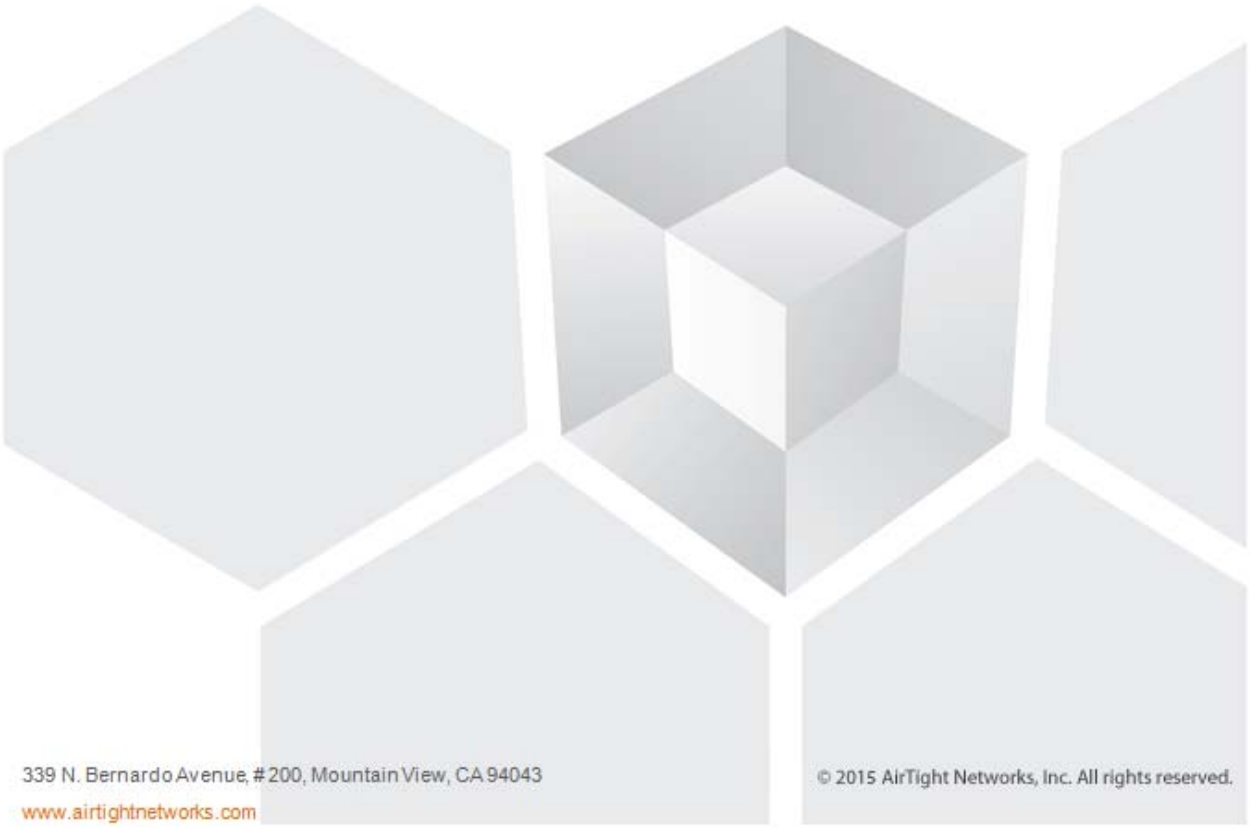
Installation Guide

W-68 Access Point/Sensor



339 N. Bernardo Avenue, #200, Mountain View, CA 94043
www.airtightnetworks.com

This page is intentionally left blank.

END USER LICENSE AGREEMENT

Please read the End User License Agreement before installing the W-68 Access Point/Sensor. The End User License Agreement is available at the following location http://www.airtightnetworks.com/fileadmin/pdf/AirTight-EULA.pdf.

Installing the W-68 Access Point constitutes your acceptance of the terms and conditions of the End User License Agreement.

DISCLAIMER

THE INFORMATION IN THIS GUIDE IS SUBJECT TO CHANGE WITHOUT ANY PRIOR NOTICE.

AIRTIGHT® NETWORKS, INC. IS NOT LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.

THIS PRODUCT HAS THE CAPABILITY TO BLOCK WIRELESS TRANSMISSIONS FOR THE PURPOSE OF PROTECTING YOUR NETWORK FROM MALICIOUS WIRELESS ACTIVITY. BASED ON THE POLICY SETTINGS, YOU HAVE THE ABILITY TO SELECT WHICH WIRELESS TRANSMISSIONS ARE BLOCKED AND, THEREFORE, THE CAPABILITY TO BLOCK AN EXTERNAL WIRELESS TRANSMISSION. IF IMPROPERLY USED, YOUR USAGE OF THIS PRODUCT MAY VIOLATE US FCC PART 15 AND OTHER LAWS. BUYER ACKNOWLEDGES THE LEGAL RESTRICTIONS ON USAGE AND UNDERSTANDS AND WILL COMPLY WITH US FCC RESTRICTIONS AS WELL AS OTHER GOVERNMENT REGULATIONS. AIRTIGHT IS NOT RESPONSIBLE FOR ANY WIRELESS INTERFERENCE CAUSED BY YOUR USE OF THE PRODUCT. AIRTIGHT NETWORKS, INC. AND ITS AUTHORIZED RESELLERS OR DISTRIBUTORS WILL ASSUME NO LIABILITY FOR ANY DAMAGE OR VIOLATION OF GOVERNMENT REGULATIONS ARISING FROM YOUR USAGE OF THE PRODUCT, EXCEPT AS EXPRESSLY DEFINED IN THE INDEMNITY SECTION OF THIS DOCUMENT.

LIMITATION OF LIABILITY

AirTight Networks will not be liable to customer or any other party for any indirect, incidental, special, consequential, exemplary, or reliance damages arising out of or related to the use of AirTight Wi-Fi, AirTight WIPS, AirTight Cloud Services, and AirTight devices under any legal theory, including but not limited to lost profits, lost data, or business interruption, even if AirTight Networks knows of or should have known of the possibility of such damages. Regardless of the cause of action or the form of action, the total cumulative liability of AirTight Networks for actual damages arising out of or related to the use of AirTight Wi-Fi, AirTight WIPS, AirTight Cloud Services or AirTight devices will not exceed the respective price paid for AirTight Wi-Fi, AirTight WIPS, AirTight Cloud Services, or AirTight devices.

Powered by Marker Packet™, Active Classification™, Live Events™, VLAN Policy Mapping™, Smart Forensics™, WEPGuard™ and WPAGuard™. AirTight Networks and the AirTight Networks logo are trademarks and AirTight is a registered trademark of AirTight Networks, Inc.

