

Advanced Wireless Settings

RTS/CTS Threshold: bytes (range: 0 ~ 2347, default 2347)

Beacon Interval: milliseconds (range 20 ~ 999, default 100)

DTIM: (range 1 ~ 255, default 1)

Fragment Size: bytes (range 256 ~ 2346, default 2346)

Short GI: 400ns 800ns

Aggregation: Enable Disable

Aggregated Frames Number: (range 1 ~ 32, default 32)

Maximum Aggregated Size: (range 2346 ~ 65536, default 50000)

Tx ChainMask: ▼

Rx ChainMask: ▼

WiFi Multimedia

WMM Capable Enable Disable

Figure 5-17 Advanced Settings

Object	Description
• RTS/CTS Threshold	When the length of a data packet exceeds this value, the router will send an RTS frame to the destination wireless node, and the latter will reply with a CTS frame, and thus they are ready to communicate. The default value is 2347.
• Beacon Interval	Set beacon interval, the value range is from 20 to 999. The default value is 100.
• DTIM	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
• Fragment Size	A data packet that exceeds this value in length will be divided into multiple packets. The number of packets influences wireless network performance. Avoid setting this value low. Default at 2346.
• Short GI	Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Only effect under Mixed Mode.
• Aggregation	A part of the 802.11n standard that allows sending multiple frames per

	single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source, destination end points, and traffic class (QoS) into one large frame with a common MAC header
• Aggregated Frames Number	Determines the number of frames combined in the new larger frame.
• Maximum Aggregated Size	Determines the size (in bytes) of the larger frame.
• Tx ChainMask	Displays the number of independent spatial data streams the device is transmitting (TX) and receiving (RX) simultaneously within one spectral channel of bandwidth. Multiple chains increase data transfer performance significantly.
• Rx ChainMask	Displays the number of independent spatial data streams the device is transmitting (TX) and receiving (RX) simultaneously within one spectral channel of bandwidth. Multiple chains increase data transfer performance significantly.
• WMM Capable	Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

WMM Parameters of Station				
	Aifsn	CWMin	CWMax	Txop
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1504"/>
WMM Parameters of Access Point				
	Aifsn	CWMin	CWMax	Txop
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1504"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Close"/>				

Figure 5-18 WMM Configuration

WMM Capable	
BE	Traditional IP data, medium throughput and delay.
BK	High throughput, non time sensitive bulk data e.g. FTP
VI	Time sensitive video data with minimum time delay.
VO	Time sensitive data such as VoIP and streaming media with minimum time delay.
Aifsn	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
CWMin	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).
CWMax	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
Txop	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value effects higher priority.

5.1.9 Access Control

Choose the operation mode you require, and then enter “**Access Control**” by clicking the **Setup** button next to it and the following page will be displayed. This section allows you to configure the wireless access control settings.

Access Control Settings

This feature allows you to define a list of MAC addresses that are authorized to access or denied from accessing the wireless network.

Wireless Access Control Mode:

Mac Address: (xx:xx:xx:xx:xx:xx)

Comment :

Figure 5-19 Access Control

Object	Description
Wireless Access Control Mode	You can choose “Disable”, “Allow Listed” or “Deny Listed”.
Mac Address	The MAC address to be filtered.
Comment	Enter a comment of this setting.

5.1.10 WAN Port Settings

Click “Operation Mode” → “AP Router” or “Wireless ISP” and then enter the “WAN Port Settings” by clicking the **Setup** button next to it. This section allows you to configure the internet connection settings.

■ DHCP (Auto Config)

Choose “DHCP” and the router will automatically obtain IP addresses, subnet masks and gateway addresses from your ISP.

WAN Port Settings

WAN Connection Type:

Host Name(optional) :

Figure 5-20 WAN Port Settings – DHCP

■ Static Mode (Fixed IP)

If your ISP offers you static IP Internet connection type, select “**Static Mode**” and then enter IP address, subnet mask, primary DNS and secondary DNS information provided by your ISP in the corresponding fields.

