DSA-3600
User Guide

Version DSA-3600-1.0 April, 2007

Trademarks

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, D-Link Corporation reserves the right to make any changes to products described in this document without notice. D-Link Corporation shall be indemnified against any liability that may occur due to the use or application of the product(s) described herein.

Table of Contents

Chapter 1. Before You Start

1.1 Audience

This manual is intended for use by system integrators, field engineers and network administrators to help them set up DSA-3600 Multi-Service Business Gateway in their network environments. It contains step by step procedures and pictures to guide users with basic network system knowledge to complete the installation.

1.2 Document Conventions

The following information provides the details of conventions used in this manual.

For cautionary statements or warning requiring special attention by readers, a text box with italic font will be used:

Warning: *For security purposes, you should immediately change the administrator's password.*

When any of the button symbol shown below is selected, the following action will be executed accordingly:

Apply all settings configured

Clear all settings configured prior to applying

Please Note: Screen captures and pictures used in this manual may be displayed in part or in whole, and may vary or differ slightly from the actual product, depending on versioning and menu accessed.

Chapter 2. Overview

2.1 Introduction of DSA-3600

DSA-3600 is a Multi-Service Business Gateway specially designed for small and medium business, and branch office operational environments. The major functional areas include user management, access control, AP management, security management, and VLAN. The major features of DSA-3600 can be grouped into four functional blocks:

A. User Access Control
B. Network Security (examples: Firewall, VLAN and VPN)
C. Web-based administration and centralized AP management
D. General networking features

2.2 System Concept

Small and Midsize Business (SMB) Network Environment

Networking devices such as switches, hubs, and access points are usually included in SMB environments. The Internet connection of a SMB is usually via ADSL or cable modem. Figure-2.2a shows a typical network deployment example which includes switches, access points, and connections to the Internet via ADSL/cable modem.

The DSA-3600 provides user authentication, authorization and management. The user account information is stored in the local database or specified external databases server. User authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The appended figures are typical examples of DSA-3600 deployed in a SMB environment. Figure-2.2b shows DSA-3600 authenticating the users of its built-in database, as well as the users of external authentication database. Both LAN and WLAN can be secured by IPSec VPN. PPTP VPN is supported for remote users to increase security at remote sites. The DSA-3600 also supports Site-to-site VPN, WAN Failover, and DMZ.

The DSA-3600 can be used to control access to the company's intranet. In a managed network that includes cable and wireless network users, users located at the managed network can be set to be unable to access the network resource without permission. In the event access right to the network beyond the managed area is required, an Internet browser, such as the Internet Explorer, may be opened to connect to any website. When the browser attempts to connect to a website, the DSA-3600 will force the browser to redirect to the user login webpage. The user must then enter the username and password, where upon successful identification and authentication, the user will then be granted proper access right as defined in the DSA-3600.

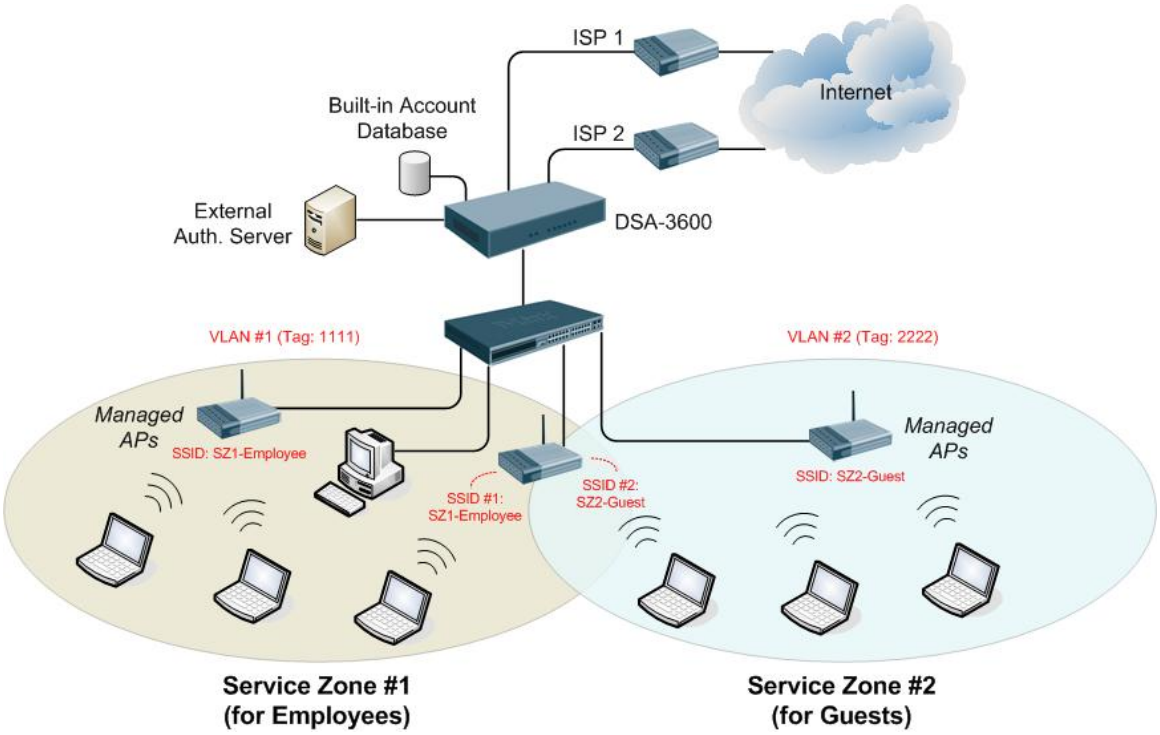


Figure-2.2a: An example deployment using DSA-3600

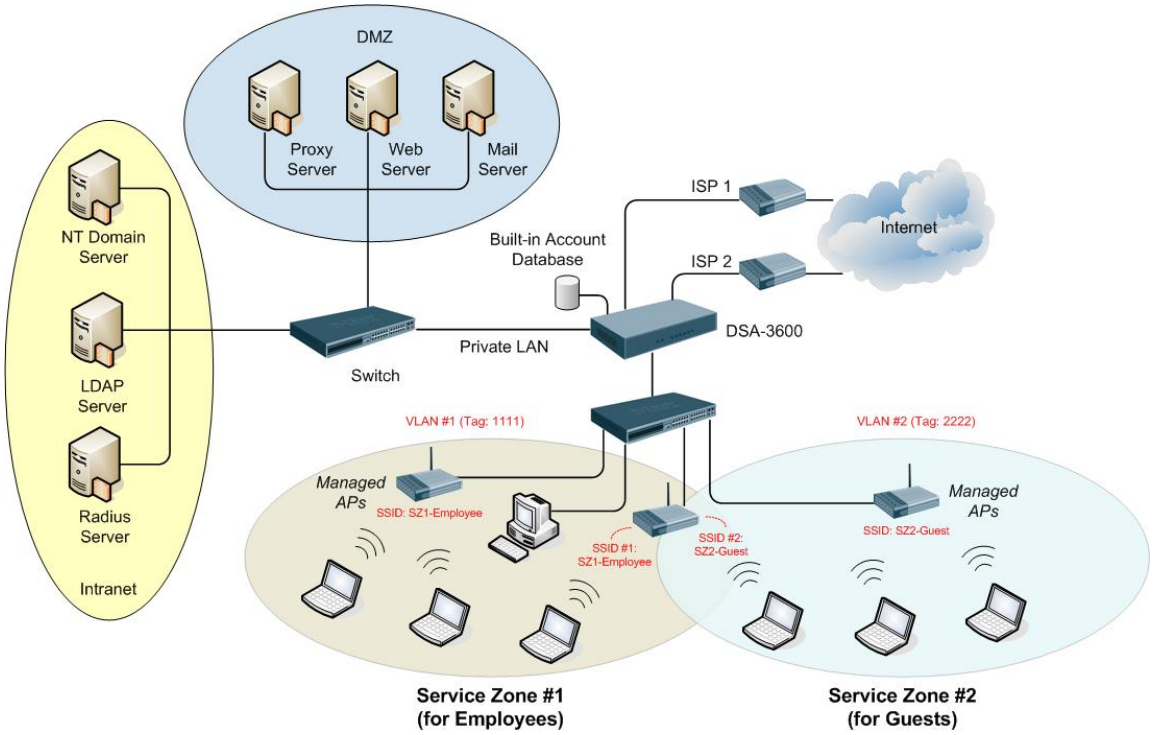


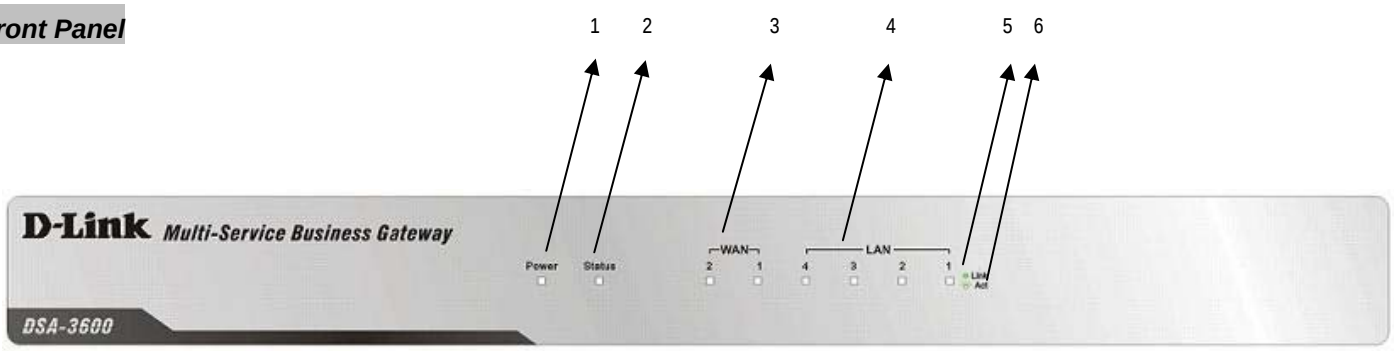
Figure-2.2b: An example of SMB environment using DSA-3600

Chapter 3. Hardware Installation

3.1 Panel Function Descriptions

The DSA-3600 is implemented on an embedded platform with mini-desktop form factor. On the front panel of the product, there are eight LEDs that are used to indicate the system power, system status, and the link status of the six fast Ethernet ports. The interface ports are installed on the rear panel. Six fast Ethernet (100Mbps) ports are provided by DSA-3600. Two are configured as WAN Ports, and the other four are configured as LAN Ports. Located on the rear panel are a serial console port, a reset button, and the power socket.

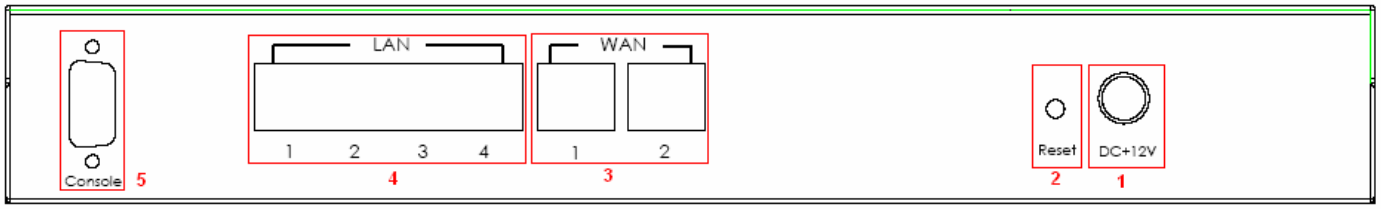
Front Panel



1. Power	**3. LEDs: WAN1~WAN2**	**5. Sign: Link**
2. Status	**4. LEDs: LAN1~LAN4**	**6. Sign: Act**

1. **Power**
   - ON indicates that power is on and OFF indicates that power is off.
2. **Status**
   - While system power is on, status OFF indicates BIOS is running, BLINKING indicates the OS is running, and ON indicates system is ready.
3. **WAN1~WAN2 LEDs**
   - OFF indicates no connection, ON indicates connection and BLINKING indicates transmitting data.
4. **LAN1~LAN4 LEDs**
   - OFF indicates no connection, ON indicates connection and BLINKING indicates transmitting data.
5. **Link Sign**
   - Sign to indicate the LED of WAN1~WAN2 and LAN1~LAN4 in the status of connection.
6. **Act Sign**
   - Sign to indicate the LED of WAN1~WAN2 and LAN1~LAN4 in the status of transmitting data.

Rear Panel



1 Power Socket:

- The power adapter is attached here.

2 Reset Button:

- Press and hold the Reset button about five seconds, status LED on front panel starts to blink before restarting the DSA-3600.
- Press and hold the Reset button for more than ten seconds, status LED on the front panel starts to speed up blinking before resetting the DSA-3600 to default configuration.

3 WAN1~WAN2:

- The two WAN ports connected to an external network not managed by the DSA-3600. These ports may be used to connect to the ATU-Router of an ADSL, or the port of a Cable Modem, or a Switch or Hub on the LAN of an organization.

4 LAN1~LAN4:

- The four LAN ports connect to networks managed by DSA-3600, such as to clients' networking devices or APs. There are two modes for service zone supported by DSA-3600, Port-Based and Tag-Based. By default, all LAN ports are in Tag-based service zone. Under Tag-Based mode, service zones will be distinguished by VLAN tagging instead of physical LAN ports.

5 Console:

- The serial RS-232 DB9 cable attaches here.

3.2 Package Contents

The standard package of the DSA-3600 includes:

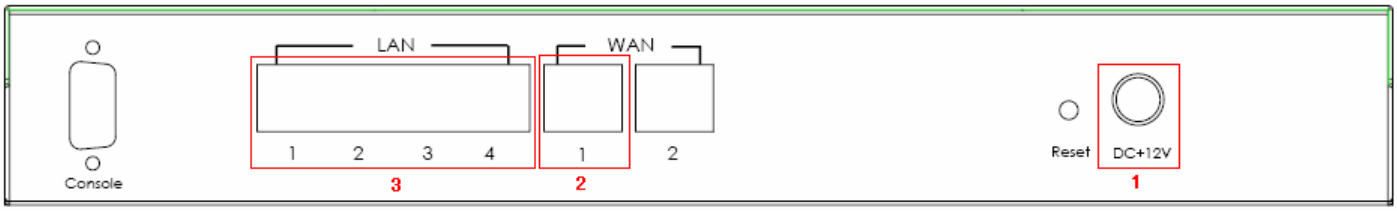
- DSA-3600 x 1
- Quick Installation Guide x 1
- CD-ROM x 1
- Console Cable x 1
- Straight-through Ethernet Cable x 1
- Power Cord x 1
- Power Adapter x 1

3.3 System Requirement

- Standard 10/100BaseT including network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.4 Installation Steps

Please follow the steps mentioned below to install the hardware of DSA-3600:



1. Connect the power adapter to the power socket on the rear panel. The Power LED on the front panel should be ON to indicate a proper connection.

   ***Warning**: Using a non-certified power adapter may damage this product.*

2. Connect an Ethernet cable to the WAN1 Port on the rear panel. Connect the other end of the Ethernet cable to a networking device such as an ADSL modem, a cable modem, a switch, or a hub. The LED of WAN1 port should light up to indicate a proper connection.
3. Connect an Ethernet cable to any LAN Port on the rear panel. Connect the other end of the cable to a networking device such as the administrator's PC. The LED of the LAN should be ON to indicate a proper connection.

After the hardware of the DSA-3600 is installed completely, the system is ready to be configured in the following sections. This manual will guide you step by step to set up the system using a single DSA-3600 to manage the network.

Chapter 4. Web Interface Configuration

This chapter provides further detailed information on setting up the DSA-3600. The following table shows all the functions of DSA-3600.

In the web management interface, there are three main interface areas: **Tools Menu**, **Main Menu Tree** and **Working Area**. The **Working Area** occupies the largest area of the web interface on the center right. It is also referred as **the current management page**. The current management page is where status is displayed, controlled are issued or parameters are configured. **Main Menu Tree**, on the left side of the web management interface, allows administrators to traverse to various management functions of this system. The management functions are grouped into five branches: System (System Settings), Users (User Management), Access Points (AP Management), Network (Network Settings) and Status (Status and Report).

OPTION	FUNCTION
System	General
	WAN 1
	WAN 2
	WAN Traffic
	LAN Port Mapping
	Service Zones
Users	Authentication
	Black List
	Policy
	Additional Control
Access Points	List
	Discovery
	Adding
	Templates
	Firmware
	Upgrade
Network	NAT
	Privilege
	Monitor IP
	Walled Garden
	Proxy Server
	DDNS
	Client Mobility

	VPN
Status	System
	Interface
	Online Users
	User Logs
	E-mail & SYSLOG
Tools	Setup Wizard
	Password Change
	Backup & Restore
	System Upgrade
	Restart
	Wake-On-LAN
	Quick Links

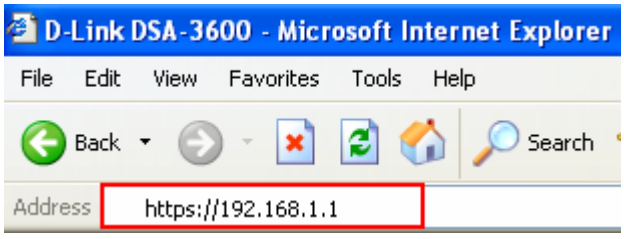
Caution: *After finishing the configuration, please click* ***Apply*** *and pay attention to see if a restart message appears on the screen. If the message appears, the system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.*

Web Management Interface

The DSA-3600 provides a web management interface for configuration. After completing the hardware installation, the administrator can configure the DSA-3600 via web browsers with JavaScript enabled such as Internet Explorer version 6.0.

After the basic installation has been completed according to the instructions of the previous chapter, the DSA-3600 can further be configured with the following steps:

1. First, set a PC as DHCP in the network with TCP/IP setting to get an IP address from the DHCP server automatically. Next, connect the PC to the DSA-3600 via any LAN port. An IP address will be assigned to the PC automatically via the DSA-3600 built-in DHCP server. Launch a web browser to access the web management interface of DSA-3600 by entering ***"https://192.168.1.1"*** in the URL. (Note: ***https*** is used for a secured connection.)



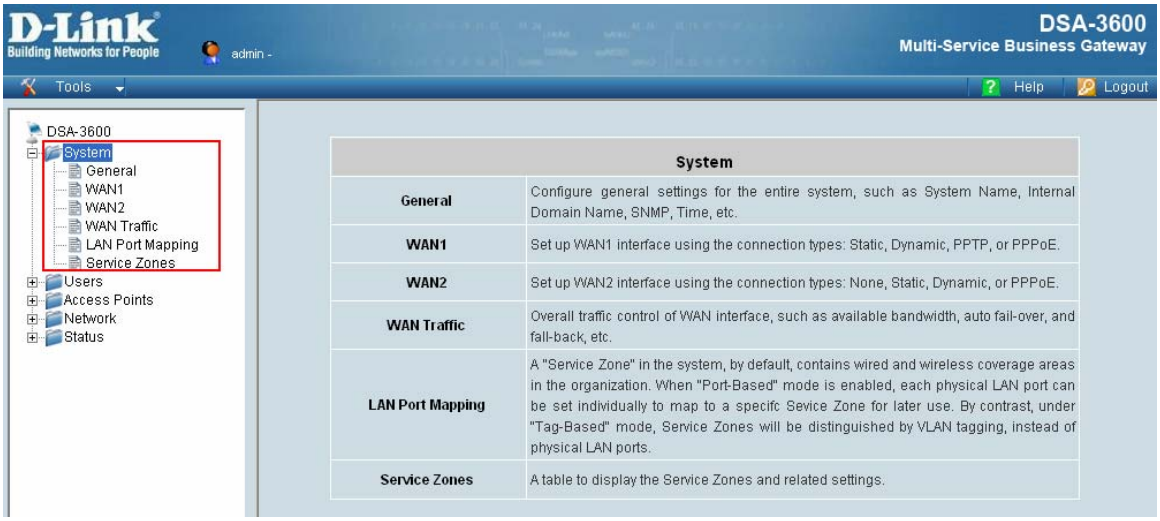
Once the DSA-3600 has been connected, the Administrator Login Page will appear. Enter “admin” for both the default username and password in the Username and Password fields. Select the Enter button to log in.

Caution: *If you are unable to get to the login screen, please check the IP address used. The IP address should be in the same subnet of the default gateway. set a static IP address such as 192.168.1.x in your network and then open a new browser again.*

1. After successfully logging into the DSA-3600, the System Overview page of the web management interface will appear. To logout, simply click the ***Logout*** icon on the upper right corner of the interface to return to the Administrator Login Page.

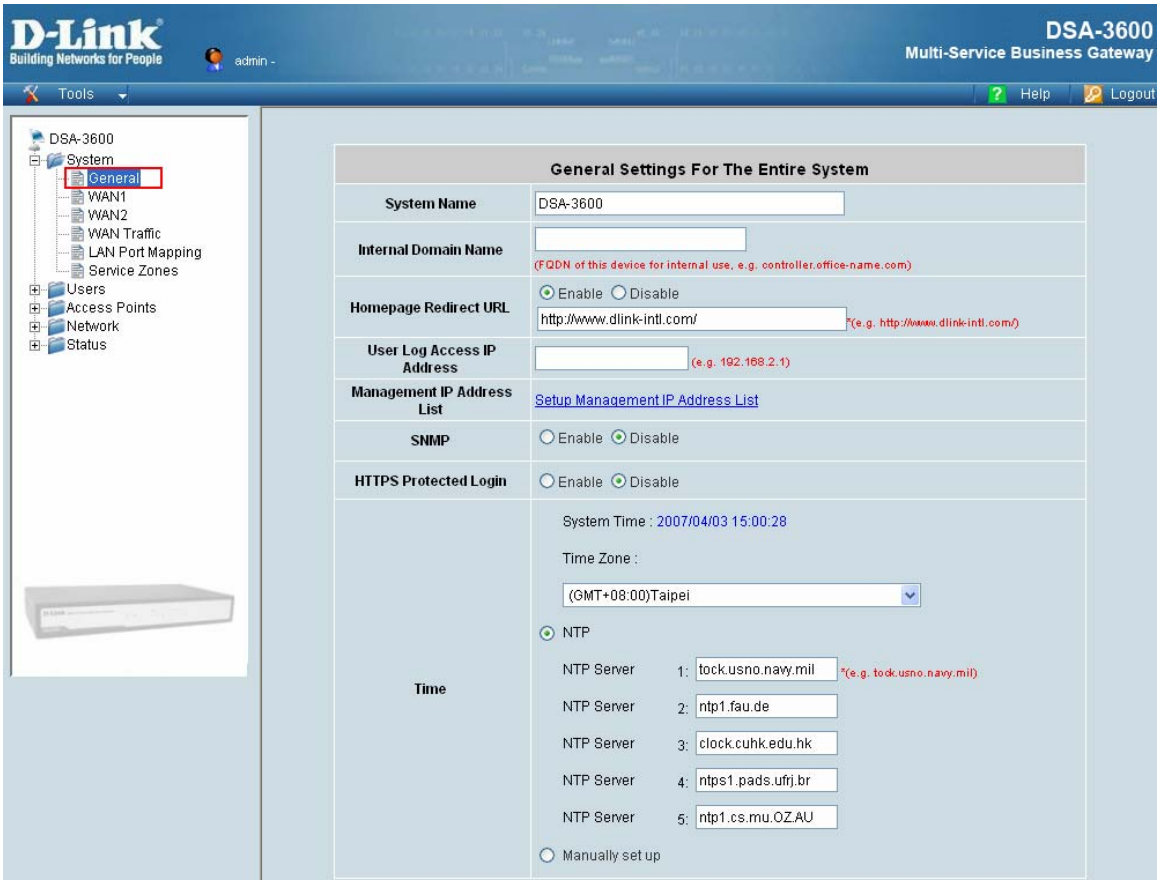
4.1 System

This section provides information on the following functions: **General**, **WAN1**, **WAN2, WAN Traffic, LAN Port Mapping** and **Service Zones**.



4.1.1 General

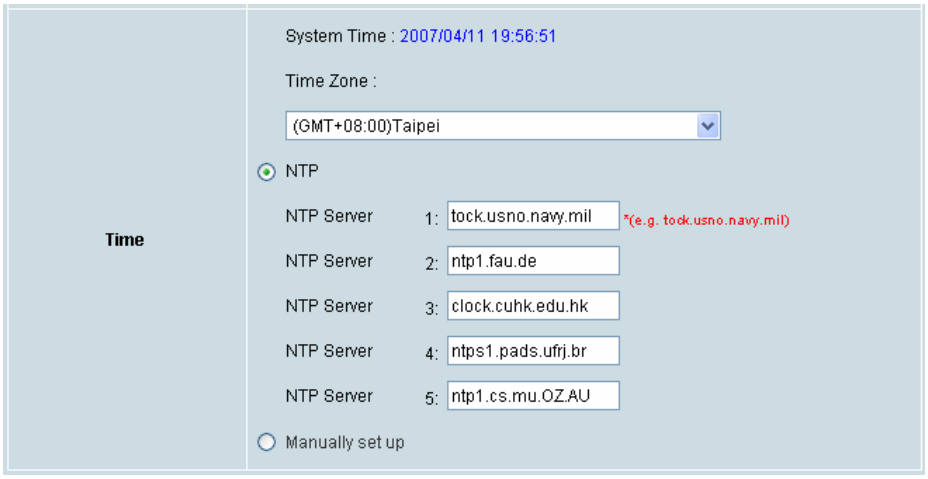
The system and network related parameters such as System Name, Homepage Redirect URL, Management IP Address List, and HTTPS Protected Login can be configured from the menu as shown below.

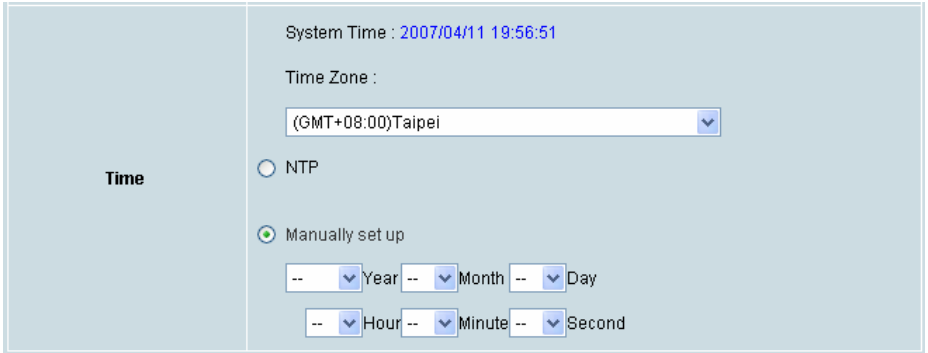


- **System Name:** Set the name of the system or use the default.
- **Internet Domain Name:** A fully qualified domain name (FQDN) of the system. When the administrator enters a desired domain name in the Internal Domain Name field, the entered Internal Domain Name will be shown in the top left of the Login Success page instead of an LAN IP address. In addition, when HTTPS is enabled, entering the domain name of the uploaded certificate will increase login speed and the URL in the User Login page will be changed. For example, if the Internal Domain Name is configured as ashop.com, the URL in the User Login page will be https://ashop.com/loginpages/login.shtml.
- **Homepage Redirect URL:** Enter a URL in this field. When the clients are logged-in to the DSA-3600 successfully, their browsers will be directed to this URL regardless of the original homepage setting in their browsers.
- **User Log Access IP Address:** An external billing system may access the system's user logs by specifying a desired IP address of the external billing system in this field. Only the billing system with this IP address may directly access the system's user logs in text format via browsers. For example, if the access interface of DSA-3600 is “10.30.1.23”, the user log can be found in following URLs.
  User Log is located in the URL：https://10.30.1.23/status/history/2006-11-01
  Guests User Log is located in the URL：https://10.30.1.23/status/odhistory/2006-11-01

- **Management IP Address List:** Set the IP addresses within a range which the administrator can use to connect to the web management interface of DSA-3600 via its WAN and/or LAN ports. For example, if 10.2.3.0/24 is set in this list, it means as long as the administration PCs are within the IP address range of 10.2.3.0/24, the administrator can reach the administration page of DSA-3600. If the bit number of the IP range is omitted, 32 are used to specify a single IP address.

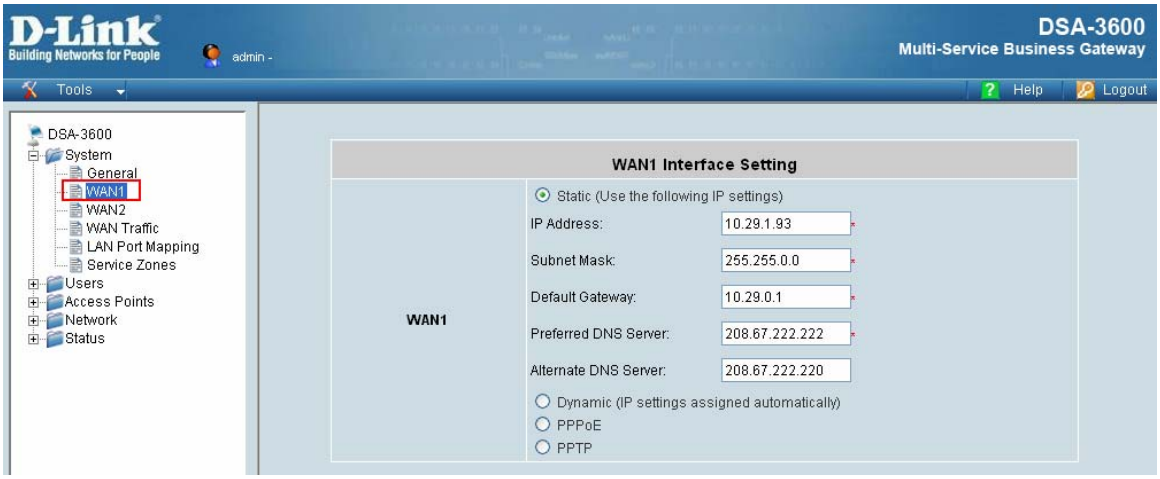
  PLEASE NOTE: While the default IP address of Network Interface is changed at **System→Service Zones→Basic Settings→DHCP Server→Enable DHCP Server,** the management IP address has to be setup again from default IP address to the new IP as the format, x.x.x.x/x.
- **SNMP:** The DSA-3600 supports SNMPv2. If the function is enabled, the Manager IP address and the SNMP community name have to be configured to allow the SNMP server to access the management information base (MIB) of DSA-3600.
- **HTTPS Protected Login:** Enable this function to activate https (encryption) or disable this function to activate http (non encryption) user login page.
- **Time:** The DSA-3600 supports NTP communication protocol to synchronize the system time with remote time servers. At least one NTP server has to be configured with the correct time zone, together with the IP address of the NTP server in order to enable the DSA-3600 to automatically adjust its system time with the configured NTP server. Up to five NTP servers may be configured in the system. The system time can also be manually configured when selecting **Manually set up**. Please enter the date and time into the respective fields.





4.1.2 WAN1

There are four methods of obtaining IP address for the WAN1 Port: **Static**, **Dynamic**, **PPPoE**, and **PPTP**.



- **Static (Use the following IP Settings):** Select **Static** to specify a static IP address for WAN1 port manually when a static IP address is available for DSA-3600. Fields with red asterisks are required to be filled in.

  IP Address: The IP address of the WAN1 port.

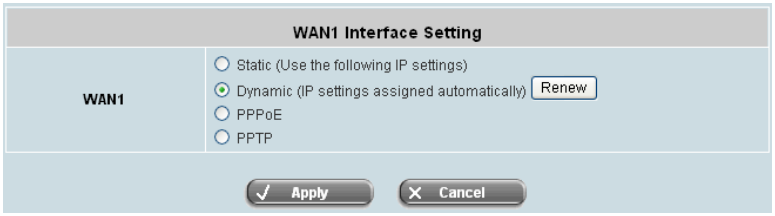
  Subnet Mask: The subnet mask of the WAN1 port.

  Default Gateway: The gateway of the WAN1 port.

  Preferred DNS Server: The primary DNS Server of the WAN1 port

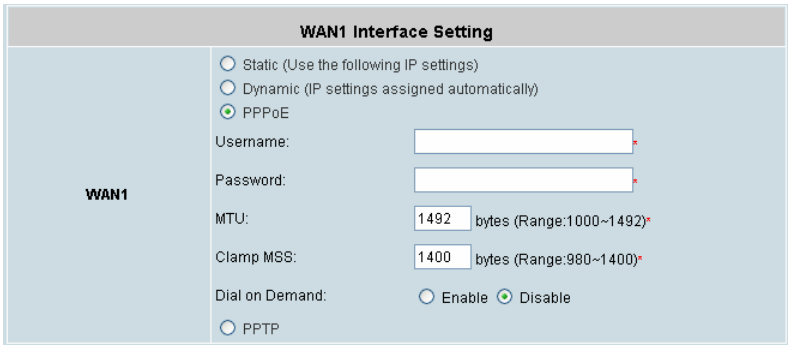
  Alternate DNS Server: The substitute DNS Server of the WAN1 port. This is optional.

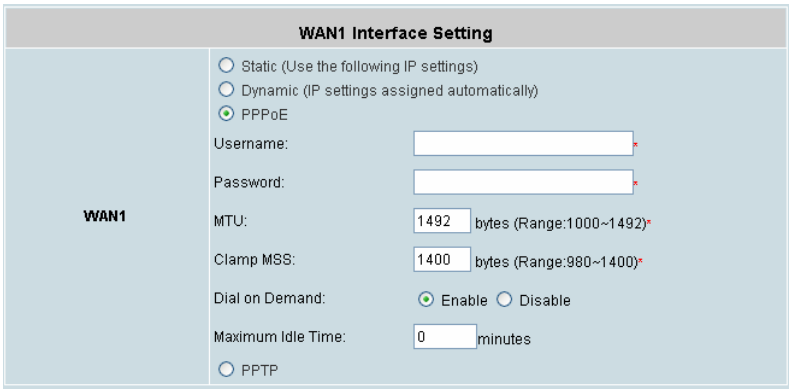
- **Dynamic (IP settings assigned automatically):** This connection type is only applicable when the DSA-3600 is connected to a network with the presence of a DHCP Server. Select the option when a DHCP server is available in the network implementation above the WAN1 port of the system. When Dynamic is selected, the system works as a DHCP client and get an IP address for its WAN1 port automatically from the DHCP server.



- **PPPoE:** This is the common connection type for ADSL. To properly configure PPPoE connection type, the **Username**, **Password**, **MTU** and **Clamp MSS** fields are required. The **Dial on Demand** function is used to guard the idle time out of the connection. The **Maximum Idle Time** field is required to enable this function. When the idle time is reached, the connection will be automatically disconnected.

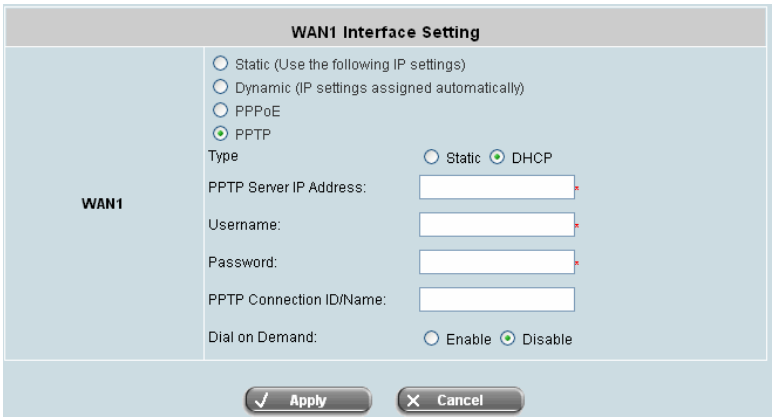
  Select the option when PPPoE is the connection protocol provided by the network service providers. When Dial on Demand is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached.

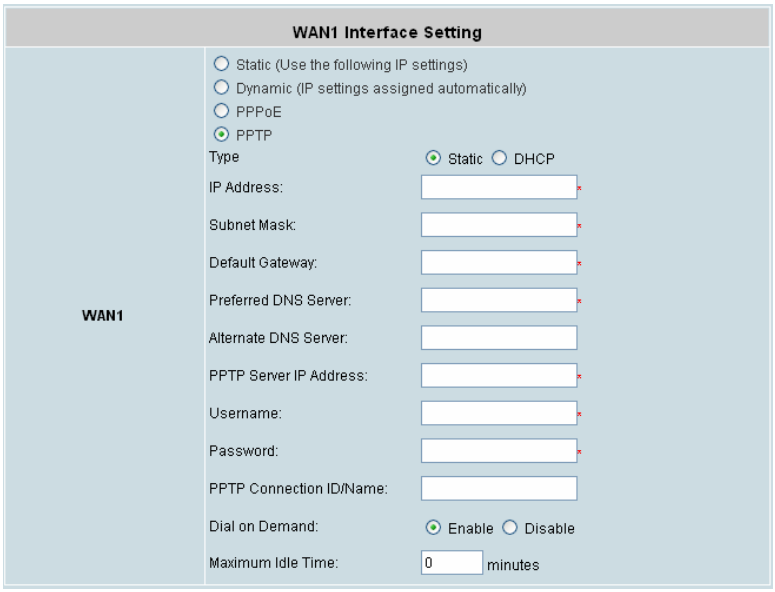




- **PPTP:** Point to Point Tunneling Protocol is a service that applies to broadband connection used mainly in Europe and Israel. Select **Static** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on Demand** function under PPTP. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

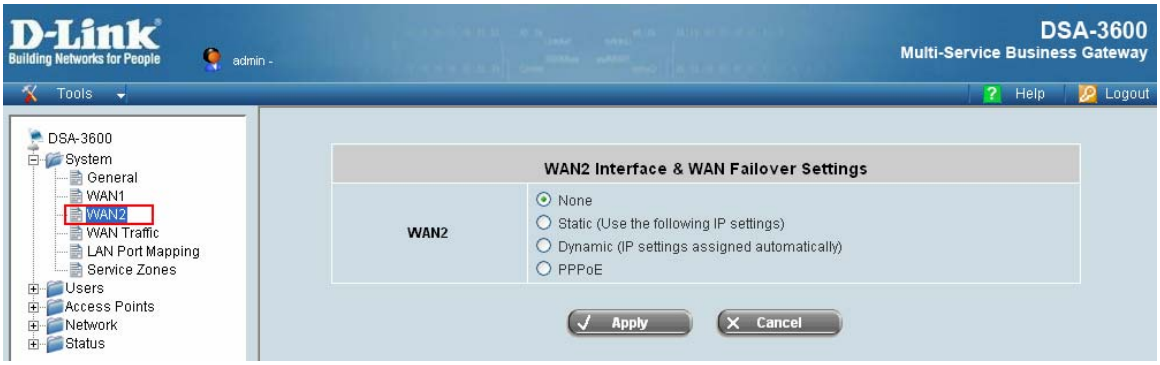
Select the option when PPTP (Point to Point Tunneling Protocol) is the connection protocol provided by the network service providers. When Dial on Demand is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached.



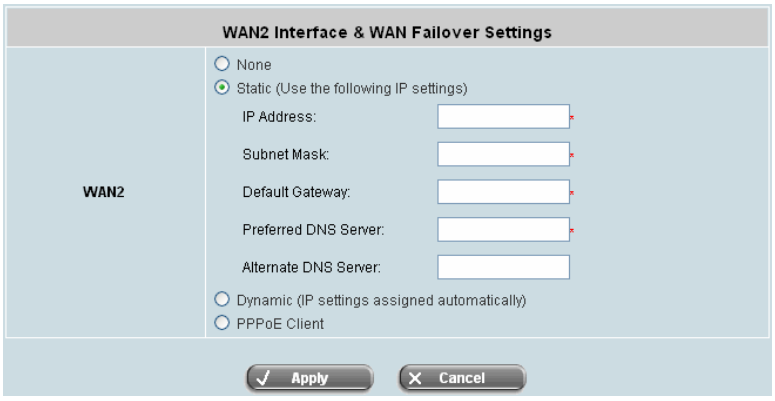


4.1.3 WAN2

The WAN2 can be disabled when selecting **None**. When WAN2 Port is enabled, it supports 3 connection types: **Static**, **Dynamic** and **PPPoE**.



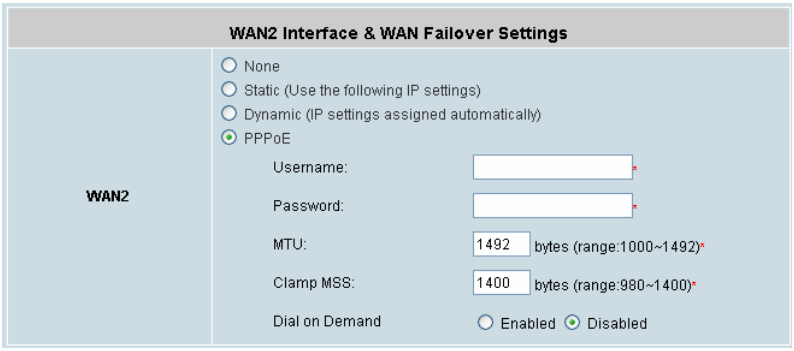
- **None**: The WAN2 Port is disabled.
- **Static (Use the following IP Settings):** Specify the **IP Address**, **Subnet Mask**, **Default Gateway, Preferred DSN Server and Alternate DSN Server** of WAN2 Port, which should be applicable for the network environment. Select the option to specify a static IP address for WAN2 interface manually when a static IP address is available for the system.

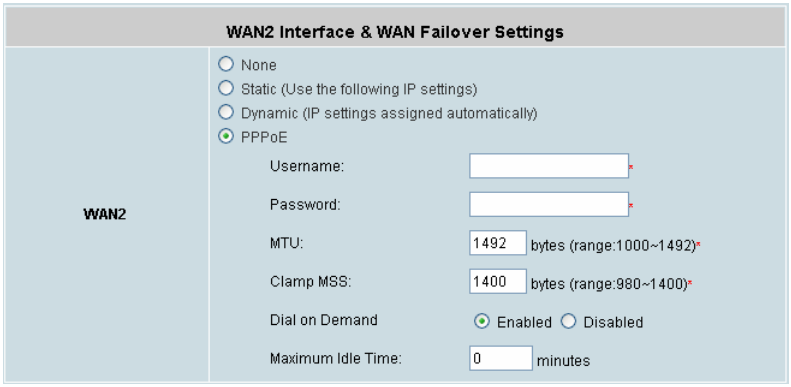


- **Dynamic (IP settings assigned automatically):** Select the option when a DHCP server is available in the network implementation above the WAN2 port of the system. When Dynamic is selected, the system works as a DHCP client and get an IP address for its WAN2 port automatically from the DHCP server.

