D-Link®
Building Networks for People

DAP-3860
Release 1.00

Long Distance Wireless Outdoor Bridge

User Manual

Business Class Networking

Copyright

About This Manual

This user manual is intended to guide professional installer to install the DAP-3860 and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

 **Note:**

- This indicates an important note that you must pay attention to.

 **Warning:**

- This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

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

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

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.

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.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Content

Figure

Table

Chapter 1 Introduction

Introduction

The DAP-3860 is a high-performance outdoor-deployable wireless bridge that provides wireless connectivity among multiple network locations. The DAP-3860 has a built-in 23dBi planar antenna that can deliver up to a 40Km connection. An external antenna may also be used to improve signal quality and improve distance. The DAP-3860 allows for link aggregation by combining multiple links into one link with greater transmission rate.

The DAP-3860 supports bridge mode,it allows for local area network (LANs) in different locations (buildings) to be easily interconnected. The DAP-3860 delivers "last mile" broadband connectivity through its PTP and PTMP capabilities.

The DAP-3860 allows to be operated on PTP mode in one card and on bridge in another. And with an external omni antenna for bridge side may provide users with flexibility in various local coverage applications.

With high throughput and long-distance transmission, the DAP-3860 is an ideal backhaul solution for Carriers, Service Providers and Enterprises!

Appearance

Figure 1 DAP-3860

Key Features

- Provide easy installation and high performance wireless connectivity of up to 40km
- IP67 waterproof housing endures almost any harsh environments
- Support Bridge mode
- Support 64/128/152-bit WEP,TKIP and AES Encryption
- Support WMM and Quality of service (QoS) for enhanced performance
- Proprietary Antenna Alignment Tool helps identify the antenna orientation with the best signal strength
- Link aggregation combines multiple links into one with greater transmission rate
- Buzzer design helps to determine the device power initial condition
- Super mode to boost the data rate up to 108Mbps
- Advanced management tools like SNMP and Secure Shell (SSH)
- User-friendly Web, SSH and SNMP-based management interface

Typical Applications

This section describes typical applications of the DAP-3860.

Telemedicine Broadband Wireless Application

The DAP-3860 primary usage is as a relay or bridging technology that may be combined with cost effective solar power solution allowing for telemedicine application in remote and rural environments. The DAP-3860 is able to deliver stable and high performance broadband connectivity for typical telemedicine applications in a Line-of-Sight environment.

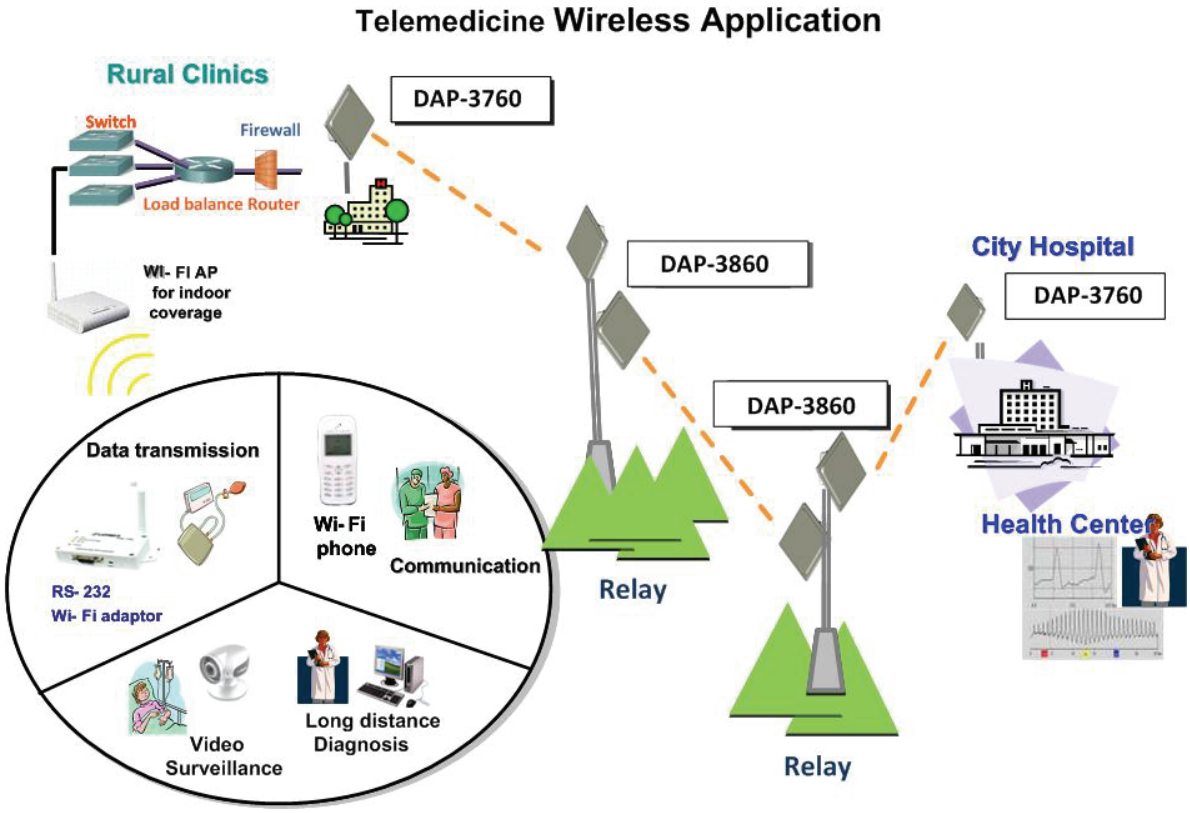


Figure 2 Telemedicine Wireless Broadband

Education Broadband Wireless Application

School in remote area or rural areas can be provided with broadband connectivity via local Internet service providers The relay ability of the DAP-3860 allows for multiple hops to be made thus allowing the DAP-3860 to reach more remote LOS locations beyond 40Kms or to circumvent natural obstructions like mountains..

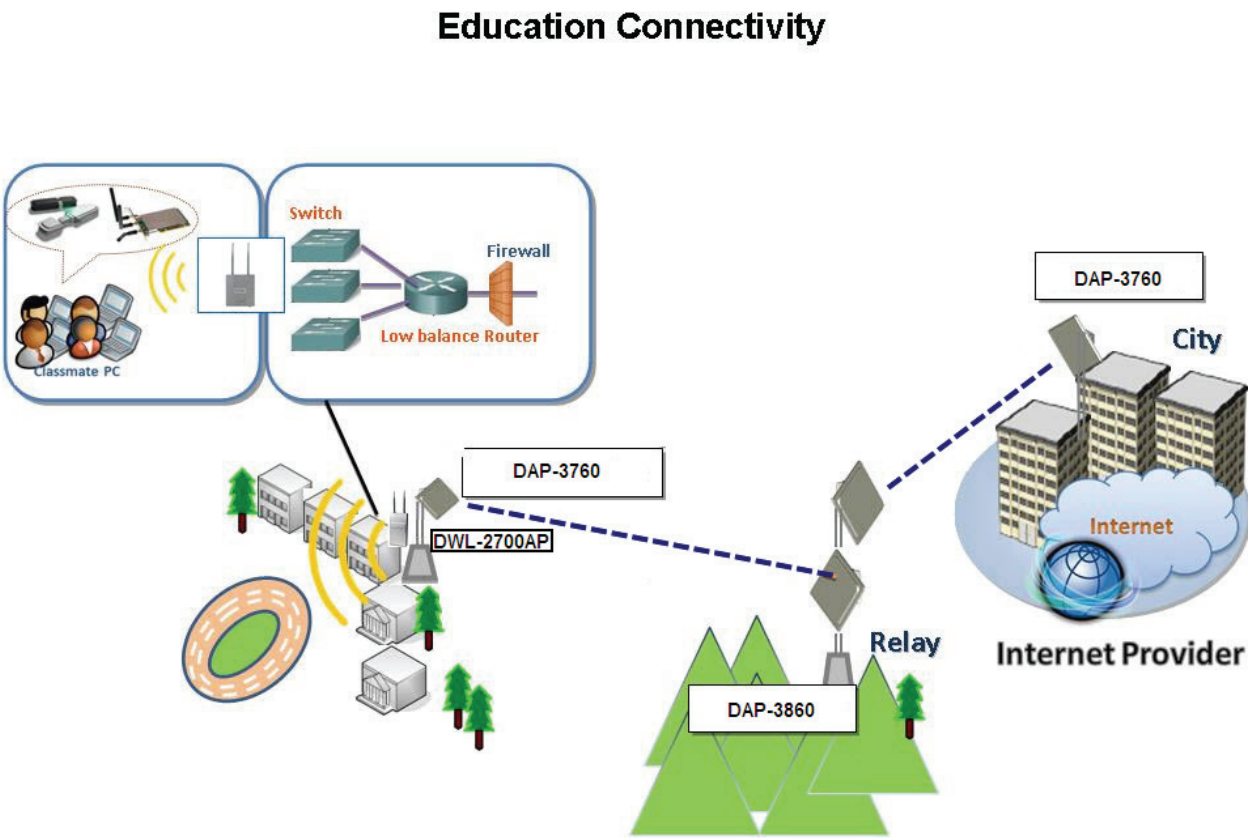


Figure 3 Campus Wireless Broadband

Besides, the DAP-3860 can also be applied into the following environments:

- Cost-effectively provide long distance backhaul for remote areas (like village, oil well, island, mountain and etc.)
- Establish local backhaul for campus, farm and factory
- Provide and access for video streaming or surveillance for industrial and mining enterprises
- Plays as a relay connecting different networks

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing DAP-3860.

Preparation before Installation

Professional Installation Required

1. Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.
2. The DAP-3860 is distributed through distributor and system installer with professional technicians and will not be sold directly through retail store.
3. The equipment shall be installed in RESTRICTED ACCESS LOCATIONS. Access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken. Furthermore, access is through the use of a tool or lock and key, or other means of security, and is controlled b the authority responsible for the location.
4. If you are intended to use an external antenna with the DAP-3860, please contact your supplier/installer to ensure that your unit is set for you have fulfilled all the local regulatory requirements. It is the responsibility of the installer/user to check that the equipment as deployed meets local regulatory requirements.

Safety Precautions

For your safety and proper installation, please read and follow the instructions below:

- ONLY qualified service personnel should service or disassemble this device;
- When installing the device, note the followings:
  - Do NOT use a metal ladder;
  - Do NOT work on a windy or raining day;
  - Do NOT install, use or service the device during a thunderstorm, as this may cause a remote risk of electric shock from lightning;
  - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
  - When the system is operational, avoid standing directly in front of the antenna. Strong RF fields are present when the transmitter is on.
- Ground the device properly with grounding wire to protect against lightening;
- Use ONLY appropriate accessories for the device.
- If the temperatures of the unit surface exceeds the limit, be precautious not to continuous held or touch the device for a certain period of time. 

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

- DAP-3860 with integrated 23dBi antenna ×1
- Mounting Kit ×1
- PoE Injector & Power cord ×1
- Grounding Wire w/ screw ×1
- Waterproof RJ-45 Connector Kit ×1
- Quick Installation Guide ×1
- Product CD ×1

Note:

- Product CD contains Management Tool, Quick Installation Guide and User Manual!

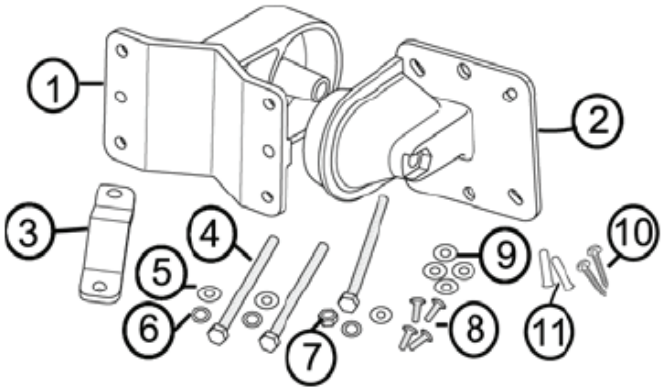
Mounting Kit

- **Wall/Pole Mounting Bracket**

  1. T-Form Bracket ×1
  2. Articulation Pole ×1
  3. Pole Mount Bar ×1

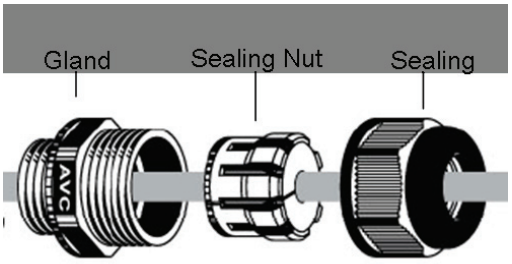
- Fasteners

  4. M8×80 Screw ×2
     M8×90 Screw ×1
  5. M8 Washer ×3
  6. M8 Spring Washer ×3
  7. M8 Nut ×1
  8. M5×16 Screw ×4
  9. M5 Washer ×4
  10. Wood Screw ×4 (for Wall Mount)
  11. Wall/Gyprock Plug ×4 (for Wall Mount)



Waterproof RJ-45 Connector Kit

1. Gland ×1
2. Sealing Nut ×1
3. Sealing ×1



Hardware Installation

Assemble the Mounting Bracket

1. Place the main bracket into the seating and use a spanner to fasten the bracket to the DAP-3860 with M5×16 screws ⑧ and M5 washers ⑨ provided in the hardware packets;

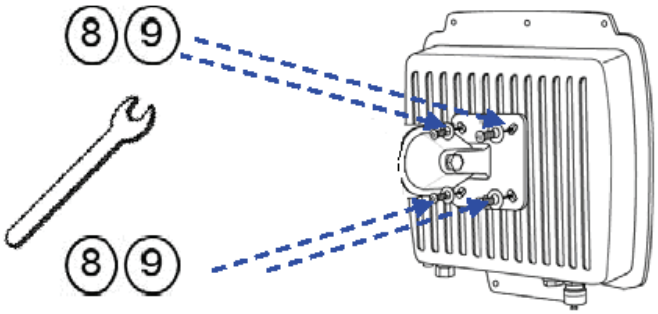


Figure 4 Bracket Mounting – Step 1

2. Assemble the main bracket by placing articulation pole ② to the T-form bracket ① via a M8×90 ④ screw through the insertion axe and fix with the M8 washer ⑤ , spring washer ⑥ and M8 nut ⑦;

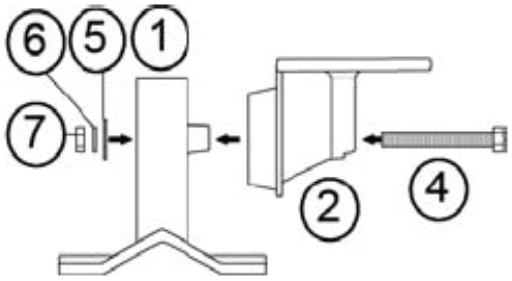


Figure 5 Bracket Mounting – Step 2

Pole Mounting

1. Install the main bracket and the pole mount bar ③ over the top of the pole by securing the drill holes of the pole mount bar to the main bracket ones and insert two M8×80 ④ screws, spring washers ⑥ and washers ⑤ through the drill holes and main bracket;

