LANPRO LP-NC1
User's Manual

Version 1.00

Table of Contents

Chapter 1. Before You Start

1.1 Preface

This manual is for Hotspot owners, SMBs, or administrators in enterprises to set up network environment using LANPRO LP-NC1. It contains step by step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Convention

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

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

 Indicates that clicking this button will return to the homepage of this section.

 Indicates that clicking this button will return to the previous page.

Indicates that clicking this button will apply all of your settings.

Indicates that clicking this button will clear all inputs before clicking Apply button.

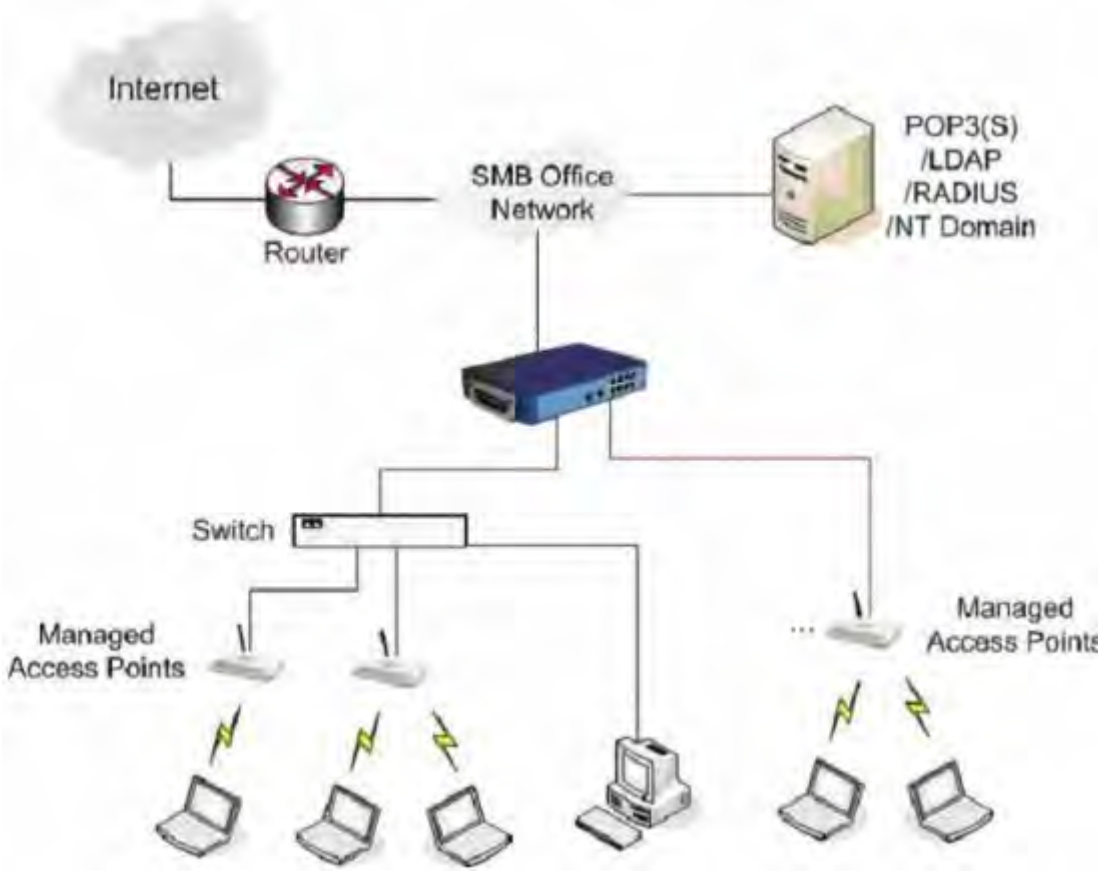
Chapter 2. System Overview

2.1 Introduction of LANPRO LP-NC1

LANPRO LP-NC1 is a Network Access Controller, specially designed for the small-scaled wireless, wired network management and access control. The major functional areas include user management, access control, AP management, and security management.

2.2 System Concept

LANPRO LP-NC1 dedicates to 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 following figure is an example of LANPRO LP-NC1 set to control a part of the company's intranet. The whole managed network includes the users in LAN and WLAN.



2.3 Specification

2.3.1 Hardware Specification

- **General**

  Form Factor: Mini-desktop

  Dimensions (W x D x H): 243 mm x 150 mm x 45.5 mm

  Weight: 1.4 Kg

  Operating Temperature: 0 ~ 45 ℃

  Storage Temperature: 0 ~ 65 ℃

  Power: 110~220 VAC, 50/60 Hz

  Ethernet Interfaces: 10 x Fast Ethernet (10/100 Mbps)

- **Connectors & Display**

  WAN Ports: 2 x 10BASE-T/100BASE-TX RJ-45

  LAN Ports: 8 x 10BASE-T/100BASE-TX RJ-45

  Console Port: 1 x RJ-11

  LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 8 x LAN

2.3.2 Technical Specification

- **Networking**

  Supports Router, NAT mode

  Supports Static IP, DHCP, PPPoE on WAN interface

  Configurable LAN ports authentication

  Supports IP Plug and Play (IP PnP)

  Built-in DHCP server and supports DHCP relay

  Supports NAT:

  1. IP/Port Destination Redirection
  2. DMZ Server Mapping
  3. Virtual Server Mapping

  Supports static route

  Supports Walled Garden (free surfing zone)

  Supports MAC Address Pass-Through

  Supports HTTP Proxy

- **Security**

  Supports data encryption: WEP (64/128-bit), WPA, WPA2

  Supports authentication: WPA-PSK, WPA2-PSK, IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP)

  Supports VPN Pass-through(IPSec and PPTP)

  Supports DoS attack protection

  Supports user Black List

  Allows user identity plus MAC address authentication for local accounts

- **User Management**

  Supports up to 120 concurrent users for LANPRO LP-NC1

  Provides 500 local accounts for LANPRO LP-NC1

  Provides 2000 on-demand accounts

  Simultaneous support for multiple authentication methods (Local and On-demand accounts, POP3(S), LDAP, RADIUS, NT Domain)

  Role-based and policy-based access control (per-role assignments based on Firewall policies, Routing, Login Schedule, Bandwidth)

  Customizable login and logout portal page

  User Session Management:

  1. SSL protected login portal page
  2. Supports multiple logins with one single account
  3. Session idle timer
  4. Session/account expiration control
  5. Friendly notification email to provide a hyperlink to login portal page
  6. Windows domain transparent login
  7. Configurable login time frame

- **AP Management**

  Supports up to 12 IEEE 802.11b/g APs (Cipherium A200)

  Centralized remote management via HTTP/SNMP interface

  Automatic discovery of managed APs and list of managed APs

  Allows administrators to add and delete APs from the AP list

  Allows administrators to enable or disable managed APs

  Provides MAC Access Control List of client stations for each managed AP

  Locally maintained configuration profiles of managed APs

  Single UI for upgrading and restoring managed APs' firmware

  System status monitoring of managed APs and associated client stations

  Automatic recovery of APs in case of system failure

  System alarms and status reports on managed APs

- **Monitoring and Reporting**

  Status monitoring of on-line users

  IP-based monitoring of network devices

  WAN connection failure alert

  Syslog support for diagnosing and troubleshooting

  User traffic history logging

- **Accounting and Billing**

  Support for RADIUS accounting, RADIUS VSA (Vendor Specific Attributes)

  Built-in billing profiles for on-demand accounts

  Enables session expiration control for on-demand accounts by time (hour) and data volume (MB)

  Provides billing report on screen for on-demand accounts

  Traffic history report in an automatic email to administrator

- **System Administration**

  Multi-lingual, web-based management UI

  SSH remote management

  Remote firmware upgrade

  NTP time synchronization

  Backup and restore of system configuration

Chapter 3. Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

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

3.1.2 Package Contents

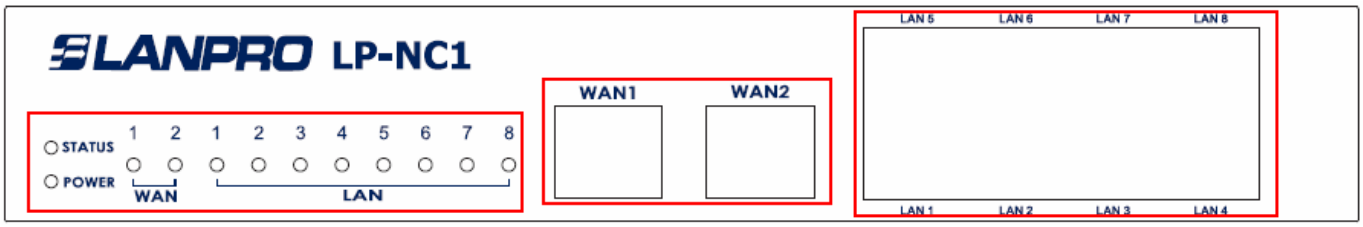
The standard package of LANPRO LP-NC1 includes:

- LANPRO LP-NC1 x 1
- CD-ROM (with User's Manual and QIG) x 1
- Quick Installation Guide x 1
- DC 12V Power Adapter x 1
- Ethernet Cable x 1
- Console Cable x 1

Warning: It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

3.1.3 Panel Function Descriptions

Front Panel



- **LED:** There are four kinds of LED, Power, Status, WAN and LAN, to indicate different status of the system.
- **WAN1/WAN2:** The two WAN ports are connected to a network which is not managed by the LANPRO LP-NC1 system, and this port can be used to connect the ATU-Router of the ADSL, the port of a cable modem, or a switch or a hub on the LAN of a company.
- **LAN1~LAN8:** Clients' machines connect to LANPRO LP-NC1 via LAN ports. Each LAN port can be configured to one of the two roles, controlled or uncontrolled. The differences of these two roles for a client connected to are:
  - Clients connected to the controlled port need to be authenticated to access network.
  - Clients connected to uncontrolled port don't need to be authenticated to access network and can access the web management interface.

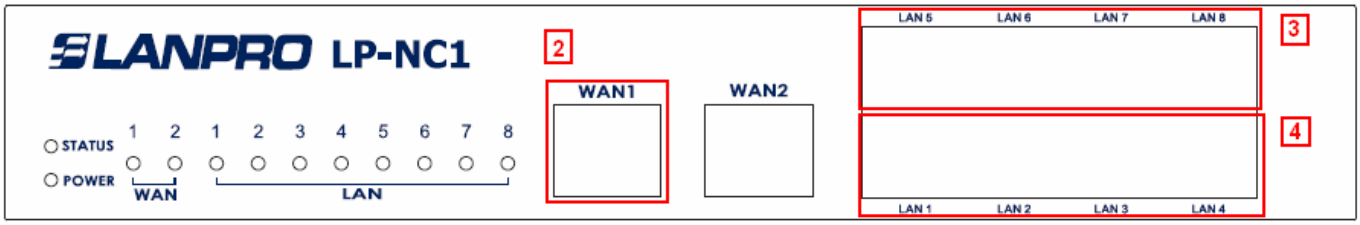
Rear Panel

- **Reset:** Press this button to restart the system.
- **Console:** The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's HyperTerminal to login to the configuration console interface to change admin password or monitor system status, etc.
- **DC+12V:** The power adapter attaches here.

3.1.4 Installation Steps

Please follow the following steps to install LANPRO LP-NC1:

1. Connect the 12V power adapter to the power socket on the rear panel. The Power LED should be on to indicate a proper connection.



2. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an ADSL modem, a cable modem or a switch/hub of the network. The LED of WAN1 port should be on to indicate a proper connection.
3. Connect an Ethernet cable to one of the LAN5~LAN8 Ports on the front panel. Connect the other end of the Ethernet cable to an administrator's PC or a notebook. The LED of the connected port should be on to indicate a proper connection. (Note: The default role of these four ports is ***Uncontrolled Port***.)
4. Connect an Ethernet cable to one of the LAN1~LAN4 Ports on the front panel. Connect the other end of the Ethernet cable to a client PC, AP or switch in managed network. The LED of the connected port should be on to indicate a proper connection. (Note: The default role of these four ports is ***Controlled Port***.)

Attention:

1. ***LANPRO LP-NC1 supports Auto Sensing MDI/MDIX. You may use either straight through or cross over cable to connect the Ethernet Port.***
2. ***Usually a straight cable could be applied when LANPRO LP-NC1 connects to an Access Point which supports automatic crossover. If after the AP hardware resets, the LANPRO LP-NC1 could not be able to connect to the AP while connecting with a straight cable, the user have to pull out and plug-in the straight cable again. This scenario does NOT occur while using a crossover cable.***

After the hardware of LANPRO LP-NC1 is installed completely, the system is ready to be configured in the following sections.

3.2 Software Configuration

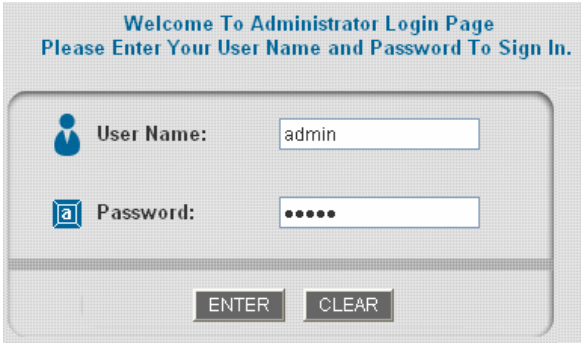
3.2.1 Quick Configuration

There are two ways to configure the system: using **Configuration Wizard** or changing the setting by demands manually. The Configuration Wizard has 6 steps providing a simple and easy way to guide you through the setup of LANPRO LP-NC1. Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting LANPRO LP-NC1, it is ready to use. There will be **6** steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Methods
6. Save and Restart LANPRO LP-NC1

Please follow the following steps to complete the quick configuration.

1. Use the network cable of the 10/100BaseT to connect a PC to the uncontrolled port, and then open a browser (such as Microsoft IE 6.0 or Firefox). Next, enter the gateway IP address as the web management interface's URL, the default gateway IP address is https://192.168.2.254. In the opened webpage, you will see the login page. Enter ***"admin"***, the default username and ***"admin",*** the default password, in the ***User Name*** and ***Password*** field. Click ***Enter*** to log in.



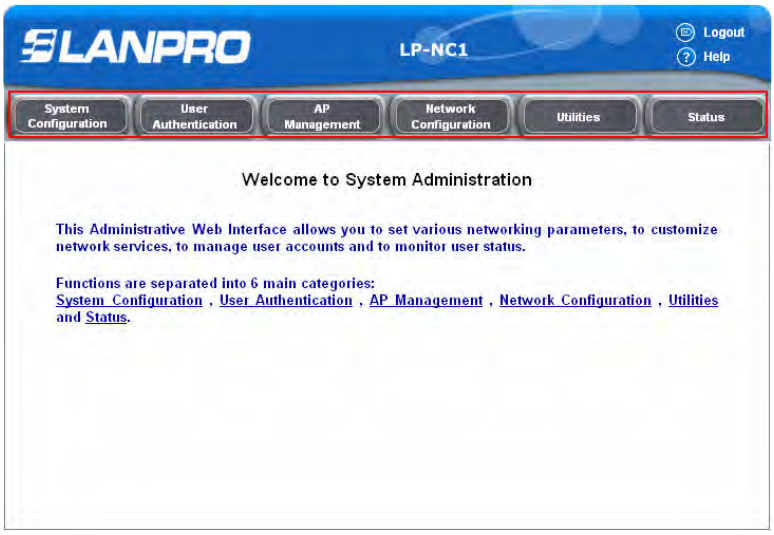
Caution: If you can't get the login screen, the reasons may be: 1. The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port; 2. The IP address and the default gateway are not under the same network segment. Please use default IP address such as 192.168.2.xx in your network and then try it again. For the PC configuration on PC, please refer to Appendix C. Network Configuration on PC.

LANPRO LP-NC1 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default username and password as follows.

Admin: The administrator can access all area of the LANPRO LP-NC1.

User Name: **admin**

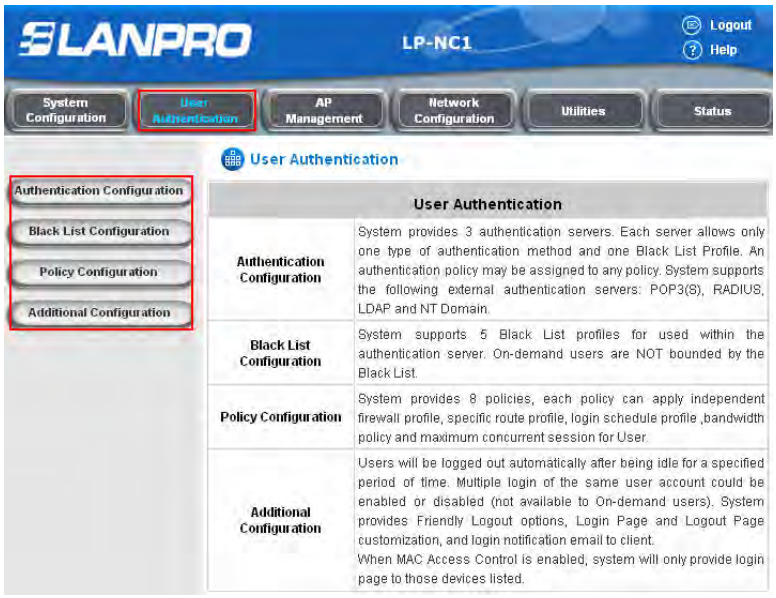
Password: **admin**



Manager: The manager can access the area under ***User Authentication*** to manage the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

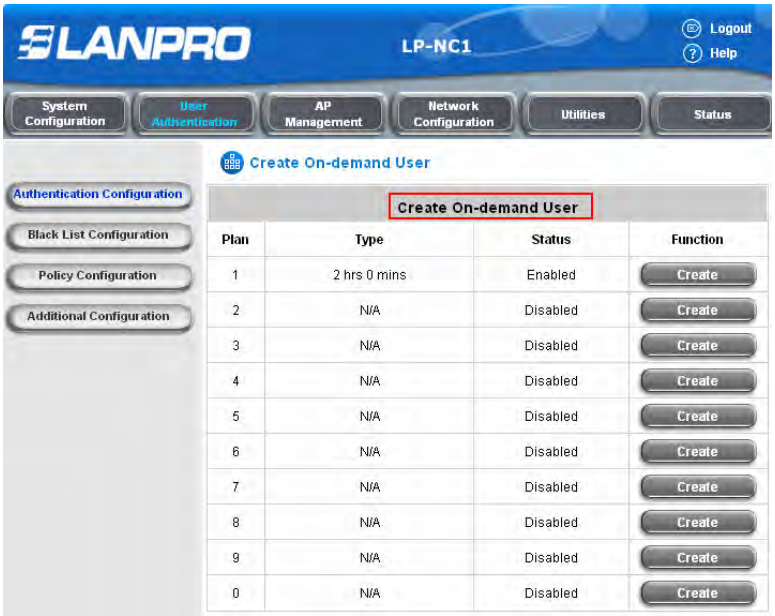
Password: **manager**



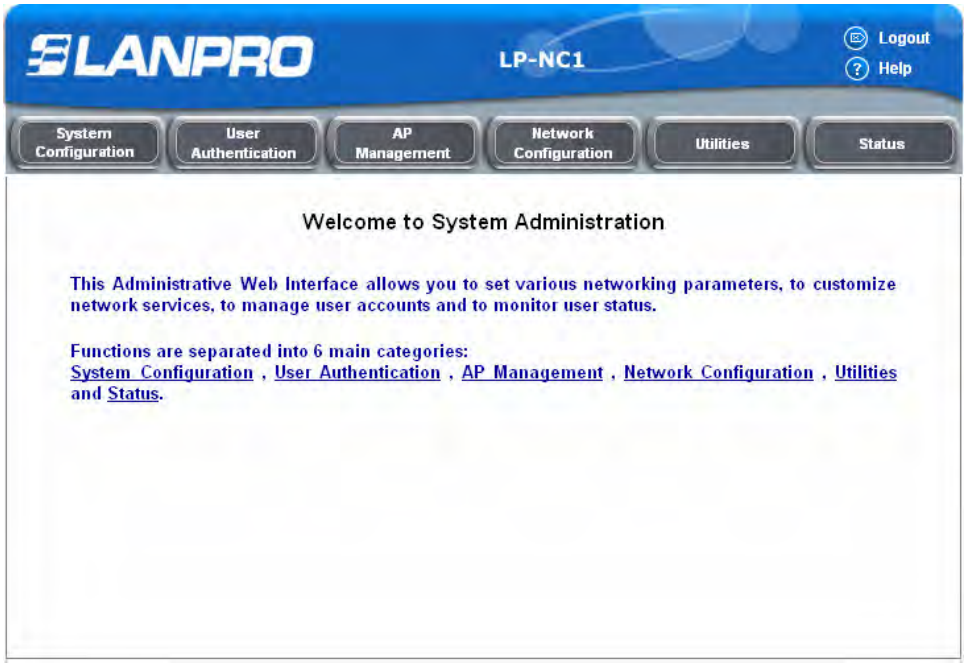
Operator: The operator can only access the area of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**



2. After successfully logging into LANPRO LP-NC1, enter the web management interface and see the welcome page. There is a ***Logout*** button on the upper right corner to log out the system when finished.



3. Then, run the configuration wizard to complete the configuration. Click ***System Configuration,*** the **System Configuration** page will appear.

4. Then, click on ***Configuration Wizard*** and click the ***Run Wizard*** to start the wizard.

5. **Configuration Wizard**

A welcome page that briefly introduces the 6 steps will appear. Click ***Next*** to begin.

- **Step 1. Change Admin's Password**

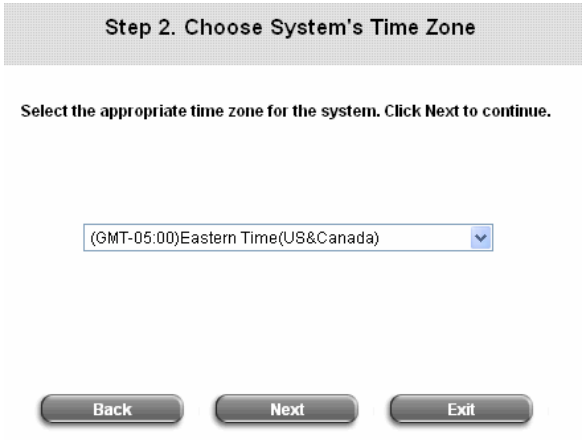
  Enter a new password for the admin account and retype it in the Verify Password field (twenty-character is the maximum and spaces are not allowed).

  Click ***Next*** to continue.

- **Step 2. Choose System's Time Zone**

  Select a proper time zone via the drop-down menu.

  Click ***Next*** to continue.



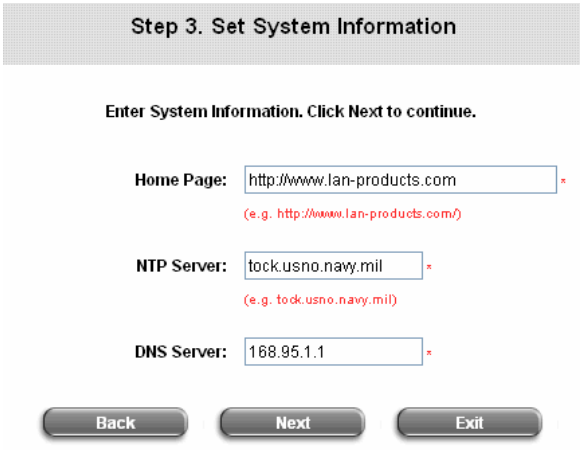
- **Step 3. Set System Information**

  Home Page: Enter the URL to where the users should be directed when they are successfully authenticated.

  NTP Server: Enter the IP address or the domain name of an external time server for LANPRO LP-NC1 to do time synchronization or use the default.

  DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

  Click ***Next*** to continue.



- **Step 4. Select the Connection Type for WAN Port**

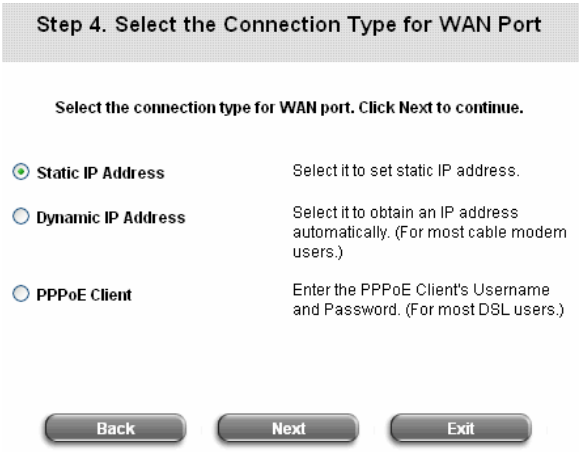
  There are three connection types of WAN1 port supported in the wizard: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

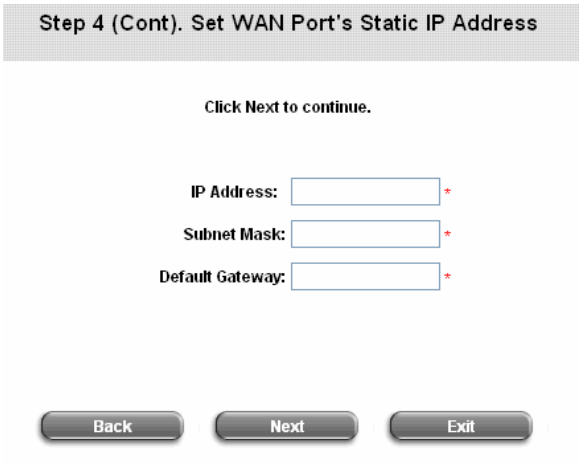
  Select a proper Internet connection type and click ***Next*** to continue.

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

    Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by your ISP or network administrator.

    Click ***Next*** to continue.

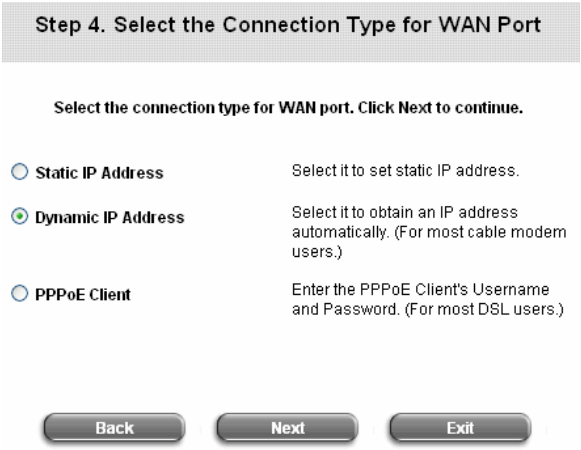




- **Dynamic IP Address**

  If this option is selected, LANPRO LP-NC1 will get an IP address for WAN1 from an external DHCP server automatically.

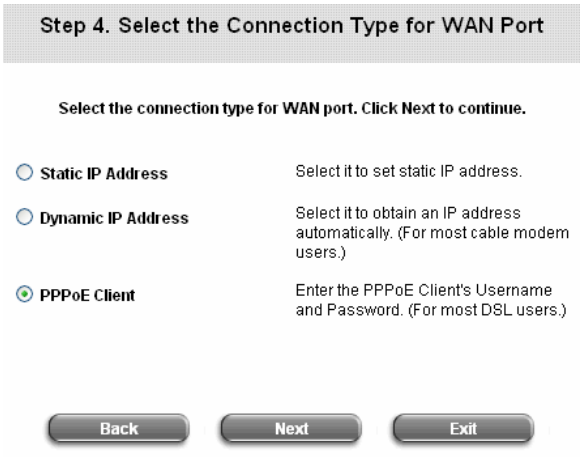
  Click ***Next*** to continue to Step 5 directly.

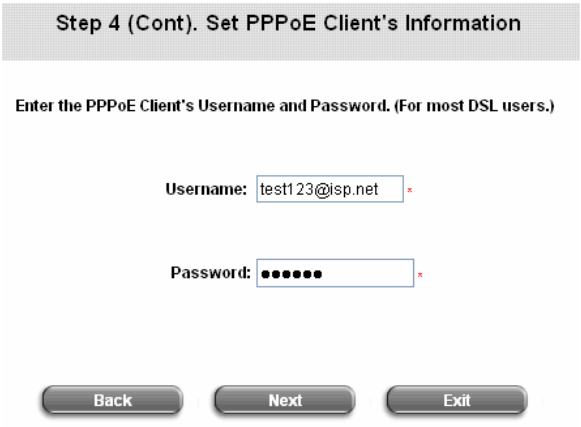


- **PPPoE Client: Set PPPoE Client's Information**

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

  Click ***Next*** to continue.

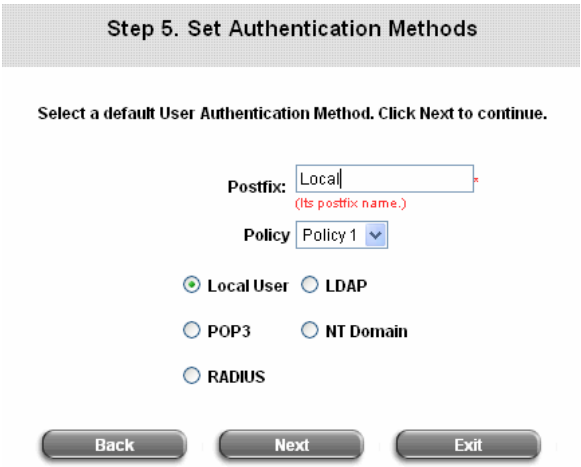




- **Step 5. Set Authentication Methods**

  Enter an identified name as the postfix name in the ***Postfix*** field (e.g. Local), select a policy to assign to, and choose an authentication method. The selected authentication method will be the default authentication method.

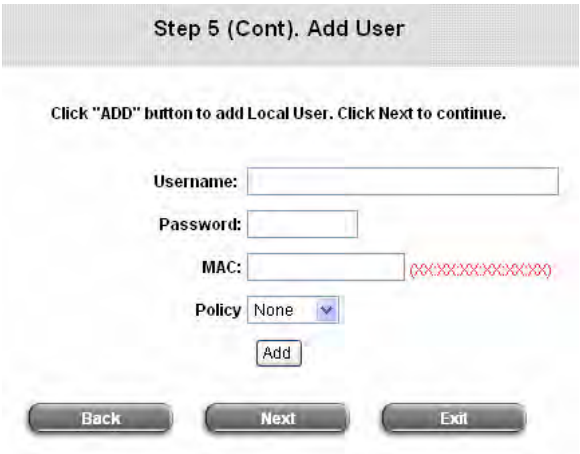
  Click ***Next*** to continue.



➢ **Local User: Add User**

A new user can be added to the local user data base. To add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC*** (optional, to specify a valid MAC address for this user) and assign a policy (or use the default). Click the ***ADD*** button to add this user.

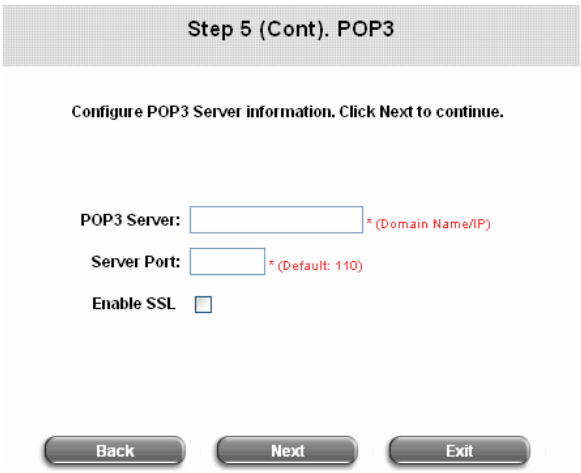
Attention: The policy selected in this step is applied to this user only. Per-user policy setting takes over the group policy setting at precious step unless you select None here. Click Next to continue.



- **POP3 User: POP3**

  Enter Domain Name/IP, Server Port of the POP3 server provided by the ISP, and then choose to enable SSL or not.

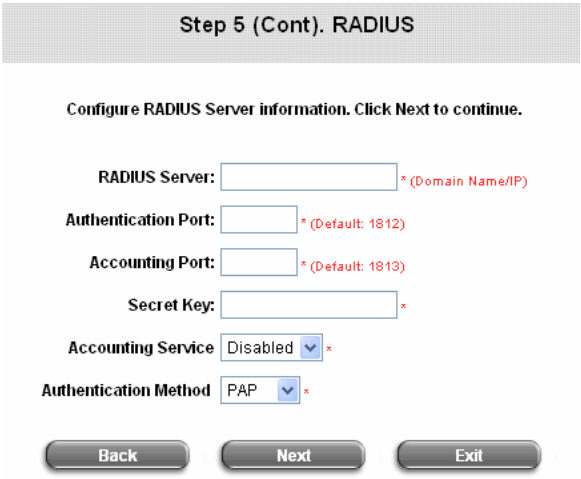
  Click ***Next*** to continue.



- **RADIUS User: RADIUS**

  Enter the Domain Name/IP of the **RADIUS server**, **Authentication Port**, **Accounting Port** and **Secret Key**. Then choose to enable the **Accounting Service** or not, and choose the desired **Authentication Method**.

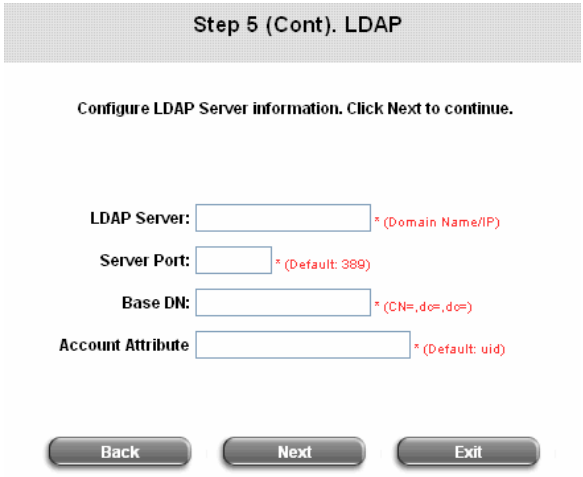
  Click ***Next*** to continue.



- **LDAP User: LDAP**

  Enter the **LDAP Server**, **Server Port**, **Base DN,** and **Account Attribute** of the LDAP server.

  Click **Next** to continue.

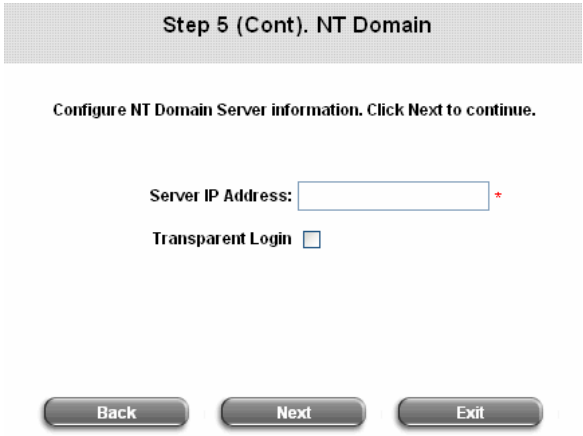


➢ **NT Domain User: NT Domain**

When NT Domain authentication method is selected, enter the **Server IP Address**, and choose to enable/disable **Transparent Login**.

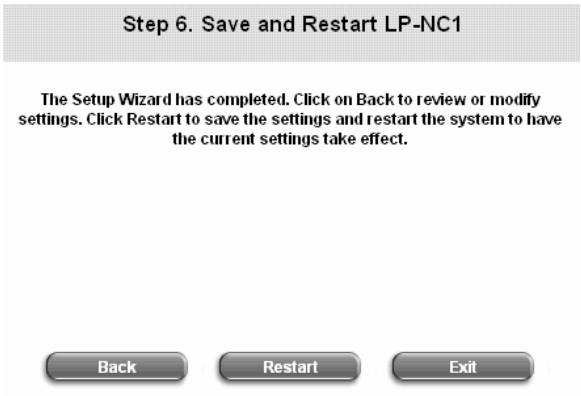
If "Transparent Login" is selected, users will be logged in the system NT Domain active directory and authenticated automatically when they log into their Windows OS domain.

Click ***Next*** to continue.

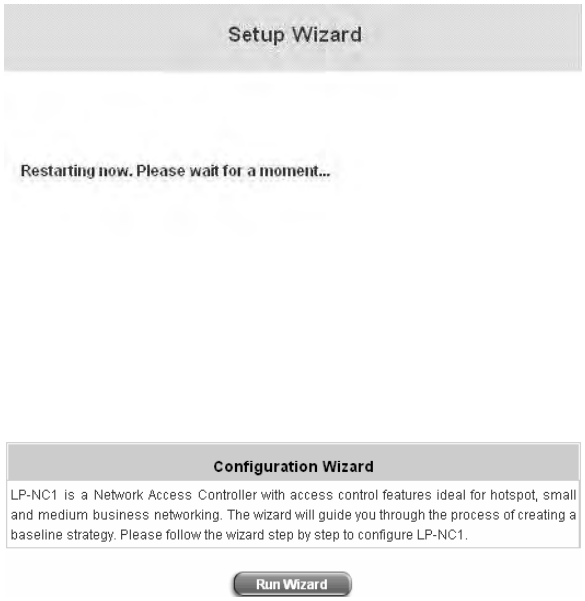


- **Step 6. Save and Restart LANPRO LP-NC1**

Click ***Restart*** to save the current setting and restart LANPRO LP-NC1. The Setup Wizard is completed now.



- **Setup Wizard:** During LANPRO LP-NC1 restart, a **"Restarting now. Please wait for a moment…"** message will appear on the screen. Please do not interrupt LANPRO LP-NC1 until the message has disappeared. The **Configuration Wizard** is shown on the screen. This indicates that a completed and successful restart process is finished.



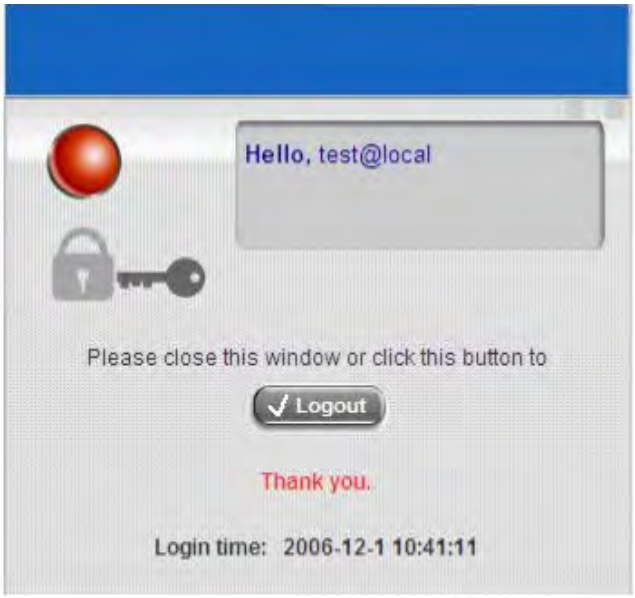
Caution: During each step of the wizard, if you want to go back to modify the setting, please click the Back button to go back to the previous step.

3.2.2 User Login Portal Page

To login from the login portal page via the controlled port, the user has to be authenticated by the system with username and password. The administrator also can verify if the configuration of LANPRO LP-NC1 has been done properly.

1. First, connect a client's device (for example, a PC) to the controlled port of LANPRO LP-NC1, and set the device to obtain an IP address automatically. After the client obtains the IP address, open an Internet browser. Try to launch any website and then the default **User Login Page** will appear. Enter a valid **User Name** and **Password** (e.g. ***test@local*** for the username and ***test*** for the password). Click ***Submit*** button.

2. Login success page will appear if LANPRO LP-NC1 has been installed and configured successfully. Now, clients can access the network or surf on the Internet.



3. When an on-demand user login successfully, the following **Login Success** page will appear. There is extra information showing **"Remaining usage"** and a **"Redeem"** button on the bottom.

   - **Remaining usage:** Show the remaining quota that the on-demand user can use to surf Internet.

   - **Redeem:** When the remaining credit is going to use up, the client has to pay for adding credit to the counter, and then, the client will get a new username and password. After clicking the ***Redeem*** button, a **Redeem Page** will appear. Please enter the new username and password obtained and click ***Enter*** button. The total available time or data size will be shown up after adding credit.