WAN Port Settings

WAN Connection Type:

IP Address Assigned by Your ISP:

IP Subnet Mask:

ISP Gateway IP Address:

Primary DNS Server:

Secondary DNS Server:

Figure 5-21 WAN Port Settings – Static IP

Object	Description
• IP Address Assigned by Your ISP	Enter the WAN IP address provided by your ISP. Enquire your ISP if you are not clear.
• IP Subnet Mask	Enter WAN Subnet Mask provided by your ISP.
• ISP Gateway IP Address	Enter the WAN Gateway address provided by your ISP.
• Primary DNS Server	Enter the necessary DNS address provided by your ISP. Default is 8.8.4.4.
• Secondary DNS Server	Enter the other DNS address if your ISP provides you with 2 such addresses. Default is 8.8.8.8.

■ PPPOE (ADSL)

Select **PPPOE** if your ISP is using a PPPoE connection and provide you with PPPoE user name and password info.

The screenshot shows a dialog box titled "WAN Port Settings". Inside, there is a dropdown menu for "WAN Connection Type" set to "PPPOE (ADSL)". Below it are three text input fields: "User Name:", "Password:", and "Verify Password:". At the bottom, there are two buttons: "Save" and "Cancel".

Figure 5-22 WAN Port Settings – PPPOE

Object	Description
• User Name	Enter the User Name provided by your ISP.
• Password	Enter the password provided by your ISP.
• Verify Password	Enter the password again to verify if it is correct.

5.1.11 Dynamic DNS Settings

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**Dynamic DNS Settings**” by clicking the **Setup** button next to it. This section allows you to configure the DDNS settings.

The screenshot shows a dialog box titled "Dynamic DNS Settings". It contains a paragraph: "You may configure DDNS Settings here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services." Below this are several fields: "DDNS option:" with a dropdown menu showing "Disable" selected; "Easy Domain Name" and "DDNS Settings" with a dropdown menu showing "Enable Easy DDNS" selected; "Dynamic DNS Provider:" with a dropdown menu showing "None" selected; "Account:", "Password:", and "DDNS:" with text input fields. At the bottom, there are two buttons: "Apply" and "Cancel".

Figure 5-23 Dynamic DNS Settings

Object	Description
• DDNS option	Disable: Disable DDNS function Enable Easy DDNS: Enable PLANET Easy DDNS Enable Dynamic DDNS: You are allowed to modify the DDNS settings.
• Dynamic DNS Provider	Select a server provider or disable the existing server.
• Account	Enter the DDNS user name of the DDNS account.
• Password	Enter the DDNS password of the DDNS account.
• DDNS	Enter the host name or domain name provided by DDNS provider.

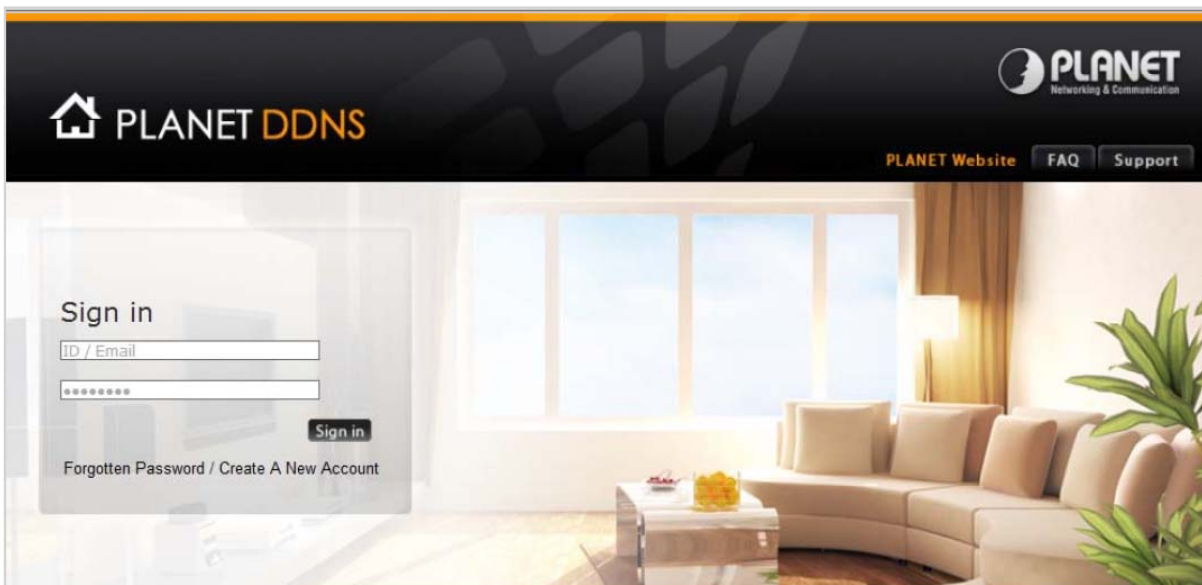
Example of Planet DDNS Settings:



Note

Please go to <http://www.planetddns.com/> to register a Planet DDNS account.

Please refer to the FAQ (<http://www.planetddns.com/index.php/faq>) for how to register a free account.



Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**”, select **Dynamic DNS Settings** and press “**Setup**”.

Dynamic DNS Settings:

Setup

Step 1. Select “**Enable Dynamic DDNS**” and “**PlanetDDNS.com**” from the list of Dynamic DNS Provider to use the Planet DDNS service.

Dynamic DNS Settings

You may configure DDNS Settings here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services.

DDNS option:	Enable Dynamic DDNS ▼
Easy Domain Name	Disable
DDNS Settings	Enable Easy DDNS
Dynamic DNS Provider:	PlanetDDNS.com ▼
Account:	username
Password:	*****
DDNS:	username

Apply Cancel

Step 2. Configure the DDNS account that has been registered in Planet DDNS website.

Account: Enter your DDNS host (format: xxx.planetddns.com, xxx is the registered domain name)

Password: Enter the password of your account.

DDNS: Enter your DDNS host again.

Step 3. Go to “Remote Management” to enable remote access from WAN port.

Remote Management Settings

Remote management (via WAN):	Enable ▼
Ping from WAN:	Enable ▼

Save Cancel

Step 4. Go to “WAN Port Settings” to configure WAN connection to Static Mode (fixed IP).

WAN Port Settings

WAN Connection Type: Static Mode (fixed IP) ▾

IP Address Assigned by Your ISP: 210.66.155.70

IP Subnet Mask: 255.255.255.224

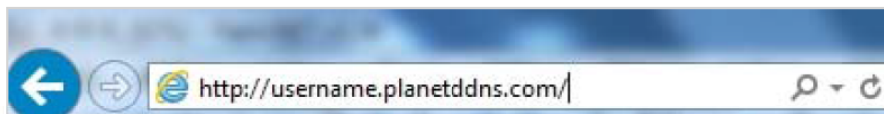
ISP Gateway IP Address: 210.66.155.94

Primary DNS Server: 8.8.4.4

Secondary DNS Server: 8.8.8.8

Save
Cancel

Step 5. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable. In a remote computer, enter the DDNS host name as the figure shown below. Then, you should be able to login the WNAP-6325 remotely.



Example of Easy DDNS Settings:



This service is not required to register any DDNS account.

Please refer to the procedure listed as follows to configure using Planet Easy DDNS service.

Step 1. Select "**Enable Easy DDNS**" to use the Planet Easy DDNS service.

Easy Domain Name: Display the specified domain name for this device. (Format: ptxxxxx.planetddns.com, [xxxxxx](#) is the last six-digit of the WAN Port MAC address)

Dynamic DNS Settings

You may configure DDNS Settings here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services.

DDNS option:

Easy Domain Name: WNAP-6325

DDNS Settings

Dynamic DNS Provider:

Account:

Password:

DDNS:

Step 2. Go to “Remote Management” to enable remote access from WAN port.

