User’s Manual

Powerline 200M
Wall-Mount Wireless-N AP

Index

FCC Part 68

This equipment complies with Part 68 of the FCC Rules. On the bottom of this equipment is a label that contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. You must provide this information to the telephone company upon request.

The REN is useful to determine the quantity of devices you may connect to the telephone line and still have those entire devices ring when your number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may discontinue your service temporarily.
If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible.
You will be advised of your right to file a complaint with the FCC.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this modem, please contact your dealer for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

FCC Part 15

The modem generates and uses radio frequency energy. If it is not installed and used properly in strict accordance with the user's manual, it may cause interference with radio and television reception. The modem has been tested and found to comply with the limits for Class B computing devices in accordance with the specifications in Subpart B, Part 15 of the FCC regulations. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. FCC regulations require that shielded interface cables be used with your modem.

If interference does occur, we suggest the following measures be taken to rectify the problem:

1) Move the receiving antenna.

2) Move the modem away from the radio or TV.

3) Plug the modem into a different electrical outlet.

4) Discuss the problem with a qualified radio / TV technician.

CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance to the FCC Rules could void the user's authority to operate this equipment.

Cable connections:

All equipment connected to this modem must use shielded cable as the interconnection means.

Notes:

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.

Chapter 1 Introduction

Congratulations on your purchase of an Instant Powerline 200M 11n AP. The Powerline AP is the perfect option to connect a small group of PCs or small wireless clients. Integrated Wireless to Powerline networks, the device can extend large coverage and less dead space for your home network.

1.1 Overview

Using Powerline and wireless 11 b/g/n benefit, you can connect the pc to internet in anywhere of your home..

1.2 Features

③ Internet Access

- TCP/IP, UDP, ICMP, ARP, RARP, Static IP assignment

③ Standard

- IEEE 802.3, 802.3u Ethernet standards
- HomePlug AV
- IEEE 802.11b/g and 11n Wireless standards

③ QoS

- Prioritized random access, contention-free access and segment bursting
- Eight levels of prioritized random access, contention-free access, and segment bursting

③ Powerline Modulation

- OFDM (Orthogonal Frequency Division Multiplexing) with patented signal processing techniques for high data reliability in noisy media conditions
- Supports QAM 256/64/16, DQPSK, DBPSK and ROBO modulation schemes

③ Security

- Provide 128-bit AES link encryption for Powerline network

③ Wireless Features

- Support 802.11b/g and n Wireless Access Point, WDS and AP Client
- Support 128-Bit and 64-Bit WEP encryption , 802.1x, WPA, WPA2 and WPS

③ Other

- High-Speed Powerline adapter with Ethernet interface for fast data transfer over the existing household power supply
- The high-speed transfer rates of 200Mbps even make it possible to transmit video in DVD quality
- No need new wires and use at any power socket with up to ranges of 200 meters

③ HTTP Web-Based Management

- Firmware upgrade by UI
- Password protected access

1.3 System Requirements

1) Personal computer (PC)

2) Pentium II 233 MHz processor minimum

3) 32 MB RAM minimum

4) 20 MB of free disk space minimum

5) Ethernet Network Interface Controller (NIC) RJ45 Port

6) Internet Browser

Chapter 2 Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

2.1 Checklist

Check the shipping box carefully to ensure that the contents include the items you ordered. If any of the items are missing or damaged, contact your local distributor. The contents of your carton may vary depending on your service provider.

