123 Manual, LP-N24 V2.0, 2.4 GHz Wireless-N Broadband Router and/or Access Point (AP). Access Control to the WAN through MAC Address.

LPN24V2_M123_ENJ01W



123 Manual, LP-N24 V2.0, 2.4 GHz Wireless-N Broadband Router and/or Access Point (AP). Access Control to the WAN through MAC Address. SLANPRO

The following manual explains how you can configure the access control to the Internet through the LP-N24 V2.0 router.

1 Open the web browser of your preference and type the same default address, which is 192.168.0.1 as shown in Figure 1. 🖉 LanPro LPN24V2 150 N Wireless Router - Windows Internet Explorer http://192.168.0.1 --> × File Edit View Favorites Tools Help Figure 1 2 In case your router has a password, it will be requested in Login a window. Select Ok as shown in Figure 2. ***** Password: (Initial password: NULL) Ok Cancel Figure 2 3 Select the option Advance settings as shown in Figure 3. LanPro LPN24V2 150 N W - 4 × 🗷 Der p. G - + ktp://192.168.0.1/ File Edit View Favorites Tools Help Favorites 🛛 😹 LarPro LPN24V2 150 N Wreless Router Advanced Settings Δ Internet Connection Settings Connection Type: C PPPoE @ DHCP For other connection types .go to 'Advanced Settings' Wireless Security Settings Figure 3 Security Key: 12345578 (Default Security Key 12345678) Ok Cancel

4

Select the options **Security settings** and **MAC Address Filter Settings.** In **Filter Mode** select the type of filtering you want to establish. If your goal is to allow only the MAC addresses from the list to navigate, then you must select **Permit only.** On the contrary, if you want that only the MAC addresses from the list cannot navigate, select **Forbid only**, as shown in **Figure 4**.

Figure 4

NOTE: If access to certain MAC addresses in the list is allowed, the remaining MAC addresses will be denied. If certain MAC addresses in the list are denied, the others will be allowed.



5

Once you have selected one of the filtering options mentioned above, the options for the access policy configuration will be displayed. It is important to mention that you can add up to 10 MAC addresses and you can also set **Time** and **Date** range to each of them in which the policy is applied, as shown in **Figure 5**).

SLANPRO

Client Filter Settings MAC Address Filter Settings URL Filter Settings Remote Web Management

Virtual

Ac	cess Policy:	(1) 💌	
	Remark:		
M	AC address:		
	Time:		
	Date:	Sunday 💽 ~ Saturday 💌	
	Enable:	Clear this item: Clear	

6

Look at the following example: If we want that solely the MAC Address 00:27:11:00:00:0 (Client 1) be allowed to navigate only from Monday to Friday, from 6 AM to 6 PM, then the access policy must be configured as shown in **Figure 6.**

Advanced Wireless DHCP settings settings Server

Client Filter Settings MAC Address Filter Settings URL Filter Settings Remote Web Management
Filter Mode : Permit only
Access Policy: (1)
Remark: Rule1
MAC address: 00 27 11 00 00 01
MAC address: 00 27 11 00 00 01
Time: 6 0 0 - 18 0 0
Date: Monday - Friday
Enable:
Clear this item Clear

Ok Cancel

setting

Figure 6

Figure 5



8

If you want to edit or add a new access policy, select its number in **Access Policy**, as shown in **Figure 8**. Then, fill the other fields as explained in number 5. Save changes by selecting **Ok**.

Advanced \ settings	Wireless settings	DHCP Server	Virtual server	Security settings	Routing settings	Systen tools
Client Filter Sett	tings MAC A	Address Filte	r Settings U	RL Filter Settin	ngs Remote	Neb
Management						
Filter Mo	ode : Permit on	nly 💌				
Filter Mc	ode : Permit or Access Poli	nly 💌 icy: (1) 💌				
Filter Mc	ode : Permit on Access Poli Rema	nly 💌 icy: (1) 💌 ark: (2)				
Filter Mo	ode : Permit or Access Poli Rema MAC addres	nly 💌 icy: (1) 💌 ark: (2) ss: (3)	·	00 : 01		
Filter Mo	ode : Permit or Access Poli Rema MAC addre: Tin	nly v icy: (1) v ark: (2) ss: (3) (4) ne: (5)	7]; [1]]; [00] 0] ▼ ~[18 ▼;	00 : 01		
Filter Mc	ode : Permit or Access Poli Rema MAC addres Tin Da	nly (1) (1) (2) (3) (4) (5) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	2) [11] [00] 2) ▼ ~ [18 ▼ :[2) ▼ ~ [18 ▼ :[1

Figure 8