



User Manual

WAP373-C
Version 1.0

IMPORTANT

To install this Access Point
Please refer to the
Quick Installation Guide included in the product packaging

Chapter1

ProductOverview



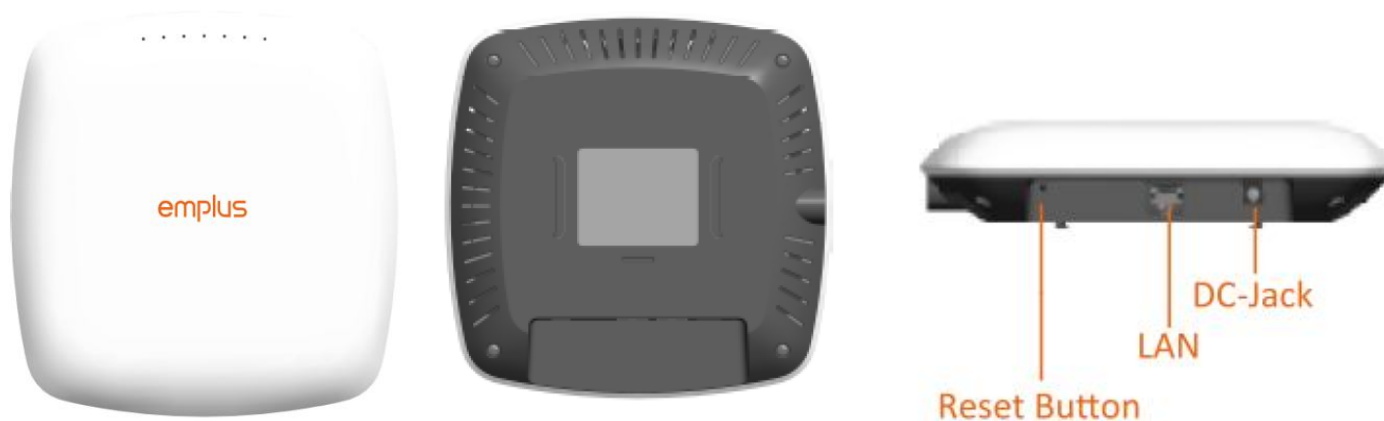
Introduction

Key Features

- Supports IEEE802.11ac/a/b/g/n wireless standards
- Four 2.4 GHz Metal PIFA Antennas
- Four 5 GHz Metal PIFA Antennas
- Support Wave 2 MU-MIMO function
- Support Tx Beamforming to enlarge the transmitting distance.
- IEEE802.11 PoE af Input design with Gigabit port supports.
- Flexible application by the built-in 2nd LAN port.
- More customized items on Band Steering for intelligent Management.
- Secured Guest Network option available

The AP is 802.11 ac wave2/a/b/g/n Access Point with speeds up to 800 Mbps on 2.4GHz and 1,733Mbps on 5GHz band. It can be configured as an Access Point, or WDS (AP, Station). The AP is an affordable solution which is built in high-powered radios and long-range settings to replace the ordinary Access Points that do not have the range and reach to connect to a growing number of wireless users. With Wave2 features, the Access Point could reduce the handling period on client devices and network with more client devices at the same time. Meanwhile, the beamforming will gather energy to a specific direction and increase the transmitting distance.

Physical Interface (WAP373)



Standard	802.11ac/a/b/g/n
Frequency	2.4GHz + 5GHz
Data Rates	800Mbps + 1733Mbps
Antennas	2.4GHz:3.29dBi; 5GHz:5.84dBi
Physical Interface	1 x GE, DC Jack (12V)
Radio Chains/Streams	4 x 4 : 4

Physical & Environment

Power Source	DC Input: 12 VDC/2A PoE: compatible with 802.3af/at 54Vdc/0.6A
Internal High Gain Antenna (Peak Gain)	~3.29dBi 2.4GHz antennas ~5.84dBi 5GHz antennas
Interface	1 x 10/100/1000Mbps Ethernet Port with 802.3af/at PoE 1 x DC power connector 1 x reset button
Dimensions (W x D x H)	200x200x40 mm
Mounting	Ceiling, T-Rail and Wall mount
Environment	Operating temperature: 0°C~50°C Operating humidity: 0%~90% typical
Technical Specifications	Storage temperature: -30°C~80°C

Applications

Wireless LAN (WLAN) products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of WLANs:

- **Difficult-to-Wire Environments:** There are many situations where wires cannot be installed, deployed easily, or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas that make the installation of a Ethernet-based LAN impossible, impractical or expensive are sites where WLAN can be a network solution.
- **Temporary Workgroups:** Create temporary workgroups/networks in more open areas within a building; auditoriums, amphitheaters classrooms, ballrooms, arenas, exhibition centers, or temporary offices where one wants either a permanent or temporary Wireless LAN established.
- **The Ability to Access Real-Time Information:** Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.
- **Frequently Changing Environments:** Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).
- **Small Office and Home Office (SOHO) Networks:** SOHO users require a cost-effective, easy, and quick installation of a small network.
- **Training/Educational Facilities:** Training sites at corporations or students at universities use wireless connectivity to exchange information between peers and easily access information for learning purposes.

EnGenius Technologies

1580 Scenic Ave.

Costa Mesa, CA

92626

Contact Name/Title: Eric Chen / Product Marketing

Contact Information (Email/Tel): eric.chen@engeniustech.com / 714-432-8668

Chapter2

Before YouBegin

Computer Settings

Windows XP/Windows 7/Windows 8/Windows 10

In order to use the Access Point, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

1a. Click the Start button and open the Control Panel



WindowsXP



Windows7

1b. Move your mouse to the lower right hot corner to display the Charms Bar and select the Control Panel in Windows 8 OS.



Windows 8

1c. In Windows 10, click Start to select All APPs to enter the folder of Windows system for selecting Control Panel.



Windows 10

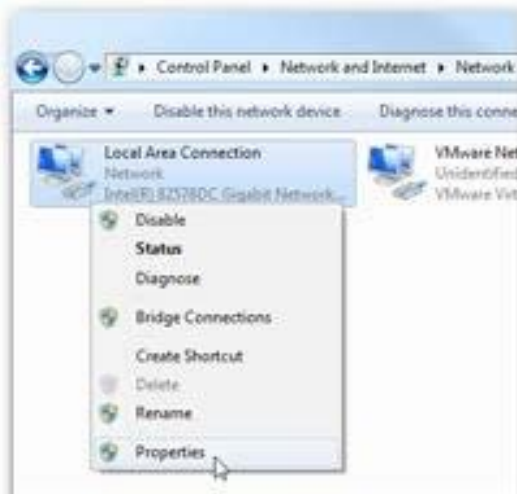
2a. In Windows XP, click Network Connections.



