Secondary DNS Enter the secondary DNS server address.

Discard Ping on WAN Check to Enable to recognize pings on the ENS202EXT WAN interface or Disable to block pings on the ENS202EXT WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

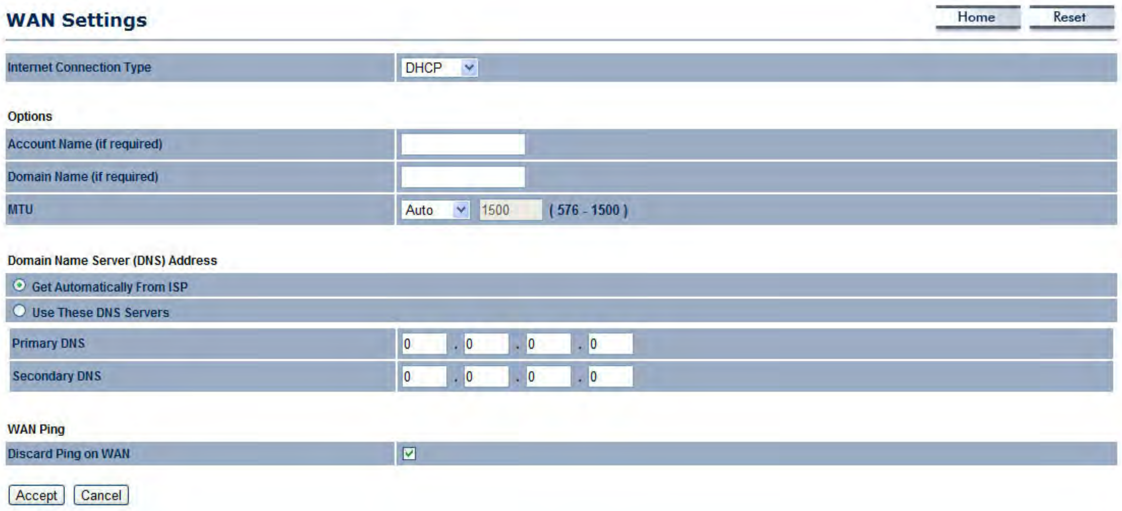
Dynamic IP

Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.

Account Name Enter the account name provided by your ISP.

Domain Name Enter the domain name provided by your ISP.

MTU The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for static IP is 1500. The MTU size can be set between 512 and 1500.



WAN Settings

Internet Connection Type	DHCP

Options

Account Name (if required)	
Domain Name (if required)	
MTU	Auto 1500 (576 - 1500)

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN	☑

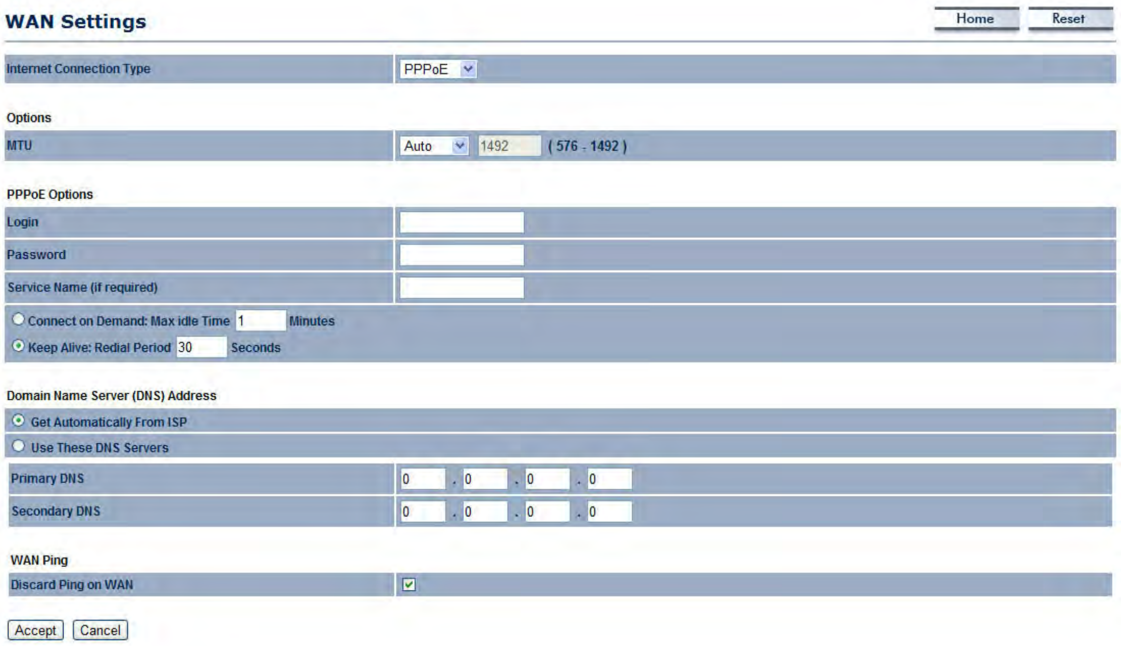
Get Automatically From ISP Click the radio button to obtain the DNS automatically from the DHCP server.

Use These DNS Servers Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN Check to Enable to recognize pings on the ENS202EXT WAN interface or Disable to block pings on the ENS202EXT WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

Point-to-Point Protocol over Ethernet (PPPoE)



WAN Settings

Internet Connection Type	PPPoE

Options

MTU	Auto 1492 (576 - 1492)

PPPoE Options

Login	
Password	
Service Name (if required)	

○ Connect on Demand: Max idle Time 1 Minutes
● Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN	☑

Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet.

MTU Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an internet transmission (PPPoE default: 1492). The MTU size can be set between 512 and 1492.

Login Enter the username assigned by an ISP.

Password Enter the password assigned by an ISP.

Service Name Enter the service name of an ISP (optional).

Connect on Demand Select the radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.

Keep Alive Select whether to keep the Internet connection always on, or enter a redial period once the internet lose connection.

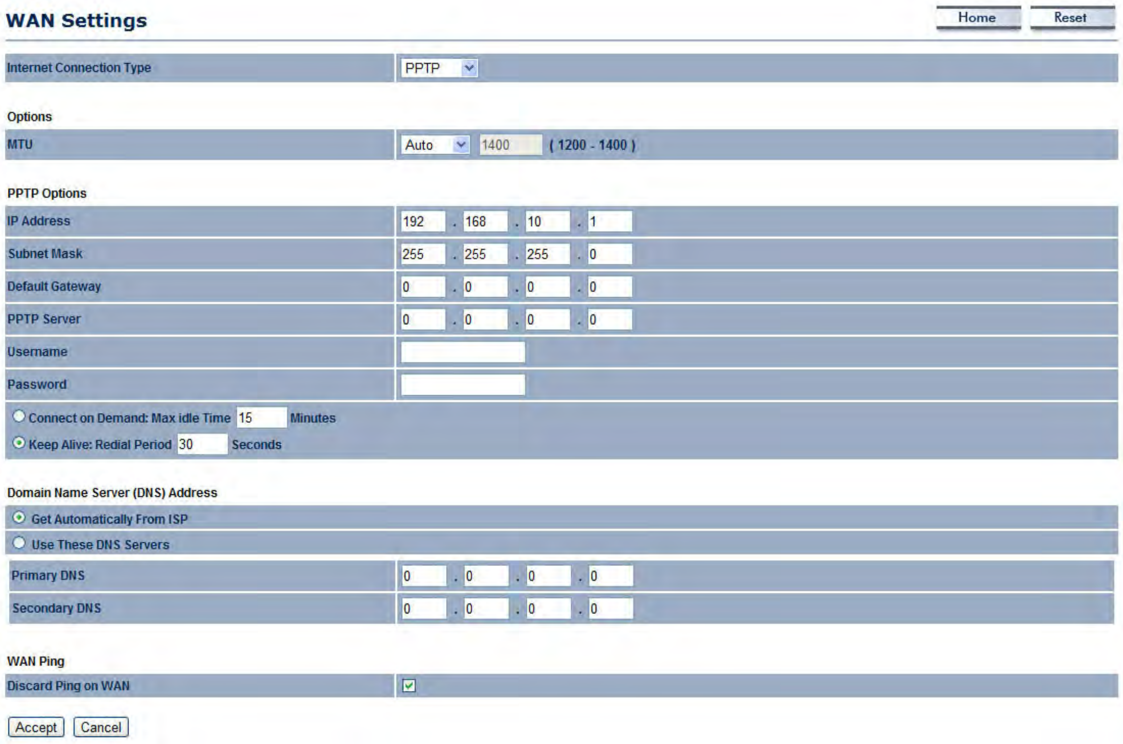
Get Automatically From ISP Click the radio button to obtain the DNS automatically from the DHCP server.

Use These DNS Servers Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN Check to Enable to recognize pings on the ENS202EXT WAN interface or Disable to block pings on the ENS202EXT WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

Point-to-Point Tunnelling Protocol (PPTP)



WAN Settings

Internet Connection Type	PPTP
Options	
MTU	Auto 1400 (1200 - 1400)
PPTP Options	
IP Address	192 . 168 . 10 . 1
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
PPTP Server	0 . 0 . 0 . 0
Username	
Password	
○ Connect on Demand: Max idle Time 15 Minutes	
● Keep Alive: Redial Period 30 Seconds	
Domain Name Server (DNS) Address	
● Get Automatically From ISP	
○ Use These DNS Servers	
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0
WAN Ping	
Discard Ping on WAN	☑

The point-to-point tunnelling protocol (PPTP) is used in association with virtual private networks (VPNs). There a two parts to a PPTP connection: the WAN interface settings and the PPTP settings.

MTU Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an internet transmission (PPPoE default: 1492). The MTU size can be set between 512 and 1492.

IP Address Enter the router’s WAN IP address.

Subnet Mask Enter the router’s WAN subnet IP address.

Default Gateway Enter the router’s WAN gateway IP address.

PPTP Server Enter the IP address of the PPTP server.

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

Connect on Demand If you want the ENS202EXT to end the Internet connection after it has been inactive for a period of time, select this option and enter the number of minutes you want that period of inactivity to last.

Keep Alive If you want the ENS202EXT to periodically check your Internet connection, select this option. Then specify how often you want the ENS202EXT to check the Internet connection. If the connection is down, the ENS202EXT automatically re-establishes your connection

Get Automatically From ISP Obtains the DNS automatically from DHCP server.

Use These DNS Servers Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN Check to Enable to recognize pings on the ENS202EXT WAN interface or Disable to block pings on the ENS202EXT WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

4.3.2 Configuring LAN Settings

IP Address Enter the LAN IP address.

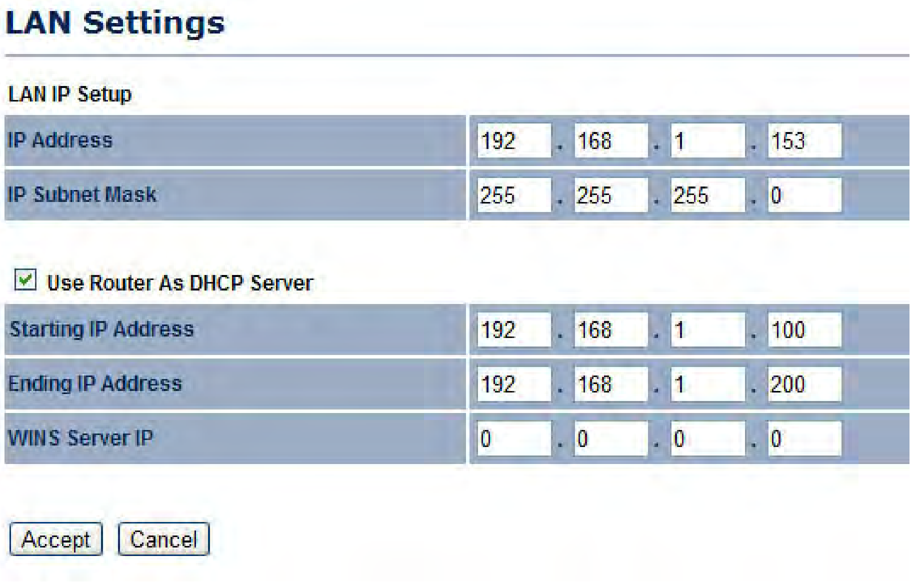
IP Subnet Mask Enter the LAN IP subnet mask.

