

LP-NC1

LPNC1_M123_ENB01W

Characteristics

- IEEE802.3 10Base-T and IEEE802.3u 100Base-TX specifications compliant.
- Supports the IEEE802.3x Half/Full-Duplex standard.
- Store-and-Forward switching ensuring data completeness.
- Automatic separation technology can reduce network traffic congestion preventing packet losses.
- Plug and play, a status Led shows when the device is working.
- 2Mbyte Internal Memory, More Speed less disorder.
- Supports Auto-Negotiation, Half/Full-Duplex with auto-detection.
- With a dedicated UPLINK push-button, easy to connect
- Internal separate FIFO, no data packet loss warranty.
- Separate External power ensures work stability.



LanPro LP-NC1 Network Access Controller 123 Manual

The LP-NC1 by LanPro is a Network Access Controller, specially designed for wired and wireless data network environments in small to middle scaled businesses. It features integrated management and secured data transmission and, at the same time, ensures a mobile and efficiently productive working environment. System administrators can effectively monitor wired or wireless users, including employees and guest users via its user management interface. The LanPro's LP-NC1 performance is that of a powerful network controller but at a very competitive price.

The Lanpro's LP-NC1 is a very versatile and functional equipment that requires the handling and understanding of the following definitions and/or terminology, please read them before trying to connect this equipment

Ports: it refers to all the physical connections to this equipment that are made with patch-cords.

Uncontrolled Ports: It refers to the connections able to manage and configure the LP-NC1.

Controlled Ports: Are those connections able to use the resources in a controlled manner. They need no access to the configuration console.

User Validation: this is the LP-NC1 is user validation process.

In this document, three (3) typical connection cases are presented. There are more implementation possibilities based on each specific environment.

Scenario 1

Scenario #1: Using the LP-NC1 in a small size corporation without a user validation server and with access control and bandwidth restriction per user.

Please see figure 42

Scenario 2

Scenario #2: Using the LP-NC1 in a medium size corporation, where there is need for user access restriction and validation to an internal Server and to the corporation resources, there also is a group of users with Internet service access and bandwidth limitation.

Please see figure 43

Scenario 3

Scenario #3: Using the LP-NC1 in an ISP that requires bandwidth control to their affiliated users and their monitoring. User validation through another server (Not the LP-NC1)

Please see figure 44

LP-NC1 Installation steps.

1. Please review box contents as shown in figure 1:

Contents:

- A. 1 LP-NC1 Equipment.
- B. 1 120-240 VAC a 12 VAC 1.5 A , wall power supply.
- C. 1 Fast Installation Guide 123 (This document)
- D. 1 CD With Manuals.
- E. 2 patch-cords



figure 1

Default values Table:

- Controlled Ports Lan1, Lan2, Lan3, Lan4 network segment: 192.168.1.x DHCP server active
- Not Controlled ports: Lan5, Lan6, Lan7, Lan8 network segment: 192.168.2.x DHCP server active
- User: admin, manager, operator
- Password: admin, manager, operator
- Equipment administration address, not controlled ports only: 192.168.2.254
- Wan1 port: Set to obtaining Dynamic address
- Wan2 port: not configured. For fault tolerant management only.

Important Notice: Once the user password: "admin" is changed, the only way to reestablish the factory values is with a console cable and a program similar to "Telnet".

Please use figure 2 for cable specifications:

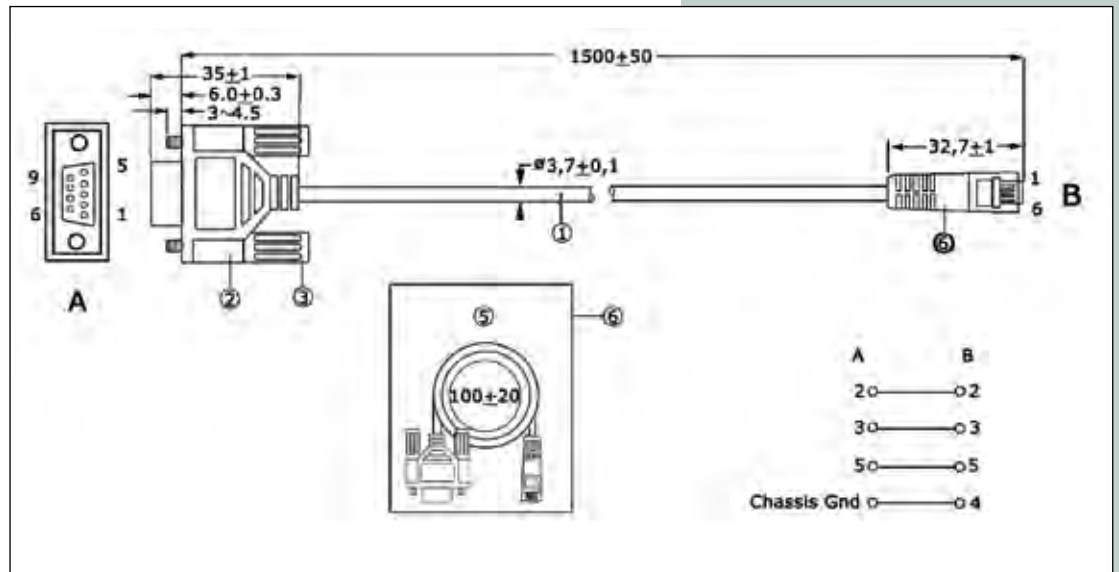


figure 2

2. The Basic configuration for the LP-NC1 for any of the scenarios is as follows:

A. Connect your Internet service to the Wan1 port as shown in figure 3



figure 3

B. Connect your computer to a non-controlled port (Lan5, Lan6, Lan7 o Lan8), configure the network card of your computer to obtain the IP address automatically, as shown in figure 4.