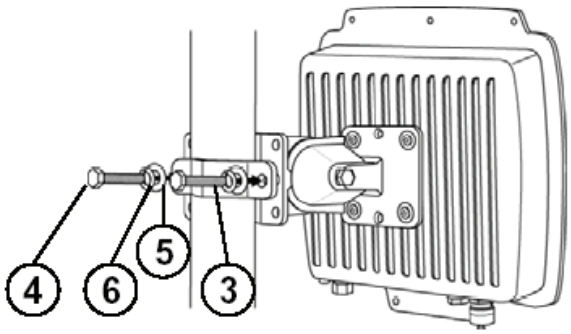


Figure 6 Pole Mounting –Step 1

2. Fasten two M8×80 screws ④ and washers ⑤ through the drill holes and main bracket with a spanner;

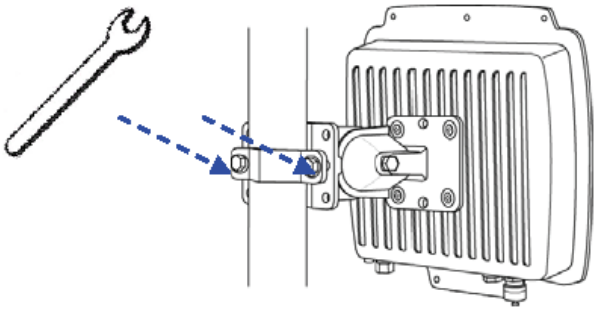


Figure 7 Pole Mounting – Step 2

3. Adjust the antenna for appropriate tilt / vertical orientation.

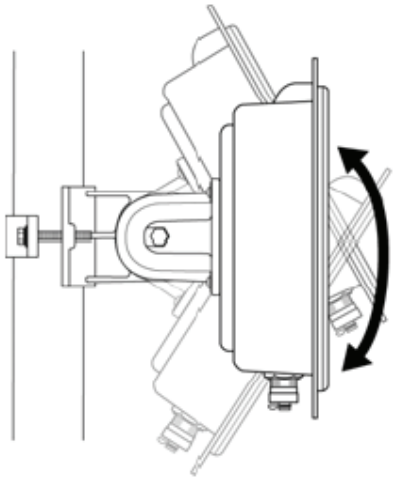


Figure 8 Pole Mounting – Step 3

Note:

- The horizontal and vertical beamwidth of DAP-3860 default antenna is about 10 degree respectively.

Interface Definition

The DAP-3860 currently provides two interfaces at the bottom, which are PoE & Data with a black plastic cover and RS-232 with a light gray cover that labed "WARNING! No PoE". Among which, a black RJ45 waterproof connector will be provided for the PoE + Data interface.

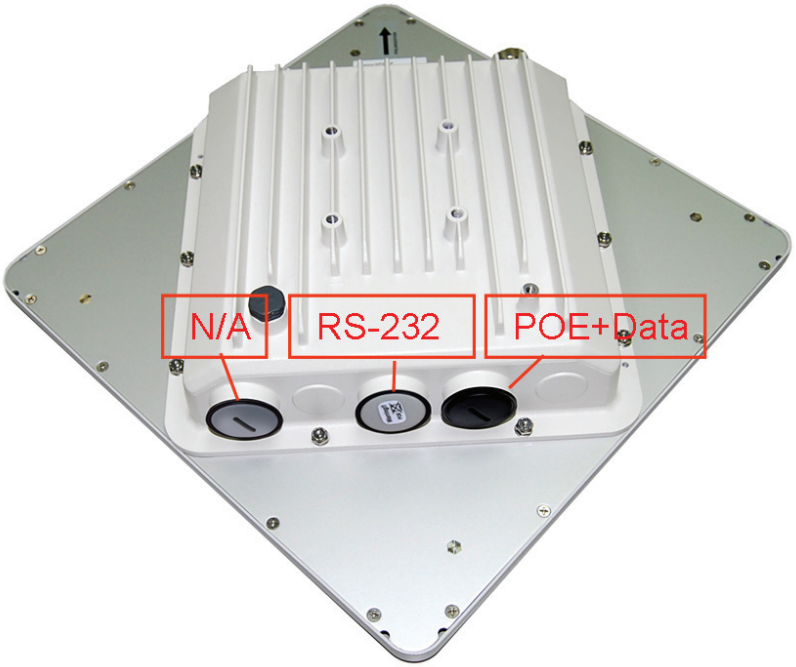


Figure 9 Interface Definition

RS-232

RS-232, which is labeled **COM/RESET**, is used for debugging purposes as well as for hard reset of the DAP-3860. Below you may find the pin definition of the RS-232.

Table 1 PIN Definition

Pin Assignment	Name	Description
P1	TXD0	Data Transmit 0
P2	DSR0	Data Set Ready 0
P3	RXD0	Data Receive 0
P4	TXD1	Data Transmit 1
P5	RXD1	Data Receive 1
P6	DTR1	Data Terminal Ready
P7	Hard Reset	Hard reset the unit
P8	GND	Ground

To reset the device, short P7 (Hard Reset) to P8 (GND) for less than 1 second and the system will reset. If P7 (Hard Reset) is shorted to P8 (GND) for over 5 seconds, the DAP-3860 will be reset to the factory default settings.

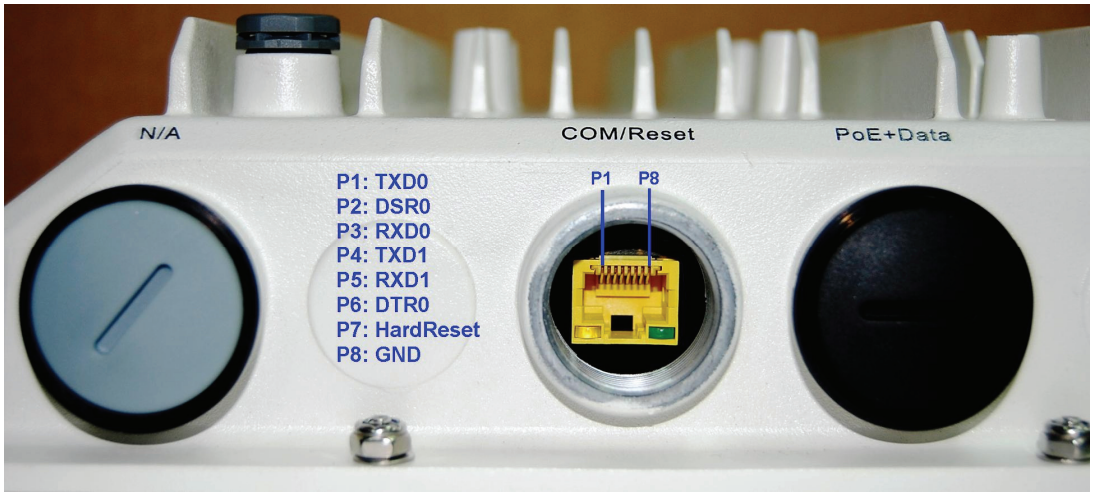


Figure 10 Detailed View of RS-232 Port

Below are the views of RS-232 cover and RJ-45 port respectively, please note the label covered on and DO strictly follow the instructions to avoid damaging your equipment!

Figure 11 Warning Label

Warning:

- Do NOT connect PoE powered Ethernet cable to the RS-232 port; otherwise the port may burnout!

- If RS-232 cable is used outdoor, please DO add a surge protector to protect the equipment circuit!
- Strongly recommend to add a lightning arrestor on the RS-232 port to prevent from lightning attack!

Vent

The vent is designed to exclude vapors and moisture out of the unit as well as repel water, dust, and dirt by the specially designed membrane, thereby preventing the DAP-3860 from electric malfunctioning.

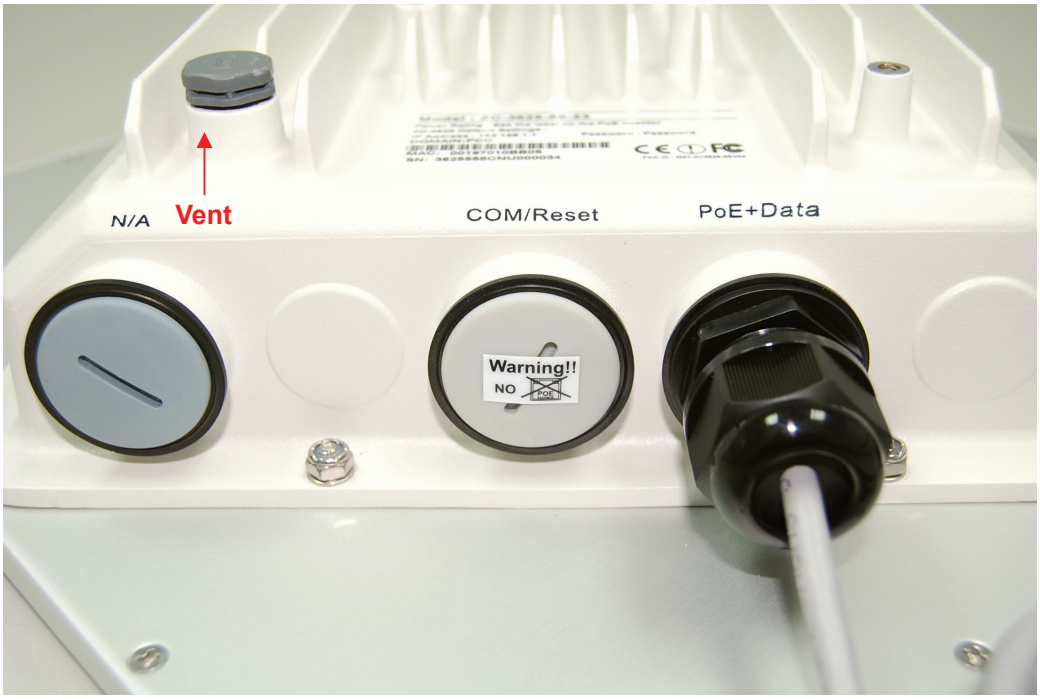


Figure 12 Vent

Connect Up

Before installing the Ethernet cable with a waterproof RJ-45 connector, it is recommended that the Cat-5 RJ-45 coaxial cable be used for the DAP-3860 to power PoE connector.

1. To connect to the hole labeled PoE+Data, open the black cover in advance by using a coin or a slotted screwdriver and then screw in the body of the gland and tighten.

Figure 13 Connect Up – Step 1

2. Slide the sealing nut to the RJ-45 cable from its middle breach and then insert the sealing into the cable.

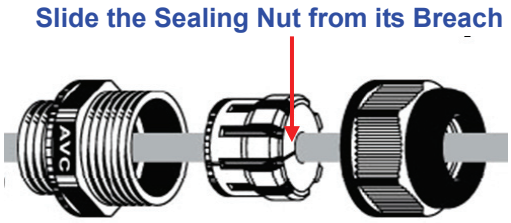


Figure 14 Connect Up – Step 2

3. Insert the RJ-45 connector and make sure that the locking tab snaps home.

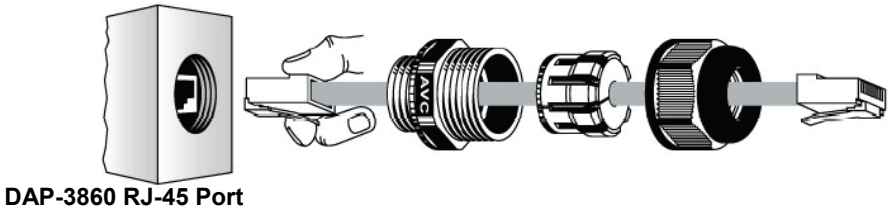


Figure 15 Connect Up – Step 3

4. Screw the sealing on the gland and tighten.

Figure 16 Connect Up – Step 4

Grounding

The DAP-3860 is shipped with a grounding wire. The unit must be properly grounded to protect against power surges. The DAP-3860 grounding point can be found on the bottom of the unit. It is supplied with an appropriate grounding lug for attachment to the ODU.

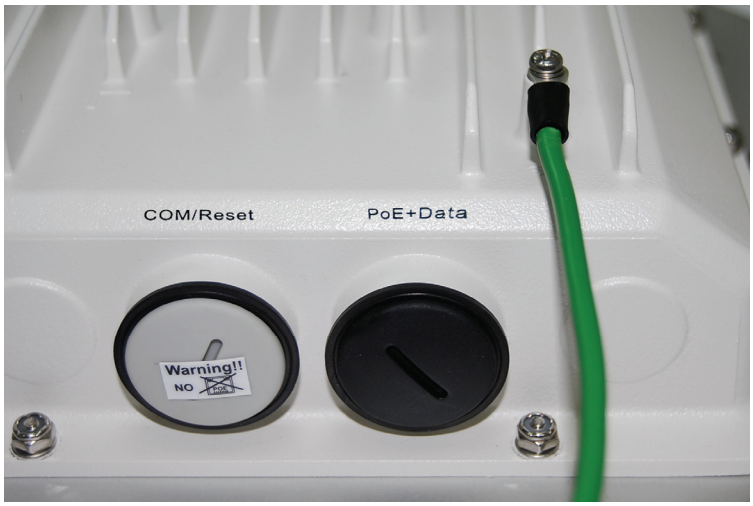


Figure 17 Grounding

Power On

To power up the DAP-3860, follow the steps bellow:

1. Plug a user-supplied Cat-5 Ethernet cable from your wired LAN (or a computer) into the power injector RJ-45 jack (**DATA IN**);
2. Plug a user-supplied Cat-5 Ethernet cable from the DAP-3860 into the power injector RJ-45 jack (**P+DATA OUT**);
3. Connect the power module to the power injector and plug the AC cord into an AC power receptacle;
4. After being powered on, the device will send out the beep sound lasting about 1.5 seconds, informing you that the DAP-3860 is powered up! Wait for about 60 seconds the system will be initialized and start working!

