




IFS WMC251-1W-1T-300 User Manual

Copyright	© 2015 United Technologies Corporation Interlogix is part of UTC Building & Industrial Systems, Inc. a unit of United Technologies Corporation. All rights reserved.
Trademarks and patents	The WMC251-1W-1T-300 name and logo are trademarks of United Technologies. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	UTC Fire and Security 3211 Progress Drive, Lincolnton, NC 28092 USA Authorized EU manufacturing representative: UTC Climate Controls & Security B.V., Kelvinstraat 7, 6003 DH Weert, Netherlands
Intended use	Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.Interlogix.com .
Certification	  N4131
ACMA compliance	Notice! This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
European Union directives	2004/108/EC (EMC Directive): Hereby, UTC Building & Industrial Systems, Inc. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense. Any changes or modifications not expressly approved by UTC could void the user's authority to operate this equipment under the rules and regulations of the FCC.

FCC Caution:

To assure continued compliance, (for example, use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the 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
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CAUTION: Changes or modifications not expressly approved by UTC for compliance could void the user's authority to operate the equipment.



This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the DC-plug to disconnect the device from the power circuit. Without removing the DC-plug, the device still consumes power from the power circuit. In view of Saving the Energy, it is strongly suggested to remove the DC-plug for the device if this device is not intended to be active.

Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 247 and RSS 102 of Industry Canada.

This Class B digital device complies with Canadian ICES-003 (NMB-003).

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

- (1) This device may not cause interference; and*
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.*

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et*
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

WMC251-1W-1T-300 complies with IC requirements, IC: 20201-WMC251300.

This radio transmitter (IC: 20201-WMC251300) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

- Built-in 14dBi Dual-Polarization Antenna

Le présent émetteur radio (IC: 20201-WMC251300) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

- **Intégré 14dBi antenne double polarisation**

Digital Transmission Systems (DTSs)

DTSs include systems that employ digital modulation techniques resulting in spectral characteristics similar to direct sequence systems. The following applies to the bands 902-928 MHz and 2400-2483.5 MHz.

(1) The minimum 6 dB bandwidth shall be 500 kHz.

(2) The transmitter power spectral density conducted from the transmitter to the antenna shall not be greater than 8 dBm in any 3 kHz band during any time interval of continuous transmission. This power spectral density shall be determined in accordance with the provisions of Section 5.4(4), (i.e. the power spectral density shall be determined using the same method as is used to determine the conducted output power).

For DTSs employing digital modulation techniques operating in the bands 902-928 MHz and 2400-2483.5 MHz, the maximum peak conducted output power shall not exceed 1W. Except as provided in Section 5.4(5), the e.i.r.p. shall not exceed 4 W.

As an alternative to a peak power measurement, compliance can be based on a measurement of the maximum conducted output power. The maximum conducted output power is the total transmit power delivered to all antennas and antenna elements, averaged across all symbols in the signalling alphabet when the transmitter is operating at its maximum power control level. Power must be summed across all antennas and antenna elements. The average must not include any time intervals during which the transmitter is off or transmitting at a reduced power level. If multiple modes of operation are implemented, the maximum conducted output power is the highest total transmit power occurring in any mode.

(5) Fixed point-to-point systems in the bands 2400-2483.5 MHz and 5725-5850 MHz are permitted to have an e.i.r.p. higher than 4 W provided that the higher e.i.r.p. is achieved by employing higher gain directional antennas and not higher transmitter output powers. Point-to-multipoint systems,² omnidirectional applications and multiple co-located transmitters transmitting the same information are prohibited from exceeding an e.i.r.p. of 4 W.

(6) Transmitters may operate in the band 2400-2483.5 MHz, employing antenna systems that emit multiple directional beams simultaneously or sequentially, for the purpose of directing signals to individual receivers or to groups of receivers, provided that the emissions comply with the following:

(i) Different information must be transmitted to each receiver.

(ii) If the transmitter employs an antenna system that emits multiple directional beams, but does not emit multiple directional beams simultaneously, the total output power conducted to the array or arrays that comprise the device (i.e. the sum of the power supplied to all antennas, antenna elements, staves, etc., and summed across all carriers or frequency channels) shall not exceed the applicable output power limit specified in sections 5.4(2) and 5.4(4). However, the total conducted output power shall be reduced by 1 dB below the specified limits for each 3 dB that the directional gain of the antenna/antenna array exceeds 6 dBi. The directional antenna gain shall be computed as the sum of $10 \log$ (number of array elements or staves) plus the directional gain of the element or stove having the highest gain.

(iii) If a transmitter employs an antenna that operates simultaneously on multiple directional beams using the same or different frequency channels, the power supplied to each emission beam is subject to the applicable power limit specified in sections 5.4(2) and 5.4(4). If transmitted beams overlap, the power shall be reduced to ensure that their aggregate power does not exceed the applicable limit specified in sections 5.4(2) and 5.4(4). In addition, the aggregate power transmitted simultaneously on all beams shall not exceed the applicable limit specified in sections 5.4(2) and 5.4(4) by more than 8 dB.

(iv) Transmitters that transmit a single directional beam shall operate under the provisions of sections 5.4(2), 5.4(4) and 5.4(5).

5.5 Unwanted Emissions

In any 100 kHz bandwidth outside the frequency band in which the spread spectrum or digitally modulated device is operating, the RF power that is produced shall be at least 20 dB below that in the 100 kHz bandwidth within the band that contains the highest level of the desired power, based on either an RF conducted or a radiated measurement, provided that the transmitter demonstrates compliance with the peak conducted power limits. If the transmitter complies with the conducted power limits based on the use of root-mean-square averaging over a time interval, as permitted under Section 5.4(4), the attenuation required shall be 30 dB instead of 20 dB. Attenuation below the general field strength limits specified in RSS-Gen is not required.

The measurement procedure defined in [Annex A](#) of RSS-247 shall be used to verify the compliance to the e.i.r.p. at different elevations.

No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from UTC Fire and Security.

UTC, reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of UTC to provide notification of such revision or change. UTC provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. UTC may make improvements or

changes in the product(s) described in this manual at any time.

CAUTION: TO ENSURE REGULATORY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Wireless LAN and your Health

The WMC251-1W-1T-300 like other radio devices, emits radio frequency electromagnetic energy, but operates within the guidelines found in radio frequency safety standards and recommendations.

Restrictions on Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, these situations may include:

Using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guideline documentation that comes with the product.

Postpone router installation until there is no risk of thunderstorm or lightning activity in the area.

Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.

Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.

Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.

Place this equipment on a stable surface.

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- . Read all of the instructions {listed here and/or in the user manual} before you operate this equipment.

Give particular attention to all safety precautions.

Retain the instructions for future reference.

- . Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.

- . Comply with all instructions that accompany this equipment.

- . Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges. We also recommend the use of ESP300 20Kv protection on the input at the switch or network.

- . Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.

- . Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges.

Different types of cord sets may be used for connections to the main supply circuit. Use only a main line cord that complies with all applicable product safety requirements of the country of use. Installation of this product must be in accordance with national wiring codes.

Place unit to allow for easy access when disconnecting the power cord/adaptor of the device from the AC wall outlet.

Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

This product was qualified under test conditions that included the use of the supplied cables between system components. To be in compliance with regulations, the user must use these cables and install them properly. Connect the unit to a grounding type AC wall outlet using the power adapter supplied with the unit.

Do not cover the device, or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

Installation must at all times conform to local regulations.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reasons/remarks
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use; limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Reframing of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

WEEE regulation



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Contact Information For contact information, see www.-.com or www.utcssecurityproducts.eu.

User's Manual**CONTENTS**

Chapter 1.Product Introduction	14
1.1 Package Contents	14
1.2 Product Description	15
1.3 Product Features	16
1.4 Product Specification	17
Chapter 2.Hardware Installation	19
2.1 Hardware Description	19
2.1.1 The Bottom Panel – Port	20
Chapter 3.Connecting to the AP	23
3.1 Preparation before Installation	23
3.1.1 Professional Installation Required	23
3.1.2 Safety Precautions.....	23
3.2 Installation Precautions	23
3.3 Installing the AP	25
Chapter 4.Quick Installation Guide	27
4.1 Manual Network Setup - TCP/IP Configuration	27
4.1.1 Configuring the IP Address Manually	27
4.2 Starting Setup in the Web UI	30
Chapter 5.Configuring the AP	33
5.1 Operation Mode	33
5.1.1 Access Point	33
5.1.2 Client.....	35
5.1.3 WDS AP	36
5.1.4 WDS Client	37
5.1.5 AP Router	37
5.1.6 Wireless ISP	38
5.1.7 Security Setting.....	38
5.1.8 Advanced Settings	43
5.1.9 Access Control.....	46
5.1.10 WAN Port Settings	46
5.1.11 Dynamic DNS Settings	48
5.1.12 Remote Management	52
5.1.13 DHCP Server Settings	52
5.1.14 DMZ Settings	53
5.1.15 Virtual Server Settings	54
5.1.16 IP Filtering Settings.....	54
5.1.17 Port Filtering Settings	55
5.1.18 MAC Filtering Settings.....	55

5.1.19	Bandwidth Control	56
5.1.20	SNMP.....	57
5.2	System Configuration.....	58
5.2.1	Default IP Settings	58
5.2.2	Time Settings	59
5.2.3	Password Settings	59
5.2.4	System Management.....	60
5.2.5	Ping Watchdog.....	61
5.2.6	Firmware Upgrade	62
5.2.7	Configuration Save and Restore	62
5.2.8	Factory Default	63
5.2.9	Reboot System	63
5.2.10	Schedule Reboot	63
5.3	Tools.....	65
5.3.1	Network Ping	65
5.3.2	Network Traceroute	66
5.4	Device Status.....	67
5.4.1	Device Information.....	68
5.4.2	Wireless Information	69
5.4.3	LAN Information.....	69
5.4.4	Wireless Client Table	70
5.4.5	System Log.....	71
5.5	Logout	72
Appendix A: Troubleshooting.....		73
Appendix B: FAQ.....		75
Q1: How to set up the AP Client Connection.....		75
Q2: How to set up the WDS Connection		83

FIGURES

FIGURE 2-1 THREE-WAY VIEW	19
FIGURE 2-2 LED	20
FIGURE 2-3 BOTTOM PANEL	21
FIGURE 2-4 POE INJECTOR.....	21
FIGURE 3-1 CONNECT THE ANTENNA.....	25
FIGURE 3-2 CONNECT THE ETHERNET CABLE.....	25
FIGURE 3-3 CONNECT THE POE INJECTOR.....	26
FIGURE 3-4 POLE MOUNTING.....	26
FIGURE 4-1 TCP/IP SETTING.....	28
FIGURE 4-2 WINDOWS START MENU	29
FIGURE 4-3 SUCCESSFUL RESULT OF PING COMMAND	29
FIGURE 4-4 FAILED RESULT OF PING COMMAND.....	30
FIGURE 4-5 LOGIN BY DEFAULT IP ADDRESS.....	30
FIGURE 4-6 LOGIN WINDOW.....	31
FIGURE 4-7 WMC251 WEB UI SCREENSHOT	31
FIGURE 4-8 CHOOSE OPERATION MODE	32
FIGURE 4-9 CONFIGURE WIRELESS SETTINGS	32
FIGURE 5-1 MAIN MENU	33
FIGURE 5-2 OPERATION MODE.....	33
FIGURE 5-3 BASIC SETTINGS - AP.....	34
FIGURE 5-4 BASIC SETTINGS - CLIENT.....	35
FIGURE 5-5 BASIC SETTINGS – WDS AP	36
FIGURE 5-6 BASIC SETTINGS – WDS CLIENT.....	37
FIGURE 5-7 BASIC SETTINGS – AP ROUTER	37
FIGURE 5-8 BASIC SETTINGS – WISP	38
FIGURE 5-9 SECURITY SETTINGS	38
FIGURE 5-10 SECURITY SETTINGS – WEP	39
FIGURE 5-11 SECURITY SETTINGS – WPA PERSONAL.....	40
FIGURE 5-12 SECURITY SETTINGS – WPA ENTERPRISE	40
FIGURE 5-13 SECURITY SETTINGS – WPA2 PERSONAL.....	41
FIGURE 5-14 SECURITY SETTINGS – WPA2 ENTERPRISE.....	41
FIGURE 5-15 SECURITY SETTINGS – WPA-MIXED PERSONAL.....	42
FIGURE 5-16 SECURITY SETTINGS – WPA-MIXED ENTERPRISE.....	42
FIGURE 5-17 ADVANCED SETTINGS	43
FIGURE 5-18 WMM CONFIGURATION	45
FIGURE 5-19 ACCESS CONTROL	46
FIGURE 5-20 WAN PORT SETTINGS – DHCP	46
FIGURE 5-21 WAN PORT SETTINGS – STATIC IP.....	47
FIGURE 5-22 WAN PORT SETTINGS – PPPOE.....	48
FIGURE 5-23 DYNAMIC DNS SETTINGS	48
FIGURE 5-24 REMOTE MANAGEMENT	52
FIGURE 5-25 DHCP SERVER SETTINGS	52
FIGURE 5-26 DMZ SETTINGS.....	53
FIGURE 5-27 VIRTUAL SERVER SETTINGS.....	54
FIGURE 5-28 IP FILTERING SETTINGS.....	54

FIGURE 5-29 PORT FILTERING SETTINGS	55
FIGURE 5-30 MAC FILTERING SETTINGS	55
FIGURE 5-31 BANDWIDTH CONTROL SETTINGS	56
FIGURE 5-32 SNMP SETTINGS	57
FIGURE 5-33 SYSTEM CONFIGURATION DEFAULT PAGE	58
FIGURE 5-34 DEFAULT IP SETTINGS	58
FIGURE 5-35 TIME SETTINGS	59
FIGURE 5-36 PASSWORD SETTINGS	60
FIGURE 5-37 SYSTEM MANAGEMENT	60
FIGURE 5-38 PING WATCHDOG	61
FIGURE 5-39 FIRMWARE UPGRADE	62
FIGURE 5-40 CONFIGURATION SAVE AND RESTORE	62
FIGURE 5-41 FACTORY DEFAULT	63
FIGURE 5-42 REBOOT SYSTEM	63
FIGURE 5-43 SCHEDULE REBOOT	63
FIGURE 5-44 SCHEDULE REBOOT - EXAMPLE	64
FIGURE 5-45 NETWORK PING	65
FIGURE 5-46 NETWORK TRACEROUTE	66
FIGURE 5-47 DEVICE STATUS	67
FIGURE 5-48 DEVICE INFORMATION	68
FIGURE 5-49 WIRELESS INFORMATION	69
FIGURE 5-50 LAN INFORMATION	70
FIGURE 5-51 WIRELESS CLIENT TABLE	71
FIGURE 5-52 SYSTEM LOG	71
FIGURE 5-53 LOGOUT	72
FIGURE 5-54 RE-LOGIN	72

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing IFS, - WMC251. Before installing the AP, please verify the contents inside the package box.

WMC251-1W-1T-300



Quick Installation Guide

1. Package Contents
Thank you for choosing IFSNET WMAP-6325. Before installing the AP, please verify the contents inside the package box.

2. Installation Precautions
1. Users **MUST** use a proper and well-installed surge protector and grounding device with the WMAP-6325. Otherwise, a sudden lightning could cause fire. **Damage to the WMAP-6325 AND EQUIPMENT DAMAGE IS NOT COVERED UNDER WARRANTY.**
2. Users **MUST** use the "Power cord and PoE Injector" provided in the box with the WMAP-6325. Use of other options will cause damage to the WMAP-6325.

3. Physical Introduction
Rear Panel Description - LED Indication

Power LED LAN 1 LED
LAN 2 LED Wireless LED

4. Hardware Installation
STEP 1: (A) Push the latch on the bottom of the WMAP-6325 to remove the access cover.

Bottom Panel Description - Part
Reset Button Grounding Terminal
LAN2 PoE LAN

STEP 2: Plug the power cord into the DC port and the other side into the AC socket. Then, plug the PoE cable (as shown in picture 4 under Step 1) into the PoE part of the PoE injector.

PoE Injector & Power Cord



Plastic Strap x 1



If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description



Cost-effective Wireless Solution with Superior Performance

IFS, WMC251 is designed to provide a highly-stable, better performance and cost-effective wireless solution in outdoor wireless deployment. With the same transmission power, it offers better significant range and excellent throughput than those of the traditional 802.11g wireless device. Via the embedded 12dBi dual-polarization (vertical and horizontal) directional antenna, it provides good diversity coverage and better noise immunity effect, thus heightening the performance of a long-distance, outdoor connectivity even though the environment is flooded with many 2.4GHz wireless equipment.

Designed for Various Requirements

The WMC251 is dedicatedly designed for WISP solution that provides CPE users with Internet access via the WISP provider in rural areas. Besides, it caters to various wireless communication connectivity (AP / Client / WDS PtP / WDS PtMP / WISP), thus meeting users' application requirements.

Advanced Security and Rigorous Authentication

The WMC251 supports WEP, WPA / WPA2, WPA-PSK and WPA2-PSK wireless encryptions, the advanced WPA2-AES mechanism and 802.1X RADIUS authentication, which can effectively prevent eavesdropping by unauthorized users or bandwidth occupied by unauthenticated wireless access. Furthermore, any users are granted or denied access to the wireless LAN network based on the ACL (Access Control List) that the administrator pre-established. In addition, with the multiple-SSIDs feature, you can set up different wireless networks. The WMC251 can therefore serve as a virtual access point for segmented networks tailored to any industrial need.

