

D-Link[®]

DSA-3100

Airspot Public/Private Gateway

User Manual

Third Edition (April 2004)

Printed In Taiwan



RECYCLABLE

Table of Contents

1、 Introduction.....	1
a. Product Overview	1
b. Unpacking.....	1
c. Identifying External Components	2
1. Front Panel	2
2. Rear Panel.....	3
d. Specification	4
e. Key Features	5
2、 Installation	6
a. Requirements.....	6
b. Procedure.....	6
1. Ensure the DSA-3100 is power off.....	7
2. WAN port connection.....	7
3. Private LAN port connection.....	7
4. Public LAN port connection	7
5. Power up	7
6. Check the LED	7
c. Configure PCs on Your LAN.....	8
1. TCP/IP network setting	8
2. Internet Access Configuration	8
3、 Quick Configure.....	11
4、 System Configuration	13
a. Instruction	13
1. General Features	14
b. Home	15
1. Wizard.....	15
2. System	24
3. WAN	25
4 Public LAN	27
5. Private LAN.....	28
6. User Manager	31
c. Advanced.....	45
1. Port and IP Redirect	45
2. Pass Through	46

3. Virtual Server	47
4. DMZ	47
5. Free Surfing Area	48
6. Static Route.....	49
7. Firewall	51
d. Tools	53
1. Monitor IP List	53
2. Change Password	54
3. Upload	55
4. System	59
5. Firmware.....	60
6. Misc.	60
7. Restart.....	61
e. Status	62
1. Device Info	62
2. Interface	64
3. Current Users	66
4. Traffic History	67
f. Help	68
Appendix 1.....	73
Windows TCP/IP Setup	73
Appendix 2.....	75
Source Code.....	75

Table of Figures

1、 Introduction.....	1
Figure 1-1 Front Panel.....	2
Figure 1-2 Rear Panel	3
Figure 1-3 DSA-3100 Network View Page	5
2、 Installation	7
Figure 2-1 Connecting the DSA-3100.....	7
Figure 2-2 Control Panel	10
Figure 2-3 Internet Connection Wizard.....	11
3、 Quick Configuration.....	12
Figure 3-1 Home-Wizard Page	13
Figure 3-2 User Manager Page	13
4、 Working with Manager	14
Figure 4-1 Home-Wizard Page	14
Figure 4-2 Home-Wizard Page.....	16
Figure 4-3 Setup Wizard Page	16
Figure 4-4 Change Admin's Password	17
Figure 4-5 Choose System's Time Zone	17
Figure 4-6 Set System Information.....	18
Figure 4-7 Select the Connection Type for WAN Port.....	18
Figure 4-8 Static IP Address configuration.....	19
Figure 4-9 Dynamic IP Address configuration	19
Figure 4-10 PPPoE Client configuration.....	19
Figure 4-11 Set PPPoE Client's Information.....	20
Figure 4-12 Configure Public LAN Port.....	20
Figure 4-13 Set DHCP server information.....	21
Figure 4-14 Select Public LAN Method	21
Figure 4-15 Local User configuration	22
Figure 4-16 POP3 User configuration	22
Figure 4-17 RADIUS User configuration.....	22
Figure 4-18 LDAP User configuration	23
Figure 4-19 Setup Completed.....	23
Figure 4-20 System Configuration Page	25
Figure 4-21 Static IP Address Configuration.....	26

Figure 4-22 Dynamic IP Address Configuration	26
Figure 4-23 PPPoE Configuration	26
Figure 4-24 NAT Mode	27
Figure 4-25 NAT_IP_PNP Mode	27
Figure 4-26 Router Mode	27
Figure 4-27 DHCP Server Disable	28
Figure 4-28 DHCP Server Enable	28
Figure 4-29 DHCP Relay	29
Figure 4-30 NAT Mode	29
Figure 4-31 Router Mode	30
Figure 4-32 DHCP Disable	30
Figure 4-33 DHCP Server	31
Figure 4-34 DHCP Relay	31
Figure 4-35 User Manager Page	32
Figure 4-36 User Control	33
Figure 4-37 Guest Account	33
Figure 4-38 Guest Account List	34
Figure 4-39 Guest Account ACL	34
Figure 4-40 MAC Address Control	35
Figure 4-41a MAC ACL Control	35
Figure 4-41b MAC ACL Control	35
Figure 4-42 Default Group	36
Figure 4-43 Local Configuration	36
Figure 4-44 Local Users List	37
Figure 4-45 Add Users	38
Figure 4-46 Edit Account	38
Figure 4-47 Upload User Account	39
Figure 4-48 Receipt Information	40
Figure 4-49 On-Demand User Configuration	41
Figure 4-50 On-Demand User List	42
Figure 4-51 Local User Group Configuration	42
Figure 4-52 POP3 Configuration	43
Figure 4-53 RADIUS Configuration	43
Figure 4-54 802.1x Enable	45
Figure 4-55 802.1x Device Configuration	46
Figure 4-56 LDAP Configuration	47
Figure 4-57 Login Schedule Configuration	47
Figure 4-58 Edit Login Schedule	48

Figure 4-59	Port and Destination IP Redirection	49
Figure 4-60	Pass-Through host definition.....	50
Figure 4-61	Defining Vrtual Servers	51
Figure 4-62	Defining DMZ mappings	52
Figure 4-63	Defining Free Surfing Area Hosts	53
Figure 4-64	Sample Static Route	54
Figure 4-65	Defining Filter Rule.....	55
Figure 4-66	Edit Filter Rule.....	55
Figure 4-67	Monitor IP List.....	57
Figure 4-68	Change Password.....	58
Figure 4-69	Upload Login Page.....	59
Figure 4-70	Login page required HTML code snippet.....	59
Figure 4-71	Upload Logout Page	59
Figure 4-72	Logout page required HTML code snippet.....	60
Figure 4-73	Upload Login error Page	60
Figure 4-74	Upload Login Succeed Page	60
Figure 4-75	Upload Logout Succeed Page.....	61
Figure 4-76	System Settings.....	61
Figure 4-77	Firmware Upgrade From File.....	62
Figure 4-78	System Status	63
Figure 4-79	Interface Status	66
Figure 4-80	Current Users.....	67
Figure 4-81	Traffic History	67
Figure 4-81	Help.....	68

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning:

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

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l'utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l'utente debba assumere

1, *INTRODUCTION*

a. Product Overview

The D-Link Airspot Public/Private Gateway DSA-3100 is a simple to use network access control system. It controls access to the network at your network edge no matter it is a traditional wired Ethernet or an IEEE 802.11 wireless LAN. Even a mixed environment where wired Ethernet and WLAN co-exist could be managed.

The DSA-3100 is compatible with almost every client operating system as long as the system supports TCP/IP and a capable HTML browser such as Internet Explorer. To name a few, Windows 9x/Me/NT/2000/XP, Linux, Mac OS and Pocket PC 2000/2002 are compatible with the DSA-3100. With the single device solution provided by the DSA-3100, your network will be well guarded right at its edge.

b. Unpacking

Open the shipping carton of DSA-3100, and this carton should contain the following items:

- Airspot Public/Private Gateway DSA-3100
- CD-ROM (Containing Manual and Warranty)
- DSA-3100 Quick Installation Guide
- DSA-3100 User Manual
- Ethernet (CAT5 UTP/Straight-Through) cable x 2
- Ethernet (CAT5 UTP/Cross over) cable x 1
- Console Cable x 15V DC, 3A Power Adapter

c. Identifying External Components

1. Front Panel

Figure 1-1 Front Panel



- Power Indicator
- Status Indicator
- WAN port Indicator
- Private LAN port Indicator
- Public LAN port Indicator

Power Indicator:

The power indicator is kept bright while DSA-3100 is power on.

Status Indicator:

The Status indicator is kept bright while system ready, and it's sparking while system rebooting or firmware upgrading.

WAN port Indicator:

The WAN indicator is kept bright while you plug the cable end into a WAN port.

Private LAN port Indicator:

The Private LAN Indicator is kept bright while you plug the cable end into a Private LAN port.

Public LAN port Indicator:

The Public LAN indicator is kept bright while you plug the cable end into an Public LAN port.

The indicator ordered from left to right be for WAN, Private LAN, Public LAN and every indicator has two LED lights. When you plug the cable end into a connector port, the upper

light will light up to notify you that a link is detected on the internal interface. The lower light will be sparkling while data transmission. (Table 1-1)

Table 1-1 Monitoring Port Status

Item	Status		Description
Power light	Green		System ready
Status light	Green		System ready
	Sparkling		System rebooting or Firmware Upgrading
Link light	WAN	Green	On line
	Private LAN	Green	On line
	Public LAN	Green	On line
Activity light	WAN	Sparkling	Data transmission
	Private LAN	Sparkling	Data transmission
	Public LAN	Sparkling	Data transmission

2. Rear Panel

Figure 1-2 Rear Panel



- WAN Port
- Public LAN Port
- Private LAN Port
- DC Power Outlet
- Console Port

WAN Port:

Connect to the Unmanaged Network here. The Unmanaged Network's interface maybe is ADSL Router's LAN port, Cable Modem's LAN port or Intranet Switch.

Public LAN Port:

Connect to the Managed Network here. The Managed Network's interface maybe is a traditional wired Ethernet or an IEEE 802.11 wireless LAN. All of the users under the Public LAN Port must to login before. If they want to access any network resource.

Private LAN Port:

Connect to the PC, hub or switch to this port. Private LAN port for connecting a Trusted Network onto the DSA-3100, which permits access to WAN, and LAN from Private LAN without Public LAN, but must under the Firewall rules. You can put the Web server, Mail server or FTP server under the Private LAN Port.

DC Power Outlet:

Connect the supplied power adapter here.

Console Port:

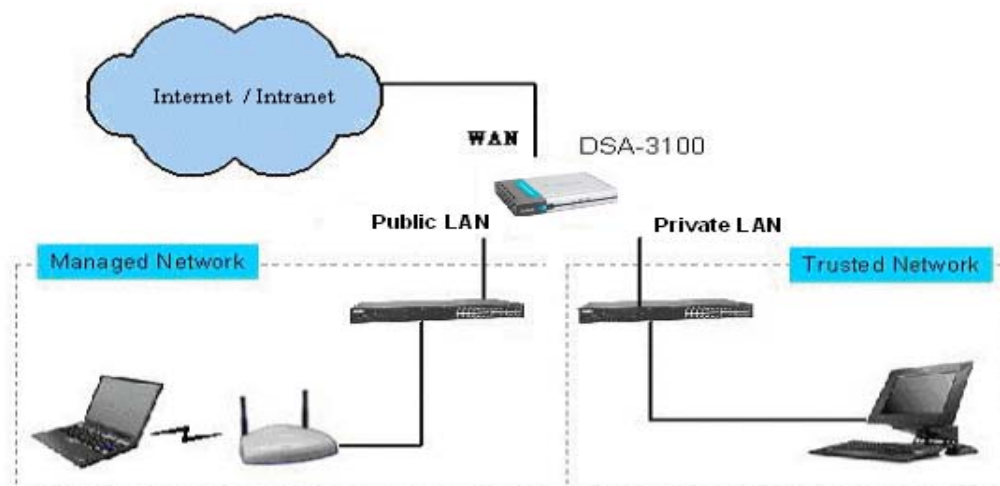
If you need to configure the admin password, please connect one PC to this port and change above items with the terminal linking applications on the PC, e.g. HyperTerminal. (96000, 8-N-1)

d. Specification

- CPU: Intel Xscale IXP420@266MHz
- System Memory:
 - 32MB DRAM
 - 16 MB Flash
- Ethernet MAC: D-Link DL10030B Ethernet 10/100Base-TX MAC+PHY
- Switch IC: ICPlus 175A
- Power: 3A/5V

e. Key Features

Figure 1-3 DSA-3100 Network View Page



- Manages up to 250 users account data with internal user account database.
- Manages up to 2000 on-demand users account data with internal on-demand user database
- Provide 5 local user groups to define different bandwidth for each local user group.
- Supports at least 50 on-line users.
- ID/Password based Public LAN and Authorization, which could be combined with MAC address locking to provide stricter access control.
- Supports POP3, RADIUS and LDAP external Public LAN mechanism. Only one of them could be chosen at once.
- Provides on-line status monitoring and history traffic data review.
- SSL protected access to the administration interface and user Public LAN interface.
- Customizable user login, logout, login success, login error, logout success web page.
- Customizable user logout timer.
- Customizable target URL for users who successfully get authorization.
- Console mode administration interface via serial console port.
- Supports NAT for managed clients.
- Supports static IP address, DHCP client and PPPoE client on WAN port interface.
- DHCP server built-in to service managed clients.
- High speed policy routing engine built-in.
- Customizable preemptory traffic redirection. (IP and Port Redirect)
- NTP client built-in.
- Provides a Private LAN port for connecting a Trusted Network onto the DSA-3100, which permits access to WAN without Public LAN.
- Supports external DSA-3100P printer to print On-demand user's ID and password. (Optional)

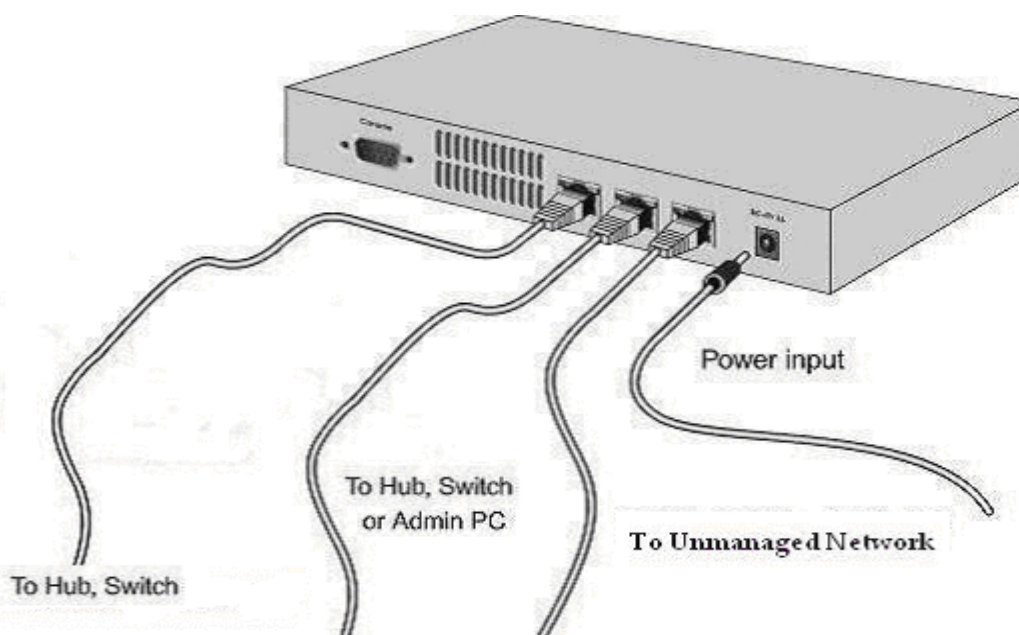
2、 INSTALLATION

a. Requirements

- Three of standard 10/100Base T network cables with RJ45 connectors.
 - TCP/IP network protocol must be installed on all PCs.
-

b. Procedure

Figure 2-1 Connecting the DSA-3100



You can follow those steps below to install the DSA-3100

1. Ensure the DSA-3100 is power off
2. WAN port connection
3. Private LAN port connection
4. Public LAN port connection
5. Power up
6. Check the LED

1. Ensure the DSA-3100 is power off.

Please check the DSA-3100 front panel power indicator is off.

