



ALL02860ND



WLAN N Dual Band Access Point



Table of Contents

1	INTRODUCTION.....	5
1.1	Features and Benefits	6
1.2	Package Contents.....	6
1.3	System Requirements	7
1.4	Applications	7
2	BEFORE YOU BEGIN.....	9
2.1	Considerations for Wireless Installation	9
2.2	Computer Settings (in Windows XP/Windows 7).....	10
2.3	Computer Settings in Apple Mac OS X.....	12
2.4	Hardware Installation	13
3	CONFIGURING YOUR ACCESS POINT.....	17
3.1	Default Settings	17
3.2	Web Configuration	18
4	BUILDING A WIRELESS NETWORK.....	20
4.1	Access Point Mode.....	20
4.2	WDS AP Mode.....	21
4.3	WDS Bridge Mode	22
4.4	Repeater mode	23
5	STATUS.....	24
5.1	Save/Reload.....	24
5.2	Main.....	25
5.3	2.4G/5G Wireless Client List.....	27
5.4	2.4G/5G Connection Status	28



5.5	2.4G/5G WDS Link List.....	29
5.6	System Log	30
6	SYSTEM.....	31
6.1	Operation Mode.....	31
6.2	IP Settings	32
6.3	Spanning Tree Setting	33
7	2.4G/5G WIRELESS.....	34
7.1	Wireless Network.....	34
7.2	Wireless Security.....	38
7.3	Site Survey.....	41
7.4	Wireless MAC Filtering.....	44
7.5	Wireless Advanced.....	45
7.6	WPS (Wi-Fi Protected Setup).....	46
7.7	WDS Link Settings	48
8	MANAGEMENT.....	50
8.1	Administration	50
8.2	Management VLAN Settings.....	51
8.3	Wireless Traffic Shaping.....	52
8.4	SNMP Settings	53
8.5	Backup/Restore.....	55
8.6	Auto Reboot Settings	56
8.7	Firmware Upgrade	57
8.8	Time Setting.....	58
8.9	Log.....	59



8.10	Diagnostics	60
8.11	LED Control	60
8.12	Logout	61
8.13	Reset	61
8.14	ALLNET GPL Code Statement	62
8.15	CE Declaration of Conformity	69



1 Introduction

The **ALL02860ND** is a high-powered, long-range dual-band concurrent wireless 802.11a/b/g/n access point with four major functional modes. The ALL02860ND is designed to operate in numerous environments from large homes, small and medium-sized businesses, multiple-floor offices, hotels and other venues to larger enterprise deployments. Its high-powered, long-range characteristics make it a cost-effective alternative to ordinary access points that don't have the range and reach to connect to a growing number of wireless users who wish to connect to a large home or business network.

The ALL02860ND supports the 2.4GHz frequency band under 802.11 b/g/n mode while at the same time providing 5GHz band for communicating or transferring files in a less congested network frequency band.

The ALL02860ND delivers up to 6x faster wireless speeds and 7x extended coverage than legacy 802.11a/b/g wireless devices. Even though the ALL02860ND has been designed and engineered for traffic heavy and demanding business environments it is also quite at home in larger house scenarios because it efficiently extends the wireless range of an existing home router, especially in very architecturally-challenging structures to provide whole home connectivity.

To protect sensitive data during wireless transmissions, the ALL02860ND offers different encryption settings for wireless transmissions including industry-standard WPA and WPA2 encryption. The ALL02860ND also includes MAC address filtering to allow network administrators to offer network access only to known computers and other devices based on their MAC addresses.

1.1 Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300 Mbps for each band (2.4GHz / 5GHz)	Capable of handling heavy data payloads such as HD multimedia streaming.
10/100/1000 Gigabit Ethernet	Support up to 1000Mbps wired networking speed.
IEEE 802.11n Compliant and Backwards Compatible with 802.11 a/b/g devices	Fully compatible with IEEE 802.11 a/b/g/n devices.
Multi-Function	Allowing users to select any one of the following modes: Access Point, WDS AP, WDS Bridge, and Repeater depending on their specific networking deployment need.
Support Multiple SSID in AP mode (up to 8 in each frequency band)	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID through the built in software.
WPA/WPA2/IEEE 802.1x Support	Powerful data security.
MAC Address Filtering in AP Mode	For more secure network connections with known users and devices.
User Isolation Support (AP mode)	Offers an additional layer of protection within the network by isolating specific client users.
Power-over-Ethernet (IEEE802.3at/af)	Allows installers to deploy the access point in locations via a PoE connection (Ethernet cable) where a power outlet may not be available.
Save User Settings	Enables network administrators to save their device settings so firmware upgrades do not permanently delete previous device settings.
SNMP Remote Configuration Management	Allows remote connection to configure or manage the ALL02860ND easily.
QoS (WMM) support	Prioritizes bandwidth-intensive and sensitive data traffic.

1.2 Package Contents

The ALL02860ND package contains the following items (all items must be in package to issue a refund):

- ALL02860ND Access Point
- 12V/2A 100V~240V Power Adapter
- RJ-45 Ethernet LAN Cable

- Wall Mount Kit: Mounting Bracket, Wall/Ceiling Mounting Hardware Kit, T-Rail Mounting Hardware Kit
- CD with User's Manual
- Quick Installation Guide
- **Please use only the power supply unit that is delivered with the device.**
- **Bitte verwenden Sie nur das mitgelieferte Netzteil.**

1.3 System Requirements

The following are the Minimum System Requirements in order to configure the device.

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7), Mac OS, or Linux-based operating systems
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or another similar browser application)

1.4 Applications

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

a) Difficult-to-Wire Environments

There are many situations where wires cannot be installed or deployed easily or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas make the installation of an Ethernet-based LAN impossible, impractical or expensive.

b) Temporary Workgroups

Create temporary workgroups/networks in more open areas within a building – auditoriums, amphitheater classrooms, ballrooms, arenas, exhibition centers, temporary offices where one wants either a permanent or temporary Wireless LAN established.

c) The Ability to Access Real-Time Information

Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.

d) Frequently Changing Environments

Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).

e) Small Office and Home Office (SOHO) Networks

SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless Extensions to Existing Ethernet-based Networks



Devices like the ALL02860ND enable network administrators, installers and end-users to extend the range and reach of an existing Ethernet-based network.

g) Training/Educational Facilities

Training sites at corporations or students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2 Before you Begin

This section will guide you through the installation process. Placement of the EnGenius ALL02860ND is essential to maximize the access point's performance. Avoid placing the ALL02860ND in an enclosed space such as a closet, cabinet, or stairwell.

2.1 Considerations for Wireless Installation

The operating distance of all wireless devices cannot be pre-determined due to a number of unknown obstacles in the environment that the device is deployed in. These could be the number, thickness, and location of walls, ceilings, or other objects that the ALL02860ND's wireless signals must pass through. Here are some key guidelines to allow the ALL02860ND to have optimal wireless range.

- Keep the number of walls and/or ceilings between the ALL02860ND and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in lower signal strength.
- Building materials makes a difference. A solid metal door and/or aluminum studs may have a significant negative effect on the signal strength of the ALL02860ND. Locate your wireless devices carefully so the signal can pass through a drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets and/or brick can also diminish wireless signal strength.
- Interference from your other electrical devices and/or appliances that generate RF noise can also diminish the ALL02860ND's signal strength. The most common types of devices are microwaves or cordless phones.

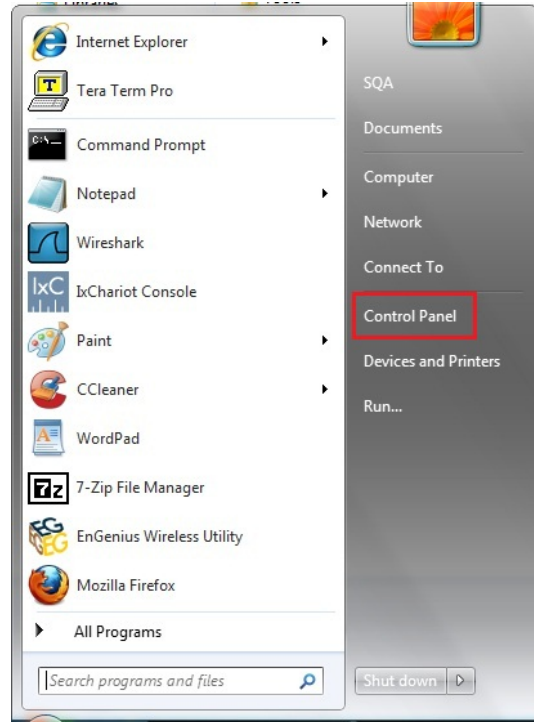
2.2 Computer Settings (in Windows XP/Windows 7)

In order to use the ALL02860ND, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

- Click **Start** button and open **Control Panel**.

