Setup
- Internet Connection Setup

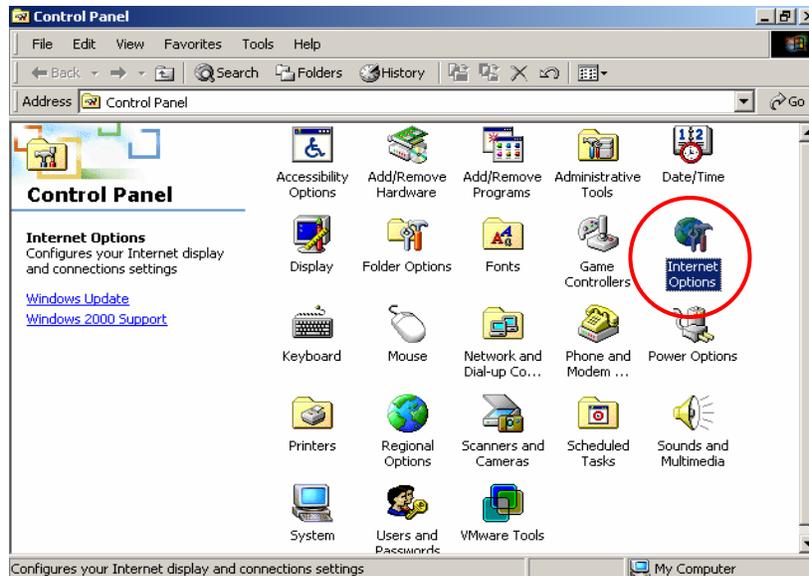
#### **6.1.1 TCP/IP Network Setup**

- If the operating system of your PC is Windows 2000/XP, then you just need to keep the default setting (without any change) to directly start/restart the system.
- During the process of starting the system, the DSA-3200 with DHCP function will automatically assign an appropriate IP address (and related information) for each PC.
- For the Windows based systems other than those for servers, the default setting of the TCP/IP will be a DHCP client, and the setting is “obtain an IP address automatically”.
- If you want to use the static IP in the Public LAN or Private LAN section or to check the TCP/IP setup, please refer to section 6.2 for more information.

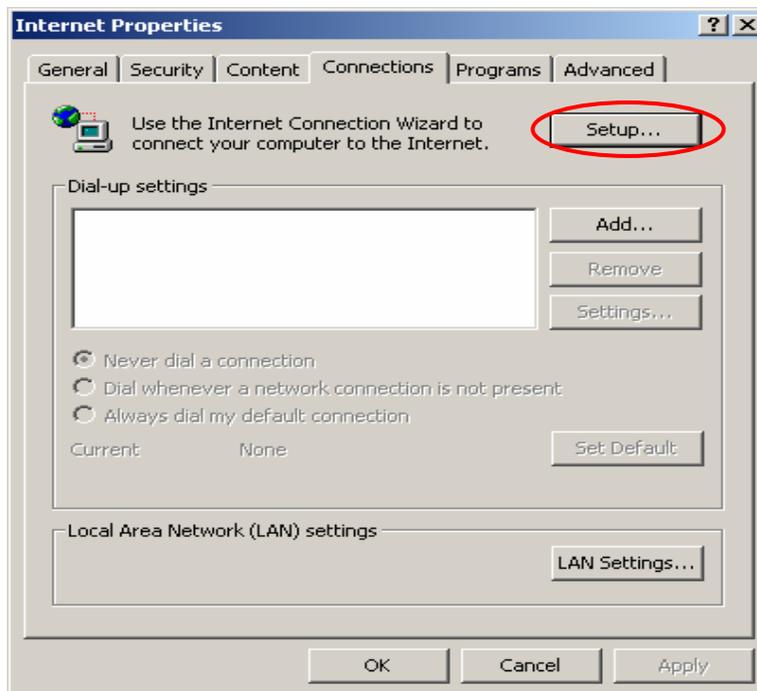
## 6.1.2 Internet Connection Setup

### Windows 2000

1. Choose **Start – Control Panel – Internet Options**.



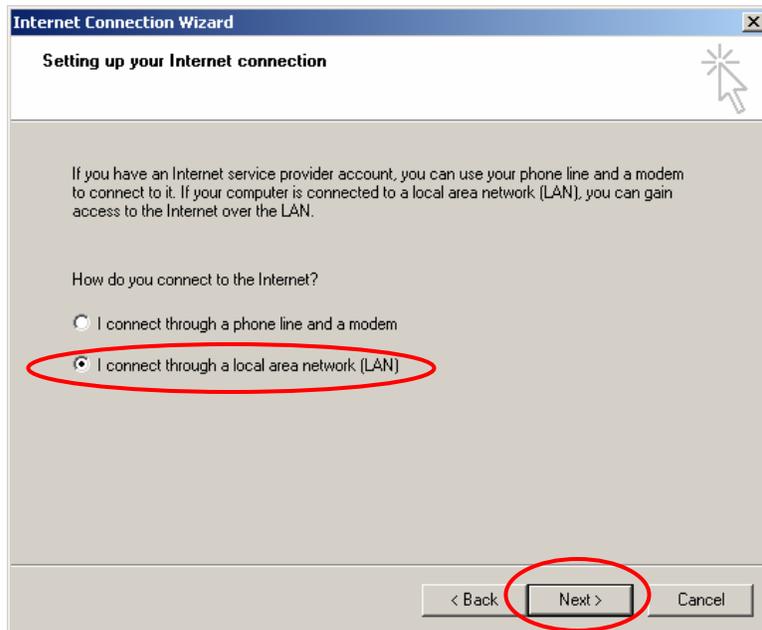
2. Choose the **“Connections”** Icon, and then click **“Setup”**.



