



DSA-3100
Wireless Service Gateway
User Manual

First Edition (December 2002)

Printed In Taiwan



RECYCLABLE

Table of Contents

1	Introduction	1
1	Product Overview	1
2	Unpacking	1
3	Identifying External Components	2
a	Front Panel	2
b	Rear Panel	3
4	Specification	4
5	Key Features	4
2	Installation	6
1	Requirements	6
2	Procedure	7
3	Configure PCs on your LAN	8
a	TCP/IP network setting	8
b	Internet Access Configuration	9
3	Network Configuration	11
1	Home	15
a	System	15
b	Interface	16
c	User Management	21
d	Logout	32
2	Advanced	32
a	Port and IP Redirect	32
b	Pass Through	33
c	Virtual Server	34
d	DMZ	35
e	Free Surfing Area	36
f	Static Route	36
g	Firewall	38
3	Tools	39
4	Status	43
	Appendix 1	46
	Windows TCP/IP Setup	46

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

1 、 Product Overview

The D-Link wireless service 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.

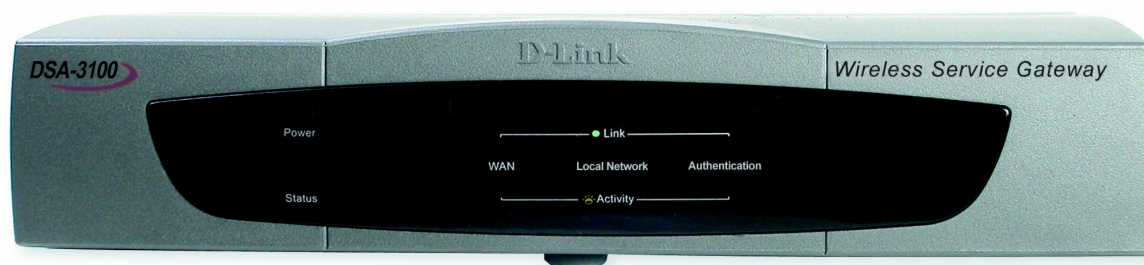
2 、 Unpacking

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

- ◆ **Wireless Service 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**

3 · Identifying External Components

a · Front Panel



- ◆ **Power Indicator**
- ◆ **WAN Indicator**
- ◆ **Local Network Indicator**
- ◆ **Authentication Indicator**

The power indicator is kept bright while DSA-3100 is power on. The indicators ordered from left to right are for WAN, Local Network and Authentication 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.

Power light	Green		System ready
Status light	Green		System ready
	Sparkling		System rebooting or Firmware Upgrading
Link light	WAN	Green	On line
	Local Network	Green	On line
	Authentication	Green	On line
Activity light	WAN	Sparkling	Data transmission
	Local Network	Sparkling	Data transmission
	Authentication	Sparkling	Data transmission

b · Rear Panel



- ◆ **WAN External Port**
- ◆ **Local Network Internal Port**
- ◆ **Authentication Internal Port**
- ◆ **DC Power Outlet**
- ◆ **Console Port**

a.) 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.

b.) Authentication 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 Authentication Port must to login before. If they want to access any network resource.

c.) Local Network Port:

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

d.) DC Power Outlet:

Connect the supplied power adapter here.

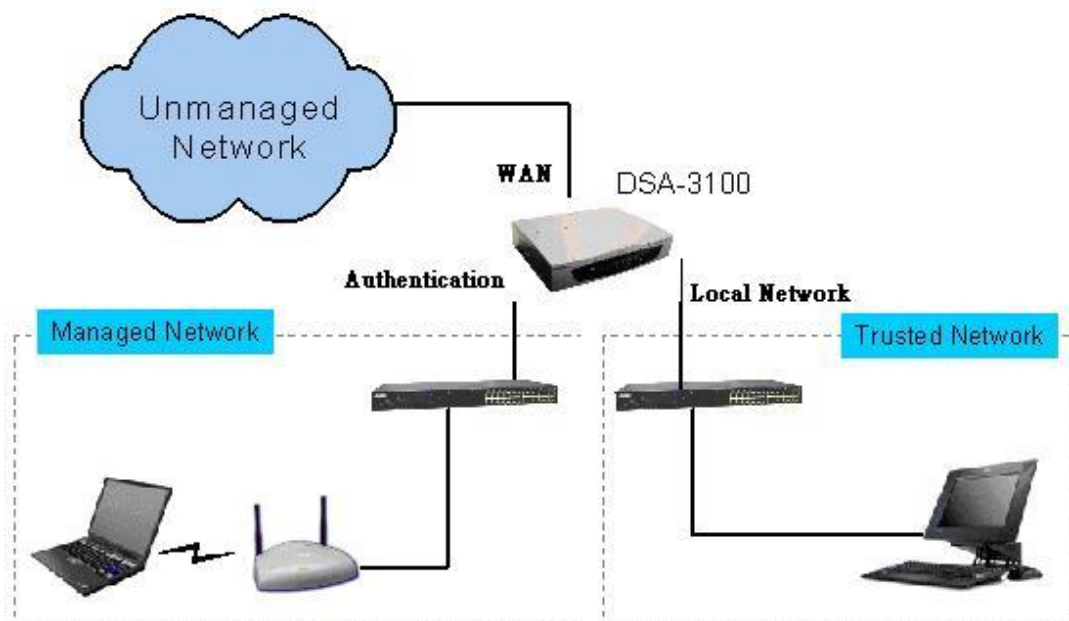
e.) Console Port:

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. (115200 8-N-1)

4 、 Specification

- ◆ CPU: NS Geode GX1-300MHz
- ◆ System: 32MB SDRAM Memory
- ◆ WAN: One Realtek RTL8139C 10/100 Ethernet controller
- ◆ Authentication: One Realtek RTL8139C 10/100 Ethernet controller
- ◆ Local Network: One Realtek RTL8139C 10/100 Ethernet controller
- ◆ Power: 3A/5V

5 、 Key Features



- u Manages up to 250 user account data with internal user account database.
- u Supports at least 50 on-line users.
- u ID/Password based authentication and authorization, which could be combined with MAC address locking to provide stricter access control.
- u Supports POP3, RADIUS and LDAP external authentication mechanism. Only one of

