Quick Guide

V1.0

1 Packing List

No.	Name	Qty	Unit
1	Equipment	2	PCS
2	Power adapter	2	PCS
3	Combiner	2	PCS
4	Hoop	2	PCS
5	Quick Guide	1	PCS

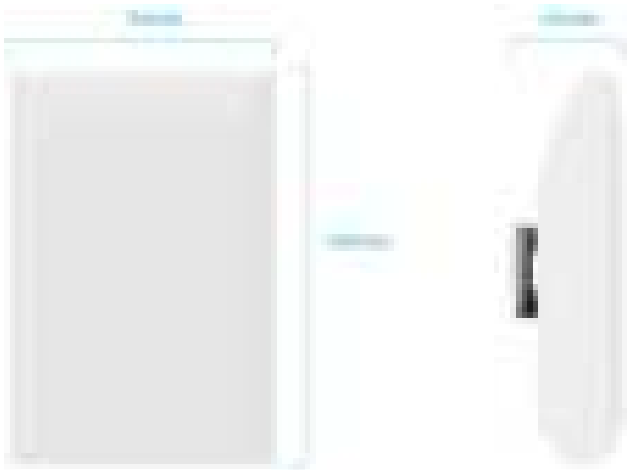
2 Product Overview

2.1 Specifications

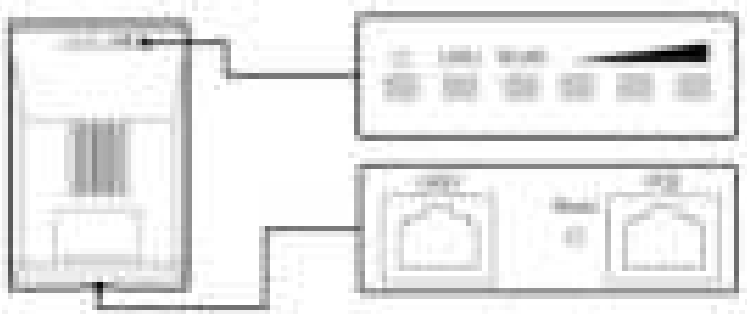
Hardware	Dimensions(mm)	140x93x43mm
	Weight(kg)	0.19kg
	Installation	Pole mounting Diameter≤55mm
	Protection Level	IP65
	Antenna Gain	ANT 1: 10.77dBi; ANT 2: 10dBi
	Beam Width	H：35°，V：35°
	Power Supply	12V,1A
	Max Power Consumption(W)	6W
	Average Power Consumption(W)	4W
	CPU	AR9344
	DDR & Memory	64MB DDR2,8MB Flash
	Physical Interface	2*10/100Mbps
	Indicator Light	1*Power Indicator 1*LAN1 Indicator 1*WLAN Indicator 3* Signal Strength Indicator
	Working Temperature	-40℃~65℃
	Storage Temperature	-40℃~85℃

	Working Humidity	5%~95%RH Non-condensing
	Surge	POE/GE: CM 4KV , DM 2KV
	ESD Protection	Contact 6KV , Air 8KV
	Wind Survivability	134km/h
Software	Protocol	802.11a/n
	Frequency	5180~5320MHz、5745~5825MHz（China） 5180~5240、5745~5825(United States) 5160~5340MHz 、 5480~5720MHz 、 5745~5865MHz（India） 5160~5340MHz 、 5480~5720MHz 、 5745~5825MHz（United Arab Emirates） 5745~5805MHz（Indonesia）
	Operating Mode	AP, Station, WDS AP, WDS Station
	Security	WPA2-PSK, Hidden SSID, IP/MAC Filtering
	Network Mode	Bridge/ Router
	Management	Support Web/AC/SNMP
	Other	Timed restart，Support VLAN，QoS, Watchdog

2.2 Dimension



2.1 Interface



Indicator	Color	Indication
POWER	Green	power light
LAN1	Green	Network connection lamp The light is on, indicating that the LAN port of POE power supply is connected to IPC or other network equipment, and flashes when there is data
WLAN	Green	Wireless indicator light The light is on to indicate wireless access and flashes when data is available
	Green	Signal strength indicator light Only one light is on, indicating a weak signal or no signal
	Green	Only two lights are on, indicating moderate signal strength
	Green	All three lights are on, indicating high signal strength