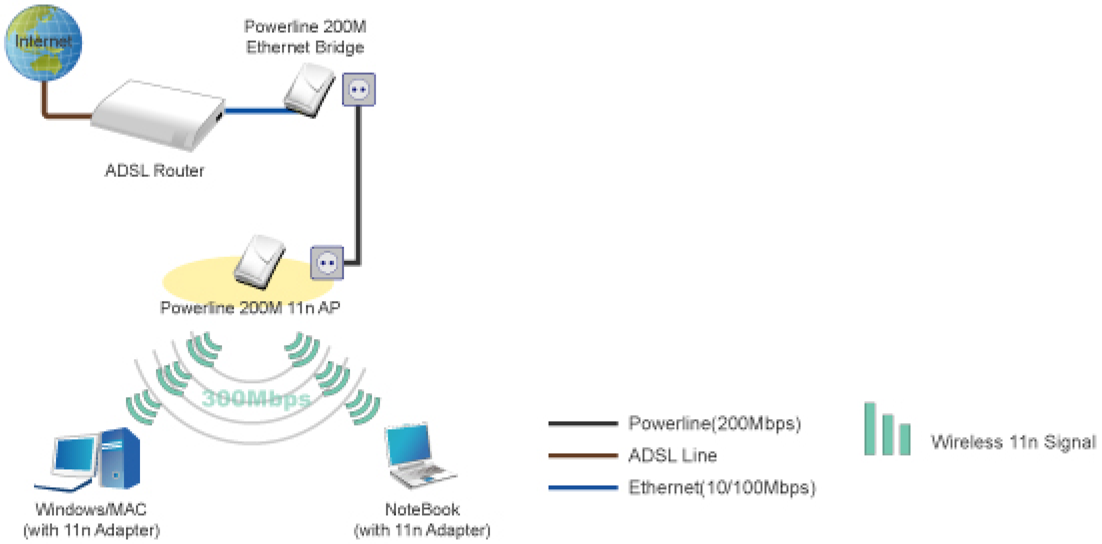
Contents description

1) Powerline 200M Wireless-N Extender for home/office use

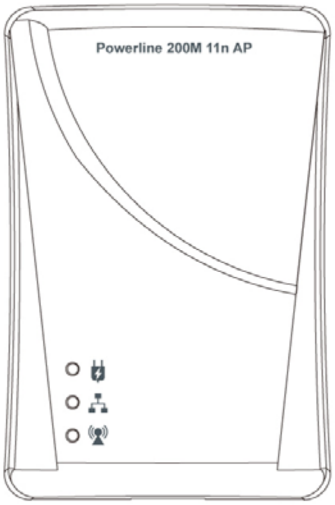
2) Powerline 200M Wireless-N Extender Installation and Operation Guide (this publication)

3) Ethernet cable Ethernet category 5 twisted pair cable (6 ft)

Application for this device

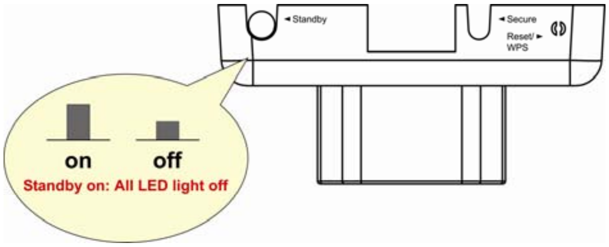


2.2 The Front LEDs



LED	State		Description
Powerline	🔌	ON	Powerline network activity.
		OFF	Search or no Powerline network activity.
Ethernet	🖧	ON	Ethernet connection is OK.
		Flashing	Data transfer.
		OFF	No link to Ethernet.
Wireless	📡	ON	Wireless Function Enable
		Flashing	Data transfer.

2.3 The Rear Ports



Connector	Description
RJ-45 Port	Connect to the Ethernet Cable
Secure Button	Button can auto secure and group the Powerline devices.
Reset/WPS Button	**WPS :** Press 1 second can enable the WPS search function.
	Reset: Press 5 seconds can reset the device to factory default.
Standby Button	**Press this button to enable the standby mode(EuP/ErP function).** **This function will stop the device activities in order to save energy.**

Chapter 3 Configuration

3.1 Determine your connection settings

Before you configure the router; you need to know the connection information supplied by your service provider.

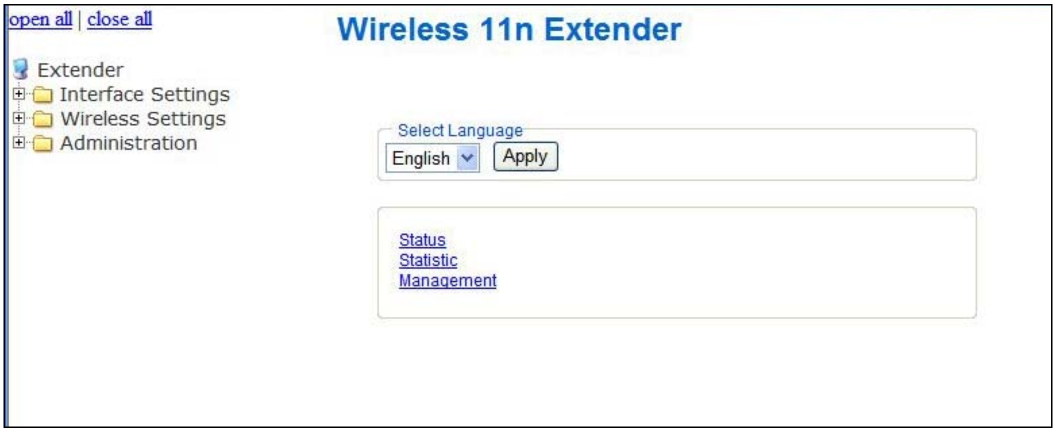
3.2 Connecting the Powerline Extender to your network