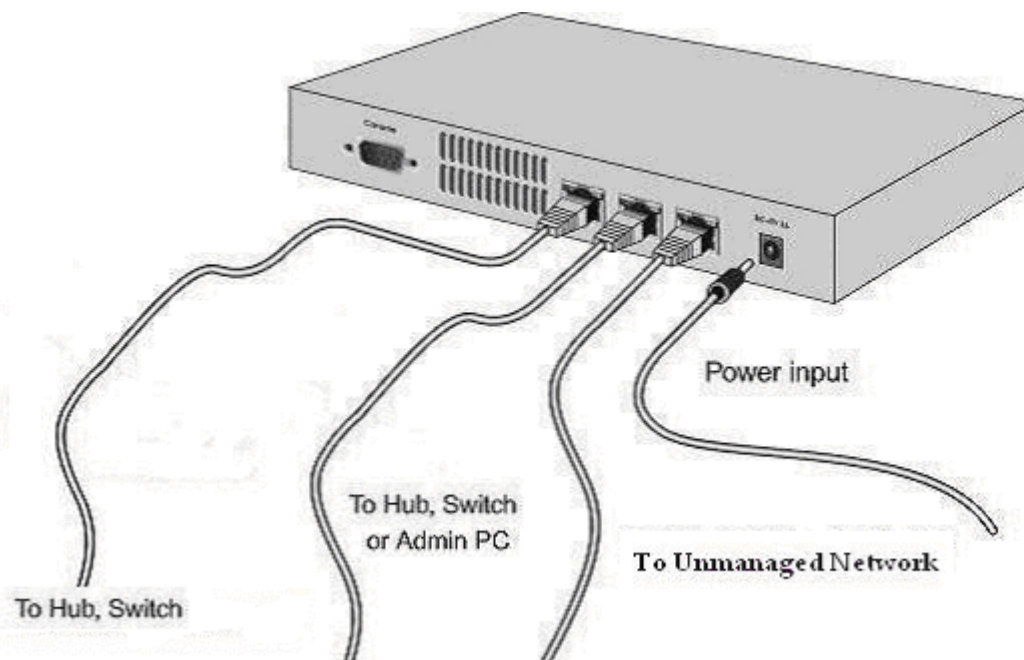
them could be chosen at once.

- u Provides on-line status monitoring and history traffic data review.
- u SSL protected access to the administration interface and user authentication interface.
- u Customizable user login & logout web interface.
- u Customizable user logout timer.
- u Customizable target URL for users who successfully get authorization.
- u Console mode administration interface via serial console port.
- u Supports display of text messages on the login page. An administrator could use the administration interface to input texts. Network users will see those texts on the DSA-3100 web-based login page
- u Supports NAT for managed clients.
- u Supports static IP, DHCP client and PPPoE client on WAN interface.
- u DHCP server built-in to service managed clients.
- u High speed policy routing engine built-in.
- u Customizable peremptory traffic redirection. (IP and Port Redirect)
- u NTP client built-in.
- u Provides a Local Network port for connecting a trusted network onto the DSA-3100, which permits access to WAN, and LAN from Local Network without authentication. It is useful to connect your wired Ethernet while connecting the wireless network to the Ethernet port of DSA-3100.

2、INSTALLATION

1、Requirements

- ◆ Network cable. Use standard 10/100Base T network (UTP) cable with RJ45 connectors.
- ◆ TCP/IP network protocol must be installed on all PCs.



2 、 Procedure

a 、 Ensure the DSA-3100 are power OFF.

b 、 WAN port connection

Use 10/100BaseT connections 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.

c 、 Local Network port connection

Use 10/100BaseT connections to connect your admin PC with the internal Switch or Hub that connected to the Local Network 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.

d 、 Authentication port connection

Use 10/100BaseT connections to connect your client PC with the internal Switch or Hub that connected to the Authentication 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.

e 、 Power up

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

f 、 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 Local Network or Authentication Indicator should be ON while a network device connected to the Local Network Port or the Authentication Internal Port.

3 、 Configure PCs on your LAN

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

- ◆ **TCP/IP network setting**

- ◆ **Internet Access configuration**

a 、 TCP/IP network setting

- ◆ **If your PC uses the default Windows 95/98/ME/2000/XP setting, no changes need to be made. Just star/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 boots.**

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

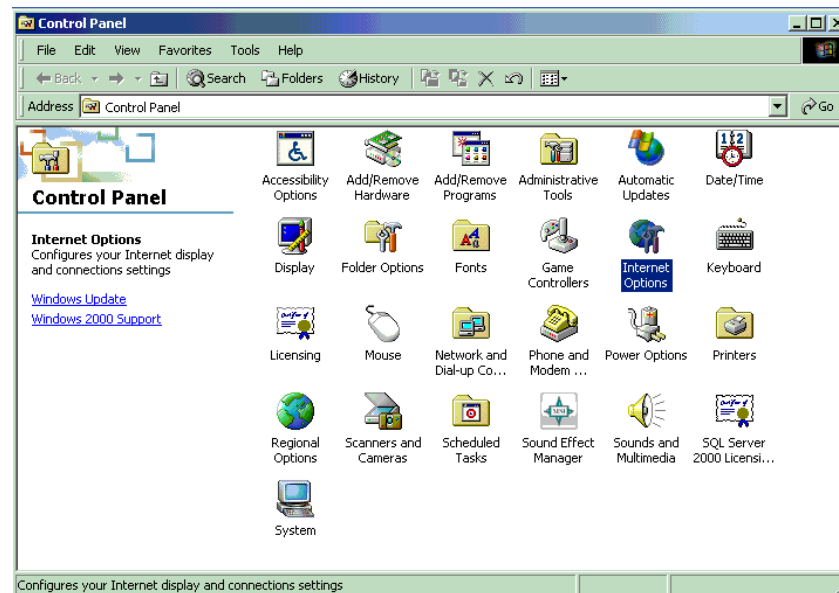
- ◆ **If using fixed IP Address on your LAN, or you wants to check your TCP/IP setting, refer to Appendix 1 - Windows TCP/IP Setup.**