2. WAN port connection

Use 10/100BaseT network cable to connect the Unmanaged Network. The Unmanaged Network's interface maybe ADSL Router's LAN port, Cable Modem's LAN port or Intranet Switch port.

3. Private LAN port connection

Private LAN port is connected to a Trusted Network without Public LAN. Use 10/100BaseT network cable to connect your Admin PC, or Web Server, Mail Server with internal Switch or Hub that connected to the Private LAN Port on DSA-3100. If you want to directly connect the DSA-3100 to this PC or the Server or the wireless AP, you have to use a Cross Over Line.

4. Public LAN port connection

Public LAN port is connected to a Managed Network with Public LAN. Use 10/100BaseT network cable to connect your Client PC with the internal Switch or Hub that connected to the Public LAN Port on DSA-3100. If you want to directly connect the DSA-3100 to this PC or the wireless AP, you have to use a Cross Over Line.

5. Power up

Connect the supplied power adapter to the DSA-3100 and power up.

6. Check the LED

The Power Indicator and WAN Indicator should be ON, if the corresponding WAN Port was connected to an Unmanaged Network.

The corresponding Private LAN or Public LAN Indicator should be ON while a network device connected to the Private LAN Port or the Public LAN Internal Port.

c. Configure PCs on Your LAN

After DSA-3100 installation, for each PC, the following procedure may need to be configured:

- TCP/IP network setting
- Internet Access configuration

1. TCP/IP network setting

If Your PC is Windows 95/98/ME/2000/XP, uses the default TCP/IP network setting, no changes need to be made. Just restart your PC.

DSA-3100 will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC starts.

For all non-Server versions of Windows, the default TCP/IP network setting is to act as a DHCP client. In Windows, it called **Obtain an IP address automatically**.

If using fixed IP Address on your LAN, or you wants to check your TCP/IP setting, refer to Appendix 1 - Windows TCP/IP Setup.

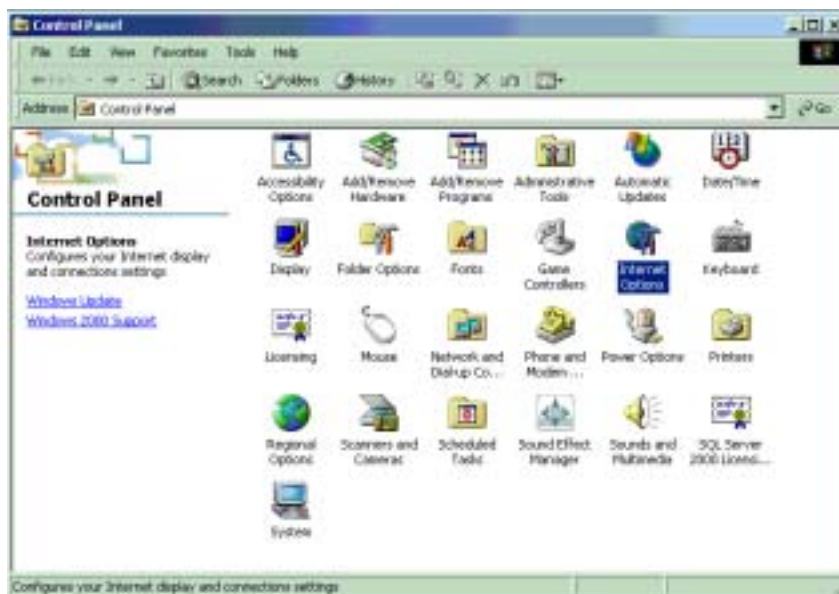
2. Internet Access Configuration

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

For Windows 9x/2000

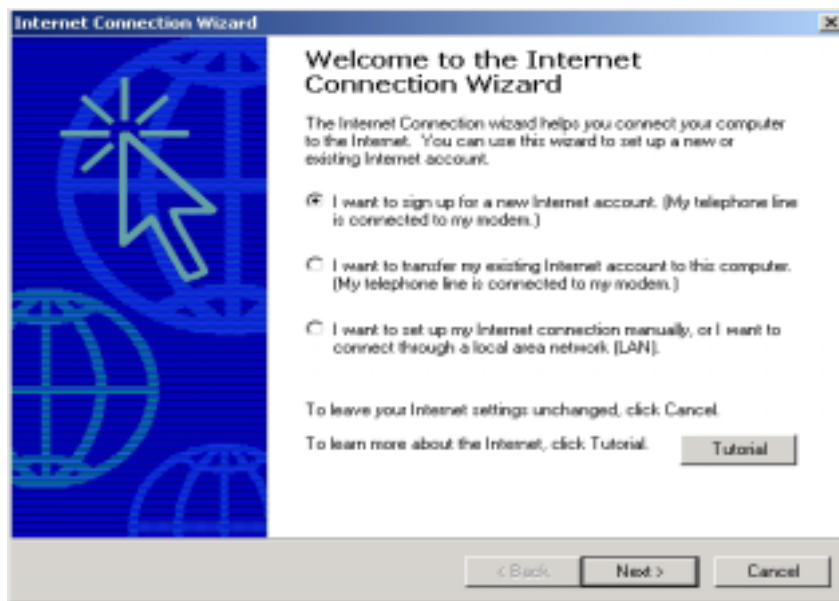
- 1、 Please select **Star Menu - Control Panel - Internet Options**.

Figure 2-2 Control Panel



2. Select the Connection tab, and click the **Setup** button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)" and click next.

Figure 2-3 Internet Connection Wizard



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

For Windows XP

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

3、 QUICK CONFIGURE

You can set up related configurations by following steps to quick configure the DSA-3100.

DSA-3100 provides 2 built-in user accounts: “admin” and “manager”

- admin: This user is the administrator in the DSA-3100.
- manager: This user has right to manager user account, the rest of function is denied.

(For **admin** quick configure)

Step1. Please ensure that system admin connects his PC to Private LAN Port of the DSA-3100, by default DSA-3100 is configurable only by PCs that are connected to Private LAN Port.

Step2. Open admin PC's browser. (Ex: Microsoft Internet Explore)

Step3. Enter <https://192.168.0.40> in the Address or Location box to connect to the Web Management Interface.

Step4. Please enter the default username: **admin** in the Username field and password: **admin** in the Password field.

Step5. Select **Home - Wizard**. You should see a screen like the following (Figure 3-1):

Step6. Click **Run Wizard** to through the process of creating a baseline Strategy. For more information, see the “Wizard” section on page 16

(For **manager** quick configure)

Step1. Please ensure that manager connects his PC to Private LAN Port of the DSA-3100, by default DSA-3100 is configurable only by PCs that are connected to Private LAN Port.

Step2. Open manager PC's browser. (Ex: Microsoft Internet Explore)

Step3. Enter <https://192.168.0.40> in the Address or Location box to connect to the Web Management Interface.

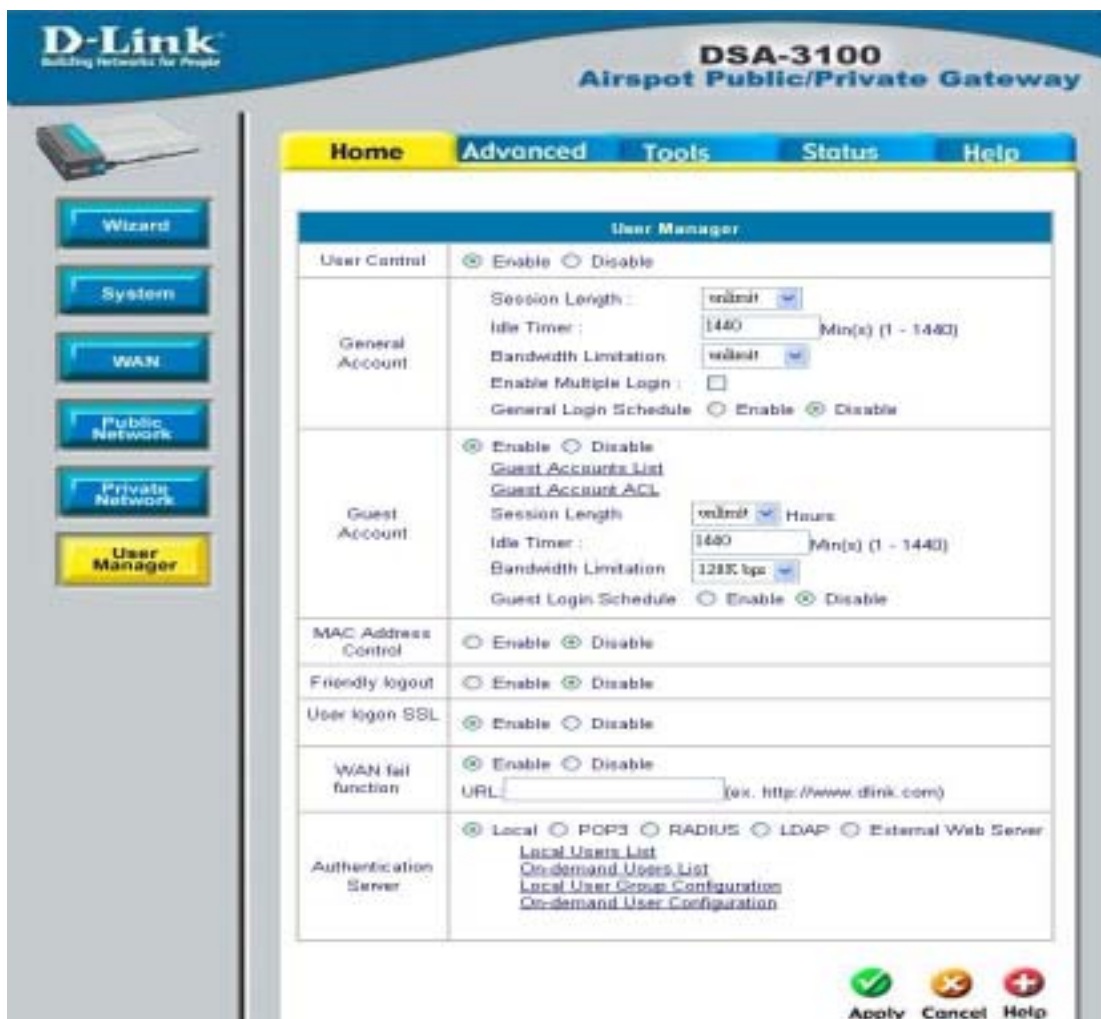
Step4. Please enter the default username: **manager** in the Username field and password: **manager** in the Password field.

Step5. You should see this page **User Manager** (Figure 3-2). For more information, see the “User Manager” section on page 39

Figure 3-1 Home - Wizard Page



Figure 3-2 User Manager Page



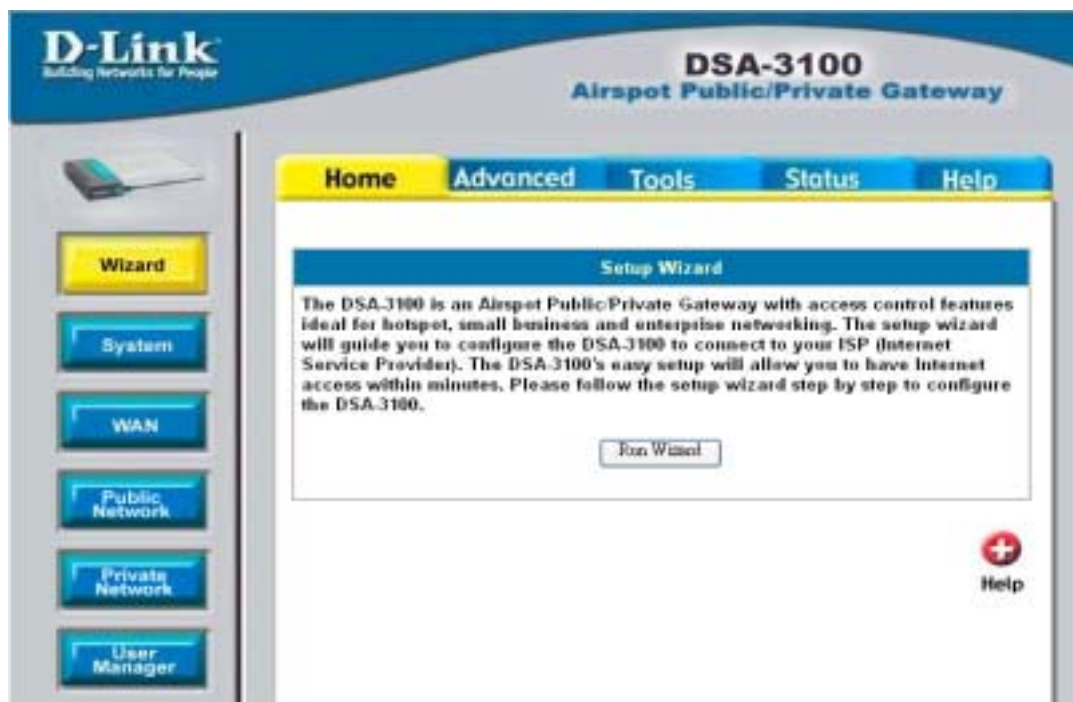
4、 SYSTEM CONFIGURATION

For using further features of DSA-3100, You have to set up related configurations by the Web Management Interface of DSA-3100.

a. Instruction

When you enter the Web Management Interface of DSA-3100, you'll find the following main features on top of the screen (Figure 4-1), such as **Home**, **Advanced**, **Tools**, **Status**, **Help**.