This product contains components from Open Source software. These components are governed by the terms and conditions of the GNU Public License. To read these terms and conditions visit http://www.gnu.org/copyleft/gpl.html.

Protected by one or more of U.S. patent Nos. 7,002,943; 7,154,874; 7,216,365; 7,333,800; 7,333,481; 7,339,914; 7,406,320; 7,440,434; 7,447,184; 7,496,094; 7,536,723; 7,558,253; 7,710,933; 7,751,393; 7,764,648; 7,804,808; 7,856,209; 7,856,656; 7,970,894; 7,971,253; 8,032,939; and international patents: AU 200429804; GB 2410154; JP 4639195; DE 60 2004 038 621.9; and GB/NL/FR/SE 1976227. More patents pending. For more information on patents, please visit: www.airtightnetworks.com/patents.

Federal Communication Commission Interference Statement

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.

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

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR MOBILE DEVICE USAGE (>20cm/low power) Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

Note: The country code selection is for non-US models only and is not available to all US models. Per FCC regulations, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Industry Canada Statement

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

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

CAUTION

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

AVERTISSEMENT

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont reserves uniquement pour une utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux;

(ii) De plus, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

FOR MOBILE DEVICE USAGE (>20cm/low power)

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

Declaration d'exposition aux radiations
Cet equipement est conforme aux limites d'exposition aux rayonnements IC etablies pour un environnement non controle. Cet equipement doit @tre installe et utilise avec un minimum de 20 cm de distance entre la source de rayonnement et votre cmps.

About this Guide

This installation guide explains how to mount the W-68 access point (AP)/sensor and the various configuration details.

Important! Please read the EULA before installing the W-68. Installation constitutes your acceptance of the terms and conditions of the EULA mentioned above in this document.

Intended Audience

This guide can be referred by anyone who wants to install and configure the W-68 access point.

Document Overview

This guide contains the following chapters:

1. Package Contents
2. W-68 Overview
3. Installing the W-68
4. Manually Configuring W-68
5. Config Shell Commands
6. Troubleshooting

Note: All instances of the term 'server' in this document refer to the AirTight Wi-Fi / AirTight WIPS server, unless the server name or type is explicitly stated.

Product and Documentation Updates

To receive important news on product updates, please visit our website at http://www.airtightnetworks.com.

We continuously enhance our product documentation based on customer feedback. To obtain the latest copy of this document, visit http://www.airtightnetworks.com/home/support.html.

Contact Information

AirTight® Networks, Inc.
339 N, Bernardo Avenue, Suite #200,
Mountain View, CA 94043
Tel: +1 650-961-1111
Fax: +1 650-963-3388

For technical support, send an email to support@airtightnetworks.com.

1. Package Contents

Please ensure that the items shown in Figure 1-1 are included in the W-68 device package:

Figure 1-1 W-68 Package Contents

Note: The MAC address of the device is printed on a label at the bottom of the product and the packaging box. Note down the MAC address, before mounting the device on the ceiling or at a location that is difficult to access.

If the package is not complete, please contact AirTight® Networks, Inc. technical support at support@airtightnetworks.com, or return the package to the vendor or dealer where you purchased the product.

IMPORTANT! The device is intended for industry/enterprise/commercial use only. The device cannot be sold retail, to the general public or by mail order. It must be sold to dealers or have strict marketing control.

2. W-68 Overview

W-68 is a 2x2 802.11a/b/g/n/ac access point/sensor. This chapter provides an overview of the W-68 and describes the side and the rear panels.

The left panel of the W-68 has 7 LEDs that indicate the working of the device.

Figure 2-1 Left Panel of W-68

The following table indicates the device states based on the LEDs.

Table 2-1 LED Details for W-68 in the AP/Sensor mode

Power	WLAN 2.4/5 GHz	Uplink	LAN1, LAN2, LAN3, LAN4	Description
Solid Green	Any	Solid Green	On/Off	The AP is receiving power and is working normally. The AP is connected to the server.
Solid Green	Slow Blink Orange	Slow Blink Green	On/Off	The AP upgrade is in progress.
Solid Green	Any	Off	On/Off	The AP is unable to get Ethernet link.
Solid Green	Any	Fast Blink Green	On/Off	The AP did not receive a valid IP address via the DHCP.
Solid Green	Any	Slow Blink Green	On/Off	The AP is unable to connect to the server.
Off	Off	Off	Off	The AP is not powered on or it is in the process of starting up.

***Note**: LAN1, 2, 3, 4 is ON if the link is up, and is OFF if the link is down on the respective LAN ports. The 2.4 GHz /5 GHz LED blinks when there is activity on either of the radios.*

The rear panel of the W-68 has an Ethernet port labelled LAN1, that enables you to connect the device to a wired

LAN through a switch or a hub and provides the power for the device by using the 802.3af standard.

