LanPro LP-1520ai WLAN AP

LP1520ai_UG_ENB01W

Features

- High Power: 0.8W output power for longer range.
- Environment: Outdoor Capable, weatherproof Enclosure.
- Antenna: Integrated.
- No need for a local power supply. Powered through the Ethernet Data cable. Complies the IEEE 802.3af PoE Standard
- Self Healing: Watch Dog Timer prevents soft resets.
- Security WEP/WPA/WPA2 encryption.
- Capable of serving as an AP, Bridge, Hot-Spot and Repeater.

LanPro LP-1520ai WLAN AP with IEEE 802.3af Compatible PoE Input User Manual V1.0

The LanPro's LP1520ai Wireless AP's most remarkable characteristics are it's ***full Weatherproof*** features which enable this equipment to operate in very harsh environmental conditions (Salty, Sun, Humidity, etc). Besides this, the LP-1520ai has ***800 mW*** of RF Power into the Antenna, enough to warrant reliable communications over 2 Km links of point to point to multi-point networks or 3.5Km on ISP WIFI cell client applications.

The Integrated antenna of the LP-1520ai minimizes cable losses and facilitates its mounting on walls or poles by combining the AP and it's Antenna.

PoE IEEE 802.3af standard support facilitates powering of the device and simplifies installation. Distance supported: 100 m.

The LP-1520ai's ***Watch Dog Timer*** function, named by ISP's as *"The Magical Electronics"*, delivers a *"Self Reset"* to the hardware in the event that the device *"Hangs-up"*, inhibiting proper operation of the device. All of these features make the LP-1520ai a reliable, robust and integrated solution for WIFI based projects.

Table of Contents

A LP-1520ai Physical Description.

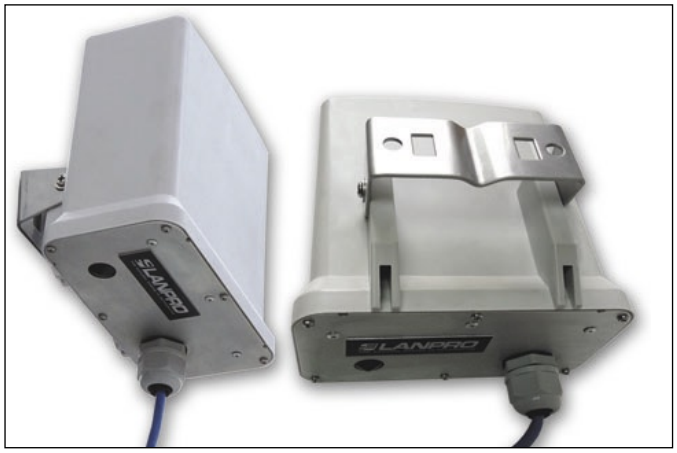


Figure 1

The LanPro LP-1520ai WLAN Access Point is a 802.11 b/g Compliant device

Designed for pole or wall mounting, it has the necesary hardware for installing and pointing it's built in panel antenna. (Please see figure 1)

The LP-1520ai is a Power Over Ethernet (PoE) compliant device as per the IEEE-802.3af standard.

The WAN options are not enabled in this model number please disregard any WAN function mentioned in the text.

Bottom Panel Connectors

- **1.** The LP-1520ai bottom panel includes a water tight RJ-45 connector for outdoor use. This port is IEEE/802.3 af standard for PoE compliant (Power Over Ethernet), (Please see figure 2).

- **2.** This port is also IEEE 802.3/802.3u compliant, suporting LAN autosensing on 10/100 Mbps and half/ full duplex.