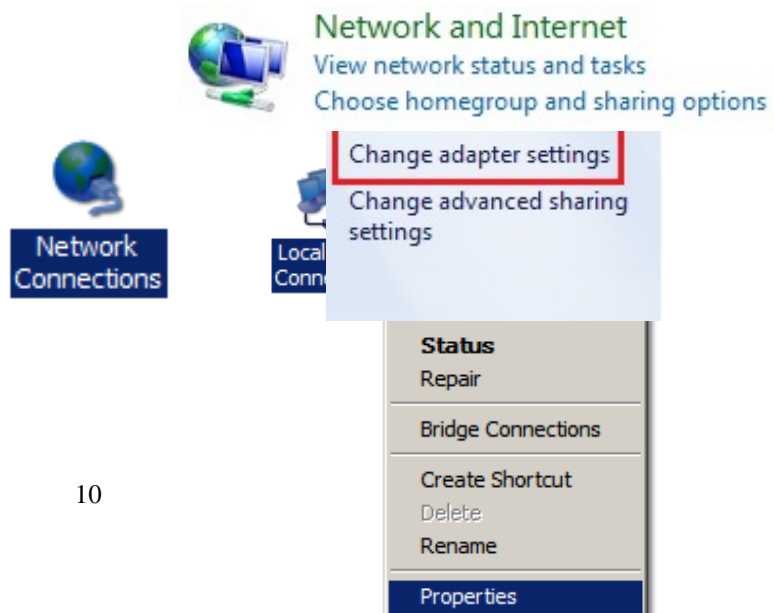


Windows XP

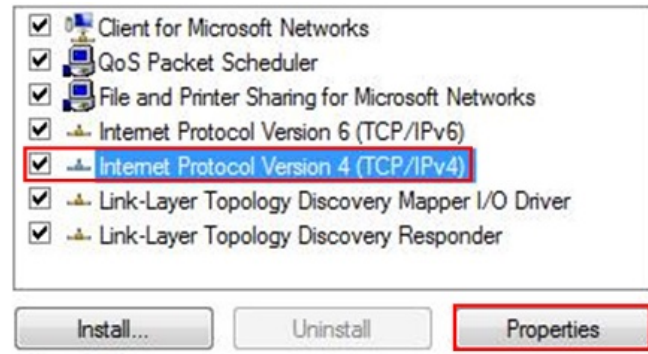


Windows 7

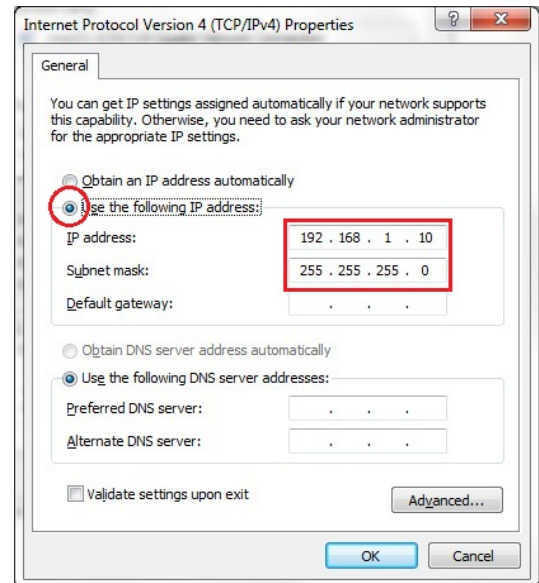
- In **Windows XP**, click **Network Connections**
- In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet** section, then select **Change adapter settings**



- Right click on **Local Area Connection** and select **Properties**



- Select **"Internet Protocol Version 4 (TCP/IPv4)"** and then select **Properties**



- Select **Use the following IP address** and enter an IP address that is different from the ALL02860ND and subnet mask then click **OK**.

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

For example:

ALL02860ND IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

PC subnet mask: 255.255.255.0

2.3 Computer Settings in Apple Mac OS X

- Go to **System Preferences** (can be opened in the **Applications** folder or selecting it in the Apple Menu)
- Select **Network** in the **Internet & Network** section
- Highlight **Ethernet**
- In **Configure IPv4**, select **Manually**
- Enter an IP address that is different from the ALL02860ND and subnet mask then press **OK**

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

For example: ALL02860ND IP address: 192.168.1.1

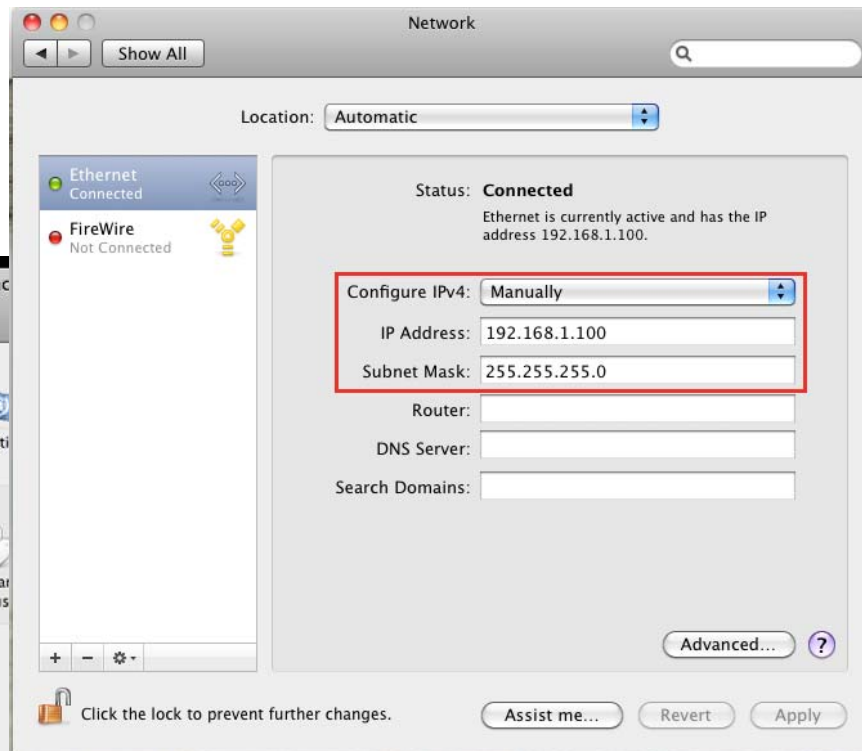
PC IP address:

192.168.1.2 – 192.168.1.255

PC subnet mask:

255.255.255.0

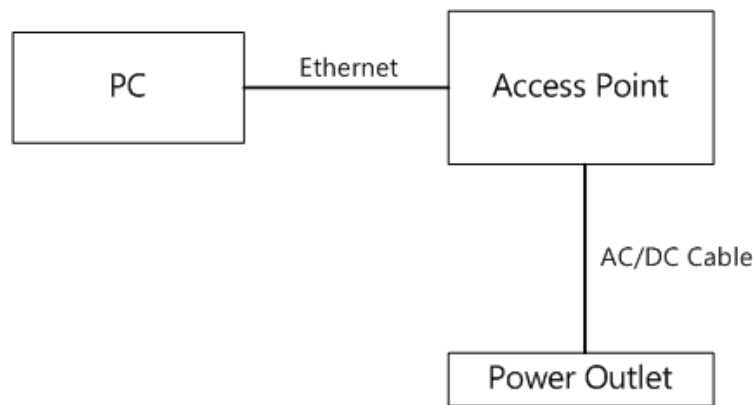
- Click **Apply** when done.



2.4 Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller (RJ-45 Ethernet Port). For more information, verify with your computer's user manual.
2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the ALL02860ND and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the ALL02860ND and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the ALL02860ND and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:
 - a) Ensure that the **POWER** light is on (it will be orange).
 - b) Ensure that the **2.4GHz/5GHz WLAN** light is on (it will be green for 5G, blue for 2.4G).
 - c) Ensure that the **LAN (Computer/ALL02860ND Connection)** light is on (it will be blue).
 - d) Once all three lights are on, proceed to set up the access point using the computer.

This diagram depicts the hardware configuration.



Mounting the ALL02860ND

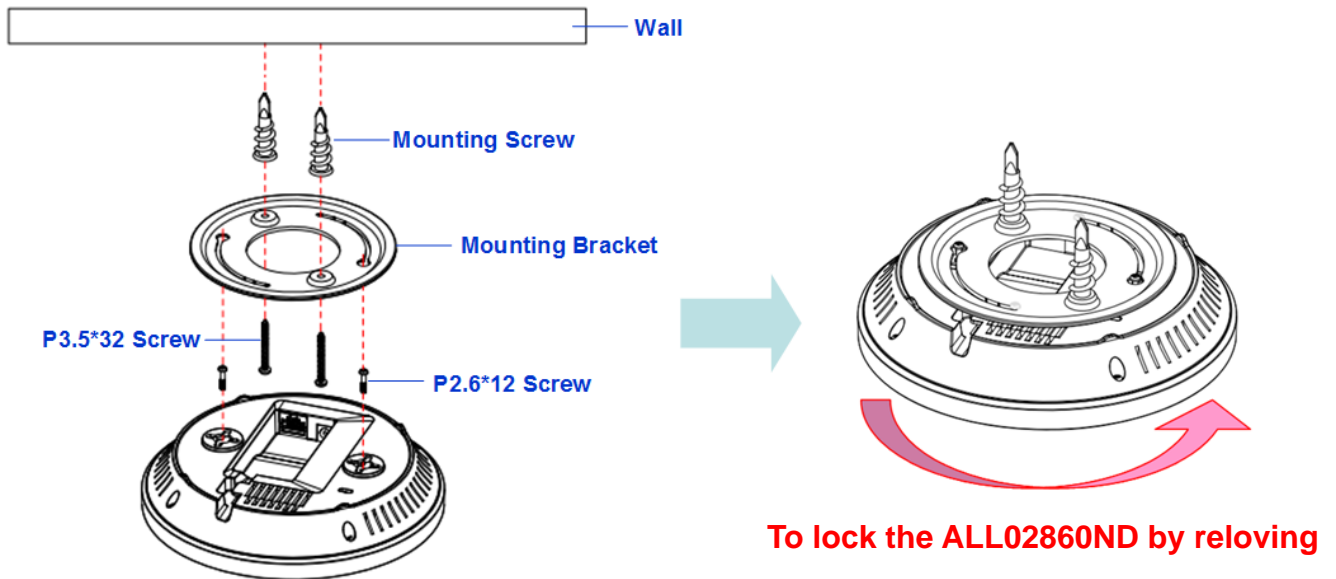
Using the provided hardware, the ALL02860ND can be attached to a ceiling or wall.