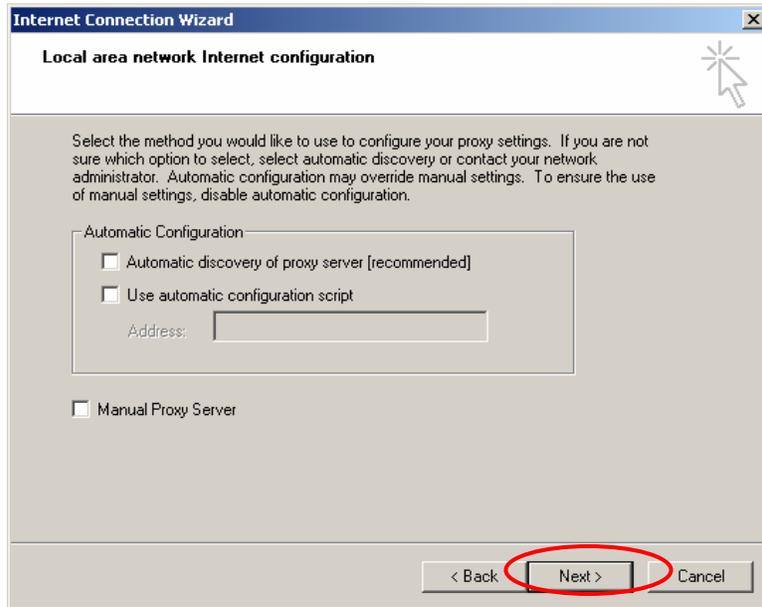
3. Choose “I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)”, and then click “Next”.



4. Choose “I connect through a local area network (LAN)” and click “Next”.



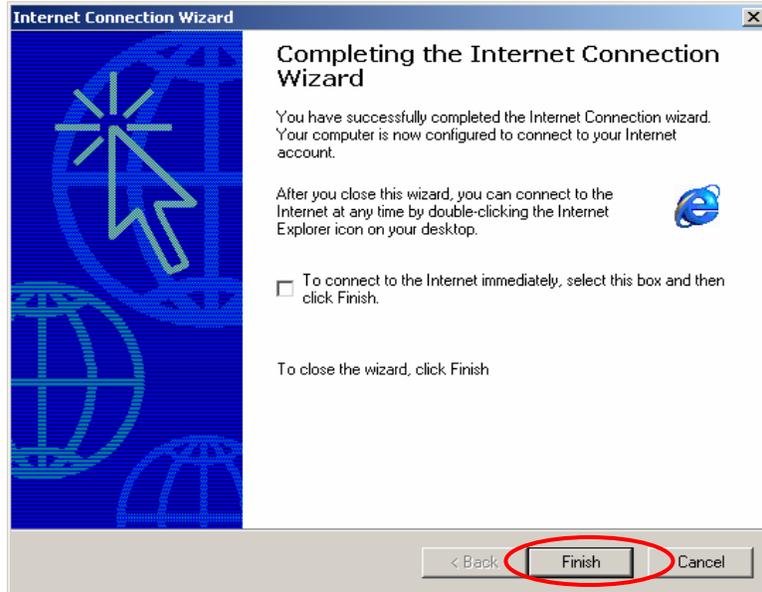
5. **Do not choose** any option in the following LAN window for Internet configuration, and just click **“Next”**.



6. When the system asks **“Do you want to set up an Internet mail account now?”**, choose **“No”**, and click **“Next”**.