figure 4

C. Open your preferred browser in the following address: 192.168.2.254 as shown in figure 5

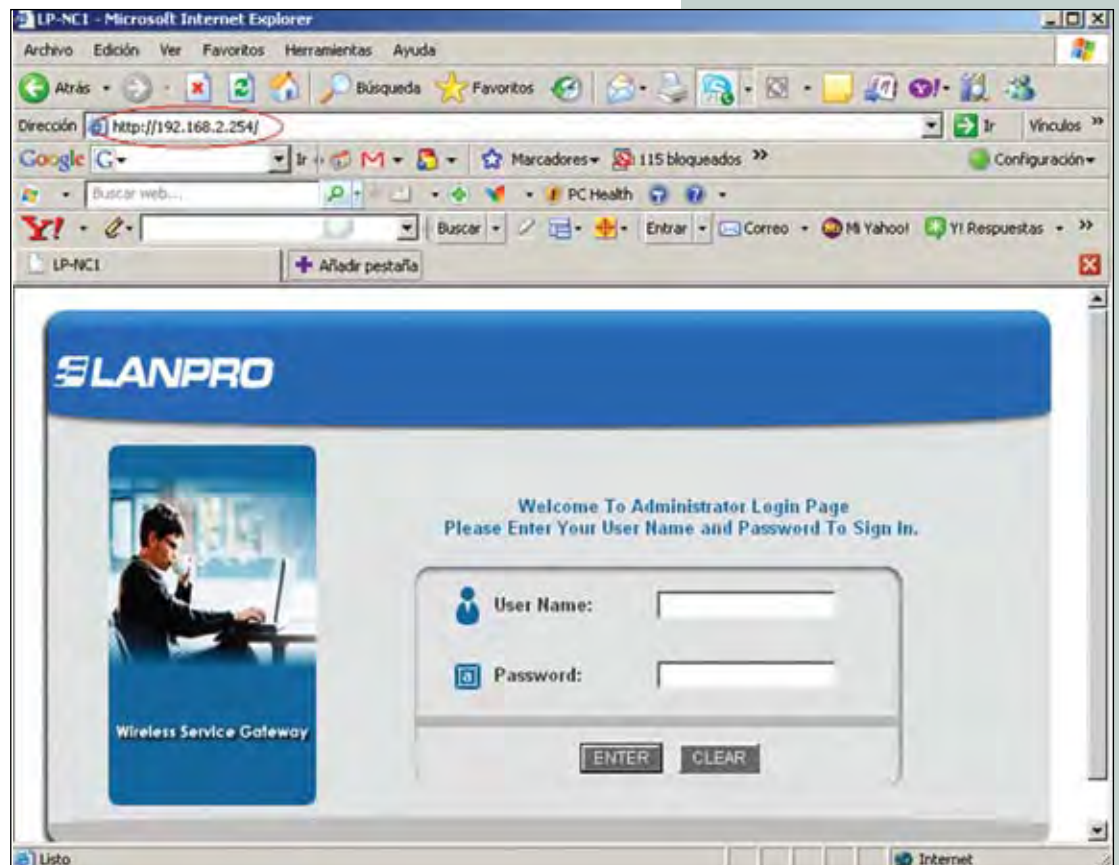


figure 5

D. Once the equipment prompts with the validation window, use the word: "admin" in both fields, as shown in figure 6.

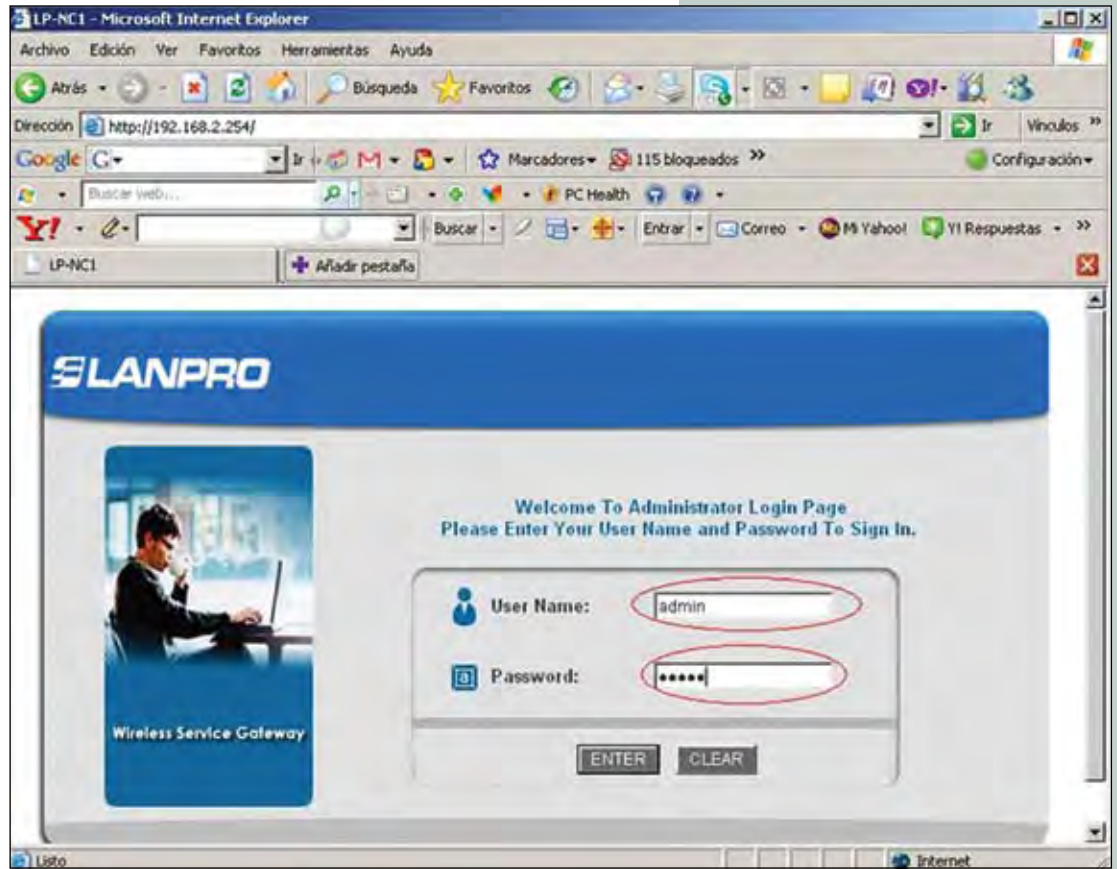


figure 6

E. Once the entries are validated, the system will show configuration menus and sub-menus as shown in figure 7, the welcome window.

At this moment, you must be aware of the configuration chosen from the ones presented in this manual. You can adapt it to your needs instead.



figure 7

F. It is recommended to have a password change policy. It must be stored in a safe place. In case you lose it, a restore procedure requiring a console cable is mandatory. This cable is mentioned in paragraph 1. Select the "Utilities" submenu as shown in figure 8, and then: "Change Password" option.



figure 8

G. The password change window will prompt you now as shown in figure 9. It is important to mention that the LP-NC1 has three (3) management levels and you will be able to change all of them in this page. The differences between these three levels are:

Admin: Can change all the configurations of this equipment.

Manager: The manager can change accounts, modes of authentication, group management, all for controlled ports.

Operator: Restricted to user account provisioning demand and will be automatically redirected to this site.

All the positions should be filled, and then select: "Apply" in each of the options so the change takes place. Please take in mind that the "Login" will always be: "admin", "manager" or "operator".