To attach the ALL02860ND to a ceiling or wall using the mounting bracket:

- 1) Attach the mounting bracket to the wall or ceiling using the provided wall/ceiling mounting hardware kit.
- 2) Insert the provided short screws into the bottom cover of the ALL02860ND.

Leave enough of the screws exposed to ensure that the unit can be attached to the mounting bracket.

If extra space is required, use the provided spacers and long screws from the T-Rail mounting hardware kit to increase the space between the unit and the mounting bracket.



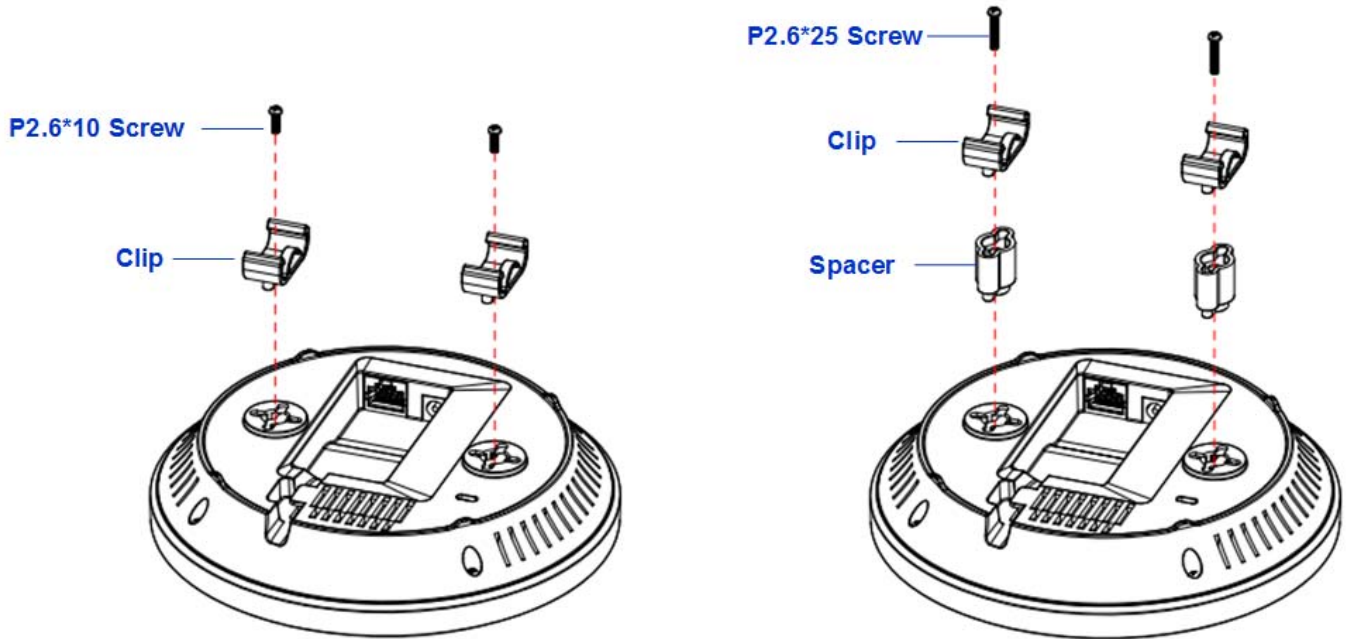
- 3) Mount the ALL02860ND on the mounting bracket by rotating the unit clockwise about 90 degrees to secure it in place.

To attach the ALL02860ND to a ceiling using the provided T-rail connectors:

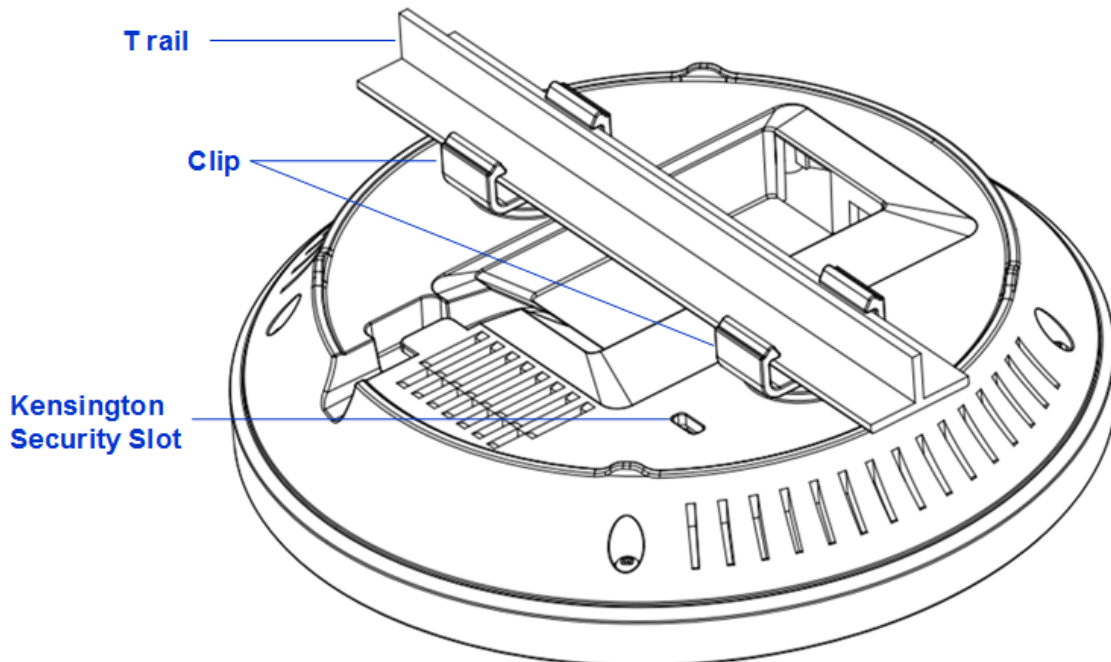
- 1) Attach the T-rail connectors to the bottom cover of the ALL02860ND using the provided short screws.

Two sizes of T-rail connectors are included in the mounting hardware kit: 15/16in (2.38cm) and 9/16in (1.43cm).

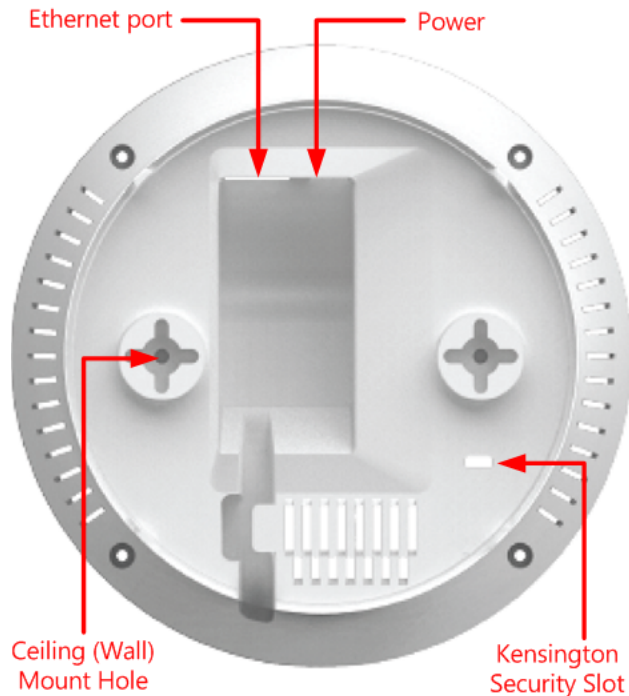
If extra space is required to accommodate drop ceiling tiles, use the provided spacers and long screws.



- 2) Line up the connected T-rail connectors with an appropriately sized rail and press the unit onto the rail until it snaps into place.



Note: To protect your ALL02860ND, use the Kensington security slot to attach a cable lock (cable lock is not included).