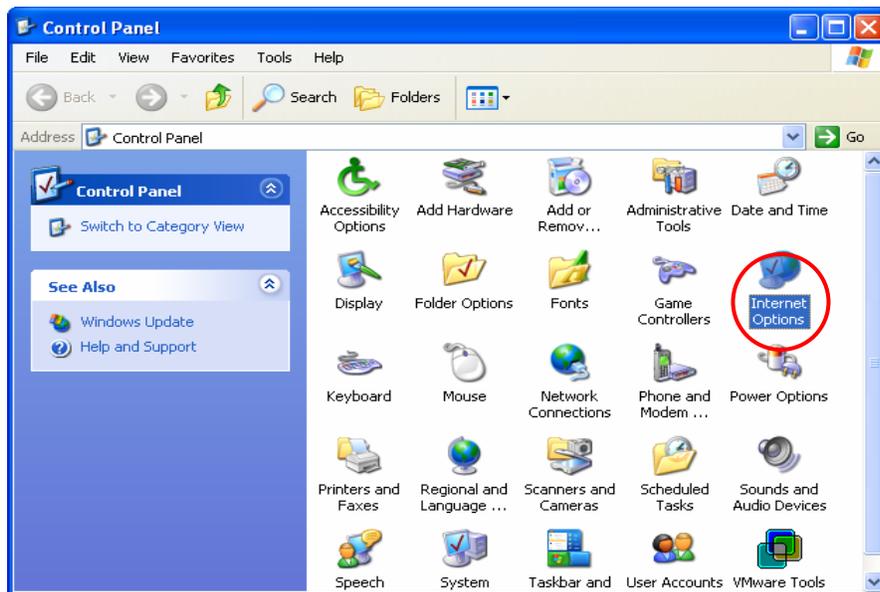


7. Click **“Finish”** to exit the Internet Connection Wizard. Now, you have completed the setup.

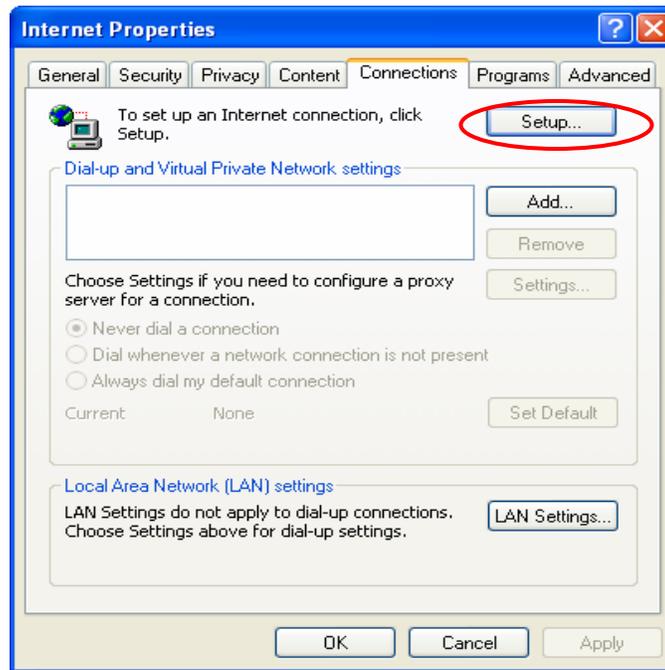


## **Windows XP**

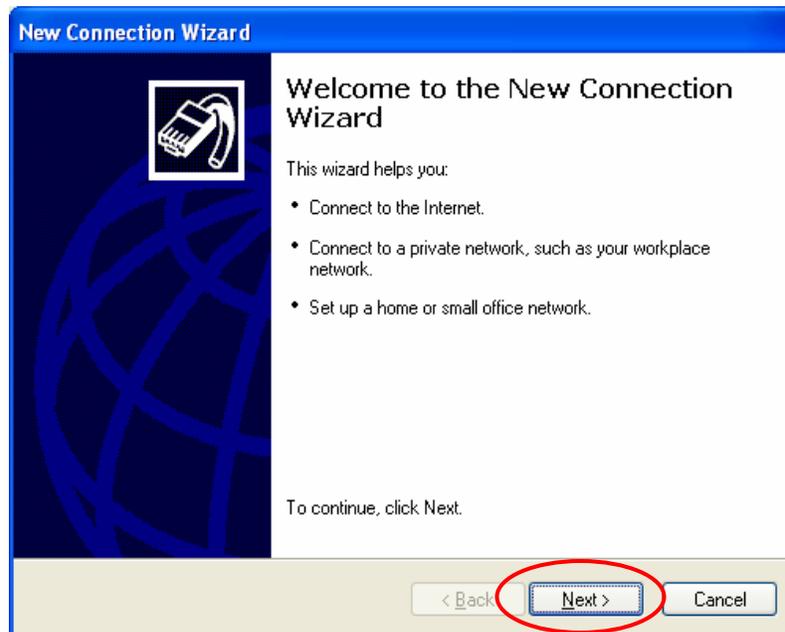
1. Choose **Start – Control Panel – Internet Option**.



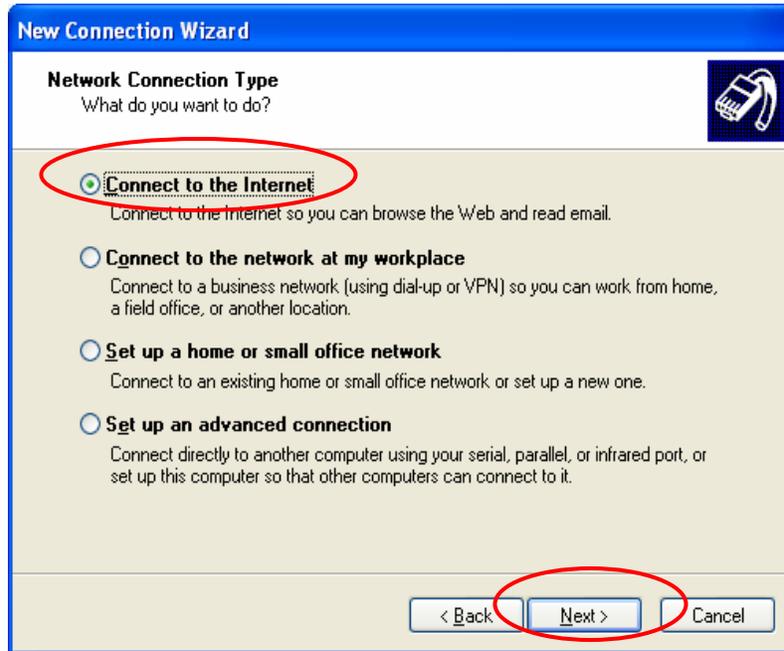
2. Choose the “**Connections**” icon, and then click “**Setup**”.