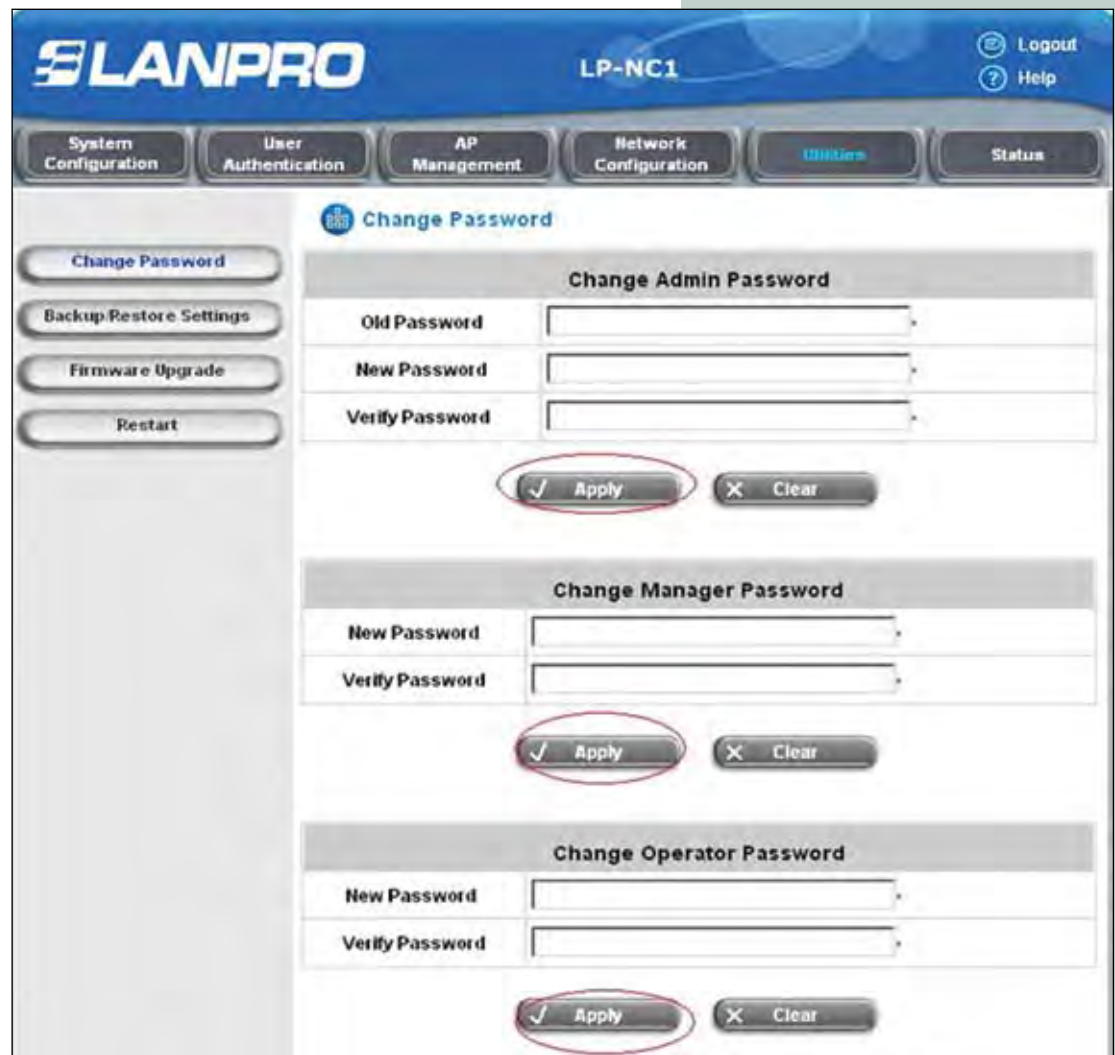


figure 9

- Once done and if needed, you can proceed to change WAN ports configurations. This depends on your ISP settings. At this moment you must decide if you need the fault tolerant mode, if so, proceed to configure it.
- Once done and if needed, you can proceed to change WAN ports configurations. This depends on your ISP settings. At this moment you must decide if you need the fault tolerant mode, if so, proceed to configure it.



figure 10

- Please proceed to select the option "WAN2 & Failover" if needed, as shown in figure 11, you must place there the type of WAN2 connection which supports a fixed or dynamic IP only, then, you should write the URL against the which you detect the missing internet service. You will be able to place a message by selecting the "Warning of Internet Disconnection" in case there is no ISP service.



figure 11

- You can now proceed to configure the roles of the controlled or non-controlled ports by selecting the LAN Port Roles option and marking the positions of the ports you want to set as controlled, please see figure 12. Take care not to change the port you are using for administration, as you will move it to another segment and will not be able to administer the equipment anymore. It should be mentioned at this point that by connecting a switch to any of these ports, it replicates the characteristics of controlled or non-controlled to all the associated ports. i.e.: by connecting a switch to a controlled port, all the ports become controllable. Once selected, please proceed to make the changes by selecting the "Apply" button.



figure 12

- Now proceed to configure the network characteristics of the controlled ports by selecting the "Controlled Configuration" option and specifying if you want to "NAT" or route, the IP address of the default gateway and the SUBNET. (See figure 13). Besides being able to configure DHCP option for assigning addresses to these connections, you can relay the DHCP requests to a dedicated Server by selecting the "DHCP Relay" option. After the selection, click "Apply". There is an available option that lets you add reserved addresses inside the segment.