- **PPPoE:** Select the option when PPPoE is the connection protocol provided by the network service providers. When Dial on Demand is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached. This is the common connection type for ADSL. To properly configure PPPoE connection type, the **Username**, **Password**, **MTU** and **Clamp MSS** fields are required. The **Dial on Demand** function is used to guard the idle time out of the connection. The **Maximum Idle Time** field is required to enable this function. When the idle time is reached, the connection will be

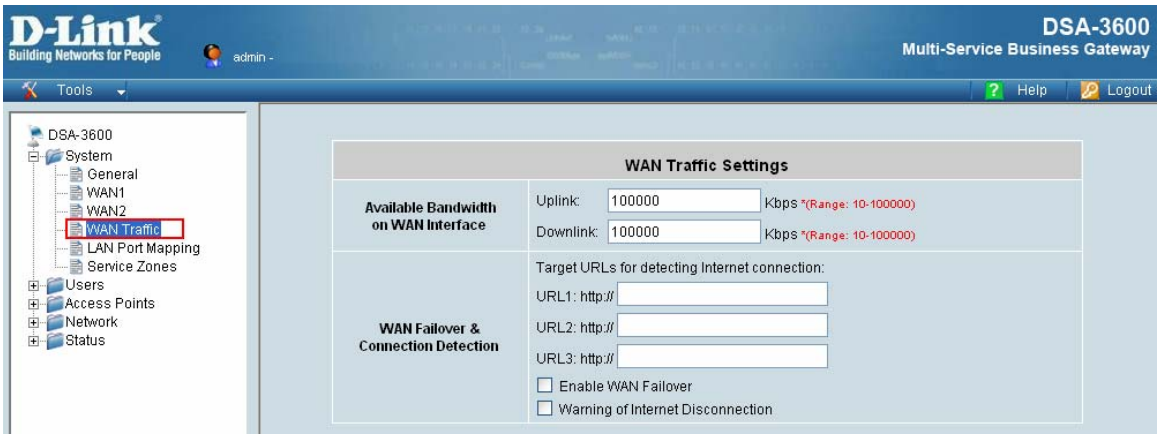
automatically disconnected.

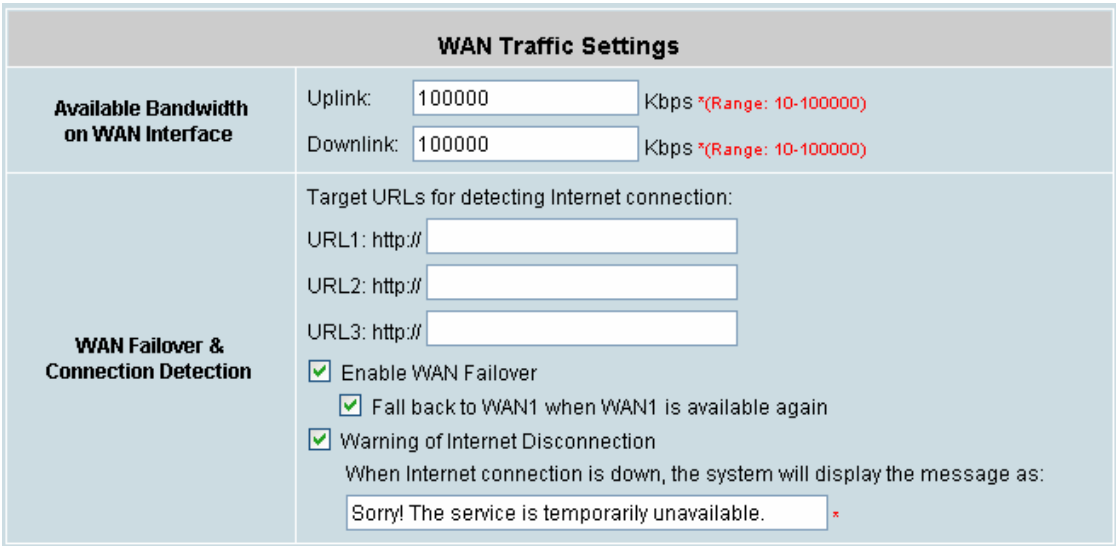




4.1.4 WAN Traffic

DSA-3600 supports uplink/downlink bandwidth management and WAN Failover feature.





Available Bandwidth on WAN Interface:

- **Uplink:** It defines the maximum uplink bandwidth allowed to share by clients within WAN interface.
- **Downlink:** It defines the maximum downlink bandwidth allowed to share by clients within WAN interface.
- **WAN Failover & Connection Detection:** The system supports WAN Failover feature. Check Enable WAN Failover to activate this function.

WAN Failover & Connection Detection: The DSA-3600 supports WAN Failover feature and the ability to detect WAN connection. Check **Enable WAN Failover** check box to activate WAN Failover function.

- **Target URLs:** To verify the connection to the internet, the system keeps up to three target URLs. These URLs are used for the system as the detected targets of WAN Failover and Warning of Internet Disconnection. To enable WAN Failover, at least one URL must be configured in the Target URLs.
- **Enable WAN Failover:** The purpose of WAN Failover is to have a backup link for WAN1 when WAN2 is available. Check the check box of Enable WAN Failover to active the WAN failover function of the DSA-3600. Normally a service zone uses WAN1 as it primary gateway. WAN Failover is to have a backup link for WAN1 if WAN2 is available. WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a service zone's policy can also use WAN2 as its gateway; in that case, if WAN2 is down, the WAN2's traffic under its policy also will be routed to WAN1.

- **Fall back to WAN1 when WAN1 is available again:** If **WAN Failover** is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. A Fall back to WAN1 when WAN1 is available again function will appear when Enable WAN Failover check box is checked. If **Fall back to WAN1 when WAN1 is available again** function is enabled, the routed traffic will be back to WAN1 when WAN1 connection is recovered.
- **Warning of Internet Disconnection:** An Internet disconnection detection feature is supported by the system. Check the check box of Warning of Internet Disconnection will enable this function. There is a text box available for the administrator to enter a reminding message. This reminding message will appear on clients' screens when Internet connection is down.

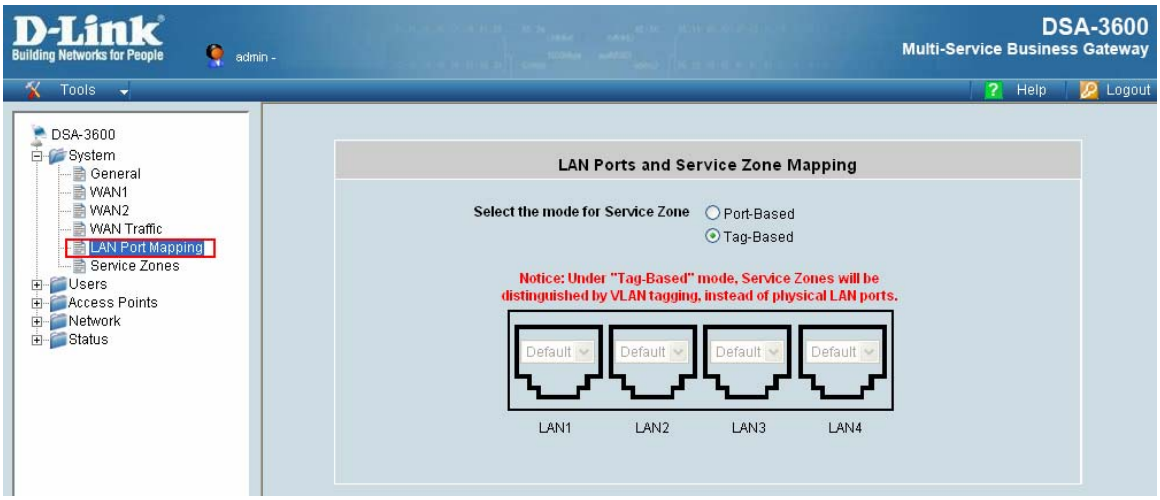
4.1.5 LAN Port Mapping

The DSA-3600 supports multiple service zones in either of the two VLAN modes, **Port-Based VLAN** or **Tag-Based VLAN**, but not concurrently. In the wireless environment, a service zone of the DSA-3600 is mapped to the VLAN with an associated SSID. When the DSA-3600 is set for tag-based VLAN, a managed Access Point with multiple SSIDs turned on can service multiple service zones. It is recommended that the administrator decides a mode before the system configuration when considering which mode is better for a multiple-service-zone deployment.

For more details about Service Zone, please refer to Chapter 4.3.

In LAN Port Mapping, the service zones can be configured by modes, **Port-Based,** which will be distinguished by physical LAN ports, or **Tag-Based**, which will be distinguished by VLAN tagging. Each LAN port of Port-Based mode can be selected among **Default** to **SZ1~SZ4**.

Supporting multiple service zones, one D-Link DSA-3600 system can behave virtually like multiple systems. Each service zone is one-to-one mapped to a VLAN. Messages to or from each service zone are sorted by the VLAN tag in the message frame.

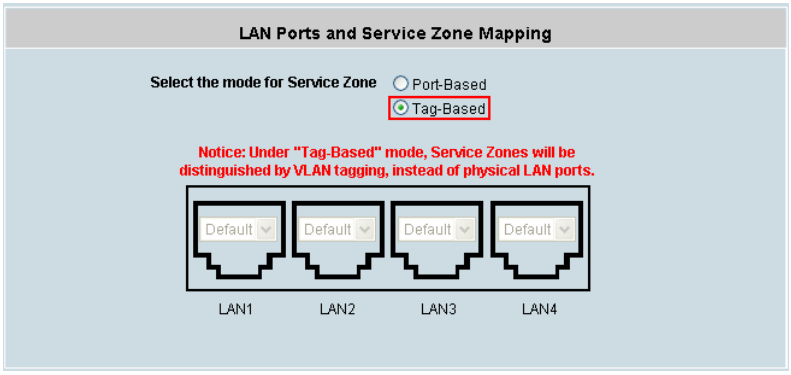


- **Tag-Based:**
  For tagged service zone, each LAN port is Hybrid port, which supports both tagged VLAN and untagged frames. Each port can join any VLAN (up to 4) group.

  The system supports five service zones, one default and other 4 service zones; each can be enabled of disable except the default one. The four service zones are mapped to 4 VLANs and the default service zone is mapped to 1 untagged subnet. Each service zone functions like a virtual system; each has an independent set of settings such as SSID, Wireless Security, Network setting, DHCP setting, Customized Pages, Default Policy, Authentication Servers setting and Default Authentication Server.

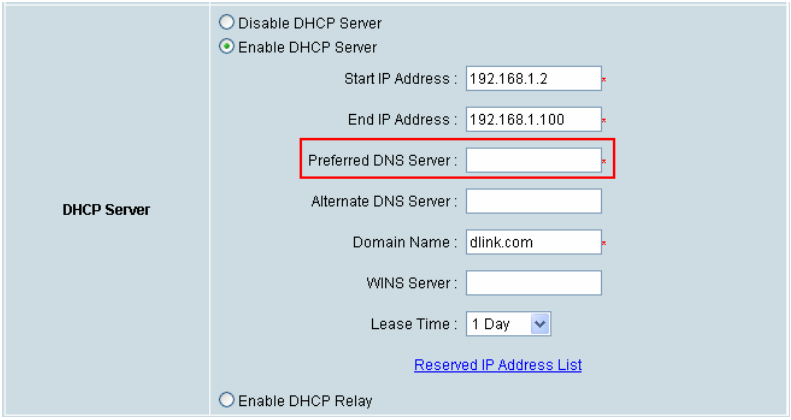
Tag-based Service Zones Configuration Example – Enabling Two Service Zones

Log in to the web management interface and enter **"admin"** for both the default username and password in the Username and Password fields of the Administrator Login Page. After logging-in the web management interface, from the Menu Tree, click ***System*** and then click ***LAN Port Mapping*** to verify that **Tag-Based** service zone mode is selected.



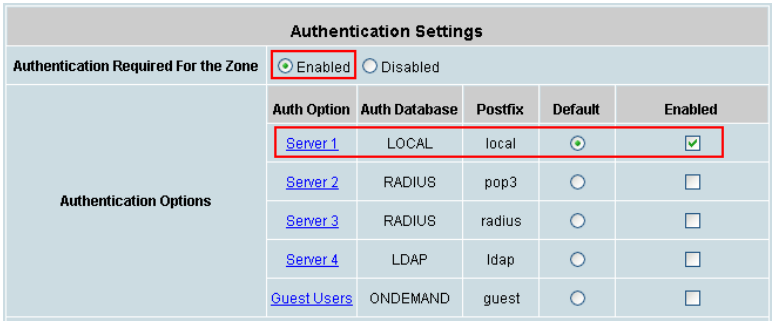
Click ***System*** and then click ***Service Zones*** to enter the **Service Zone Settings** page as shown below.

Click the ***Configure*** button of Default Service zone to enter its Basic Settings page. While in this Basic Settings page, enter an IP address for **Preferred DNS Server** in the area of DHCP Server. (Empty **Preferred DNS Server** will result in problems when using the Internet.)



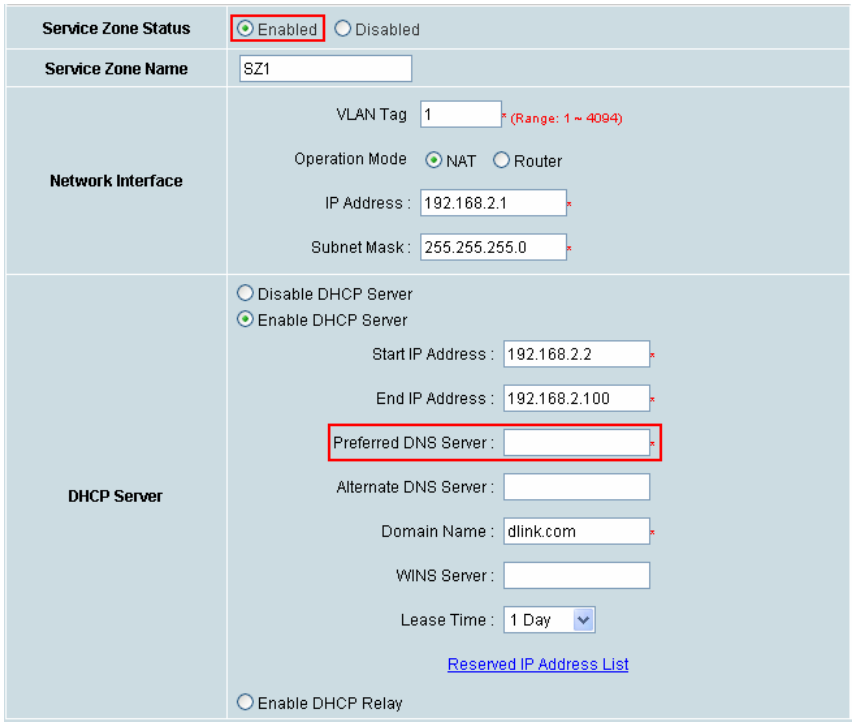
Scroll down to near bottom of page and in the Wireless Settings area enter the **SSID** (e.g. ssid-staff) for connecting to this service zone.

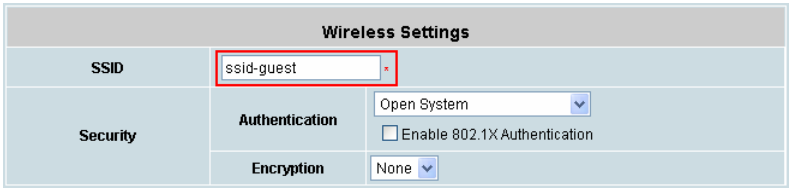
Scroll up to the middle of the page where the **Authentication Settings** is, and check the ***Enabled*** box for the **Authentication Required for the Zone** option. The users will now need to be authenticated to connect to the service zone. Make sure only Server1 is checked ***Enabled*** for this service zone.



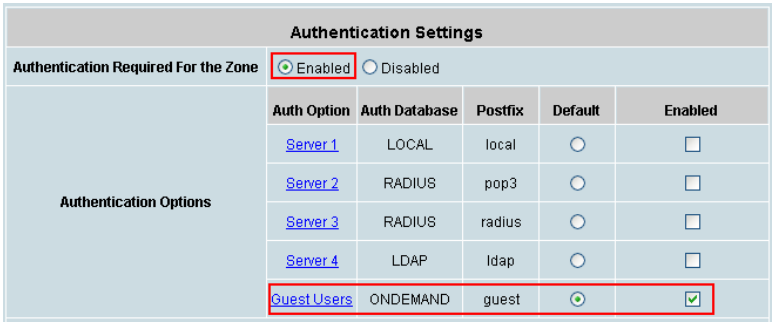
Click the ***Apply*** button to activate the changes for the default service zone. (We can restart the system later, since we want to continue to configure a second service zone for the guest users.)

Following similar procedures, click on **Service Zones** menu item on the Menu Tree again, this time is to configure another service zone such as SZ1. Enter its Basic Settings page. Enable the service zone, enter the IP address of the **Preferred DNS server**, and set its **SSID** for guests such as '**ssid-guest**'.





Remember to enable Authentication requirement for this service zone and enable the **Guest Users** authentication options only.



Click ***Apply*** to activate the changes for the second service zone. Now is the time to restart the system. After the restart, the system will be configured according to Figure-4.1.5a.

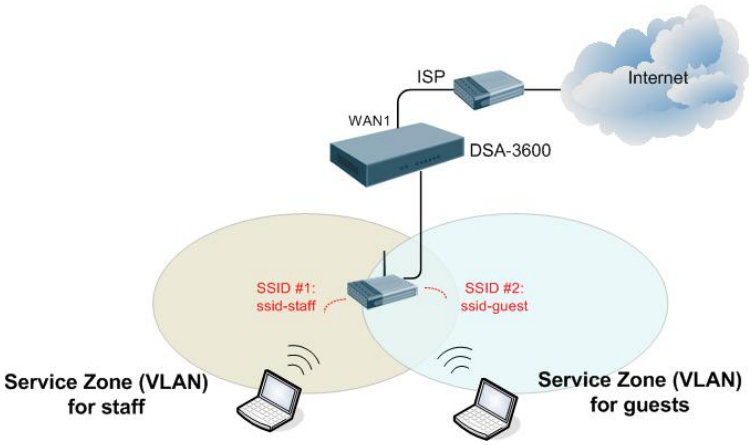
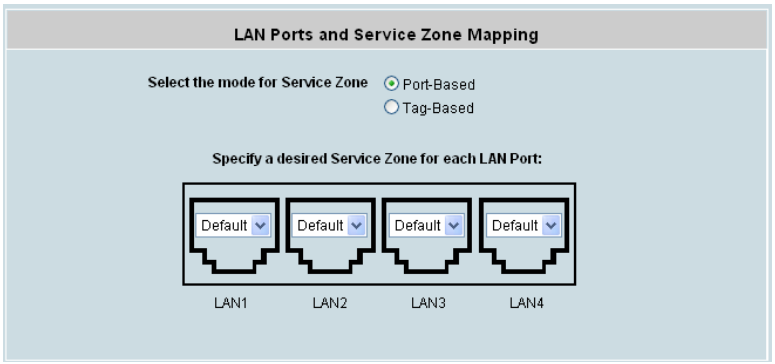


Figure-4.1.5a: An example using Tag-Based service zones

- **Port-Based:**

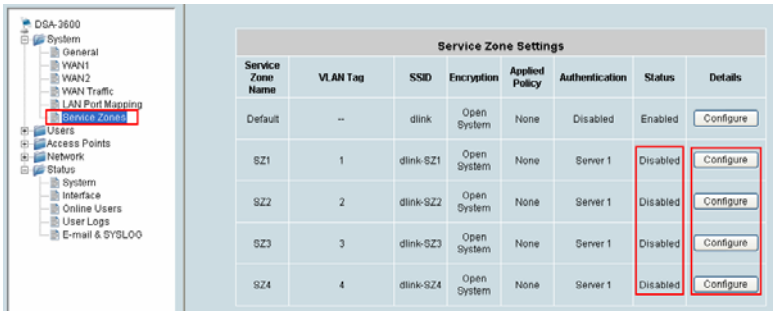
  For port-based service zone, each LAN port can be assigned to a service zone since a LAN port can be mapped to a VLAN tag. The mapping between the ports and the service zones are many-to-one. With factory default setting, all ports belong to the Default service zone and other 4 service zones are gray-out. The other 4 service zones will appear after the specific service zone is configured as enabled in **System** → **Service Zones**.



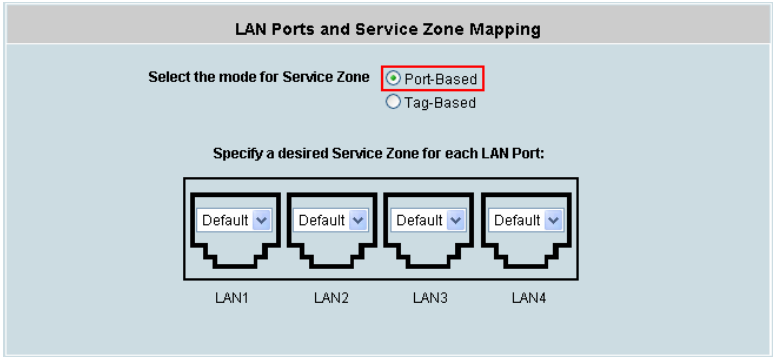
Port-based Service Zones Configuration Example

After running through **Setup Wizard** on a factory default system, the DSA-3600 is ready to use the default tag-based VLAN for separating networks.

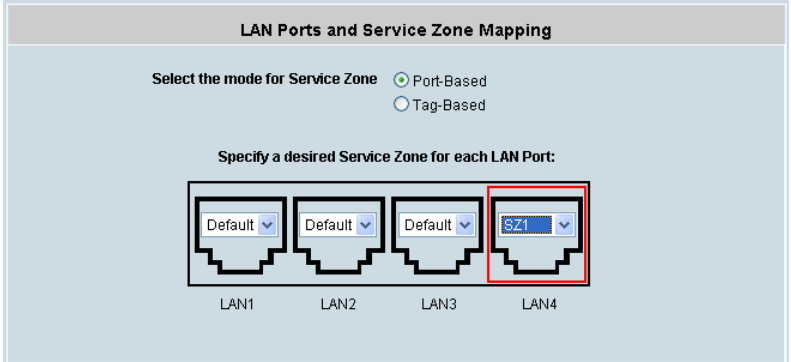
Log in to the web management interface and enter **"admin"** for both the default username and password in the Username and Password fields of the Administrator Login Page. After logging-in the web management interface, from the Menu Tree, click **System** then **Service Zones** to enter the Service Zone Settings page. Click ***Configure*** of the desired service zone to enter its Basic Settings page, and then enable the service zone used for port-based service zone deployment.



Click ***System*** from the Menu Tree and then click ***LAN Port Mapping***. Select **Port-Based** mode for service zone.



Assume LAN1, LAN2, LAN3 will be used by Default service zone for internal staff while LAN4 is to be assigned to another service zone for external guests only. In the abovementioned page, click **LAN4**'s drop-down menu to select the desired second zone such as 'SZ1' for LAN4 (select only enabled service zones). Click ***Apply*** and reboot the system.



In tag-based mode, each LAN port can serve traffic from any service zone because VLAN tags carried in message frame will not be modified. In port-based mode, each LAN port can only service traffic of one service zone, where all messages through the LAN port will be re-tagged with the tag assigned to the port. Compare Figure-4.1.5a and Figure-4.1.5b to see the differences.

For single zone deployment, use the Default service zone with port-based mode.

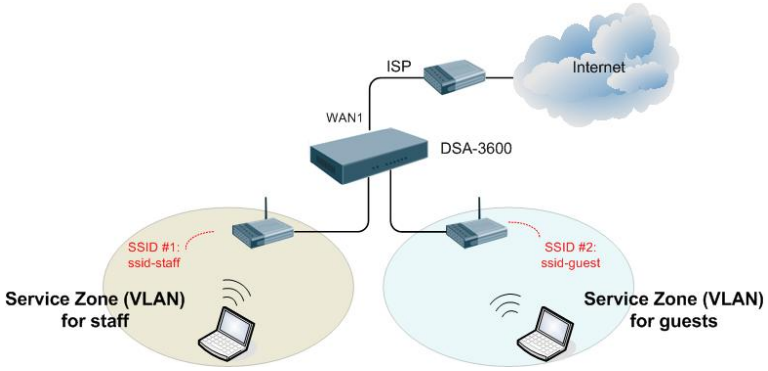


Figure-4.1.5b: An example using Port-Based service zones

4.1.6 Service Zones

There are five types of Service Zone Settings: **Default, SZ1, SZ2, SZ3** and **SZ4.** Click ***Configure*** button to complete the settings of each Service Zone.

For more details about Service Zone, please refer to Appendix E and F.

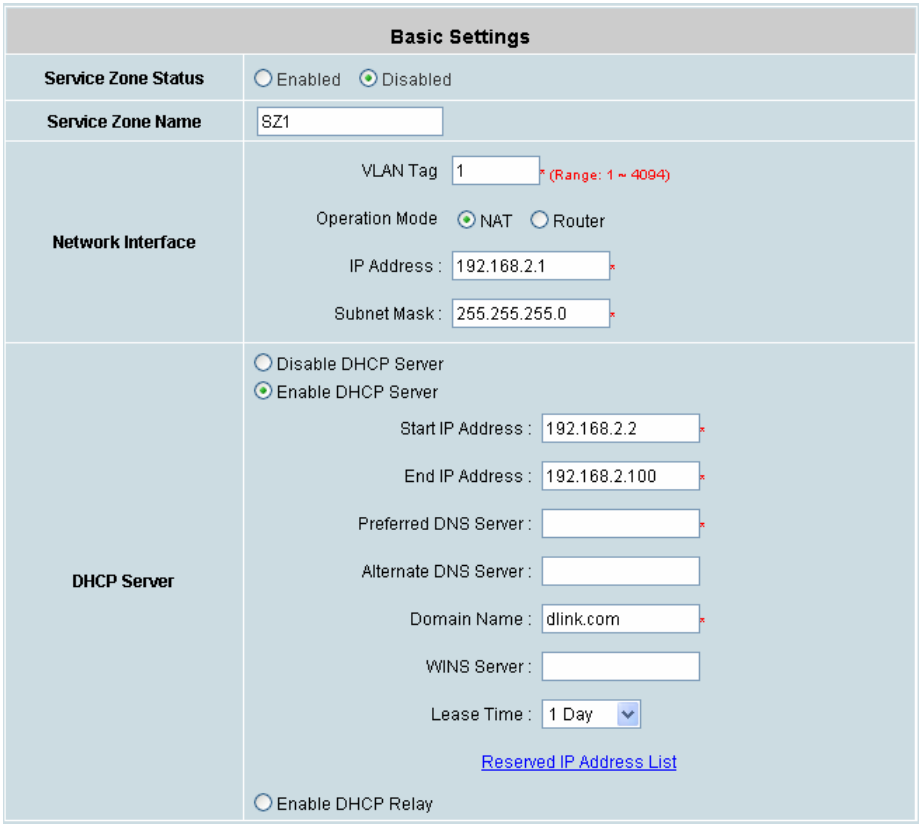
- **Service Zone Name:** Enter a name of this service zone.
- **VLAN Tag:** Each service zone is one-to-one mapped to the VLAN. Messages to each service are sorted by the VLAN tag in the message frame.
- **SSID:** Each service zone must setup its own SSID.
- **Encryption:** Encryption supports WEP (64/128 bit), WPA and WPA2 for AP security.
- **Applied Policy:** The policy plan applied to the service zone settings.
- **Authentication:** There are 5 authentication methods that DSA-3600 supports: **Local**, **POP3**, **RADIUS**, **LDAP** and **NT Domain**. The selected authentication method in Authentication Settings will be shown in this column.
- **Status:** Each service zone can be enabled or disabled.
- **Details:** Setup detailed settings for each service zone.

Click the button of ***Configure***, more configurations will appear, including **Basic Settings**, **Authentication Settings** and **Wireless Settings**. The managed AP(s) in the specific service zone will be shown in this page as well if there is an AP set in this service zone.

1) Service Zone Settings – Basic Settings

The system supports three types of DHCP modes, **Disable DHCP Server**, **Enable DHCP server**, and **Enable DHCP relay**. Each service zone can have its own DHCP setting. Select the radio button of Disable DHCP Server to disable the built-in DHCP server when clients are assigned static IP addresses. Select the radio button of Enable DHCP Server to enable the built-in DHCP server. When the Enable DHCP server is chosen, the system will act as a DHCP server and assign IP addresses to its clients. Select the radio button of Enable DHCP Relay when a service zone is connected to an external DHCP server. When Enable DHCP Relay is chosen, the IP addresses of clients will be assigned by an external DHCP server. The system will only relay DHCP

information from the external DHCP server to downstream clients of this service zone.

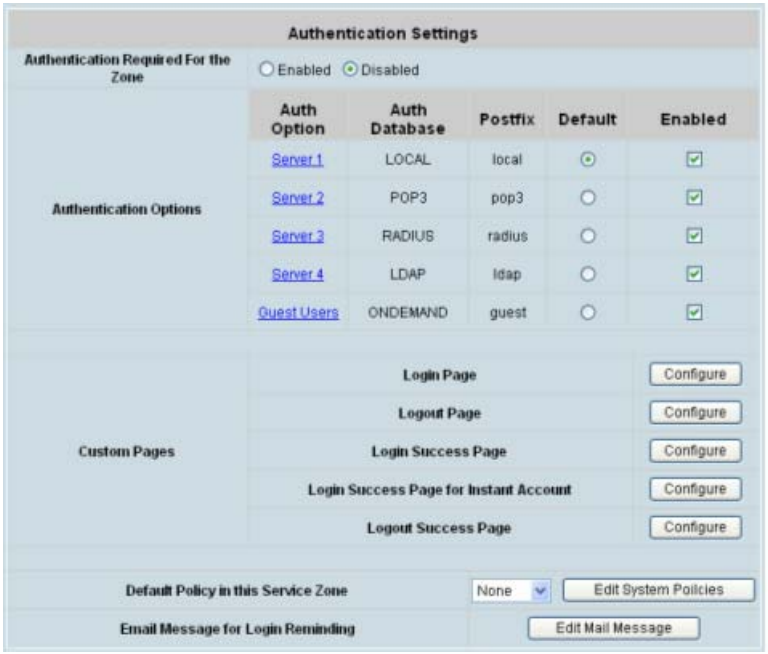


- **Service Zone Status:** Each service zone can be enabled or disabled except the default service zone.
- **Service Zone Name:** The name of service zone can be input here.
- **Network Interface:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
- **VLAN Tag:** An identifier associates a frame with a specific VLAN and provides the information needed to process the frame.
- **IP address:** The IP Address of this service zone.
- **Subnet Mask:** The subnet Mask of this service zone.
- **DHCP Server:** Related information needed on setting up the DHCP Server is described as follows: DHCP pool Start IP Address, DHCP pool End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List.
- **WINS Server IP:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
- **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.
- **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with certain MAC address.
- **Domain Name:** Enter the Windows domain name for this service zone.
- **Enable DHCP server:** This allows the enabling/disabling the built-in DHCP server.
- **Start IP / End IP:** Set a range of IP addresses that built-in DHCP server will assign to clients. Please

change it accordingly at System→General→Management IP Address List to let the administrator to login to the DSA-3600 admin page after the default IP address of Network Interface is changed.

2) Service Zone Settings – Authentication Settings

The system supports five types of authentication database that are Local, POP3, RADIUS, LDAP, and NT Domain and provides up to four authentication options and one Guest Users authentication option. The administrator needs to activate and configure at least one of these authentication databases for an enabled service zone. Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Each authentication option is distinguished by the postfix in clients' username such as "user1@postfix1". One of authentication database can be assigned as default for a service zone. For authentication option assigned as default, the postfix can be omitted while entering username.

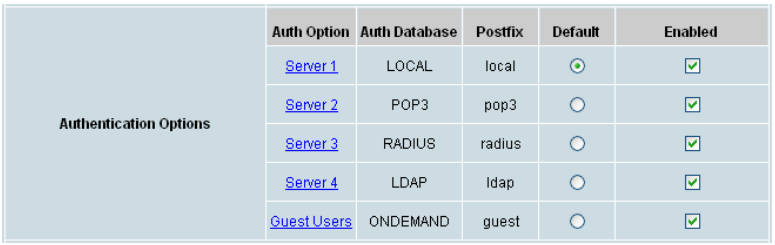


- **Custom Pages:** There are five users' login and logout pages that can be customized by administrators for each service zone.
- **Default Policy in this Service Zone:** There are one Global and eight sets of policy supported by the system. Each policy contains options for setting Firewall, Specific Route, Schedule, QoS, and Privilege. Global policy only has Firewall and Specific Route profile. Policies can be defined in the policy tab. The administrator can select one of the defined policies to apply it to the specific service zone.
- **E-mail Message for Login Reminding:** Click ***Edit Mail Message*** to change the content for Login reminding words. Clients will receive an e-mail with this reminding content when they access their mail servers before logging in the system.

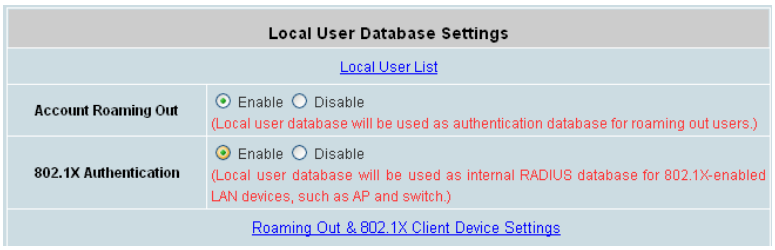
2.1) Authentication Options

Click the hyperlink of **Auth Option**, the **Authentication option** page will appear, showing options for **Server1** to **Server4** and **Guest Users.**

Click the button of ***Configure*** to have further configuration.



Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	◉	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
	Guest Users	ONDEMAND	guest	○	☑



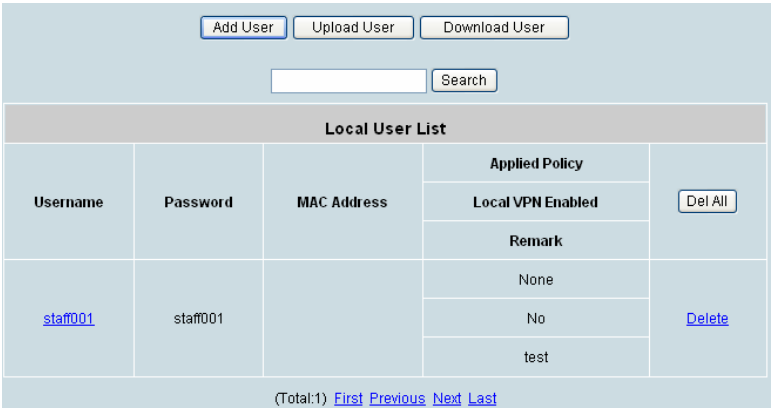
Local User Database Settings	
Local User List	
Account Roaming Out	◉ Enable ○ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	◉ Enable ○ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
Roaming Out & 802.1X Client Device Settings	

- **Name:** Set a name for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Postfix:** A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Warning: *The Postfix Name cannot contain these words: MAC and IP.*

- **Black List:** There are five sets of the black lists. Select one of them or choose **"None"**. Please refer to **4.2.2 Black List**.
- **Authentication Database:** There are five authentication methods, **Local, POP3**, **RADIUS**, **LDAP** and **NT Domain**, to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration. Local authentication method can be chosen for one Auth Option.

Click the hyperlink ***Configure*** to enter the Local User Database Settings and then click the hyperlink ***Local User Setting***:

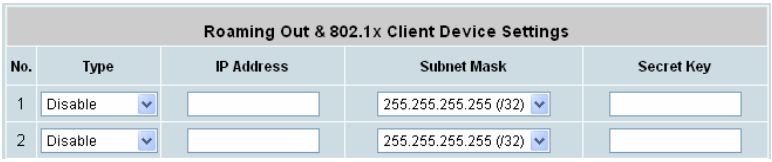


- **Add User:** Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"**. Select a desired **Policy and choose whether to enable Local VPN.** Only **"Username"** and **"Password"** are required information. The rest are optional.
  For the Policy configuration, please check section on Policy Configuration.

Click ***Apply*** to complete adding the user or users.

- **Upload User:** Click this to enter the **Upload User From File** interface. Click the ***Browse*** button to select the text file for uploading user account, then click ***Upload*** to execute the upload process.
  The file for uploading should be a text file containing in each line the following information: ***Username, Password, MAC Address, Applied Policy, Remark, Local VPN enabled***. There must be no spaces between the fields and commas. The MAC field can be omitted, but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by the new.
- **Download User:** Use this function to create a .txt file with all built-in user account information and then save it on disk.
- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- **Del All:** Click on this button to delete all the users at once and click on **Delete** to delete the user individually.
- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **Editing Existing User Data** Interface for that particular user, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"**, **"Policy"** and **"Remark"** (optional) . Then, click ***Apply*** to complete the modification.
- **Account Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled, this system acts as a RADIUS server for other external RADIUS clients. The Local user with RADIUS roaming out permission needs to be configured in the *Roaming out & 802.1X Client Device Settings* first. The Local user in the list may then log on the system via the other domain, such as a branch office, as long as the RADIUS clients are configured accordingly. Selecting either of the options will bring up the hyperlink called ***Roaming out & 802.1X Client Device Settings***.

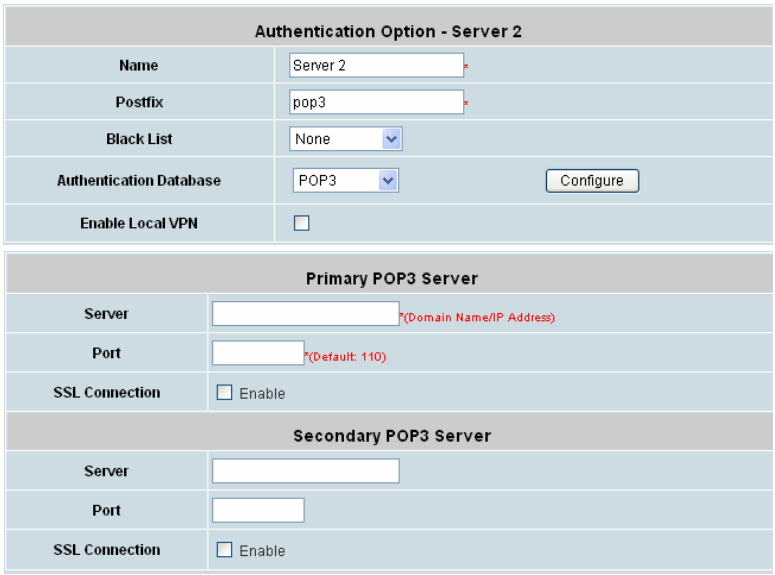
Click the hyperlink ***Roaming out & 802.1X Client Device Settings*** to enter the **Roaming out & 802.1X Client Device Settings** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1X**, and key in the related data and then click ***Apply*** to complete the settings.



- **802.1x Authentication:** 802.1x is the IEEE security standard for wired and wireless LANs. It encapsulates EAP (Extensible Authentication Protocol) processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client (called a supplicant in 802.1x parlance) and the authentication server (such as a RADIUS), letting the "authenticator" middleman simply pass the packets back and forth.

2.1.1) Authentication Options → POP3

POP3 refers to Post Office Protocol 3, a standard protocol used to retrieve e-mail stored in a mail server. The system may authenticate users by using POP mail accounts. Two POP3 servers are supported by the system: primary and secondary. When POP3 Server is enabled, at least one POP3 server will be required. Local VPN function can be enabled for clients authenticated by POP3 authentication method.



- **Server:** Set a name for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

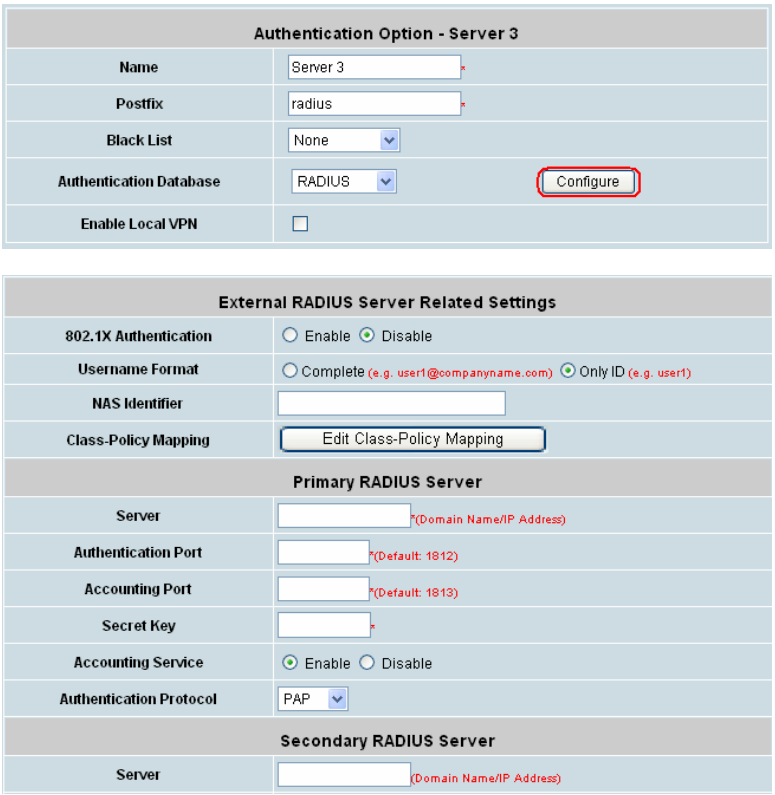
Warning: *The Postfix Name cannot contain these words: MAC and IP.*

- **Black List:** There are five sets of the black lists. Select one of them or choose **"None"**. For details, please refer to **4.2.2 Black List.**
- **Authentication Database:** There are five authentication methods, **Local, POP3**, **RADIUS**, **LDAP** and **NT Domain**, to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration. Local authentication method can be chosen for one Auth Option.
- **Server:** Enter the IP address/domain name given by the ISP.
- **Port:** Enter the Port given by the ISP. The default value is 110.
- **SSL Setting**: If this option is enabled, the POP3 protocol will perform the authentication.

2.1.2) Authentication Options → RADIUS

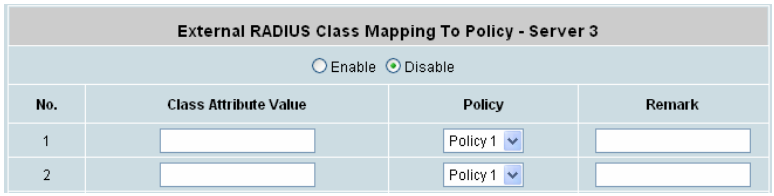
RADIUS refers to Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). The system may authenticate users using external RADIUS server including both primary and secondary RADIUS server.

Click the hyperlink ***Configure*** for further configuration. The RADIUS server sets the external authentication for clients. Enter the related information for the primary RADIUS server and/or the secondary RADIUS server (the secondary server is not required). Information must be entered for fields with red asterisks. These settings will be effective immediately after clicking the Apply button.



- **802.1X Authentication:** Select the *Enable* radio button to enable this function and the hyperlink ***802.1X Client Device Settings*** will appear. Click the hyperlink ***802.1X Client Device Settings*** and the **Roaming Out & 802.1X Client Device Settings** interface will show up. For more information about ***Roaming out & 802.1X Client Device Settings***, please refer previous description in Authentication Options → Local.
- **Username Format:** Complete means to send completed username to the RADIUS server for authentication, and Only ID means only send user ID without postfix to the RADIUS server for authentication.
- **NAS Identifier:** This is a Network Access Server (NAS) Identifier of this system for the external RADIUS server.
- **Class-Policy Mapping**

  This function applies the selected policy to specific clients grouped by the RADIUS class attribute. The clients will be applied with the assigned policy while logging on to the system.