Chapter 4. Web Interface Configuration

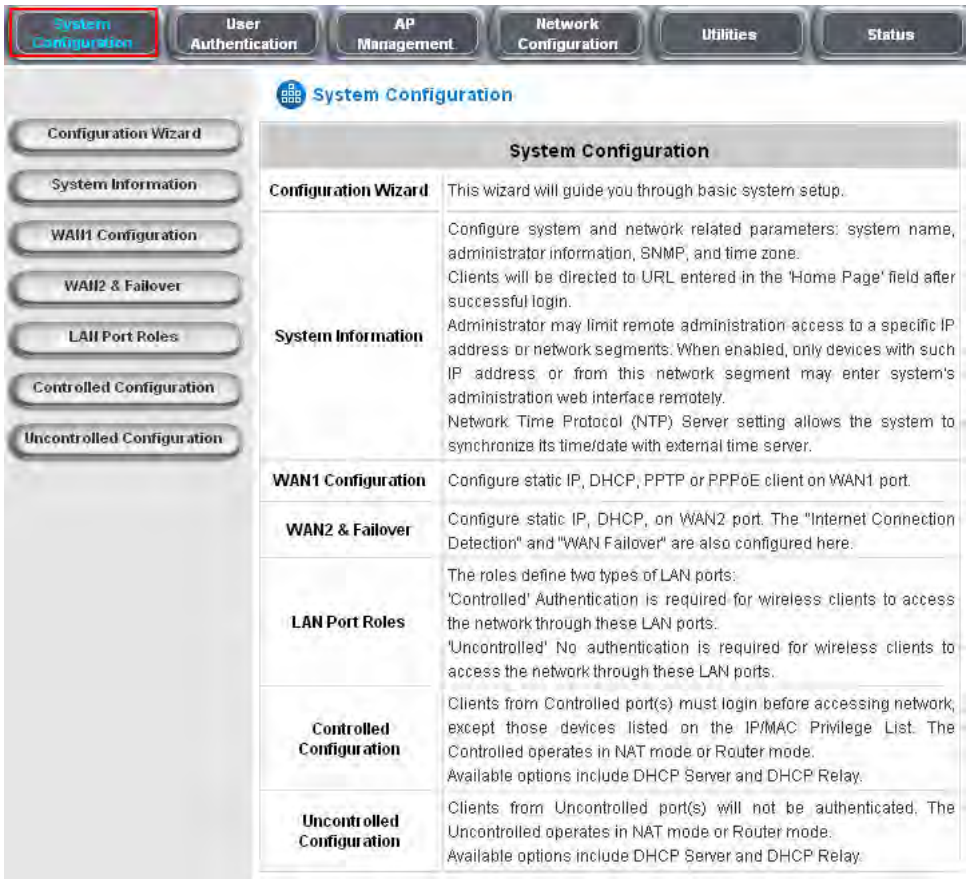
This chapter will guide you through further detailed settings. The following table is the UI and functions of LANPRO LP-NC1. The administration system allows you to set various networking parameters, enable and customize network services, manage user accounts and monitor user status. Administration functions are separated into 6 categories: System Configuration, User Authentication, AP Management, Network Configuration, Utilities, and Status.

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Policy Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Current Users
	WAN2 & Failover	Additional Configuration	Template Settings	Walled Garden List	Restart	Traffic History
	LAN Port Roles		Firmware Management	Proxy Server Properties		Notification Configuration
	Controlled Configuration		AP Upgrade	Dynamic DNS		
	Uncontrolled Configuration			IP Mobility		
				VPN Configuration		

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

4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 & Failover**, **LAN Port Roles**, **Controlled Configuration** and **Uncontrolled Configuration**.

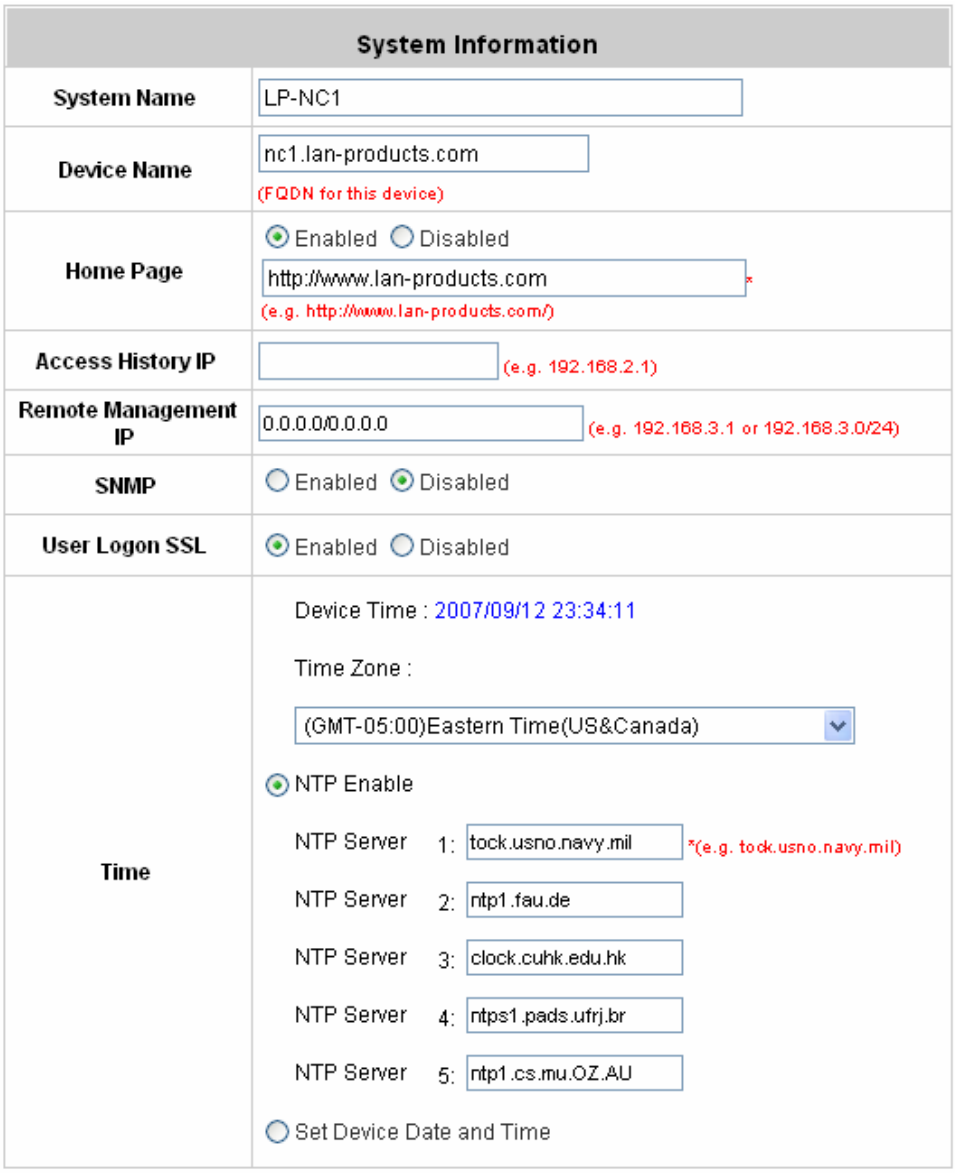


4.1.1 Configuration Wizard

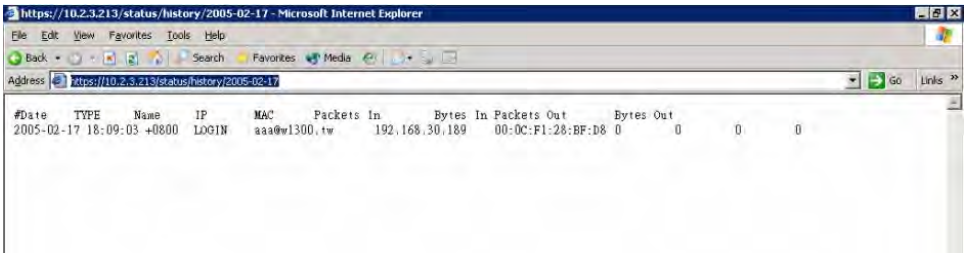
There are two ways to configure the system: using **Configuration Wizard** or changing the setting by demands manually. The Configuration Wizard has 6 steps providing a simple and easy way to go through the basic setup of LANPRO LP-NC1 and is served as **Quick Configuration**. Please refer to **3.2.1 Quick Configuration** for the introduction and description of **Configuration Wizard**.

4.1.2 System Information

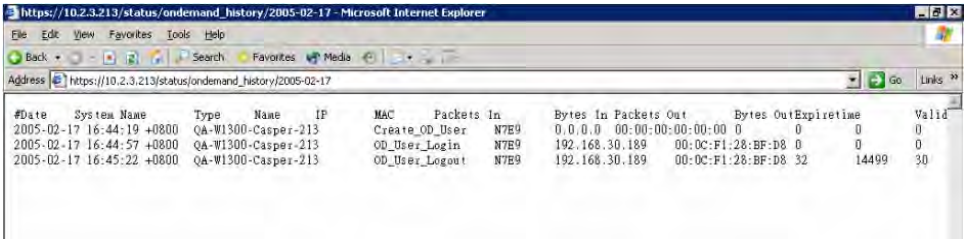
Most of the major system information about LANPRO LP-NC1 can be set here. Please refer to the following description for each field:



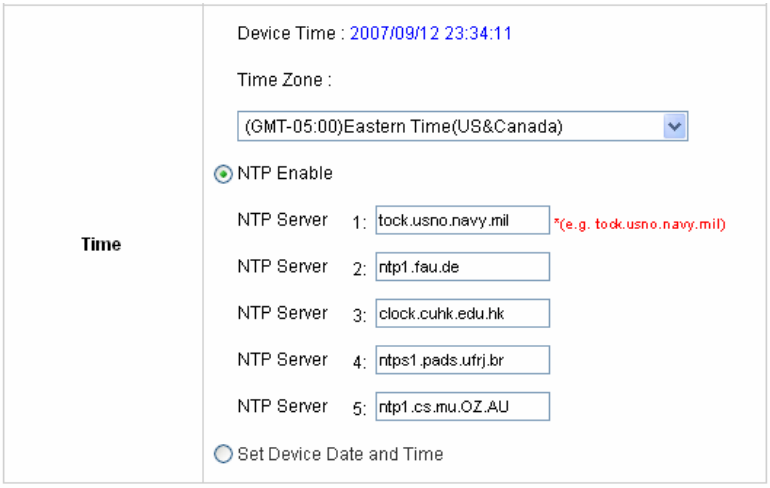
- **System Name:** Set the name of the system or use the default.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is used as the domain name used in login page. For example, if Device Name=ashop.com, the URL of login page will be https://ashop.com/loginpages/login.shtml.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users login successfully, they will be directed to this homepage. Usually, the homepage is the company's website, such as http://www.yahoo.com. If select ***Disable*** here, it will redirect to the original webpage that configured in the clients' computers.
- **Access History IP:** The IP address of external billing system. Only device with this IP address may directly access system's billing records. Specify an IP address of the administrator's computer or to get history information directly with fixed format URLs as the following example:
  Traffic History：https://10.2.3.213/status/history/2005-02-17

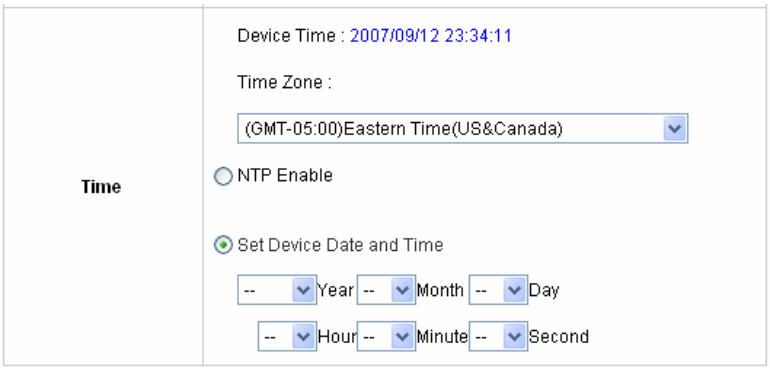


On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17



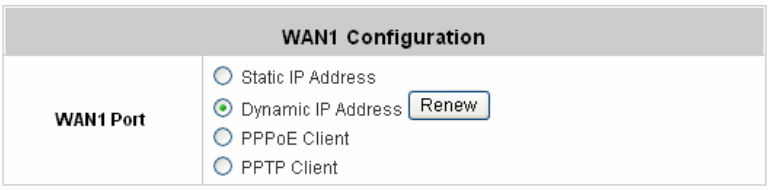
- **Remote Management IP:** The IP address or subnet of remote management PC. Only PC with this IP range may access system's web management interface. Set the IP addresses or IP ranges which have permission to access the web management interface via WAN and/or controlled port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of LANPRO LP-NC1. If the IP range bit number is omitted, 32 is used to specify a single IP address.
- **SNMP:** Configure IP address and community ID of external SNMP management device. If the function is enabled, it is able to assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system.
- **User Logon SSL:** Enable Secured Socket Layer (SSL) Web Login (HTTPS) or disable it (HTTP). Enable this function to activate https (encryption) or disable this function to activate http (non encryption) user login page.
- **Time:** Configure system time manually or use up to 5 external NTP(Network Time Protocol) serves for time synchronization. Please specify the time zone and IP address of at least one NTP server in the system configuration interface for adjusting the system time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can also be set manually when selecting **"Set Device Date and Time"**. Please enter the date and time into these fields.



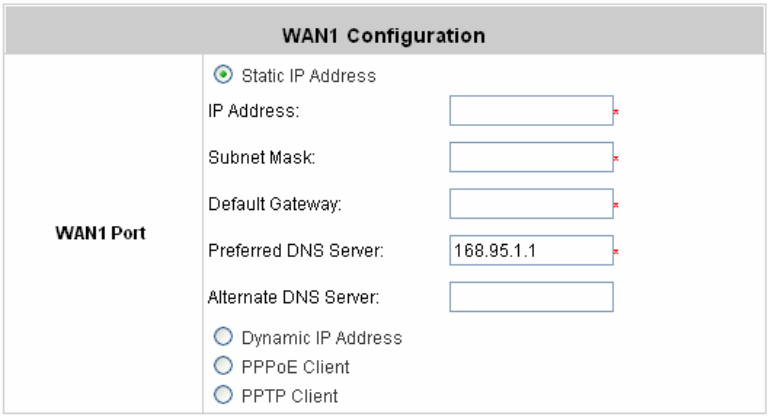

Time
Device Time : 2007/09/12 23:34:11
Time Zone :
(GMT-05:00)Eastern Time(US&Canada)
NTP Enable
Set Device Date and Time
-- Year -- Month -- Day
-- Hour -- Minute -- Second

4.1.3 WAN1 Configuration

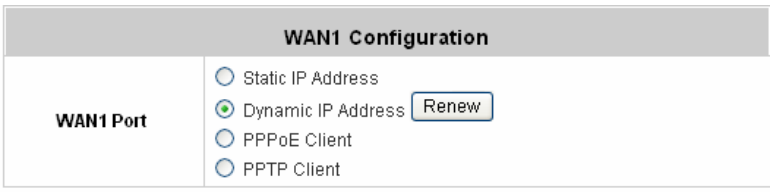
System supports four different WAN connection types: **Static IP Address**, **Dynamic IP Address**, **PPPoE Client** and **PPTP Client**.



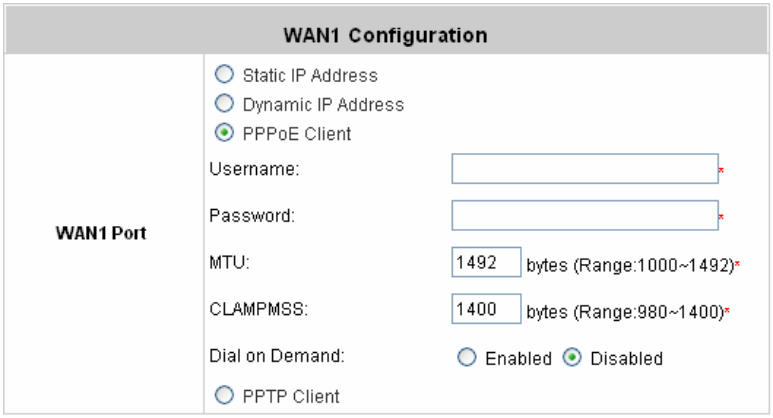
- **Static IP Address:** Manually specifying the IP address of the WAN1 Port is applicable for the network environment where the DHCP service is unavailable. The fields with red asterisks are required to be filled in.
  IP Address: The IP address of the WAN1 port.
  Subnet Mask: The subnet mask of the 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 not required.



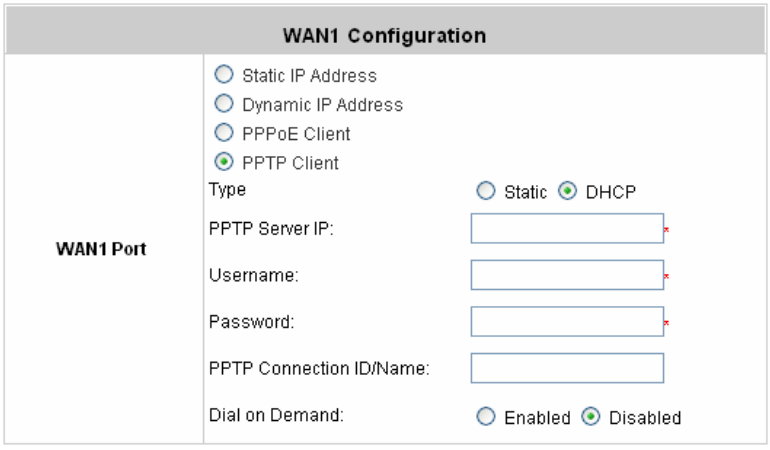
- **Dynamic IP address:** Configure WAN Port settings automatically using external DHCP Server. Click the ***Renew*** button to get an IP address.



- **PPPoE Client:** This is the common connection type for ADSL. When selecting PPPoE to connect to the network, please enter the **Username**, **Password**, **MTU** and **CLAMPMSS**. There is a **Dial on Demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



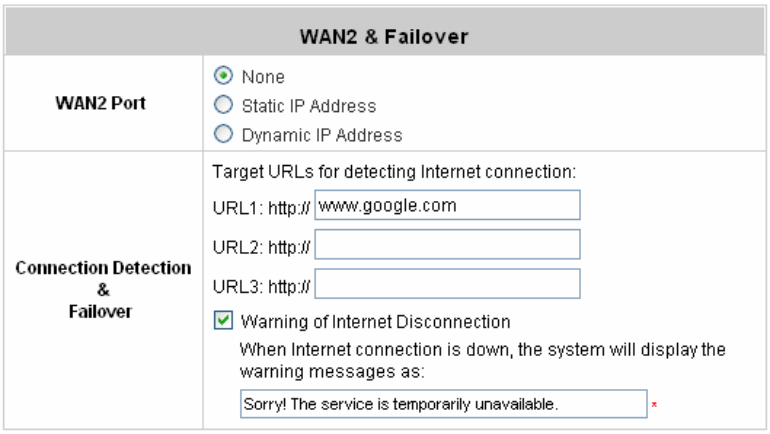
- **PPTP Client:** Point to Point Tunneling Protocol is a service that applies to broadband connection used mainly in Europe and Israel. Select **Static** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required 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.



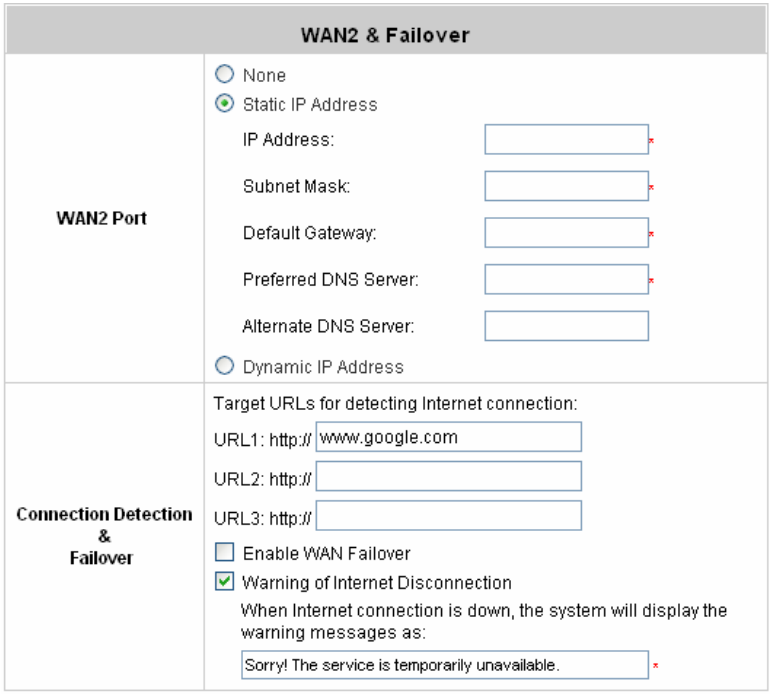
4.1.4 WAN2 & Failover

Except selecting **None** to disable WAN2 port, there are 2 connection types for the WAN2 port: **Static IP Address** and **Dynamic IP Address**. The probe target supports up to three URLs. Check **"Warning of Internet Disconnection"** to work with the WAN **Failover** function. When **Warning of Internet Disconnection** is enabled, the system will check the three URLs to detect the WAN ports connection status.

- **None**: The WAN2 Port is disabled. The probe target of up to three URLs can still be entered. Check **"Warning of Internet Disconnection"** to detect the WAN1 port connection status.

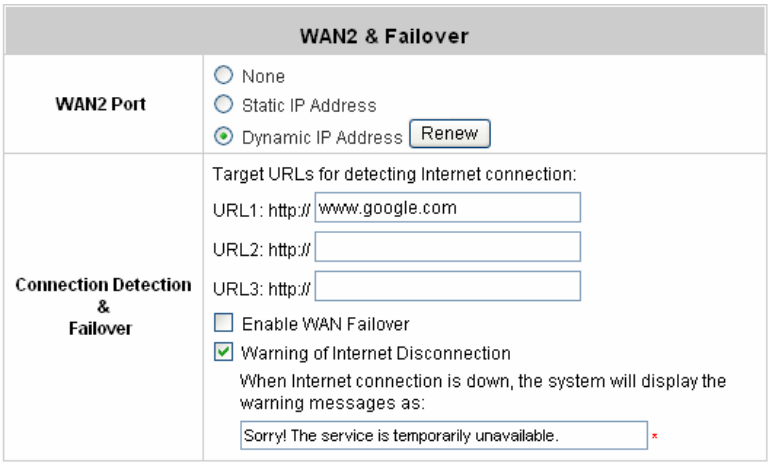


- **Static IP Address:** Configure WAN Port settings manually. Specify the **IP Address**, **Subnet Mask** and **Default Gateway** of WAN2 Port, which should be applicable for the network environment.



If **WAN Failover** function is enabled, when WAN1 connection fails, the traffic will be routed to WAN2 automatically. If **"Fall back to WAN1 when possible"** function is enabled, the routed traffic will be back to WAN1 when WAN1 connection is recovered.

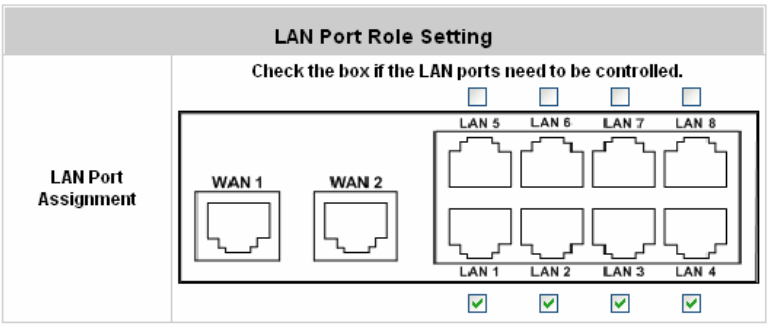
- **Dynamic IP Address:** Configure WAN Port settings automatically using external DHCP Server. Select this item when WAN2 Port can obtain an IP address automatically. For example, a DHCP Server is available for WAN2 Port. The probe target supports up to three URLs to detect the URLs. They can check with the **"WAN Failover"** and **"Warning of Internet Disconnection"** functions. The system will check these three URLs to detect the WAN ports connection status.
- **Warning of Internet Disconnection:** By putting at least one external URL address for system to check the internet connection possible availability continuously.
- **WAN Failover:** To trigger WAN2 port start to serve system's WAN traffic when WAN1 fail was detected. A possible fallback of WAN traffic from WAN2 to WAN1 (if WAN1's internet connection is resumed again) could be selected.



For Dynamic IP Address, **WAN Failover** and **Fall back to WAN1 when possible** functions also can be enabled like as the functions for **Static IP Address**. If **Warning of Internet Disconnection** is enabled, a warning message can be entered to indicate what the system should display when Internet connection is down.

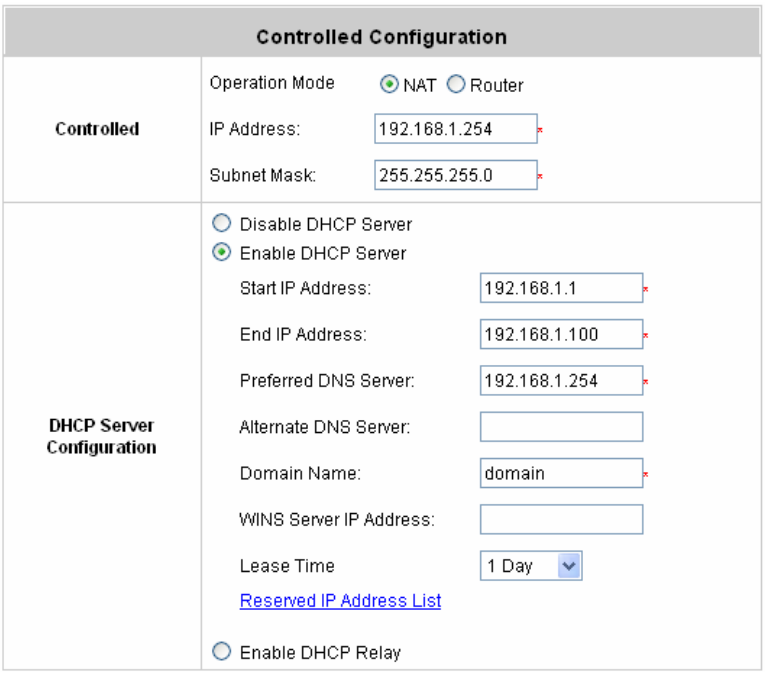
4.1.5 LAN Port Roles

Administrators can choose which LAN port(s) to be Controlled port(s) by checking the box. Each LAN port can be configured as one of two roles, controlled or uncontrolled. The differences of these two roles for a client connected to are: Clients connect to the **Controlled Port** that need authentication to access the network; Clients connect to **Uncontrolled Port** that don't need authentication to access the network and can also access the web management interface without **Remote Management IP** configuration.

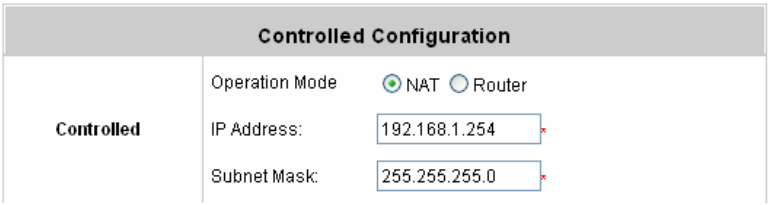


4.1.6 Controlled Configuration

The clients of Controlled Port can access the network without authentication first. In this section, you can set the related configuration of Controlled Port.



- **Controlled**



Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, according to requirements.

IP Address: Enter the desired IP address for the interface of the controlled port.

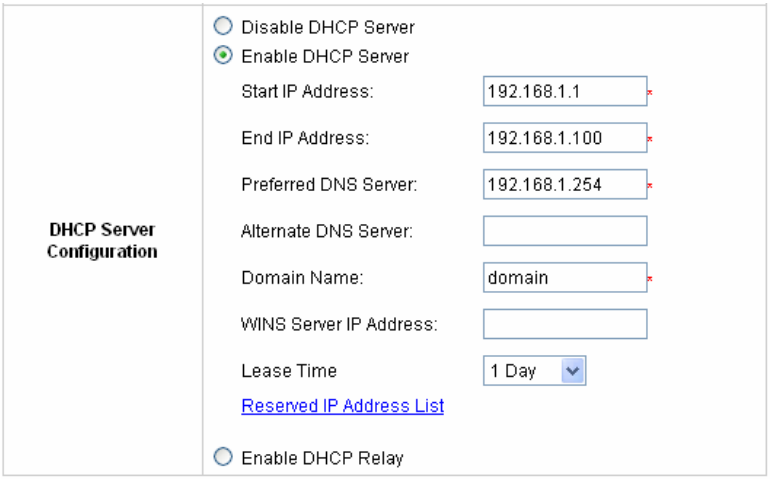
Subnet Mask: Enter the desired subnet mask for the controlled port.

- **DHCP Server Configuration**

  There are three types of DHCP server methods: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**. When enabled, the system acts as DHCP Server issuing network configuration information to clients connecting to Controlled Port. When DHCP Relay is checked, system will relay DHCP information from external DHCP Server to downstream clients.

  1. **Disable DHCP Server:** Disable DHCP Server function of LANPRO LP-NC1.

  2. **Enable DHCP Server:** When enabled, the system acts as Choose **Enable DHCP Sever** function and set the appropriate configuration for the built-in DHCP server of LANPRO LP-NC1. The fields with red asterisks are required. Please fill in these fields.



  DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"**. **Start IP Address** means the fist IP address of the DHCP scope. **End IP Address** means the last IP address of the DHCP scope. These two settings define the IP address range that will be assigned to the clients of Controlled Port.
  Preferred DNS Server: This means the primary DNS server for the DHCP of Controlled Port.
  Alternate DNS Server: This means the substitute DNS server for the DHCP of Controlled Port.
  Domain Name: This means the domain name of Controlled Port.
  WINS Server IP: This means the IP address of the WINS server if used.
  Lease Time: This means the time period that IP addresses got from the DHCP server are valid and available.
  Reserved IP Address List: Reserves up to 40 IP addresses from predefined DHCP Scope and prevents systems from issuing these IP address to downstream users. For the detail setting of Reserved IP Address List, please click the hyperlink of ***Reserved IP Address***. After clicking, the Reserved IP Address List as shown in the following figure will appear. Enter the related **Reserved IP Address**, **MAC**, and **Description** (not compulsory). When finished, click ***Apply*** to complete the setting.

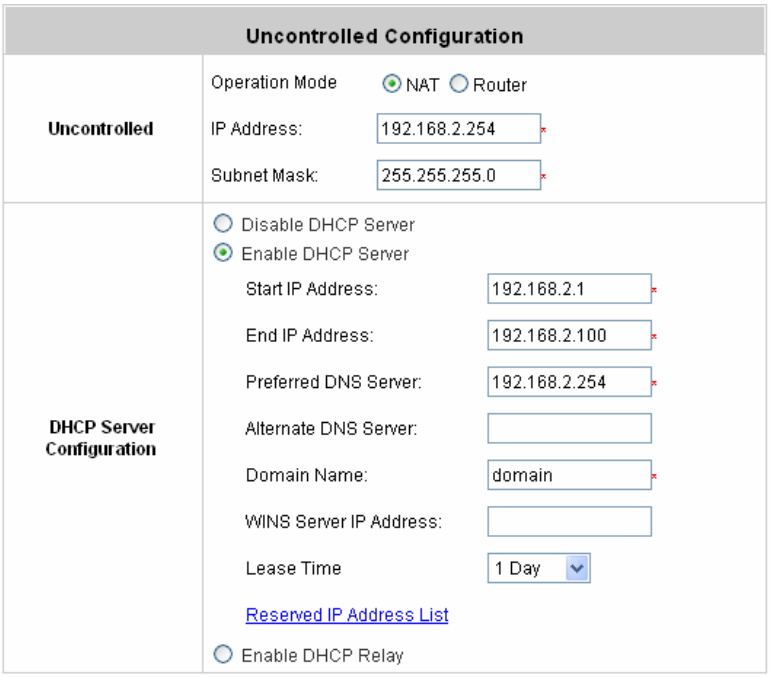
Reserved IP Address List - Controlled			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			

Enable DHCP Relay: The DHCP Server IP address must be entered when this function is enabled. For more details about DHCP Relay, please see ***Appendix G. DHCP Relay.***

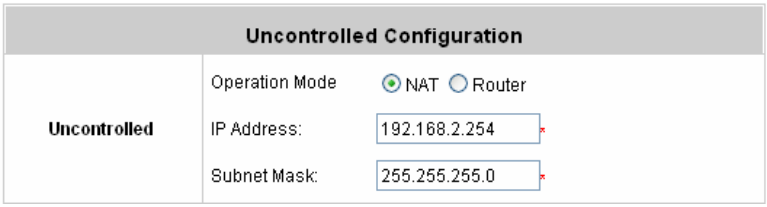
DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP: *

4.1.7 Uncontrolled Configuration

The clients of Uncontrolled Port can access the network without authentication first. In this section, you can set the related configuration of Uncontrolled Port.



- **Uncontrolled**



Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, according to requirements.

IP Address: Enter the desired IP address for the interface of the controlled port.

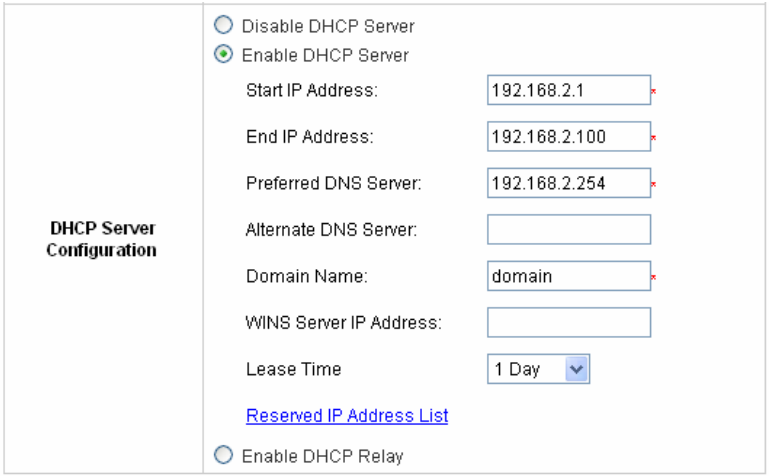
Subnet Mask: Enter the desired subnet mask for the controlled port.

- **DHCP Server Configuration**

  There are three types of DHCP server methods: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

  1. **Disable DHCP Server:** Disable DHCP Server function of LANPRO LP-NC1.

  2. **Enable DHCP Server:** Choose **Enable DHCP Sever** function and set the appropriate configuration for the built-in DHCP server of LANPRO LP-NC1. The fields with red asterisks are required. Please fill in these fields.



  DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"**. **Start IP Address** means the fist IP address of the DHCP scope. **End IP Address** means the last IP address of the DHCP scope. These two settings define the IP address range that will be assigned to the clients of Uncontrolled Port.
  Preferred DNS Server: This means the primary DNS server for the DHCP of Uncontrolled Port.
  Alternate DNS Server: This means the substitute DNS server for the DHCP of Uncontrolled Port.
  Domain Name: This means the domain name of Uncontrolled Port.
  WINS Server IP: This means the IP address of the WINS server if used.
  Lease Time: This means the time period that IP addresses got from the DHCP server are valid and available.
  Reserved IP Address List: For the detail setting of Reserved IP Address List, please click the hyperlink of ***Reserved IP Address***. After clicking, the Reserved IP Address List as shown in the following figure will appear. Enter the related **Reserved IP Address**, **MAC**, and **Description** (not compulsory). When finished, click ***Apply*** to complete the setting.

Reserved IP Address List - Uncontrolled			
Item	Reserved IP Address	MAC	Description
1			
2			
3			

Enable DHCP Relay: The DHCP Server IP address must be entered when this function is enabled. For more details about DHCP Relay, please see ***Appendix G– DHCP Relay.***

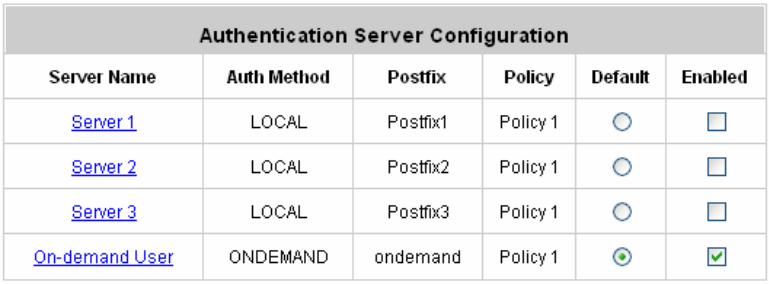
DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP: *

4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Policy Configuration**, and **Additional Configuration**. This section relates to user authentication, authorization and accounting.

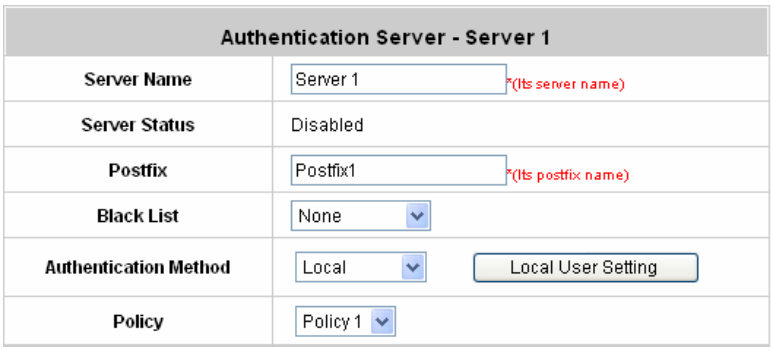
4.2.1 Authentication Configuration

This function is used to configure the settings of authentication servers. The system supports up to three internal or external user database plus On-Demand User. User database can be one of the followings: RADIUS, LDAP, POP3, NT Domain Server, or Local database. The system supports 802.1x authentication for downstream clients. Click the server name to set the related configurations for that particular authentication server. Without typing the postfix is allowed to fasten the login process when clients log into the default authentication server.



Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy 1	○	☐
Server 2	LOCAL	Postfix2	Policy 1	○	☐
Server 3	LOCAL	Postfix3	Policy 1	○	☐
On-demand User	ONDEMAND	ondemand	Policy 1	◉	☑

- There are 5 kinds of authentication methods that LANPRO LP-NC1 supports: Local User, POP3, RADIUS, LDAP and NTDomain. Click the server name to enter the **Authentication Server** page.



Authentication Server - Server 1	
Server Name	Server 1 *(Its server name)
Server Status	Disabled
Postfix	Postfix1 *(Its postfix name)
Black List	None
Authentication Method	Local — Local User Setting
Policy	Policy 1

Server Name: Set a name for the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

Sever Status: The status shows that the server is enabled or disabled.

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

Note: The Policy Name cannot contain these words: MAC and IP.

Black List: There are 5 sets of black lists. Select one of them or choose **"None"**. Please refer to **4.2.2 Black List Configuration** for more information.

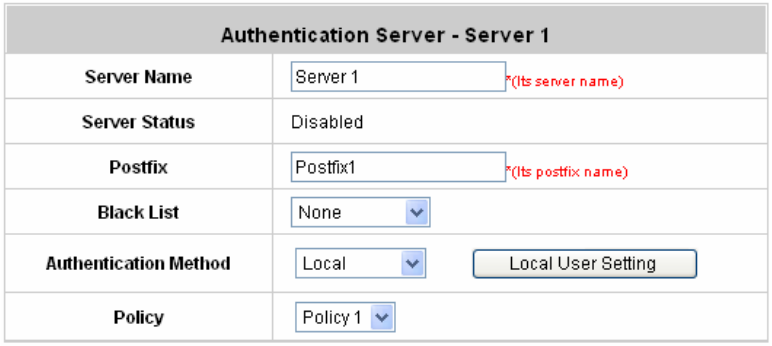
Authentication Method: There are 5 authentication methods that LANPRO LP-NC1 supports: **Local**, **POP3**, **Radius**, **LDAP** and **NTDomain**. Select the desired authentication method and then click the link next to the drop-down menu for more advanced configuration. For more details, please refer to **4.2.1.1~5 Authentication Configuration**.

Notice: Enabling two or more servers of the same authentication method is not allowed.