Use Router As DHCP Server Check this option to enable the ENS202EXT internal DHCP server.

Starting IP Address Specify the starting IP address range for the pool of allocated for private IP addresses. The starting IP address must be on the same subnet as the ending IP address; that is the first three octets specified here must be the same as the first three octets in End IP Address.

Ending IP Address Specify the ending IP address range for the pool of allocated for private IP addresses. The ending IP address must be on the same subnet as the starting IP address; that is the first three octets specified here must be the same as the first three octets in Start IP Address.

WINS Server IP Enter the IP address of the WINS server.



LAN Settings

LAN IP Setup

IP Address	192 . 168 . 1 . 153
IP Subnet Mask	255 . 255 . 255 . 0

☑ Use Router As DHCP Server

Starting IP Address	192 . 168 . 1 . 100
Ending IP Address	192 . 168 . 1 . 200
WINS Server IP	0 . 0 . 0 . 0

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

4.3.3 Configuring VPN Pass-Through

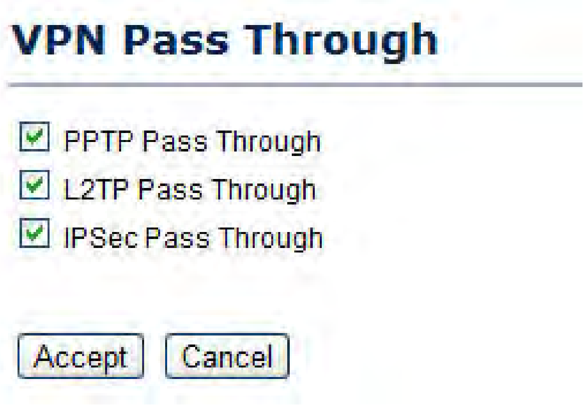
VPN Pass-through allows a secure virtual private network (VPN) connection between two computers. Enabling the options on this page opens a VPN port and enables connections to pass through the ENS202EXT without interruption.

PPTP Pass-through Check this option to enable PPTP pass-through mode.

L2TP Pass-through Check this option to enable L2TP pass-through mode.

IPSec Pass-through Check this option to enable IPSec pass-through mode.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.



VPN Pass Through

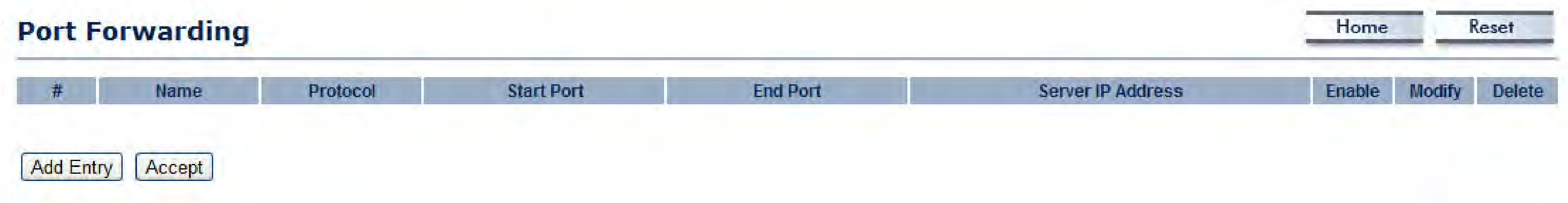
☑ PPTP Pass Through

☑ L2TP Pass Through

☑ IPSec Pass Through

4.3.4 Configuring Port Forwarding

Port forwarding enables multiple server applications on a LAN to serve clients on a WAN over a single WAN IP address. The router accepts incoming client packets, filters them based on the destination WAN, or public, port and protocol and forwards the packets to the appropriate LAN, or local, port. Unlike the DMZ feature, port forwarding protects LAN devices behind the firewall.



Port Forwarding

#	Name	Protocol	Start Port	End Port	Server IP Address	Enable	Modify	Delete

NO. Displays the sequence number of the forwarded port.

Name Displays the name of the forwarded port.

Protocol Displays the protocol to use for mapping from the following: `TCP`, `UDP` or `Both`.

Start Port Displays the LAN port number that WAN client packets will be forward to.

End Port Displays the port number that the WAN client packets are received.

Server IP Displays the IP address of the server for the forwarded port.

Enable Click to enable or disable the forwarded port profile.

Modify Click to modify the forwarded port profile.

Delete Click to delete the forwarded port profile.

Click `Add Entry` to add port forwarding rules.

Click `Accept` to confirm the changes.

Service Name Enter a name for the port forwarding rule.

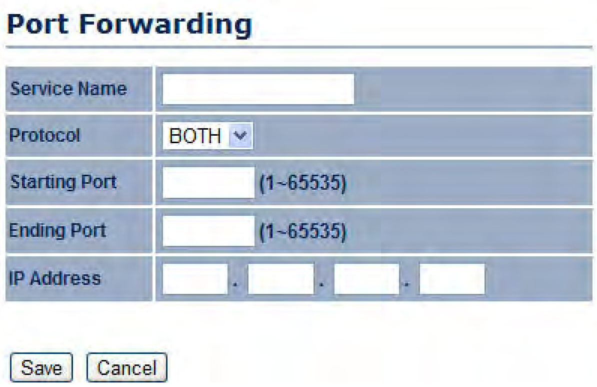
Protocol Select a protocol for the application: Choices are Both, TCP, and UDP.

Starting Port Enter a starting port number.

Ending Port Enter an ending port number. All ports numbers between the starting and ending ports will forward users to the IP address specified in the IP Address field.

IP Address Enter the IP address of the server computer on the LAN network where users will be redirected.

Click `Save` to apply the changes or `Cancel` to return previous settings.



Port Forwarding

Service Name	
Protocol	BOTH
Starting Port	(1~65535)
Ending Port	(1~65535)
IP Address	. . .

4.3.5 Configuring Demilitarized Zone

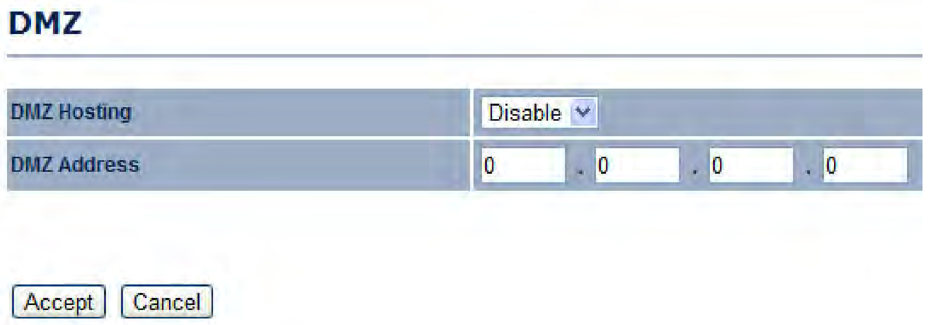
Configuring a device on the LAN as a demilitarized zone (DMZ) host allows unrestricted two-way Internet access for Internet applications, such as online video games, to run from behind the NAT firewall. The DMZ function allows the router to redirect all packets going to the WAN port IP address to a particular IP address on the LAN. The difference between the virtual server and the DMZ function is that a virtual server redirects a particular service or Internet application, such as FTP, to a particular LAN client or server, whereas a DMZ redirects all packets, regardless of the service, going to the WAN IP address to a particular LAN client or server.

WARNING!
The PC defined as a DMZ host is not protected by the firewall and is vulnerable to malicious network attacks. Do not store or manage sensitive information on the DMZ host.

DMZ Hosting Select `Enable DMZ` to activate DMZ functionality.

DMZ Address Enter an IP address of a device on the LAN.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.



DMZ

DMZ Hosting	Disable
DMZ Address	0 . 0 . 0 . 0

4.4 Configuring Wireless LAN

4.4.1 Configuring Wireless Settings

Instructions on how to configure the wireless and security settings for each of the possible operating modes.

WARNING!
Incorrectly changing these settings may cause the device to stop functioning. Do not modify the settings in this section without a thorough understanding of the parameters.

Access Point Mode

The ENS202EXT supports Access Point Mode. In this mode, users with a wireless client device within range can connect to the ENS202EXT to access the WLAN.

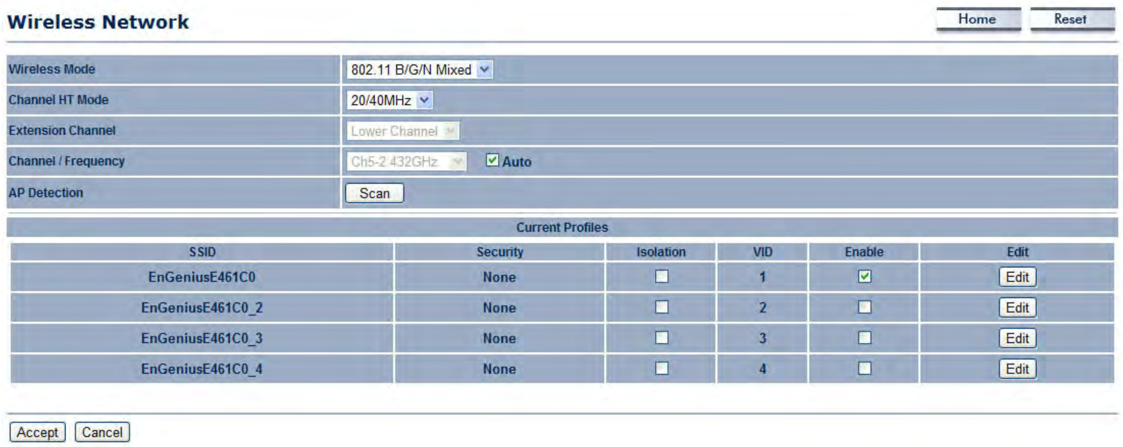
Wireless Mode Wireless mode supports 802.11b/g/n mixed modes.

Channel HT Mode The default channel bandwidth is 40 MHz. The larger the channel, the better the transmission quality and speed.

Extension Channel Select upper or lower channel. Your selection may affect the Auto channel function.

Channel / Frequency Select the channel and frequency appropriate for your country's regulation.

Auto Check this option to enable auto-channel selection.



Wireless Network

Wireless Mode	802.11 B/G/N Mixed
Channel HT Mode	20/40MHz
Extension Channel	Lower Channel
Channel / Frequency	Ch5-2.432GHz ☑ Auto
AP Detection	Scan

Current Profiles

SSID	Security	Isolation	VID	Enable	Edit
EnGeniusE461C0	None	□	1	☑	Edit
EnGeniusE461C0_2	None	□	2	□	Edit
EnGeniusE461C0_3	None	□	3	□	Edit
EnGeniusE461C0_4	None	□	4	□	Edit

AP Detection AP Detection can select the best channel to use by scanning nearby areas for Access Points.

Current Profile Configure up to four different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click `Edit` to configure the profile and check whether you want to enable extra SSIDs.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

SSID Specify the SSID for the current profile.

