

# **D-Link Airspot DSA-3100 Public/Private Gateway**

## Manual

June 2004  
Rev. B

**D-Link<sup>®</sup>**

**Building Networks for People**

# Contents

Package Contents .....	3
Introduction .....	4
Front Panel .....	5
Rear Panel .....	6
Features .....	7
Sample Scenarios .....	8
Installation .....	10
Setting Up the DSA-3100 .....	11
Configure PCs on your LAN .....	12
TCP/IP Network Setting .....	12
Internet Access Configuration .....	13
Using the Configuration Utility .....	15
Networking Basics .....	56
Technical Specifications .....	71
Technical Support .....	73
Warranty and Registration .....	74

# Package Contents



## Contents of Package:

- 1** D-Link DSA-3100 Airspot Gateway
- 2** CD-ROM (containing Manual and Warranty)
- 3** Quick Installation Guide
- 4** Two (2) CAT5 UTP/Straight-through (Ethernet) cables
- 5** One (1) CAT5 UTP/Cross-over cable
- 6** One (1) Console cable
- 7** 5V DC, 3A Power Adapter

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

## System Requirements for Configuration:

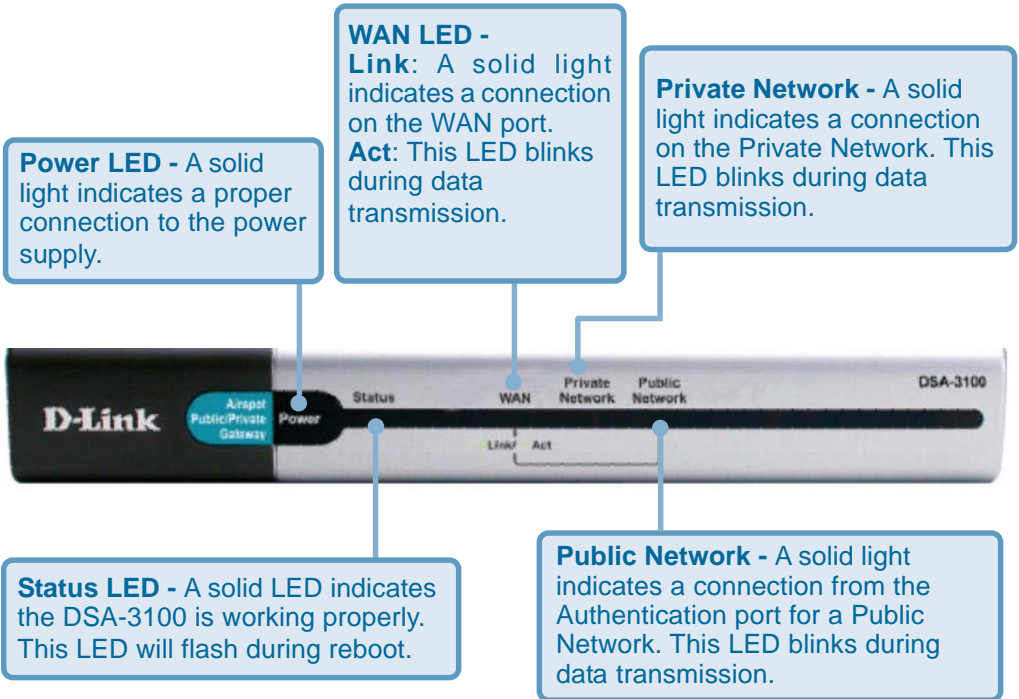
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 6.0 and above

# Introduction

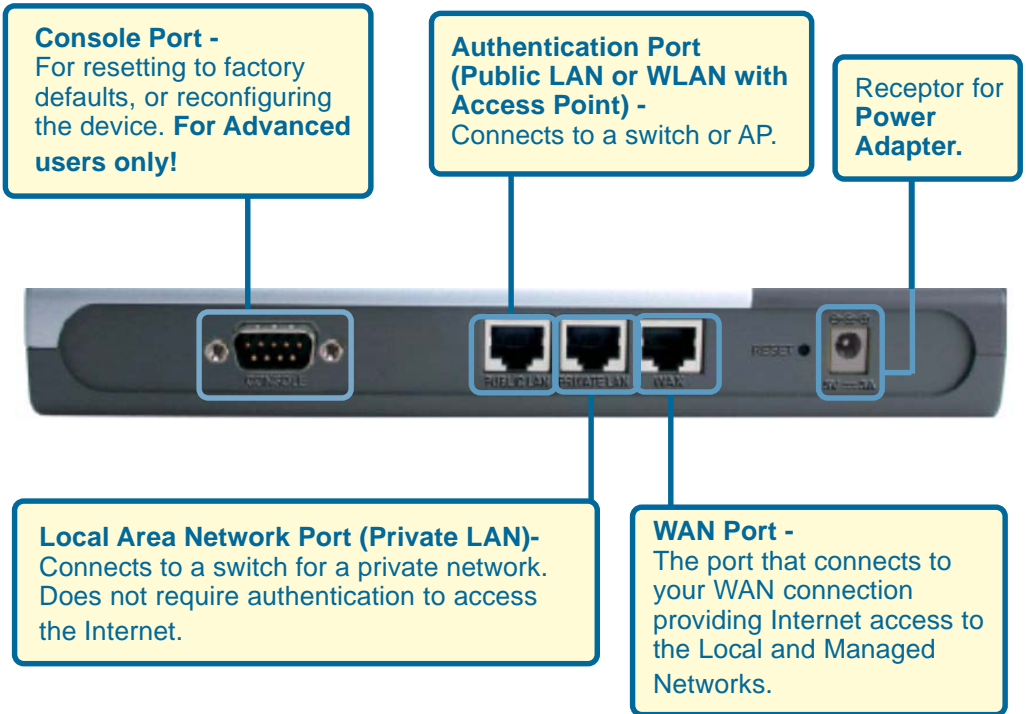
The D-Link DSA-3100 Airspot Gateway is a simple-to-use network access control system supporting Ethernet, Fast Ethernet or an IEEE 802.11 wireless LAN (WLAN) separately and simultaneously.

The DSA-3100 can be configured with a standard HTML browser (i.e., Internet Explorer, Netscape Navigator) operating on Windows 98SE/Me/2000/XP, Macintosh OS 9, Mac OS X (v10.1.5 or later), Linux, or Pocket PC 2000/2002. The DSA-3100 allows the operator to offer wired or wireless networking services and access to the Internet when used with a switch or wireless access point respectively. The device features many management settings allowing for private and public access to the Internet and the necessary privilege mechanisms to permit this usage.

# Front Panel



# Rear Panel



# Features

- Creates two separate and discreet networks allowing the owner/administrator to create a wired or wireless hotspot and provide Internet access to visitors, guests, or customers.
- Manages up to 250 user accounts with an internal database.
- Supports at least 50 users accessing the Internet at any given time.
- Allows ID/Password-based authentication and authorization (can also be combined with MAC address locking for even stricter access control).
- Supports either POP3, RADIUS, or LDAP external authentication servers.
- Provides on-line status monitoring and historical traffic data.
- SSL-protected access to the administration interface and user authentication interface.
- Customizable user log-in and log-out Web interface.
- Customizable user log-out timer.
- Customizable target URL for users who successfully authenticate.
- Console mode administration interface via serial console port.
- Supports display of text messages on the log-in page. An administrator could use the administration interface to input messages (promotions, alerts, additional usage time/services with corresponding fees).
- Supports NAT for managed clients.
- Supports static IP, DHCP client and PPPoE client on the WAN interface.
- Built-in DHCP server to manage clients.
- Built-in, high-speed policy routing engine.
- Customizable preemptory traffic redirection (IP and Port-Redirect).
- Built-in NTP client.

# Sample Scenarios

1

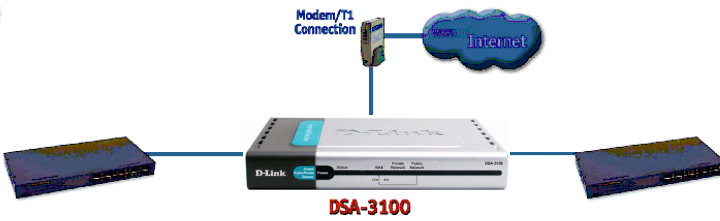


PRIVATE LAN / BACK OFFICE



PUBLIC WLAN / HOTSPOT

2



PRIVATE LAN / BACK OFFICE



PUBLIC LAN / HOTSPOT



# Sample Scenarios (continued)

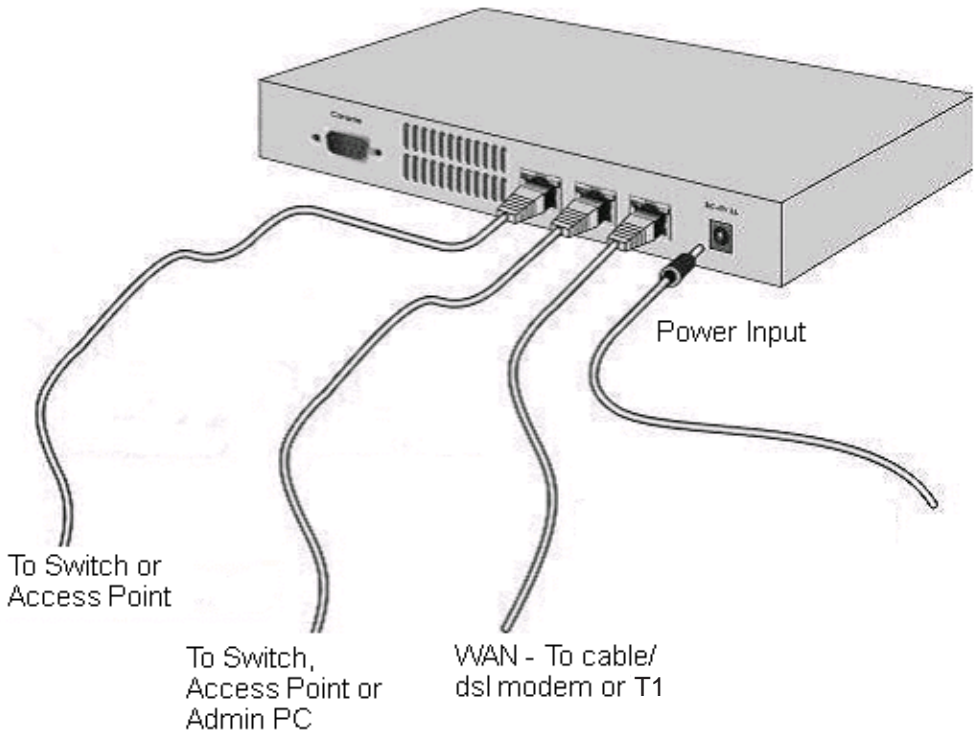
3



# Installation

## Requirements

- **Standard 10/100Base-T network (UTP/Cat5 Ethernet) cable with RJ45 connectors.**
- **TCP/IP network protocol must be installed on all networked computers and related devices.**



# Setting up the DSA-3100

- **Make sure the DSA-3100 unit is not connected to the power adapter and is powered OFF.**
- **WAN port connection**  
Use 10/100BaseT connections to connect the unmanaged network. The unmanaged network's interface may be the ADSL router's LAN port, cable modem's LAN port or Intranet switch port.
- **Private LAN port connection**  
Use to connect to a local network. All ports are auto-mdix, which means that you can use a straight-through or a crossover cable for connections.
- **Public LAN port connection**  
Use to connect to a switch or an access point for Hotspot access. All ports are auto-mdix, which means that you can use a straight-through or a crossover cable for connections.
- **Power ON**  
Connect the supplied power adapter to the DSA-3100 and insert the plug on the other end into an electric outlet.
- **Check the LEDs**  
The power LED and WAN LED should be ON, if the corresponding WAN port is connected to an active cable/DSL modem or T1 line.
- The corresponding local network or authentication indicator should be ON if a network device is connected to the private network port or the public network port.

# Configure PCs on your LAN

After installing the DSA-3100, each computer's **TCP/IP network settings** and **Internet** access configuration may need to be re-configured:

## TCP/IP network settings

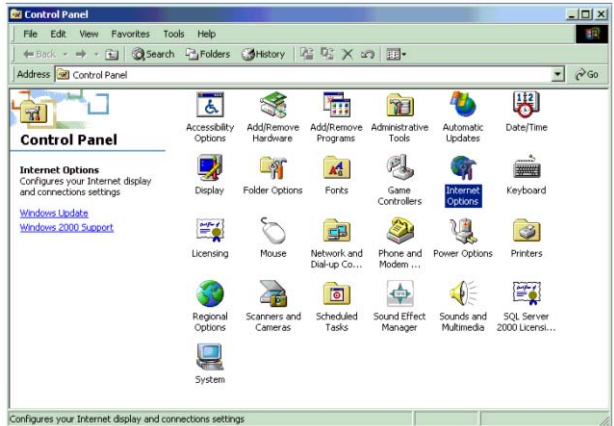
- If your PC uses the default Windows XP/2000/Me/98SE setting, no changes need to be made. Just restart your PC.
- If you are running Mac OS 9 or OS X, set your network settings to DHCP and select **Apply**.
- DSA-3100 will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each computer when the computer reboots or when the network settings refresh.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. In Windows, the setting for this is *Obtain an IP address automatically*.
- If you are using a fixed IP address on your LAN, or if you want to check your TCP/IP setting, refer to the **Networking Basics** section in this manual.

# Internet Access Configuration

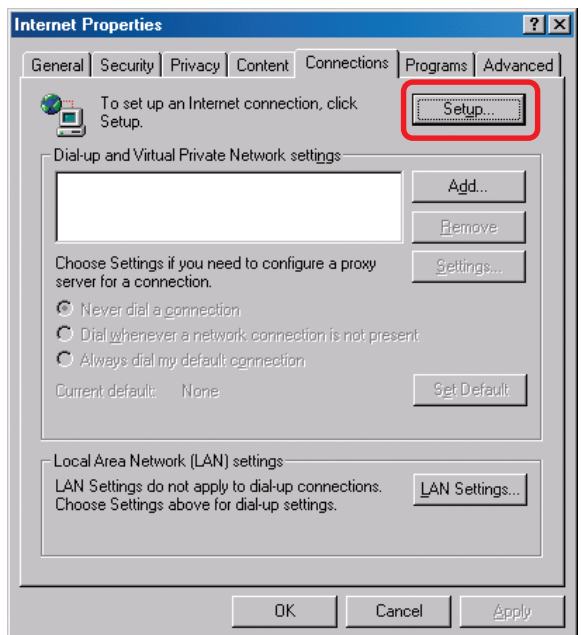
To configure your PCs to use the DSA-3100 for Internet access, follow this procedure.