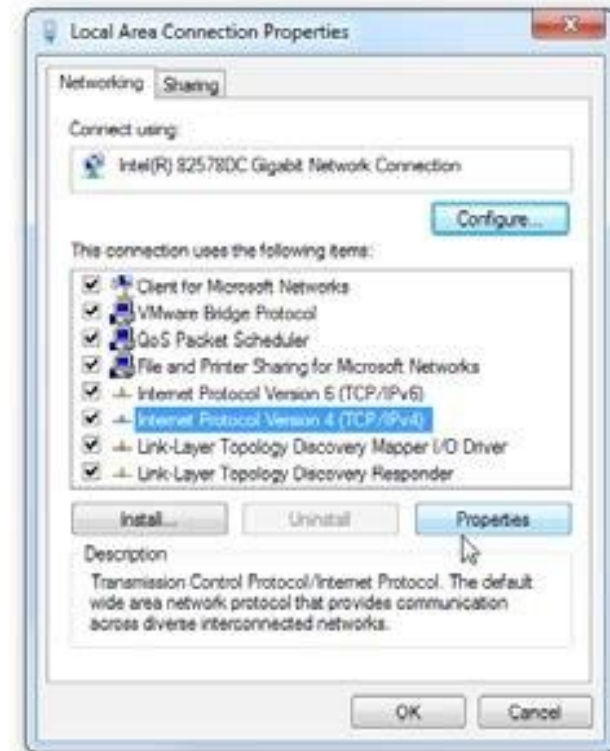
2b. In Windows 7/Windows 8/Windows 10, click View Network Status and Tasks in the Network and Internet section, then select Change adapter settings.



3. Right-click on Local Area Connection and select Properties.



4. Select Internet Protocol Version 4 (TCP/IPv4) and then select Properties.



5. Select Use the following IP address and enter an IP address that is different from the Access Point and Subnet mask, then click OK.

Note: Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: WAP373 IP address: 192.168.1.1

PC IP address: 192.168.1.2–192.168.1.255

PC Subnet mask: 255.255.255.0



Apple Mac OSX

1. GotoSystemPreferences(Whichcanbeopenedinthe ApplicationsfolderorselectingitintheAppleMenu).
2. SelectNetworkintheInternet&Networksection.



3. HighlightEthernet.

4. InConfigureIPv4,selectManually.
5. EnteranIPaddressthatisdifferentfromtheAccess PointandSubnetmaskthenpressOK.

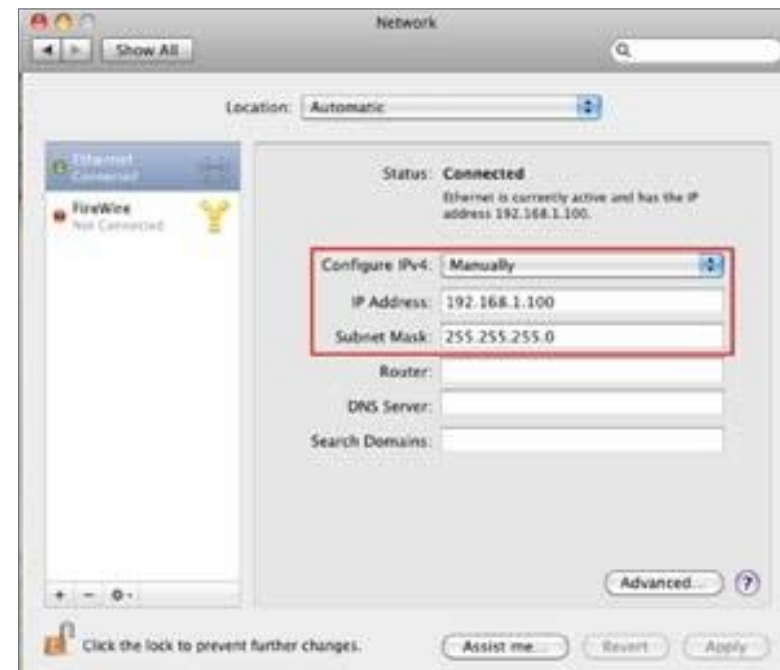
Note: EnsurethattheIPaddressandSubnetmaskare on the same subnet as the device.

For example: A device IP address: 192.168.1.1 PCIPaddress:

192.168.1.2–192.168.1.255

PCSubnetmask:255.255.255.0

6. ClickApplywhendone.



Chapter 3 **Configuring Your Access Point**

Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

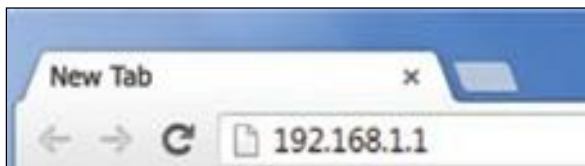
Default Settings

Please use your Ethernet port or wireless network adapter to connect the Access Point.

IP Address	192.168.1.1
Username / Password	none

Web Configuration

1. Open a web browser (Internet Explorer/Firefox/Safari/Chrome) and enter the IP Address <http://192.168.1.1>



Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

2. The default username and password are admin. Once you have entered the correct username and password, click the Login button to open the web-base configuration page.

WAP373

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH. [Go to password configuration...](#)

Authorization Required

Please enter your username and password.

Username

Password

Powered by LuCI WAP373-C branch (git-18.332.37659-aefdc4) / OpenWrt Chaos Calmer 15.05.1 unknown

- * The model name will be varied by different models.
3. If successful, you will be logged in and see the User Menu of this Access Point.