Figure 2-2 Rear Panel of W-68

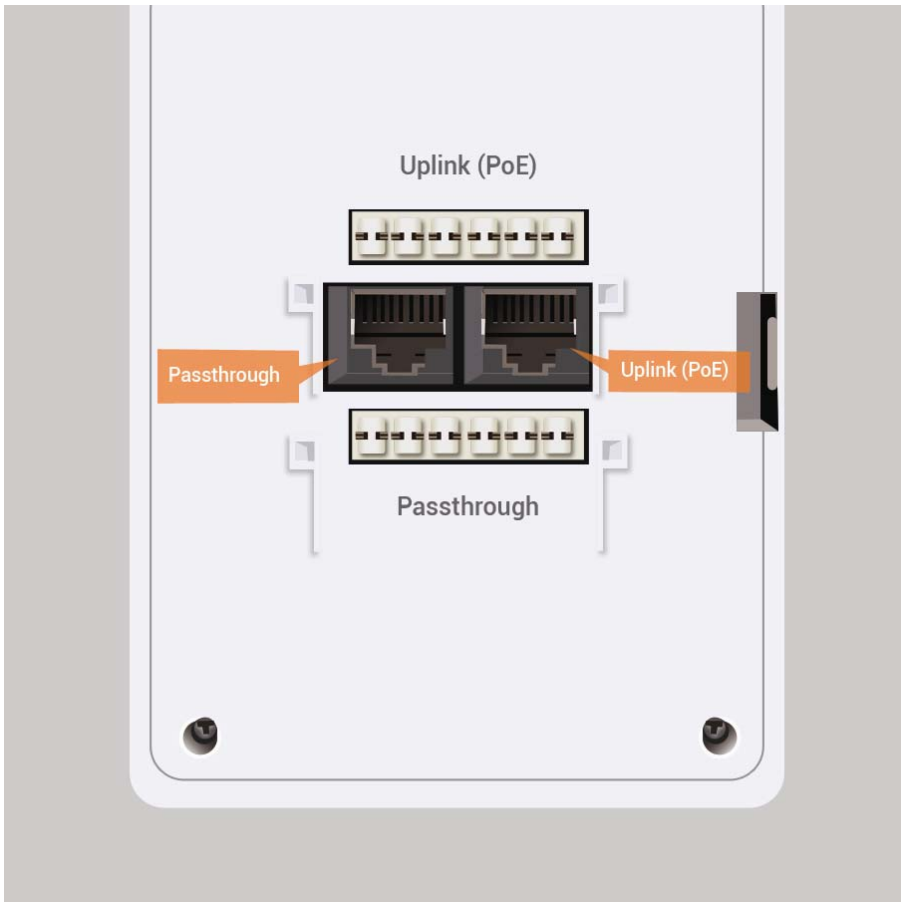
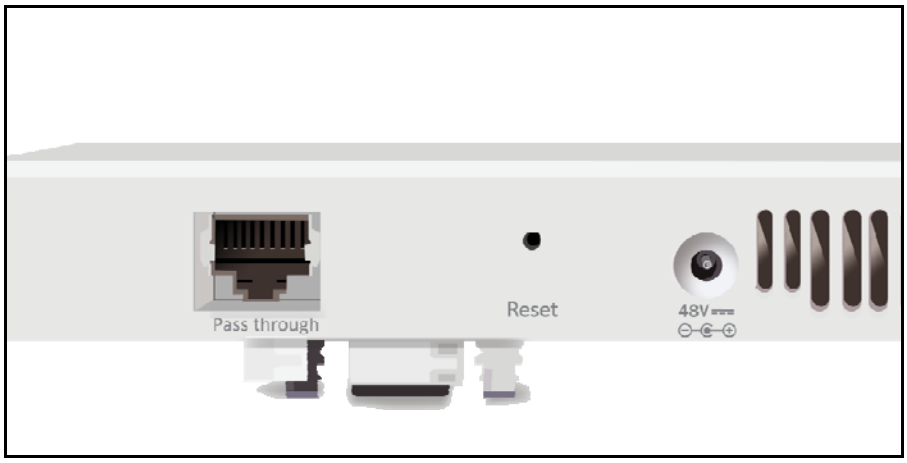


Table 2-2 Rear Panel Port Settings for W-68

Port	Description	Connector Type	Speed/Protocol
Pass-through port	This is a wired port that facilitates extension of the wired network after the AP is mounted on the wall. Another device can be plugged in to the pass-through port on the right side of the W-68 device. The traffic on the pass-through port does not interfere with the AP traffic. No policies can be applied on the pass-through port traffic.	RJ45	-
Uplink (PoE) port	Enables you to connect the device to a wired LAN through a switch or a hub. The device can then communicate with the server. This port also provides the power for the device using the 802.3af standard	RJ45	10/100/1000 Mbps Ethernet Power over Ethernet

Figure 2-3 Right side of W-68



The right side of the W-68 device has the following

- **Power Receptacle**: The power receptacle enables the user to power on the device using 48 V DC power adapter.
- **Reset Pin Hole**: The Reset Pin Hole is on the right side of the device as shown in the figure above**.** The Reset Pin Hole resets the W-68 device to factory defaults. To reset the device, power cycle the device (remove the power cable once and connect it back again) and while plugging the power cable back into the power source, press and hold down the Reset Pin Hole for 45 seconds until the power, WAN, 2.4/5 GHz LEDs go green,amber respectively. Pressing the Reset Pin Hole while the device is running will not have any effect. When you reset the device, the following settings are reset:
    - Config shell password is reset to **config**.
    - Server discovery value is erased and changed to the default, **wifi-security-server**.
    - All the VLAN configurations are lost.
    - Device mode is changed to **Sensor Only**.
    - If static IP is configured on the device, the IP address is erased and DHCP mode is set.

  After reset, all the LEDs will blink once, indicating that the reset is successful, and the system boot sequence is initiated.
- **Pass-through Port**: The pass-through port is used to plug in a device into another wired port that is available on the wall where the AP is installed. The pass-through port at the rear of the device and pass-through port on the right side of the device are internally connected.

Figure 2-4 Bottom Panel of W-68

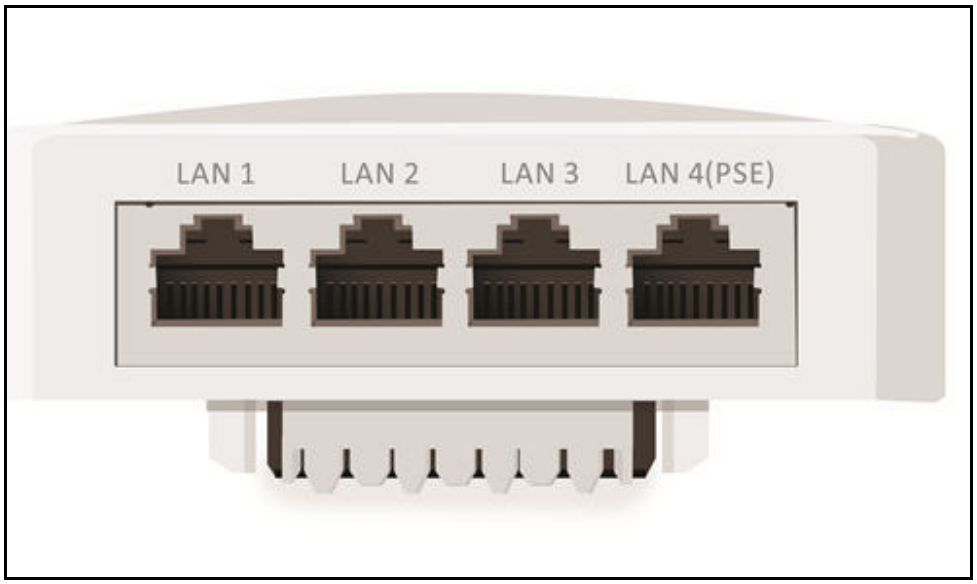


Table 2-3 Bottom Panel Ports for W-68

Port	Description	Connector Type	Speed/Protocol
LAN 1 LAN 2 LAN 3 LAN 4	Enables you to connect a device to a wired LAN through a switch or a hub. The device can then communicate with the server. The LAN 4 port can provide power for a device connected to it using the 802.3af standard, only if the W-68 access point is powered by an 802.3at power supply.	RJ-45	10/100/1000 Mbps Gigabit Ethernet

3. Installing the W-68

When the W-68 functions as a WIPS sensor, it monitors your network and communicates with the server to guard your corporate network against over-the-air attacks.