Unlike a simple hub or switch, the setup of the Powerline Extender consists of more than simply plugging everything together.

3.3 Configuring with Web Browser

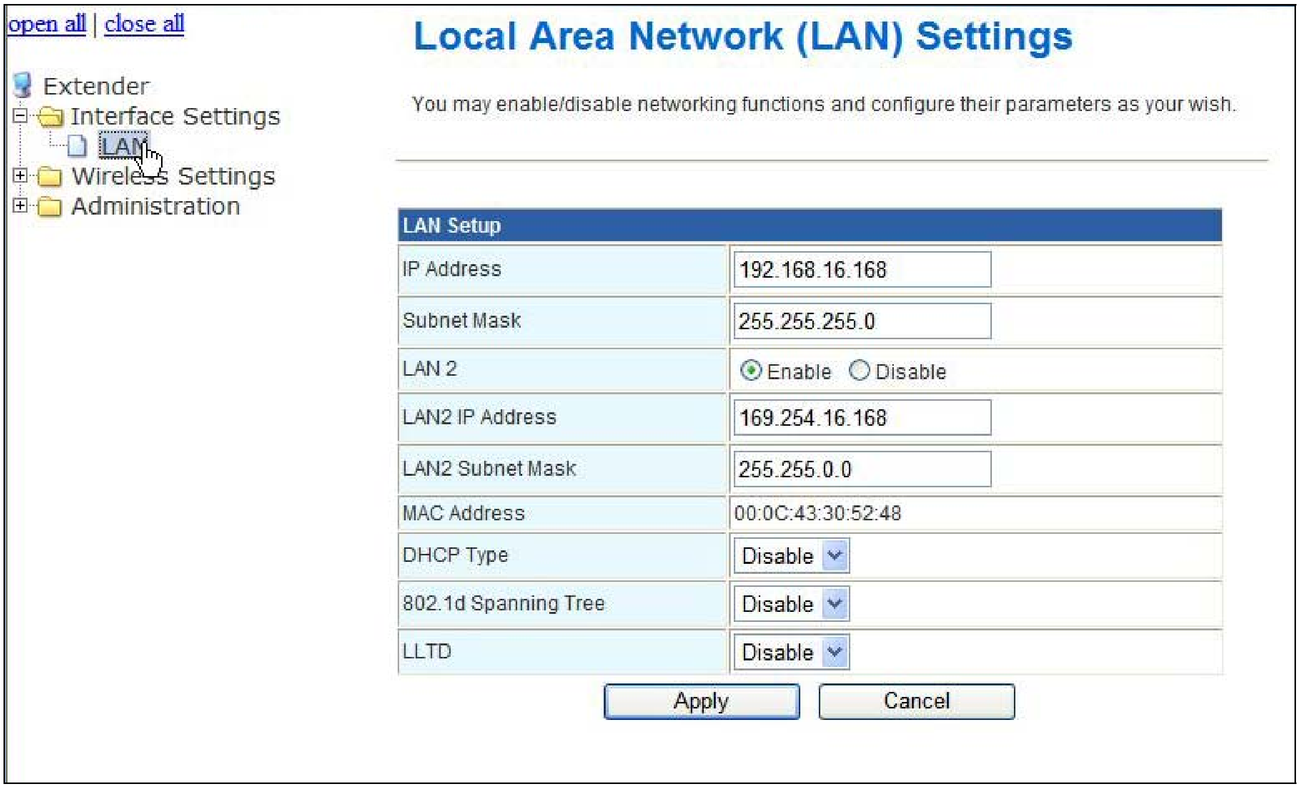
It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type '**http://192.168.16.168**' into the address bar and click 'Go' to get to the login page. Save this address in your Favorites for future reference.