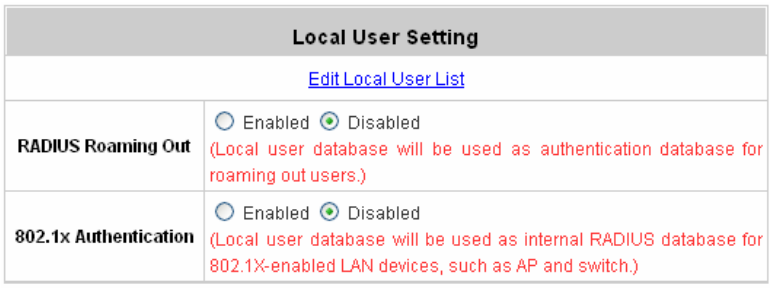
Policy: There are 8 policies that can be chosen to apply to this particular server.

4.2.1.1 Authentication Method – Local User Setting

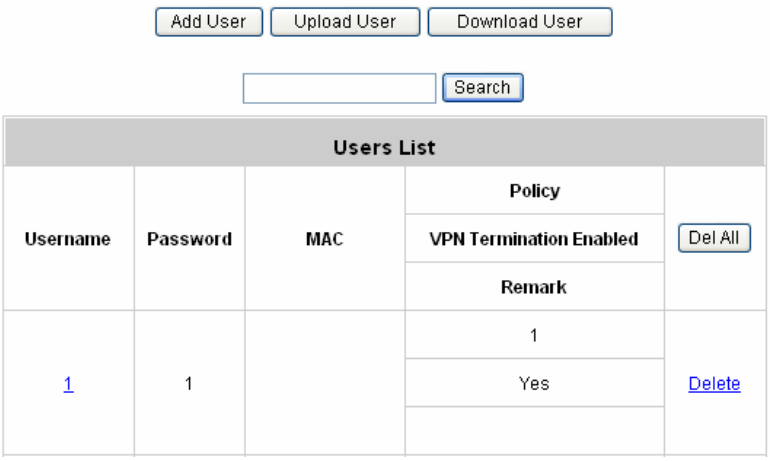
Choose **Local User** in the **Authentication Method** field, the button besides the drop-down menu will become to ***Local User Setting***.



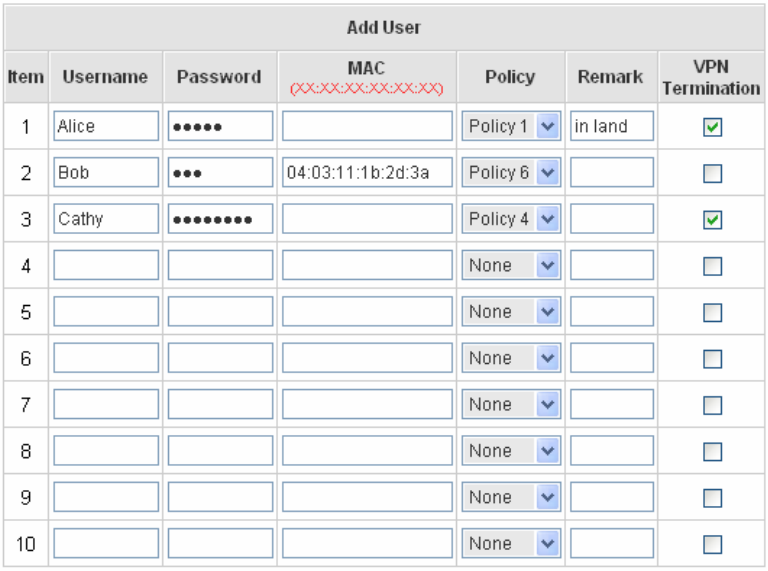
Click the button of **Local User Setting** for further configuration.



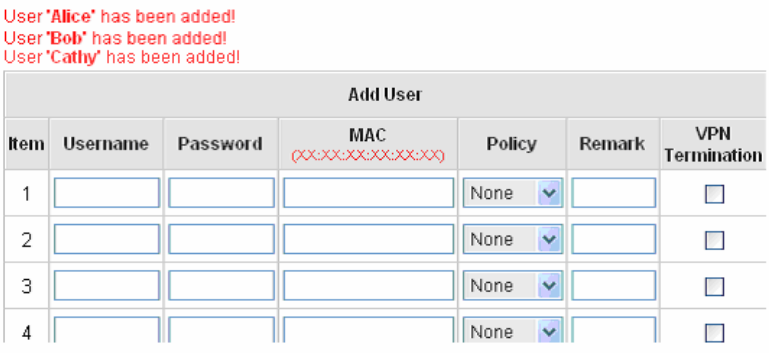
- **Edit Local User List:** To view, add, delete, upload a list of users from a file and backup user accounts from this device. Press Refresh button to refresh the information status of users list. VPN connection for individual local user must be checked to enable for each user account. Click the button of **Edit User Setting** to enter the **Local User List** page.



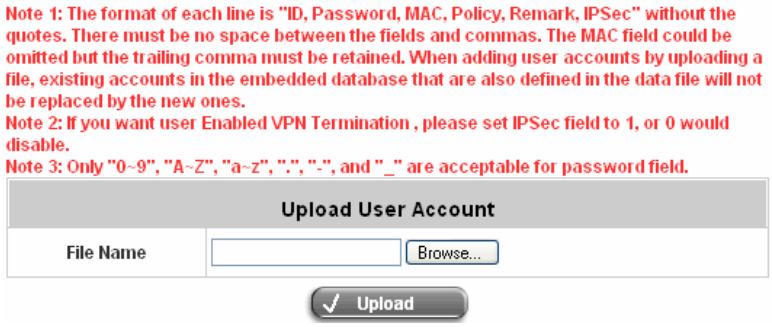
- **Add User:** Click this to enter the **Add User** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** (optional) and **"Remark"** (optional). Select a desired **Policy**, check whether to enable **VPN Termination**.



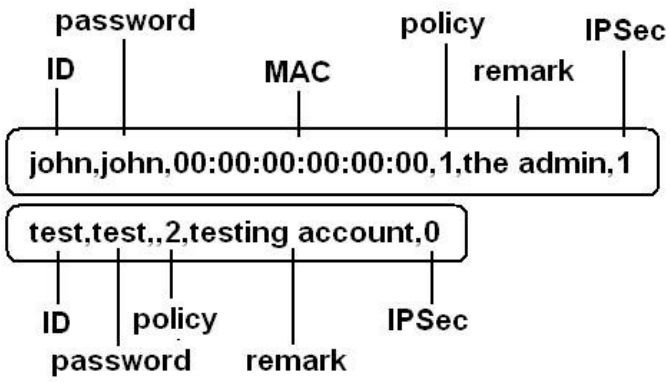
Click Apply to save all the settings after finishing to add users.



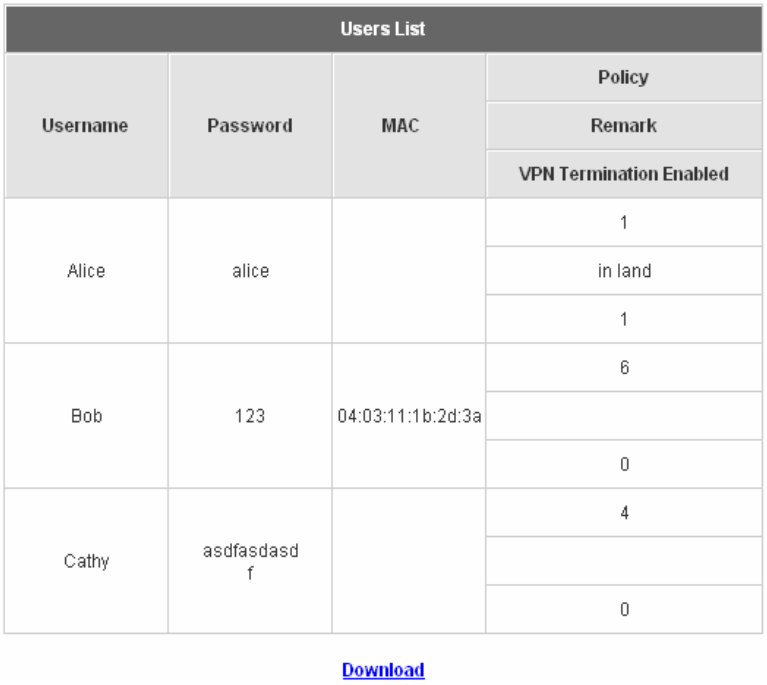
Upload User: Click this to enter the **Upload User** interface. Click the ***Browse*** button to select the text file for uploading the user accounts. Then click ***Submit*** to complete the upload process.



The uploading file should be a text file and the format of each line is ***"ID, Password, MAC, Policy, Remark, IPSec"*** without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. The Group field indicates policy number to use. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones. If you want user Enable VPN Termination, please set **IPSec** field to 1 to enable VPN, or 0 to disable VPN.



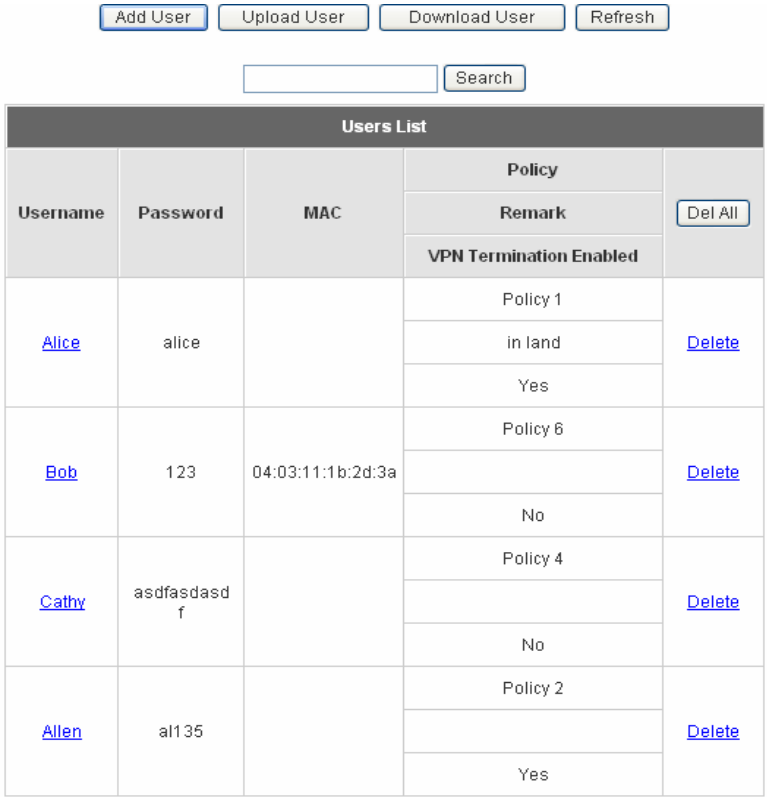
Download User: Click this to enter the **Users List** page and the system will directly show a list of all created user accounts. Click ***Download*** to create a .txt file and then save it on the disk.



Users List			
Username	Password	MAC	Policy Remark VPN Termination Enabled
Alice	alice		1 in land 1
Bob	123	04:03:11:1b:2d:3a	6 0
Cathy	asdfasdasdf		4 0

Download

Refresh: Click this to renew the **Users List** page.

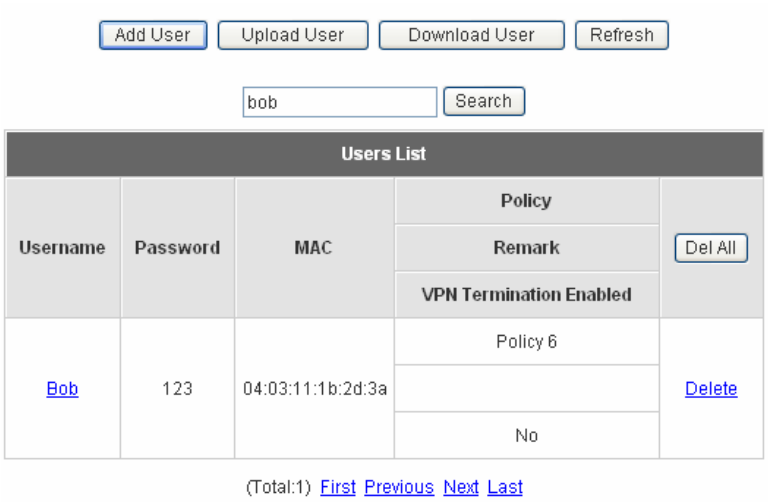


Add User | Upload User | Download User | Refresh

Search

Users List				
Username	Password	MAC	Policy Remark VPN Termination Enabled	Del All
Alice	alice		Policy 1 in land Yes	Delete
Bob	123	04:03:11:1b:2d:3a	Policy 6 No	Delete
Cathy	asdfasdasdf		Policy 4 No	Delete
Allen	al135		Policy 2 Yes	Delete

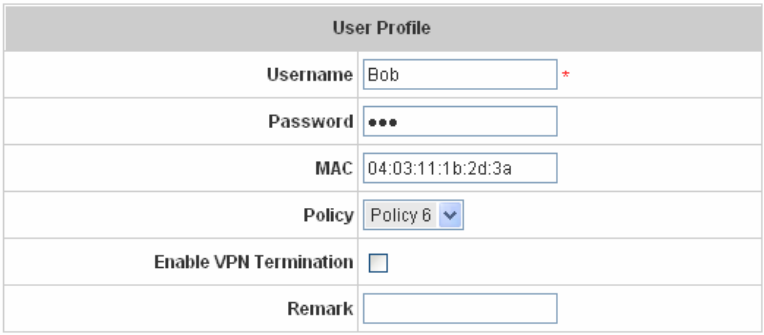
Search: Enter a keyword of a username that you want to search and click this button to perform the search. All usernames matching the keyword will be listed.



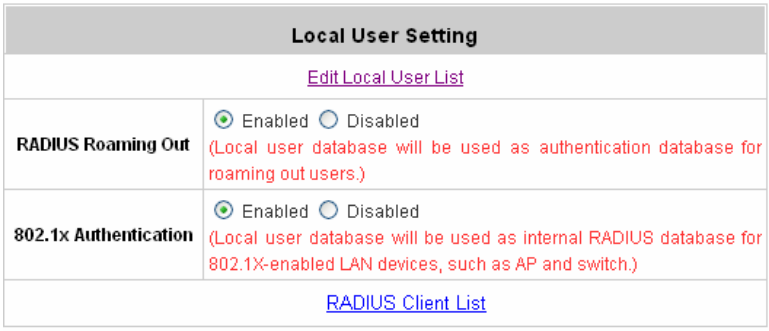
Del All: This will delete all users at once.

Delete: This will delete a specific user individually.

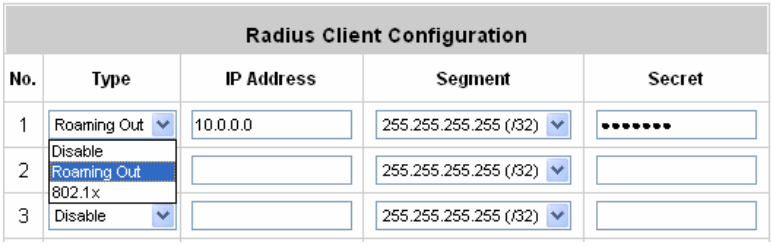
Edit User: If you want to edit the content of an individual user account, click the username of the desired user account to enter the **User Profile** page of the particular user, and then modify or add any desired information such as **Username**, **Password**, **MAC** (optional), **Policy** and **Remark** (optional). Then check **VPN Termination** to enable this function or not. Click ***Apply*** to complete the modification.



RADIUS Roaming Out / 802.1x Authentication: When enabled, local user may login to other connected external RADIUS clients. This system will act as RADIUS Server for that specific external RADIUS client. These 2 functions can be enabled or disabled by checking the radio buttons. Checking either of them makes the hyperlink of ***Radius Client List*** appear.



Click the hyperlink of ***Radius Client List*** to enter the **Radius Client Configuration** page. Choose the desired type, **Disable**, **Roaming Out** or **802.1x** and key in the related data and then click ***Apply*** to complete the configurations.

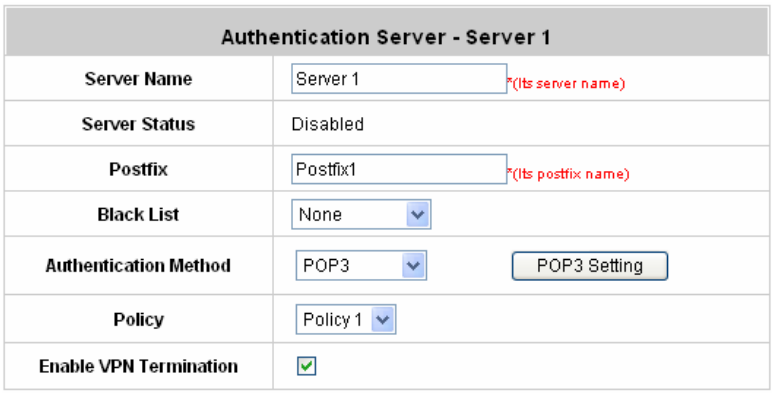


RADIUS Roaming Out: When **RADIUS Roaming Out** is enabled, local users can login from other domains by using their original local user accounts.

802.1x Authentication: 802.1x is a 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.

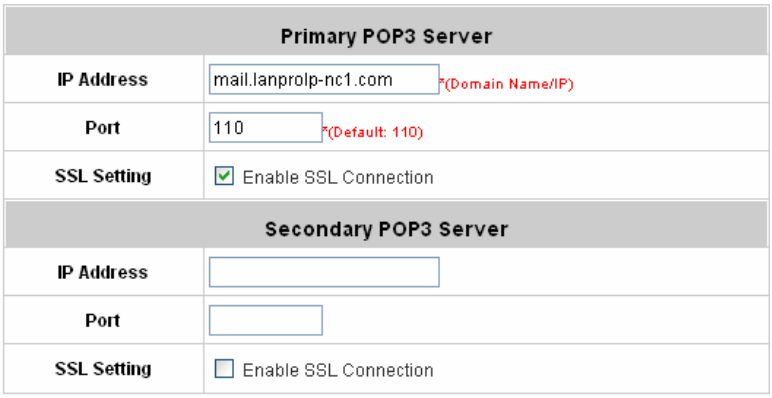
4.2.1.2 Authentication Method – POP3

This system may authenticate users using their POP3 email accounts. You may configure both primary and secondary POP3 server for fault tolerance. Choose **POP3** in the **Authentication Method** field, the button next to the drop-down menu will become ***POP3 Setting***.



Enable VPN Termination: Check to enable the VPN tunneling between client's device and the controller automatically to secure the transmissions for user under Windows XP SP1, SP2 and Windows 2000. Once the box is checked, it will be activated and applied to all users been authenticated by the selected authentication server.

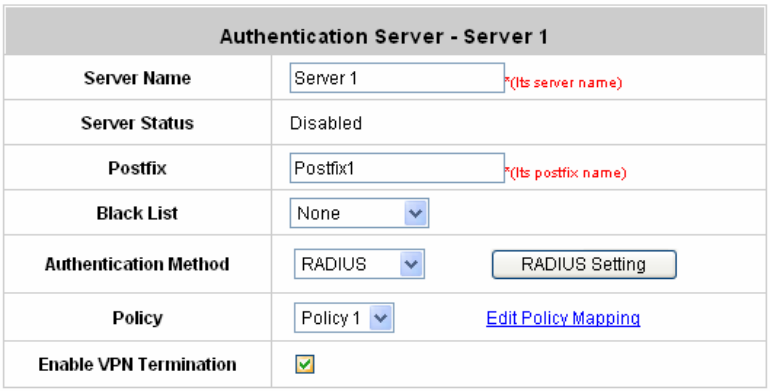
When **POP3**, **RADIUS**, **LDAP** or **NTDomain** is selected from the drop-down menu, the function of **Enable VPN Termination** will show up. Check **Enable VPN Termination** to enable this function. Click the hyperlink of ***POP3 Setting*** for further configuration. Enter the related information of the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisks are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



- **IP Address:** IP address of the POP3 server.
- **Port:** POP3 Server authentication port.
- **Enable SSL Connection:** Enable or disable Secured Socket Layer connection.

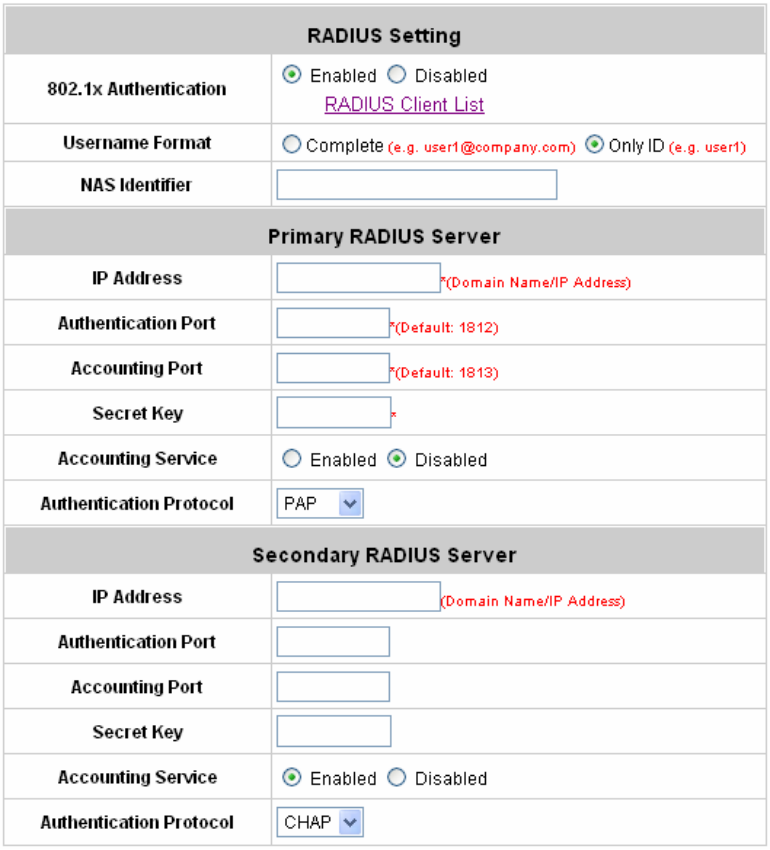
4.2.1.3 Authentication Method – RADIUS

The system may authenticate users using external RADIUS server. You may configure both primary and secondary RADIUS server for fault tolerance. Choose **RADIUS** in the **Authentication Method** field, the button next to the drop-down menu will become to ***RADIUS Setting***.



Enable VPN Termination: Check to enable the VPN tunneling between client's device and the controller automatically to secure the transmissions for user under Windows XP SP1, SP2 and Windows 2000. Once the box is checked, it will be activated and applied to all users been authenticated by the selected authentication server.

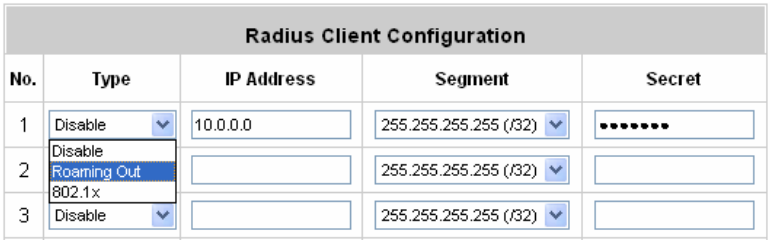
When **POP3**, **RADIUS**, **LDAP** or **NTDomain** is selected from the drop-down menu, the function of **Enable VPN Termination** will show up. Check **Enable VPN Termination** to enable this function. Click the button of ***RADIUS Setting*** for further configuration. Enter the related information of the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisks are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



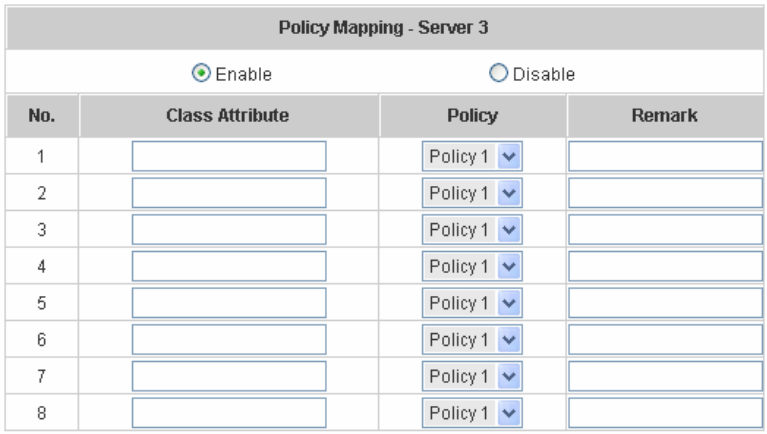
RADIUS Setting	
802.1x Authentication	Enabled Disabled RADIUS Client List
Username Format	Complete (e.g. user1@company.com) Only ID (e.g. user1)
NAS Identifier	
Primary RADIUS Server	
IP Address	*(Domain Name/IP Address)
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	Enabled Disabled
Authentication Protocol	PAP
Secondary RADIUS Server	
IP Address	(Domain Name/IP Address)
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	Enabled Disabled
Authentication Protocol	CHAP

- **802.1x Authentication:** When enabled, please click to edit "RADIUS Client List".
- **RADIUS Client List:** Configure RADIUS clients and secret key. Local user may login to any of the listed RADIUS clients as long as the RADIUS clients are configured accordingly.
- **Username Format:** When "Complete" option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when "Only ID" option is checked, only the username will be transferred to the external RADIUS server for authentication.
- **NASID:** The Network Access Server (NAS) Identifier of this system for the external RADIUS server.
- **IP Address:** IP address of the external RADIUS server.
- **Authentication Port:** Radius server authentication port.
- **Accounting Port:** RADIUS server accounting port.
- **Secret Key:** Secret Key for authentication.
- **Accounting Service:** Enable or Disable Accounting Service.
- **Authentication Protocol:** Define authentication transmission protocol. Configurations must match remote RADIUS configurations. PAP (Password Authentication Protocol) transmit password in plain text without encryption. CHAP (Challenge Handshake Authentication Protocol) is a more secured authentication protocol using hash encryption.

- **802.1X Authentication:** When enabling this function, the hyperlink of ***Radius Client List*** will appear. Click the hyperlink to get into the **RADIUS Client Configuration** page for further configuration. In the **RADIUS Client Configuration** page, the clients, which are using 802.1X as the authentication method, shall be put into this table. LANPRO LP-NC1 will forward the authentication request from these clients to the configured Radius Server.



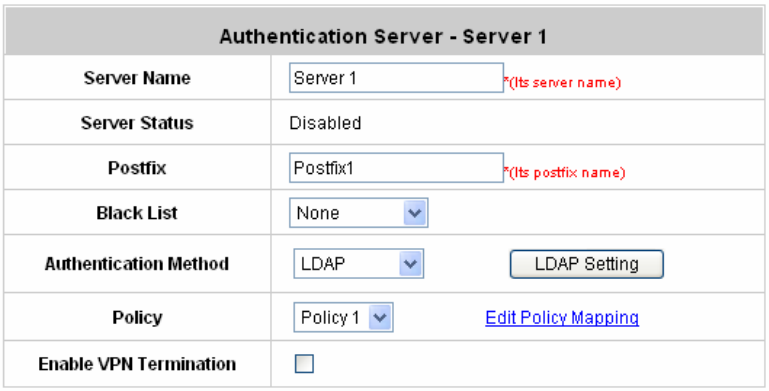
- **Trans Full Name:** When enabled, both the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to RADIUS server for authentication.
- **NAS Identifier:** Enter the NASID of the LANPRO LP-NC1 for the RADIUS server.
- **Server IP:** 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:** Choose to enable or disable the accounting service for accounting capabilities.
- **Authentication Protocol:** There are two methods, CHAP and PAP, for selection.
- **Edit Policy Mapping:** Click the hyperlink of **Edit Policy Mapping** to enter the **Policy Mapping** page. Choose to enable or disable policy mapping by RADIUS class attributes.



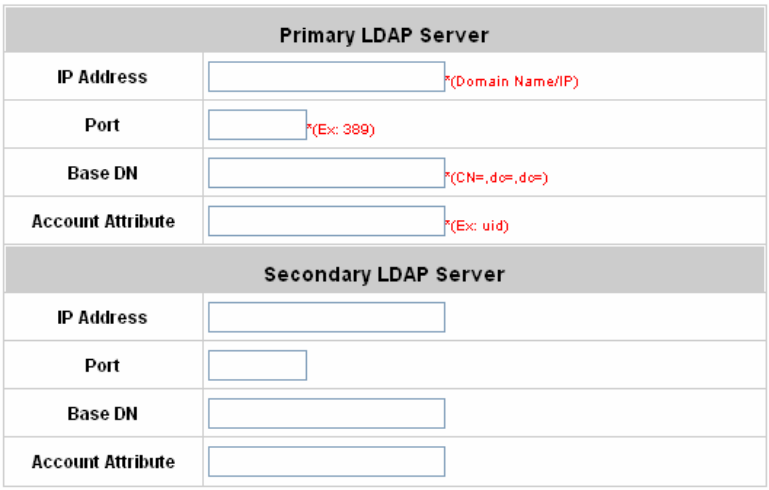
- **Class Attribute:** Class attribute sent from the RADIUS server.
- **Policy:** Select the mapping policy of this class attribute.
- **Remark:** Add some description if needed.

4.2.1.4 Authentication Method – LDAP

This system may authenticate users using external LDAP Server. You may configure both primary and secondary LDAP server for fault tolerance. Choose **LDAP** in the **Authentication Method** field, the button next to the drop-down menu will become to **LDAP Setting**.



When **POP3**, **RADIUS**, **LDAP** or **NTDomain** is selected from the drop-down menu, the function of **Enable VPN Termination** will show up. Check **Enable VPN Termination** to enable this function. Click the button of **LDAP Setting** for further configuration. Enter the related information of the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisks are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



- **IP Address:** Server IP Address**.** 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 for the navigation path of LDAP account.
- **Account Attribute:** Enter the account attribute of the LDAP server.
- **Edit Policy Mapping:** Click the hyperlink of **Edit Policy Mapping** to enter the **Policy Mapping** page. Choose to enable or disable policy mapping by LDAP class attributes.

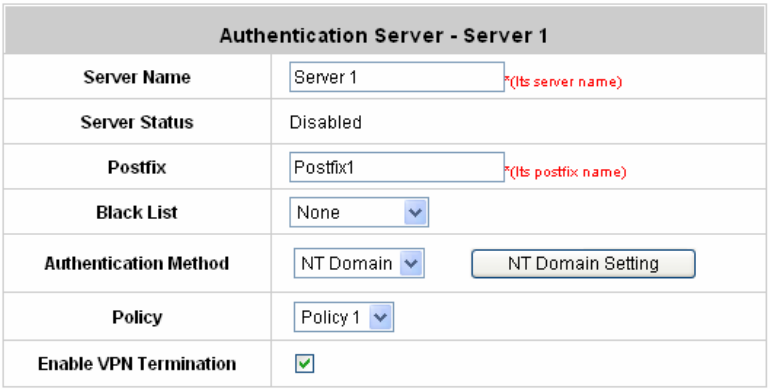
LDAP Policy Mapping - Server 1

◉ Enable ○ Disable

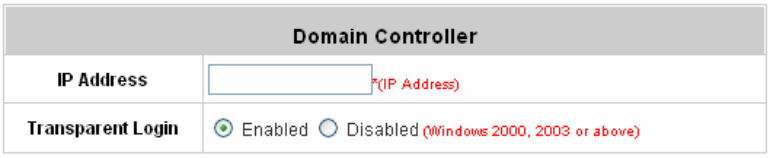
No.	LDAP Attribute Name	LDAP Attribute Value	Policy	Remark
1			Policy 1	
2			Policy 1	

4.2.1.5 Authentication Method – NT Domain

The system may authenticate users using external NT Domain Server. Choose **NTDomain** in the **Authentication Method** field, the button next to the drop-down menu will become to ***NTDomain Setting***.



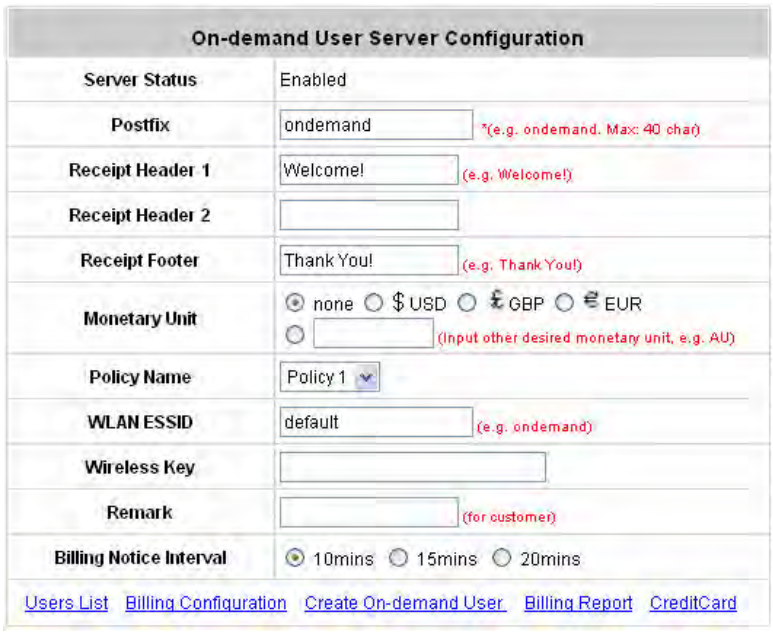
When **POP3**, **RADIUS**, **LDAP** or **NTDomain** is selected from the drop-down menu, the function of **Enable VPN Termination** will show up. Check **Enable VPN Termination** to enable this function. Click the button of ***NT Domain Setting*** for further configuration. Enter the related information of the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisks are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



- **IP address:** Server IP Address. Enter the server IP address of the NT Domain Server
- **Transparent Login:** Enable this option for transparent user login to NT Domain (login once only). If the function is enabled, users will log into the system automatically when they log into the Windows domain and the IP of NT Domain Server should be added into walled garden.

4.2.1.6 Authentication Method – On-demand User

When the customers need to use wireless Internet service in stores, they have to get printed receipts with usernames and passwords from the store to log in the system for wireless access. There are 2000 On-demand User accounts available.



Server Status: The status shows that the server is enabled or disabled.

Postfix: Set a postfix that is easy to identify (e.g. Local) for the server by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters 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.

Monetary Unit: Select or enter the desired monetary unit.

Policy Name: Select a policy for the on-demand user.

WLAN ESSID: Enter the ESSID of APs.

Wireless Key: Enter the Wireless key of APs.

Remark: Enter any additional information that will appear at the button of the receipt.

Billing Notice Interval: While an on-demand user is still logged in, the system will update the billing notice of the login success page by the time interval defined here.

Users List: Currently available user list.

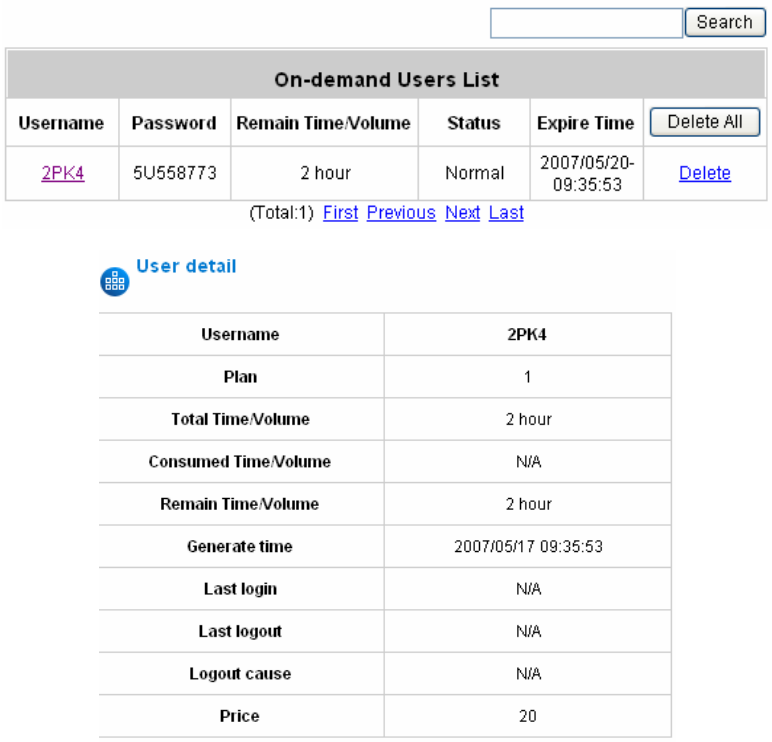
Billing Configuration: Setup different billing plans.

Create On-demand User: On-demand user creation page.

Billing Report: Summary report for on-demand account usage.

4.2.1.6.1 User List

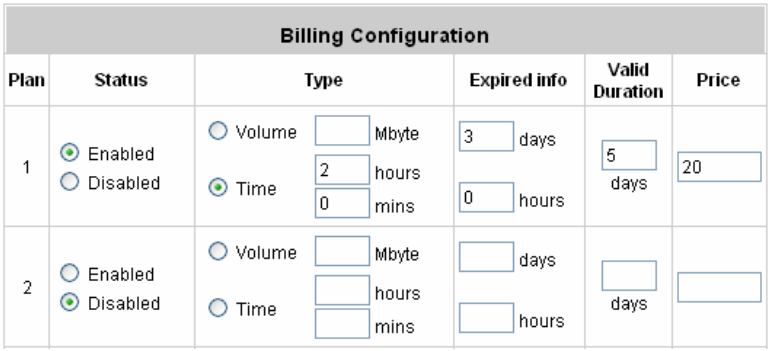
Click to enter the **On-demand Users List** page. In the **On-demand Users List**, detailed information will be shown here.



- **Search:** Enter a keyword of a username to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the on-demand user.
- **Password:** The login password of the on-demand user.
- **Remain Time/Volume:** The total time/Volume that the user still can use currently.
- **Status:** The status of the on-demand 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.
- **Expire Time:** The expiration time of the account.
- **Delete All:** This will delete all users at once.
- **Delete:** This will delete a specific user individually.

4.2.1.6.2 Billing Configuration

Click this to enter the **Billing Configuration** page. In the **Billing Configuration** page, the administrator may configure up to 10 plans.



Billing Configuration

Plan	Status	Type	Expired info	Valid Duration	Price
1	◉ Enabled ○ Disabled	○ Volume [ ] Mbyte ◉ Time [2] hours [0] mins	[3] days [0] hours	[5] days	[20]
2	○ Enabled ◉ Disabled	○ Volume [ ] Mbyte ○ Time [ ] hours [ ] mins	[ ] days [ ] hours	[ ] days	[ ]

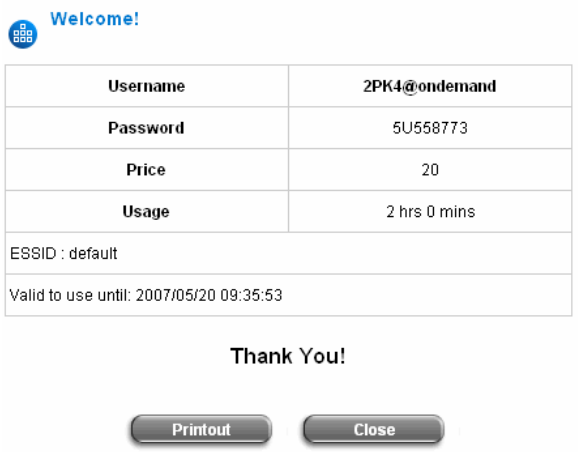
- **Plan:** The ID of a specific billing configuration.
- **Status:** Select to enable or disable this plan.
- **Type:** Quota type (time or data volume). Set the billing plan by **"Volume"** (the maximum volume allowed is 9999999 Mbytes) or **"Time"** (the maximum time allowed is 999 hours and 59 minutes).
- **Expired info:** A period of time in which the account must be activated after it is created. This is the duration of time that the user needs to activate the account after the generation of the account. If the account is not activated during this duration, the account will self-expire.
- **Valid Duration:** Account life time after it is activated. This is the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expire.
- **Price:** Account price. The price charged for this billing plan.

4.2.1.6.3 Create On-demand User

Click this to enter the **Create On-demand User** page.

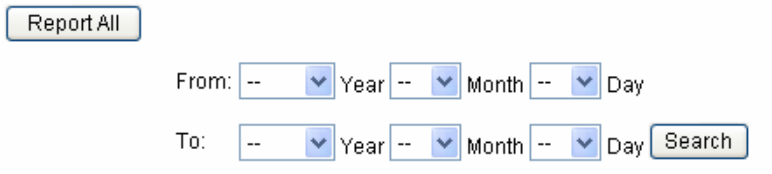
Create On-demand User				
Plan	**Type**	**Price**	**Status**	**Function**
1	2 hrs 0 mins	20	Enabled	Create
2	N/A	N/A	Disabled	Create
3	N/A	N/A	Disabled	Create

Pressing the ***Create*** button for the desired plan, an on-demand user will be created, then click ***Printout*** to print a receipt which will contain this on-demand user's information. There are 2000 on-demand user accounts available.