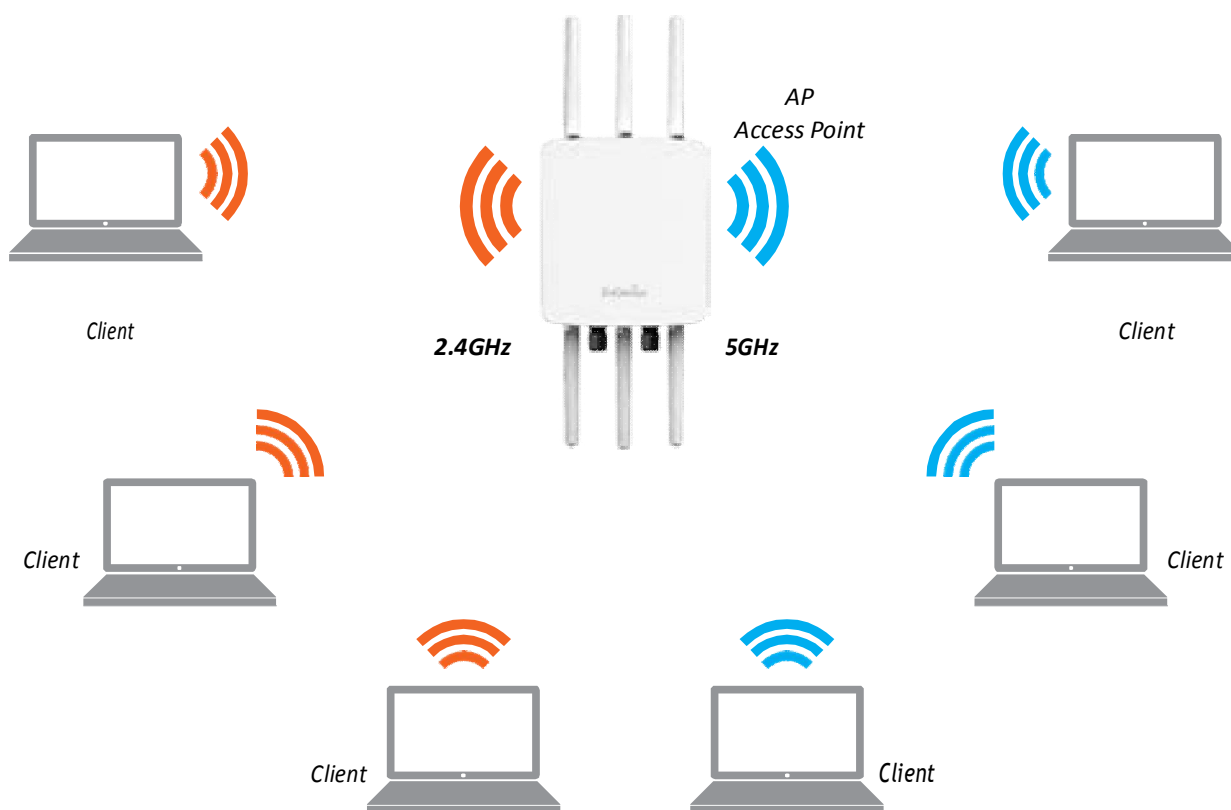
Chapter4

Building aWireless Network

Before starting to configure this Access Point, you may realize the used scenario under varied operating modes. The AP has the ability to operate in various modes. This chapter describes purpose of different operating modes and lists down the operating modes for Access Points or Client Premise Equipments (CPE).

Access Point Mode

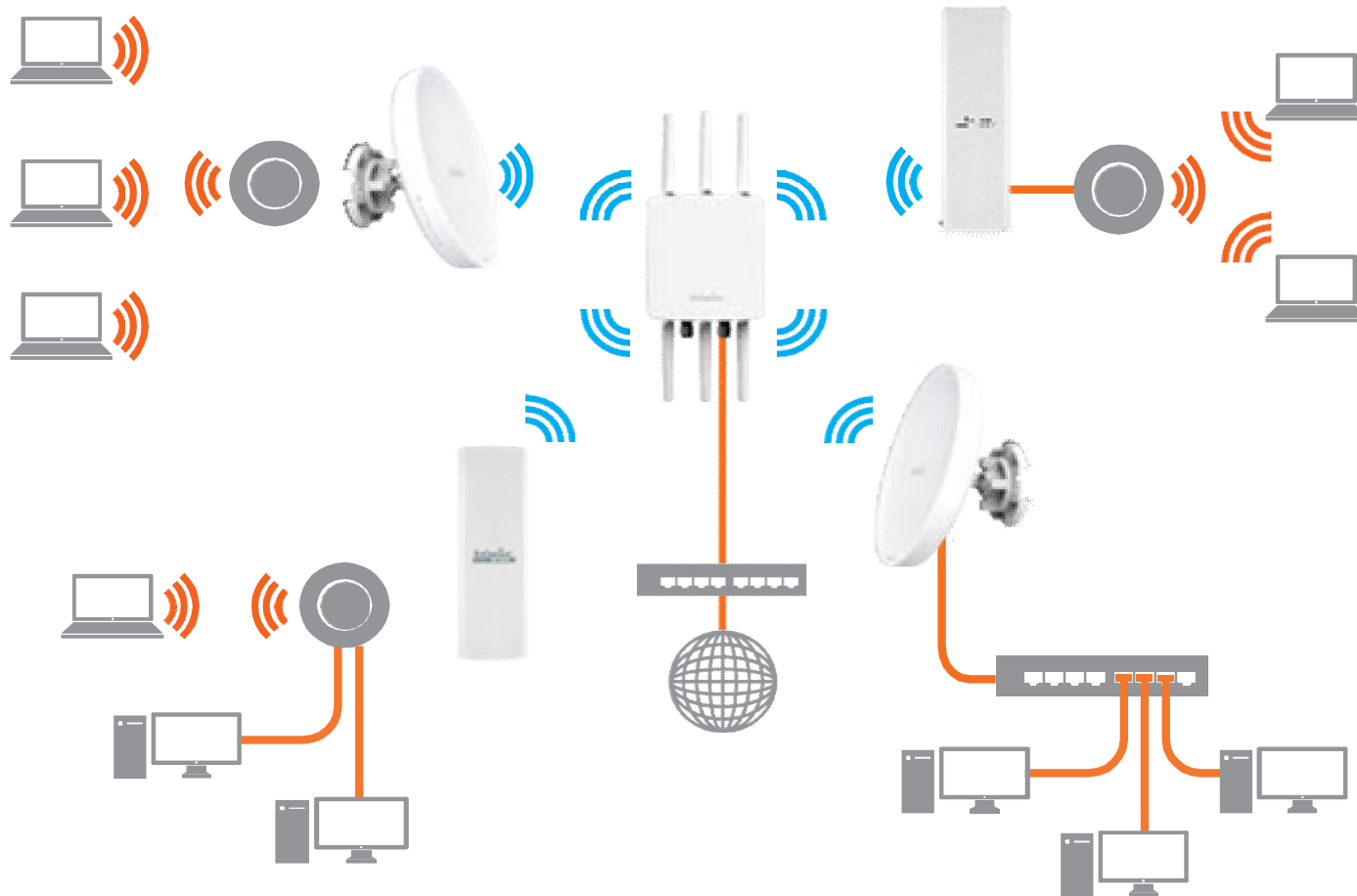
In Access Point Mode, AP behaves like a central connection for stations or clients that support IEEE 802.11ac/a/b/g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the AP. The AP supports up to eight SSIDs per band at the same time for secure access.