At the Password prompt, the User name is '**admin**' and the password is ’**admin**’. You can change these later if you wish. Click **'OK**' to login.

3.3.1 Management LAN IP



Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.16.168
Subnet Mask	255.255.255.0
LAN 2	● Enable ○ Disable
LAN2 IP Address	169.254.16.168
LAN2 Subnet Mask	255.255.0.0
MAC Address	00:0C:43:30:52:48
DHCP Type	Disable
802.1d Spanning Tree	Disable
LLTD	Disable

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment. Default IP is **192.168.16.168**.

IP Address: The IP of the device’s LAN port (default 192.168.16.168).

Subnet Mask: Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.

LAN2: Enable / Disable LAN 2.

LAN2 IP: The IP address of LAN2. (default 169.254.16.168

LAN2 Subnet Mask: Subnet Mask of LAN2.

DHCP Type: To give your LAN Client an IP, you have to enable DHCP server. If not, manual setting up your client IP is necessary when you want to use the router as your client’s default gateway.

Start IP Address: Specify the DHCP Client start IP address.

End IP Address: Specify the DHCP Client End IP address.

Note: The number of the “End IP” must be greater than “Start IP”, and cannot be the same as the router’s IP address.

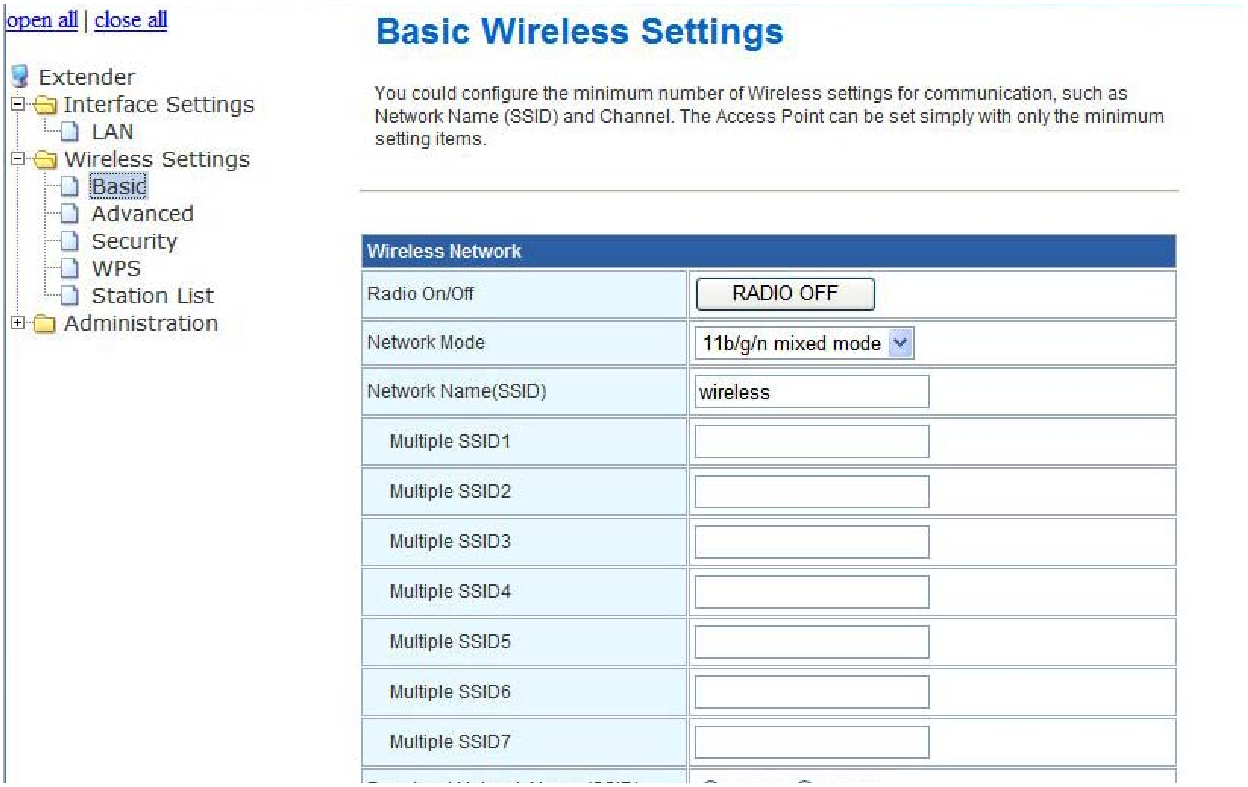
DHCP Lease Time: Choose the length of the time for the device to recycle and give out the IP addresses to the devices in your network (default 86400).