## For Windows 98SE/2000

- Please select **Start Menu - Control Panel - Internet Options**.

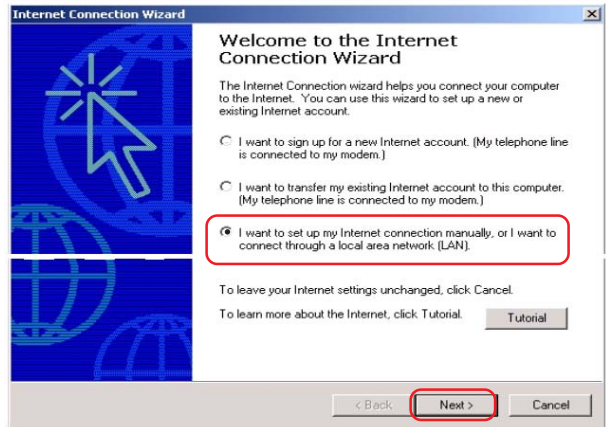


- Select the Connection tab, and click the **Setup** button.



# Internet Access Configuration (continued)

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



- Select “**I connect through a local area network (LAN)**” and click **Next**.
- Ensure all of the boxes on the local area network Internet configuration screen are **unchecked**.
- Check **No**, when promoted “**Do you want to set up an Internet mail account now?**”
- Click **Finish** to close the Internet Connection Wizard. Setup is now completed.

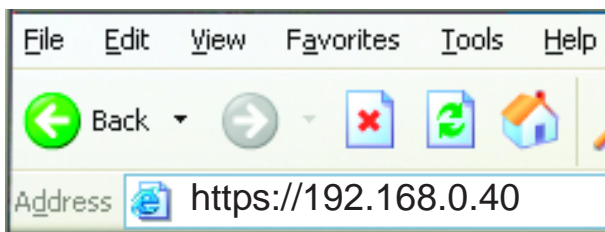
## For Windows XP

- Please select **Star Menu - Control Panel - Network and Internet Connection**.
- Select the Connection tab, and click the **Setup** button.
- Click **Next** on the **New Connection Wizard** screen.
- Select **Connect to the Internet** and click **Next**.
- Select **Set up my connection manually** and click **Next**.
- Check **Connect using a broadband connection this always on** and click **Next**.
- Click **Finish** to close the New Connection Wizard. Setup is now completed.

# Using the Configuration Utility

To configure the DSA-3100, use a computer which is connected to the local network port of the DSA-3100 with an Ethernet cable.

- First, disable the **Access the Internet using a proxy server** function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.
- Start your Microsoft Internet Explorer Web browser program.
- Type **https://192.168.0.40**, which is the default IP address of the DSA-3100, in the address field and press Enter. Make sure that the IP addresses of the DSA-3100 and your computer are in the same subnet.



## Login Screen

### Log-in Screen

You can log in as **admin** or as **manager**.

**admin** - the administrator of the DSA-3100.

**User Name:** admin

**Password:** admin

**manager** - access to the manager user account only.

**User Name:** manager

**Password:** manager

After you log in, click **Enter**.



# Using the Configuration Utility (continued)

On the bottom of each configuration screen you will find the buttons shown below.

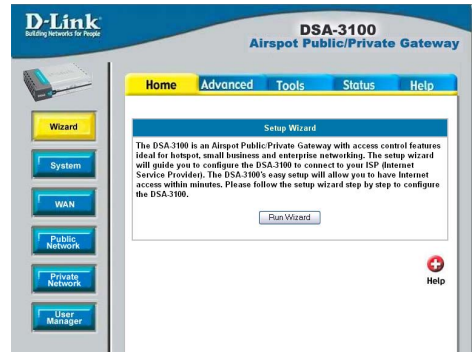
Click **Apply** in each screen of the **Configuration Utility** in which you have made changes.



**Restart the DSA-3100 after completing any changes to its configuration.**

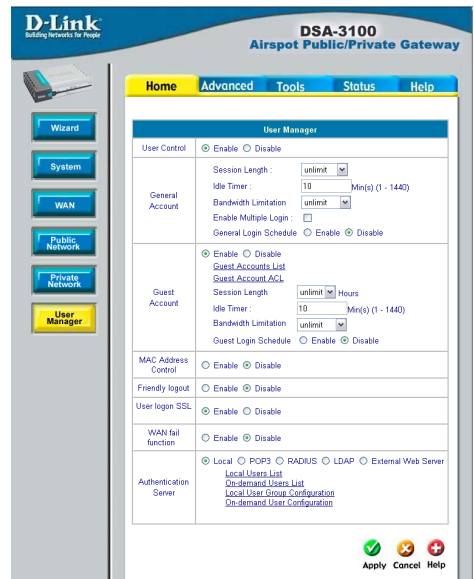
## Home > Wizard

The **Home>Wizard** screen will appear if you logged in as an **admin**. For more information on the **Setup Wizard**, please see the *Quick Installation Guide*, included with your purchase. You can access the configuration features from this window.



## Home > User Manager

The **Home>User Manager** screen will appear if you logged in as a **manager**. Please refer to the *Quick Installation Guide* for more information regarding the Setup Wizard. This screen will be explained in more detail in the following pages.





# Using the Configuration Utility (continued)

Home > System

The screenshot shows the D-Link configuration utility for a DSA-3100 Airspot Gateway. The interface has a blue header with the D-Link logo and the device name. A navigation bar includes 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. On the left, there are buttons for 'Wizard', 'System' (highlighted), 'WAN', 'Public Network', 'Private Network', and 'User Manager'. The main content area is titled 'System Configuration' and contains the following fields:

System Name	DSA-3100
Admin Detail	
Succeed Page	<a href="http://www.dlink.com">http://www.dlink.com</a> (ex. <a href="http://www.dlink.com">http://www.dlink.com</a> )
Device Time	2004/05/19 22:28:55
Time	<input checked="" type="radio"/> Enable NTP NTP Server <a href="http://timekeeper.isi.edu">timekeeper.isi.edu</a> (ex. <a href="mailto:tock.usno.navy.mil">tock.usno.navy.mil</a> ) Time Zone <a href="#">(GMT-08:00)Pacific Time(US&amp;Canada);Tijuana</a>
DNS Server	<input type="radio"/> Set Device Date and Time Primary DNS Server <a href="#">67.130.140.2</a> Secondary DNS Server <a href="#">192.152.81.1</a>

At the bottom right, there are three icons: a green checkmark for 'Apply', a yellow 'X' for 'Cancel', and a red plus sign for 'Help'.

## System Name:

DSA-3100 is the default system name. You may wish to rename it to indicate your company, department, or the service you would like to provide.

## Admin Detail:

You can edit the System Administrator's information here (e.g., name, phone number, and e-mail). If a user encounters a problem connecting to the WAN Port of the DSA-3100, the system administrator's information will be shown on the user login page

## Succeed Page:

Enter a URL for all users to be directed to after successful login. This is typically defined as the home page of the host company, e.g.: <http://www.dlink.com>. No matter to which URL a user originally attempts to connect, he/she will be directed to the URL defined here first.

## Time:

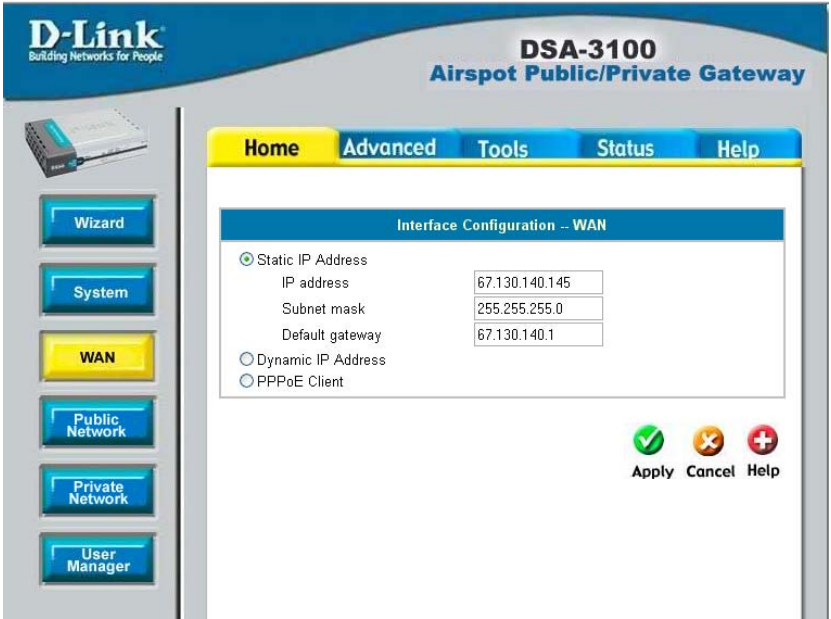
You may use **NTP** (Network Time Protocol) or you may input the time yourself. To use NTP please specify a timeserver's domain name and select the time zone.

## DNS:

Specify DNS servers for the DSA-3100 for the Preferred DNS (preferred IP address) and Alternate DNS (alternate IP address).

# Using the Configuration Utility (continued)

Home > WAN > Static IP Address



## Static IP Address:

**IP address:** Enter the IP address provided to you by your ISP.

**Subnet mask:** Enter the subnet mask provided to you by your ISP. All devices on the network must have the same netmask.

**Default Gateway:** Enter the IP address of the gateway, provided to you by your ISP.

**Dynamic IP Address:** Make this selection if there is a DHCP server in the network. (See the following pages.)

**PPPoE Client:** Make this selection if you connect to the Internet using DSL. (See the following pages.)

# Using the Configuration Utility (continued)

## Home > WAN > Dynamic IP Address

Select this option to obtain an IP address automatically from your ISP.

### Renew

Click **Renew** to renew the IP configuration.

The screenshot shows the D-Link configuration utility interface for the DSA-3100 Airspot Public/Private Gateway. The left sidebar contains navigation buttons: Wizard, System, WAN (highlighted in yellow), Public Network, Private Network, and User Manager. The main content area is titled 'Interface Configuration - WAN' and features three radio button options: 'Static IP Address', 'Dynamic IP Address' (which is selected), and 'PPPoE Client'. A 'Renew' button is positioned to the right of the 'Dynamic IP Address' option. At the bottom right of the main area, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a red plus icon).

## Home > WAN > PPPoE

Most DSL users will select this option.

### User Name & Password:

Enter the user name and password that is assigned by your ISP.

### Dial on demand:

This field is optional.

The screenshot shows the D-Link configuration utility interface for the DSA-3100 Airspot Public/Private Gateway. The left sidebar contains navigation buttons: Wizard, System, WAN (highlighted in yellow), Public Network, Private Network, and User Manager. The main content area is titled 'Interface Configuration - WAN' and features three radio button options: 'Static IP Address', 'Dynamic IP Address', and 'PPPoE Client' (which is selected). Below these options are two text input fields for 'User Name' and 'Password'. A 'Dial on demand' option is present with two radio buttons: 'Enable' and 'Disable' (which is selected). At the bottom right of the main area, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a red plus icon).

# Using the Configuration Utility (continued)

Home > Public Network

The screenshot shows the D-Link configuration utility for the DSA-3100 gateway. The 'Public Network' tab is selected in the left sidebar. The main area displays the 'Interface Configuration - Public LAN' settings. The 'Mode' dropdown is set to 'NAT'. The 'IP Address' field is set to 'NAT\_IP\_PNP' and the 'Subnet Mask' is '255.255.255.0'. Under 'DHCP Configuration', the 'Enable DHCP Server' radio button is selected. The DHCP pool settings are: Start IP Address '192.168.1.101', End IP Address '192.168.1.200', Lease Time '1 Day', Domain Name 'dlink.com', Primary DNS Server '67.130.140.2', and Secondary DNS Server '192.152.81.1'. The 'Disable DHCP Relay' radio button is unselected. At the bottom right, there are 'Apply', 'Cancel', and 'Help' buttons.

The DSA-3100 allows the gateway to be set to one of three Authentication modes.

**Mode:** Select **NAT**; **NAT\_IP\_PNP** or **Router**

**NAT:** This mode protects the identity of the devices within the LAN from those devices outside the network.

**NAT\_IP\_PNP:** All devices, regardless of their IP address, can gain access to the Internet through the DSA-3100 in this mode.

**Router:** In this mode, the DSA-3100 will **not** protect the identity of the connected devices by translating their IP addresses and shielding them from detection outside the LAN.

**IP Address:** Enter the IP address for the Authentication interface (the Public Network).

**Subnet Mask:** Enter the subnet mask for the Authentication interface.

**Disable DHCP Server:** Make this selection if you do not wish to use the built-in DHCP feature in the DSA-3100.

# Using the Configuration Utility (continued)

## Home > Public Network (continued)

### Enable DHCP Server:

Selecting this option activates the device's built-in DHCP server. Configure the DHCP server with the following properties:

**DHCP Pool Start IP Address:** Enter the starting IP address, from which the DHCP server will assign to the DHCP-enabled devices (clients) on the network.

**DHCP Pool End IP Address:** Enter the last IP address in the sequence of addresses from which the DHCP server will assign to clients on the network.

**Lease Time:** Select the length of time during which the DHCP assigned address will be in effect.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the WINS server's IP address, if one is present on the network.

**Primary DNS Server:** Enter the IP address of the preferred DNS server.

**Secondary DNS Server:** Enter the IP address of the alternate DNS server.

### Enable DHCP Relay:

Select this mode to specify another DHCP server's IP address.

# Using the Configuration Utility (continued)

Home > Private Network

The screenshot shows the D-Link configuration utility for the DSA-3100 Airspot Public/Private Gateway. The interface has a blue header with the D-Link logo and the device name. Below the header is a navigation bar with tabs for Home, Advanced, Tools, Status, and Help. On the left side, there is a vertical menu with buttons for Wizard, System, WAN, Public Network, Private Network (highlighted in yellow), and User Manager. The main content area is titled 'Interface Configuration -- Private LAN'. It contains several fields: Mode (set to NAT), IP Address (set to ROUTER), and Subnet Mask (set to 255.255.255.0). Below these is the DHCP Configuration section, which includes radio buttons for 'Disable DHCP Server' and 'Enable DHCP Server' (selected). The 'Enable DHCP Server' section has several input fields: DHCP Pool Start IP Address (192.168.0.101), DHCP Pool End IP Address (192.168.0.200), Lease Time (1 Day), Domain Name (dlink.com), WINS IP Address, Primary DNS server, and Secondary DNS server. At the bottom right of the configuration area, there are three buttons: Apply (with a green checkmark), Cancel (with a red X), and Help (with a red plus sign).