Device

POE port: Connect with the POE port with its own power supply

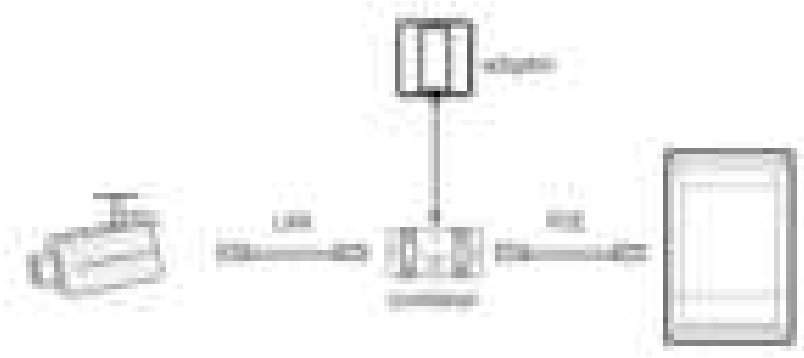
LAN2 port: reserved network port, can be connected with IPC and other front-end network equipment

Device Reset:When the device is working, please press the reset button for 10 seconds and wait for 2~3 minutes to restore the default factory settings

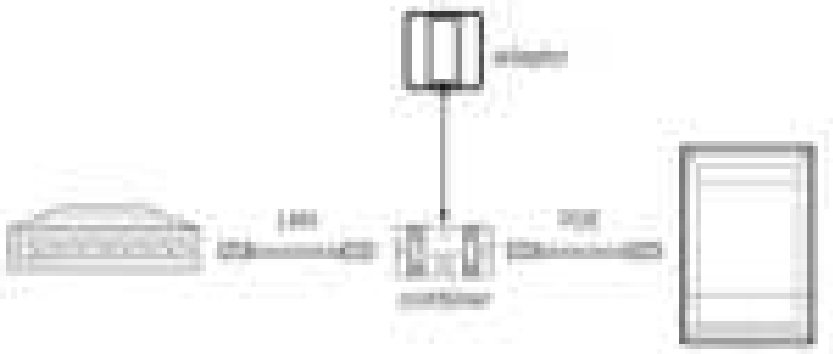
POE

POE port: Connect with the POE port of the device

3 Installation



Schematic diagram of the installation completion of the transmitter device



Schematic diagram of the installation completion of the receiver equipment

4 Software configuration

4.1.1 Configuration default settings

Default factory settings

transmitter device
IP address: 192.168.1.35
Username: root
Password: admin

receiver equipment
IP address: 192.168.1.36
Username: root
Password: admin

Device reset

When the device is working, please press the reset button for 10 seconds and wait for 2~3 minutes to restore the default factory Settings

Troubleshooting methods for network failure and excessive delay

1) Confirm that the devices are aligned and visible, and there are no obstructions in the middle;
2) Confirm that the various indicator lights of the equipment are working normally, and the signal strength indicator is in the medium or above indication condition;
3) There may be interference from other frequencies. Adjust the working frequency of the device away from the interference frequency.

4.1.2 Preparation

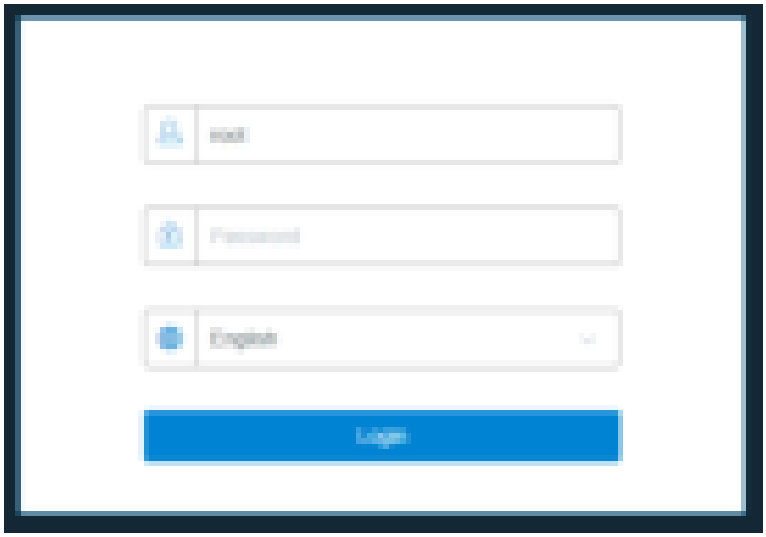
Step 1 Use a network cable to connect the computer to the LAN interface of the device or PoE power supply to prepare the device. First, you need to configure the computer IP address and the device's default IP address to be on the same network segment. Take the Windows 7 system as an example. Click the network logo in the lower right corner of the desktop and click Open Network & Internet settings - Network and Sharing Center. As shown below.