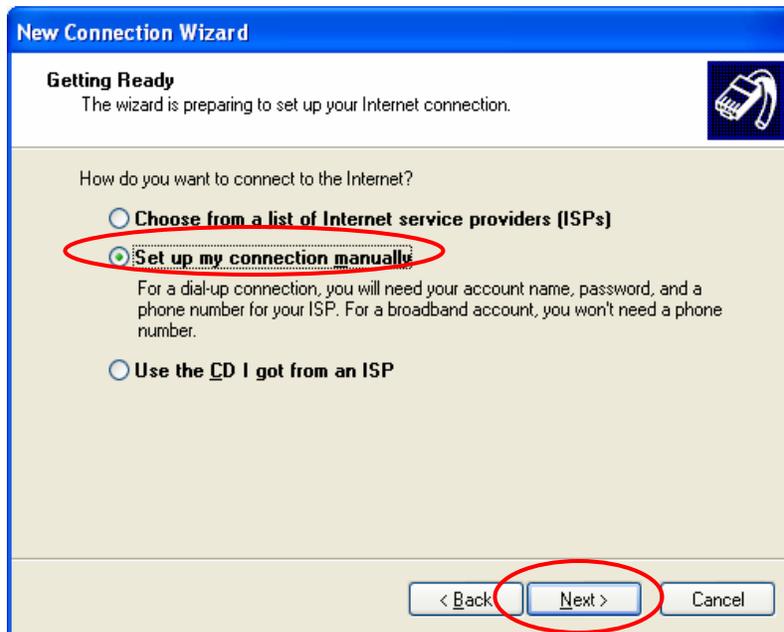
3. Press “**Next**” when the new connection wizard appears on the screen.



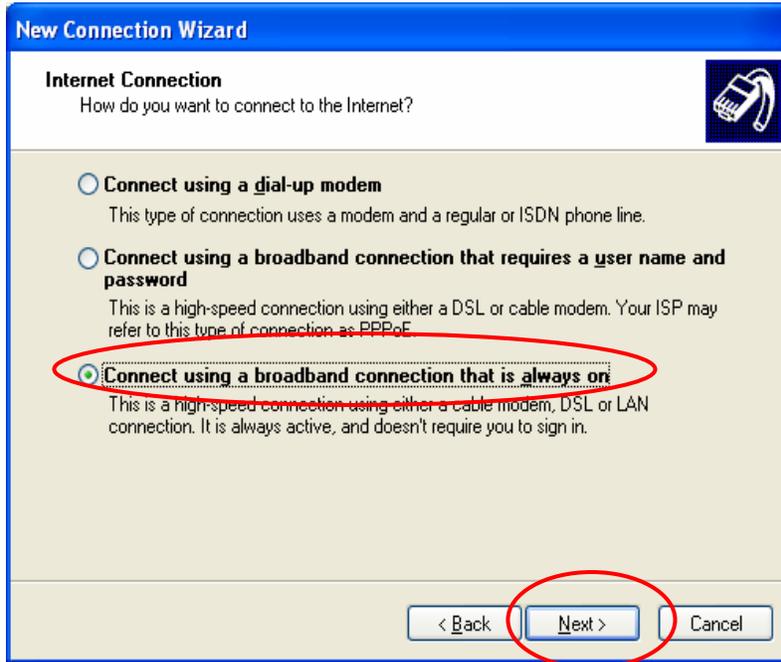
4. Choose “**Connect to the Internet**” and then click “**Next**”.



5. Choose “**Set up my connection manually**”, and then click “**Next**”.



6. Choose “**Connect using a broadband connection that is always on**”, and then click “**Next**”.



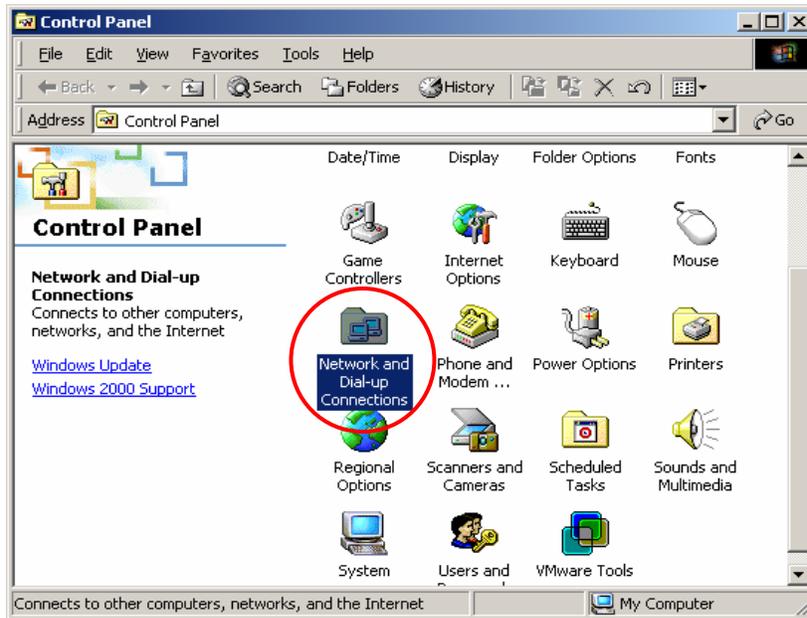
7. Click “**Finish**” to exit the Connection Wizard. Now, you have completed the setup.