**NAT** and **Router** are the two local network port modes.

**Nat mode:** All outbound IP addresses on the local network port will be translated to the IP address of the WAN port to proceed.

**Router mode:** All outbound IP addresses on the local network port will retain their IP addresses.

For an explanation of each field on this screen, please see the previous screen:  
[Home > Public Network](#)

# Using the Configuration Utility (continued)

## Home > User Manager > General Account

The screenshot shows the configuration utility for a D-Link DSA-3100 Airspot Public/Private Gateway. The interface is in Chinese. The main navigation bar includes Home, Advanced, Tools, Status, and Help. The left sidebar contains buttons for Wizard, System, WAN, Public Network, Private Network, and User Manager (which is highlighted). The main content area is titled 'User Manager' and contains several sections:

- User Control:**  Enable  Disable
- General Account:**
  - Session Length:
  - Idle Timer:  Min(s) (1 - 1440)
  - Bandwidth Limitation:
  - Enable Multiple Login:
  - General Login Schedule:  Enable  Disable
- Guest Account:**
  - Enable  Disable
  - [Guest Accounts List](#)
  - [Guest Account ACL](#)
  - Session Length:  Hours
  - Idle Timer:  Min(s) (1 - 1440)
  - Bandwidth Limitation:
  - Guest Login Schedule:  Enable  Disable
- MAC Address Control:**  Enable  Disable
- Friendly logout:**  Enable  Disable
- User logon SSL:**  Enable  Disable
- WAN fail function:**  Enable  Disable
- Authentication Server:**
  - Local  POP3  RADIUS  LDAP  External Web Server
  - [Local Users List](#)
  - [On-demand Users List](#)
  - [Local User Group Configuration](#)
  - [On-demand User Configuration](#)

At the bottom right, there are three buttons: Apply (with a green checkmark), Cancel (with a red X), and Help (with a red plus sign).

### User Control:

Select Enable or Disable. When disabled, only the MAC Address Control function is available.

### General Account

#### Session Length:

Limit the duration of each session established by the general account from 5 minutes to an unlimited period.

#### Idle Timer:

When enabled, on-line users who become inactive on the network after a specified period of time will be logged out automatically. The period can range from 1~1440. 10 minutes of time is the default value.

#### Bandwidth Limitation:

Limit the outbound traffic bandwidth for each session established by a Guest Account.

#### Enable Multiple Login:

Check this function to allow a single user account to log into the system multiple times.

#### General Login Schedule:

Select Enable or Disable. To define the login time and duration click Enable; the screen on the following page will appear.

# Using the Configuration Utility (continued)

## Home > User Manager > General Account

Define the login time and duration here.

Login Schedule -- General							
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"/>
6	<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"/>
7	<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"/>
8	<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"/>
9	<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"/>
10	<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"/>
11	<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"/>
12	<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"/>
13	<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"/>
14	<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"/>
15	<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"/>
16	<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"/>
17	<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"/>
18	<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"/>
19	<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"/>
20	<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"/>
21	<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"/>
22	<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"/>
23	<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"/>



# Using the Configuration Utility (continued)

## Home > User Manager > Guest Account

Guest Account	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	<a href="#">Guest Accounts List</a>
	<a href="#">Guest Account ACL</a>
	Session Length <input type="text" value="unlimit"/> Hours
	Idle Timer : <input type="text" value="10"/> Min(s) (1 - 1440)
	Bandwidth Limitation <input type="text" value="unlimit"/>
Guest Login Schedule <input type="radio"/> Enable <input checked="" type="radio"/> Disable	

**Guest Account:** Select Enable or Disable.

## Guest Account List

Up to 10 guest accounts can be defined. To activate a particular **Guest Account**, simply enter the corresponding password in the **Password** column and click **Apply**.

**D-Link** Building Networks for People  
**DSA-3100** Airspot Public/Private Gateway

Home Advanced Tools Status Help

Guest Account List		
No.	User Name	Password
1	guest1	<input type="text"/>
2	guest2	<input type="text"/>
3	guest3	<input type="text"/>
4	guest4	<input type="text"/>
5	guest5	<input type="text"/>
6	guest6	<input type="text"/>
7	guest7	<input type="text"/>
8	guest8	<input type="text"/>
9	guest9	<input type="text"/>
10	guest10	<input type="text"/>

Back Apply Cancel Help

## Guest Account ACL

Define network areas where the **Guest Account** function is disallowed access, for instance 10.2.3.0/24.

**D-Link** Building Networks for People  
**DSA-3100** Airspot Public/Private Gateway

Home Advanced Tools Status Help

Guest Account ACL		
No.	Network ID	Subnet Mask
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"/>
11	<input type="text"/>	<input type="text"/>

# Using the Configuration Utility (continued)

## Home > User Manager > MAC Address Control

MAC Address Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
---------------------	---

### MAC Address Control:

When MAC address control is enabled, users connected to the Authentication Port can not login to the DSA-3100 unless they have registered their MAC Address at MAC Address Control. In other words, only 40 users will be allowed to login when this function is enabled. Please refer to the configuration screen as follows.

MAC ACL Control			
No.	MAC Address (XX:XX:XX:XX:XX:XX)	No.	MAC Address (XX:XX:XX:XX:XX:XX)
1	00:07:0E:B3:B0:09	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	
21		22	
23		24	
25		26	
27		28	
29		30	

**Note:** MAC address format is **XX:XX:XX:XX:XX:XX** or **XX-XX-XX-XX-XX-XX**. A newly created user account will be valid instantly. Restarting the DSA-3100 is not necessary.

# Using the Configuration Utility (continued)

## Home > User Manager (continued)

### Friendly logout:

If you enable Friendly logout, a pop-up window asking “Do you want to logout?” will appear after closing the login window. If you disable this function, no pop-up window will appear.

Friendly logout	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
-----------------	---

### User Logon SSL:

Allow administrator to choose between activating https (encryption), or http (non-encryption) for the login page.

### WAN Fail Function:

Enter a URL, if you enable this function. The DSA-3100 detects the WAN port connection by linking the URL defined here. It will pop up the alarm page when the WAN port fails to connect.

### Authentication Server:

Supports multiple user Public LAN methods including Local, POP3 server, RADIUS Server, LDAP Server and External Web Server.

Authentication Server	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Web Server <a href="#">Local Users List</a> <a href="#">On-demand Users List</a> <a href="#">Local User Group Configuration</a> <a href="#">On-demand User Configuration</a>
-----------------------	---

### Local:

User accounts are stored in the embedded database on the DSA-3100.

# Using the Configuration Utility (continued)

## Home > User Manager > Authentication Server > Local

**Local Users List:** A list of all local user accounts stored in the embedded database for user account management. You can add, edit, and delete users. A sample list is shown here.

Local Users List			
User Name	MAC	Group	<input type="button" value="Delete"/>
<a href="#">admin</a>	00:80:c8:10:91:10	123	<input type="checkbox"/>
<a href="#">charlie</a>	00:07:0e:b3:b0:09	345	<input type="checkbox"/>

(Total:2) [First](#) [Prev](#) [Next](#) [Last](#)



### Delete User:

Click the box next to the user name and click **Delete**.

### Add Users:

Click **Add User** to create new accounts. The screen below will appear.

Add Users				
No	User Name	Password	MAC (XX:XX:XX:XX:XX:XX)	Group
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1 <input type="button" value="v"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1 <input type="button" value="v"/>

### Edit Account:

Make changes to the account by clicking on the User Name as indicated above. The screen below will appear.

Local Users List			
User Name	MAC	Group	<input type="button" value="Delete"/>
<a href="#">Lisa</a>		group5	<input type="checkbox"/>
<a href="#">Hans</a>		group2	<input type="checkbox"/>
<a href="#">Roson</a>		group1	<input type="checkbox"/>
<a href="#">Gavin</a>		group3	<input type="checkbox"/>

(Total:4) [First](#) [Prev](#) [Next](#) [Last](#)



Edit the account information here.

Edit Account	
User Name	<input type="text" value="Lisa"/>
Password	<input type="text"/> *Please leave the field blank, if you don't want to change
MAC	<input type="text"/>
Group	group5 <input type="button" value="v"/>


# Using the Configuration Utility (continued)

Home > User Manager > Authentication Server > Local > Local Users List

## Upload User Accounts:

Local Users List			
User Name	MAC	Group	<input type="button" value="Delete"/>
<a href="#">Lisa</a>		group5	<input type="checkbox"/>
<a href="#">Hans</a>		group2	<input type="checkbox"/>
<a href="#">Roson</a>		group1	<input type="checkbox"/>
<a href="#">Gavin</a>		group3	<input type="checkbox"/>

(Total:4) [First](#) [Prev](#) [Next](#) [Last](#)

 **Back**

Besides adding user accounts one by one through the Web interface, you can prepare a text file, which contains user account information, store it on your hard drive and then upload it to the DSA-3100.

Each line of the text file can be in one of the following two formats:

**UserID, Password, MAC**  
**UserID, Password,**

Please note that there must be no space or other characters between the user ID, password and the MAC address. The MAC address could be omitted, but the trailing comma must be retained. A user ID should be between 1 to 32 characters and the password should be between 0 to 20 characters. Special characters are not allowed for user name and password.

Upload User Account	
File Name	<input type="text"/>

After you have created the text file for the user account as described above, click **Upload User Accounts** as shown in the illustration at the top of this page. Click Browse and highlight the text file you have created.

Click **Refresh** for the latest information. Click **Apply** to update your changes.



**Caution:** When adding user accounts by uploading a file, existing accounts with the same ID will be replaced by the new ones.

# Using the Configuration Utility (continued)

Home > User Manager > Authentication Server > Local > On-demand User Configuration

Authentication Server	<input checked="" type="radio"/> Local	<input type="radio"/> POP3	<input type="radio"/> RADIUS	<input type="radio"/> LDAP	<input type="radio"/> External Web Server
	<a href="#">Local Users List</a>				
	<a href="#">On-demand Users List</a>				
	<a href="#">Local User Group Configuration</a>				
	<a href="#">On-demand User Configuration</a>				

**On-demand User:** When you connect the DSA-3100P (the plug and play receipt printer) to the DSA-3100's console port, you can create a database of up to 2000 on-demand users. By default, the on-demand user database is empty. While you press the DSA-3100P's button, the on-demand user will be created in the database, a receipt will then be printed which will contain the on-demand user's information.

```

Welcome!
-----
Username: D-Link1
Password: q6m34m3b
Price: US$2
Usage: 60 minute(s)
-----
ESSID:
dlink
Shared WEP Keys
(HEX 40 bit):
1:
2:
3:
4:
-----
Valid to use until:
2003/09/09 12:46:56
-----
Thank You!
```

*Shown above is an example of a an on-demand receipt.*

# Using the Configuration Utility (continued)

Home > User Manager > Authentication Server > Local > On-demand User Configuration (continued)

On-demand User Configuration	
Store name	D-Link (e.g.: D-Link. Max: 8 char)
Account range	from 0001 to 1000 (e.g.: 0001~2000. Max: 2000)
Receipt header	Welcome! (e.g.: Welcome!)
Receipt footer	Thank You! (e.g.: Thank You!)
Printer baud rate	9600
Account expires after	3 days
Session expires after	60 minutes
Idle timer	10 Min(s) (1 - 1440)
WLAN ESSID	dlink (e.g.: dlink)
WEP key	1: <input type="text"/>
WEP key	2: <input type="text"/>
WEP key	3: <input type="text"/>
WEP key	4: <input type="text"/>
Price	US\$2 (e.g.: US\$2)

Field	Description
<b>Store Name</b>	You can specify the prefix of the user name. The maximum is 8 characters (e.g., D-Link).
<b>Account Range</b>	You can specify the maximum user amount which cannot exceed 2000.
<b>Receipt Header</b>	You can configure the receipt's header in this field.
<b>Receipt Footer</b>	You can configure the receipt's footer in this field.
<b>Printer baud rate</b>	You can specify the baud rate to support a specific printer. The default setting is 9600.
<b>Account expires after __ days</b>	You can specify the days before expiration in this field. After the expiration date the user account will no longer be available. A new session will be required.
<b>Session expire after __ minutes</b>	You can specify how many minutes this account will be available after successful login.
<b>Idle timer</b>	Logout user if the user doesn't access the Internet for a certain period.
<b>WLAN ESSID</b>	You can specify the access point's ESSID in this field.
<b>WEP Key</b>	You can specify the access point's WEP key in the WEP key field.
<b>Price</b>	You can specify the price in this field.

# Using the Configuration Utility (continued)

## Home > User Manager > Management Type > Local > On-demand User Configuration (continued)

### On-demand Users List

Authentication Server

Local  POP3  RADIUS  LDAP  External Web Server

[Local Users List](#)  
[On-demand Users List](#)  
[Local User Group Configuration](#)  
[On-demand User Configuration](#)

Click **On-demand Users List** in the screen above and the screen below will appear showing a list of the on-demand users. You can delete users in this window.

On-demand Users List					
User Name	Password	Expiration Date	Session Length	Status	
					<input type="button" value="Delete"/>
					<input type="button" value="Delete All"/>

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

### Local > Local User Group Configuration



Back

Authentication Server

Local  POP3  RADIUS  LDAP  External Web Server

[Local Users List](#)  
[On-demand Users List](#)  
[Local User Group Configuration](#)  
[On-demand User Configuration](#)

The DSA-3100 provides 5 local user groups; each group can designate a different outbound traffic bandwidth. The Logout Timer will logout a user that has not accessed the Internet for a certain time period. A sample list is shown below.

Local User Group Configuration			
No	Group Name	Logout Timer Min(s) (1 - 1440)	Rate Average
1	<input type="text" value="group1"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/>
2	<input type="text" value="group2"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/>
3	<input type="text" value="group3"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/>
4	<input type="text" value="group4"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/>
5	<input type="text" value="group5"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/>



# Using the Configuration Utility (continued)

## Home > User Manager > Authentication Server > POP3

Authentication Server	<input type="radio"/> Local <input checked="" type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Web Server
	<a href="#">Local Users List</a>
	<a href="#">On-demand Users List</a>
	<a href="#">Local User Group Configuration</a>
	<a href="#">On-demand User Configuration</a>

To use POP3 as the authentication method, input the **POP3** server IP address or domain name and its POP3 server port. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes if there are any online users.