Figure 2

B Installation of the LanPro LP-1520ai WLAN AP

Figure 3

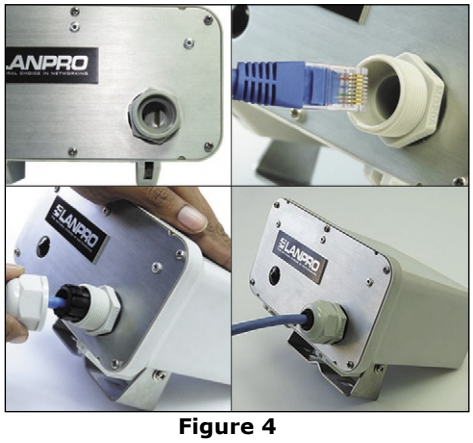


Figure 4

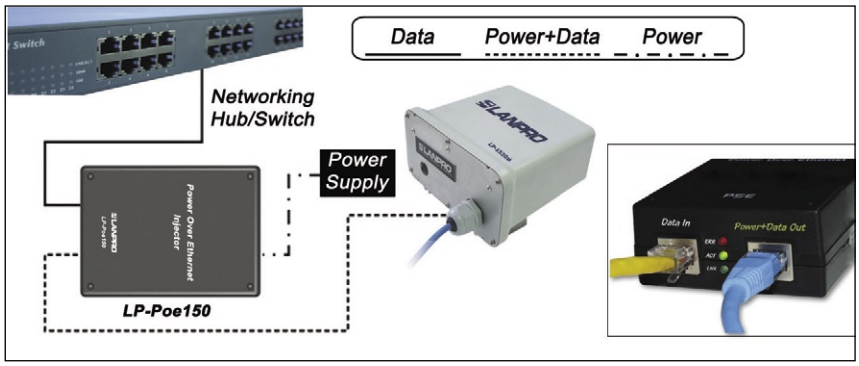


Figure 5

Hardware Installation

- **Step 1:** Fix the LP-1520ai to the mounting pole or wall with the mounting bracket as shown in figure 3. A clamp is included.

- **Step 2:** Connect the LP-1520ai to the local network cable through the water tight ethernet connector, as show in figure 4.

- **Step 3:** The LP-1520ai is IEEE-802.3af compatible, obtaining power fron the ethernet cable (PoE).

- **Step 4:** Please connect the other end of the patchcord to the LP-PoE150 port labeled Power+Data Out. Also connect your network to the Data In port by using another patchcord. Finally connect the mains cable to the Power Input connector of the LP-PoE150. Figure 5

Software Installation

There are no software drivers, patches or utilities installation needed, only the configuration settings. Please refer to the software configuration.

The web based management and configuration functions allow you to do the step-by-step procedure very easily. The LP-1520ai is delivered with the following factory default parameters on the Ethernet LAN interfaces. Default IP Address: 192.168.1.254 Default IP subnet mask: 255.255.255.0 WEB login User Name: <empty> WEB login Password: <empty>.

For Microsoft Windows 2000/XP/Vista

- **1.** Click the Start button and select Settings, then click Control Panel. The Control Panel window will appear.
- **2.** Move mouse and double-click the right button on Network and Dial-up Connections icon. Move mouse and double-click the Local Area Connection icon. The Local Area Connection window will appear. Click Properties button in the Local Area Connection window.
- **3.** Check the installed list of Network Components. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.
- **4.** Select Protocol in the Network Component Type dialog box and click Add button.
- **5.** Select TCP/IP in Microsoft of Select Network Protocol dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
- **6.** Select TCP/IP and click the properties button on the Network dialog box.
- **7.** Select Specify an IP address and type in values as following example. IP Address: 192.168.1.1, IP address within the range of 192.168.1.1 to 192.168.1.253 is used to connect the AP IP Subnet Mask: 255.255.255.0
- **8.** Click OK to complete the IP parameters setting.
- **9.** Open your preferred web browser and use the following address:

Figure 6

C Configuration of the LP-1520ai WLAN AP

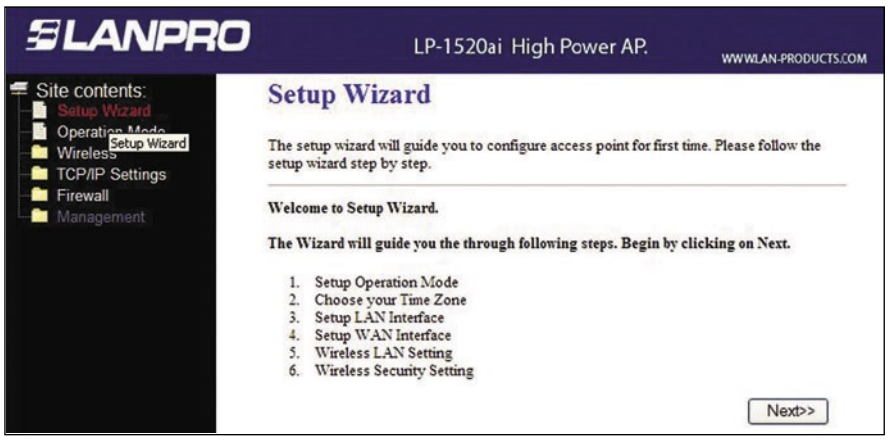


Figure 7. Screen snapshot - Setup Wizard

Setup Wizard

This page guides you to configure The LP-1520ai WLAN AP for the first time.

1.- Setup LAN Interface. This page is used to configure local area network IP address.

2.- Wireless LAN Setting. This page is used to configure wireless LAN Setting.

3.- Wireless Security Setup. This page is used to configure wireless security Screen.

Status

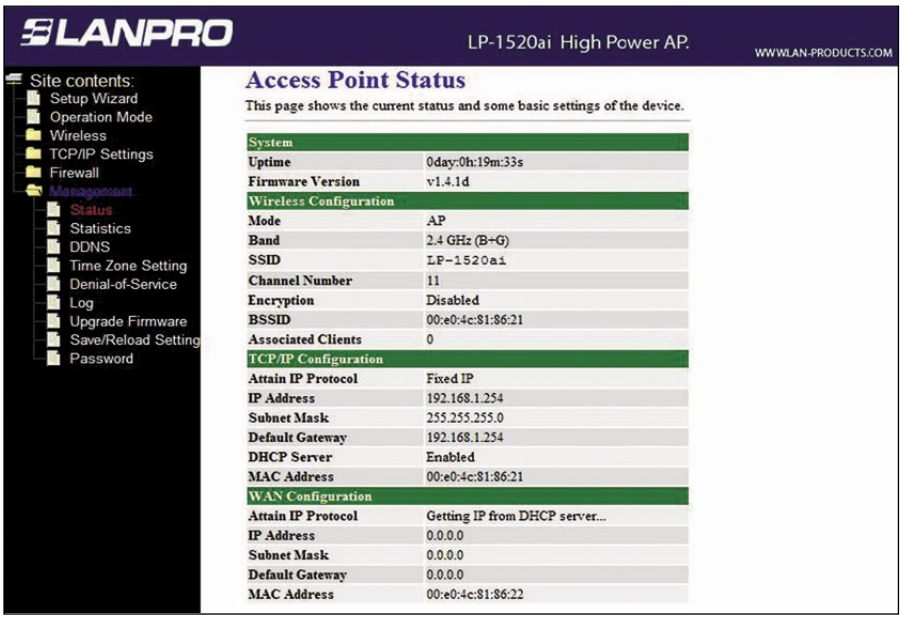


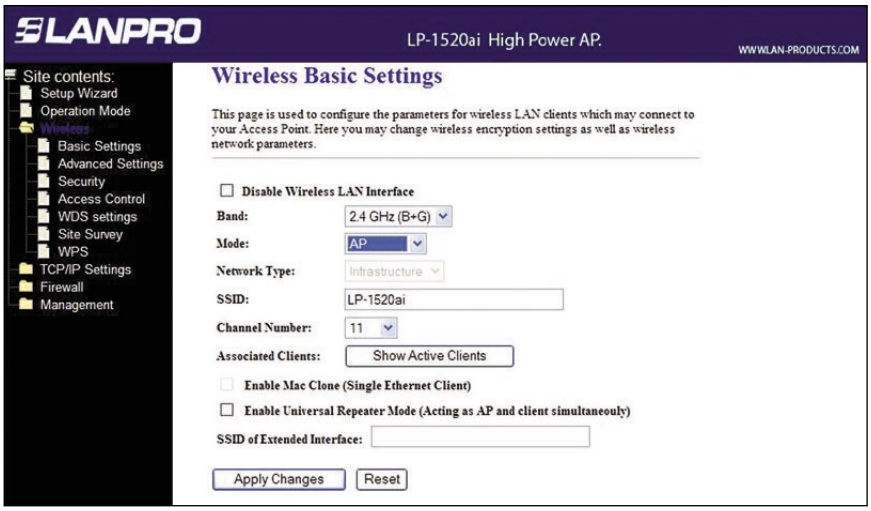
Figure 8. Screen snapshot - Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and (WAN)* configuration information.