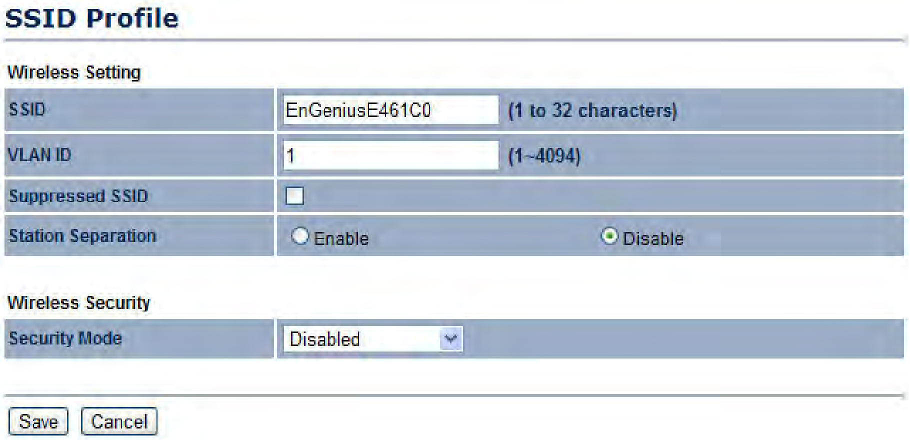
VLAN ID Specify the VLAN tag for the current profile.

Suppressed SSID Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Station Separation Click the appropriate radio button to allow or prevent communication between client devices.

Wireless Security For details on wireless security settings, see *Configuring Wireless Security*.

Click `Save` to accept the changes or `Cancel` to cancel and return previous settings.



SSID Profile

Wireless Setting

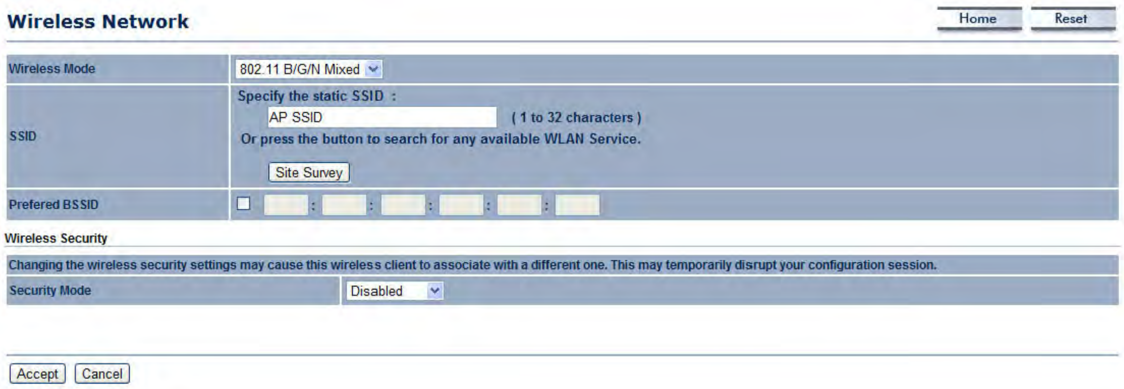
SSID	EnGeniusE461C0 (1 to 32 characters)
VLAN ID	1 (1~4094)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	Disabled

Client Bridge Mode

Client Bridge Mode lets you connect two LAN segments via a wireless link as though they are on the same physical network. Since the computers are on the same subnet, broadcasts reach all machines. As a result, DHCP information generated by the server reach all client computers as though the clients residing on one physical network.



Wireless Network

Wireless Mode	802.11 B/G/N Mixed
SSID	Specify the static SSID : AP SSID (1 to 32 characters) Or press the button to search for any available WLAN Service.
Prefered BSSID	□ : : : : :

Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	Disabled

Wireless Mode Wireless mode supports 802.11b/g/n mixed modes.

SSID Specify the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.

Site Survey Scans nearby locations for Access Points. You can select a discovered Access Point to establish a connection.

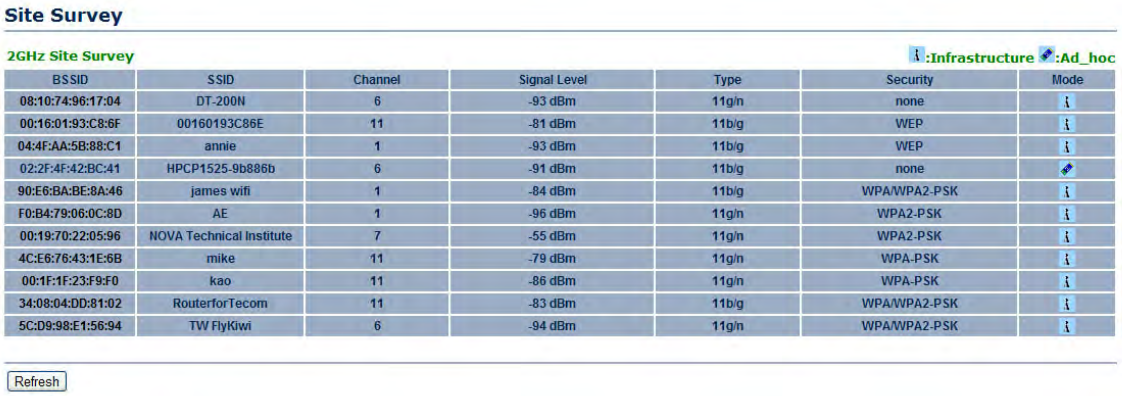
Prefer BSSID Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.

Wireless Security For details on wireless security settings, see *Configuring Wireless Security*.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

Profiles If you used the Site Survey, the Web Configurator shows nearby Access Points. To connect to an Access Point, click the Access Point’s BSSID.

Click `Refresh` to scan again.



Site Survey

2GHz Site Survey

ℹ:Infrastructure ◆:Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
08:10:74:96:17:04	DT-200N	6	-93 dBm	11g/n	none	ℹ
00:16:01:93:C8:6F	00160193C86E	11	-81 dBm	11b/g	WEP	ℹ
04:4F:AA:5B:88:C1	annie	1	-93 dBm	11b/g	WEP	ℹ
02:2F:4F:42:BC:41	HPCP1525-9b886b	6	-91 dBm	11b/g	none	◆
90:E6:BA:BE:8A:46	james wifi	1	-84 dBm	11b/g	WPA/WPA2-PSK	ℹ
F0:B4:79:06:0C:8D	AE	1	-96 dBm	11g/n	WPA2-PSK	ℹ
00:19:70:22:05:96	NOVA Technical Institute	7	-55 dBm	11g/n	WPA2-PSK	ℹ
4C:E6:76:43:1E:6B	mike	11	-79 dBm	11g/n	WPA-PSK	ℹ
00:1F:1F:23:F9:F0	kao	11	-86 dBm	11g/n	WPA-PSK	ℹ
34:08:04:DD:81:02	RouterforTecom	11	-83 dBm	11b/g	WPA/WPA2-PSK	ℹ
5C:D9:98:E1:56:94	TW FlyKiwi	6	-94 dBm	11g/n	WPA/WPA2-PSK	ℹ

WDS Bridge Mode

Unlike traditional bridging. WDS Bridge Mode allows you to create large wireless networks by linking several wireless access points with WDS links. WDS is normally used in large, open areas, where pulling wires is cost prohibitive, restricted or physically impossible.

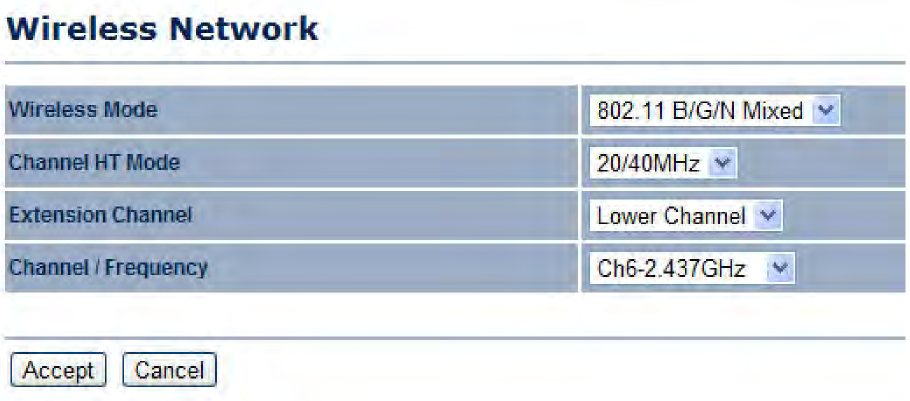
Wireless Mode Wireless mode supports 802.11b/g/n mixed modes.

Channel HT Mode The default channel bandwidth is 40 MHz. The larger the channel, the better the transmission quality and speed.

Extension Channel Select upper or lower channel. Your selection may affect the Auto channel function.

Channel / Frequency Select the channel and frequency appropriate for your country's regulation.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.



Wireless Network

Wireless Mode	802.11 B/G/N Mixed
Channel HT Mode	20/40MHz
Extension Channel	Lower Channel
Channel / Frequency	Ch6-2.437GHz

Security Select the type of WDS security: None, WEP, or AES.

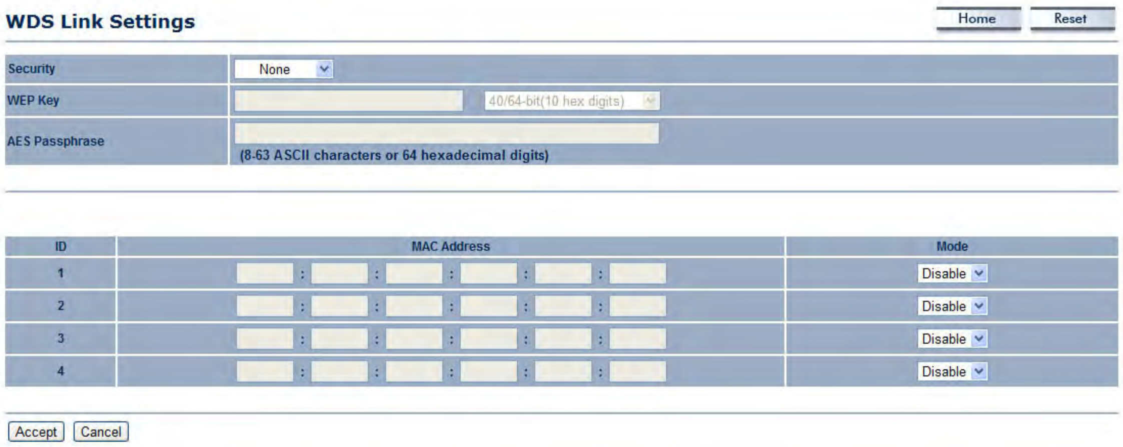
WEP Key Enter the WEP key.

AES Pass phrase Enter the AES pass phrase.

MAC Address Enter the MAC address of the Access Point to which you want to extend wireless connectivity.

Mode Select Disable or Enable to disable or enable WDS.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.



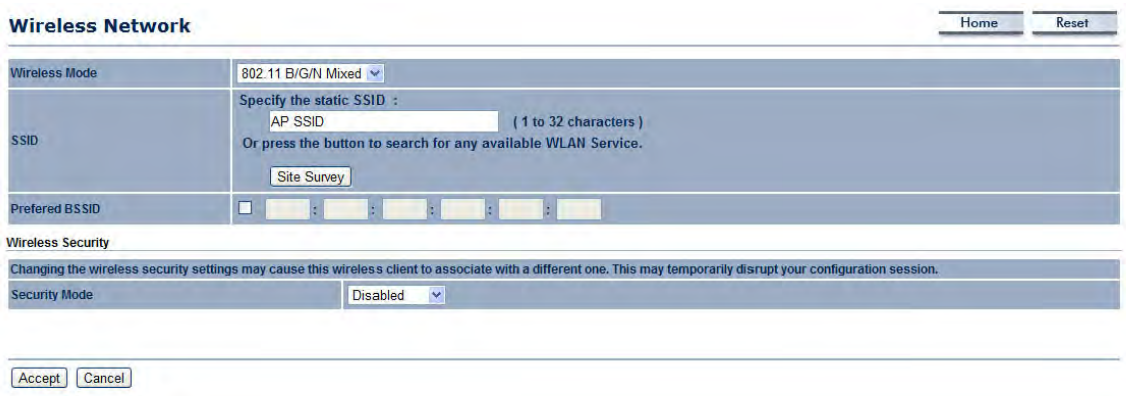
WDS Link Settings

Security	None
WEP Key	40/64-bit(10 hex digits)
AES Passphrase	(8-63 ASCII characters or 64 hexadecimal digits)

ID	MAC Address	Mode
1	: : : : :	Disable
2	: : : : :	Disable
3	: : : : :	Disable
4	: : : : :	Disable

Client Router Mode

In Client Router Mode, you can access the Internet wirelessly with the support of a WISP. It also supports VPN pass-through for sensitive data secure transmission.