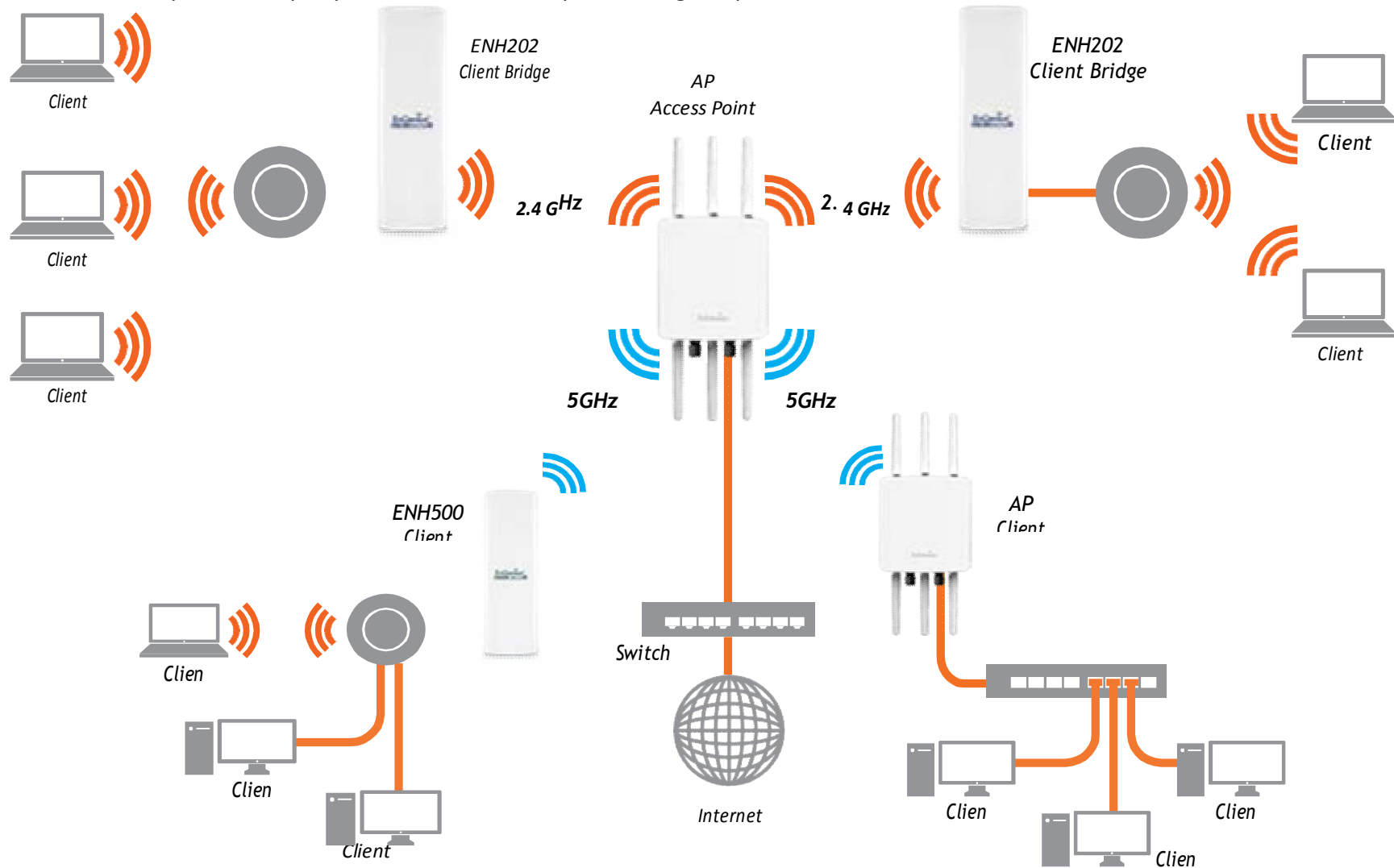
Client Bridge Mode

The Access Point essentially acts as a wireless adapter that connects to an access point to allow a system of wireless access to the network in the Client Bridge mode. Since the computers are on the same subnet, the Access Point can broadcast to each end-device.

If you use the client bridge mode in this Access Point, you can use the AP Detection feature to scan for Access Points within range. When you find an Access Point, configure this Access Point to use the same SSID and Security Password as the Access Point to associate with it.

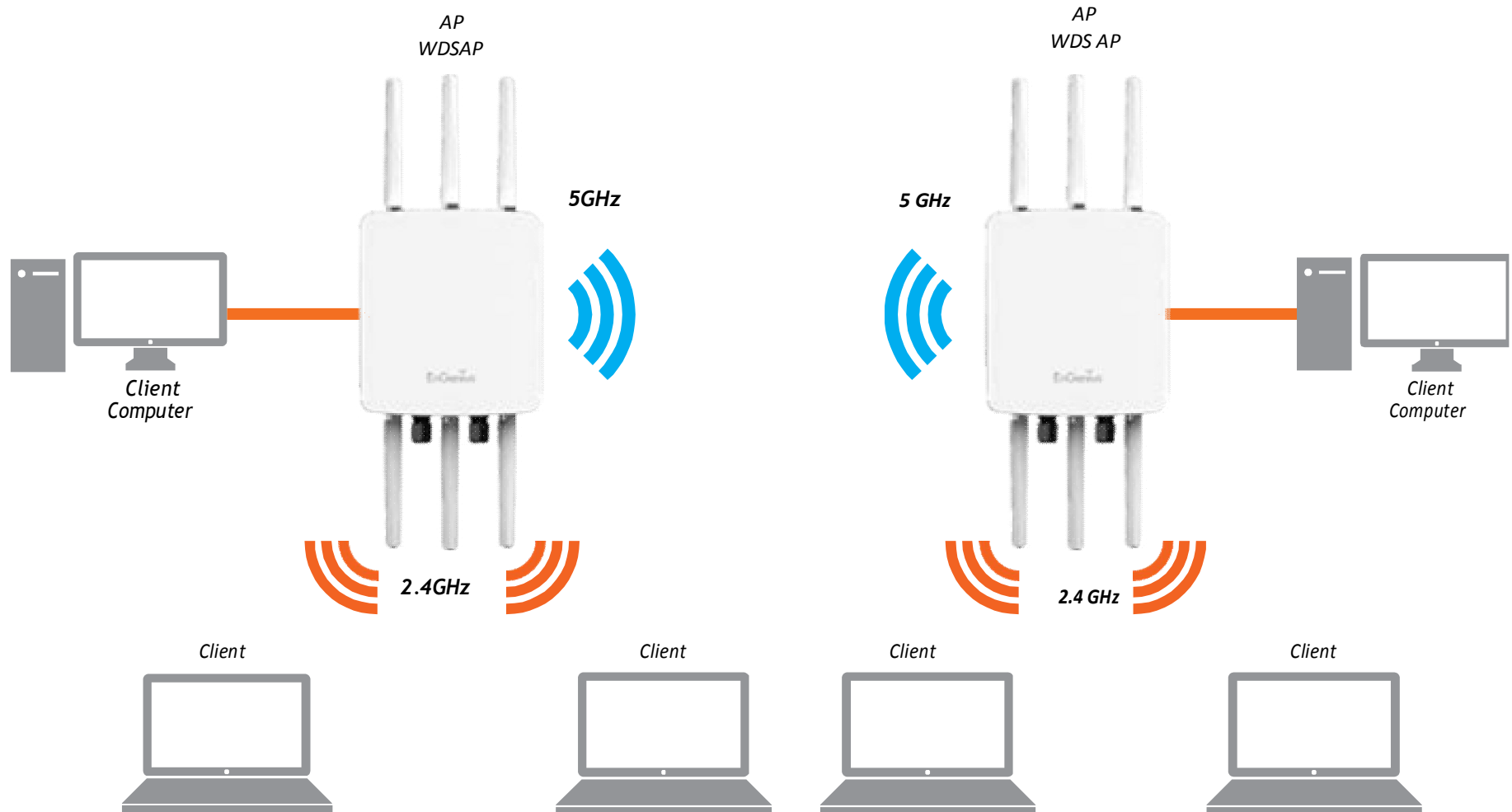


The AP can be used as a centralized Access Point with which other Wireless 802.11b/g/n 2.4 or a/n 5GHz Client Bridges can associate; leveraging the long-range capability of their internal high-gain directional antennas, resulting in a very cost-effective solution to expand a company network over a multiple building campus.