(*)Note: WAN option doesn't apply to this model number.

Item	Description
System	
Uptime	It shows the duration since WLAN AP is powered on.
Firmware version	It shows the firmware version of The LP-1520ai.
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of the LP-1520ai. The SSID is the unique name of WLAN AP and shared among its service area, so all devices attempts to join the same wireless network can identify it. Channel Number It shows the wireless channel connected currently. Encryption It shows the status of encryption function. Associated Clients It shows the number of connected clients (or stations, PCs).
BSSID	It shows the BSSID address of the AP. BSSID is a six-byte.
TCP/IP configuration	
Attain IP Protocol	It shows how the AP gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by the DHCP Client
IP Address	It shows the IP address of LAN interfaces of the AP.
Subnet Mask	It shows the IP subnet mask.
Default Gateway	It shows the default gateway.

Wireless - Basic Settings

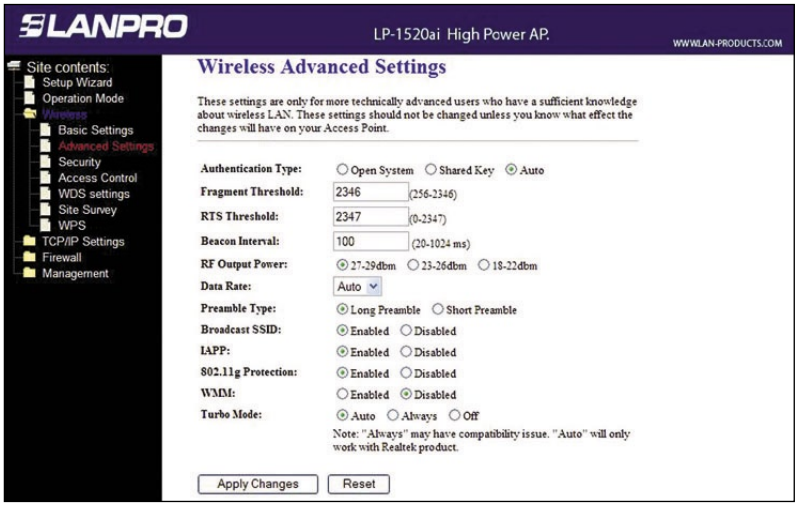


This page is used to configure the parameters for wireless LAN clients that may connect to your AP.

Figure 9.
Screen snapshot
Wireless Basic Settings

Item	Description
Band	It shows the current wireless operating frequency.
Mode	Operation mode WDS, WDS + AP, AP, AP Client.
SSID	It shows the SSID of this AP. The SSID is the unique name of WLAN AP and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows how to Select the wireless communication channel from pull-down menu. The firmware version of AP.
Associated Clients	Click the **Show Active Clients** button to open Active Wireless Client.Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client. Enable Mac Clone (Single Ethernet Client).
Apply Changes	Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

Wireless - Advanced Settings



These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your LP-1520ai WLAN AP.

Figure 10.
Screen snapshot
Wireless Advanced Settings

Item	Description
Authentication Type	Click to select the authentication type in **Open System**, **Shared Key** or **Auto selection**.
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to D.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to D.11 What is RTS(Request To Send) Threshold? Beacon Interval Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to D.12 What is Beacon Interval?
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1.1M, 5.5M, 2M or 1Mbps. Preamble Type Click to select the **Long Preamble** or **Short Preamble** support on the wireless data packet transmission. Refer to D.13 What is Preamble Type? Broadcast SSID Click to enable or disable the SSID broadcast function. Refer to D.14 What is SSID Broadcast? IAPP Click to enable or disable the IAPP function. Refer to D.20 What is Inter-Access Point Protocol(IAPP)
802.11g Protection	Protect 802.11b user.
Apply Changes	Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