Clients can connect to your corporate network in wireless mode through the W-68 AP(s).

The W-68 must be plugged into your corporate network to perform the above-mentioned operation.

As a WIPS sensor, W-68 can be configured in one of the following two modes:

- **Sensor Mode:** This is the default mode. In this mode, the device can be connected to a trunk port (802.1Q capable) on a switch. The device then monitors the VLANs that are configured on that trunk port and are chosen by the user. In this mode, the W-68 can monitor up to 16 VLANs. The wireless interface of the sensor is enabled for WIPS operations.
- **Network Detector (ND) Mode:** This mode needs to be explicitly configured. In this mode, the device can be connected to a trunk port (802.1Q capable) on a switch. The device then monitors the VLANS that are configured on that trunk port and are chosen by the user. In this mode, the W-68 can monitor up to 100 VLANs. The wireless interface of the ND is disabled.

Important: To prevent disconnection or tampering by unauthorized personnel, it is extremely important to install the device such that it is difficult to unplug the device from the network or from the power outlet.

Zero-Configuration of W-68 as Sensor

Zero-configuration is supported under the following conditions:

- The device is in sensor mode.
- A DNS entry **wifi-security-server** is set up on all the DNS servers. This entry should point to the IP address of the server. By default, the device looks for the DNS entry **wifi-security-server**.
- The device is placed on a subnet that is DHCP enabled.

Important: If the device is placed on a network segment that is separated from the server by a firewall, you must first open port 3851 for User Datagram Protocol (UDP) and Transport Control Protocol (TCP) bidirectional traffic on that firewall. This port number is assigned to AirTight® Networks. If multiple devices are set up to connect to multiple servers, zero-configuration is not possible. In this case, you must manually configure the sensors. Refer to Manually Configuring W-68 for further details.

The steps to install the device with no configuration (zero-configuration) are as follows.

1. Mount the device
2. Power on the device.
3. Connect the device to the network.

Connecting W-68

This involves mounting the W-68, powering on the device, and connecting it to the wired network.

Mount W-68

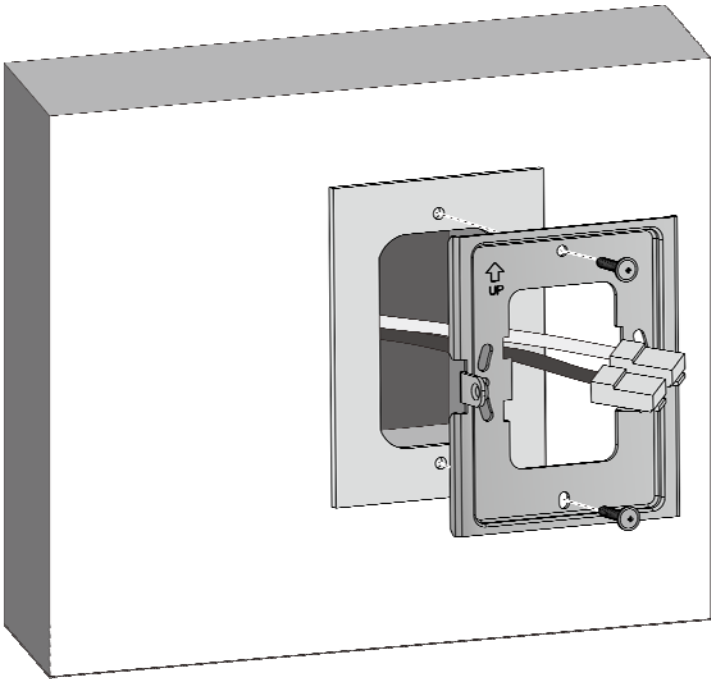
Take a configured W-68, that is, ensure that a static IP is assigned to the device or the settings have been changed for DHCP. Note the MAC address and the IP address of the device in a safe place before it is installed in its appropriate location. The MAC address of the device is printed on a label at the rear side of the product.

Recommended: You should label the devices using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the devices.

Wall Mounting

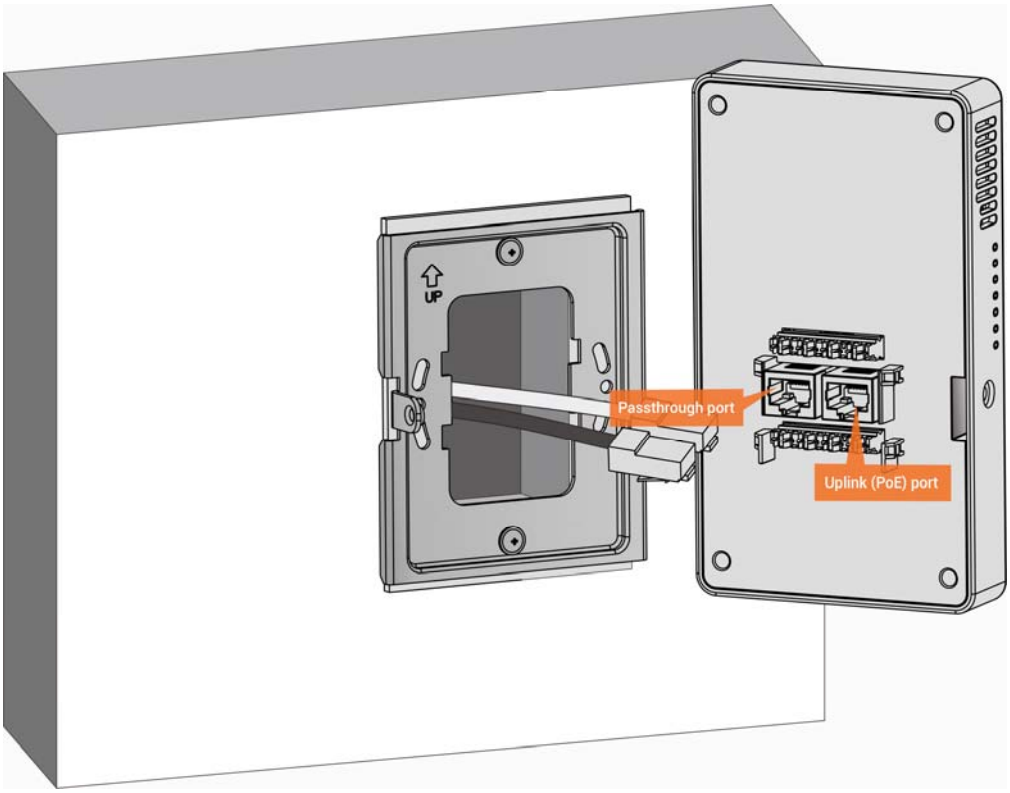
Use the mounting bracket to install the W-68 on the wall. To mount the device:

1. Attach the mounting bracket to the wall by using the mounting hardware kit.



.