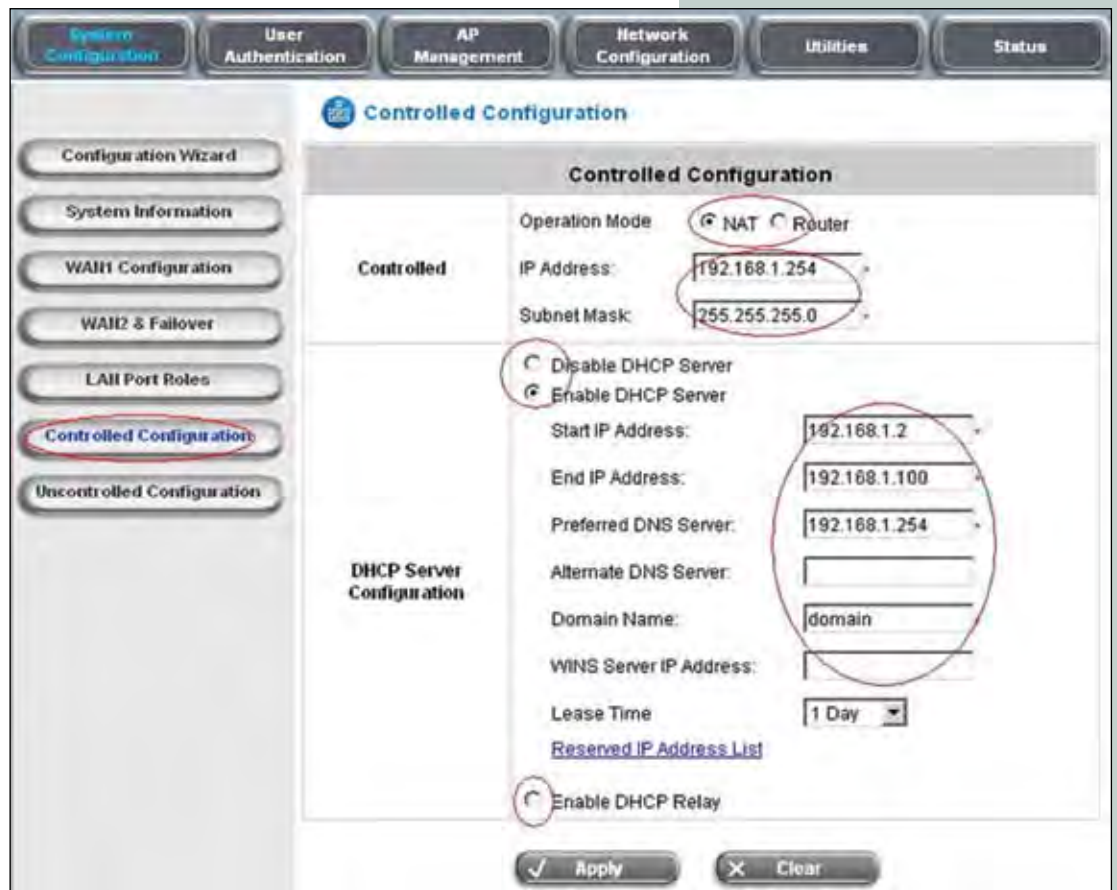


figure 13

• Please proceed to configure the network characteristics of the controlled ports by selecting the “Uncontrolled Configuration” button as seen in figure 14. Once there, please specify if you want to do “NAT” or routing of the “IP” address to the default gateway, the subnet. Besides being able to configure DHCP options for assigning these connection IP addresses, you can relay the DHCP requisitions to a dedicated server by selecting: “Enable DHCP Relay”. Once changes are selected, press “Apply”. There is an available option that lets you add reserved addresses inside the segment.

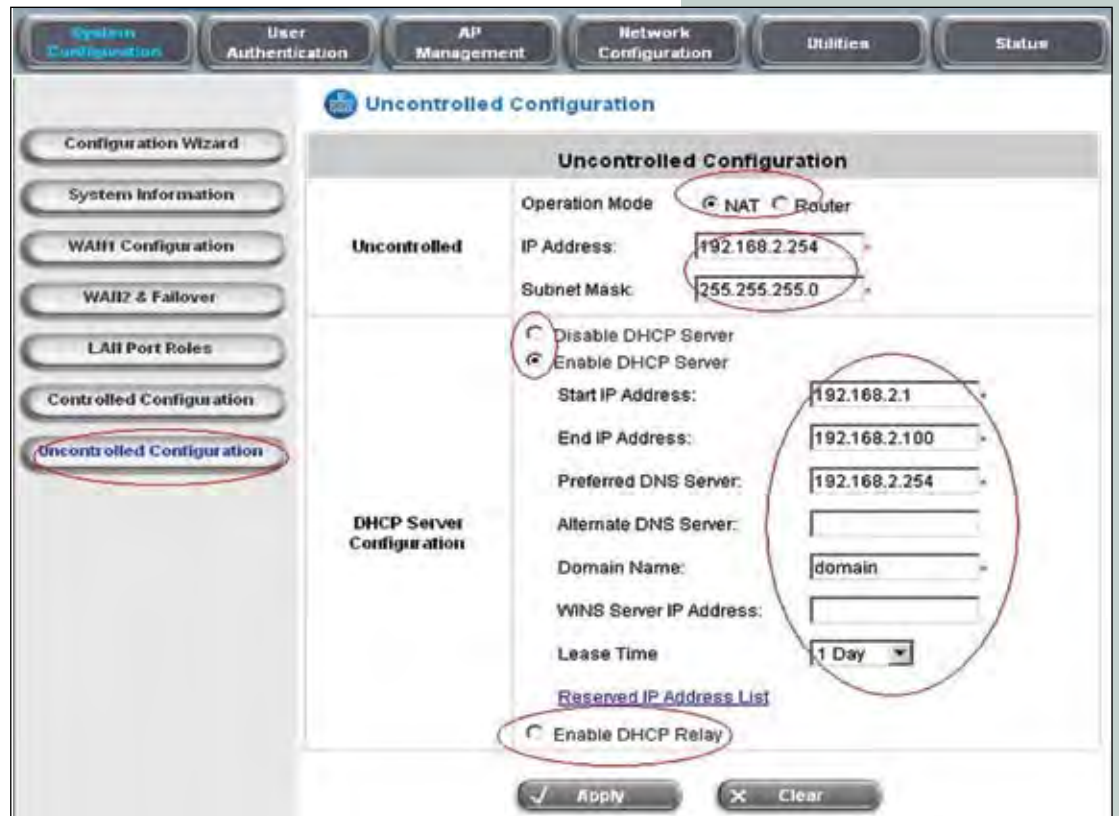


figure 14

3. Once you arrive to this point in the configuration of the LP-NC1, it is almost done. You can now configure depending on the chosen scenario. You can find an example matching your needs in the following paragraphs:

A. Scenario #1 (Please see figure 42). Assemble the connections as per the network diagram and proceed to configure the LP-NC1 as follows.

a) Authentication module configuration:

In the window shown in figure 15, select: “User Authentication” sub-menu, then: “Authentication Configuration”, enable Server #1 as default. It is important to remark that there can be more than one authentication server but only one will be the default one. This means that it doesn’t require a postfix for validation. In this particular case, a local methodology applies in which the names are created by the LP-NC1. Select the “Apply” command for the selections to take place. Once done, select the Server name. When the configuration window pops-up you can add the accounts and user group policies as explained in the following paragraphs:



figure 15

b) In the window shown in figure 16, proceed to configure options like the server name, or to change the "Postfix" (which applies to server authentication only, except the one marked as default). If you need more information, please refer to the manual. Proceed to select "Local User Settings" that will take you to the next step. You can now select this user group policy setting (Explained in paragraph number h). Remember that there is no need to change any of these options, unless you wish to customize them.



figure 16

c) In the window shown in figure 17, select "Edit Local User List"