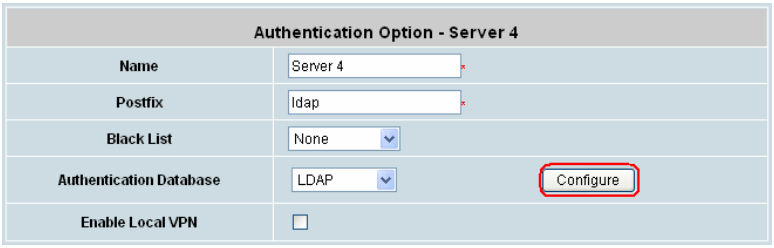
- **Server:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port of the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the **"Accounting Service"** for accounting capabilities.
- **Authentication Protocol:** There are two methods for selection: CHAP or PAP.

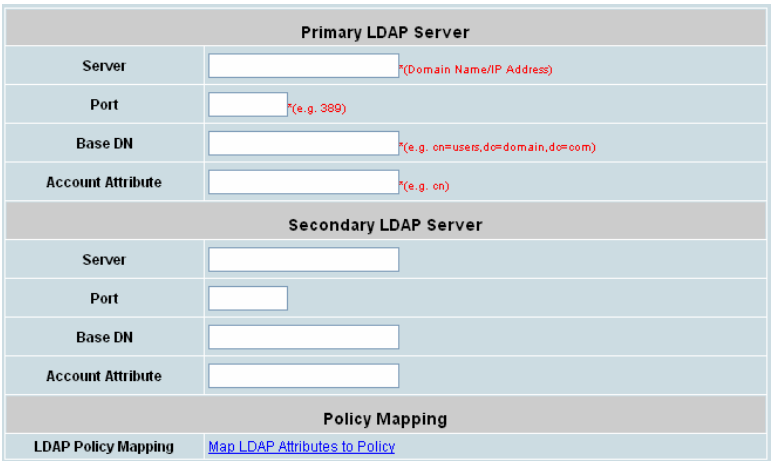
Notice: *If the RADIUS Server does not assign idle-timeout value, the DSA-3600 will use the local idle-timeout.*

2.1.3) Authentication Options → LDAP

LDAP refers to Lightweight Directory Access Protocol, a set of protocols for accessing information directories. The system may authenticate users using external LDAP server including primary and secondary.

Click the hyperlink ***Configure*** for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). Information is required for fields with red asterisks. These settings will be effective immediately after clicking the *Apply* button.

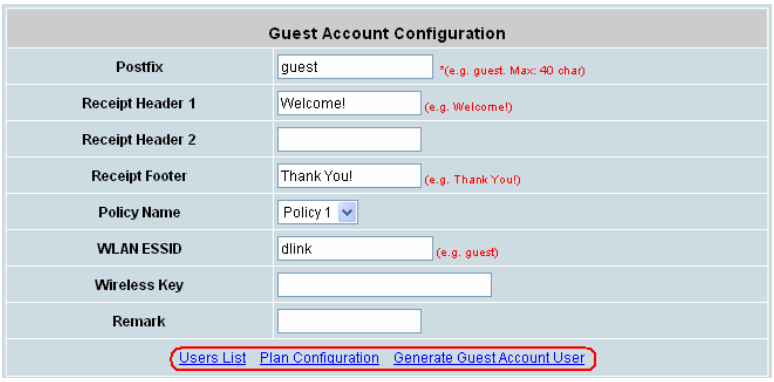




- **Server:** Enter the IP address/domain name of the LDAP server.
- **Port:** Enter the Port of the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name of the LDAP server.
- **Account Attribute**: Use the user account's login username and password of the system, and then type one Account Attribute (UID, CN) to access the LDAP server.
- **LDAP Policy Mapping**: This function is to apply selected policy to certain clients grouped by LDAP attribute. The clients will be applied with the assigned policy while logging on the system.

2.1.4) Authentication Options → On-demand

This is needed in a retail environment. When customers need to use wireless Internet in a store, they have to get printed receipts with username and password from the store to log in the system for wireless access.

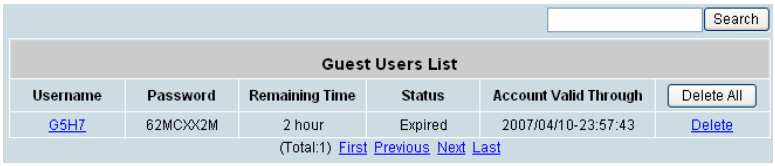


- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Receipt Header:** There are two fields, Receipt Header 1 and Receipt Header 2, for the receipt's header. Enter receipt header message or use the default.

- **Receipt Footer**: Enter receipt footer message here or use the default.
- **Policy Name:** Select a policy applied to Guest account.
- **WLAN ESSID:** Enter the ESSID of the AP which will print on the receipt for clients' reference.
- **Wireless Key:** Enter the key of the AP which will print on the receipt for clients' reference.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.

2.1.5.1) Authentication Options → Guest Users → **Users List**

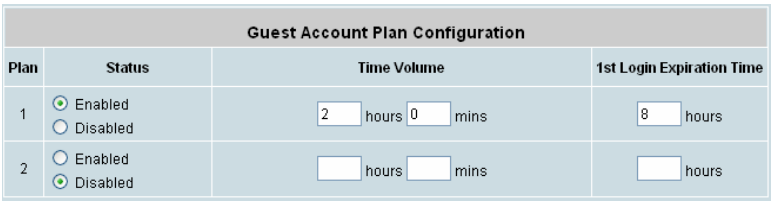
Click to enter the Guest Users List page's screen. By default, the On-demand Guest user database is empty.



- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the Instant user.
- **Password:** The login password of the Instant user.
- **Remaining Time:** The total Time that the user can use currently.
- **Status:** The status of the account.
  - Normal indicates that the account is not in-use and not overdue.
  - Online indicates that the account is in-use and not overdue.
  - Expire indicates that the account is overdue and cannot be used.
- **Account Valid Through:** The expiration time of the account.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

2.1.5.2) Authentication Options → Plan Configuration → **Plan Configuration**

Click this to enter the Guest Account Plan Configuration screen. In the Guest Account Plan Configuration screen, the administrator may configure up to 10 billing plans.

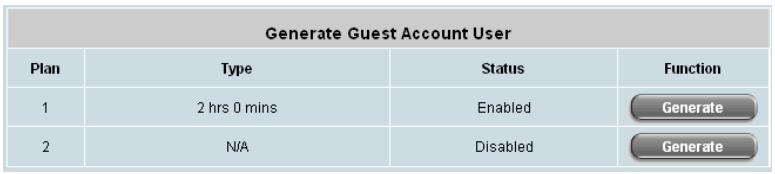


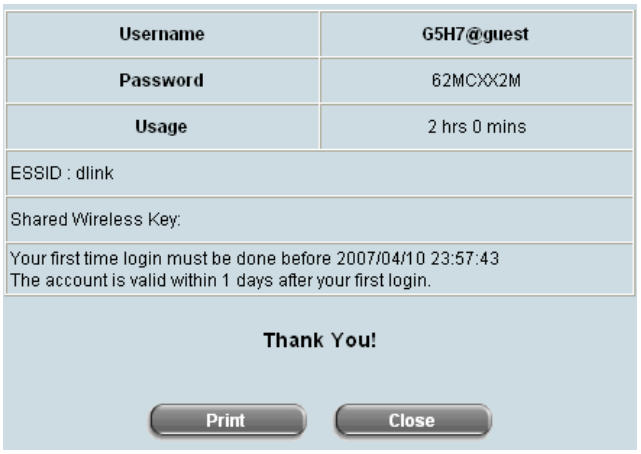
- **Status:** Select to enable or disable this account plan.
- **Time Volume:** Set the guest account plan by inputting hours and minutes
- **1st Login Expiration Time:** This is the time period that the client has to activate the account after the account is generated. After this time, the account will self-expire.

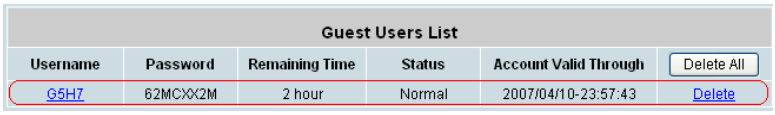
2.1.5.3) Authentication Options → Guest Users → **Generate Guest Account User**

Click this to enter the Generate Guest Account User screen. Click on the ***Generate*** button of the desired plan and a guest account will be created. Click ***Print*** to print a receipt which will contain the guest user's information, including the username and password.

Note: The printer used by ***Print*** is a local printer connected to the administrator's computer or a printer pre-configured by the administrator



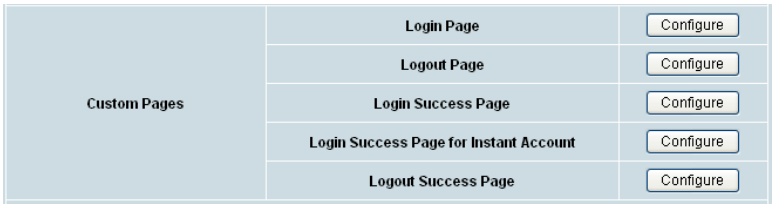




2.2) Custom Pages

There are five users' login and logout pages for each service zone that can be customized by administrators.

Click the button ***Configure***, and the **Login (Logout)** page will appear, with configuration options for **Login Page**, **Logout Page**, **Login Success Page**, **Login Success Page for Instant Account** and **Logout Success Page.** Click the button of the respective page selections to make further configuration.

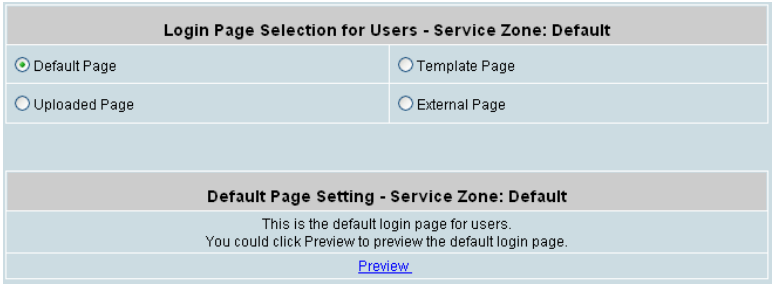


2.2.1) Custom Pages → **Login Page**

The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login page.

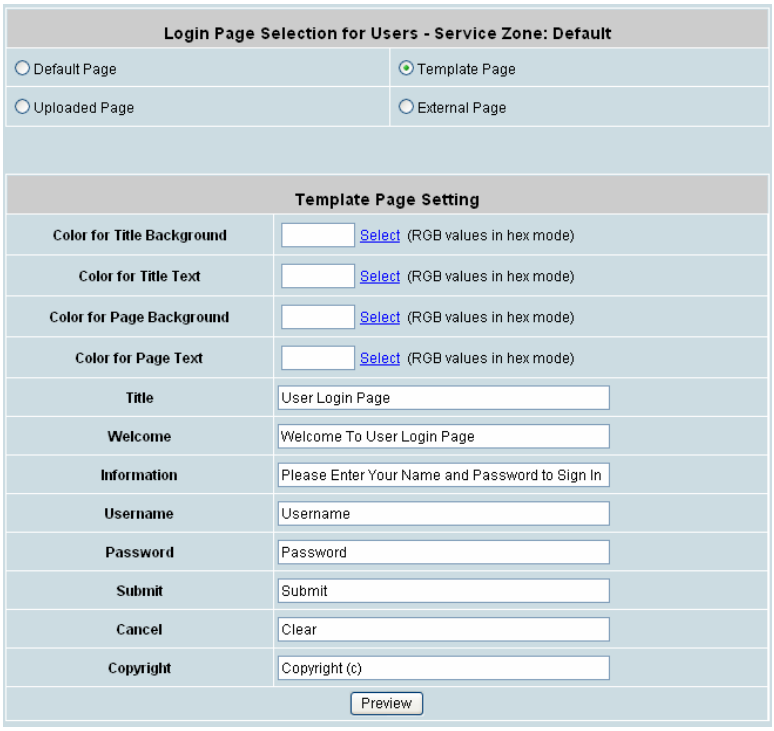
- *Custom Pages → Login Page →* ***Default Page***

  Choose Default Page to use the default login page.



- *Custom Pages → Login Page →* ***Template Page***

  Choose Template Page to make a customized login page. Click Select to pick up a color and then fill in all of the blanks. Click Preview to see the result first.



- *Custom Pages → Login Page →* ***Uploaded Page***

  Choose Uploaded Page and upload a login page.

  The user-defined login page must include the following HTML codes to provide the necessary fields for username 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>
```

If the user-defined login page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

Remote VPN	**: <img src=images/xx.jpg”>**
Default Service zone	**: <img src=images0/xx.jpg”>**
Service zone 1	**: <img src=images1/xx.jpg”>**
Service zone 2	**: <img src=images2/xx.jpg”>**
Service zone 3	**: <img src=images3/xx.jpg”>**
Service zone 4	**: <img src=images4/xx.jpg”>**

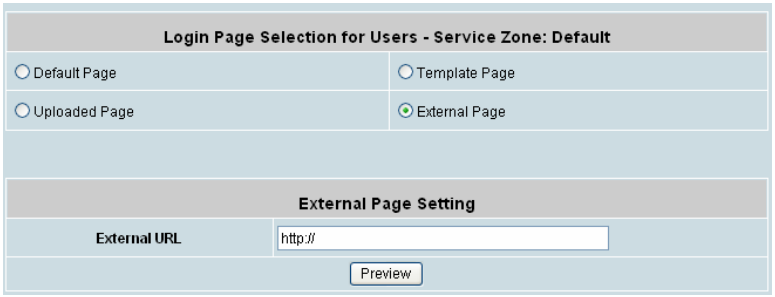
Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

Next, enter or browse the filename of the images to be uploaded in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the ***Use Default Page*** button to restore it to default.

After the image file is uploaded, the file name will show on the **“Existing Image Files”** field. Check the file and click ***Delete*** to delete the file.

After the upload process is completed and applied, the new login page can be previewed by clicking ***Preview*** button at the button.

- Custom Pages → Login Pages → **External Page**



Choose the ***External Page*** selection and get the login page from the specific website. In the External Page Setting, enter the URL of the external login page and then click ***Apply***.

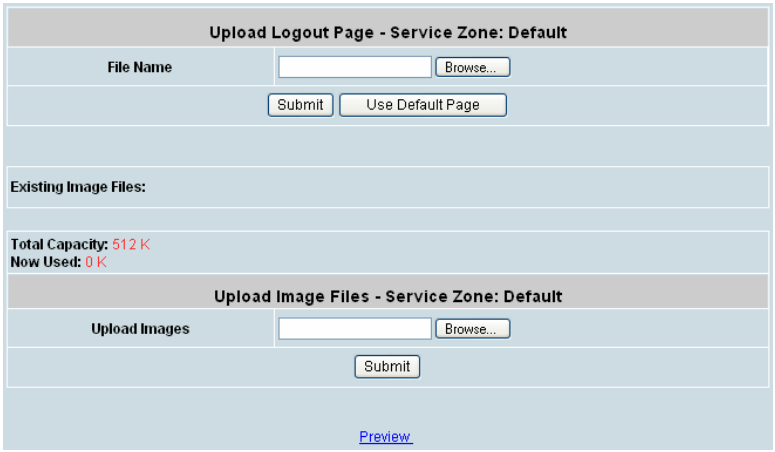
After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

The user-defined logout page must include the following HTML codes to provide the necessary fields for username 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>
```

2.2.2) Custom Pages → **Logout Page**

The administrator can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the instructions on Login Page → Uploaded Page for details.