Figure 4-1 Home – Wizard Page



1. General Features

The DSA-3100 includes these features and functions. (See Table 4-1)

Table 4-1 DSA-3100 General Features and Functions

Features	Home	Advanced	Tools	Status	Help
Functions	Wizard	Port and IP Redirect	Monitor IP List	Device Info	
	System	Pass Through	Change Password	Interface	
	WAN	Virtual Server	Upload	Current Users	
	Public LAN	DMZ	System	Traffic History	
	Private LAN	Free Surfing Area	Firmware		
	User Manager	Static Route	Misc.		
		Firewall	Restart		

b. Home

This feature provides basic settings of the D-Link DSA-3100, including **Wizard**, **System**, **WAN**, **Public LAN**, **Private LAN** and **User Manager**.

1. Wizard

The wizard guides you through the process of creating a baseline Strategy. You can follow the wizard step by step to configure the DSA-3100. You should see a screen like the following.

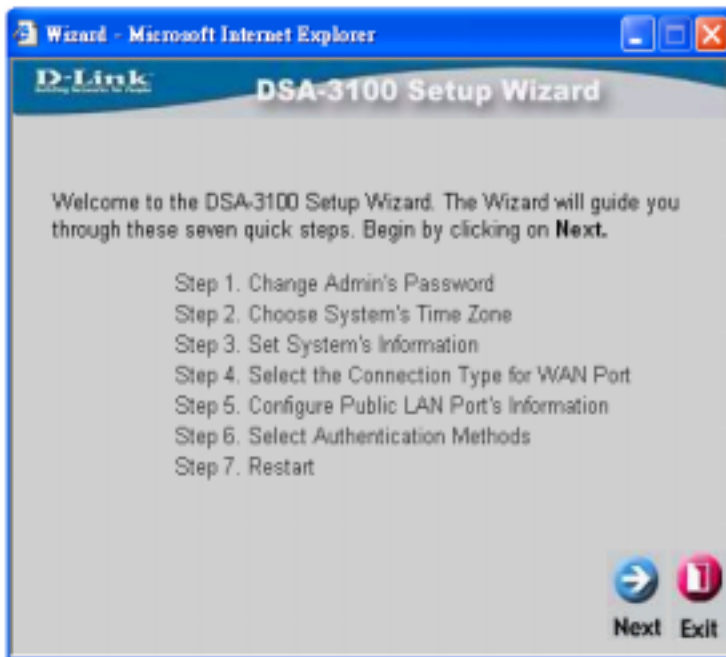
- If you want to use the setup wizard, please click **Run Wizard** on this page (Figure 4-2).

Figure 4-2 Home – Wizard Page



- The Setup Wizard will help you to finish these seven steps, please click **Next** to continue.

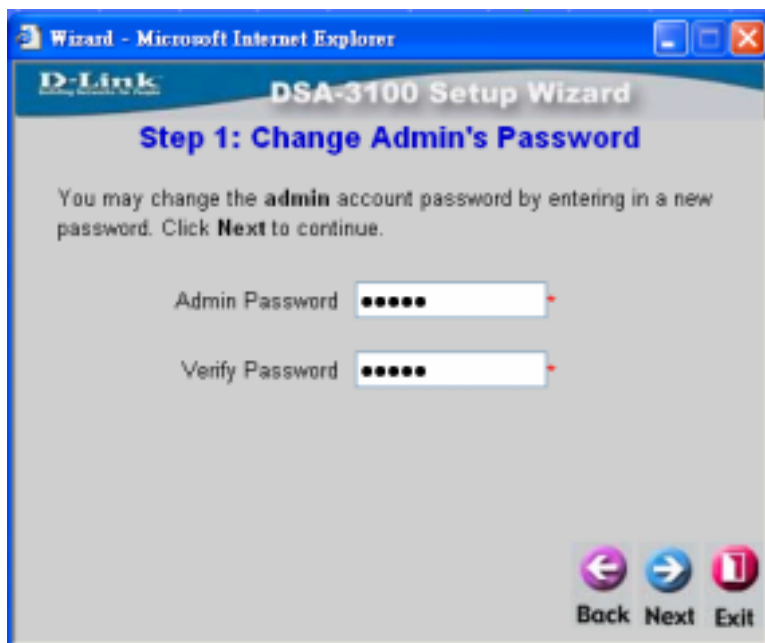
Figure 4-3 Setup Wizard Page



- Step1. Change Admin's Password

Please enter admin's **password** and **verify password**, then click **Next**.

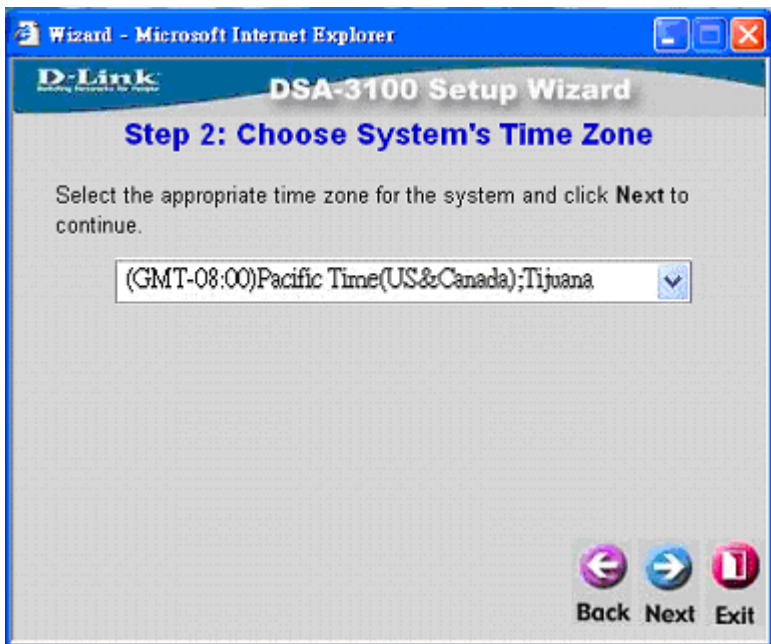
Figure 4-4 Change Admin's Password



- Step2. Choose System's Time Zone

Select the appropriate time zone for your location then click **Next**.

Figure 4-5 Choose System's Time Zone



• Step3. Set System Information

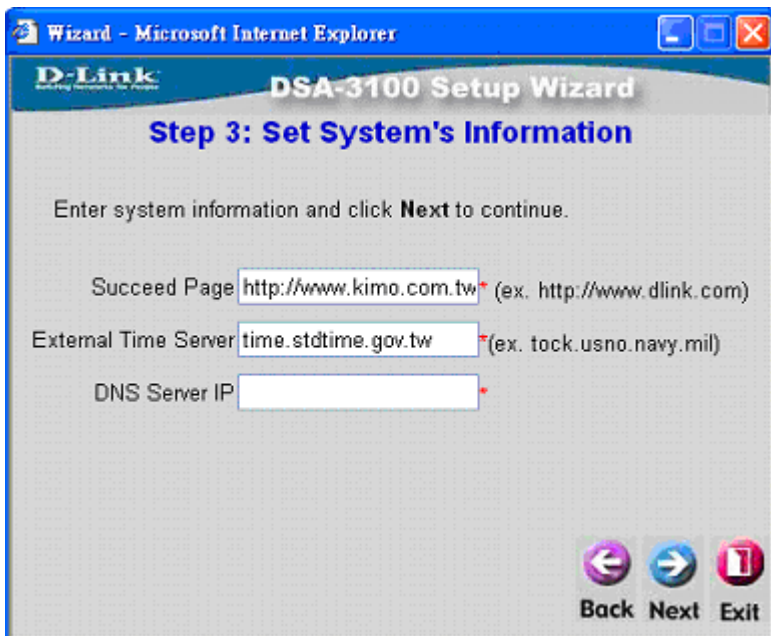
Please enter your system information, such as **Succeed Page**, **External Time Server**, **DNS Server IP** on this page, then click **Next**.

Succeed Page: Home page which will appear when user logon success.

External Time Server: Set DSA-3100 and External Time Server for clock synchronization (ex.tock.usno.navy.mil).

DNS Server IP: Domain Name Server IP address.

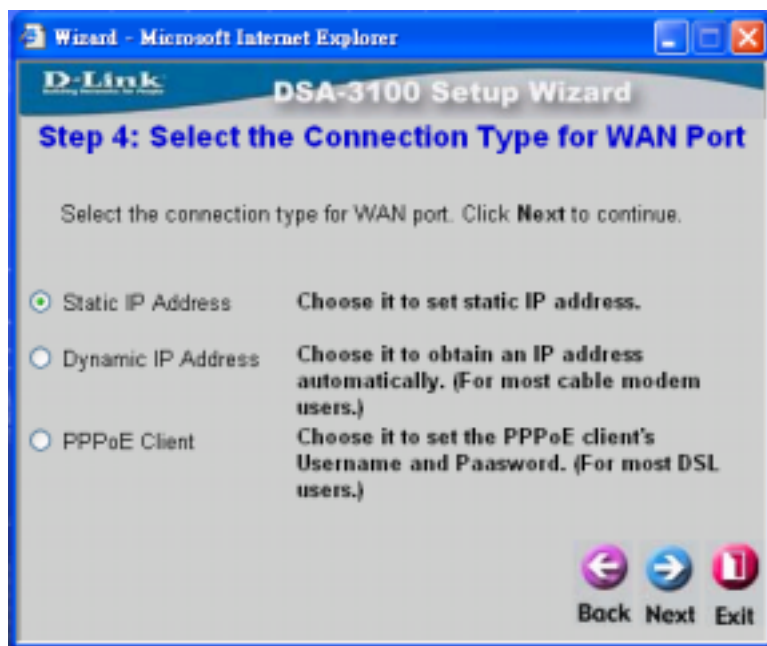
Figure 4-6 Set System Information



- Step4. Select the Connection Type for WAN Port

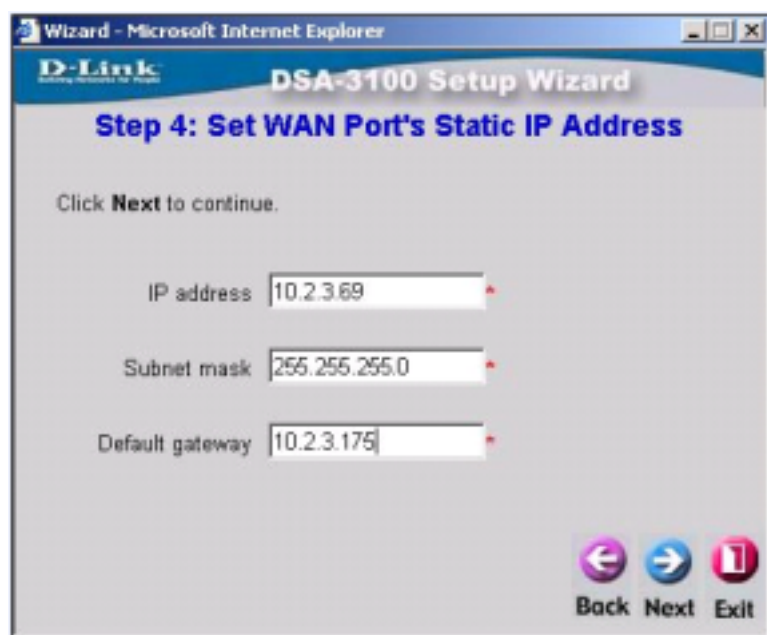
It' depends on your network environment type to select the connection type.