b · Internet Access Configuration

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

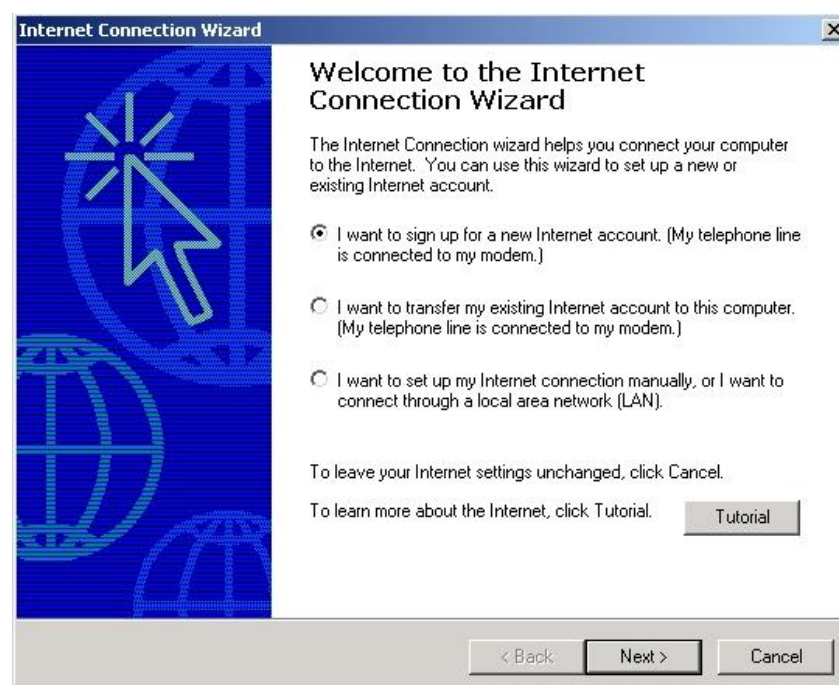
For Windows 9x/2000

1 · Please select Star Menu - Control Panel - Internet Options.



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**.



- 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" option 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、NETWORK CONFIGURATION

For using further applications of DSA-3100, you have to set up related configurations by following steps after reboot the PC.

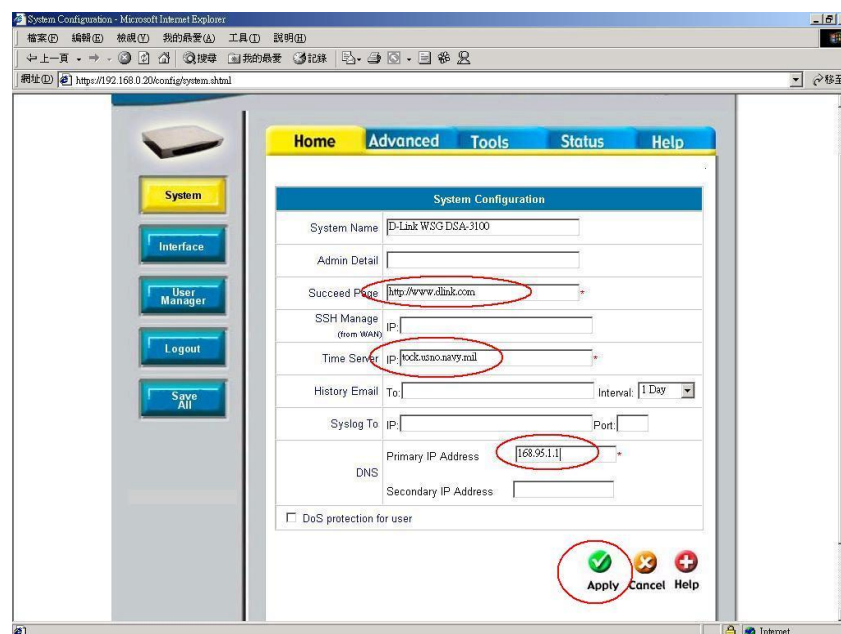
Step 1、Please ensure that system admin connects his PC to Local Network Port of the DSA-3100, because by default DSA-3100 is configurable only by PCs that are connected to Local Network Port.

Step 2、Open admin PC's browser. (Ex: Microsoft Internet Explore)

Step 3、Enter <https://192.168.0.40> in the Address or Location box to connect to the WEB management interface.

Step 4、Please enter default username “admin” in the “Username” column and password “admin” in the “Password” column.

Step 5、Select Home - System. You should see a screen like the following:



- Enter: a.) Succeed Page (ex: <http://www.dlink.com>)
- b.) Time Server (ex: tock.usno.navy.mil)
- c.) DNS-Primary IP Address (ex: 168.95.1.1)

Step 6、Click **Apply**.

Step 7、Select Home - Interface. You should see a screen like the following:

Interface Configuration	
WAN	<input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE
Authentication	Mode: NAT IP Address: 192.168.1.20 Subnet Mask: 255.255.255.0 Broadcast: 192.168.1.255
Authentication DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server DHCP Pool Start IP Address: 192.168.1.21 DHCP Pool End IP Address: 192.168.1.250 Lease Time: 1 Day Domain Name: dlink.com WINS IP Address: DNS Primary IP Address: 168.95.1.1 DNS Secondary IP Address: <input type="radio"/> DHCP Relay
Local Network	Mode: NAT IP Address: 192.168.0.20 Subnet Mask: 255.255.255.0 Broadcast: 192.168.0.255
Local Network DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server DHCP Pool Start IP Address: 192.168.0.21 DHCP Pool End IP Address: 192.168.0.250 Lease Time: 1 Day Domain Name: dlink.com WINS IP Address: DNS Primary IP Address: 168.95.1.1 DNS Secondary IP Address: <input type="radio"/> DHCP Relay

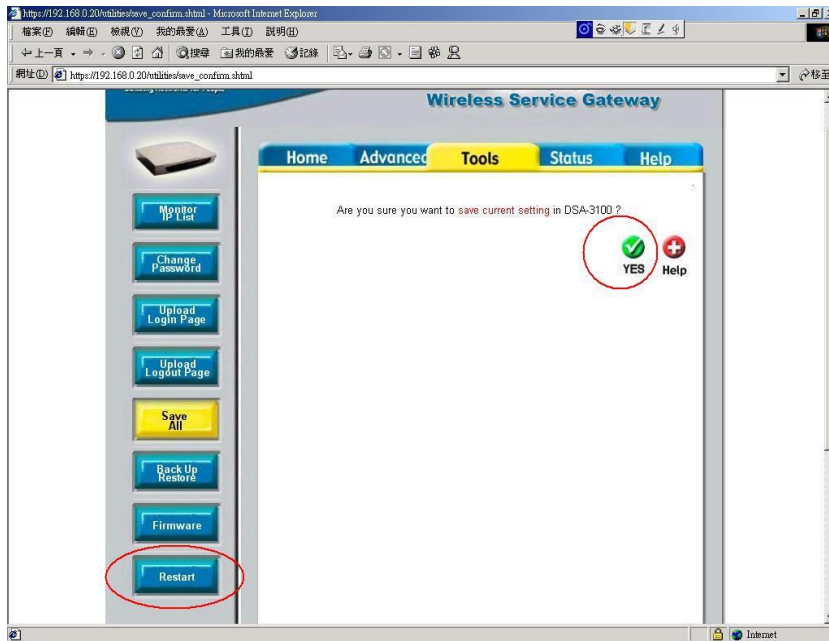


- Enter: a.) Select one mode for WAN to obtain IP (ex: Dynamic IP Address)
 b.) Authentication DHCP Configuration
 DNS-Primary IP Address (ex: 168.95.1.1)
 c.) Local Network DHCP Configuration
 DNS-Primary IP Address (ex: 168.95.1.1)