Wireless Network

Wireless Mode	802.11 B/G/N Mixed
SSID	Specify the static SSID : AP SSID (1 to 32 characters) Or press the button to search for any available WLAN Service.
Prefered BSSID	□ : : : : :

Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	Disabled

Wireless Mode Wireless mode supports 802.11b/g/n mixed modes.

SSID Specify the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.

Site Survey Scans nearby locations for Access Points. You can select a discovered Access Point to establish a connection.

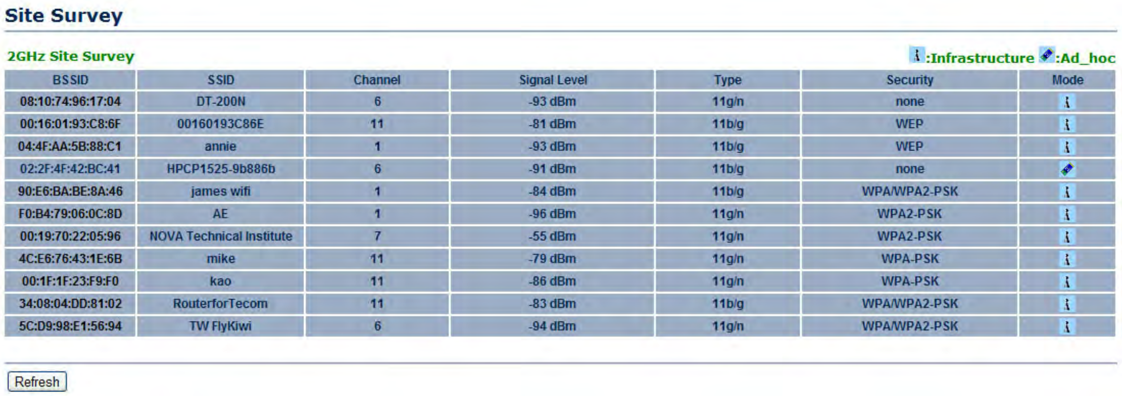
Prefer BSSID Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.

Wireless Security For details on wireless security settings, see *Configuring Wireless Security*.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

Profiles If you used the Site Survey, the Web Configurator shows nearby Access Points. To connect to an Access Point, click the Access Point's BSSID.

Click `Refresh` to scan again.



Site Survey

2GHz Site Survey

ℹ:Infrastructure ✎:Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
08:10:74:96:17:04	DT-200N	6	-93 dBm	11g/n	none	ℹ
00:16:01:93:C8:6F	00160193C86E	11	-81 dBm	11b/g	WEP	ℹ
04:4F:AA:5B:88:C1	annie	1	-93 dBm	11b/g	WEP	ℹ
02:2F:4F:42:BC:41	HPCP1525-9b886b	6	-91 dBm	11b/g	none	✎
90:E6:BA:BE:8A:46	james wifi	1	-84 dBm	11b/g	WPA/WPA2-PSK	ℹ
F0:B4:79:06:0C:8D	AE	1	-96 dBm	11g/n	WPA2-PSK	ℹ
00:19:70:22:05:96	NOVA Technical Institute	7	-55 dBm	11g/n	WPA2-PSK	ℹ
4C:E6:76:43:1E:6B	mike	11	-79 dBm	11g/n	WPA-PSK	ℹ
00:1F:1F:23:F9:F0	kao	11	-86 dBm	11g/n	WPA-PSK	ℹ
34:08:04:DD:81:02	RouterforTecom	11	-83 dBm	11b/g	WPA/WPA2-PSK	ℹ
5C:D9:98:E1:56:94	TW FlyKiwi	6	-94 dBm	11g/n	WPA/WPA2-PSK	ℹ

4.4.2 Configuring Wireless Security

The Wireless Security Settings section lets you configure the ENS202EXT’s security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you use WPA2-PSK.

Wired Equivalent Privacy (WEP)

Security Mode Select WEP from the drop-down list to begin the configuration.

Auth Type Select Open System or Shared.

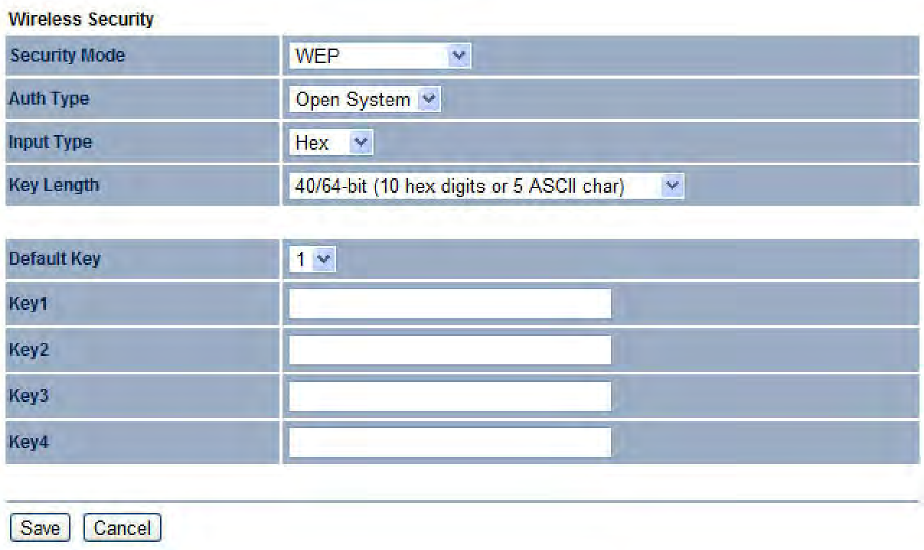
Input Type Select an input type of Hex or ASCII.

Key Length Level of WEP encryption applied to all WEP keys. Select a 64/128/152-bit password lengths.

Default Key Specify which of the four WEP keys the ENS202EXT uses as its default.

Key1 - Key4 Specify a password for the security key index. For security, each typed character is masked by a dot.

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

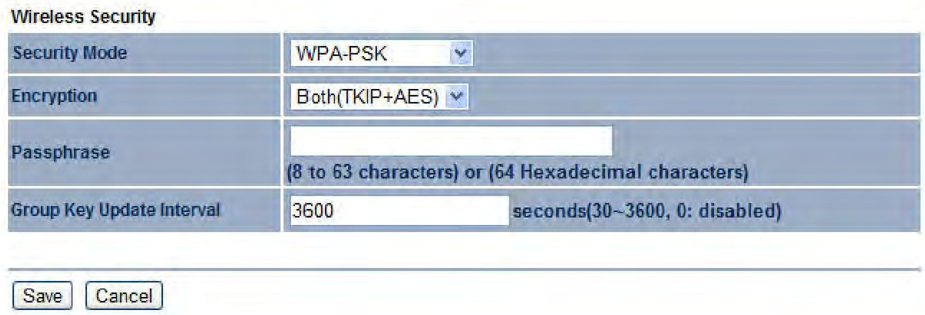


Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)



Wireless Security

Security Mode	WPA-PSK
Encryption	Both(TKIP+AES)
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

Security Mode Select WPA-PSK from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires passphrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

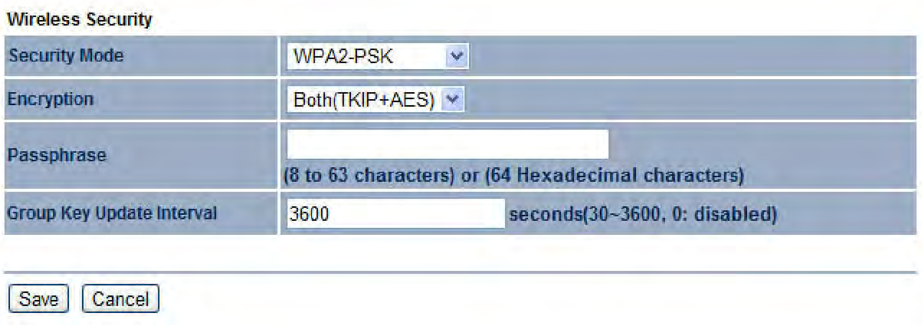
Passphrase Specify the security password. For security, each typed character is masked by a dot.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK)



Wireless Security

Security Mode	WPA2-PSK
Encryption	Both(TKIP+AES)
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

Security Mode Select WPA2-PSK from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires passphrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

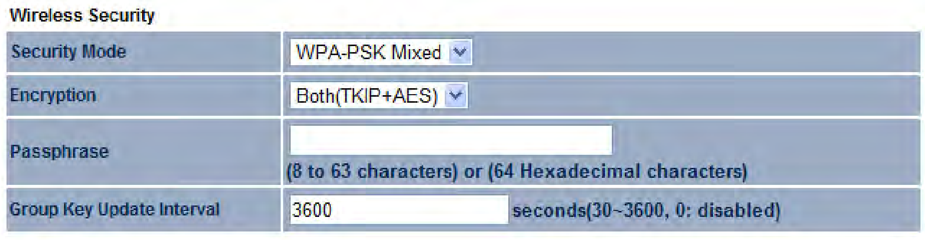
Passphrase Specify the security password. For security, each typed character is masked by a dot.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) Mixed



Wireless Security

Security Mode	WPA-PSK Mixed
Encryption	Both(TKIP+AES)
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

Security Mode Select WPA2-PSK Mixed from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires passphrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

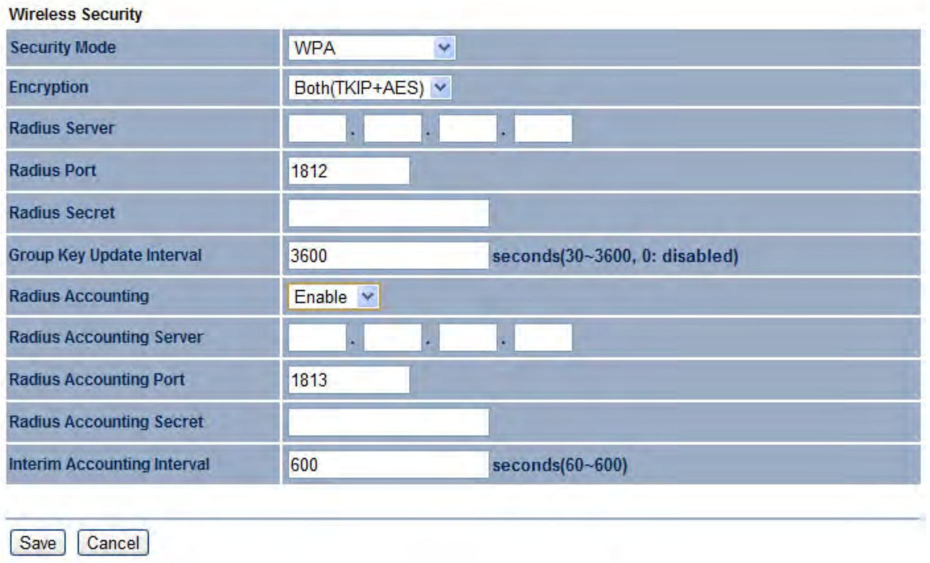
Passphrase Specify the security password. For security, each typed character is masked by a dot.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
WPA-PSK Mixed can allow multiple security modes at the same time. 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access (WPA)



Wireless Security

Security Mode	WPA
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable
Radius Accounting Server	. . .
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 seconds(60~600)

Security Mode Select WPA from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires pass-phrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server Specify the IP address of the RADIUS server.

Radius Port Specify the port number that your RADIUS server uses for authentication. Default port is 1812.