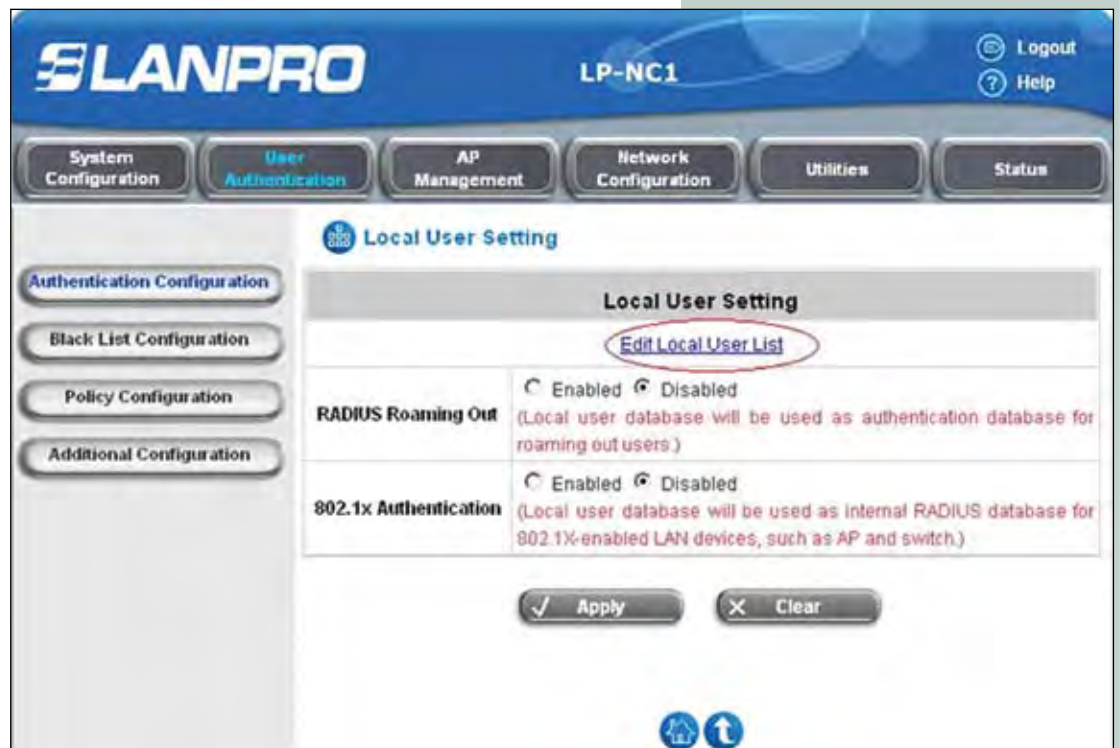


figure 17

d) In the window shown in figure 18, you can add the user one by one or load them from a text file. You can back it up also in a text file. We will describe the steps to follow and for making the back up of the users in a text file.



figure 18

e) Adding a user needs that you select option "Add User", (in the window shown in figure 19). Add the "Username", password and the policy to be applied. Remember that the differentiation in bandwidth limitations will be applied as per these policies. At this time, you must define user groups and in paragraph h, you will know how to modify these policies. Select Apply when finished and you will be immediately informed that the users were added.



figure 19

f) In order to Load the User List, select option: Upload Users as shown in the window pictured in figure 20. Explore and select the file. Then select the option: Upload. We have included an example of that file in figure 21, for more details please refer to the LP-NC1 Technical Manual.

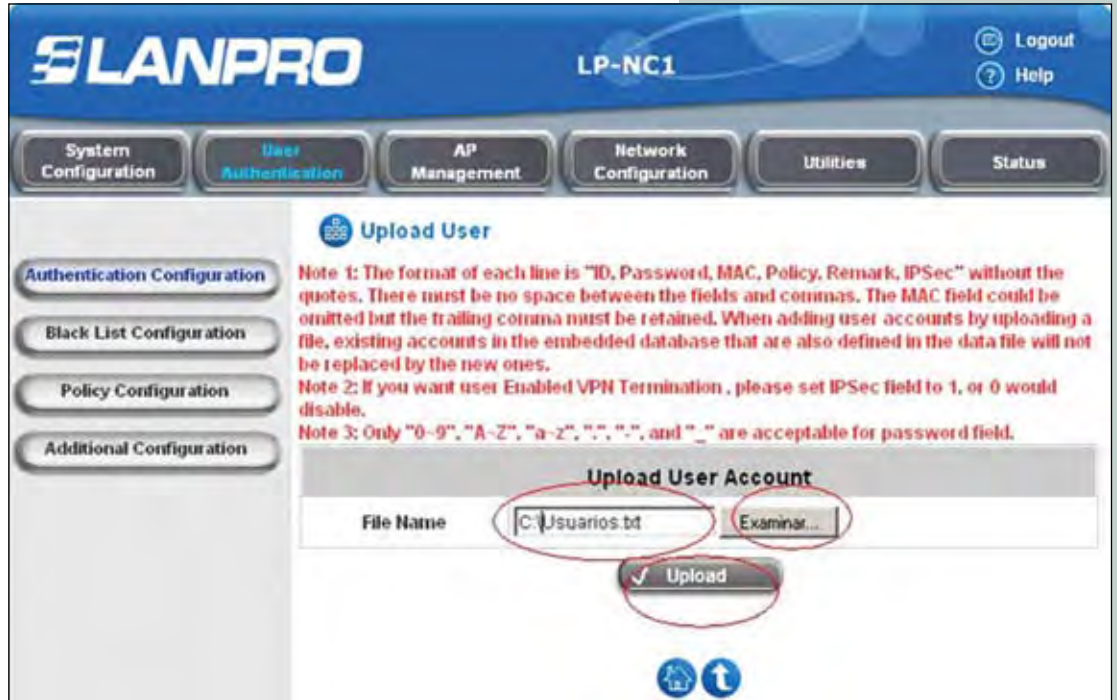


figure 20

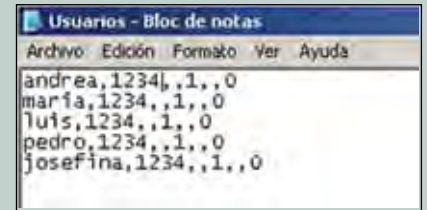


figure 21

g) Backing up the User List can be done when you select the option: "Download Users", as shown in figure 22. a new window appears in HTML format: select: "Save As" and specify the location.