Remote Management Settings

Remote management (via WAN):

Ping from WAN:

Step 3. Go to “WAN Port Settings” to configure WAN connection to Static Mode (fixed IP).

WAN Port Settings

WAN Connection Type:

IP Address Assigned by Your ISP:

IP Subnet Mask:

ISP Gateway IP Address:

Primary DNS Server:

Secondary DNS Server:

Step 6. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable. In a remote computer, enter the Easy Domain Name displayed in **Step 1**. Then, you should be able to login the WNAP-6325 remotely.



5.1.12 Remote Management

Click "**Operation Mode**" → "**AP Router**" or "**Wireless ISP**" and then enter the "**Remote Management**" by clicking the **Setup** button next to it. This section allows you to enable or disable the remote management through the WAN port.

 A screenshot of a dialog box titled "Remote Management Settings". Inside the dialog, there are two settings: "Remote management (via WAN):" with a dropdown menu set to "Disable", and "Ping from WAN:" with a dropdown menu set to "Enable". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Figure 5-24 Remote Management

Object	Description
<ul style="list-style-type: none"> Remote management (via WAN) 	Enable or Disable this function.
<ul style="list-style-type: none"> Ping from WAN 	Enable or Disable this function.

5.1.13 DHCP Server Settings

Click "**Operation Mode**" → "**AP Router**" or "**Wireless ISP**" and then enter the "**DHCP Server Settings**" by clicking the **Setup** button next to it. This section allows you to configure the DHCP server.

Figure 5-25 DHCP Server Settings

Object	Description
• DHCP Server	Select as DHCP server or disable the function.
• Lease Time	Select the time for using one assigned IP from the dropdown list. After the lease time, the AP automatically assigns new IP addresses to all connected computers.
• From	The start IP address of all the available successive IPs.
• To	The end IP address of all the available successive IPs.

5.1.14 DMZ Settings

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**DMZ Settings**” by clicking the **Setup** button next to it. This section allows you to configure the DMZ server.

Figure 5-26 DMZ Settings

Object	Description
• DMZ Setting	Disable or Enable DMZ function.
• DMZ IP Address	Enter the DMZ IP address.

5.1.15 Virtual Server Settings

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**Virtual Server Settings**” by clicking the **Setup** button next to it. This section allows you to configure the virtual server.

Virtual Server Settings

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

Virtual Server: ▾

Protocol: ▾

IP Address:

Port Range: -

Comment:

Figure 5-27 Virtual Server Settings

Object	Description
• Virtual Server	Enable or disable Virtual Server.
• Protocol	You can choose TCP, UDP or Both.
• IP Address	Enter the LAN IP.
• Port Range	Set the range of public port.
• Comment	Set a name for the rule.

5.1.16 IP Filtering Settings

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**IP Filtering Settings**” by clicking the **Setup** button next to it. This section allows you to configure the IP filtering settings.

IP Filtering Settings

Filtering: ▾

Protocol: ▾

IP Address:

Comment:

Figure 5-28 IP Filtering Settings

Object	Description
• Filtering	Enable or disable IP Filtering.
• Protocol	You can choose TCP, UDP or Both.
• IP Address	Enter the IP address to be filtered.
• Comment	Set a name for the rule.

5.1.17 Port Filtering Settings

Click “Operation Mode” → “AP Router” or “Wireless ISP” and then enter the “Port Filtering Settings” by clicking the **Setup** button next to it. This section allows you to configure the port filtering settings.

Port Filtering Settings

Filtering:

Protocol:

Port Range: -

Comment:

Figure 5-29 Port Filtering Settings

Object	Description
• Filtering	Enable or disable IP Filtering.
• Protocol	You can choose TCP, UDP or Both.
• Port Range	Enter the range of Port to be filtered.
• Comment	Set a name for the rule.