Figure 4-7 Select the Connection Type for WAN Port



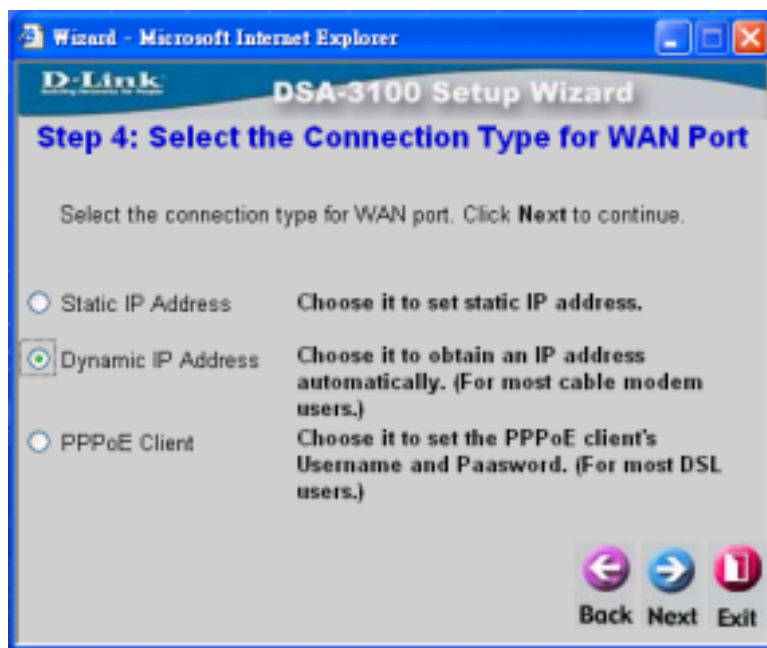
- If you want to use static IP address, please select **Static IP Address** (Figure 4-8).
- If you want to use dynamic IP, please select **Dynamic IP Address** (Figure 4-9).
- If you are xDSL user and use PPPoE to Internet, please select **PPPoE Client** (Figure 4-10, 4-11).
- When you select **Static IP Address**, please enter the **IP**, **subnet mask**, **Default Gateway** then click **Next**.

Figure 4-8 Static IP Address configuration



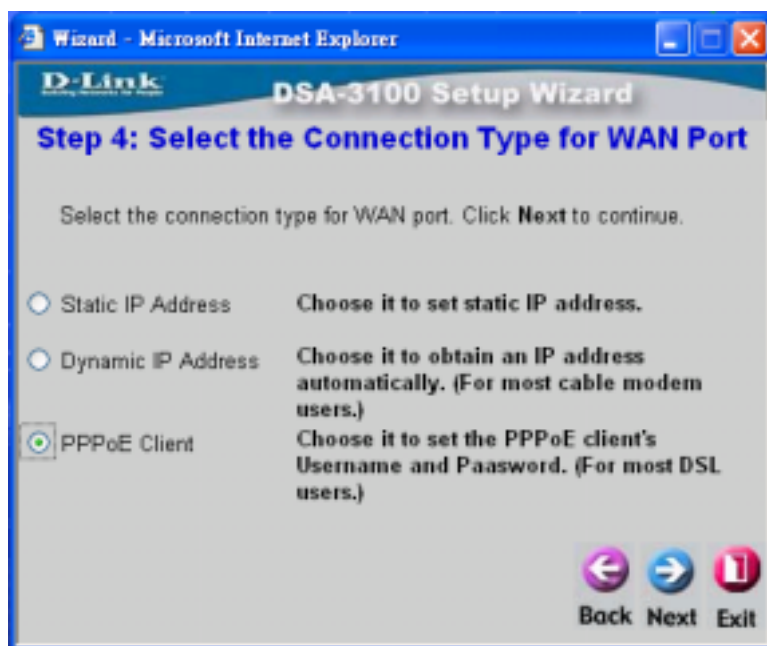
- When you select **Dynamic IP Address**, please click **Next**.

Figure 4-9 Dynamic IP Address configuration



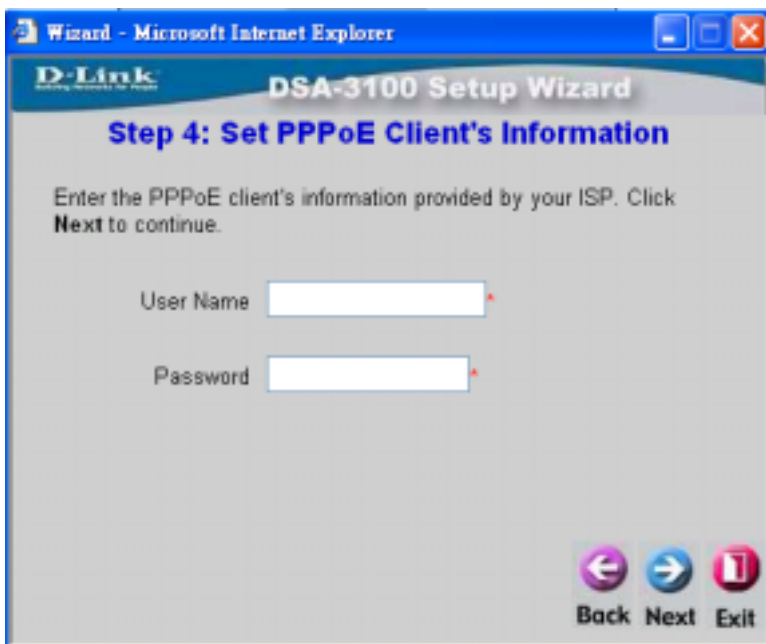
- When you select **PPPoE Client**, please click **Next**.

Figure 4-10 PPPoE Client configuration



- Please enter the PPPoE Client's **User name** and **Password** then click **Next** .

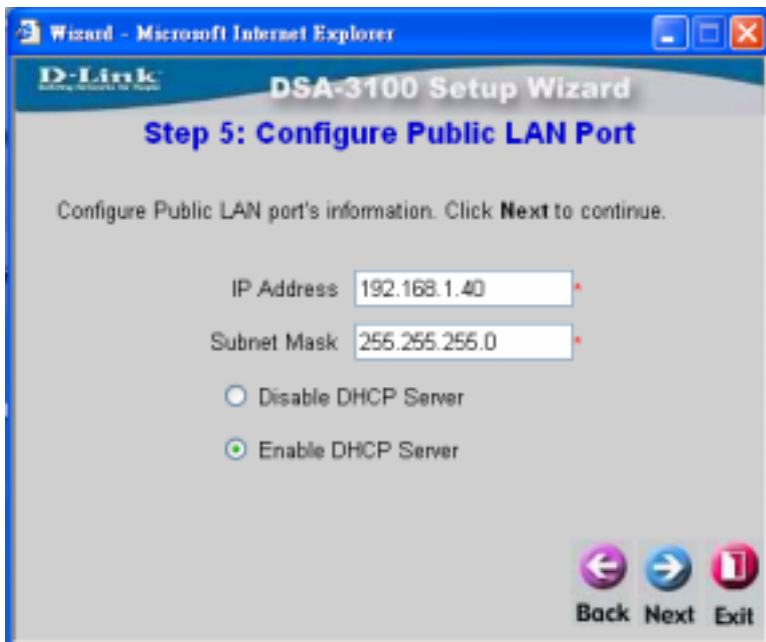
Figure 4-11 Set PPPoE Client's Information



- **Step5. Configure Public LAN Port**

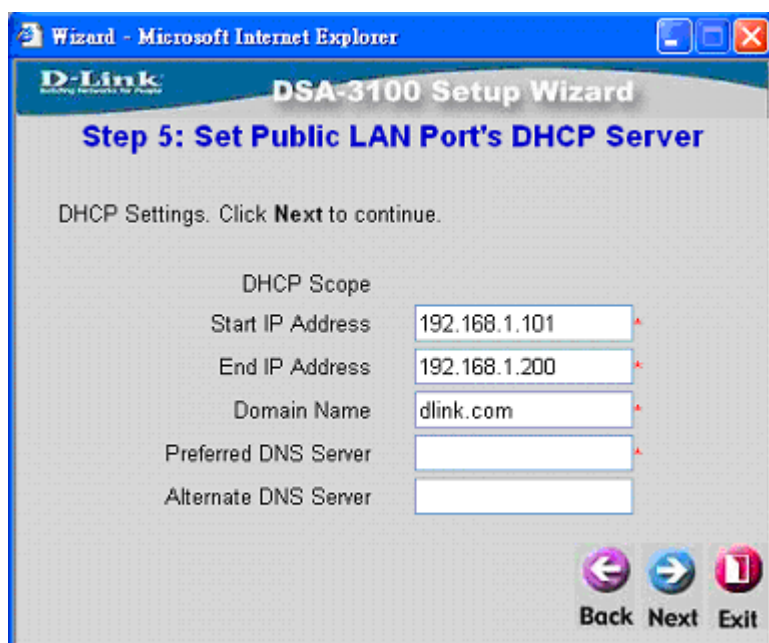
Please enter the Public LAN port's information, such as **IP address**, **Subnet Mask** and **Enable/Disable DHCP Server** on this network segment, then click **Next**.

Figure 4-12 Configure Public LAN Port



- When you select Enable DHCP Server, please enter the DHCP scope information, such as DHCP Start IP Address, DHCP End IP Address, Domain Name, Preferred DNS IP Address, Alternate DNS IP Address (Option) then click Next .

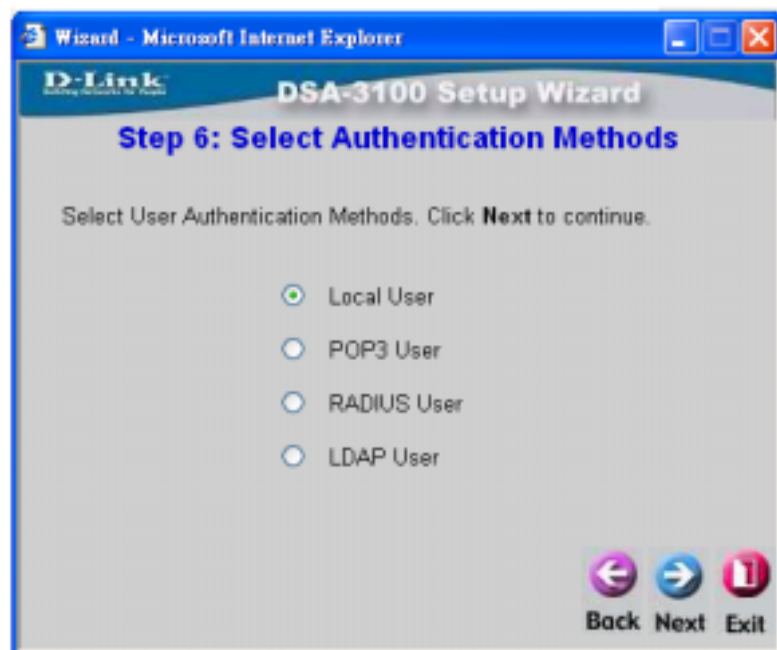
Figure 4-13 Set DHCP server information



• **Step6. Select Authentication Methods**

DSA-3100 provides four types of Authentication methods.

Figure 4-14 Select Authentication Methods



- **Local User:** User accounts are stored in the embedded database on DSA-3100.
- **POP3 User:** User accounts are stored in POP3 server.
- **RADIUS User:** User accounts are stored in RADIUS server.
- **LDAP User:** User accounts are stored in LDAP server.

Please select one, then click **Next**

- When You select **Local User**, please enter **User Name**, **Password**, **MAC** (option) and choose **Group** then click **ADD** to create one new user account. If you are finish, please click **Next** .

Figure 4-15 Local User configuration



- When You select **POP3**, please enter POP3 Server's **IP address/Domain Name** and **Server Port number** then click **Next**.

Figure 4-16 POP3 User configuration



- When You select **RADIUS**, please enter RADIUS Server's **IP address/Domain Name**, **Public LAN Port number**, **Accounting Port number**, **Secret Key**, **Accounting Service**, **Public LAN Method**, then click **Next**.

Figure 4-17 RADIUS User configuration

Wizard - Microsoft Internet Explorer

D-Link DSA-3100 Setup Wizard

Step 6: Authentication Method-RADIUS

Configure RADIUS Server information. Click **Next** to continue.

RADIUS Server (Domain Name/IP address)

Authentication Port (Default:1812)

Accounting Port (Default:1813)

Secret Key

Accounting Service

Authentication Method

← Back Next → Exit

- When You select **LDAP**, please enter LDAP Server's **IP address/Domain Name**, **Server Port number** then click **Next** .

Figure 4-18 LDAP User configuration

Wizard - Microsoft Internet Explorer

D-Link DSA-3100 Setup Wizard

Step 6: Authentication Method-LDAP

Configure LDAP Server information. Click **Next** to continue.

LDAP Server (Domain Name/IP address)

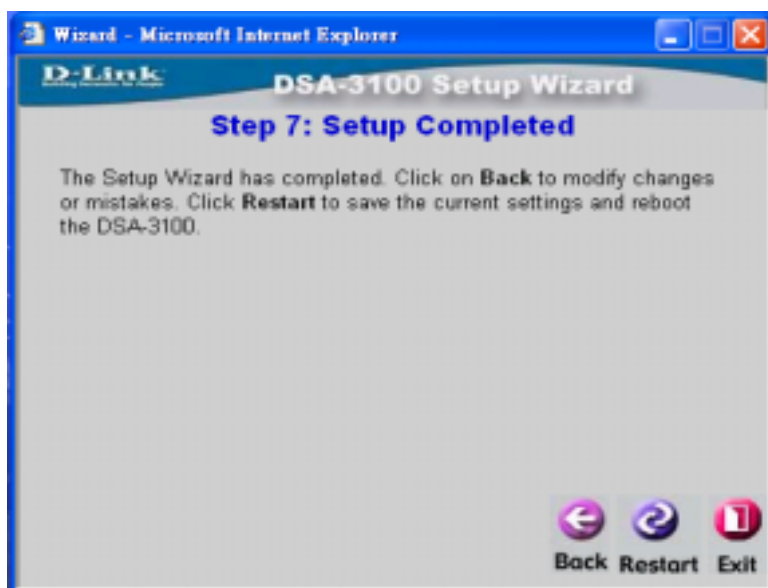
Server Port (Default:389)

Base DN
(CN=Users,DC=dlink,DC=com)

← Back Next → Exit

- **Step7. Setup Completed.** Please click **Restart** to reboot your DSA-3100.