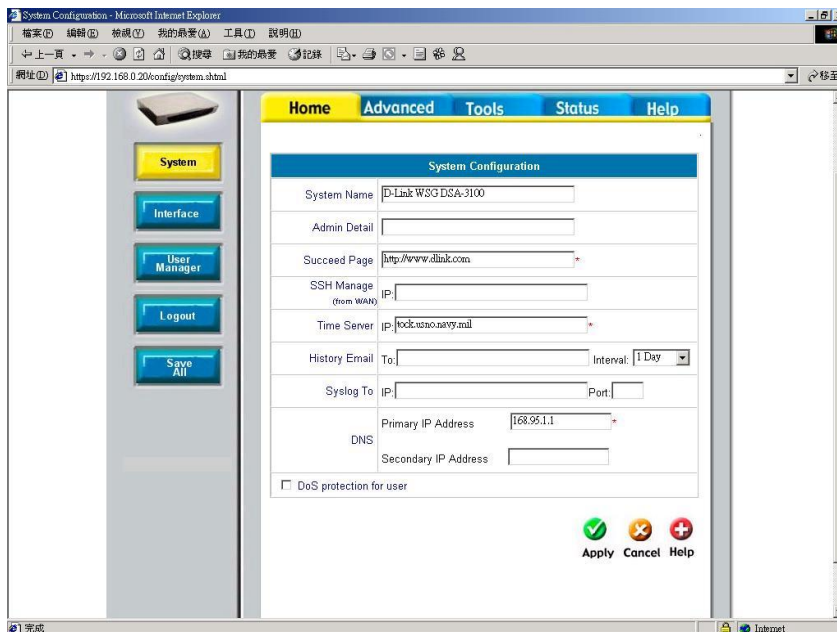
Step 8 · Click **Apply**.

Step 9 · Select Save All - YES - Restart. The basic configuration is now completed, as shown

in the following screen:



Step 10、When entering the WEB management interface of DSA-3100, you'll find the following main items on the screen.



◆ Home

Basic settings of the D-Link DSA-3100, including system, interface and user management.

◆ 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, including “Monitor IP List”, “Change Password”, “Upload Login Page”, “Upload Logout Page”, “Back Up Restore”, “Firmware” and “Restart”.

◆ **Status**

System status information and on-line user status, including “System”, “Interface”, “Current Users” and “Traffic History”.

◆ **Help**

Online instructions for operating DSA-3100.

1 、 Home

a 、 System

- a.) System Name:** Name of this facility, D-Link WSG DSA-3100 is the default.
- b.) Admin Detail:** You can edit system administrator's information right here, 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.
- c.) 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.
- d.) SSH Manage:** Specify an IP address 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.
- e.) Time Server:** The DSA-3100 supports the NTP protocol. Please specify a timeserver's IP address via the web interface. If you do not know any timeserver near you, you could leave the field blank and the DSA-3100 will use its default timeserver for clock synchronization. The time zone of the DSA-3100 internal clock is **UTC** (Coordinated Universal Time, formerly know as GMT, Greenwich Mean Time).
- f.) 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.
- g.) Syslog To:** Specify the IP address and Port of Syslog server.
- h.) DNS:** Specify a DNS server for DSA-3100, can be Primary DNS (Primary IP Address) and Secondary DNS (Secondary IP Address).
- i.) DoS protection for user:** The DSA-3100 protects users against various hacker attacks including NMAP FIN/URG/PSH, Xmas Tree, SYN/RST, Ping of Death, Null Scan, and SYN/FIN

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

System Configuration	
System Name	<input type="text" value="D-Link WSG DSA-3100"/>
Admin Detail	<input type="text"/>
Succeed Page	<input type="text" value="http://www.dlink.com"/> *
SSH Manage (from WAN)	IP: <input type="text" value="10.2.3.0/24"/>
Time Server	IP: <input type="text" value="clock.stdtime.gov.tw"/> *
History Email	To: <input type="text"/> Interval: <input type="text" value="1 Day"/> <input type="button" value="v"/>
Syslog To	IP: <input type="text"/> Port: <input type="text"/>
DNS	Primary IP Address <input type="text" value="168.95.1.1"/> *
	Secondary IP Address <input type="text" value="168.95.192.1"/>
<input type="checkbox"/> DoS protection for user	

Figure 1-1 Sample system configuration page

b · Interface

a.) WAN : The DSA-3100 offers three ways for WAN to obtain IP address(as shown in following screens):

- 1.) Static IP Address: Manually specify WAN Port IP address, suitable when WAN Port cannot automatically obtain an IP address.
- 2.) 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.
- 3.) PPPoE: Suggested when PPPoE is connected to WAN Port.

Interface Configuration	
WAN	<input checked="" type="radio"/> Static IP Address
	IP <input type="text" value="10.2.3.242"/>
	Netmask <input type="text" value="255.255.255.0"/>
	Broadcast <input type="text" value="10.2.3.255"/>
	Gateway <input type="text" value="10.2.3.254"/>
<input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE	

Use Static IP Address

Interface Configuration	
WAN	<input type="radio"/> Static IP Address
	<input checked="" type="radio"/> Dynamic IP Address
	<input type="radio"/> PPPoE

Use Dynamic IP Address

Interface Configuration	
WAN	<input type="radio"/> Static IP Address
	<input type="radio"/> Dynamic IP Address
	<input checked="" type="radio"/> PPPoE
	User Name <input type="text" value="yt@msa.hinet.net"/>
Password <input type="text" value="***"/>	

Use PPPoE

b.) Authentication : Select one mode for Authentication Port and specify IP address, Subnet Mask, and Broadcast(as shown below).

Authentication	Mode	<input type="text" value="NAT"/>
	IP Address	<input type="text" value="192.168.1.20"/> *
	Subnet Mask	<input type="text" value="255.255.255.0"/> *
	Broadcast	<input type="text" value="192.168.1.255"/> *

The DSA-3100 comes with three Authentication modes, namely NAT and Router (as shown below).