Statically Assigned: Can statically assigned the client MAC and IP address. There are three IP can assign.

802.1d Spanning Tree: Enable/Disable. The Spanning Tree Protocol is an OSI layer-2 protocol that ensures a loop-free topology for any bridged LAN.

LLTD: Enable/Disable. Link Layer Topology Discovery (LLTD) is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics. It was developed by Microsoft as part of the Windows Rally set of technologies. The LLTD protocol operates over both wired (IEEE 802.3 Ethernet) as well as wireless (IEEE 802.11) networks.

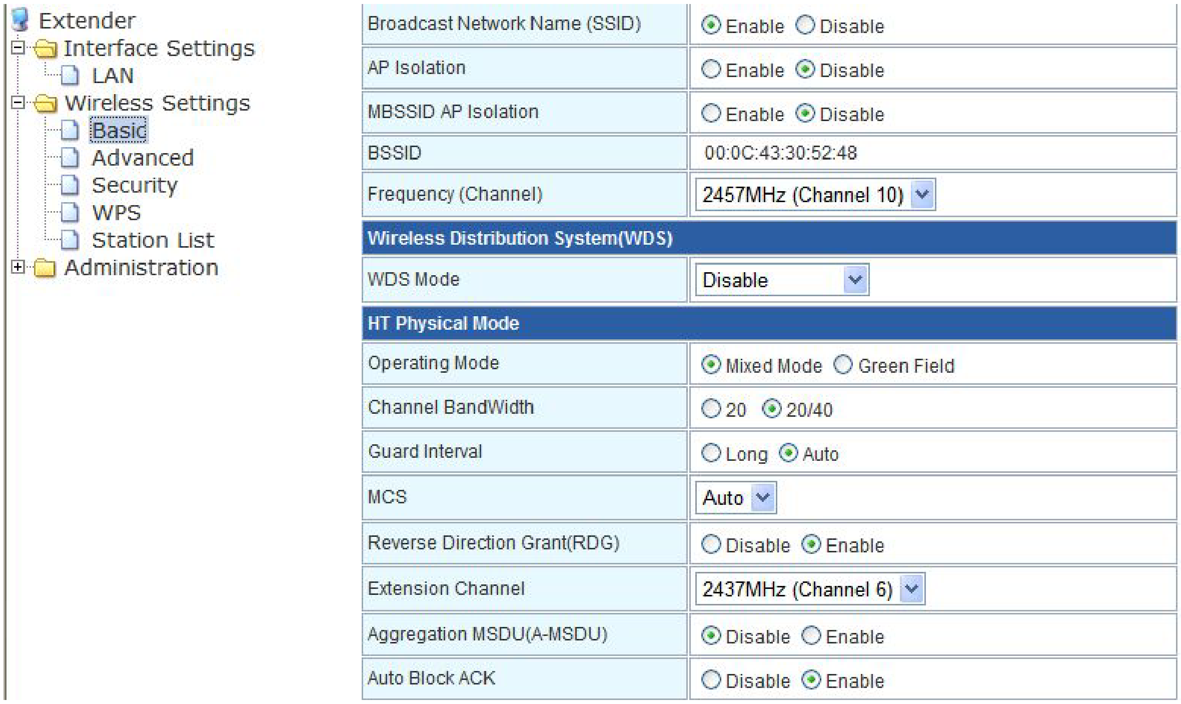
3.4.1 Wireless Basic Settings



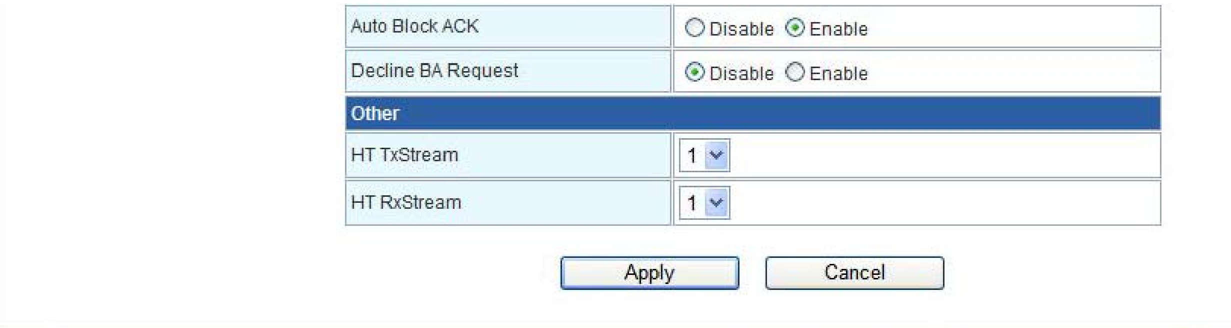
Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	wireless
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	



Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:0C:43:30:52:48
Frequency (Channel)	2457MHz (Channel 10)
Wireless Distribution System(WDS)	
WDS Mode	Disable
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2437MHz (Channel 6)
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable



Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
Other	
HT TxStream	1
HT RxStream	1

Radio Off: Enable/Disable the wireless.

Network Mode: There are 3 modes can choose, 11/b/g/n mixed mode/11b only/11g only.

SSID: set up the wireless ID, default is wireless.

Multiple SSID 1 ~ 7: You can set up to four SSID for this wireless network.

Broadcast Network Name(SSID): Enable/Disable the SSID broadcast.

AP Isolation: Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.

MBSSID AP Isolation: Enable/Disable this function.

BSSID: Displays the Basic Service Set Identity (BSSID) of this router. This parameter is the same as the MAC address of LAN port.

WDS (Wireless Distribution System):

WDS Mode: Default is Disable, there are 3 Mode can choose, Lazy Mode(Auto), Bridge Mode(Bridge Only) and Repeater Mode(AP + Bridge).

Phy Mode: Select the option in the drop-down list to enable CCK, OFDM, HTMIX, or GREENFIELD mode for physical layer transceivers.

EncrypType: Select the option in the drop-down list to enable WEP, TKIP, and AES encryption types. If you select None, any data will be transmitted without encryption and any station can access the router.

EncrypKey: For encryption type of TKIP and AES, you have to fill in the WPA encryption key. Please use Pass Phrase (8~32bytes) key format.

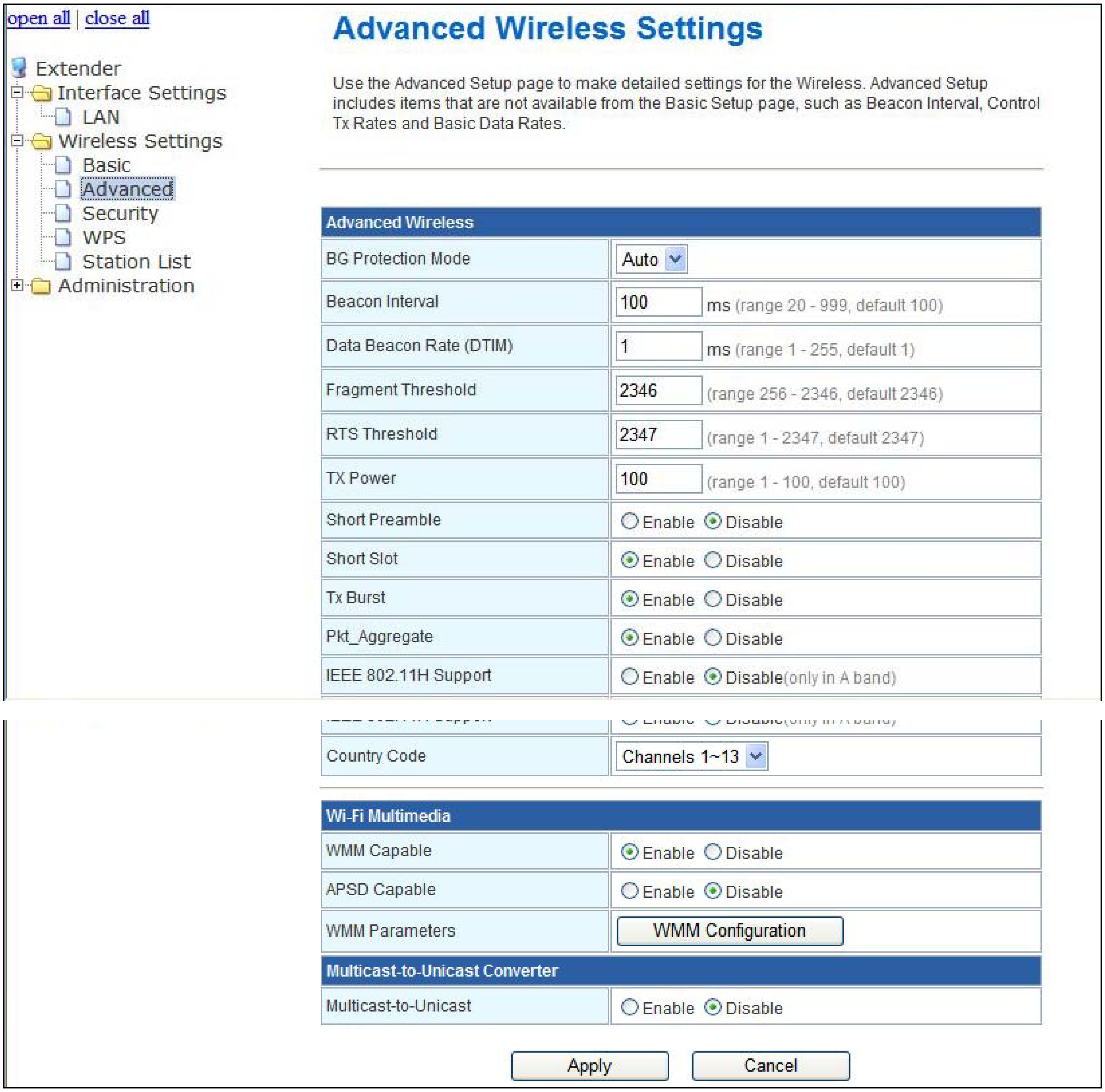
AP MAC Address: For encryption type of TKIP and AES, you have to fill in the WDS AP MAC. You can fill up to 4 sets of WDS AP MAC lists.