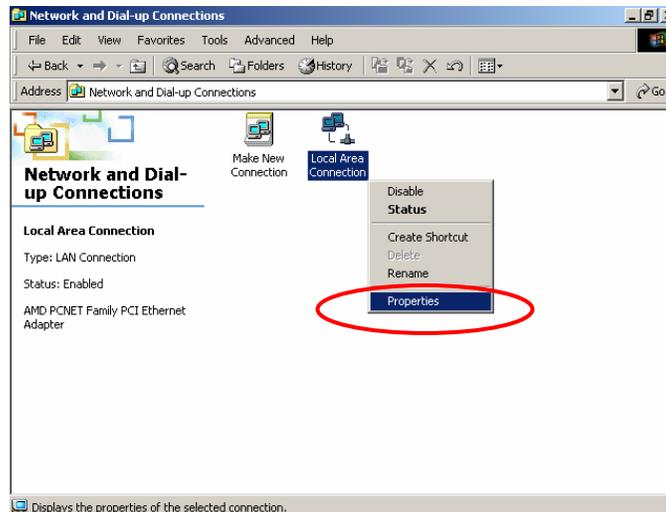
If the version of Windows operating system is not for servers, the default TCP/IP settings will treat the PC as the DHCP client. You can check the TCP/IP setup according to the following procedure:

## 6.2 Configure TCP/IP in Windows 2000

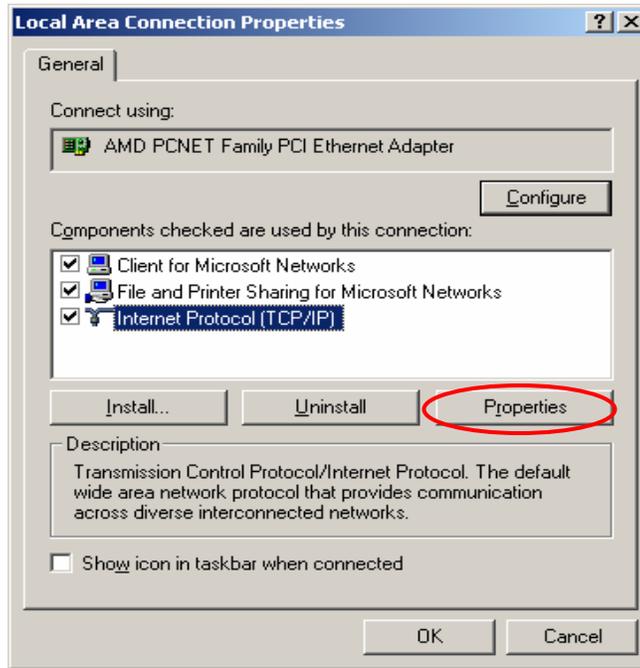
1. Select **Start - Console – Network and Dial-up Connections**.