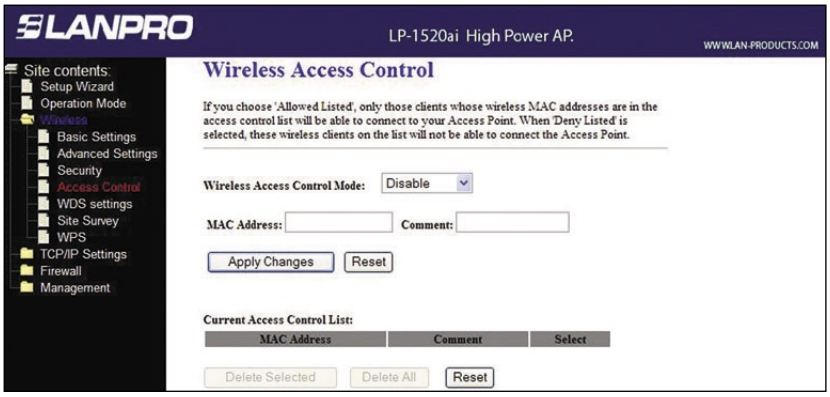
Wireless - Security Setup

This page allows you to setup the wireless security. Turning on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

Figure 11.
Screen snapshot
Wireless Security Setup

Item	Description
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed Refer to D.9 What is WEP? D.15 What is Wi-Fi Protected Access (WPA)? D.16 What is WPA2(AES)? D.17 What is 802. 1X Authentication? D.18 What is Temporal Key Integrity Protocol (TKIP)? D.19 What is Advanced Encryption Standard (AES)? Use 802.1x Authentication While Encryption is selected to be WEP. Click the check box to enable IEEE 802. 1x authentication function. Refer to D.16 What is 802. 1x Authentication?.
WPA Authentication Mode	While Encryption is selected to be WPA . Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to D.15 What is Wi-Fi Protected Access (WPA)? Pre- Shared Key FormatWhile Encryption is selectedto be WPA.
Pre-share key	Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). **[WPA, Personal(Pre-Shared Key) only]** Pre-Shared Key Fill in the key value. [WPA, Personal(Pre- Shared Key) only] Enable Pre-Authentication Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only] Authentication RADIUS Server Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the **Reset** button to abort change and recoverthe previous configuration setting.

Wireless - Access Control

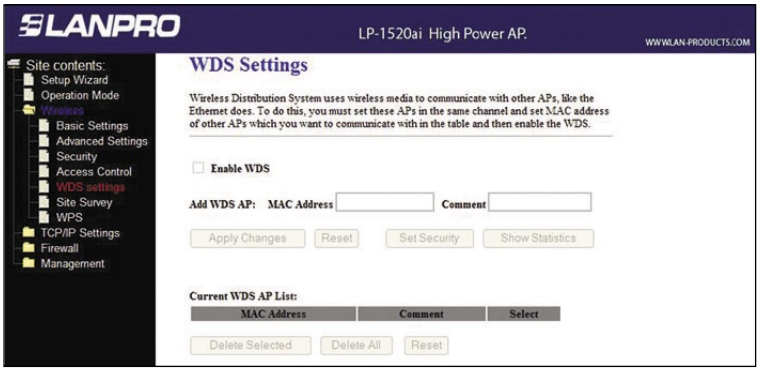


If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

Figure 12.
Screen snapshot
Wireless Access Control

Item	Description
Wireless Access Control Mode	Click the Disabled, Allow Listed or Deny Listed of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this AP.
MAC Address	Fill in the MAC address of client to register this WLAN AP access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the **Apply Changes** button to register the client to new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this AP.
Delete Selected	Click to delete the selected clients that will be access right removed from this AP.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

WDS Settings

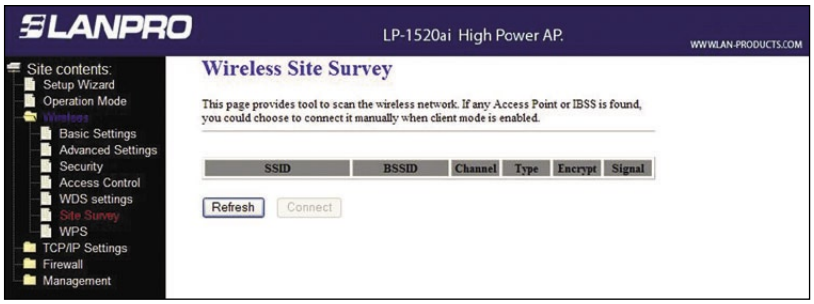


Wireless Distribution System uses wireless media to communicate with other AP's, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