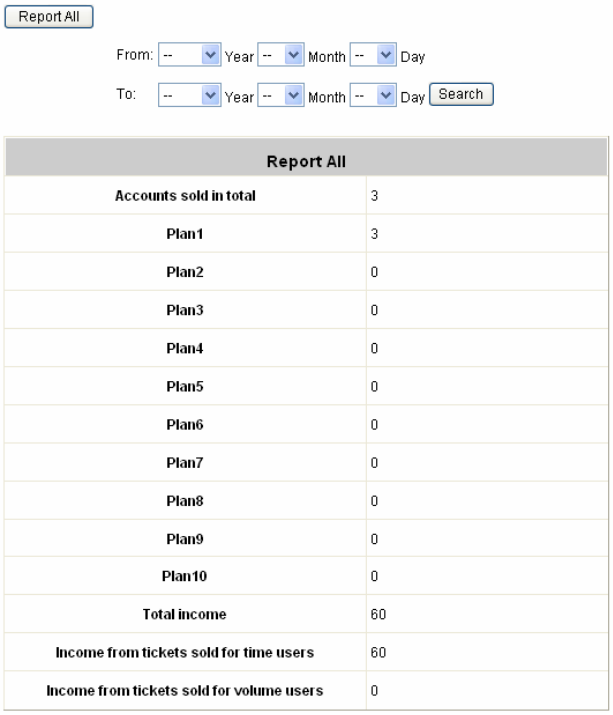


4.2.1.6.4 Billing Report

Click this to enter the **On-demand users Summary report** page. In **On-demand users Summary report** page, the administrator can get a complete report or a report within a particular period.

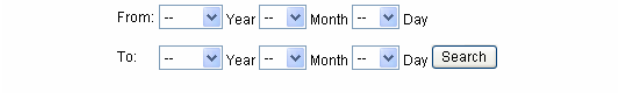


- **Report All:** Click this to get a complete report including all the on-demand records. This report shows the total expenses and individual accounting of each plan for all plans available.



Report All	
Accounts sold in total	3
Plan1	3
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	60
Income from tickets sold for time users	60
Income from tickets sold for volume users	0

- **Search:** Select a time period to get a periodical report. The report tells the total expenses and individual accounting of each plan for all plans available for that period of time.



Report from 2006/01/01 ~ 2007/04/15	
Accounts sold in total	2
Plan1	2
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	40
Income from tickets sold for time users	40
Income from tickets sold for volume users	0

4.2.1.6.5 Credit Card

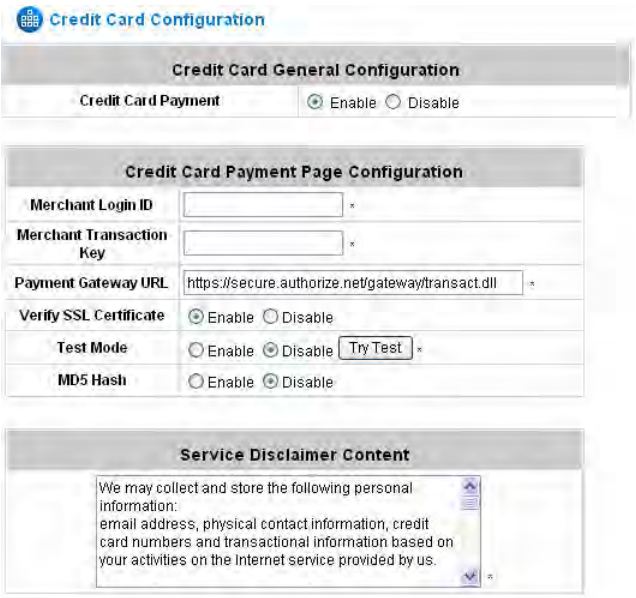
Click this to enter the **Credit Card Configuration** page.

This section is about how independent HotSpot owners can enable the credit card payment function, making the HotSpot an e-commerce environment for end users to pay for and get Internet access using their credit cards. Before the "Credit Card" and related functions can be managed appropriately, LANPRO LP-NC1 requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that LANPRO LP-NC1 supports now. Please see ***Appendix B. The Configuration on Authorize.Net*** to setup an Aurthourize.Net account and other necessary information.

After getting an Authorize.Net account, set the following configuration in Credit Card Configuration of LANPRO LP-NC1.

- **Credit Card General Configuration**

  Credit Card Payment: Enable or disable credit card payment as a method for customers to purchase on-demand accounts.



- **Credit Card Payment Page Configuration**

  Merchant Login ID: Administrator needs this ID from the online payment system/organization before cooperating with each other in transactions.

  Merchant Transaction Key: Administrator needs this key from the online payment system/organization before cooperating with each other in transactions.

  Payment Gateway URL: The URL of the online payment system/organization in order to process the transactions.

  Verify SSL Certificate: ***Secure Sockets Layer***, a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt

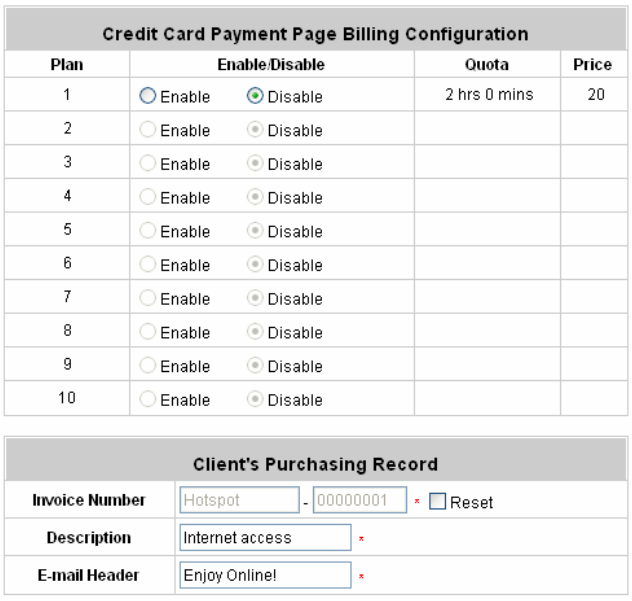
data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Test Mode: When the test mode is enabled, "Try Test" button can be clicked to input some information and test if the information will go through without really sending out the information and being charged.

MD5 Hash: This feature enhances the network security when transferring customers' inputted data from this gateway to the online payment system/organization. The hash value must be both implemented in online payment system/organization and this gateway.

- **Service Disclaimer Content**

  View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.



Credit Card Payment Page Billing Configuration

Plan	Enable/Disable	Quota	Price
1	Enable Disable	2 hrs 0 mins	20
2	Enable Disable		
3	Enable Disable		
4	Enable Disable		
5	Enable Disable		
6	Enable Disable		
7	Enable Disable		
8	Enable Disable		
9	Enable Disable		
10	Enable Disable		

Client's Purchasing Record

Invoice Number	Hotspot - 00000001 * Reset
Description	Internet access *
E-mail Header	Enjoy Online! *

- **Credit Card Payment Page Billing Configuration**

  These 10 plans are the plans in **Billing Configuration**, and desired plan can be enabled.

- **Client's Purchasing Record**

  Invoice Number: An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any format of information.

  Description: Some remarks can be made here for the transaction.

  Email Header: What appears as the header of the email sent to customers.

Credit Card Payment Page Fields Configuration

Item	Displayed Text	Required
☑ Credit Card Number	Credit Card Number *	☑
☑ Credit Card Expiration Date	Credit Card Expiration Date *	☑
☑ Card Type	Card Type * ☑ Visa ☑ American Express ☑ Master Card ☑ Discover	☑
☑ Card Code	Card Code *	☑
☑ E-mail	E-mail *	☐
☐ Customer ID	Room Number *	☐
☑ First Name	First Name *	☑
☑ Last Name	Last Name *	☑
☑ Company	Company *	☐
☑ Address	Address *	☐
☑ City	City *	☐
☑ State	State *	☐
☑ Zip	Zip *	☐
☑ Country	Country *	☐
☑ Phone	Phone *	☐
☑ Fax	Fax *	☐

*Displayed text fileds must be filled.

- **Credit Card Payment Page Fields Configuration:** These are features from which administrator can choose to appear for customers to fill in credit card information page when customers want to purchase on-demand accounts. Administrator can also make certain fields mandatory to be filled in.

  Display: Check the box to show this item on the customer's payment interface.

  Item: Enter what needs to be shown for this field.

  Required: Check the box to indicate this item as a required field.

  Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

  Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in the format of MMYY. For example, an expiration date of July 2005 should be entered as 0705.

  Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

  Card Code: The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

  Email: An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

  Customer ID: This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any format of information.

  First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

  Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

  Company: The name of the company associated with the billing or shipping information entered on a given transaction.

  Address: The address entered either in the billing or shipping information of a given transaction.

  City: The city is associated with either the billing address or shipping address of a transaction.

  State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

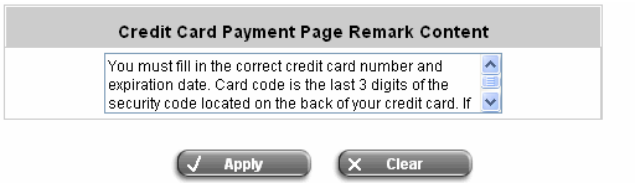
  Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

  Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

  Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

  Fax: A fax number may be associated with the billing information of a transaction. This number may be

entered as all number or contain parentheses and dashes to separate the area code and number.

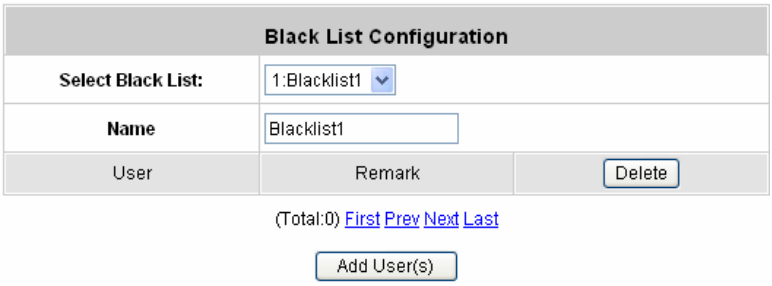


- **Credit Card Payment Page Remark Content**

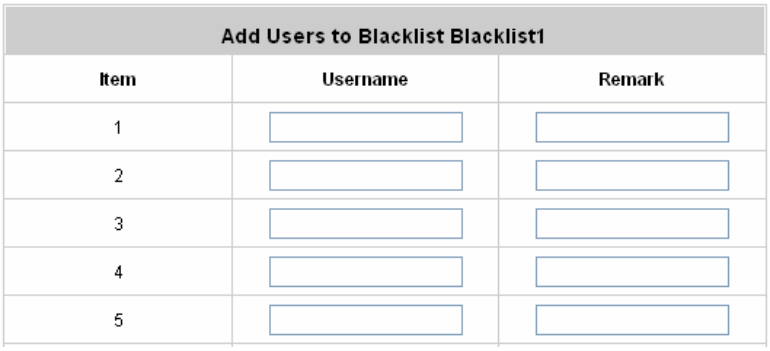
  Some reminder/notice that can appear in customer's credit card information page. Administrator can choose to use the default credit card payment note or write a new one to suit the current circumstances better.

4.2.2 Black List Configuration

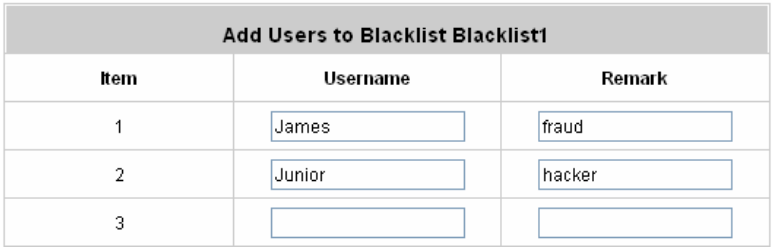
The administrator can add, delete, or edit the black list for user access control. System supports up to 5 Black Lists. Each Black List contains up to 40 user accounts. The user accounts may not access network. If a user in the black list wants to log into the system, the user's access will be denied. The administrator can use the pull-down menu to select the desired black list to edit adding users into the black list.



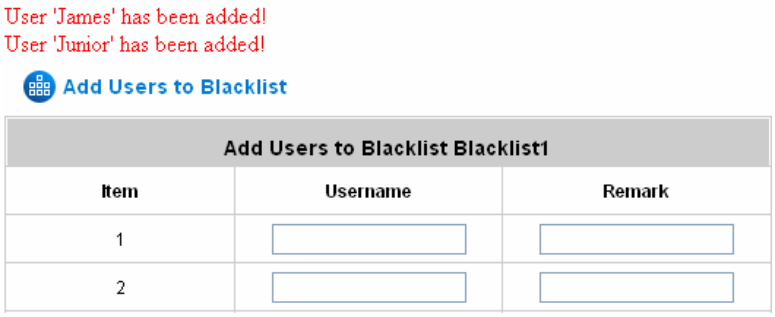
- **Select Black List:** There are 5 lists that LANPRO LP-NC1 supports to select from. Each list configures up to 10 items.
- **Name:** Set the name of the black list and it will show in the pull-down menu above.
- ***Add Users*:** Click the button of ***Add Users***, the **Add Users to Blacklist** page will appear for adding users to the selected black list.



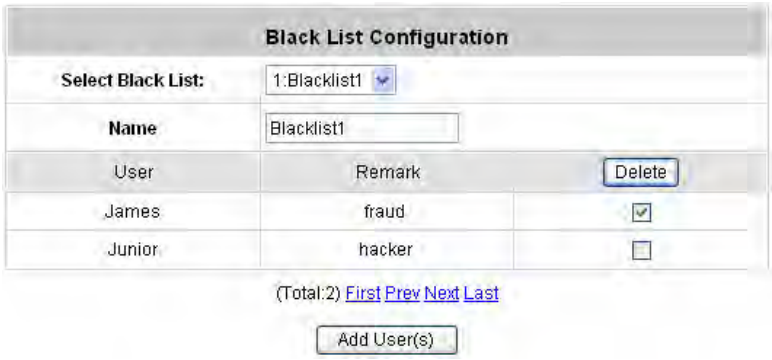
After entering the usernames in the **Username** field and the related information in the **Remark** field (not required).



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



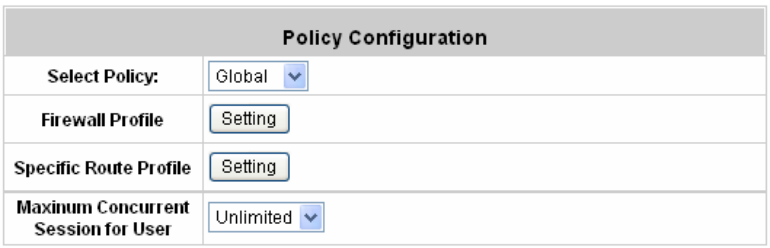
If the administrator wants to remove a user from the black list, just select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.



4.2.3 Policy Configuration

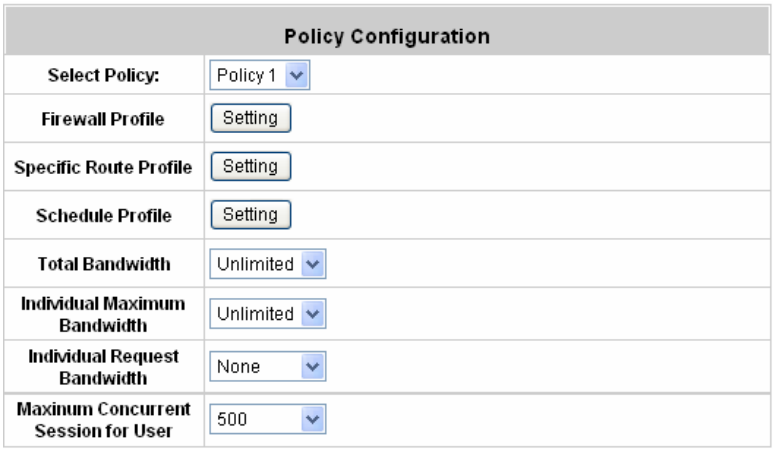
There is one Global policy and eight other policies. Every **Policy** has three different network related access **profiles** and **bandwidth** control for that policy. Each policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as **Bandwidth** settings such as **Total Bandwidth**, **Individual Maximum Bandwidth**, and **Individual Request Bandwidth** for that policy. **Global** policy is the system's universal policy, where the **Firewall Profile** and **Specific Route Profile** are set and applied to all users. The other eight policies are configured by the users in the section of Authentication Configuration in the screen of Authentication Server. Once a policy is configured (Policy 1, Policy 2,.., Policy 8), with the combinations of Firewall, Specific Route, Schedule, Total Bandwidth, Individual Maximum Bandwidth and Individual Request Bandwidth profiles, administrator may assign one policy to one user group according to selected Authentication method. Different user groups may share the same policy.

4.2.3.1 Global Policy



- **Select Policy:** Select **Global** to set the **Firewall Profile**, **Specific Route Profile** and **Maximum Concurrent Session for User**.
- **Firewall Profile:** Click the button of Setting for Firewall Profile, the Firewall Profiles list will appear. Click the numbers of Filter Rule Item to edit individual rules and click Apply to save the settings. The rule status will show on the list. Check "Active" to enable that rule.
- **Specific Route Profile:** When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Maximum Concurrent Session for User:** Concurrent Session for each user, it can be restricted by administrator.

4.2.3.2 Policy 1~8

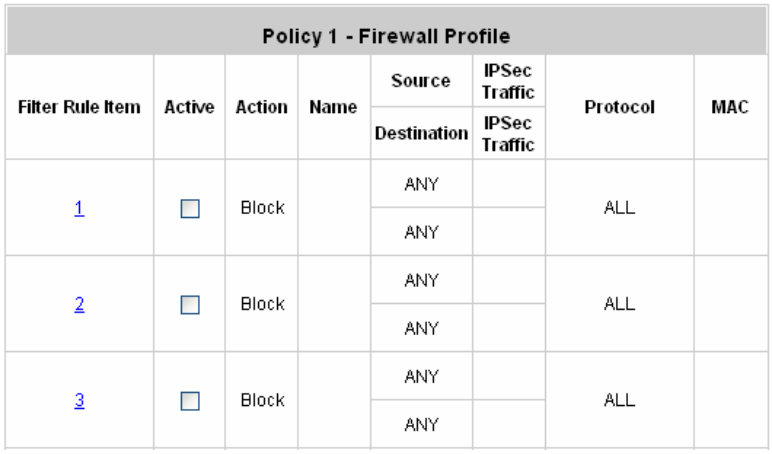


- **Select Policy:** Select **Policy1~8** to set the **Firewall Profile**, **Specific Route Profile, Schedule Profile, Total Bandwidth, Individual Maximum Bandwidth, Individual Request Bandwidth** and **Maximum Concurrent Session for User**.
- **Firewall Profile:** Define up to 10 firewall rules.
- **Specific Route Profile:** Define up to 10 static routes.
- **Schedule Profile:** Define allowed access hours.
- **Total Bandwidth:** Define maximum bandwidth allowed of the total bandwidth shared by the users within the same policy.
- **Individual Maximum Bandwidth:** Define maximum bandwidth allowed for individual user, the individual maximum bandwidth can not exceed the value of Total Bandwidth.
- **Individual Request Bandwidth:** Define the guaranteed minimum bandwidth for individual user, the minimum bandwidth can not exceed the setting value of Total Bandwidth and Individual Maximum Bandwidth.
- **Maximum Concurrent Session for User:** Concurrent sessions for each user, it can be restricted by administrator.

- **Firewall Profile**

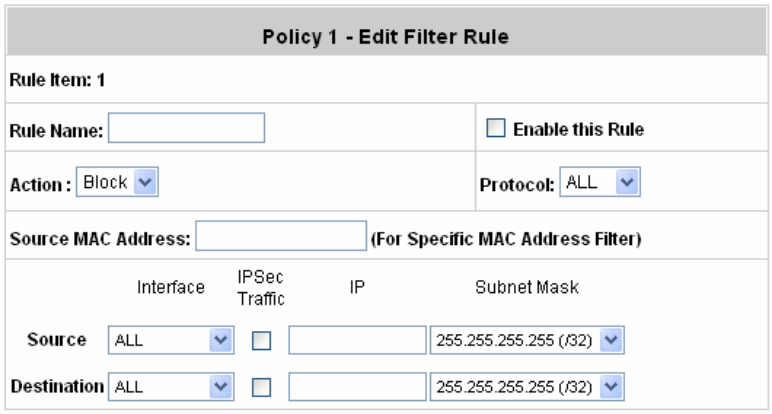
  Click the button of ***Setting*** for **Firewall Profile**, the **Firewall Profile** page will appear. Click the numbers of ***Filter Rule Item*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **Active** to enable that rule.

Attention: Filter Rule Item 1 is the highest priority, Filter Rule Item 2 is the second priority, and so on.



Policy 1 - Firewall Profile

Filter Rule Item	Active	Action	Name	Source / Destination	IPSec Traffic	Protocol	MAC
1	☐	Block		ANY / ANY		ALL	
2	☐	Block		ANY / ANY		ALL	
3	☐	Block		ANY / ANY		ALL	



Policy 1 - Edit Filter Rule

Rule Item: 1

Rule Name: ☐ Enable this Rule

Action : Block Protocol: ALL

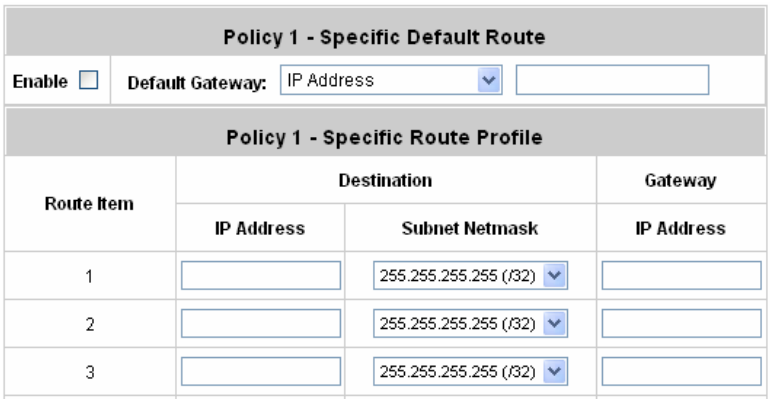
Source MAC Address: (For Specific MAC Address Filter)

	Interface	IPSec Traffic	IP	Subnet Mask
Source	ALL	☐		255.255.255.255 (/32)
Destination	ALL	☐		255.255.255.255 (/32)

- **Rule Item:** This is the rule selected.
- **Rule Name:** The rule name can be changed here. The rule name can be set to easily identify, for example: ***"from file server"***, ***"HTTP request"*** or ***"to web"***, etc.
- **Enable this Rule:** After checking this function, the rule will be enabled.
- **Action:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.
- **Protocol:** There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.
- **Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.
- **IPSec Traffic:** Check the check box will only filter the traffic with IPSec.
- **Source/Destination Interface:** There are four interfaces to choose, **ALL, WAN1**, **WAN2**, **Controlled Port** and **Uncontrolled Port**.
- **Source/Destination IP:** Enter the source and destination IP addresses.
- **Source/Destination Subnet Mask:** Enter the source and destination subnet masks.
- **Source/Destination Start/End Port:** Enter the range of source and destination ports.

• **Specific Route Profile**

Click the button of ***Setting*** for **Specific Route Profile**, the **Specific Default Route and Specific Route Profile** page will appear.

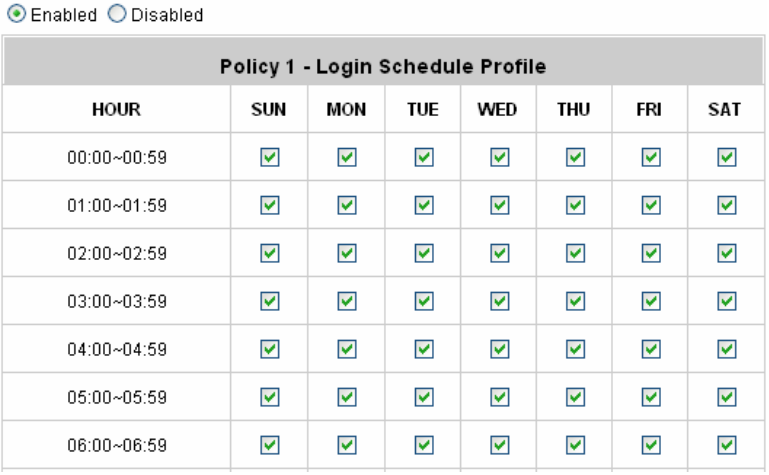


Specific Default Route:

- **Enable:** Click to enable the setting of specific default route.
- **Default Gateway:** There are 3 methods of the default gateway that ***Specific Default Route*** supports.
- **Destination IP Address:** The destination IP address of the host or the network.
- **Destination Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **Gateway IP Address:** The IP address of the gateway or the router to the destination.

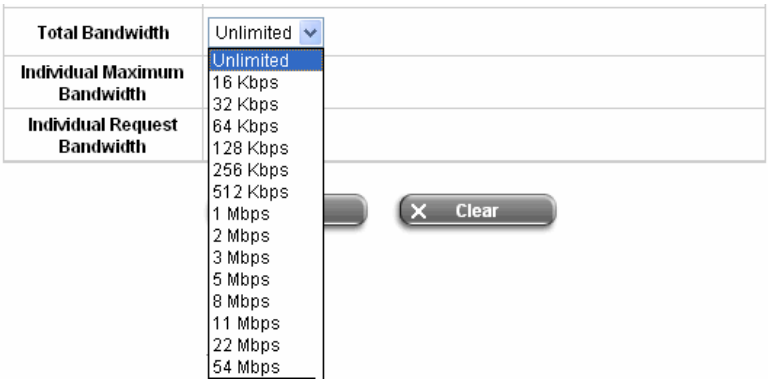
- **Schedule Profile**

  Click the button of ***Setting*** for **Schedule Profile** to enter the Schedule Profile list. Select **Enable** to show the list. This function is used to restrict the time for users to log in. Please enable/disable the desired time slot and click ***Apply*** to save the settings. These settings will become effective immediately after clicking the ***Apply*** button.



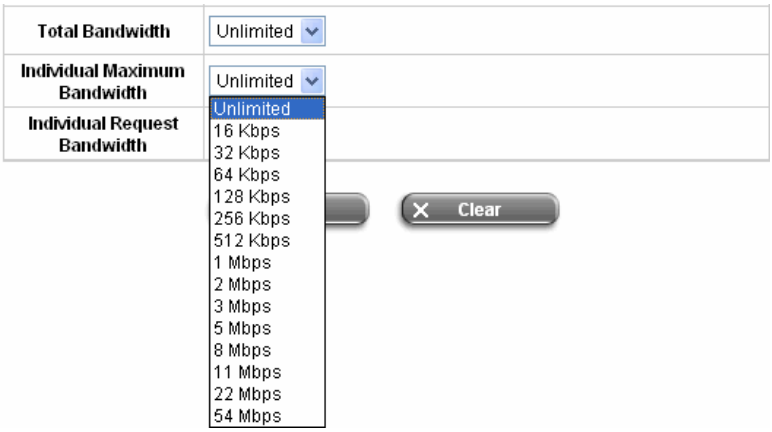
- **Total Bandwidth**

  Select the bandwidth from the drop-down menu. It's the total bandwidth the users under this particular policy need to share.



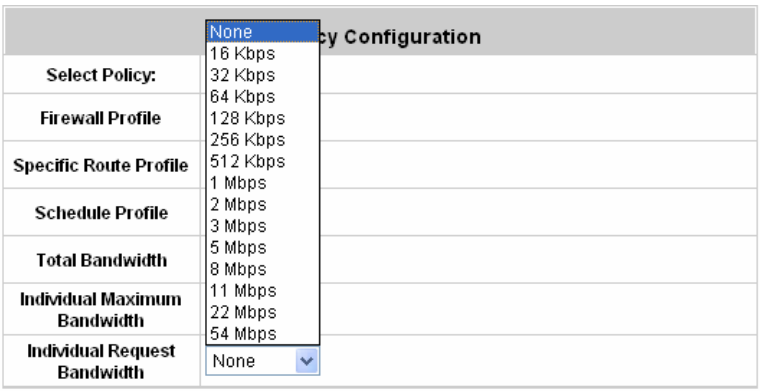
- **Individual Maximum Bandwidth**

  Select the bandwidth from the drop-down menu. It's the most bandwidth an individual user can obtain under this particular policy, which cannot exceed the value for **Total Bandwidth**.



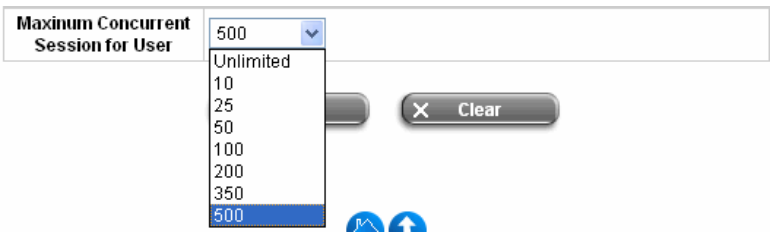
- **Individual Request Bandwidth**

  Select the bandwidth from the drop-down menu. It's the requested bandwidth for a user under this particular policy, which cannot exceed the value for **Individual Maximum Bandwidth**.



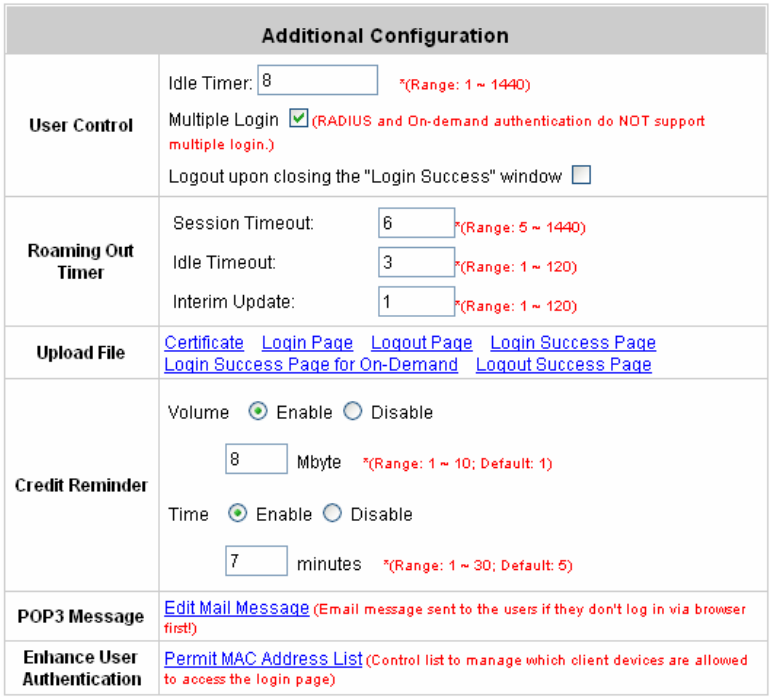
- **Maximum Concurrent Session for User:** The concurrent sessions for each user, it can be restricted by administrator. Use the drop-down list to select the maximum number of concurrent sessions which is allowed to be established by each user.

  Note: For more information, please refer to ***Appendix H. Session Limit and Session Log***.



4.2.4 Additional Configuration

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



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

  Idle Timer: Define user's idle time-out value. 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: Enable or disable multiple logins on a single user account. This function is not valid for On-demand Account and RADIUS Account.

  Logout upon closing the "Login Success" window: When enabled, there will be a new popup window to confirm if users are sure to logout the system when users try to close the login success page in case users close it by accident.

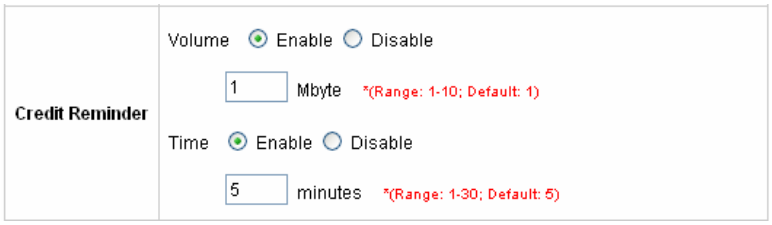
- **Roaming Out Timer**

  Session Timeout: Maximum session timeout.

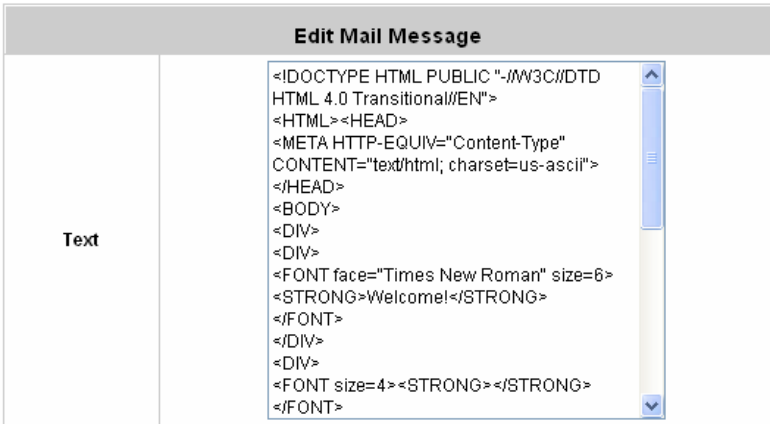
  Idle Timeout: Maximum idle timeout.

  Interim Update: Constant records update time interval.

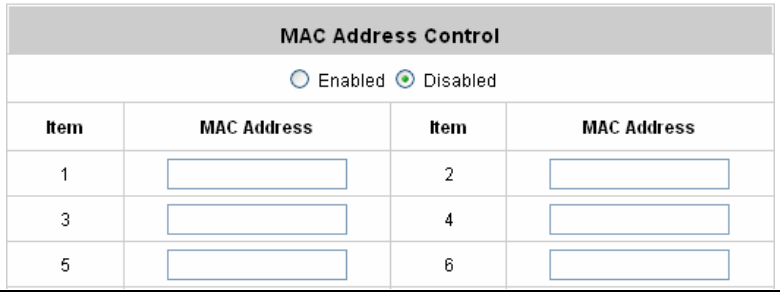
- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.



- **POP3 Message:** If a user tries to retrieve mail from POP3 mail server before login, the users will receive a welcome mail from LANPRO LP-NC1. The administrator can edit the content of this welcome mail.



- **Enhance User Authentication:** With this function enabled, only the users with their MAC addresses in this list can log into LANPRO LP-NC1. There will only be 40 users allowed in this MAC address list. User authentication is still required for these users. Please click the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



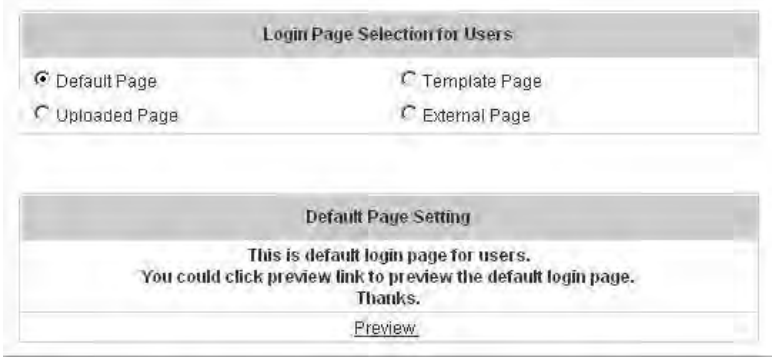
Caution: The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

- **Upload File:** The system allows great customization on end-user interface. Administrators may upload device certificate, customized login, and logout web-pages.
  1. **Certificate:** The administrator can upload new private key and customer certification. Click the ***Browse*** button to select the file for the certificate upload. Then click ***Submit*** to complete the upload process.

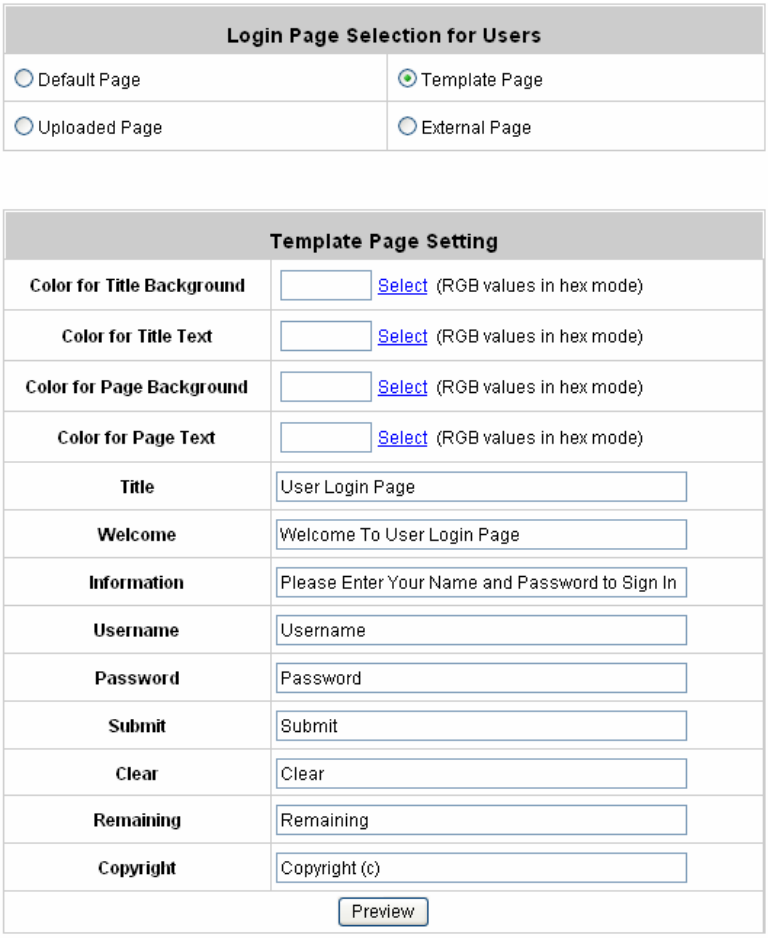
Click ***Use Default Certificate*** to use the default certificate and key.

2. **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, you can click ***Preview*** to see the login page.

   a. Choose ***Default Page*** to use the default login page.