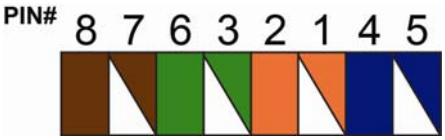
2. Plug the Ethernet cable and, optionally, a pass-through cable, if any, into the Uplink port and the pass-through port respectively.



Alternatively, you could seat an 8-wire Ethernet cable with a punch-down tool into the punch-down block provided at the rear of the W-68 device. The upper punch-down block is for the uplink or PoE.The lower punch-down block is for the pass-through port.

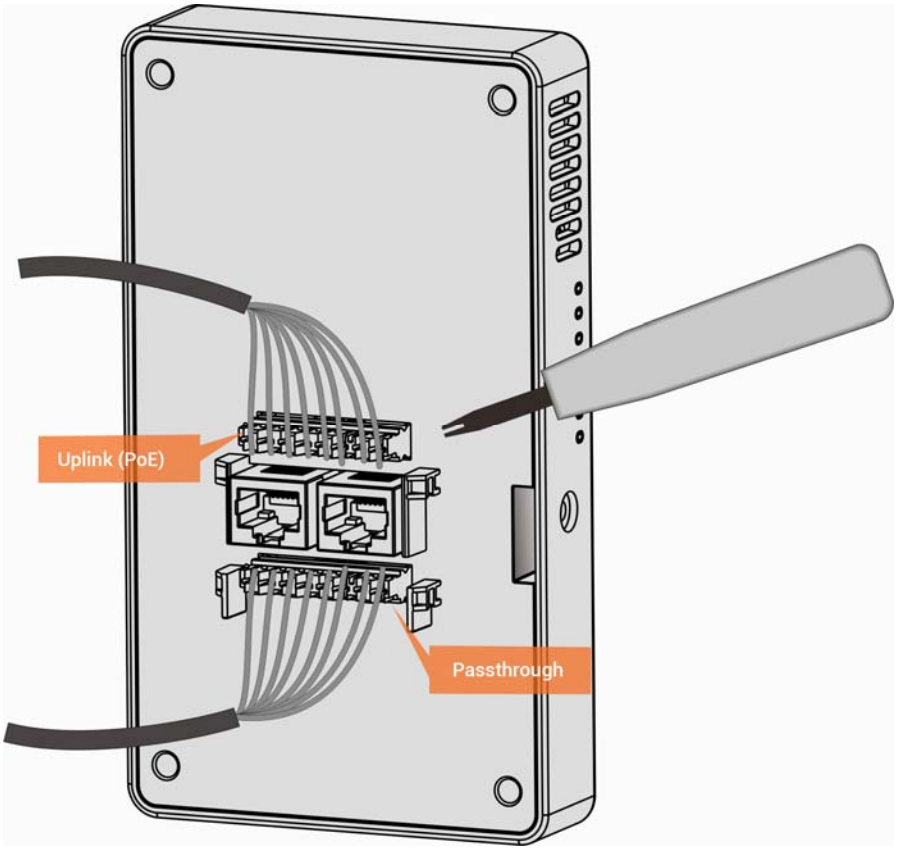
An 8-pin Ethernet cable has four pairs of color-coded wires.

The following image and table explain the color codes of the wires the 8-pin Ethernet cable in detail.

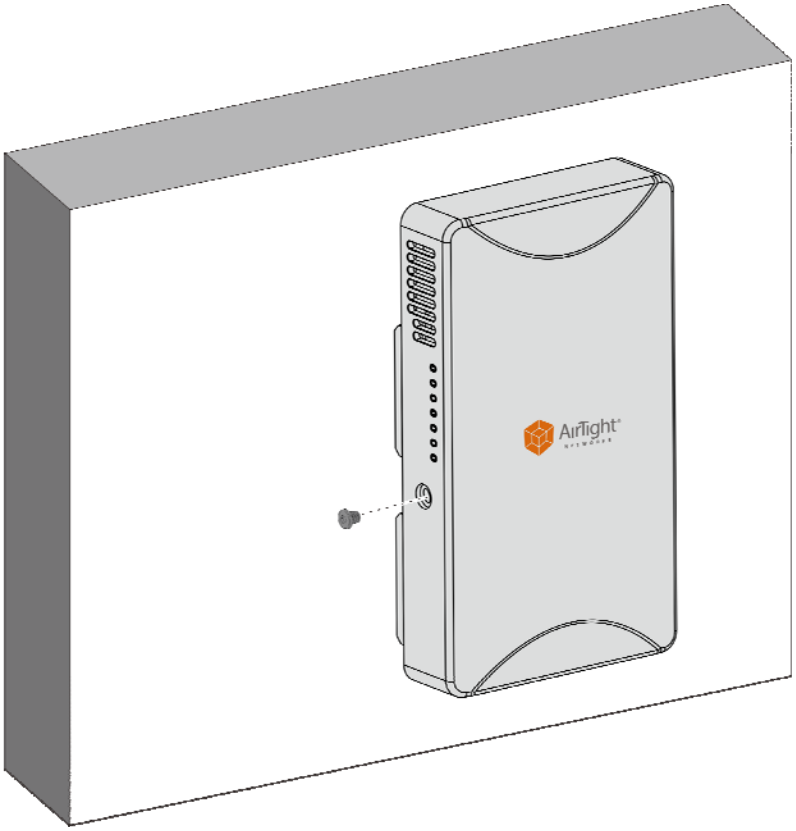


PIN#	Wire Color
1	White/orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown

The following image illustrates two cables, one punched down into the uplink punch-down block and the other into the pass-through punch-down block.



3. Insert the provided short screw into the side of the W-68 device.



4. The device is ready for use.

Power on W-68

A W-68 device can be powered on by 802.3af Class 0 Power Over Ethernet (PoE) of Nominal input voltage 48V DC. You can connect the device to the network using PoE or a power adapter.

Connect W-68 to the Network

To connect W-68 to the network, perform the following steps.

1. Ensure that a DHCP server is already available on the network to enable network configuration of the W-68.
2. Add the DNS entry **wifi-security-server** on all DNS servers. This entry should point to the IP address of the server.
3. Ensure that DHCP is running on the subnet to which the device will be connected.