Please Note: While this process is similar to that of the Login Page, the HTML code for the user-defined logout interface however is different. The following HTML code must be added in order for the user to enter the username 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>
```

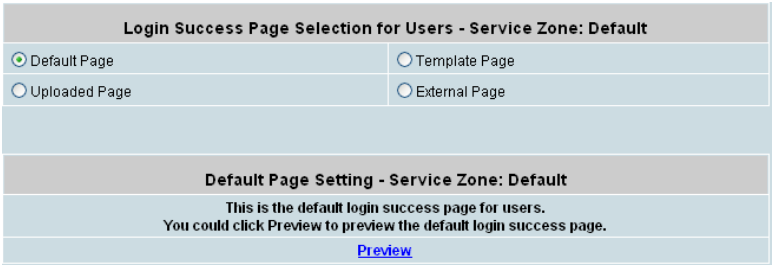
After the upload is completed, the customized logout page can be previewed by clicking ***Preview*** at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "**Use Default Page"** button.

2.2.3) Custom Pages → **Login Success Page**

The users can apply their own Login Success page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

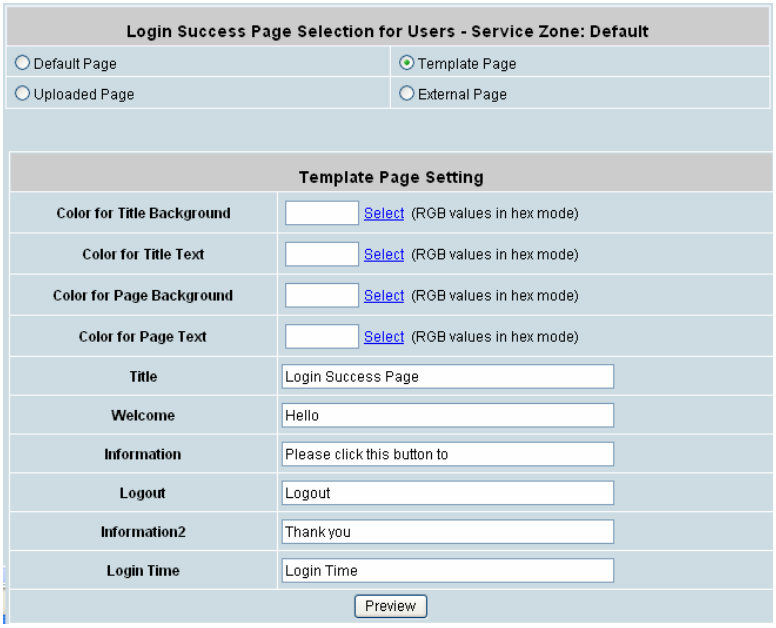
- *Custom Pages → Login Success Page →* ***Default Page***

  Choose Default Page to use the default login success page.



- *Custom Pages → Login Success Page →* ***Template Page***

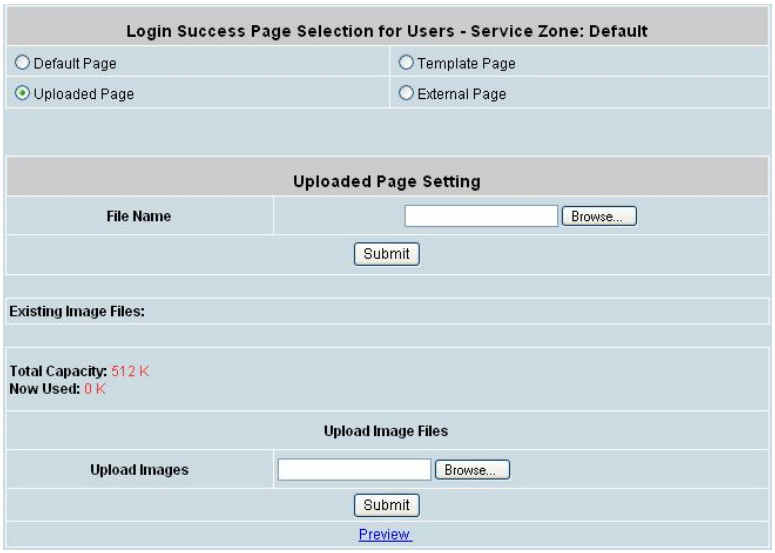
  Choose Template Page to make a customized login success page. Click ***Selec***t to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



- Custom *Pages → Login Success Page →* ***Uploaded Page***

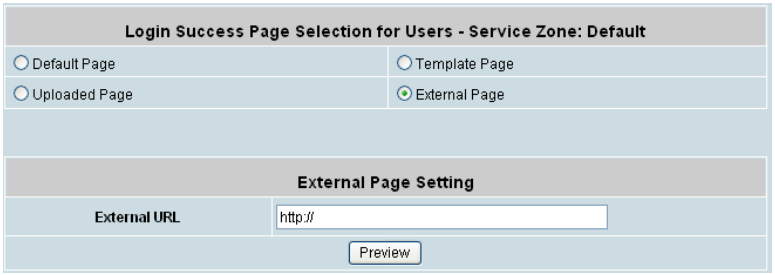
  Choose Uploaded Page to upload the login success page. Click the Browse button to select the file for the login success page upload. Next, click Submit to complete the upload process.

  After the upload process is completed and applied, the new login success page can be previewed by clicking Preview button at the bottom.



- *Custom Pages → Login Success Page →* ***External Page***

  Choose the External Page selection to get the login success page from the specific website. In the External Page Setting, enter the URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking Preview button at the bottom of this page

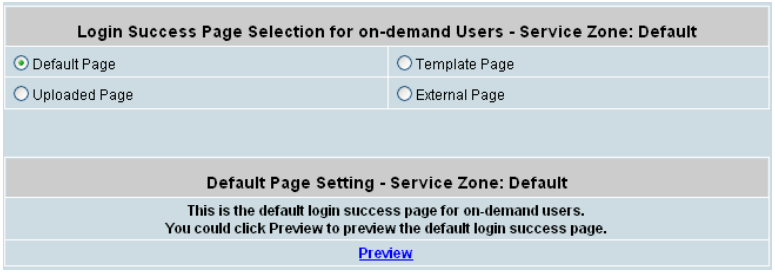


2.2.4) Custom Pages → Login Success Page for Instant Account

The users can apply their own Login Success page for Instant Users in the menu. As the process is similar to that of the Login Page, please refer to the instructions on Login Page for more details.

- Custom Pages → Login Success Page for Instant Account → Default Page

  Choose Default Page to use the default login success page for Instant account

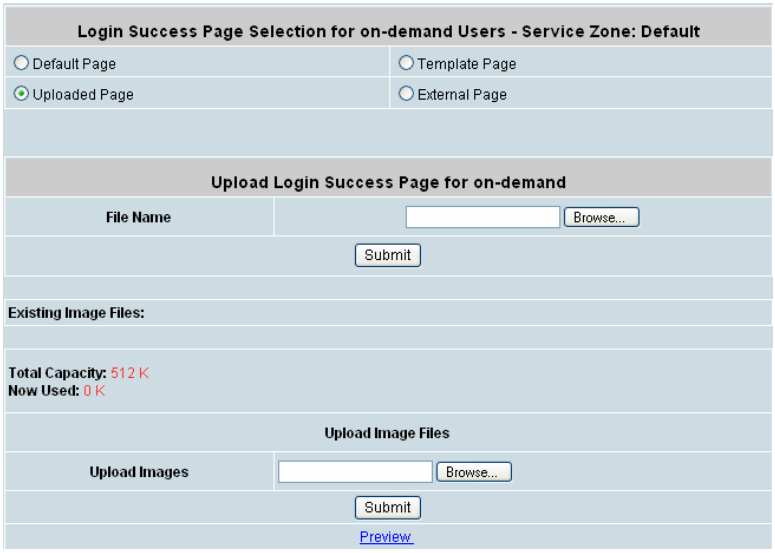


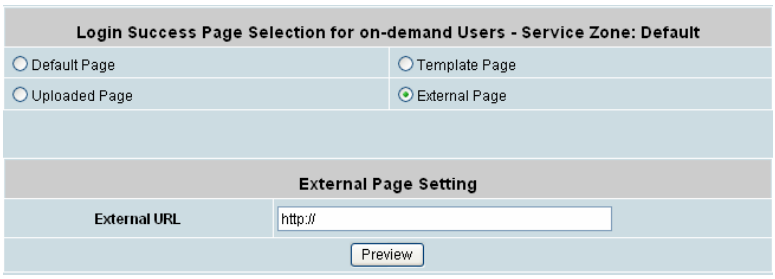
- *Custom Pages → Login Success Page for Instant Account →* ***Template Page***

  Choose Template to make a customized login success for Instant account. Click *Select* to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result.

- *Custom Pages → Login Success Page for Instant Account →* ***Uploaded Page***

  Choose Uploaded Page and get the login success page for Instant by uploading. Click the ***Browse*** button to select the login success page file for instant upload. Then click ***Submit*** to complete the upload process.

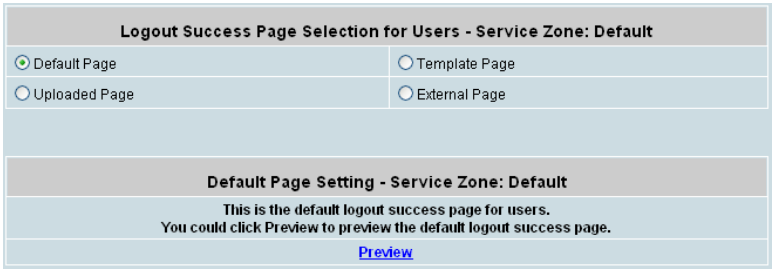




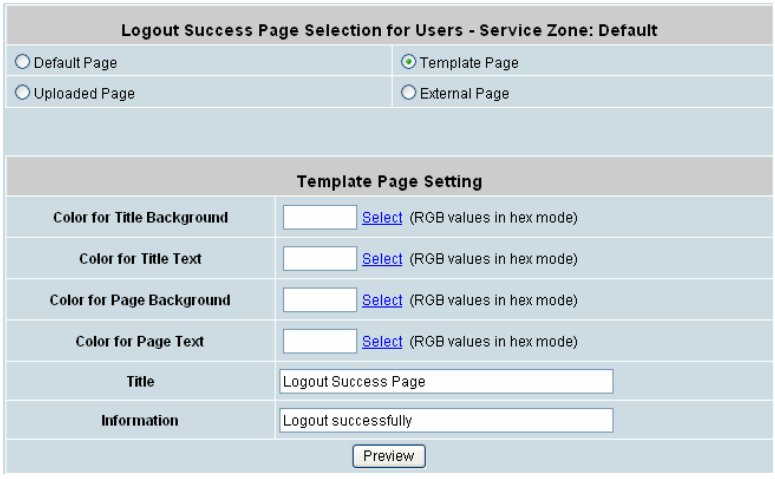
2.2.5) Custom Pages → **Logout Success Page**

The administrator can apply their own Logout Success page for Users in the menu. As the process is similar to that of the Login Page, please refer to the instructions on Login Page for more details.

- *Custom Pages* → Logout Success Page → Default Page
  Choose Default Page to use the default logout success page.

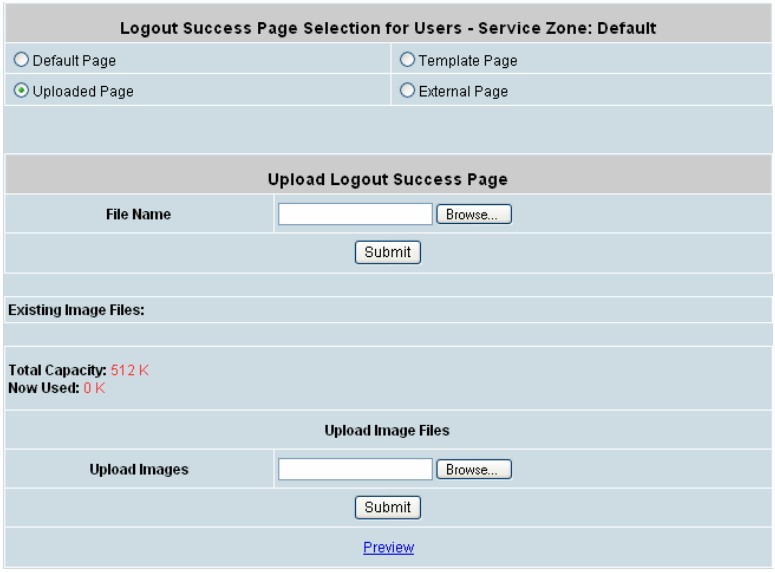


- *Custom Pages → Logout Success Page →* ***Template Page***
  Choose Template Page to make a customized logout success page. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



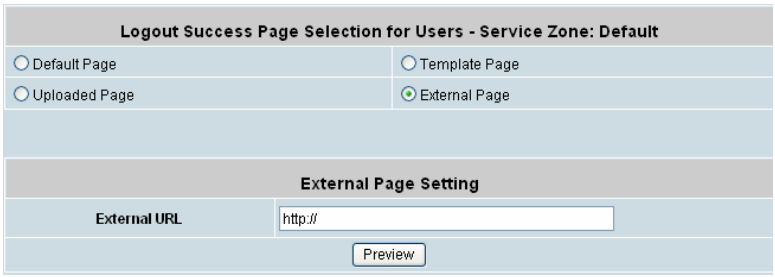
- *Custom Pages → Logout Success Page →* ***Uploaded Page***

  Choose Uploaded Page to get the logout success page for upload. Click the ***Browse*** button to select the file for the logout success page upload. Next, click ***Submit*** to complete the upload process. After the upload process is completed and applied, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.

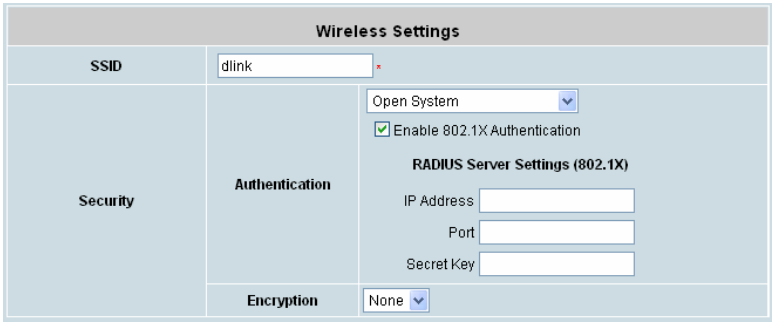


- Custom Pages → Logout Success Page → External Page

  Choose the External Page selection and get the logout success page from the specific website. Enter the website address in the External Page Setting field and then click Apply. After applying the setting, the new logout success page can be previewed by clicking Preview button at the bottom of this page.



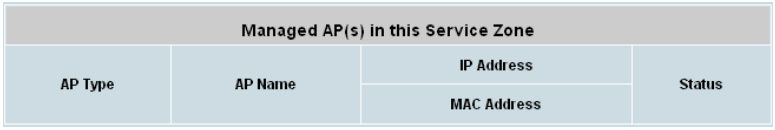
3) Service Zone Settings – Wireless Settings



- **SSID:** Each service zone must setup its own SSID.
- **Security:** Each service zone can setup its own **Authentication** and **Encryption** support. Authentication support: WPA-PSK, IEEE 802.1X (EAP-MD5, EAP-TLS, CHAP, PEAP); and encryption support: WEP (64/128bit), WPA and WPA2.

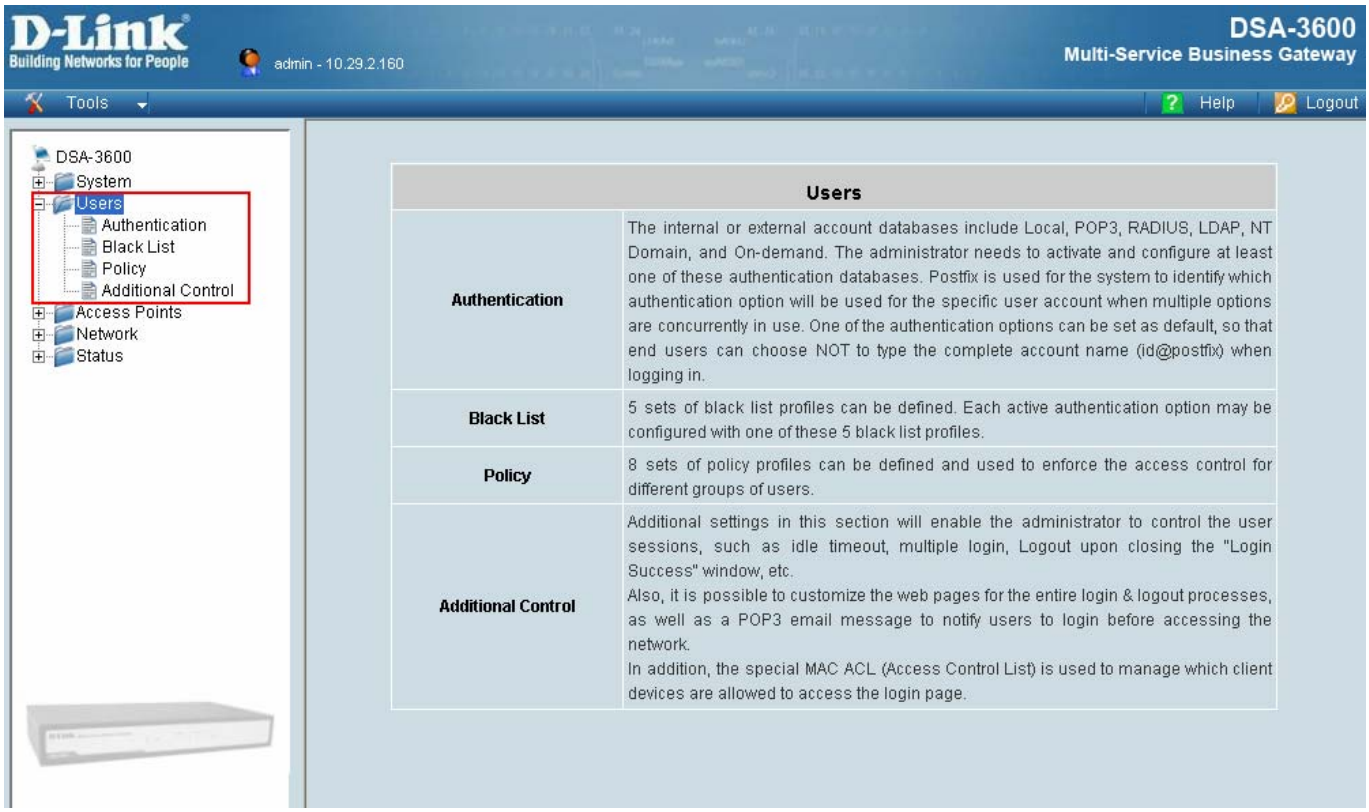
4) Service Zone Settings – Managed AP(s) in the service Zone

- **Managed AP in this Service Zone:** List all APs belonging to this service zone.



4.2 Users

This section provides information on the following functions: **Authentication, Black List, Policy** and **Additional Control**.



Users	
Authentication	The internal or external account databases include Local, POP3, RADIUS, LDAP, NT Domain, and On-demand. The administrator needs to activate and configure at least one of these authentication databases. Postfix is used for the system to identify which authentication option will be used for the specific user account when multiple options are concurrently in use. One of the authentication options can be set as default, so that end users can choose NOT to type the complete account name (id@postfix) when logging in.
Black List	5 sets of black list profiles can be defined. Each active authentication option may be configured with one of these 5 black list profiles.
Policy	8 sets of policy profiles can be defined and used to enforce the access control for different groups of users.
Additional Control	Additional settings in this section will enable the administrator to control the user sessions, such as idle timeout, multiple login, Logout upon closing the "Login Success" window, etc. Also, it is possible to customize the web pages for the entire login & logout processes, as well as a POP3 email message to notify users to login before accessing the network. In addition, the special MAC ACL (Access Control List) is used to manage which client devices are allowed to access the login page.

4.2.1 Authentication

This function is used to authenticate users against internal or external account database. The DSA-3600 supports several types of authentication database: Local, POP3, RADIUS, LDAP, and NT Domain. The DSA-3600 provides up to three external authentication servers, one Local users authentication server and one Guest Users authentication server. The administrator needs to activate and configure at least one of these authentication servers. Postfix is used to inform the system which authentication server to use for authentication when multiple authentication servers are concurrently in use. One of authentication server option can be assigned as default. For the authentication server assigned as default, the Postfix can be omitted.

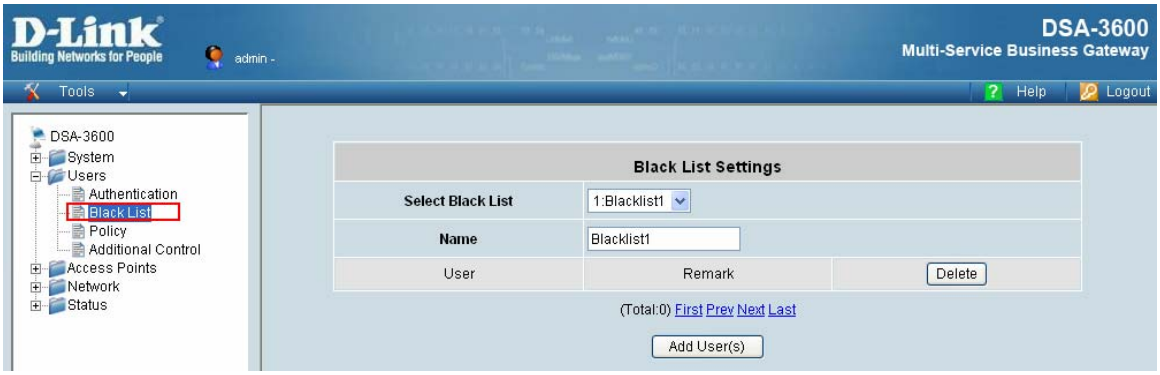
- **Authentication Option:** There are 5 kinds of authentication database supported by DSA-3600: Local User, POP3, RADIUS, LDAP, NT Domain and Guest Users. Click the hyperlink of the respective Authentication Option to enter the Authentication Option page.
- **Authentication Database:** There are 6 different authentication methods supported in DSA-3600 Authentication Database: Local, POP3, Radius, LDAP, NT Domain and ONDEMAND. Select the desired authentication database and then click the hyperlink ***Configure*** next to the drop-down menu for further configuration.
- **Postfix:** Set a postfix that is easy to identify (e.g. local) for the authentication option by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Please Note: Not more than one Auth Option is allowed to be enabled for Local, Guest Users or NT Domain Authentication Database.

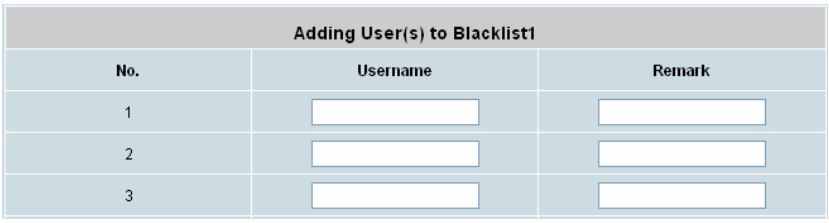
For more information on **Authentication Methods,** please refer to **4.1.6 Service Zone Settings – Authentication Settings.**

4.2.2 Black List

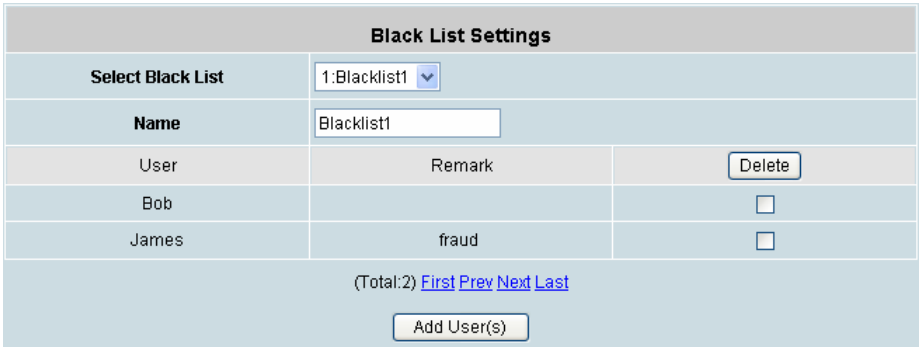
The administrator can add or delete users in the black list for user access control. There are 5 sets of black lists provided by the system. Each Black List allows up to 40 user accounts. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from the drop-down menu and this black list will be applied to this specific authentication option.



- **Select Black List:** There are 5 lists supported by DSA-3600 for selections.
- **Name:** Set the name of the black list and it will show in the pull-down menu above.
- **Adding User(s):** After clicking **Adding User(s)**, the **Adding Users to Blacklist** page will appear for adding users to the selected black list.



After entering the usernames in the **Username** field and the related information in the **Remark** field (not required), click ***Apply*** to save the settings and the following page will appear.



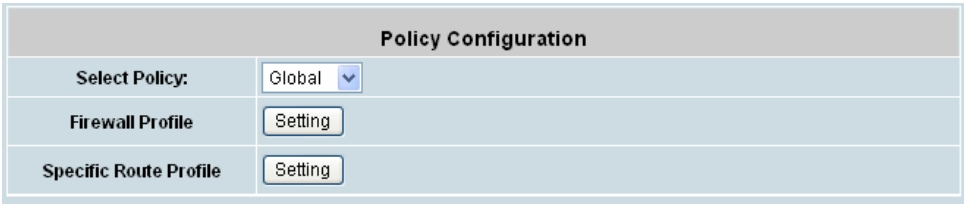
If the administrator wants to remove a user from the black list, just select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.

4.2.3 Policy

There are nine policies, **Global** and **Policy1 to Policy8** provided by the system. **Global** is the system's universal policy including **Firewall Profile** and **Specific Route Profile** which will be applied to all users unless the user has been regulated and applied to another policy. Each of the policies has a profile for **Firewall, Specific Route, Schedule, QoS,** and **Privilege Profile.**

Policy1 to Policy8 will be used and shared with the **Service Zone** default policy settings and Authentication Databases settings. Once a policy is configured, you may assign it to the default policy of a service zone. Two service zones may share the same policy. Policies can be selected in the Policy tab. The administrator can select one of the defined policies to have policy-based user management supported by the DSA-3600. All user clients' access to this service zone will be bound to this policy. When **Local** is the selected Authentication Database, a policy can be applied per user basis. When **RADIUS** is the selected Authentication Database, the **Class-Policy Mapping** function is available to let the administrator assign a policy for a RADIUS Class attribute. When **LDAP** is the selected Authentication Database, the **Attribute-Policy Mapping** function will be available to let the administrator assign a policy for a LDAP Attribute.

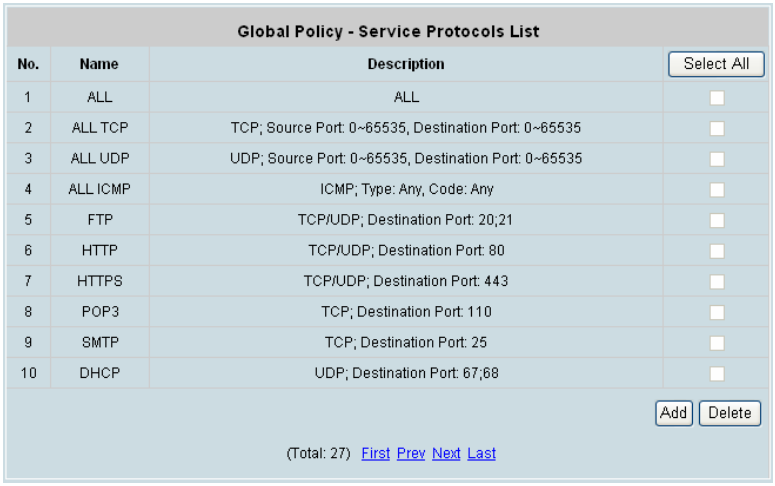
4.2.3.1 Global Policy



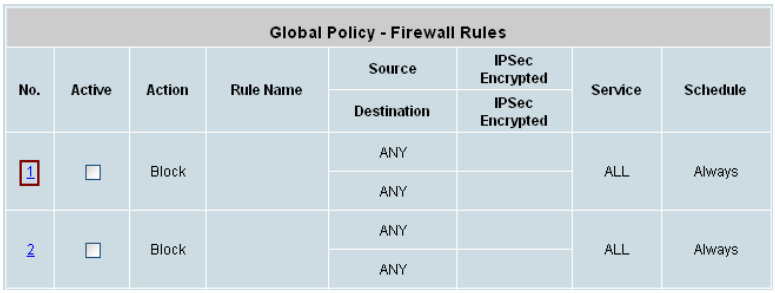
Select Policy: Select **Global** to set the **Firewall Profile** and **Specific Route Profile**.

A. Firewall Profile: Click the hyperlink of ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

a. Predefined and Custom Service Protocols: There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.

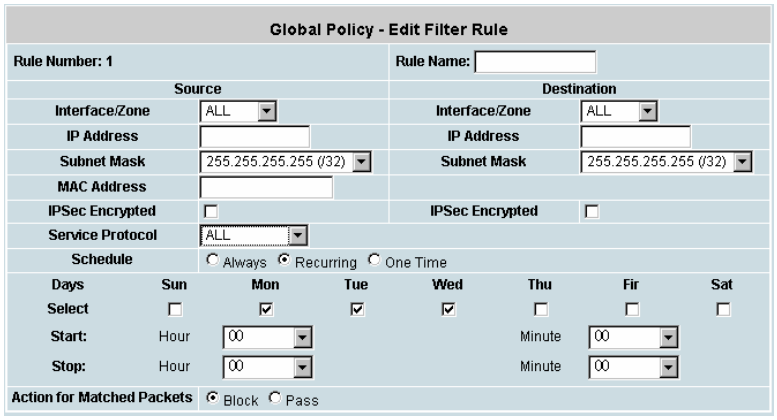


b. Firewall Routes: Click the number of ***Filter Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** box and click ***Apply*** to enable that rule.



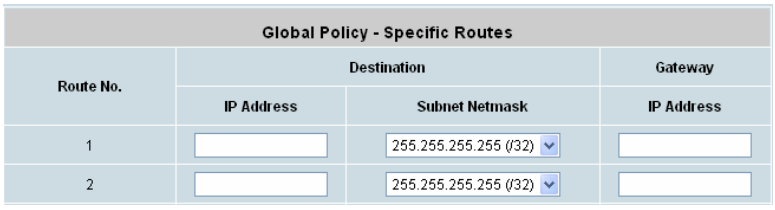
Selecting the Filter Rule Number 1 as the example:

- **Rule Number:** This is the rule selected "1".
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface:** There are choices of **ALL, WAN1**, **WAN2**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP:** Enter the source and destination IP addresses.
- **Source/Destination – Subnet Mask:** Enter the source and destination subnet masks.
- **Source- MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.
- **Source/Destination – IPSec-Encrypted:** check the box for only filtering on the encrypted traffic.



- **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.
- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

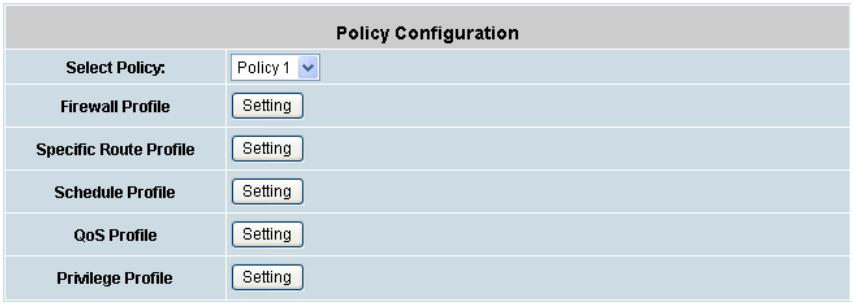
B. Specific Route Profile: Click the hyperlink of Setting for Specific Route Profile, the Specific Route Profile list will appear.



- **Route No.:** The number of route.
- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.

4.2.3.2 Policy1 to Policy8

Select Policy: Select a desired policy for configuration.

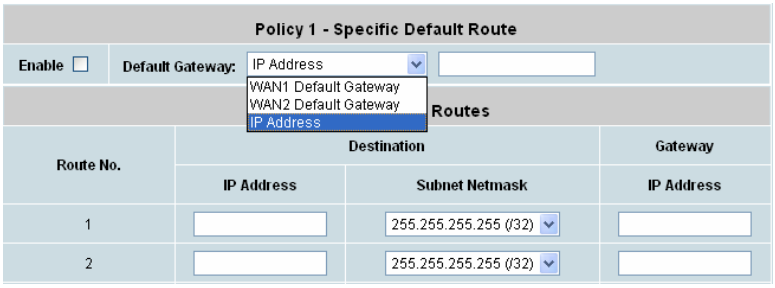


A. Firewall Profile: Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules. Please refer to 4.2.3.1 **Global Policy** section **A** for the same operations.

B. Specific Route Profile: Click the hyperlink of Setting for Specific Route Profile, the Specific Route Profile list will appear.

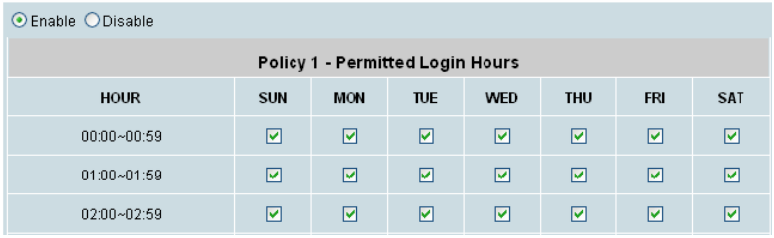
The **Default Gateway** of WAN1, WAN2, or a desired IP address can be defined in a policy. When **Default Gateway** is enabled, all clients applied this policy will access the Internet through this default gateway. In addition, the system supports up to 10 specific routes for each policy.

- **Enable:** Check this option to apply the **Default Gateway**.
- **Default Gateway:** Select the default gateway as WAN1, WAN2 or an assigned IP Address.

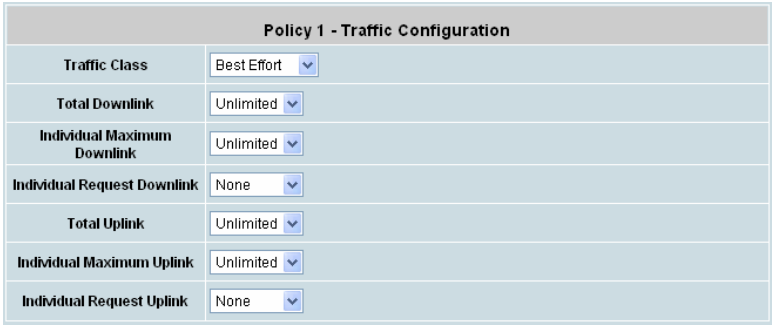


- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.

C. Schedule Profile: Click the hyperlink of ***Setting for Schedule Profile*** to enter the Schedule Profile list. Select “Enable” to show the list. This function is used to restrict the hours the users can log in. Please check the desired time slot and click **Apply** to save and enable the settings (on the screen below is shown only for 0 to 02:59, but the system can be configured based on 24 hours, 00:00 to 23:59). These settings will become effective immediately after clicking the Apply button. The Login Hours in a 7x24 format is used to control the clients' login time. When Schedule is enabled, clients applied polices are only allowed to login the system at the time which is checked in the applied policies.

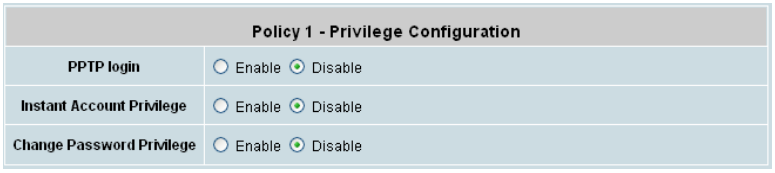


D. QoS Profile: Click the hyperlink of Setting for QoS Profile to enter the Traffic Configuration.



- **Traffic Class:** Each login user will be categorized into a policy. Each policy can choose its own traffic class. There are four traffic classes: Voice, Video, Best-Effort and Background. Voice and Video will be put into high priority queue. When select Best-Effort or Background, it also can configure the Downlink and Uplink Bandwidth.
- **Total Downlink:** The Total Downlink defines the maximum bandwidth allowed to share by clients within the same policy.
- **Individual Maximum Downlink:** The Individual Maximum Downlink defines the maximum bandwidth allowed for an individual client; the Individual Maximum Bandwidth can not exceed the value of Total Bandwidth.
- **Individual Request Downlink:** The Individual Request Downlink defines the guaranteed minimum bandwidth allowed for an individual client; the Individual Request Bandwidth can not exceed the value of Total Bandwidth and Individual Maximum Bandwidth.
- **Total Uplink:** The Total Uplink defines the maximum bandwidth allowed to share by clients within the same policy.
- **Individual Maximum Uplink:** The Individual Maximum Uplink defines the maximum bandwidth allowed for an individual client; the Individual Maximum Bandwidth can not exceed the value of Total Bandwidth.
- **Individual Request Uplink:** The Individual Request Uplink Bandwidth defines the guaranteed minimum bandwidth allowed for an individual client; the Individual Request Bandwidth can not exceed the value of Total Bandwidth and Individual Maximum Bandwidth.

E. Privilege Profile: Click the hyperlink of Setting for QoS Profile to enter the Privilege Configuration Including PPTP login, Instant Account Privilege and Change Password Privilege.



- **PPTP login:** When PPTP login is enabled, the policy applied user is able to access the internal network from the external network via establishing a PPTP VPN tunnel when **Remote VPN** function under **Network** category is enabled.
- **Instant Account Privilege:** When Instant Account Privilege is enabled, the authenticated users are allowed to create guest accounts via the Login Success Page.
- **Change Password Privilege:** When Change Password Privilege is enabled, the authenticated Local users are allowed to change password via the Login Success Page.

.

4.2.4 Additional Control

In this section, additional settings are provided for the administrator to the following for user management.

- **User Session Control:** Functions under this section applies for all general users.

  Idle Timeout: If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.

  Multiple Login: When enabled, the same account can be logged in by different clients at the same time. (This function doesn't support users authenticated with Guest users or RADIUS server)

  Logout upon closing the "Login Success" window: When a client logs into the network without VPN, a small window will appear to show the client's information and there is a logout button for the logout. If enabled. When the clients try to close the small window, there will be a new popup window to confirm the logout in case the users click the logout button by accident.

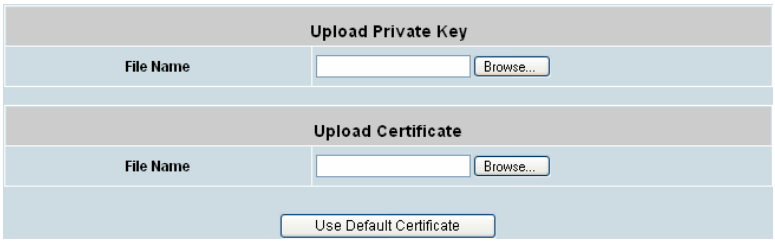
- **Built-in RADIUS Server Settings**

  Session Timeout: The time that the user can access the network while roaming. When the time is up, the client will be kicked out automatically.

  Idle Timeout: If a client has been idled with no network activities, the system will automatically kick out the client.

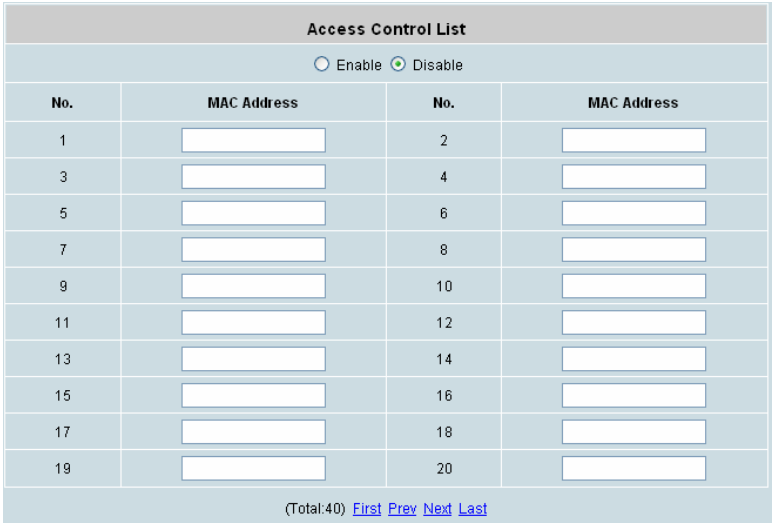
  Interim Update: The system will update the clients' current status and usage according to this time periodically.

- **Customization:** The administrator can upload their own certificate to the system.



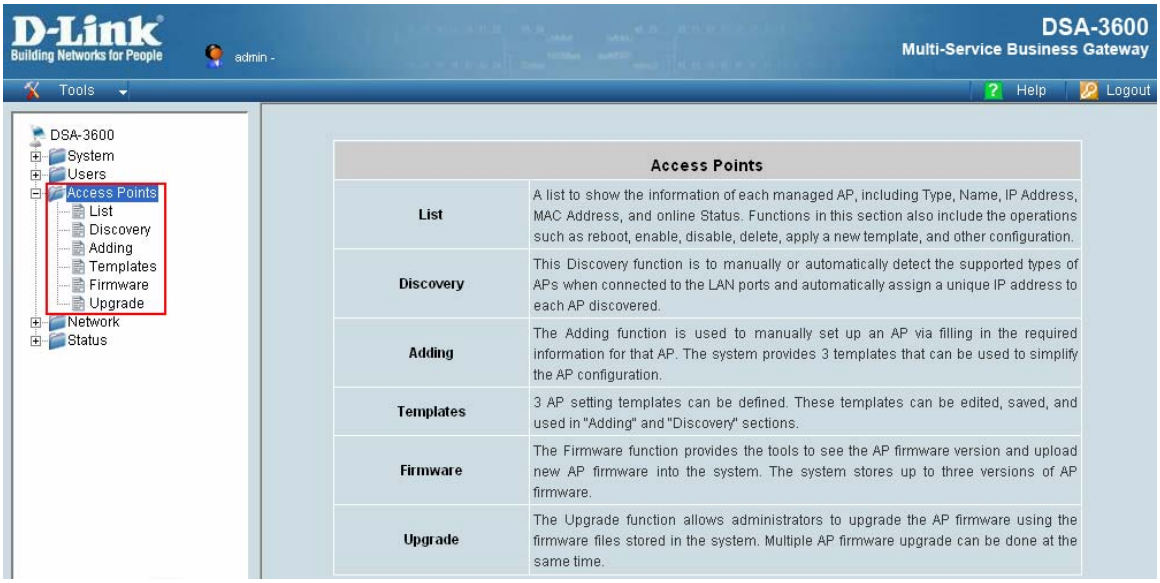
- **Remaining Time Reminder:** There is a Remaining Time Reminder supported by the system to remind guest users that their accounts are about to expire within the set time. When Remaining Time Reminder is enabled, there will be a message appearing on guest user's screen to remind them.

- **MAC ACL:** Enter the MAC address of the network device. When MAC ACL is enabled, only the clients with their MAC addresses listed in this list can access the system on this WEB interface or getting a login page. There will be up to forty sets provided in this MAC Control List. User authentication is still required for these users.



4.3 Access Points

This section provides information on the following functions: **List, Discovery, Adding, Templates, Firmware** and **Upgrade**.

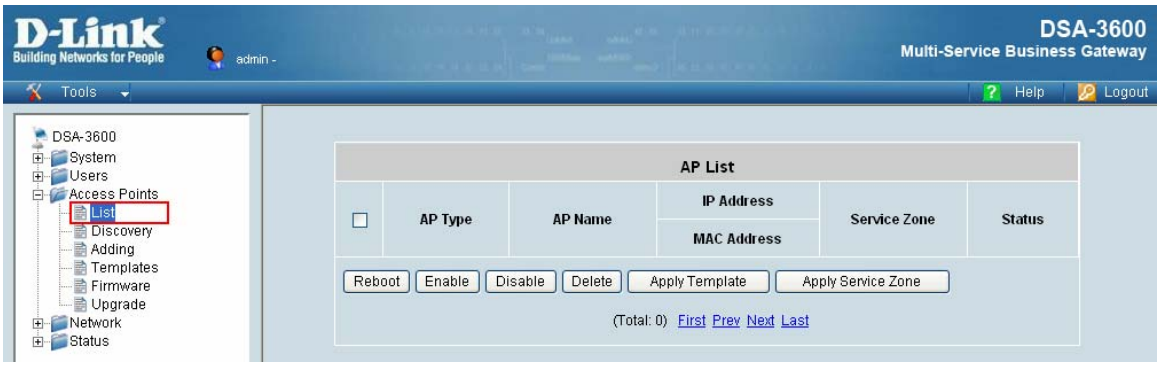


Access Points	
List	A list to show the information of each managed AP, including Type, Name, IP Address, MAC Address, and online Status. Functions in this section also include the operations such as reboot, enable, disable, delete, apply a new template, and other configuration.
Discovery	This Discovery function is to manually or automatically detect the supported types of APs when connected to the LAN ports and automatically assign a unique IP address to each AP discovered.
Adding	The Adding function is used to manually set up an AP via filling in the required information for that AP. The system provides 3 templates that can be used to simplify the AP configuration.
Templates	3 AP setting templates can be defined. These templates can be edited, saved, and used in "Adding" and "Discovery" sections.
Firmware	The Firmware function provides the tools to see the AP firmware version and upload new AP firmware into the system. The system stores up to three versions of AP firmware.
Upgrade	The Upgrade function allows administrators to upgrade the AP firmware using the firmware files stored in the system. Multiple AP firmware upgrade can be done at the same time.

4.3.1 List

All of the supported managed APs (such as DWL-2100AP with hardware version A3 and above, firmware version v2.20EU and above) under management of the system will be shown in the list. The list is empty during first setup. The administrator can add supported APs from Discovery or the Adding menu tab. After the APs are added, this list will show the current managed APs including AP type, AP name, IP Address, MAC Address, Service Zone and Status. The administrator can reboot, enable, disable, delete the managed APs, or apply template to them by checking the check box in front of each individual AP or selecting all the APs together by checking the top check box.