Figure 13.
Screen snapshot - WDS

Item	Description
MAC Address	Fill in the MAC address of client to register this WLAN Broadband AP access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the **Apply Changes** button to register the client to new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.
Current WDS AP List	It shows the registered clients that are allowed to link to this AP
Delete Selected	Click to delete the selected clients that will be access right removed from this AP.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

Site Survey

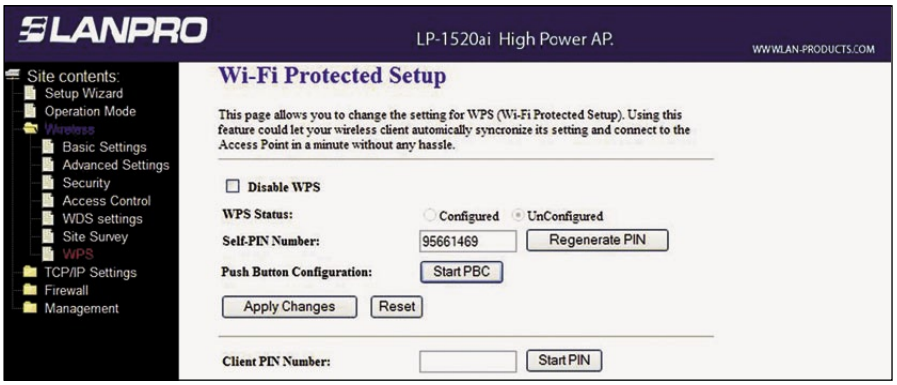


This page is used to view or configure other APs near yours.

Figure 14.
Screen snapshot
Wireless Site Survey

Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP. Select Click to select AP or client you'd like to connect.
Refresh	Click the Refresh button to re-scan site survey on the screen.
Connect	Click the Connect button to establish connection

WPS



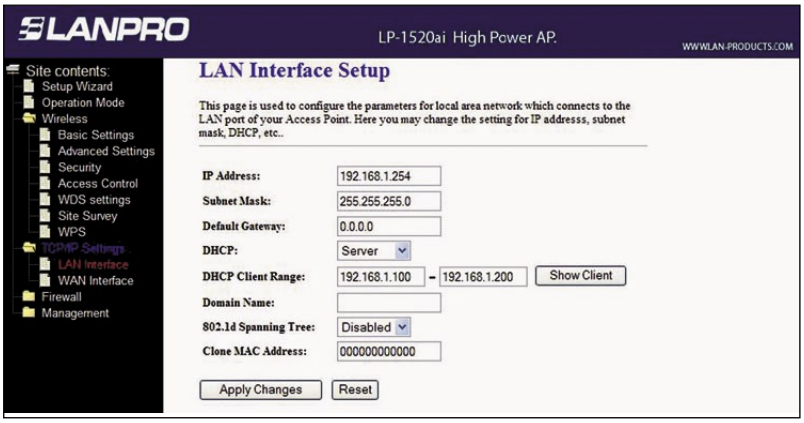
This page allows you to change the setting WPS.

Figure 15.
Screen snapshot - WPS

Item	Description
Self-PIN Number	Fill Self-PIN Number in the tag
Apply Changes	Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

Press WPS button and set as the GUI.

TCP/IP - LAN Interface Setup

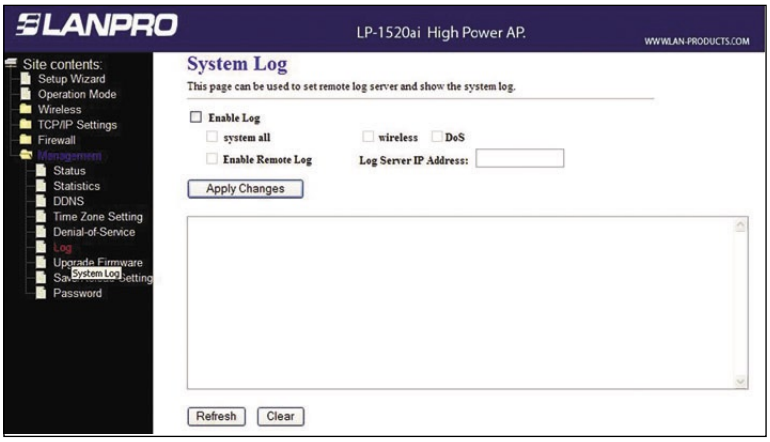


This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN AP. Here you may change the setting for IP address, subnet mask, DHCP, etc.