Radius Secret Specify RADIUS secret furnished by the RADIUS server.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Radius Accounting Select to enable or disable RADIUS accounting.

Radius Accounting Server Specify the IP address of the RADIUS accounting server.

Radius Accounting Port Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.

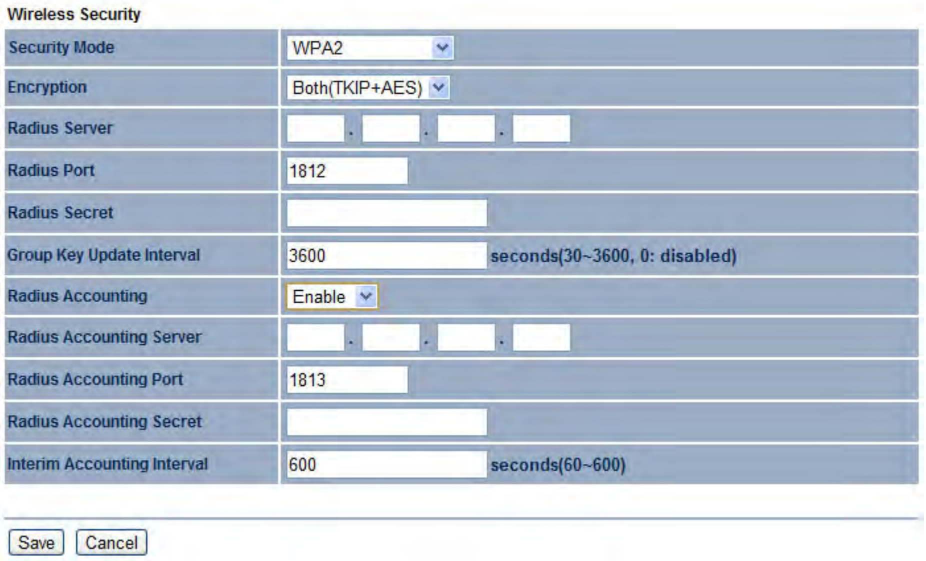
Radius Accounting Secret Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval Specify the interem accounting interval (60 - 600 seconds).

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access 2 (WPA2)



Wireless Security

Security Mode	WPA2
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable
Radius Accounting Server	. . .
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 seconds(60~600)

Security Mode Select WPA2 from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires passphrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server Specify the IP address of the RADIUS server.

Radius Port Specify the port number that your RADIUS server uses for authentication. Default port is 1812.

Radius Secret Specify RADIUS secret furnished by the RADIUS server.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Radius Accounting Select to enable or disable RADIUS accounting.

Radius Accounting Server Specify the IP address of the RADIUS accounting server.

Radius Accounting Port Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.

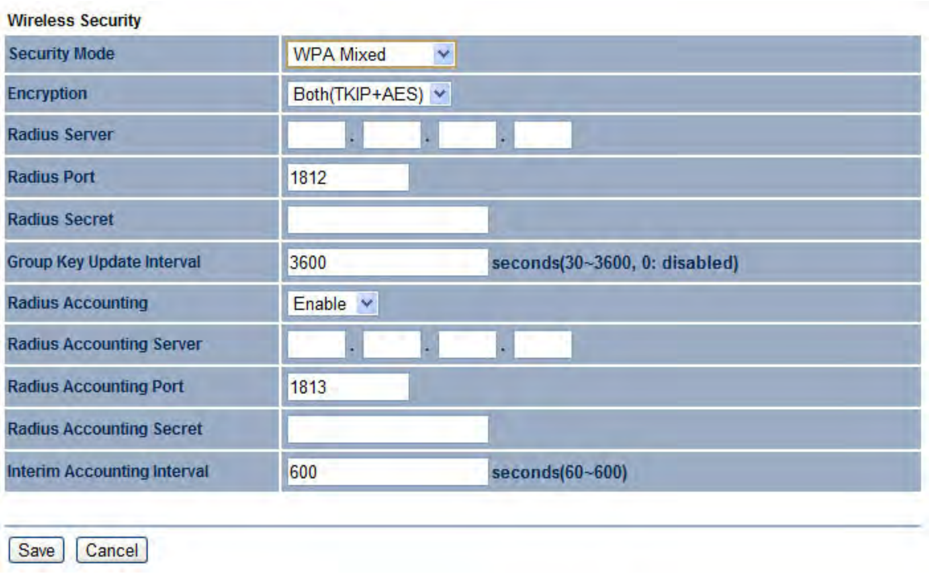
Radius Accounting Secret Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval Specify the interem accounting interval (60 - 600 seconds).

Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

Wi-Fi Protected Access (WPA) Mixed



Wireless Security

Security Mode	WPA Mixed
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable
Radius Accounting Server	. . .
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 seconds(60~600)

Security Mode Select WPA Mixed from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.
- TKIP = automatic encryption with WPA-PSK; requires pass-phrase.
- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server Specify the IP address of the RADIUS server.

Radius Port Specify the port number that your RADIUS server uses for authentication. Default port is 1812.

Radius Secret Specify RADIUS secret furnished by the RADIUS server.

Group Key Update Interval Specify how often, in seconds, the group key changes.

Radius Accounting Select to enable or disable RADIUS accounting.

Radius Accounting Server Specify the IP address of the RADIUS accounting server.

Radius Accounting Port Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.

Radius Accounting Secret Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval Specify the interem accounting interval (60 - 600 seconds).

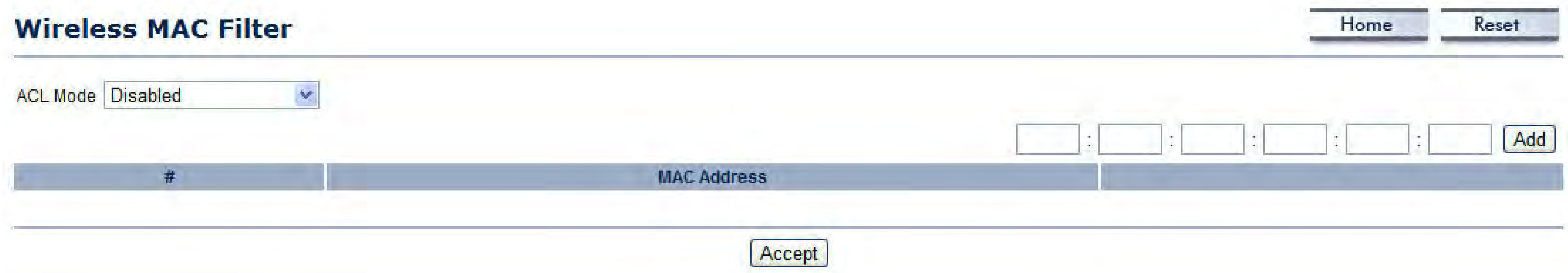
Click `Save` to save the changes or `Cancel` to cancel and return previous settings.

Note:
802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will change from 802.11n to 802.11g.

4.4.3 Configuring Wireless MAC Filter

Note:
This section applies to Access Point and WDS Access point mode.

Wireless MAC Filters are used to allow or deny network access to wireless clients according to their MAC addresses. You can manually add a MAC address to restrict the permission to access ENS202EXT. The default setting is Disable Wireless MAC Filters.



Wireless MAC Filter

ACL Mode: Disabled

#	MAC Address	

ACL Mode Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. Choices are Disable, Deny MAC in the list, or Allow MAC in the list.

MAC Address Filter Enter the MAC address of the device.

Click Add to add the MAC address to the MAC Address table.

Click `Apply` to apply the changes.

4.4.4 Configuring WDS Link Settings

Using WDS Link Settings, you can create a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple Access Points without the need for a wired backbone to link them, as is traditionally required.

Security Select the type of WDS security: None, WEP, or AES.

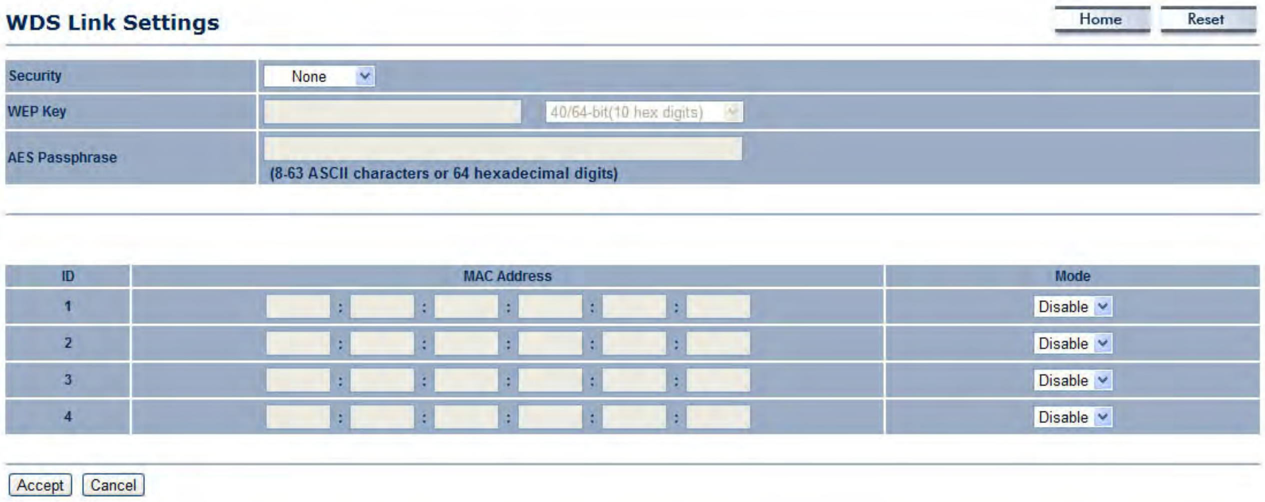
WEP Key Enter the WEP key.

AES Passphrase Enter the AES passphrase.

MAC Address Enter the MAC address of the Access Point to which you want to extend wireless connectivity.

Mode Select Disable or Enable to disable or enable WDS.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.



WDS Link Settings

Security	None
WEP Key	40/64-bit(10 hex digits)
AES Passphrase	(8-63 ASCII characters or 64 hexadecimal digits)

ID	MAC Address	Mode
1	: : : : :	Disable
2	: : : : :	Disable
3	: : : : :	Disable
4	: : : : :	Disable

Note:

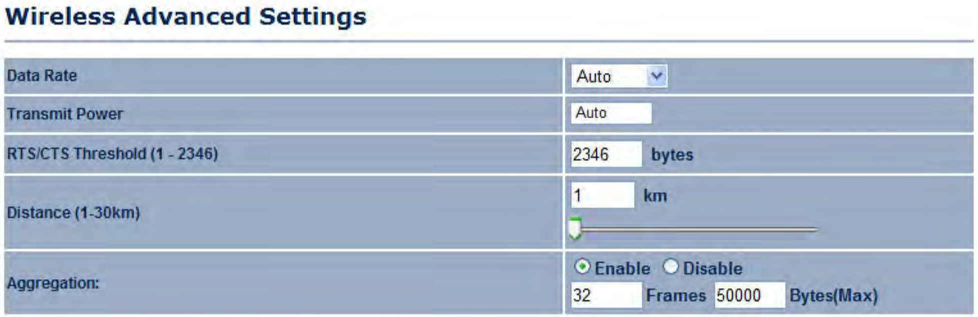
You must enter the ENS202EXT’s MAC address in an access point to establish a connection to it. For more information on how to enter a MAC address in the access point, refer to its documentation. Not all access points support this feature.

4.4.5 Configuring Wireless Advanced Settings

Configure the advanced wireless settings for your access point using the screens in this section. Leave these settings to their default values if you are not sure what values to enter.

Data Rate Select a data rate from the drop-down list. The data rate affects throughput. If you select a low data rate value, for example, the throughput is reduced but the transmission distance increases.