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



c. Choose ***Uploaded Page*** and upload a login page. Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

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

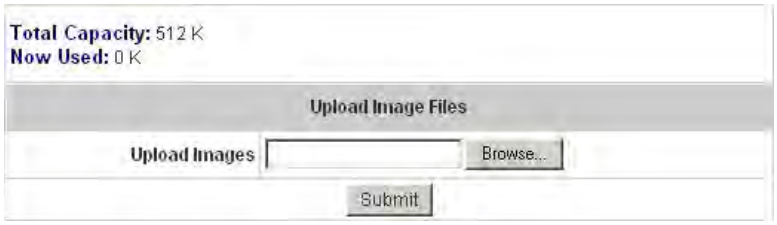
The user-defined login page must include the following HTML codes to provide the necessary fields for username and password.

```
<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 you will upload.

<img src="images/xx.jpg">

Then, enter or browse the filename of the images to upload 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.

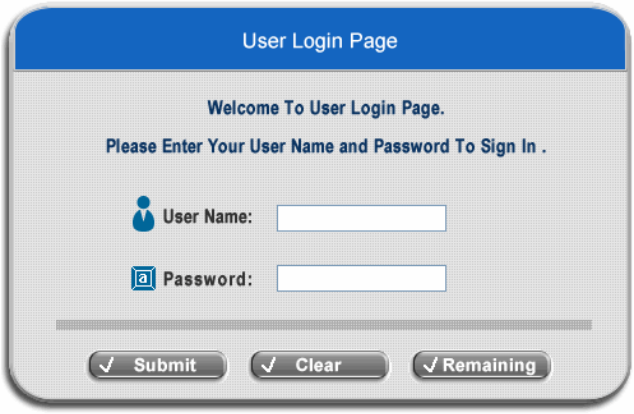
In LANPRO LP-NC1, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

For more details about the codes of the disclaimer, please refer to Appendix G.

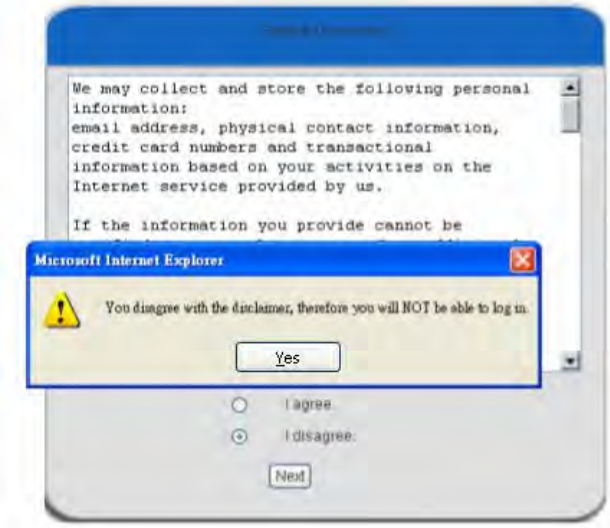
If the page is successfully loaded, an **upload success** page will show up.

"Preview" can be clicked to see the uploaded page.

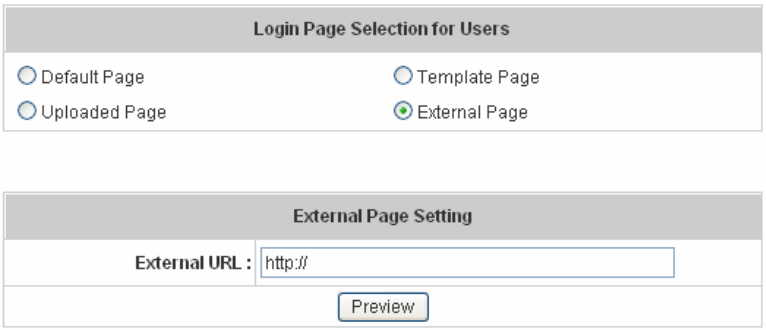
If a user checks **"I agree"** and clicks ***Next***, then he/she is prompted to fill in the login name and password.



If a user checks **"I disagree"** and clicks ***Next***, a window will pop up to tell user that he/she cannot log in



d. Choose the ***External Page*** selection and get the login page from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***.



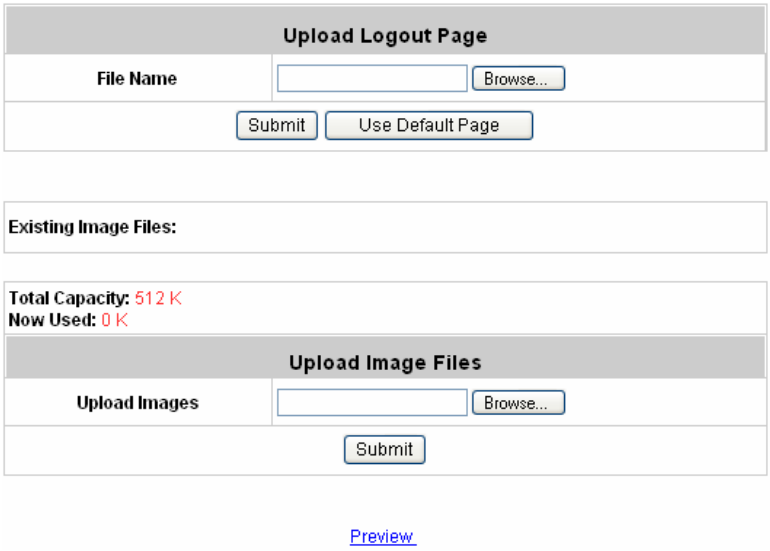
After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

Please note that:

```
<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>
```

The above is needed in your HTML code to make sure the page works correctly.

3. **Logout Page:** The administrator can apply customized logout page here. The process is similar to that of Login Page.

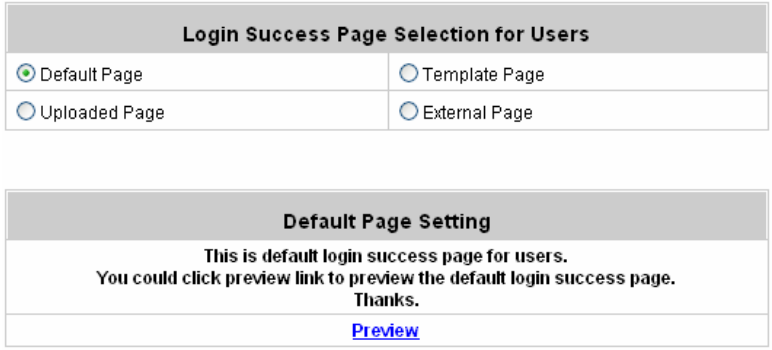


The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the user-defined login user interface can be previewed by clicking ***Preview*** at the bottom of this page. If want to restore the factory default setting of the logout interface, click the "**Use Default Page"** button.

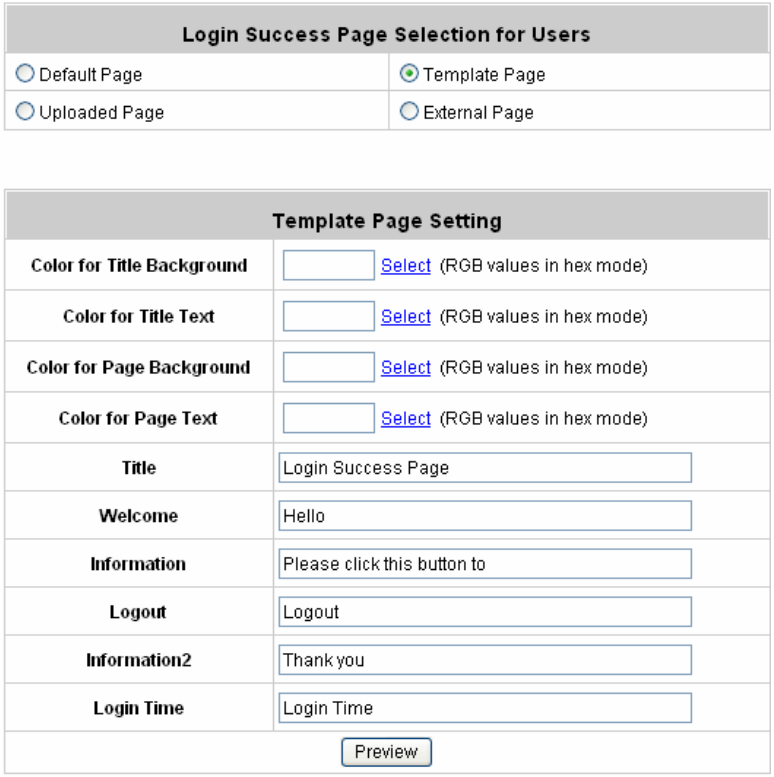
```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

4. **Login Success Page:** The administrator can use the default login success page or get the customized login success page by setting the template page, uploading the page or using the external website. After finishing the setting, you can click ***Preview*** to see the login success page.

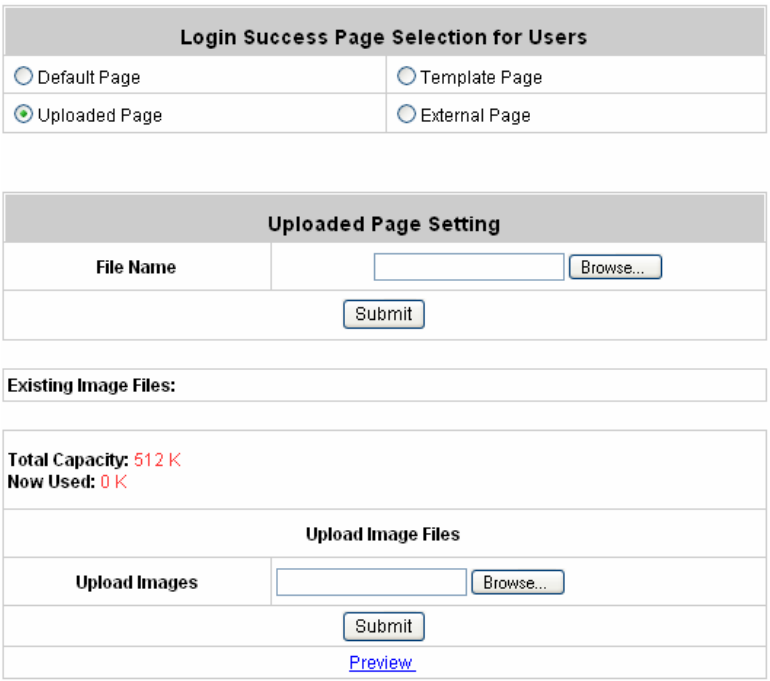
   a. Choose ***Default Page*** to use the default login success page.



b. Choose ***Template Page*** to make a customized login success page here. Click ***Select*** to pick up a color and then fill in all of the blanks. You can click ***Preview*** to see the result first.



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

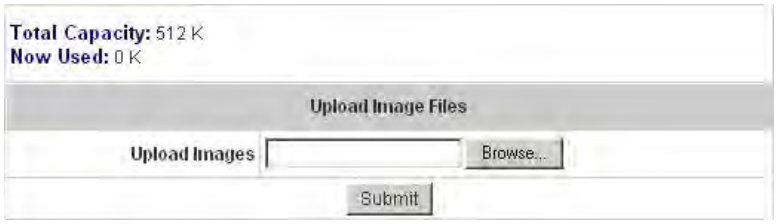


After the upload process is completed, the new login success page can be previewed by clicking ***Preview*** button at the bottom.

If the user-defined login success page includes an image file, the image file path in the HTML code must be the image file you will upload.

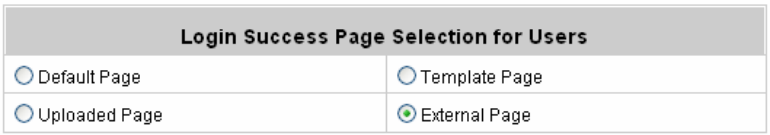
```
<img src="images/xx.jpg">
```

Then, enter or browse the filename of the images to upload 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 success page, click the ***Use Default Page*** button to restore it to default.

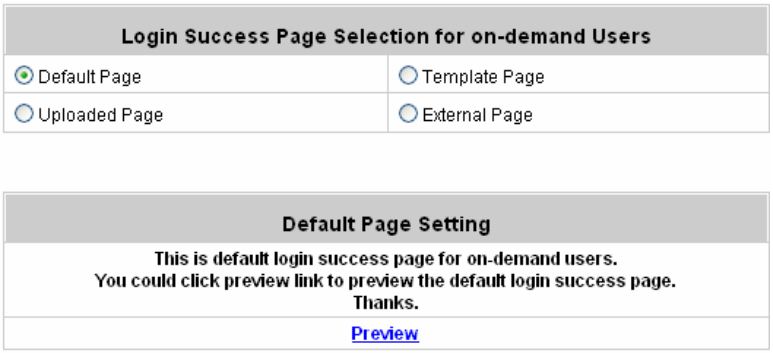


After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

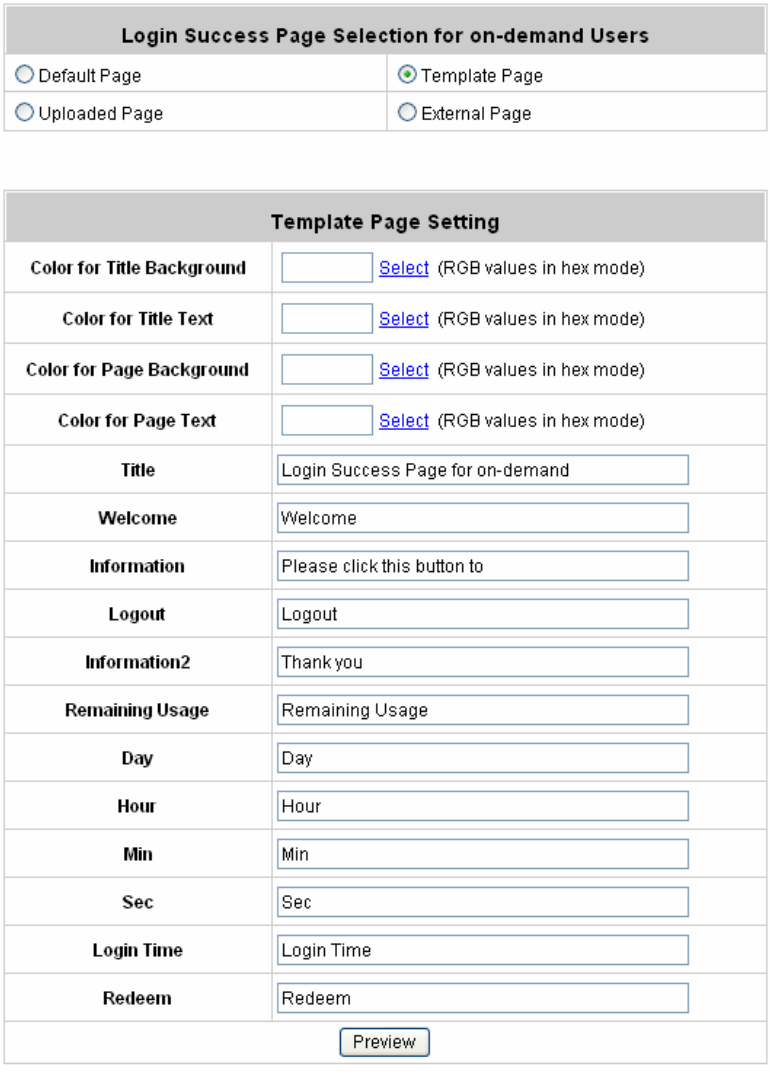
d. Choose the ***External Page*** selection and you can get the login success page e from the specific website. Enter the website address in the **External Page Setting** field and then click ***Apply***. After applying the setting, the new login success page can be previewed by clicking ***Preview***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



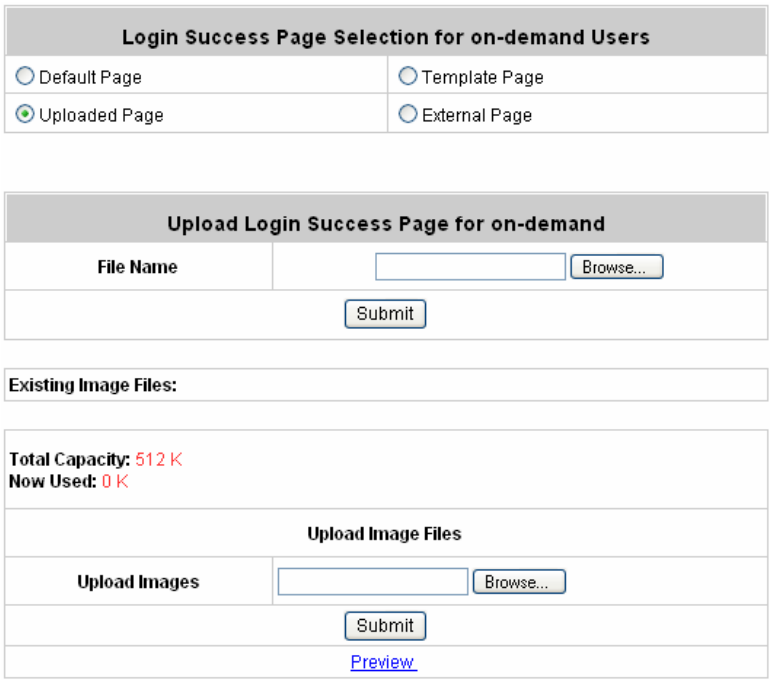
5. **Login Success Page for On-Demand:** The administrator can use the default login success page for On-Demand or get the customized login success page for On-Demand by setting the template page, uploading the page or using the external website. After finishing the setting, you can click ***Preview*** to see the login success page for On-Demand.
   a. Choose ***Default Page*** to use the default login success page for On-Demand.



   b. Choose ***Template Page*** to make a customized login success page for On-Demand here. Click ***Select*** to pick up a color and then fill in all of the blanks. You can click ***Preview*** to see the result first.



c. Choose ***Uploaded Page*** and you can get the **Login Success Page Section for On-Demand Users**. Click the ***Browse*** button to select the file for the login success page for On-Demand. Then click ***Submit*** to complete the upload process.

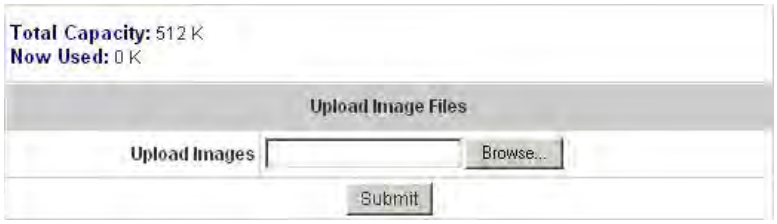


After the upload process is completed, the new login success page for On-Demand can be previewed by clicking ***Preview*** button at the bottom.

If the user-defined login success page for On-Demand includes an image file, the image file path in the HTML code must be the image file you will upload.

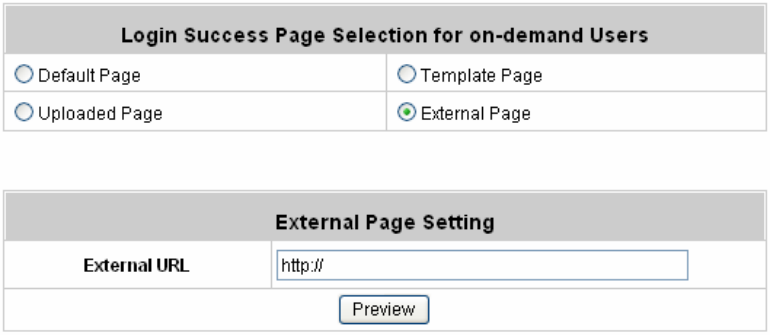
```
<img src="images/xx.jpg">
```

Then, enter or browse the filename of the images to upload 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.



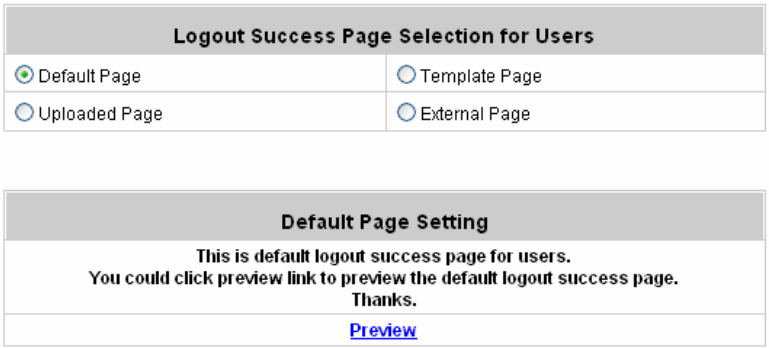
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

d. Choose the ***External Page*** selection and you can get the login success page for On-Demand from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new login success page for On-Demand can be previewed by clicking ***Preview*** button at the bottom of this page.

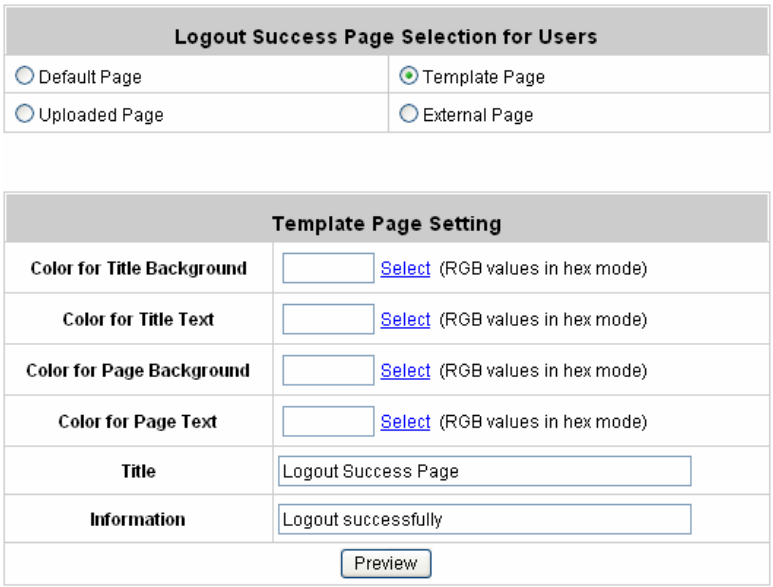


6. **Logout Success Page:** The administrator can use the default logout success page or get the customized logout success page by setting the template page, uploading the page or using the external website. After finishing the setting, you can click ***Preview*** to see the logout success page.

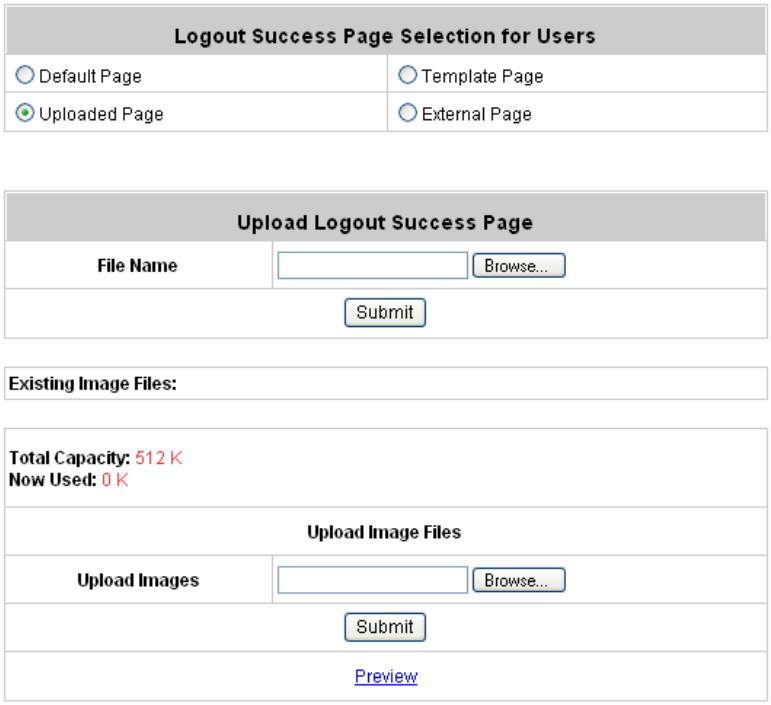
a. Choose ***Default Page*** to use the default logout success page.



b. Choose ***Template Page*** to make a customized logout success page here. Click ***Select*** to pick up a color and then fill in all of the blanks. You can click ***Preview*** to see the result first.



c. Choose ***Uploaded Page*** and you can get the logout success page by uploading. Click the ***Browse*** button to select the file for the logout success page upload. Then click ***Submit*** to complete the upload process.

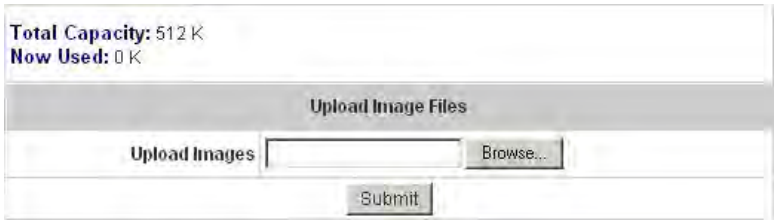


After the upload process is completed, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.

If the user-defined logout success page includes an image file, the image file path in the HTML code must be the image file you will upload.

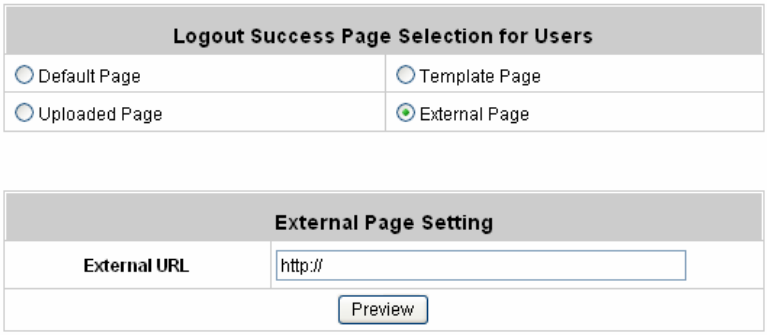
```
<img src="images/xx.jpg">
```

Then, enter or browse the filename of the images to upload 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.



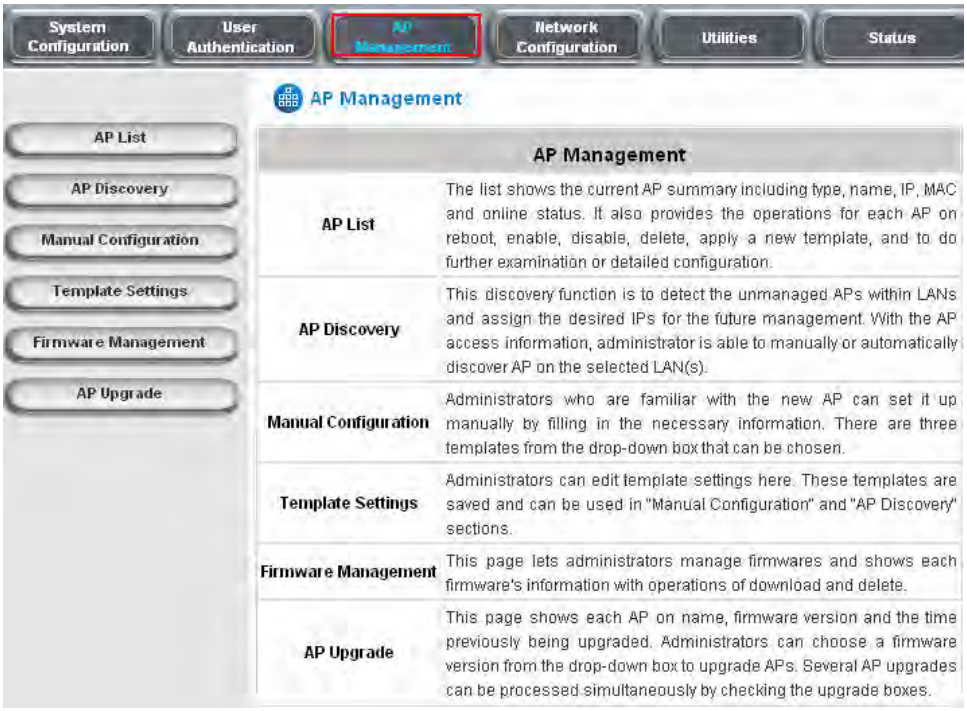
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

d. Choose the ***External Page*** selection and you can 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.



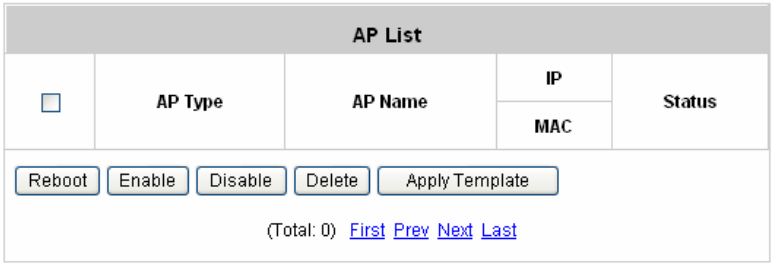
4.3 AP Management

This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management** and **AP Upgrade**. This section is used to manage the APs. Besides the various attributes of APs, there are different functions provided for various configurations.



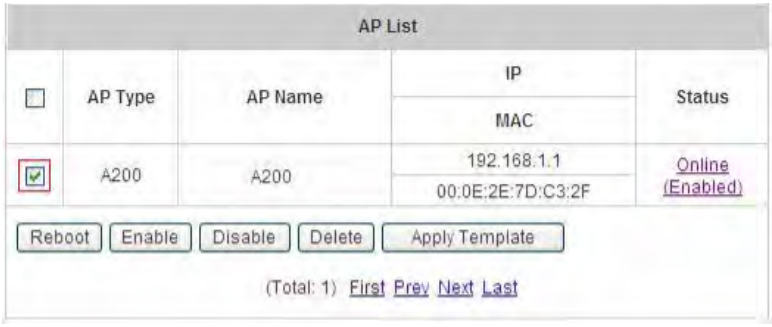
4.3.1 AP List

All of the supported APs under the management of LANPRO LP-NC1 will be shown in the list. At first the list is empty; administrators can add APs from AP Discovery page (see **4.3.2. AP Discovery** for details) or Manual Configuration page (see **4.3.3. Manual Configuration** for details)



After adding an AP:

Check any AP and click the button below to ***Reboot***, ***Enable***, ***Disable*** and ***Delete*** the checked AP.



- **AP Type:** This is the supported type of APs for centralized management.
- **AP Name:**

  The AP name will be shown as hyperlink. Click the hyperlink of each managed AP can have for configurations about the specific AP. 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:**

  Each AP's status will be shown in this column. Click the hyperlink of shown status of each managed AP will have detail status information about the specific AP such as System Status, LAN Status, Wireless Status, Access Control Status and Associated Client Status. Current status of the AP, is including **Configuring**, **Online**, **Offline**, **Upgrading**, and **Lost/Unknown**.

  (1) **Online:** The hyperlink of Online (Enabled) indicates that the AP is currently online and in service; Online (Disabled) indicates that the AP is currently online but not ready in service.

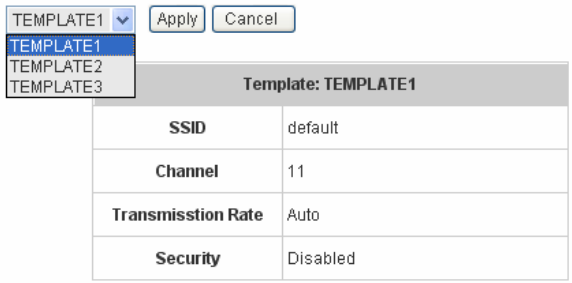
  (2) **Offline:** The AP is currently offline; for example: it is displayed as Offline when the power of the AP is off for any reason.

  (3) **Configuring:** It is displayed as Configuring when the newly discovered AP is being added to the list (and being configured) or new setting is being applied to the AP.

  (4) **Upgrading:** The AP is undergoing firmware upgrade.

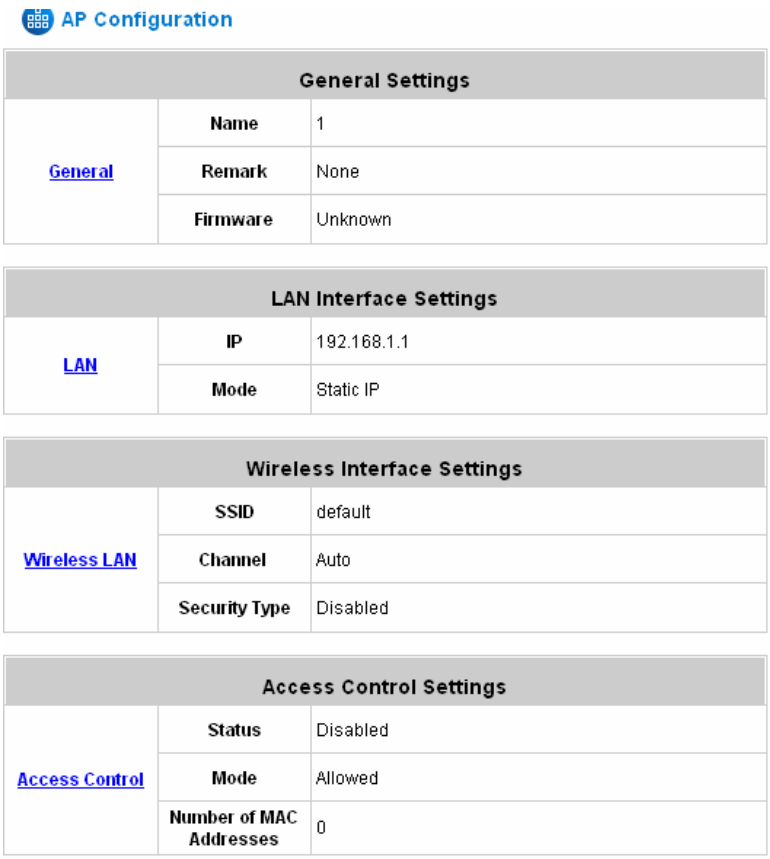
  (5) **Lost/Unknown:** After the system reboots and before it tries to probe the AP and determine the exact status, the status will be displayed as Lost or Unknown temporary.

Click ***Apply Template*** to select one template to apply to the AP.

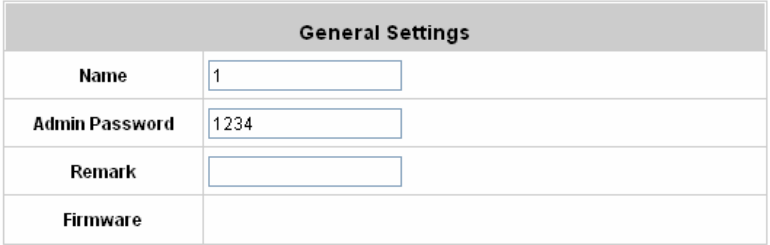


- **AP Name**

  Click the hyperlink of **AP Name** and enter the interface about related settings. There four kinds of settings, **General Settings**, **LAN Interface Settings**, **Wireless Interface Settings** and **Access Control Settings**. Click the hyperlink of each individual setting to have further configurations.



  - **General Settings:** Click the hyperlink of General to enter the **General Settings** interface. Revise the AP **Name**, **Admin Password** and **Remark** here if desired. Firmware information can also be viewed here.



- **LAN Settings:** Click the hyperlink of **LAN** to enter the **LAN Settings** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN Settings	
IP Address	192.168.1.1 *
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.254 *

- **Wireless LAN:** Click ***Wireless LAN*** to enter the **Wireless** interface. The data of **Properties** and **Security** need to be filled.

Wireless		
Properties	SSID	default
	SSID Broadcast	Enable
	Channel	0
	Transmission Mode	Mixed
	Transmission Rate	Auto (Default: Auto; Range: from 1 to 54 Mbps)
	CTS Protection	Disable (Default: Disable)
	Fragment Threshold	2346 (Default: 2346; Range: from 256 to 2346)
	RTS Threshold	2347 (Default: 2347; Range: from 0 to 2347)
	Beacon Interval (ms)	100 (Default: 100; Range: from 20 to 1024 msec)
	Preamble Type	Long (Default: Long)
	IAPP	Enable (Default: Enable)
	Block Relay	Disable (Default: Disable, not supported in versions before V1.25)
	Tx Power Level	100% (Default: 100%, not supported in versions before V1.25)
Security	Security Type	Disable ☐ 802.1X Authentication
	WEP	Authentication Type Both

Properties

- **SSID:** The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive and has a maximum length of 32 bytes.
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Channel:** Select the appropriate channel from the list to correspond with the network settings; for example, 1 to 11 channels are suitable for the North America area.
- **Transmission Mode:** There are 3 modes to select, **802.11b** (2.4G, 1~11Mbps)**, 802.11g** (2.4G, 54Mbps)

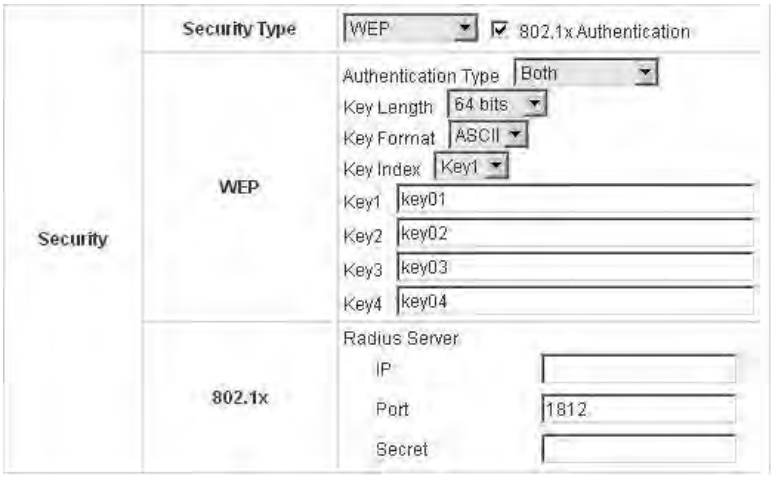
and **Mix mode** (b and g).

- **Transmission Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **CTS Protection:** The default value is **Disable**. When select **"Enable"**, a protection mechanism will decrease collision probability when many 802.11g devices exist simultaneously. However, performance of the 802.11g devices may decrease.
- **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
- **RTS Threshold:** Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.
- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.
- **Block Relay:** Select whether to enable this function.
- **Tx Power Level:** Choose which Tx power level desired from the drop-down menu.

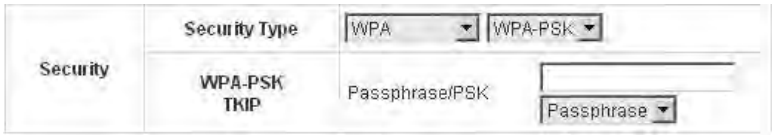
Security:

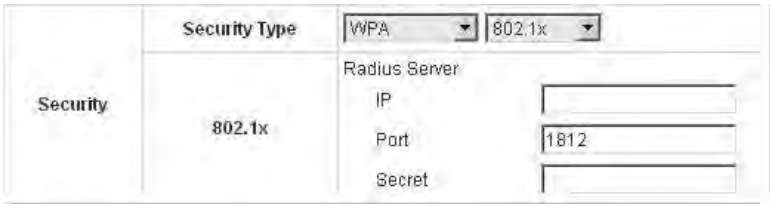
- **Security Type:** Choose one security type from the drop-down menu.
- **WEP:** Choose WEP authentication type here.

- **WEP:** WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Select **Authentication Type** (Open System, Shared Key or Both), **Key Length** (64 bits or 128 bits), **Key Index** (Key1~Key4) and then input the **Key**. Check **802.1x Authentication** to enable this function and enter the related data, if necessary.

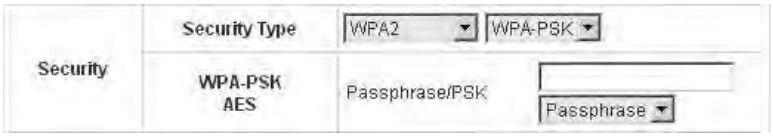


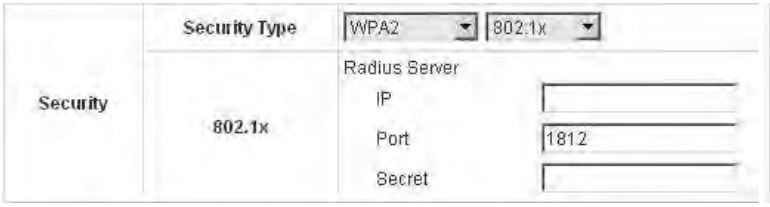
- **WPA:** WPA is Wi-Fi's encryption method that protects unauthorized network access by verifying network users through a server. Select 802.1x or WPA-PSK security type and enter the related information below.



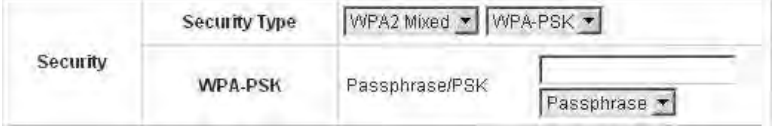


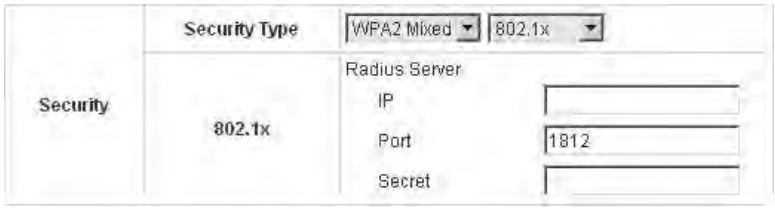
- **WPA2**: Wi-Fi Protected Access version 2. The follow on security method to WPA for Wi-Fi networks that provides stronger data protection and network access control. Select 802.1x or WPA-PSK security type and enter the related information below. WPA2 only can use AES encryption type.