Authentication Server	<input type="radio"/> Local <input checked="" type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Web Server
	Server IP <input type="text"/>
	Server Port <input type="text" value="110"/>

## Home > User Manager > Authentication Server > RADIUS

Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input checked="" type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Web Server
	Session/Idle <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	<b>Primary Server</b>
	802.1x <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Server IP <input type="text"/>
	Authentication Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
	Secret Key <input type="text"/>
	Accounting Service <input type="text" value="Disabled"/>
	Authentication Method <input type="text" value="CHAP"/>
	<b>Secondary Server</b>
	Server IP <input type="text"/>
	Authentication Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
	Secret Key <input type="text"/>
Accounting Service <input type="text" value="Disabled"/>	
Authentication Method <input type="text" value="CHAP"/>	

To use RADIUS as the authentication method, input the RADIUS server IP address or domain name, public LAN port, accounting Port, secret key and select the accounting service and public LAN method function. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes if there are any online users.

# Using the Configuration Utility (continued)

## Home > User Manager > Authentication Server > RADIUS > 802.1x

Select **Enable** to use the 802.1x feature. The DSA-3100 supports integrated single sign-on when used with 802.1x enabled access points. By using the integrated RADIUS proxy function in the DSA-3100, users can use the EAP methods such as EAP-MD5 or EAP-TLS to login and get the service depending on the authentication methods which the backend RADIUS server and APs support.

The assumption, for this scenario, is that the network administrator has configured an EAP-enabled RADIUS server like Microsoft Internet Authentication Service on Windows 2000 or .NET Server 2003. If EAP-TLS is required for the dynamic key exchange, Microsoft Certification is also required. It is also recommended that the system administrator perform an authentication test to make sure everything is correct before connecting the network to the DSA-3100. (802.1x is available only when RADIUS is selected here, under *Home>User Manager>Authentication Server* in the DSA-3100 Configuration).

To utilize 802.1x, all the devices on the network must be 802.1x and EAP enabled. The APs and the RADIUS server must share the same secret word, and the DSA-3100 and the RADIUS server must share the same secret word.

### Configuring network devices for use with 802.1x:

To use 802.1x, please configure the RADIUS server, the access points and the DSA-3100 as follows :

#### RADIUS server:

The system administrator should create a client account for the DSA-3100 first and define the required secret. (We suggest that you use a different one than the one the APs are using). The RADIUS server is capable of multiple “secret keys” each assigned to a specific device. In order to participate in the network, each device must share the secret key that has been assigned to it in the RADIUS server’s configuration.

#### DSA-3100:

In the configuration utility, select Home>User Manager>Authentication Server and select RADIUS.

#### Access Points:

When configuring the access point, include the IP address of the RADIUS server in the appropriate field. The corresponding secrets for each AP should match the settings in DSA-3100.

# Using the Configuration Utility (continued)

## Home > User Manager > Authentication Server > RADIUS > 802.1x (continued)

Input the IP addresses and secret keys for the devices on the network.

802.1x Device Configuration		
No	IP (Segment) Address	Secret
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"/>



If you are using the 802.1x supplicant provided by Microsoft, the idle time out will be longer than the settings in RADIUS/AP and DSA-3100. Except for the idle timer, there is no way for the user to logoff from 802.1x Access Point in the current 802.1x implementation by Microsoft.

# Using the Configuration Utility (continued)

## Home > User Manager > Authentication Server > LDAP

### LDAP:

Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input checked="" type="radio"/> LDAP <input type="radio"/> External Web Server	
	Server IP	<input type="text"/>
	Server Port	<input type="text" value="389"/>
	Base DN	<input type="text" value="CN=Users,DC=dlink,DC=com"/>

To use LDAP as the authentication method, input the LDAP server IP address or domain name and its LDAP server port. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes, if there are any online users.

## Home > User Manager > Authentication Server > External Web Server

Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input checked="" type="radio"/> External Web Server	
	Protocol <input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS	
	Server IP	<input type="text"/>
	Server Port	<input type="text" value="80"/>
	Login Page	<input type="text"/>
Logout Page	<input type="text"/>	

The DSA-3100 can support an external web server which enables the user to put the login page on the external web server and change it at anytime to correspond with customer's needs.

- Protocol:** Choose from http or https.
- Server IP:** External Web servr IP.
- Server Port:** External Web server Port number.
- Login Page:** Login page location.
- Logout Page:** Logout page location.

# Using the Configuration Utility (continued)

## Advanced > Port and IP Redirect



The screenshot shows the configuration utility for a D-Link DSA-3100 Airspot Public/Private Gateway. The interface includes a navigation menu with tabs for Home, Advanced (selected), Tools, Status, and Help. On the left, there is a sidebar with buttons for various configuration options: Port and IP Redirect (highlighted), Pass Through, Virtual Server, DMZ, Free Surfing Area, Static Route, and Firewall. The main content area displays the 'Port and IP Redirect' configuration table, which allows defining up to 10 sets of traffic redirection criteria. Each row includes a number, a service name, destination IP address and port, conversion to destination IP address and port, and a type (TCP or UDP). At the bottom right, there are three buttons: Apply (with a green checkmark), Cancel (with a red X), and Help (with a red plus sign).

Port and IP Redirect						
No.	Service Name	Destination		Convert to Destination		Type
		IP Address	Port	IP Address	Port	
1						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
2						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
3						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
4						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
5						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
6						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
7						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
8						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
9						<input checked="" type="radio"/> TCP <input type="radio"/> UDP
10						<input checked="" type="radio"/> TCP <input type="radio"/> UDP

Up to 10 sets of traffic redirection criteria can be defined through this interface. Clients who try to access a specific destination that matches one of the defined destinations will be forced to a matching redirection target. These settings will take effect immediately after you click the **Apply** button.

# Using the Configuration Utility (continued)

## Advanced > Pass-Through

To maintain an adequate level of security, each client on the network can be managed. To allow some devices to be unmanaged, input their IP addresses or MAC addresses in this interface. Up to 20 IP addresses and 10 MAC addresses can be assigned unmanaged access. MAC address format is XX:XX:XX:XX:XX:XX

No.	IP Address	No.	IP Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

No.	MAC Address	No.	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	



**Caution:** Allowing unmanaged access from specific IP or MAC addresses could adversely affect the security of your network.

This feature allows you to define up to 10 virtual servers to enable access to servers connected to the authentication and local network port from outside of the managed network. Depending on the service provided, the service might run on TCP ports, UDP ports or both. Click **Enable** to activate the rule. Changes to the settings of virtual servers will take effect immediately after you click the **Apply** button.

## Advanced > Virtual Server

No.	External Service Port	Local Server IP Address	Local Service Port	Type	Enable
1				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10				<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

**Note:** Each local server connected to the authentication port must also be allowed IP or MAC address pass-through. Please enter its IP or MAC address via the interface shown in the pass-through configuration screen.

# Using the Configuration Utility (continued)

If you have multiple IP addresses available to assign to the DSA-3100's WAN interface, you could define up to 10 pairs of Ethernet side (Private IP) and WAN side (Public IP) addresses. The WAN interface will bind the extra public IP addresses automatically.

## Advanced > DMZ

The screenshot shows the configuration utility for the DSA-3100. The sidebar on the left contains buttons for: Port and IP Redirect, Pass Through, Virtual Server, DMZ (highlighted in yellow), Free Surfing Area, Static Route, and Firewall. The main content area is titled "DMZ" and contains a table with 10 rows. Each row has a "No." column and two "IP Address" columns (Private and Public). At the bottom right, there are "Apply", "Cancel", and "Help" buttons with corresponding icons.

No.	Private IP Address	Public IP Address
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"/>

To allow users access to a few websites before they log in, enter the IP addresses of those sites in the **Free Surfing Area** list. Up to 20 sites can be defined. For example, a website that provides introduction and guidance for local facilities and routes or sites with content suitable or appropriate for public viewing could be listed in the **Free Surfing Area**. Guest users of the network cannot access other parts of the network but could still connect to these sites. These sites provide a free experience but can also indicate other areas of the Internet that can be accessed for an additional fee.

## Advanced > Free Surfing Area

The screenshot shows the configuration utility for the DSA-3100. The sidebar on the left contains buttons for: Port and IP Redirect, Pass Through, Virtual Server, DMZ, Free Surfing Area (highlighted in yellow), Static Route, and Firewall. The main content area is titled "Free Surfing Area" and contains a table with 20 rows. Each row has a "No." column and two "IP Address / Domain Name" columns. At the bottom right, there are "Apply", "Cancel", and "Help" buttons with corresponding icons.

No.	IP Address / Domain Name	No.	IP Address / Domain Name
1	www.dlink.com	2	64.7.210.132
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"/>

# Using the Configuration Utility (continued)

## Advanced > Static Route

In this example, if you want the 192.168.202.0/24 and 192.168.100.0/24 network to have access to each other, you should add a static route in the DSA-3100 and also in the 192.168.200.253 IP router. These settings show the DSA-3100's static route configurations.

Static Route			
No.	Destination		Gateway
	Network ID	Subnet Mask	IP Address
1	<input type="text" value="192.168.202.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.0.253"/>
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"/>



### Destination Network ID:

Specifies the target network or host IP. In this example we use network 192.168.202.0 as the routed target.

### Destination Subnet Mask:

Specifies the target subnet mask. In the example, we use the subnet mask 255.255.255.0.

### Gateway IP Address:

Specifies the IP address of the next hop router. In the example, we set this to 192.168.0.253 as the 192.168.202.0 network is behind the router.

### Click Apply:

Always click **Apply** to save the changes/additions.

**Note:** For the static route to work, the next hop route must also have added a static route to forward all 192.168.100.0/24 IP packets to the DSA-3100. After clicking the **Apply** button, you will see the added route is shown in the current running routing table. Click **View Routing table** to verify.



Every change to the static route settings must be stored by using the **Save Setting** function, and restarting the DSA-3100.



# Using the Configuration Utility (continued)

## Advanced > Firewall

Click the **Filter Rule** number to enter the firewall page for each filter. The chart on the following page explains each configurable item in detail.

**D-Link**  
Building Networks for People

**DSA-3100**  
Airsport Public/Private Gateway

Home **Advanced** Tools Status Help

IP Filter / Firewall

Filter Rule	Active	Action	Name	Source	Destination	Protocol
1	<input type="checkbox"/>	Block		ANY	ANY	ALL
2	<input type="checkbox"/>	Block		ANY	ANY	ALL
3	<input type="checkbox"/>	Block		ANY	ANY	ALL
4	<input type="checkbox"/>	Block		ANY	ANY	ALL
5	<input type="checkbox"/>	Block		ANY	ANY	ALL
6	<input type="checkbox"/>	Block		ANY	ANY	ALL
7	<input type="checkbox"/>	Block		ANY	ANY	ALL
8	<input type="checkbox"/>	Block		ANY	ANY	ALL
9	<input type="checkbox"/>	Block		ANY	ANY	ALL
10	<input type="checkbox"/>	Block		ANY	ANY	ALL

First Prev Next Last

## Edit the filter rule

Filter rule is a set of filters that determine whether traffic will be allowed to pass between the source and destination or whether it will be dropped. To display the detail, click the **index number** in the screen above.

IP Filter / Firewall > Edit Filter Rule

Rule: 1

Name:   Check to enable this rule

Action:  Protocol:

Source MAC:

	IF	Address	Subnet Mask	Operator	Start Port	End Port
Source	<input type="text" value="AU"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="LN"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>

Please see the next page for an explanation of the fields in the configuration screen shown above.

# Using the Configuration Utility (continued)

## Advanced > Firewall (continued)

Filter	Description
Name	Gives a name to the IP Filter rule
Check to enable this rule	Enables this rule if it is marked
Action	Specifies the action to be taken when packets match the rule Block: Packets matching the rule will be dropped Pass: Packets matching the rule will be passed
Protocol	Specifies the protocol(s) this filter rule will apply to
Source MAC	Source MAC address (optional)
Source/ Destination IF	Source/Destination Interface (IF). You can select WAN port or LAN port or Authentication port or ALL ports
Source/ Destination IP Address	Source/Destination IP Address
Source/Destina- tion Subnet Mask	Source/Destination Subnet Mask
Source/Destination Operator	Select =(equal), != (not equal), >(greater than), <(smaller than) operator rule
Source/Desti- nation Start Port	Source/Destination Start Port
Source/Destina- tion End Port	Source/Destination End Port

# Using the Configuration Utility (continued)

## Admin E-mail

**Send From:** Enter the E-mail address from which you wish to send the DSA-3100 history log.

**Send To:** Enter the E-mail address here to which you wish to send the DSA-3100 history log.

**Interval:** Enter the interval at which you would like the history to be sent.

## Monitor IP List

The DSA-3100 can monitor up to 20 IP addresses on the network.

The system periodically sends out packets to check the status of the selected network devices by pinging every 30 minutes. If the device cannot be reached, the DSA-3100 will send an E-mail to the admin every 30 minutes. For example: if you specify a device which can't be reached, the DSA-3100 will send an E-mail to the admin at 1:00, 1:30, 2:00, 2:30, 3:00 etc., until the problem is fixed.

The DSA-3100 provides 2 built-in user accounts:

**Admin:** This user is the administrator of the DSA-3100.

**Manager:** This user has the right to manage a user account, the admin functions are denied. The Admin and the Manager can change their passwords; specify the current password first. The new password must be entered twice.