Flexible and Reliable Outdoor Characteristics

The WMC251 is definitely suitable for such applications as IP surveillance, backhaul link of building to building and backbone of public service. Additionally, the self-healing/schedule reboot capability keeps connection alive all the time. Meeting the IP55 rating for outdoor UV resistant enclosure, the WMC251 can perform normally under rigorous weather conditions, meaning it can be installed in any harsh, outdoor environments. With the proprietary Power over Ethernet (PoE) design, the WMC251 can be easily installed in the areas where power outlets are not available.

Easy Deployment and Management

With user-friendly Web UI and step-by-step setup wizard, the WMC251 is easy to install, even for users who never experience in setting up a wireless network. Furthermore, with the IFS, - SNMP-based management interface, the WMC251 is convenient to be managed and configured remotely.

1.3 Product Features

- **Industrial Compliant Wireless LAN and WAN**
 - Compliant with the IEEE 802.11n wireless technology (with data rate of up to 300Mbps)
 - Backward compatible with 802.11g standard
 - Equipped with 10/100Mbps RJ45 ports for LAN and WAN; auto MDI/ MDI-X supported
- **Fixed-network Broadband Router**
 - Supported connection types: Dynamic IP, Static IP, PPPoE
 - Supports virtual server and DMZ for various networking applications
 - Supports DHCP server, UPnP and IFS, - DDNS
- **RF Interface Characteristics**
 - Built-in 12dBi dual-polarization antenna
 - High output power up to 500mW with multiply-adjustable transmit power control
- **Outdoor Environmental Characteristics**
 - IP55 enclosure
 - Passive Power over Ethernet design
 - Operating temperature: -20~70°C
- **Multiple Operations and Wireless Modes**
 - Multiple operation modes: Bridge, WISP
 - Multiple wireless modes: AP, Client CPE (WISP), WDS PtP, WDS PtMP
 - Supports multiple SSIDs to allow users to access different networks through a single AP
 - Supports WMM (Wi-Fi multimedia)
- **Secure Network Connection**
 - Supports software Wi-Fi Protected Setup (WPS)
 - Advanced security: 64/128-bit WEP, WPA / WPA2, WPA-PSK / WPA2-PSK (TKIP/AES) and 802.1x RADIUS authentication
 - Supports IP / Protocol-based access control and MAC filtering
- **Easy Installation and Management**
 - Web-based UI and quick Setup Wizard for easy configuration
 - SNMP-based management interface
 - System status monitoring includes DHCP Client and System Log

1.4 Product Specification

Product	WMC251-1W-1T-300 300Mbps 802.11n Wireless Outdoor CPE	
Hardware		
Standard Support	IEEE802.11b/g/n IEEE 802.3 IEEE 802.3u IEEE 802.3x	
Chipset	Atheros AR9344	
Memory	64 Mbytes DDR SDRAM 16 Mbytes Flash	
PoE	Passive PoE	
Interface	Wireless IEEE802.11b/g/n, 2T2R PoE LAN (LAN 1): 1 x 10/100BASE-TX, auto-MDI/MDIX, passive PoE LAN 2: 1 x 10/100BASE-TX, auto-MDI/MDIX, passive PoE out pass-through	
Antenna	Built-in 12dBi Dual-Polarization Antenna - Horizontal: 30 degrees - Vertical: 20 degrees	
Data Rate	IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: up to 54Mbps IEEE 802.11n (20MHz): up to 150Mbps IEEE 802.11n (40MHz): up to 300Mbps	
Media Access Control	CSMA/CA	
Modulation	Transmission/Emission type: OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM	
Frequency Band	2.412GHz ~ 2.484GHz	
Operating Channel	America/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels) Japan/ TELEC: 2.412~2.484GHz (14 Channels)	
RF Output Power (dBm)	IEEE 802.11b: up to 26 ± 1dBm IEEE 802.11g: up to 23 ± 1dBm IEEE 802.11n: up to 22 ± 1dBm	
Receiver Sensitivity (dBm)	IEEE 802.11b: -94dBm IEEE 802.11g: -91dBm IEEE 802.11n: -89dBm	
Output Power Control	12~27Bm	
Power Consumption	12W	
Power Requirements	LAN	24VDC, 1A/ Passive PoE Pin 4,5 VDC+ Pin 7,8 VDC- Pin 3 Reset
Environment & Certification		

Operating Temperature	-20~70°C
Operating Humidity	10~95% non-condensing
IP Level	IP55
Regulatory	CE, FCC, RoHS
Software	
LAN	Built-in DHCP server supporting static IP address distributing
	Support 802.1d STP (Spanning Tree)
WAN	<ul style="list-style-type: none"> ■ Static IP ■ Dynamic IP ■ PPPoE
Operation Modes	<ul style="list-style-type: none"> ■ Bridge ■ WISP
Firewall	NAT firewall with SPI (Stateful Packet Inspection)
	Built-in NAT server supporting Virtual Server, and DMZ
	Built-in firewall with Port/ IP address/ MAC/ URL filtering
Wireless Modes	<ul style="list-style-type: none"> ■ AP ■ Client ■ WDS PTP ■ WDS PTMP ■ WISP
Channel Width	20MHz / 40MHz
Wireless Isolation	Enable it to isolate each connected wireless client so that they cannot access mutually.
Encryption Type	64/128-bit WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X
Wireless Security	Provides wireless LAN ACL (Access Control List) filtering
	Wireless MAC address filtering
	Enable/Disable SSID Broadcast
Max. Wireless Clients	25
Max. WDS AP	8
Max. Wired Clients	60
WMM	Supports Wi-Fi multimedia
QoS	Supports Quality of Service for bandwidth control
NTP	Network Time Management
Self Healing	Supports Schedule Reboot
Management	Web UI, DHCP Client, Configuration Backup & Restore, Dynamic DNS, SNMP
Diagnostic Tool	System Log, Ping Watchdog

Chapter 2. Hardware Installation

Please follow the instructions below to connect the WMC251 to the existing network devices and your computers.

2.1 Hardware Description

- **Dimensions:** 127 x 63 x 254 mm (W x D x H)



Figure 2-1 Three-way View

Rear Panel – LED



Figure 2-2 LED

LED Definition

LED	State	Meaning
Power	On	System On
	Off	System Off
Wireless	On	Wi-Fi On
	Off	Wi-Fi Off
LAN 1	On	Port linked.
	Off	No link.
LAN 2	On	Port linked.
	Off	No link.

Table 2-1 The LED indication

2.1.1 The Bottom Panel – Port

The Bottom panel provides the physical connectors connected to the power adapter and any other network device. [Figure 2-3](#) shows the bottom panel of the WMC251.

Bottom Panel

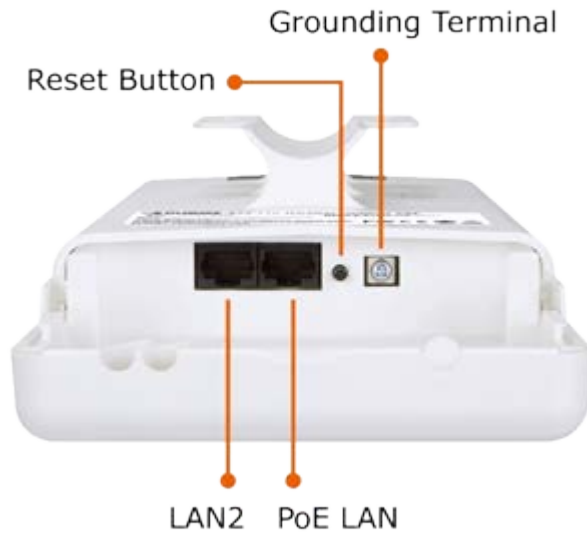


Figure 2-3 Bottom Panel

PoE Injector



Figure 2-4 PoE Injector

H/W Interface Definition

Object	Description
PoE LAN (Passive PoE)	10/100Mbps RJ45 port , auto MDI/ MDI-X and passive PoE supported Connect LAN port to the PoE injector to power on the device. Pin assignment: Pin 4, 5 (+) Pin 7, 8 (-) Pin 3 (Reset)
LAN 2	10/100Mbps RJ45 port, auto MDI/ MDI-X Connect this port to the network equipment. ※ When the option “Enable POE Passthrough” on the System Management page is checked, the LAN2 can supply passive PoE power to the second WMC251 or WMC251 through LAN 2.

Reset	<p>Press the Reset button on the device or on the PoE injector over 5 seconds to return to factory default setting.</p> <p>※ If you have connected with a lightning protector like IFS, - ESP300, please DO NOT press the reset button on the PoE injector to prevent the ESP300 from being damaged. Remove the Lighting protector before push the reset button.</p>
--------------	--

Table 2-2 The PoE Injector Indication

Chapter 3. Connecting to the AP

3.1 Preparation before Installation

3.1.1 Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

3.1.2 Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing the WMC251 for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing the WMC251, please note the following things:
 - ◆ Do not use a metal ladder;
 - ◆ Do not work on a wet or windy day;
 - ◆ Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

3.2 Installation Precautions

- Users **MUST** use a proper and well-installed surge arrester and grounding kit with WMC251; otherwise, a random lightning could easily cause fatal damage to the WMC251. (**Lightning DAMAGE IS NOT COVERED UNDER WARRANTY**).
- Users **MUST** use the "Power cord and PoE Injector" shipped in the box with the WMC251. Use of other options will cause damage to the WMC251.



OUTDOOR INSTALLATION WARNING

IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK! Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

CONTACTING POWER LINES CAN BE LETHAL. Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these lines. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure that equipment or personnel do not come in contact directly or indirectly with power lines.



The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination. This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

- Select equipment locations that will allow safe, simple equipment installation.
- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Use approved non-conducting ladders and other safety equipment. Make sure all equipment is in good repair.
- If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or mast does come in contact with a power line, **DON'T TOUCH IT OR ATTEMPT TO MOVE IT.** Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS. This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

- The base of the antenna mast or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 1 OAWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE:

- **DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.**
- Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.

Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

3.3 Installing the AP

Please install the AP according to the following Steps. Don't forget to pull out the power plug and keep your hands dry.

Step 1. Push the latch on the bottom of the WMC251 to remove the sliding cover.



Figure 3-1 Connect the Antenna

Step 2. Plug the RJ45 Ethernet cable into the PoE LAN Port of the WMC251. Then, slide back the cover of the WMC251 to finish the installation.

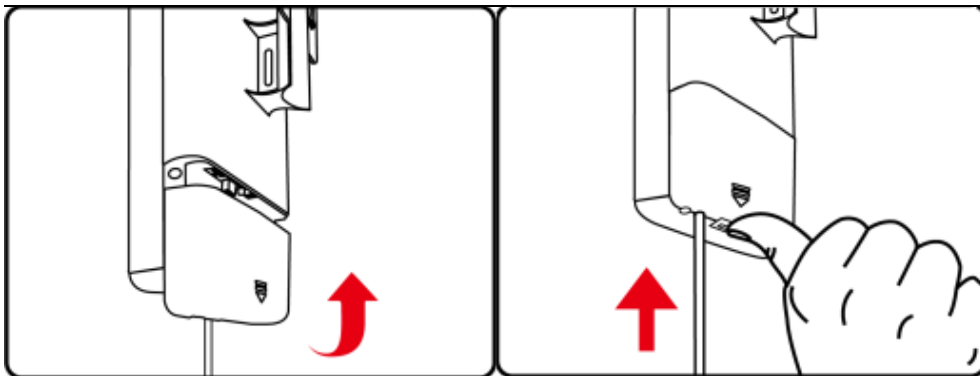


Figure 3-2 Connect the Ethernet cable

Step 3. Plug the power cord into the DC port and the other end into the AC socket. Then, plug the RJ45 cable (as shown in picture 4 under Step 1) into the POE port of the PoE injector.

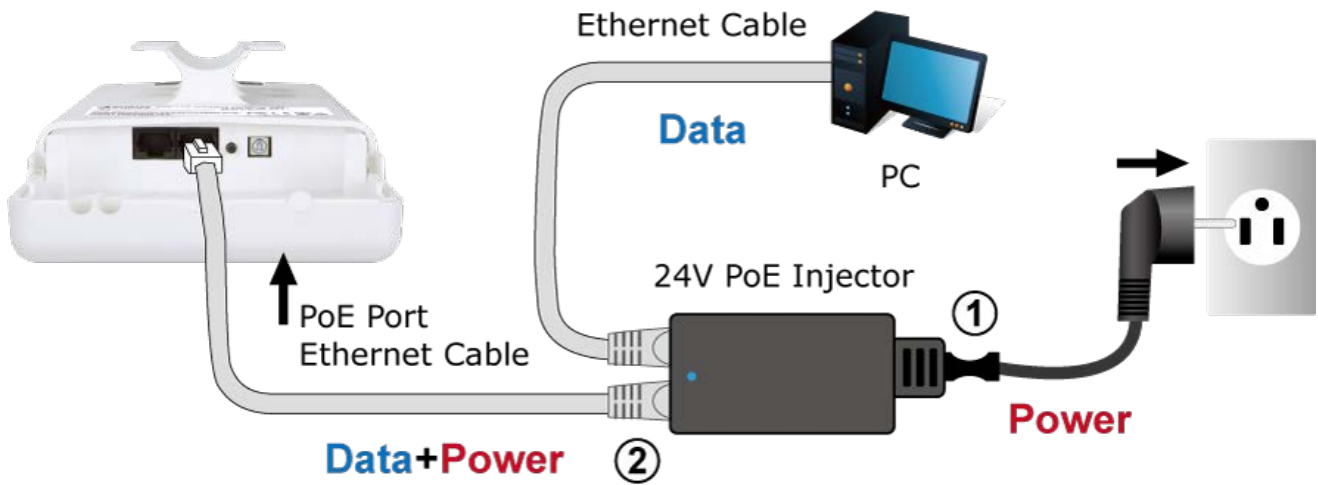


Figure 3-3 Connect the PoE injector

Step 4. Pole Mounting:

Place the strap through the slot on the back of the WMC251 and then around the pole. Tighten the strap to secure the WMC251.



Figure 3-4 Pole Mounting

Chapter 4. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AP within minutes.



A computer with wired Ethernet connection to the Wireless AP is required for the first-time configuration.

4.1 Manual Network Setup - TCP/IP Configuration

The default IP address of the WMC251 is **192.168.0.100**. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the WMC251 with your PC via an Ethernet cable which is then plugged into a LAN port of the PoE injector with one end and into a LAN port of the PC with the other end. Then power on the WMC251 via PoE injector or PoE switch.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 7**. And the procedures in other operating systems are similar. First, make sure your Ethernet adapter is working, and refer to the Ethernet adapter's manual if needed.

4.1.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.0.xxx("xxx" is any number from 2 to 252), Subnet Mask is 255.255.255.0, and Gateway is 192.168.0.100 (The AP's default IP address)

- 1 Select **Use the following IP address** radio button.
- 2 If the AP's LAN IP address is 192.168.0.1, enter IP address 192.168.0.x (x is from 2 to 254), and **Subnet mask** 255.255.255.0.
- 3 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field, you can enter the DNS server IP address which has been provided by your ISP

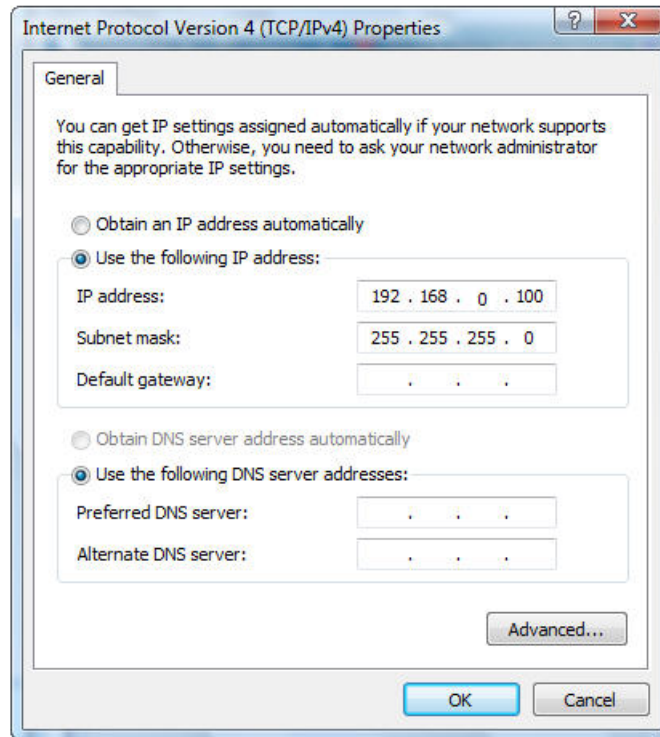


Figure 4-1 TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 7** OS. Please follow the Steps below:

1. Click on **Start > Run**.
2. Type "**cmd**" in the Search box.

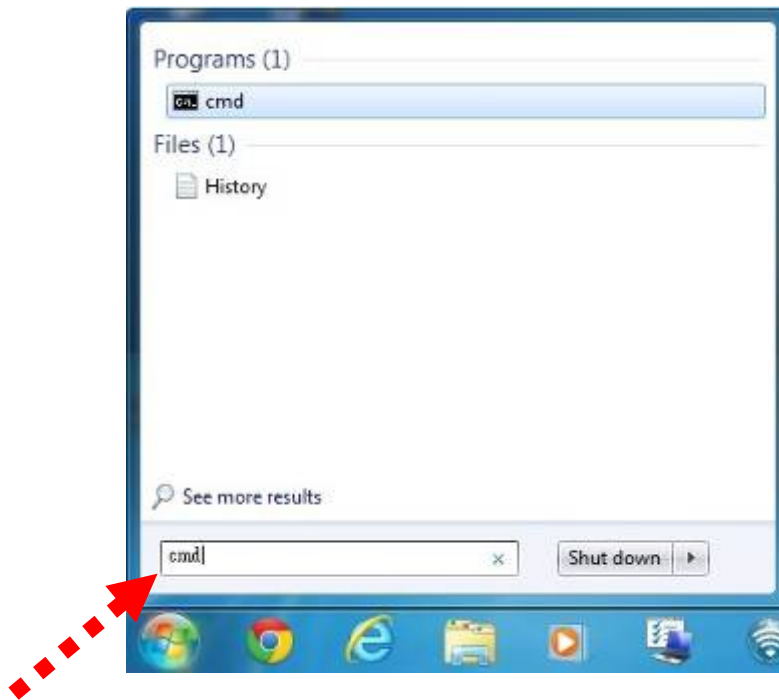


Figure 4-2 Windows Start Menu

3. Open a command prompt and type **ping 192.168.0.100**, and then press **Enter**.

If the result displayed is similar to [Figure 4-3](#), it means the connection between your PC and the AP has been established well.