Transmit Power Auto



Wireless Advanced Settings

Data Rate	Auto
Transmit Power	Auto
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	1 km
Aggregation:	● Enable ○ Disable 32 Frames 50000 Bytes(Max)

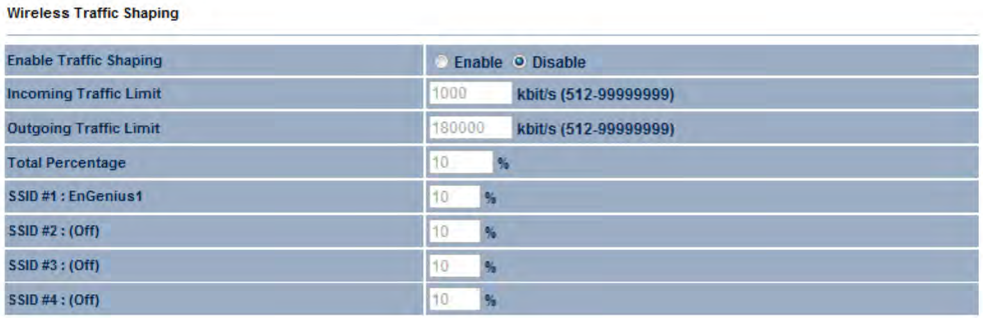
RTS/CTS Threshold Specify the threshold package size for RTC/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth.

Distance Specify the distance between Access Points and clients. Longer distances may drop high-speed connections.

Aggregation Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes.

Wireless Traffic Shaping

Enable Traffic Shaping Check this option to enable wireless traffic shaping. Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.



Wireless Traffic Shaping

Enable Traffic Shaping	○ Enable ● Disable
Incoming Traffic Limit	1000 kbit/s (512-99999999)
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : EnGenius1	10 %
SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %

Incoming Traffic Limit Specify the wireless transmission speed used for downloading.

Outgoing Traffic Limit Specify the wireless transmission speed used for uploading.

Total Percentage Specify the total percentage of the wireless traffic that is shaped.

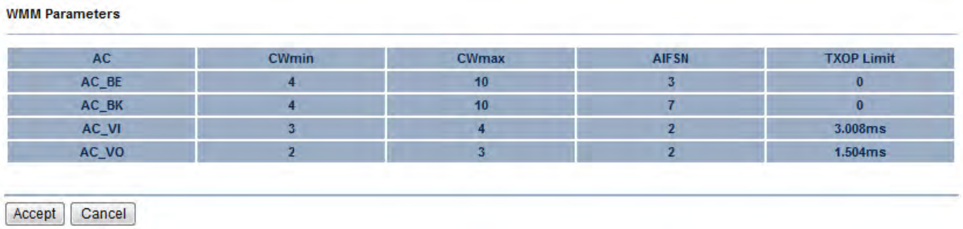
SSID1 to SSID4 Specify the percentage of the wireless traffic that is shaped for a specific SSID.

Wi-Fi Multimedia (WMM) Parameters

WMM manages the priority of audio, video and voice data over a Wi-Fi network so that data from other applications are less likely to interfere with transmission. The parameters CWmin, CWmax and AIFS together control the priority of the four access categories (AC).

AC Displays the following access categories that WMM prioritizes:

- AC_VO = voice
- AC_VI = video
- AC_BE = best effort
- AC_BK = background



WMM Parameters

AC	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

CWmin Displays the minimum size of the contention window.

CWmax Displays the maximum size of the contention window.

AIFSN Displays the arbitration inter frame space value (AIFS).

TXOP Limit Displays the transfer opportunity limit in units of 32 microseconds.

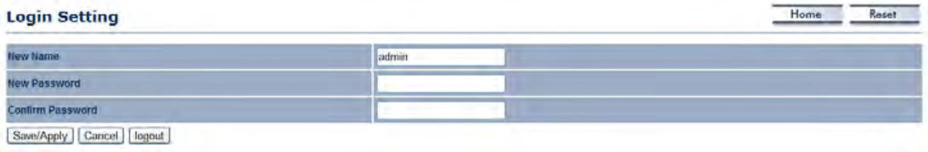
Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

4.5 Management Setup

The Management section lets you configure administration, management VLAN, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log settings. This chapter describes these settings.

4.5.1 Configuring Administrator Account

Click the Administration link under the Management menu to change the user name and password used to log on to the ENS202EXT Web Configurator. The default user name is `admin` and the default password is `admin`. Changing these settings protects the ENS202EXT configuration settings from being accessed by unauthorized users.



Login Setting

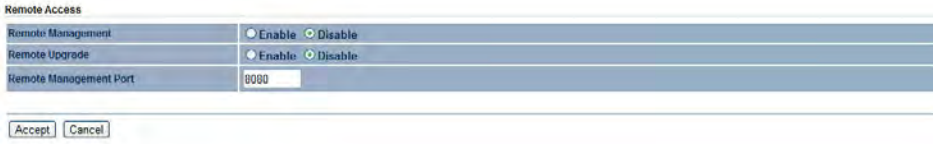
New Name	admin
New Password	
Confirm Password	

New Name Enter a new username for logging in to the Web Configurator.

New Password Enter a new password for logging in to the Web Configurator

Confirm Password Re-enter the new password for confirmation.

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.



Remote Access

Remote Management	○ Enable ● Disable
Remote Upgrade	○ Enable ● Disable
Remote Management Port	8080

Remote Management Enable or disable remote management.

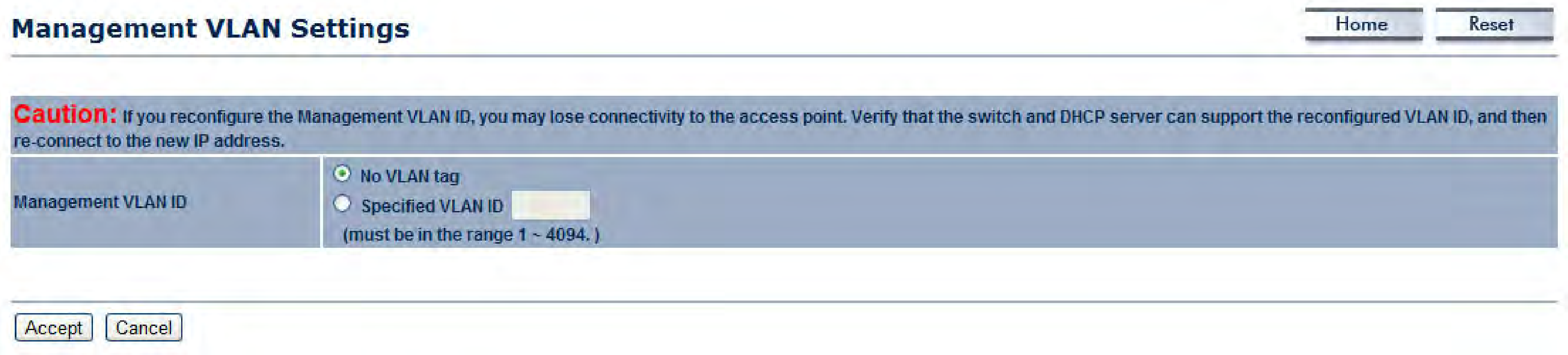
Remote Upgrade Specify whether the ENS202EXT firmware can be upgraded remotely.

Remote Management Port If remote management is enabled, enter the port number to be used for remote management. For example: If you specify the port number 8080, enter **`http://<IP address>:8080`** to access the ENS202EXT Web Configurator.

Click `Accept` to apply the changes or `Cancel` to return previous settings.

4.5.2 Configuring Management VLAN

Click the Management VLAN link under the Management menu to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN



Management VLAN Settings

Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID	● No VLAN tag ○ Specified VLAN ID (must be in the range 1 ~ 4094.)

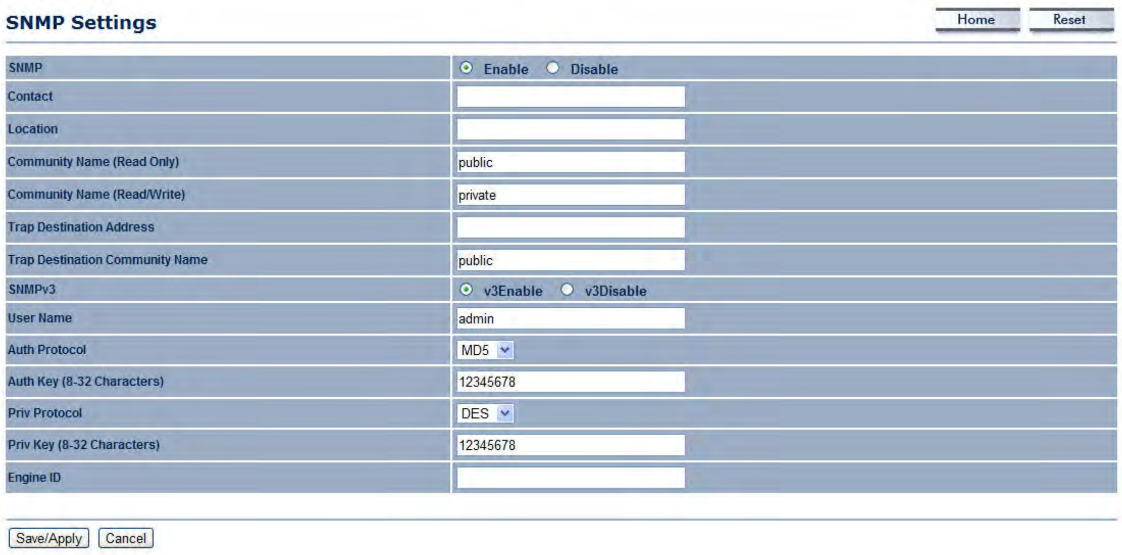
Management VLAN ID If your network includes VLANs and if tagged packets need to pass through the Access Point, enter the VLAN ID. Otherwise, click No VLAN tag.

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

Note:
If you reconfigure the Management VLAN ID, you may lose your connection to the ENS202EXT. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the ENS202EXT using the new IP address.

4.5.3 Configuring SNMP

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.



SNMP Settings

SNMP	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination Address	
Trap Destination Community Name	public
SNMPv3	● v3Enable ○ v3Disable
User Name	admin
Auth Protocol	MD5
Auth Key (8-32 Characters)	12345678
Priv Protocol	DES
Priv Key (8-32 Characters)	12345678
Engine ID	

SNMP Enable or disable the ENS202EXT SNMP function.

Contact Enter the contact details of the device.

Location Enter the location of the device.

Community Name (Read Only) Enter the password for accessing the SNMP community for read-only access.

Community Name (Read/Write) Enter the password for accessing the SNMP community for read and write access.

Trap Destination Address Enter the IP address where SNMP traps are to be sent.

Trap Destination Community Name Enter the password of the SNMP trap community.

SNMPv3 Enable or Disable the SNMPv3 feature.

User Name Specify the username for SNMPv3.

Auth Protocol Select the authentication protocol type: MD5 or SHA.

Auth Key (8-32 Characters) Specify the authentication key for authentication.

Priv Protocol Select the privacy protocol type: DES.

Priv Key (8-32 Characters) Specify the privacy key for privacy.

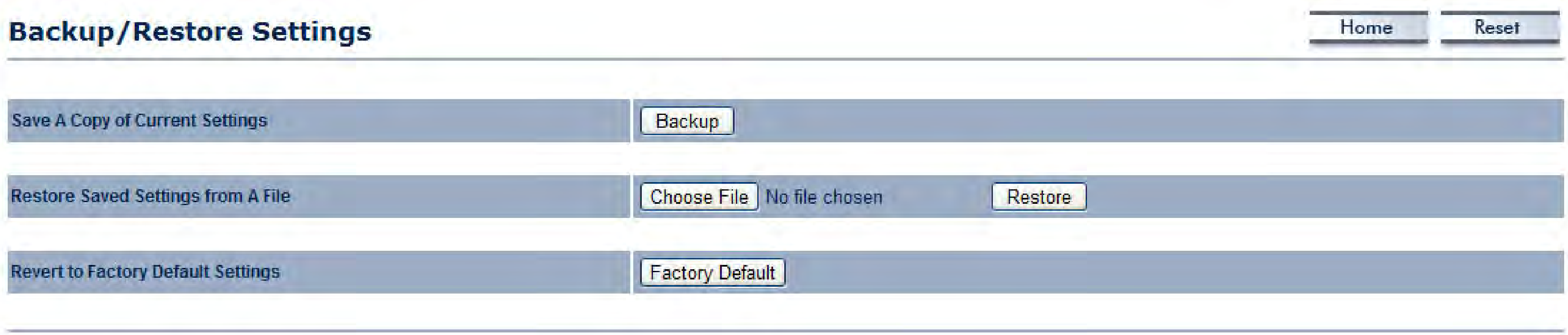
Engine ID Specify the engine ID for SNMPv3.