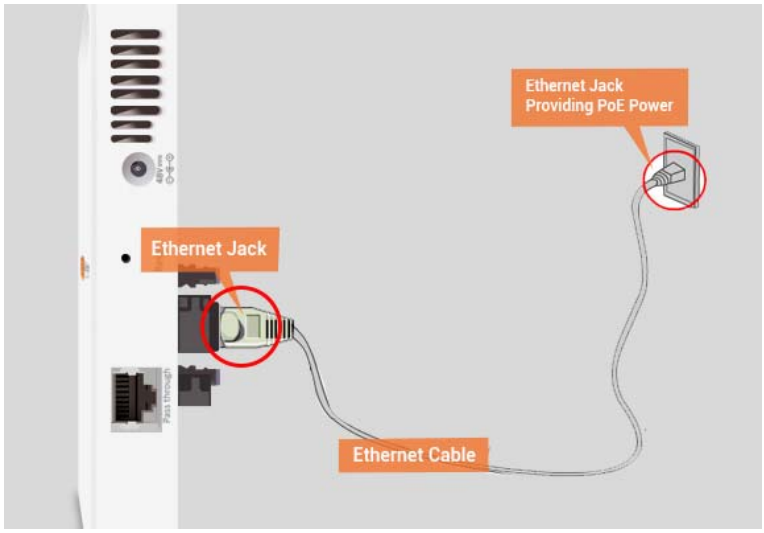
Important: If DHCP is not enabled on a subnet, the device cannot connect to that subnet with zero-configuration. If the DNS entry is not present on the DNS servers or you do not have the DHCP server running on the subnet, you must manually configure the device. Refer to Manually Configuring W-68 for further details.

Using W-68 with PoE

To power on and connect W-68 to the network using PoE, do the following:

1. Connect one end of the network interface cable to the Ethernet port at the rear of the W-68.
2. Connect the other end of the network interface cable to the Ethernet jack that provides PoE power.

Figure 3-1 Power Up and Connect W-68 using PoE



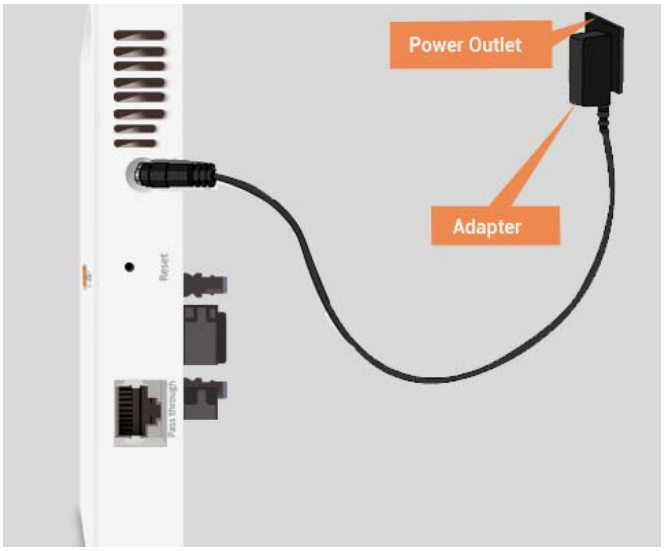
Using W-68 with power adapter

To power up the device, perform the following steps:

1. Plug the power cable into the DC power receptacle at the rear of the device.
2. Plug the other end of the power cable into an 110V~240V 50/60 Hz AC power source.

   Wait until the device is ready. Refer to the respective LED details table based on the configured device mode.

   Figure 3-2 Power Up W-68

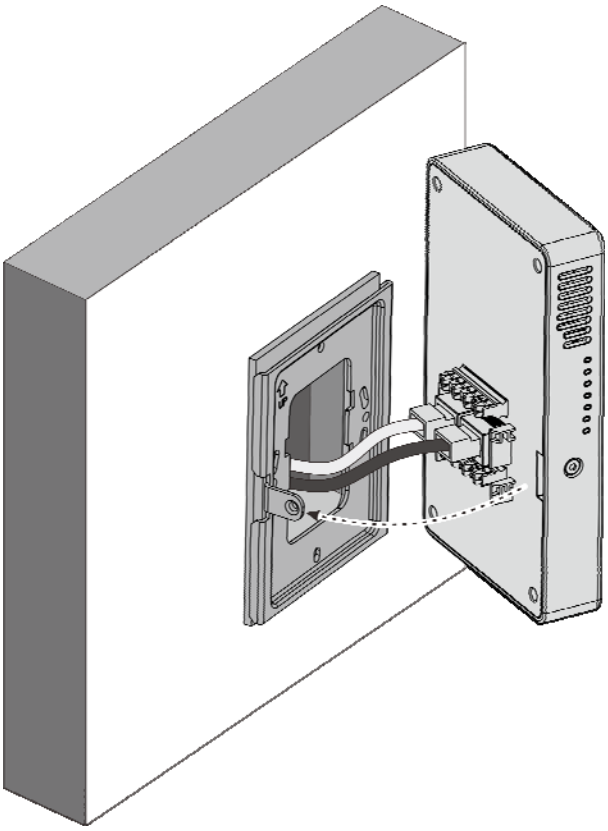


To connect W-68 to the network, perform the following steps:

1. Ensure that a DHCP server is available on the network to provide network configuration to the W-68.
2. Connect one end of the network interface cable to the Ethernet port at the rear of the W-68.
3. Connect the other end of the network interface cable to an Ethernet jack on the desired subnet.

   Wait until the device is ready (approx. 10 minutes).

Figure 3-3. Connect W-68 to network



4. Check the status LEDs on the device. If all LEDs have a solid color glow, then the device is operational and connected to the server.
5. Log on to the server through SSH and run the `get sensor list` command.
   You would see a list of all AirTight devices that are recognized by the server. AirTight Cloud Services users can go to the **Devices** tab and check whether the device is visible under the **Devices** tab.

The device is configured and ready to go operational.

Note: If the zero configuration is not successful, the device must be configured manually. Refer to Manually Configuring W-68 for details.

IMPORTANT! The device is subject to professional installation only. Additionally, if the device is being installed in outdoor environment in the US region, the device template must be appropriately configured and applied on the device by using the AirTight Management Console. You must ensure that the frequencies designated for indoor use are not configured in the device template applied on any device installed in an outdoor environment.

4. Manually Configuring W-68

Important: If the installation in the previous chapter was successful, stop! You do not need to configure the device manually.

Introduction

Manual configuration of W-68 is typically required in the following cases:

- Devices cannot connect to the server through zero-configuration.
- Device needs to be configured in the ND mode.
- Sensor Only (SO) devices cannot connect to the server through zero-configuration. The DNS entry for the server has been changed to an entry other than **wifi-security-server** or a DNS server is not present in the network. This is applicable for multi-server installations.
- Device is placed on a subnet that is not DHCP enabled.