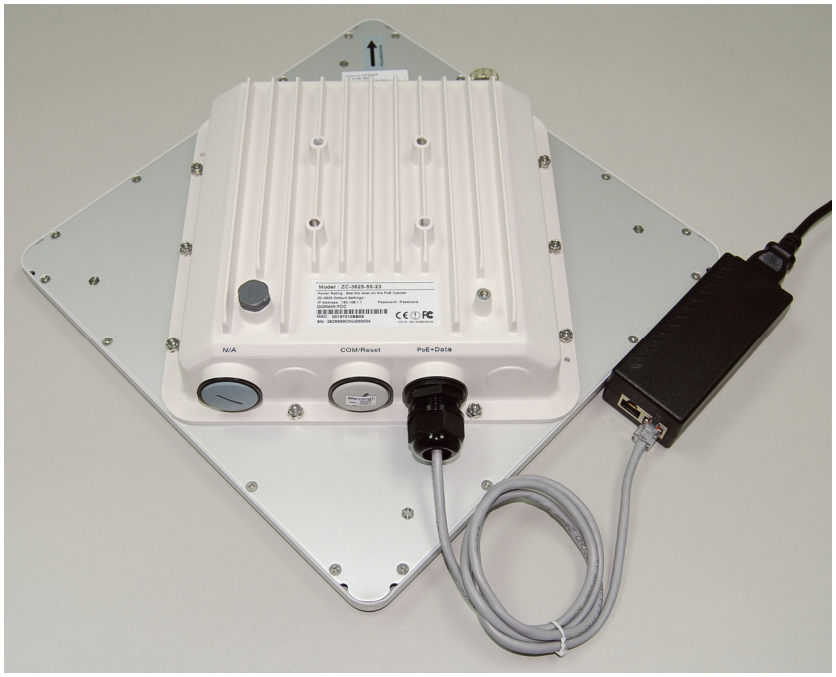
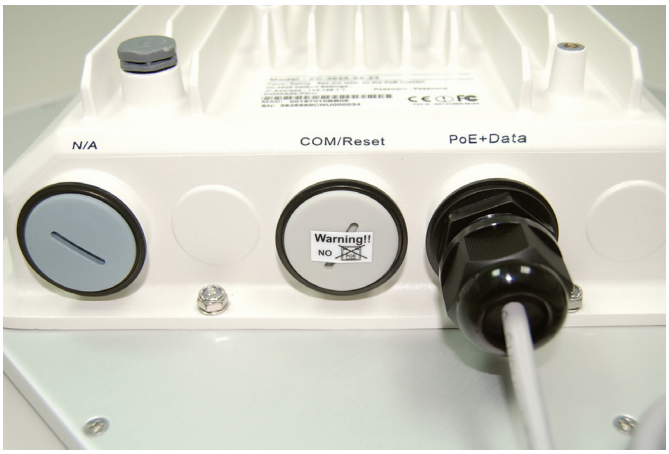


Figure 18 PoE Connection

Warning:

- Make sure PoE is correctly connected to the RJ-45 port on the DAP-3860 labeled PoE+Data, otherwise the extender will be severely damaged!



- When install the secondary antenna, please make sure power off the device to prevent unexpected damage.

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the DAP-3860 factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 2 DAP-3860 Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		Null
Device Name		DAP-3860
Mode		Bridge (CSMA)
Ethernet Data Rate		AUTO
LAN	IP Address	192.168.0.50
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Dynamic(DHCP)		Disable
Spanning Tree		Disable
Link Aggregation		Disable
Wireless Band		IEEE802.11a
Channel/Frequency		149/5.745GHz (CE: 100/5.5GHz)
Data Rate		Best
Bandwidth		20MHz
WMM		Disable
Super Mode		Disable
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Distance in Meters		10000
Security		Open System
Encryption		None
SSH (Secure Shell)		Enable
SNMP Settings	Enable/Disable	Disable
	Public Community String	Public
	Private Community String	Private
	IP Address	0.0.0.0

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.0.x, as the default IP address of DAP-3860 is 192.168.0.50, X can not be 0, 50, nor 255;
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape or Firefox.

How to Login the Web-based Interface

The DAP-3860 provides you with user-friendly Web-based management tool.

- Open IE and enter the default IP address (Default: **192.168.0.50**) of DAP-3860 into the address field. A Security Alert window may popup as below, due to browser's security trusted sites. You may choose to continue to the login webpage.

Figure 19 Security Alert

- Click "**Yes**" will usher you into the login page:

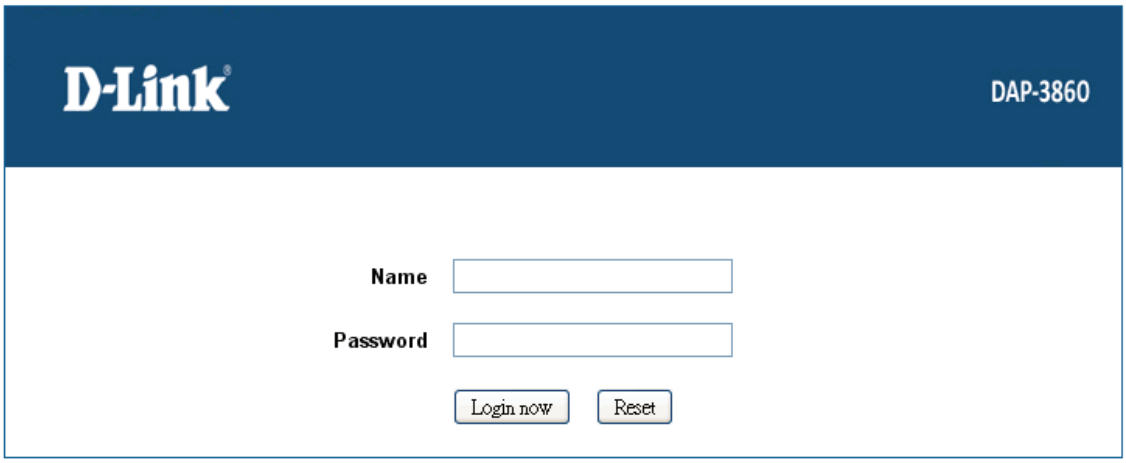


Figure 20 Login

- Enter the username (Default: **admin**) and password (Default: **Null**) respectively and click "**Login Now**" to login the main page of DAP-3860. As you can see, this management interface provides four main options in the black bar above, which are **System**, **Wireless**, **Status** and **Administrator Settings**.

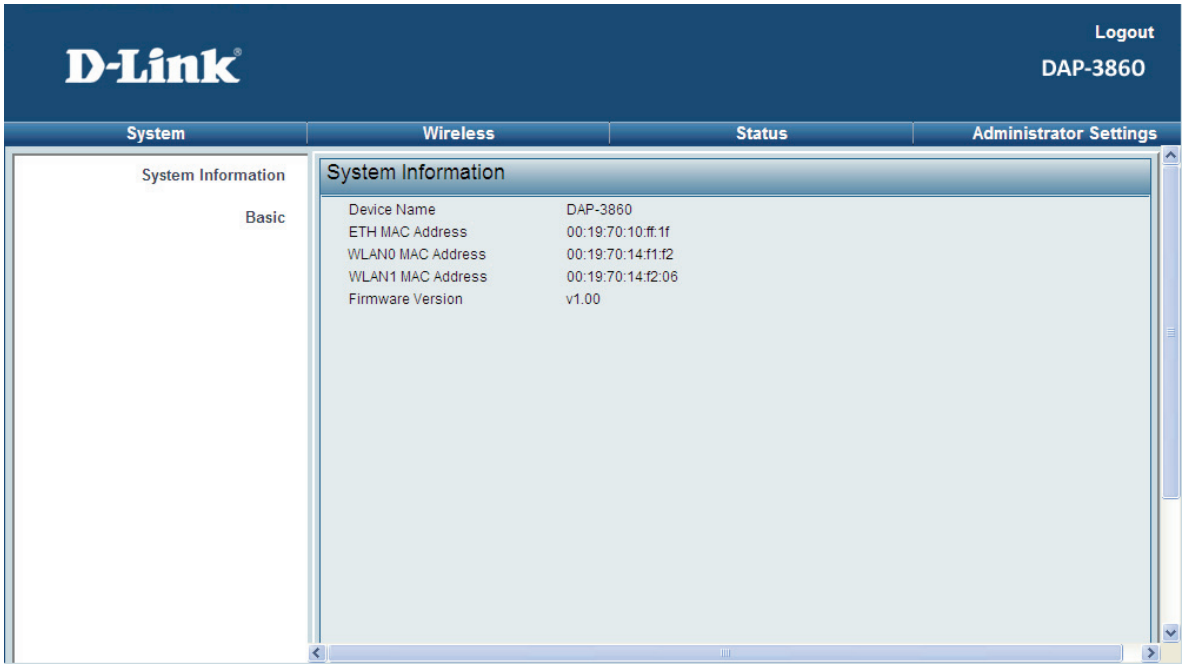


Figure 21 Main Page

Note:

- The username and password are case-sensitive, and the password is no more than 19 characters!

Basic System Setup

For users who use the DAP-3860 for the first time, it is recommended that you begin configuration from "**Basic**" in "**System**" shown below:

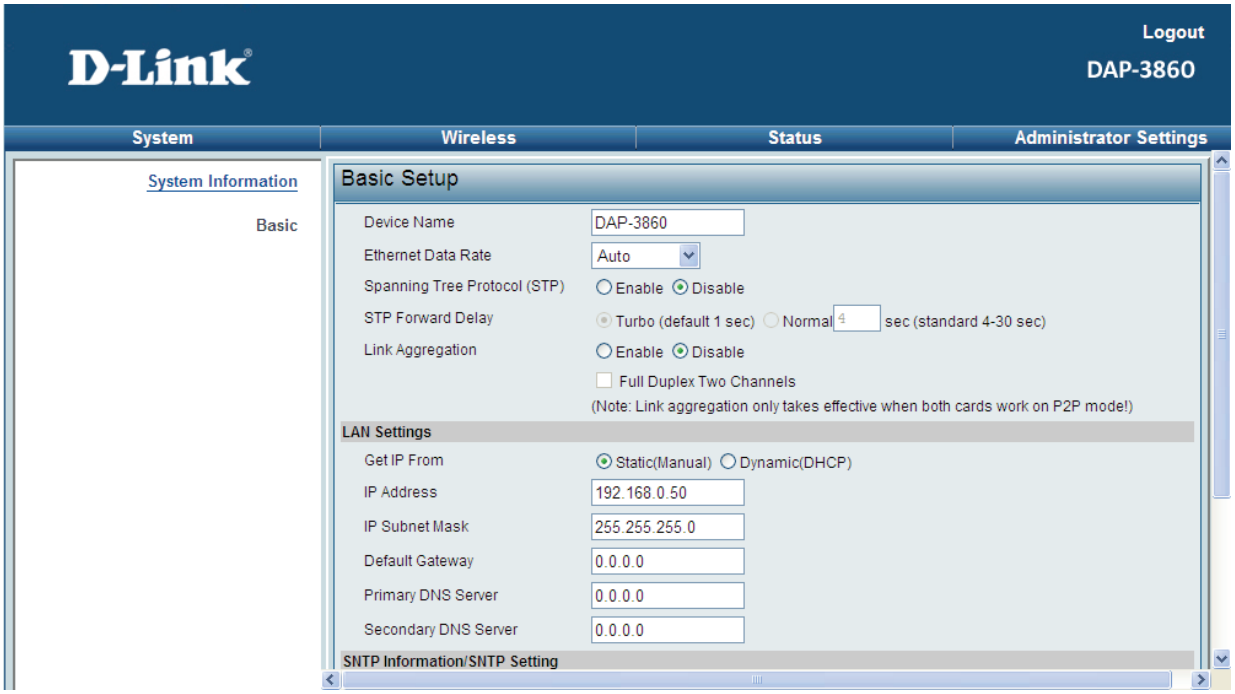


Figure 22 Basic Setup

- **Device Name**

  Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

- **Ethernet Data rate**

  Specify the transmission rate of data.

- **IP Address**

  If you select "**Static**(**Manual)**", you have to specify a static IP address, subnet mask, default gateway and DNS server for your local area network which connects to the LAN port of DAP-3860. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

- **Dynamic(DHCP)**

  Enable "Dynamic" to allow the DHCP server within your local area network to assign an IP address automatically.

- **Spanning Tree Protocol (STP)**

Spanning Tree Protocol is a link management protocol for RCP bridges which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the RCP bridges but establish the redundant link as a backup if the initial link fails.

- **STP Forward Delay**

  STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec. Select Normal if you would like to modify the parameter (4-30 seconds).

- **Link Aggregation**

  Link Aggregation combines two physical network links into a single logical link for increased bandwidth. Besides, it provides load balancing.

Basic Wireless Settings

Open "**Radio**" in "**Wireless**" as below and select "**WLAN 0**" or "**WLAN 1**" to make basic wireless configuration on radio card 1 and 2.

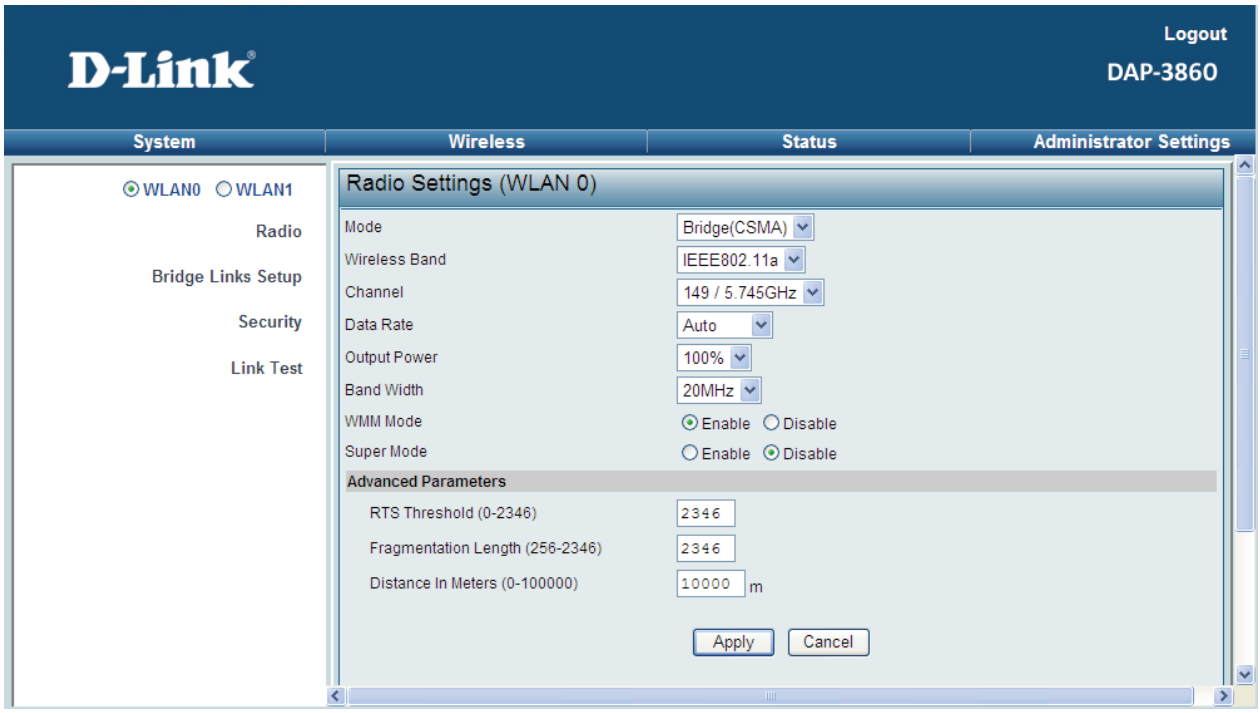


Figure 23 Basic Wireless Settings

- **Mode**

  In a point to point environment where there are only two radios, Peer to Peer is recommended as it works more efficiently.