Step 2 Click “Local Area Connection” on the right and click “Properties”. As shown below.

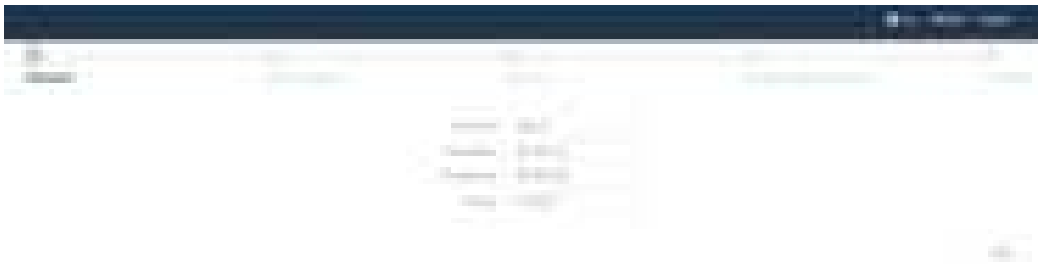
Step 3 Double-click Internet Protocol Version 4 (TCP/IPv4). As shown below.

4.1.3 Configuration

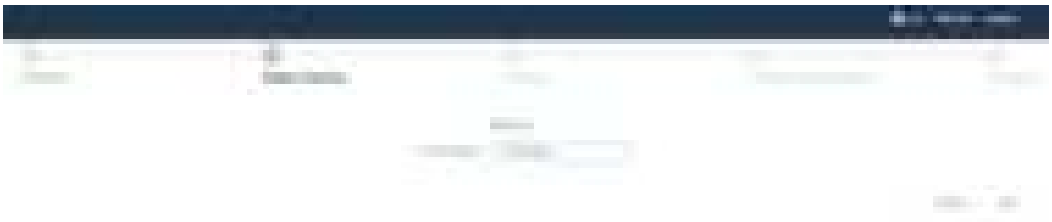
Step 1 Make sure that the IP address of the computer is inconsistent with the default IP address of the device. On the same network segment, use a browser to log in to the device, open a browser（The default IP address for the AP is 192.168.1.35, and the default IP address for the client is 192.168.1.36）



Step 2 Go to the device page, click "Wizard" in the upper right corner of the page to configure the IP address. The IP address must be ensured not to cause conflicts. After configuring, click "Next".

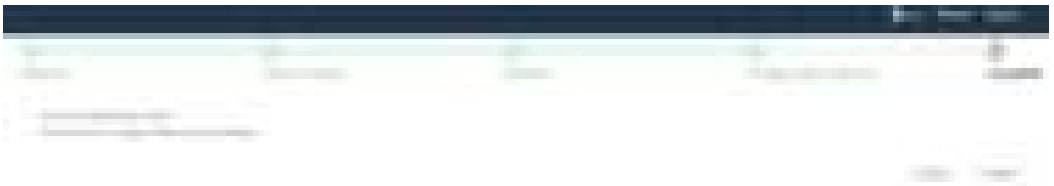


Step 3 Enter the country code configuration, select the country/region where the device is located, and click "Next" after configuring



Step 4 Enter the wireless configuration page, where you can modify wireless-related parameters. The AP side should be configured as Access Point (WDS), while the client side should be configured as Client (WDS). The SSID needs to be unique and consistent between the access point and the client. In access point mode, the channel width should be set to 40MHz, while other parameters remain default. In client mode, the SSID should be the same as the access point, and the channel width should be configured as 20/40MHz, while other parameters remain default. If the encryption and key method are modified, they should be consistent between the access point and the client. Click "Next" after completing the configuration.

Step 5 Go to the Setup “Wizard – Finish” page and click “Complete” to save the configuration.



Disclaimer and Safety Warnings

Copyright Statement

Trademark Acknowledgements

Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described

in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

EU Authorised Representative

UNV Technology EUROPE B.V. Room 2945,3rd Floor,Randstad 21-05 G,1314 BD,Almere,Netherlands.

Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change default password and set strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.

- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.
- **The following are recommendations for enhancing network security of your device:**
- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.

- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Regulatory Compliance

FCC Statements

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

Visit http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/ for SDoC.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A 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 own expense.

LVD/EMC Directive

This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU

The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC

Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.