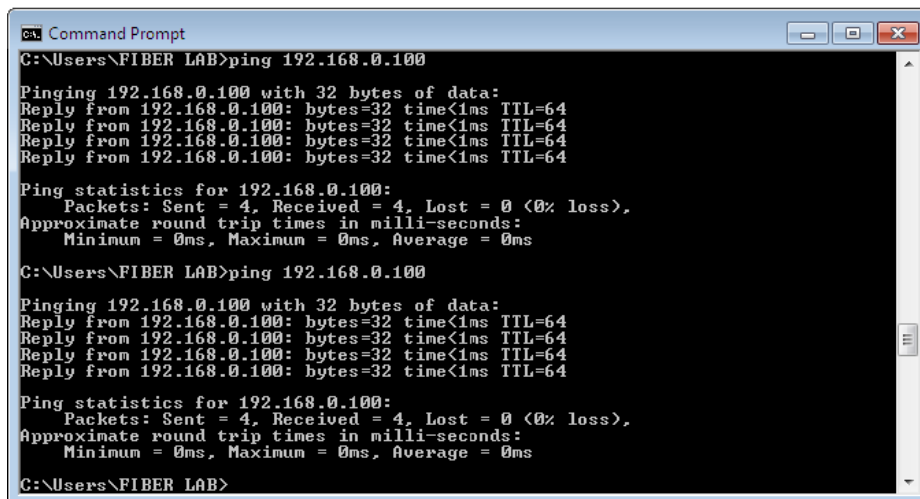


Figure 4-3 Successful result of Ping command

If the result displayed is similar to [Figure 4-4](#), it means the connection between your PC and the AP has failed.

```
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\FIBER LAB>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:
Reply from 192.168.0.100: bytes=32 time<1ms TTL=64
Reply from 192.168.0.100: bytes=32 time<1ms TTL=64
Reply from 192.168.0.100: bytes=32 time<1ms TTL=64
Reply from 192.168.0.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\FIBER LAB>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.201: Destination host unreachable.
Reply from 192.168.0.201: Destination host unreachable.
Reply from 192.168.0.201: Destination host unreachable.
Reply from 192.168.0.201: Destination host unreachable.

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\FIBER LAB>
```

Figure 4-4 Failed result of Ping command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

4.2 Starting Setup in the Web UI

It is easy to configure and manage the WMC251 with the web browser.

Step 1. To access the configuration page, open a web browser and enter the default IP address <http://192.168.0.100> in the web address field of the browser.

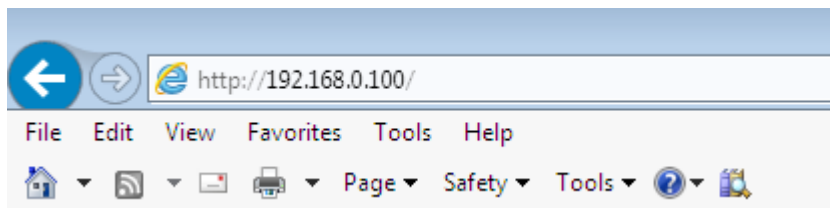


Figure 4-5 Login by default IP address

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 4-6 Login Window

Default IP Address: **192.168.0.100**

Default User Name: **admin**

Default Password: **admin**



If the above screen does not pop up, it may mean that your web browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings** in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

After entering the username and password, the **Operation Mode** page screen appears as in **Figure 4-8**

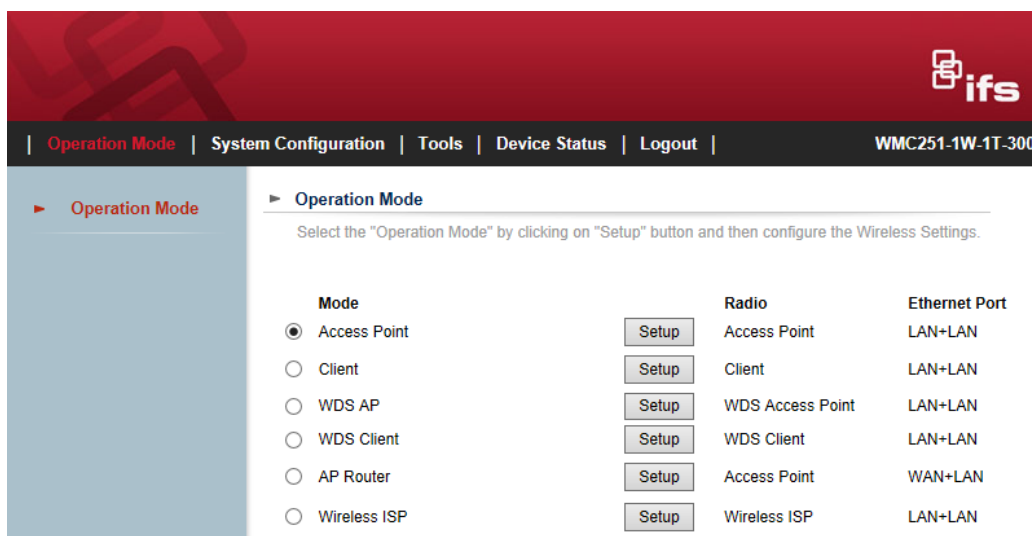


Figure 4-7 WMC251 Web UI Screenshot

Step 2. You can choose an Operation Mode. Please refer to the instructions in the next chapter for configuring

the other Operation Modes.

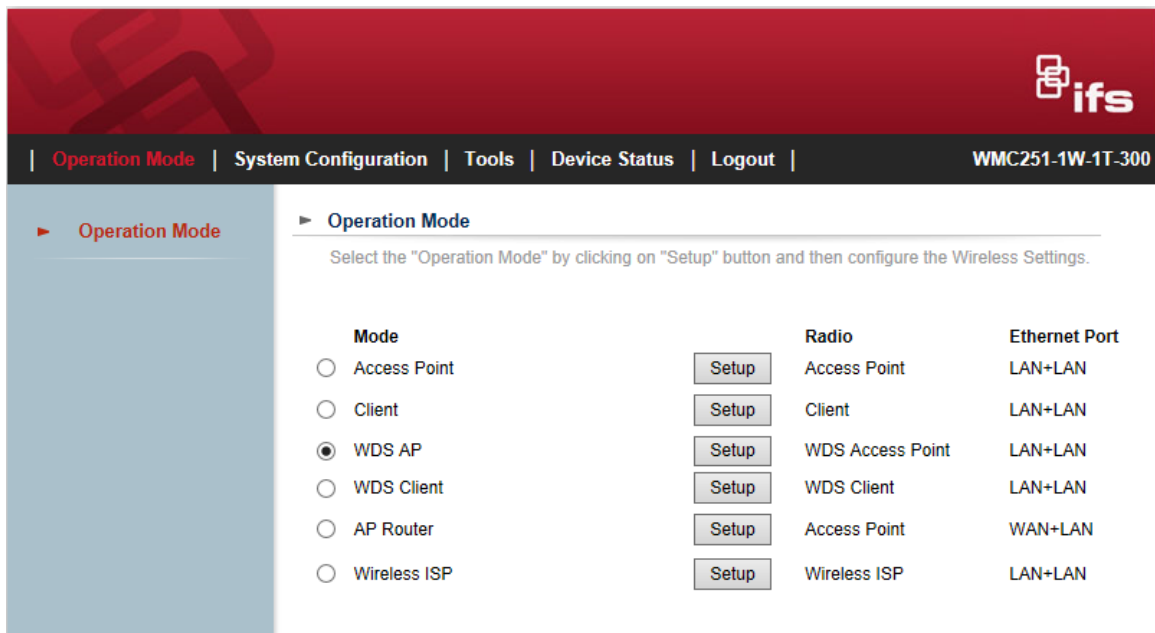


Figure 4-8 Choose Operation Mode

Step 3. Please enter the SSID and configure your Encryption Settings, Pre-Shared Key, etc. Then click the **Save** button to make the configuration take effect immediately.

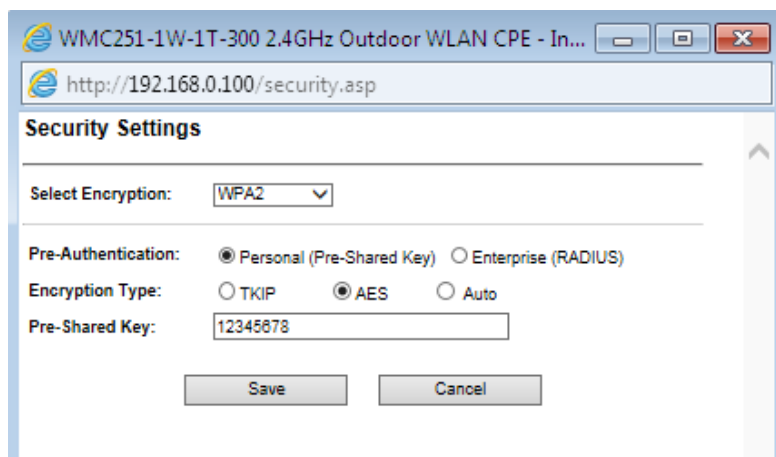


Figure 4-9 Configure Wireless Settings

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and features under 4 main menus (**Operation Mode**, **System Configuration**, **Tools** and **Device Status**) below, allowing you to manage the AP with ease.

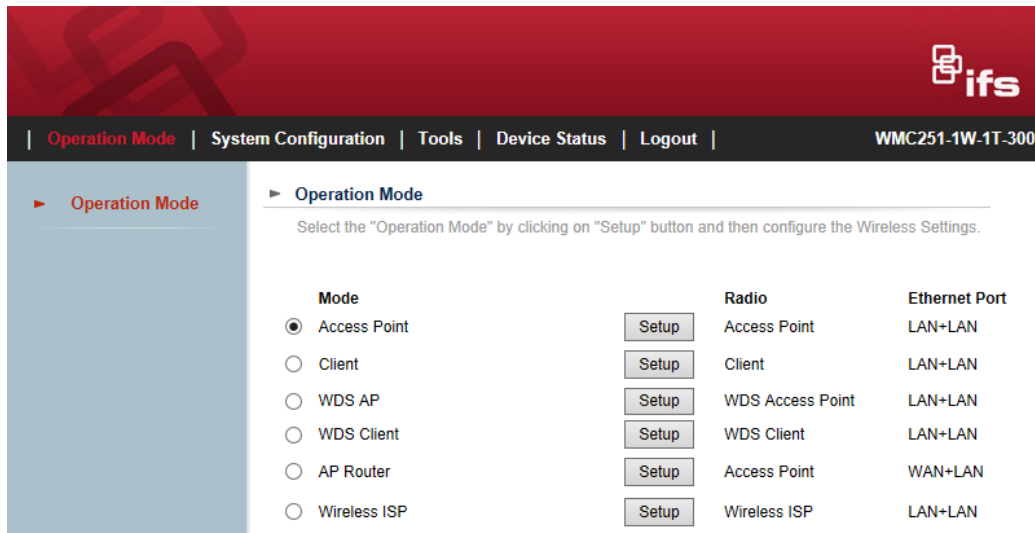


Figure 5-1 Main Menu

5.1 Operation Mode

On this page, you can select different operation modes of the WMC251, including Access Point, Client, WDS AP, WDS Client, AP Router and Wireless ISP.

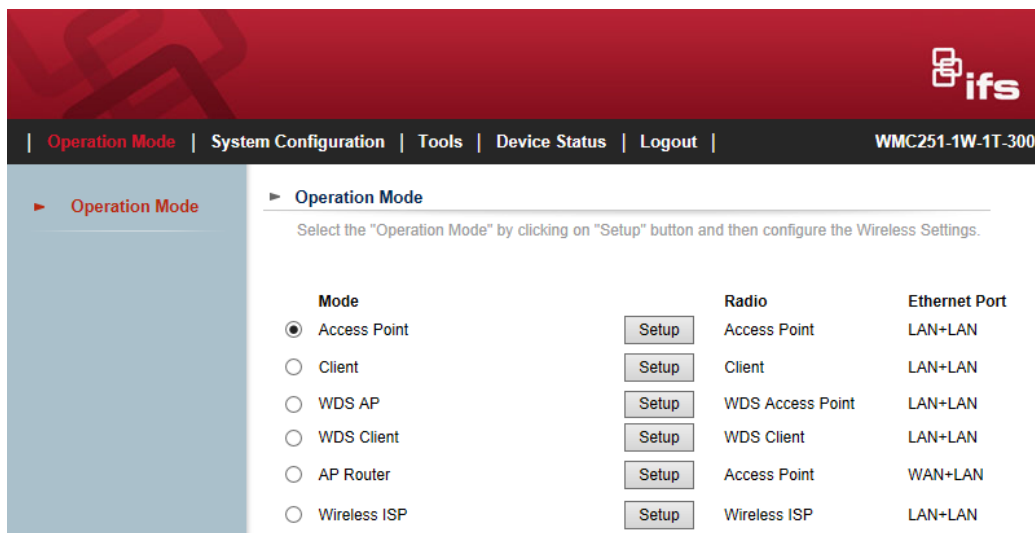


Figure 5-2 Operation Mode

5.1.1 Access Point

Click "**Operation Mode**" → "**Access Point**" and the following page will be displayed. This section allows you to configure the Access Point mode.

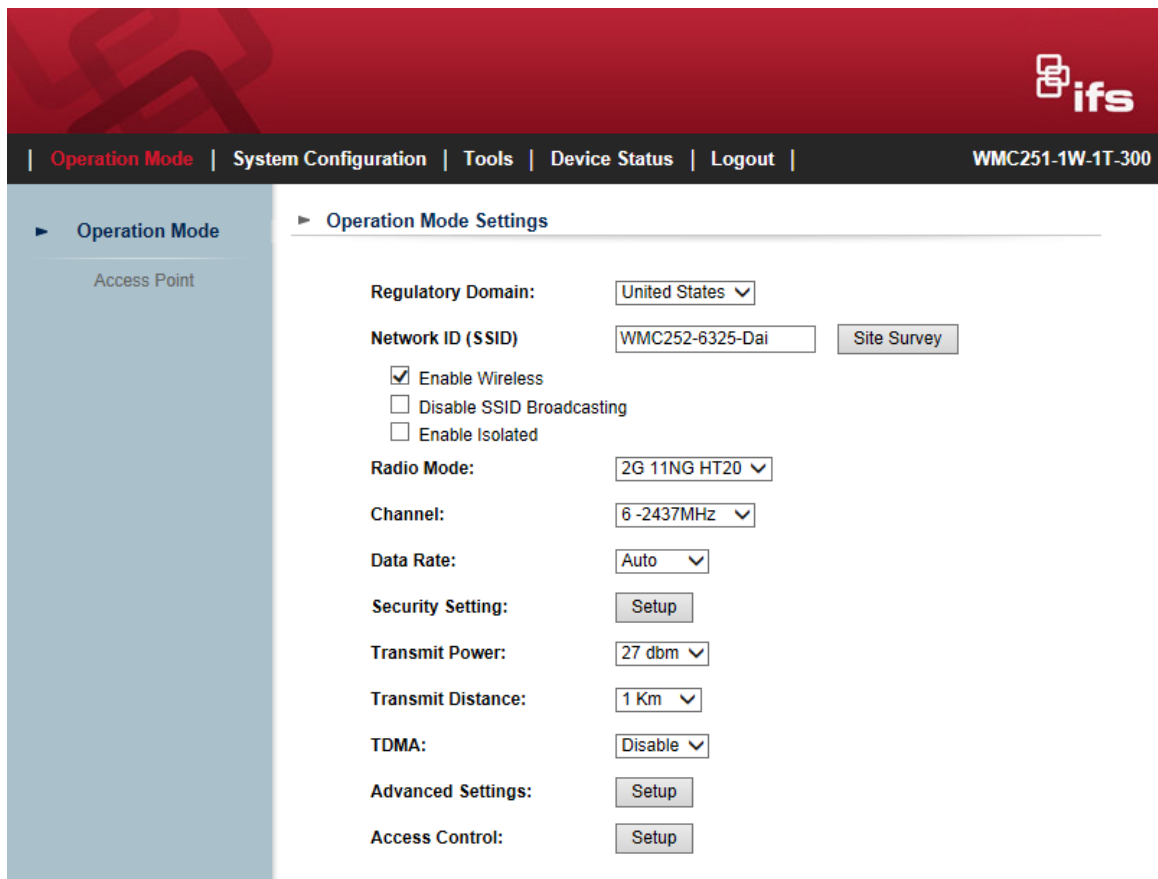


Figure 5-3 Basic Settings - AP

Object	Description
• Regulatory Domain	Select your domain from the list.
• Network SSID	It is the wireless network name. The default SSID is WMC251 .
• Site Survey	Click " Site Survey " to check the signal of remote sites.
• Enable Wireless	Check it to enable Wireless function.
• Disable SSID Broadcasting	Check it to disable SSID broadcasting.
• Enable Isolated	Check it to isolate each connected wireless clients so that they cannot access each other.
• Radio Mode	Select the channel width to " Auto Select ", " 2G 11NG HT20 " or " 2G 11NG HT40 ".
• Channel	Select the operating channel you would like to use. The channel range will be changed by selecting a different domain.
• Data Rate	Select MCS0~15 or Auto from the pull-down menu. The default is " Auto ".
• Security Setting	Press "Setup" for more configurations. Please refer to 5.1.7 Security Setting for more information.
• Transmit Power	The range of transmit power is " 12~27 dbm ". In case of shortening the distance and the coverage of the wireless

	network, input a smaller value to reduce the radio transmission power.
• Transmit Distance	Select a specified distance of the two nodes.
• TDMA	Displays the System Time.
• Advanced Settings	Press “ Setup ” for more configurations. Please refer to 5.1.8 Advanced Settings for more information.
• Access Control	Press “ Setup ” for more configurations. Please refer to 5.1.9 Access Control for more information.