Front Panel	
Reset Button	One click for reset the device. Press over 10 seconds for reset to factory default.
LED Lights	LED lights for WPS, WLAN 5G, WLAN 2.4G, Ethernet port and Power.
Rear Panel	
Power	DC IN for Power.
Ethernet Port	Ethernet port for RJ-45 cable.
Ceiling (Wall) Mount Hole	Using the provided hardware, the ALL02860ND can be attached to a ceiling or wall.
Kensington Security Slot	To protect your ALL02860ND, use the Kensington security slot to attach a cable lock.

3 Configuring Your Access Point

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

3.1 Default Settings

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

Default Settings

IP Address	192.168.1.1
Username / Password	admin / admin
Operation Mode	AP / AP

3.2 Web Configuration

- Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address **http://192.168.1.1**

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



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

A screenshot of the ALLNET login page. At the top center is the ALLNET logo, which consists of a stylized globe icon and the text "ALLNET®". Below the logo are two input fields: "Username:" with the text "admin" entered, and "Password:" with five black dots. At the bottom of the form are two buttons: "Login" and "Reset".

- If successful, you will be logging in and see the ALL02860ND User Menu.



Firefox | http://192.168.1.1/cgi-bin/luci/stok=a7202a4d08fa5b100be9f9f576a057f3

192.168.1.1/cgi-bin/luci/stok=a7202a4d08fa5b100be9f9f576a057f3

ALLNET | **Wireless Access Point/Client Bridge**

AP/AP

- Status**
 - Save/Reload:0
 - Main
 - 2.4G Wireless Client List
 - 5G Wireless Client List
 - System Log
- System**
 - Operation Mode
 - IP Settings
 - Spanning Tree Settings
 - Band Steer
- 2.4G Wireless**
 - Wireless Network
 - Wireless MAC Filter
 - Wireless Advanced Settings
 - WPS
- 5G Wireless**
 - Wireless Network
 - Wireless MAC Filter
 - Wireless Advanced Settings
 - WPS
- Management**
 - Administration
 - Management VLAN
 - Wireless Traffic Shaping
 - SNMP Settings
 - Backup/Restore Settings
 - Firmware Upgrade
 - Time Settings
 - Schedule
 - CLI Settings
 - Log
 - Diagnostics
 - Led Control
 - Logout

Main Home Reset

System Information

Device Name	ALL02860ND
Ethernet MAC Address	00:02:6F:EC:B2:D4
2.4G Wireless MAC Address (SSID/MAC)	1 00:02:6F:EC:B2:D4
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
5G Wireless MAC Address (SSID/MAC)	1 00:02:6F:EC:B2:D5
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Country	Germany
Current Time	Thu Aug 8 09:46:50 UTC 2013
Firmware Version	1.3.8
Management VLAN ID	Untagged

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
Spanning Tree Protocol	Disabled
IPv6 IP Address	None
IPv6 Link-Local Address	FE80::202:6FFF:FEEC:B2D4
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	101.386 KB (1236 PKts.)
TX(Packets)	968.752 KB (1366 PKts.)

Current 2.4G Wireless Settings

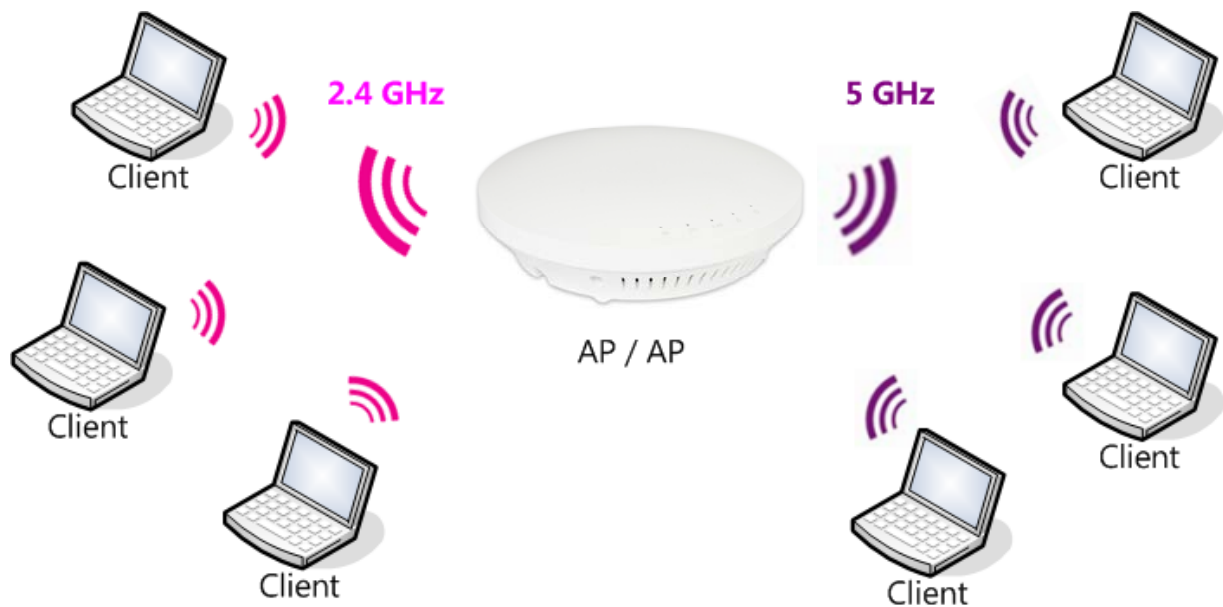
Operation Mode	Access Point
Wireless Mode	802.11 B/G/N Mixed
Channel Bandwidth	20.40 MHz
Frequency/Channel	2.437 GHz (Channel 6)
	1
	2 N/A

4 Building a Wireless Network

The ALL02860ND has the ability to operate in various modes. This chapter describes the operating modes of the ALL02860ND.

4.1 Access Point Mode

In Access Point Mode, ALL02860ND behaves like a central connection for stations or clients that support IEEE 802.11a/b/g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the ALL02860ND. The ALL02860ND supports up to eight SSIDs at the same time for secure access.



4.2 WDS AP Mode

The ALL02860ND also supports WDS AP mode. This operating mode allows wireless connections to the ALL02860ND using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports four AP MAC addresses.



4.3 WDS Bridge Mode

In WDS Bridge Mode, the ALL02860ND can wirelessly connect different LANs by configuring the MAC address and security settings of each ALL02860ND device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the ALL02860ND to wirelessly connect two wired LANs, as shown in the following figure.

WDS Bridge Mode can establish four WDS links, creating a star-like network.



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

4.4 Repeater mode

The Repeater mode is used to regenerate or replicate signals from a wireless router or other access point/station that is unable to reach certain areas in a building. When this mode is activated in the ALL02860ND, the ALL02860ND receives the wireless signal from an existing router or AP and relays it to other devices within its range so they can join the network.



5 Status

The **Status** section contains the following options: **Main, 2.4G/5G Wireless Client List, 2.4G/5G Connection Status, 2.4G/5G WDS Link List** and **System Log**.

The following sections describe these options.

5.1 Save/Reload

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

Save/Reload Home Reset

Unsaved changes list

```
wireless.wifi0.WLANHTMode=40
wireless.wifi0.hwmode=11n_pure
wireless.wifi0.channel=7
wireless.w0_index0.wps_configured=1
wireless.w0_index0.ssid=ALL02860ND
wireless.w0_index0.encryption=psk2 aes
wireless.w0_index0.key=Pa$6w0rd123
wireless.w0_index0.WLANWpaRadiusAccSrvIP=...
wireless.w0_index0.hidden=0
wireless.w0_index0.server=...
-wireless.w0_index16.WLANWDSPeer
```

Save & Apply Revert

5.2 Main

Clicking the **Main** link under the **Status** menu or clicking **Home** at the top-right of the ALL02860ND Page shows the status information about the current operating mode.

- The **System Information** section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID (**Note:** VLAN ID is only applicable in Access Point or WDS AP mode).

System Information	
Device Name	ALL02860ND
Ethernet MAC Address	00:02:6F:EC:B2:D4
2.4G Wireless MAC Address (SSID/MAC)	1 00:02:6F:EC:B2:D4
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
5G Wireless MAC Address (SSID/MAC)	1 00:02:6F:EC:B2:D5
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Country	Germany
Current Time	Thu Aug 8 09:46:50 UTC 2013
Firmware Version	1.3.8
Management VLAN ID	Untagged

- The **LAN Settings** section shows the Local Area Network settings such as the LAN IP Address, Subnet Mask, and DNS Address.

LAN Settings	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
Spanning Tree Protocol	Disabled

- The **Current 2.4G/5G Wireless Settings** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the ALL02860ND supports multiple-SSIDs, information about each SSID, the ESSID and security settings, are displayed (**Note:** Profile Settings is only applicable in Access Point, WDS AP).



Current 2.4G Wireless Settings

Operation Mode	Access Point
Wireless Mode	802.11 N only
Channel Bandwidth	40 MHz
Frequency/Channel	2.442 GHz (Channel 7)
Profile Settings (SSID/Security/VID/802.1Q)	1 ALL02860ND/WPA2-PSK AES/1/OFF
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	1.64746 KB (7 PKts.)