WDS AP Mode

The AP also supports WDS AP mode. This operating mode allows wireless stations to connect with Access Point via using WDS technology. In this mode, configure the MAC address or SSID in both Access Point to enlarge the wireless area by enabling WDS Link settings. WDS AP mode supports up to four (4) AP MAC addresses and four (4) SSIDs at the same time.

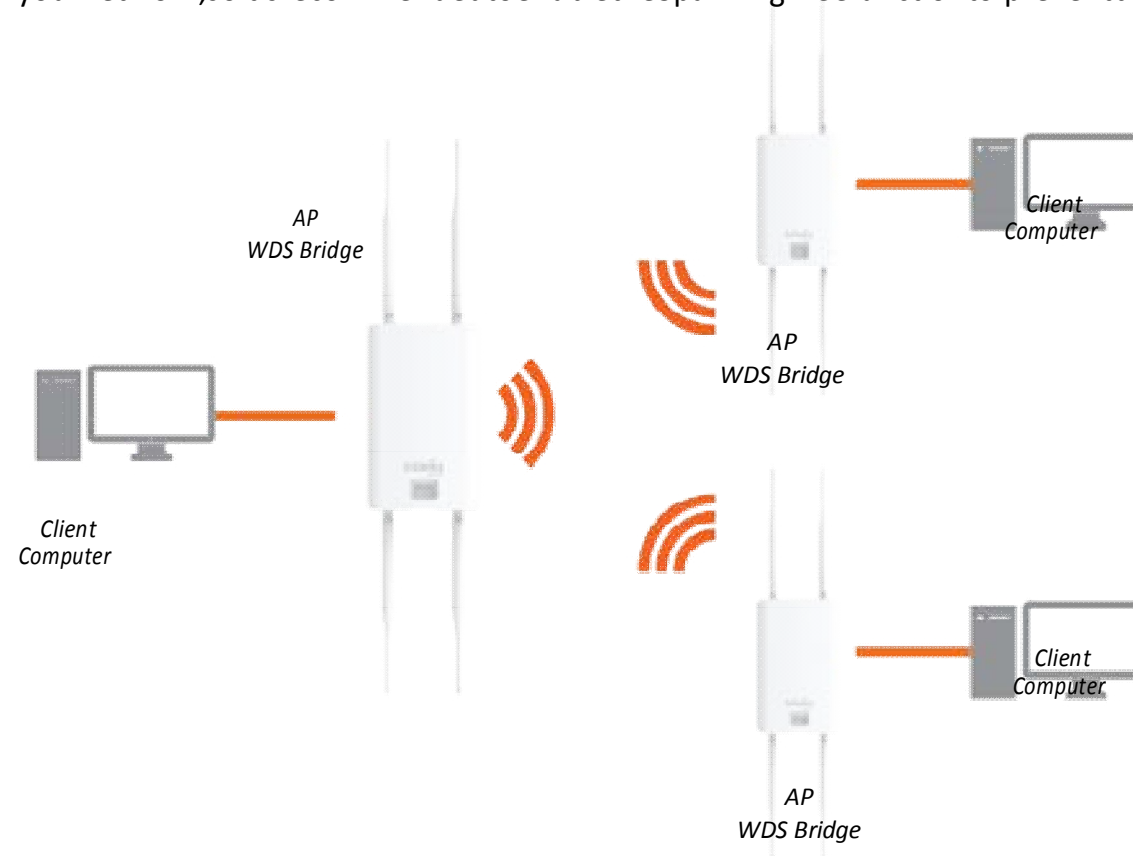


WDS Bridge Mode

In WDS Bridge Mode, the Access Point can wirelessly connect different LANs by configuring the MAC address and security settings of each Access Point. Use this operating mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the Access Point to wirelessly connect two wired LANs, as shown in the following diagram.

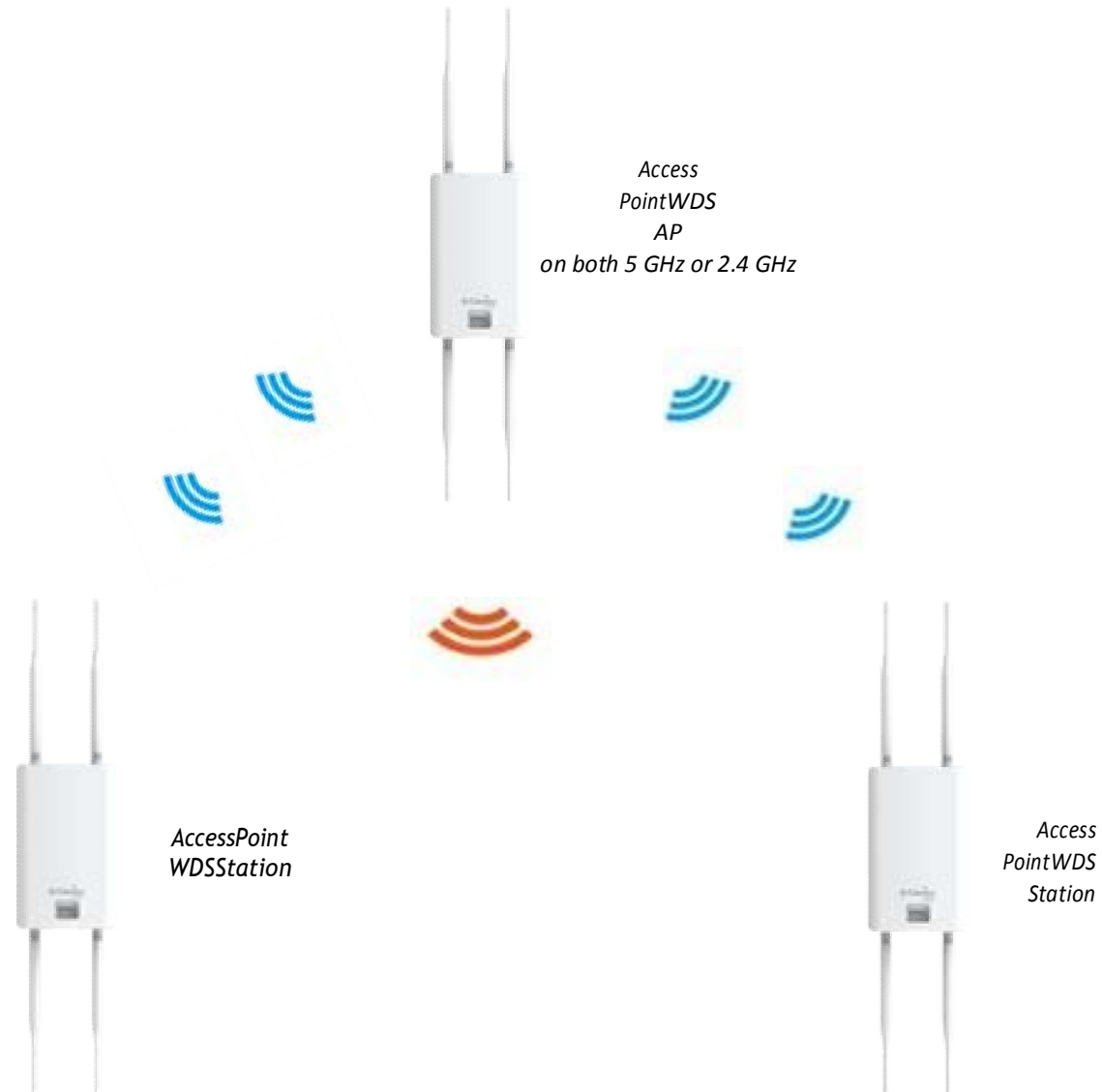
WDS Bridge Mode can establish up to four (4) to eight (8) WDS links, creating a star-like network.