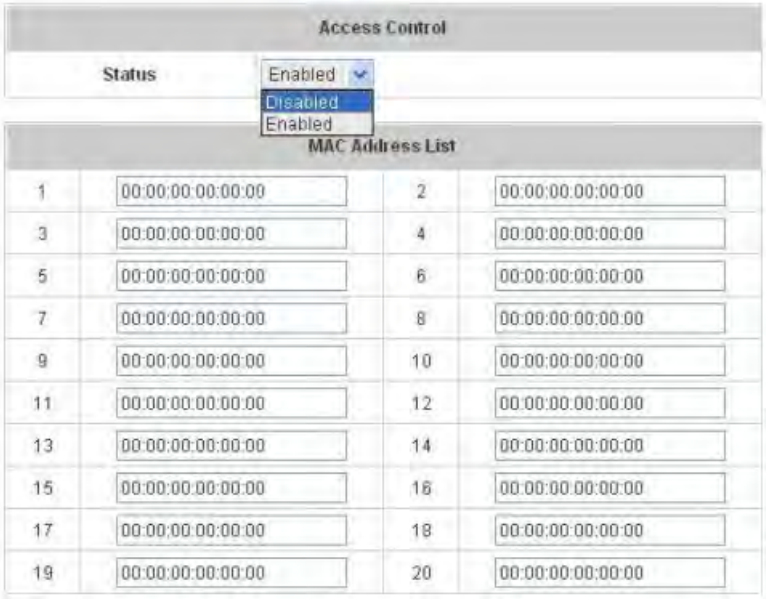


- **WPA Mixed:** If using TKIP and AES encryption type at the same time is desired, choose this security type. Select 802.1x or WPA-PSK security type and enter the related information below.





- **Access Control:** In this function, when the status is **Enabled**, only these clients which MAC addresses are listed in the list can be allowed to connect LANPRO LP-NC1. When **Disabled** is selected, all clients can connect LANPRO LP-NC1. The default is **Disabled**.



- **Status**

  After clicking the hyperlink of Status, the basic information of the AP including **AP Name**, **AP Type**, **LAN MAC**, **Wireless LAN MAC**, **Up Time**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark** will be shown. In the below of the **AP Status Detail**, there are the related detailed information, **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.

AP Status Summary	
AP Name	NEWDEV-00001
AP Type	A200
LAN MAC	00:0e:2e:7d:c3:2f
Wireless LAN MAC	00:0e:2e:7d:c3:2f
Up Time	0day:1h:27m:21s
Report Time	2006-11-30 13:26:48
SSID	default
Number of Associated Clients	0
Remark	

AP Status Detail
System Status
LAN Status
Wireless LAN Status
Access Control Status
Associated Client Status

- **System Status:** The table shows the information about **AP Name**, **AP Status** and **Last Reporting Time**.

System Information	
AP Name	NEWDEV-00002
AP Status	Online
Last Reporting Time	2006-06-28 10:27:37

- **LAN Status:** The table shows the information about **IP Address**, **Subnet Mask** and **Gateway**.

LAN Interface	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Gateway	0.0.0.0

- **Wireless LAN Status:** The table shows all of the related wireless information.

Wireless Interface	
Up Time	0day:15h:45m:48s
SSID	default
Beacon Interval (ms)	100
RTS Threshold	2347
Channel	11
Transmission Rate	Auto
Preamble Type	Long Preamble
IAPP	Enabled
Security	Disable

- **Access Control Status:** The table shows the status of MAC of clients under the control of the AP.

Access Control	
Status	Disabled

Access Control	
Status	Enabled

Control List	
00:00:00:00:00:01	00:00:00:00:00:02
00:00:00:00:00:03	00:00:00:00:00:04
00:00:00:00:00:05	00:00:00:00:00:06
00:00:00:00:00:07	00:00:00:00:00:08
00:00:00:00:00:09	00:00:00:00:00:10
00:00:00:00:00:11	00:00:00:00:00:12
00:00:00:00:00:13	00:00:00:00:00:14
00:00:00:00:00:15	00:00:00:00:00:16
00:00:00:00:00:17	00:00:00:00:00:18
00:00:00:00:00:19	00:40:96:A1:AF:dd

- **Associated Client Status:** The table shows the clients connecting to the AP and the related information of the client including Client List, Number, MAC, Mode, Rate, RSSI and Power Saving.

Client List							
No	MAC	User ID	TX Packet (s)	RX Packet (s)	Rate	Power Saving	Expiration countdown
1	00:02:8a:f3:aa:a4	N/A	2	6	11	No	300

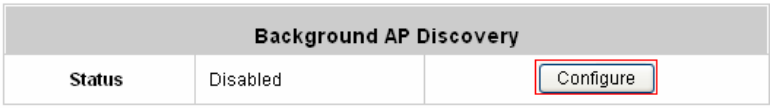
4.3.2 AP Discovery

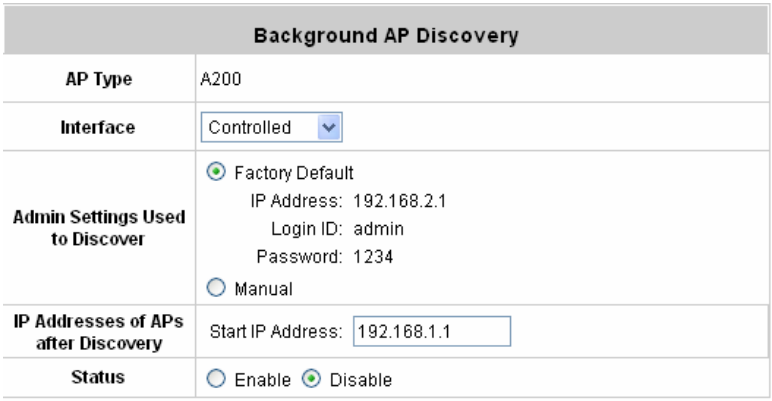
With the newly connected APs, administrators are able to discover them by clicking "Scan Now" button with the following information.

- **AP Discovery:** By pre-defining the settings of those APs in this AP Discovery interface, administrator will be able to discover (by clicking on the ***Scan Now*** button) all manageable APs at once. After these APs are discovered, administrator can apply the template of AP setting and add to the AP List for later maintenance.

  - **AP Type**: The type of manageable APs to be discovered.
  - **Interface:** The LAN interface (Controlled or Uncontrolled) to which the APs are connected.
  - **Admin Settings Used to Discover:** This is the setting of web-based Administration UI of the specific AP. If the APs are not reset to "Factory Default" values, administrator can select ***Manual*** to manually enter the current IP address range, Login ID and Password of the APs.
  - **IP Addresses of APs after Discovery**: The start IP address of IP address range to be assigned to the discovered APs. If nay APs are discovered, the APs will be assigned the IP addresses starting from the Start IP Address.
  - **Scan Now:** Click this button to start the discovery. All discovered APs will be shown in the ***Discovered AP List***. If any IP address to be assigned to a specific AP is used, there will be a warning message showing up. If so, please change the **IP Addresses of APs after Discovery** and then click ***Scan Now*** again.

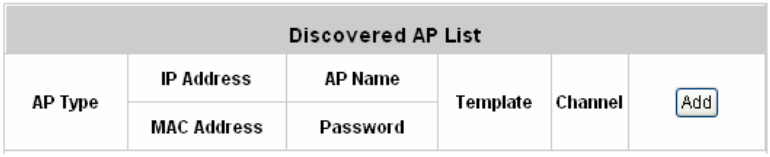
- **Background AP Discovery:** The system can be set up to discover APs periodically in background





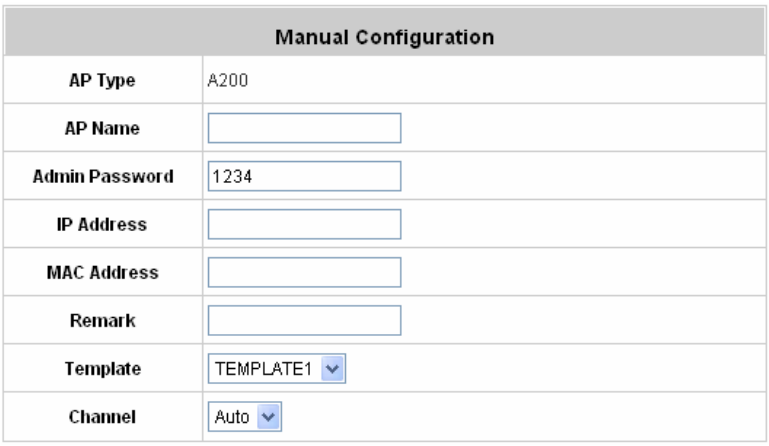
Settings of ***Background AP Discovery*** are the same as the in the ***AP Discovery*** settings mentioned above. For the ***Status***, when enabled, the system will discover APs in background at the time interval (Default: 10 minutes). If any AP is discovered and "Auto-Add AP" enabled, the system will add the discovered APs into the ***AP List*** table automatically, apply the selected ***Template*** of AP setting to the APs, and assign available IP addresses to the APs.

- **Discovered AP List**: Administrator can click ***Add*** button to register the APs to the ***AP List*** for management. The Service Zone to which the APs will belong is specified here. By clicking **Add** button, 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 Manual Configuration

Administrators who choose to manually configure an AP can utilize the function with the following information. Enter the related information of the AP and select a **Template**. Click ***ADD*** and then the AP will be added to the **AP List**.

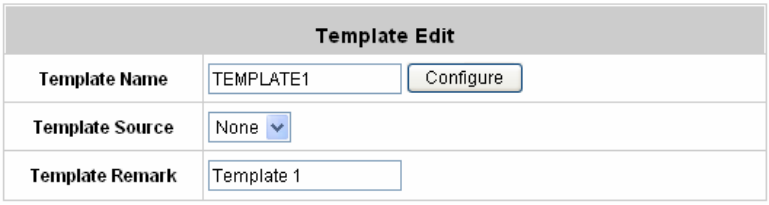


- **AP Type**: This is the supported type of APs for centralized management.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **Remark:** Some extra information to be filled in for this AP if desired.
- **Template:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.

4.3.4 Template Settings

Template is a model that can be copied to every AP without having to configure the each AP individually. There are three templates provided. Click ***Edit*** to go to configuration.

Enter the **Template Name** and **Template Remark** (optional) and click the hyperlink of ***Configure*** to have further configuration.



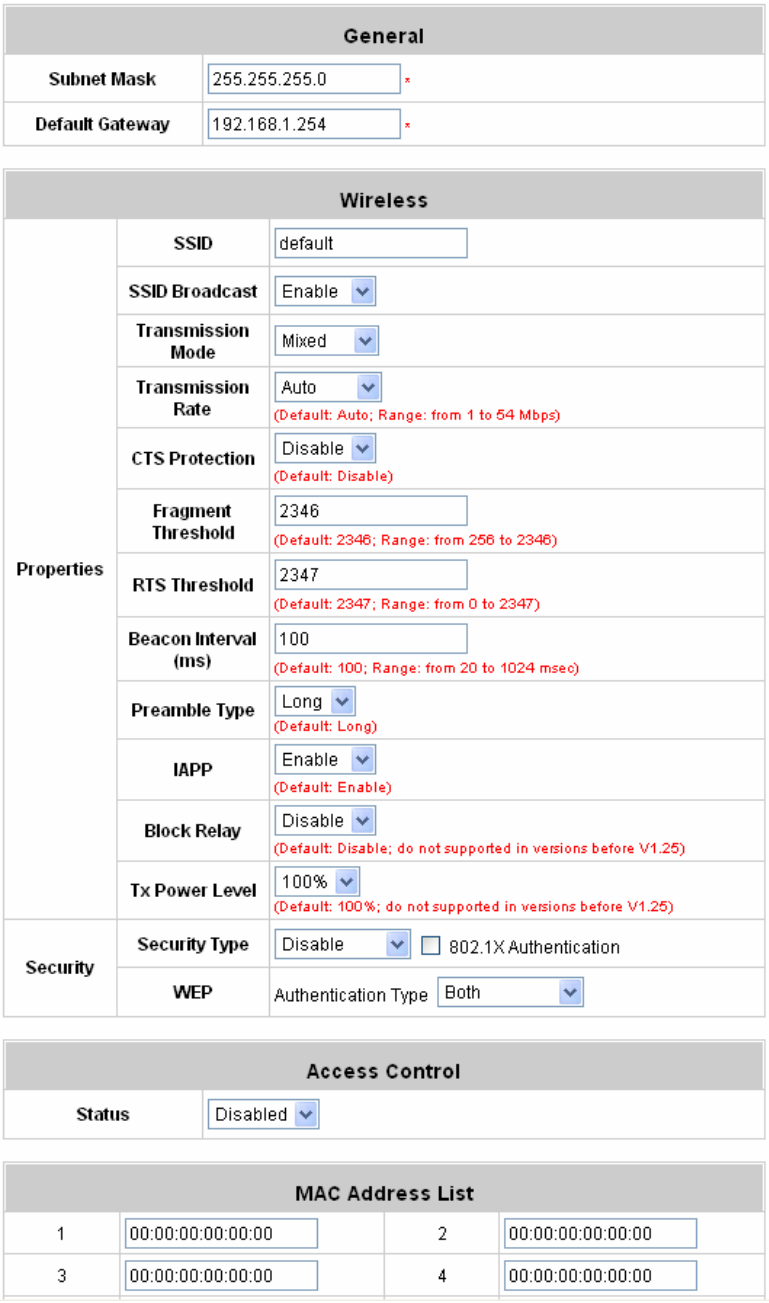
- **Template Edit**: Here is the section that administrators can configure template name, template source, and template remark.
- **Template Name**: The name shown for this particular template will change according to what given by administrators.
- **Template Source:** Select an existing AP and click Apply to save its settings as the template settings.

After click the button of ***Configure*** to enter the **Template Edit** page, revise the configuration for demand such as **SSID** or **Channel**. About other functions of **Wireless** section, please refer to **4.3.1 AP List**.

Access Control 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** this function 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.

- **AP A200**

The AP includes standards 802.11b and g. The connection could be select to enable 802.11b/g or disable. The The AP is fully compatible with the IEEE 802.11b and 802.11g standards.



Subnet Mask: The default is 255.255.255.0. All devices in the network must share the same subnet mask.

Default Gateway: The default is 192.168.1.254. Enter the gateway IP address for the network, typically a router.

Properties

- **SSID:** The SSID is the unique name shared among all devices in a wireless network.
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can

prevent the SSID from being seen on networked.

- **Transmission Mode:** There are 3 modes to select, **802.11b** (2.4G, 1~11Mbps)**, 802.11g** (2.4G, 54Mbps) and **Mix mode** (b and g).
- **Transmission Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **CTS Protection:** Select Enable or Disable this feature.
- **Fragment Threshold:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Threshold:** Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.
- **Beacon Interval:** Enter a value between 20 and 1024 msec. The default value is 100 milliseconds.
- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.
- **Block Relay:** Select whether to enable this function.
- **Tx Power Type:** Choose which Tx power level desired from the drop-down menu.

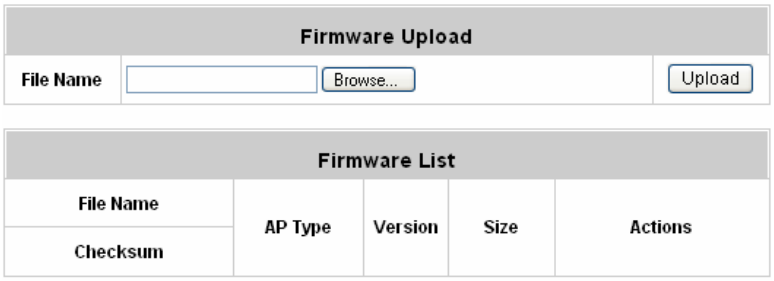
Security

- **Security Type:** Choose one security type from the drop-down menu
- **WEP:** Choose WEP authentication type here.

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. When this function is enabled, please make sure the MAC Address List is not empty.

4.3.5 Firmware Management

In this function, AP's firmware can be uploaded. The page includes the Preloaded Firmware, a function to upload desired firmware and shows the already uploaded firmware's name, checksum, AP type, version and size. Administrators are also given the option to download or delete the firmware.



- **File Name**: Name of the file to be uploaded.
- **Upload:** Can be clicked to upload the file.
- **Firmware List:** Shows the already uploaded firmware.
- **Checksum:** The automatically detected security identification of the firmware.
- **AP Type:** The AP type of the firmware.
- **Version:** The version of the AP firmware.
- **Size:** File size of the firmware.
- **Download:** Can be clicked to save the current firmware.

- **Delete:** Can be clicked to delete the current firmware.

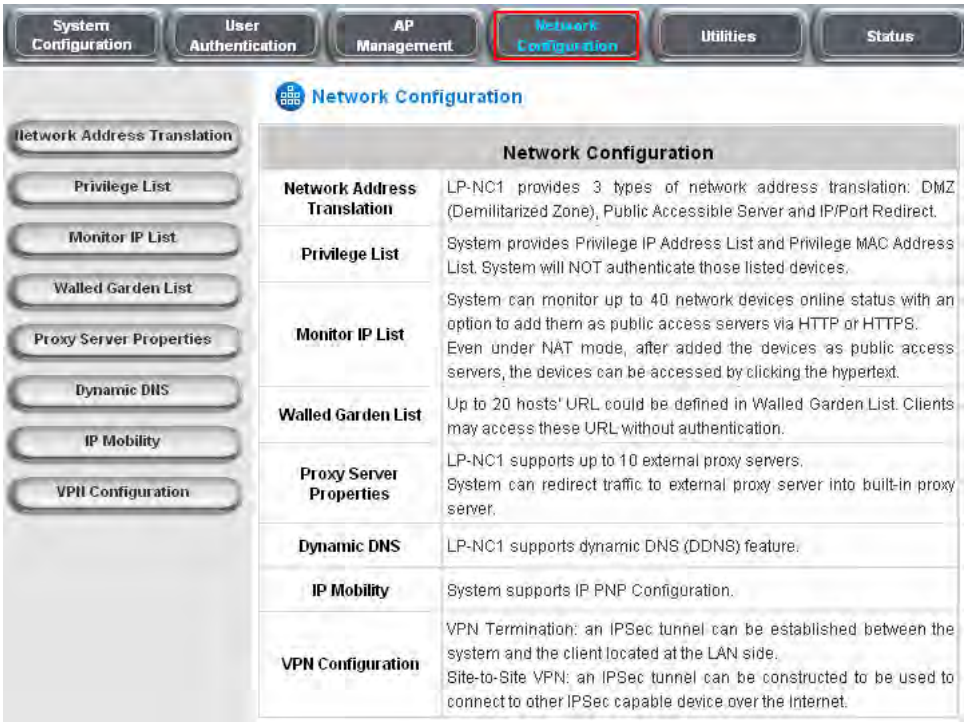
4.3.6 AP Upgrade

Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.

- **Upgraded Time**: Shows when the AP was last upgraded.
- **New Version:** Version of the firmware to upgrade the AP.

4.4 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties** and **Dynamic DNS**, **IP Mobility** and **VPN Configuration**. This section is used to set all the internet settings.



4.4.1 Network Address Translation

There are three parts, **DMZ (Demilitarized Zone), Public Accessible Server** and **Port and IP Redirect**, need to be set.

Network Address Translation
DMZ (Demilitarized Zone)
Public Accessible Server
Port and IP Redirect

- **DMZ (Demilitarized Zone)**

  In the DMZ functions, the administrator can define mandatory external to internal IP mapping, hence a user on 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 Address** 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.

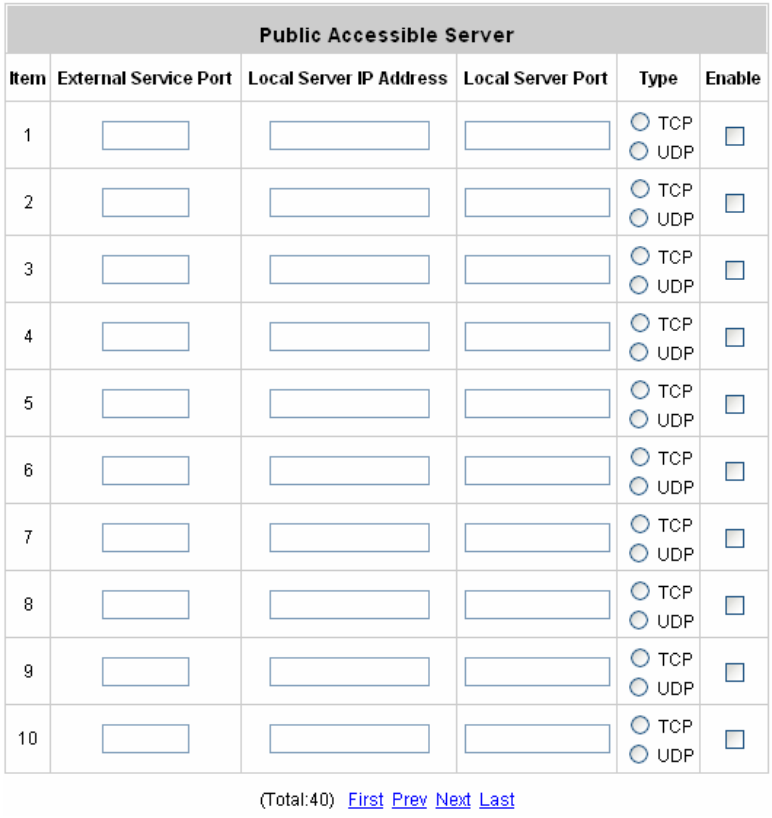
Automatic WAN IP Assignment			
Enable	External IP Address	External Interface	Internal IP Address
☐	10.29.2.204	WAN1	

Static Assignments			
Item	External IP Address	External Interface	Internal IP Address
1		WAN1	
2		WAN1	
3		WAN1	
4		WAN1	
5		WAN1	
6		WAN1	
7		WAN1	
8		WAN1	
9		WAN1	
10		WAN1	

(Total:40) First Prev Next Last

- **Public Accessible Server**

  In this function, the administrator can set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network via WAN1 port IP of LANPRO LP-NC1. Please enter the **External Service Port**, **Local Server IP Address** and **Local Server Port**. According to the different services provided, the network service can use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.



Public Accessible Server					
Item	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**

  In this function, the administrator can set up to 40 sets of the IP address ports for redirection purpose. 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**. Please enter the **IP Address** and **Port** of **Destination**, and the **IP Address** and **Port** of **Translated to Destination**. According to the different services provided, choose **TCP** or **UDP** protocol. These settings will become effective immediately after clicking ***Apply***.

Port and IP Redirect

Item	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

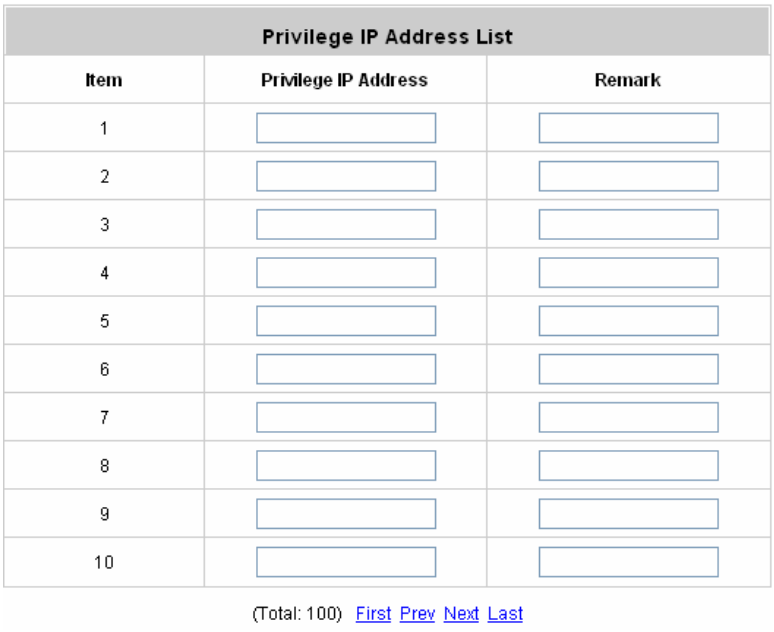
(Total:40) First Prev Next Last

4.4.2 Privilege List

LANPRO LP-NC1 provides two privilege lists, **Privilege IP Address List** and **Privilege MAC Address List**. In the Privilege List function, the administrator can add desired IP addresses and MAC addresses in these lists. The IP addresses and MAC addresses in these lists are allowed to access the network without authentication.

- **Privilege IP Address List**

  The IP address listed here can access internet directly without going through the login page. 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. The **Remark** is optional but useful to keep track. LANPRO LP-NC1 provides up to 100 privilege IP addresses. These settings will become effective immediately after clicking ***Apply***.

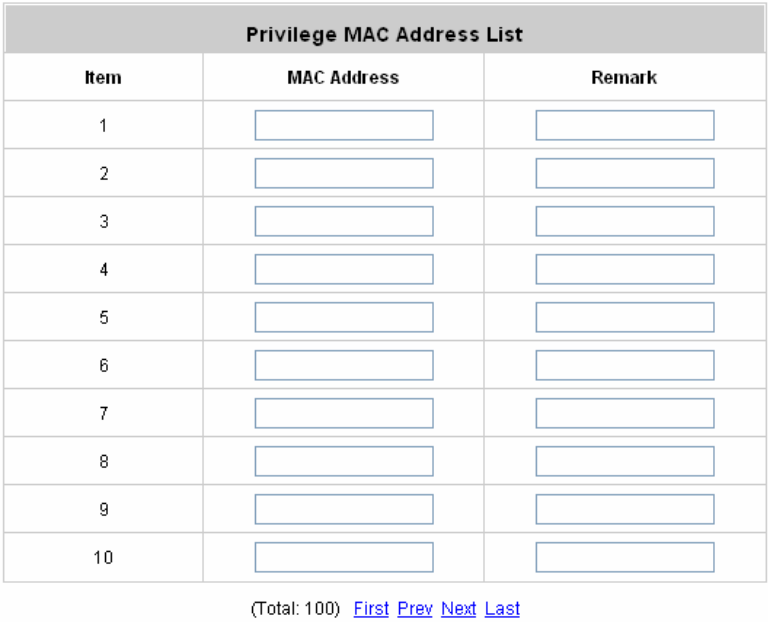


***Warning:* Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.**

- **Privilege MAC Address List**

  The MAC address listed here can access internet directly without going through the login page. In addition to the IP addresses, you can also set the clients' MAC addresses in this list, so authentication is not required when they use the network. LANPRO LP-NC1 allows 100 privilege MAC addresses at most.

  If you want to manually create the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking ***Apply***.



Privilege MAC Address List		
Item	MAC Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

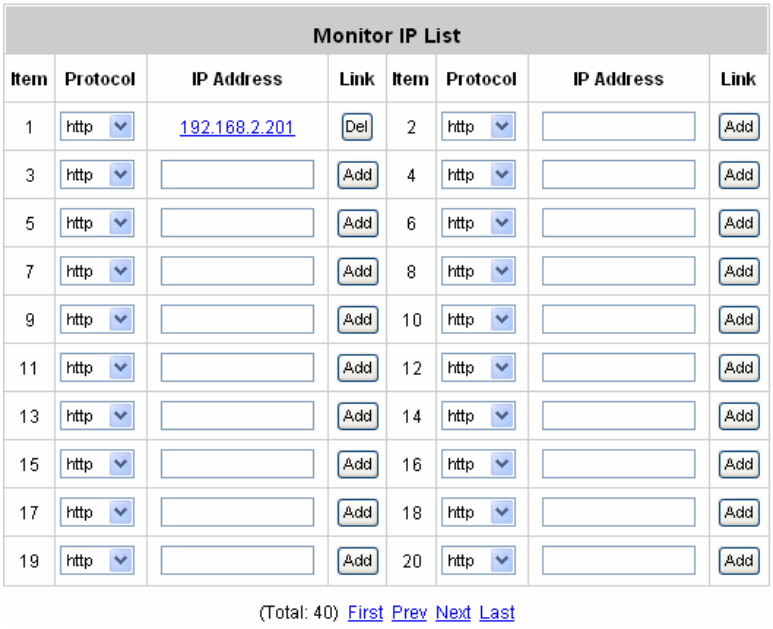
(Total: 100) First Prev Next Last

Warning: Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.

4.4.3 Monitor IP List

Administrators can input IPs to monitor their status. After inputting the desired IPs to be monitored, click ***Monitor*** button and a new page will show which IPs are unreachable (red dot) and which are reachable and alive (green dot). The administrator can setup the report emails for Monitor IP List. This system will periodically Ping the specified IPs and send out the emails. 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 the hyperlink of theirs IP addresses. To add the monitored IP addresses as hyperlink accessible mode by clicking ***Add*** button in Link column.



When **Monitor** button is clicked, **Monitor IP Result** 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 result

No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

On each monitored device with a WEB server running, you may add a link for the easy access by selecting a protocol, http or https, and click the ***Add*** button. After clicking Add button, the IP address will become a hyperlink, and then you can easily access the host by clicking the hyperlink. Click the ***Del*** button to remove the setting.

Monitor IP List

Item	Protocol	IP Address	Link	Item	Protocol	IP Address	Link
1	http	10.171.1.129	Del	2	http	10.171.1.130	Add
3	http	1.2.3.4	Add	4	http		Add
5	http		Add	6	http		Add
7	http		Add	8	http		Add
9	http		Add	10	http		Add
11	http		Add	12	http		Add
13	http		Add	14	http		Add
15	http		Add	16	http		Add
17	http		Add	18	http		Add
19	http		Add	20	http		Add

(Total40) First Prev Next Last

Monitor

4.4.4 Walled Garden List

This system provides the free services to the users to access websites listed here before authentication. IP address or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. This function provides some free surfing areas that users can access before login and authenticated. Users without the network access right can still have a chance to experience the actual network service free of charge. Please enter the **IP Address** or **Domain Name** of the website in the list and these settings will become effective immediately after clicking ***Apply***.

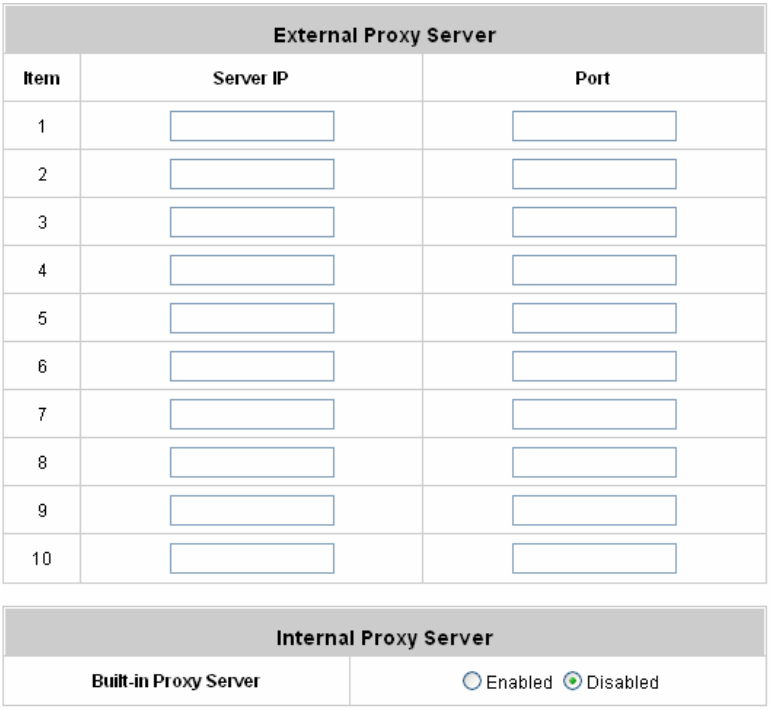
Walled Garden List

Item	Address	Item	Address
1	www.yahoo.com	2	www.valuepointnet.com
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Caution: To use the domain name, the LANPRO LP-NC1 has to connect to DNS server first or this function will not work.

4.4.5 Proxy Server Properties

System supports Internal Proxy Server and External Proxy Server functions. System has a built-in proxy server. If this function is enabled, the end-users will be forced to treat this system as the proxy server regardless of the end-users' original proxy settings. The system will match the External Proxy Server list to the end-users' proxy setting. If there is no matched setting, then the end-users will not be able to reach the login page and thus unable to access the network. If there is a matched setting, then the end-users will be directed to the system first for authentication.



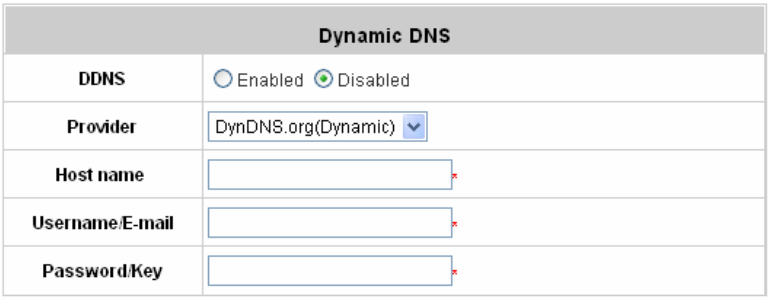
External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

- **External Proxy Server:** Under the LANPRO LP-NC1 security management, the system will match the proxy setting of **External Proxy Server** list to the clients' proxy setting when clients' have proxy setting in their browsers. If there is no matching, the clients will not be able to get the login page and then unable to access the network. If there is a matching, then the clients will be directed to the system first for authentication. After successful authentication, the clients' will be redirected back to the desired proxy servers.
- **Internal Proxy Server:** LANPRO LP-NC1 has a built-in proxy server. If this function is enabled, the clients will be forced to treat LANPRO LP-NC1 as the proxy server regardless of the clients' original proxy settings.
  For more details about how to set up the proxy servers, please refer to Appendix E. and F.

4.4.6 Dynamic DNS

System provides a convenient DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking ***Apply***.



- **DDNS:** 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.

The fields with red asterisks are necessary to fill in.

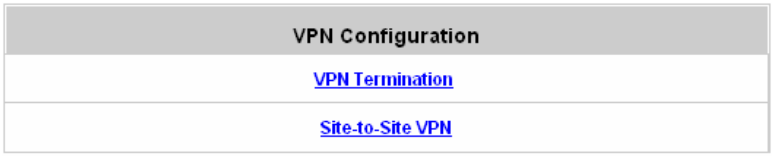
4.4.7 IP Mobility

LANPRO LP-NC1 supports IP PNP function. When enabled IP PNP, PC with static IP address will access the network properly. When disabled the feature, PC with static IP address cannot access network if IP address is in the predefined IP range.

IP Mobility	
IP PNP	○ Enable ◉ Disable

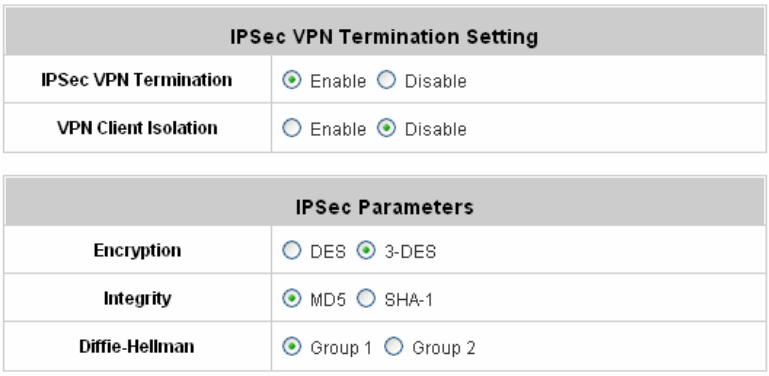
4.4.8 VPN Configuration

Virtual Private Network, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POPS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database. There are two types of VPN connection supported in the system, including **VPN Termination**, and **Site-to-Site VPN**.



- **VPN Termination**

It allows the system to create the VPN tunnel between a user's device and LANPRO LP-NC1, to encrypt the data transmission. Only when this function is enabled here do users of the entire system are able to use VPN Termination. In addition, VPN Termination users can be isolated from each other when ***VPN Client Isolation*** is enabled. For more information about VPN Termination, please see ***Appendix D. IPSec VPN Termination***



- **Site-to-Site VPN**

Enable Site-to-Site VPN can create the IPSec VPN tunnel between two remote networks/sites to encrypt the data transmission. Click ***Add A New Site Entry*** button to set configuration about remote VPN capable devices such as a VPN gateway. Click ***Add A Local Entry*** button to set configuration about local site.

Remote Site Configuration

Name	IP Address	Pre-shared Key	Edit	Delete
TPE	1.2.3.4	12345	Edit	Delete
BJ	2.3.4.5	1111	Edit	Delete

Add A Remote Site

Local Site Configuration

Local Subnet	Local Interface	Remote VPN Gateway	Remote Subnet	Edit	Delete
192.168.1.0/24	WAN1	1.2.3.4	192.168.11.0/24	Edit	Delete
192.168.2.0	WAN1	2.3.4.5	192.168.4.0/24	Edit	Delete

Add A Local Site

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

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)

Click ***Add A Local Site*** to enter the **Site Information** page for further configuration of local site.

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

Click ***NEW*** 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)

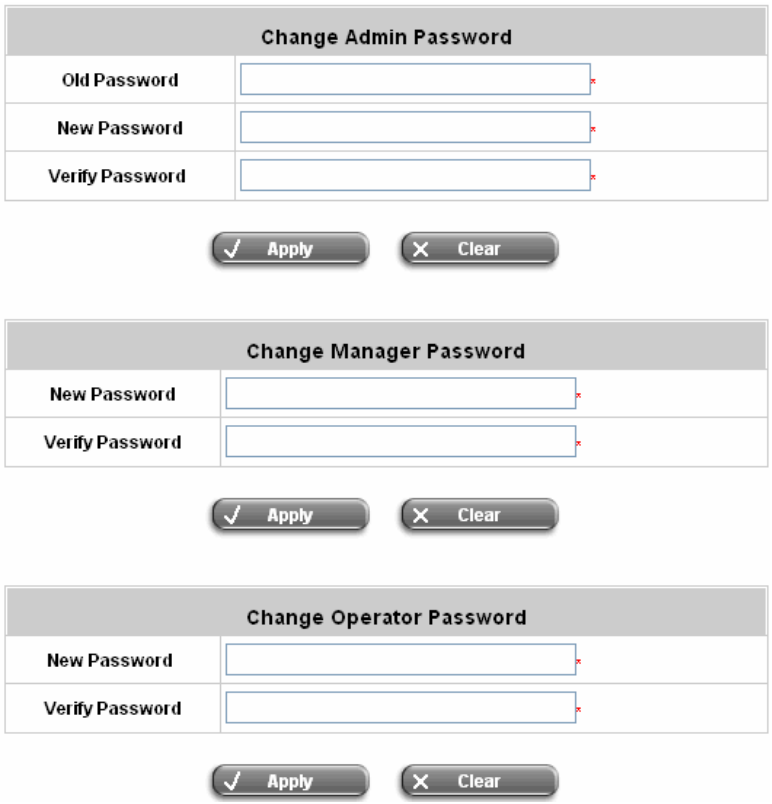
Remote Subnet		
No.	Network	Mask
1		255.255.255.255 (/32)
2		255.255.255.255 (/32)
3		255.255.255.255 (/32)
4		255.255.255.255 (/32)
5		255.255.255.255 (/32)

4.5 Utilities

This section provides functions for modifying user's **Password**, file of **Backup/Restore** system, **Firmware Upgrade** and **Restart** service.

4.5.1 Change Password

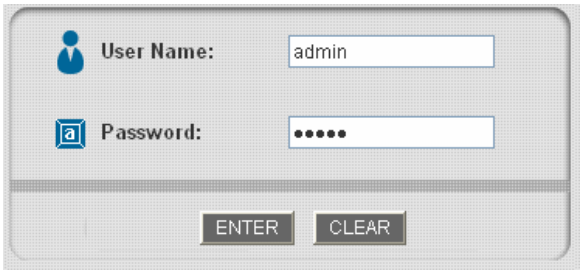
The system provides three different types of management accounts, each assigned with different access privileges. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords are as follow:



Administrator: The administrator can access all web management interfaces.

User Name: **admin**

Password: **admin**



Manager: The manager account may modify all user authentication options, including user group management.

User Name: **manager**

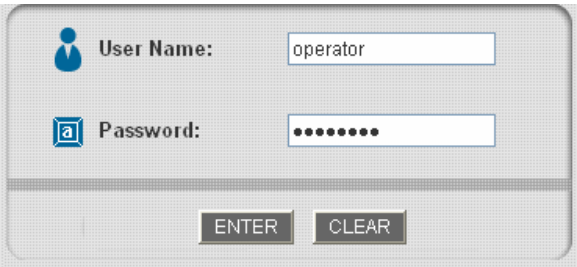
Password: **manager**

Operator: The operator account may only create **On-demand User** Account from the administrative webpage.

When login with Operator account, user will Be direct to On-demand User Account page immediately with no access to other management webpage. This account is intended for store clerk when the system is deployed at Hotspot or corporate meeting rooms.