- 1.) NAT mode: All outbound IP addresses (the addresses must belong to the network connected to Authentication Port) on Authentication Port will be translated to the IP address of WAN Port to proceed.
- 2.) Router mode: All outbound IP addresses on Authentication Port will retain their addresses; DSA-3100 functions as a router in this mode.

Authentication	Mode	NAT
	IP Address	NAT
	Subnet Mask	ROUTER
	Broadcast	192.168.1.255

c.) Authentication DHCP Configuration: Configure DHCP Server on Authentication Port.

The DSA-3100 comes with three DHCP Server options (as shown below):

- 1.) DHCP Disable: Shut down DHCP Server.
- 2.) 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 Pools End IP Address, Lease Time, Domain Name, WINS IP Address, DNS Primary IP Address, DNS Secondary IP address.
- 3.) DHCP Relay: In DHCP Relay mode. It is required to specify other DHCP Server IP address to select this mode.

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

DHCP Disable

Authentication DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay	
	DHCP Pool Start IP Address	192.168.1.21 *
	DHCP Pool End IP Address	192.168.1.250 *
	Lease Time	1 Day
	Domain Name	dlink.com *
	WINS IP Address	
	DNS Primary IP Address	168.95.1.1 *
	DNS Secondary IP Address	

DHCP Server Enable

Authentication DHCP Configuration	<input type="radio"/> DHCP Disable <input type="radio"/> DHCP Server <input checked="" type="radio"/> DHCP Relay Server IP: 10.2.3.1
---	---

DHCP Relay

d.) Local Network: Select one mode for Local Network Port and specify IP address, Subnet Mask, and Broadcast (as shown below).

Local Network	Mode	NAT
	IP Address	192.168.0.20
	Subnet Mask	255.255.255.0
	Broadcast	192.168.0.255

The DSA-3100 comes with two Local Network Port modes, NAT and Router (as shown below).

- 1.) NAT mode: All outbound IP addresses (the IP addresses must belong to the network connected to Local Network Port) on Local Network Port will be translated to the IP address of WAN Port to proceed.
- 2.) Router mode: All outbound IP addresses on Local Network Port will retain their addresses; DSA-3100 functions as a router in this mode.

Local Network	Mode	NAT
	IP Address	NAT
	Subnet Mask	255.255.255.0
	Broadcast	192.168.0.255

e.) Local Network DHCP Configuration: Configure DHCP Server on Local Network Port.

The DSA-3100 comes with three DHCP Server options (as shown below):

- 1.) DHCP Disable: Shut down DHCP Server.
- 2.) 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 Pools End IP Address, Lease Time, Domain Name, WINS IP Address, DNS Primary IP Address, DNS Secondary IP address.
- 3.) DHCP Relay: In DHCP Relay mode. It is required to specify other DHCP Server IP address to select this mode.

Local Network DHCP Configuration	<input checked="" type="radio"/> DHCP Disable <input type="radio"/> DHCP Server <input type="radio"/> DHCP Relay
--	--

DHCP Disable

Local Network DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server DHCP Pool Start IP Address <input type="text" value="192.168.0.21"/> * DHCP Pool End IP Address <input type="text" value="192.168.0.250"/> * Lease Time <input type="text" value="1 Day"/> * Domain Name <input type="text" value="dlink.com"/> * WINS IP Address <input type="text"/> DNS Primary IP Address <input type="text" value="168.95.1.1"/> * DNS Secondary IP Address <input type="text"/> <input type="radio"/> DHCP Relay
--	---




DHCP Server Enable

Local Network DHCP Configuration	<input type="radio"/> DHCP Disable <input type="radio"/> DHCP Server <input checked="" type="radio"/> DHCP Relay Server IP <input type="text" value="10.2.3.2"/>
--	---

DHCP Relay

Note: The 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 Authentication interface of the DSA-3100. Devices on the network connected to Authentication gain access to the network on Local Network and WAN interfaces of the DSA-3100 without authentication. A sample system configuration is shown in Figure 1-2 Sample Interface configuration page.

Interface Configuration	
WAN	<input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE
Authentication	Mode: <input type="text" value="NAT"/> IP Address: <input type="text" value="192.168.1.20"/> * Subnet Mask: <input type="text" value="255.255.255.0"/> * Broadcast: <input type="text" value="192.168.1.255"/> *
Authentication DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server DHCP Pool Start IP Address: <input type="text" value="192.168.1.21"/> * DHCP Pool End IP Address: <input type="text" value="192.168.1.250"/> * Lease Time: <input type="text" value="1 Day"/> Domain Name: <input type="text" value="dlink.com"/> * WINS IP Address: <input type="text"/> DNS Primary IP Address: <input type="text" value="168.95.1.1"/> * DNS Secondary IP Address: <input type="text"/> <input type="radio"/> DHCP Relay
Local Network	Mode: <input type="text" value="NAT"/> IP Address: <input type="text" value="192.168.0.20"/> Subnet Mask: <input type="text" value="255.255.255.0"/> Broadcast: <input type="text" value="192.168.0.255"/>
Local Network DHCP Configuration	<input type="radio"/> DHCP Disable <input checked="" type="radio"/> DHCP Server DHCP Pool Start IP Address: <input type="text" value="192.168.0.21"/> * DHCP Pool End IP Address: <input type="text" value="192.168.0.250"/> * Lease Time: <input type="text" value="1 Day"/> Domain Name: <input type="text" value="dlink.com"/> * WINS IP Address: <input type="text"/> DNS Primary IP Address: <input type="text" value="168.95.1.1"/> * DNS Secondary IP Address: <input type="text"/> <input type="radio"/> DHCP Relay

Apply Cancel Help

Figure 1-2 Sample Interface configuration page

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

c · User Management

a.) **User Control** : Define Logout Time and Multiple Login (as shown below).

1.) Logout Time : 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.

2.) Multiple Login: Check this function to allow a single user account to log into the system multiple times.

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

User Control	
User Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Logout Timer : <input type="text" value="10"/> Min(s) (1 - 1440) Multiple Login : <input type="checkbox"/>

b.) Guest Account: Select Enable to activate Guest Account (as shown below).

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

Guest Account	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Guest Accounts Guest Policy Session Length <input type="text" value="unlimit"/>
---------------	--

1.) Guest Accounts: 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		
No	Username	Password
1	guest1	<input type="text" value="12345678"/>
2	guest2	<input type="text"/>
3	guest3	<input type="text"/>
4	guest4	<input type="text"/>
5	guest5	<input type="text"/>
6	guest6	<input type="text"/>
7	guest7	<input type="text"/>
8	guest8	<input type="text"/>
9	guest9	<input type="text"/>
10	guest10	<input type="text"/>

2.) Guest Policy: Define network areas where Guest Account is disallowed access, for instance 10.2.3.0/24(as shown below).