5.1.18 MAC Filtering Settings

Click “Operation Mode” → “AP Router” or “Wireless ISP” and then enter the “Mac Filtering Settings” by clicking the **Setup** button next to it. This section allows you to configure the MAC filtering settings.

Mac Filtering Settings

Filtering:

Mac Address:

Comment:

Figure 5-30 Mac Filtering Settings

Object	Description
• Filtering	Enable or disable Mac Filtering.
• Mac Address	Enter the Mac address to be filtered.
• Comment	Set a name for the rule.

5.1.19 Bandwidth Control

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**Bandwidth Control**” by clicking the **Setup** button next to it. This section allows you to configure the bandwidth control.

Bandwidth Control Settings

Quality of Service: ▾

Type: ▾

Local IP Address: -

MAC address: (xx:xx:xx:xx:xx:xx)

Uplink BandWidth (Kbps):

Downlink BandWidth (Kbps):

Comment:

Figure 5-31 Bandwidth Control Settings

Object	Description
• Quality of Service	Enable or disable the QoS service.
• Type	Select QoS type IP Address or Mac Address .
• Local IP Address	The IP address segment which uses this QoS rule.
• MAC Address	The Mac address which uses this QoS rule.
• Uplink BandWidth (Kbps)	Set the maximum uplink bandwidth allowed by the listed QoS rules.
• Downlink BandWidth (Kbps)	Set the maximum downlink bandwidth allowed by the listed QoS rules.
• Comment	Set a name for the rule.

5.1.20 SNMP

Click “**Operation Mode**” → “**AP Router**” or “**Wireless ISP**” and then enter the “**SNMP**” by clicking the **Setup** button next to it. This section allows you to configure the SNMP.

SNMP Settings

SNMP:

Read Community:

Write Community:

Trap IP 1:

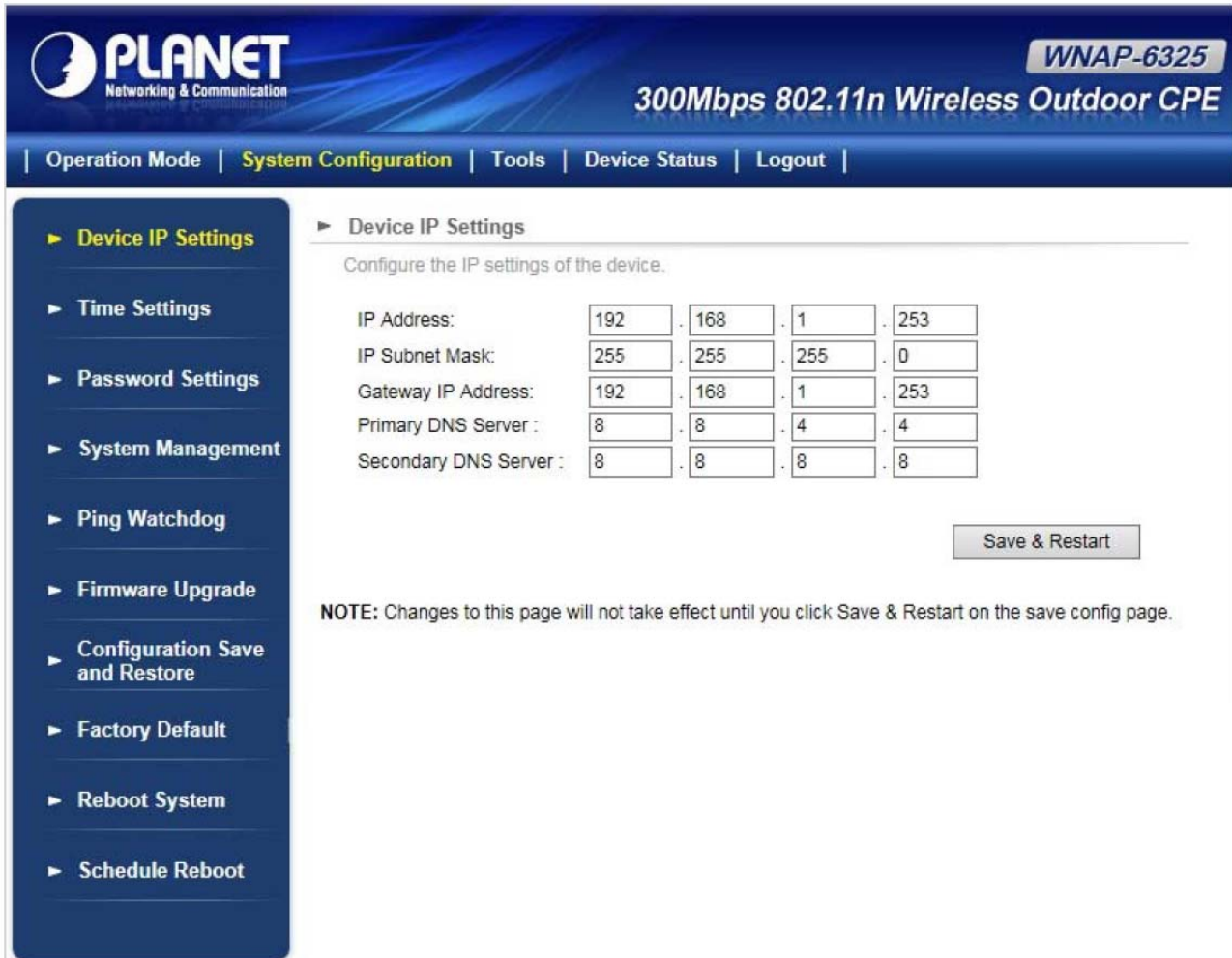
Trap Community 1:

Figure 5-32 SNMP Settings

Object	Description
• SNMP	Enable or disable the SNMP service.
• Read Community	Enter a Read Community name for verification with the SNMP manager for SNMP Read requests.
• Write Community	Enter a Write Community name for verification with the SNMP manager for SNMP Write requests.
• Trap IP 1	Enter the Trap IP address.
• Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP Trap requests.

5.2 System Configuration

On this page, you can configure the system of the WNAP-6325, including IP settings, Time settings, Password settings, System management, Ping Watchdog, Firmware upgrade, Configuration save and restore, Factory default, Reboot and Schedule reboot.



PLANET
Networking & Communication

WNAP-6325
300Mbps 802.11n Wireless Outdoor CPE

| Operation Mode | **System Configuration** | Tools | Device Status | Logout |

▶ **Device IP Settings**

▶ Time Settings

▶ Password Settings

▶ System Management

▶ Ping Watchdog

▶ Firmware Upgrade

▶ Configuration Save and Restore

▶ Factory Default

▶ Reboot System

▶ Schedule Reboot

▶ **Device IP Settings**

Configure the IP settings of the device.

IP Address: 192 . 168 . 1 . 253

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 1 . 253

Primary DNS Server : 8 . 8 . 4 . 4

Secondary DNS Server : 8 . 8 . 8 . 8

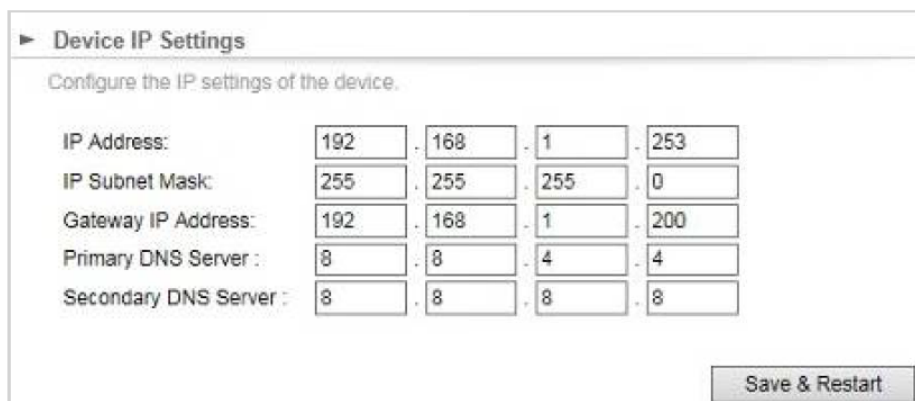
Save & Restart

NOTE: Changes to this page will not take effect until you click Save & Restart on the save config page.