Current 5G Wireless Settings

Operation Mode	Access Point
Wireless Mode	802.11 A/N Mixed
Channel Bandwidth	20-40 MHz
Frequency/Channel	5.22 GHz (Channel 44)
Profile Settings (SSID/Security/VID/802.1Q)	1 ALL02860ND-5G/WPA2-PSK AES/51/OFF
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	0 B (0 PKts.)

5.3 2.4G/5G Wireless Client List

Clicking the **2.4G/5G Wireless Client List** link under the **Status** menu displays the list of clients associated to the ALL02860ND's 2.4GHz/5GHz, along with the MAC addresses and signal strength for each client. Clicking **Refresh** updates the client list.

Note: Only applicable in Access Point, WDS AP, and Repeater mode.

2.4G / Client List

Home

Reset

SSID:#	MAC Address	RSSI(dBm)
SSID1:#1	00:02:6f:4d:f2:1e	-23
SSID1:#2	00:02:6f:11:ac:93	-31

Refresh

5G / Client List

Home

Reset

SSID:#	MAC Address	RSSI(dBm)
SSID51:#1	00:02:6f:63:69:19	-38

Refresh

5.4 2.4G/5G Connection Status

Click on the **2.4G/5G Connection Status** link under the **Status** menu. This page displays the current status of the Network, including Network Type, SSID, BSSID, Connection Status, Wireless Mode, Current Channel, Security, Data Rate, Noise Level, and Signal Strength.

Note: Only applicable in Repeater mode.

2.4G / Connection Status

Home

Reset

Network Type	Repeater
SSID	Test2013
BSSID	88:DC:96:07:3A:4C
Connection Status	Associated
Wireless Mode	IEEE 802.11b/g/n Mixed
Current Channel	2.432 GHz(Channel 5)
Security	WPA2-PSK AES
Tx Data Rates(Mbps)	300 Mbps
Current noise level	-95 dBm
Signal strength	-29 dBm

Refresh

5G / Connection Status

Home

Reset

Network Type	Repeater
SSID	Test_ALL0558N
BSSID	88:DC:96:08:19:28
Connection Status	Associated
Wireless Mode	IEEE 802.11n/a Mixed
Current Channel	5.26 GHz(Channel 52)
Security	WPA2-PSK AES
Tx Data Rates(Mbps)	270 Mbps
Current noise level	-95 dBm
Signal strength	-39 dBm

Refresh

5.5 2.4G/5G WDS Link List

Click on the **2.4G/5G WDS Link List** link under the **Status** menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

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

2.4G / WDS Link List

Home

Reset

WDS Link ID	MAC Address	Link Status	RSSI (dBm)
1	00:02:6f:ca:e6:be	UP	-96

Refresh

5G / WDS Link List

Home

Reset

WDS Link ID	MAC Address	Link Status	RSSI (dBm)
1	00:02:6f:11:22:33	DOWN	--

Refresh

5.6 System Log

The ALL02860ND automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **System Log** link under the **Status** menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

System Log

[Home](#) [Reset](#)

Show log type All ▾

```

May 17 16:10:03 user.notice root: starting ntpclient
May 17 16:10:01 cron.err crond[1107]: USER root pid 487 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 16:05:03 user.notice root: starting ntpclient
May 17 16:05:01 cron.err crond[1107]: USER root pid 472 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 16:00:03 user.notice root: starting ntpclient
May 17 16:00:01 cron.err crond[1107]: USER root pid 457 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:55:04 user.notice root: starting ntpclient
May 17 15:55:02 cron.err crond[1107]: USER root pid 442 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:50:04 user.notice root: starting ntpclient
May 17 15:50:01 cron.err crond[1107]: USER root pid 3561 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:45:03 user.notice root: starting ntpclient
May 17 15:45:01 cron.err crond[1107]: USER root pid 2691 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:40:03 user.notice root: starting ntpclient
May 17 15:40:01 cron.err crond[1107]: USER root pid 2040 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:35:03 user.notice root: starting ntpclient
May 17 15:35:01 cron.err crond[1107]: USER root pid 1818 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:30:03 user.notice root: starting ntpclient
May 17 15:30:01 cron.err crond[1107]: USER root pid 1803 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:25:03 user.notice root: starting ntpclient
May 17 15:25:01 cron.err crond[1107]: USER root pid 1788 cmd . /etc/hotplug.d/iface/20-ntpcli
May 17 15:20:03 user.notice root: starting ntpclient
May 17 15:20:01 cron.err crond[1107]: USER root pid 1773 cmd . /etc/hotplug.d/iface/20-ntpcli

```

[Refresh](#) [Clear](#)

System Log	
Refresh	Update the log.
Clear	Clear the log.

6 System

6.1 Operation Mode

The ALL02860ND supports four operating modes: Access Point, WDS AP, WDS Bridge, and Repeater.

System Properties Home Reset

System Properties

Device Name	ALL02860ND (1 to 32 characters)
Country/Region	Germany
Operation Mode	2.4G Wireless Configuration <input checked="" type="radio"/> Access Point <input type="radio"/> WDS 5G Wireless Configuration <input type="radio"/> Access Point <input type="radio"/> WDS <input checked="" type="radio"/> Repeater

Accept Cancel

System Properties	
Device Name	Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.
Country/Region	Select a Country/Region to conform to local regulations.
Operation Mode	Use the radio button to select an operating mode.
Save & Apply / Cancel	Click Save & Apply to confirm the changes or Cancel to cancel and return previous settings.

6.2 IP Settings

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

IP Settings

Home

Reset

System Information

IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 1
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

Accept

Cancel

IP Settings	
IP Network Setting	Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.
IP Address	The IP Address of this device.
IP Subnet Mask	The IP Subnet Mask of this device.
Default Gateway	The Default Gateway of this device. Leave it blank if you are unsure of this setting.
Primary / Secondary DNS	The primary / secondary DNS address for this device.

6.3 Spanning Tree Setting

This page allows you to modify the Spanning Tree settings. Enabling Spanning Tree protocol will prevent network loops in your LAN network.

Spanning Tree Settings

[Home](#) [Reset](#)

Spanning Tree Status	<input type="radio"/> On <input checked="" type="radio"/> Off
Bridge Hello Time	<input type="text" value="2"/> seconds (1-10)
Bridge Max Age	<input type="text" value="20"/> seconds (6-40)
Bridge Forward Delay	<input type="text" value="4"/> seconds (4-30)
Priority	<input type="text" value="32768"/> (0-65535)

[Accept](#) [Cancel](#)

Spanning Tree	
Spanning Tree Status	Enable or disable the Spanning Tree function.
Bridge Hello Time	Specify Bridge Hello Time, in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.
Bridge Max Age	Specify Bridge Max Age, in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be dead.
Bridge Forward Delay	Specify Bridge Forward Delay, in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it analyzes data traffic before participating.
Priority	Specify the Priority Number. A smaller number has greater priority.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

7 2.4G/5G Wireless

7.1 Wireless Network

This page displays the current status of the Wireless settings of the ALL02860ND.

Access Point / WDS AP mode:

2.4G / Wireless Network

Home

Reset

Wireless Mode	802.11 B/G/N Mixed ▾
Channel HT Mode	20/40MHz ▾
Extension Channel	Upper Channel ▾
Channel / Frequency	Ch7-2.442GHz ▾ <input checked="" type="checkbox"/> Auto
AP Detection	<input type="button" value="Scan"/>

Current Profiles

SSID	Security	VID	Enable	Edit
ALL02860ND-2.4G	WPA2-PSK AES	1	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_2	None	2	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_3	None	3	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_4	None	4	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_5	None	5	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_6	None	6	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_7	None	7	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-2.4G_8	None	8	<input type="checkbox"/>	<input type="button" value="Edit"/>

5G / Wireless Network

Home Reset

Wireless Mode	802.11 A/N Mixed ▾
Channel HT Mode	20/40MHz ▾
Extension Channel	Upper Channel ▾
Channel / Frequency	Ch36-5180GHz ▾ <input checked="" type="checkbox"/> Auto
AP Detection	<input type="button" value="Scan"/>

Current Profiles				
SSID	Security	VID	Enable	Edit
ALL02860ND-5G	WPA2-PSK AES	51	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_2	None	52	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_3	None	53	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_4	None	54	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_5	None	55	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_6	None	56	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_7	None	57	<input type="checkbox"/>	<input type="button" value="Edit"/>
ALL02860ND-5G_8	None	58	<input type="checkbox"/>	<input type="button" value="Edit"/>

2.4G/5G Wireless Network (Access Point / WDS AP mode)	
Wireless Mode	Wireless mode supports 802.11b/g/n mixed mode in 2.4G and 802.11a/n mixed mode in 5G.
Channel HT Mode	The default channel bandwidth is 20/40MHz. The larger the channel, the better the transmission quality and speed.
Extension Channel	Select upper or lower channel. Your selection may affect the Auto channel function.
Channel / Frequency	Select the channel and frequency appropriate for your country's regulation.
Auto	Check this option to enable auto-channel selection.
AP Detection	AP Detection can select the best channel to use by scanning nearby areas for Access Points.
Current Profile	Configure up to eight different SSIDs (four in WDS AP mode). If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click Edit to configure the profile and check whether you want to enable extra SSID.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

2.4G/5G SSID Profile

2.4G / SSID Profile

Wireless Setting

SSID	ALL02860ND-2.4G (1 to 32 characters)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Security

Security Mode	Disabled ▼
---------------	------------

5G / SSID Profile

Wireless Setting

SSID	ALL02860ND-5G (1 to 32 characters)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Security

Security Mode	Disabled ▼
---------------	------------

2.4G/5G SSID Profile	
SSID	Specify the SSID for the current profile.
Suppressed SSID	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
Station Separation	Click the appropriate radio button to allow or prevent communication between client devices.
Wireless Security	See the Wireless Security section.
Save / Cancel	Click Save to accept the changes or Cancel to cancel and return previous settings.