5.1.2 Client

Click “**Operation Mode**” → “**Client**” and the following page will be displayed. This section allows you to configure the Client mode.

Figure 5-4 Basic Settings - Client

Object	Description
• Regulatory Domain	Select your domain from the list.
• Network SSID	It is the wireless network name. The default SSID is WMC251 .
• Site Survey	Click “ Site Survey ” to find the remote sites to associate.
• Enable Wireless	Check it to enable Wireless function.

• Disable SSID Broadcasting	Check it to disable SSID broadcasting.
Enable Isolated	Check it to isolate each connected wireless clients so that they cannot access each other.
Lock to AP MAC	Enter the Mac address of the remote AP.
Radio Mode	Select the channel width to “ Auto Select ”, “ 2G 11NG HT20 ” or “ 2G 11NG HT40 ”
• Data Rate	Select MCS0~15 or Auto from the pull-down menu. The default is “ Auto ”.
• Security Setting	Press “ Setup ” for more configurations. Please refer to 5.1.7 Security Setting for more information.
• Transmit Power	The range of Transmit power is “ 12~27 dbm ”. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power.
• Transmit Distance	Select a specified distance of the two nodes.
• TDMA	Displays the System Time.
• Advanced Settings	Press “ Setup ” for more configurations. Please refer to 5.1.8 Advanced Settings for more information.
• Access Control	Press “ Setup ” for more configurations. Please refer to 5.1.9 Access Control for more information.

5.1.3 WDS AP

Click “**Operation Mode**” → “**WDS AP**” and the following page will be displayed. This section allows you to configure the WDS AP mode. For each wireless parameter, please refer to section **5.1.1 AP** for more information.

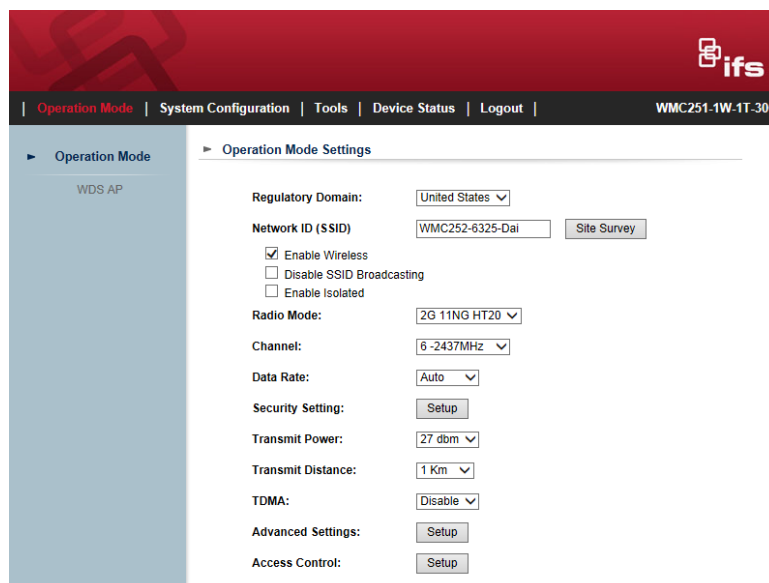
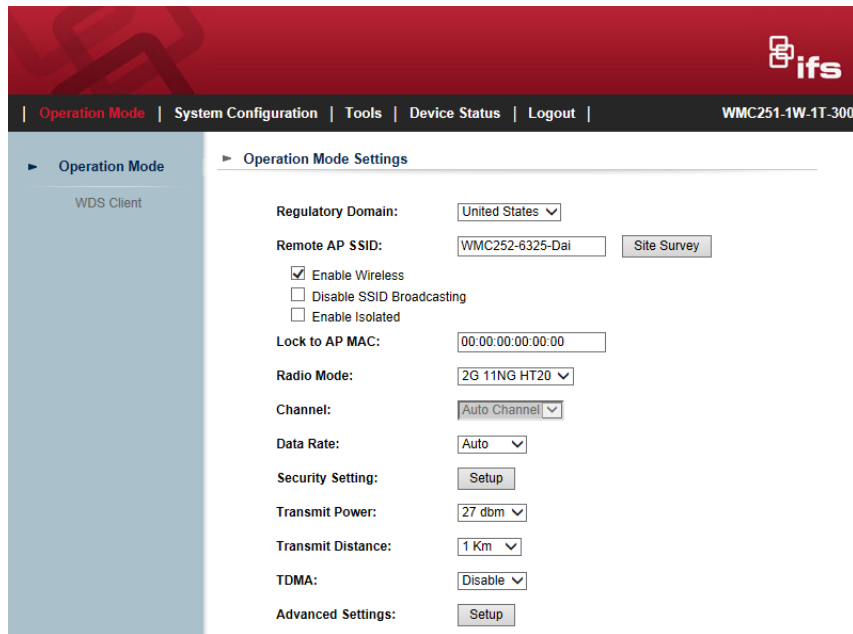


Figure 5-5 Basic Settings – WDS AP

5.1.4 WDS Client

Click “**Operation Mode**” → “**WDS Client**” and the following page will be displayed. This section allows you to configure the WDS Client mode. For each wireless parameter, please refer to section **5.1.2 Client** for more information.



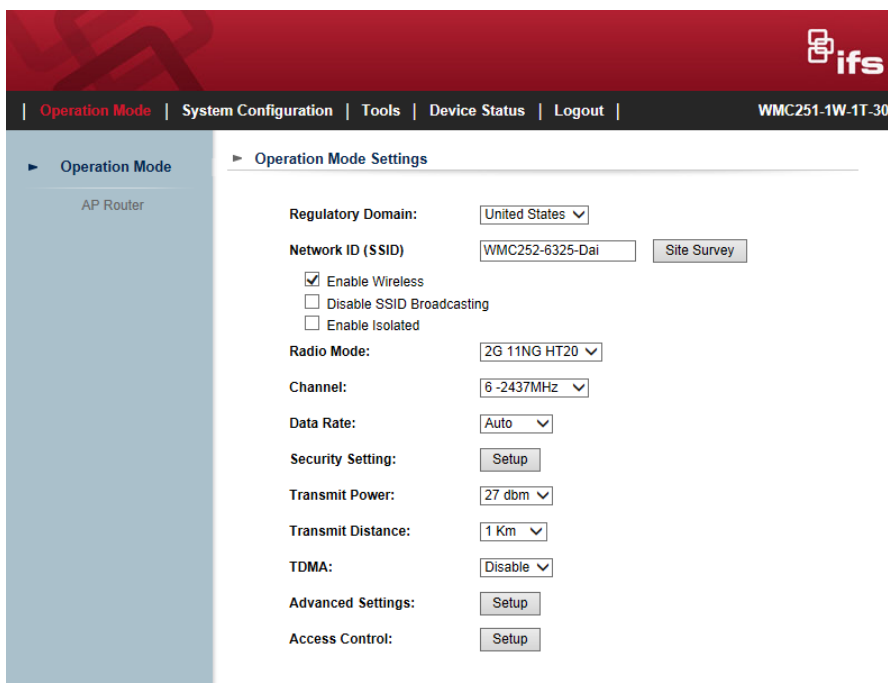
The screenshot shows the WDS Client configuration page. The top navigation bar includes "Operation Mode", "System Configuration", "Tools", "Device Status", and "Logout". The user is logged in as "WMC251-1W-1T-300". The left sidebar shows "Operation Mode" with "WDS Client" selected. The main content area is titled "Operation Mode Settings" and contains the following configuration options:

- Regulatory Domain: United States (dropdown)
- Remote AP SSID: WMC252-6325-Dai (text input) with a "Site Survey" button
- Enable Wireless: (checked)
- Disable SSID Broadcasting: (unchecked)
- Enable Isolated: (unchecked)
- Lock to AP MAC: 00:00:00:00:00:00 (text input)
- Radio Mode: 2G 11NG HT20 (dropdown)
- Channel: Auto Channel (dropdown)
- Data Rate: Auto (dropdown)
- Security Setting: Setup (button)
- Transmit Power: 27 dbm (dropdown)
- Transmit Distance: 1 Km (dropdown)
- TDMA: Disable (dropdown)
- Advanced Settings: Setup (button)

Figure 5-6 Basic Settings – WDS Client

5.1.5 AP Router

Click “**Operation Mode**” → “**AP Router**” and the following page will be displayed. This section allows you to configure the AP Router mode.



The screenshot shows the AP Router configuration page. The top navigation bar includes "Operation Mode", "System Configuration", "Tools", "Device Status", and "Logout". The user is logged in as "WMC251-1W-1T-300". The left sidebar shows "Operation Mode" with "AP Router" selected. The main content area is titled "Operation Mode Settings" and contains the following configuration options:

- Regulatory Domain: United States (dropdown)
- Network ID (SSID): WMC252-6325-Dai (text input) with a "Site Survey" button
- Enable Wireless: (checked)
- Disable SSID Broadcasting: (unchecked)
- Enable Isolated: (unchecked)
- Radio Mode: 2G 11NG HT20 (dropdown)
- Channel: 6 -2437MHz (dropdown)
- Data Rate: Auto (dropdown)
- Security Setting: Setup (button)
- Transmit Power: 27 dbm (dropdown)
- Transmit Distance: 1 Km (dropdown)
- TDMA: Disable (dropdown)
- Advanced Settings: Setup (button)
- Access Control: Setup (button)

Figure 5-7 Basic Settings – AP Router

5.1.6 Wireless ISP

Click “**Operation Mode**” → “**Wireless ISP**” and the following page will be displayed. This section allows you to configure the Wireless ISP mode.

ifs
WMC251-1W-1T-300

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

Operation Mode Settings

Regulatory Domain: United States

Remote AP SSID: WMC252-6325-Dai Site Survey

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Lock to AP MAC: 00:00:00:00:00:00

Radio Mode: 2G 11NG HT20

Channel: Auto Channel

Data Rate: Auto

Security Setting: Setup

Transmit Power: 27 dbm

Transmit Distance: 1 Km

TDMA: Disable

Advanced Settings: Setup

Access Control: Setup

Figure 5-8 Basic Settings – WISP

5.1.7 Security Setting

Choose the operation mode you required, and then enter “**Security Setting**” by clicking the **Setup** button next to it and the following page will be displayed. This section allows you to configure the wireless security settings.

Security Settings

Select Encryption: WEP

Authentication: Open System Shared Key Auto

Key Length: 64-bit 128-bit

Key Format: ASCII(5 Characters)

Encryption Key:

Save Cancel

Figure 5-9 Security Settings

Object	Description
<ul style="list-style-type: none"> • Select Encryption 	<p>Select the encryption that you need.</p> <p>None: No security required</p> <p>WEP: Input 5, 13 (ASCII) or 10, 26 (HEX) character for WEP key.</p> <p>WPA: Enter ASCII characters between 8 and 63 character or 8 to 64 hexadecimal characters.</p> <p>WPA2: Enter ASCII characters between 8 and 63 character or 8 to 64 hexadecimal characters.</p> <p>WPA-Mixed: Enter ASCII characters between 8 and 63 character or 8 to 64 hexadecimal characters.</p>

■ **None**

Authentication is disabled and no password/key is required to connect to the access point.

■ **WEP**

WEP (Wired Equivalent Privacy) is a basic encryption. For a higher level of security consider using the WPA encryption.

The screenshot shows a 'Security Settings' dialog box. At the top, it says 'Select Encryption:' with a dropdown menu currently showing 'WEP'. Below this, there are three rows of radio button options: 'Authentication:' with 'Open System' (selected), 'Shared Key', and 'Auto'; 'Key Length:' with '64-bit' (selected) and '128-bit'; and 'Key Format:' with a dropdown menu showing 'ASCII(5 Characters)'. At the bottom, there is a text input field for 'Encryption Key:' which is currently empty. Below the input field are two buttons: 'Save' and 'Cancel'.

Figure 5-10 Security Settings – WEP

Object	Description
<ul style="list-style-type: none"> • Authentication 	You can select Open System , Shared Key or Auto .
<ul style="list-style-type: none"> • Key Length 	Choose the WEP key length. You can choose 64-bit or 128-bit .
<ul style="list-style-type: none"> • Key Format 	You can choose ASCII or Hex .
<ul style="list-style-type: none"> • Encryption Key 	Enter the keys in the fields.

■ WPA

Security Settings

Select Encryption:

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key:

Figure 5-11 Security Settings – WPA Personal

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

RADIUS Server IP Address:

RADIUS Server Port:

RADIUS Server Password:

EAP Reauthorization Period: Seconds (300 ~ 3600 Seconds)

RSN Reauthorization:

WPA Group Rekey Interval: Seconds (300 ~ 3600 Seconds)

Figure 5-12 Security Settings – WPA Enterprise

Object	Description
• Pre-Authentication	Select “Personal (Pre-Shared Key)” or “Enterprise (RADIUS)” encryption type.
• Encryption Type	Set the WPA to be TKIP , AES or Auto .
• Pre-Shared Key	Enter the keys in the fields.
• RADIUS Server IP Address	Enter the RADIUS server host IP address.
• RADIUS Server Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 and 65535.
• RADIUS Server Password	Enter a shared secret/password between 1 and 99 characters in length.

<ul style="list-style-type: none"> • EAP Reauthorization Period 	Set duration of session timeout in seconds between 300 and 3600.
<ul style="list-style-type: none"> • RSN Reauthorization 	Enable or disable RSN reauthorization.
<ul style="list-style-type: none"> • WPA Group Rekey Interval 	Set duration of session timeout in seconds between 300 and 3600.

■ **WPA2**

Please refer to WPA for more information.

Security Settings

Select Encryption:

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key:

Figure 5-13 Security Settings – WPA2 Personal

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

RADIUS Server IP Address:

RADIUS Server Port:

RADIUS Server Password:

EAP Reauthorization Period: Seconds (300 ~ 3600 Seconds)

RSN Reauthorization:

WPA Group Rekey Interval: Seconds (300 ~ 3600 Seconds)

Figure 5-14 Security Settings – WPA2 Enterprise

■ WPA-Mixed

Please refer to WPA for more information.

Security Settings

Select Encryption: ▾

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key:

Figure 5-15 Security Settings – WPA-Mixed Personal

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

RADIUS Server IP Address:

RADIUS Server Port:

RADIUS Server Password:

EAP Reauthorization Period: Seconds (300 ~ 3600 Seconds)

RSN Reauthorization: ▾

WPA Group Rekey Interval: Seconds (300 ~ 3600 Seconds)

Figure 5-16 Security Settings – WPA-Mixed Enterprise

5.1.8 Advanced Settings

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

Advanced Wireless Settings

RTS/CTS Threshold:	<input type="text" value="2347"/>	bytes (range: 0 ~ 2347, default 2347)
Beacon Interval:	<input type="text" value="100"/>	milliseconds (range 20 ~ 999, default 100)
DTIM:	<input type="text" value="1"/>	(range 1 ~ 255, default 1)
Fragment Size:	<input type="text" value="2346"/>	bytes (range 256 ~ 2346, default 2346)
Short GI:	<input type="radio"/> 400ns <input checked="" type="radio"/> 800ns	
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Aggregated Frames Number:	<input type="text" value="32"/>	(range 1 ~ 32, default 32)
Maximum Aggregated Size:	<input type="text" value="50000"/>	(range 2346 ~ 65536, default 50000)
Tx ChainMask:	<input type="text" value="2 Chain"/> ▼	
Rx ChainMask:	<input type="text" value="2 Chain"/> ▼	

WiFi Multimedia

WMM Capable Enable Disable

Figure 5-17 Advanced Settings

Object	Description
<ul style="list-style-type: none"> • RTS/CTS Threshold 	When the length of a data packet exceeds this value, the router will send an RTS frame to the destination wireless node, and the latter will reply with a CTS frame, and thus they are ready to communicate. The default value is 2347.
<ul style="list-style-type: none"> • Beacon Interval 	Set beacon interval, the value range is from 20 to 999. The default value is 100.
<ul style="list-style-type: none"> • DTIM 	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
<ul style="list-style-type: none"> • Fragment Size 	A data packet that exceeds this value in length will be divided into multiple packets. The number of packets influences wireless network performance. Avoid setting this value low. Default at 2346.