Figure 5-33 System Configuration default page

5.2.1 Default IP Settings

Click "**System Configuration**" → "**Device IP Settings**" and the following page will be displayed.



▶ **Device IP Settings**

Configure the IP settings of the device.

IP Address: 192 . 168 . 1 . 253

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 1 . 200

Primary DNS Server : 8 . 8 . 4 . 4

Secondary DNS Server : 8 . 8 . 8 . 8

Save & Restart

Figure 5-34 Default IP Settings

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • IP Address 	WNAP-6325's LAN IP. The default is 192.168.1.253 . You can change it according to your needs.
<ul style="list-style-type: none"> • IP Subnet Mask 	WNAP-6325's LAN subnet mask.
<ul style="list-style-type: none"> • Gateway IP Address 	The Gateway IP address of WNAP-6325.
<ul style="list-style-type: none"> • Primary DNS Server 	Enter the DNS server. The default is 8.8.4.4.
<ul style="list-style-type: none"> • Secondary DNS Server 	Enter the DNS server. The default is 8.8.8.8.

5.2.2 Time Settings

Click "**System Configuration**" → "**Time Settings**" and the following page will be displayed.

Figure 5-35 Time Settings

Object	Description
<ul style="list-style-type: none"> • Enable NTP 	Enable it to support NTP (Network Time Protocol) for automatic time and date setup.
<ul style="list-style-type: none"> • Server Name 	Enter the host name or IP address of the time server if you wish.
<ul style="list-style-type: none"> • NTP Request Interval 	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.
<ul style="list-style-type: none"> • Local Time Zone 	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.
<ul style="list-style-type: none"> • Local Date and Time 	Set the access point's date and time manually.

5.2.3 Password Settings

Click “**System Configuration**” → “**Password Settings**” and the following page will be displayed.

Figure 5-36 Password Settings

Object	Description
• Current Password	Set the access point’s administrator password. This is used to log in to the browser based on the configuration interface.
• New Password	Enter a new password.
• Re-enter New Password	Enter the new password again.

5.2.4 System Management

Click “**System Configuration**” → “**System Management**” and the following page will be displayed.

Figure 5-37 System Management

Object	Description
• Device Name	Enter a name for this access point. Default is WNAP-6325 .
• POE Passthrough	Enable the POE Passthrough function. ※ When the option “ Enable POE Passthrough ” in the System Management page is checked, the LAN2 can supply passive PoE power to the second WNAP-7325 or WNAP-6325 through the LAN 2.
• UPnP	Check to enable the UPnP function. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. This option is only available in AP Router mode.
• Syslog	Check to enable Syslog function.
• IGMP	Check to enable the IGMP Proxy function. This option is only available in AP Router mode.

5.2.5 Ping Watchdog

Click “**System Configuration**” → “**Ping Watchdog**” and the following page will be displayed.

► Ping Watchdog

The Ping Watchdog will ping the specified IP address for connection status. If the remote IP address does not respond to Ping, the device will power reboot.

Ping Watchdog: Enable Disable

IP Address 1: . . .

Ping Frequency: Seconds (10 to 999, default is: 120)

Failed tries: (default is 2 tries)

Action:

NOTE: Watchdog will take effect 10 minutes after startup, when failed, IP Address 1 must fail to respond for watchdog to take action.

Figure 5-38 Ping Watchdog

Object	Description
• Ping Watchdog	Enable or Disable this function.
• IP Address 1	Enter the IP address which pings every time interval
• Ping Frequency	Set times from 10 to 999.
• Failed tries	Select failed tries from 1 to 5.