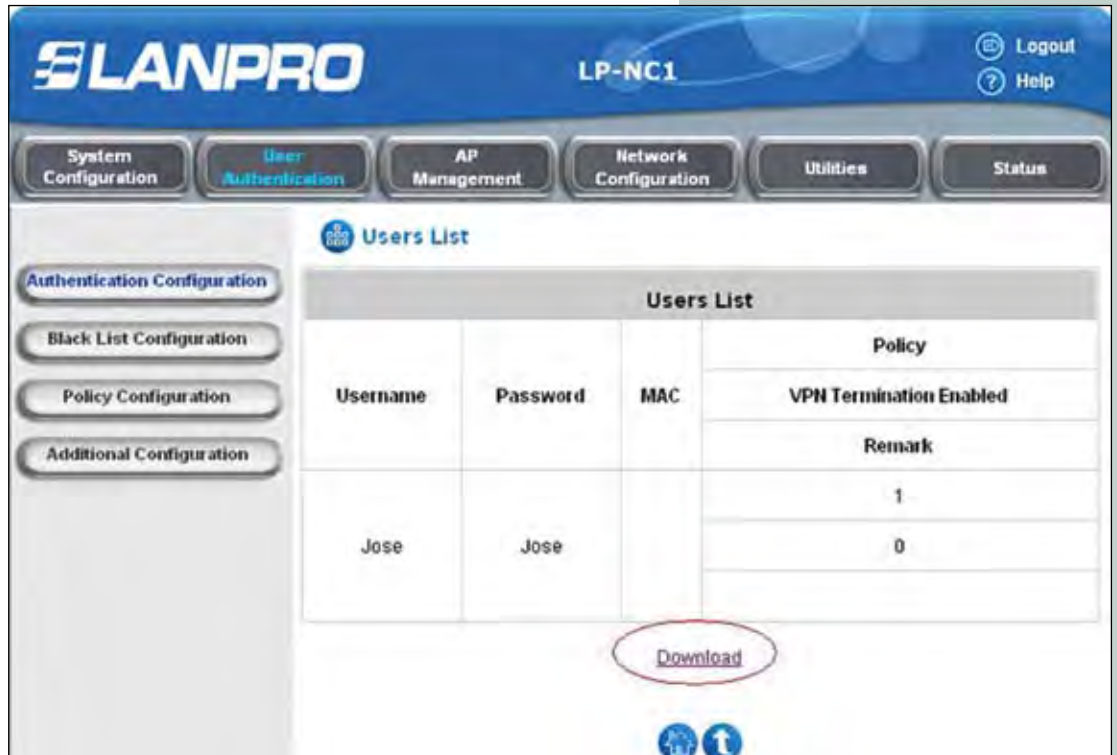


figure 22

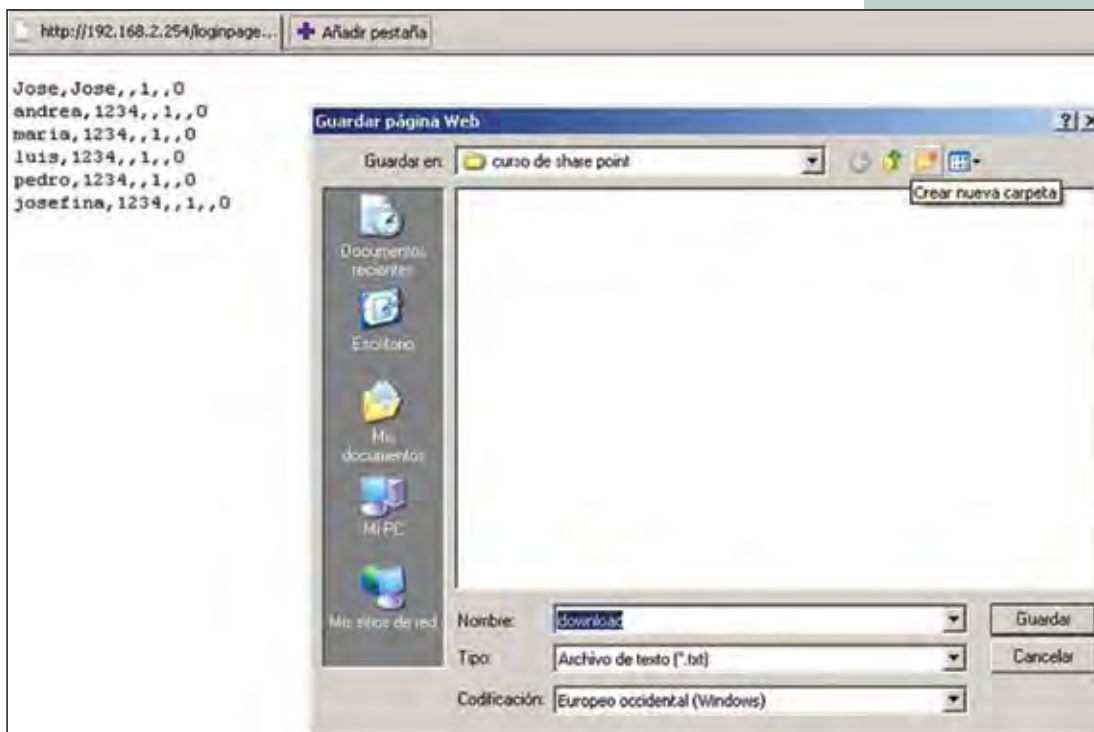


figure 23

h) In figure 24, select the "User Authentication" submenu, then select the "Policy Configuration" option. You will be able to configure the policies that apply to the user accounts in this window. Select the policy and execute the changes. In the "Firewall Profile" you will be able to configure the firewall policies, in the Route Profile you will be able to modify the routing policies. In "Schedule Profile", you will be able to establish the permitted hours of the day for that policy. In "Total Bandwidth", you will be able to establish the maximum bandwidth per user and in "Maximun Concurrent session for the User", you will be able to establish the maximum number of concurrent sessions for the users. Please review the LP-NC1 manual for mores details.



figure 24

i) With these steps, the user configuration will now conclude for the users that authenticate through controlled ports. Please remember that there are more options that can be used as per your requirements. We recommend that you read the Manual in order to be able to take advantage of these options.

B. Scenario #2. Please review figure 43. Set-up the connections as per the drawings and proceed to configure the LP-NC1 as shown in the following paragraphs:

a) Authentication Mode configuration: In figure 25, please select the "User Authentication" submenu, then select: "Authentication Configuration". Enable the server 1 as default. It is important to remark that the configuration is by default. The Server that validates the corporation will apply the validation methods (LDAP, POP3, RADIUS o NT DOMAIN). Depending on each case, select the secondary validation Server 2, in which you will use local accounts configured in the LP-NC1. In order to perform this, you must use the postfix when placing the user name. Select "Apply" to do the changes. Once done, select the Server name and a configuration window will pop-up asking for the type of validation and the Server configuration considered (Server 1)



figure 25

b) Once the Server is selected, proceed to configure the authentication and its parameters, as shown in figure 26. The post-fix for the default Server is not indispensable as the default server will validate the user data if this postfix is not added to the user name. Please select the authentication mode, the type: I.e.: Nt domain and then proceed to select the corresponding button, then fill the required data. In this example an NT Server is used. Remember to place the Server IP address. It must be located inside the same segment of the controlled ports. Each type of authentication will require different data, select the policy that applies to these user. You can configure these policies as shown in figure 24.