User Name: **operator**

Password: **operator**

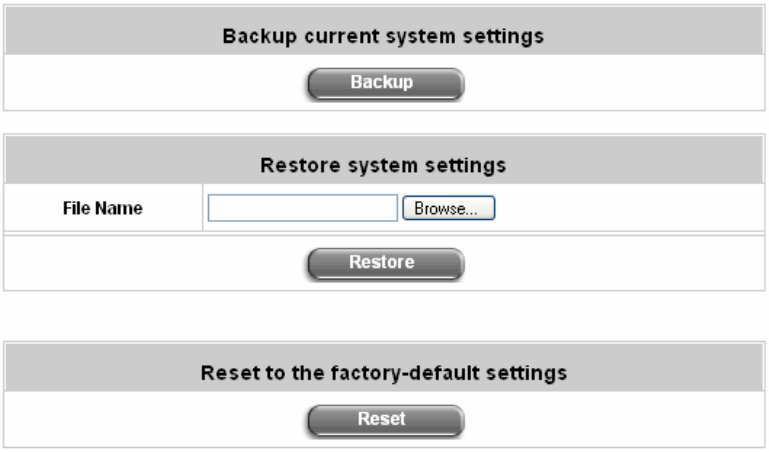


The administrator can change the passwords here. Please enter all the required fields with red asterisks if changing the password is desired. Click ***Apply*** to activate this new password.

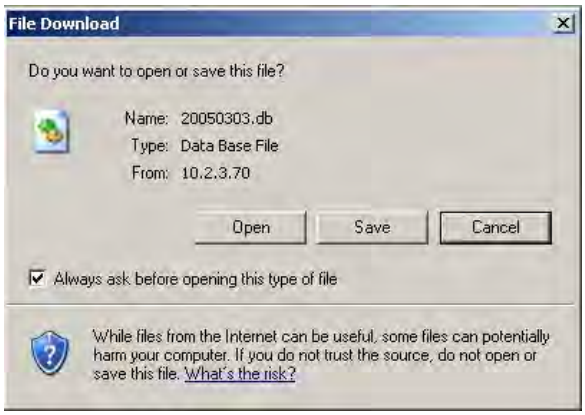
Caution: If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port.
Passwords is allowed to set by using number (0~9), alphabets (a~z or A~Z), dash(-), underline(_) and dot(.) with a maximum of 40 characters; all other letters are not allowed.
All accounts and passwords have default value. Please consult your user guide for default password.

4.5.2 Backup/Restore Settings

This function is used to backup/restore the settings of LANPRO LP-NC1. Also, LANPRO LP-NC1 can be reset to the factory default settings here.



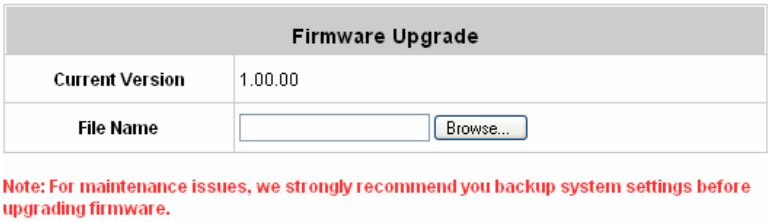
- **Backup current system settings:** Click ***Backup*** to create a .db database backup file and save it on disk.



- **Restore system settings:** Click ***Browse*** to search for a .db database backup file created by LANPRO LP-NC1 and click ***Restore*** to restore to the same settings at the time the backup file was created.
- **Reset to the factory-default settings:** Click ***Reset*** to load the factory default settings of LANPRO LP-NC1.

4.5.3 Firmware Upgrade

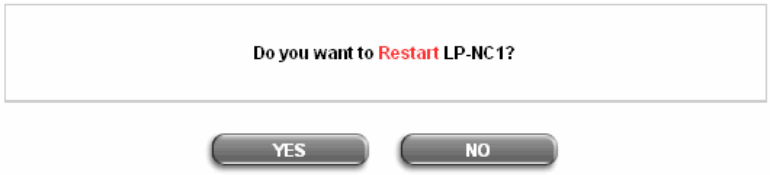
The administrator can download the latest firmware from website and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** to go on with the firmware upgrade process. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.



Warning: 1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation 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. It may damage the system and cause it to malfunction. 3. Firmware upgrade may take up to 5 minutes, please wait for the confirmation page.

4.5.4 Restart

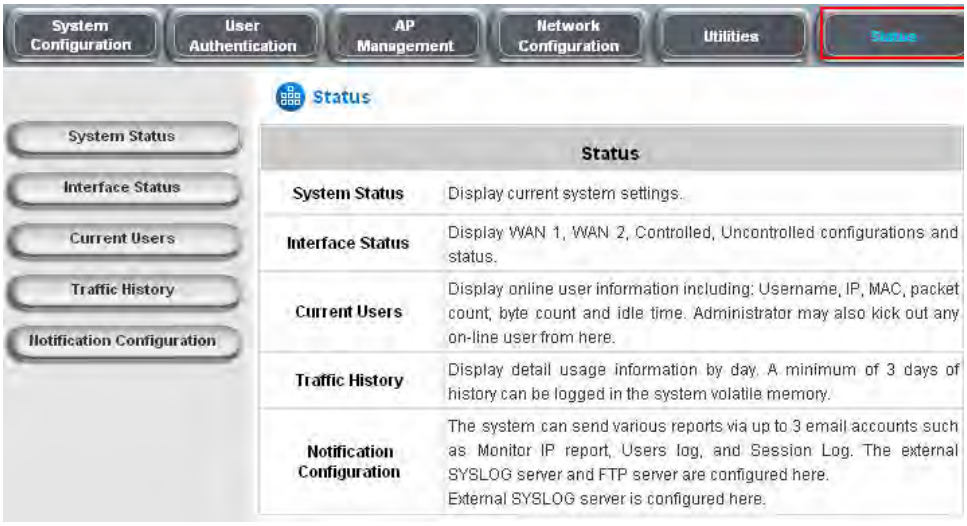
This function allows the administrator to safely restart LANPRO LP-NC1 and the process should take about 100 seconds. Click ***YES*** to restart LANPRO LP-NC1; click ***NO*** to go back to the previous screen. Please don't power off the system until this restart process has finished. Please wait for countdown timer to finish before accessing the system management webpage again.



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

4.6 Status

This section includes **System Status**, **Interface Status**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.



4.6.1 System Status

This page displays all important system, network, and user account configurations. It also shows the WAN connection status and system time.

System Status		
Current Firmware Version		1.00.00
Build		00200
System Name		LP-NC1
Home Page		http://www.lan-products.com
Syslog server-Traffic History		N/A:N/A
Syslog server-On demand User log		N/A:N/A
Proxy Server		Disabled
Friendly Logout		Enabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Management	Remote Management IP	0.0.0.0/0.0.0.0
	SNMP	Disabled
History	Retained Days	3 days
	Email To	N/A
		N/A
		N/A
Time	NTP Server	tock.usno.navy.mil
	Date Time	2007/09/13 05:53:56 -0400
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	cipherium.com.tw

The description of the table is as follows:

Item		***Description***
Current Firmware Version		The present firmware version of LANPRO LP-NC1
System Name		The system name. The default is LANPRO LP-NC1
Home Page		The page to which the users are directed after initial login success.
Syslog server-Traffic History		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Syslog server-On demand 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		Show WAN1 and WAN2 status when WAN Failover is enabled.
Management	**Remote Management IP**	The IP or IPs that is allowed for accessing the management interface.
	SNMP	Enabled/disabled stands for the current status of the SNMP management function.
History	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Email To	The email address that the traffic history information will be sent to.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	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.

4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **Controlled Port** and **Uncontrolled Port**.

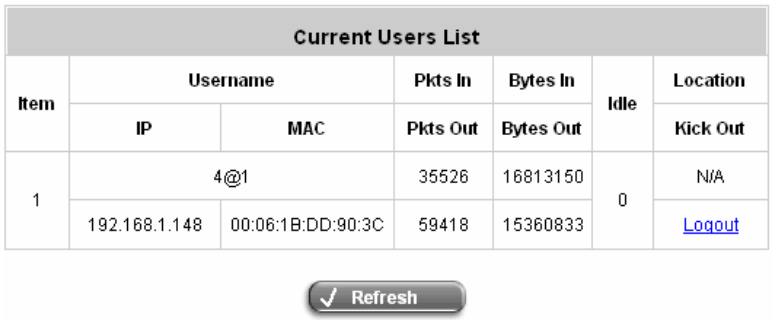
Interface Status		
WAN1	MAC Address	00:30:00:00:00:03
	IP Address	10.2.3.88
	Subnet Mask	255.255.255.0
Controlled	Mode	NAT
	MAC Address	00:30:00:00:00:01
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
Controlled DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Uncontrolled	Mode	NAT
	MAC Address	00:30:00:00:00:01
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
Uncontrolled DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)

The description of the table is as follows.

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
WAN2	**MAC Address**	The MAC address of the WAN2 port.
	IP Address	The IP address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
Controlled	**Mode**	The NAT or Router mode of the controlled port.
	MAC Address	The MAC address of the controlled port.
	IP Address	The IP address of the controlled port.
	Subnet Mask	The Subnet Mask of the controlled port.
Controlled DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the controlled port.
	WINS IP Address	The WINS server IP. N/A means that it is not configured.
	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 IP address.
Uncontrolled	**Mode**	The NAT or Router mode of the uncontrolled port.
	MAC Address	The MAC address of the uncontrolled port.
	IP Address	The IP address of the uncontrolled port.
	Subnet Mask	The Subnet Mask of the uncontrolled port.
Uncontrolled DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the uncontrolled port
	WINS IP Address	The WINS server IP. N/A means that it is not configured.
	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 IP address.

4.6.3 Current Users

A list of all online users currently login on the system including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Idle, Location** and **Kick Out** can be obtained. Administrator may terminate any user session by pressing Logout button next to individual user account. Administrator can use this function to force a specific online user to log out. Just click the hyperlink of ***Kick Out*** next to the online user's name to logout that particular user. Click ***Refresh*** to renew the current users list.



Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out
1	4@1		35526	16813150	0	N/A
	192.168.1.148	00:06:1B:DD:90:3C	59418	15360833		Logout

Refresh

4.6.4 Traffic History

This function is used to check the history of LANPRO LP-NC1. The history of each day will be saved separately in the DRAM for 3 days. Sorted by time, the traffic history provides all login and logout activity of specific date. Other information includes User Name, IP address, MAC address, In-bound Packet Count, Out-bound Packet Count, In-bound Byte Count, and out-bound Byte Count.

Traffic History	
Date	Size (Byte)
2007-09-13	65
On-demand User Log	
Date	Size (Byte)
2007-09-13	105
Roaming Out Traffic History	
Date	Size (Byte)
2007-09-13	106
Roaming In Traffic History	
Date	Size (Byte)
2007-09-13	112

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 **History Email** has been entered under the **Notify Configuration** page, then the system will automatically send out the history information to that email address.

- **Traffic History**

  As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out,** and **Bytes Out**, of user activities.

Traffic History 2007-08-22

Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2007-08-22 13:42:33	LOGIN	4@1	192.168.1.148	00:06:1B:DD:90:3C	0	0	0	0

  - **Date:** The date and time of record.
  - **Type:** Record type: Authentication Accept / Reject, Account Expire /Redeem etc.
  - **Name:** On-demand Account Name.
  - **IP/MAC:** IP and MAC address of login device.
  - **Pkts In / Bytes In / Pkts Out / Bytes Out:** In-bound and outbound Packet/Byte count.

- **On-demand User Log**

  As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Expiretime**, **Validtime** and **Remark**, of user activities.

On-demand User Log 2005-03-22

Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	Expiretime	Validtime	Remark
2005-03-22 17:55:58 +0800	My Service	Create_OD_User	P4SP	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:55:58	None	2 hrs 0 mins
2005-03-22 17:56:03 +0800	My Service	Create_OD_User	62H6	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:03	None	2 hrs 0 mins
2005-03-22 17:56:07 +0800	My Service	Create_OD_User	886D	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:07	None	2 hrs 0 mins

  - **Date:** The date and time of record.
  - **System Name:** The system name defined at System Information page.
  - **Type:** Record type: Authentication Accept / Reject, Account Expire /Redeem etc.
  - **Name:** On-demand Account Name.
  - **IP/MAC:** IP and MAC address of login device.
  - **Pkts In / Bytes In / Pkts Out / Bytes Out:** In-bound and outbound Packet/Byte count.
  - **Expiretime:** Time of account expiration (for accounts based on time limit, not data rate)
  - **Validtime:** Time when account is valid. When valid time is reached, account is disabled regardless of actual account usage.
  - **Remark:** Any remark added by administrator at ON-Demand User Group configuration.

- **Roaming Out Traffic History**

  This log shows the Roaming-out Traffic User History when system is the system is deployed with roaming center. As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

- **Date:** The date and time of record.
- **Type:** Record type: Authentication Accept / Reject, Account Expire /Redeem etc.
- **Name:** Roaming-Out user name.
- **NASID:** System ID of remote RADIUS.
- **NASIP:** The IP address of the RADIUS server.
- **NASPort:** The port number of remote RADIUS server.
- **UserMAC:** User MAC address.
- **SessionID:** Session ID, usually the time stamp.
- **SessionTime:** Session length in seconds.
- **Bytes In/Out:** Byte count for in bound and outbound traffic.
- **Pkts In/Out:** Packet count for inbound and outbound traffic.
- **Message:** System response. Common messages are reject, accept, idle time out, session time out, etc.

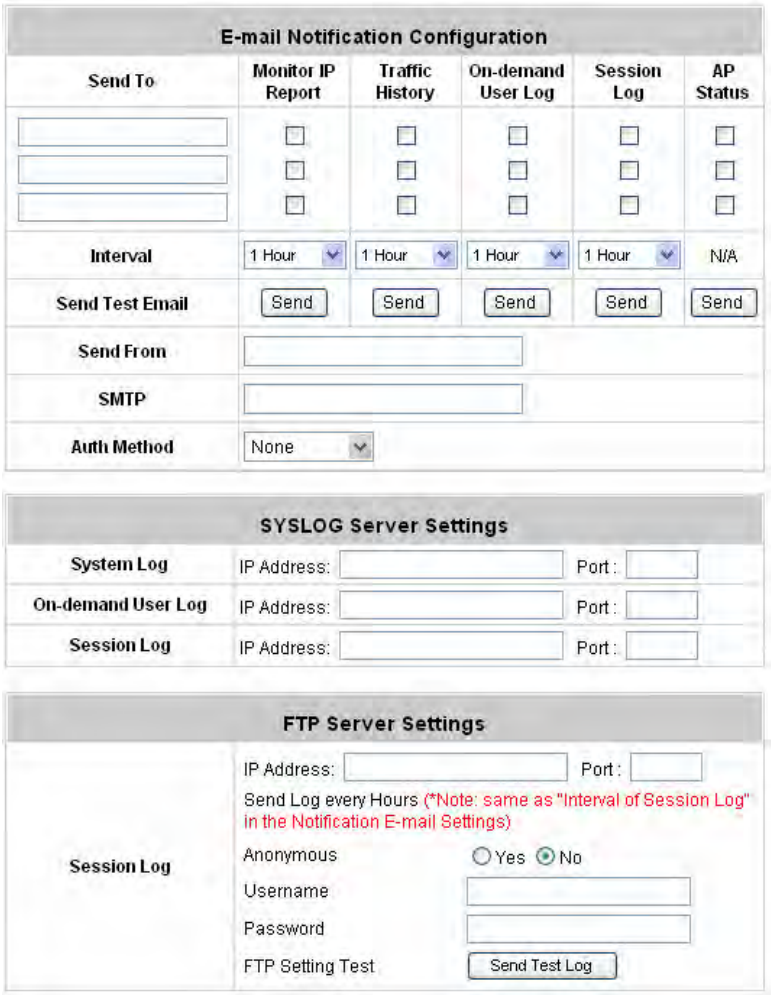
- **Roaming In Traffic History**

As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

- **Date:** Record time/date.
- **Type:** Record type: Authentication Accept / Reject, Account Expire /Redeem etc.
- **Name:** Roaming-Out user name.
- **NASID:** System ID, usually MAC address of WAN port of this system.
- **NASIP:** The IP address of the RADIUS server.
- **NASPort:** The port number of remote RADIUS server.
- **UserMAC:** User MAC address.
- **SessionID:** Session ID, usually the time stamp.
- **SessionTime:** Session length in seconds.
- **Bytes In/Out:** Byte count for in bound and outbound traffic.
- **Pkts In/Out:** Packet count for inbound and outbound traffic.
- **Message:** System response. Common messages are reject, accept, idle time out, session time out, etc.

4.6.5 Notification Configuration

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



- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail. Check which type of report to be sent—Monitor IP Report, Traffic History, On-demand User Log, and AP Status.
- **Interval:** The time interval to send the e-mail report. Choose a proper number from the drop-down box.
- **Send Test Email:** To test the settings correct or not.
- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **SMTP:** The IP address of the SMTP server.
- **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 3 parts: System Log, On-demand User Log and Session Log. Enter the IP address and Port to specify which and from where the report should be sent.

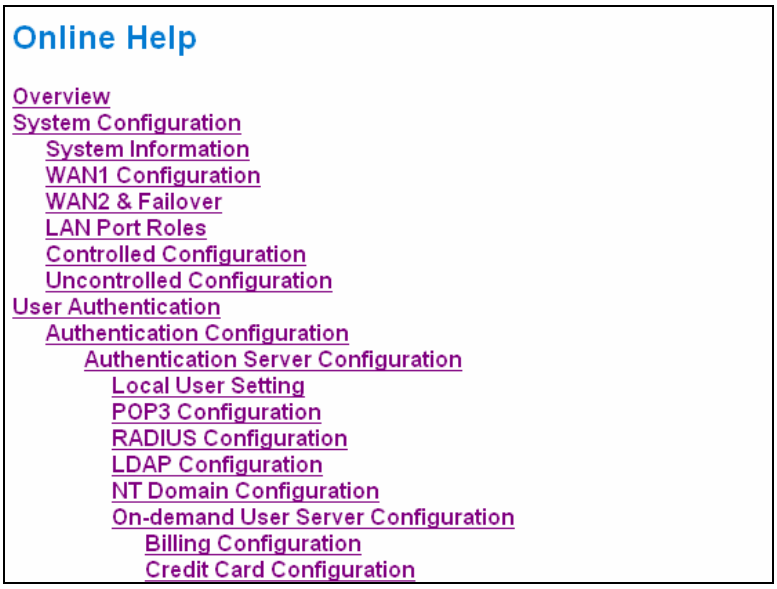
Note: When the number of a user's sessions (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this Syslog server. For more information about Session Limit, please refer to Appendix H.

- **FTP Server Settings:** Session Log allows uploading the log file to a FTP server periodically. The delivering frequency of session log to target repository can be adjusted via Interval time on **E-mail Notification Configuration.**
  - **Session Log:** Log each connection created by users and tracking the source IP/Port and destination IP/Port.

4.7 Help

On the screen, the **Help** button is on the upper right corner.

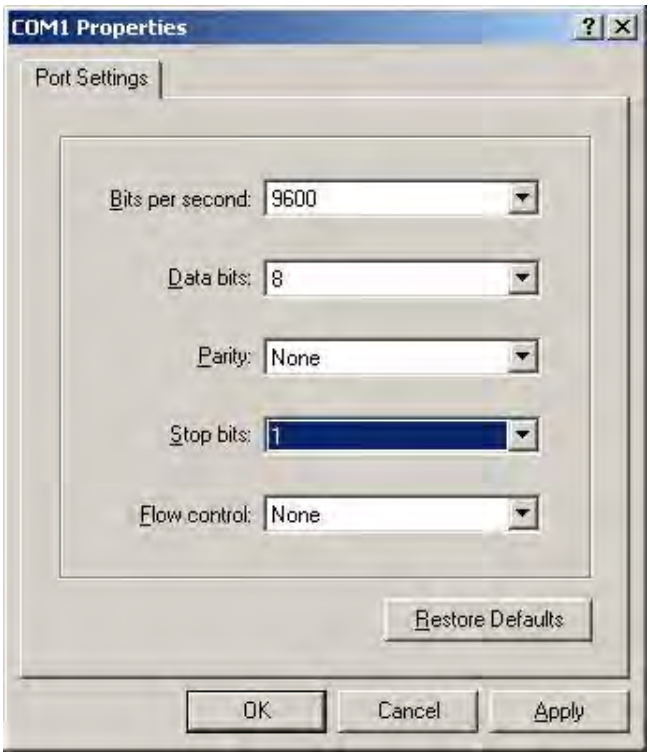
Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



Appendix A. Console Interface

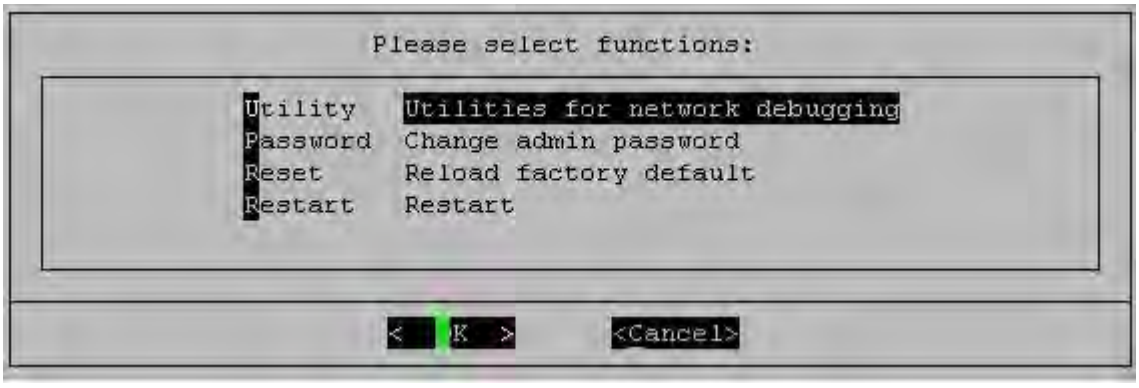
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. To connect the console port of LANPRO LP-NC1, you need a console, modem cable and a terminal simulation program, such as the Hyper Terminal.
2. If you use Hyper Terminal, please set the parameters as **9600,8,n,1**.



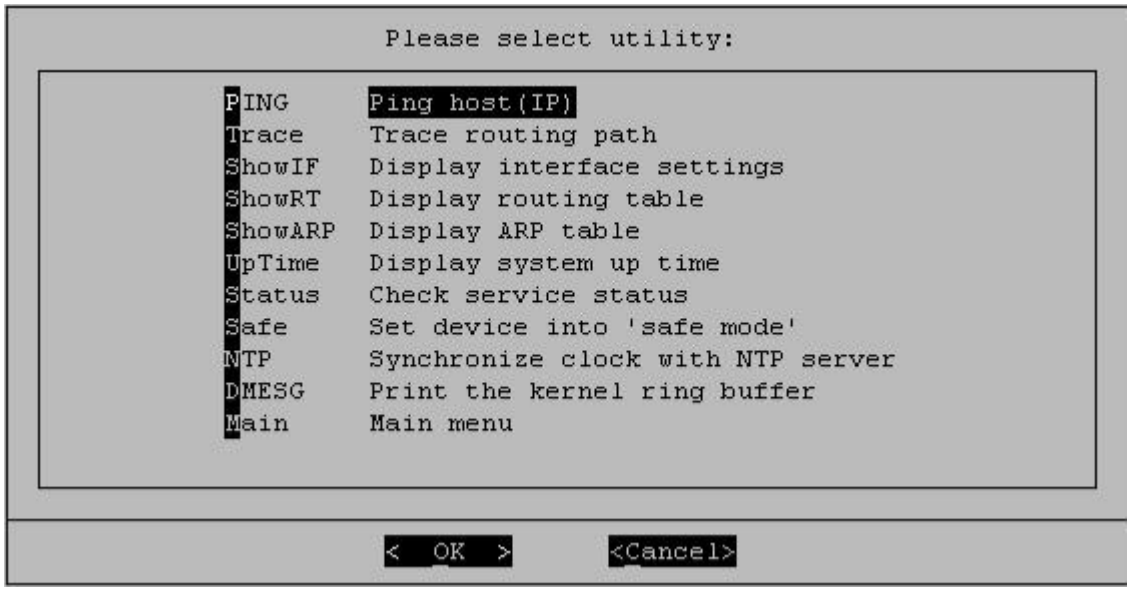
Caution: the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the Enter key to make selection or confirm what you enter.

3. Once the console port of LANPRO LP-NC1 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system and the welcome screen or the main menu should appear. If you are still unable to see the welcome screen or the main menu of the console, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follow:



  - 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: It 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 turn on) is displayed.
  - Check service status: Check and display the status of the system.
  - Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set LANPRO LP-NC1 into safe mode, then administrator can management this device with browser again.
  - 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, therefore we must reset the internal clock through the NTP.
  - Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
  - Main menu: Go back to the main menu.

- **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, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

  The username is "admin" and the default password is also "admin", which is the same as for the web management interface. You can use this option to change the administrator's password. Even if you forgot the password and are unable to log in the management interface from the web or the remote end of the SSH, you can still use the null modem to connect the console management interface and set the administrator's password again.

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, we recommend you to immediately change the LANPRO LP-NC1 Admin username and password after logging in the system for the first time.

- **Reload factory default**

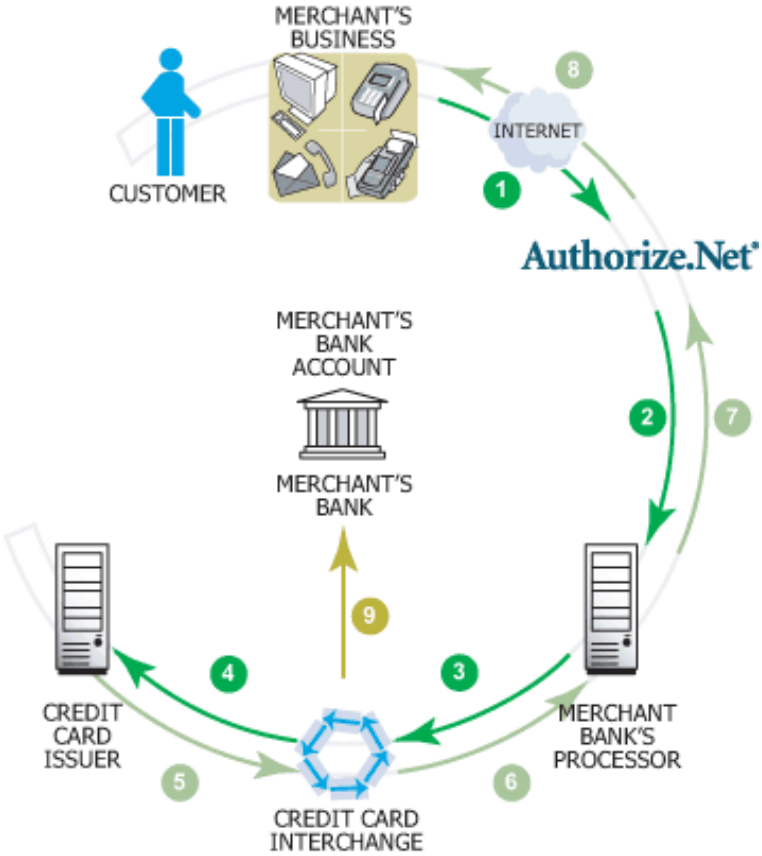
  Choosing this option will reset the system configuration to the factory defaults.

- **Restart LANPRO LP-NC1**

  Choosing this option will restart LANPRO LP-NC1.

Appendix B. Configuration on Authorize.Net

Before the "Credit Card" and related functions can be managed appropriately, LANPRO LP-NC1 requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that LANPRO LP-NC1 supports now. The figure below shows the process of the credit card billing and we will introduce some important procedures for configurations on Authorize.Net.



1. Setting Up

1.1 Open Accounts

As shown in the above figure, four elements are needed to begin an on-line business:

Element	Description
E-COMMERCE WEB SITE	LANPRO LP-NC1 has built-in web pages to present to end users to use credit cards
INTERNET MERCHANT ACCOUNT	A type of bank account that allows a business to accept Internet credit card
PAYMENT GATEWAY ACCOUNT	An Authorize.Net account is the type of account that is supported by LANPRO LP-NC1
CONNECTION METHOD	LANPRO LP-NC1 will take care of the communication with the Authorize.Net

Therefore, to set up LANPRO LP-NC1 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account). If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/. When the four elements are prepared, start configuring the settings on LANPRO LP-NC1 and Athorize.Net.

1.2 Configure LANPRO LP-NC1 using an Authorize.Net account

Please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → Click ***Credit Card*** → ***Credit Card Configuration***

Some major fields are required:

Setting	Description
Merchant Login ID	This is the "Login ID" that comes with the Authorize.Net account.
Merchant Transaction Key	To get a new key, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → Click ***Obtain Transaction Key*** → Enter **"Secret Answer"** → Click ***Submit***.
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll (default payment gateway)
MD5 Hash	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: **"MD5 Hash Value"**.

Note: For detailed description, please see 4.2.1.6.5 Credit Card.

1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of LANPRO LP-NC1

Settings of the merchant account on Authorize.Net should be matched with the configuration of LANPRO LP-NC1:

Setting	Description
MD5 Hash	To configure **"MD5 Hash Value"**, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***MD5 Hash*** → Enter **"New Hash Value"** & **"Confirm Hash Value"** → Click ***Submit***.
Required Card Code	If the **"Card Code"** is set up as a required field, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Card Code Verification*** → Check the ***Does NOT Match (N)*** box → Click ***Submit***.
Required Address Fields	After setting up the required address fields on the **"Credit Card Payment Page Fields Configuration"** section of LANPRO LP-NC1, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Address Verification System (AVS)*** → Check the boxes accordingly → Click ***Submit***.

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between LANPRO LP-NC1 and Authorize.Net, please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Credit Card*** → ***Credit Card Configuration*** → Go to "**Credit Card Payment Page Configuration**" section → Enable the **"Test Mode"** → Click ***Try Test*** and follow the instructions

2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as LANPRO LP-NC1.

2.1 Void A Transaction and Remove the On-demand Account Generate on LANPRO LP-NC1

Sometimes, a transaction may need to be canceled as well as the related user account on LANPRO LP-NC1 before it has been settled with the bank.

a. To void an unsettled transaction, please log in Authorize.Net. Click ***Unsettled Transactions*** → Try to locate the specific transaction record on the **"List of Unsettled Transactions"** → Click the ***Trans ID*** number → Confirm and click ***Void***.

Note: To find the on-demand account name, click Show Itemized Order Information in the "Order Information" section → Username can be found in the "Item Description"

b. To remove the specific account from LANPRO LP-NC1, please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Users List*** → Click ***Delete*** on the record with the account name.

2.2 Refund A Settled Transaction and Remove The On-demand Account Generated on LANPRO LP-NC1

a. To refund a credit card, please log in Authorize.Net. Click ***Virtual Terminal*** → Select Payment Method → Click ***Refund a Credit Card*** → Payment/Authorization Information → Type information in at least three fields: Card Number, Expiration Date, and Amount → Confirm and click ***Submit***.
b. To remove the specific account from LANPRO LP-NC1, please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Users List*** → Click ***Delete*** on the record with the account name

2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click ***Unsettled Transactions*** → Try to locate the specific transaction record on the **"List of Unsettled Transactions"** → Click the ***Trans ID*** number → Click ***Show Itemized Order Information*** in the **"Order Information"** section → Username and Password can be found in the **"Item Description"**.

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, LANPRO LP-NC1 will automatically send the customer an email receipt for each successful transaction via Authorize.Net. To change the information on the receipt for customer, please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Credit Card*** → ***Credit Card Configuration*** → ***Client's Purchasing Record*** → Type in information in the text boxes: **"E-mail Header and Description"** → Confirm and click ***Apply***.

2.5 Send An Email Receipt for Each Transaction to The Merchant Owner

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click ***Settings and Profile*** → Go to the **"General"** section → click ***Manage Contacts*** → click ***Add New Contact*** to → Enter necessary contact information on this page → Check the ***"Transaction Receipt"*** box → Click ***Submit***.

3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during A Period

Please log in Authorize.Net. Click ***Reports*** → Check **"Statistics by Settlement Date"** radio button → Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria → Click ***Run Report***

3.2 Transaction Statistics by Different Location

a. To deploy more than one LANPRO LP-NC1, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in LANPRO LP-NC1. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Credit Card*** → ***Credit Card Configuration*** → Go to **"Client's Purchasing Record"** section → Check the **"Reset"** box → A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number"** → Confirm and click ***Apply***.

b. Please log in Authorize.Net → Click ***Search and Download*** → Specify the transaction period (or ALL Settled, Unsettled) in **"Settlement Date"** section → Go to **"Transaction"** section → Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the **"Invoice #"** text box → Click ***Search*** → If transaction records can be found, the number of accounts sold is the number of search results → Or, click ***Download To File*** to download records and then use MS Excel to generate more detailed reports.

3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click ***Search and Download*** → Enter the information for a specific customer as criteria → Click ***Search*** → Click the ***Trans ID*** number to view the transaction details.

For more information about Authorize.Net, please see www.authorize.net.

Appendix C. Network Configuration on PC

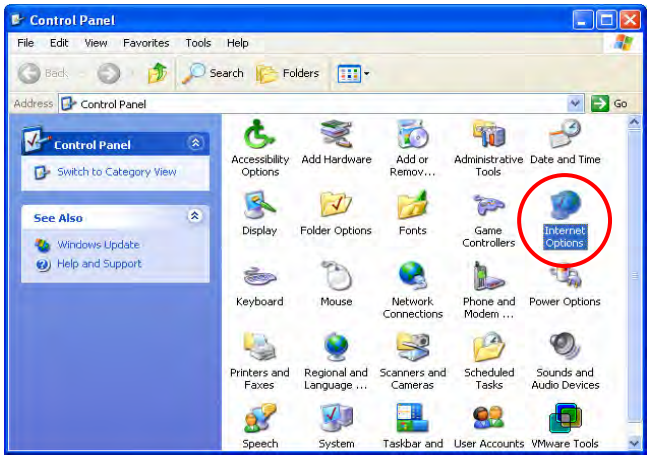
After LANPRO LP-NC1 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

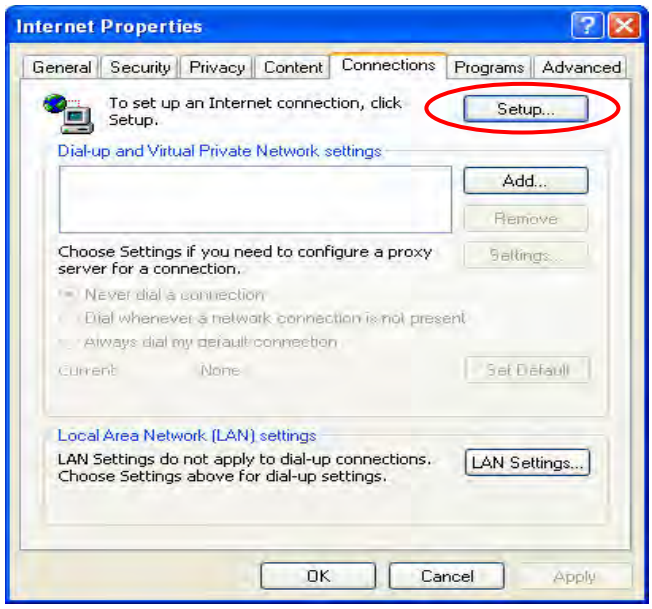
  If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

  ◆ **Windows XP**

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

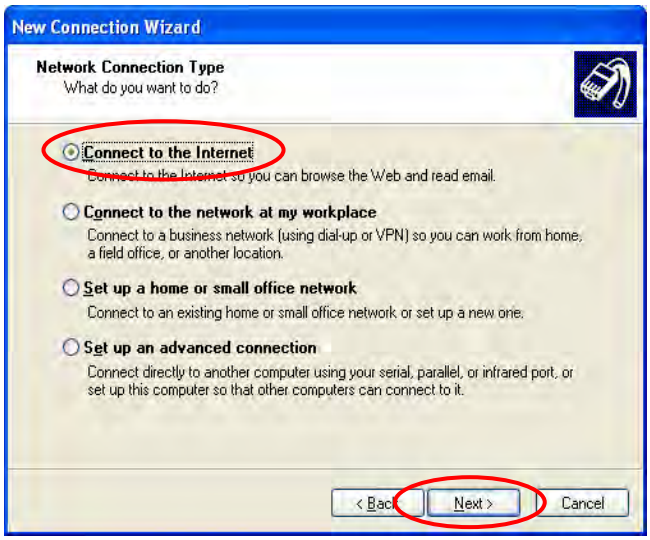


  2. Choose the **"Connections"** label, and then click ***Setup***.

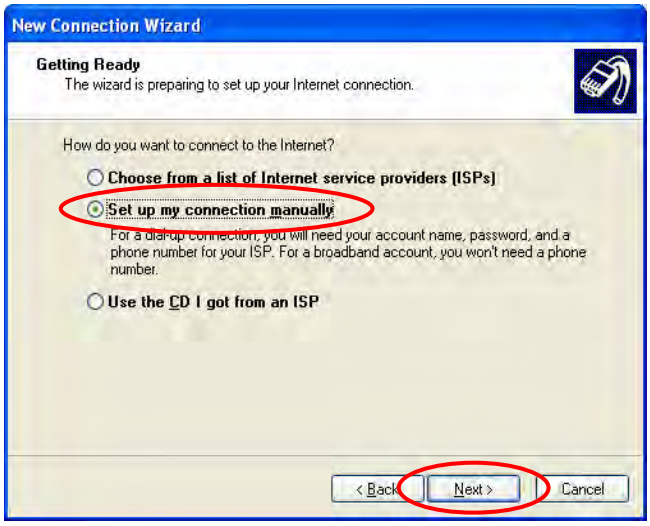


3. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.

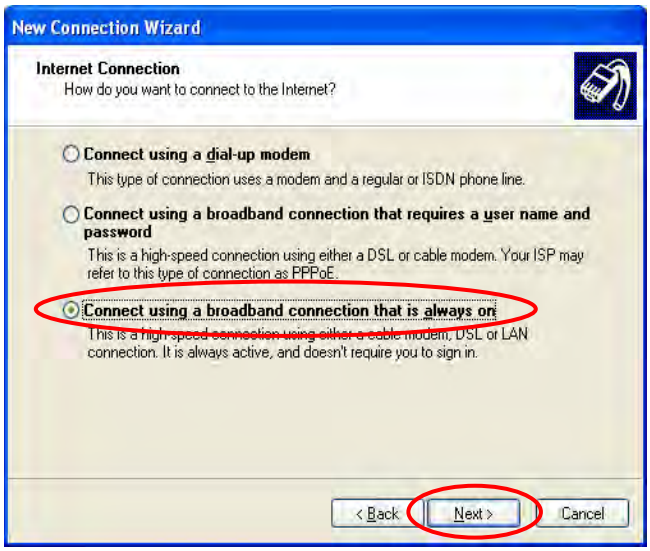
4. Choose **"Connect to the Internet"** and then click ***Next***.



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



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



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

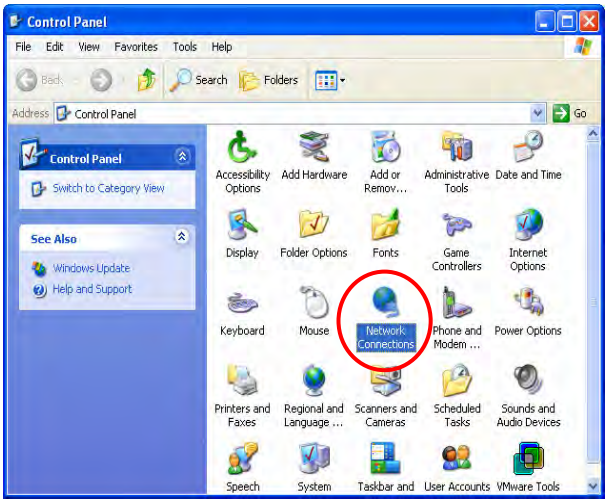
- **TCP/IP Network Setup**

  In the default configuration, LANPRO LP-NC1 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.