Bridge (CSMA): The DAP-3860 connects to another wireless device within the same networking program using CSMA protocol. CSMA ensures that only one node is transmitting on the network at any one time. Under this mode, both PTP and PTMP are available. It is highly recommended to use this mode when the distance between two nodes is less than 20km.

Bridge (TDMA): The DAP-3860 connects to another wireless device within the same networking program using TDMA protocol. TDMA divides each cellular channel into multiple time slots to increase the amount of data that can be carried; hence increase the throughput. Under this mode, only PTP is available and is suggested to use when the distance between the two DAP-3860s is greater than 20km.

- **Wireless Band**

  The DAP-3860 can only communicate with wireless devices of 802.11a.

- **Channel/Frequency**

  Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Data Rate**

  Usually "**Best**" is preferred. Under this rate, the DAP-3860 will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low data rate for compromise of a long distance.

- **Band Width**

  Four levels are available: 20MHz and 40MHz. Among them, 40MHz can enhance the data rate more effectively, but will take more bandwidth, thus cause possible interference.

- **WMM**

  WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should support it.

- **Super Mode**

Super mode is an effective way to enhance performance. It can boost the transmission data rate up to 108Mbps. To enable Super Mode, the remote DAP-3860 should enable the function as well.

Chapter 4 Advanced Settings

Advanced Wireless Settings

Open "**Radio**" in "**Wireless**" and turn to "**Advanced Parameters**" at the bottom to make advanced wireless settings.

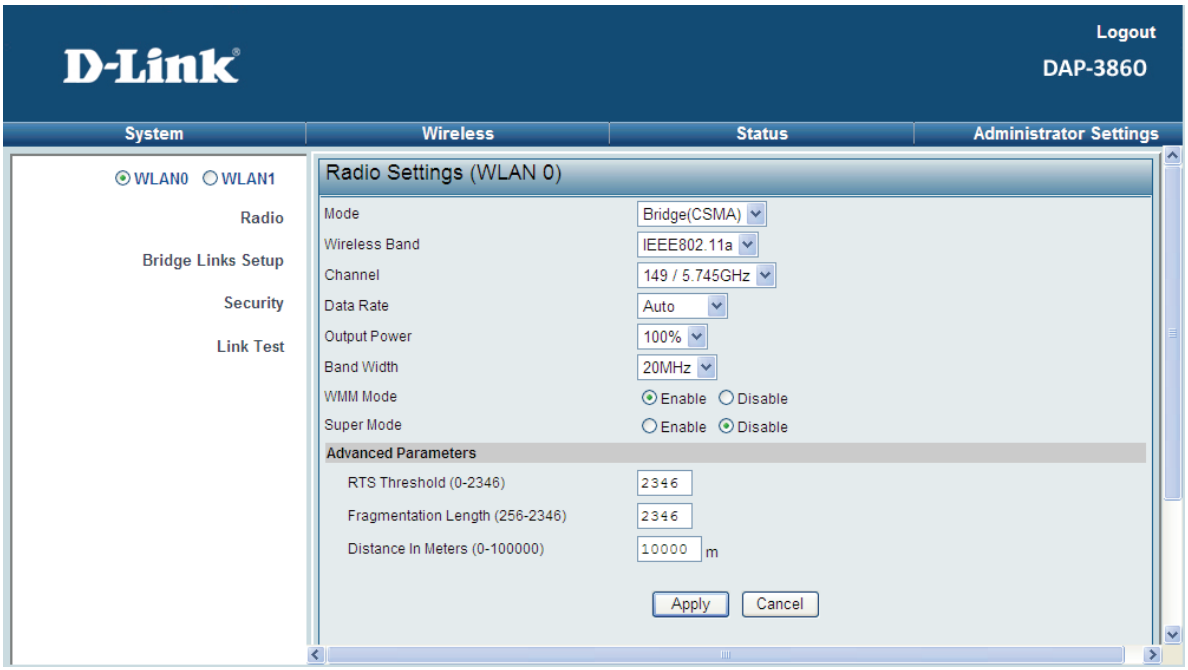


Figure 24 Advanced Parameters

- **RTS Threshold**

  The DAP-3860 sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0-2346 in byte.

- **Fragmentation Length**

  Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Distance in Meters**

  To decrease the chances of data retransmission at long distance, DAP-3860 can auto adjust proper ACK timeout value by specifying distance of the two nodes. Default distance is 10km. This will be only usefully in CSMA mode.

Note:

- We strongly recommended you leave most advanced settings at their defaults except Distance in Meters; any modification on them may negatively impact the performance of your wireless network.

Bridge Links

Open "**Bridge Links Setup**" in "**Wireless**". Bridge Links allow establishing PTP or PTMP connectivity with as most four remote wireless devices, this feature only available under Bridge (CSMA) mode. Select "**WLAN 0**", and input the MAC addresses of radio cards from remote unit respectively.

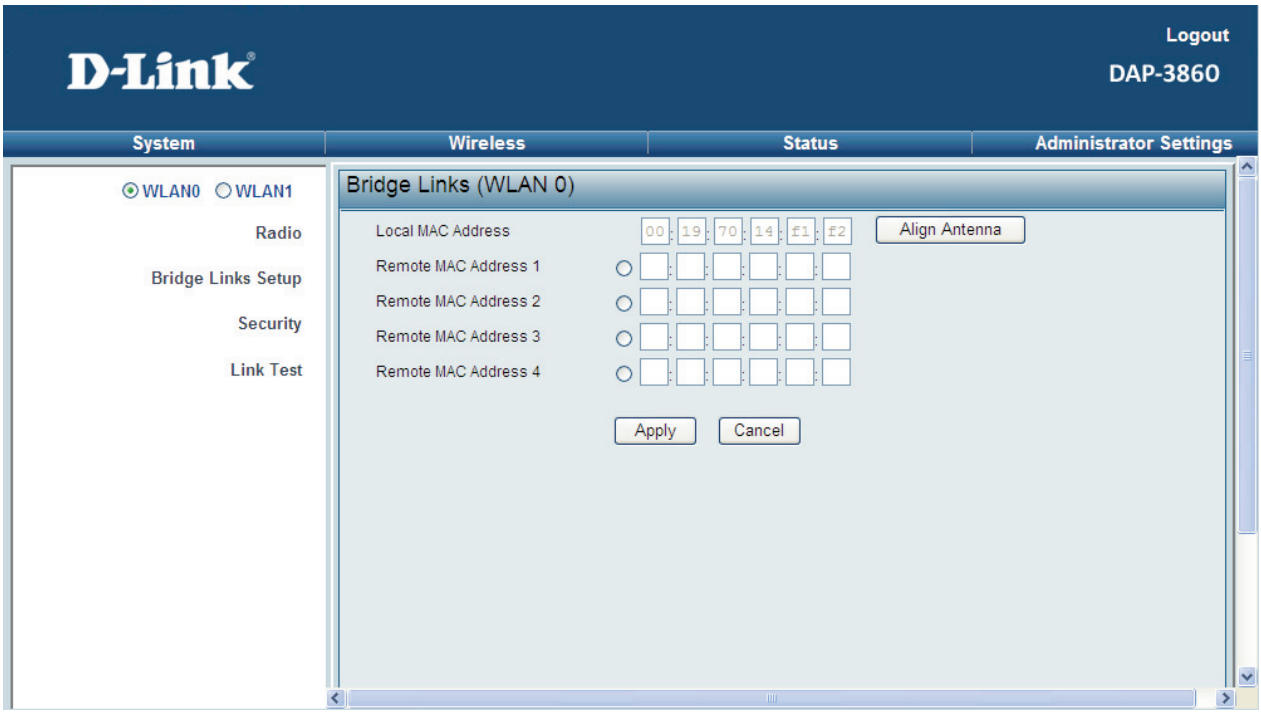


Figure 25 Bridge Links for CSMA

The other way to establish PTMP connectivity is to setup the same group id under "**Radio**" in "**Wireless**". This feature only available under Bridge (TDMA) mode and only devices with the same Group ID can communicate.

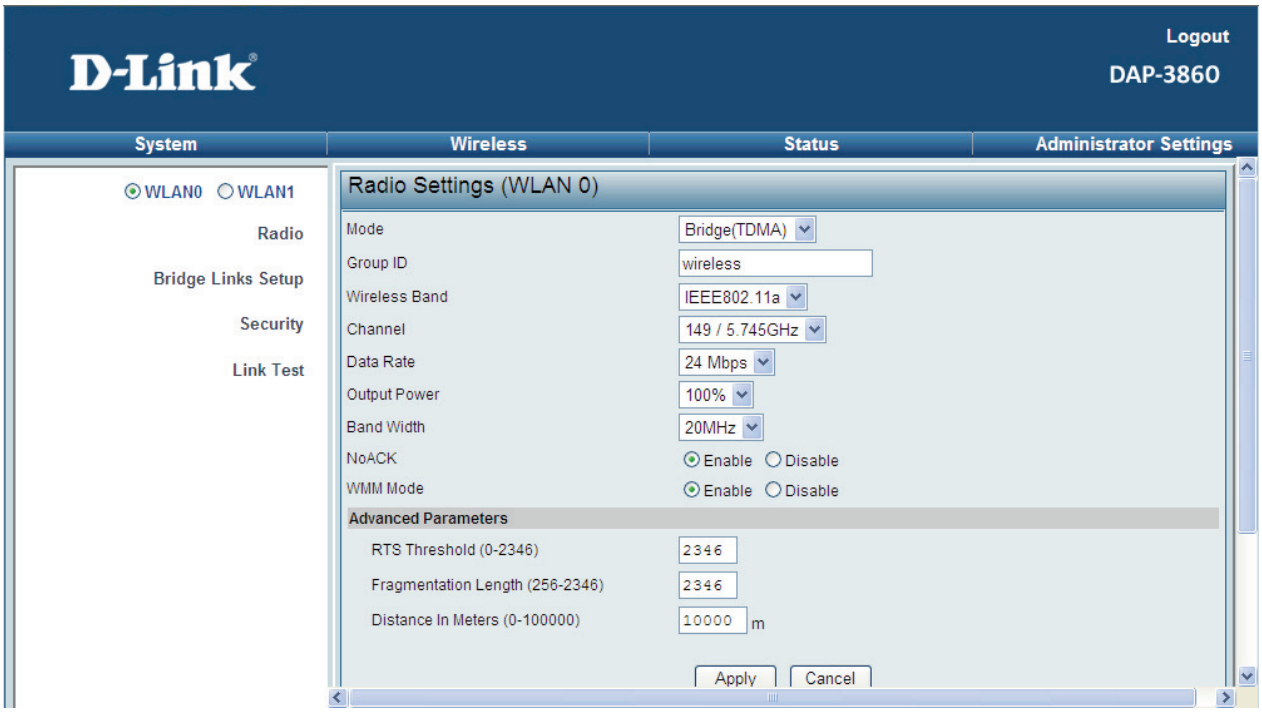


Figure 26 Bridge Links for TDMA

Note:

- When establish PTMP network, make sure all the remote wireless devices are within the antenna beam width.

Antenna Alignment Tool

Under Bridge (CSMA) mode, Antenna Alignment Tool is available. This function helps to point in the approximate direction of the remote DAP-3860 antenna and assist user easily align the local antenna to reach maximum signal strength.

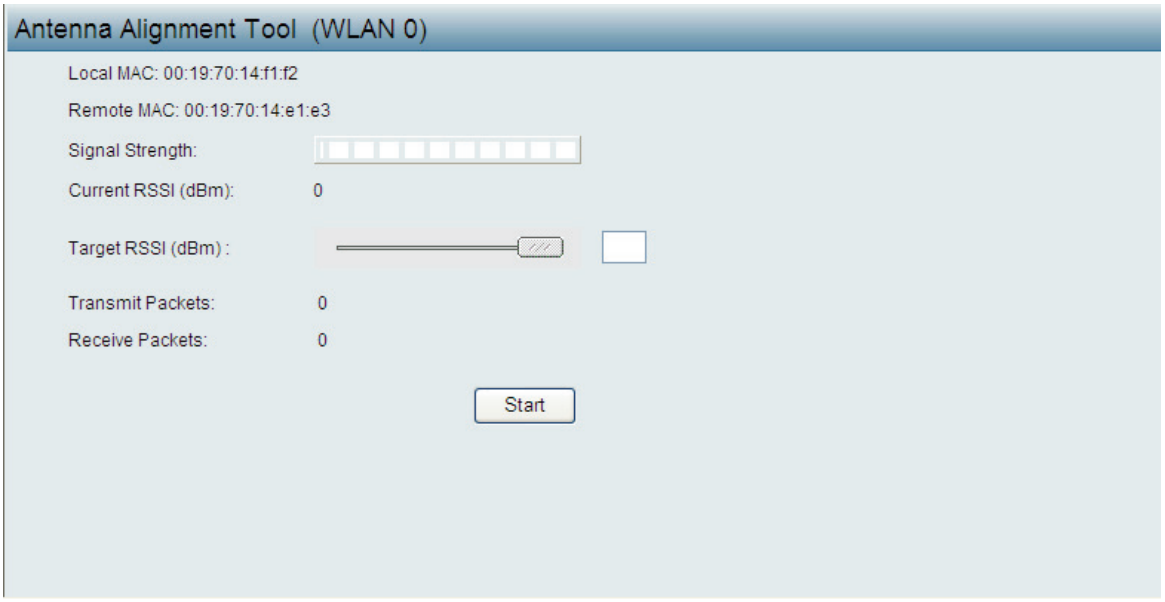


Figure 27 Antenna Alignment Tool

To use Antenna Alignment Tool, follow the steps bellow:

- Open "**Bridge Links Setup**" and select "**WLAN 0**" or "**WLAN 1**". By clicking "**Align Antenna**" button, "**Antenna Alignment Tool**" window will popup.
- Set the target RSSI (e.g. -70dBm) and click "**Start**" button.
- Wait about 5 seconds, the antenna alignment starts and performs alignment every one second.
- Fix the local antenna and adjust the remote antenna elevation and horizontal direction. During the adjustment, observe "**Current RSSI**" in local DAP-3860. The value will refresh every 1 second. Fix the remote antenna when it reaches your expectation. Usually, RSSI between -60 and -70dBm indicates rather good signal strength.
- Adjust the local antenna after fixing the remote one. During the adjustment, observe "**Current RSSI**" in the remote DAP-3860. Fix the local antenna when it reaches your expectation.
- When the antenna alignment tool starts, the DAP-3860 will issue beep sound to indicate current RSSI. Once the tool is closed the DAP-3860 will stop beeping. Frequency of beep indicate the following RSSI:

Table 3 RSSI-Beep Frequency

RSSI	Beep Frequency
>-50	100 /sec
-50~-60	50 /sec
-60~-70	5 /sec
-70~-80	2 / sec
-80~-90	1 /sec
< -90	No beep sound

Link Test

Under Base Station, CPE or Bridge (TDMA) mode when Antenna Alignment Tool is not available, Link Test provides another option to check the signal strength towards the connecting device. Open "**Link Test**" in "**Wireless**" as below, and click "**Refresh**" to view the current signal strength of wireless connectivity. The table will be updated every 3 seconds. If the signal is not so good, align the antenna manually.