## Tools > Monitor IP List

**D-Link** Building Networks for People  
**DSA-3100**  
Airspot Public/Private Gateway

Home Advanced **Tools** Status Help

**Admin Email**

Send From:   
Send To:   
Interval: 1 Day

Apply Cancel Help

**Monitor IP List**

No.	IP Address	No.	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"/>

Apply Cancel Help

## Tools > Change Password

**D-Link** Building Networks for People  
**DSA-3100**  
Airspot Public/Private Gateway

Home Advanced **Tools** Status Help

**Change Admin Password**

Old Password:   
New Password:   
New Password (confirm):

Apply Cancel Help

**Change Manager Password**

Old Password:   
New Password:   
New Password (confirm):

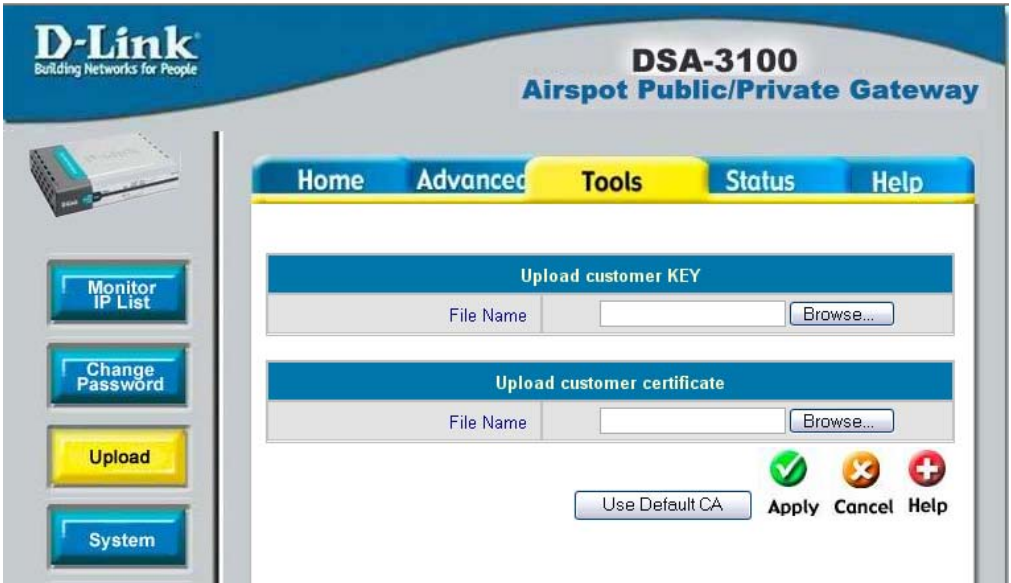
Apply Cancel Help



**Note:** If you lose the administrator's password, you can change the administrator's password from the console interface.

# Using the Configuration Utility (continued)

Tools > Upload



## Upload customer key

To provide a custom key page in order to support a specific certificate, please click **Browse** to search for the file name for the customer key. Click **Apply** to upload it onto the DSA-3100.

## Upload customer certificate

To provide a custom key page in order to support a specific certificate, please click **Browse** to search for the file name for the customer certificate. Click **Apply** to upload it onto the DSA-3100. If you want to get back to the default customer certificate page, simply click the **Use Default CA** button.

*continued on the next page*

# Using the Configuration Utility (continued)

## Tools > Upload Login Page



The screenshot shows a web-based configuration utility titled "Upload Login Page". It features a blue header bar with the title. Below the header, there is a "File Name" label followed by an empty text input field and a "Browse..." button. To the right of the input field, there are three circular icons: a green checkmark, an orange 'X', and a red plus sign. Below these icons are three buttons: "Apply" (with the green checkmark icon), "Cancel" (with the orange 'X' icon), and "Help" (with the red plus sign icon). A "Preview" link is located to the left of the "Use Default Page" button.

To provide a custom user login page, please specify the file name to upload onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login page, simply click the **Preview** button

The uploaded custom login page must contain the following HTML codes to provide users a place to input the user name and password.

### Required HTML code

```
<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>
```

# Using the Configuration Utility (continued)

## Tools > Upload Logout Page

The screenshot shows a web-based configuration utility titled "Upload Logout Page". It features a blue header bar with the title. Below the header, there is a "File Name" label followed by an empty text input field and a "Browse..." button. To the right of the input field, there are three circular icons: a green checkmark, a yellow 'X', and a red plus sign. Below these icons are three buttons: "Preview" (with a blue underline), "Use Default Page", "Apply", "Cancel", and "Help".

To provide a custom user logout page, please click **Browse** to specify the file name and upload it onto the DSA-3100 by clicking **Apply**. If you want to get back to the default user logout page, simply click the **Use Default Page** button. If you want to display the Logout page, simply click the **Preview** button.

The uploaded custom logout page must contain the following HTML codes to provide users a place to input the user name and password.

### Required HTML code

```
<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>
```

# Using the Configuration Utility (continued)

## Tools > Upload

### Tools > Upload Error Page

Upload Error Page: To provide a custom error page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Error Page, simply click the **Preview** button.

The screenshot shows the 'Upload Error Page' configuration form. It has a 'File Name' input field with a 'Browse...' button. Below the input field are three icons: a green checkmark, a yellow 'X', and a red plus sign. At the bottom, there are four buttons: 'Preview' (with a blue underline), 'Use Default Page', 'Apply', and 'Cancel'. A 'Help' link is also present.

### Tools > Upload Login Succeed Page

Upload Login Succeed Page: To provide a custom user “login ok” page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login Succeed Page, simply click the **Preview** button.

The screenshot shows the 'Upload Login Succeed Page' configuration form. It has a 'File Name' input field with a 'Browse...' button. Below the input field are three icons: a green checkmark, a yellow 'X', and a red plus sign. At the bottom, there are four buttons: 'Preview' (with a blue underline), 'Use Default Page', 'Apply', and 'Cancel'. A 'Help' link is also present.

The screenshot shows the 'Upload Logout Succeed Page' configuration form. It has a 'File Name' input field with a 'Browse...' button. Below the input field are three icons: a green checkmark, a yellow 'X', and a red plus sign. At the bottom, there are four buttons: 'Preview' (with a blue underline), 'Use Default Page', 'Apply', and 'Cancel'. A 'Help' link is also present.

The screenshot shows the 'Upload Image Files' configuration form. It has an 'Upload Images' input field with a 'Browse...' button. Below the input field are three icons: a green checkmark, a yellow 'X', and a red plus sign. At the bottom, there are four buttons: 'Preview' (with a blue underline), 'Use Default Page', 'Apply', and 'Cancel'. A 'Help' link is also present.

### Tools > Upload Logout Succeed Page

Upload Logout Succeed Page: To provide a custom user logout page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user logout page, simply click the **Use Default Page** button. If you want to display the Logout Succeed Page, simply click the **Preview** button.

### Tools > Upload Image Files

If the user-defined logon interface includes a graphic file, the HTML code of the graphic file path must be the upload graphic file. Enter the path and file name of the graphic file or browse to select the file. The maximum size of the graphic file is 512K.

#### Path of Graphic File in User Logon Interface

```

```

After the graphic file is uploaded, the Existing Image Files section will list the graphic files uploaded to the system. You can select or delete any graphic file, and the system will list the size of the graphic file.

# Using the Configuration Utility (continued)

Allows you to make a backup image and restore the backup copy to the DSA-3100. This page also enables you to restore the DSA-3100 back to the factory default settings.

## Create Backup Image:

Make a backup image file.

## Restore Setting From File:

Browse the hard drive to locate and restore the backup image file. (Important: The image must be created by the DSA-3100.)

## Reset To Factory Default:

Click **Reset** to restore the DSA-3100 back to the factory default settings.

Please click the link in the configuration screen shown here to check for firmware upgrades on the D-Link website. After you download the new firmware file to your hard drive, click **Browse** and then click **Apply** to upgrade the firmware.



### Caution:

*Firmware upgrades might result in configuration data loss. Some other restrictions might also apply. Please refer to the release notes of new firmware upgrades. When the system is upgrading its firmware, the Status LED blinks until done. When finished, the web interface will display a successful message.*

## Tools > System

## Tools > Firmware



*Please restart the DSA-3100 using the administration interface. Do not directly power it off and on. Restarting the DSA-3100 in this way, after a firmware upgrade, might result in corruption of the DSA-3100 firmware. (Online user sessions will be terminated when the system restarts.)*

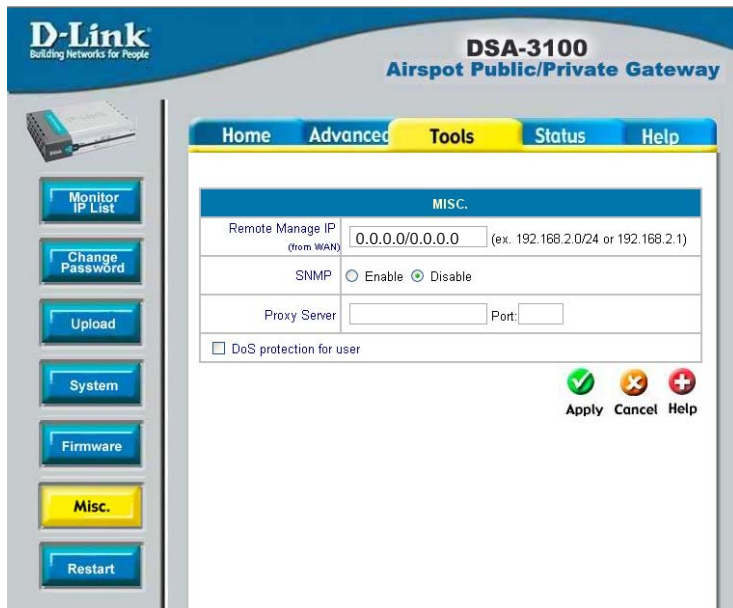


# Using the Configuration Utility (continued)

## Tools > Misc.

### Remote Manage IP:

Specify 0.0.0.0/0.0.0.0 as the IP address here, in order to manage the device from any location. Or you can enter an IP address to specify a single computer or network.



**SNMP:** The DSA-3100 provides SNMP v2 Read-only (RO) management,

- **Manager IP:** A trap manager is a management station that receives and processes traps. When you configure a trap manager, assign an IP address to the management station.

- **Community:** Community strings serve as passwords for SNMP messages, DSA-3100 allows Read-only (RO) access.

If you select **Enable** SNMP, enter the IP address, community string to the field.

**Proxy Server:** Based on DSA-3100 security management, only port 80 is allowed (it will appear on logon webpage). If you have built a Proxy Server in your network environment, and the user's browser is set to Proxy, you must set your External Proxy Server IP Address and Proxy Port here in order to have proper operations in the Proxy network environment. These settings will be effective immediately after you click **Apply**.

### DoS protection for user:

The DSA-3100 protects users against various hacker attacks including NMAP FIN/URG/PSH, Xmas Tree, SYN/RST, Ping of Death, Null Scan, and SYN/FIN.

# Using the Configuration Utility (continued)

## Tools > Restart

Reboots the DSA-3100. It takes about 75 seconds for the DSA-3100 to reboot. If you have to turn off the power of the DSA-3100 for some time, please reboot it, and after you hear a beep, remove the power adapter.

**Note:** *On-line user sessions will be terminated when the system restarts.*

The screenshot shows the 'Tools > Restart' page in the D-Link configuration utility. The main content area displays a confirmation message: "Are you sure?". Below the message are two buttons: a green checkmark labeled "Yes" and a red cross labeled "Help". The left sidebar contains a vertical list of navigation buttons: "Monitor IP List", "Change Password", "Upload", "System", "Firmware", "Misc.", and "Restart". The top navigation bar includes "Home", "Advanced", "Tools", "Status", and "Help".

## Status > Device Info

This feature displays a system configuration summary. For a chart defining each term, please see the following page.

The screenshot shows the 'Status > Device Info' page in the D-Link configuration utility. The main content area displays a table of system status information. The left sidebar contains navigation buttons: "Device Info", "Interface", "Current Users", and "Traffic History". The top navigation bar includes "Home", "Advanced", "Tools", "Status", and "Help".

System Status	
Current Firmware Version	2.22B3C3
System Name	DSA-3100
Admin Detail	N/A
Succeed Page	http://www.dlink.com
External Syslog Server	N/A/N/A
Console Port Baud Rate	9600 bps
Manage	SSH N/A
History	Retain Days 3 Days
	Email To N/A
Time	External Time Server timekeeper.isi.edu
	Date Time Fri May 21 23:50:16 PDT 2004
User	Idle Timer 10 Min(s)
	Multiple Login Disabled
	User Type LOCAL
	Guest Account Enabled
DNS	Primary DNS Server 67.130.140.2
	Secondary DNS Server 192.152.81.1

# Using the Configuration Utility (continued)

## Status > Device Info (continued)

Current Firmware Version		Displays the current firmware version
System Name		System name; DSA-3100 is the default
Admin Detail		Information about the admin
Succeed Page		The URL that appears after a successful user login—usually a corporation’s homepage
External Syslog Server		Shows the IP address and the Port of the Syslog server
Console Port Baud Rate		9600bps
Manage	SSH	The IP address that connects to the WAN port for configuring the DSA-3100
History	Retain Days	The system will keep user login information for 3 days
	E-mail to	E-mails the traffic history file to this address
Time	External Time Server	Used for clock synchronization
	Date Time	Displays Greenwich time
User	Idle Logout Timer	10 Min(s)
	Multiple Login	When disabled, it disallows a single user from logging in multiple times
	User Type	Displays the user account authentication method
	Guest Account	Displays guest account status
DNS	Preferred DNS server	DNS server IP address (Primary).
	Alternate DNS server	DNS server IP address (Secondary).

## Using the Configuration Utility (continued)

With this feature, you can get Interface management information about the **WAN port**, **Authentication port**, and **Local Network port**. For more detail see the following page:

### Status > Interface

Interface Status		
WAN	MAC Address	00:E0:4C:39:00:03
	IP Address	10.2.3.82
	Subnet Mask	255.255.255.0
	DNS IP Address	168.95.1.1
Public LAN	Mode	NAT
	MAC Address	00:E0:4C:39:00:01
	IP Address	192.168.1.40
	Subnet Mask	255.255.255.0
Public LAN DHCP Server	DNS IP Address	168.95.1.1
	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.50
	End IP Address	192.168.1.200
Private LAN	Lease Time	1440 Min(s)
	Mode	NAT
	MAC Address	00:E0:4C:39:00:02
	IP Address	192.168.0.40
	Subnet Mask	255.255.255.0
Private LAN DHCP Server	DNS IP Address	168.95.1.1
	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.0.101
	End IP Address	192.168.0.200
Private LAN DHCP Server	Lease Time	1440 Min(s)

# Using the Configuration Utility (continued)

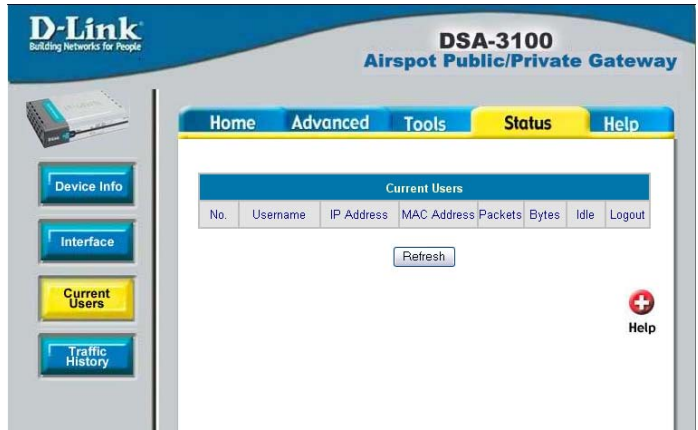
## Status > Interface (continued)

Item		Description
WAN	MAC Address	WAN port's MAC address
	IP Address	WAN port's IP address
	Subnet Mask	WAN port's Subnet Mask
	DNS IP Address	WAN port's DNS IP address
Public LAN	Mode	Public LAN port's mode: NAT mode
	MAC Address	Public LAN port's MAC address
	IP Address	Public LAN port's IP address
	Subnet Mask	Public LAN port's Subnet Mask
	DNS	Public LAN port's DNS IP address
Public LAN DHCP Server	Status	Enable DHCP server on Public LAN port
	WINS IP Address	Configure WINS server IP address on DHCP server
	Start IP Address	DHCP pool start IP address
	End IP address	DHCP pool end IP address
	Lease Time	IP address lease time
Private LAN	Mode	Private LAN port's mode: NAT mode
	MAC Address	Private LAN port's MAC address
	IP Address	Private LAN port's IP address
	Subnet Mask	Private LAN port's Subnet Mask
	DNS IP Address	Private LAN port's DNS IP address
Private LAN DHCP Server	Status	Enable DHCP function on Private LAN port.
	WINS IP Address	Configure WINS server IP address on DHCP server
	Start IP Address	DHCP pool start IP address
	End IP address	DHCP pool end IP address
	Lease Time	IP address lease time

# Using the Configuration Utility (continued)

## Status > Current Users

With this feature, you can get information about online users including **Username, IP, MAC, packet count, byte count** and **idle time**. It also allows the administrator to force an on-line user to get off-line by clicking the **log out** link beside a user's data.