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.

4.5.4 Configuring Backup/Restore Settings

Click the Backup/Restore Setting link under the Management menu to save the ENS202EXT's current settings in a file on your local disk or load settings onto the device from a local disk. This feature is particularly convenient administrators who have several ENS202EXT devices that need to be configured with the same settings.

This page also lets you return the ENS202EXT to its factory default settings. If you perform this procedure, any changes made to the ENS202EXT default settings will be lost.



Backup/Restore Settings

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	Choose File No file chosen Restore
Revert to Factory Default Settings	Factory Default

Save A Copy of Current Settings Click `Backup` to save the current configured settings.

Restore Saved Settings from A File To restore settings that have been previously backed up, click `Browse`, select the file, and click `Restore`.

Revert to Factory Default Settings Click `Factory Default` to restore the ENS202EXT to its factory default settings.

4.5.5 Configuring Firmware Upgrade

Firmware is system software that operates and allows the administrator to interact with the router.

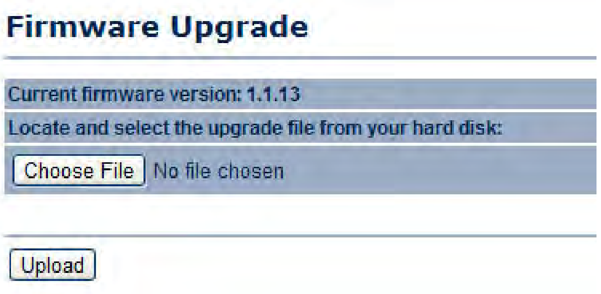
WARNING!

Upgrading firmware through a wireless connection is not recommended. Firmware upgrading must be performed while connected to an Ethernet (LAN port) with all other clients disconnected.

The firmware upgrade procedure can take several minutes. Do not power off the ENS202EXT during the firmware upgrade, as it can cause the device to crash or become unusable.

To update the firmware version, follow these steps:

1. Download the appropriate firmware approved by EnGenius Networks from an approved web site.



Firmware Upgrade

Current firmware version: 1.1.13

Locate and select the upgrade file from your hard disk:

Note:

Save the firmware file to a local hard drive.

2. Click `Choose File`.
3. Browse the file system and select the firmware file.
4. Click `Upload`.
5. The ENS202EXT restarts automatically after the upgrade completes.

4.5.6 Configuring System Time

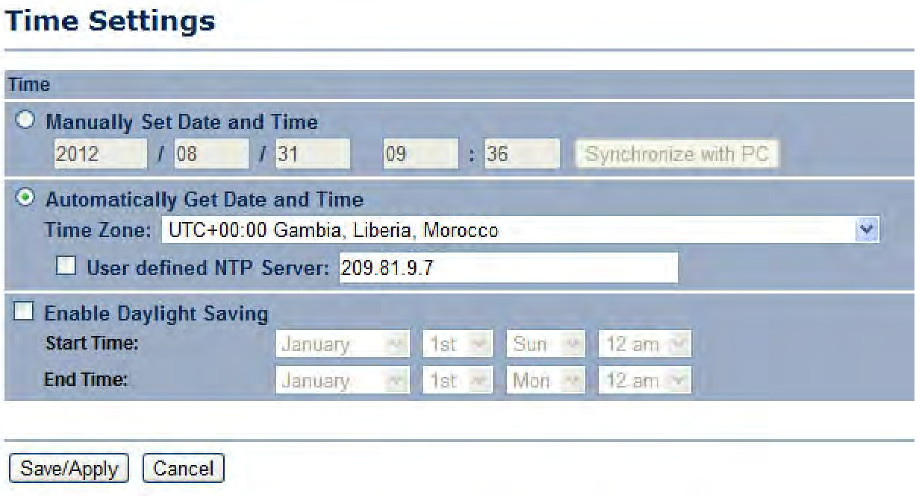
Change the system time of the ENS202EXT by manually entering the information, synchronizing the device with a PC, or setup automatic updates through a network time (NTP) protocol server.

Manually Set Date and Time Enter the date and time values in the date and time fields or click the `Synchronize with PC` button to get the date and time values from the administrator's PC.

Automatically Get Date and Time Select a time zone from the drop-down list and check whether you want to enter the IP address of an NTP server or use the default NTP server.

Enable Daylight Saving Click to enable or disable daylight savings time. Select the start and stop times from the `Start Time` and `Stop Time` dropdown lists.

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.



Time Settings

Time

○ Manually Set Date and Time

2012 / 08 / 31 09 : 36 Synchronize with PC

● Automatically Get Date and Time

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

□ User defined NTP Server: 209.81.9.7

□ Enable Daylight Saving

Start Time: January 1st Sun 12 am

End Time: January 1st Mon 12 am

4.5.7 Configuring Wi-Fi Schedule

Use the Wi-Fi schedule function to control the wireless power ON/OFF service that operates on a routine basis.

Add a Schedule Service

Create a schedule service type and date/time parameters for a specific service.

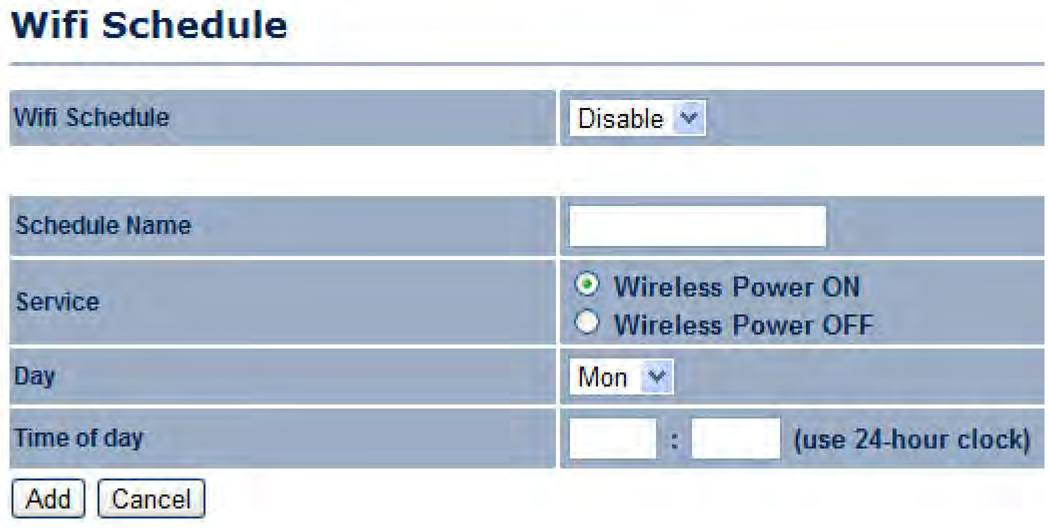
Schedule Name Enter the description of the schedule service.

Service Select the type of schedule service, either `Wireless Power ON` or `Wireless Power OFF`.

Day Select the days of the week to enable the schedule service.

Time of Day Set the start time that the service is active.

Click Add to append the schedule service to the schedule service table, or `Cancel` to discard changes.



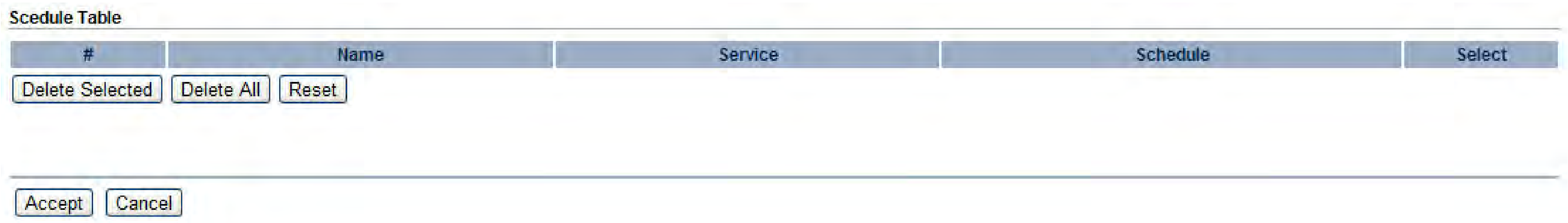
Wifi Schedule

Wifi Schedule	Disable

Schedule Name	
Service	● Wireless Power ON ○ Wireless Power OFF
Day	Mon
Time of day	: (use 24-hour clock)

Schedule Services Table

The Schedule function relies on the GMT time setting acquired from a network time protocol (NTP) server. For details on how to connect the ENS202EXT to an NTP server, see *Configuring System Time*.



Scedule Table

#	Name	Service	Schedule	Select

Schedule Table Displays a list of scheduled services for the ENS202EXT. The properties of each service displayed are:

Displays the ID number of the service in the table.

Name Displays the description of the service.

Service Displays the type of service, either `Wireless Power ON` or `Wireless Power OFF`.

Schedule Displays the schedule information of when the service is active.

Select Select one or more services to edit or delete.

Click `Delete Selected` to delete the selected services or `Delete All` to delete all services.

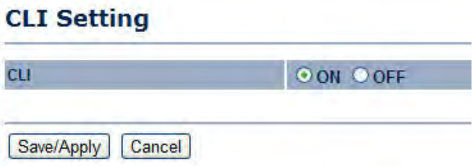
Click `Apply` to save the settings or `Cancel` to discard changes.

4.5.8 Configuring Command Line Interface

Most users will configure the ENS202EXT through the graphical user interface (GUI). However, for those who prefer an alternative method there is the command line interface (CLI). The CLI can be access through a command console, modem or Telnet connection.

CLI Select to enable or disable the ability to modify the ENS202EXT via a command line interface (CLI).

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.



CLI Setting

CLI ● ON ○ OFF

4.5.9 Configuring Logging

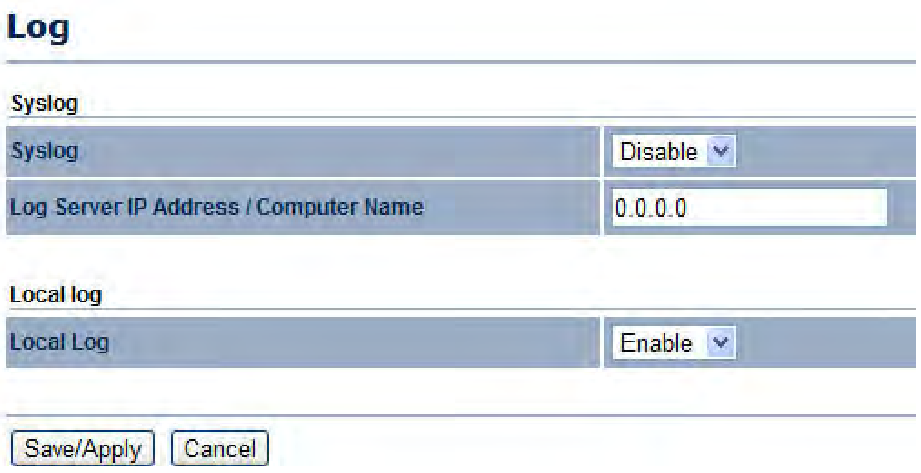
Display a list of events that are triggered on the ENS202EXT Ethernet and wireless interfaces. You can consult this log if an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

Syslog Enable or disable the ENS202EXT syslog function.