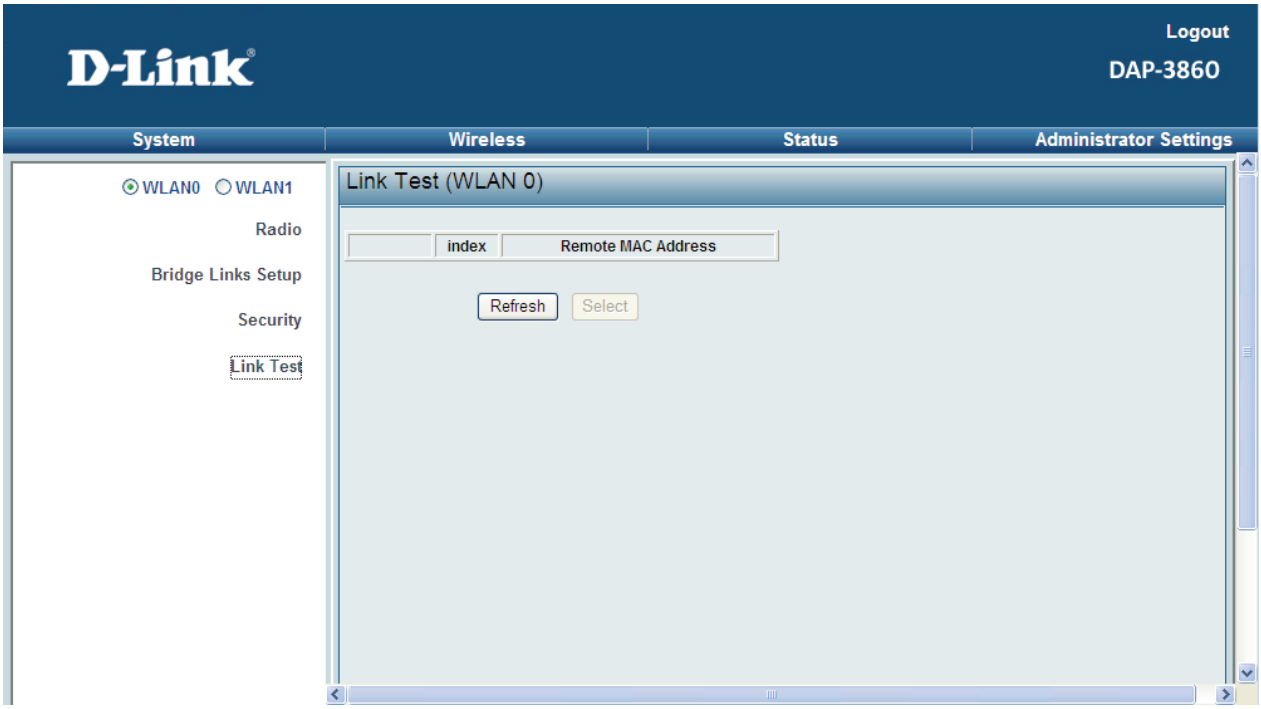


Figure 28 Link Test

Link Aggregation

Link Aggregation combines two physical network links into a single logical link for increased bandwidth. With it enabled, users can increase the capacity and availability of the communications channel between devices (both switches and end stations). Besides, link aggregation also provides load balancing.

Open "**Basic**" in "**System**", Link Aggregation is as below:

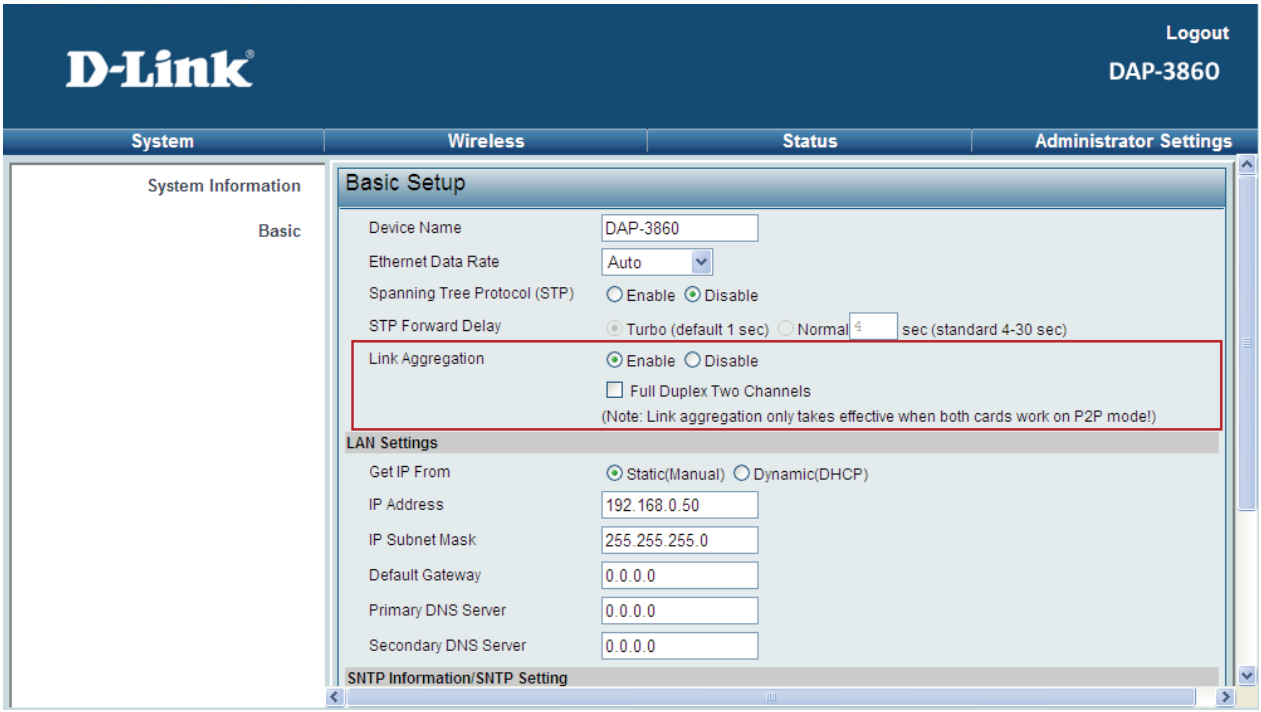


Figure 29 Link Aggregation

- **Full Duplex Two Channels:** Normally, the wireless module in DAP-3860 receives and transmits wireless packets concurrently; if check this box, it only transmits wireless packets on WLAN but stops receiving. Thus the wireless performance could be enhanced further more.

Note:

- Link aggregation takes effect only when both cards work on Bridge (CSMA) mode!

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, DAP-3860 provides you with rock solid security settings.

Security Profile Configuration

Open "**Security**" in "**Wireless**" as below:

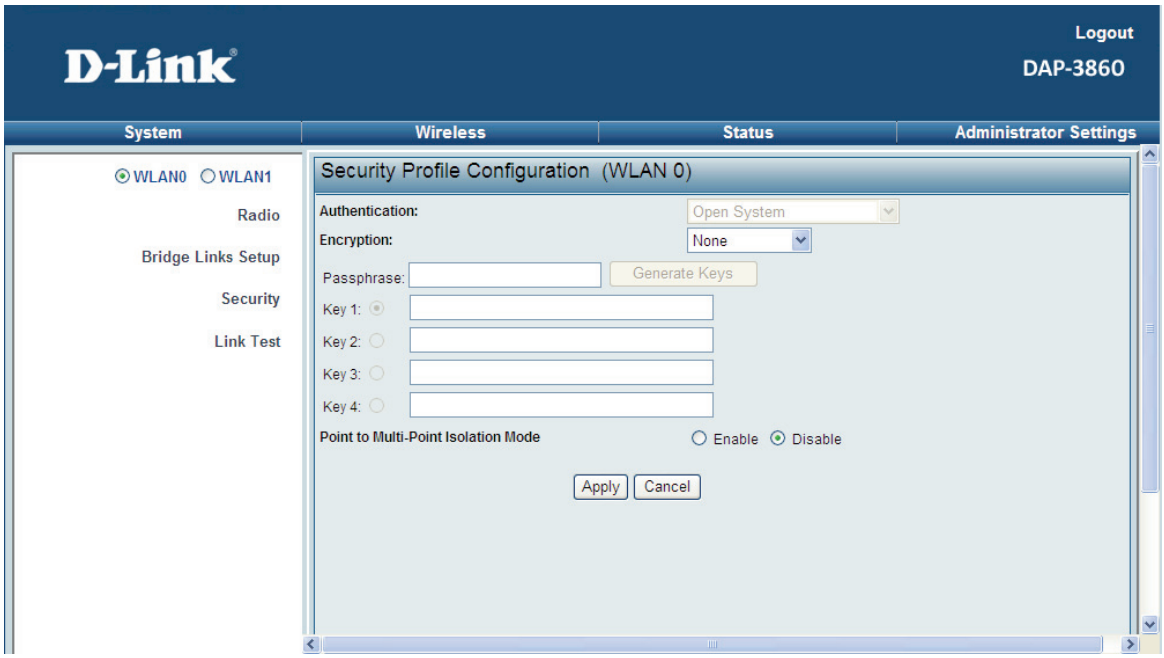


Figure 30 Security

- **Network Authentication**

  Open: It allows any device to join the network without performing any security check.

- **Encryption**

  If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

  None: Available only when the authentication type is open system.

  64 bits WEP: It is made up of 10 hexadecimal numbers.

  128 bits WEP: It is made up of 26 hexadecimal numbers.

  152 bits WEP: It is made up of 32 hexadecimal numbers.

  TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

  AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the DAP-3860 and other wireless devices that connecting with it, can the communication be established!

Chapter 5 Management

View DAP-3860 Basic Information

Open "**System Information**" in "**System**" to check the basic information of DAP-3860, which is read only.

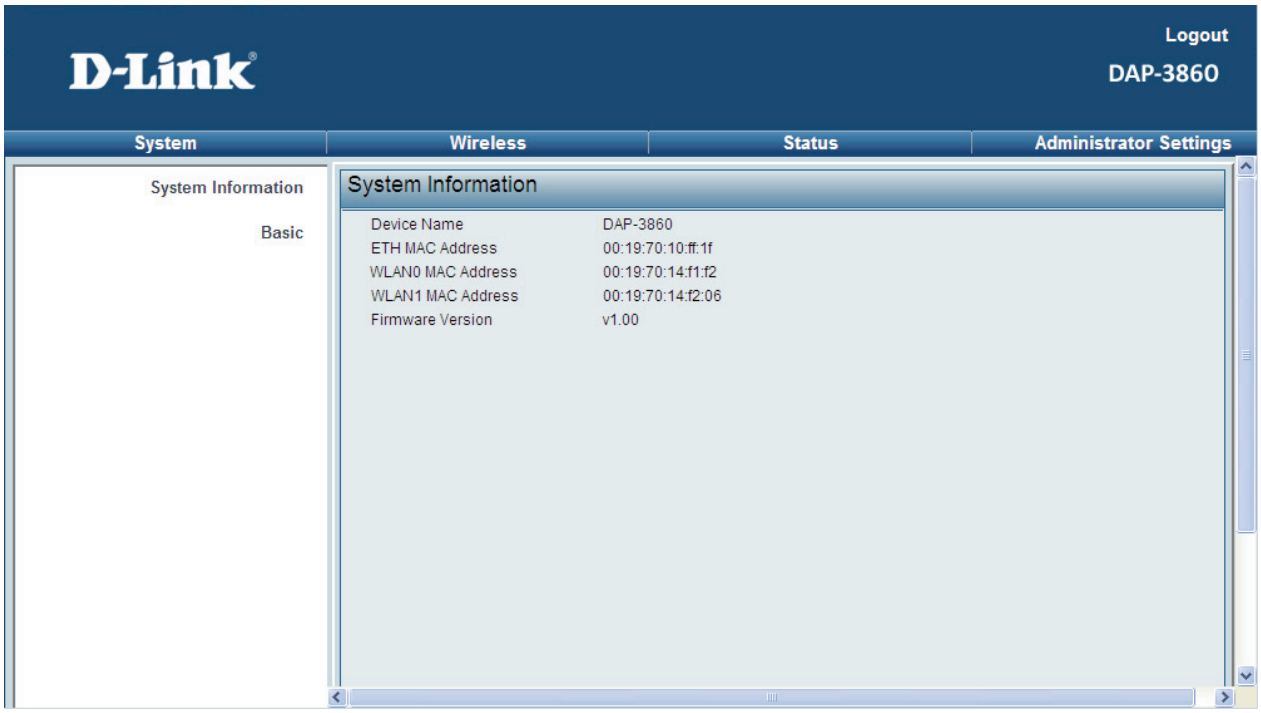


Figure 31 Basic Information

View Ethernet Traffic Statistics

Open "**Ethernet Status**" in "**Status**" to check the data packets received on and transmitted from the Ethernet port in LAN. Click "**Refresh**" to view current statistics. All is read only.

Figure 32 Ethernet Traffic Statistics

View Wireless Statistics

Open "**Wireless Status**" in "**Status**" to check the data packets received on and transmitted via wireless network. Click "**Refresh**" to view current statistics. All is read only.