## Status > Traffic History

### History E-mail

The DSA-3100 keeps traffic history in its volatile memory. To have the traffic history sent to you automatically, enter your E-mail address in the **History E-mail** field and the period of time between two history files

History Email	
Send From	<input type="text"/>
Send To	<input type="text"/>
Interval	1 Day <input type="button" value="v"/>

### Access History IP

Specify an IP address that allows the billing system to connect to the DSA-3100 via this IP address to get history information for billing.

Access History IP	
Access History IP (for Billing)	<input type="text"/> (ex. 192.168.2.1)

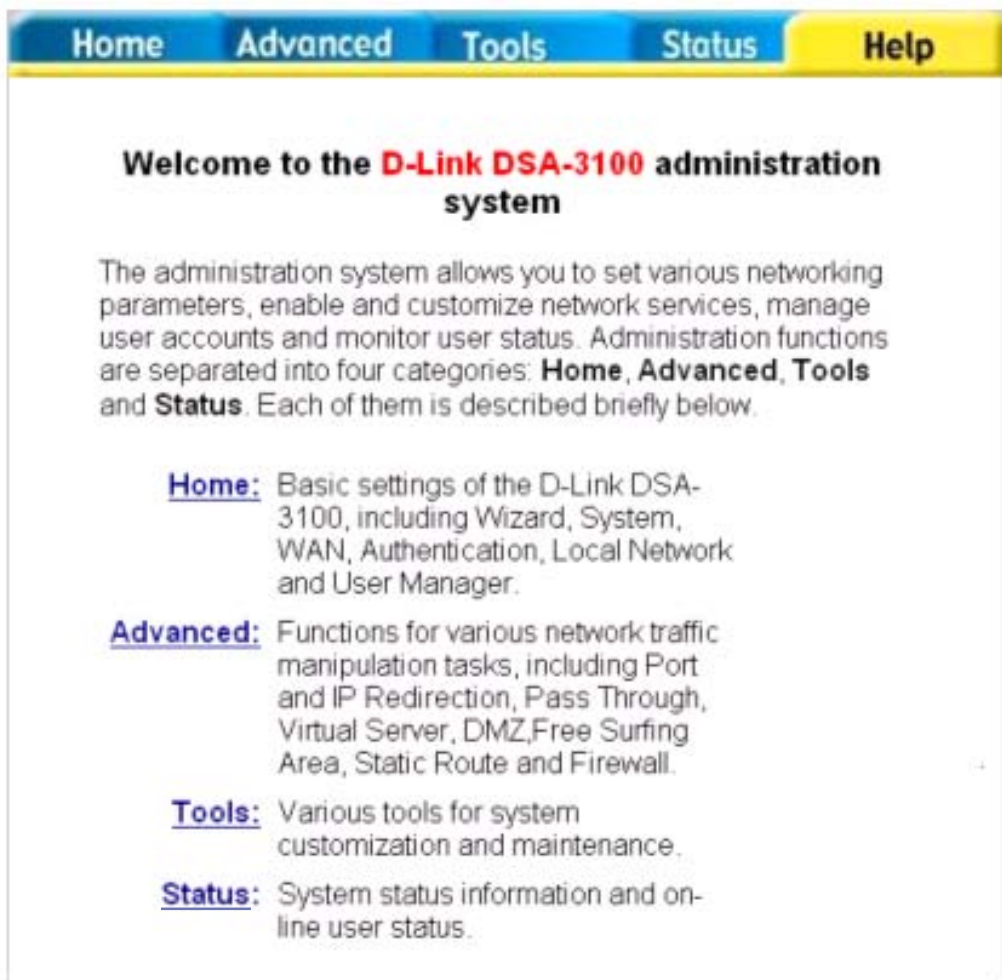
### External Syslog Server

Specify the IP address and the Port of the External Syslog server.

External Syslog Server	
External Syslog Server	<input type="text"/> Port: <input type="text"/>

# Using the Configuration Utility (continued)

## Help



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

**Welcome to the D-Link DSA-3100 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 four categories: **Home**, **Advanced**, **Tools** and **Status**. Each of them is described briefly below.

- Home**: Basic settings of the D-Link DSA-3100, including Wizard, System, WAN, Authentication, Local Network and User Manager.
- Advanced**: Functions for various network traffic manipulation tasks, including Port and IP Redirection, Pass Through, Virtual Server, DMZ, Free Surfing Area, Static Route and Firewall.
- Tools**: Various tools for system customization and maintenance.
- Status**: System status information and on-line user status.

This feature provides online instructions for operating the DSA-3100, you can click the hyperlink for a more detailed description.

# Networking Basics

## Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP**.

*Note: Please refer to websites such as <http://www.homenethelp.com> and <http://www.microsoft.com/windows2000> for information about networking computers using Windows 2000, ME or 98.*

Go to **Start>Control Panel>Network Connections**  
Select **Set up a home or small office network**

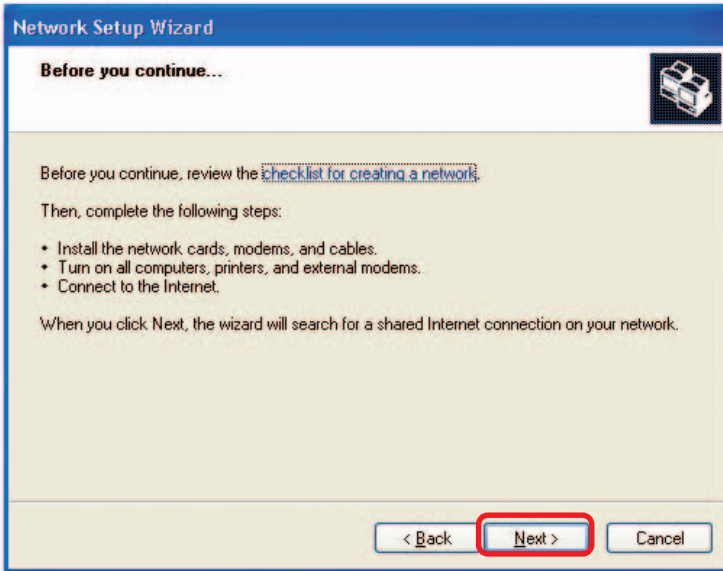


When this screen appears, Click **Next**.



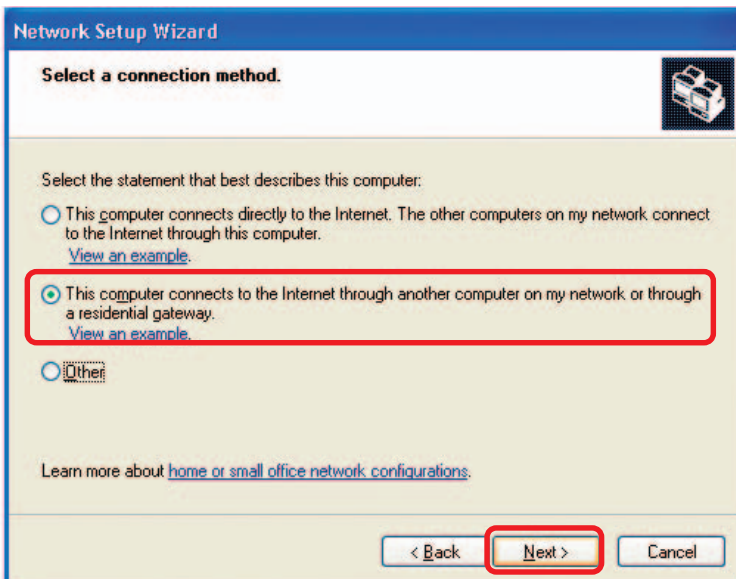
# Networking Basics (continued)

Please follow all the instructions in this window:



Click **Next**

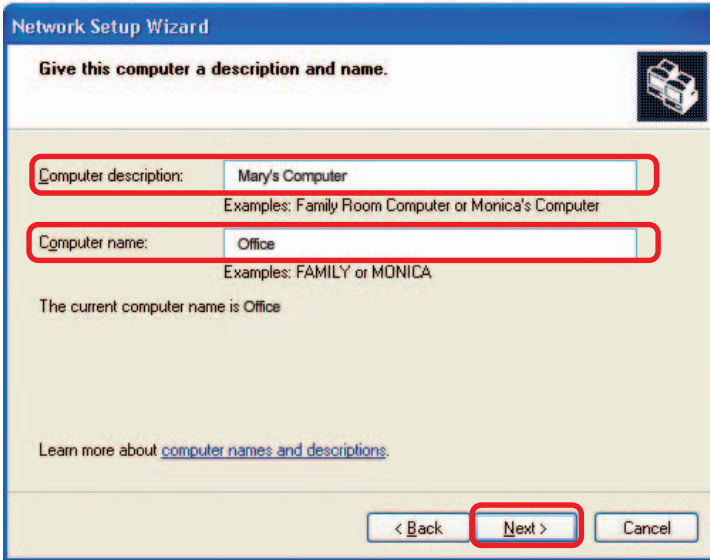
In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



Click **Next**

# Networking Basics (continued)

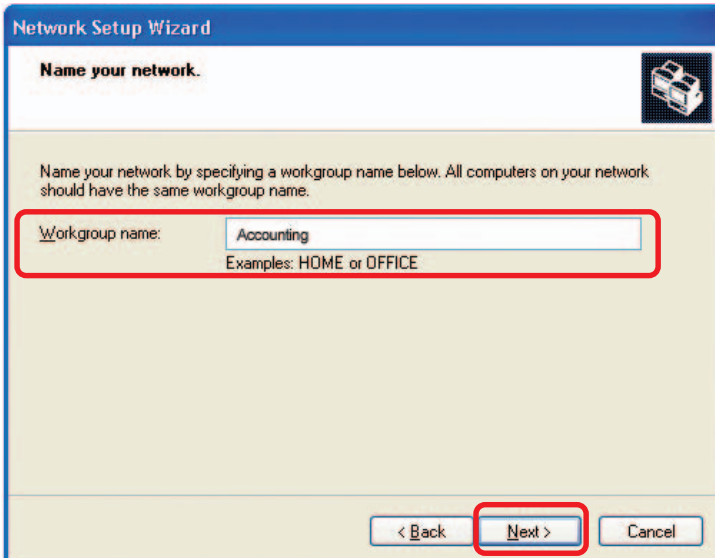
Enter a **Computer description** and a **Computer name** (optional.)



The screenshot shows the 'Network Setup Wizard' window with the title 'Give this computer a description and name.' The window contains two text input fields. The first field is labeled 'Computer description:' and contains the text 'Mary's Computer'. Below it, there are examples: 'Examples: Family Room Computer or Monica's Computer'. The second field is labeled 'Computer name:' and contains the text 'Office'. Below it, there are examples: 'Examples: FAMILY or MONICA'. Below the fields, it says 'The current computer name is Office'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Click **Next**

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name**.

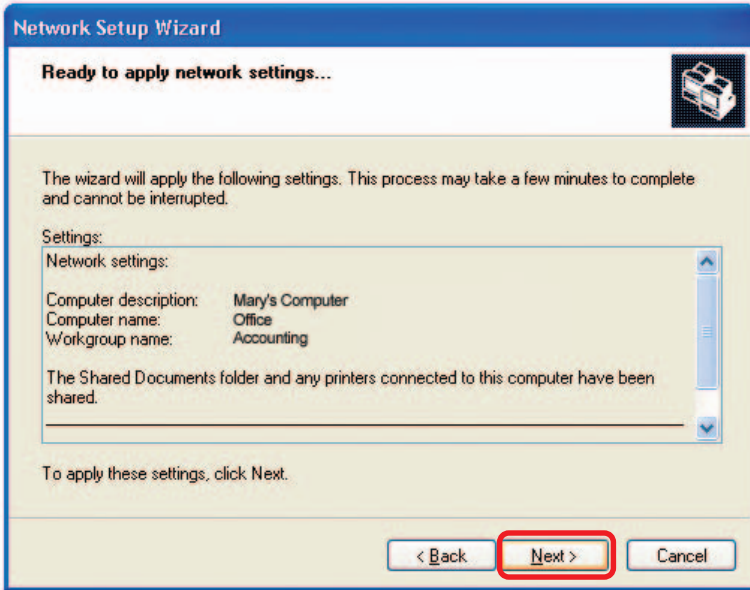


The screenshot shows the 'Network Setup Wizard' window with the title 'Name your network.' The window contains a text input field labeled 'Workgroup name:' with the text 'Accounting'. Below it, there are examples: 'Examples: HOME or OFFICE'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Click **Next**

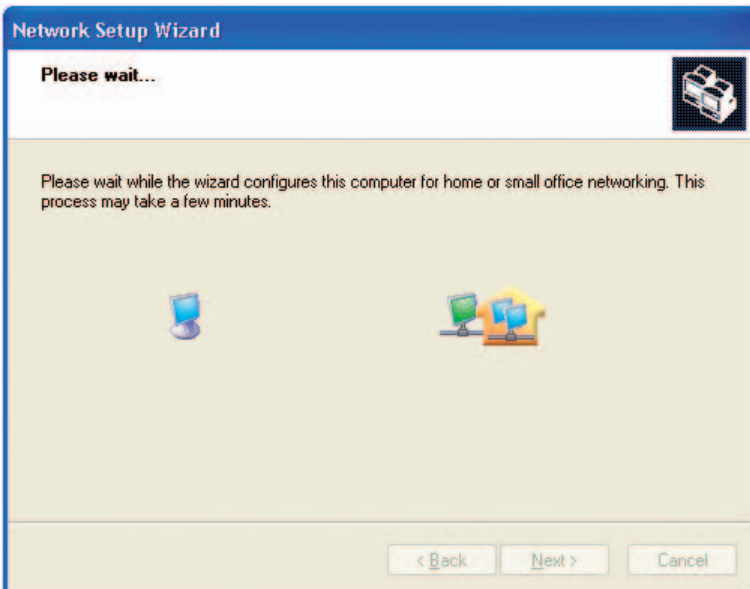
# Networking Basics (continued)

Please wait while the **Network Setup Wizard** applies the changes.