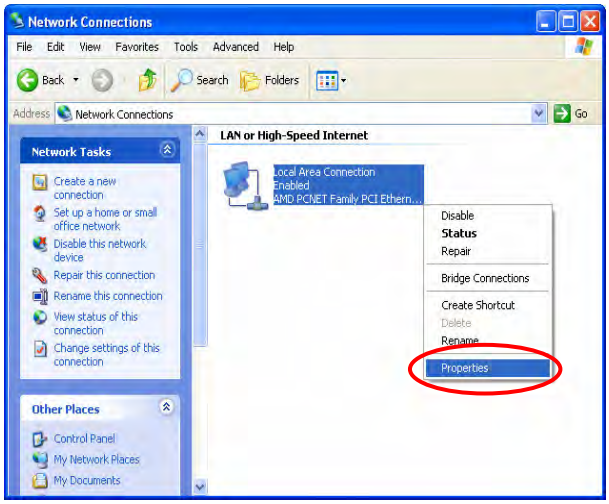
  If you want to check the TCP/IP setup or use a static IP to connect to LANPRO LP-NC1 LAN port, please follow the following steps:

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

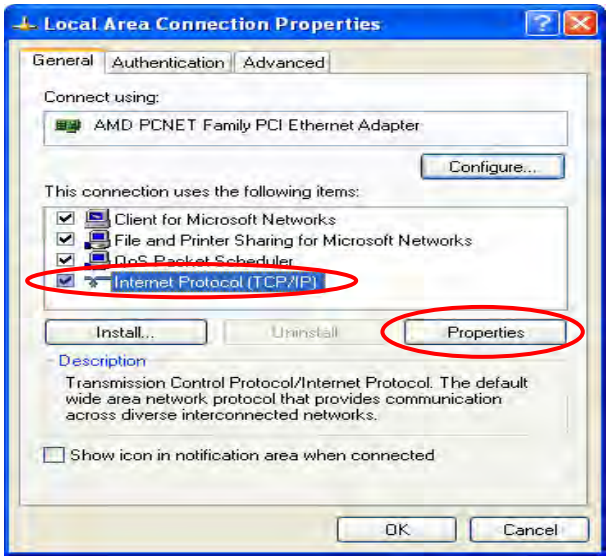
1. Select **Start > Control Panel > Network Connection**.



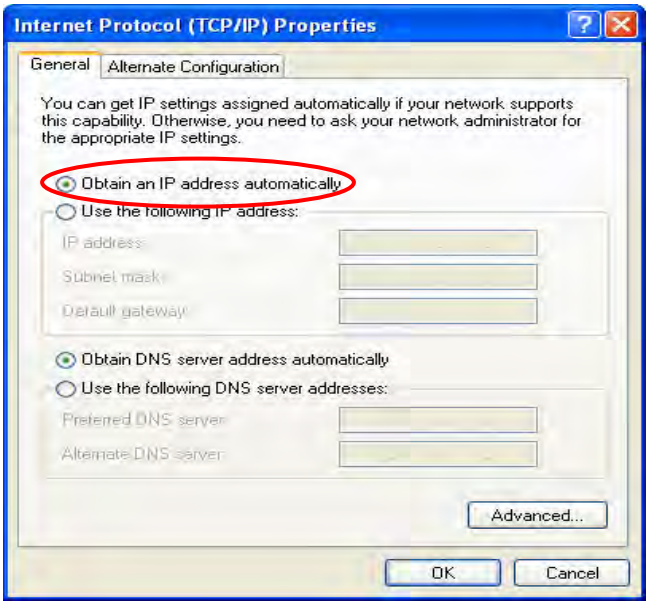
2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



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.

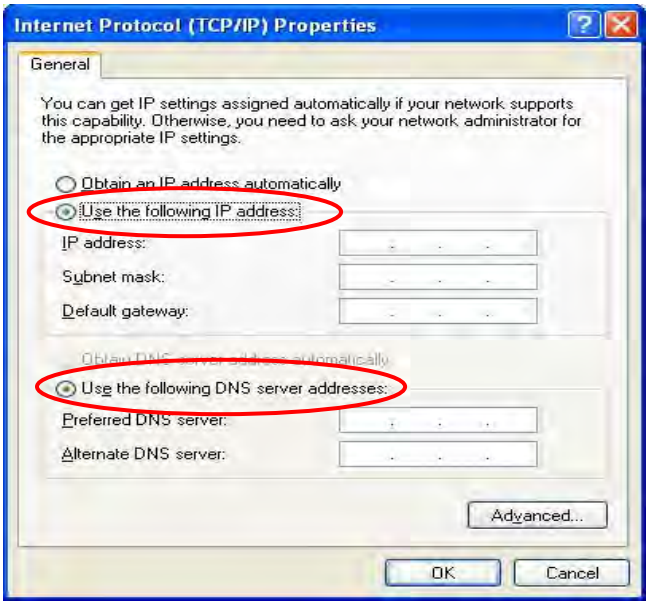


1-2. **Using DHCP:** If want to use DHCP, please choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from LANPRO LP-NC1.



2-2. **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of the LANPRO LP-NC1: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

- Please 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***.

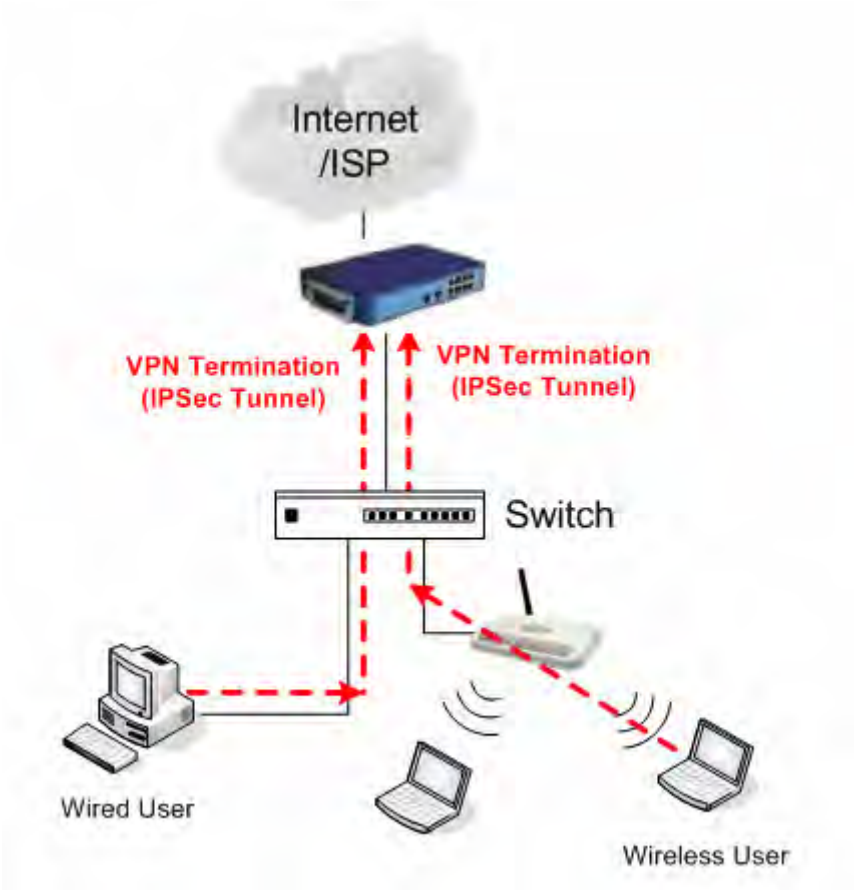


Appendix D. IPSec VPN Termination

LANPRO LP-NC1 has equipped with IPSec VPN feature starts from released version v1.00. To fully utilize the nature supported IPSec VPN by Microsoft Windows XP SP2(with patch) and Windows 2000 operating systems, LANPRO LP-NC1 implement IPSec VPN tunneling technology between client's windows devices and LANPRO LP-NC1 itself, no matter of through wired or wireless network.

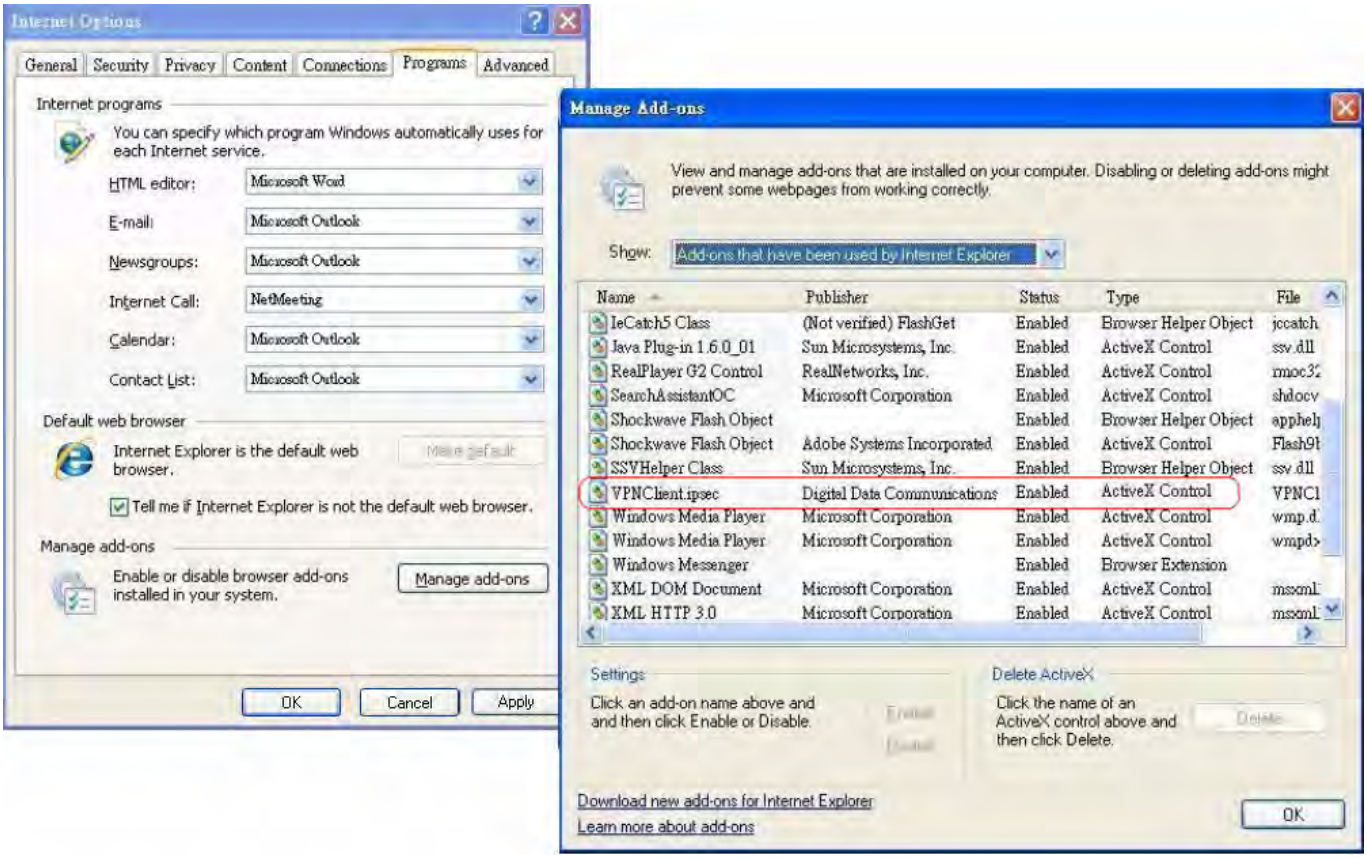
By pushing down ActiveX to the client's Windows device from LANPRO LP-NC1, no extra client software to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is configured automatically. At the end of this setup, a build-in IPSec VPN feature was enabled to be ready to serve once it is called to be setup.

The design goal is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of LANPRO LP-NC1 is based on ActiveX and the built-in IPSec VPN client of Windows OS.



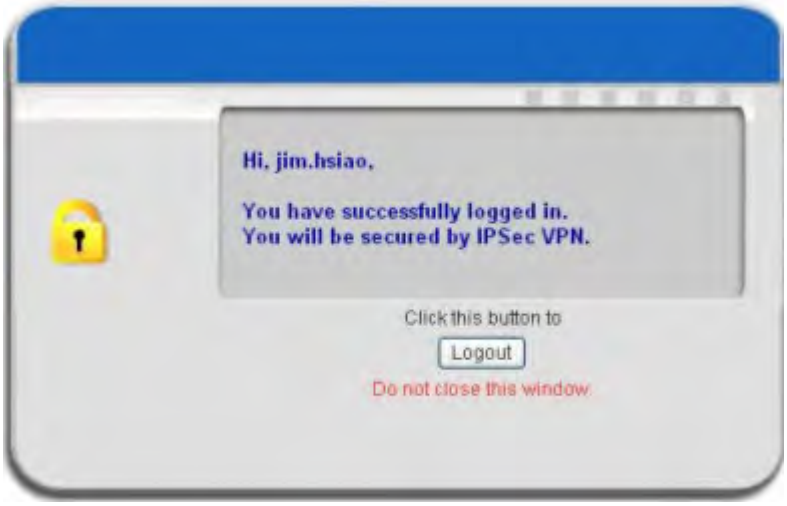
1. ActiveX component

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 was enabled.

During the first-time login to LANPRO LP-NC1, Internet Explorer will ask user to download the ActiveX component of IPSec VPN. This ActiveX component once downloaded will be running paralleled with the "Login Success Page" after the page being brought up successfully. The ActiveX component helps to setup the IPSec VPN tunnel between client's device and the LANPRO LP-NC1 controller, and 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 decompose the IPSec tunnel. Once the IPSec VPN tunnel was 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 design of LANPRO LP-NC1's IPSec VPN feature directly solves possible data security leak problem between client and the controller via either wireless or wired connection without extra hardware or client software installed.



2. Limitations

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

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

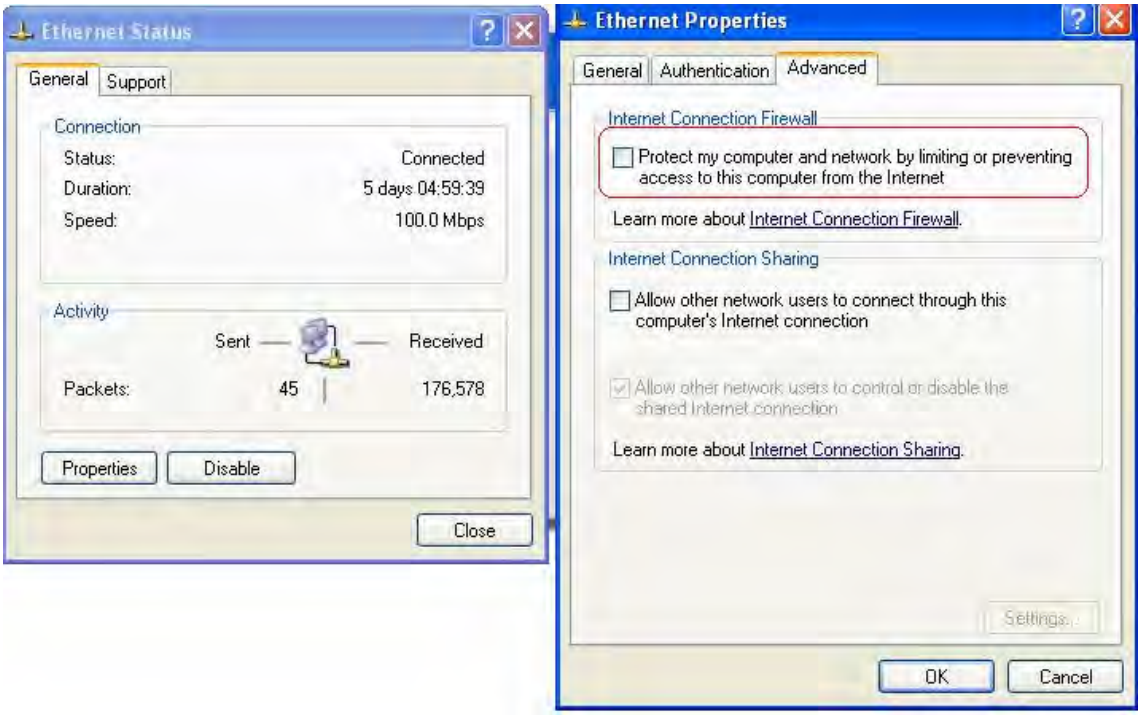
b. Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.

c. The Forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes IPSec tunnel can't be cleared 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.

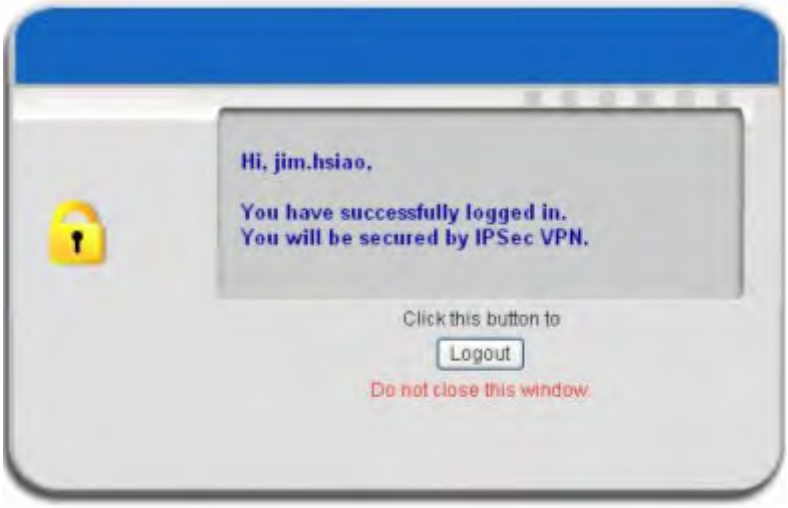
4. ICMP and Active Mode FTP

On Windows XP SP2 without patching by KB889527, it will drop ICMP packets from IPSec tunnel. This problem 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 the problem of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2.

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

5. The Termination of ActiveX

The ActiveX component for IPSec VPN is running paralleled with the web page of "Login Success". Unless user decides to close the session and to disconnect with LANPRO LP-NC1, the following conditions or behaviors of using browser shall be avoided in order to maintain the built IPSec VPN tunnel always alive.



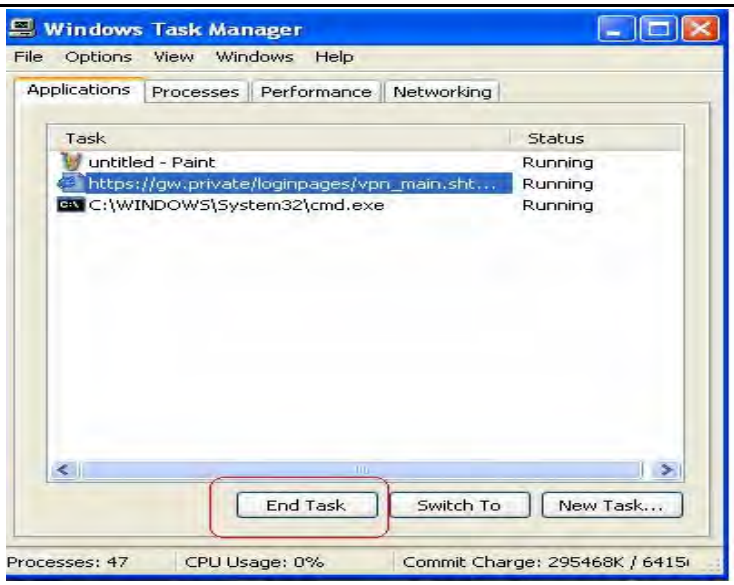
Reasons may cause the Internet Explorer to stop the ActiveX unexpectedly as followings:

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: Don't terminate this VPN task of Internet Explorer.



c. There are some cases of Windows messages by which LANPRO LP-NC1 will hint current user to:

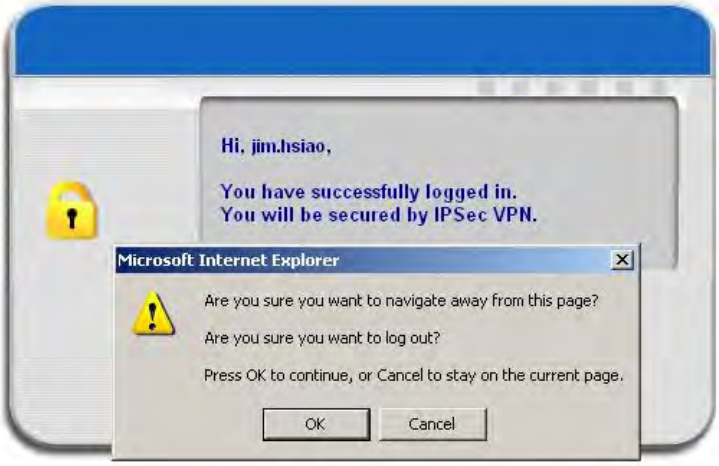
(1) Close the Windows Internet Explorer,

(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. email of Outlook) that occupies this existing Internet Explorer.



That shall all cause the termination of IPSec VPN tunneling if user chooses to click "Yes". The user has to log in again to regain the network access.

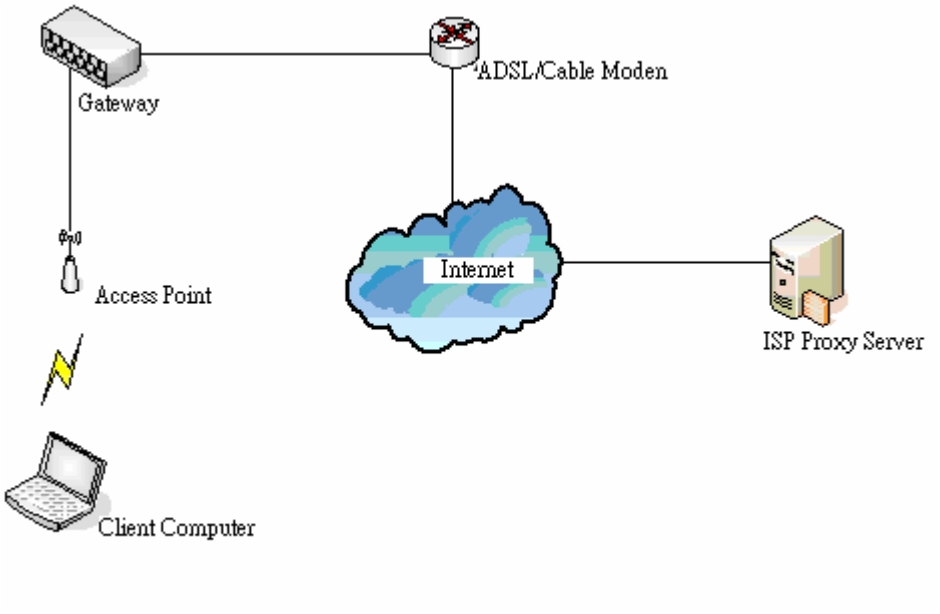
Suggestion: Click "Cancel" if you do not intend to stop the IPSec VPN connection yet.

6. Non-supported OS and Browser

In current version, Windows Internet Explorer is the only browser supported by LANPRO LP-NC1.Windows XP and Windows 2000 are the only two supported OS along with this release.

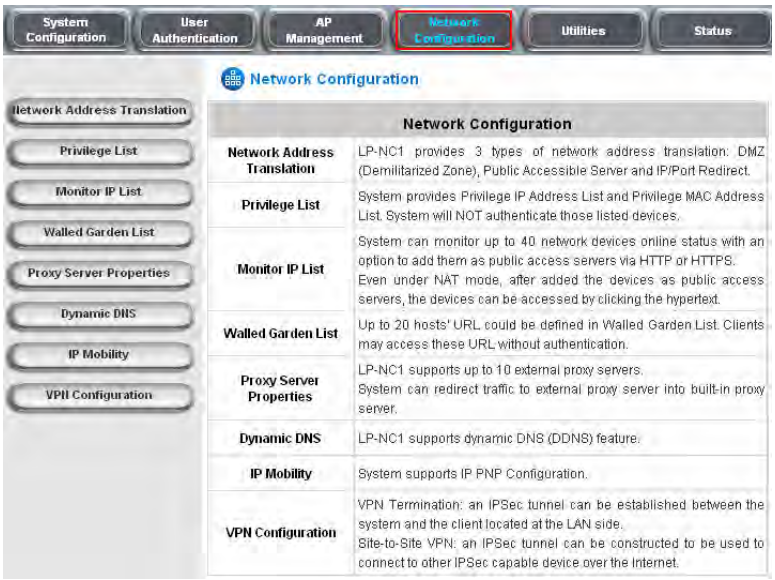
Appendix E. Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.



In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration：

1. Login Gateway by using "***admin***".
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



3. Click the ***Proxy Server Properties*** from left menu and the homepage of the **Proxy Server Properties** will appear.

External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

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

External Proxy Server		
Item	Server IP	Port
1	10.2.3.230	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

5. ***Enable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.

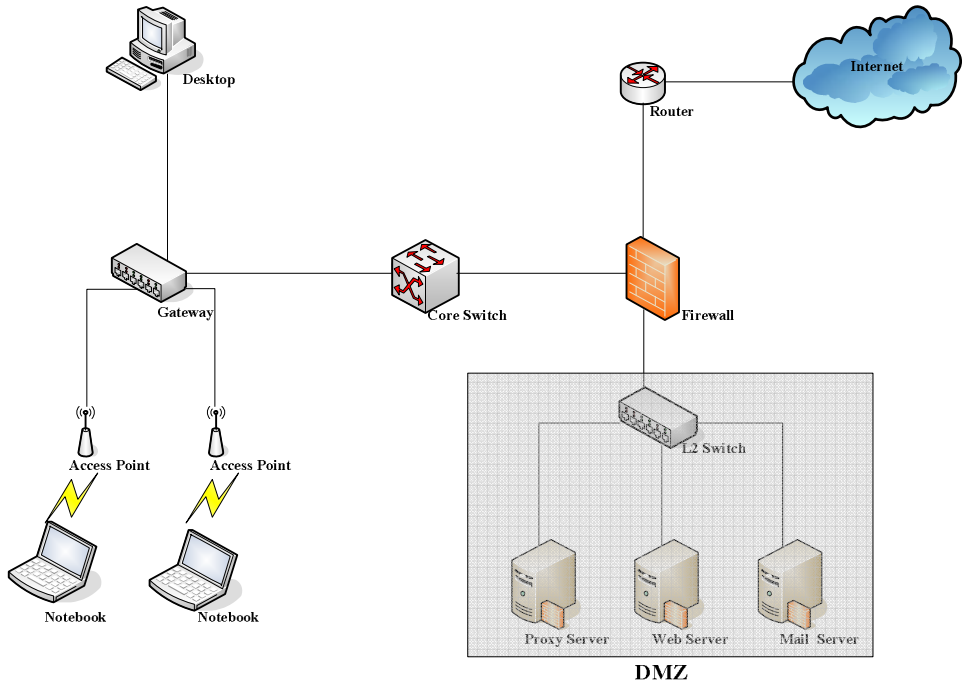
External Proxy Server		
Item	**Server IP**	**Port**
1	10.2.3.230	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	(•) Enabled ( ) Disabled

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

Appendix F. Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



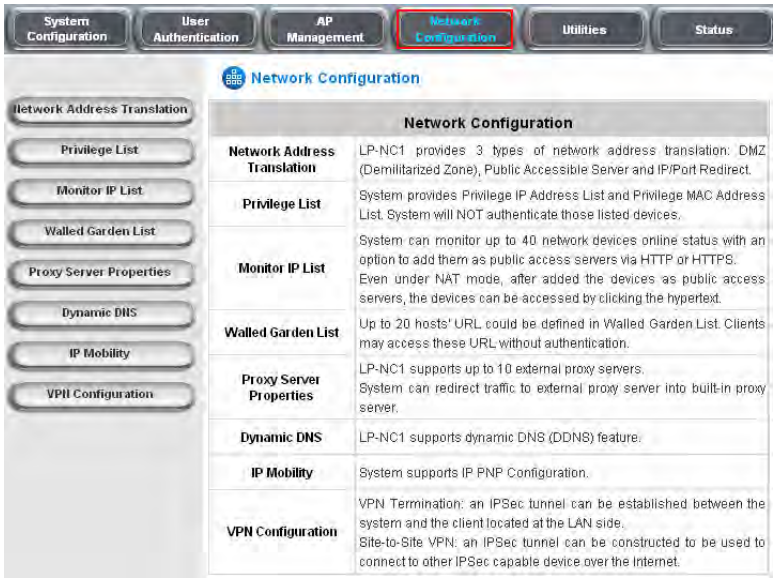
In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

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

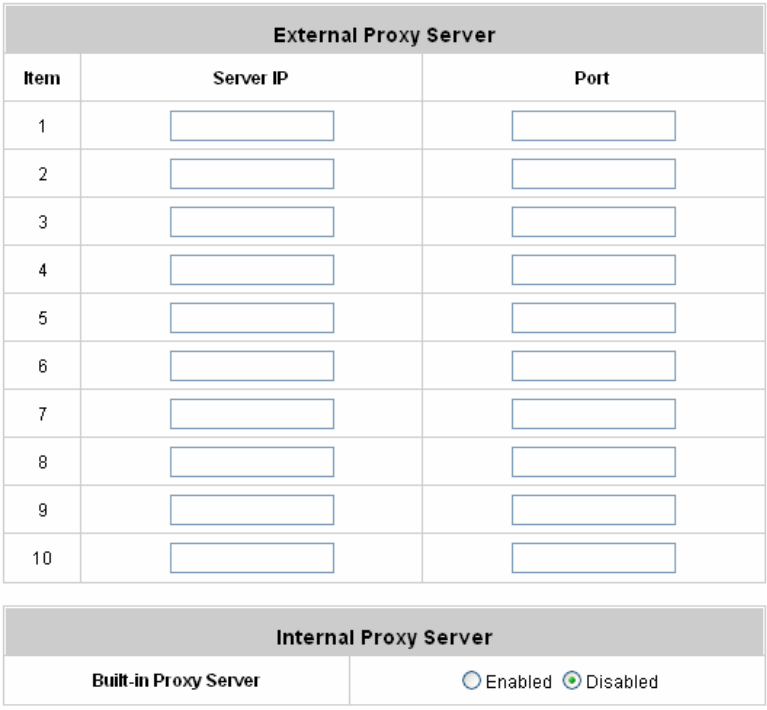
Please follow the steps to complete the proxy configuration：

■ Gateway setting

1. Login Gateway by using "***admin***".
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



3. Click the ***Proxy Server Properties*** from left menu and the homepage of the ***Proxy Server Properties*** will appear.



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

External Proxy Server		
Item	Server IP	Port
1	10.2.3.230	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

5. ***Disable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.

External Proxy Server		
Item	Server IP	Port
1	10.2.3.230	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

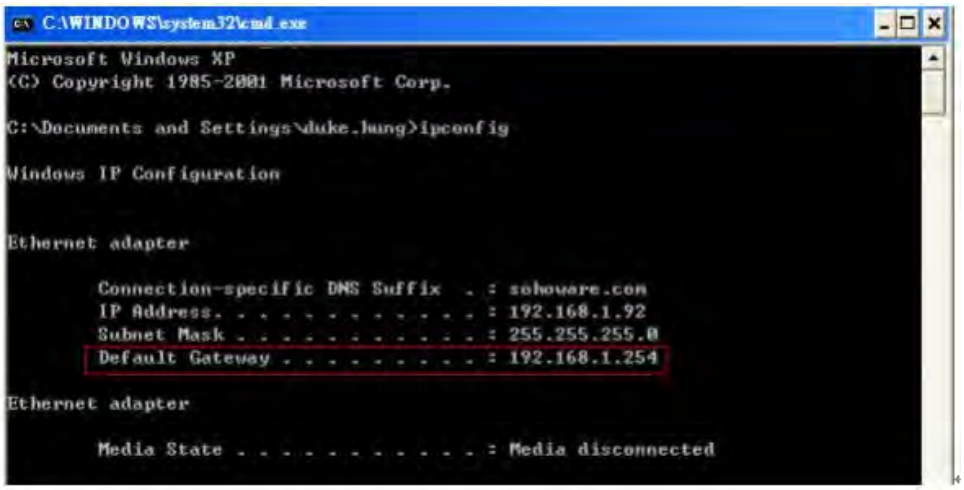
6. Click ***Apply*** to save the settings***.***

Warning : ***If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page won't appear because the proxy server is down. Please make sure your proxy server is always available.***

Client setting

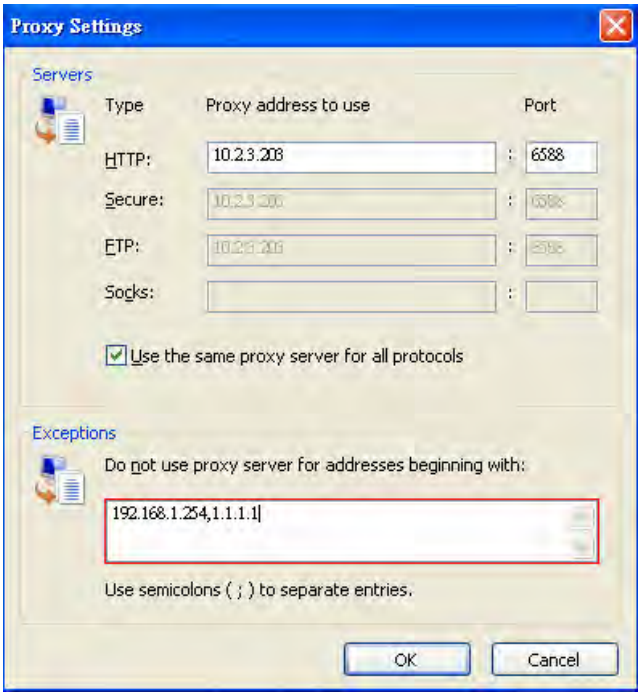
It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

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

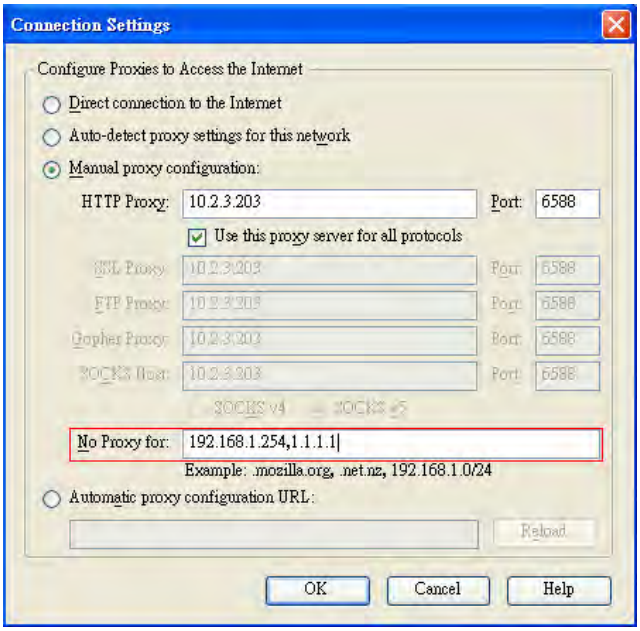


2. Open browser to add ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into proxy exception information.

   - For I.E



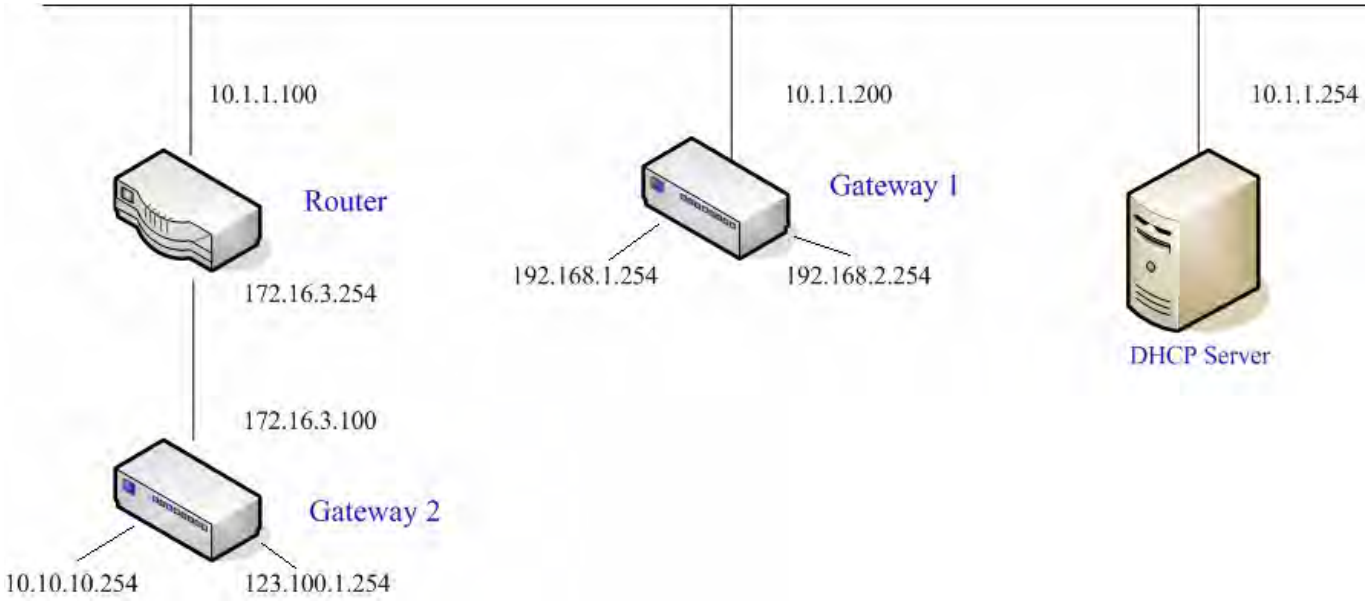
- For Firefox


Connection Settings
Configure Proxies to Access the Internet
Direct connection to the Internet
Auto-detect proxy settings for this network
Manual proxy configuration:
HTTP Proxy: 10.2.3.203
Port: 6588
Use this proxy server for all protocols
SSL Proxy: 10.2.3.203 Port: 6588
FTP Proxy: 10.2.3.203 Port: 6588
Gopher Proxy: 10.2.3.203 Port: 6588
SOCKS Host: 10.2.3.203 Port: 6588
SOCKS v4 SOCKS v5
No Proxy for: 192.168.1.254,1.1.1.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
OK
Cancel
Help

Appendix G. DHCP Relay

LANPRO LP-NC1 supports DHCP Relay defined according to RFC 3046. For scaling reasons, it is advantageous to set up an external DHCP server other than having the internal DHCP server implemented in LANPRO LP-NC1 to assign an IP. When forwarding client-originated DHCP packets 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 the information to implement IP address or other parameter assignment policies. The external DHCP server then echoes the option back to the relay agent in server-to-client replies, and the relay agent strips 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 DHCP Server.

When a client requests IP address from Gateway 1 Public LAN through the build-in DHCP relay agent of LANPRO LP-NC1, the DHCP server will receive a DHCP REQUEST packet with Option 82 (a code defined in RFC 3046). Also a Circuit ID will be sent by LANPRO LP-NC1 when DHCP relay is enabled to define where the packet is sent from, and this Circuit ID should have a format of MAC_IP, such as 00:E0:22:DF:AC:DF_192.168.1.254. Therefore, when the external DHCP server gets the request packet, it knows 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;
        }
```

From the file, client that connects to LANPRO LP-NC1 sends out a DHCP request. DHCP relay function in LANPRO LP-NC1 is enabled and sending a Circuit ID 00:90:0B:07:60:91_192.168.1.254 to the external DHCP server. When 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 can be 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.

Appendix H. Session Limit and Session Log

▪ Session Limit

To prevent ill-behaved clients or malicious software from using up system's connection resources, administrators will have to restrict the number of concurrent sessions that a user can establish.

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350, and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to the Syslog server specified in the ***Notification Configuration.***
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in the network deployment to protect the network in daily operation.

▪ Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- The following table shows the fields of a session log record.

Field	**Description**
Date and Time	The date and time that the session is established
Session Type	[New]: This is the newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user; It shows "N.A." if the user or device does not need to log in with a username. For example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Note: Only 31 characters are available for the combination of Session Type plus Username. Please change the account name accordingly, if the name is not identifiable in the record.
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the user's computer or device
SIP	The source IP address of the user's computer or device
SPort	The source port number of the user's computer or device
DIP	The destination IP address of the user's computer or device
DPort	The destination port number of the user's computer or device

- The following table shows an example of the session log data.

Jul 20 12:35:05 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
Jul 20 12:35:05 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
Jul 20 12:35:06 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
Jul 20 12:35:06 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
Jul 20 12:35:07 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
Jul 20 12:35:09 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
Jul 20 12:35:10 2007 [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80

P/N: V20020070921