Other :

HT TxStream: Set the Tx via 1 or 2 antennas.

HT RxStream: Set the Rx via 1 or 2 antennas.

3.4.2 Wireless Advance Settings



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	Channels 1~13

Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration
Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

Advanced Wireless:

BG Protection Mode: Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select “Auto” to turns it on or off automatically, select “On” to support protection or select “Off” to disable this function.

Beacon Interval: Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.

Data Beacon Rate(DTIM): Enter a value between 1 and 255 (default 1) for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Fragment Threshold: This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.

RTS Threshold: Request To Send threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.

Tx Power: Transmit power. You can set the output power of wireless radio. This value should remain at its default setting of 100. If you

Short Preamble: The length of CRC blocks in the frames during the wireless communication.

Short Slot: Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present

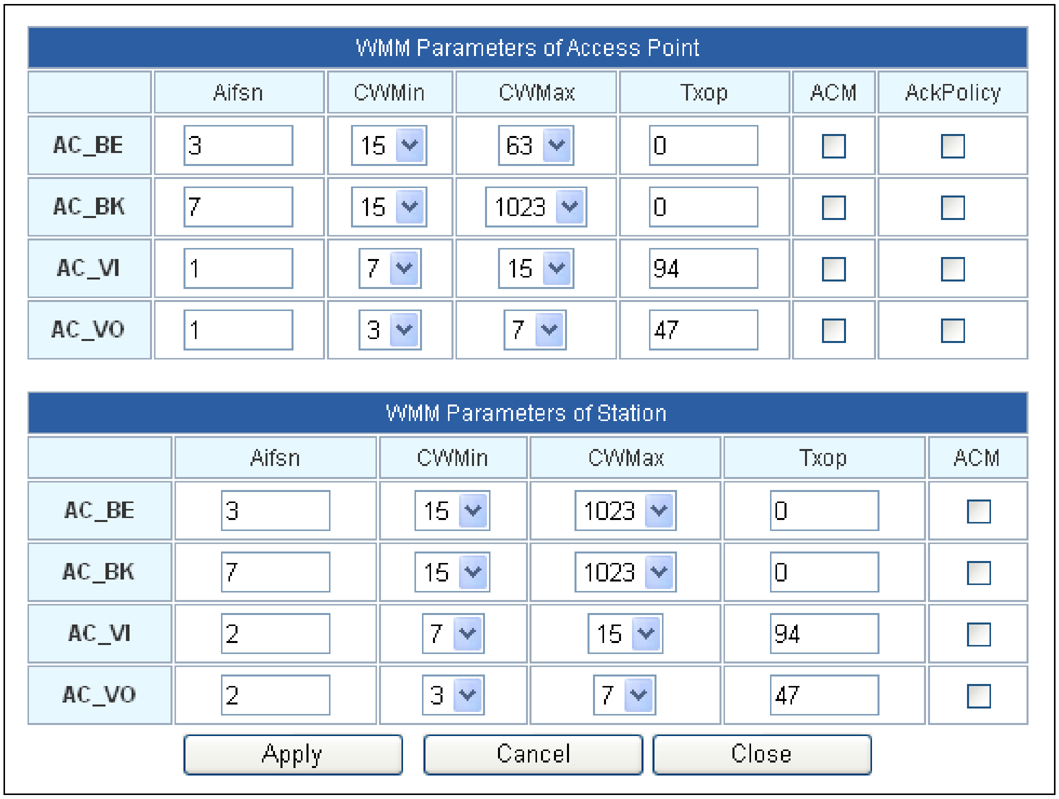
Tx Burst: Select to enable or disable connecting to a Tx Burst supported device.