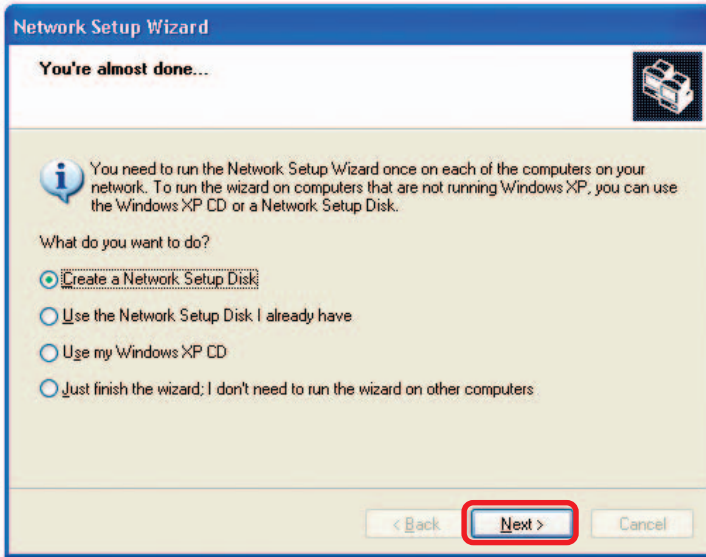
When the changes are complete, Click **Next**.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.



# Networking Basics (continued)

In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.

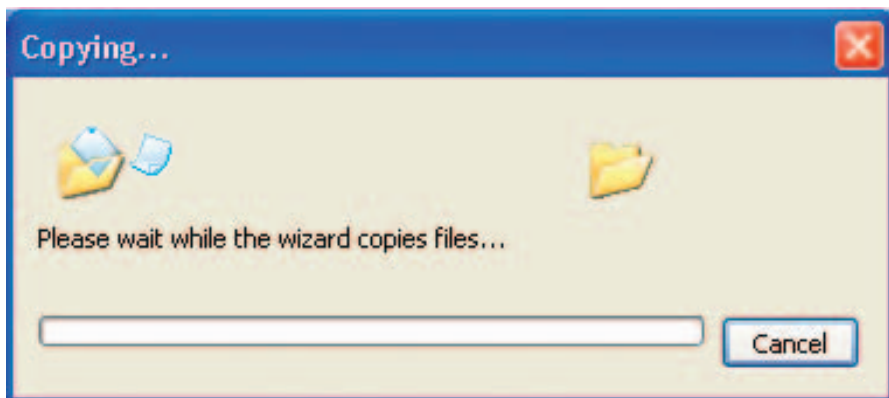


Insert a disk into the Floppy Disk Drive, in this case drive **A**.

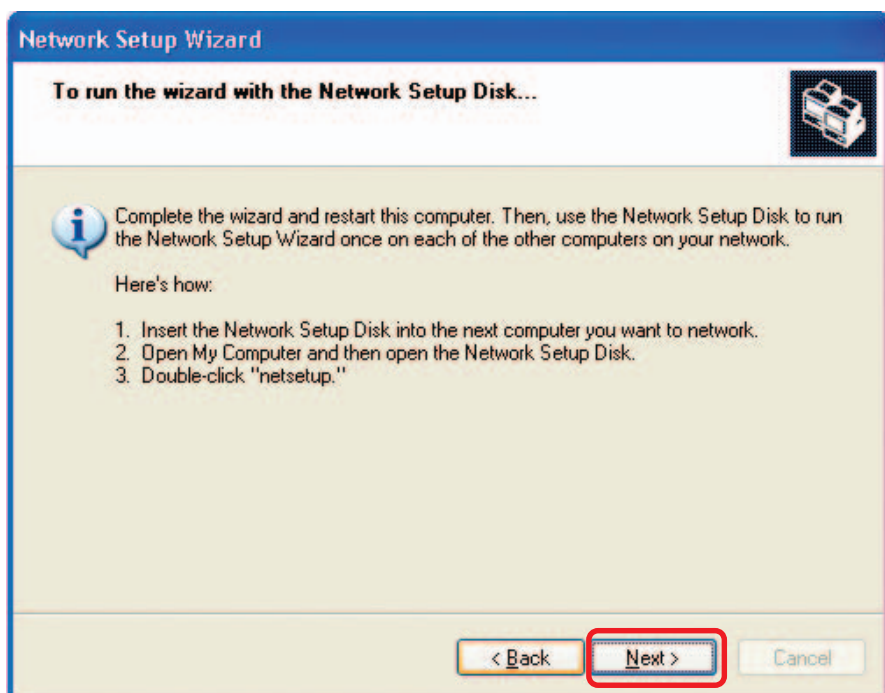


Click **Next**

## Networking Basics (continued)

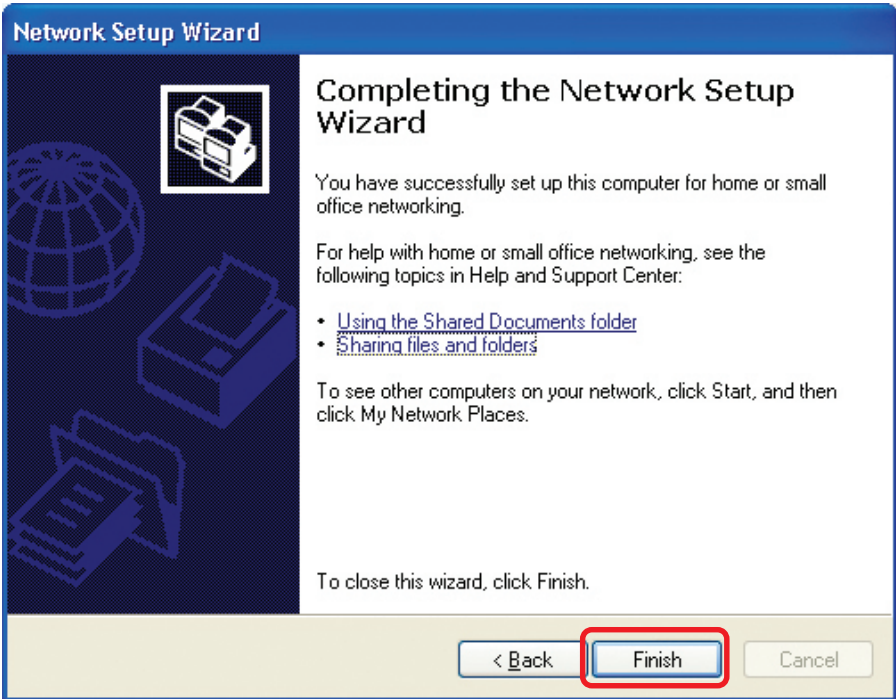


Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. Click **Next**.

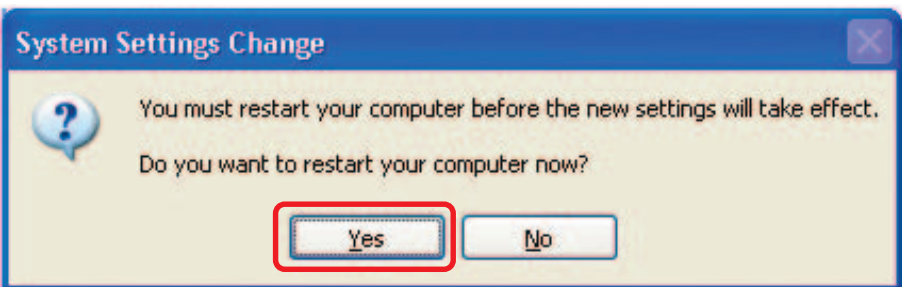


# Networking Basics (continued)

Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.



The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.



You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

# Networking Basics (continued)

## Naming your Computer

To name your computer In **Windows XP**, please follow these directions:

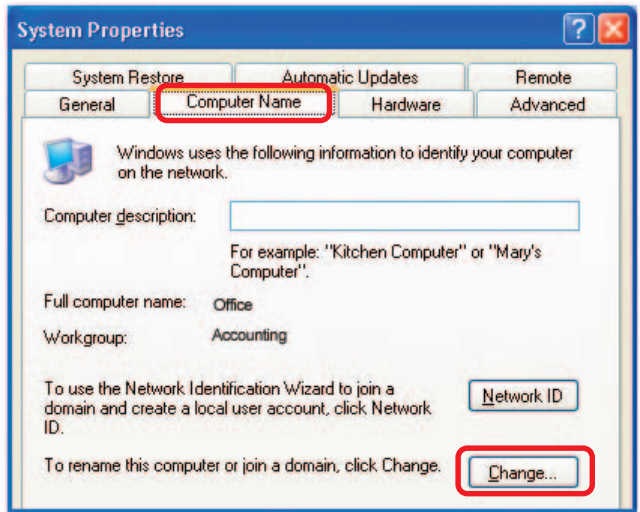
- Click **Start** (in the lower left corner of the screen)
- **Right-click** on **My Computer**
- Select **Properties**



- Select the **Computer Name Tab** in the System Properties window.

- You may enter a **Computer Description** if you wish; this field is optional.

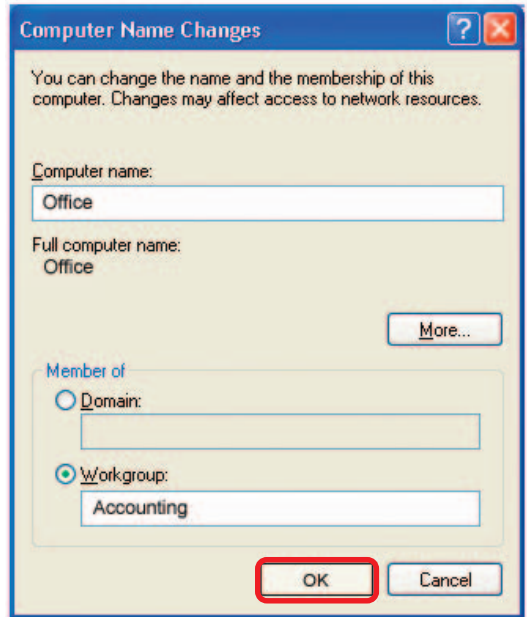
- To rename the computer and join a domain, click **Change**.



# Networking Basics (continued)

## Naming your Computer (continued)

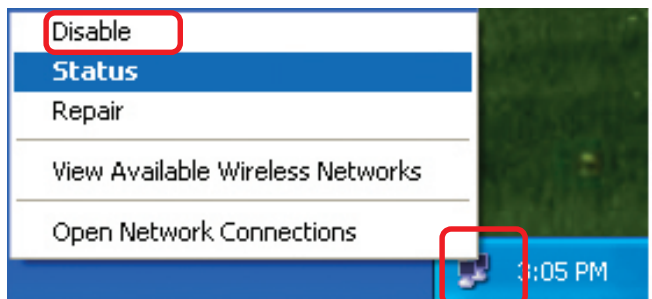
- In this window, enter the **Computer name**.
- Select **Workgroup** and enter the name of the **Workgroup**.
- All computers on your network must have the same **Workgroup** name.
- Click **OK**



## Checking the IP Address in Windows XP

The adapter-equipped computers in your network must be in the same IP Address range (see *Getting Started* in this manual for a definition of IP Address Range.) To check on the IP Address of the adapter, please do the following:

- Right-click on the **Local Area Connection icon** in the task bar
- Click on **Status**





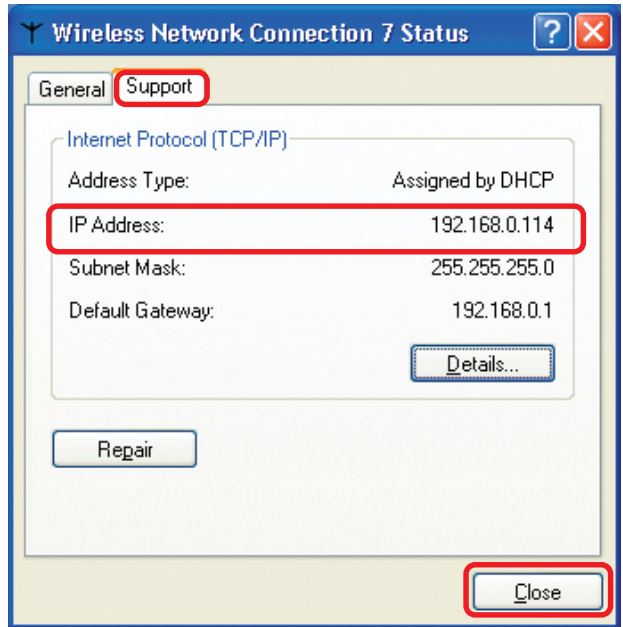
# Networking Basics (continued)

## Checking the IP Address in Windows XP (continued)

This window will appear.