2. Click the right button of the mouse on **“Local Area Connection”** icon to select **“Properties”**.

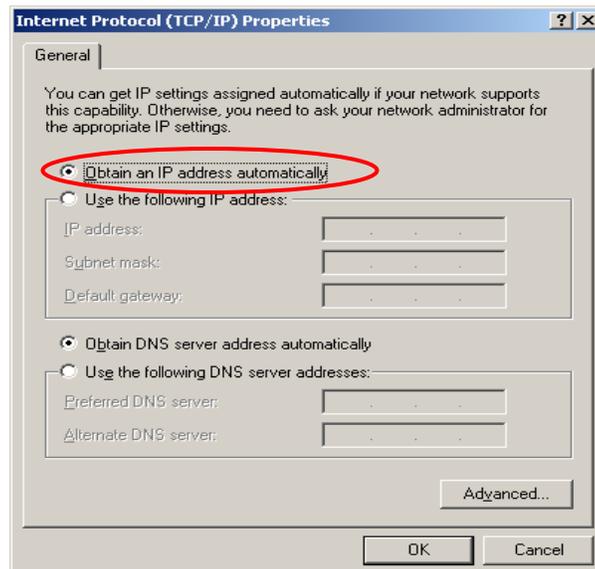


3. Select **Internet Protocol (TCP/IP)**, and then click **“Properties”**.



### Using DHCP

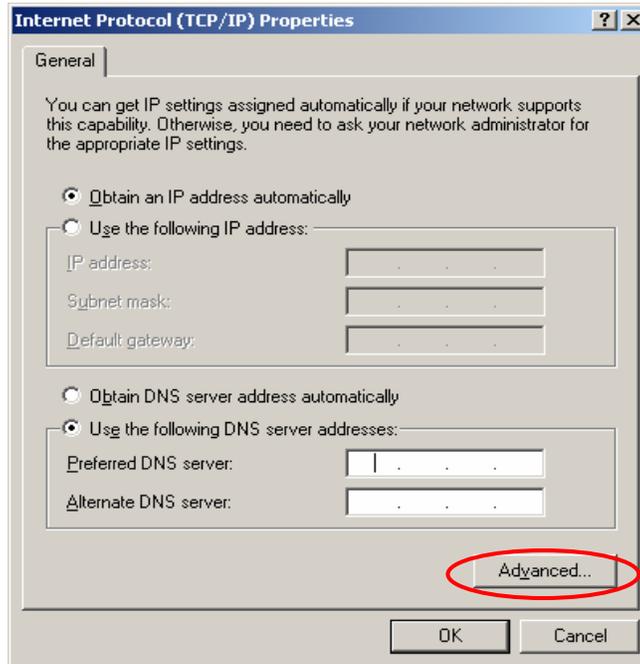
If you want to use DHCP, please select **“Obtain an IP Address Automatically”**, which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the DSA-3200.



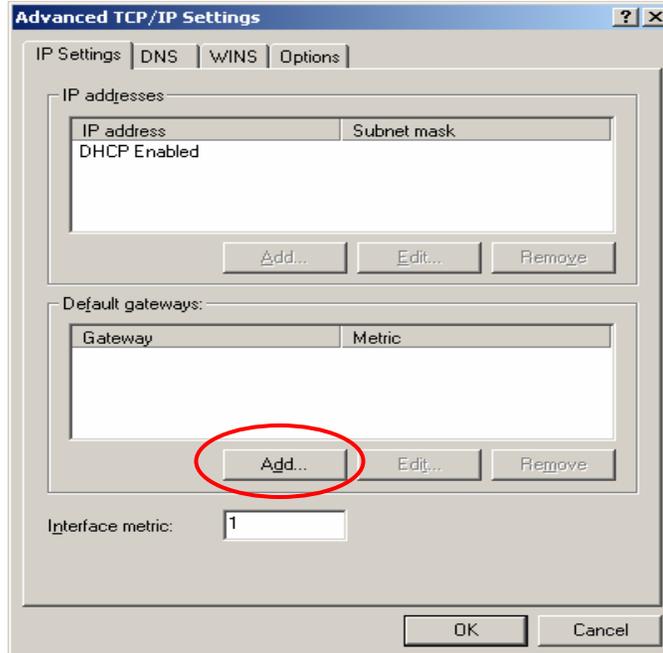
### Using Static IP Address

If you have completed the setup for your PC, please inform the network administrator before modifying the following setup.

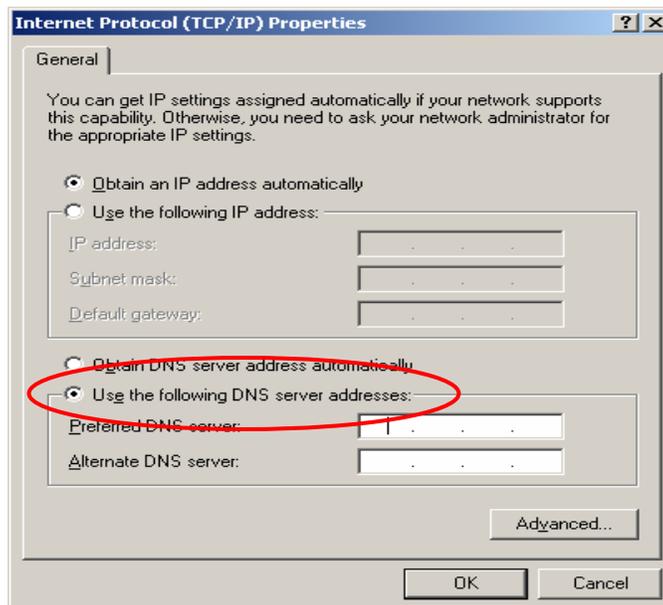
1. Click “**Advanced**” in the window of **Internet Protocol (TCP/IP)**.



2. Click the “**IP Settings**” icon, and then “**Add**” in the “**Default Gateways**” column to enter the IP address of the DSA-3200. After this procedure is completed, click “**Add**”. (You can ask the network administrator to give you the IP address specified for the DSA-3200.)

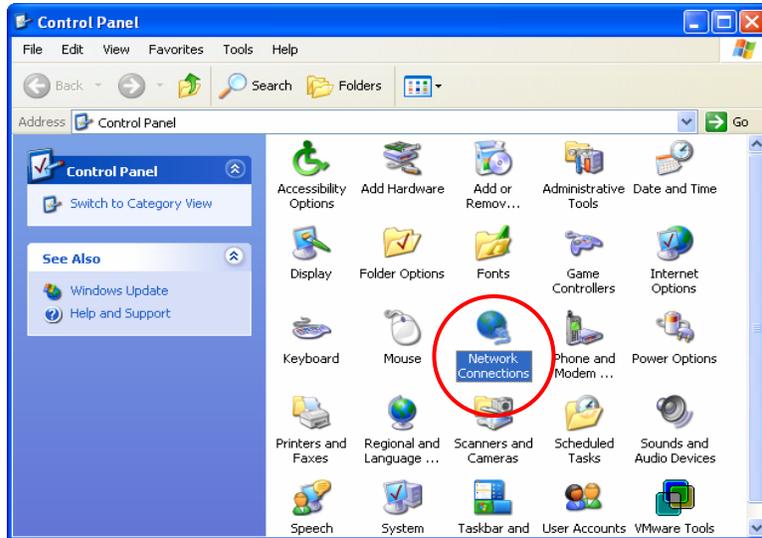


3. If the DNS Server column is blank, please click **“Using the following DNS Server Address”** in the window of Internet Protocol (TCP/IP), and then enter the DNS address or the DNS address provided by ISP. After this procedure is completed, click **“OK”**.