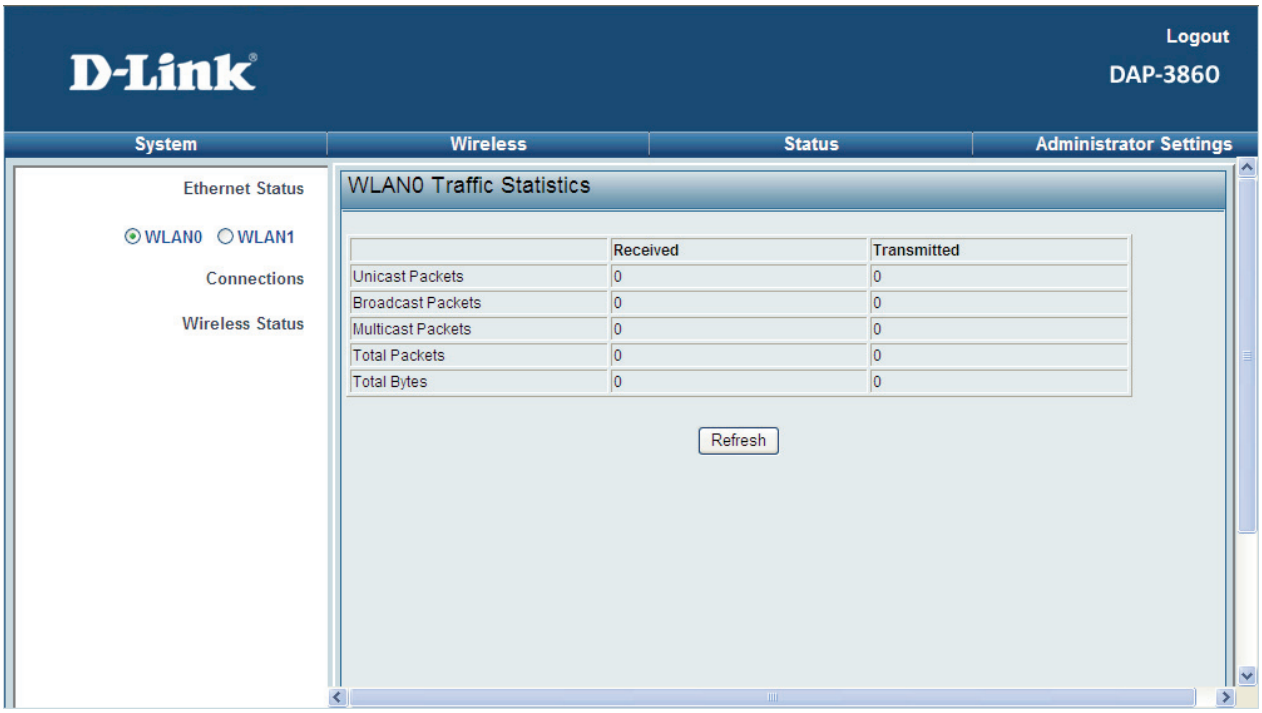


Figure 33 Wireless Statistics

Connections

Open "**Connections**" in "**Status**" to check the information of remote devices connected with the DAP-3860, these values also help determine whether the antenna is aligned in an appropriate direction. The table will be updated every 30 seconds. All is read only.

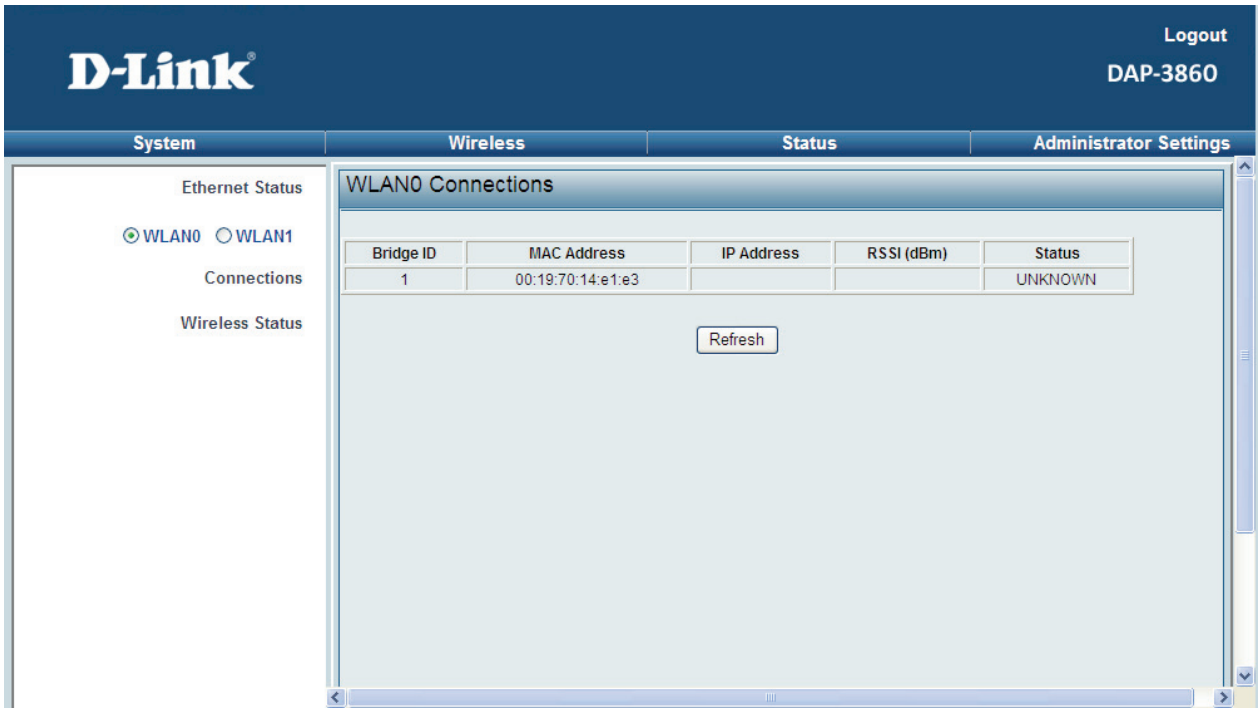


Figure 34 Connections

Password

From "**Password**" in "**Administrator Settings**", you can change or default the password to manage your DAP-3860.

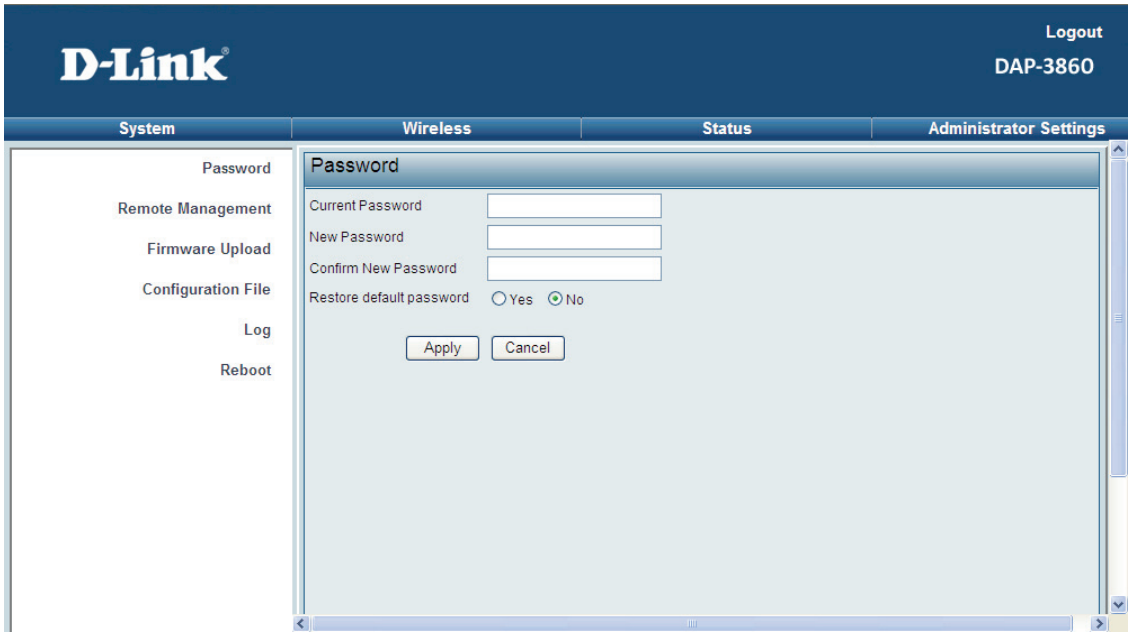


Figure 35 Password

- **Password**

  For security concern, you have to enter the current password first and then enter the new one twice respectively in "**New Password**" and "**Confirm New Password**" fields.

- **Restore Default Password**

  If you would like to restore the default password, enter the current password first and then check "**Yes**" and click "**Apply**" to default the password.

Note:

- The password is case-sensitive and its length can not exceed 19 characters!

Remote Management

The DAP-3860 provides you with two more options for device management, which are SSH (Secure Shell) and SNMP Settings.

Open "**Remote Management**" in "**Administrator Settings**" to configure the remote management of DAP-3860.

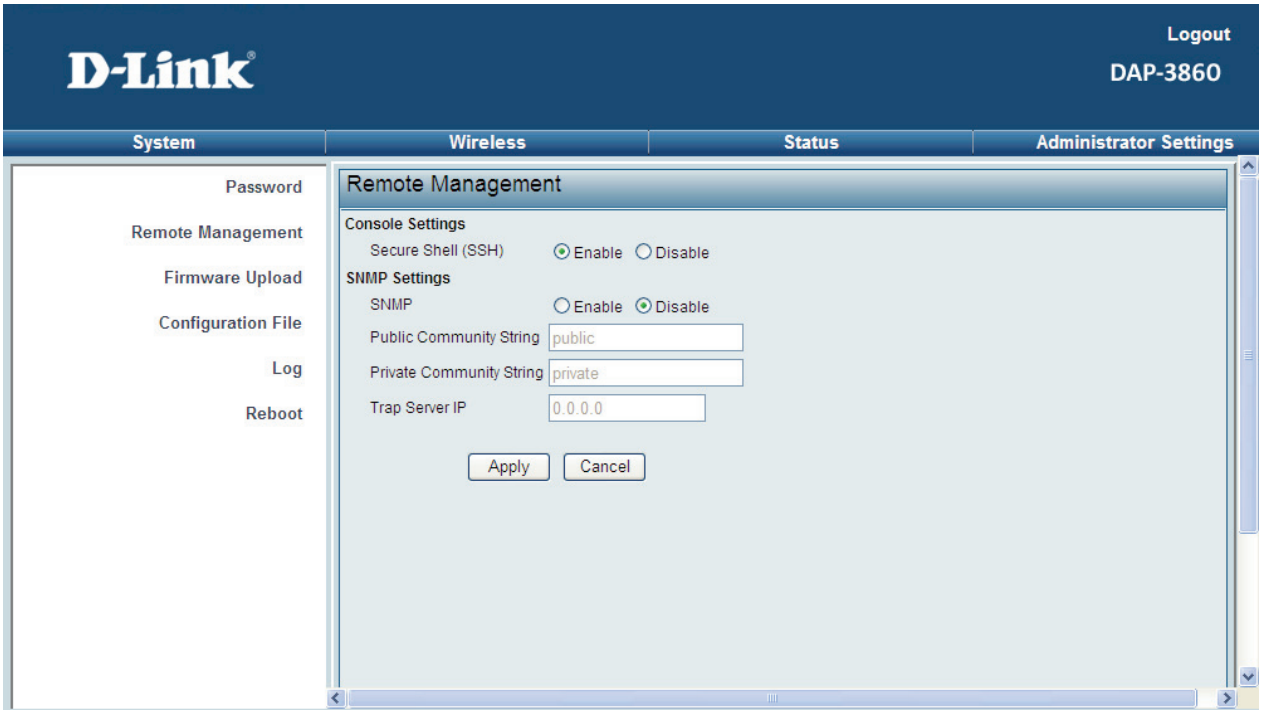


Figure 36 Remote Management

Console Settings

The DAP-3860 supports CLI management, which could be accessed by Secure Shell (SSH). It is recommended PuTTY be used to login. Download it from http://www.putty.org/ for free. The minimum system requirement for using PuTTY is Windows 95, 98, ME, NT, 2000, XP and Vista on Intel x86.

Follow the steps below to implement:

- Once the program is downloaded, open up by double-clicking  putty.exe; Note that before using PuTTY, be sure you are able to connect to the DAP-3860.
- Enter IP Address of DAP-3860 (Default: **192.168.0.50**), Port (22) and check SSH as connection type;

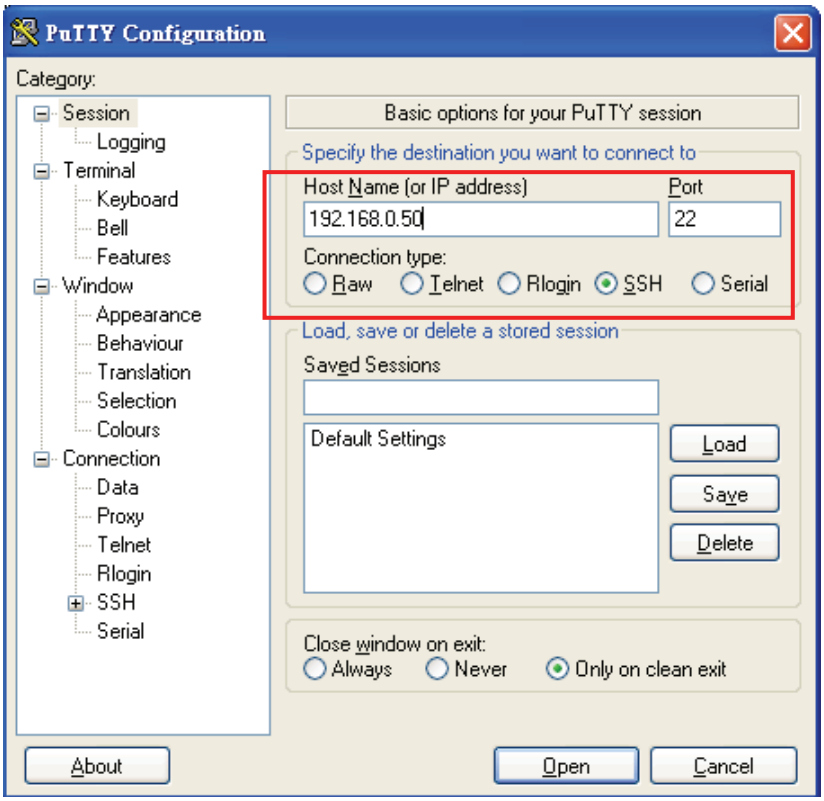


Figure 37 PuTTY Configuration 1

- From "**Connection**" in the left menu bar, click "**SSH**"; select "**2**" as "**Preferred SSH protocol version**"; make "**3DES**" the top position in "**Encryption cipher selection policy**";

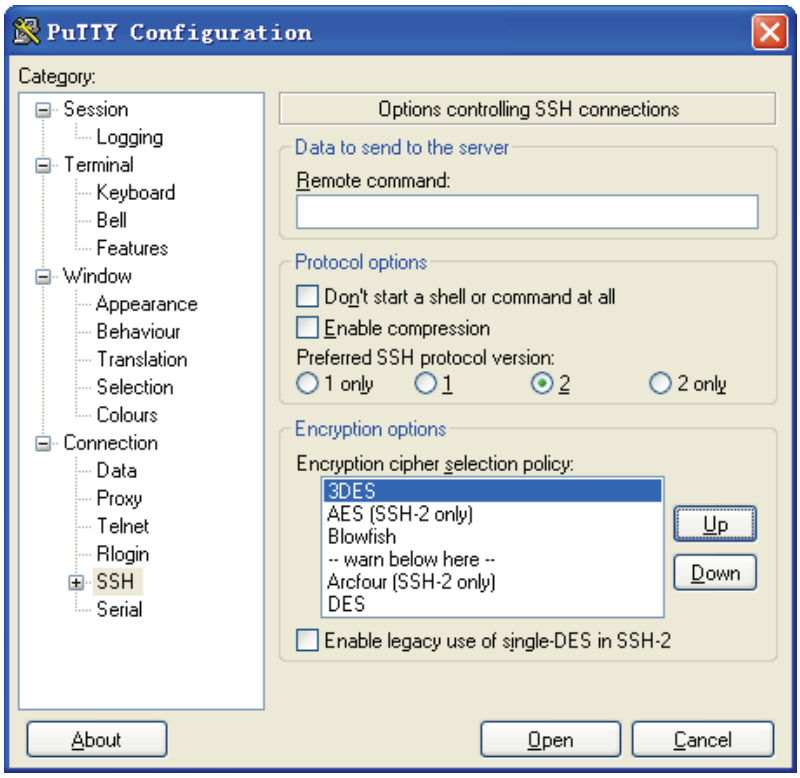


Figure 38 PuTTY Configuration 2

- Click "**Open**", a window as below will popup:

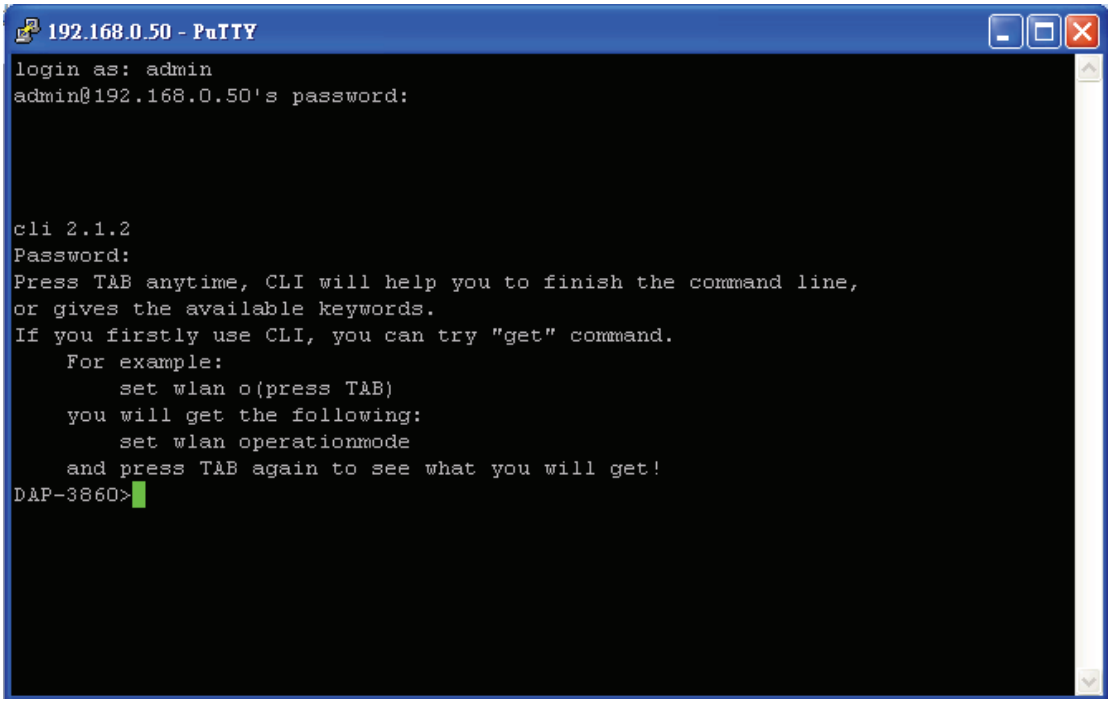


Figure 39 SSH

- Enter the user name and password (Default user name/ password: admin/password) respectively, you will see "DAP-3860**>**", which is the name of DAP-3860;
- Enter "**help**" command to get setting information; alternatively, you can refer to Appendix C. SSH Settings for details.

SNMP SETTINGS

The DAP-3860 supports SNMP management. Set the SNMP parameters and obtain MIB file before remote management.

- From "**Remote Management**" in "**Administrator Settings**", set the parameters for SNMP:
  - Enable SNMP by checking "**Enable**";
  - Specify the "**Public Community String**", "**Private Community String**" and "**Trap Server IP**"
  - Hit "**Apply**" to save settings.
- Obtain MIB file via FTP:
  - Enter ftp 192.168.0.50 , user name (Default: admin) and password (Default: Null);
  - After successful login, enter command "**get Dlink.mib**", the information will as below and then bridge.mib file is obtained.

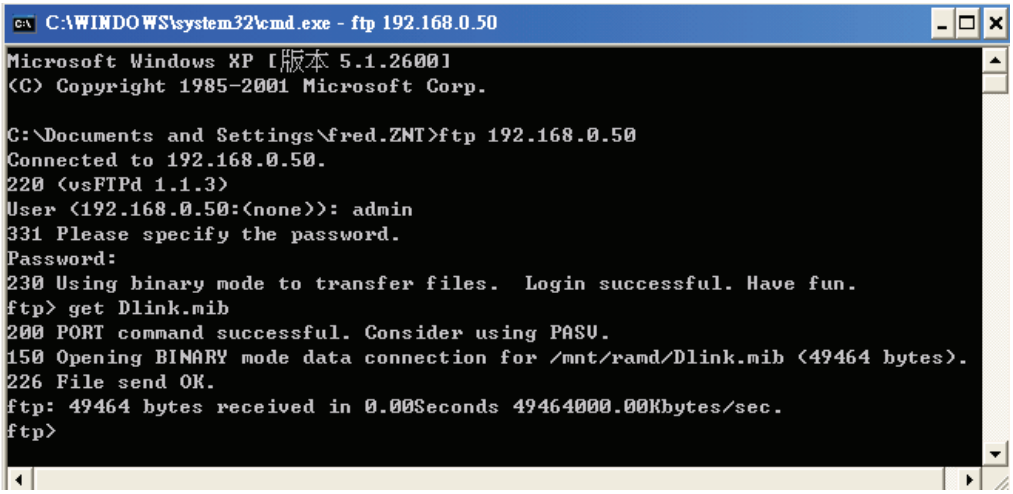


Figure 40 Obtain MIB File

SNTP Information/SNTP Setting

Compliant with NTP, the DAP-3860 is capable of keeping its time in complete accord with the Internet time.

Make configuration in "**Basic**" from "**System**":

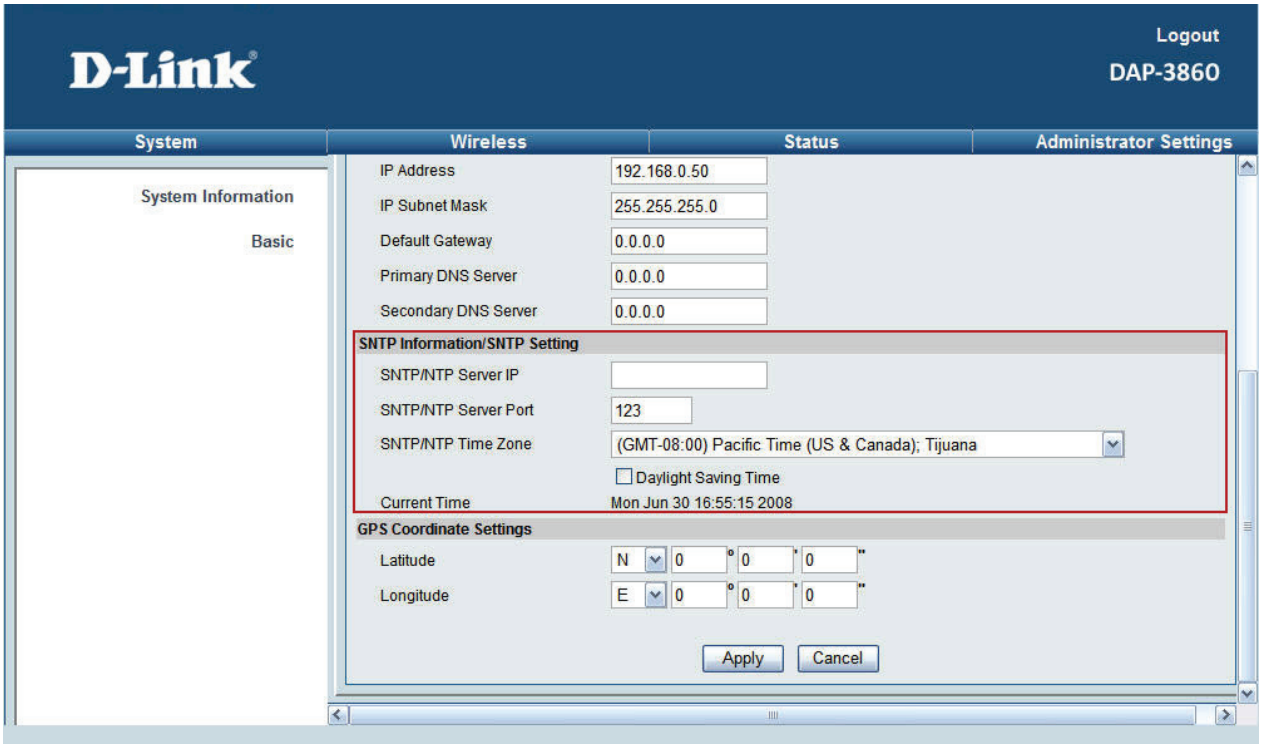
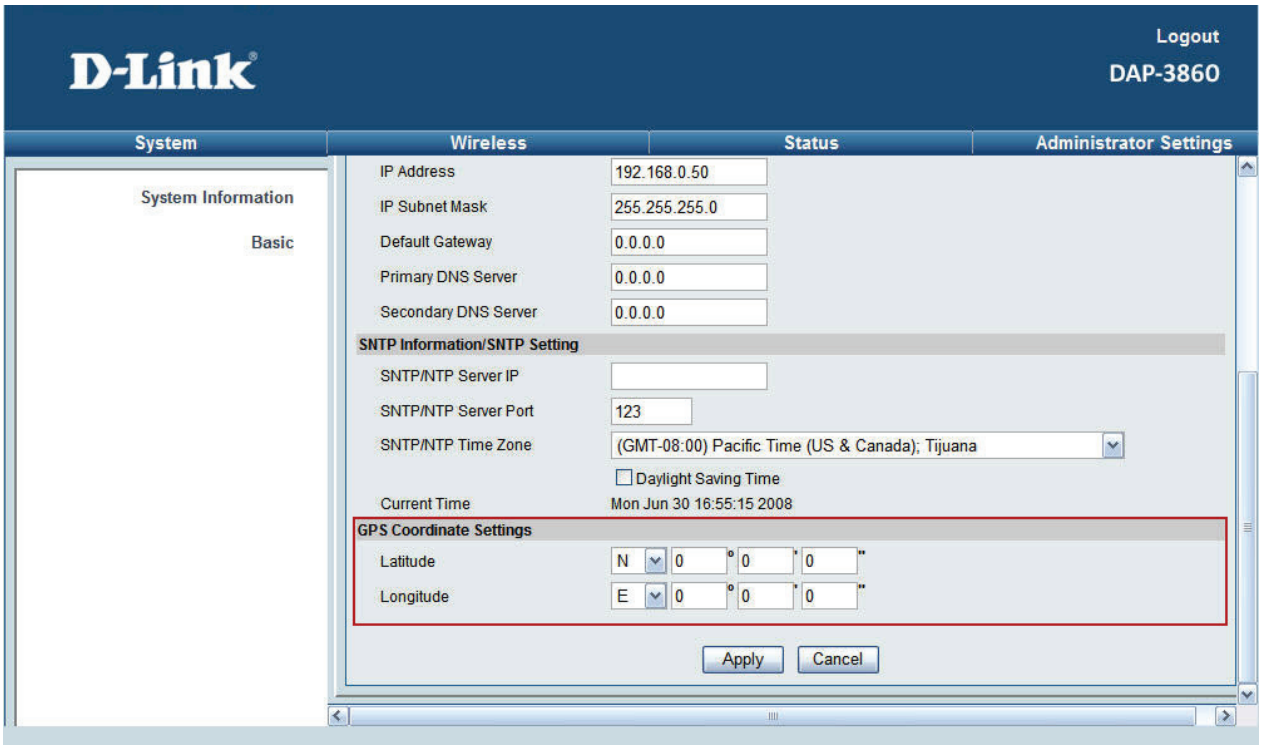


Figure 41 SNTP Information/SNTP Setting

- Enter the SNTP/NTP Server IP IP address and port respectively in "**SNTP/NTP Server IP**" and "**SNTP/NTP Server Port**" fields;
- Select your desired SNTP/NTP Time Zone from the drop-down list, check "**Daylight Saving Time**" if necessary;
- Hit "**Apply**" to save settings.

GPS Coordinate Settings

It allows you to set your AP's location manually using latitude and longitude.



- Enter the latitude and longitude of your AP in this field.

Firmware Upload

Open "**Firmware Upload**" in "**Administrator Settings**" and follow the steps below to upgrade firmware locally or remotely through DAP-3860's Web:

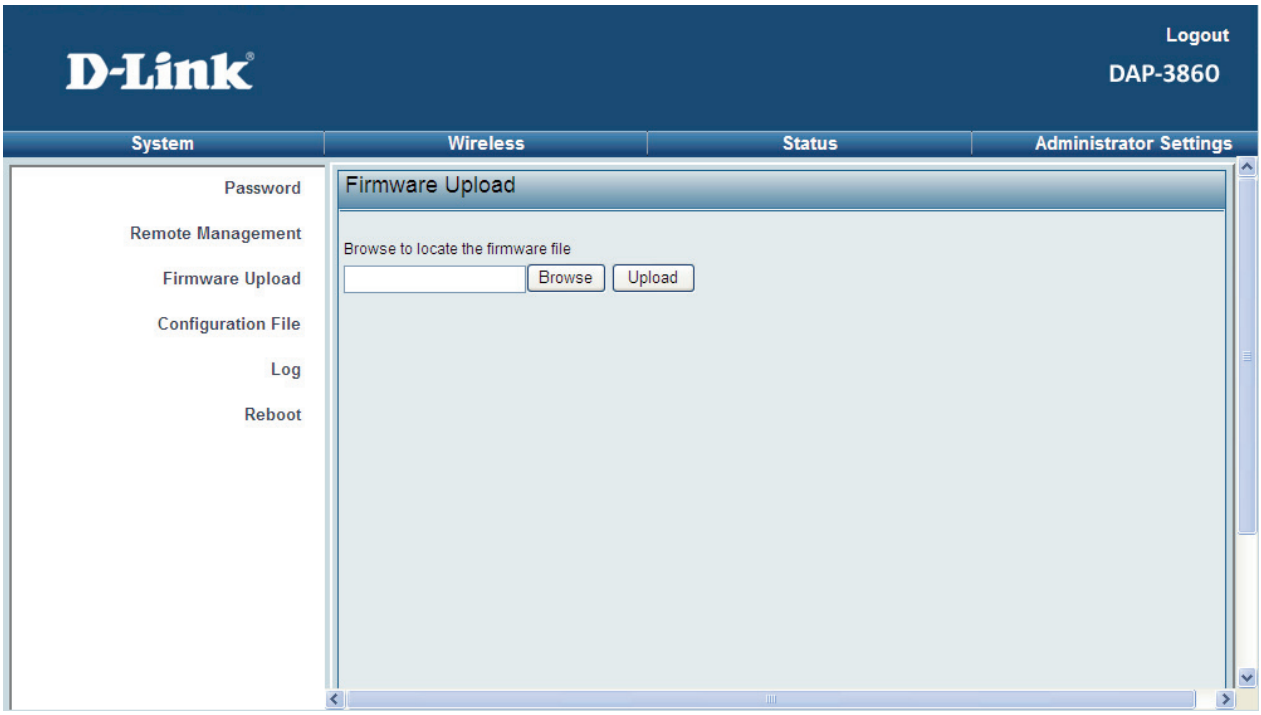


Figure 42 Firmware Upload

- Click "**Browse**" to select the firmware file.
- Click "**Upload**" to load the file into the DAP-3860.
- Wait a moment, the system will reboot after successfully upgrade.

Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Configuration File

It is strongly recommended to back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "**Configuration File**" in "**Administrator Settings**" as below:

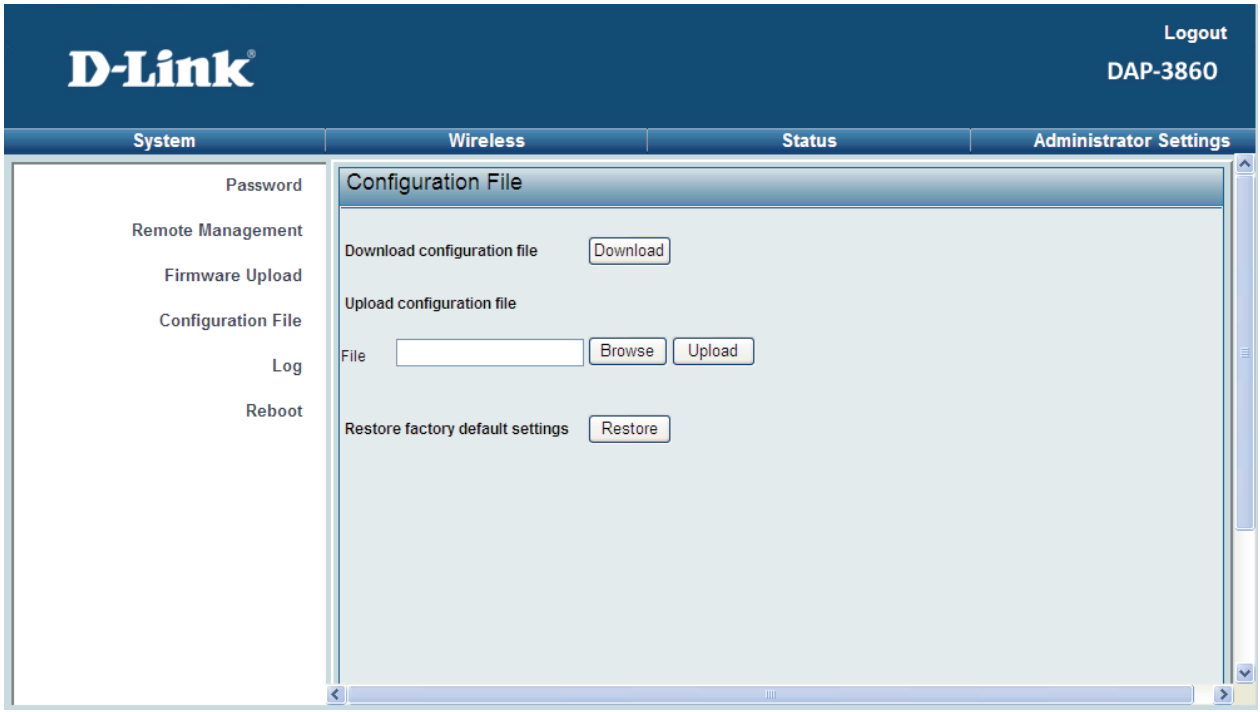


Figure 43 Configuration File

- **Download Configuration File**

  By clicking "**Download**" a dialog box will popup. Save it, then the configuration file is saved to your local computer.

- **Upload Configuration File**

  By clicking "**Browse**" a file selection menu will appear, select the file you want to load, like Dlink.cfg; Click "**Upload**" to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The DAP-3860 provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

  From "**Configuration File**", clicking "**Restore**" will eliminate all current settings and reboot your device, then default settings are applied.

Figure 44 Restore Settings

- **Restore factory default settings via RS-232**

  If software in DAP-3860 is unexpectedly crashed and no longer reset the unit via WEB, you may do hardware reset via RS-232. For detailed instructions please refer to Chapter 2 RS-232 section.

Log Settings

Log Settings is used for recording events occurred on the DAP-3860, including station connection, disconnection, system reboot and etc.

Open "**Log**" in "**Administrator Settings**" as below.

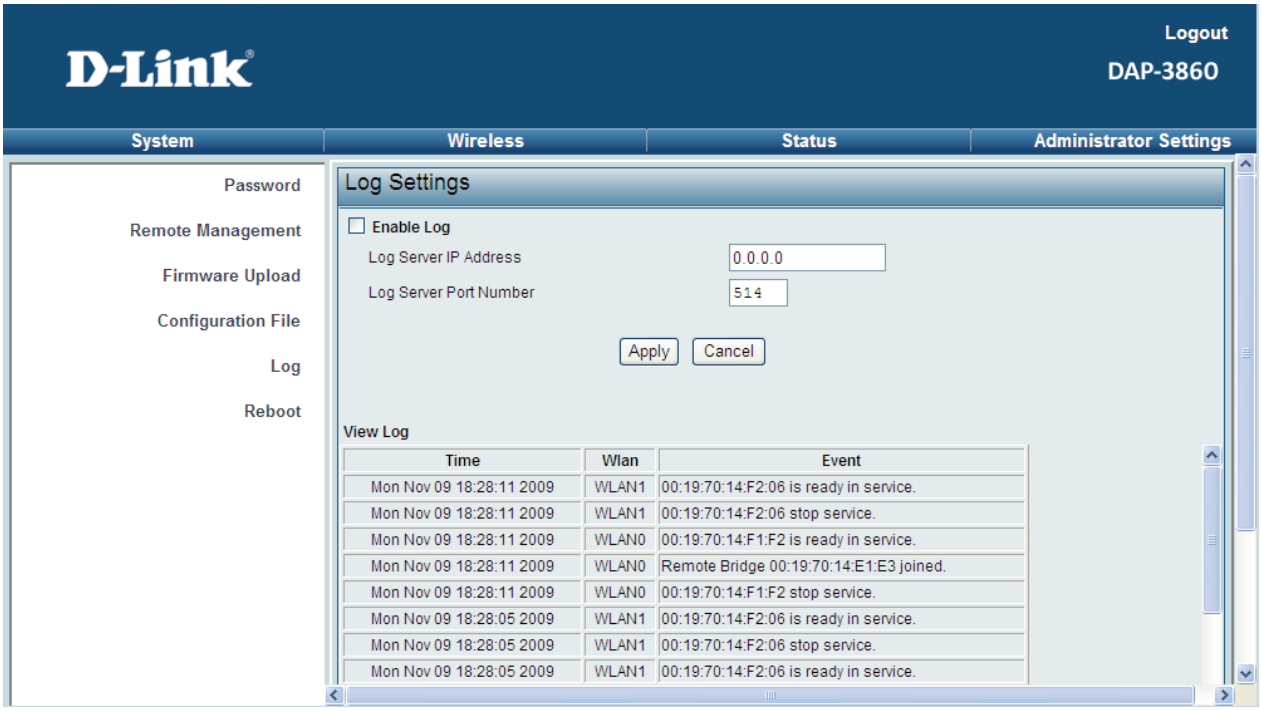


Figure 45 Log Settings

- Enable Log: Enable System log or not;
- Log Server IP Address: Specify the IP address of the server;
- Log Server Port Number: Specify the port number of the server;
- Hit "**Apply**" to save settings;
- View Log: Lists all occurred events in this field.

Reboot

You can reboot your device from "**Reboot**" in "**Administrator Settings**" as below:

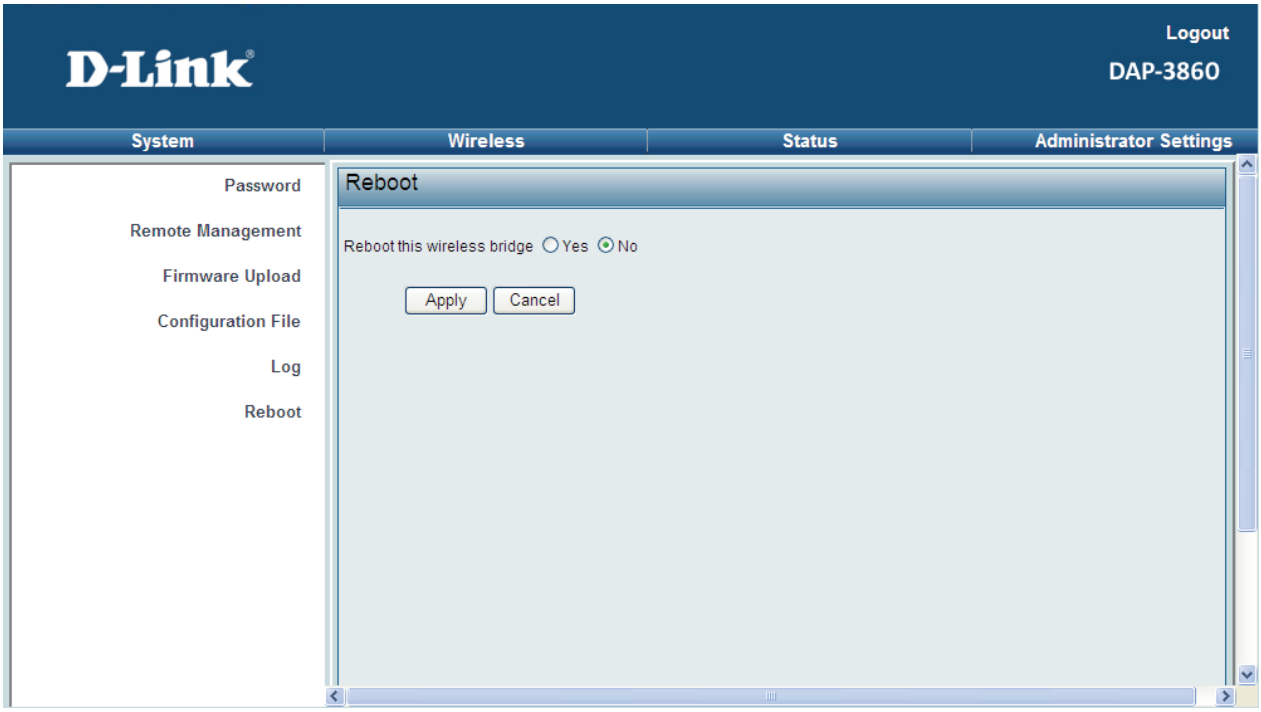


Figure 46 Reboot

- Check "**Yes**" and click "**Apply**" to reboot the DAP-3860. This takes a few minutes, during which the device will send out the buzzing sound, informing you the system is rebooting.

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the DAP-3860. For warranty assistance, contact your service provider or distributor for the process.

Q 1. What if my DAP-3860 fails to connect to the remote one?

- **Ethernet Link**: Check the availability of power to the bridge by observing the LED status on the power injector or on top of the RJ-45 Jack of the unit.
  - Green: The DAP-3860 is connecting to the backhaul network.
  - Off: The DAP-3860 disconnects from the wired network, check whether the power cord and Ethernet cables to the network and bridge are correctly connected.
- **Basic Configurations**: Mismatched basic settings among bridges are the most common cause of connectivity fail. If the bridge does not associate with a remote bridge, check whether in each device are identical.
- **Security Settings**: Remote bridges attempting to authenticate to your DAP-3860 must support the same security options configured in your bridge, such as WEP and AES. If your bridge fails to associate with others, check whether the security settings are the same as your bridge settings.
- **Antenna Alignment**: If the methods above are all checked to be correct, you can observe and verify antenna alignment with RSSI value.

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in "**Configuration File**" from "**Administrator Settings**"

Q 3. What if I would like to download and restore my configuration settings?

You may download by generating a configuration file or upload the settings you have backed up previously in "**Configuration File**" from "**Administrator Settings**".

Q 4. What if I can not open the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browser such as Firefox.
- Hard reset the unit.

Q 5. What if the signal quality is poor or not so good?

- Check whether there is obstacle between units. Obstacle may lead to poor signal.
- Check the antenna height. Place the unit in a high position can help to get a better communication in long distance transmission.
- Check the polarization direction of antenna. Keep the polarization direction of antennas on two associating units the same; if not (one is horizontal, another is vertical), the signal quality may reduce dramatically.
- Check the antenna angle. Align the antenna to the remote one if using directional antenna. Big angle shift may lead to poor signal.
- Check the feeder length. Too long feeder may increase the signal loss and affect the unit performance

Appendix GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there are may contain some public software, if it is, please read below carefully:

1. Definition

"Public Software", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found .

"Public Software" shall mean each of:

(a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and

(b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2. Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting

from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY.

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. 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 LICENSEE.

5. Public Software Name and Description

Table 4 Public Software Name and Description

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
Redboot	**Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.**	**ftp://ftp.gnutools.redhat.com/private/gnupro-xscale-030422/redboot-intel-xscale-030630.tar.Z**	**eCos License**	**http://sources.redhat.com/ecos/ecos-license/**
Busybox		**http://www.busybox.net/downloads/busybox-1.01.tar.bz2**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
brctl	**Copyright (C) 2000 Lennert Buytenhek**	**http://nchc.dl.sourceforge.net/sourceforge/bridge/bridge-utils-1.0.6.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
dropbear	**Copyright (c) 2002-2006 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu**	**http://matt.ucc.asn.au/dropbear/dropbear-0.51.tar.bz2**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**

hostapd	Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
wpa_supplicant	Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
mtdutil		ftp://ftp.uk.linux.org/pub/people/dwmw2/mtd/cvs/mtd/util/	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ntpclient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icarus.com/ntpclient/ntpclient_2003_194.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
procps	Author: Albert Cahalan, Michael K. Johnson, Jim Warner, etc.	http://procps.sourceforge.net/procps-3.2.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2 GNU LIBRARY GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html http://www.gnu.org/licenses/old-licenses/library.html
vsftpd	Author: Chris Evans	ftp://vsftpd.beasts.org/users/cevans/vsftpd-1.1.2.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.20.3.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html