Note: WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. This configuration can be susceptible to generate endless network loops in your network, so it is recommended to enable the Spanning Tree function to prevent this from happening.



WDS Station Mode

WDSstation(WDSSTA)modeexpandstheWDSbyreceivingawirelessignal/serviceandsharingitthroughtheEthernet port. With WDS STA mode,



Chapter5

Status

Overview

SaveChanges

This page lets you save and apply the settings shown under Unsaved changes list, or Revert the unsaved changes and revert to the previous settings that were in effect.

Status

System	
Hostname	WAP373
Model	QCA IPQ8064/AP161
Firmware Version	OpenWrt Chaos Calmer 15.05.1 unknown / LuCI WAP373-C branch (git-18.332.37659-aefdc4)
Kernel Version	3.14.77
Local Time	Thu Dec 6 11:16:57 2018
Uptime	0h 49m 20s
Load Average	0.00, 0.01, 0.05

Device Status

Clicking the Device Status link under the Overview menu shows the status information about the current operating mode.

- The Device Information section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID

Note: VLAN ID is only applicable in Access Point, WDS AP or WDS BR mode.

Network	
IPv4 WAN Status	 Not connected
IPv6 WAN Status	 Not connected
Active Connections	269 / 16384 (1%)

- The Memory Information section shows usage of Memory such as Total Available, Free, Cached, Buffered

Memory	
Total Available	58860 kB / 213872 kB (27%)
Free	50128 kB / 213872 kB (23%)
Buffered	8732 kB / 213872 kB (4%)

- The LAN Information section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, Primary DNS Address, Secondary DNS Address, status of DHCP client, and status of Spanning Tree protocol (STP).

Network

IPv4 WAN Status	 Not connected
IPv6 WAN Status	 Not connected
Active Connections	270 / 16384 (1%)

The Wireless LAN Information 2.4 GHz/5 GHz section shows wireless information such as Operation Mode, Frequency, and Channel. Since this Access Point supports multiple SSIDs, information about each SSID, the ESSID, and security settings, are displayed.

Note: Profile Settings are only applicable in Access Point and WDS AP modes.

Wireless

Generic 802.11ac Wireless Controller (wifi0)	 SSID: WAP373-5G1 100% Mode: Master Channel: 161 (5.805 GHz) Bitrate: 1733.3 Mbit/s BSSID: EC:43:F6:F9:18:09 Encryption: None
Generic 802.11bgn Wireless Controller (wifi1)	 SSID: WAP373-2.4G 100% Mode: Master Channel: 6 (2.437 GHz) Bitrate: 378.4 Mbit/s BSSID: 00:02:6F:12:34:56 Encryption: None
Generic 802.11bg Wireless Controller (wifi2)	 SSID: WAP373-5G2 0% Mode: Master Channel: 40 (0.000 GHz) Bitrate: ? Mbit/s <i>Wireless is disabled or not associated</i>

Connections

2.4 GHz/5 GHz Connection List

Click the connection link under the Overview menu displays the connection list of clients associated to the AP's 2.4 GHz/5 GHz, along with the MAC addresses and signal strength for each client. Clicking Refresh updates the client list.

Note: Only applicable in Access Point and WDS AP modes.

2.4 GHz/5 GHz WDS Link List

Click the connection link under the Overview menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

Note: Only applicable in WDS AP and WDS Bridge modes.

Associated Stations

MAC-Address	Network	Signal	Noise	RX Rate	TX Rate
 00:00:00:00:00:00	Master "WAP373-5G1"	-95 dBm	-95 dBm	0.0 Mbit/s	0.0 Mbit/s
 00:00:00:00:00:00	Master "WAP373-2.4G"	-95 dBm	-95 dBm	0.0 Mbit/s	0.0 Mbit/s

Realtime

Realtime

The Realtime section contains the following options:



CPU Loading: 3 minutes CPU loading percentage information, it displays current loading, average loading and peak loading status. Left bar is loading percentage; button is time tracing. Interval is every 3 seconds

Chapter6

Network

Basic

IPv4/IPv6 Settings

This page allows you to modify the device's IP settings.

[WAN](#) [WAN6](#) [LAN](#)

Interfaces

Interface Overview

Network	Status	Actions
LAN  br-lan	Uptime: 0h 54m 32s MAC-Address: 44:5D:31:CD:78:D6 RX: 470.92 KB (4277 Pkts.) TX: 681.06 KB (2816 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd16:ab22:d369::1/60	   
WAN  wan	Unsupported protocol type. Install protocol extensions...	   
WAN6  wan6	Unsupported protocol type. Install protocol extensions...	   

 Add new interface...

IP Network Settings: Select whether the device IP address will use a static IP address specified in the IP address field or be obtained automatically when the device connects to a DHCP server. **IP Address:** The IP address of this device.

Subnet Mask: The IP Subnet mask of this device.

Gateway: The Default Gateway of this device. Leave it blank if you are unsure of this setting.

Primary/Secondary DNS: The primary/secondary DNS address for this device.