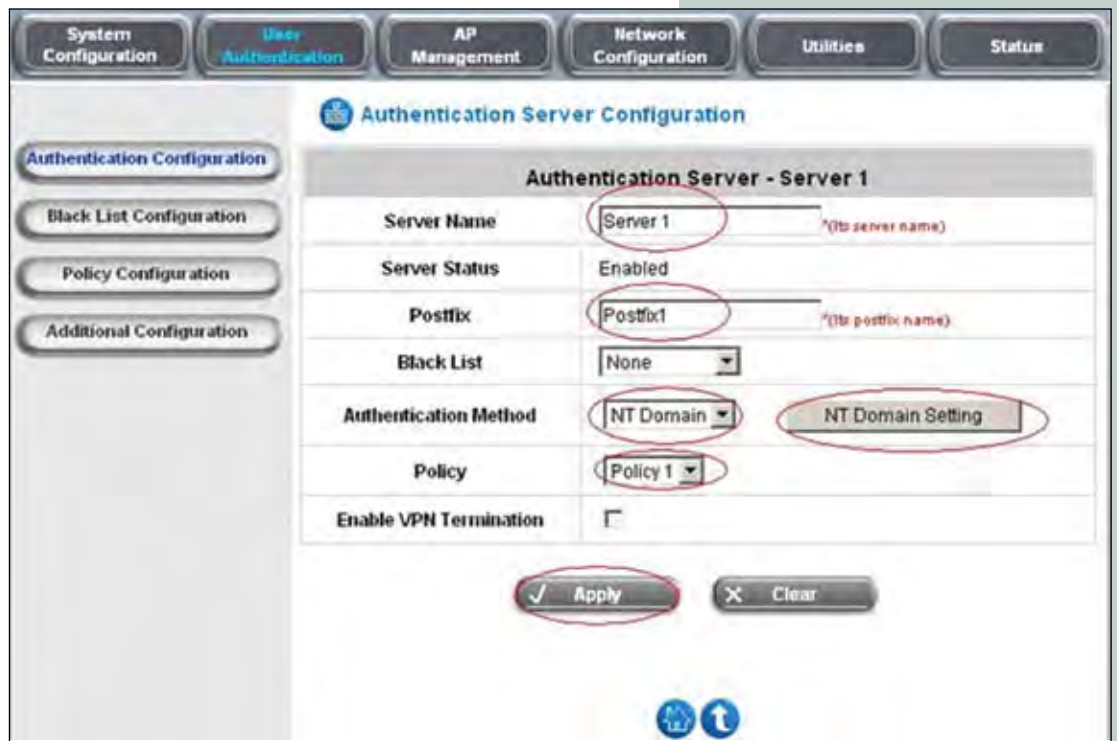


figure 26



figure 27

c) Once done, the accounts shall be added and user policies can be applied to the Server 2 group of users as shown in the following step. Remember to change the postfix and inform the users considered as visitors to write their usernames in the validation windows in the following format: "user@postfix".



figure 28

d) Proceed to select "Local User Setting" as shown in figure 28, this will drive you to the next step. You can select the policy to be applied to this user group and for this kind of application, (explained in paragraph j)

Please remember that this kind of scenario needs no change of options, unless you wish to personalize them.

e) Select : " Edit Local User List" as shown in figure 29



figure 29

f) In the window pictured in figure 30 you can add the users one by one or add them from a text file, or back-up those users in a text file. We will describe the needed steps in the following paragraphs.

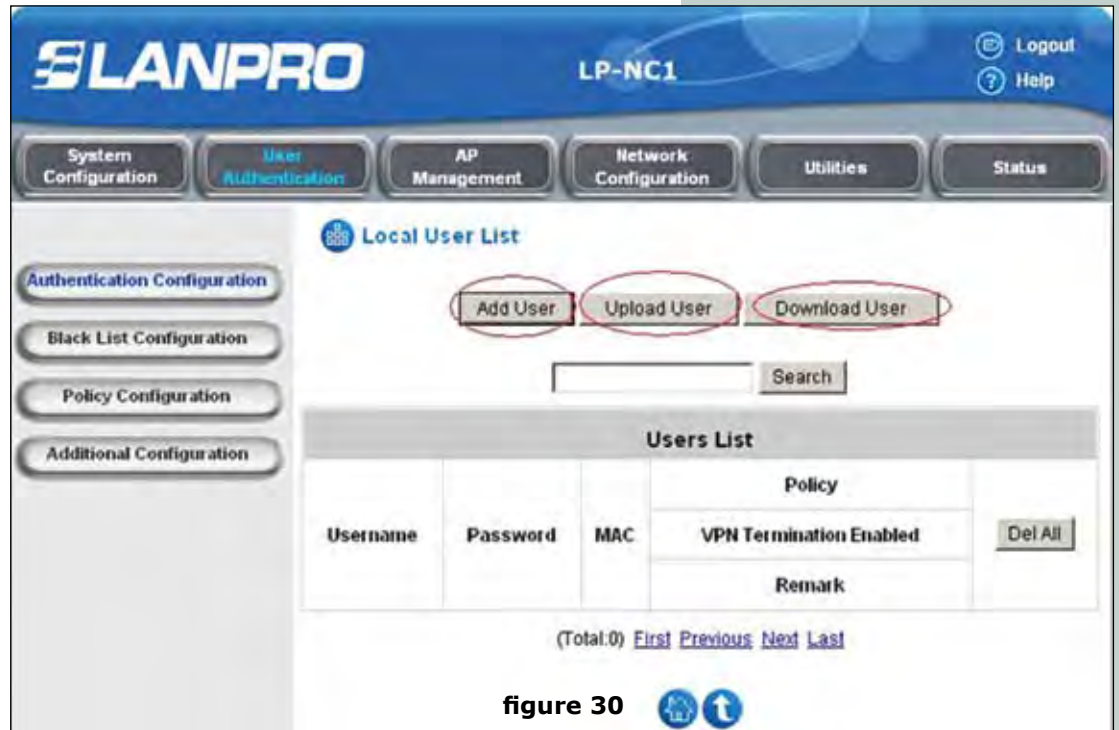


figure 30

g) In order to add a user, please select the "add user" option as shown in figure 31. Add the "Username", "Password" and the "Policy" that will be applied to him/her, please remember the restrictions on bandwidth differences that will be applied to these policies. Now is time to define the user groups and how to modify them. Once done, please select "Apply" and a message will pop-up saying that the users were added.



figure 31

h) In order to upload the User List, please select "Upload Users" as shown in the figure 32. Explore and select the file, then click on the upload button. An example file is attached as shown in figure 33. Please consult the LP-NC1 manual for details.



figure 32

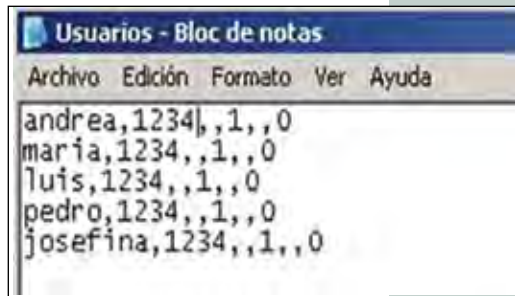


figure 33

i) Backing up of this user list can be done by selecting the "Download Users" option button as shown in figure 34. Click the "Download" button. A window in HTML will pop-up (Figure 35), select "Save": File and the location.