Figure 4-19 Setup Completed



2. System

Table 4-2 lists the System Configure Page Field and Description that helps you can easy setup **System Configure** (Figure 4-20), and don't forget to click **Apply** to enable this function

Table 4-2 System Configuration Page Field and Description

Field	Description
System Name	Name of this facility, DSA-3100 is the default.
Admin Detail	The system administrator's information, for instance his name, phone number, and e-mail, etc. If a user encounters problem connecting to WAN Port of DSA-3100, system admin information will be shown on user login page.
Succeed Page	Enter a URL for all users to be directed to after successful login, usually defined as the home page of a corporation, for instance: http://www.dlink.com . No matter which URL a user originally attempts to connect, he/she will be directed to the URL defined here

Time	The DSA-3100 supports the NTP protocol. You must specify a time server's for DSA-3100. The time zone of the DSA-3100 internal clock is UTC (Coordinated Universal Time, formerly know as GMT, Greenwich Mean Time)
DNS Server	Specify DNS servers for DSA-3100, can be Preferred DNS server (Primary) and Alternate DNS server (Secondary).

Figure 4-20 System Configuration Page

System Configuration	
System Name	DSA-3100
Admin Detail	
Succeed Page	http://www.dlink.com *(ex. http://www.dlink.com)
Time	Device Time : 2004/05/03 19:54:10 <input checked="" type="radio"/> Enable NTP NTP Server tock.usno.navy.mil *(ex. tock.usno.navy.mil) Time Zone (GMT-08:00)Pacific Time(US&Canada);Tijuana <input type="radio"/> Set Device Date and Time
DNS Server	Primary DNS Server 168.95.1.1 * Secondary DNS Server

Note: After changing configuration information, you had better restart the DSA-3100 to ensure proper system operation with the new configuration.

3. WAN

WAN : The DSA-3100 offers three ways for WAN to obtain IP address:

Static IP Address: Manually specify WAN Port IP address, Subnet mask, Default Gateway. Suitable when WAN Port cannot automatically obtain an IP address.

Figure 4-21 Static IP Address Configuration

Interface Configuration -- WAN

Static IP Address

IP address

Subnet mask

Default Gateway

Dynamic IP Address

PPPoE Client

Dynamic IP Address: Suitable when WAN Port can automatically obtain an IP address; for instance when a DHCP Server is in the network connected to WAN Port. You can click the **Renew** button to renew the IP configuration.

Figure 4-22 Dynamic IP Address Configuration

Interface Configuration -- WAN

Static IP Address

Dynamic IP Address

PPPoE Client

PPPoE Client: If you are xDSL user and use PPPoE to Internet, please select **PPPoE**, then you must enter **User Name** and **Password**. The Maximum Idle Time and Dial on demand are optional.

Figure 4-23 PPPoE Client Configuration

Interface Configuration -- WAN

Static IP Address

Dynamic IP Address

PPPoE Client

User Name

Password

Maximum Idle Time Minutes

Dial on demand Enable Disable

4 Public LAN

Public LAN : Select one of the Public LAN modes and specify IP address, Subnet Mask then depend on your request, enable or disable DHCP Configuration.

- **Mode:** The DSA-3100 comes with three Public LAN modes, namely NAT, NAT_IP_PNP and Router.

NAT mode: All outbound IP addresses (the addresses must belong to the network connected to Public LAN Port) on Public LAN Port will be translated to the IP address of WAN Port to proceed.

Figure 4-24 NAT Mode

Interface Configuration -- Public LAN	
Mode	NAT
IP Address	192.168.1.40
Subnet Mask	255.255.255.0

NAT_IP_PNP mode: The clients can use any IP address to connect to DSA-3100. No matter what's the client IP address, they can get the DSA-3100's Login page and access the Internet correctly.

Figure 4-25 NAT_IP_PNP Mode

Interface Configuration -- Public LAN	
Mode	NAT_IP_PNP
IP Address	192.168.1.40
Subnet Mask	255.255.255.0

ROUTER mode: All outbound IP addresses on Public LAN Port will retain their Addresses; DSA-3100 functions as a router in this mode.

Figure 4-26 Router Mode

Interface Configuration -- Public LAN	
Mode	ROUTER
IP Address	192.168.1.40
Subnet Mask	255.255.255.0

- **DHCP Configuration:** Configure DHCP Server on Public LAN Port. The DSA-3100 comes with three DHCP Server options (as shown below):

Disable DHCP Server: Inactivate DHCP Server.

Enable DHCP Server: Activate DHCP Server. DHCP Server needs to be configured properly for successful activation. Related configuration items includes: DHCP Pool Start IP Address, DHCP Pool End IP Address, Lease Time, Domain Name, WINS IP Address, Primary DNS server IP Address, Secondary DNS server IP address.

Enable DHCP Relay: In DHCP Relay mode. It is required to specify other DHCP Server IP addresses to select this mode.

Figure 4-27 DHCP Server Enable

Interface Configuration -- Public LAN		
Mode	NAT_IP_PNP ▾	
IP Address	192.168.1.40 *	
Subnet Mask	255.255.255.0 *	
DHCP Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server	
	DHCP Pool Start IP Address	192.168.1.101 *
	DHCP Pool End IP Address	192.168.1.200 *
	Lease Time	1 Day ▾
	Domain Name	dlink.com *
	WINS IP Address	
	Primary DNS Server	
	Secondary DNS Server	
	<input type="radio"/> Enable DHCP Relay	

5. Private LAN

Private LAN: Select one mode for Private LAN Port and specify IP address, Subnet Mask, then depend on your request, enable or disable DHCP Configuration.

- **Mode:** The DSA-3100 comes with two Private LAN Port modes, namely NAT and Router.

NAT mode: All outbound IP addresses (the IP addresses must belong to the network connected to Private LAN Port) on Private LAN Port will be translated to the IP address of WAN Port to proceed.

Figure 4-28 NAT Mode

Interface Configuration -- Private LAN	
Mode	NAT
IP Address	192.168.0.40
Subnet Mask	255.255.255.0
DHCP Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

ROUTER mode: All outbound IP addresses on Private LAN Port will retain their addresses; DSA-3100 functions as a router in this mode.

Figure 4-29 Router Mode

Interface Configuration -- Private LAN	
Mode	ROUTER
IP Address	192.168.0.40
Subnet Mask	255.255.255.0
DHCP Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

- **DHCP Configuration:** Configure DHCP Server on Private LAN Port. The DSA-3100 comes with three DHCP Server options (as shown below):

Disable DHCP Server: Inactivate DHCP Server.

Enable DHCP Server: Activate DHCP Server. DHCP Server needs to be

configured properly for successful activation. Related configuration items includes: DHCP Pool Start IP Address, DHCP Pool End IP Address, Lease Time, Domain Name, WINS IP Address, Preferred DNS server IP Address, Alternate DNS server IP address.

Enable DHCP Relay: In DHCP Relay mode. It is required to specify other DHCP Server IP address to select this mode.

Figure 4-30 DHCP Server

Interface Configuration -- Private LAN	
Mode	NAT
IP Address	192.168.0.40
Subnet Mask	255.255.255.0
DHCP Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server 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 * Secondary DNS server <input type="radio"/> Enable DHCP Relay

Note: The Private LAN IP address must be set to enable network access between the DSA-3100 and managed client devices. The built-in DHCP server could be enabled or not. It is recommended that a DNS server be specified to provide the DSA-3100 and clients complete networking parameters. If you have another network that you want to connect to the DSA-3100 to facilitate its network services, you could connect that network to the Private LAN interface of the DSA-3100. Devices connected to Private LAN interface gain access to the network without Public LAN.

Note: After changing configuration information, you had better restart the DSA-3100 to ensure proper system operation with the new configuration.

6. User Manager

User Manager: It's provides User Control, Group Account, MAC Address Control, Default Group, Management Type and Login Schedule

Figure 4-31 User Manager Page

User Manager	
User Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
General Account	Session Length : <input type="text" value="unlimit"/> <small>▼</small> Idle Timer : <input type="text" value="10"/> Min(s) (1 - 1440) Bandwidth Limitation <input type="text" value="64K bps"/> <small>▼</small> Enable Multiple Login : <input type="checkbox"/> General Login Schedule <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Guest Account	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Guest Accounts List Guest Account ACL Session Length <input type="text" value="unlimit"/> <small>▼</small> Hours Idle Timer : <input type="text" value="3"/> Min(s) (1 - 1440) Bandwidth Limitation <input type="text" value="64K bps"/> <small>▼</small> Guest Login Schedule <input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Address Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Friendly logout	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User logon SSL	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WAN fail function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
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 Local Users List On-demand Users List Local User Group Configuration On-demand User Configuration

- **User Control** : When User Control is disabled, only activate **MAC Address Control** function. .
- **General Account**: Define Session Length, Idle Timer, Bandwidth limitation, Multiple Login and General Login Schedule.
 - 1.) Session length: Limit the duration for each session established by General Account, from 5 min~12 hours.
 - 2.) Idle Timer: When enabled, on-line users with no network activity after the specified period will be logged out automatically. The period can range from 1~1440, with 10 minutes as the default value.
 - 3.) Bandwidth Limitation: Limit the outbound traffic bandwidth for each session established by Guest Account. There is no limit to the duration by default
 - 4.) Enable Multiple Login: Check this function to allow a single user account to log into the system multiple times.
 - 5.) General Login Schedule: Define the time where DSA-3100 is located and login duration for General accounts. Select **Enable - Edit** to enter the management interface (Please refer to the below table). After durations are defined, you need to click **Apply**, and then **Save All** to let the new functions take effect.

Note: *To let the functions take effect, you need to click **Apply**, and then **Save All** after Enable is selected.*

Figure 4-32 Edit Login Schedule

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"/>

- **Guest Account:** Select **Enable** to activate Guest Account for visitors.

Guest Accounts List: Up to 10 guest accounts could be defined. To activate a particular Guest Account, simply enter the corresponding password in the “Password” column and click **Apply**, and then **Save All**.

Guest Account ACL: Define network areas where Guest Account is disallowed access, for instance 10.2.3.0/24, Network ID is 10.2.3.0, Subnet Mask is 255.255.255.0.

Please refer to the definition of Session Length, Idle Timer, Bandwidth Limitation and Guest Login Schedule as described above for General Account.

Note: To let the functions take effect, you need to click **Apply**, and then **Save All** after **Enable** is selected.

- **MAC Address Control:** When MAC Address Control is enabled, users connected to Public LAN Port cannot login to DSA-3100 unless they have registered their MAC Address at MAC ACL Control (Figure 4-33a, 4-33b). In other words, only 40 users will be allowed to login when this function is enabled. Please refer to configuration screen as follows.

Figure 4-33 MAC Address Control

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

Note: MAC address format is **XX:XX:XX:XX:XX:XX** or **XX-XX-XX-XX-XX-XX**. Newly created user account will be valid instantly. Restart of the DSA-3100 is not necessary (as shown below).

Figure 4-33a MAC ACL Control

MAC ACL Control			
No.	MAC Address (XX:XX:XX:XX:XX:XX)	No.	MAC Address (XX:XX:XX:XX:XX:XX)
1	11:22:33:44:55:66	2	33:44:55:66:77:88
3		4	
5		6	

Figure 4-33b MAC ACL Control

35	<input type="text"/>	36	<input type="text"/>
37	<input type="text"/>	38	<input type="text"/>
39	<input type="text"/>	40	<input type="text"/>

MAC ACL Control modify success.



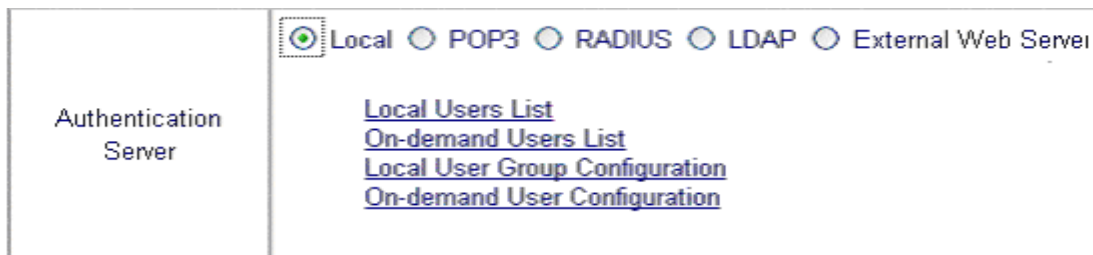
Note: To let the functions take effect, you need to click **Apply**, and then **Save All** after **Enable** is selected.

- **Friendly logout:** It relates to the pop up windows that will appear when user login success. If you enable it, while you close the pop up window, it will ask you “do you want to logout? ”, otherwise it doesn’t ask you “do you want to logout?”
- **User Logon SSL:** enable user to choose from activating https (encryption), or http (non encryption) as login page.
- **WAN Fail Function:** Provide a definable URL link for detection Internet connection. When Internet connection fail is detected, then an error page will display unit the abnormal status is recovered.
- **Authentication Server :** Support multiple user Public LAN methods including **Local, POP3 Server, RADIUS Server, LDAP Server and External Web Server.**

Note: To let the functions take effect, you need to click **Apply**, and then **Save All** after **Management Type** is selected.

1.) **Local:** User accounts are stored in the embedded database on DSA-3100.

Figure 4-34 Local Configuration




(1) **Local User List:** A list of all local user accounts that stored in the embedded database for user account management. You can add, edit, and delete users. A sample list is shown below.

Figure 4-35 Local Users List

Local Users List				
User Name	MAC	Group	Delete	Delete All
mix		group4	<input type="checkbox"/>	<input type="checkbox"/>

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


Back

To delete specific users accounts, click on the checkboxes besides those user accounts then click the **Delete** button. To delete all user accounts, click **Delete All**.

Add Users: Create new accounts, including Username (mandatory), Password (mandatory), and MAC (optional) and assign to a user group, as shown below.

Note: To let the functions take effect, you need to click **Apply**, and then **Save All** after new accounts are created

Figure 4-36 Add Users

Add Users				
No	User Name	Password	MAC (XX:XX:XX:XX:XX:XX)	Group
1				group1 ▾
2				group1 ▾
3				group1 ▾
4				group1 ▾
5				group1 ▾
6				group1 ▾
7				group1 ▾
8				group1 ▾
9				group1 ▾
10				group1 ▾

Edit Account: The figure below display User Name, Password, MAC, Group that you can modify while you click the user account on the User Name field.