<ul style="list-style-type: none"> • Short GI 	Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Only effect under Mixed Mode.
<ul style="list-style-type: none"> • Aggregation 	A part of the 802.11n standard that allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source, destination end points, and traffic class (QoS) into one large frame with a common MAC header
<ul style="list-style-type: none"> • Aggregated Frames Number 	Determines the number of frames combined in the new larger frame.
<ul style="list-style-type: none"> • Maximum Aggregated Size 	Determines the size (in bytes) of the larger frame.
<ul style="list-style-type: none"> • Tx ChainMask 	Displays the number of independent spatial data streams the device is transmitting (TX) and receiving (RX) simultaneously within one spectral channel of bandwidth. Multiple chains increase data transfer performance significantly.
<ul style="list-style-type: none"> • Rx ChainMask 	Displays the number of independent spatial data streams the device is transmitting (TX) and receiving (RX) simultaneously within one spectral channel of bandwidth. Multiple chains increase data transfer performance significantly.
<ul style="list-style-type: none"> • WMM Capable 	Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

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

Figure 5-18 WMM Configuration

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

5.1.9 Access Control

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

Figure 5-19 Access Control

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

5.1.10 WAN Port Settings

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

■ DHCP (Auto Config)

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

Figure 5-20 WAN Port Settings – DHCP

■ Static Mode (Fixed IP)

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

WAN Port Settings

WAN Connection Type: ▾

IP Address Assigned by Your ISP:

IP Subnet Mask:

ISP Gateway IP Address:

Primary DNS Server:

Secondary DNS Server:

Figure 5-21 WAN Port Settings – Static IP

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

■ **PPPOE (ADSL)**

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

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

Figure 5-22 WAN Port Settings – PPPOE

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

5.1.11 Dynamic DNS Settings

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

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

Figure 5-23 Dynamic DNS Settings

Object	Description
<ul style="list-style-type: none"> • DDNS option 	<p>Disable: Disable DDNS function</p> <p>Enable Easy DDNS: Enable IFS, - Easy DDNS</p> <p>Enable Dynamic DDNS: You are allowed to modify the DDNS settings.</p>
<ul style="list-style-type: none"> • Dynamic DNS Provider 	Select a server provider or disable the existing server.
<ul style="list-style-type: none"> • Account 	Enter the DDNS user name of the DDNS account.
<ul style="list-style-type: none"> • Password 	Enter the DDNS password of the DDNS account.
<ul style="list-style-type: none"> • DDNS 	Enter the host name or domain name provided by DDNS provider.

Example of DDNS Settings:



Please go to xxx.Yourddns.xxx to register with a DDNS account.

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



Step 1. Select “**Enable Dynamic DDNS**” and select from the list your Dynamic DNS Provider.

Dynamic DNS Settings

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

DDNS option: ▼

Easy Domain Name:

DDNS Settings:

Dynamic DNS Provider: ▼

Account:

Password:

DDNS:


Step 2. Configure the DDNS account that has been registered in IFS, - DDNS website.

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

Password: Enter the password of your account.

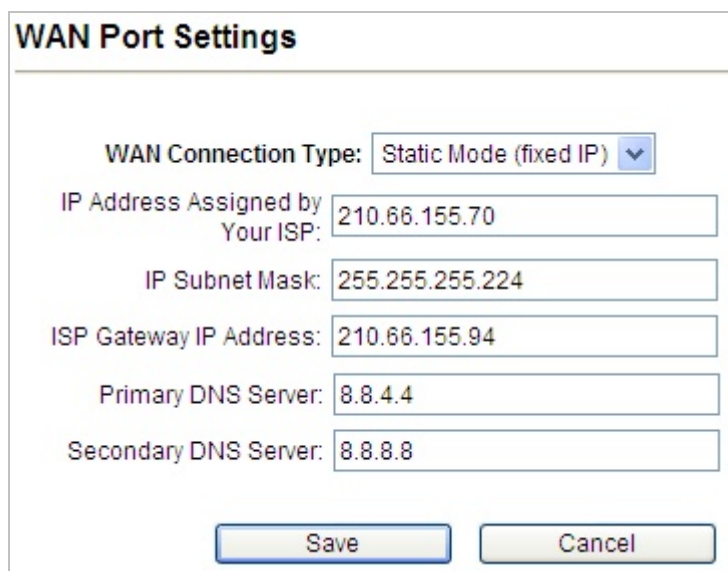
DDNS: Enter your DDNS host again.

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



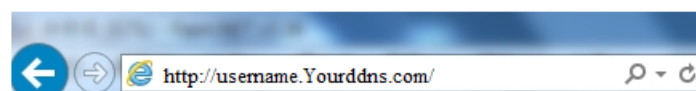
The screenshot shows a dialog box titled "Remote Management Settings". It contains two dropdown menus: "Remote management (via WAN):" set to "Enable" and "Ping from WAN:" set to "Enable". At the bottom are "Save" and "Cancel" buttons.

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



The screenshot shows a dialog box titled "WAN Port Settings". It contains several input fields and a dropdown menu: "WAN Connection Type:" set to "Static Mode (fixed IP)", "IP Address Assigned by Your ISP:" with value "210.66.155.70", "IP Subnet Mask:" with value "255.255.255.224", "ISP Gateway IP Address:" with value "210.66.155.94", "Primary DNS Server:" with value "8.8.4.4", and "Secondary DNS Server:" with value "8.8.8.8". At the bottom are "Save" and "Cancel" buttons.

Step 5. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable. In a remote computer, enter the DDNS host name as the figure shown below. Then, you should be able to login the WMC251 remotely.



Example of Easy DDNS Settings:



This service is not required to register any DDNS account.

Please refer to the procedure listed as follows to configure using “Enable Easy DDNS”service.

Step 1. Select “Enable Easy DDNS” to use your selected DDNS service.

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

Dynamic DNS Settings

You may configure your ddns here using standard Dynamic DNS services.

DDNS option:

Easy Domain Name:

DDNS Settings

Dynamic DNS Provider:

Account:

Password:

DDNS:

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

Remote Management Settings

Remote management (via WAN):

Ping from WAN:

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

WAN Port Settings

WAN Connection Type:

IP Address Assigned by Your ISP:

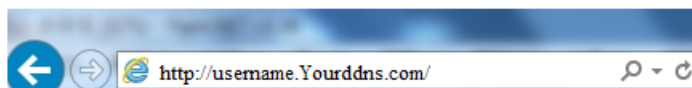
IP Subnet Mask:

ISP Gateway IP Address:

Primary DNS Server:

Secondary DNS Server:

Step 6. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable. In a remote computer, enter the Easy Domain Name displayed in [Step 1](#). Then, you should be able to login the WMC251 remotely.



5.1.12 Remote Management

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

Figure 5-24 Remote Management

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

5.1.13 DHCP Server Settings

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

Figure 5-25 DHCP Server Settings

Object	Description
--------	-------------

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

5.1.14 DMZ Settings

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

Figure 5-26 DMZ Settings

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

5.1.15 Virtual Server Settings

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

Virtual Server Settings

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

Virtual Server:

Protocol:

IP Address:

Port Range: -

Comment:

Figure 5-27 Virtual Server Settings

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

5.1.16 IP Filtering Settings

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

IP Filtering Settings

Filtering:

Protocol:

IP Address:

Comment:

Figure 5-28 IP Filtering Settings

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

5.1.17 Port Filtering Settings

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

Figure 5-29 Port Filtering Settings

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

5.1.18 MAC Filtering Settings

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

Figure 5-30 Mac Filtering Settings

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

5.1.19 Bandwidth Control

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

Figure 5-31 Bandwidth Control Settings

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

5.1.20 SNMP

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

SNMP Settings

SNMP

Read Community:

Write Community:

Trap IP 1:

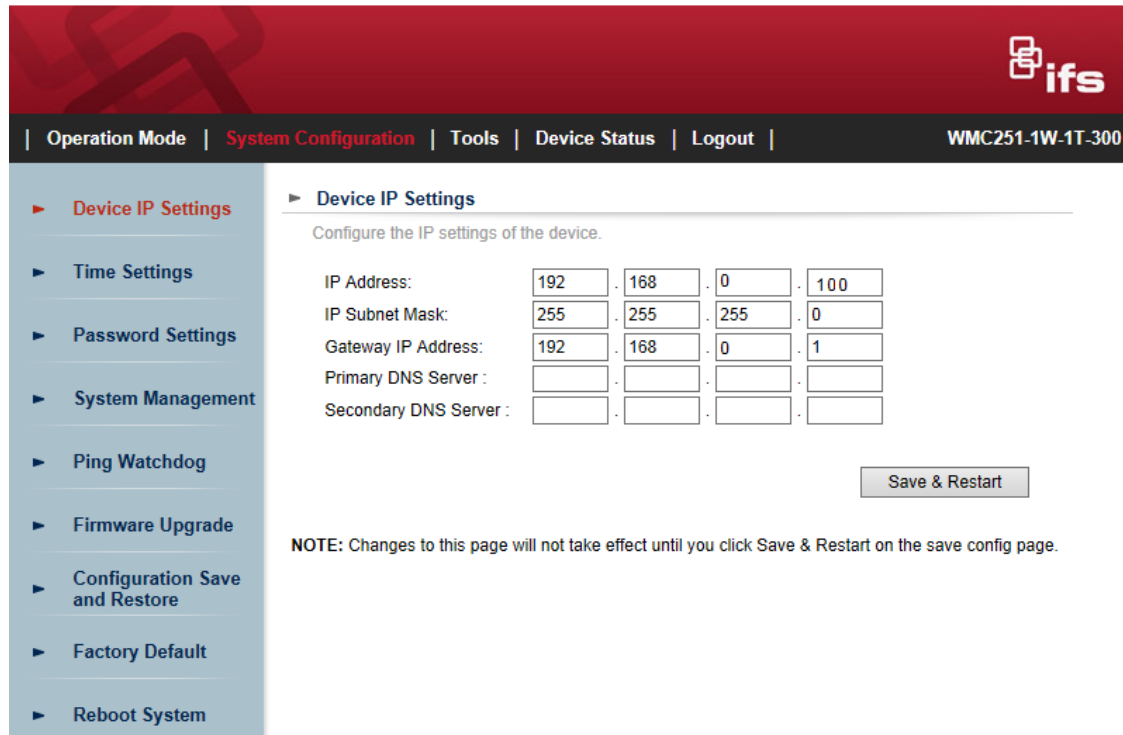
Trap Community 1:

Figure 5-32 SNMP Settings

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

5.2 System Configuration

On this page, you can configure the system of the WMC251, including IP settings, Time settings, Password settings, System management, Ping Watchdog, Firmware upgrade, Configuration save and restore, Factory default, Reboot and Schedule reboot.

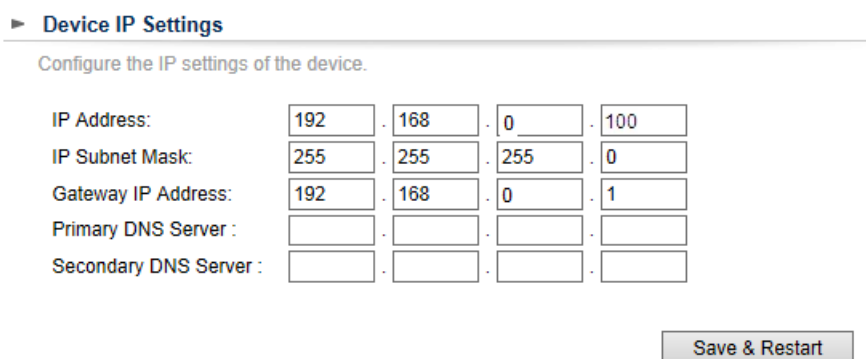


The screenshot shows the WMC251 web interface. The top navigation bar includes 'Operation Mode', 'System Configuration' (highlighted), 'Tools', 'Device Status', and 'Logout'. The device model 'WMC251-1W-1T-300' is displayed in the top right. A left sidebar contains menu items: 'Device IP Settings' (highlighted), 'Time Settings', 'Password Settings', 'System Management', 'Ping Watchdog', 'Firmware Upgrade', 'Configuration Save and Restore', 'Factory Default', and 'Reboot System'. The main content area is titled 'Device IP Settings' and contains the instruction 'Configure the IP settings of the device.' Below this are input fields for IP Address (192.168.0.100), IP Subnet Mask (255.255.255.0), Gateway IP Address (192.168.0.1), Primary DNS Server, and Secondary DNS Server. A 'Save & Restart' button is located at the bottom right of the form. A note below the form states: 'NOTE: Changes to this page will not take effect until you click Save & Restart on the save config page.'

Figure 5-33 System Configuration default page

5.2.1 Default IP Settings

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



The screenshot shows the 'Device IP Settings' page. It features the same navigation and sidebar as Figure 5-33. The main content area is titled 'Device IP Settings' and contains the instruction 'Configure the IP settings of the device.' Below this are input fields for IP Address (192.168.0.100), IP Subnet Mask (255.255.255.0), Gateway IP Address (192.168.0.1), Primary DNS Server, and Secondary DNS Server. A 'Save & Restart' button is located at the bottom right of the form.

Figure 5-34 Default IP Settings

The page includes the following fields:

Object	Description
• IP Address	WMC251's LAN IP. The default is 192.168.0.100 . You can change it according to your needs.
• IP Subnet Mask	WMC251's LAN subnet mask.

- **Gateway IP Address** The Gateway IP address of WMC251.
- **Primary DNS Server** Enter the DNS server. The default is 8.8.4.4.
- **Secondary DNS Server** Enter the DNS server. The default is 8.8.8.8.

5.2.2 Time Settings

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

► **Time Settings**

Enable NTP

Please select a type for accessing NTP server.

Server name:

NTP request interval : hours. (range: 1-300, default 24)

Local time zone:

Local date and time:

: :

HH MM SS

Figure 5-35 Time Settings

Object	Description
• Enable NTP	Enable it to support NTP (Network Time Protocol) for automatic time and date setup.
• Server Name	Enter the host name or IP address of the time server if you wish.
• NTP Request Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.
• Local Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.
• Local Date and Time	Set the access point's date and time manually.

5.2.3 Password Settings

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

► Username and Password Settings

Change Username and Password

To change your administrative password, enter your current password and then the new password twice.

Username:

Current Password:

New Password:

Re-enter New Password:

Save & Change

Figure 5-36 Password Settings

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

5.2.4 System Management

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

► System Management

Device Name:

POE Pass Through
 Enable POE Pass Through

UPnP
 Enable UPnP

Syslog
 Enable Syslog

IGMP
 Enable IGMP

Save & Start

Figure 5-37 System Management

Object	Description
• Device Name	Enter a name for this access point. Default is WMC251 .
• POE Passthrough	Enable the POE Passthrough function. ※ When the option “ Enable POE Passthrough ” in the System Management page is checked, the LAN2 can supply passive PoE power to the second WMC251 or WMC251 through the LAN 2.
• UPnP	Check to enable the UPnP function. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. This option is only available in AP Router mode.
• Syslog	Check to enable Syslog function.
• IGMP	Check to enable the IGMP Proxy function. This option is only available in AP Router mode.

5.2.5 Ping Watchdog

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

► **Ping Watchdog**

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

Ping Watchdog: Enable Disable

IP Address 1: . . .

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

Failed tries: (default is 2 tries)

Action:

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

Figure 5-38 Ping Watchdog

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

• Action	System will reboot when failing to ping the IP.
-----------------	---

5.2.6 Firmware Upgrade

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

► **Firmware Upgrade**

Select the firmware file by clicking Browse, and click UPGRADE.

WARNING : Don't use wireless connection to upload the firmware, To avoid system crashes.

NOTE:

1. Do not power off the router while upgrading the firmware.
1. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path.

Figure 5-39 Firmware Upgrade

Object	Description
• Browse	Click Browse to select the firmware file, and click Upgrade to upgrade the firmware.

5.2.7 Configuration Save and Restore

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

► **Configuration Save and Restore**

Click SAVE to save the configuration to a management host.

Select the text configure file by clicking Browse, then click RESTORE.

NOTE:
Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path.

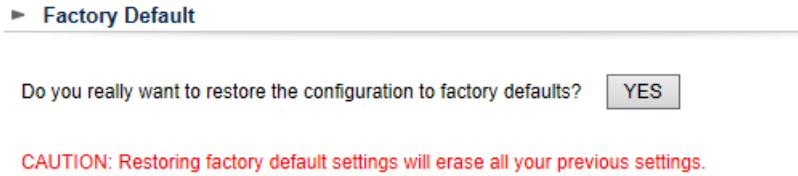
Figure 5-40 Configuration Save and Restore

Object	Description
• SAVE	Click SAVE to save the configuration to a management host.
• Browse	Click Browse to select the configuration file, and click Restore to restore the configuration file.

5.2.8 Factory Default

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

Press **YES** to restore to factory default.



► **Factory Default**

Do you really want to restore the configuration to factory defaults?

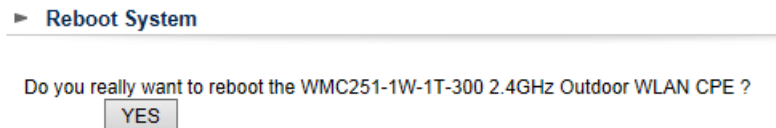
CAUTION: Restoring factory default settings will erase all your previous settings.