- Click the **Support** tab

- Click **Close**



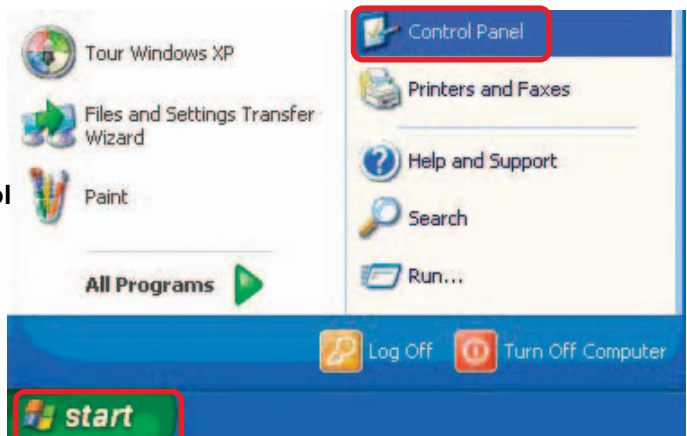
## Assigning a Static IP Address in Windows XP/2000

*Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.*

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

- Go to **Start**

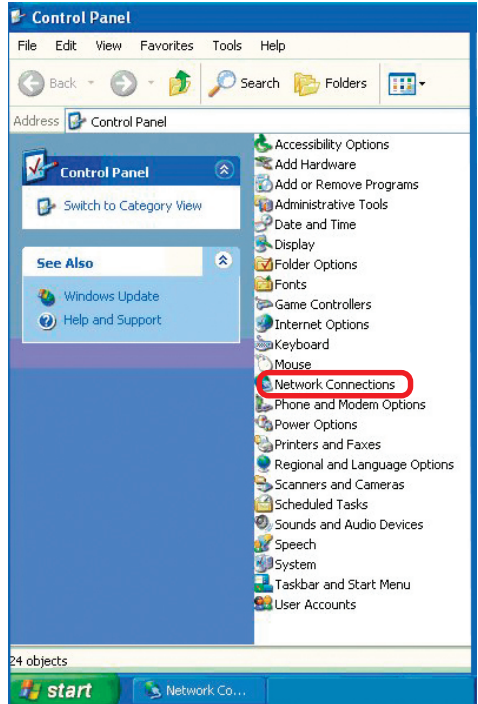
- Click on **Control Panel**



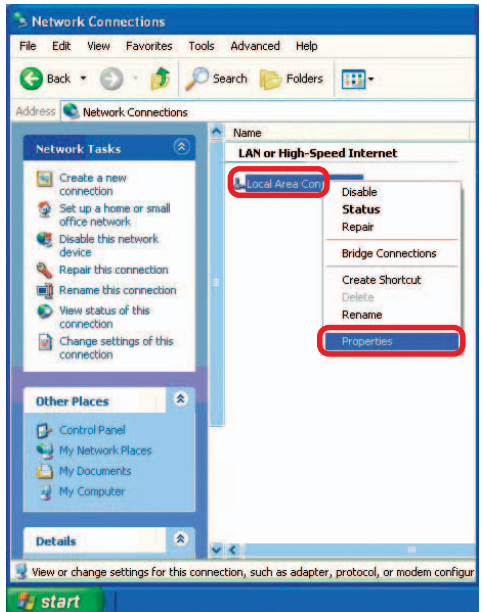
# Networking Basics (continued)

## Assigning a Static IP Address in Windows XP/2000 (continued)

- Double-click on **Network Connections**



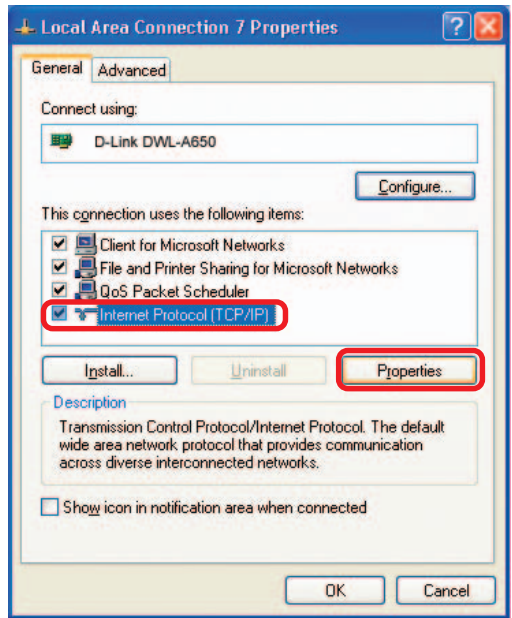
- Right-click on **Local Area Connections**
- Click on **Properties**



# Networking Basics (continued)

## Assigning a Static IP Address in Windows XP/2000

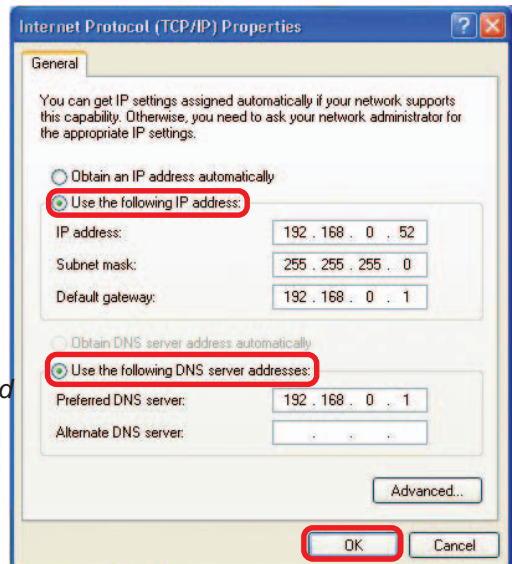
- Click on **Internet Protocol (TCP/IP)**
- Click **Properties**
- Input your **IP Address and subnet mask**. (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)



- Input your **DNS server addresses**. (Note: If you are entering a DNS server, you must enter the IP Address of the Default Gateway.)

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

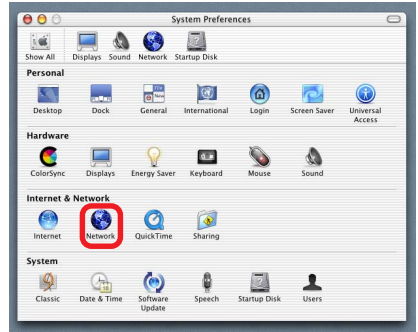
- Click **OK**



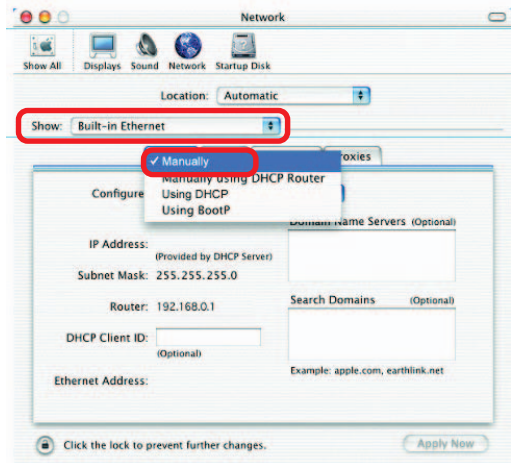
# Networking Basics (continued)

## Assigning a Static IP Address with Macintosh OSX

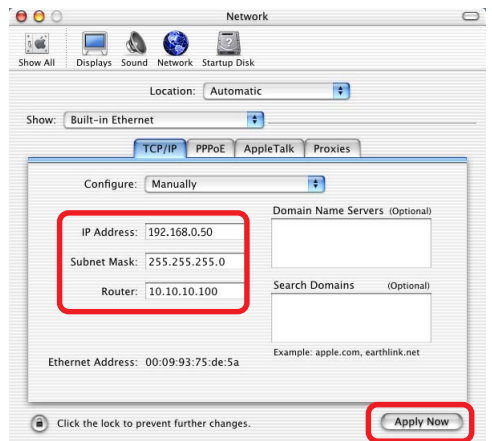
- Go to the **Apple Menu** and select **System Preferences**
- Click on **Network**



- Select **Built-in Ethernet** in the **Show** pull-down menu
- Select **Manually** in the **Configure** pull-down menu



- Input the **Static IP Address**, the **Subnet Mask** and the **Router IP Address** in the appropriate fields

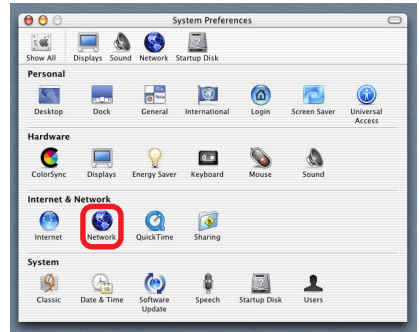


- Click **Apply Now**

# Networking Basics (continued)

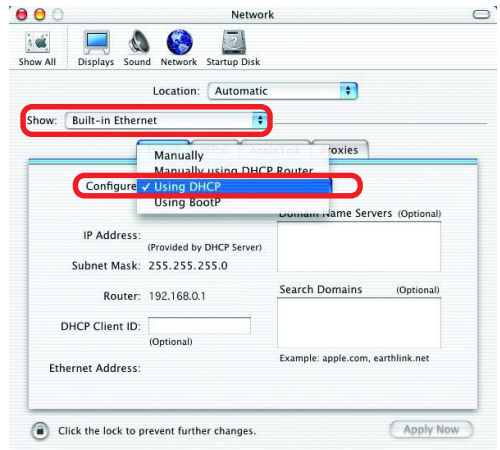
## Selecting a Dynamic IP Address with Macintosh OSX

- Go to the **Apple Menu** and select **System Preferences**



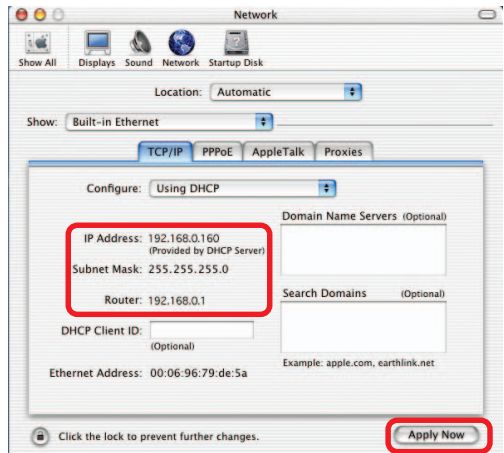
- Click on **Network**

- Select **Built-in Ethernet** in the **Show** pull-down menu



- Select **Using DHCP** in the **Configure** pull-down menu

- Click **Apply Now**



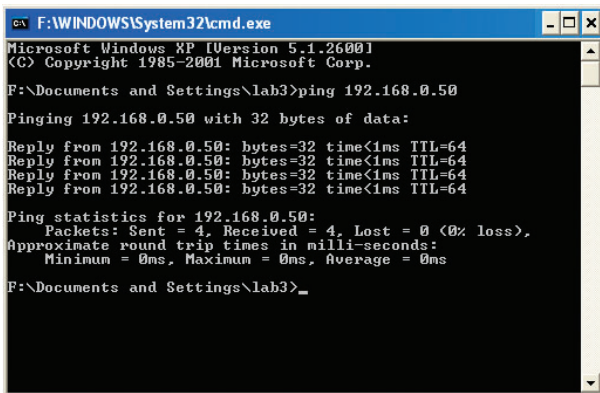
- The **IP Address**, **Subnet mask**, and the **Router's IP Address** will appear in a few seconds

# Networking Basics (continued)

## Checking the Wireless Connection by Pinging in Windows XP/2000

Note: The following illustrations are examples only. The IP Address that you are pinging may be different from those in the following examples.

- Go to **Start > Run >** type **cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the Wireless Router or Access Point, as shown.



```
cmd F:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab3>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

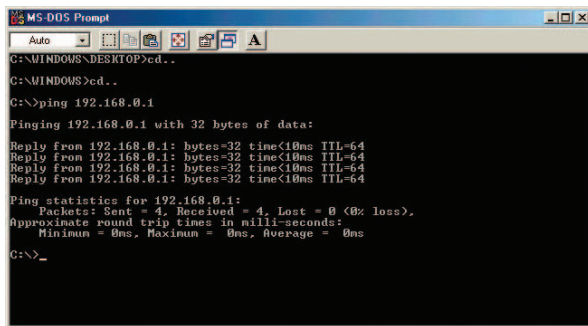
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

F:\Documents and Settings\lab3>_
```

## Checking the Wireless Connection by Pinging in Windows Me/98

- Go to **Start > Run >** type **command**. A window similar to this will appear. Type **ping xxx.xxx.xxx.xxx** where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the wireless router or access point, as shown.



```
MS-DOS Prompt
Auto
C:\WINDOWS\DESKTOP>ed..
C:\WINDOWS>ed..
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

# Technical Specifications

## Functions Provided

**3 10/100Mbps Fast Ethernet ports** for WAN connection, trusted LAN connection and untrusted LAN connection

**Manages up to 250 user account** data with internal user account database

**Supports up to 50 on-line users**

**ID/Password based authentication and authorization-** Can be combined with MAC Address locking to provide stricter access control

**POP3, RADIUS and LDAP external authentication mechanism support** - Only one of these can be selected at a time

**On-line status monitoring and history traffic data review**

**SSL protected access** to the administration interface and user authentication interface

**Customizable user login, logout web interface**

**Customizable target URL** for users who successfully get authorization

**Built-in DHCP server**

**High-speed policy routing engine**

**Customizable preemptory traffic redirection NTP client**

**Local network port for connecting a trusted network**

Permits access to WAN and LAN from local network without authentication

Permits connection to wired Ethernet while connecting the wireless network to this Ethernet port

# Technical Specifications (continued)

**Device Ports** - All ports (except the console port) are auto-mdix, which means that you can use a straight-through or a crossover cable for connections.

**WAN port:** 10/100Mbps Fast Ethernet

**Private LAN port:** 10/100Mbps Fast Ethernet connects to workstations & servers that do not need authentication

**Public LAN port:** 10/100Mbps Fast Ethernet connects to workstations & devices that need authentication

**Console port:** RS-232 (default set to 115200, n, 8, 1, no flow control)

## **Power Supply**

External Power Adapter

## **Power Input**

DC 5V/3A

## **Dimensions**

45 mm (H) x 163 mm (D) x 215 mm (W)

## **Operating Temperature**

0° - 50°C

## **Storage Temperature**

-25° - 55°C

## **EMI Certification**

FCC Class A

CE Class A

VCCI Class A

C-Tick

## **Safety**

UL

CSA

TUV/GS

T-Mark



# 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 web site, or by phone.

## Tech Support for customers within the United States:

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

(877) 453-5465

6:00AM to 6:00PM PST, Monday through Friday

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

<http://support.dlink.com>

email:[support@dlink.com](mailto:support@dlink.com)

## Tech Support for customers within Canada:

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

(800) 361-5265

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

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

<http://support.dlink.ca>

email:[support@dlink.ca](mailto:support@dlink.ca)

# D-Link®

## Limited Warranty (USA only)

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© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

**FCC Statement:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. 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.