Save: Click Save to confirm the changes.

Chapter7

2.4GHz&5GHz Wireless

Wireless

Wireless Settings

Interface Configuration

General Setup | **Wireless Security** | Advanced Settings

ESSID:

Mode:

Network: ☒ lan:    

☐ wan: (no interfaces attached)

☐ wan6: (no interfaces attached)

☐ create:

Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

Hide ESSID: ☐

DeviceName: Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.

Band Steering (Available on WAP353): Enable Band Steering to send 802.11n clients to the 5GHz band, where 802.11b/g clients cannot go, and leave 802.11b/g clients in 2.4GHz to operate at their slower rates. Before implementing this feature, we suggest you to assure the both 2.4GHz and 5GHz SSID, as well as security settings must be the same. Enable Genius Band Steering supports following advanced settings,

*Force5GHz: When band steering is configured to Force 5GHz mode, the AP will not dual band capable client

Devices on network to the 2.4GHz band only if the client devices are not currently associated on 2.4GHz radio in this AP.

*Prefer5GHz: When band steering is configured to Prefer 5GHz mode, the AP will steer dual band capable client devices to 5GHz radio when the RSSI value of these client devices on 5GHz radio is more than set tone. The allowed RSSI value for default setting is -75dBm.

*BandBalance: When band steering is configured to Band Balance mode, the AP will steer dual band capable client devices to 5GHz when the RSSI value of these client devices on 5GHz radio is more than set tone. To evenly allocate RF resource on the both 2.4GHz and 5GHz radios, users also can set the portion of client devices on 5GHz radio to assure smooth connection. The default value of the 5GHz radio is 75%.

Save: Click Save to confirm the changes.

This page displays the current status of the Wireless settings of this AP.

2.4 GHz/5 GHz Wireless Network

Device Configuration

General Setup

Advanced Settings

Status

100%

Mode: Master | **SSID:** WAP373-2.4G
BSSID: 00:02:6F:12:34:56 | **Encryption:** None
Channel: 6 (2.437 GHz) | **Tx-Power:** 25 dBm
Signal: -97 dBm | **Noise:** -95 dBm
Bitrate: 378.4 Mbit/s | **Country:** 00

Wireless network is enabled

Disable

Operating frequency

Mode

Channel

Width

N

6 (2437 MHz)

40 MHz

Transmit Power

25 dBm (316 mW)

dBm

Device Configuration

General Setup

Advanced Settings

Status

100%

SSID: WAP373-5G1 | **Mode:** Master
Wireless is disabled or not associated

Wireless network is disabled

Enable

Operating frequency

Mode

Channel

Legacy

161 (5805 MHz)

Transmit Power

24 dBm (251 mW)

dBm

OperationMode: Scroll down this list to select operation modes for implementing on this radio. The default operation mode is Access Point on base stations and Access Points and is Client Bridge on Client Premise Equipments (CPE). Meanwhile, EnGenius devices also support WDS modes for peer-to-peer or peer-to-multi-peer connections.

WirelessMode: Scroll down this list to select wireless broadcasting standard on 2.4GHz and 5GHz frequency bands.

ChannelHTMode: Scroll down this list to select bandwidth for operating under a frequency band. The default channel bandwidth is 20 MHz on 2.4 GHz frequency radio and 40 MHz on 5 GHz frequency radio. Considering the different applications, users can decide to implement a channel bandwidth to fulfill real applications. The larger the channel, the greater the transmission quality and speed.

Transmit Power (Tx Power): Default Tx power is Auto to obey regulatory power of each country.

Channel: Click Configuration button to open a new window to configure channels for performing wireless service.

*Default configuration: Default setting of channel selection is "All" to perform auto channel on the exist channel list.

*None: Click "None" to disable the setting on this radio. This radio is disabled.

*Group Configuration: Click specific groups of channels for performing auto channel function. For example, users can click U-NII-1 and U-NII-3 to perform auto channel on these bands; the mechanism of this AP will select the relatively optimal channel to perform wireless service.

Data Rate: Select a data rate from the drop-down list. The data rate affects throughput of data in the AP. Select the best balance for you and your network but not that the lower the data rate, the lower the throughput, though transmission distance is also lowered.

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

Client Limits: Limits the total number of clients on this radio. Once setting the ceiling of client numbers, the maximum

Associated client devices will be restricted at this number.

Aggregation: Integrate multiple data packets into one packet to deliver to client devices. This option reduces the number of packets, but also increases packet sizes.

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

Distance: Specifies the distance between Access Points and client devices. The proper setting for this parameter may assist Access Points to avoid the improper operation when transmitting data under a field application.

Save: Click Save to confirm the changes or Cancel to cancel and return to previous settings.

2.4 GHz/5 GHz SSID Profile

Interface Configuration

[General Setup](#) [Wireless Security](#) [Advanced Settings](#)

ESSID

WAP373-5G1

Mode

Access Point

Network

☒ lan:    

☐ wan: (no interfaces attached)

☐ wan6: (no interfaces attached)

☐ create:

 Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID

☐

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

Interface Configuration

[General Setup](#) [Wireless Security](#) [Advanced Settings](#)

ESSID

WAP373-2.4G

Mode

Access Point

Network

☒ lan:    

☐ wan: (no interfaces attached)

☐ wan6: (no interfaces attached)

☐ create:

 Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID

☐

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

(eight (8) per band). If multiple 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 SSID.

Current Profile: You can configure up to sixteen (16) different SSIDs

Enable: Click this checkbox to enable this SSID interface.

The default SSIDs are enable on the both first 2.4GHz and 5GHz SSID.

SSID: Specifies the SSID for the current profile.

Hidden SSID: Check this option to hide the SSID from clients.

If checked, the SSID will not appear in the site survey.

Client Isolation: Click the appropriate radio button to enable this function for allowing or preventing communication between client devices.

VID: Specifies the VLAN tag for each profile. If your network includes VLANs, you can specify a VLAN ID for packets pass through the Access Point with a tag.

Wireless Security: See the Wireless Security section.

VLAN Isolation: Restrict clients communicating with different VIDs by selecting the radio button.

L2 Isolation: Enable this function prevent client devices to communicate on the both WLAN and LAN.

Save: Click Save to accept the changes.

Wireless Security

The Wireless Security section lets you configure the AP's security modes

Security Mode: Including WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you use WPA2-PSK mode.

* Setting of WEP mode:

Auth Type: Select Open System or Shared Key.

Input Type:

ASCII: Regular Text (recommended)

Hexadecimal Numbers (For advanced users)

Key Length: Select the desired option and ensure that wireless clients use the same setting. Your choices are 64, 128, and 152-bit password lengths.

Default Key: Select the Key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key.

Encryption Key Number: Enter the Key Value or values you wish to use. Only the Key selected as Default is required. The others are optional.