Guest Policy		
No.	Intranet Disallow	
	Intranet Subnet	Intranet Netmask
1	<input type="text" value="10.2.3.0"/>	<input type="text" value="255.255.255.0"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>
13	<input type="text"/>	<input type="text"/>
14	<input type="text"/>	<input type="text"/>
15	<input type="text"/>	<input type="text"/>
16	<input type="text"/>	<input type="text"/>
17	<input type="text"/>	<input type="text"/>
18	<input type="text"/>	<input type="text"/>
19	<input type="text"/>	<input type="text"/>
20	<input type="text"/>	<input type="text"/>

3.) Session Length: Limit the duration for each session established by Guest Account, from 1~12 hours. There is no limit to the duration by default.

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

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

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

MAC ACL 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).

MAC ACL Control			
No.	MAC Address	No.	MAC Address
1	00-E0-18-18-63-22	2	00.E0:18:18:63:23
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	
21		22	
23		24	
25		26	
27		28	
29		30	
31		32	
33		34	
35		36	
37		38	
39		40	

d.) Bandwidth: Limit the outbound traffic bandwidth for users connected to Authentication Port, from 190Kbps~1.0Mbps(as shown below).

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

Bandwidth	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Rate Average
Management Type	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RA <input type="radio"/> AP Add Users Users List

190K bps
 190K bps
 480K bps
 660K bps
 730K bps
 900K bps
 1.0M bps

e.) Management Type : Support multiple account management methods including Local,

POP3 Server, RADIUS Server, and LDAP 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 (as shown below).

Management Type	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP
	Add Users
	Users List
	Upload User Account

(1.) **Add Users:** Create new accounts, including Username (mandatory), Password (mandatory), and MAC (blank accepted), as shown below.

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

Add Users			
No	Username	Password	MAC
1	rosen	rosen	00-E0-18-18-63-23
2	Hans	Hans	
3			
4			
5			
6			
7			
8			
9			
10			

(2.) **User List:** A list of all local user accounts could be obtained if you are using the embedded database for user account management. A sample list is shown below.

Users List	
UserName	<input type="button" value="Delete"/> <input type="button" value="Delete All"/>
rosen	<input type="checkbox"/>
hans	<input type="checkbox"/>

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.) Upload User Account:

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.

Upload User Account

File Name

2.) POP3: To use POP3 as the authentication 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.

Management Type	<input type="radio"/> Local <input checked="" type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP
	Server IP <input type="text" value="mail.dlink.com"/>
	Server Port <input type="text" value="110"/>

3.) RADIUS: To use RADIUS as the authentication method, input the RADIUS server IP address or domain name, Authentication Port, Accounting Port, Secret Key and select the “Accounting Service” and “Authentication 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.

Management Type	<input type="radio"/> Local <input type="radio"/> POP3 <input checked="" type="radio"/> RADIUS <input type="radio"/> LDAP
	Primary Server
	802.1x <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Server IP <input type="text" value="10.2.3.245"/>
	Authentication Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
	Secret Key <input type="text" value="DLink"/>
	Accounting Service <input type="text" value="Enabled"/>
	Authentication Method <input type="text" value="CHAP"/>
	Secondary Server
	Server IP <input type="text" value="10.2.3.245"/>
	Authentication Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
	Secret Key <input type="text" value="DLink"/>
Accounting Service <input type="text" value="Enabled"/>	
Authentication Method <input type="text" value="CHAP"/>	

(1.) **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 authentication methods which the backend RADIUS server and APs support.

The assumption is that user had configured a EAP enabled RADIUS server like Microsoft Internet Authentication Service on Windows 2000 or .NET Server 2003. If EAP-TLS is required for the dynamic key exchange, 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 authentication test and make sure every thing is correct before you connect the network to DSA-3100.

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

Management Type	<input type="radio"/> Local <input type="radio"/> POP3 <input checked="" type="radio"/> RADIUS <input type="radio"/> LDAP	
	Primary Server	
	802.1x	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Edit
	Server IP	<input type="text" value="172.16.1.1"/>
	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"/>	

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 authentication 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 authentication server etc.) to the IP address of “Authentication” 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:

802.1x Device Configuration		
No	IP (Segment) Address	Secret
1	172.16.99.250	dlink1
2	172.16.99.251	dlink2
3	172.16.99.252	dlink3
4		
5		
6		
7		
8		
9		
10		

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 authentication 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.

Management Type	<input type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input checked="" type="radio"/> LDAP
	Server IP: 172.16.1.3
	Server Port: 389
	Base DN: CN=Users,DC=dlink,DC=com

f.) Login Schedule: Define the time zone where DSA-3100 is located and login duration for Guest and General accounts.

1.) Time Zone: Define the time zone where DSA-3100 is located. By default the time zone is GMT-07:00.

Login Schedule	Time Zone	GMT-07:00 ▾
	Guest	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	General	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Login Schedule	Time Zone	GMT-07:00 ▾
	Guest	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Edit"/>
	General	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

2.) Define login duration for Guest accounts. Select Enable - Apply - Edit to enter the management interface (as shown below). After durations are defined, you need to click **Apply**, and then **Save All** to let the new functions take effect.

Login Schedule -- Guest							
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"/>

Note: The default user management menu is shown in Figure1-3. The DSA-3100 user management interface allows you to add, list, delete users and define guest accounts for visitors if it is configured to use embedded database for user accounts.

User Control	
User Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Logout Timer : <input type="text" value="10"/> Min(s) (1 - 1440) Multiple Login : <input type="checkbox"/>
Guest Account	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Guest Accounts Guest Policy Session Length <input type="text" value="unlimit"/>
MAC ACL Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable MAC ACL Control
Bandwidth	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Rate Average <input type="text" value="190K bps"/>
Management Type	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP Add Users Users List Upload User Account
Login Schedule	Time Zone <input type="text" value="GMT+08:00"/> Guest <input type="radio"/> Enable <input checked="" type="radio"/> Disable General <input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure1-3 Sample User management interface

d · Logout

Terminates current administration session. You have to login again to use the administration interface. The administration interface also has a built-in session timer, if you do not interact with the interface for some time, the session times out and you have to log in again.