Figure 5-41 Factory Default

5.2.9 Reboot System

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

Press **YES** to reboot the system.



► **Reboot System**

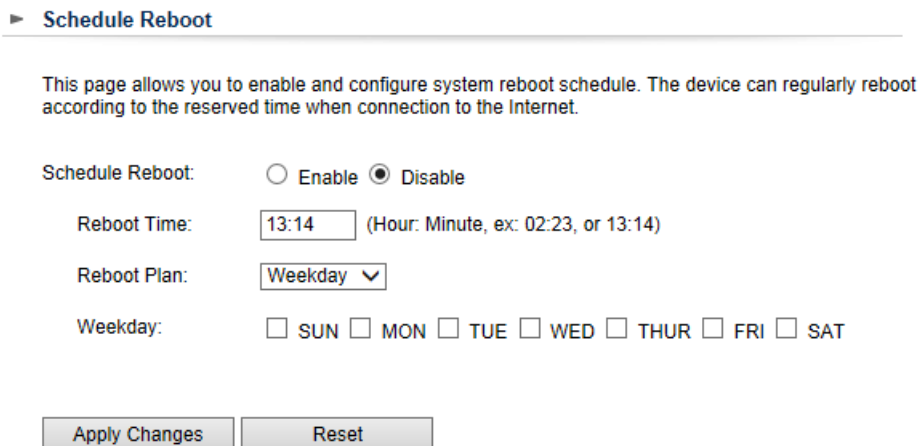
Do you really want to reboot the WMC251-1W-1T-300 2.4GHz Outdoor WLAN CPE ?

Figure 5-42 Reboot System

5.2.10 Schedule Reboot

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

This page allows you to enable and configure system reboot schedule. The device can regularly reboot according to the reserved time when connecting to the Internet.



► **Schedule Reboot**

This page allows you to enable and configure system reboot schedule. The device can regularly reboot according to the reserved time when connection to the Internet.

Schedule Reboot: Enable Disable

Reboot Time: (Hour: Minute, ex: 02:23, or 13:14)

Reboot Plan: ▼

Weekday: SUN MON TUE WED THUR FRI SAT

Figure 5-43 Schedule Reboot

Object	Description
• Schedule Reboot	Enable or Disable this function.
• Reboot Time	Enter the time that you want to reboot this device.
• Reboot Plane	Select Weekday to reboot in the day you choose or Every day .
• Weekday	Select the day that you want to reboot.



1. This setting will only take effect when the Internet connection is accessible and the GMT time is configured correctly.
2. You must select at least one day when choosing “**Weekday**” as your reboot plan.
3. When choosing “**Every day**” as your reboot plan, the “**Weekday**” will be grayed out (disabled), which means **Every day** will auto reboot at the time that you schedule.

■ Example of how to configure **Schedule Reboot**. Please take the following Steps:

Before configuring schedule reboots, please ensure the Internet connection is accessible and the GMT time is configured correctly according to **NTP Settings** page.

Step 1. Enable the “Schedule Reboot”.

Step 2. Enter the Reboot Time (24-hour format) to enable this function to take effect. For example, if you want this function to work at 23:00 every Sunday, choose "Weekday" in the Reboot Plan field.

► **Schedule Reboot**

This page allows you to enable and configure system reboot schedule. The device can regularly reboot according to the reserved time when connection to the Internet.

Schedule Reboot: Enable Disable

Reboot Time: (Hour: Minute, ex: 02:23, or 13:14)

Reboot Plan: ▼

Weekday: SUN MON TUE WED THUR FRI SAT

Figure 5-44 Schedule Reboot - Example

Step 3. Click the “Apply Changes” button to take this function effect.

5.3 Tools

5.3.1 Network Ping

Click “Tools” → “Network Ping” and the following page will be displayed.

Ping is a network tool used to test whether a particular host is reachable across an IP network.

Enter the IP, Ping Count, and click “**Ping**” to diagnostic your internet connection.

► **Network Ping**

Please assign an IP address to run Ping function against.

Destination IP Address:

Ping Number:

Ping Packet Size: Bytes

Ping Result:

```
PING 192.168.0.100 (192.168.0.100) 56 data bytes
64 bytes from 192.168.0.100 : icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 192.168.0.100 : icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 192.168.0.100 : icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 192.168.0.100 : icmp_seq=0 ttl=64 time=0.2 ms
--192.168.0.100 ping statistics
```

Figure 5-45 Network Ping

5.3.2 Network Traceroute

Click “Tools” → “Network Traceroute” and the following page will be displayed.

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It can help identify connection problems. Enter the IP and click “Traceroute” to diagnostic your internet connection.

► Network Traceroute

Please assign an IP address to run Traceroute function against.

Destination IP Address:

Max hop:

Result:

Host	Response Time
1 192.168.0.100 (192.168.0.100	0.26ms 0.222ms 0.176ms

Figure 5-46 Network Traceroute

5.4 Device Status

The screenshot displays the 'Device Status' page of the IFS WMC251-1W-1T-300. The page is divided into a left-hand navigation menu and a main content area. The navigation menu includes 'Device Information' (highlighted), 'Wireless Information', 'LAN Information', 'Internet Information', 'Wireless Client Table', and 'System Log'. The main content area is titled 'Device Information' and contains several sections:

- Device Information:** A list of system parameters including Firmware Version (1.0.1), Device IP (192.168.0.100), Device MAC (A8:F7:E0:05:FD:ED), Gateway IP (192.168.0.1), DNS IP, Wireless MAC (A8:F7:E0:05:FD:EF), Uptime (0 day 0:29:46), and CPU Loading (0%).
- Memory Information:** A table showing memory usage with progress bars and values.

Category	Percentage	Value
Total Available:	73%	47820KB / 65536KB
Used:	15%	7160KB / 47820KB
Free:	85%	40660KB / 47820KB
Buffers:	0%	0KB / 7160KB
Cached:	13%	904KB / 7160KB
- ARP Table:** A table listing network connections.

IP Address	MAC Address	Interface
192.168.0.100	00:14:22:ef:5e:74	br0

Figure 5-47 Device Status

5.4.1 Device Information

Click “Device Status” → “Device Information” and the following page will be displayed.

The screenshot shows the IFS management interface for device WMC251-1W-1T-300. The left sidebar contains navigation options: Device Information (selected), Wireless Information, LAN Information, Internet Information, Wireless Client Table, and System Log. The main content area is titled 'Device Information' and contains the following data:

- Firmware Version:** 1.0.1 (May 12 2015)
- Device IP:** 192.168.0.100
- Device MAC:** A8:F7:E0:05:FD:ED
- Gateway IP:** 192.168.0.1
- DNS IP:**
- Wireless MAC:** A8:F7:E0:05:FD:EF
- Uptime: (dd:hh:mm:ss)** 0 day 0:29:46
- CPU Loading:** 0%

Memory Information

Total Available:	73%	47820KB / 65536KB
Used:	15%	7160KB / 47820KB
Free:	85%	40660KB / 47820KB
Buffers:	0%	0KB / 7160KB
Cached:	13%	904KB / 7160KB

ARP Table

IP Address	MAC Address	Interface
192.168.0.100	00:14:22:ef:5e:74	br0

Figure 5-48 Device Information

The page includes the following fields:

Object	Description
• Firmware Version	Displays current F/W version.
• Device IP	Displays IP of AP.
• Device MAC	Displays AP's LAN MAC address.
• Gateway IP	Displays Gateway IP of AP.
• DNS IP	Displays DNS IP of AP.
• Wireless MAC	Displays AP's Wireless MAC address.
• Uptime	Display the uptime of AP.
• CPU Loading	Display the CPU loading of AP.

5.4.2 Wireless Information

Click “Device Status” → “Wireless Information” and the following page will be displayed.

The screenshot shows a web interface with a red header and a navigation menu. The main content area is titled "Wireless Information" and contains the following data:

Operation Mode:	Wireless ISP
Physical Address:	A8:F7:E0:05:FD:EF
Remote AP SSID:	WMC251-300
Band:	11NGHT20
Radio Channel:	Auto Channel
Remote Encryption:	NONE
Transmit Power:	27 dBm

Below this is a section for "WLAN Statistics" with a table:

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	577024	2576	0

Figure 5-49 Wireless Information

The page includes the following fields:

Object	Description
• Operation Mode	Displays current Operation Mode.
• Physical address	Displays AP's Wireless MAC address.
• SSID	It is the wireless network name. The default SSID is WMC251 .
• Band	Display operating channel width which is 11NG HT20 or 11NG HT40 .
• Radio Channel	Display the channel you would like to use. The channel range will be changed by selecting different domain.
• Wireless Encryption	Display the encryption type that you would like to use.
• Transmit Power	Display the TX power that you would like to use.

5.4.3 LAN Information

Click “Device Status” → “LAN Information” and the following page will be displayed.

The screenshot shows a web interface with a left sidebar containing menu items: Device Information, Wireless Information, LAN Information (highlighted), Internet Information, Wireless Client Table, and System Log. The main content area is titled 'LAN Information' and displays the following configuration details:

- Physical Address: A8:F7:E0:05:FD:ED
- IP Address: 192.168.0.100
- Network Mask: 255.255.255.0
- Default Gateway: 192.168.0.1
- DHCP Server: Enabled
- DHCP Start IP Address: 192.168.1.100
- DHCP Finish IP Address: 192.168.1.200

Below the configuration details is a section titled 'LAN Statistics' with a table showing the following data:

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

Figure 5-50 LAN Information

The page includes the following fields:

Object	Description
• Physical Address	Displays AP's LAN MAC address.
• IP Address	Displays IP of AP.
• Network Mask	Displays Network Mask of AP.
• Default Gateway	Displays Gateway IP of AP.
• DHCP Server	Enable or Disable DHCP server.
• DHCP Start IP Address	Enter the starting IP address for the DHCP server's IP assignment.
• DHCP Finish IP Address	Enter the ending IP address for the DHCP server's IP assignment.

5.4.4 Wireless Client Table

Click "Device Status" → "Wireless Client Table" and the following page will be displayed.

The screenshot shows a web interface with a top navigation bar containing: Operation Mode | System Configuration | Tools | Device Status | Logout | WMC251-1W-1T-300. The left sidebar contains menu items: Device Information, Wireless Information, LAN Information, Internet Information, Wireless Client Table (highlighted), and System Log. The main content area is titled 'Wireless Client Table' and displays a table with the following columns:

No.	Mac Address	Connection Speed(Mbps)	Signal Strength (dB)
-----	-------------	------------------------	----------------------

Figure 5-51 Wireless Client Table

The page includes the following fields:

Object	Description
• No.	Displays the number of connecting device.
• Mac Address	Displays Mac address of AP.
• Connection Speed	Displays connection speed of device.
• Signal Strength	Display signal strength of device. The signal strength between “-30 and 70” can setup a reliable connection.

5.4.5 System Log

Choose menu “Device Status → “System Log” to view the logs of the Wireless AP.

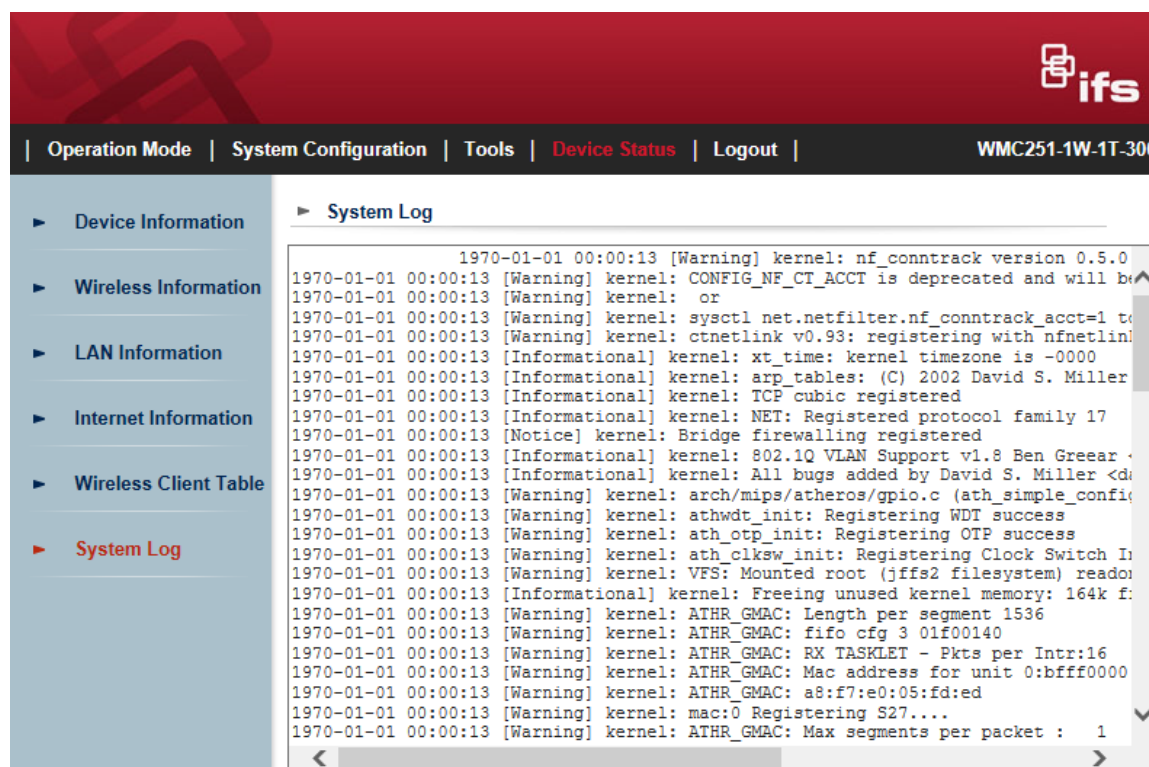


Figure 5-52 System Log

5.5 Logout

Select **Logout** to logout the system.

Figure 5-53 Logout



Figure 5-54 Re-login

Appendix A: Troubleshooting

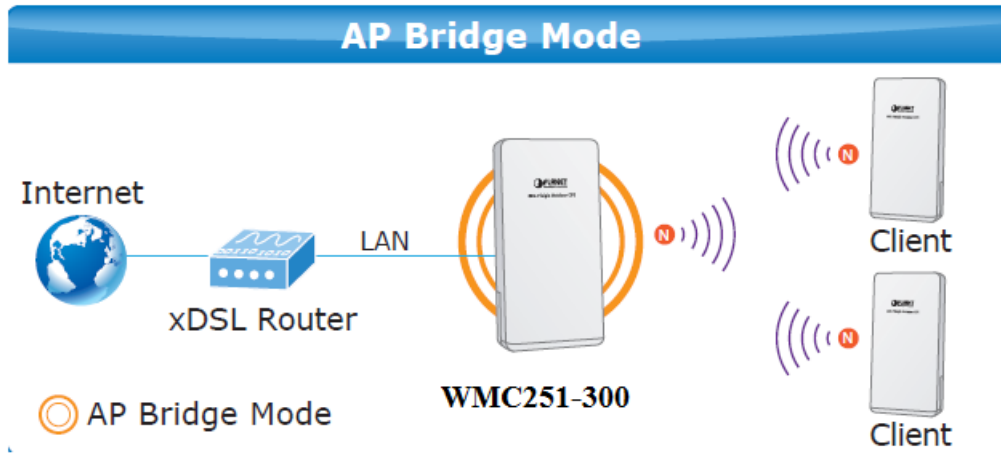
If you found the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the IFS, - Tech Support for help. Some problems can be solved by yourself within very short time.

Scenario	Solution
The AP is not responding to me when I want to access it by web browser.	<ol style="list-style-type: none"> Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be correctly and firmly inserted to the AP. If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered. You must use the same IP address section that AP uses. Are you using MAC or IP address filter? Try to connect the AP by another computer and see if it works; if not, please reset the AP to the factory default settings (Press the 'reset' button for over 10 seconds). If you did a firmware upgrade and this happens, contact the IFS, - Tech Support for help. If all the solutions above don't work, contact the IFS, - Tech Support for help.
I can't get connected to the Internet.	<ol style="list-style-type: none"> Check the Internet connection status from the router that is connected with the AP. Please be patient. Sometimes Internet is just that slow. If you have connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. Check PPPoE / L2TP / PPTP user ID and password in your router again. Call your Internet service provider and check if there's something wrong with their service. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. Try to reset the AP and try again later. Reset the device provided by your Internet service provider. Try to use IP address instead of hostname. If you can use IP address to communicate with a remote server, but can't use hostname, please check DNS setting.
I can't locate my AP by my wireless device.	<ol style="list-style-type: none"> 'Broadcast ESSID' set to off? The antenna is properly secured. Are you too far from your AP? Try to get closer.