Configuring AP through Config Shell

The Config Shell supports a pre-defined set of commands used to configure the W-68 device. Log in to the device console using the SSH shell.

The steps to configure the device manually through the SSH shell are as follows:

1. Log in and change the default password
2. Set Server Discovery
3. Set Sensor Mode
4. Configure Network Settings

Log in and Change the Default Password

Log in to the Config Shell using the user name **config** and password **config**. Change the default password using the `passwd` command. You can change the device password using device templates. Refer to *Manage Device Template* section under the *AirTight Management Console Configuration* chapter, in the *AirTight Management Console User's Guide* for more details.

Recommended: Although not mandatory, as a best practice we recommend that you change the default password.

Set Server Discovery

The next step is to set the server discovery information. The following are the types of server discovery:

- Server IP based discovery (preferred)
- Service Location Protocol (SLP) based discovery (if wifi-security-server service has been configured)

Use the `set server discovery` command to point the AP device to the correct server.

Figure 4-1 The set server discovery Command

```
Welcome to the Sensor Config Shell.
---------------------------------
Type 'help' to list available commands in the Sensor config shell.
[config]$ set server discovery
Sets information used by Sensor to connect to the Server.

Settings for Server discovery
Please wait while we retrieve the settings...
Select Server Discovery Settings:
1. Server ID Discovery
2. Server IP/DNS Discovery
3. SLP Discovery
Select Option [2]: 2
Set: Server ID Discovery = [OFF]
Set: Server IP/DNS Discovery = [ON]
Set: SLP Discovery = [OFF]
Primary Server IP/Hostname [192.168.8.173]:
Set: Primary Server IP/Hostname = [192.168.8.173]
Secondary Server IP/Hostname [192.168.8.173]:
Set: Secondary Server IP/Hostname = [192.168.8.173]
[config]$
```

Note: If IP address/ host name based discovery is being used and more than one server is present on the network, then you must enter the IP address of the appropriate server.

Set Sensor Mode

The next step is to set the mode of the sensor. There are two possible modes:

- **Sensor Mode:** This is the default mode. In this mode, the device can be connected to a trunk port (802.1Q capable) on a switch. The device then monitors multiple VLANs that are configured on that trunk port and are chosen by the user. The wireless interface of the sensor is enabled. In this mode, a W-68 can monitor up to 16 VLANs.
- **ND Mode:** This mode needs to be explicitly configured. In this mode, the device can be connected to a trunk port (802.1Q capable) on a switch. It then monitors multiple VLANs that are configured on that trunk port and are chosen by the user. The wireless interface of the ND is disabled. In this mode, a W-68 functioning as a WIPS sensor can detect and monitor up to 100 VLANs.

Use the `set mode` command to set the device mode for W-68.

Figure 4-2 The set mode Command for W-68

```
[config]$ set mode
Device operating in AP mode. Please use SGE UI to change mode.
[config]$
```

Configure Network Settings

After the mode is set, you have to configure the network settings. For the Network Detector/Sensor mode, use the `set vlan config` command to configure the IP addresses on the ND.

With the **`set vlan config`** command, you can do the following.

- Add /modify VLAN settings to be configured with DHCP.
- Add/modify VLAN settings to be configured with a static IP address.
- Set communication VLAN.

To configure VLANs, do the following.

1. Type the **`set vlan config`** command to configure all the VLANs.
2. Choose option **1** to configure VLANs for DHCP and option **2** to configure VLANs with static IP address.

The device will restart / reboot after the VLAN configuration.

```
[config]$ set vlan config
Settings for VLAN:
VLAN for Communication with Server (Communication VLAN): Untagged VLAN
================================================================================
ID   Type       IP              Mask            Gateway         Status
================================================================================
U    dhcp   192.168.9.98     255.255.252.0     192.168.11.254   Active and Not M
onitored
================================================================================
DNS settings for Communication VLAN:
        Primary DNS IP Address: [172.31.1.160]
        Secondary DNS IP Address: []
        Tertiary DNS IP Address: []
        DNS Suffix: [testing.test]

Choose from the following options
1.  Add/Modify VLAN settings to be configured with DHCP
2.  Add/Modify VLAN settings to be configured with Static IP Address
3.  Set Communication VLAN
4.  Delete VLAN(s)
5.  Exit
?
```

To configure VLANs with DHCP, you must provide comma-separated VLAN IDs.

```
Choose from the following options
1.  Add/Modify VLAN settings to be configured with DHCP
2.  Add/Modify VLAN settings to be configured with Static IP Address
3.  Set Communication VLAN
4.  Delete VLAN(s)
5.  Exit
? 1

Enter VLAN IDs to be configured for DHCP (as a list of comma separated values
or range of values. For example: 1,5,7-10,13) [u=Untagged,1-4094]: 1,4,6

Use 'get vlan status' command to know the status of the configured vlan(s).

Choose from the following options
1.  Add/Modify VLAN settings to be configured with DHCP
2.  Add/Modify VLAN settings to be configured with Static IP Address
3.  Set Communication VLAN
4.  Delete VLAN(s)
5.  Exit
?
```

To configure VLANs with static IP address, you must provide the IP address, the subnet mask and the gateway.

```
Enter VLAN IDs to be configured with static IP address(as a list of comma
separated values or range of values.For example:1,5,7-10,13)[u=Untagged,1-4094]:
 56
VLAN [56]
IP Address []: 172.17.56.100
Set: IP Address = [172.17.56.100]
Subnet Mask []: 255.255.255.0
Set: Subnet Mask = [255.255.255.0]
Gateway []:  172.17.56.254
Set: Gateway = [172.17.56.254]
Confirm? ([y]/n): y


Use 'get vlan status' command to know the status of the configured vlan(s).

Choose from the following options
1.  Add/Modify VLAN settings to be configured with DHCP
2.  Add/Modify VLAN settings to be configured with Static IP Address
3.  Set Communication VLAN
4.  Delete VLAN(s)
5.  Exit
? 5
Restarting Sensor...
Re-initializing the interfaces using the new configuration settings.
```

To configure/ change the Communication VLAN, do the following

1. Type the **`set vlan config`** command**.**
2. Choose option **3** from the menu that appears.

Configure a static IP address in absence of a DHCP server

1. Connect a crossover cable from the computer to the Ethernet port of W-68.
2. Configure the LAN IP address on the computer in the subnet `192.168.1.0/24`.
3. SSH to IP address: `192.168.1.245` (factory default)
4. Log in to the CLI of the device using default credentials.
5. Configure server discovery on the device.
6. Configure a static IP address on the device. For example: Untagged VLAN `192.168.2.x/24`.
   After completing this step you will lose the SSH connection.
7. Configure the LAN IP address in the range of `192.168.2.x/24` and again SSH to the address assigned in step 6.
8. Check the configuration settings.
9. Remove the crossover connection to the computer and connect the Ethernet port to the local switch.