Figure 4-37 Edit Account

Edit Account	
User Name	<input type="text" value="mix"/>
Password	<input type="password"/> <i>*Please leave the field blank, if you don't want to change password.</i>
MAC	<input type="text"/>
Group	<input type="text" value="group4"/> ▼

Upload User Accounts:

Besides adding user accounts one by one through the web interface, you could prepare a text file, which contains user account information, and upload it to the DSA-3100. As the below figure shows. The DSA-3100 provides you a way to upload user account data. The user account data file is a text file. Each line of the text file contains one user account data. Each line is of the 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.

Caution: *When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will be replaced by the new ones. Other existing accounts are not affected.*

Figure 4-38 Upload User Account

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

Refresh: To display the latest user list, just click **Refresh** to get that information.

On-demand user: When you connect the DSA3100P to the DSA-3100's console port, there is 2000 On-demand users could be used. By default, the On-demand user database is empty. While you press the DSA-3100P's button, the On-demand user will be create, then printing a receipt which will contain this On-demand user's information.

Figure 4-39 Receipt 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!

1999
```

(2) **On-demand Users List:** A list about on-demand user. A sample list is shown below.

Figure 4-40 On-Demand User List

On-demand Users List						
User Name	Password	Expiration Date	Session Length	Status	Delete	Delete All
(Total:0) First Prev Next Last						



Back

To delete specific users accounts, click on the checkboxes besides those user accounts then click the **Delete** button. To delete all user accounts, click **Delete All**.

(3) **Local User Group Configuration:** DSA-3100 provides 5 local user groups; each group can be set different outbound traffic bandwidth. A sample list is shown below.

Figure 4-41 Local User Group configuration

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"/> ▼
2	<input type="text" value="group2"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> ▼
3	<input type="text" value="group3"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> ▼
4	<input type="text" value="group4"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> ▼
5	<input type="text" value="group5"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/> ▼

(4) **On-demand User Configuration:**

Table 4-3 On-demand user Page Field and Description

Field	Description
Store Name	You can specify the prefix of the user name, max is 8 char., for example: D-Link.
Account Range	You can specify the max user amount, max is 2000
Receipt Header	You can configure the receipt's header in this filed.
Receipt Footer	You can configure the receipt's header in this filed.
Printer baud rate	You can specify the baud rate to support specific printer, which provide from D-Link. The default setting is 9600.

Account expires after ___ days	You can specify the expires day in this filed, If this user account is not login (first time), and time is expired, this user account will not be use anymore.
Session expire after ___ minutes	You can specify how long will this account can use when he (she) login successful.
Idle timer	You can specify the idle duration in this field.
WLAN ESSID	You can specify the AP's ESSID in this filed.
WEP Key	You can specify the AP's WEP key in WEP Key filed.
Price	You can specify the price in this filed.

Figure 4-42 On-Demand User Configuration

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
Logout 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)

2.) **POP3:** To use POP3 as the Public LAN method, just 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. However, it is recommended that you restart the DSA-3100 after these changes if there is any on-line user.

Figure 4-43 POP3 Configuration

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" value="mail.cipherium.com.tw"/>
	Server Port <input type="text" value="110"/>

3.) **RADIUS:** To use RADIUS as the Public LAN 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. However, it is recommended that you restart the DSA-3100 after these changes if there is any on-line user.

Figure 4-44 RADIUS Configuration

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
	Primary Server
	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"/>
	Secondary Server
	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"/>	

802.1x: DSA-3100 support integrated single sign-on when using combine with the 802.1x enabled APs. By using the integrated RADIUS proxy function in DSA-3100, users can use the EAP methods such as EAP-MD5 or EAP-TLS to login and get the service depending on the Public LAN methods which the backend RADIUS server and APs support.

The assumption is that user had configured a EAP enabled RADIUS server like Microsoft Internet Public LAN Service on Windows 2000 or .NET Server 2003. If EAP-TLS is required for the dynamic key exchange, a CA integrated with Microsoft Active Directory or an external trusted CA is also required. Of course the user should get the certificate from the CA before he/she connects to the Wireless LAN.

We suggest the system administrator perform the Public LAN test and make sure everything is correct before you connect the network to DSA-3100.

Note: *The function of 802.1x can only be enabled when the user Public LAN method was set to "RADIUS"*

There are some settings should be configured at these three components in the network:

- RADIUS server:

System administrator should create a client account for DSA-3100 first and define the required secret (We suggest you to use the one differ than the ones APs using).

- DSA-3100:

Please select the manual in "Home->User Management" then select the Public LAN method to "RADIUS".

- Access Points:

Please specify the Primary and Secondary RADIUS server IP address (Some APs may have different wording such as IAS server or Public LAN server etc.) to the IP address of "Public LAN" port on DSA-3100.

The corresponding secrets for each AP should match the settings in DSA-3100 just as the values, as shown in sample figure below:

Figure 4-45 802.1x Device Configuration

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"/>

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

4.) **LDAP:** To use LDAP as the Public LAN method, just 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. However, it is recommended that you restart the DSA-3100 after these changes if there is any on-line user.

Figure 4-46 LDAP Configuration

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"/>

5.) **External Web Server:** Not only the 5 authentication methods as described above, but DSA-3100 can also support external web server (including database), enable user to put the login page on external web server and change the login page anytime as per customer's requirement.

Figure 4-47 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"/>			

Protocol: Choose from http or https.

Server IP: External Web server IP.

Server Port: External Web server Port number.

Login Page: Login page location.

Logout Page: Logout page location.

c. Advanced

This feature provides several functions for various network traffic manipulation tasks, including **Port and IP Redirect, Pass Through, Virtual Server, DMZ, Free Surfing Area, Static Route and Firewall.**

1. Port and IP Redirect

Up to 10 sets of traffic redirection criteria could be defined through this interface. Specify the Service Name to identify the type of traffic.

Clients who try to access a specific destination that matches one of the defined destinations will be enforced to a matching redirection target. These settings will take effect immediately after you click the **Apply** button

Figure 4-48 Port and Destination IP Redirection

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

2. Pass Through


While each client should be managed, it is sometimes desired to have some exception. For example, servers in the managed network might be given access to the network without user intervention. To allow some clients unmanaged access, specify their IP addresses or MAC addresses on the interface. See (Figure 4-49) for a look at the interface. Up to 20 IP addresses and 10 MAC addresses could be assigned unmanaged access. MAC address format is **XX:XX:XX:XX:XX:XX**.

Caution: Allowing unmanaged access from specific IP addresses or MAC addresses could introduce security hole.

Figure 4-49 Pass-Through host definition

Pass through IP & MAC Configuration			
No.	IP Address	No.	IP Address
1	<input type="text" value="192.168.1.25"/>	2	<input type="text" value="192.168.1.26"/>
3	<input type="text" value="192.168.1.27"/>	4	<input type="text" value="192.168.1.28"/>
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"/>
No.	MAC Address	No.	MAC Address
1	<input type="text" value="11:22:11:33:11:44"/>	2	<input type="text" value="22:33:44:11:22:33"/>
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"/>





Apply Cancel Help




Setting is applied and effective now.

3. Virtual Server

This feature allows you to define up to 10 virtual servers to enable access to servers connected to Public LAN and Private LAN Port from outside of the managed network. Depending on the service provided, the service might run on TCP ports, UDP ports or both. It's also providing the checkbox to enable or disable for each rule. Changes to the settings of virtual servers will take effect immediately after you click the **Apply** button.

Figure 4-50 Defining Virtual Servers

Virtual Server Table					
No.	External Service Port	Local Server IP Address	Local Service Port	Type	Enable
1	80	192.168.1.45	80	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="checkbox"/>
2				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

Apply Cancel Help

Note: Each local server connected to Public LAN Port must also be allowed for IP or MAC address pass-through. Please enter its IP or MAC address via the interface shown in.

4. DMZ

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 Address) and WAN side (Public IP Address). The WAN interface will bind the extra public IP addresses automatically.

Figure 4-51 Defining DMZ mappings

DMZ		
No.	Private IP Address	Public IP Address
1	<input type="text" value="192.168.0.10"/>	<input type="text" value="203.19.112.20"/>
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"/>

5. Free Surfing Area

To allow users access to a few sites before they log in, enter the IP addresses or domain name of those sites in the Free Surfing Area list. Up to 20 sites could be defined. The Free Surfing Area feature allows you to provide free services to users. For example, a web site that provides introduction and guidance for local facilities and routes could be listed in the Free Surfing Area. Guest users of the network could not access other parts of the network but could still connect to the Free Surfing Area and get precious information of local facilities. It could also be used for providing users free experience of the network service. Customers get real service instead of prepared demonstration.

Figure 4-52 Defining Free Surfing Area Hosts

Free Surfing Area			
No.	IP Address / Domain Name	No.	IP Address / Domain Name
1	<input type="text" value="www.dlink.com"/>	2	<input type="text" value="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"/>

6. Static Route

In the above 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. The following settings show the DSA-3100's static route configurations.

Following settings show the DSA-3100's static route configurations:

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.

Figure 4-53 Sample Static Route

Static Route			
No.	Destination		Gateway
	Network ID	Subnet Mask	IP Address
1	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
2	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
3	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
4	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
5	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
6	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
7	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
8	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
9	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>
10	<input type="text"/>	255.255.255.255 (β2) ▼	<input type="text"/>

Note : For the static route to work, the next hop route must also have added a static route to forward all 192.168.0.0/24 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 Save Setting function, and restarts D-Link DSA-3100.

7. Firewall

Click the Filter Rule index button to enter the firewall Page for each filter. The following explains each configurable item in detail.

Figure 4-54 Defining Filter Rule

IP Filter / Firewall						
Filter Rule	Active	Action	Name	Source	Destination	Protocol
1	<input checked="" type="checkbox"/>	Block	AU-LN Disallow	ANY	ANY	ALL
2	<input type="checkbox"/>	Block		ANY	ANY	TCP
3	<input type="checkbox"/>	Block		ANY	ANY	TCP
4	<input type="checkbox"/>	Block		ANY	ANY	TCP
5	<input type="checkbox"/>	Block		ANY	ANY	TCP
6	<input type="checkbox"/>	Block		ANY	ANY	TCP
7	<input type="checkbox"/>	Block		ANY	ANY	TCP
8	<input type="checkbox"/>	Block		ANY	ANY	TCP
9	<input type="checkbox"/>	Block		ANY	ANY	TCP
10	<input type="checkbox"/>	Block		ANY	ANY	TCP

Rule: Filter Rule is a set of filter that determines whether traffic will be allowed to pass between the Source and Destination or whether it will be dropped. To display the detail, click **index number**.

Figure 4-55 Edit Filter Rule

IP Filter / Firewall > Edit Filter Rule			
Rule: 1			
Name:	<input type="text" value="PubLN-PriLN Disallow"/>	<input checked="" type="checkbox"/>	Check to enable this rule
Action:	<input type="text" value="Block"/>	Protocol	<input type="text" value="ALL"/>
Source MAC:	<input type="text"/>		
	IF	Address	Subnet Mask
Source	<input type="text" value="PubLN"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (B2)"/>
Destination	<input type="text" value="PriLN"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (B2)"/>

Caution: If choosing "All", user won't be able to select Start/End Port of Source/Destination field.

Table 4-4 IP Filter/Firewall page Filter and Description

Filter	Description
Name	To give a name to IP Filter rule.
Check to enable this rule	Enable this rule if it be marked.
Action	Specifies the action to be taken when packets match the rule Block : Packets matching the rule will be dropped immediately. Pass : Packets matching the rule will be passed immediately.
Protocol	Specifies the protocol(s) this filter rule will apply to.
Source MAC	Source MAC address.
Source/Destination IF	Source/Destination Interface. You can select WAN port(WAN) or Private LAN port(PriLN) or Public LAN port (PubLN) or ALL(ALL) port.
Source/Destination IP Address	Source/Destination IP address.
Source/Destination Subnet Mask	Source/Destination Subnet Mask.
Source/Destination Operator	Select =(equal), != (not equal), >(greater than), <(smaller than) operator rule.
Source/Destination Start Port	Source/Destination Start Port.
Source/Destination End Port	Source/Destination End Port.

d. Tools

This feature provides various tools for system customization and maintenance, including **Monitor IP List, Change Password, Upload, System, Firmware, Misc. and Restart.**

1. Monitor IP List

The system will send out the packet regularly to monitor and control the status of the machine on the list. If the monitored IP address does not exist, the system will send out an e-mail to the Admin once every 30 minutes, such as: 1:00, 1:30, 2:00, 2:30, and 3:00 until the problem is fixed. Click **Apply** button to view all monitored IP (**Figure 4-56**). There are a maximum of 20 IP address for the monitoring here.

Admin Email: If you want to automatically send the history to your email address, please enter your e-mail address in the following column. It will take effect immediately after you click the **Apply** button.

Send From: The email address of administrator server who is in charge of the monitoring.

Send To: The email address of a predefined IP user who is being monitored.

Interval: The Interval column shows the interval for sending the history email. If you choose one day, then the history mail will be sent to you once a day.

Figure 4-56 Monitor IP List

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



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"/>



2. Change Password




DSA-3100 provides 2 built-in user accounts: “admin” and “manager”

- **admin:** This user is the administrator in the DSA-3100.
- **manager:** This user has right to manager user account, the rest of function is denied.

Either admin or manager to change the password; specify the current password to ensure that you have appropriate right to manage this system. The new password must be entered twice to help make sure a correct new password is given.




Figure 4-57 Change Password

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

Apply Cancel Help

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

Apply Cancel Help

Note: If unfortunately you lost the administrator’s password, you could still change the administrator’s password from the console interface.

3. Upload

DSA-3100 provides upload function that you can customize your web page, like this: Private KEY, Customer certificate, Login page, Logout page, Login error page, Login succeed page and Logout succeed page. We also provide the Login error page, Login succeed page and Logout succeed page Source Code in the Appendix 2 that you can refer to it.

- 1) Upload Private KEY / Certificate:** DSA-3100 can support user to upload customer certification.

Figure 4-58 Upload Primary Key



- 2) **Upload Login Page:** To provide a custom user login 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 page, simply click the **Preview** button.

Figure 4-59 Upload Login Page



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

Figure 4-60 Login page required HTML code snippet