Encryption

No Encryption
WEP Open System
WEP Shared Key
WPA-PSK
WPA2-PSK
WPA-PSK/WPA2-PSK Mixed Mode

*Setting of WPA-PSK, WPA2-PSK and WPA-PSK Mixed (Pre-Shared Key):

Encryption: You may select AES, TKIP or Both (TKIP+AES) to be the encryption type you would like. Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

Group Key Update Interval: Specifies how often, in seconds, the Group Key changes. The default value is 3600.

* Setting of WPA-Enterprise & WPA2-Enterprise (Pre-Shared Key):

Encryption: Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the port number used for connections to the Radius server.

RadiusSecret:Enterthesecretrequiredtoconnecttothe Radiusserver.

Radius Accounting: Enable or disable accounting feature.

Radius Accounting Server: Enter the IP address of the Radius accountingserver.

RadiusAccountingPortEntertheportnumberusedfor connectionstotheRadiusaccountingserver.

RadiusAccountingSecret:Enterthesecretrequiredto connect to the Radius accounting server.

InterimAccountingInterval:Specifieshowoften,in seconds, the accounting data sends.

Note: 802.11n does not allow WEP/WPA-PSK TKIP/ WPA2-PSK TKIP security mode. The connectionmode willautomaticallychange from802.11nto802.11g.

Wireless MAC Filtering

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access this AP. The default setting is: Disable Wireless MAC Filter.

Note: Only applicable in Access Point and WDS AP modes.

ACL Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Your choices are: Disabled, Deny MAC in the list, or Allow MAC in the list.

MAC Address: Enter the MAC address of the wireless client.

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

Delete: Delete the selected entries.

Save: Click Save to apply the changes.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator to install and connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note: All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four Access Points.

Note: Only applicable in WDS AP and WDS Bridge modes.

2.4 GHz/5 GHz WDS Link Settings

Interface Configuration

General Setup **Wireless Security** Advanced Settings

ESSID: WAP373-2.4G

Mode: Access Point (WDS)

Network: ☒ lan:    

☐ wan: (no interfaces attached)

☐ wan6: (no interfaces attached)

☐ create:

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID: ☐

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

Security: Select None or AES from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use.

Other Access Points: must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

Mode: Select to disable or enable from the drop-down list.

Save: Click Save to confirm the changes.

Account

This page allows you to change the AP username and password. By default, the username is: admin and the password is: admin. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.

Account Settings

Router Password

Changes the administrator password for accessing the device

Password		
Confirmation		

Administrator Username: Enter a new username for logging into the new Name entry box.

Current Password: Enter the old password for logging in to the Old Password entry box.

New Password: Enter the new password for logging into the New Password entry box.

Verify Password: Re-enter the new password in the Confirm Password entry box for confirmation.

Apply: Click Apply to apply the changes.

Firmware

Firmware Upgrade

This page allows you to upgrade the firmware of the AP.

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ☒

Image: 瀏覽...

To Perform the Firmware Upgrade:

1. Click the Choose File button and navigate to the OS file system to the location of the upgrade file.
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the Upload button to commence the firmware upgrade.

Note: The device is unavailable during the Firmware upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

Backup/Restore

This page allows you to save the current device configurations. When you save your configurations, you also can reload the saved configurations into the device through the Restore Saved Settings from a file section. If extreme problems occur, or if you have set the AP incorrectly, you can use the Reset button in the Revert to Factory Default Settings section to restore all the configurations of the AP to the original default settings.

Backup Setting: Click Export to save the current configured settings.

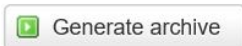
Restore New Setting: To restore settings that have been previously backed up, click Browse, select the file, and click Restore.

Restore to Default: Click Reset button to restore the AP to its factory default settings.

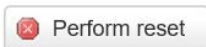
Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:



Reset to defaults:



To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:



User Setting

The function allows you to backup the current device configurations into the AP as the default value. If extreme problems occur, or if you have set the AP incorrectly, you can push the Reset button to revert all the configurations of the AP to the user default.

Back Up Setting as Default: Click Backup to backup the user settings you would like to the device's memory for the default settings.

Restore to User Default: Click Restore to restore user settings to the factory standard settings.

Note 1: After setting the current settings as the default, you should click the Restore to Default on the web interface for reverting the settings into the factory default instead of pushing the reset button.

Note 2: Please write down your account and password before saving. The user settings will now become the new default settings at the next successful login.

Log

System Log

The AP automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the Log link under the System Manager menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

System Log

```
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.019525] siwfreq
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.020598] Set freq vap 0 stop send + c6660000
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.025194] Set freq vap 0 stop send -c6660000
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.056918] Set wait done -c6660000
Thu Dec 6 10:28:21 2018 user.emerg syslog: Interface doesn't accept private locl...
Thu Dec 6 10:28:21 2018 user.emerg syslog: statfd (8BE0): Invalid argument
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.100920]
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.100920] DES SSID SET=
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.106747] [DEBUG] vap-0(ath0):set SIOC80211NWID, 10 characters
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.112007]
Thu Dec 6 10:28:21 2018 kern.warn kernel: [ 43.112007] DES SSID SET=WAP373-5G1
Thu Dec 6 10:28:21 2018 user.emerg syslog: sh: 0: unknown operand
Thu Dec 6 10:28:21 2018 user.emerg syslog: sh: 0: unknown operand
```

Logout

Logout: Click Logout in Management menu to logout.

Authorization Required

Please enter your username and password.

Username

Password

Reset

In some circumstances, it may be required to force the device to reboot. Click on Reset to reboot the AP.

Once you click reset button, you will see the options for reboot or restore this AP.

Reboot the device: Click it to reboot this device.

Restore to Factory Default: Click it to reset this device to factory default setting.

Restore to User Default: Click it to reset this device to user default settings. For realizing the setting method,

Appendix A - FCC Interference Statement

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.



FCC Caution:

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.

IMPORTANT NOTE:

Radiation Exposure Statement

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

Appendix B - IC Interference Statement

Industry Canada Statement

This device complies with Canada license-exempt RSSs 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 RSS Canada sans licence 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.

Caution:



- (i) the device for operation in the band 5150-5250 MHz is only for use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:



- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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 21cm 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 21cm de distance entre la source de rayonnement et votre corps.

Industry Canada Warning

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications. Ce produit répond aux spécifications techniques applicables à l'innovation, Science et Développement économique Canada.

Appendix C - CE Interference Statement

Europe – EU Declaration of Conformity

- EN60950-1

Safety of Information Technology Equipment

- EN50385

Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

- EN 300 328

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- EN 301 893

Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

- EN 301 489-1

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-17

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

The frequency and the maximum transmitted power in EU are listed below:

2412-2472MHz: 17dBm

5150-5250 & 5725-5850MHz: 18dBm

CE 0560

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type o</i>

	<i>f equipment / iekārtas tips</i>] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadcza, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyypinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.