2 · Advanced

a · Port and IP Redirect

Up to 10 sets of traffic redirection criteria could be defined through this interface.

Port and IP Redirect					
No.	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 checked="" type="radio"/> TCP <input type="radio"/> UDP
2	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
4	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
6	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
8	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP

Figure 2-1 Port and destination IP redirection

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.

b · ***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 2-2 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.*

Pass through IP & MAC Configuration			
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"/>
No.	MAC Address	No.	MAC 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"/>

Figure 2-2 Pass-through host definition

c · Virtual Server

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

Virtual Server Table				
No.	External Service Port	Local Server IP Address	Local Server Port	Type
1	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
3	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
5	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
7	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP
9	<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 checked="" type="radio"/> TCP <input type="radio"/> UDP

Figure 2-3 Defining virtual servers

Note: Each local server connected to Authentication Port must also be allowed for IP or MAC address pass-through. Please enter its IP or MAC address via the interface shown in Figure 2-2 Pass-through host definition

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

DMZ		
No.	Private IP	Public IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Figure 2-4 Defining DMZ mappings

e · Free Surfing Area

To allow users access to a few sites before they log in, enter the IP addresses of those sites in the Free Surfing Area list. Up to 10 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.

Free Surfing Area			
No.	IP (Segment) Address	No.	IP (Segment) 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"/>

Figure 2-5 Defining Free Surfing Area hosts

f · 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.

Static Route			
No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	192.168.202.0	255.255.255.0	192.168.200.253
2			
3			
4			
5			
6			
7			
8			
9			
10			

Figure 2-6 Sample Static Route

a.) Destination IP Address:

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

b.) Destination Subnet Mask:

Specifies the target network mask. In the example, we use the subnet mask of network 192.168.202.0.

c.) Gateway IP Address:

Specifies the IP address of the next hop router. In the example, we set this to 192.168.200.253 as the 192.168.202.0 network is behind the router.

Click **Apply**

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

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

g · Firewall

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

IP Filter / Firewall > Edit Filter Rule						
Rule: 1						
Name:	<input type="text"/>	<input type="checkbox"/> check to enable this Rule				
Action:	<input type="button" value="Block"/>	Protocol		<input type="button" value="all"/>		
	IP Address	Subnet Mask	Operator	Start Port	End Port	
Source	<input type="text"/>	<input type="button" value="255.255.255.255 (/32)"/>	<input type="button" value="!"/>	<input type="text"/>	<input type="text"/>	
Destination	<input type="text"/>	<input type="button" value="255.255.255.255 (/32)"/>	<input "="" type="button" value="="/>	<input type="text"/>	<input type="text"/>	

Figure 2-7 Defining Filter Rule

a.) Name:

Enter filter set name/description. Maximum length is 15 characters.

b.) Check to enable this Rule:

Enables the filter rule.

c.) 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.

d.) Protocol:

Specifies the protocol(s) this filter rule will apply to.

e.) IP Address:

Specifies a source and destination IP address for this filter rule to apply to. Placing the symbol ! before a particular IP Address will prevent this rule from being applied to that IP address. It is equal to the logical NOT operator.

f.) Subnet Mask:

Specifies the Subnet Mask for the IP Address column for this filter rule to apply to.

g.) Operator:

The operator column specifies the port number setting. If the Start Port is empty, the Start Port

- and the End Port column will be ignored. The filter rule will filter out any port number.
- = : If the End Port is empty , the filter rule will set the port number to be value of the **Start Port** . Otherwise, the port number ranges between the **Start Port** and the **End Port** (including the **Start Port** and the **End Port**).
 - ! = : If the End Port is empty ,the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the **Start Port** and the **End Port** (including the **Start Port** and the **End Port**).
 - > : Specifies the port number is larger than the **Start Port** (including the **Start Port**).
 - < : Specifies the port number is less than the **Start Port** (including the **Start Port**).

3 、 Tools

a 、 Monitor IP List

Up to 20 IP addresses could be monitored. The system periodically sends out packets to check the status of the selected network nodes.

Monitor IP List			
No.	IP Address	No.	IP Address
1	<input type="text" value="168.95.1.1"/>	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"/>

Figure 3-1 Sample Monitor IP List

b · Change Password

To change the administrator's 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.

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

Figure 3-2 Change administrator's password

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

c · 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.

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

Figure 3-3 Upload custom login page

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

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

Figure 3-4 Login page required HTML code snippet

d · 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 login page, simply click the **Use Default Page** button.

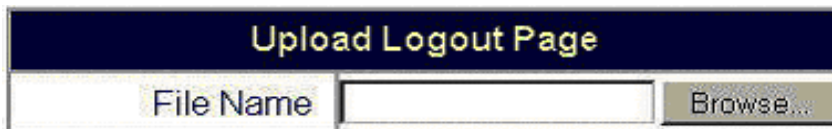


Figure 3-5 Upload custom logout page

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

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

Figure 3-6 Logout page required HTML code snippet

e \ Save All

Stores current settings to the non-volatile memory of the D-Link DSA-3100. **Every change to the settings must be stored by using this function.** Otherwise, any changes to the settings would go when the D-Link DSA-3100 restarts.

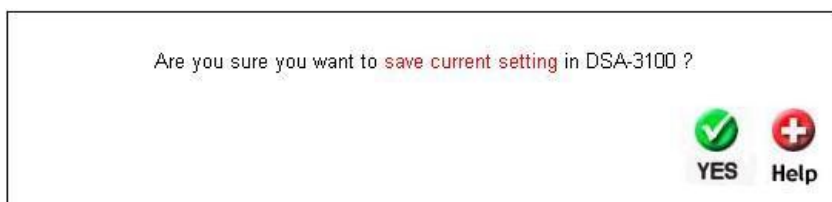


Figure 3-7 Defining Free Surfing Area hosts

f \ Backup Restore

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.

Backup & Restore
Create Backup Image
Restore Setting From File
Reset To Factory Default

Figure 3-8 Backup & Restore

- a.) Create Backup Image : make a backup Image file.
- b.) Restore Setting From File : restore the backup image file. (Important : The image must created by the D-Link DSA-3100.)
- c.) Reset To Factory Default : restore the D-Link DSA-3100 back to the factory default.

g · Firmware

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

Firmware Upgrade From File	
Current Firmware Version	2.0.7_20021101
File Name	<input type="text"/> <input type="button" value="Browse"/>

Figure 3-9 Firmware Upgrade Form File

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.

h · 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 you hear a beep from it.