Repeater mode:

2.4G / Wireless Network

Home

Reset

Wireless Mode	802.11 B/G/N Mixed ▾
SSID	Specify the static SSID : AP SSID <input type="text"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Preferred BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Wireless Security

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

Security Mode ▾

5G / Wireless Network

Home

Reset

Wireless Mode	802.11 A/N Mixed ▾
SSID	Specify the static SSID : AP SSID <input type="text"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Preferred BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Wireless Security

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

Security Mode ▾

2.4G/5G Wireless Network (Repeater mode)	
Wireless Mode	Wireless mode supports 802.11b/g/n mixed mode in 2.4G and 802.11a/n mixed mode in 5G.
SSID	The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the Site Survey .
Site Survey	Click on Site Survey to search the existing Access Points.
Preferred BSSID	Specify the BSSID (Access Point's MAC Address).
Wireless Security	The encryption is using. It must the same as Access Point's encryption.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

7.2 Wireless Security

The Wireless Security section lets you configure the ALL02860ND's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. It is strongly recommend to use WPA2-PSK.

WEP Encryption:

Wireless Security

Security Mode	WEP ▾
Auth Type	Open System ▾
Input Type	Hex ▾
Key Length	40/64-bit (10 hex digits or 5 ASCII char) ▾
Default Key	1 ▾
Key1	1234567890
Key2	
Key3	
Key4	

WEP Encryption	
Auth Type	Select Open System or Shared Key .
Input type	ASCII: Regular Text (recommended) HEX: Hexadecimal Numbers (For advanced users)
Key Length	Select the desired option and ensure the wireless clients use the same setting. Choices are 64, 128, 152-bit password lengths.
Default Key	Select the key you wish to be default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key .
Encryption Key #	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

WPA-PSK (WPA Pre-Shared Key) Encryption:

Wireless Security

Security Mode	WPA-PSK Mixed ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

WPA-PSK (WPA Pre-Shared Key) Encryption

Encryption	Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.
Passphrase	Wireless clients must use the same key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEXformat, the Key must be 64 HEX characters in length.
Group Key Update Interval	Specify how often, in seconds, the group key changes.

WPA Encryption: Only in Access Point / WDS AP mode

Wireless Security

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

WPA Encryption	
Encryption	Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.
Radius Server	Enter the IP address of the Radius server.
Radius Port	Enter the port number used for connections to the Radius server.
Radius Secret	Enter the secret required to connect to the Radius server.
Group Key Update Interval	Specify how often, in seconds, the group key changes.
Radius Accounting	Enable or disable accounting feature.
Radius Accounting Server	Enter the IP address of the Radius accounting server.
Radius Accounting Port	Enter the port number used for connections to the Radius accounting server.
Radius Accounting Secret	Enter the secret required to connect to the Radius accounting server.
Interim Accounting Interval	Specify how often, in seconds, the accounting data sends.

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

7.3 Site Survey

Use this feature to scan nearby Access Points.

Note: Only applicable in Repeater mode.

1. Click **Site Survey**.

Wireless Network Home Reset

Wireless Mode	802.11 B/G/N Mixed ▾
SSID	Specify the static SSID : <input type="text" value="AP SSID"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Preferred BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Wireless Security

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

Security Mode	Disabled ▾
---------------	------------

2. Scanning the nearby Access Points

Scanning

Please wait...

3. The ALL02860ND will list the available access points after site survey.



2.4G / Site Survey

2GHz Site Survey

:Infrastructure :Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:11:E5:03:FC:4A	ALLPrint	6	-47 dBm	11g/n	WPA2-PSK	
00:0F:C9:0D:8B:1A		5	-52 dBm	11g/n	WPA2-PSK	
00:0F:C9:03:0C:3C	bridgewb	6	-82 dBm	11b/g	WPA2-PSK	
74:91:1A:11:76:C8	ALL-Support	13	-45 dBm	11g/n	WPA2-PSK	
00:24:01:C1:C8:86		6	-85 dBm	11g/n	WPA/WPA2-PSK	
88:DC:96:07:3A:4C	Test2013	5	-28 dBm	11g/n	WPA2-PSK	
50:A7:33:1C:EC:58	ALLNET-INT1	1	-46 dBm	11g/n	WPA2-PSK	
50:A7:33:5C:EC:58	ALLNET-Guest	1	-47 dBm	11g/n	WPA2-PSK	
50:A7:33:9C:EC:58		1	-47 dBm	11g/n	WPA2-PSK	
50:A7:33:DC:EC:58		1	-46 dBm	11g/n	WPA2-PSK	
00:02:6F:E6:1C:18	ALLNET_ECB350	10	-40 dBm	11g/n	WPA2	
00:02:6F:E8:08:4C	ALLNET_EAP350	11	-47 dBm	11g/n	WPA2	
02:02:6F:E8:08:4C	ALLNET_EAP350_2	11	-95 dBm	11g/n	WPA2	
7A:44:01:9A:CE:2B	MMLAN_EXT	6	-90 dBm	11b/g	WPA-PSK	
68:7F:74:41:FC:4F	AeroFlot	12	-95 dBm	11b/g	WPA2-PSK	
8A:25:2C:5C:77:91	EasyBox-21D657	2	-90 dBm	11g/n	WPA/WPA2-PSK	
74:91:1A:51:76:C8	ALL-Guest	13	-45 dBm	11g/n	none	
34:08:04:24:79:10	Raubfischteam	4	-83 dBm	11g/n	WEP	

Site Survey (Repeater mode)	
BSSID	Access Point's wireless MAC address.
SSID	SSID that the Access Point is broadcasting.
Channel	Channel that the Access Point is using.
Signal Level (dBm)	Signal strength from the Access Point to your station.
Type	The band that the Access Point is using.
Security	Encryption method that the Access Point is using to secure data over the WLAN.
Refresh	Click Refresh to rescan nearby Access Point.

4. Select an Access Point and click that Access Point's BSSID.

2.4G / Site Survey

2GHz Site Survey i:Infrastructure :Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:11:E5:03:FC:4A	ALLPrint	6	-47 dBm	11g/n	WPA2-PSK	i
00:0F:C9:0D:8B:1A		5	-52 dBm	11g/n	WPA2-PSK	i
00:0F:C9:03:0C:3C	bridgewb	6	-82 dBm	11b/g	WPA2-PSK	
74:91:1A:11:76:C8	ALL-Support	13	-45 dBm	11g/n	WPA2-PSK	i
00:24:01:C1:C8:86		6	-85 dBm	11g/n	WPA/WPA2-PSK	i
88:DC:96:07:3A:4C	Test2013	5	-28 dBm	11g/n	WPA2-PSK	i
50:A7:33:1C:EC:58	ALLNET-INT1	1	-46 dBm	11g/n	WPA2-PSK	i
50:A7:33:5C:EC:58	ALLNET-Guest	1	-47 dBm	11g/n	WPA2-PSK	i
50:A7:33:9C:EC:58		1	-47 dBm	11g/n	WPA2-PSK	i
50:A7:33:DC:EC:58		1	-46 dBm	11g/n	WPA2-PSK	i
00:02:6F:E6:1C:18	ALLNET_ECB350	10	-40 dBm	11g/n	WPA2	i
00:02:6F:E8:08:4C	ALLNET_EAP350	11	-47 dBm	11g/n	WPA2	i
02:02:6F:E8:08:4C	ALLNET_EAP350_2	11	-95 dBm	11g/n	WPA2	i
7A:44:01:9A:CE:2B	MMLAN_EXT	6	-90 dBm	11b/g	WPA-PSK	i
68:7F:74:41:FC:4F	AeroFlot	12	-95 dBm	11b/g	WPA2-PSK	i
8A:25:2C:5C:77:91	EasyBox-21D657	2	-90 dBm	11g/n	WPA/WPA2-PSK	i
74:91:1A:51:76:C8	ALL-Guest	13	-45 dBm	11g/n	none	i
34:08:04:24:79:10	Raubfischteam	4	-83 dBm	11g/n	WEP	i

Refresh

5. Enter the correct security setting.

2.4G / Wireless Network

Home Reset

Wireless Mode	802.11 B/G/N Mixed
SSID	Specify the static SSID : Test2013 (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Preferred BSSID	<input type="checkbox"/> 00 : 08 : 54 : A2 : B2 : C6
Wireless Security	
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.	
Security Mode	WPA2-PSK
Encryption	AES
Passphrase	Pa\$\$w0rd (8 to 63 characters) or (64 Hexadecimal characters)

Accept Cancel

7.4 Wireless MAC Filtering

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict the permission to access ALL02860ND. The default setting is **Disable Wireless MAC Filter**.