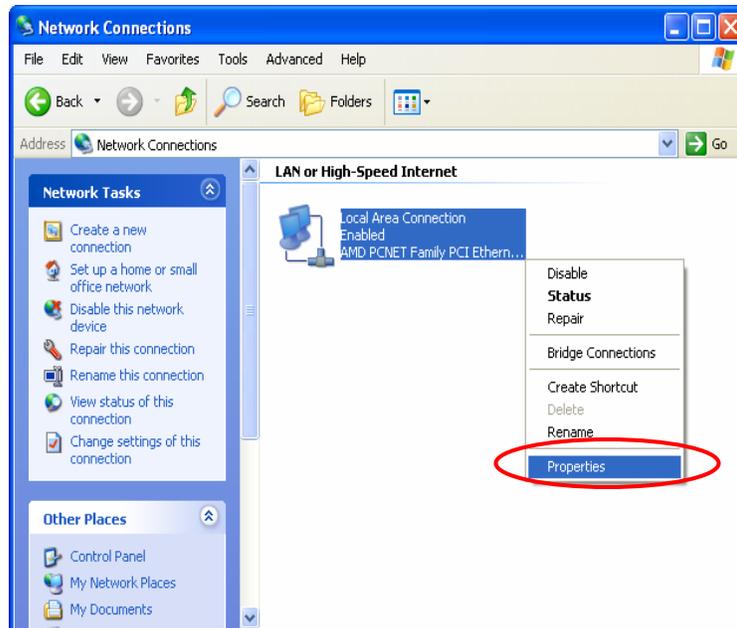


## 6.3 Configure TCP/IP in Windows XP

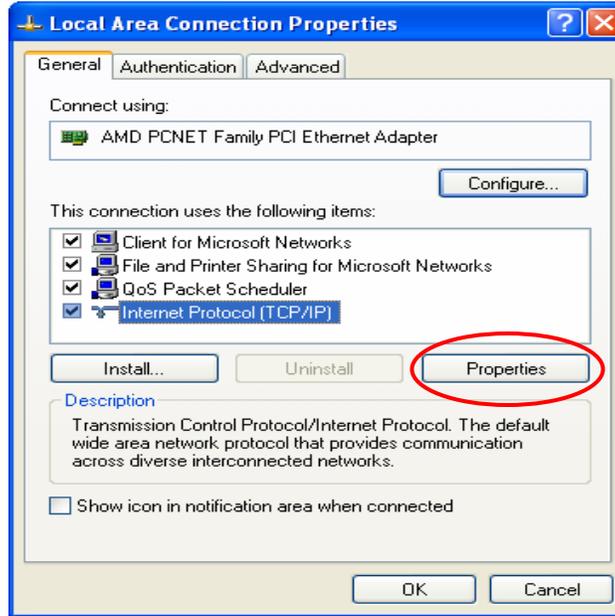
1. Select **Start - Console – Network Connection**.