Log Server IP Address Enter the IP address of the log server.

Local Log Enable or disable the local log service.

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.



Log

Syslog

Syslog	Disable
Log Server IP Address / Computer Name	0.0.0.0

Local log

Local Log	Enable

4.5.10 Configuring Diagnostics

The diagnosis feature allow the administrator to verify that another device is available on the network and is accepting request packets. If the ping result returns a`live`, it means a device is on line. This feature does not work if the target device is behind a firewall or has security software installed.

Target IP / Domain Name Enter the IP address you would like to search.

Ping Packet Size Enter the packet size of each ping.

Number of Pings Enter the number of times you want to ping.

Start Ping Click `Start Ping` to begin pinging.

Trace route target Enter an IP address or domain name you want to trace.

Start Traceroute Click `Start Traceroute` to begin the traceroute operation.

Target Address Enter the IP address of the target PC.

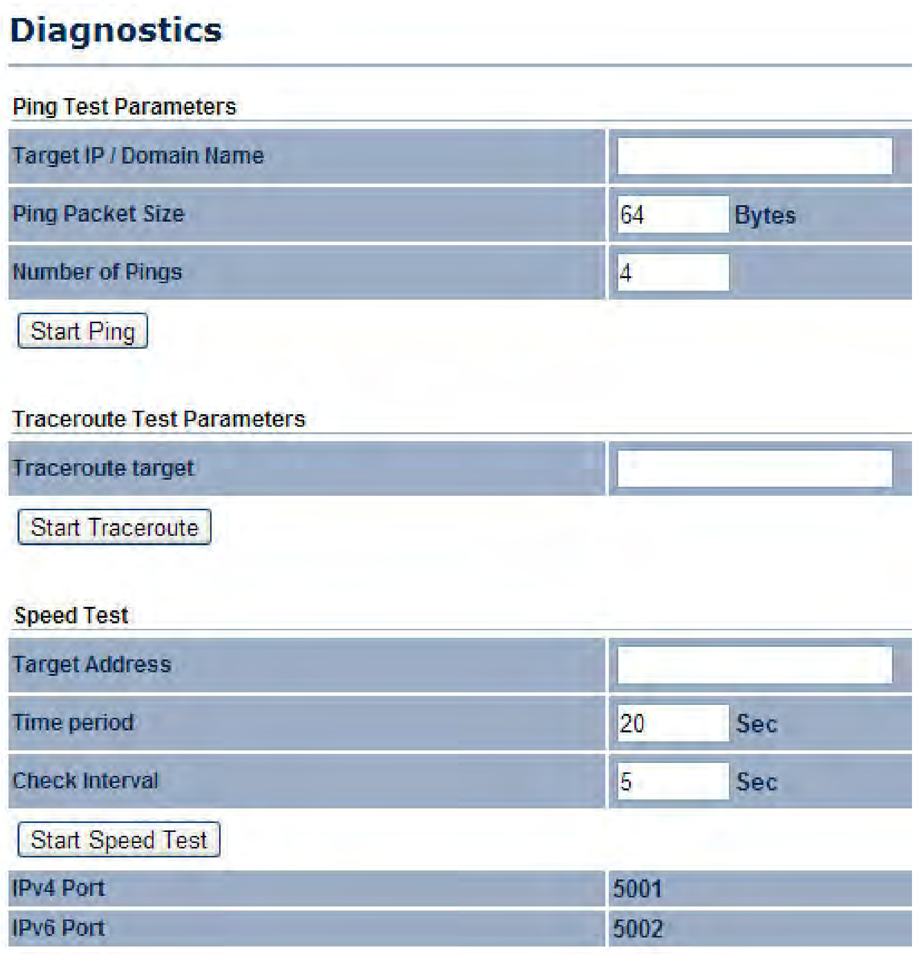
Time period Enter time period for the speed test.

Check Interval Enter the interval for the speed test.

Start Speed Test Click `Start Speed Test` to begin the speed test operation.

IPv4 Port Displays the IPv4 port number of the ENS202EXT.

IPv6 Port Displays the IPv6 port number of the ENS202EXT.



Diagnostics

Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

Start Ping

Traceroute Test Parameters

Traceroute target	

Start Traceroute

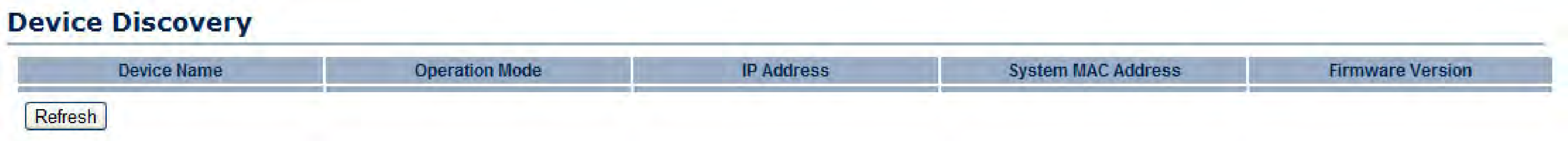
Speed Test

Target Address	
Time period	20 Sec
Check Interval	5 Sec

Start Speed Test

IPv4 Port	5001
IPv6 Port	5002

4.5.11 Viewing Device Discovery



Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

Device Name Displays the name of the devices connected to the network.

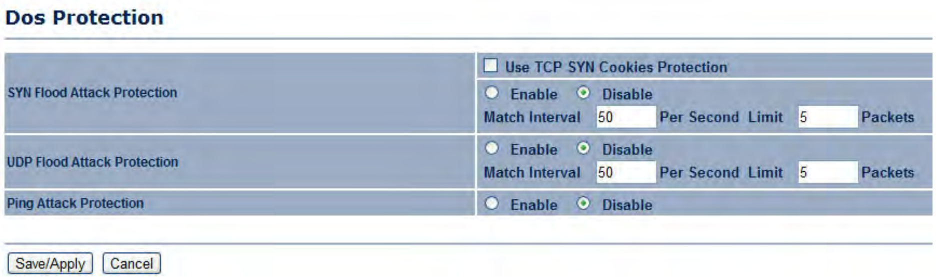
Operation Mode Displays the operation mode of the devices connected to the network.

IP Address Displays the IP address of the devices connected to the network.

System MAC Address Displays the system MAC address of the devices connected to the network.

Firmware Version Displays the firmware version of the devices connected to the network.

4.5.12 Configure Denial of Service Protection



Dos Protection

SYN Flood Attack Protection	□ Use TCP SYN Cookies Protection ○ Enable ● Disable Match Interval 50 Per Second Limit 5 Packets
UDP Flood Attack Protection	○ Enable ● Disable Match Interval 50 Per Second Limit 5 Packets
Ping Attack Protection	○ Enable ● Disable

Use TCP SYN Cookies Protection Click to enable TCP SYN cookies protection.

SYN Flood Attack Protection Click to enable or disable SYN Flood Attack Protection.

Match Interval Per Second Enter the allowed number of packets per second.

Limit Packets Enter the maximum number of packets allowed per request.

UDP Flood Attack Protection Click to enable or disable UDP Flood Attack Protection.

Match Interval Per Second Enter the allowed number of packets per second.

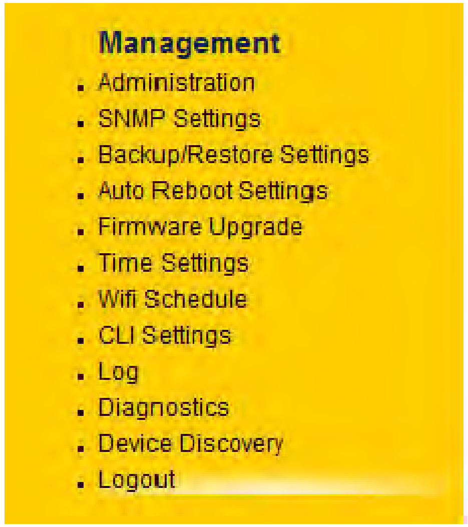
Limit Packets Enter the maximum number of packets allowed per request.

Ping Attack Protection Click to enable or disable ping attack protection.

Click `Save/Apply` to apply the changes or `Cancel` to return previous settings.

4.5.13 Logging Out

Click `Logout` to logout from the ENS202EXT.



Appendix A

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

Important:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with minimum distance 21cm between the radiator & your body.

Appendix B

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Important:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device has been designed to operate with a Dipole antenna have a maximum gain of 5 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (10103A-ENS202 / Model: ENS202, ENS202EXT) has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a ete concu pour fonctionner avec une antenne ayant un gain maximal de Dipole antenne avec dB 5. Une antenne a gain plus eleve est strictement interdite par les reglements d'Industrie Canada. L'impedance d'antenne requise est de 50 ohms.

Conformement a la reglementation d'Industrie Canada, le present emetteur radio peutfonctionner avec une antenne d'un type et d'un gain maximal (ou inferieur) approuve pourl'emetteur par Industrie Canada. Dans le but de reduire les risques de brouillage radioelectriquea l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que lapuissance isotrope rayonnee equivalente (p.i.r.e.) ne depasse pas l'intensite necessaire al'etablissement d'une communication satisfaisante.

Le present emetteur radio (10103A-ENS202 / Model: ENS202, ENS202EXT) a ete approuve par Industrie Canada pour fonctionner avec les types d'antenne enumeres ci-dessous et ayant un gain admissible maximal et l'impedance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est superieur au gain maximal indique, sont strictement interdits pour l'exploitation de l'emetteur.

Appendix C

WorldWide Technical Support

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE	SERVICE INFORMATION	
Canada	CANADA	web site	www.engeniuscanada.com
		email	rma@engeniuscanada.com
		contact numbers	Toll Free: (+1) 888-397-2788 Local: (+1) 905-940-8181
		hours of operation	Monday - Friday 9:00AM to 5:30PM EST (GMT-5)
USA	LOS ANGELES, USA	web site	www.engeniustech.com
		email	support@engeniustech.com
		contact numbers	Toll Free: (+1) 888-735-7888 Local: (+1) 714-432-8668
		hours of operation	Monday - Friday 8:00 AM to 4:30 PM PST (GMT-8)

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Mexico, Central and Southern America	MIAMI, USA	web site	[ES] es.engeniustech.com [PT] pg.engeniustech.com
		email	miamisupport@engeniustech.com
		contact numbers	Miami: (+1) 305-887-7378 Sao Paulo, Brazil: (+55)11-3957-0303 D.F., Mexico:(+52)55-1163-8894
		hours of operation	Monday - Friday 8:00 AM to 5:30PM EST (GMT-5)
Europe	NETHERLANDS	web site	www.engeniusnetworks.eu
		email	support@engeniusnetworks.eu
		contact numbers	(+31) 40-8200-887
		hours of operation	Monday - Friday 9:00 AM - 5:00 PM (GMT+1)
Africa Middle East Russia CIS / Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Ukraine, Uzbekistan Turkey Afghanistan Pakistan Bangladesh, Maldives, Nepal, Bhutan, Sri Lanka	DUBAI, UAE	web site	www.engenius-me.com
		email	support@engenius-me.com
		contact numbers	Toll Free: U.A.E.: 800-EnGenius 800-364-364-87 General: (+971) 4357-5599
		hours of operation	Sunday - Thursday 9:00 AM - 6:00 PM (GMT+4)

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Singapore, Cambodia, Indonesia, Malaysia, Thailand, Philippines, Vietnam China, Hong Kong, Korea India South Africa Oceania	SINGAPORE	web site	www.engeniustech.com.sg/e_warranty_form
		email	techsupport@engeniustech.com.sg
		contact numbers	Toll Free: Singapore: 1800-364-3648
		hours of operation	Monday - Friday 9:00 AM - 6:00 PM (GMT+8)
Others	TAIWAN, R.O.C.	web site	www.engeniusnetworks.com
		email	technology@senao.com

Note:

* Service hours are based on the local time of the service center.

* Please visit the website for the latest information about customer service.