Configure IPv6 settings

W-68 is IPv6 capable. Use the `set ipv6 config` command to configure advanced options such as DHCP settings, auto negotiation, and manual configuration.

- Enable auto negotiation to discover IP address automatically.
- Enable DHCP settings to obtain addressing as well as more information, such as the DNS address from DHCP server in the network.
- Enable manual configuration to provide manual IPv6 address as well as IPv6 default gateway.

How to configure Communication Key or Passphrase

To configure the communication key or passphrase kindly refer to Appendix A: AP-Server Mutual Authentication for further details.

5. Drawing AF Power from W-68

LAN 4 can behave as a PoE by itself. If AT power is provided through WAN, it is possible to draw AF power from the LAN4. In this situation, the LAN4 behaves as a PoE and can power another device or AP that can run on AF power.

While the existing 802.3af standard has made it possible to power VoIP phones, wireless APs, even some cameras over standard Ethernet cabling since 2003, it cannot meet the demands of some higher-end devices, including cameras with pan/tilt/zoom capabilities, door controllers and POS terminals. In addition, APs that support the upcoming 802.11n standard will likely require the power of 802.3at, although single-radio 802.11n APs should be able to work with 802.3af. As other devices that previously needed individual power supplies become more energy efficient, they might become candidates for 802.3at as their lower requirements bring them into range of that spec.

6. W-68 Config Shell Commands

The following tables detail the W-68 config shell commands.

Table 6-1 get Commands

get Commands	
Command	**Description**
`get ap`	Displays all the currently visible APs
`get interface`	Displays network interface speed and mode
`get ip config (deprecated)`	Displays the IP information
`get log`	Displays the log information as it is created
`get log config`	Displays the configuration of the logger
`get mode`	Displays the mode in which the device is currently configured
`get rf`	Displays if RF monitoring for the device is 'ON' or 'OFF'
`get serial num`	Displays the board number
`get server discovery`	Displays the server discovery/setting information
`get status`	Displays the current running status of all the components
`get version`	Displays the version and build information of all the components
`get vlan config`	Displays VLAN configuration. Both static and dynamic information is displayed.
`get vlan id`	Displays listing of all VLANs which can be detected by ND.
`get vlan status`	Displays status of VLANs which are configured for monitoring by ND.
`get vlan connectivity`	Pings the specified VLAN other than the communication VLAN.
`get model`	Displays the AP model.
`get antenna`	Displays antenna configuration (internal/ external).
`get route`	Displays IP routing table entries.
`get client logs`	Gets client connection logs as it happens.
`get wired trace`	Performs packet capture on Ethernet interface(eth0) upto file size 5MB.
`get ap status`	Displays wireless profiles and associated clients.

Table 6-2. set Commands

set Commands	
Command	**Description**
`set erase`	Sets the erase character to ^H.
`set interface`	Sets network interface properties such as auto negotiation, speed, and duplex settings.
`set ip config`	Runs through the current VLAN and IP config wizard.
`set server discovery`	Sets the server discovery information.
`set vlan config`	Configures list of VLANs and their network settings, to be monitored by ND.
`set ipv6 config`	Sets IPv6 network settings.
`set communication key`	Sets the AP-server shared secret. You must enter a hexadecimal value, of length 32, as the shared secret. It can be used instead of the `set communication passphrase` command. Use this command if you are comfortable working with hexadecimals.
`set communication key default`	Sets the communication key to its default value.
`set communication passphrase`	Sets the AP-server shared secret. You must enter a character string, of length between 10 and 127, as the shared secret. The string is internally converted to hexadecimal format. It can be used instead of the `set communication key` command.

Table 6-3. Miscellaneous commands

Other Commands	
Command	**Description**
`exit`	Exits the config shell session
`help`	Displays help for all commands
`help set`	Displays help for ‘set’ commands
`help get`	Displays help for ‘get’ commands
`help other`	Displays help for ‘other’ commands
`passwd`	Changes the config shell password
`ping <Hostname/IP address>`	Pings a host. Usage: `ping <IP_address/host_name>` For example, `ping 192.168.1.246`
`ping6 <IPv6 address or hostname>`	Pings an IPv6 host Usage: `ping6 <IPv6_address/host_name>`
`reboot`	Reboots the AP
`restart`	Restarts the AP application
`reset factory`	Resets the AP to ‘out of the box’ status
`upgrade`	Upgrades the AP manually from a given IP address

7. W-68 Troubleshooting

Following are the troubleshooting guidelines for W-68.

Symptoms	Diagnosis	Solution
Wi-Fi: any Ethernet: fast blink Power: solid Green	The device did not receive a valid IP address via the DHCP.	Ensure that the DHCP server is on and available on the VLAN/subnet to which the device is connected. If the device still fails to get a valid IP address, you can reboot it to see if the problem is resolved.
	The Ethernet cable is loose. The device is probably disconnected from the network.	Ensure that the Ethernet cable is connected.
Wi-Fi: any Ethernet: slow blink Power: solid Green	Unable to connect to the server	Ensure that the server is running and is reachable from the network to which the device is attached. If there is a firewall or a router with ACLs enabled between the device and the server, ensure that the traffic is allowed on UDP port 3851. Use the server IP-based discovery and ensure that you have correctly entered the DNS name, **wifi-security-server**, on the DNS server. Also, ensure that the DNS server IP addresses are either correctly configured on the, or are provided by the DHCP server. It is also possible that the AP is unable to connect to the server because it has failed to authenticate with the server. In this case, an 'Authentication failed for ' event is raised on the server. Refer to the event for recommended action.

Appendix A: Sensor-Server Mutual Authentication

The Sensor-server communication begins with a mutual authentication step in which the sensor and server authenticate each other using a shared secret. The sensor-server communication takes place only if this authentication succeeds.

After the authentication succeeds, a session key is generated. All communication between the sensor and server from this point on is encrypted using the session key.

The sensor and server are shipped with the same default value of the shared secret. The CLI commands are provided on both server and sensor for changing the shared secret.

Note: After the shared secret (communication key) is changed on the server, all sensors connected to the server will automatically be set up to use the new communication key. Sensors that are not connected to the server at this time must be manually set up with the same communication key to enable communication with this server.

Note: Although the server is backward compatible, that is, older version sensors can connect to a newer version server, this is not recommended.