Please Note: The supported managed AP may be vary for different DSA-3600 firmware version.



After adding an AP:

Check any AP and click the button below to **Reboot, Enable, Disable, Delete** and **Apply Template** the checked AP. Click **Apply Template** to select one template to apply to the AP.

- **AP Name**

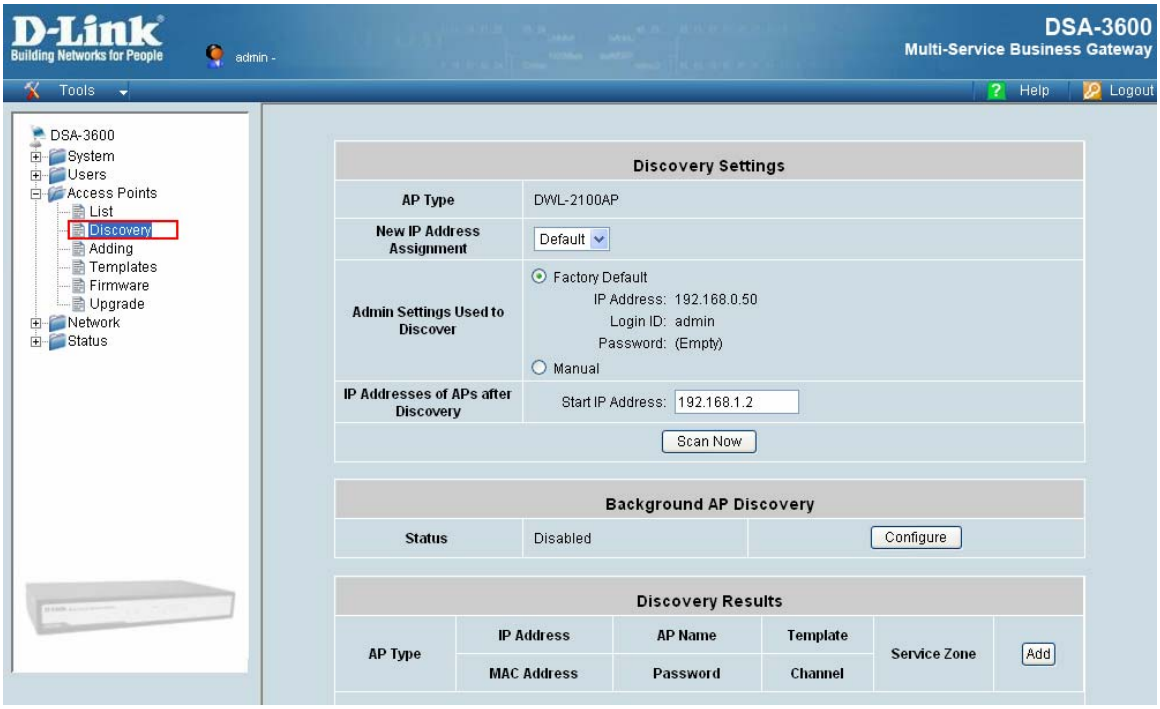
  Click the hyperlink of the **AP Name** to have more configurations. There are four kinds of settings available: **General**, **LAN**, **Wireless LAN** and **Access Control**. Click the hyperlink of each individual setting to have further configurations.

- **Status**

  After clicking the hyperlink in the Status column, there are two areas of information shown: **AP Status Summary** and **AP Status Details.** AP Status Summary includes **AP Name, AP Type**, **LAN interface MAC address**, **Wireless interface MAC address**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.

4.3.2 Discovery

Use this function to detect and manage all the supported APs in the network segments.



- **Discovery Settings**

  When the administrator tries to discover a new AP, select the Service Zone first. Second, select Factory Default or Manual in Admin Settings Used to Discover field; enter the current IP range of the APs if they are not in default value. Then click ***Scan Now*** button. If the new AP has been discovered, it will appear in the following Discovery Results list. If there is a warning message showing below the Discovery Settings, follow the instructions to change configurations.

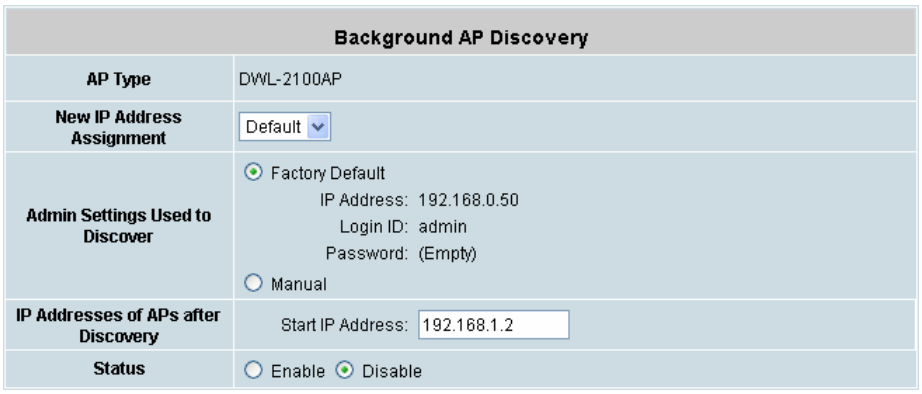
  Please fill in the required data.

  - **Interface**: Select the default service zone of the interface where APs are connected and to be scanned.
  - **Admin Settings Used to Discover:** Select Manual, enter the current IP range of the APs in IP Address field if they are not in default value. The IP of AP with factory default setting is "192.168.0.50". If the AP was discovered before, the IP address of the AP should have been changed. Please enter the right IP address of the AP or reset the AP to default values. Login ID is the admin ID of the AP. Password is the admin password of the AP. If the AP is in default value, just select Factory Default, system can discovery the APs.
  - **IP Addresses of APs after Discovery**: The start IP to be assigned will be entered here.
  - **Scan Now:** Click the ***Scan Now*** button and the APs that match the given settings will be shown in the Discovered Results below. If any IP address among the IP range assigned for a specific AP is used, there will be a warning message showing up. Please change the **IP Addresses of APs after Discovery** and then click Scan Now again. For the desired AP, input the desired AP name and admin password, select one template to apply, select the check box, and click ***Add*** to add the discovered AP to the List. For more information about the template, please refer to **4.3.4 Templates**.

- **Background AP Discovery**

  The system supports discovering APs periodically in background. The New IP Address Assignment and Access to the AP Admin Interface configuration in Background Auto Discovery page are the same as in the Discovery Settings. Click Configure and then select Enable to set the configuration. When Auto Adding AP to the list is enabled, the system will add the discovered APs into the List table automatically and apply the selected template in the Template Applied option to the AP. When the configurations are set as requirement, the system will discover new APs periodically and automatically in background.

  Click ***Configure*** to enter the **Background AP Discovery** page to have further configuration.



  The **Interface, Admin Settings Used to Discover** and **IP Addresses of APs after Discovery** configurations are the same as the settings mentioned above. Check **Enable** to have more configuration. Select **Interval** setting from the drop-down menu to set the system to scan periodically according to this setting (the default value is 10 minutes). If **Auto Adding AP to the list** is enabled, a new detected AP will be assigned an available IP address from the IP address range set in **IP Addresses of APs after Discovery** and applied with the selected template automatically.

- **Discovery Results**

  When the matched AP is discovered, it will be shown in the **Discovery Results** below and a new IP address will be given to the discovered AP automatically. Check the **Add** box to add the AP, and it will be listed in the **List**. The discovered new APs will be listed here. The administrator can click Add button to register the APs to the List for management. When the system's Service Zone is set to Tag-based mode, service zones also can be assigned here. After clicking Add, the current management page is directed to AP List, where the newly added APs will show up with a status of "configuring". It may take a couple of minutes to see the status of the newly added AP to change from "configuring" to "online" or "offline".

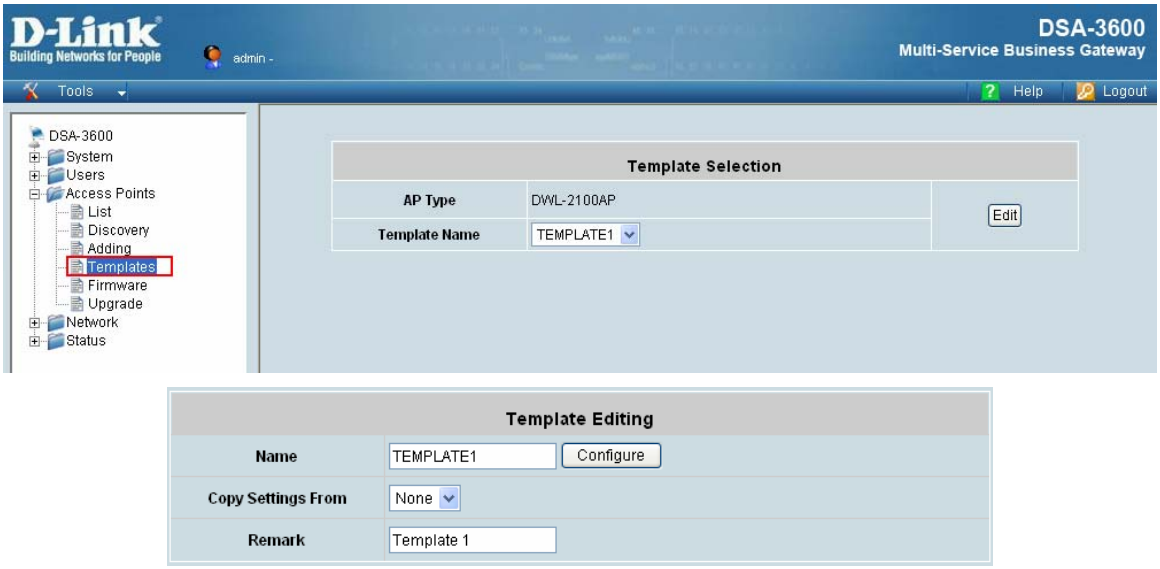
4.3.3 Adding

The supported APs (such as DWL-2100AP) can also be added into the **List** manually. Enter the related information of the AP and select a **Template Applied**. Click ***ADD*** and then the AP will be added to the **List**. Similar to the AP added after discovery, a manually added AP will show up with a status of "configuring" in the AP List initially. The system will attempt to configure the AP with the value specified. A couple of minutes later, the AP's status will become "online" or "offline" on the AP List.

- **AP Type:** The type of supported AP.
- **AP Name:** The mnemonic name of the specific AP.
- **Admin Password:** The password of the AP for the system to access it.
- **IP Address:** The IP address of the AP.
- **MAC Address:** The Media Access Control (MAC) address of the AP.
- **Remark:** The administrator can add some extra information for the AP in this field if desired.
- **Service Zone:** When the system's Service Zone is set to Tag-based mode, additional Service Zone field will be here for assigning services zones to the AP.
- **Template Applied:** The template which will be applied to the AP.

4.3.4 Templates

A template is a model that can be copied to every AP without having to configure the each AP individually. The system supports up to three templates which include configurations of APs. The administrator can configure the setting together in the template instead of logging the AP management interface to set the configurations one by one. Click ***Edit*** to go to configuration. Select the AP type (if available) and one of the three available templates, and then click ***Edit*** to have the Template Editing page.

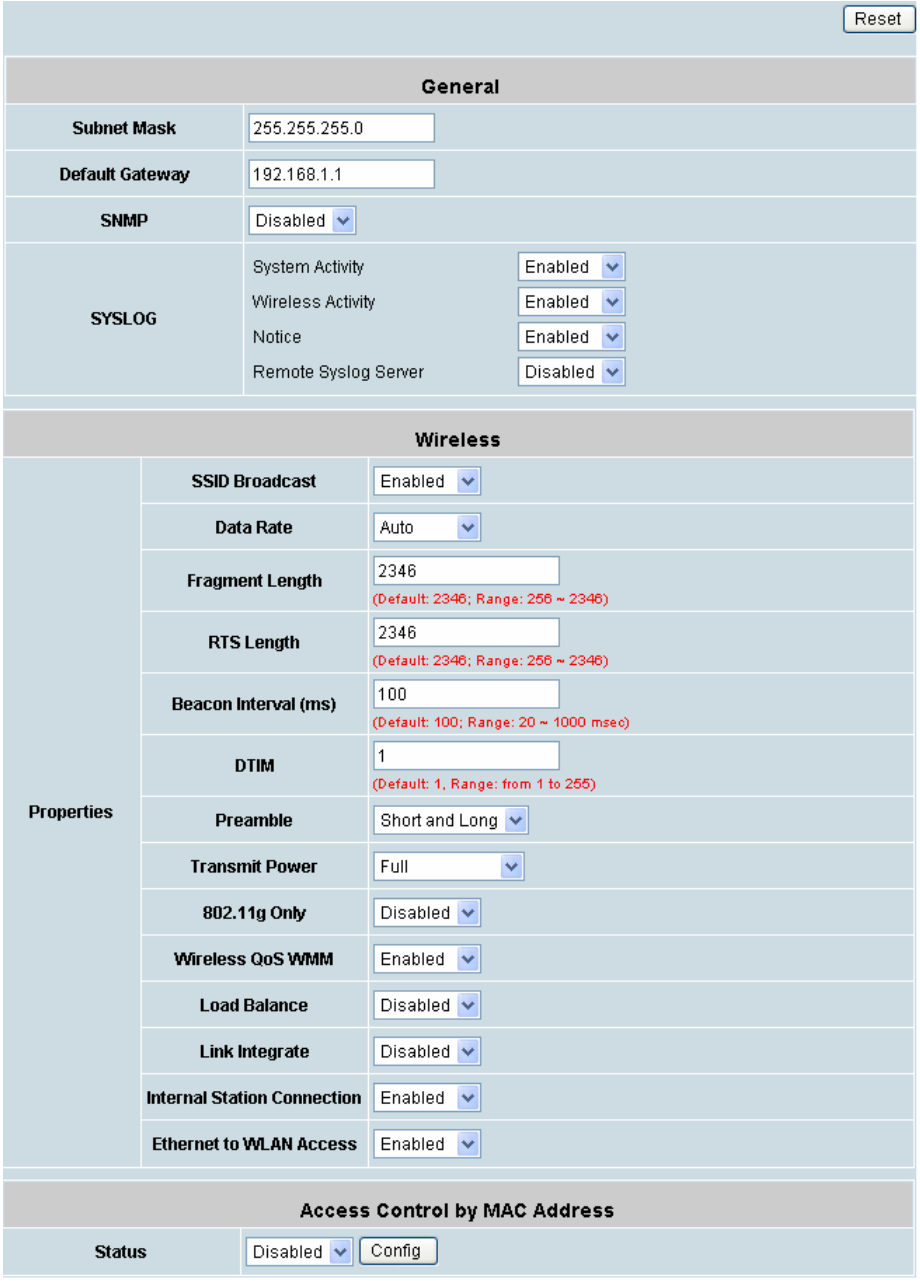


Except configuring all the template setting manually, copy the configuration of an AP to the template by selecting a **Copy Settings From** and revise some settings is also acceptable. Please select **None** if configuring the whole template from the draft is desired. Enter the **Name** and **Remark** (optional) and click ***Configure*** to have further configuration.

After clicking ***Edit*** to enter the **Details** page, revise the configuration on demands such as **SSID** or **Channel**. About other functions of **Wireless** part please refer to **4.3.1 List**.

- **Template Editing**

  The administrator can set the template configuration manually or copy the configurations from a specific existing managed AP by Copy Settings From option. Click ***Configure*** button to have detailed configurations.

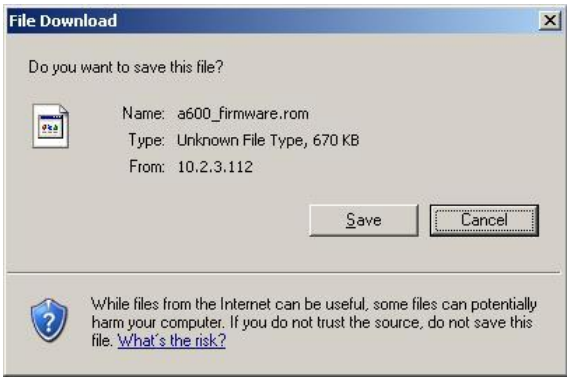


Access Control by MAC Address: This function provides to control the clients' devices that are allowed to associate with the APs applied with the desired template setting. Choose **Disabled** or **Enabled** in the **Status** column and enter the desired clients' MAC addresses in the MAC Address List. There are up to 20 MAC addresses available. When this function is enabled, please make sure the MAC Address List is not empty.

4.3.5 Firmware

This is where AP's firmware can be uploaded. The current firmware can also be downloaded to the local storage if required.

The system supports the firmware management of APs to upload new firmware, delete the existing firmware, and download the firmware to managed APs. Note that the AP's firmware version must be one that has been integrated.



- **File Name:** The name of the AP firmware to be uploaded.
- **Upload:** Click ***Upload*** button to upload the file from a local disk to the system.
- **List:** All uploaded firmware will be listed here.
- **Checksum:** The automatically detected security identification of the firmware.
- **AP Type:** The AP type of the firmware.
- **Version:** The version of the firmware.
- **Size:** The file size of the firmware.
- **Download:** Click Download to save the selected firmware to local disk.

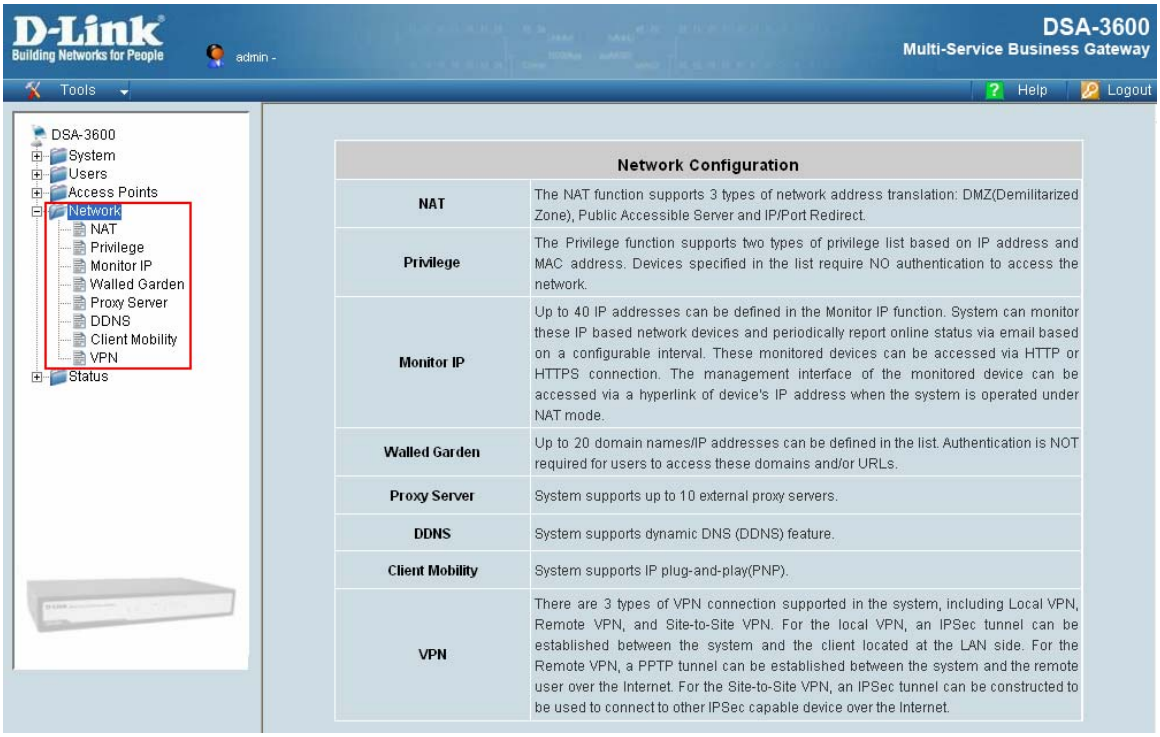
4.3.6 Upgrade

The administrator can upgrade the firmware of selected APs individually or at the same time by checking the check box of the APs in Selection column. Note that both the version before upgrade and the next version must be ones that have been integrated with the system. Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.

- **Last Upgraded Time:** The time when the AP was last upgraded.
- **Next Version:** The firmware version to be upgrade to the AP.

4.4 Network

This section provides information on **NAT, Privilege, Monitor IP, Walled Garden, Proxy Server, DDNS, Client Mobility** and **VPN.**



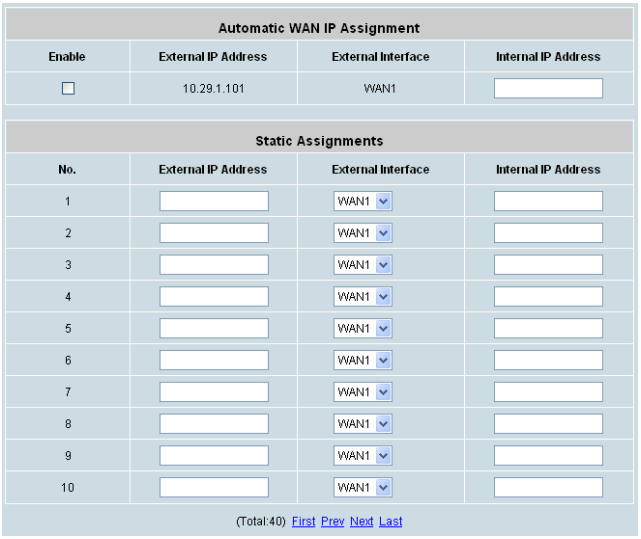
Network Configuration	
NAT	The NAT function supports 3 types of network address translation: DMZ(Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege	The Privilege function supports two types of privilege list based on IP address and MAC address. Devices specified in the list require NO authentication to access the network.
Monitor IP	Up to 40 IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.
Walled Garden	Up to 20 domain names/IP addresses can be defined in the list. Authentication is NOT required for users to access these domains and/or URLs.
Proxy Server	System supports up to 10 external proxy servers.
DDNS	System supports dynamic DNS (DDNS) feature.
Client Mobility	System supports IP plug-and-play(PNP).
VPN	There are 3 types of VPN connection supported in the system, including Local VPN, Remote VPN, and Site-to-Site VPN. For the local VPN, an IPSec tunnel can be established between the system and the client located at the LAN side. For the Remote VPN, a PPTP tunnel can be established between the system and the remote user over the Internet. For the Site-to-Site VPN, an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.

4.4.1 NAT

There are three functions that need to be set here: **DMZ (Demilitarized Zone), Public Accessible Server** and **Port and Redirect**.

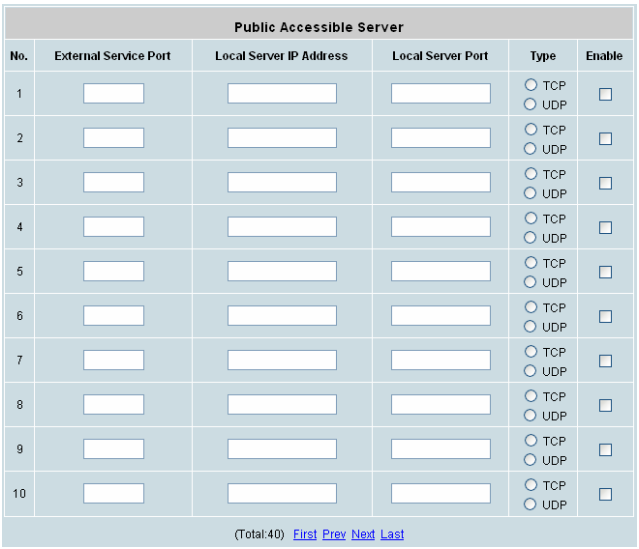
- **DMZ (Demilitarized Zone)**

The administrator can define mandatory external to internal IP mapping using this function, so that a client on the WAN side network can access the private machine by accessing the external IP. Choose to enable Automatic WAN IP Assignment by checking the **Enable** check box and enter the **Internal IP address**. When **Automatic WAN IP Assignment** function is enabled, accessing WAN1 will be mapped to access the **Internal IP Address**. For **Static Assignments**, enter **Internal** and **External** IP Addresses as a set and choose to use WAN1 or WAN2 for the **External Interface** from the drop-down menu. These settings will become effective immediately after clicking the **Apply** button.



- **Public Accessible Server**

The administrator can set up to forty virtual servers using this function, so that the computers not belonging to the managed network can access the servers in the managed network via WAN1 port IP of DSA-3600. Enter the **External Service Port**, **Local Server IP Address** and **Local Server Port** accordingly. Depending on the different services selected, the network service will be able to use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to be enabled. These settings will be effective immediately after clicking the **Apply** button.



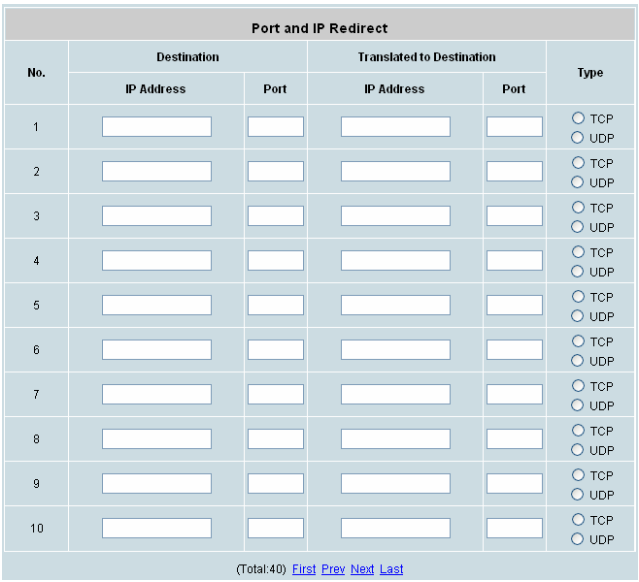
Public Accessible Server

No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	
6				TCP UDP	
7				TCP UDP	
8				TCP UDP	
9				TCP UDP	
10				TCP UDP	

(Total:40) First Prev Next Last

- **Port and IP Redirect**

The administrator can set up to forty sets of the IP address ports for redirection purpose using this function. When users attempt to connect to the port of a **Destination IP Address** listed here, the connection packet will be converted and redirected to the port of the **Translated to Destination IP Address**. Enter the **IP Address** and **Port of Destination**, and the **IP Address** and **Port of Translated to Destination** accordingly. Depending on the different services selected, choose the **TCP** protocol or **UDP** protocol. These settings will become effective immediately after clicking **Apply**.



Port and IP Redirect

No.	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP
6					TCP UDP
7					TCP UDP
8					TCP UDP
9					TCP UDP
10					TCP UDP

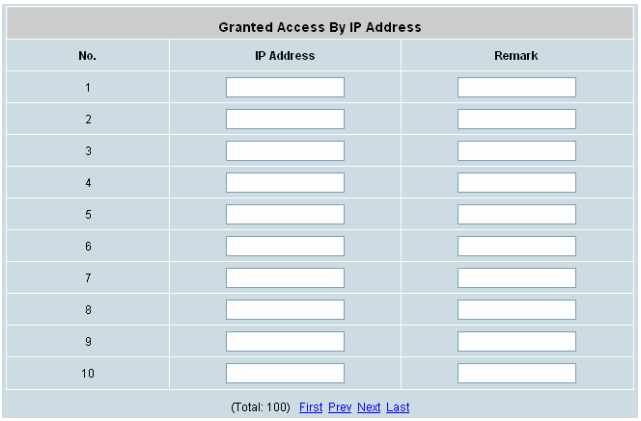
(Total:40) First Prev Next Last

4.4.2 Privilege

The DSA-3600 provides two **Privilege Lists**, **IP Address List** and **MAC Address List**. The administrator can add desired IP addresses and MAC addresses in these lists using the Privilege List function. The IP addresses and MAC addresses in these lists are allowed to access the network without authentication.

- **IP Address List**

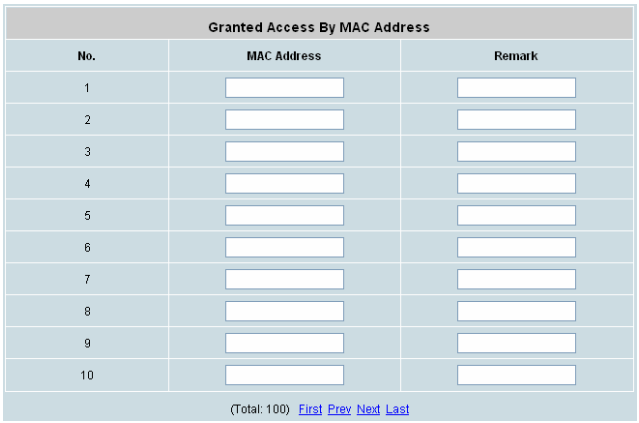
If there are some clients belonging to the managed server that need to access the network without authentication, enter the IP addresses of these clients in this list. **Remark** is optional but useful for tracking purpose. The DSA-3600 allows up to 100 privilege IP addresses. These settings will be effective immediately after clicking ***Apply***.



Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process may result in security problems.*

- **MAC Address List**

In addition to the IP addresses, the clients' MAC addresses can also be set in this list, so that authentication is not required when they using the network. The DSA-3600 allows the setting of up to 100 privilege MAC addresses. Enter the MAC address (in format: xx:xx:xx:xx:xx:xx) and the remark (optional) accordingly. These settings will be effective immediately after clicking ***Apply***.



Granted Access By MAC Address

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

(Total: 100) First Prev Next Last

Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process may result in security problems.*

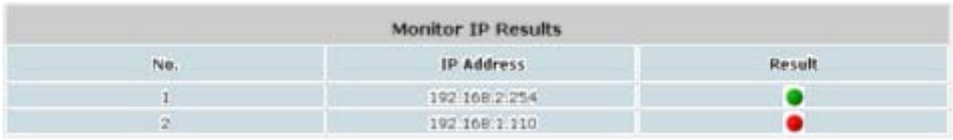
4.4.3 Monitor IP

The DSA-3600 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click ***Apply*** and these settings will become effective immediately.

When the monitored devices have built-in Web servers and connect to the LAN interfaces operating under NAT mode, they can be accessed by hyperlink of their IP addresses. To add the monitored IP addresses in hyperlink accessible mode, click the ***Create*** button in the Hyperlink column.

The Monitor IP supported by the system can monitor the devices in this list by pinging them periodically. The administrator can use this function to monitor third-party APs. Enter the IP addresses of the devices that the administrator wants to monitor and click the ***Apply*** button. When the administrator logs in the system, click the ***Monitor Now*** button to execute the monitor action manually and a new page with status of monitored devices will appear. The red dots mean the devices are unreachable and the green dots mean the devices are reachable and alive. A notification e-mail of the monitored status can be set to notify the administrator in a set interval. For more information, please refer to E-mail & SYSLOG in Status category. For monitored devices on LAN, such as third-party APs or web cameras with built-in web-based administrative interface, hyperlinks can be created for the administrator to access the administrative interface of the devices by clicking the ***Create*** button in the Hyperlink column. This hyperlink function enables the administrator to manage the devices from WAN easily.

When the ***Monitor Now*** button is clicked, **Monitor IP Results** page will appear. If the entered IP address is unreachable, a red dot under Result field will appear. A green dot indicates that the IP address is reachable and alive.



Monitor IP Results		
No.	IP Address	Result
1	192.168.2.254	
2	192.168.1.110	

4.4.4 Walled Garden

This function allows clients of specified addresses or domain names to access the Internet before login and authentication. Up to 20 addresses or domain names of websites can be defined in this list. Users without network access right in this list can make use of the actual network service free of charge.

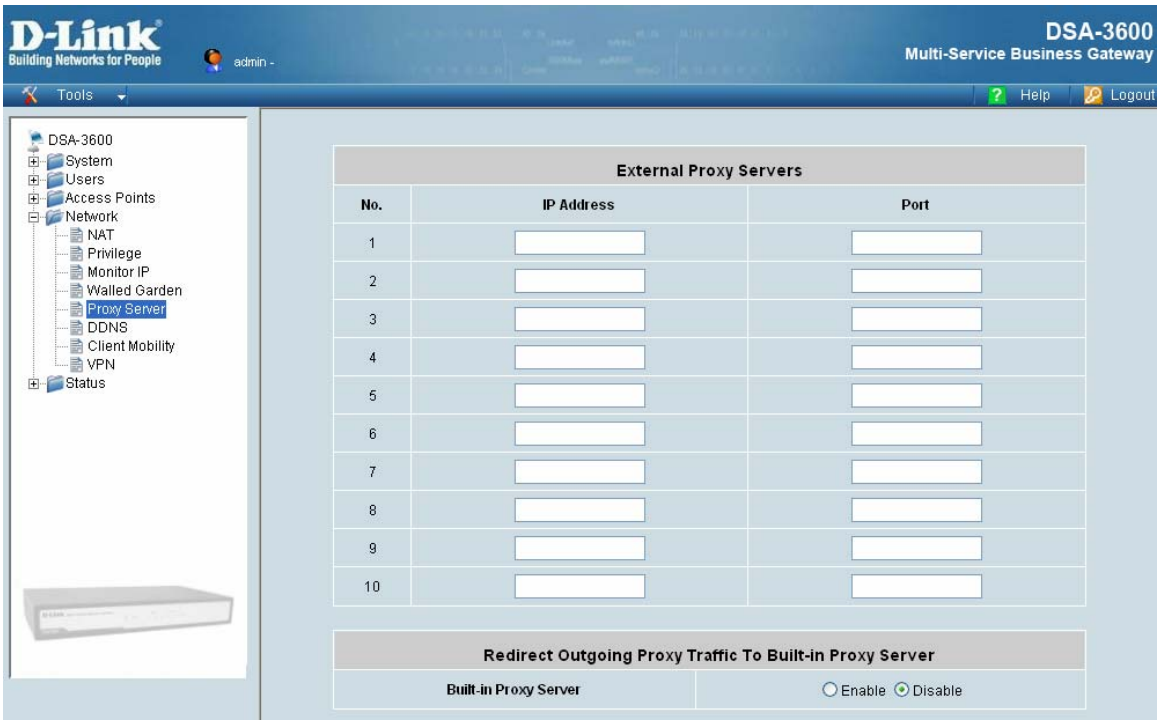
Enter the **IP Address** or **Domain Name** of the websites in the list. The settings will be effective immediately after clicking ***Apply***.

The **Walled Garden** supported by the system provides free surfing areas for clients to access before they are authenticated by the system. An example may be seen in hotels, where guests without network access right are allowed to utilize the network service free of charge.

Caution: *To use domain names in list, a DNS server must first be configured in the network in order for this function to work.*

4.4.5 Proxy Server

The DSA-3600 supports External Proxy Server functions and provides a built-in Proxy Server. Under its security management, the system will match the proxy setting of External Proxy Servers list to the clients' proxy setting in their browsers. If no matching is found, the clients will not be able to get the login page nor access the network. If a matching is found, the clients will first be directed to the system for authentication, and upon successful authentication, redirect the clients back to the desired proxy servers.

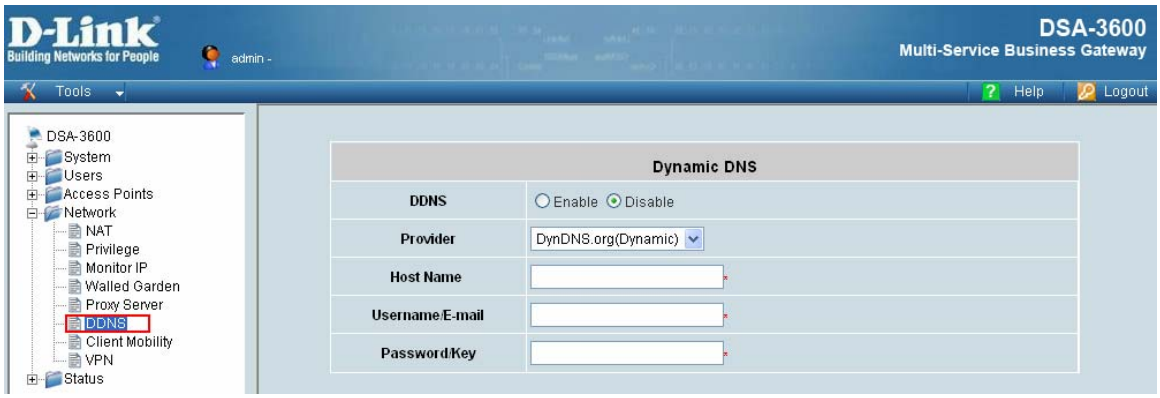


- **External Proxy Servers:** The system will match the proxy setting of the **External Proxy Servers** list to the clients' proxy setting if the setting is found in their browsers. If no matching is found, the clients will not be able to get the login page nor access the network. If a matching is found, the clients will first be directed to the system for authentication, and upon successful authentication, redirect the clients back to the desired proxy servers.
- **Redirect Outgoing Proxy Traffic To Built-in Proxy Server:** The DSA-3600 has a built-in proxy server. If this function is enabled, the clients will be forced to treat the DSA-3600 as the proxy server regardless of the clients' original proxy settings, and all traffic will be redirected through the built-in proxy server.

For more information about setting up the proxy servers, please refer to Appendix C – Proxy Configuration.

4.4.6 DDNS

The DSA-3600 provides a convenient dynamic DNS (DDNS) function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN1 port. When the DDNS is enabled, the system will update the newest IP address regularly to the DNS server if the WAN1 interface is set to Dynamic. These settings will become effective immediately after clicking ***Apply***.



- **DDNS:** Dynamic DNS, choose to enable or disable this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

Note: The fields with red asterisks are required to be filled in.

4.4.7 Client Mobility

The DSA-3600 supports **IP PNP** function. When enabled, this function allows clients with fixed or assigned IP address to authenticate through the DSA-3600 to access the network.

- **IP PNP:**

  By enabling IP PNP, a PC with a static IP address will be able to access the network even if the system enables the built-in DHCP server. No TCP/IP reconfiguration is needed.