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

4 、 Status

This feature displays a system configuration summary. An example is shown in Figure 4-1 below.

a 、 System

System Status		
	Firmware Version	2.0.7_20021101
	System Name	D-Link WSG DSA-3100
	Admin Detail	
	Succeed Page	
	Syslog To	N/A:N/A
	Console Port Baud Rate	115200 bps
Manage	SSH	10.2.3.0/24
History	Retain Days	3 Days
	Email To	
Time	Time Server	clock.stdtime.gov.tw
	Date Time	Mon Nov 25 06:41:13 UTC 2002
User	Logout Timer	10 Min(s)
	Multiple Login	Disabled
	User Type	RADIUS
	Guest Account	Disabled
	Bandwidth Control	Disabled
DNS	Primary IP Address	168.95.1.1
	Secondary IP Address	168.95.192.1

Figure 4-1 Sample System Status

b · Interface

Interface Status		
Uplink	MAC Address	00:90:0B:01:EF:9D
	IP Address	10.2.3.242
	Subnet Mask	255.255.255.0
	Broadcast	10.2.3.255
Private Ethernet	Mode	NAT
	MAC Address	00:90:0B:01:EF:9F
	IP Address	192.168.1.20
	Subnet Mask	255.255.255.0
	Broadcast	192.168.1.255
Private Ethernet DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.21
	End IP Address	192.168.1.250
	Lease Time	1440 Min(s)
Ethernet	Mode	NAT
	MAC Address	00:90:0B:01:EF:9E
	IP Address	192.168.0.20
	Subnet Mask	255.255.255.0
Ethernet DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.0.21
	End IP Address	192.168.0.250
	Lease Time	1440 Min(s)

Figure 4-2 Sample Interface Status

c · 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.

d · Traffic History

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 Figure 4-3 below.

#	Date	TYPE	name	IP	MAC	Packets	Bytes
	2002-06-28	10:47:22	LOGIN	test	192.168.1.247	0	0
	2002-06-28	10:47:32	LOGOUT	test	192.168.1.247	65	8202
	2002-06-28	10:49:18	LOGIN	test	192.168.1.247	0	0
	2002-06-28	10:49:52	LOGOUT	test	192.168.1.247	28	2414

Figure 4-3 Sample history log

Appendix 1

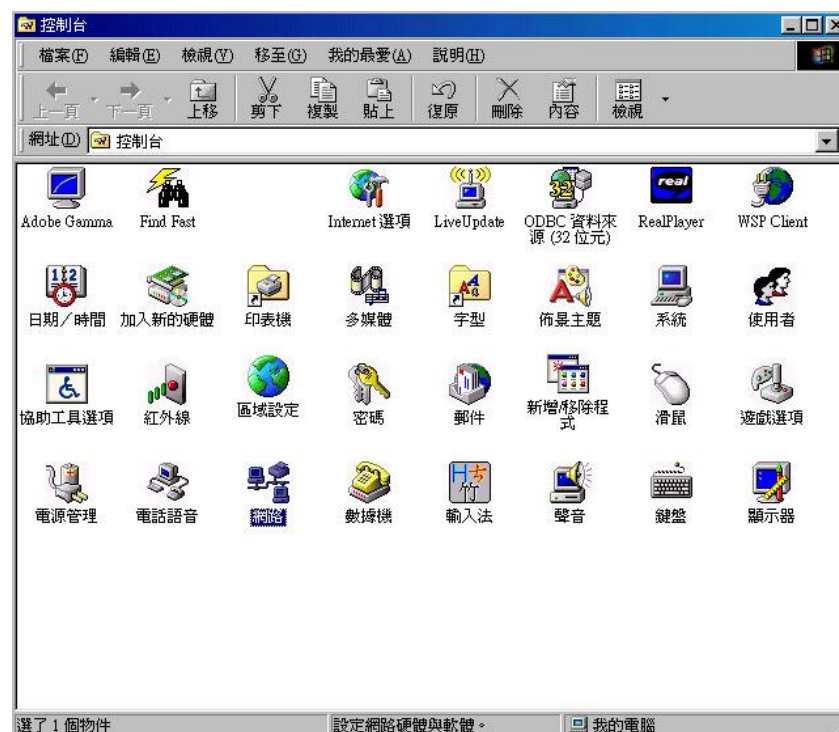
Windows TCP/IP Setup

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.

Checking TCP/IP Settings - Windows 9x/ME

1、Select Control Panel - Network. You should see a screen like the following.



2、Select the TCP/IP protocol for your network card.



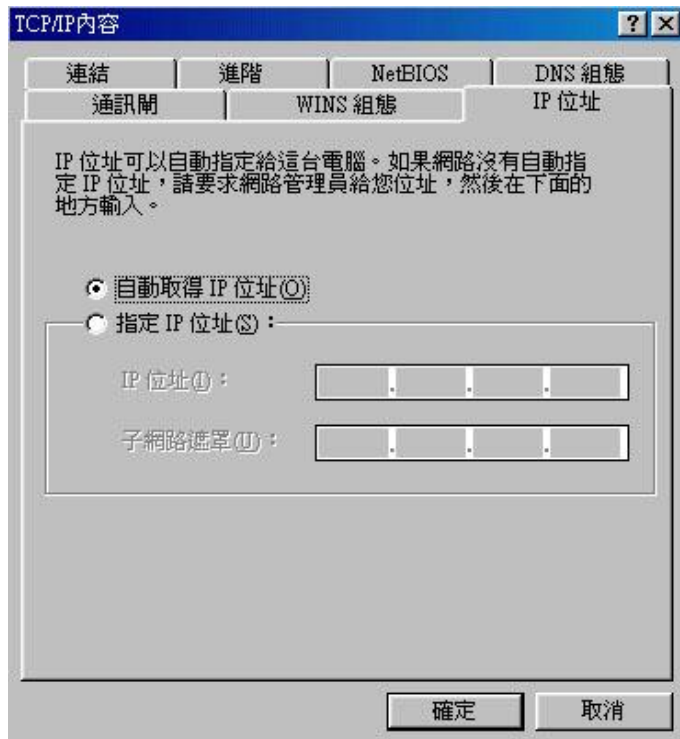
3、Click on the Properties button. You should then see a screen like the following

4、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 "Specify an IP Address"**

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

- 1、 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.



2、On the Gateway tab, enter the DSA-3100's IP address in the New Gateway field and click Add. (Your Ethernet administrator can advise you of the IP Address they assigned to the DSA-3100.)

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 enter the DNS address or addresses provided by your ISP, then click OK.