2. Click the right button of the mouse on the **“Local Area Connection”** icon to select **“Properties”**.

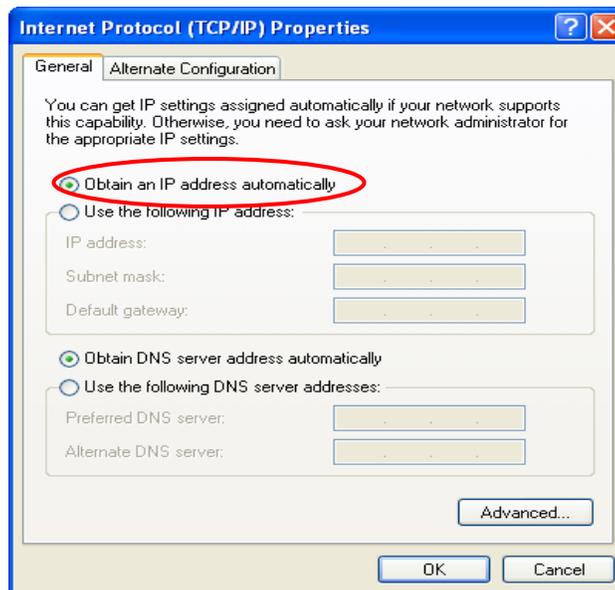


3. Click the **“General”** icon, and then select **“Internet Protocol (TCP/IP)”**. Click **“Properties”**.



### Using DHCP

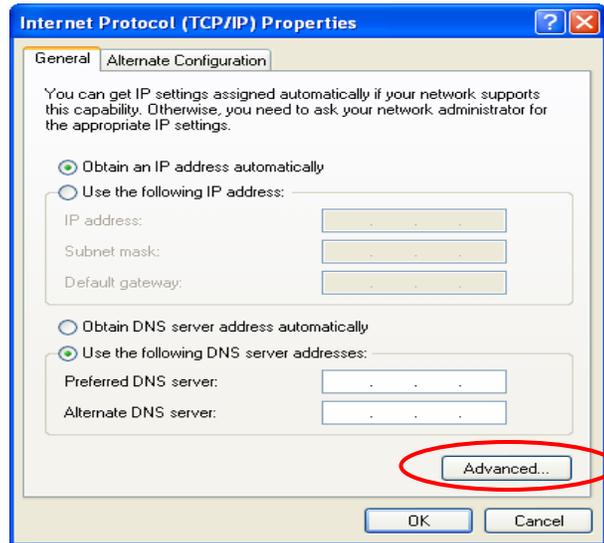
If you want to use DHCP, please select **“Obtain an IP Address Automatically”**, which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the DSA-3200.



## Using Static IP Address

If the setup for your PC is completed, please notice the network administration staff before changing the following settings.

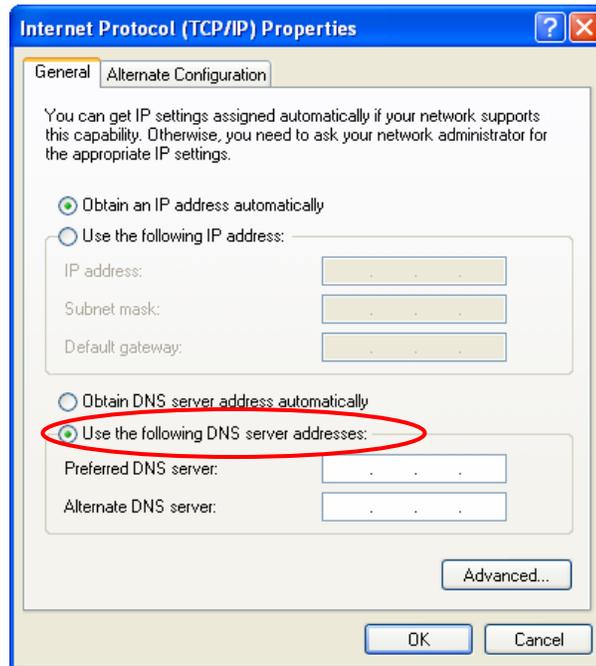
1. Click “Advanced” in the Internet Protocol (TCP/IP) window.



2. Click the “IP Settings” tab, and then click “Add.” Enter the IP address of the DSA-3200 in the “Default Gateways” column. After this procedure is completed, click “OK”. (You can ask the network administrator to give you the IP address specified for the DSA-3200.)



3. If the DNS Server field is blank, please click **“Using the following DNS Server Addresses”** in the Internet Protocol (TCP/IP) Window, and key in the DNS address or DNS address provided by ISP. After this procedure is completed, click **”OK”**



## 7 Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from: D-Link or its authorized reseller or distributor and Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

**Limited Warranty:** D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

1-Year Limited Warranty for the Product(s) is defined as follows:

Hardware (excluding power supplies and fans) One (1) Year

Power Supplies and Fans One (1) Year

Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

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

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

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

The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

The original product owner must obtain a Return Material Authorization (“RMA”) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

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

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

***What Is Not Covered:*** This limited warranty provided by D-Link does not cover: Products, if in D-Link’s judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the

product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

***Disclaimer of Other Warranties:*** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

***Limitation of Liability:*** TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK’S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE

OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

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

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

***Copyright Statement:*** *No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright® 2005 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.*

**FCC Statement:**

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

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

*Installation and use of this Wireless AP/ Router must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.*

*The device contains a low power transmitter, which will send out Radio Frequency (RF) signal when transmitting.*

**For detailed warranty information for outside the United States, please contact the corresponding local D-Link office.**

**CE Statement:**

*European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835 GHz; In France, the equipment must be restricted to the 2.4465-2.4835 GHz frequency range and must be restricted to indoor use.*

For the following equipment: Wireless AP/ Router



Is here with confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC), Low-voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC), the procedures given in European Council Directive 99/5/EC and 89/3360EEC.

The equipment was passed. The test was performed according to the following European standards:

- EN EN 300 328-2 V1.2.1 ( **2001-08**)
- EN 301 489-17 V.1.2.1 (**2002-04**)
- EN 50371: 2002
- EN 60950: 2000

## 8 Technical Support

### Technical Support

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

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

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

#### Tech Support for customers within the United States:

**D-Link Technical Support over the Telephone:**

(877) 453-5465

Monday through Friday 6:00am to 6:00pm PST

**D-Link Technical Support over the Internet:**

<http://support.dlink.com>

e-mail: [support@dlink.com](mailto:support@dlink.com)

#### Tech Support for customers within the Canada:

**D-Link Technical Support over the Telephone:**

(800) 361-5265

Monday through Friday 7:30am to 12:00am EST

**D-Link Technical Support over the Internet:**

<http://support.dlink.ca>

e-mail: [support@dlink.ca](mailto:support@dlink.ca)

## 9 Registration



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