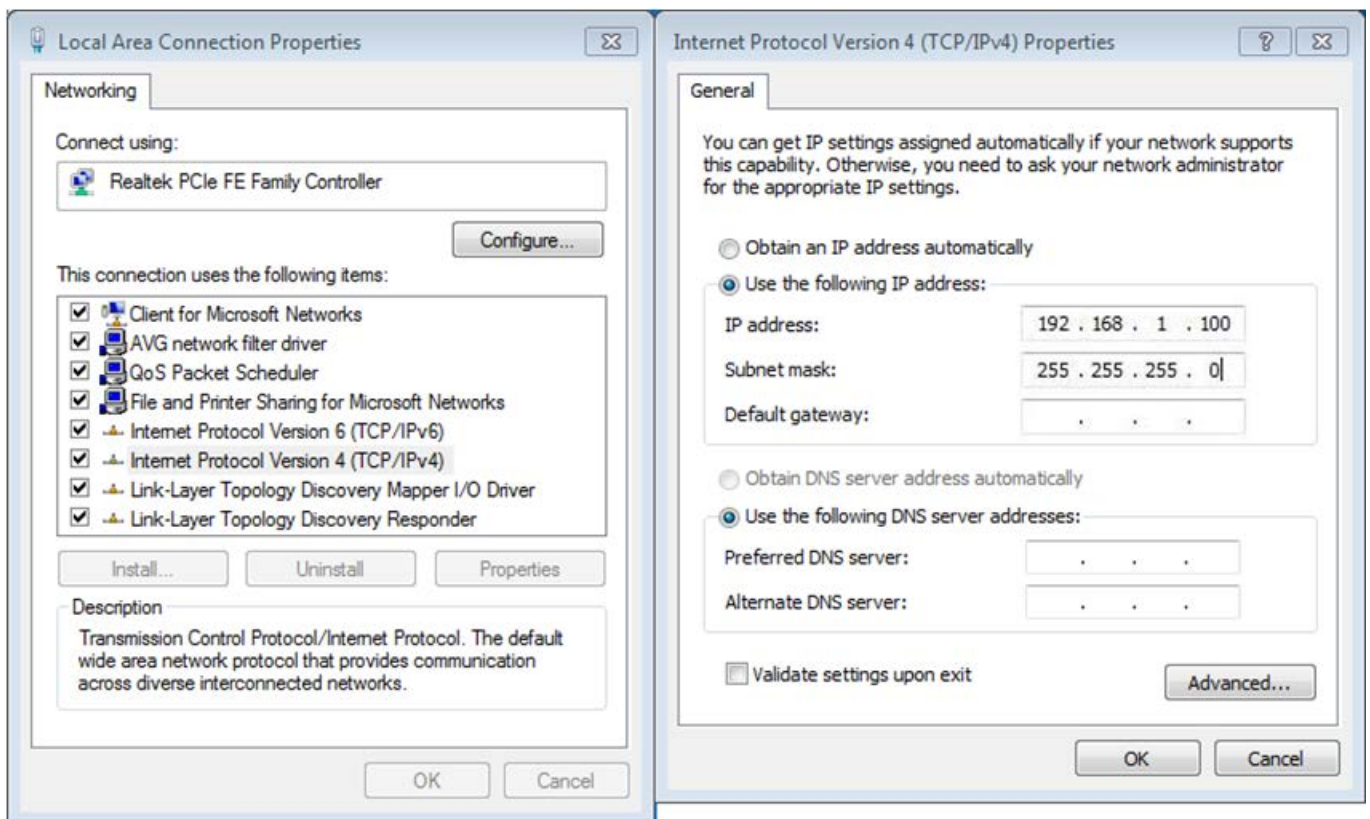
	d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	<ul style="list-style-type: none"> a. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes; try to be patient. c. Try to reset the AP and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. e. If this never happens before, call your Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; The password is wrong.	<ul style="list-style-type: none"> a. Make sure you're connecting to the correct IP address of the AP. b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The AP becomes hot	<ul style="list-style-type: none"> a. This is not a malfunction, if you can keep your hand on the AP's case. b. If you smell something wrong or see the smoke coming out from AP or A/C power adapter, please disconnect the AP and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer for help.

Q1: How to set up the AP Client Connection

Topology:



Step 1. Use static IP in the PCs that are connected with AP-1 (Site-1) and AP-2 (Site-2). In this case, Site-1 is “192.168.0.100”, and Site-2 is “192.168.1.200”.



Step 2. In AP-1, go to “**Operation Mode**” to configure it to **Access Point** Mode.

- ※ **You can also configure it in “AP Router” mode if you want to connect the WAN port of the AP to the internet directly.**

▶ **Operation Mode**

Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.

Mode		Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	<input type="button" value="Setup"/>	Access Point	LAN+LAN
<input type="radio"/> Client	<input type="button" value="Setup"/>	Client	LAN+LAN
<input type="radio"/> WDS AP	<input type="button" value="Setup"/>	WDS Access Point	LAN+LAN
<input type="radio"/> WDS Client	<input type="button" value="Setup"/>	WDS Client	LAN+LAN
<input type="radio"/> AP Router	<input type="button" value="Setup"/>	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	<input type="button" value="Setup"/>	Wireless ISP	LAN+LAN

Step 3. Click “**Setup**” to configure the following parameters and then click **Save & Restart** to save the settings.

- 1) **Network ID (SSID):** set to a unique value
- 2) **Channel:** set to a fixed one
- 3) **Security Setting:** strongly suggested to configure it.

In this case, we configure it to WPA2-PSK, AES

▶ **Operation Mode**

Access Point

▶ **Operation Mode Settings**

Regulatory Domain: United States ▼

Network ID (SSID): WMC252-6325-Dai

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Radio Mode: 2G 11NG HT20 ▼

Channel: 6 -2437MHz ▼

Data Rate: Auto ▼

Security Setting: Setup

Transmit Power: 27 dbm ▼

Transmit Distance: 1 Km ▼

TDMA: Disable ▼

Advanced Settings: Setup

Access Control: Setup

Security Settings

Select Encryption: WPA2 ▼

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key: 12345678

Save
Cancel

Step 4. In AP-2, modify the default IP to the same IP range but different from AP-1.

In this case, the IP is changed to **192.168.1.252**.

▶ Device IP Settings

Configure the IP settings of the device.

IP Address:	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="252"/>
IP Subnet Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway IP Address:	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="253"/>
Primary DNS Server :	<input type="text" value="8"/>	<input type="text" value="8"/>	<input type="text" value="4"/>	<input type="text" value="4"/>
Secondary DNS Server :	<input type="text" value="8"/>	<input type="text" value="8"/>	<input type="text" value="8"/>	<input type="text" value="8"/>

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

Step 5. In AP-2, configure it in “**Client**” mode and click “**Setup**”.

▶ Operation Mode

Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.

Mode		Radio	Ethernet Port
<input type="radio"/> Access Point	<input type="button" value="Setup"/>	Access Point	LAN+LAN
<input checked="" type="radio"/> Client	<input type="button" value="Setup"/>	Client	LAN+LAN
<input type="radio"/> WDS AP	<input type="button" value="Setup"/>	WDS Access Point	LAN+LAN
<input type="radio"/> WDS Client	<input type="button" value="Setup"/>	WDS Client	LAN+LAN
<input type="radio"/> AP Router	<input type="button" value="Setup"/>	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	<input type="button" value="Setup"/>	Wireless ISP	LAN+LAN

Step 6. Click **“Setup”** and then click **Site Survey** to find AP-1.

► Operation Mode Settings

Regulatory Domain: Europe

Remote AP SSID: WMC251-300 **Site Survey**

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Lock to AP MAC: 00:00:00:00:00:00

Radio Mode: 2G 11NG HT40

Channel: Auto Channel

Data Rate: Auto

Security Setting: Setup

Transmit Power: 27 dbm

Transmit Distance: 1 Km

TDMA: Disable

Advanced Settings: Setup

Access Control: Setup

Step 7. Site Survey results

WMC251-1W-1T-300 2.4GHz Outdoor WLAN CPE - Internet Explorer

http://192.168.0.100/sts_sitesvy.asp

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
1	The Lounge	FA:8F:CA:7E:C4:CC	6	-86 dBm	none
2	007port672726	0C:F5:A4:EF:4C:14	1	-74 dBm	Yes
3	TWW-3130_502719431	54:E4:BD:35:D2:8B	1	-64 dBm	none
4	TWW-3106_484743818	00:95:69:09:E4:81	1	-73 dBm	Yes
5	007navo668226	0C:F5:A4:EF:4C:13	1	-75 dBm	Yes
6	TWW-3104_483467653	A0:F4:59:A8:F4:F7	1	-72 dBm	none
7	007port672726	34:A8:4E:C4:2A:E4	11	-71 dBm	Yes
8	007navo668226	0C:F5:A4:EF:48:B3	11	-62 dBm	Yes
9	007port672726	0C:F5:A4:EF:48:B4	11	-62 dBm	Yes
10	007navo668226	34:A8:4E:C4:2A:E3	11	-71 dBm	Yes
11	wmc251150II	A8:F7:E0:10:78:E5	11	-84 dBm	none

Step 8. Click **“SET SECURITY”** to configure the Pre-Shared Key and then click **“Save”** to close the window.

WMC251-1W-1T-300 2.4GHz Outdoor WLAN CPE - Internet Explorer
http://192.168.1.251/security.asp

Security Settings

Select Encryption: WPA

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key: 12345678

Save Cancel

Step 9. Click **“OK”** and **“Save & Restart”** to apply the setting.

Message from webpage

? You already changed the settings, do you need to restart the device?

OK Cancel

Step 10. In AP-1, go to **“Device Status-> Wireless Client Table”** to check whether AP-2 should be in the list.

ifs

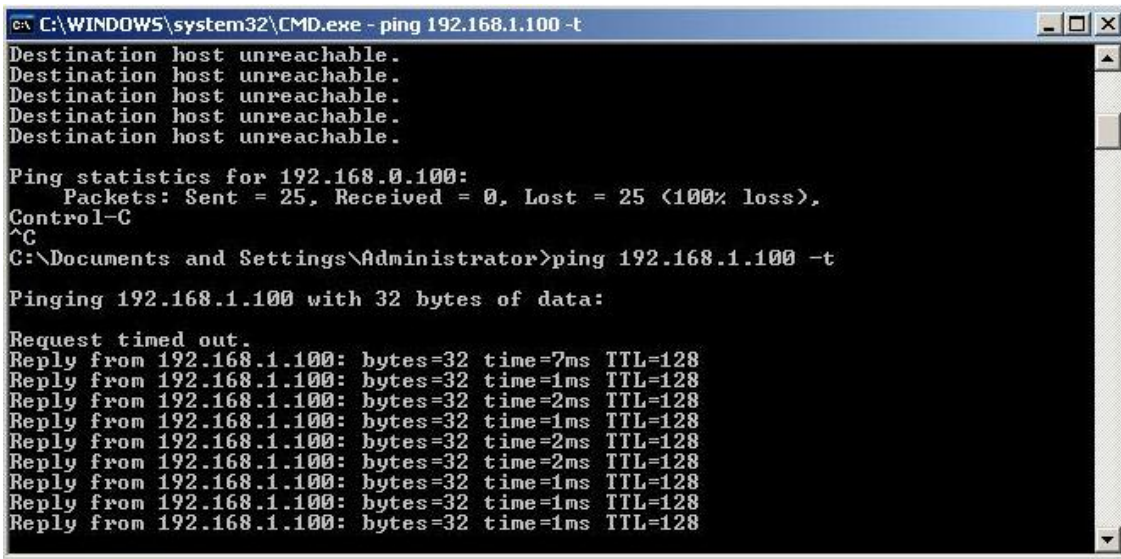
Operation Mode | System Configuration | Tools | Device Status | Logout | WMC251-1W-1T-300

- ▶ Device Information
- ▶ Wireless Client Table
- ▶ Wireless Information
- ▶ LAN Information
- ▶ Internet Information
- ▶ System Log

No.	Mac Address	Connection Speed(Mbps)	Signal Strength (dB)
-----	-------------	------------------------	----------------------

Step 11. Use command line tool to ping each other to ensure the link is successfully established.

From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.0.100.