4.4.8 VPN

Virtual **P**rivate **N**etwork (VPN) is designed to increase the security of information transferred over the Internet. VPN can work with wired or wireless networks and dial-up connections over POPS. It can create a private encrypted tunnel from the end user's computer, through the local wireless network and the Internet, to corporate servers and databases. There are 3 types of VPN connection supported by this system: **Local**, **Remote**, and **Site-to-Site**.

- **Local VPN**

When this setting is enabled, the system allows the VPN tunnel between a client's device and the system to encrypt the data transmission. The system's Local VPN supports end-users' devices using Windows 2000 and Windows XP SP1, SP2. Some IPSec parameters are available for change by the administrator. It allows the creation of encrypted channels between two servers, and can be used to filter IP traffic to authentication servers. To use this function, check **Enable** and choose the desired parameters. Click ***Apply*** to enable the Local VPN. For more information on IPSec VPN, please refer to **Appendix H– IPSec VPN**.

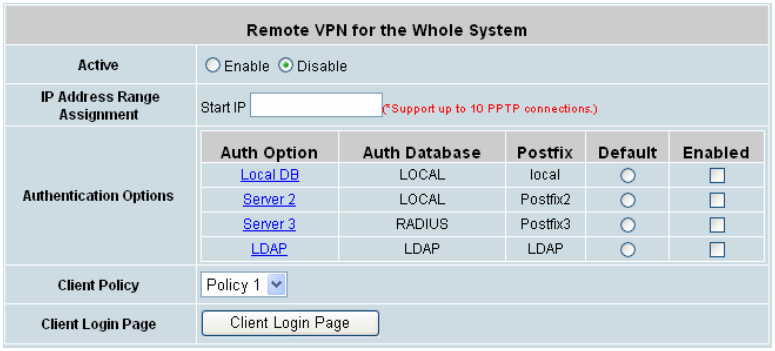
Local VPN For The Entire System	
Active	◉ Enable ○ Disable
VPN Client Isolation	○ Enable ◉ Disable
IPSec Parameters	
Encryption	○ DES ◉ 3-DES
Integrity	◉ MD5 ○ SHA-1
Diffie-Hellman	◉ Group 1 ○ Group 2

- **Remote VPN**

A PPTP tunnel can be established between the system and the remote user over the Internet. Check the **Enable** or **Disable** radio button in the Active column to activate or deactivate this function. If the Remote VPN function is enabled, enter the **Start IP** in the Client IP Address Range column.

When this setting is enabled, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP. The system's VPN supports end-users' devices using Windows 2000 and Windows XP SP1, SP2. Start IP field must be entered when enabled. The Client Policy, Supported Authentication Servers and the Remote VPN login page can also be customized here. The system supports up

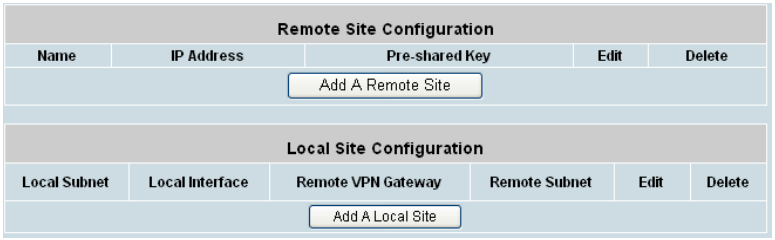
to 10 PPTP connections.



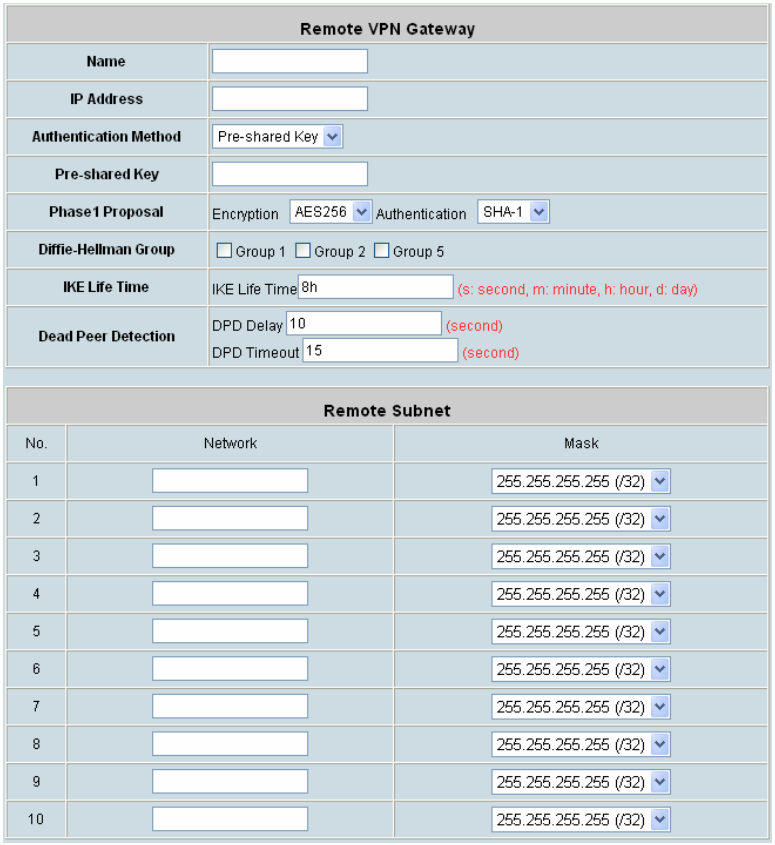
- **Site-to-Site VPN**

When the setting is enabled, the system will enable the IPSec VPN tunnel between two remote networks/sites to encrypt the data transmission. Click ***Add a Remote Site*** button to set the configuration of remote VPN capable devices, such as a VPN gateway. Click ***Add a Local Site*** button to set the configuration of the local site.

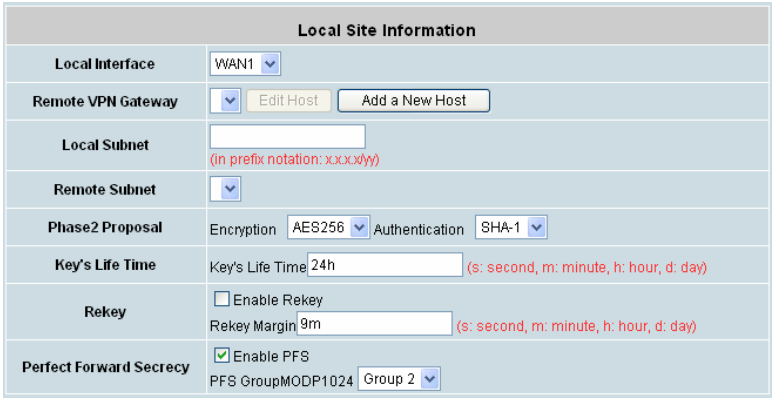
An IPSec tunnel can be constructed and used to connect to other IPSec capable devices on the Internet.



Click ***Add a Remote Site*** to enter the **Remote VPN Gateway** page for further configuration.

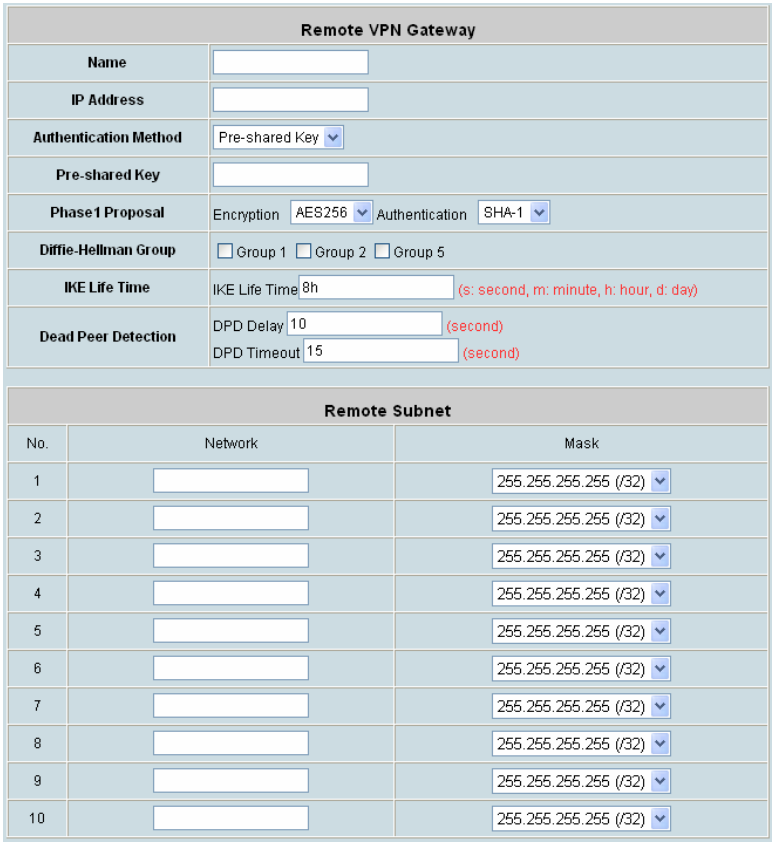


Click ***Add a Local Site*** to enter the **Local Site Information** page for further configuration.



Local Site Information	
Local Interface	WAN1
Remote VPN Gateway	Edit Host / Add a New Host
Local Subnet	(in prefix notation: x.x.x.x/yy)
Remote Subnet	
Phase2 Proposal	Encryption AES256 Authentication SHA-1
Key's Life Time	Key's Life Time 24h (s: second, m: minute, h: hour, d: day)
Rekey	Enable Rekey Rekey Margin 9m (s: second, m: minute, h: hour, d: day)
Perfect Forward Secrecy	Enable PFS PFS GroupMODP1024 Group 2

Click ***Add a New Host*** to enter the screen of **Remote VPN Gateway**.

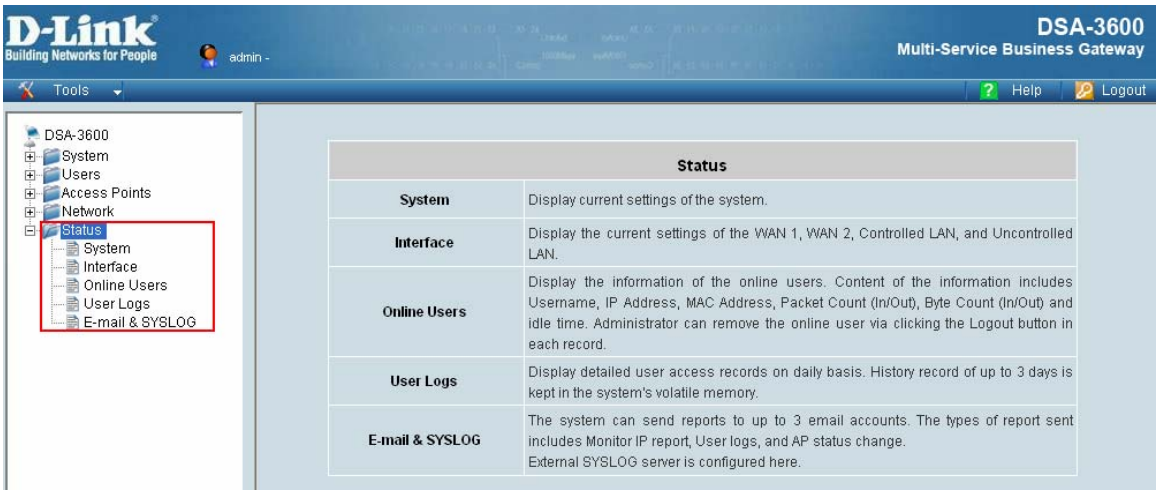


Remote VPN Gateway	
Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet		
No.	Network	Mask
1		255.255.255.255 (/32)
2		255.255.255.255 (/32)
3		255.255.255.255 (/32)
4		255.255.255.255 (/32)
5		255.255.255.255 (/32)
6		255.255.255.255 (/32)
7		255.255.255.255 (/32)
8		255.255.255.255 (/32)
9		255.255.255.255 (/32)
10		255.255.255.255 (/32)

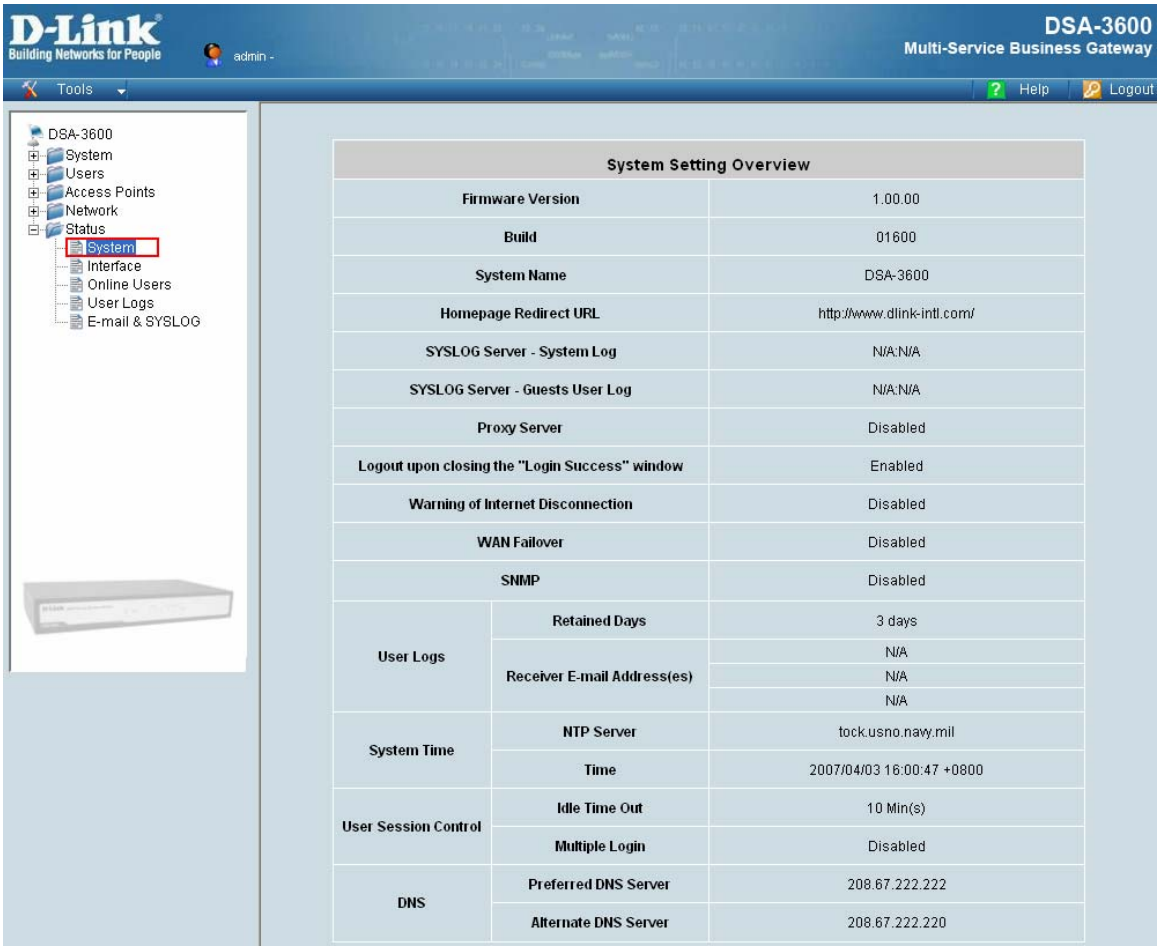
4.5 Status

This section covers the description of system status information and online user status, which include **System**, **Interface**, **Online Users**, **User Logs**, and **E-mail & SYSLOG**. An overview of the system is also provided here for the administrator's reference.



4.5.1 System

This section provides an overview of the system administration.



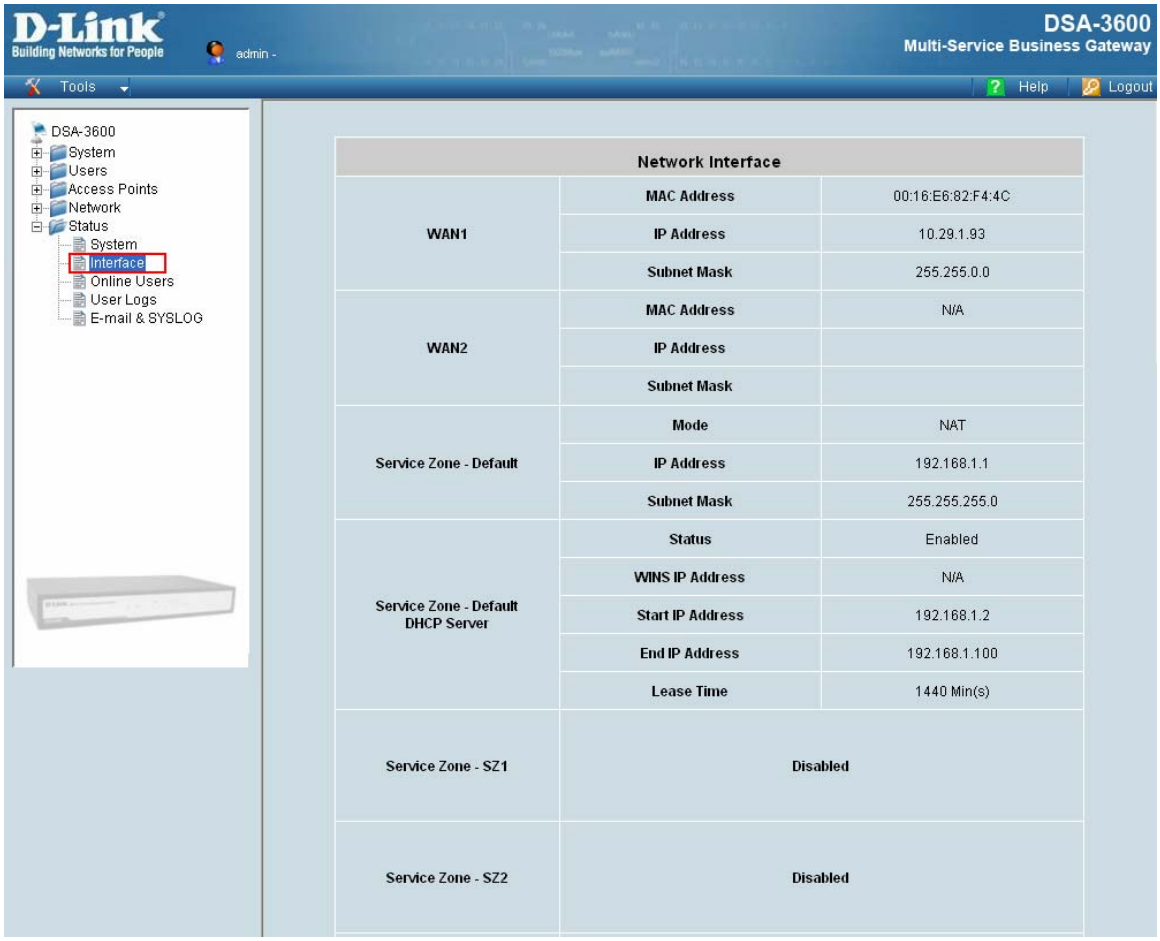
System Setting Overview		
Firmware Version		1.00.00
Build		01600
System Name		DSA-3600
Homepage Redirect URL		http://www.dlink-intl.com/
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - Guests User Log		N/A:N/A
Proxy Server		Disabled
Logout upon closing the "Login Success" window		Enabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2007/04/03 16:00:47 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	208.67.222.222
	Alternate DNS Server	208.67.222.220

The following information in the table describes all the items found in the System Setting Overview menu:

Item		***Description***
Firmware Version		The present firmware version of DSA-3600
System Name		The system name. The default is DSA-3600
Homepage Redirect URL		The page to which the users are directed after initial login success.
SYSLOG server - System Log		The IP address and port number of the external Syslog Server. N/A means that it is not configured.
SYSLOG server - Guest User log		The IP address and port number of the external Syslog Server. N/A means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Friendly Logout		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users try to close the login successful window.
Warning of Internet Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal and all online users are allowed/disallowed to log in the network.
WAN Failover		Shows the connection status of WAN1 and WAN2.
Management	**Management Console IP Address**	The IP or IPs that is allowed for accessing the web management interface.
	SNMP	Enabled/disabled stands for the current status of the SNMP management function.
User Logs	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Receiver E-mail Addresses	The e-mail address that the traffic history information will be sent to.
System Time	**NTP Server**	The network time server that the system is set to align.
	Time	The system time is shown as the local time.
User Session Control	**Idle Time Out**	The number of minutes allowed for the users to be inactive.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

4.5.2 Interface

This section provides an overview of the all interfaces for the administrator such as **WAN1, Service Zone – Default, Service Zone – Default DHCP Server.** Each service zone represents a virtual system, therefore, the information of the system's network interface is grouped by service zone.



Network Interface		
WAN1	MAC Address	00:16:E6:82:F4:4C
	IP Address	10.29.1.93
	Subnet Mask	255.255.0.0
WAN2	MAC Address	N/A
	IP Address	
	Subnet Mask	
Service Zone - Default	Mode	NAT
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.2
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	Disabled	
Service Zone - SZ2	Disabled	

The description of the table is as follows:

Item		***Description***
WAN1	**MAC Address**	The MAC address of WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
Service Zone - Default	**Mode**	The mode address of the default service zone.
	IP Address	The IP address of the default service zone.
	Subnet Mask	The Subnet Mask of the default service zone.
Service Zone – Default DHCP Server	**Status**	Enable/Disable stands for status of the build-in DHCP server on the service zone.
	WINS IP Address	The WINS server IP.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP Address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the service zone.
Service Zone – SZ1~SZ4	**Disabled**	Enable/Disable stands for status of the SZ1~SZ4 server on the service zone.

4.5.3 Online Users

Each online user's information can be obtained using this function. These include **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Idle, Access From** and **Kick Out**. All online users will be listed here. The administrator can use this function to force a specific online user to log out, or terminate any user session by clicking the hyperlink of ***Kick Out*** button.

Click ***Refresh*** to renew the current users list.

4.5.4 User Logs

This function is used to check the history of DSA-3600. The history of each day will be saved separately in the DRAM for 3 days.

Caution: *Since the history is saved in the DRAM, if you need to restart the system and also keep the history, then please manually copy and save the information before restarting.*

If the **Receiver E-mail Address for System Log** has been entered under the **E-mail & SYSLOG** page, then the system will automatically send out the history information to that e-mail address.

- **Users Log**

  The Users Log provides users' login and logout activities except guest users and RADIUS roaming in/out users such as Date, username, IP address, MAC address, Packets In count, and Packets Out count.

- **Guests User Log**

  The Guests User Log provides the login and logout activities of guest users such as Date, username, IP address, MAC address, Packets In, and Packets Out.

  - **System Name:** The system name defined in General tab of System category.
  - **Type:** The authentication status of the user.
  - **1st Login Expiration Time:** This is a constant value of 1 day.
  - **Account Valid Through:** This is the Expired info setting in Plan Configuration of Guest User.
  - **Remark:** The administrator can add extra information here about each Guest User.

- **Roaming Out User Log**

  The Roaming Out User Log provides the login and logout activities of roaming out users such as Date, username, IP address, MAC address, Packets In, and Packets Out.

  - **Type:** The authentication and accounting type of the external RADIUS server. There is a type called Accept for authentication. There are three types of accounting, Start, Interim-update, and Stop.
  - **NASID:** The System ID of the system. Usually, NASID is the MAC address of the WAN port of the

system.

- **NASIP:** The IP address of the WAN port of the system.
- **NASPort:** The port of the WAN port of the system.
- **UserMAC:** The MAC address of the user.
- **SessionID:** The system will give a unique Session ID to an authenticated user when he/she starts a new session.
- **SessionTime:** The time in seconds of this session.
- **Bytes In/Out:** The traffic amount of inbound/outbound traffic based on byte.
- **Pkts In/Out:** The traffic amount of inbound/outbound traffic based on packet.
- **Message:** The system response of why the client stops this session.

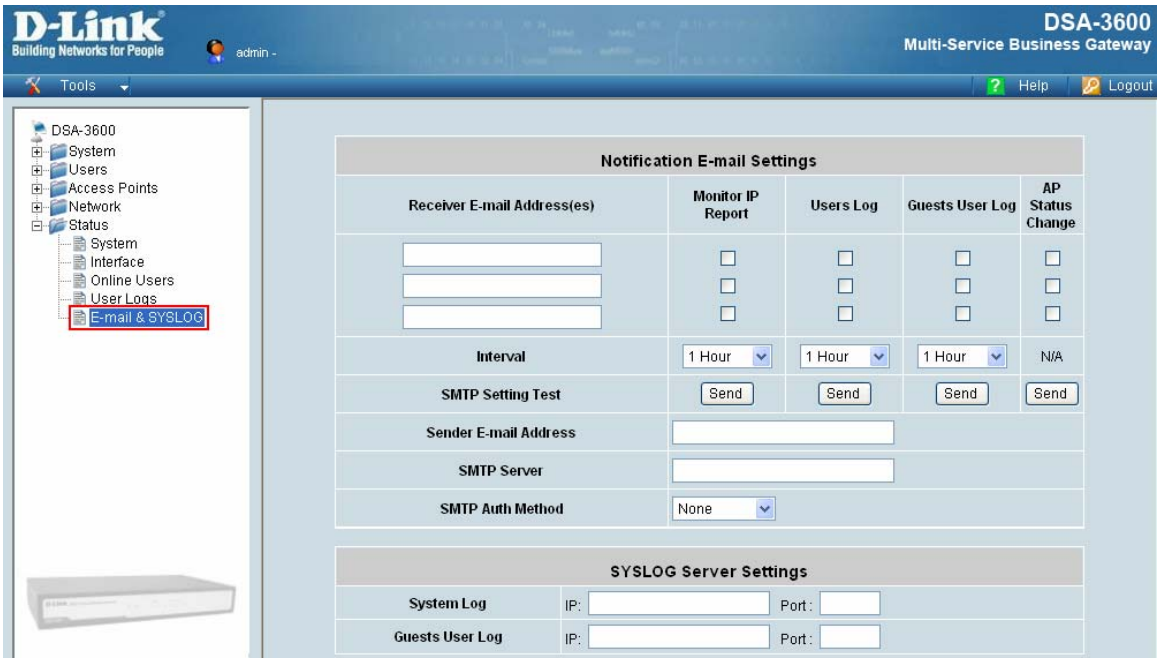
- **Roaming In User Log**

  The Roaming In User Log provides the login and logout activities of roaming in users such as Date, username, IP address, MAC address, Packets In, and Packets Out.

  - **Type:** The authentication and accounting type of the external RADIUS server. There is a type called Accept for authentication. There are three types of accounting, Start, Interim-update, and Stop.
  - **NASID:** The System ID of the system. Usually, NASID is the MAC address of the WAN port of the system.
  - **NASIP:** The IP address of the WAN port of the system.
  - **NASPort:** The port of the WAN port of the system.
  - **UserMAC:** The MAC address of the user.
  - **SessionID:** The system will give a unique Session ID to an authenticated user when he/she starts a new session.
  - **SessionTime:** The time in seconds of this session.
  - **Bytes In/Out:** The traffic amount of inbound/outbound traffic based on byte.
  - **Pkts In/Out:** The traffic amount of inbound/outbound traffic based on packet.
  - **Message:** The system response of why the client stops this session.

4.5.5 E-mail & SYSLOG

The system supports sending notification e-mails of Monitor IP Report, Users Log, Guest User Log, and AP Status Change up to 3 e-mail accounts automatically. The notifications of AP Status Change are triggered by event when a managed AP becomes unreachable, while the other three types of e-mails are sent periodically in given intervals. A trial e-mail is provided by the system for validation. In addition, the system supports recording SYSLOG of User Log and Guests User Log to external SYSLOG servers.



- **Receiver E-mail Address(es):** The e-mail address of the person whom the history e-mail is for. This will be the receiver's e-mail. Check which type of report to be sent—Monitor IP Report, System Log, Guests User Log, and AP Status Change.
- **Interval:** The time interval to send the e-mail report. Choose a proper number from the drop-down box.
- **SMTP Setting Test:** To test if the settings is correct or not.
- **Sender E-mail Address:** The e-mail address of the sender in charge of the monitoring.
- **SMTP Server:** The IP address of the SMTP server.
- **SMTP Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.

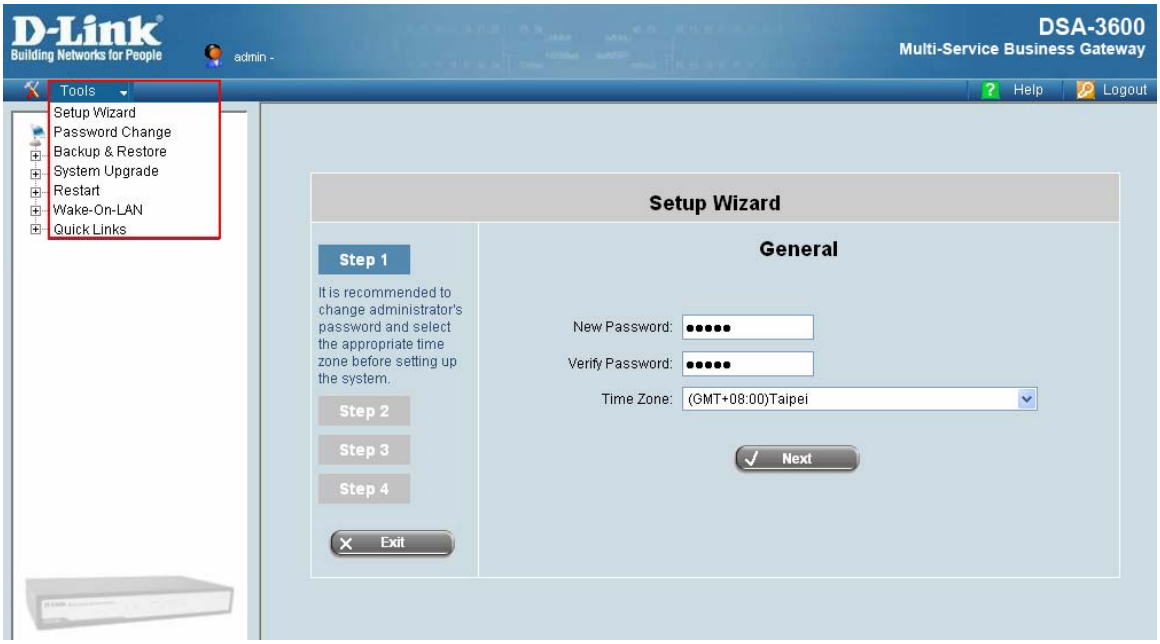
  NTLMv1 is not currently available for general use.

  Plain and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express uses **Login** as default, although they can be set to use **NTLMv1**.

  Pegasus uses **CRAM-MD5** or **Login** but can not be configured which method to use.
- **Syslog Server Settings:** There are 2 types of syslog supported: System Log and Guests User Log. Enter the IP address and Port to specify which and from where the report should be sent to.

4.6 Tools

This section provides information on seven utilities used for customizing and maintaining the system, including **Setup Wizard**, **Change Password**, **Backup/Restore Setting**, **System Upgrade, Restart, Wake-On-LAN, and Quick Links**.



4.6.1 Setup Wizard

The administrator can configure the DSA-3600 via its web management interface as specified. In order to connect to the Internet, the TCP/IP related information such as IP address, subnet mask, and gateway address, must first be obtained from the ISP. The Configuration Wizard uses four simple steps to provide easy setup of the DSA-3600.

- General
- WAN1 Interface
- Local User Account (Optional)
- Confirm and Restart

The Setup Wizard provides express setup procedures for D-Link DSA-3600 in 4 steps. Follow the instructions given at each step to change the system admin password, select time zone, configure WAN1 interface, and create local user account. Upon completing the Setup Wizard procedures, the system will need to be restarted in order for the setting to take effect. The system is ready for operation after restart. Please refer to the Quick Installation Guide of DSA-3600 if step-by-step screen images can help the process.

- **Running the Wizard**

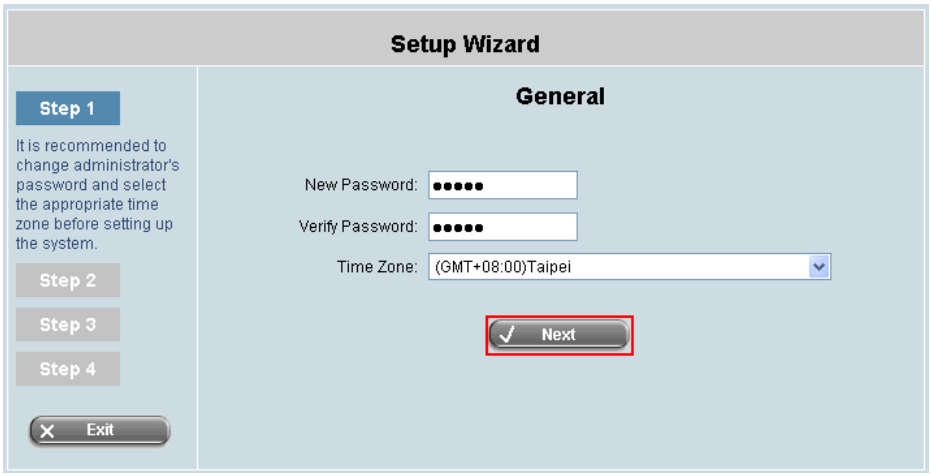
  Click ***Tool*** and **Setup Wizard** the left-top menu, and the **Setup Wizard** page will appear.

  Please read the recommendation of each step.

- **Step 1: General**

  Change Password

  Enter the administrator's **New Password** in the New Password field and retype it again in the **Verify Password** field. (Note: The maximum length of the password is twenty-character and no space is allowed.) To secure the system, changing the administration account password is recommended. Next, select a proper time zone from the **Time Zone** drop-down menu to set the system time. Click ***Next*** to continue.



- **Step 2: WAN1 Interface**

  Select the Connection Type for WAN1 Port

  Select an Internet connection type for WAN1 interface. Contact your ISP or the network administrator to make sure the connection type for WAN1. There are three connection types provided by DSA-3600: **Static**, **Dynamic** and **PPPoE**. Enter the **Username** and **Password** provided by the ISP. Click ***Next*** to continue, or click ***Back*** to change configurations in previous step.

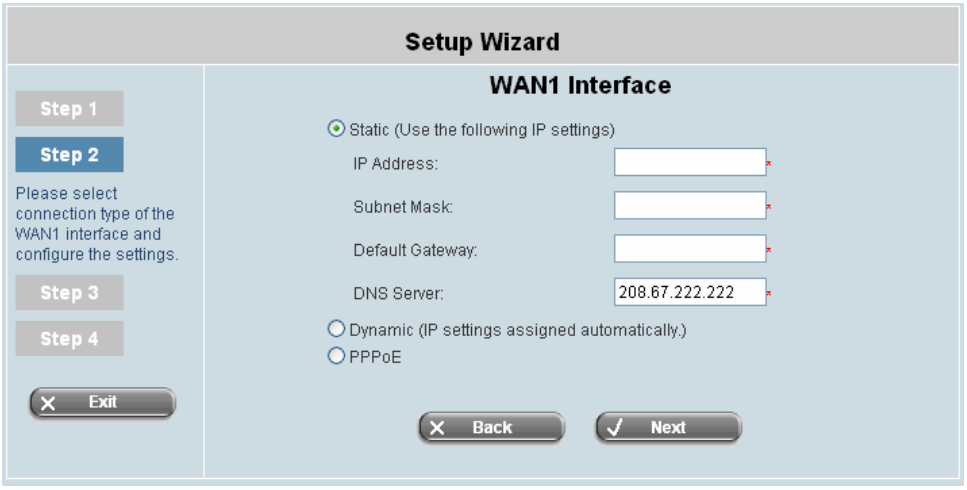
  - **Dynamic IP Address**

    If this option is selected, an appropriate IP address and related information will be assigned automatically. Click ***Next*** to continue.

  - **Static IP Address: Set WAN1 Port's Static IP Address**

    Enter the **IP Address**, **Subnet Mask** and **Default Gateway** provided by the ISP.

    Click ***Next*** to continue.



- **PPPoE: Set PPPoE Client's Information**

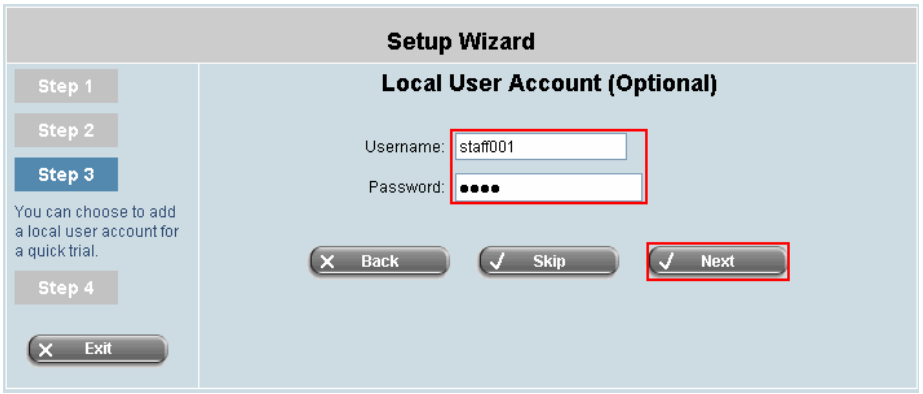
  Enter the **Username** and **Password** provided by the ISP.

  Click ***Next*** to continue.

- **Step 3: Local User Account (Optional)**

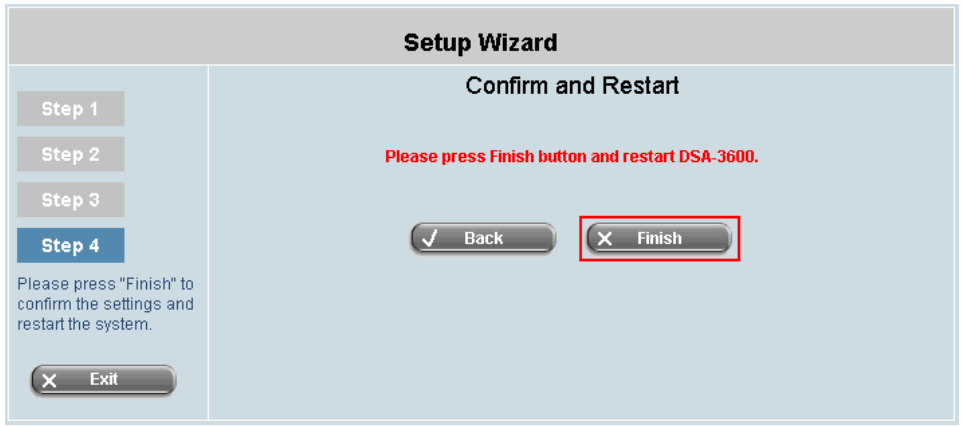
  Local User - Add User

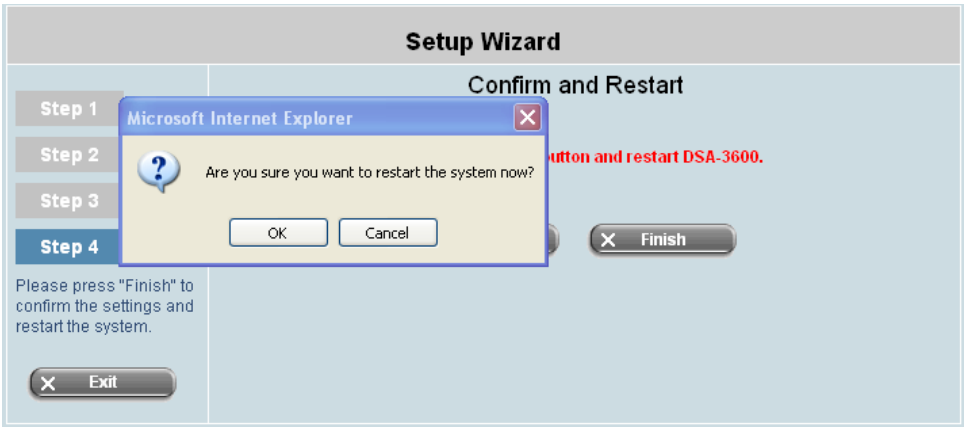
  New local accounts can be added into the local user database. Enter the **Username** (e.g. staff001) and **Password** (e.g. Jim) of the desired new account to add a new local account into the system. Click ***Skip*** to exit step 3 or click ***Next*** to validate added local accounts and continue.



- **Step 4: Confirm and Restart**

  Click ***Finish*** button to save the current settings and restart the DSA-3600. A confirming message will appear after clicking ***Finish***. Click ***OK*** to continue. The **Setup Wizard** is now completed.





During the DSA-3600 restarting, a **Confirm and Restart** page will appear on the screen. Please do not interrupt the DSA-3600 until the DSA-3600 Administrator Login Page reappears. This indicates that the restart process has been completed.

Back and Exit*: During every step of the wizard, if you wish to go back to modify the settings, please click the* ***Back*** *button to go back to the previous step. Click* ***Exit*** *to leave the Wizard.*

Please Note:

Login to web management interface again using “admin” for both the default username and password in the Username and Password fields. After logging the web management interface, click **System** and then click **Service Zones** to enter the **Basic Settings** page. Next, click the Server 1 hyperlink.

The DSA-3600 uses Virtual LAN (VLAN) along with a SSID to separate service zones. At this stage, the system is ready for use in minimum configuration. The factory default configuration uses tag-based VLAN. The ‘Default’ service zone (with SSID=’dlink’) is enabled and requires no user authentication at this initial stage.

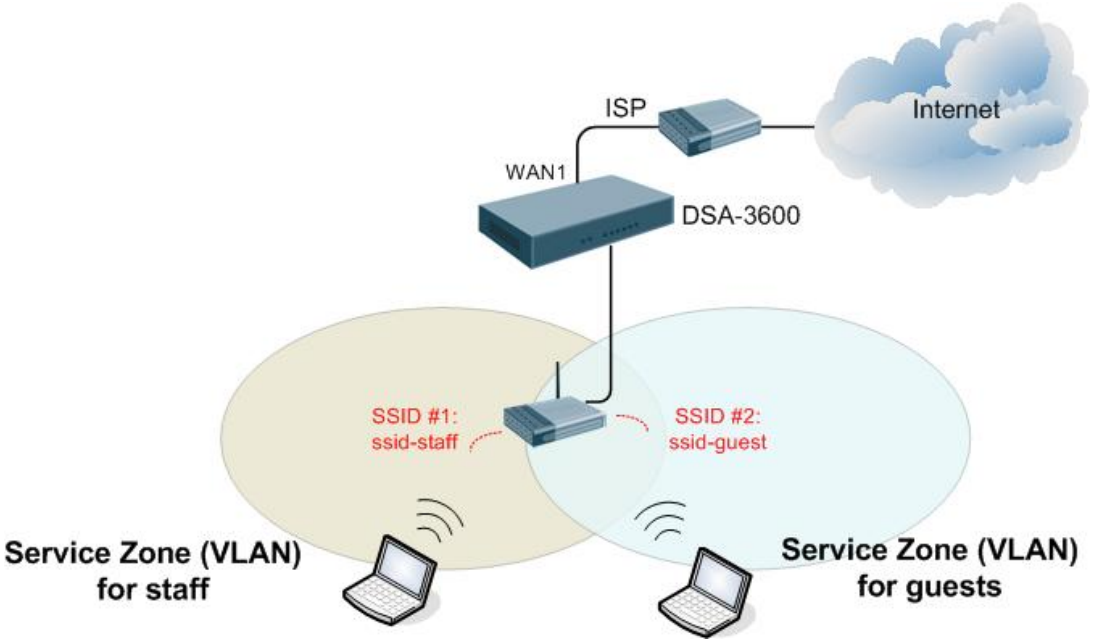


Figure-4.6.1a: An example using Tag-Based service zones

4.6.2 Change Password

The administrator can change the passwords of the system. Enter the required fields marked with red asterisks as show in the picture below. The login account for the administrator is “admin”. The admin password of the system can be changed here by entering the original password and new password. The default admin password of the system is "admin". Click ***Apply*** to activate the new passwords.

The DSA-3600 supports three types of account interface: **admin**, **manager** or **operator**. The account interfaces **are authenticated for access to specific configuration pages only,** depending on the account rights assigned**.** The default usernames and passwords are as follow:

Admin: The administrator can access all configuration pages of the DSA-3600.

User Name: **admin**

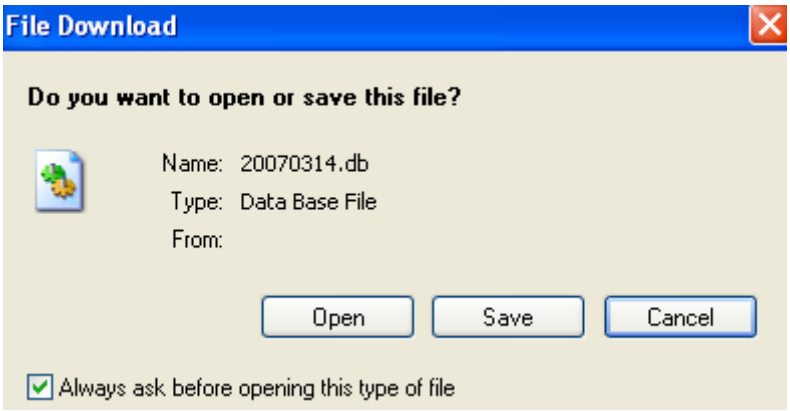
Password: **admin**

Caution: *If the administrator’s password is lost, the administrator’s password can still be changed through the text mode management interface on the console port.*

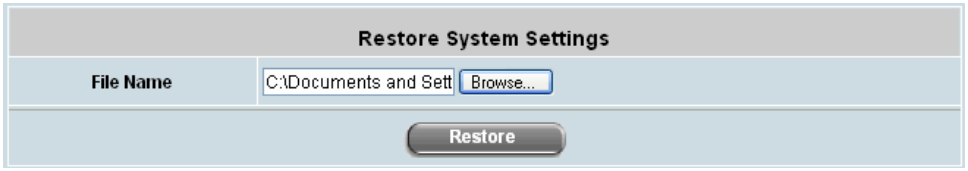
4.6.3 Backup/Restore

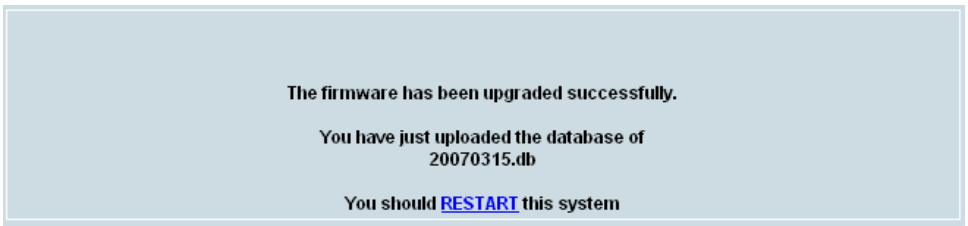
This function is used to backup/restore the DSA-3600 settings. The DSA-3600 can also be restored to the factory default settings using this function.

- **Backup System Setting:** Click ***Backup*** button to save the current system configurations to a backup file on a local disk of the management console. The backup file keeps the current system settings as well as the local user accounts information.

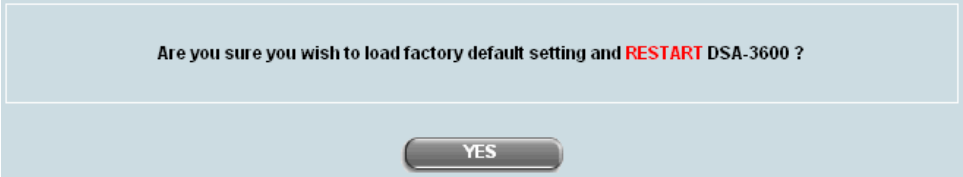


- **Restore System Settings:** Click ***Browse*** to search for a .db database backup file created by the DSA-3600 and click ***Restore*** to restore to the same settings at the time the backup file is created.





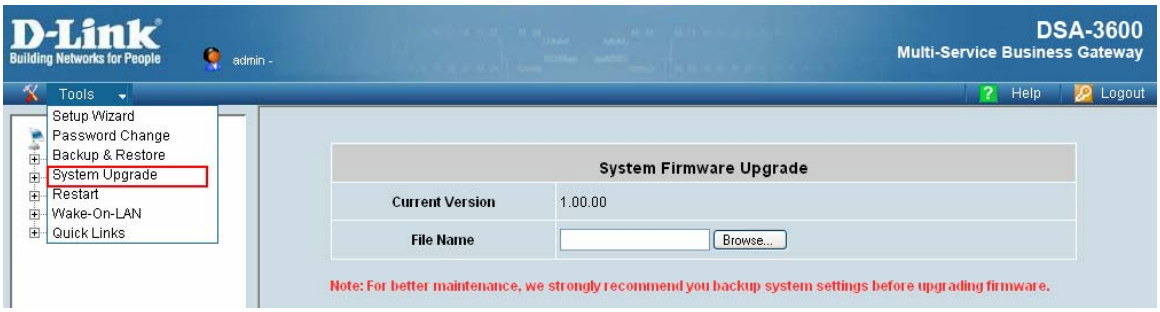
- **Reset to The Factory Default:** Click ***Reset*** to load the factory default settings of the DSA-3600.
  Note that a Reset action will wipe out the existing local user accounts. To back up the local user accounts, please export the local user accounts to a text first. Please refer to the section on Local User List for more details.