Figure 16.
Screen snapshot
LAN Interface Setup

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this AP.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this AP.
Default Gateway	Fill in the default gateway for LAN interfaces out going data packets.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range. Show Client Click to open the **Active DHCP Client Table** window that shows the active clients with their assigned IP address, MAC address and time expired information. **[Server mode only]**.
DHCP Server	Click to select **Disabled**, **Client** or **Server** in different operation mode of AP.
802.1d Spanning Tree	Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Clone MAC Address Fill in the MAC address that is the MAC address to be cloned. Refer to D.24 What is Clone MAC Address?
Apply Changes	Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

Log

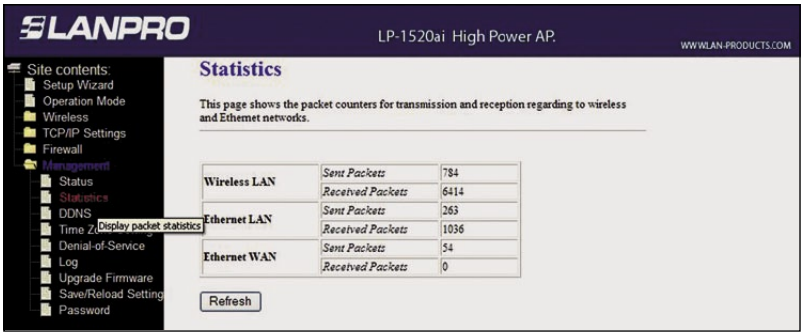


This page is used to configure the remote log server and shown the current log.

Figure 17.
Screen snapshot
Management – Log

Item	Description
Enable Log	Click the checkbox to enable log.
System all	Show all log of wireless WLAN AP
Wireless	Show wireless log
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP Address	Log Server IP Address Input the remote log IP address.
Apply Changes	Click the **Apply Changes** button to save above settings.
Refresh	Click the refresh the log shown on the screen. Clear log display screen.

Statistics



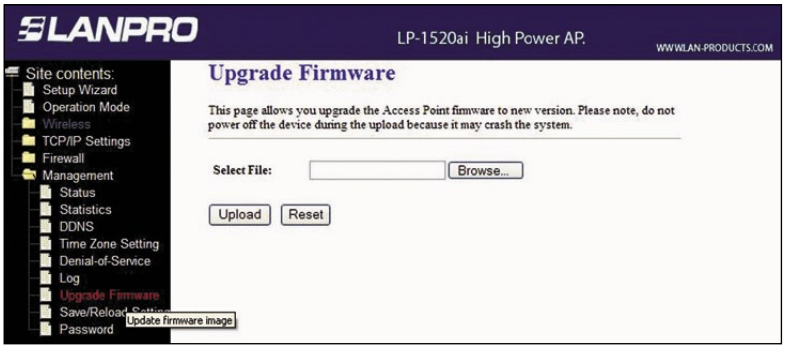
This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.*

(*)Note: WAN option doesn't apply to this model number.

Figure 18.
Screen snapshot - Statistics

Item	Description
Wireless LAN	
Sent Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Received Packets	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN	
Sent Packets	It shows the statistic count of sent packets on the Ethernet LAN interface.
Received Packets	It shows the statistic count of received packets on Ethernet LAN interface.
Refresh	Click the refresh the statistic counters on the screen.