```
<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>
```

- 3) **Upload Logout 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 page, simply click the **Preview** button.

Figure 4-61 Upload Logout Page



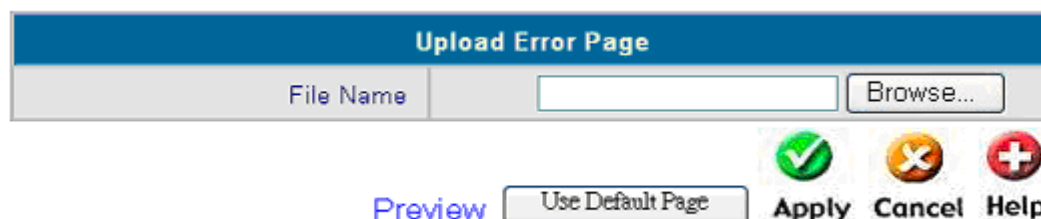
The uploaded custom logout page must contain the following HTML codes to provide users a place to input user name and password.

Figure 4-62 Logout page required HTML code snippet

```
<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>
```

- 4) **Upload Error Page:** To provide a custom user login 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 Login error Page, simply click the **Preview** button.

Figure 4-63 Upload Error Page



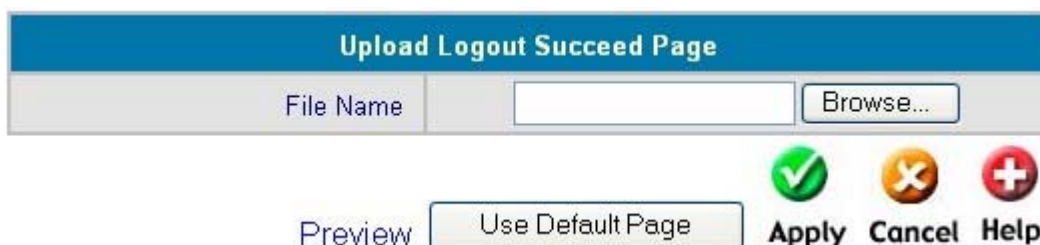
- 5) **Upload Login Succeed Page:** To provide a custom user login succeed page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login Succeed Page, simply click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

Figure 4-64 Upload Login Succeed Page



6) **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.

Figure 4-65 Upload Logout Succeed Page



7) **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. In the Upload Image at the third section of this interface Upload Image File, key in the path and file name of such graphic file or browse to select such file. The maximum size of the graphic file is 512K.




Figure 4-66 Path of Graphic File in User Logon Interface

```

```

After the graphic file is uploaded, the second section Existing Image Files of this page will list the graphic files uploaded to the system. You can select or delete any graphic file, and the system will list the using space of the graphic file in the third section.

Figure 4-67 Upload Image Files

File Name	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
   Apply Cancel Help	
Existing Image Files :	
Total Capacity: 512K	
Now used: 0K	

4. System

Allow you to make a backup and restore the backup copy to the D-Link DSA-3100. This function also enables you to restore the D-Link DSA-3100 back to the factory default.

Create Backup Image : make a backup Image file.

Restore Setting From File : restore the backup image file. (Important : The image must be created by the D-Link DSA-3100.)

Reset To Factory Default : restore the D-Link DSA-3100 back to the factory default.

Figure 4-68 System Settings

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

5. Firmware

Available firmware upgrade of the DSA-3100 could be obtained from D-Link support web site.

Figure 4-69 Firmware Upgrade From File

Firmware Upgrade From File	
Current Firmware Version	2.22B4
File Name	<input type="text"/> <input type="button" value="Browse..."/>

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.

To replace the firmware with a new one, browse to find the firmware image file on your computer and click Apply. The browser will upload the image onto the DSA-3100 and the upgrade procedure goes on. **When the system is upgrading its firmware, the Status LED blinks until done.** When finished, the web interface will also display a successful message.

The DSA-3100 must be restarted to have the new firmware take effect. If you made any change to the configuration, remember to save settings before restarting the DSA-3100.

Caution: Please restart the DSA-3100 using the administration interface. Do not directly power it off and up. Restarting the DSA-3100 this way after firmware upgrade might result in corruption of the DSA-3100 firmware.

6. Misc.

Remote Manage IP	Specify an IP address or network segment that connects to WAN Port to be allowed for configuring DSA-3100. For instance, if 10.2.3.1 is specified, then the user will be allowed to connect to WAN Port and configure DSA-3100 only from the specified address.
SNMP	The DSA-3100 provides SNMP v2 Read-only (RO) management, <ul style="list-style-type: none"> • Manager IP: A trap manager is a management station that receives and processes traps. When you configure a trap manager, assign IP address to management station.

	<ul style="list-style-type: none"> Community: Community strings serve as passwords for SNMP messages, DSA-3100 allows Read-only (RO) as password. If you select Enable SNMP, enter IP address, community string to the field.
Proxy Server	<p>Base on DSA-3100 security management, only port: 80 is allowed (it will appear 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 in this item of the DSA-3100 to have proper operations in the Proxy network environment. These settings will be effective immediately after you click "Apply".</p>
DoS protection for user	<p>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</p>

Figure 4-70 MISC.

MISC.	
Remote Manage IP <small>(from WAN)</small>	<input style="width: 150px;" type="text" value="10.2.3.0/24"/> (ex. 192.168.2.0/24 or 192.168.2.1)
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Proxy Server	<input style="width: 150px;" type="text"/> Port: <input style="width: 50px;" type="text"/>
<input type="checkbox"/> DoS protection for user	

7. Restart

Reboots the DSA-3100. It takes about 1 minute 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 remove the power after your hear a beep from it.

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

e. Status

This feature provides system status information and on-line user status, including **Device Info, Interface, Current Users** and **Traffic History**.

1. Device Info

With this feature, you could get all system configurations about DSA-3100 including **Firmware, Succeed Page...** For more detail see (Figure 4-71), (Table 4-5)

Figure 4-71 System Status

System Status		
	Current Firmware Version	2.22B4
	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	10.2.3.0/24
History	Retain Days	3 Days
	Email To	N/A
Time	External Time Server	tock.usno.navy.mil
	Date Time	Mon May 3 11:57:16 UTC 2004
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	User Type	LOCAL
	Guest Account	Enabled
DNS	Primary DNS Server	168.95.1.1
	Secondary DNS Server	N/A

Note: The Date Time show on this page is **Greenwich time (GMT+0:00)**

Table 4-5 System Status Item and Description

Item	Description
Current Firmware Version	The DSA-3100's current firmware version.
System Name	Name of this facility, DSA-3100 is the default.
Admin Detail	The information about the admin, If a user encounters problem connecting to WAN Port of DSA-3100, system admin information will be shown on user login page.
Succeed Page	The URL for all users to be directed to after successful login, usually defined as the home page of a corporation
External Syslog Server	Specify the IP address and Port of Syslog server.
Console Port baud Rate	It's the console port's baud rate that you specify. The default setting is 9600..

Manage	SSH	IP address that connects to WAN Port to be allowed for configuring DSA-3100
History	Retain Days	System will keep login user information for 3 days.
	Email To	Email the traffic history file to this mail address.
Time	External Time server	The DSA-3100 use this timeserver for clock synchronization
	Date Time	The Date Time show on this page is Greenwich time (GMT+0:00)
User	Idle Logout Timer	Idle logout time, If the on-line user is idle for 10 minutes will be logout system.
	Multiple Login	Disable a single user account to log into the system multiple times.
	User Type	User account Public LAN method: Local
	Guest Account	Enable guest account
DNS	Preferred DNS serve	DNS server IP address (Primary)
	Alternate DNS server	DNS server IP address (secondary)

2. Interface

With this feature, you could get all Interface information about interface management including **WAN port, Public LAN port, and Private LAN port.**

Figure 4-72 Interface Status

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

Table 4-6 Interface Status Item and Description

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 Address	WAN port's DNS IP address
Public LAN	Mode	Public LAN port modes: 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 modes: 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 Address	Private LAN port' 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

3. Current Users

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

Figure 4-73 Current Users

Current Users							
No.	Username	IP Address	MAC Address	Packets	Bytes	Idle	Logout
0	radius	192.168.1.200	00:09:6B:A0:54:B3	6389	24906600	0	Logout

4. Traffic History

Table 4-7 Interface History Email Item and Description

History Email	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 Email field and the period of time between two history files
External Syslog Server	Specify the IP address and Port of External Syslog server.
Access History IP	Specify an IP address that allows the billing system can connect to DSA-3100 via this IP address to get history information for billing.

Figure 4-74 History Email

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

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

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

This feature gives you access to network access history collected by the DSA-3100. Traffic histories are organized by day. The DSA-3100 will store up to 3 days of history data in its volatile memory.

Note: Since the traffic history is stored in a volatile memory, please copy the log data manually

if you need to reboot the DSA-3100 and want to keep the log data.

If you have an e-mail address entered in the system configuration interface, you will have the log sent to that e-mail everyday.

The traffic history is a pure text log. The first line is the header. From line two and so on, each line contains a single log record. Each record is consisted of seven fields and a TAB character separates each filed with each other. This format allows easy import of the log data into other programs for further processing. A sample log is shown in below

Figure 4-75 Traffic History

Traffic History	
Date	Size
2004-05-04	37



API History	
Date	Size
2004-05-04	23



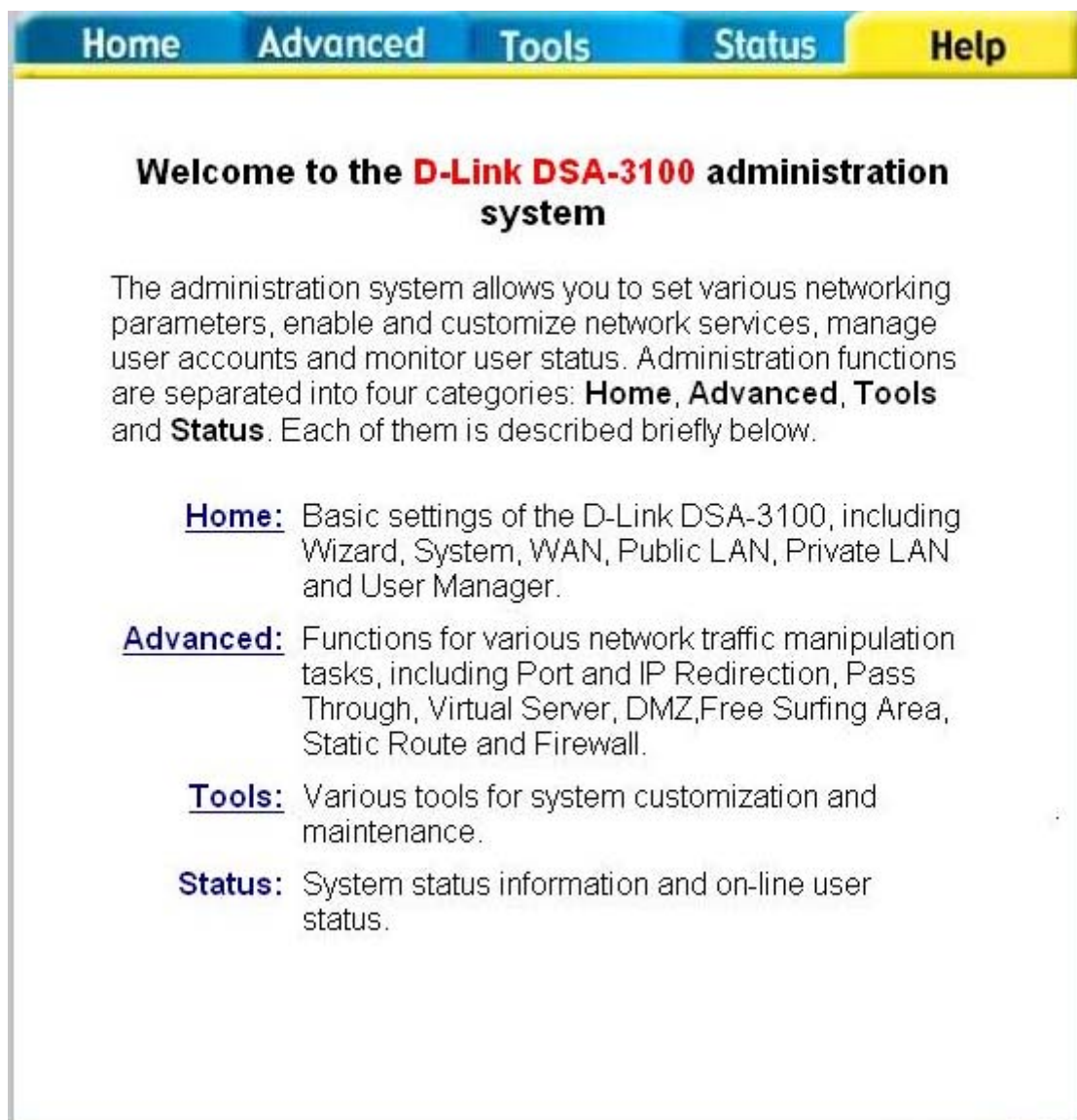
Traffic History (2004-05-04)						
Date	Type	Name	IP	MAC	Packets	Bytes
2004-05-04 16:29:14	LOGIN	casper	192.168.1.200	00:09:6B:A0:54:B3	0	0
2004-05-04 16:37:54	LOGOUT	casper	192.168.1.200	00:09:6B:A0:54:B3	3036	1439326
2004-05-04 16:39:12	LOGIN	radius	192.168.1.200	00:09:6B:A0:54:B3	0	0
2004-05-04 16:44:04	KICK	radius	192.168.1.200	00:09:6B:A0:54:B3	2940	857360
2004-05-04 21:19:17	LOGIN	radius	192.168.1.200	00:06:1B:D3:9B:08	0	0
2004-05-04 21:27:59	LOGIN	radius	192.168.1.200	00:06:1B:D3:9B:08	0	0
2004-05-04 21:28:33	LOGOUT	radius	192.168.1.200	00:06:1B:D3:9B:08	841	214047
2004-05-04 21:28:50	LOGIN	radius	192.168.1.200	00:06:1B:D3:9B:08	0	0

API History (2004-05-04)		
Date	Type	Description
2004-05-04 16:29:15	OPEN_USER	Open user: casper ok

f. Help

This feature provides online instructions for operating DSA-3100.

Figure 4-76 Help Page



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

Welcome to the D-Link DSA-3100 administration system

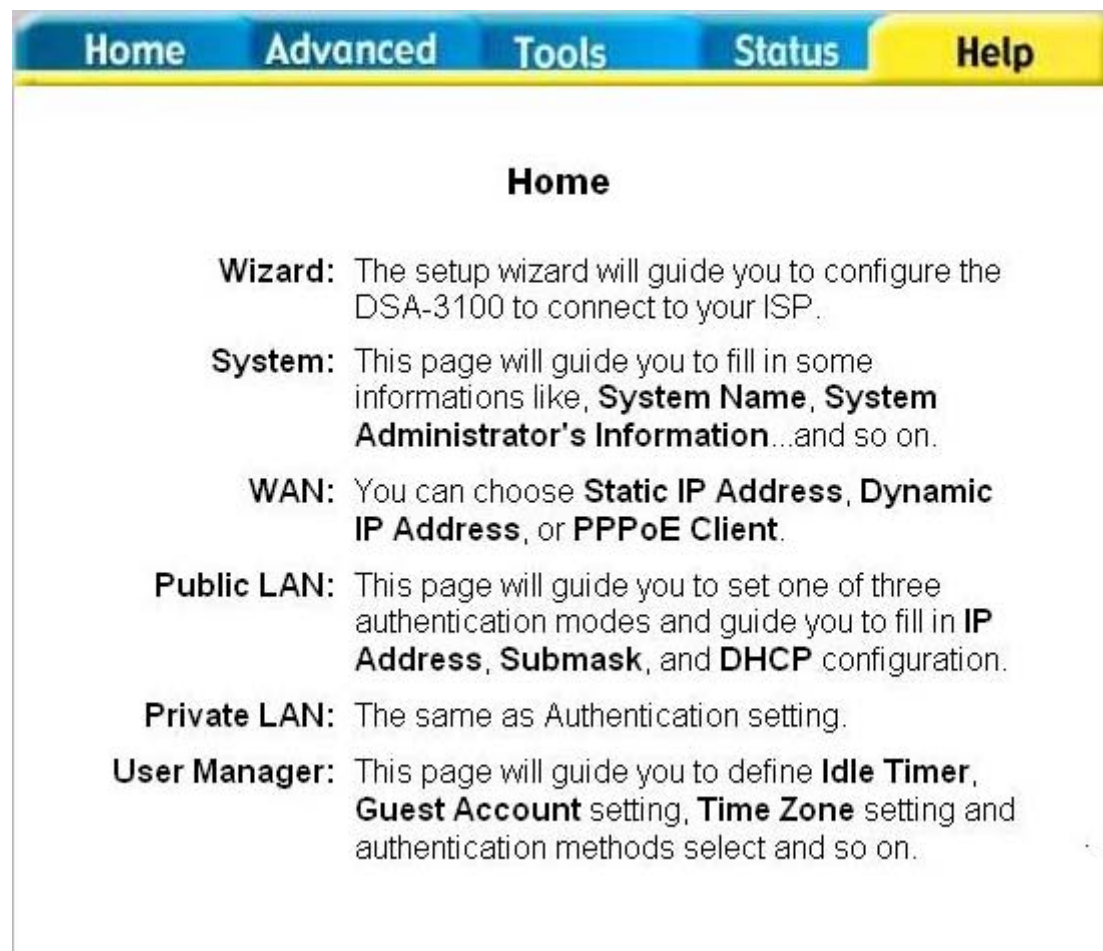
The administration system allows you to set various networking parameters, enable and customize network services, manage user accounts and monitor user status. Administration functions are separated into four categories: **Home**, **Advanced**, **Tools** and **Status**. Each of them is described briefly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

Home: Basic settings of the D-Link DSA-3100, including Wizard, System, WAN, Public LAN, Private LAN 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.



The screenshot shows a web interface with a navigation bar at the top containing five tabs: Home, Advanced, Tools, Status, and Help. The Home tab is selected and highlighted in yellow. Below the navigation bar, the page title is "Home". The main content area lists several configuration options:

- Wizard:** The setup wizard will guide you to configure the DSA-3100 to connect to your ISP.
- System:** This page will guide you to fill in some informations like, **System Name**, **System Administrator's Information**...and so on.
- WAN:** You can choose **Static IP Address**, **Dynamic IP Address**, or **PPPoE Client**.
- Public LAN:** This page will guide you to set one of three authentication modes and guide you to fill in **IP Address**, **Submask**, and **DHCP** configuration.
- Private LAN:** The same as Authentication setting.
- User Manager:** This page will guide you to define **Idle Timer**, **Guest Account** setting, **Time Zone** setting and authentication methods select and so on.



Advance

- Port and IP Redirect:** Up to 10 sets of traffic redirection criteria could be defined through this interface.
- Pass Through:** Up to 20 IP addresses and 10 MAC addresses can be assigned to unmanaged access.
- Virtual Server:** Allow you to define up to 10 virtual servers to enable access to servers connected to the authentication and local network from outside of the managed network.
 - DMZ:** You could define up to 10 pairs of Ethernet side(Private IP) and WAN side (Public IP) addresser if you have multiple IP addresses available.
- Free Suffing Area:** Up to 10 sites can be defined and allow users to access these websites before they login.
- Static Route:** If you want to access different network, you should add a static route in the DSA-3100.
- Firewall:** Setting filter rule to determine whether traffic will be allow to pass between the source and destination or not.



The screenshot shows a web interface with a navigation bar at the top containing five buttons: Home, Advanced, Tools, Status, and Help. The 'Tools' button is highlighted in yellow. Below the navigation bar, the page title is 'Tools'. The main content area lists several utility functions:

- Monitor IP List:** DSA-3100 Support UP to 20 IP Addresses can be monitored.
- Change Password:** Allow user to change their password.
- Upload:** Allow user to customize their own login, logout, login error, login succeed and logout succeed page.
- System:** Allow you to make a backup and restore to the DSA-3100.
- Firmware:** Allow user to check firmware and upgrade it from website.
- Restart:** Reboot the DSA-3100.

Appendix 1

Windows TCP/IP Setup

If using the default DSA-3100 settings, and the default Windows 95/98/ME/2000 TCP/IP settings, no changes need to be made. By default, the DSA-3100 will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.

For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. If you wish to check your TCP/IP settings, the procedure is described in the following sections.

Check TCP/IP Setting - Windows 2000

- 1、 Select Control Panel - Network and Dial-up Connection.
- 2、 Right click the Local Area Connection icon and select Properties.
- 3、 Select the TCP/IP protocol for your network card.
- 4、 Click on the Properties button.
- 5、 Ensure your TCP/IP settings are correct, as follows.

Using DHCP

To use DHCP, select the radio button to obtain an IP Address automatically. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the DSA-3100.

Using a fixed IP Address

If your PC is already configured, check with your network administrator before making the following changes.

- 1、 Enter the DSA-3100's IP address in the Default gateway field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the DSA-3100.)
- 2、 If the DNS Server fields are empty, select Use the following DNS server addresses, and enter the DNS address or addresses provided by your ISP, then click OK.

Checking TCP/IP Setting - Windows XP

- 1、 Select Control Panel - Network and Dial-up Connection.
- 2、 Right click the Local Area Connection icon and select Properties.
- 3、 Select the TCP/IP protocol for your network card.
- 4、 Click on the Properties button.
- 5、 Ensure your TCP/IP settings are correct, as follows.

Using DHCP

To use DHCP, select the radio button to obtain an IP Address automatically. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the DSA-3100.

Using a fixed IP Address

If your PC is already configured, check with your network administrator before making the following changes.

- 1、 Enter the DSA-3100's IP address in the Default gateway field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the DSA-3100.)
- 2、 If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

Appendix 2

Source Code

Login error Page