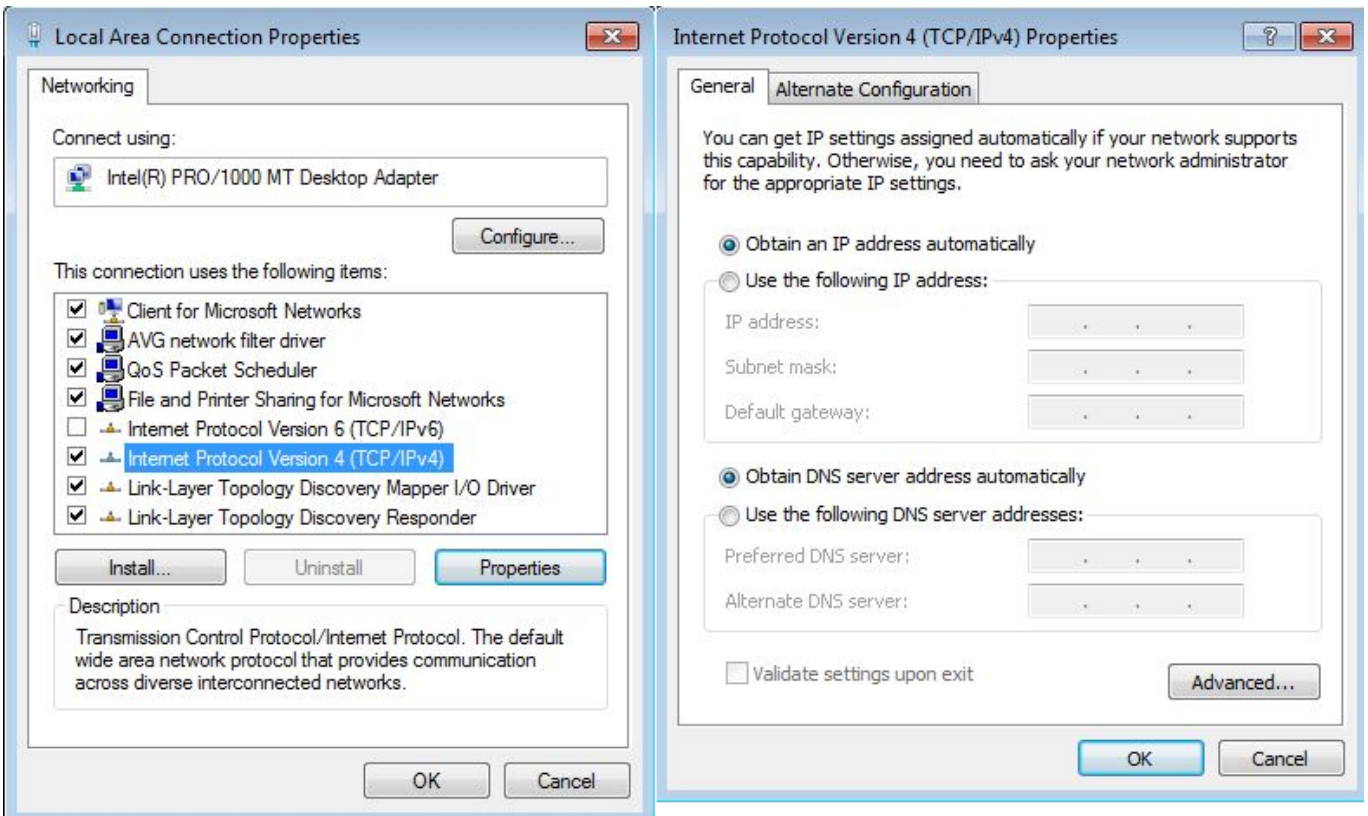
```
C:\WINDOWS\system32\CMD.exe - ping 192.168.1.100 -t
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

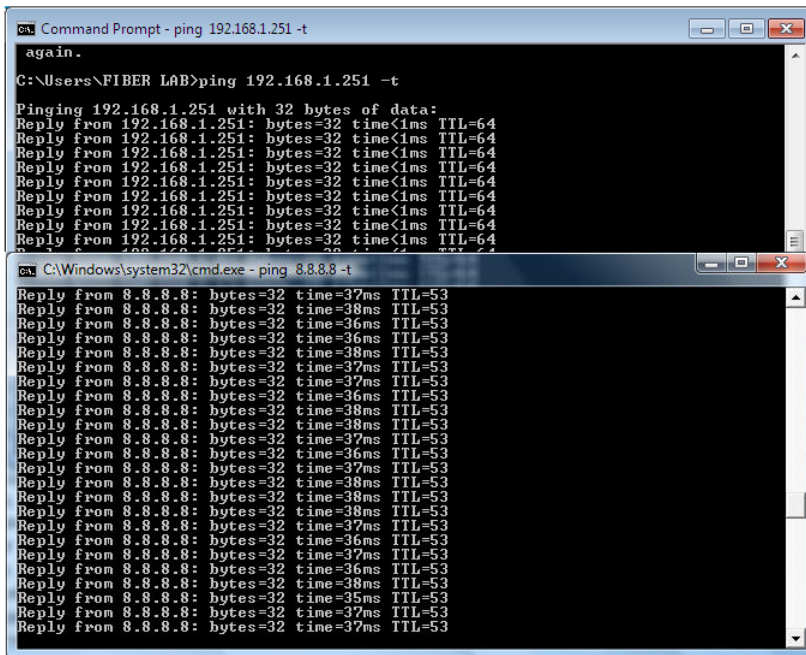
Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

Step 12. Configure the TCP/IP settings of Site-2 to “Obtain an IP address automatically”.



Step 13. Use command line tool to ping the DNS (e.g. Google) to ensure Site-2 can access internet through the wireless connection.



The image shows two overlapping screenshots of Windows Command Prompt windows. The top window has the title bar 'Command Prompt - ping 192.168.1.251 -t' and shows the command 'ping 192.168.1.251 -t' being executed. The output consists of multiple lines of 'Reply from 192.168.1.251: bytes=32 time<1ms TTL=64'. The bottom window has the title bar 'C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t' and shows the command 'ping 8.8.8.8 -t' being executed. The output consists of multiple lines of 'Reply from 8.8.8.8: bytes=32 time=37ms TTL=53'.

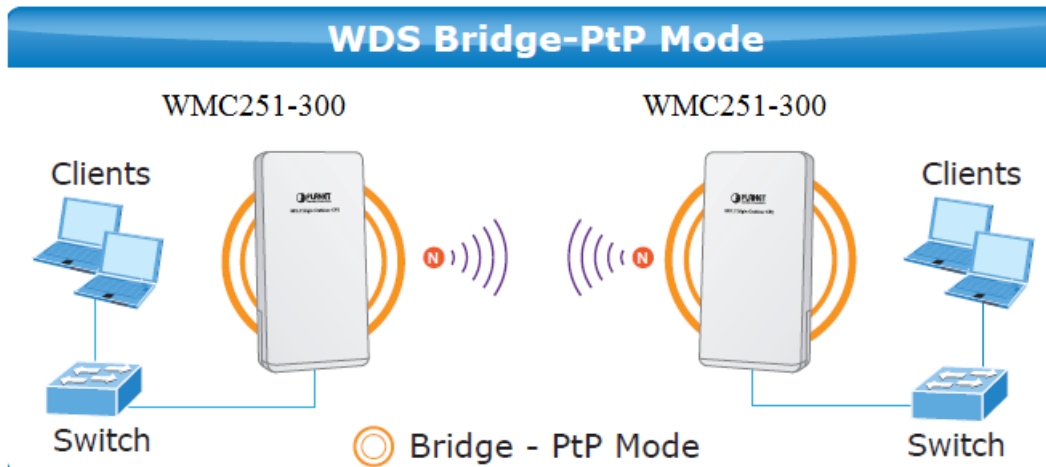
The attention of the following hints should be paid:



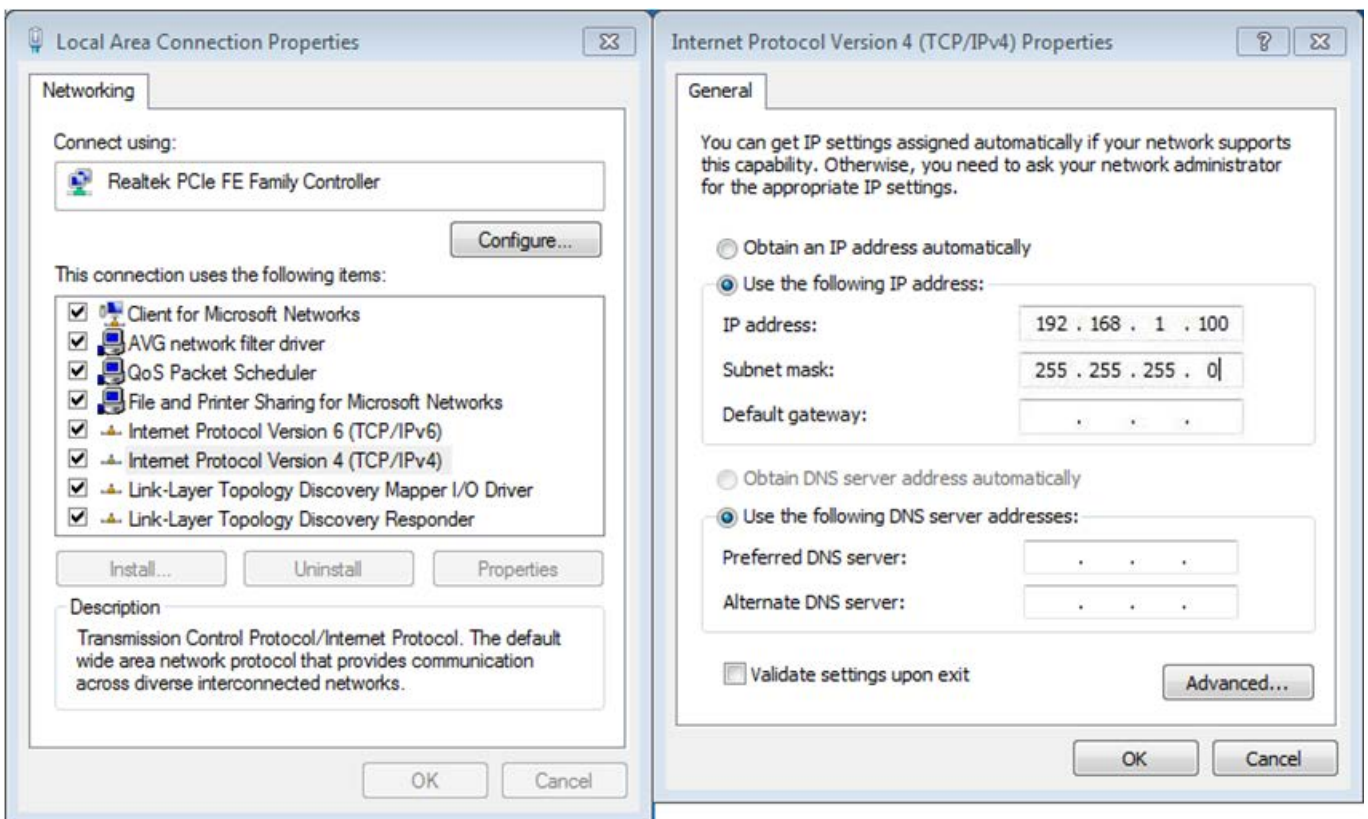
- 1) The encryption method must be the same as that of both sites if configured.
 - 2) Both sites should be Line-of-Sight.
 - 3) For the short distance connection less than 1km, please reduce the "Transmit power" of both sites.
 - 4) For the long distance connection over 1km, please adjust the "Transmit Distance" to the actual distance or double of the actual distance.
-

Q2: How to set up the WDS Connection

Topology:



Step 1. Use static IP in the PCs that are connected with WMC251-1 (Site-1) and WMC251-2 (Site-2). In this case, Site-1 is "192.168.0.100", and Site-2 is "192.168.1.200".



Step 2. In AP-1, go to “**Operation Mode**” to configure it **Access Point Mode**.

▶ **Operation Mode**

Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.

Mode		Radio	Ethernet Port
<input type="radio"/> Access Point	<input type="button" value="Setup"/>	Access Point	LAN+LAN
<input type="radio"/> Client	<input type="button" value="Setup"/>	Client	LAN+LAN
<input checked="" type="radio"/> WDS AP	<input type="button" value="Setup"/>	WDS Access Point	LAN+LAN
<input type="radio"/> WDS Client	<input type="button" value="Setup"/>	WDS Client	LAN+LAN
<input type="radio"/> AP Router	<input type="button" value="Setup"/>	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	<input type="button" value="Setup"/>	Wireless ISP	LAN+LAN

Step 3. Click “**Setup**” to configure the following parameters and then click **Save & Restart** to save the settings.

- 4) **Network ID (SSID):** set to a unique value
- 5) **Channel:** set to a fixed one
- 6) **Security Setting:** strongly suggested to configure it.

In this case, we configure it to WPA2-PSK, AES

▶ **Operation Mode Settings**

Regulatory Domain: Europe

Network ID (SSID): WMC251-300

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Radio Mode: 2G 11NG HT40

Channel: 6 -2437MHz

Data Rate: Auto

Security Setting:

Transmit Power: 27 dbm

Transmit Distance: 1 Km

TDMA: Disable

Advanced Settings:

Access Control:

Security Settings

Select Encryption:

Pre-Authentication: Personal (Pre-Shared Key) Enterprise (RADIUS)

Encryption Type: TKIP AES Auto

Pre-Shared Key:

Step 4. In AP-2, modify the default IP to the same IP range but different from AP-1.

In this case, the IP is changed to **192.168.1.252**.

► Device IP Settings

Configure the IP settings of the device.

IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

Primary DNS Server : . . .

Secondary DNS Server : . . .

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

Step 5. In AP-2, configure it in “Client” mode and click “Setup”.

► Operation Mode

Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.

Mode		Radio	Ethernet Port
<input type="radio"/> Access Point	<input type="button" value="Setup"/>	Access Point	LAN+LAN
<input type="radio"/> Client	<input type="button" value="Setup"/>	Client	LAN+LAN
<input type="radio"/> WDS AP	<input type="button" value="Setup"/>	WDS Access Point	LAN+LAN
<input checked="" type="radio"/> WDS Client	<input type="button" value="Setup"/>	WDS Client	LAN+LAN
<input type="radio"/> AP Router	<input type="button" value="Setup"/>	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	<input type="button" value="Setup"/>	Wireless ISP	LAN+LAN

Step 6. Click **Setup** and then click **Site Survey** to find AP-1.

► Operation Mode Settings

Regulatory Domain: Europe ▼

Remote AP SSID: WMC251-300 Site Survey

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Lock to AP MAC: 00:00:00:00:00:00

Radio Mode: 2G 11NG HT40 ▼

Channel: Auto Channel ▼

Data Rate: Auto ▼

Security Setting: Setup

Transmit Power: 27 dbm ▼

Transmit Distance: 1 Km ▼

TDMA: Disable ▼

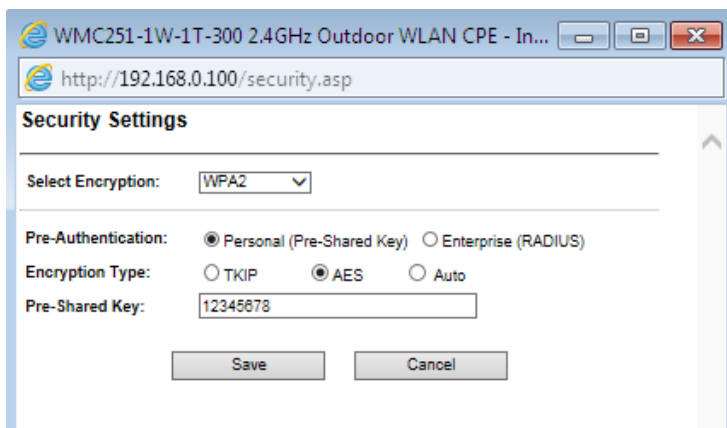
Advanced Settings: Setup

Access Control: Setup

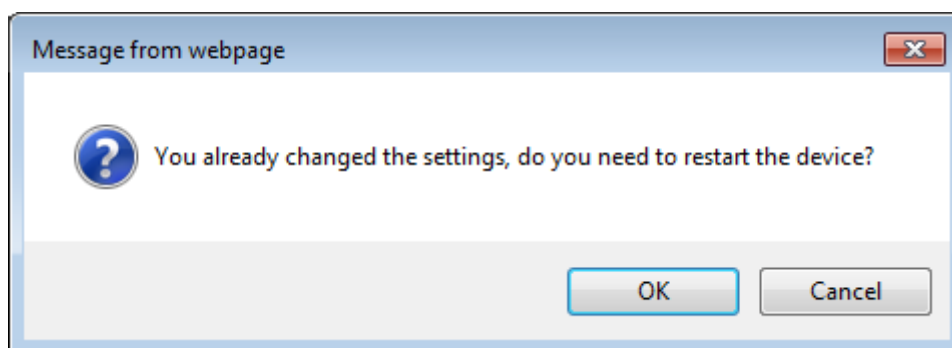
Step 7. Select AP-1 from the list.

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
1	The Lounge	FA:8F:CA:7E:C4:CC	6	-86 dBm	none
2	007port672726	0C:F5:A4:EF:4C:14	1	-74 dBm	Yes
3	TWW-3130_502719431	54:E4:8D:35:D2:88	1	-64 dBm	none
4	TWW-3106_484743818	00:95:89:09:E4:81	1	-73 dBm	Yes
5	007navo668226	0C:F5:A4:EF:4C:13	1	-75 dBm	Yes
6	TWW-3104_483467653	A0:F4:59:A8:F4:F7	1	-72 dBm	none
7	007port672726	34:A8:4E:C4:2A:E4	11	-71 dBm	Yes
8	007navo668226	0C:F5:A4:EF:48:B3	11	-62 dBm	Yes
9	007port672726	0C:F5:A4:EF:48:B4	11	-62 dBm	Yes
10	007navo668226	34:A8:4E:C4:2A:E3	11	-71 dBm	Yes
11	wmc251150II	A8:F7:E0:10:78:E5	11	-64 dBm	none

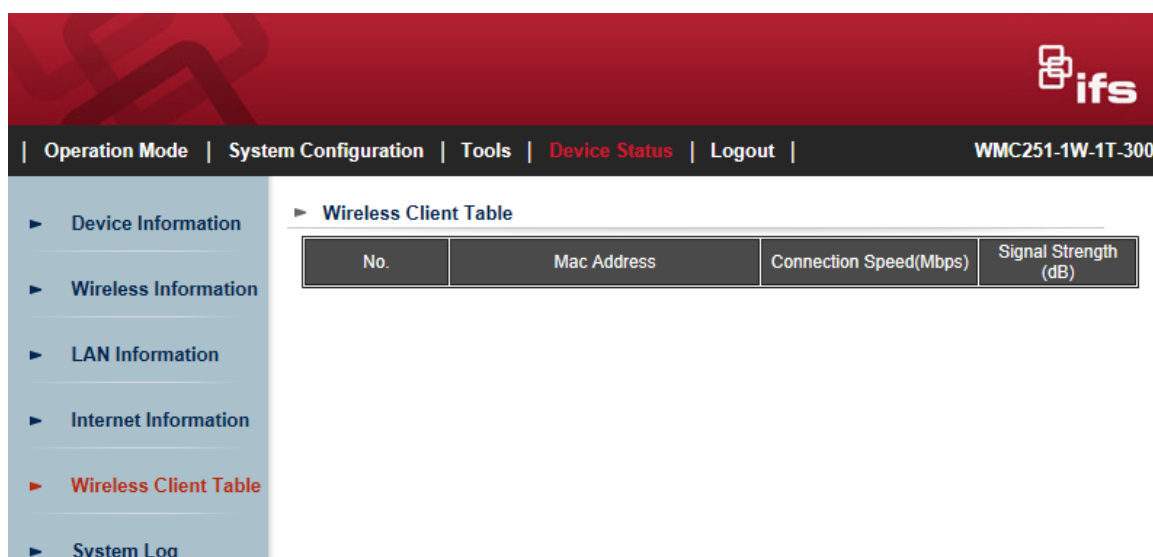
Step 8. Click **“SET SECURITY”** to configure the Pre-Shared Key and then click **“Save”** to close the window.



Step 9. Click **“OK”** and click **“Save & Restart”** to apply the setting.



Step 10. In AP-1, go to **“Device Status-> Wireless Client Table”** to check whether AP-2 should be in the list.



Step 11. Use command line tool to ping each other to ensure the link is successfully established. From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.100.

```
C:\WINDOWS\system32\CMD.exe - ping 192.168.1.100 -t
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

The attention of the following hints should be paid:



- 1) The encryption method must be the same as that of both sites if configured.
 - 2) Both sites should be Line-of-Sight.
 - 3) For the short distance connection less than 1km, please reduce the "Transmit power" of both sites.
 - 4) For the long distance connection over 1km, please adjust the "Transmit Distance" to the actual distance or double of the actual distance.
-

EC Declaration of Conformity

English	Hereby, IFS, - declares that this 300Mbps 802.11n Wireless Outdoor CPE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	Lietuviškai	Šiuo IFS, - , skelbia, kad 300Mbps 802.11n Wireless Outdoor CPE tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost IFS, - , tímto prohlašuje, že tato 300Mbps 802.11n Wireless Outdoor CPE splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	Magyar	A gyártó IFS, - , kijelenti, hogy ez a 300Mbps 802.11n Wireless Outdoor CPE megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	IFS, - , erklærer herved, at følgende udstyr 300Mbps 802.11n Wireless Outdoor CPE overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	Malti	Hawnhekk, IFS, - , jiddikjara li dan 300Mbps 802.11n Wireless Outdoor CPE jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC
Deutsch	Hiermit erkläre IFS, - , dass sich dieses Gerät 300Mbps 802.11n Wireless Outdoor CPE in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW i)	Nederlands	Hierbij verklaart, IFS, - Technology orporation , dat 300Mbps 802.11n Wireless Outdoor CPE in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eestikeeles	Käesolevaga kinnitab IFS, - , et see 300Mbps 802.11n Wireless Outdoor CPE vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma IFS, - , oświadcza, że 300Mbps 802.11n Wireless Outdoor CPE spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC”.
Ελληνικά	<i>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ, IFS, -, ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ 300Mbps 802.11n Wireless Outdoor CPE ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ</i>	Português	IFS, - , declara que este 300Mbps 802.11n Wireless Outdoor CPE está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, IFS, - , declara que 300Mbps 802.11n Wireless Outdoor CPE cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	Slovensky	Výrobca IFS, - , týmto deklaruje, že táto 300Mbps 802.11n Wireless Outdoor CPE je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, IFS, - , déclare que les appareils du 300Mbps 802.11n Wireless Outdoor CPE sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	Slovensko	IFS, - , s tem potrjuje, da je ta 300Mbps 802.11n Wireless Outdoor CPE skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente, IFS, - , dichiara che questo 300Mbps 802.11n Wireless Outdoor CPE è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	Suomi	IFS, - , vakuuttaa täten että 300Mbps 802.11n Wireless Outdoor CPE tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo IFS, - , apliecina, ka šī 300Mbps 802.11n Wireless Outdoor CPE atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, IFS, - , att denna 300Mbps 802.11n Wireless Outdoor CPE står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.