figure 34

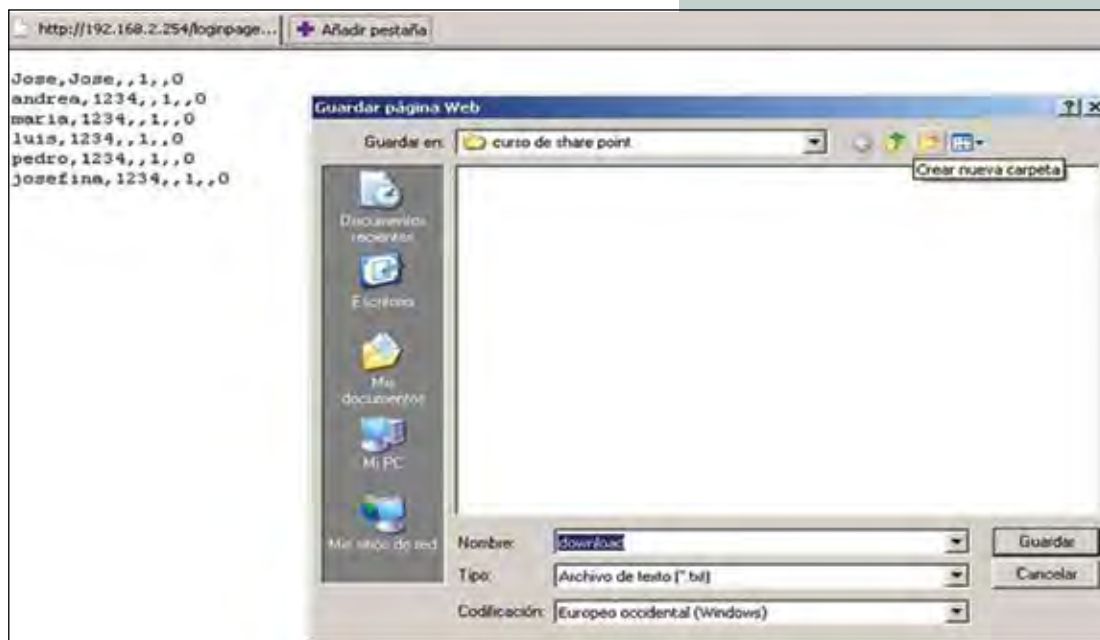


figure 35

j) In the window shown in figure 36, please select: "User Authentication" submenu, select option "Policy Configuration", in that window, you will be able to configure the policies that apply to the user accounts. Please select the policy and change them. In the "Firewall Profile" option, you will be able to establish the Firewall policies. In the "Route Profile" option, you will be able to establish Routing policies. Hourly permission policies can be established in the "Schedule profile" option. In "Total Bandwidth" you will be able to establish the total bandwidth for that user. The individual maximum bandwidth for the user can be established in "Individual Maximum Bandwidth". You can set up the maximum number of concurrent users in "Maximum Concurrent Session For Users". For more details, please refer to the LP-NC1 manual.



figure 36

k) With those steps, the user configuration concludes. User authentication should be done through the controlled ports. Many options are available that you can use as per your requirements. We recommend you to read the manual in order to fully utilize the product.

C. Scenario # 3, see figure 44. Please setup the connection as per the diagram shown and configure the LP-NC1 as follows:

a) In the window shown in figure 37, configure the Authentication Mode: Select "User Authentication" sub menu, then the "Authentication Configuration" option.

Enable Server 1 as Default. This will be the default Corporation Server. In this environment, this server will validate through any of these methods: (LDAP, POP3, RADIUS or NT DOMAIN) depending on the case. Select "Apply" to perform the changes. Now select the Server name and a configuration window will pop-up so you can change the configuration, the validation type and configuration of this server (Server 1).



figure 37

b) Once the Server is selected, proceed to configure the authentication and parameters, the postfix of the default Server is not indispensable as when you are asked for the data and only the user is given, the validation is done by the default Server. Please select the type in the authentication mode, i.e.: NT domain. In figure 38, please select the proper button and then fill the required data.

An NT server is used in this example. Please remember to give the IP address of the Server. This address must be located inside the same segment of the controlled ports. A different data requirement is needed for each type of authentication. Select the policy to be applied to these users as the same selected in the window depicted in figure 36.



figure 38



figure 39

c) In figure 40, please select the "User Authentication" submenu. Select the Policy Configuration option. In this window you can configure the user account policies, select the proper policy and perform the changes. In the "Firewall Profile" option, you can establish firewall policies. In the "Route Profile" you can configure the routing policies. In "Schedule Profile", you can establish hourly permissions for these policies. In "Total Bandwidth", you can assign the Total Bandwidth for this policy. In "Individual Maximum Bandwidth" you can set the maximum bandwidth per user. In "Individual request bandwidth" you can set the User requested maximum bandwidth. In "Maximum concurrent session for user" you can set the maximum number of concurrent sessions. For more detailed information, please consult the LP-NC1 manual.



figure 40

d) Proceed with the redirection of the monitoring files by selecting the "Status" by selecting the "Status" submenu and the "Notification Configuration" option. In this option, you have all the redirection options at your disposal. For the Log and monitoring in different formats. For more information about this, please refer to the Manual.



Nota: colocar nota de manual

figure 40

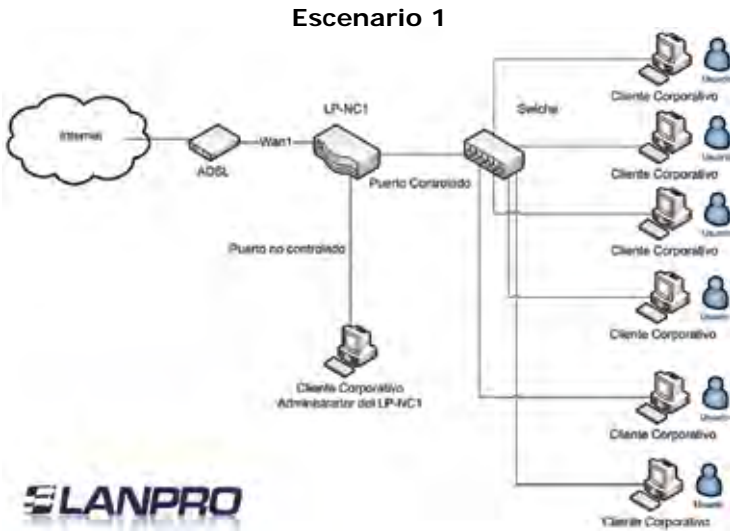


figure 41



figure 42

Escenario 3

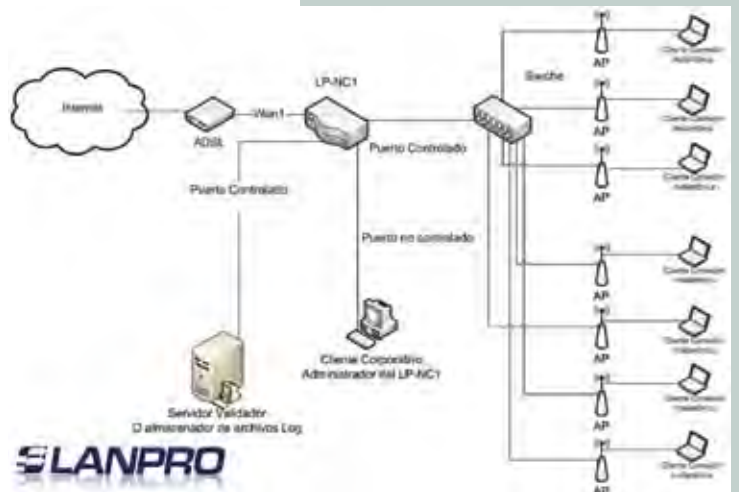


figure 43