```
<html>

<head>
<title>Error</title>
</head>

<body style="font-family: Arial" BGCOLOR=#FFFFFF leftmargin=0 topmargin=0 >
  <table width=754 border=0 cellspacing=0 cellpadding=0 height="100%" align=center>
    <tr>
      <td height="52" width="765" background="/images/down_37.gif" colspan="2">
        <div align=center>
```

```

        <map name=Map2>
            <area shape=rect coords=20,9,154,58 href=http://www.dlink.com target=_blank>
        </map>
        <img src=/images/home_01.jpg width=765 height=95 usemap=#Map2 border=0>
    </div>
</td>
</tr>

<tr>
<td height="100%" width="740" valign="top" background="/images/down_37.gif">
    <p>&nbsp;</p>
    <div align="center">
        <center>
            <table cellpadding="0" width="80%" style="border: 1 solid #000099"
                bgcolor="#E4E4E4">
                <tbody>
                    <tr>
                        <td align="center" bgColor="#FF0000" width="100%" height="30">
                            
                        </td>
                    </tr>
                    <tr>
                        <td align="center" width="100%" height="30">
                            <p style="margin-left: 10"><font color="#000080" face="Arial" size="4">
                                <? echo $msg; ?> : (<? echo $uname; ?>) </font></p>
                            </td>
                        </tr>
                    </tbody>
                </table>
            </center>
        </div>
        <p align="center"><input type="button" value="Back" onClick="history.back()"
            style="font-family: Arial; font-size: 10pt"></p>
    </td>
<td height="100%" width="25" background="/images/down_11.gif">
</td>
</tr>
</table>

```

```
</body>
```

```
</html>
```

Login ok Page

```
<?
```

```
include "../include/init.inc";
```

```
include "../include/function.inc" ;
```

```
$flogout_mode = getValue($db_path . "/flogout");
```

```
?>
```

```
<HTML>
```

```
<HEAD>
```

```
<title>My Login Success</title>
```

```
<script language="javascript">
```

```
function popOne(url)
```

```
{
```

```
    window.open(url,"",directories=0,height=200,width=440,resizable=0,scrollbar=0,status=0,menubar=0);
```

```
}
```

```
function logoff()
```

```
{
```

```
    var example=window.confirm('Are you sure want to logout ?');
```

```
    if(example)
```

```
    {
```

```
        window.close();
```

```
        popOne('logoff.shtml?uid=<? echo $uid; ?>&session=<? echo
```

```
$session; ?>');
```

```
    }
```

```
    else
```

```
    {
```

```
        window.close();
```

```
        popOne('popup11.shtml?uid=<? echo $uid; ?>&session=<? echo
```

```
$session; ?>');
```

```
    }

    return;
}
</script>
</HEAD>

<? if ($logout_mode=="Enabled") {?>
<BODY onload=logoff();>
<? } else {?>
<BODY>
<? } ?>
<form>
<p align="center">
Hello,[<? echo $uid; ?>]<BR>
My Login Success<BR>
<BR>
Please close this window or click this button to
<? if ($logout_mode=="Enabled") {?>
    <input type="submit" name="off" value="Logout" onClick='window.close()>
<? } else { ?>
    <input type="submit" name="off" value="Logout" onClick='logoff()>
<? }?>
, <BR> thank you!<BR>

<BR>
Login time:
    <script language="javascript">
        DateObj=new Date();

Todaytime=DateObj.getYear()+"-"+parseInt(DateObj.getMonth()+1)+"-"+DateObj.getDate()+
"+DateObj.getHours()+":"+DateObj.getMinutes()+":"+DateObj.getSeconds();
        document.write (Todaytime);
    </script>
</form>

</body>
</html>
```

Logut ok Page

```
<?php
include "../include/init.inc" ;
include "../include/function.inc" ;
?>
<html>

<head>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<META HTTP-EQUIV="Cache-Control" CONTENT="no-cache">
<title>D-Link</title>
</head>

<body style="font-family: Arial" BGCOLOR=#FFFFFF leftmargin=0 topmargin=0
ONLOAD=setTimeout("window.close()",5000);>

<!--
<body style="font-family: Arial" BGCOLOR=#FFFFFF leftmargin=0 topmargin=0
ONLOAD=setTimeout("window.close()",5000);>
<table width=754 border=0 cellspacing=0 cellpadding=0 height="100%" align=center>
<tr>
<td height="52" width="765" background="/images/down_37.gif" colspan="2">
<div align=center>
<map name=Map2>
<area shape=rect coords=20,9,154,58 href=http://www.dlink.com target=_blank>
</map>
<img src=/images/home_01.jpg width=765 height=95 usemap=#Map2 border=0>
</div>
</td>
</tr>

<tr>
<td height="100%" width="740" background="/images/down_37.gif">
-->

<table width=100% height=100% align=center valign=middle>
<tr>
<td align=center>
```

```
<font size="5" color="navy">
  <? echo getValue("$db_path/system_name") ?> <BR> Logout Success.
</font>
</td>
</tr>
</table>

<!--
</td>
<td height="100%" width="25" background="/images/down_11.gif">
</td>
</tr>
</table>
-->

</body>
</html>
```