Caution: *Resetting to factory default settings will clear all settings, such as policies, billing plans, all user databases, and any configuration, to its initial state.*

4.6.4 System Upgrade

The administrator can download the latest firmware from the website and upgrade the system. To upgrade the system firmware, click the ***Browse*** button to choose the new firmware file and then click ***Apply*** to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system upon successful firmware upgrade.



Warning: *1. Firmware upgrade may sometime result in loss of some data. Please ensure you read the release notes to understand the limitations before upgrading the firmware.*
2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process, as it may damage the system and cause it to malfunction.

4.6.5 Restart

This function allows the administrator to safely restart the DSA-3600. The process should take about three minutes. Click ***YES*** to restart the DSA-3600; click ***NO*** to go back to the previous screen. If turning off the power is necessary, restart the DSA-3600 and wait for it to complete the restart process before turning off.

Click ***Restart*** to restart the system. Please wait for the blinking timer to finish before accessing the system web management interface again.

Note: *The connection of all online users on the system will be disconnected when the system is in the process of restarting.*

4.6.6 Wake-On-LAN

The Wake-on-LAN function allows the remote booting-up and powering-down of the computer connected on the LAN from the system. Enter the **MAC Address** of the desired device and click ***Wake Up*** to execute this function.

4.6.7 Quick Links

Quick Links provide the shortcut to eight links for administrators to directly access frequently used functions of the web management interface. The eight functional links are: **System Status**, **Local User Management**, **Policy Management**, **AP Management**, **Online User List**, **Guest Account Management**, **Authentication Configuration** and **Firmware Management**.

4.6.7.1 System Status

The System Status quick link provides at a glance, the **System Setting Overview**, a shortcut to **4.5.1 System** in **Status** section. It provides a summary of system information to the administrator in a single page. Please refer to the section on System for details.

System Setting Overview		
Firmware Version		1.00.00
Build		00100
System Name		DSA-3600
Homepage Redirect URL		http://www.dlink-intl.com/
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - Guests User Log		N/A:N/A
Proxy Server		Disabled
Friendly Logout		Enabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Management	Management Console IP Address	N/A
	SNMP	Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2007/03/14 15:35:30 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	208.67.222.222
	Alternate DNS Server	208.67.222.220

4.6.7.2 Online User List

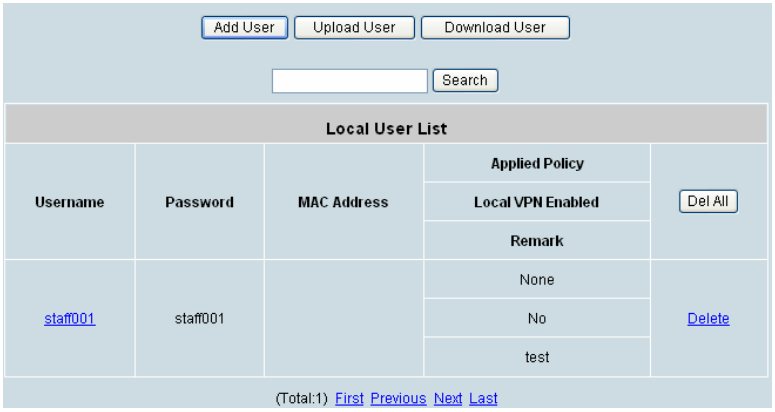
Online Users List provides information from the **Users List**, a shortcut to **4.5.3 Online Users** in **Status** section. This list provides to the administrator at a glance all the users online for easy termination of any user session. Please refer to the section on Online Users for details.

Online Users List						
No.	Username		Pkts In	Bytes In	Idle (Sec.)	Access From
	IP Address	MAC Address	Pkts Out	Bytes Out		Kick Out

Refresh

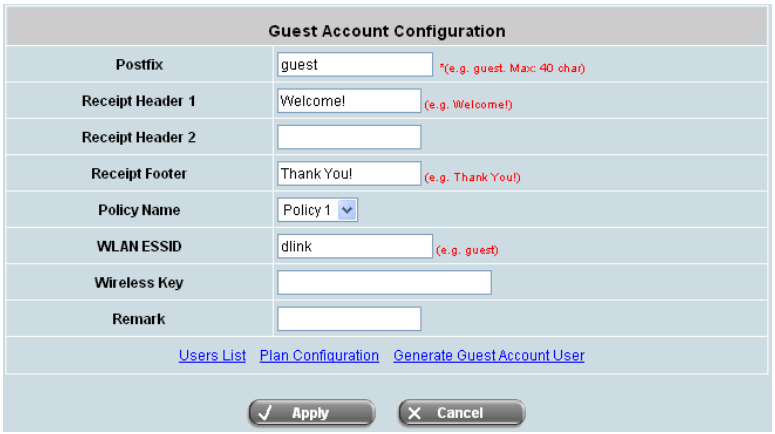
4.6.7.3 Local User Management

Local User Management provides information from the **Local User List**, a shortcut to **4.3.1 List** in **Access Points** sections and **4.1.6 Service Zone → Service Zone Settings → Authentication Settings** as well as **Authentication database → Local** in **System**. It lets the administrator add supported APs from Discovery or from the Adding menu tab, reboot, disable, and delete managed APs, and apply template. Please refer to the section on Local User List for details.



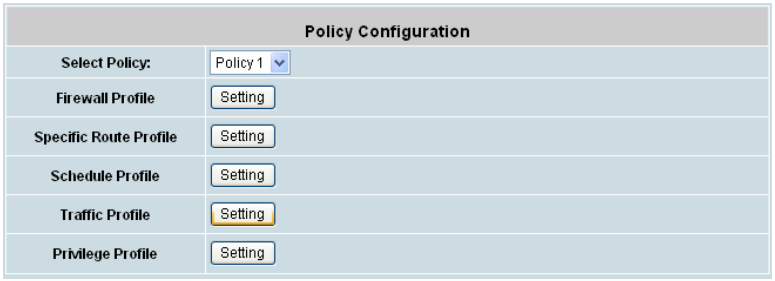
4.6.7.4 Guest Account Management

Guest Account Management provides information from the **Guest Account Configuration**, a shortcut to **4.2.1 Authentication** in **Users** sections and **4.1.6 Service Zone → On-demand Server** in **System**. It lets the customers use wireless Internet with username and password from retail environment for access. Please refer to the section on Guest Account Configuration for details.



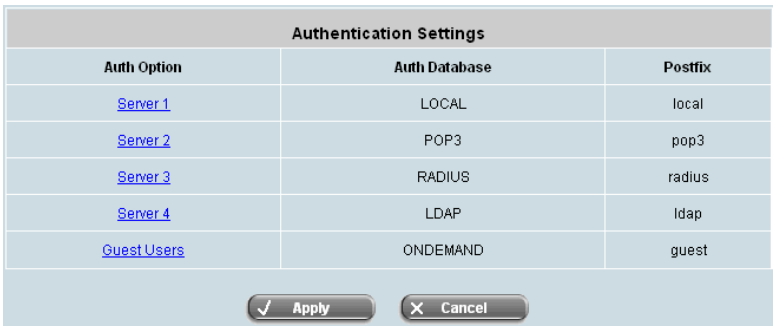
4.6.7.5 Policy Management

Policy provides information from the **Policy Configuration**, a shortcut to **4.2.3 Policy** in **Users** sections. It lets the administrator select one of the defined policies to apply to specific authentication option. Please refer to the section on Policy Configuration for details.



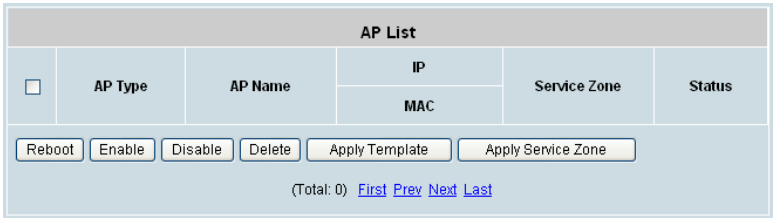
4.6.7.6 Authentication Configuration

Authentication Configuration provides information from the **Authentication Settings**, a shortcut to **4.2.1 Authentication** in **Users** sections and **4.1.6 Service Zone → Service Zone Settings → Authentication Settings** in **System**. It lets the administrator configure a list of authentication options which can be enabled or disabled within each service zone's management. Please refer to the section on Authentication for details.



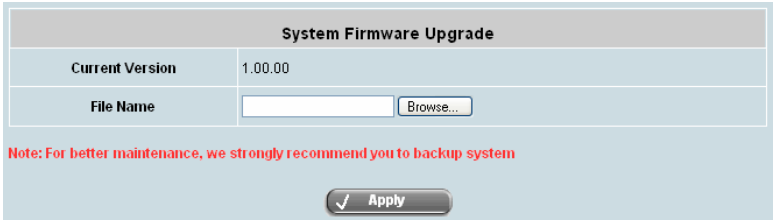
4.6.7.7 AP Management

AP Management provides information from the **AP List**, a shortcut to **4.3.1 List** in **Access Points**. It lets the administrator add supported APs from Discovery or from the Adding menu tab, reboot, enable, disable, delete the managed APs or apply template. Please refer to the section on AP List for details.



4.6.7.8 Firmware Management

Firmware Management provides information from the **System Firmware Upgrade**, a shortcut to **4.6.5 System Upgrade** in **Tools**. It lets the administrator download the latest firmware from the website and upgrade the system. Please refer to the section on System Upgrade for details.



4.7 Help

The **Help** button is at the upper right corner of the DSA-3600 display screen.

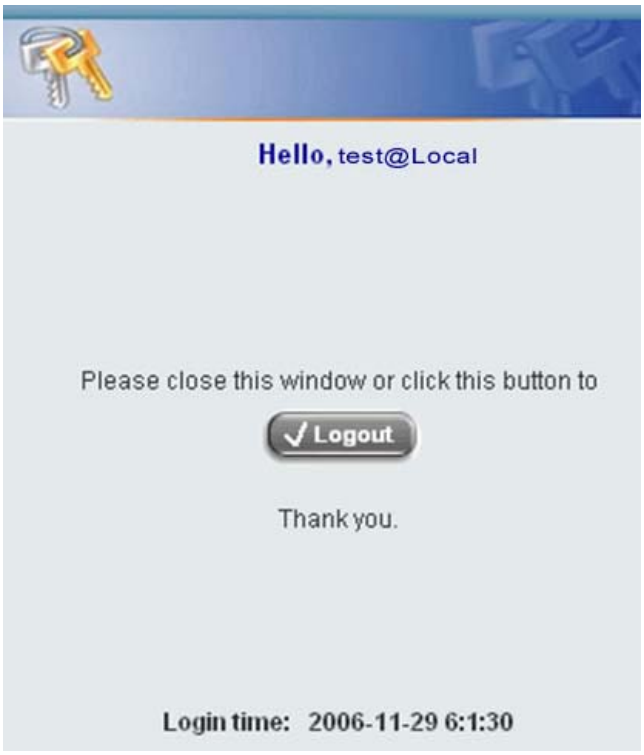
Click ***Help*** for the **Online Help** window, then click the hyperlink of the relevant information required.

Appendix A. External Network Access

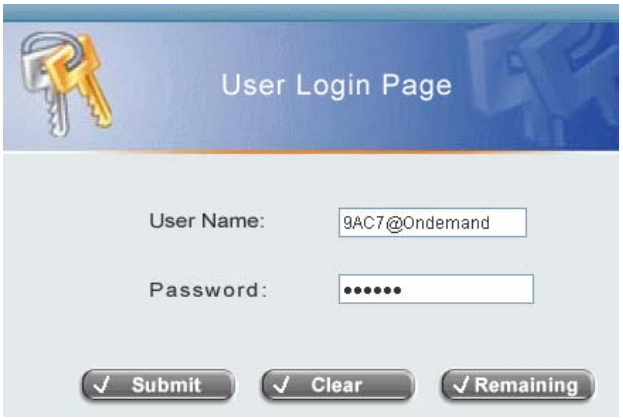
Upon completing this process, the DSA-3600 will be connected to a managed network in a controlled network access environment.

1. Connect a client's device, such as a PC, to the LAN port of the DSA-3600 with authentication required. The device will get an IP address automatically via DHCP. Next, open a web browser and access any URL. The default **User Login Page** will appear. Enter the ***User Name*** and ***Password*** created in the local user account database by the Configuration Wizard, then click ***Submit*** (e.g. ***test@Local*** for the username and ***test*** for the password).

2. If the Login page appears, it means the DSA-3600 has been installed and configured successfully. The client user can now browse the network or surf the Internet!



3. An Instant user can enter the username and password in the **User Login Page** and click the ***Remaining*** button to know the remaining time or data quota of the account.



4. When an Instant user logs in successfully, the successful **Login** screen will appear, which differs from the usual user's login successfully screen, as it contains an extra line showing **"Remaining usage"** and a ***Redeem*** button.

- **Remaining usage:** Shows the remainder usage time that the Instant user can surf the Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user will have to pay to add credit at the counter, where the user will then get a new username and password. After clicking the ***Redeem*** button, the following screen will show up.

- Enter the new username and password obtained, and click the ***Redeem*** button to merge the two accounts to add up the available usage time and data size by the system. The total available usage time and data size after adding credit will then be shown.

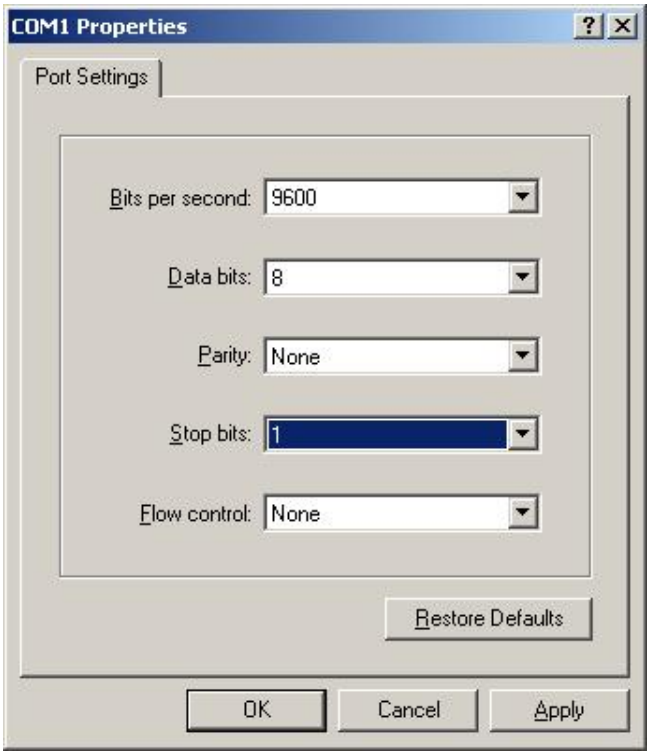
Caution: *The maximum session time/data transfer is 24305 days/2003 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process*

Appendix B. Console Interface Configuration

Upon completing this process, the console interface configuration will be accessible via the console port to handle problems and situations occurring during operation.

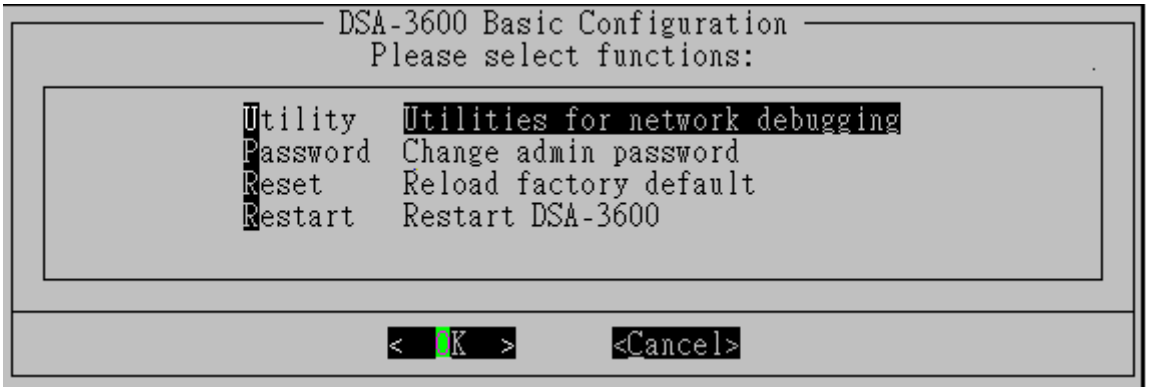
1. To connect to the console port of the DSA-3600, a console, modem cable, and a terminal simulation program such as the Hyper Terminal will be required.

2. Set the parameters as **9600, 8, n, 1** for Hyper Terminal.



Caution: *The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

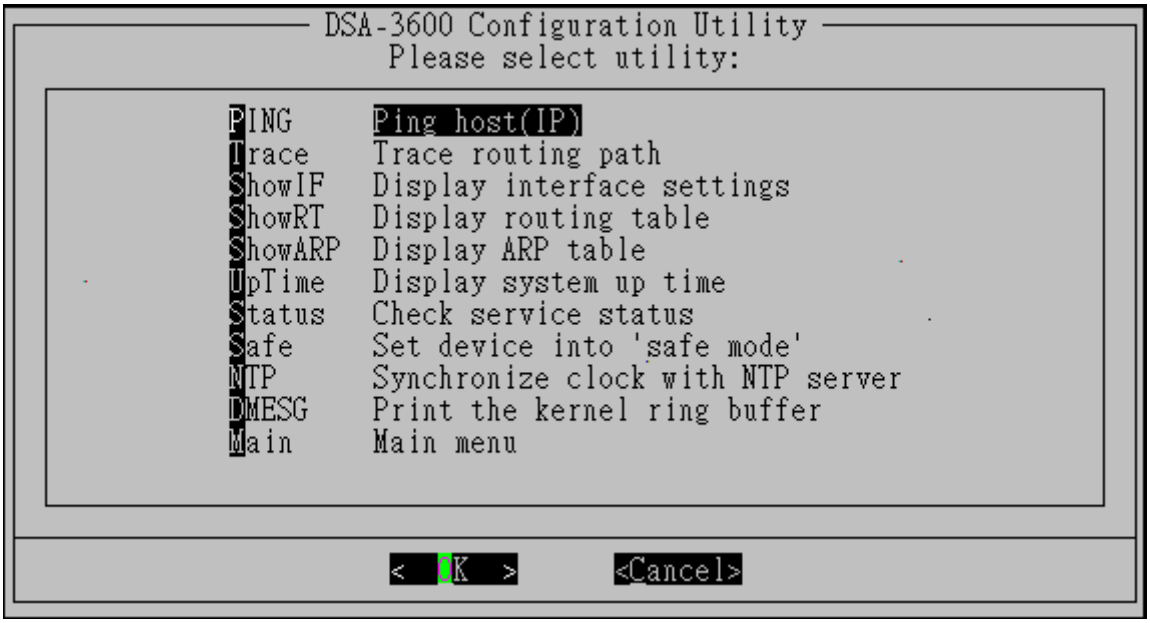
3. Once the console port of the DSA-3600 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, press the arrow keys of the keyboard to enable the terminal simulation program to send out some messages. The welcome screen or the main menu should then appear. If the welcome screen or the main menu of the console still does not appear, please check the connection of the cables and the settings of the terminal simulation program.



1. **Utilities for network debugging**

Appendix B. Console Interface Configuration

The console interface provides several utilities to assist the administrator to check the system conditions and perform debugging. The utilities are described as following:



- Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: Displays the information of each network interface setting including the MAC address, IP address, and netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Display ARP table: The internal ARP table of the system is displayed.
- Display system up time: The system live time (time for system being turned on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into “safe mode”: Used when the administrator is unable to access the Web Management Interface via the browser or when it fails inexplicitly. The administrator can choose this utility and set the DSA-3600 into safe mode to manage the device using a browser.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, reset of internal clock can only be performed through the NTP.
- DMESG: Display the kernel ring buffer to the screen. The dmesg program helps users to print out their bootup messages.

2. **Change admin password**

Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, there is no need to enter that administrator's password to access the console management interface. When connecting the system via SSH, however, the username and password will be needed.

The username and the default password is "admin" by default, which is similar to the web management interface. The administrator's password can be changed. If the password cannot be remembered and the management interface cannot be accessed from the web or the remote end of the SSH, the null modem can still be used to connect the console management interface, where the administrator can then reset the password.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, it is recommended that you immediately change the DSA-3600 admin username and password after logging into the system for the first time.*

3. **Reload factory default**

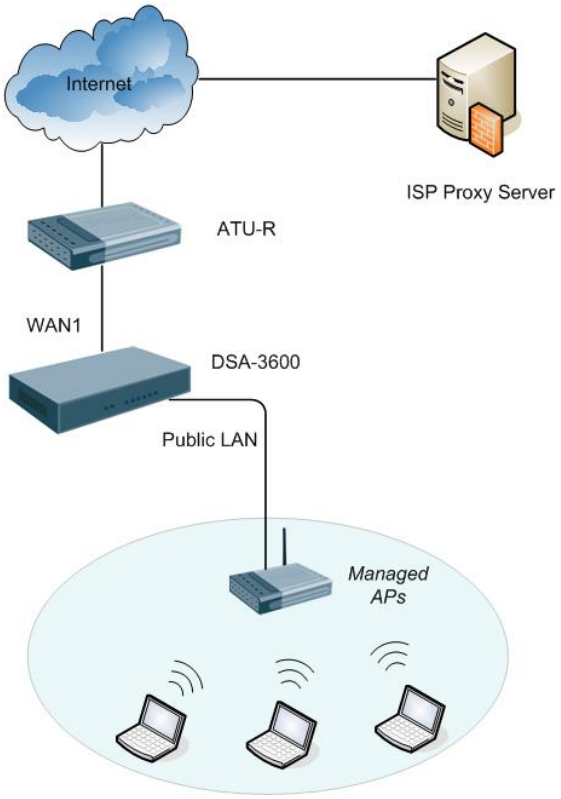
Choose this option to reset the system configuration to the factory default settings.

4. **Restart the DSA-3600**

Appendix C. Proxy Configuration

For Hotspot

A hot spot is a wireless LAN node providing Internet connection and virtual private network access from a given location, such as a coffee shop, hotel, or a public place where Wi-Fi service is made available for mobile users. A hotspot is usually implemented without sophisticated network architecture via proxy servers from the Internet Service Providers (ISPs).



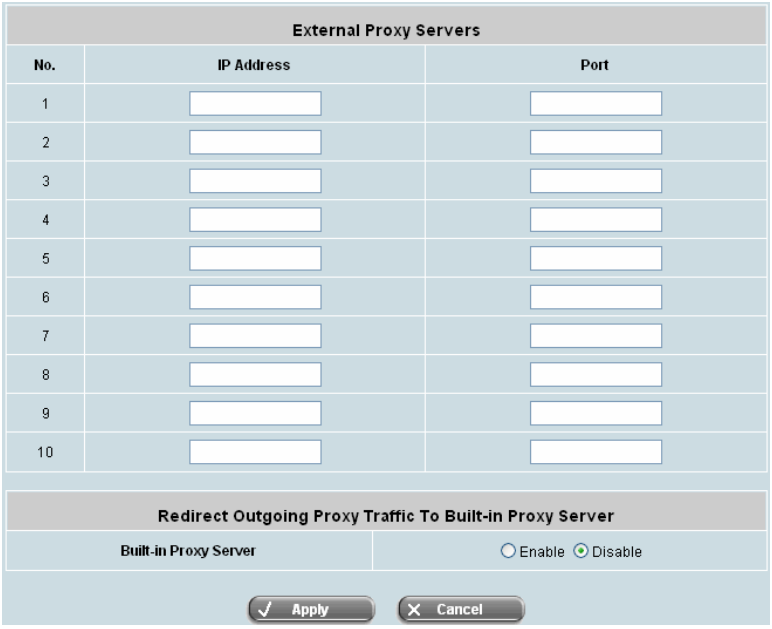
In a hotspot environment, users usually enable their proxy setting using their web browsers. The DSA-3600 likewise needs to set some proxy configuration in the Gateway. Follow these steps to complete the proxy configuration：

1. Login Gateway by using ***admin*** account.

2. Click the ***Network*** from menu tree and the ***Network Configuration*** page will appear.

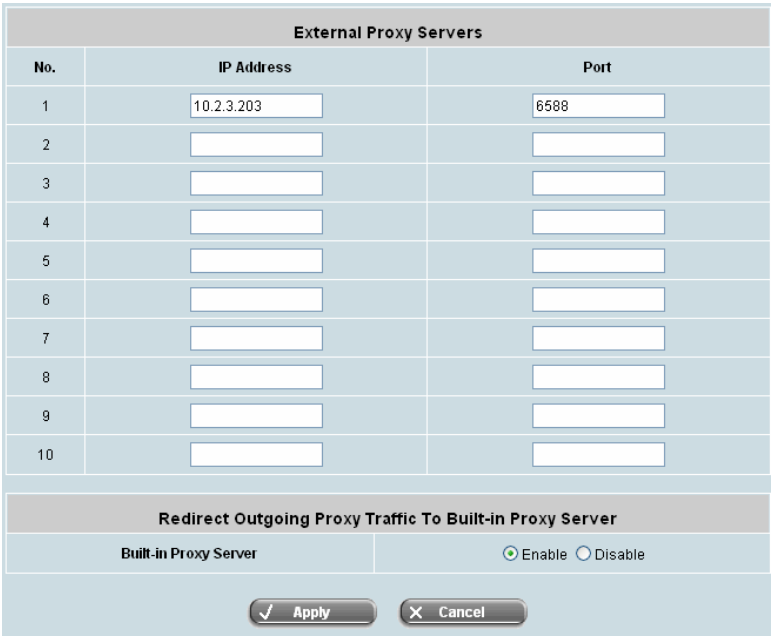
Network Configuration	
NAT	The NAT function supports 3 types of network address translation: DMZ(Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege	The Privilege function supports two types of privilege list based on IP address and MAC address. Devices specified in the list require NO authentication to access the network.
Monitor IP	Up to 40 IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.
Walled Garden	Up to 20 domain names/IP addresses can be defined in the list. Authentication is NOT required for users to access these domains and/or URLs.
Proxy Server	System supports up to 10 external proxy servers.
DDNS	System supports dynamic DNS (DDNS) feature.
Client Mobility	System supports IP plug-and-play(PNP).
VPN	There are 3 types of VPN connection supported in the system, including Local VPN, Remote VPN, and Site-to-Site VPN. For the local VPN, an IPSec tunnel can be established between the system and the client located at the LAN side. For the Remote VPN, a PPTP tunnel can be established between the system and the remote user over the Internet. For the Site-to-Site VPN, an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.

3. Click the ***Proxy Server*** from the menu and the **External Proxy Servers** page will appear.



4. Add the ISP's proxy Server IP and Port into ***External Proxy Servers*** Setting.

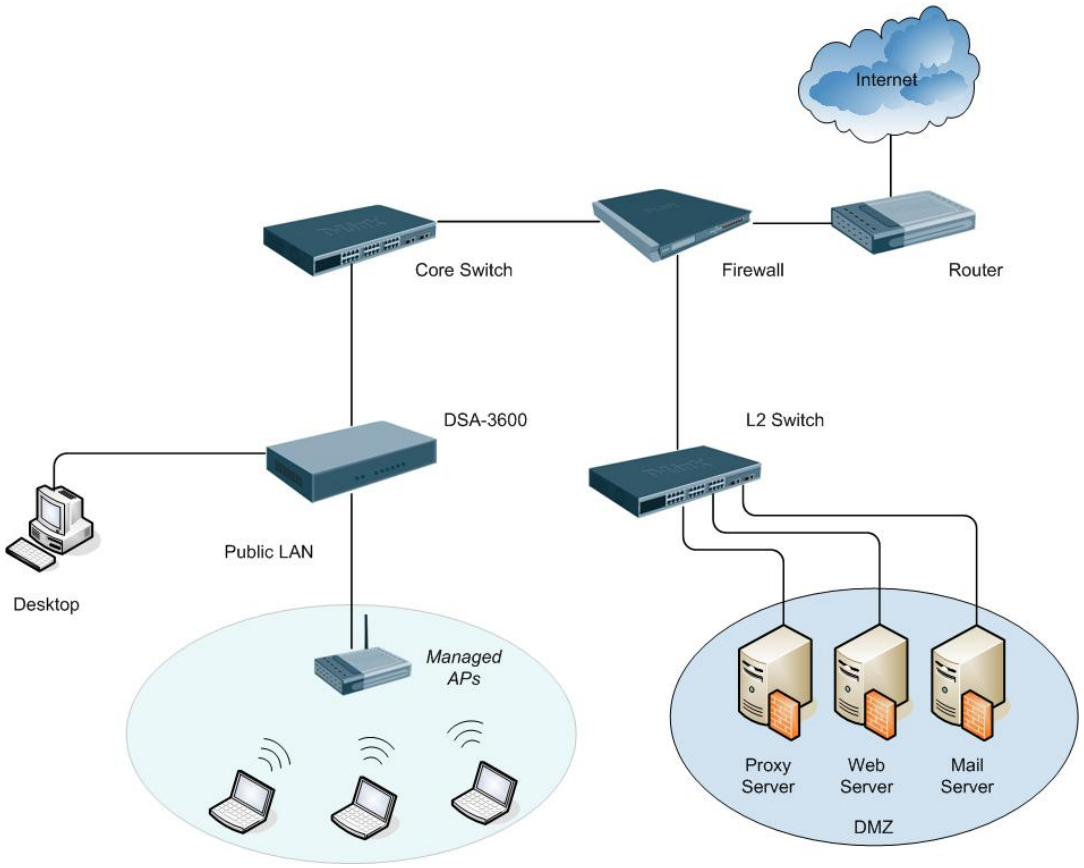
5. Enable ***Built-in Proxy Server*** in ***Redirect Outgoing Proxy Traffic to Built-in Proxy Server*** Setting.



6. Click ***Apply*** to save the settings***.***

For Enterprise

Enterprises usually isolate their intranet and internet using a more sophisticated network infrastructure. Many enterprises have their own proxy server which is usually located at the intranet or DMZ under firewall protection.



In enterprises, network managers or MIS staff often request their users to enable proxy setting in their browsers to reduce Internet access loading, therefore some proxy configuration settings in the Gateway will be necessary.

Caution：Some enterprises automatically redirect packets to proxy server by using core switch or Layer 7 devices. Using this method, the clients will not need to enable their browsers' proxy settings, and administrators will not need to set any proxy configuration in the Gateway.

Please follow the steps to complete the proxy configuration：

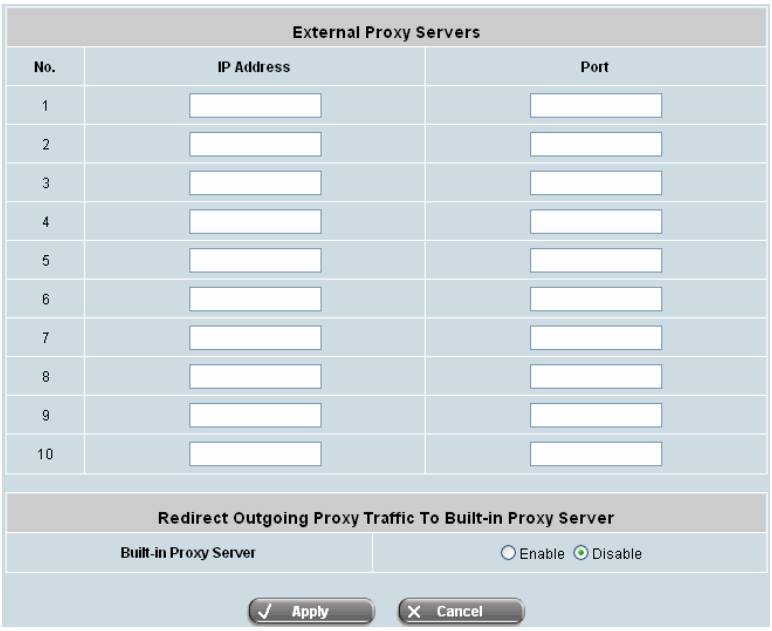
- ## Gateway setting

1. Login Gateway by using "***admin***".

2. Click ***Network*** from main menu and the **Network Configuration** page will appear.

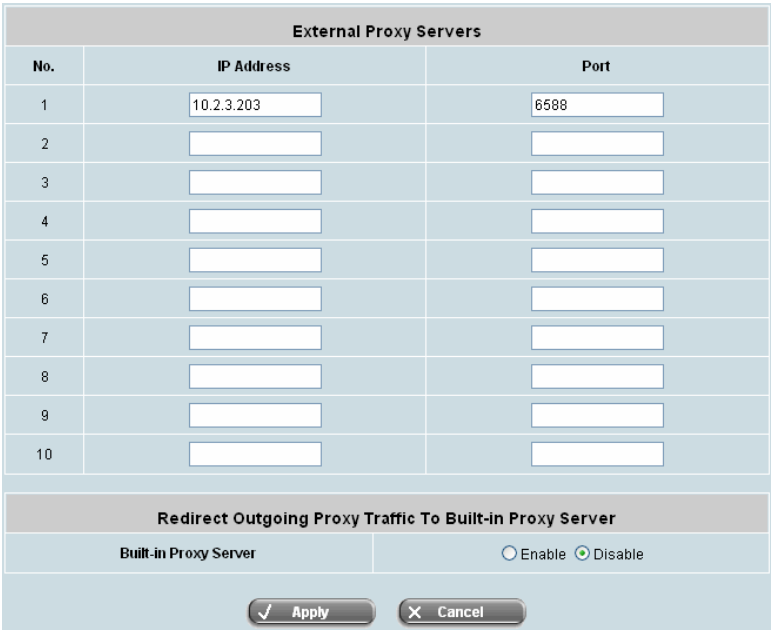
Network Configuration	
NAT	The NAT function supports 3 types of network address translation: DMZ(Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege	The Privilege function supports two types of privilege list based on IP address and MAC address. Devices specified in the list require NO authentication to access the network.
Monitor IP	Up to 40 IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.
Walled Garden	Up to 20 domain names/IP addresses can be defined in the list. Authentication is NOT required for users to access these domains and/or URLs.
Proxy Server	System supports up to 10 external proxy servers.
DDNS	System supports dynamic DNS (DDNS) feature.
Client Mobility	System supports IP plug-and-play(PNP).
VPN	There are 3 types of VPN connection supported in the system, including Local VPN, Remote VPN, and Site-to-Site VPN. For the local VPN, an IPSec tunnel can be established between the system and the client located at the LAN side. For the Remote VPN, a PPTP tunnel can be established between the system and the remote user over the Internet. For the Site-to-Site VPN, an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.

3. Click the ***Proxy Server*** from left menu and the ***External Proxy Servers page*** will appear.



4. Add your proxy Server IP and Port into ***External Proxy Servers*** Setting.

5. Disable ***Built-in Proxy Server*** in ***Redirect Outgoing Proxy Traffic to Built-in Proxy Server*** Setting.



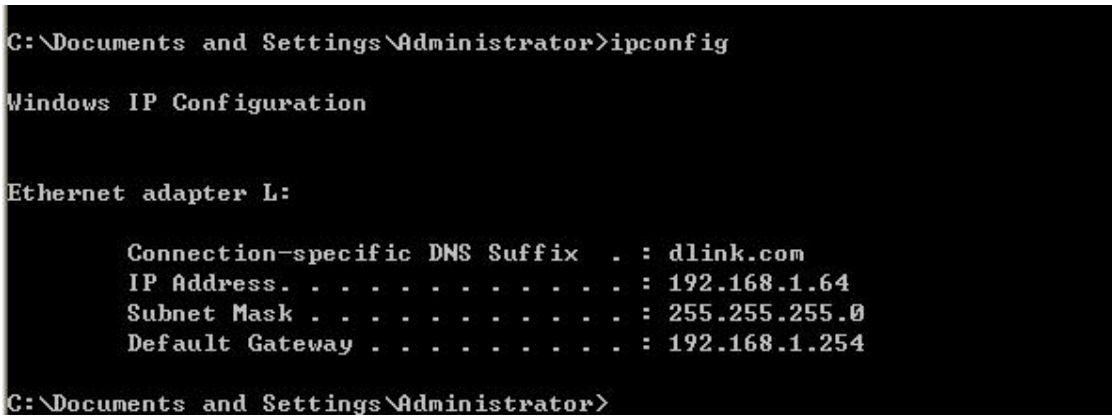
6. Click ***Apply*** to save the settings***.***

Warning：If your proxy server is disabled, it will result in abnormal user authentication. When users open their browser, the login page will not appear because the proxy server is down. Please ensure your proxy server is always available.

- **Client setting**

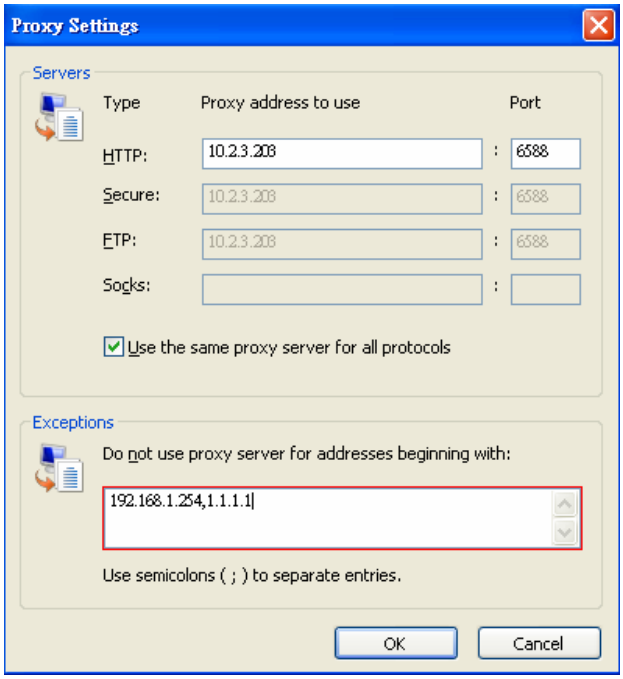
Adding a default gateway IP address into proxy exception information is a necessity for clients so that the user login successful page can show up normally.

1. Use the command "***ipconfig***" to obtain the Default Gateway IP Address.

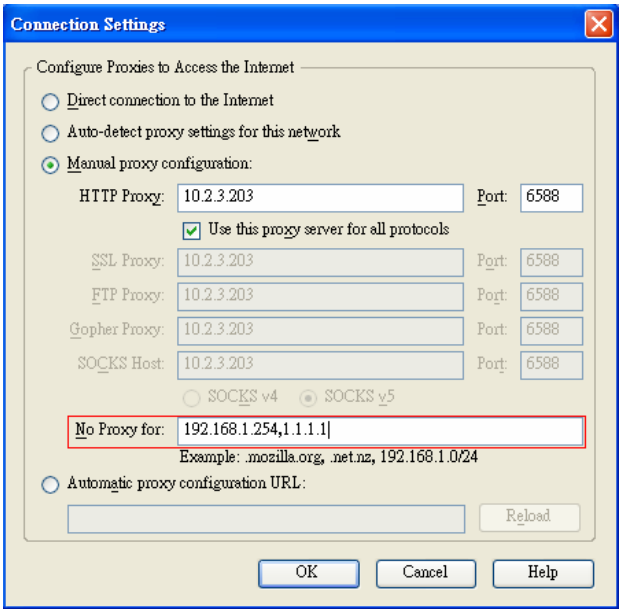


2. Open the browser to add the ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into the proxy exception information.

- For Internet Explorer



- For Mozilla Firefox



Appendix D. Certificate Settings for IE6 and IE7

▪ Certificate setting for the company with Certificate Authority

➢ Background information

Any website or high-value Web Applications will require a client to access their websites via Secure Sockets Layer (SSL). The browser will automatically ask for a public SSL certificate from the website and check if it is valid. The public SSL Certificate consists of the public key and identity information which can be signed by any established certificate authority (e.g. VeriSign). The certificate authority guarantees that the public key belongs to the named entity. Usually, website's security certificate may encounter problem only if the security certificate presented to the browser has not been signed by any certificate authority which can be trusted.
As long as the SSL function is enabled in the DSA-3600, there must be a public SSL certificate signed by an established certificate authority. To avoid the error message in the browser, a company should have its own Certificate Authority (CA). The IT department must therefore install the SSL certificate for each normal user when deploying the DSA-3600.

➢ Secure Certificate setting for both IE6 and IE7

For the company with its own Certificate Authority (CA), the certificate of the company should be trusted by all his employees' computers, and the certificate should be delivered through a trusted media. For example, the MIS staff should install the CA certificate in each computer. The company CA will issue a certificate for the DSA-3600 and export it to the DSA-3600.

Note: If the DSA-3600 is installed in a company, the administrator can create a certificate using a software instead of purchasing a public trusted certificate.

▪ Certificate setting for the company without Certificate Authority

For a company that does not have it own Certificate Authority (CA), the administrators should first apply for a trusted certificate, or create one using a certificate software. Second, the administrators should use some trusted media to install this certificate (as trusted CA) in each employee's computer, and in the meantime export this certificate to the DSA-3600.

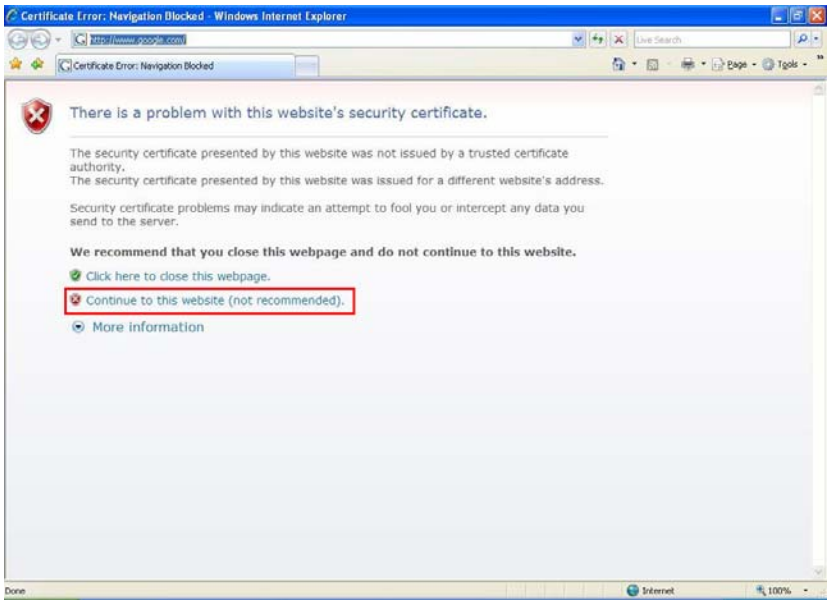
In some circumstance, the company without Certificate Authority may follow the steps stated below to avoid error message. When in the LAN environment of the office instead of a wireless environment, administrators may already have recognized certificates in the system which the CA must be verified as secured.

▪ Certificate setting for Internet Explorer 7

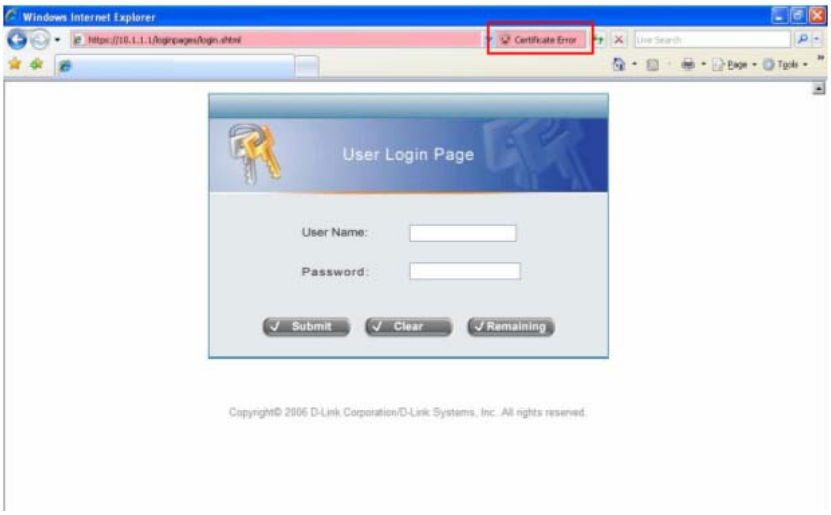
For IE7, certificate issues caused by certificate publisher not being trusted by IE7, the following steps may be taken to provide a workaround or to bypass the issue.

1. Open the IE7 browser, and you will be redirected to the default login page. If the certificate is not trusted, the following page will appear.

Click ***"Continue to this website"***.



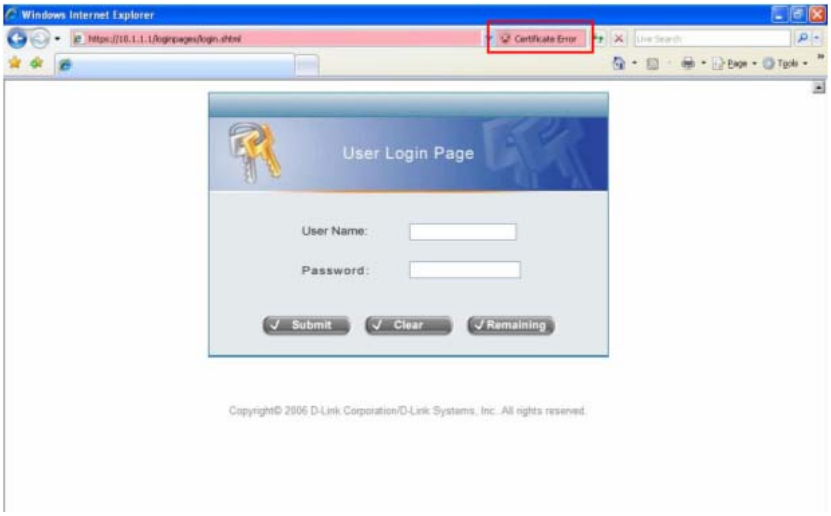