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

2.4G / Wireless MAC Filter

Home

Reset

ACL Mode

8C : 12 : 34 : 56 : 78 : 90

#	MAC Address	
1	00:02:6F:30:9A:12	<input type="button" value="Delete"/>

5G / Wireless MAC Filter

Home

Reset

ACL Mode

: : : : :

#	MAC Address	
---	-------------	--

Wireless MAC Filter (Access Point / WDS AP mode)	
ACL Mode	Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. Choices are: Disabled , Deny MAC in the list , or Allow MAC in the list .
MAC Address	Enter the MAC address of the wireless client.
Add	Click Add to add the MAC address to the MAC Address table.
Delete	Delete the selected entries.
Apply	Click Apply to apply the changes.

7.5 Wireless Advanced

This page allows you to configure wireless advance settings. It is recommended that the default settings are used unless the user has experience with more advanced networking features.

2.4G / Wireless Advanced Settings

Home

Reset

Data Rate	Auto ▾
Transmit Power	20 dBm ▾
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	1 km
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)

Accept

Cancel

5G / Wireless Advanced Settings

Home

Reset

Data Rate	Auto ▾
Transmit Power	20 dBm ▾
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	1 km
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)

Accept

Cancel

2.4G/5G Wireless Advanced	
Data Rate	Select a data rate from the drop-down list. The data rate affects throughput of data in the ALL02860ND. The lower the data rate, the throughput will be lower, but so will the transmission distance.
Transmit Power	Set the power output of the wireless signal.
RTS/CTS Threshold	Specify the threshold package size for RTC/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth.
Distance	Specify the distance between Access Points and clients. Longer distances may drop high-speed connections.
Aggregation	Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

7.6 WPS (Wi-Fi Protected Setup)

Wi-Fi Protected Setup (WPS) feature complies with the Wi-Fi Alliance WPS standard and makes it easier to quickly add client devices to an established, security-enabled Wi-Fi network.

WPS reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

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

2.4G / WPS Setting

Home Reset

WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS current status	Configured <input type="button" value="Release Configuration"/>
Self Pin Code	43384990
SSID	ALL02860ND-2.4G
Authentication Mode	WPA2-PSK AES
Passphrase Key	Pa\$\$w0rd123
WPS Via Push Button	<input type="button" value="Start to Process"/>
WPS Via Pin	<input type="text"/> <input type="button" value="Start to Process"/>

5G / WPS Setting

Home Reset

WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS current status	Configured <input type="button" value="Release Configuration"/>
Self Pin Code	43384990
SSID	ALL02860ND-5G
Authentication Mode	WPA2-PSK AES
Passphrase Key	Pa\$\$w0rd123
WPS Via Push Button	<input type="button" value="Start to Process"/>
WPS Via Pin	<input type="text"/> <input type="button" value="Start to Process"/>

WPS (Wi-Fi Protected Setup)	
WPS	Select to Enable or Disable the WPS feature.
WPS Current Status	Shows whether the WPS function is Configured or unConfigured . When it is Configured, the WPS has been used to authorize connection between the device and wireless clients.
Self Pin Code	The PIN code of this device.
SSID	The SSID (wireless network name) used when connecting using WPS.
Authentication Mode	Shows the encryption method used by the WPS process.
Passphrase Key	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.
WPS via Push Button	Click this button to initialize WPS feature using the push button method.
WPS via PIN	Enter the PIN code of the wireless device and click this button to initialize WPS feature using the PIN method.

7.7 WDS Link Settings

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

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

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

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

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

2.4G / WDS Link Settings

Home

Reset

Security	None ▾
AES Passphrase	<input type="text"/> (8-63 ASCII characters or 64 hexadecimal digits)

Caution: NAWDS was enabled, you need assign Wifi Channel manually later.

ID	MAC Address	Mode
1	00 : 02 : 6F : 11 : 22 : 33	Enable ▾
2	: : : : : :	Disable ▾
3	: : : : : :	Disable ▾
4	: : : : : :	Disable ▾

Accept

Cancel

5G / WDS Link Settings

Security	None ▾
AES Passphrase	<input type="text"/> (8-63 ASCII characters or 64 hexadecimal digits)

Caution: NAWDS was enabled, you need assign Wifi Channel manually later.

ID	MAC Address	Mode
1	00 : 02 : 6F : 44 : 55 : 66	Enable ▾
2	: : : : : :	Disable ▾
3	: : : : : :	Disable ▾
4	: : : : : :	Disable ▾

2.4G/5G WDS Link Settings	
Security	Select None or AES from drop-down list.
AES Passphrase	Enter the key values you wish to use. Other AP(s) must use the same key to establish WDS link.
MAC Address	Enter the Access Point's MAC address to which you want to extend the wireless area.
Mode	Select Disable or Enable from the drop-down list.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

8 Management

8.1 Administration

This page allows you to change the ALL02860ND username and password. By default, the username is **admin** and the password is: **admin**. The password can contain 0 to 12 alphanumeric characters and is case sensitive.

Login Setting

[Home](#) [Reset](#)

New Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save/Apply"/> <input type="button" value="Cancel"/>	

Login Setting	
New Name	Enter a new username for logging in to the New Name entry box.
Old Password	Enter the old password for logging in to the Old Password entry box.
New Password	Enter the new password for logging in to the New Password entry box.
Confirm Password	Re-enter the new password in the Confirm Password entry box for confirmation.
Save/Apply / Cancel	Click Save/Apply to apply the changes or Cancel to return previous settings.

8.2 Management VLAN Settings

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

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

Management VLAN Settings

2.4G Current Profiles				
SSID	Security	Isolation	VID	Enable
ALL02860ND-2.4G	WPA-PSK Mixed TKIP/AES	<input type="checkbox"/>	1	<input type="checkbox"/>
ALL02860ND-2.4G_2	None	<input type="checkbox"/>	2	<input type="checkbox"/>
ALL02860ND-2.4G_3	None	<input type="checkbox"/>	3	<input type="checkbox"/>
ALL02860ND-2.4G_4	None	<input type="checkbox"/>	4	<input type="checkbox"/>
ALL02860ND-2.4G_5	None	<input type="checkbox"/>	5	<input type="checkbox"/>
ALL02860ND-2.4G_6	None	<input type="checkbox"/>	6	<input type="checkbox"/>
ALL02860ND-2.4G_7	None	<input type="checkbox"/>	7	<input type="checkbox"/>
ALL02860ND-2.4G_8	None	<input type="checkbox"/>	8	<input type="checkbox"/>

5G Current Profiles				
SSID	Security	Isolation	VID	Enable
ALL02860ND-5G	WPA-PSK Mixed TKIP/AES	<input type="checkbox"/>	51	<input type="checkbox"/>
ALL02860ND-5G_2	None	<input type="checkbox"/>	52	<input type="checkbox"/>
ALL02860ND-5G_3	None	<input type="checkbox"/>	53	<input type="checkbox"/>
ALL02860ND-5G_4	None	<input type="checkbox"/>	54	<input type="checkbox"/>
ALL02860ND-5G_5	None	<input type="checkbox"/>	55	<input type="checkbox"/>
ALL02860ND-5G_6	None	<input type="checkbox"/>	56	<input type="checkbox"/>
ALL02860ND-5G_7	None	<input type="checkbox"/>	57	<input type="checkbox"/>
ALL02860ND-5G_8	None	<input type="checkbox"/>	58	<input type="checkbox"/>

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

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

Management VLAN (Only applicable in Access Point mode)	
Profile Isolation	Restricted client to communicate with different VID by selecting the radio button.
VLAN ID	Specify the VLAN tag for each profile.
Management VLAN ID	If your network includes VLANs, you can specify a VLAN ID for packets pass through the Access Point with a tag. Otherwise, select No VLAN tag .
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

Note:

1. If you reconfigure the Management VLAN ID, you may lose your connection to the ALL02860ND. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the ALL02860ND using the new IP address.
2. Clicking **Accept** does not apply the changes. To apply them, use Status > Save/Load (see section 5.1).

8.3 Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Wireless Traffic Shaping

Home

Reset

Enable Traffic Shaping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Incoming Traffic Limit	1000	kbit/s (512-99999999)
Outgoing Traffic Limit	2000	kbit/s (512-99999999)

Accept

Cancel

Wireless Traffic Shaping	
Enable Traffic Shaping	Check this option to enable wireless traffic shaping.
Incoming Traffic Limit	Specify the wireless transmission speed used for downloading.
Outgoing Traffic Limit	Specify the wireless transmission speed used for uploading.
Accept / Cancel	Click Accept to confirm the changes or Cancel to cancel and return previous settings.

8.4 SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) return the data stored in their Management Information Bases.