Upgrade Firmware

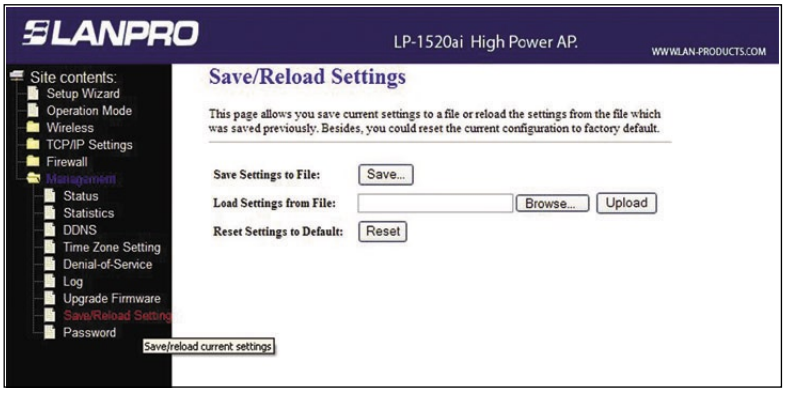


This page allows you to upgrade the Access Point firmware to a new version. Please note: do not power off the device during the upload because it may **damage** the system.

Figure 19.
Screen snapshot
Management - Upgrade Firmware

Item	Description
Select File	Click the **Browse** button to select the new version of web firmware image file.
Upload	Click the **Upload** button to update the selected webfirmware image to the AP.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

Save/Reload Settings

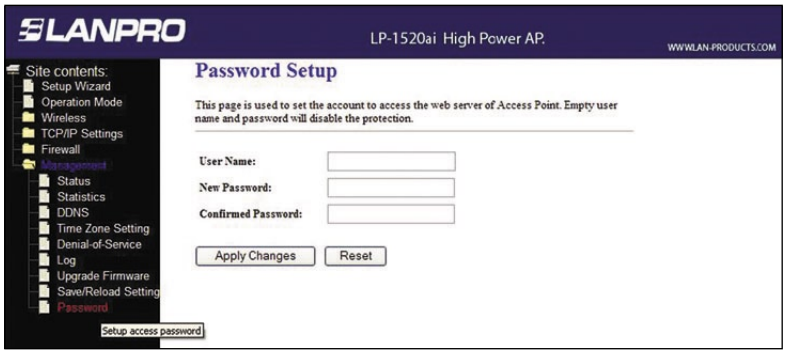


This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

Figure 20.
Screen snapshot
Management - Save/Reload Settings

Item	Description
Save Settings to File	Click the **Save** button to download the configuration parameters to your personal computer.
Up Load Settings from File	Click the **Browse** button to select the configuration files, then click the Upload button to update the selected one.
Reset Settings to Default	Click the **Reset** button to reset the configuration parameter to factory defaults.

Password Setup



This page is used to set the account to access the web server of the Access Point. Empty user name and password will disable the protection.

Figure 21.
Screen snapshot
Management - Password Setup

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clearing the **User Name** and **Password**, means to apply no web management login control. Click the **Apply Changes** button to complete the new configuration setting.
Reset	Click the **Reset** button to abort change and recover the previous configuration setting.

D Frequently Asked Questions (FAQ)

1 What is and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address. The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. To find your PC's IP and MAC address, Open the Command program in the Microsoft Windows. Type in ipconfig /all then press the Enter button. Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

2 What is a Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4 How does wireless networking work?

The 802.11 standard defines two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred.

5 What is BSSID?

A six-byte address that distinguishes a particular access point from others. Also known as just SSID. Serves as a network ID or name.

6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

7 What are potential factors that may causes interference?

Factors of interference: Obstacles: walls, ceilings, furniture… etc. Building Materials: metal door, aluminum studs. Electrical devices: microwaves, monitors and electrical motors. Solutions to overcome the interferences: Minimizing the number of walls and ceilings. Position the WLAN antenna for best reception.
Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, … etc. Add additional WLAN Access Points if necessary.

8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers. WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several values, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead. Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. If you find that your corrupted packets or asymmetric packet reception (all sent packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be ransmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion. Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point. Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11 i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.1 1i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access. To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

17 What is 802.1 x Authentication?

802. 1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284. Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.1 1i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet. IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

22 What is Universal Plug and Play (uPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

25 Wi-Fi Protected Setup™ (WPS)

WPS is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on wireless local area networks.