2. The default User Login Page will appear and the users can then login normally.



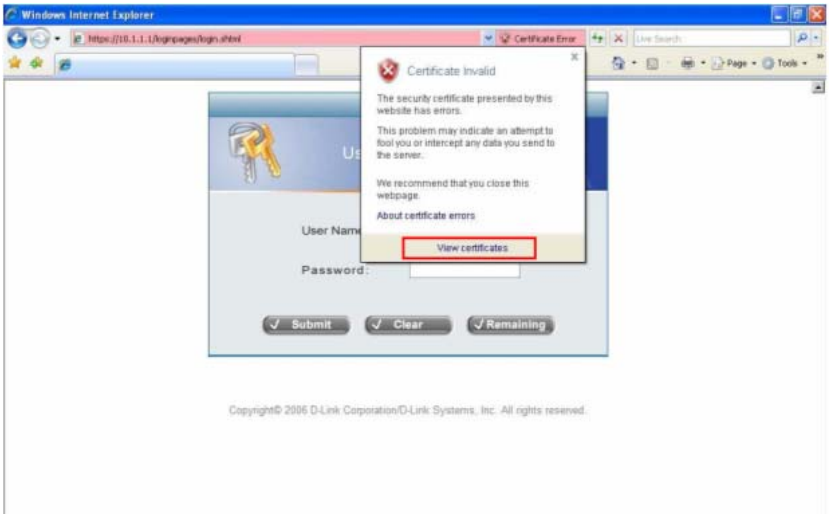
Appendix D. Certificate Settings for IE6 and IE7

For installing a trusted certificate to solve the IE7 certificate issue, please follow the instructions stated below.

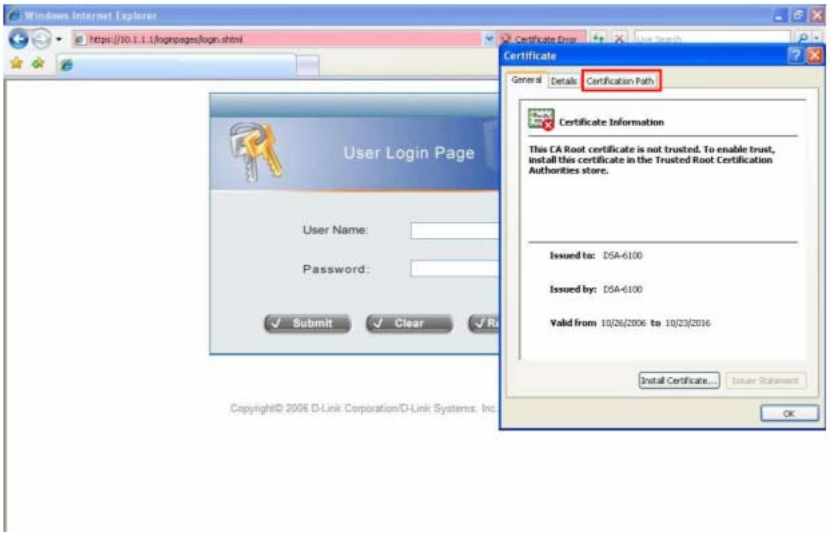
1. When the User Login page appears, click ***"Certificate Error"*** at the top.



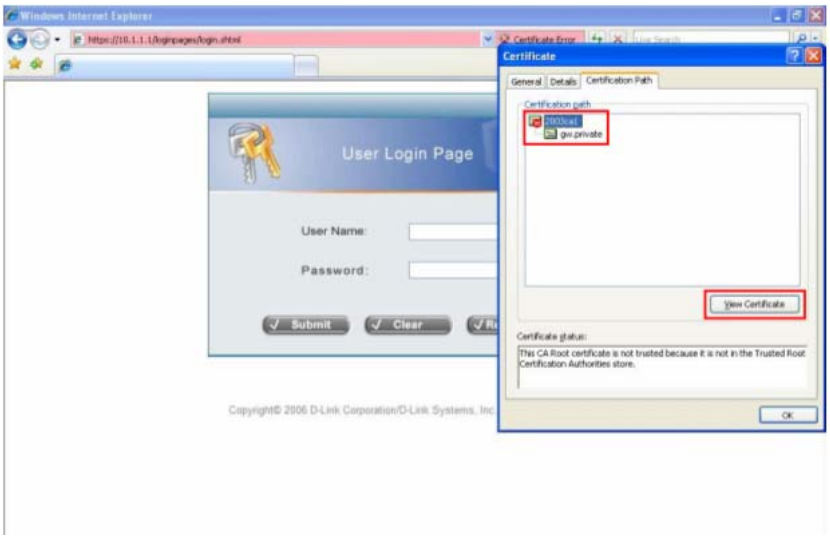
2. Click ***"View Certificate"***.



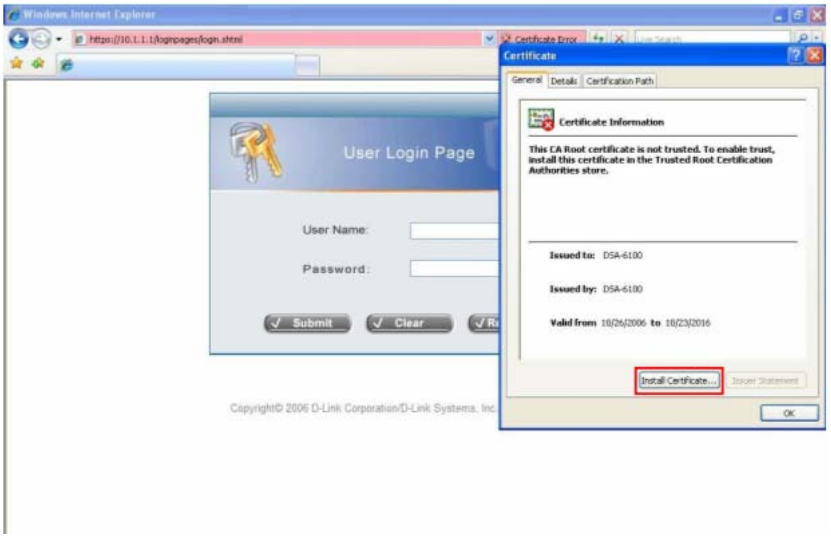
3. Click ***"Certification path"***.



4. Select root certification, then click ***"View Certificate"***.

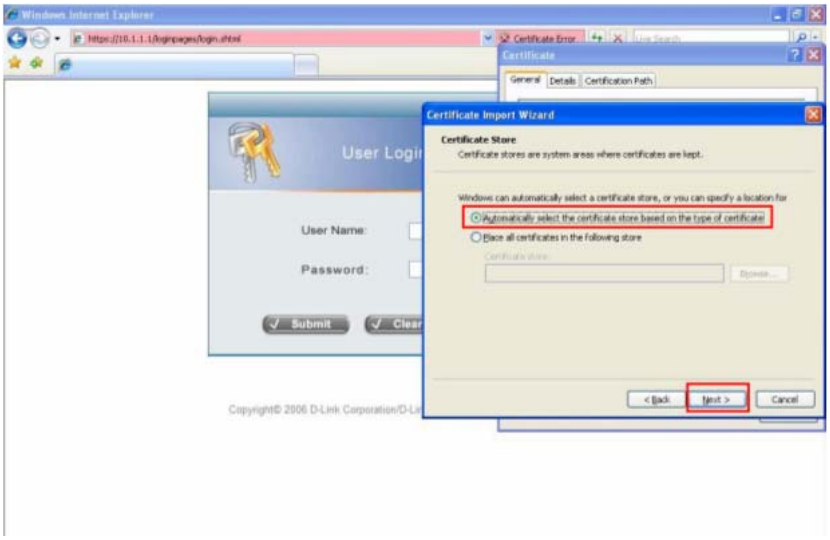


5. Click ***"Install Certificate"***.

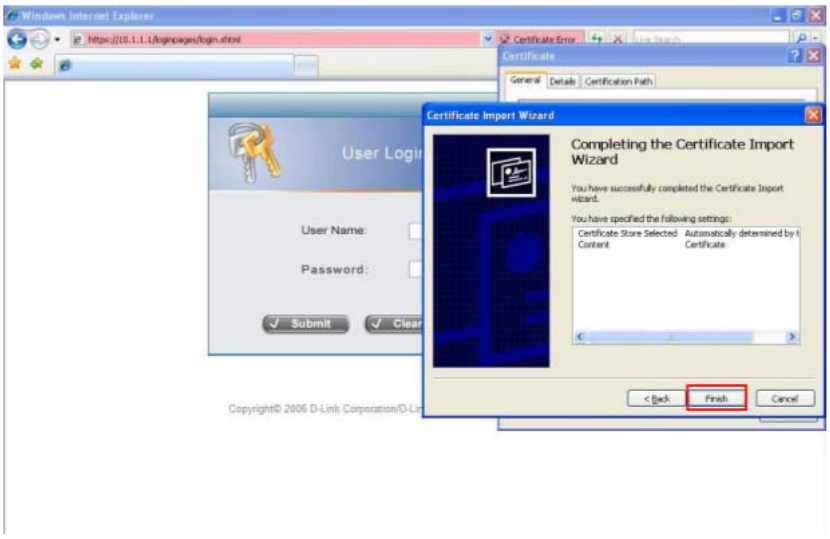


6. Click ***"Next"***.

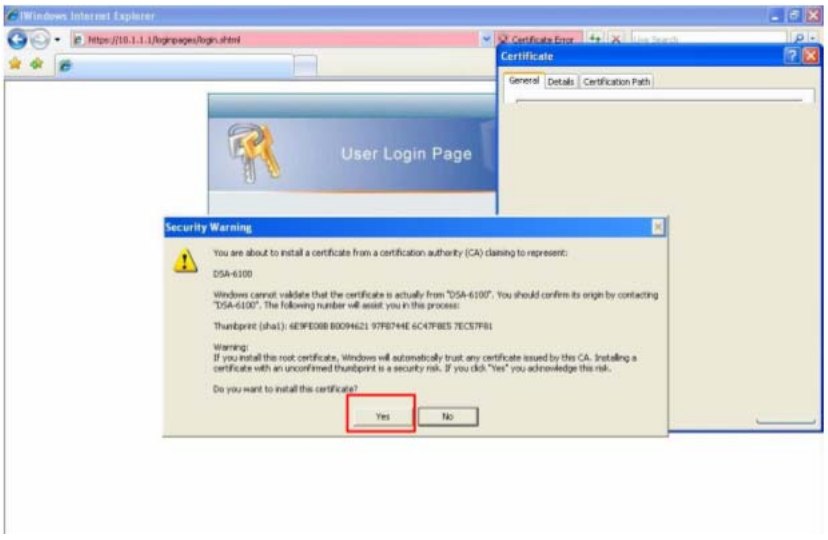
7. Select ***"Automatically select the certificate store based on the type of certificate"***, then click ***"Next"***.



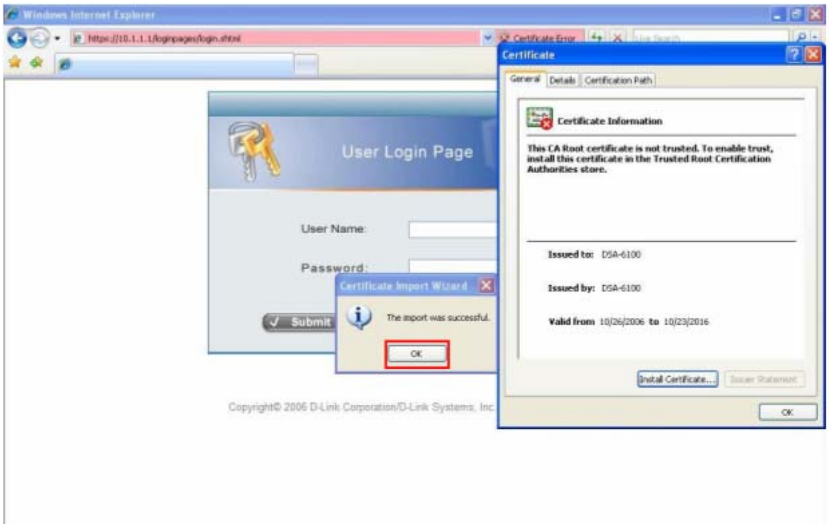
8. Click ***"Finish"***.



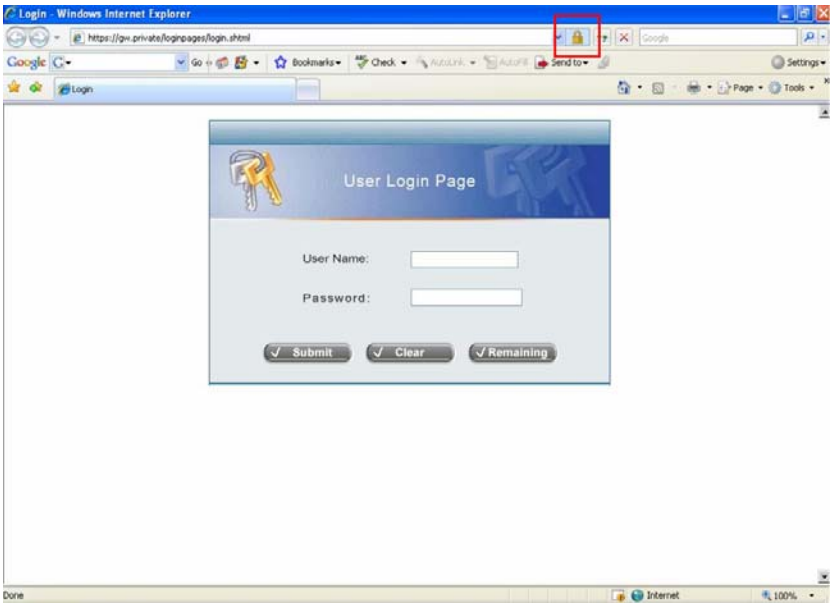
9. Click ***"Yes"***.



10. Click ***"OK"***.



11. Launch a new IE7 browser. The certificate is now trusted via IE7 according to the key symbol shown at top next to the address field.

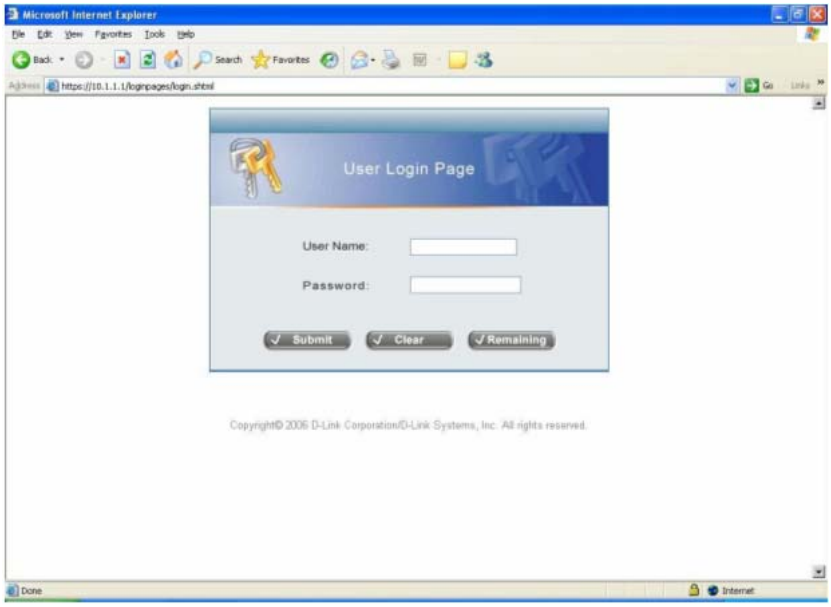


▪ Certificate setting for Internet Explorer 6

For issues relating to IE6 certificate error, the following information provides the step to take when the certificate publisher is not trusted by IE6.

1. Open an IE6 browser, the Security Alert message will be appeared if the certificate is not trusted. Click ***"Yes"*** to proceed.

2. The User Login Page will appear.

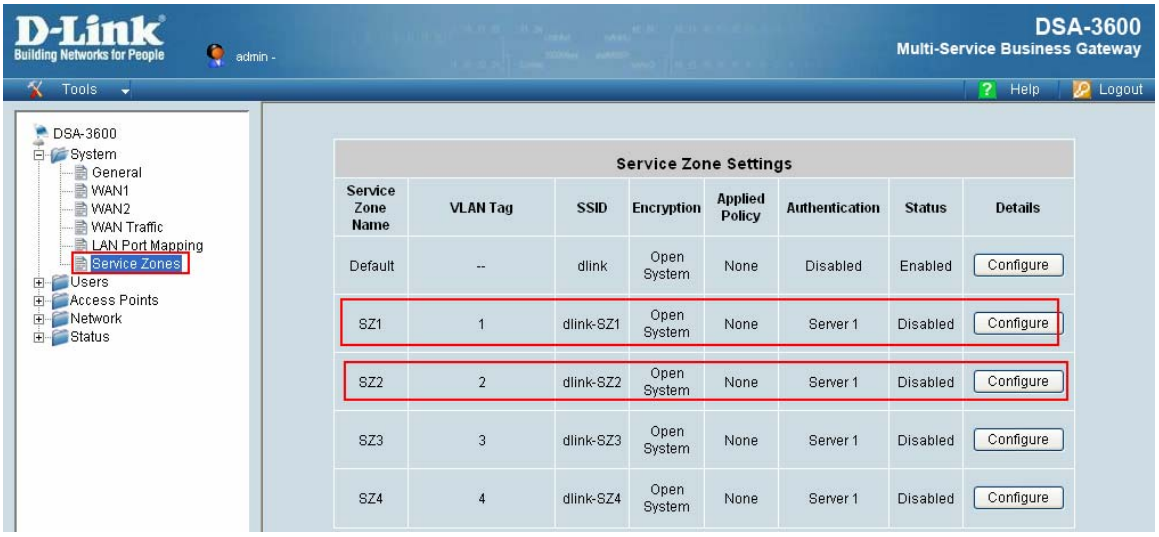


3. The user can now login normally.

Appendix E. Service Zones – Deployment Examples

▪ Typical Application Scenario: Employees vs. Guests

Typical service zone settings will separate users groups into **Employee** and **Guests** for the purpose of different authentication level.

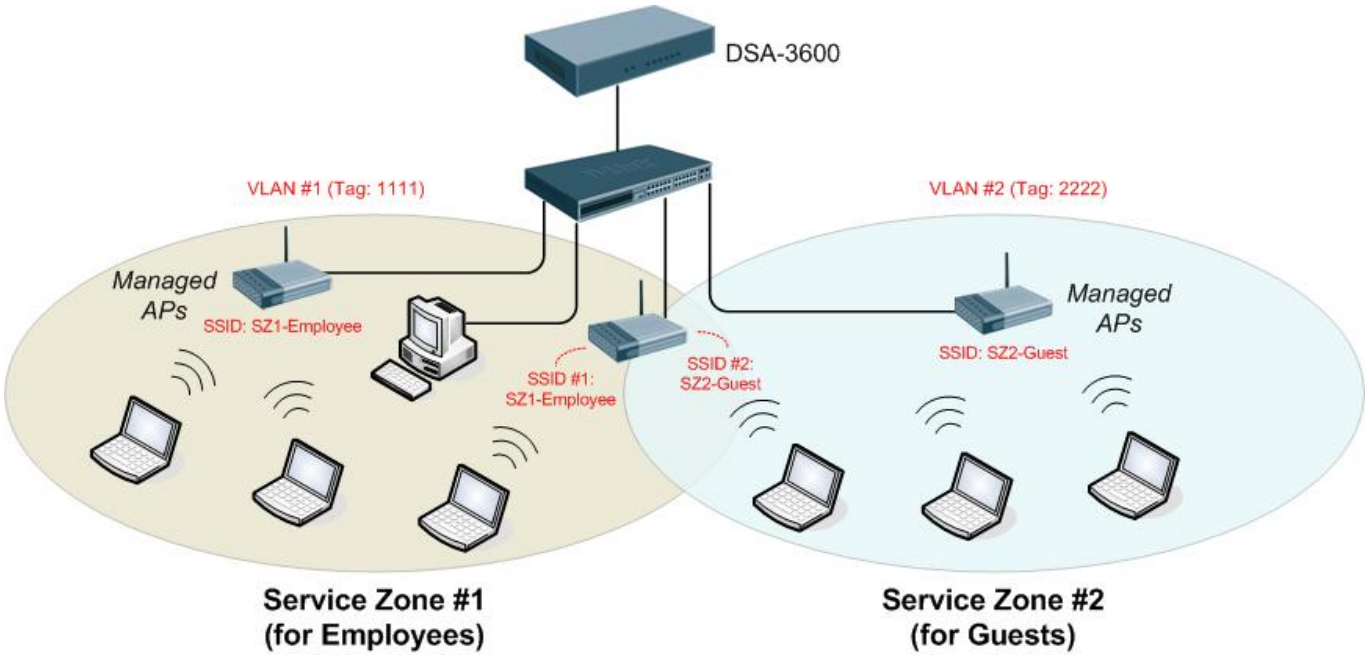


Service Zone Settings

Service Zone Name	VLAN Tag	SSID	Encryption	Applied Policy	Authentication	Status	Details
Default	--	dlink	Open System	None	Disabled	Enabled	Configure
SZ1	1	dlink-SZ1	Open System	None	Server 1	Disabled	Configure
SZ2	2	dlink-SZ2	Open System	None	Server 1	Disabled	Configure
SZ3	3	dlink-SZ3	Open System	None	Server 1	Disabled	Configure
SZ4	4	dlink-SZ4	Open System	None	Server 1	Disabled	Configure

▪ Application Network Diagram :

As shown in the diagram, assign service zone 1 to Employees and service zone 2 to Guest.



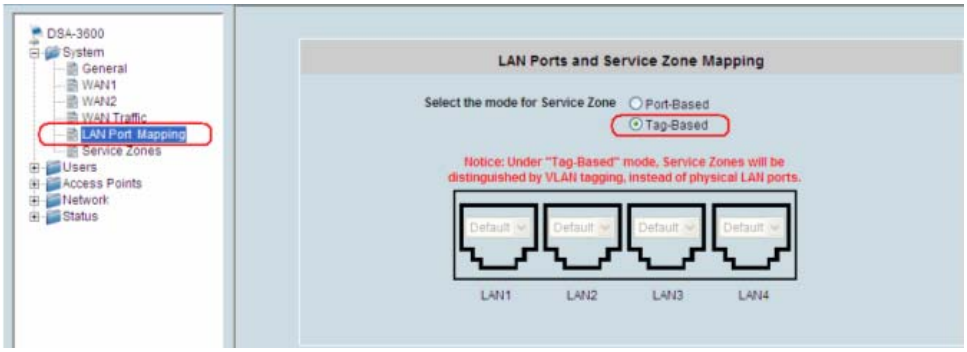
- **Requirements for the Application Scenario :**

1. Regardless of the location in the office, all users should be divided into two groups (**Employee** and **Guest**) for the purpose of authentication differences.
2. Each service zone must setup its own **SSID** to let users to access the wireless network using the specific ID. The system will give a unique Session ID to authenticated users when they start new sessions.
3. Both groups, **Employees** and **Guests**, will be redirected to different login portal pages and will be authenticated against different authentication database.
4. Apply different access control policies to seperated groups **Employee** and **Guests**.

- **Solution and Configuration in DSA-3600**

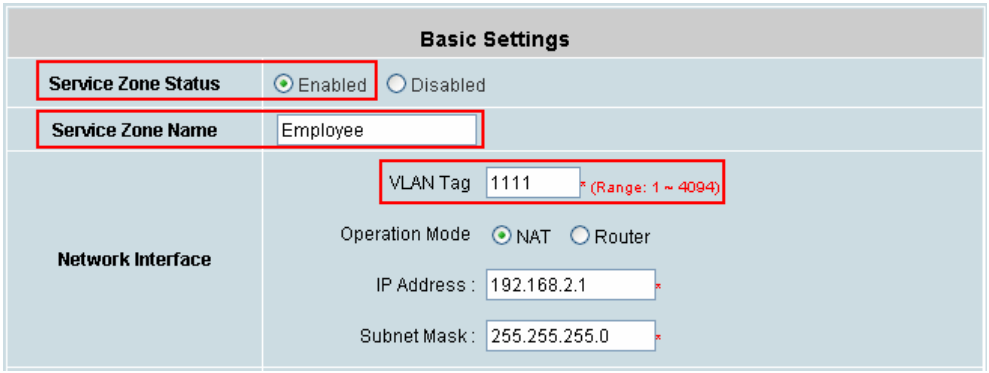
1) Configure two **service zones** to map to the two groups

Step 1: Select "**Tag-Based mode**" for all "**service zones**"

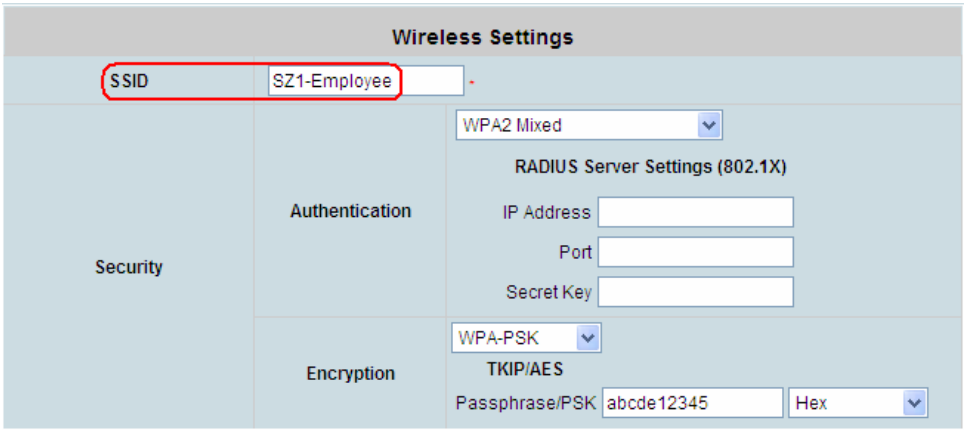


Step 2: Choose and configure the desired "**service zone**" for the specific group (e.g. Choose and configure " **SZ1**" for **Employees**)

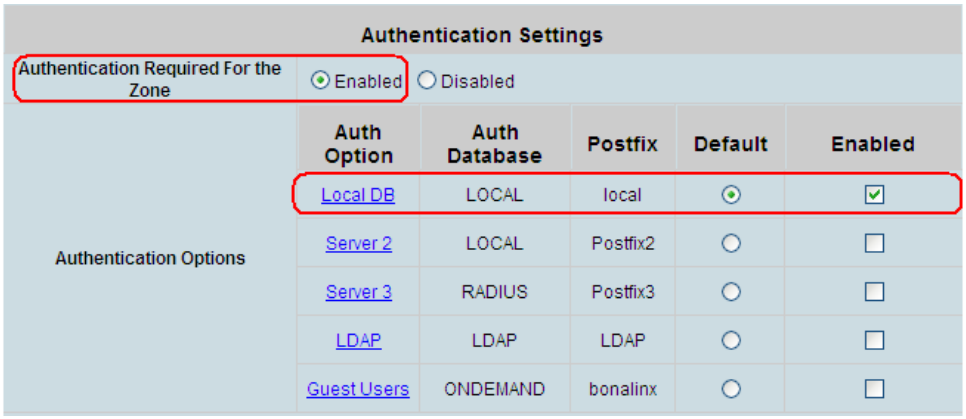
Step 3: Configure the "**service zone**" accordingly

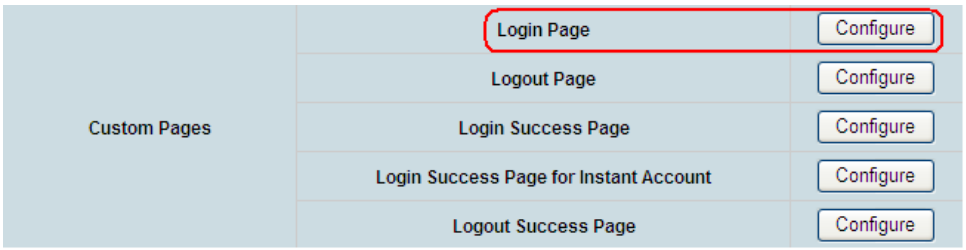


2) Configure the **SSID**

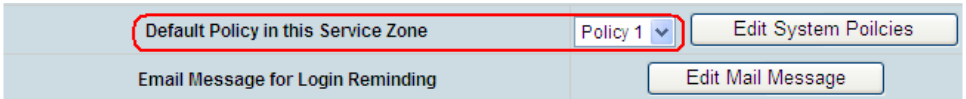


3) Choose the authentication option and configure the login page





4) Choose the appropriate policy for this "**service zone**"



- **Finished Configuration – Service Zone Settings:**

  Once the settings of two service zones are completed, the configured result will be displayed on screen in the **Service Zone Settings**. The name of the service zone and the enabled status should appear in the display.

Service Zone Settings

Service Zone Name	VLAN Tag	SSID	Encryption	Applied Policy	Authentication	Status	Details
Default	--	dlink	Open System	Policy 1	Local DB	Enabled	Configure
Employee	1111	SZ1-Employee	WPA2 Mixed	Policy 1	Local DB	Enabled	Configure
Guest	2222	SZ2-Guest	Shared Key	Policy 2	On-demand User	Enabled	Configure
SZ3	3	dlink	Open System	Policy 1	Local DB	Enabled	Configure
SZ4	4	dlink	Open System	Policy 1	Local DB	Disabled	Configure

Appendix F. Deploying DSA-3600 Using DWL-2100AP

▪ Wireless Features of DWL-2100AP

Wireless security can be addressed using the *DWL-2100AP* access point with **WPA** (Wi-Fi Protected Access) and **802.1X authentication** to provide a higher level of security for data communication amongst wireless clients. The *DWL-2100AP* is fully compatible with industry standards such as **WEP**, and can support **multiple SSIDs**, each of which can be mapped to a specific **Service Zone** (see Section 4.1.6 Service Zone) defined in the *DSA-3600*. Using the **Service Zone** based architecture, administrators can assign wireless security settings to different **SSIDs** according to the **Service Zone** profiles.

The *DWL-2100AP* can be deployed in the **Service Zones** and centrally managed via the *DSA-3600*. The **Service Zone** and **Centralized AP Management** provide an ideal solution using the *DSA-3600* together with *DWL-2100AP* for quick creation and extension of wireless local area network (WLAN) in offices and other workplaces, including hotspots.

▪ Best Practice for Wireless Settings of DWL-2100AP

To use multiple **SSIDs** in *DWL-2100AP*, creation and configuration of different **Service Zones** will be needed.

▪ Two Types of SSIDs:

The *DWL-2100AP* has two types of **SSIDs** :

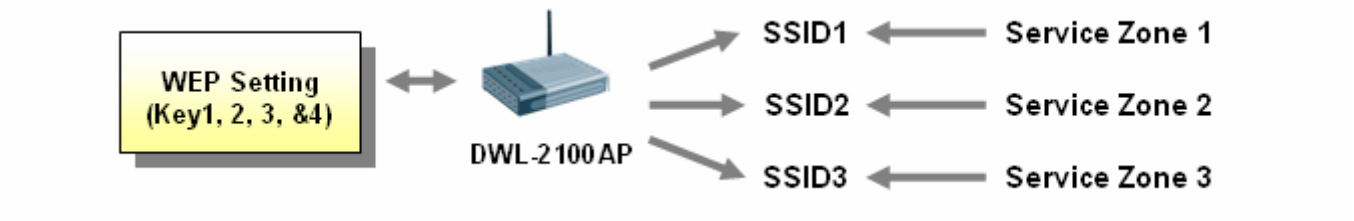
I. **Primary** (Only one for each *DWL-2100AP*) – Support every mode (**Open System**, **Shared Key**, **Open System/Shared Key**, **WPA-EAP**, **WPA2-EAP**, **WPA-Auto-EAP**, **WPA-PSK**, **WPA2-PSK**, and **WPA-Auto-PSK**) for security.

II. **Guest** (Up to 7 for each *DWL-2100AP*) – Does not support "**Open System/Shared Key**" mode for security

Caution: If an existing **SSID** is already using **Guest** type, the wireless security of a **Service Zone** which is associated with this **SSID** cannot be set in the **Open System or Shared Key** mode in *DSA-3600*.

- **Single Set of WEP Keys:**

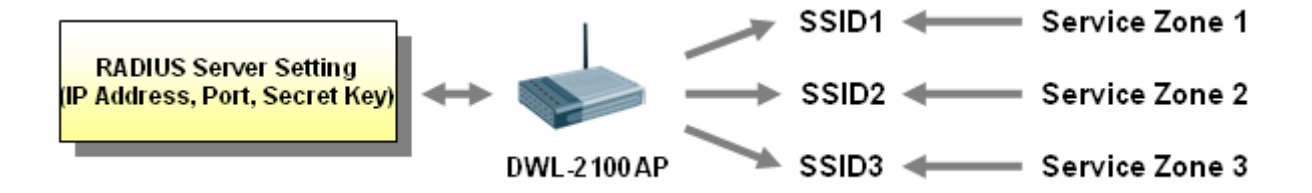
  All **SSIDs** which belong to the same *DWL-2100AP* share the same set of **WEP** Keys (Key1 ~ Key4):



> **Caution:** If two or more **SSIDs** belong to the same *DWL-2100AP* and the wireless security of the associated **Service Zones** is set in the "**Shared Key"** mode in the *DSA-3600*, those **SSIDs** cannot be mapped to the **Service Zones** that have different sets of **WEP** Keys in the *DSA-3600*.

- **Single Set of RADIUS Server Setting:**

  Only one set of **RADIUS Server** setting is provided in *DWL-2100AP*.



> **Caution:** If two or more **SSIDs** belong to the same *DWL-2100AP*, and the wireless security of the associated **Service Zones** is set in the modes which use **RADIUS**, those **SSIDs** cannot be mapped to the **Service Zones** that have different sets of **RADIUS** Server settings in the *DSA-3600.*

- **Availability of WEP Keys:**

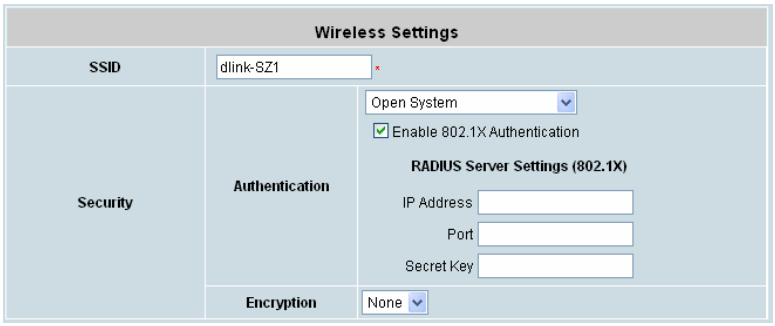
  When an **SSID** of the *DWL-2100AP* is set in "**WPA**" related modes (such as **WPA-EAP**, **WPA2-EAP**, **WPA-Auto-EAP**, **WPA-PSK**, **WPA2-PSK**, and **WPA-Auto-PSK**), it will disable the availability of **WEP** Key2 and Key3 for another **SSID**, which is set in "**Shared Key**" modes (**Shared Key or Open System/Shared Key**), in the same *DWL-2100AP*.

> **Caution**: If two or more **SSIDs** belong to the same *DWL-2100AP* and the wireless security of one associated **Service Zone** is set in the modes of "**WPA**", "**WPA2**" or "**WPA Mixed**", those **SSIDs** that are in the modes of "**Shared Key**" and "**Open System or Shared Key**" cannot use **WEP** Key2 and Key3 in the *DSA-3600.*

- **Availability of 802.1x Authentication :**

When an **SSID** (**Primary type**) of the *DWL-2100AP* is set in the mode of "**Open System**" or "**Open System/Shared Key**", it will not support **802.1x authentication**.

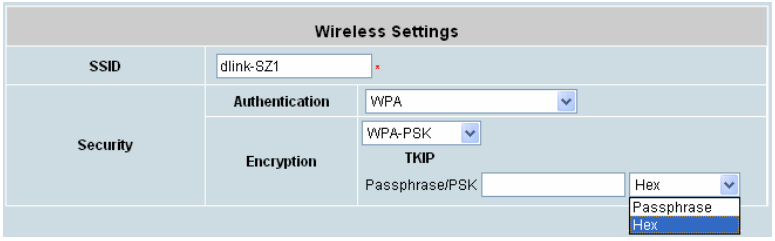
Caution: 802.1x Authentication should NOT be enabled in *DSA-3600* if any *DWL-2100AP* exists in the **Service Zone** and the associated **SSID** is in the mode of "**Open System**" or "**Open System/Shared Key**".



- **Availability of WPA Pre-Shared Keys (WPA-PSK) :**

When an **SSID** of the *DWL-2100AP* is set in the mode of **WPA-PSK**, **WPA2-PSK**, and **WPA-Auto-PSK** in *DWL-2100AP*, "**Passphrase**" is the only available Key type for Pre-Shared keys (**PSK**). In addition, the length of "**Passphrase**" for the **SSID** of Guest type is 8 to 34 characters.

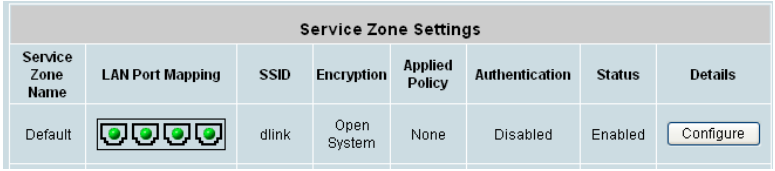
Caution: The "**HEX**" (the other Key type) should NOT be enabled in *DSA-3600* if any *DWL-2100AP* exists in the **Service Zone** and the associated **SSID** is in the mode of **WPA-PSK**, **WPA2-PSK** or **WPA-Auto-PSK**. Also, administrators will have to ensure the length of "**Passphrase**" does not exceed 34 characters and not shorter than 8 characters in *DSA-3600*.



- **Availability of Super G (108Mbp) mode :**

When multiple **SSIDs** of the *DWL-2100AP* are enabled, the "**Super G mode**" will not be available at the same time.

Caution: Administrators have to ensure that when **Service Zones** of the *DSA-3600* are set in "**Tag-based mode**", "**Super G mode**" of the *DWL-2100* is not enabled.



Appendix G. Network Configuration on PC

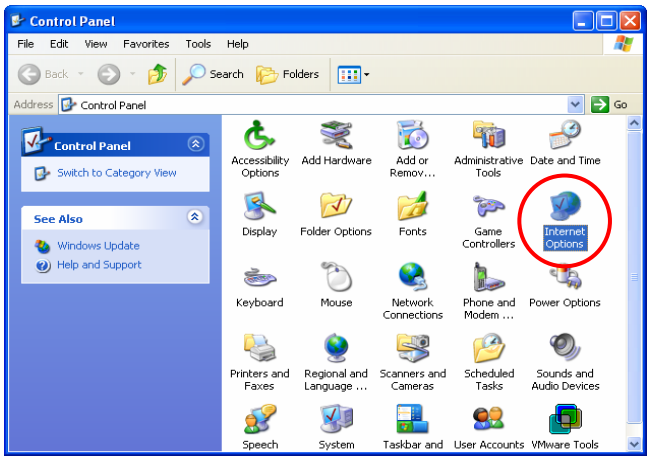
After the DSA-3600 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

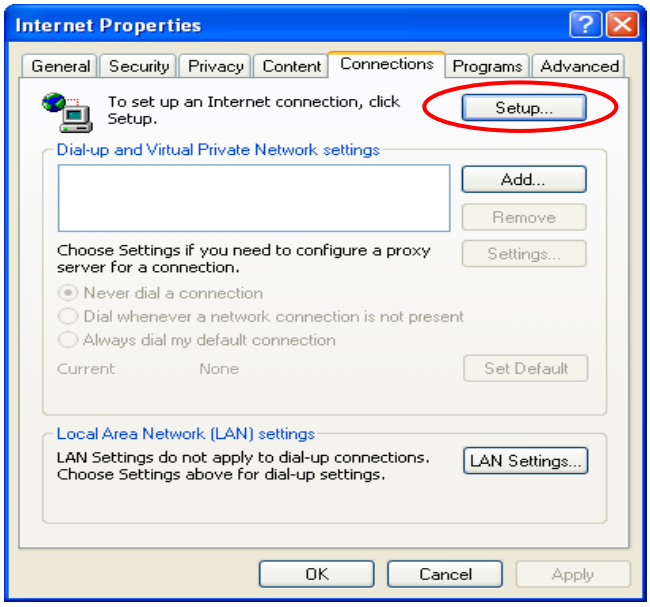
  If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

  - **Windows XP**

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

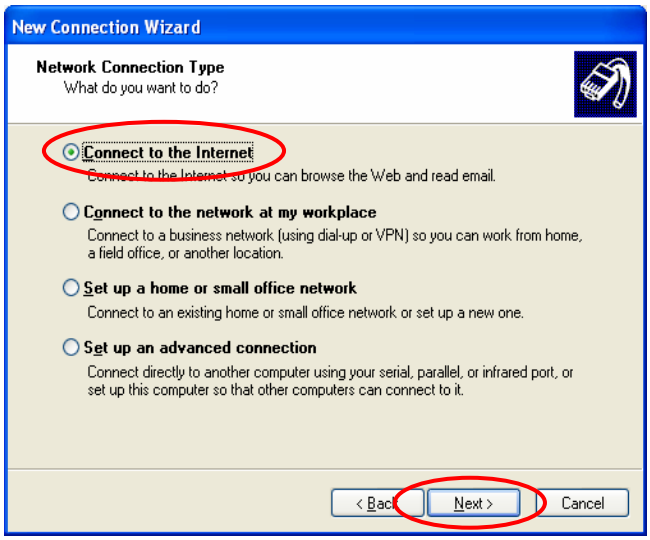


  1. Choose the **"Connections"** label, and then click ***Setup***.

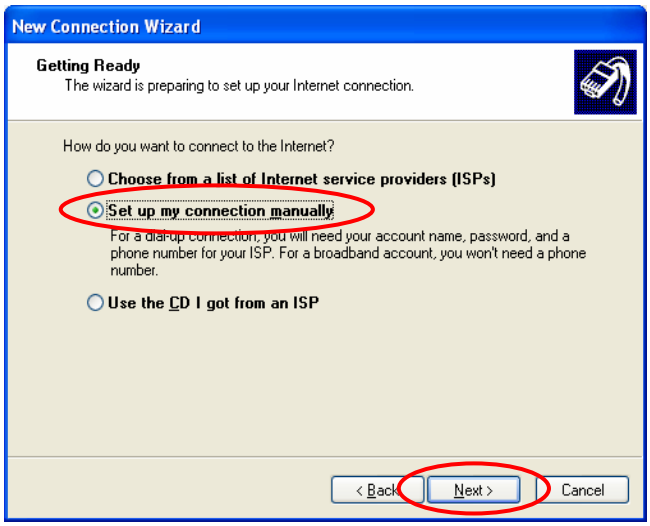


2. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.

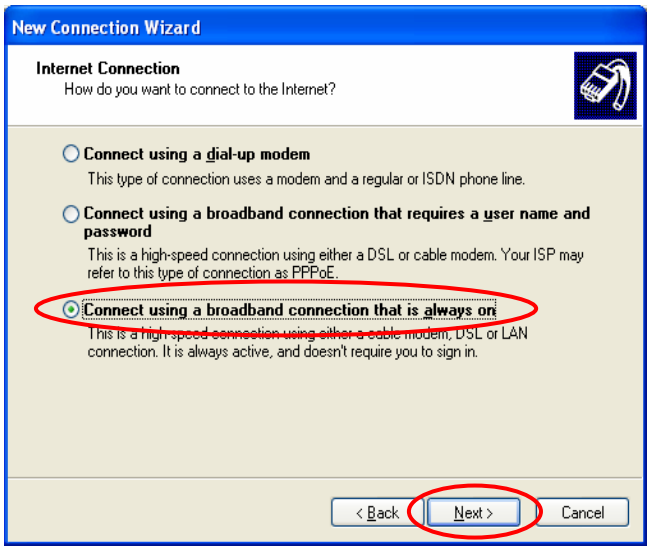
3. Choose **"Connect to the Internet"** and then click ***Next***.



4. Choose **"Set up my connection manually"** and then click ***Next***.



5. Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.



6. Finally, click ***Finish*** to exit the **Connection Wizard**. Now, you have completed the setup.

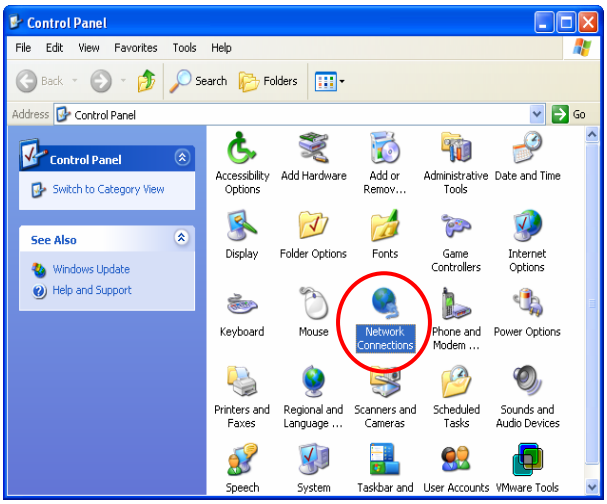
- **TCP/IP Network Setup**

  In the default configuration, the DSA-3600 will assign an appropriate IP address to a client PC which uses DHCP to obtain IP address automatically. Windows 95/98/2000/XP configures IP setup to **"Obtain an IP address automatically"** in default settings.

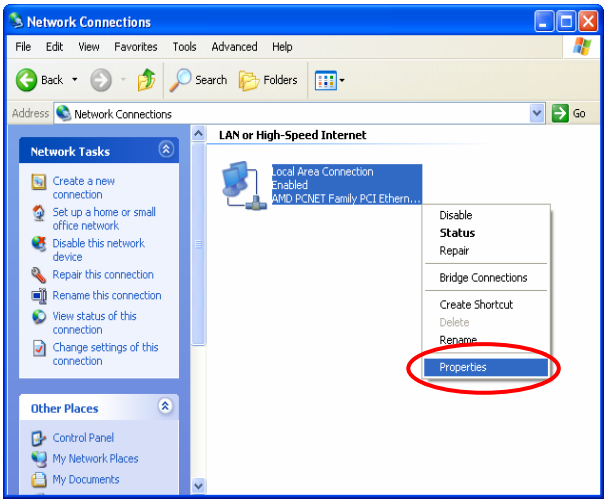
  To check the TCP/IP setup or use a static IP to connect to the DSA-3600 LAN port, please follow the following steps:

- **Check the TCP/IP Setup of Window XP**

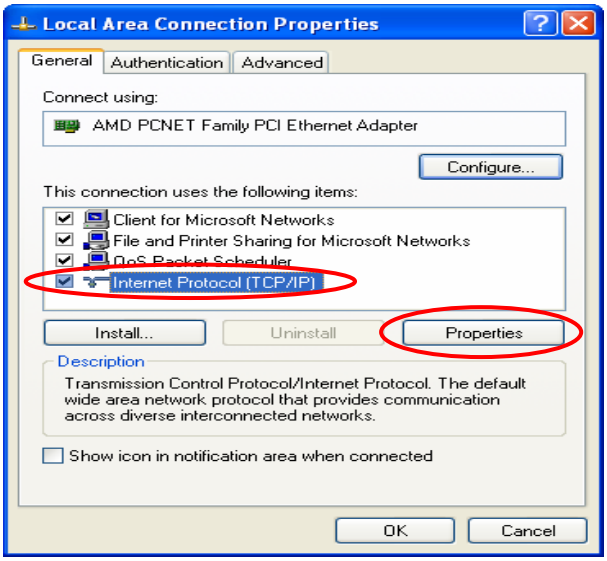
1. Select **Start > Control Panel > Network Connection**.



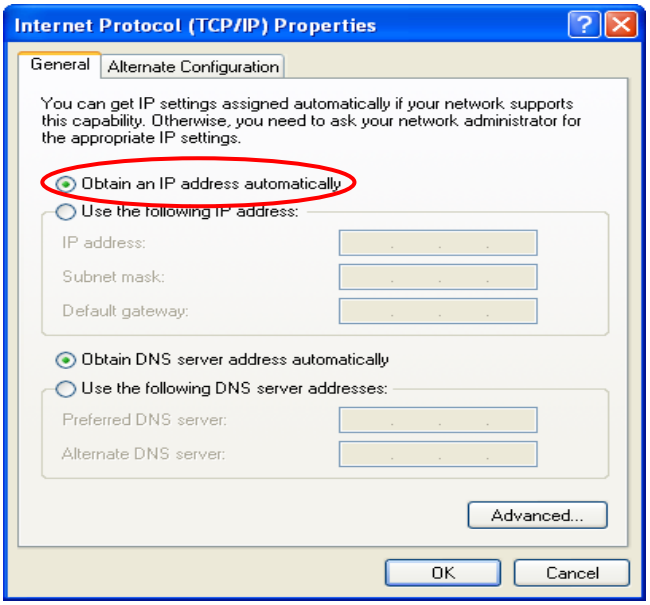
2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



3. Select **"General"** label and choose **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, you can choose to use **DHCP** or **specific IP address**, please proceed to the following steps.

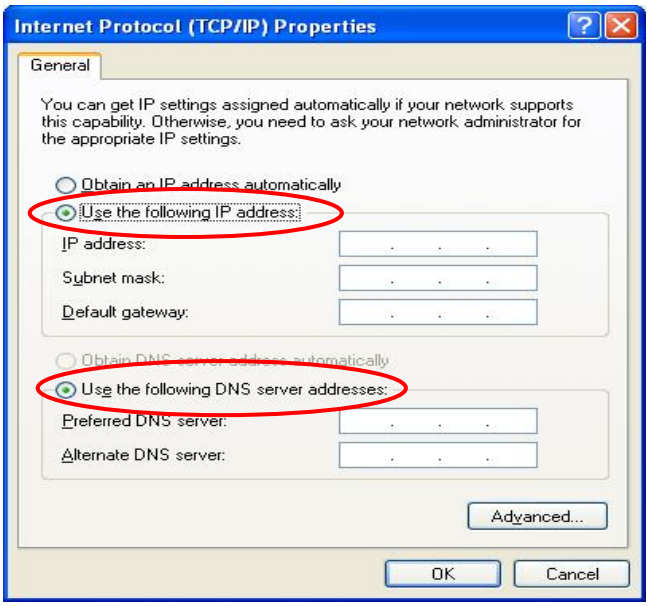


4. **Using DHCP:** To use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the DSA-3600.



5. **Using Specific IP Address:** To use specific IP address, please request from your network administrator the following information of the DSA-3600: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

   Choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"**, **"Subnet mask"** and the **"DNS address(es)"** and then click ***OK***.



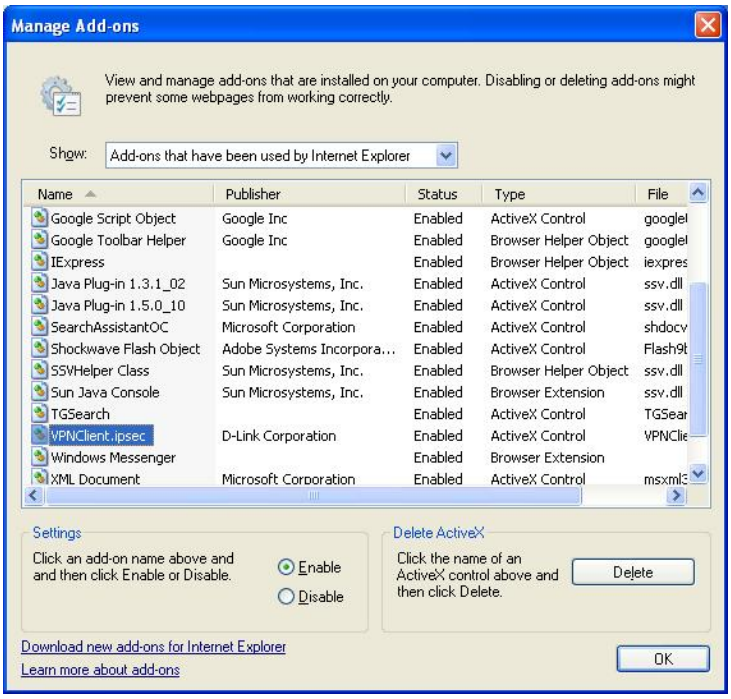
Appendix H. IPSec VPN

The DSA-3600 is equipped with IPSec VPN feature starting from release v1.00. To utilize IPSec VPN supported by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, the DSA-3600 implements IPSec VPN tunneling technology between client's windows devices and the DSA-3600 itself regardless of wired or wireless network.

By pushing down ActiveX to the client's Windows device from the DSA-3600, no extra client software is required to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is then configured automatically. At the end of this setup, a build-in IPSec VPN feature will be enabled and ready to serve once it is launched for setup. The goal of this design is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of the DSA-3600 is based on ActiveX and the built-in IPSec VPN client of Windows OS.

1. ActiveX component

The ActiveX is a software component running inside Internet Explorer. The ActiveX component can be checked by the following windows.



From Windows Internet Explorer, click "Manage add-ons" button inside "Programs" page under "Tools" to show the add-ons programs list. You can see VPNClient.ipsec is enabled.

During the first login to the DSA-3600, Internet Explorer will ask user to download the ActiveX component of IPSec VPN. This ActiveX component once downloaded will be running parallel with the “Login Success” page. The ActiveX component helps to setup the IPSec VPN tunnel between client’s device and the DSA-3600. It also helps to check the validity of the IPSec VPN tunnel between them. If the connection is down, the ActiveX component will detect the broken link and recompose the IPSec tunnel. Once the IPSec VPN tunnel is built, any packet sent will be encrypted. Without connecting to the original IPSec VPN tunnel, user or client device has no alternative to gain network connection beyond this. The DSA-3600’s IPSec VPN feature is designed to solve possible data security leak between client and the controller via either wireless or wired connection without extra hardware or client software installed.

2. Limitations

The limitation on the client side due to ActiveX and Windows OS includes:

a. Internet Connection Firewall of Windows XP or Windows XP SP1 not being compatible with IPSec protocol, hence it shall be turned off to allow IPSec packets to pass through.

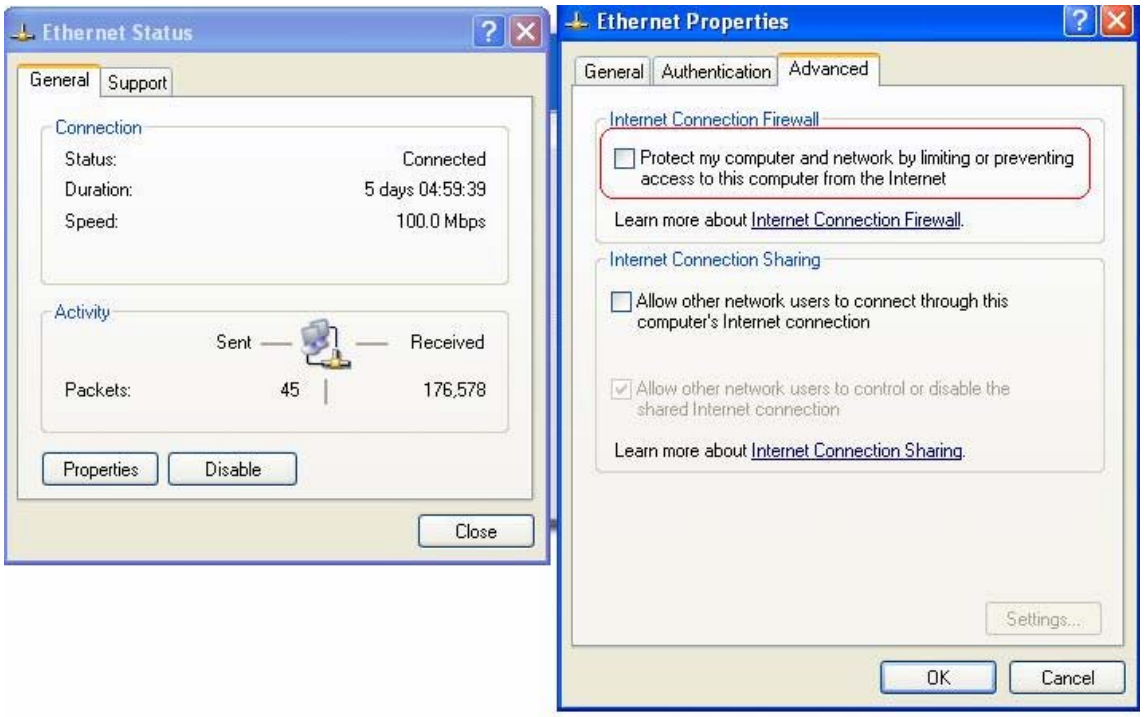
b. Without patch, ICMP (Ping) and PORT command of FTP cannot work in Windows XP SP2.

c. The Forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX, which may result in IPSec tunnel not being able to work properly at client’s device. A reboot of client’s device is needed to clear the IPSec tunnel.

d. The crash of Windows Internet Explorer may cause the same result.

3. Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPSec. Internet Connection Firewall will drop packets from tunneling of IPSec VPN.



Suggestion: *Please* ***TURN OFF*** *Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.*

4. ICMP and Active Mode FTP

On Windows XP SP2 that is without patch KB889527, ICMP packets will be dropped from IPSec tunnel. This issue can be fixed by upgrading patch KB889527. Before enabling IPSec VPN function on client device, please access the patch from Microsoft's web at: http://support.microsoft.com/default.aspx?scid=kb;en-us;889527. This patch also fixes issues of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2.

Suggestion: *Please UPDATE client's Windows XP SP2 with patch KB889527.*

5. The Termination of ActiveX

The ActiveX component for IPSec VPN is running parallel with the “Login Success” web page. Unless user decides to close the session and to disconnect with NAC DSA-3600, the following conditions or behaviors of user’s browser can be avoided in order to maintain the built IPSec VPN tunnel always alive.

Reasons why Internet Explorer may cause ActiveX to stop unexpectedly are as follows:

a. The crash of Internet Explorer on running ActiveX

Suggestion: *Please reboot client’s computer once Windows service is resumed. Go through the login process again.*

b. Terminate the Internet Explorer Task from Windows Task Manager

Suggestion: *Do not terminate this VPN task of Internet Explorer.*

c. There are some cases of Windows messages by which DSA-3600 will hint current user to:

(1) Close the Windows Internet Explorer,

(2) Click “logout” button on “login success” page,

(3) Click “back” or “refresh” of the same Internet Explorer,

(4) Enter new URL in the same Internet Explorer,

(5) Open a URL from the other application (e.g. e-mail of Outlook) that occupies this existing Internet Explorer.

All these will cause the termination of IPSec VPN tunneling if the user chooses to click “Yes”. The user has to log in again to regain the network access.

Suggestion: *Click “Cancel” if you do not intend to stop the IPSec VPN connection yet.*

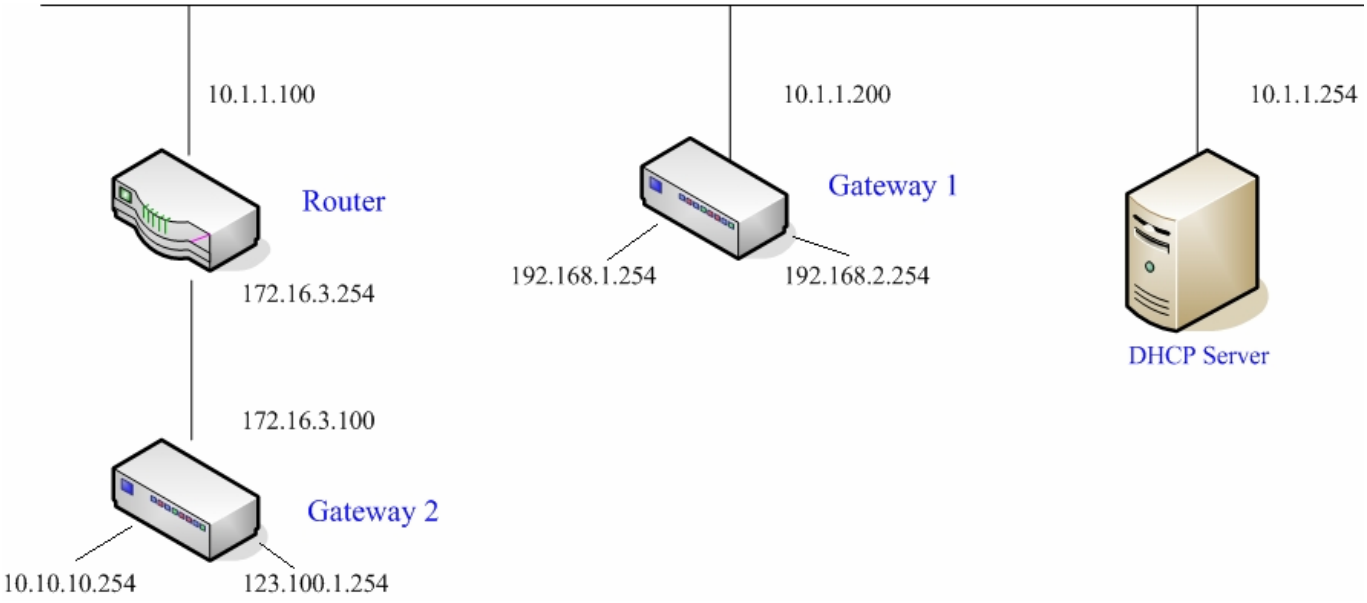
6. Non-supported OS and Browser

Currently, Windows Internet Explorer is the only browser supported by DSA-3600.Windows XP and Windows 2000 are the only two supported OS along with this release.

Appendix I. DHCP Relay

The DSA-3600 supports DHCP Relay defined according to RFC 3046. For scaling reasons, it is advantageous to set up an external DHCP server apart from using the internal DHCP server implemented in the DSA-3600 for assigning IP. When client-originated DHCP packets are forwarded to a DHCP server, a new option called the “Relay Agent Information option” is inserted by the DHCP relay agent. External DHCP servers that recognize the Relay Agent Information option may use this information to implement IP address or other parameter assignment policies. The external DHCP server will echo the option back to the relay agent in server-to-client replies, and strip-off the option before forwarding the reply to the client.

A graphic example of connecting 2 gateways with an external DHCP server:



Please note that the Router and Gateway 1 connected to the DHCP Server have to be under the same network segment as the DHCP Server.

When a client requests IP address from Gateway 1 Public LAN through the build-in DHCP relay agent of the DSA-3600, the DHCP server will receive a DHCP REQUEST packet with Option 82 (a code defined in RFC 3046). A Circuit ID will be sent by the DSA-3600 when the DHCP relay is enabled to define where the packet is sent from, and this Circuit ID will have a format of MAC_IP, such as 00:E0:22:DF:AC:DF_192.168.1.254. When the external DHCP server gets the request packet, it will therefore know where to reply to and which IP to assign.

Here is an example of configuration file of the DHCP server:

```
class "g1_public_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:91_192.168.1.254";
}

class "g1_private_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:92_192.168.2.254";
}

class "g2_public_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_10.10.10.254";
}

class "g2_private_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_123.100.1.254";
}

subnet 0.0.0.0 netmask 0.0.0.0 {

        option domain-name-servers      168.95.1.1;

        pool {
                allow members of "g1_public_lan";
                range 192.168.1.30 192.168.1.50;
                option routers 192.168.1.254;
                option subnet-mask 255.255.255.0;
        }

        pool {
                allow members of "g1_private_lan";
                range 192.168.2.30 192.168.2.50;
                option routers 192.168.2.254;
                option subnet-mask 255.255.255.0;
        }
```

Based on the above example, the client that connects to the DSA-3600 sends out a DHCP request. The DHCP relay function being enabled in the DSA-3600 sends a Circuit ID 00:90:0B:07:60:91_192.168.1.254 to the external DHCP server. When the DHCP server gets the Circuit ID, it recognizes that the request is sent from g1_public_lan and thus assigns the client a DNS server of 169.95.1.1, an IP that is in the range of 192.168.1.30 and 192.168.1.50, a default gateway of 192.168.1.254, and a subnet-mask of 255.255.255.0