SNMP Settings

Home

Reset

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination Address	<input type="text"/>
Trap Destination Community Name	public
SNMPv3	<input checked="" type="radio"/> v3Enable <input type="radio"/> v3Disable
User Name	admin
Auth Protocol	MD5 ▾
Auth Key	12345678
Priv Protocol	DES ▾
Priv Key	12345678
Engine ID	<input type="text"/>

Save/Apply

Cancel

SNMP	
SNMP Enable/Disable	Enable or Disable SNMP feature.
Contact	Specify the contact details of the device
Location	Specify the location of the device.
Community Name (Read Only)	Specify the password for the SNMP community for read only access.
Community Name (Read/Write)	Specify the password for the SNMP community with read/write access.
Trap	

Trap Destination Address	Specify the IP address of the computer that will receive the SNMP traps.
Trap Destination Community Name	Specify the password for the SNMP trap community.
SNMPv3	
SNMPv3 Enable/Disable	Enable or Disable SNMPv3 feature.
User Name	Specify the username for SNMPv3.
Auth Protocol	Select the authentication protocol type: MDS or SHA .
Auth Key	Specify the authentication key for authentication.
Priv Protocol	Select the privacy protocol type: DES .
Priv Key	Specify the privacy key for privacy.
Engine ID	Specify the engine ID for SNMPv3.
Save/Apply / Cancel	Click Save/Apply to apply the changes or Cancel to return previous settings.

8.5 Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you also can reload the saved configurations into the device through the **Restore Saved Settings from A File** section. If extreme problems occur, or if you have set the ALL02860ND wrongly, you can use the **Factory Default** button in the **Revert to Factory Default Settings** section to restore all the configurations of the ALL02860ND to the original default settings.

Backup/Restore Settings

Home

Reset

Save A Copy of Current Settings

Backup

Restore Saved Settings from A File

Browse...

Restore

Revert to Factory Default Settings

Factory Default

Backup/Restore	
Save A Copy of Current Settings	Click Backup to save the current configured settings.
Restore Saved Settings from A File	To restore settings that have been previously backed up, click Browse , select the file, and click Restore .
Revert to Factory Default Settings	Click Factory Default button to restore the ALL02860ND to its factory default settings.

8.6 Auto Reboot Settings

You can specify how long to reboot the ALL02860ND periodically.

Auto Reboot Settings

Home

Reset

Auto Reboot Setting	Disable ▾
Frequency of Auto Reboot	Min ▾ 10 Mins ▾

Save/Apply

Cancel

Auto Reboot Settings	
Auto Reboot Setting	Enable or disable the auto reboot function.
Frequency of Auto Reboot	To specify the time to reboot the ALL02860ND by Min, Hour, Day or Week.
Save/Apply / Cancel	Click Save/Apply to apply the changes or Cancel to return previous settings.

8.7 Firmware Upgrade

This page allows you to upgrade the firmware of the ALL02860ND.

Firmware Upgrade

Home

Reset

Current firmware version: 1.1.11

Locate and select the upgrade file from your hard disk:

Browse...

Upload

To perform the Firmware Upgrade:

Click the **Browse** button and navigate the OS File System to the location of the upgrade file.

Select the upgrade file. The name of the file will appear in the *Upgrade File* field.

Click the **Upload** button to commence the firmware upgrade.

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

8.8 Time Setting

This page allows you to set the internal clock of the ALL02860ND.

Time Settings

Home

Reset

Time

Manually Set Date and Time
 2012 / 06 / 15 12 : 34

Automatically Get Date and Time
 Time Zone: UTC+00:00 Gambia, Liberia, Morocco
 User defined NTP Server: 209.81.9.7

Enable Daylight Saving
 Start Time: January 1st Sun 12 am
 End Time: January 1st Mon 12 am

Save/Apply

Cancel

Time	
Manually Set Date and Time	Manually specify the date and time.
Automatically Get Date and Time	Select a time zone from the drop-down list and check whether you want to enter the IP address of an NTP server or use the default NTP server to get have the internal clock set automatically.
Enable Daylight Saving	Check whether daylight savings applies to your area.

8.9 Log

This page allows you to setup Syslog and local log functions of the ALL02860ND.

Log

Home

Reset

Syslog

Syslog	Disable ▾
Log Server IP Address	0 . 0 . 0 . 0

Local log

Local Log	Enable ▾
-----------	----------

Save/Apply

Cancel

Log	
Syslog	Enable or disable the syslog function.
Log Server IP Address	Enter the IP address of the log server.
Local Log	Enable or disable the local log service.
Save/Apply / Cancel	Click Save/Apply to apply the changes or Cancel to return previous settings.

8.10 Diagnostics

This page allows you to analyze the connection quality of the ALL02860ND and trace the routing table to a target in the network.

Diagnostics

Home

Reset

Ping Test Parameters

Target IP	<input type="text"/>
Ping Packet Size	64 Bytes
Number of Pings	4
<input type="button" value="Start Ping"/>	

Traceroute Test Parameters

Traceroute target	<input type="text"/>
<input type="button" value="Start Traceroute"/>	

Diagnosis	
Target IP	Enter the IP address you would like to search.
Ping Packet Size	Enter the packet size of each ping.
Number of Pings	Enter the number of times you want to ping.
Start Ping	Click Start Ping to begin pinging target device (via IP).
Traceroute Target	Enter an IP address or domain name you want to trace.
Start Traceroute	Click Start Traceroute to begin the trace route operation.

8.11 LED Control

This page allows you to control LED on/off for Power, LAN interface, 2.4G/5G WLAN interface and WPS.

LED Control

Home

Reset

LED Control

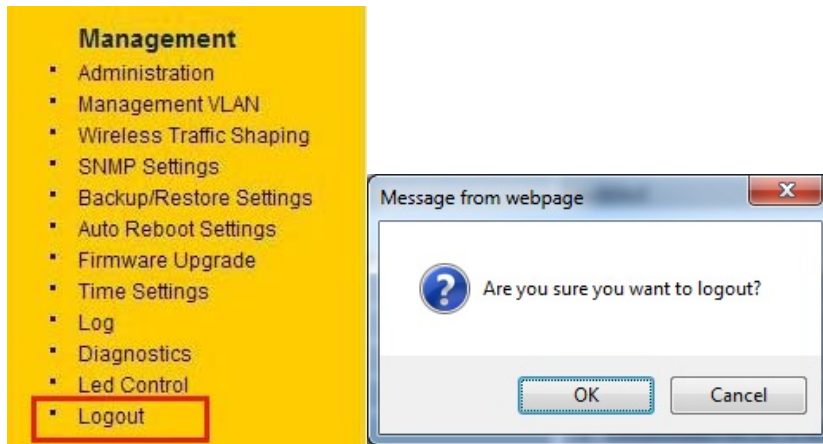
Power LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
LAN LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
2.4G LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
5G LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
WPS LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF

Save/Apply

Cancel

8.12 Logout

Click [**Logout**] in **Management** menu to logout.



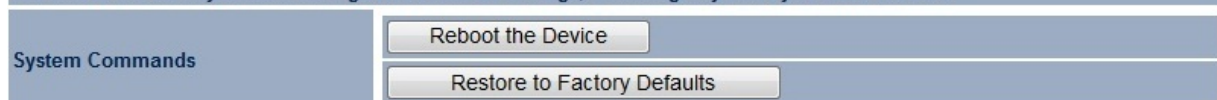
8.13 Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reboot the Device** to reboot the ALL02860ND.

Reset



The System Settings section allows you to reboot the device, or restore the device to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules you have created.





8.14 ALLNET GPL Code Statement

This ALLNET product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at: <http://www.allnet.de/gpl.html>

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

Written offer for GPL and LGPL source code

Where such specific license terms entitle you to the source code of such software, ALLNET will provide upon written request via e-mail and/or traditional paper mail the applicable GPL and LGPL source code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:

Email:

support@allnet.de

Snail Mail:

ALLNET GmbH

Maistraße 2

82110 Germering

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.



Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU General Public License

Terms and conditions for copying, distribution and modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License.

The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say,



a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.

(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written



entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing



else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present



version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS



How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) ALLNET GmbH of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'
(which makes passes at compilers) written by James Hacker.
```

```
signature of Ty Coon, 1 April 1989
```

```
Ty Coon, President of Vice
```

Source: <http://www.gnu.org/licenses/old-licenses/gpl-2.0>

8.15 CE Declaration of Conformity

For the following equipment:

Germering, 1st of August, 2013

Wireless N 300Mbit Dual Band Access Point PoE

ALL02860ND



The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL02860ND conforms to the Council EMC Directives of 2006/95/EC and 2004/108/EC.

This equipment meets the following conformance standards:

EN 60950-1:2006 +A11:2009 + A1:2010 + A12:2011

EN 60601-1-2:2007

CISPR 11:2010 ED. 5.1 (Group I, Class B)

EN 61000-3-2:2006 +A1:2009 +A2:2009, Class A

EN 61000-3-3:2008

EN 61000-4-2:2008 ED. 2.0

EN 61000-4-3:2010 ED. 3.2

EN 61000-4-4:2012 ED. 3.0

EN 61000-4-5:2005 ED. 2.0

EN 61000-4-6:2008 ED. 3.0

EN 61000-4-8:2009 ED. 2.0

EN 61000-4-11:2004 ED. 2.0

This equipment is intended to be operated in all countries.

This declaration is made by
ALLNET Computersysteme GmbH
Maistraße 2
82110 Germering
Germany

Germering, 01.08.2013

Wolfgang Marcus Bauer
CEO