Pkt_Aggregate: To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.

IEEE 802.11H Support: Enable/Disable.

Country Code: Select wireless country code. Six countries can choose.

WMM Configuration:



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

WMM Capable: This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network.

APSD Capable: Automatic Power saves Delivery. Select to enable / disable data flow using power saving mode during transmitting.

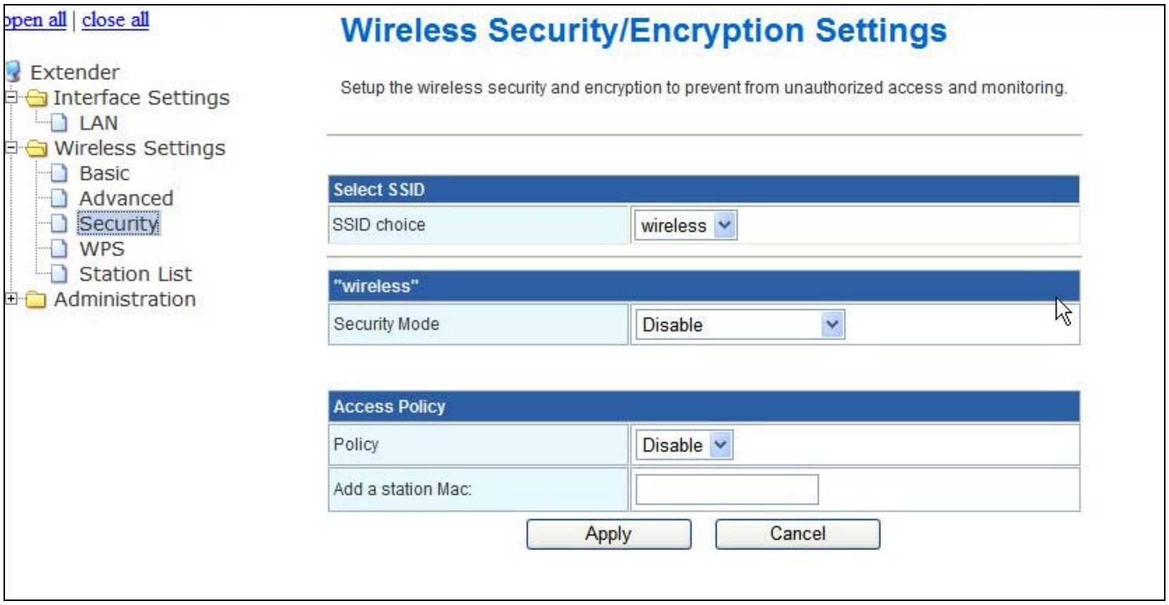
DLS Capable: Enable/Disable this function.

WMM Parameters: You can configure WMM parameters by clicking on the

button. The configuration window pops up (as shown below). Manually configure the parameters and click on the “Apply” button to execute.

Multicast-to-Unicast: It can receives Multicast streams from the network backbone, converts them to Unicast format, and routes them to the set-top-boxes of end-users over the last mile infrastructure (e.g. DSL, Ethernet, WiFi).

3.4.3 Wireless Security



Wireless Security/Encryption Settings

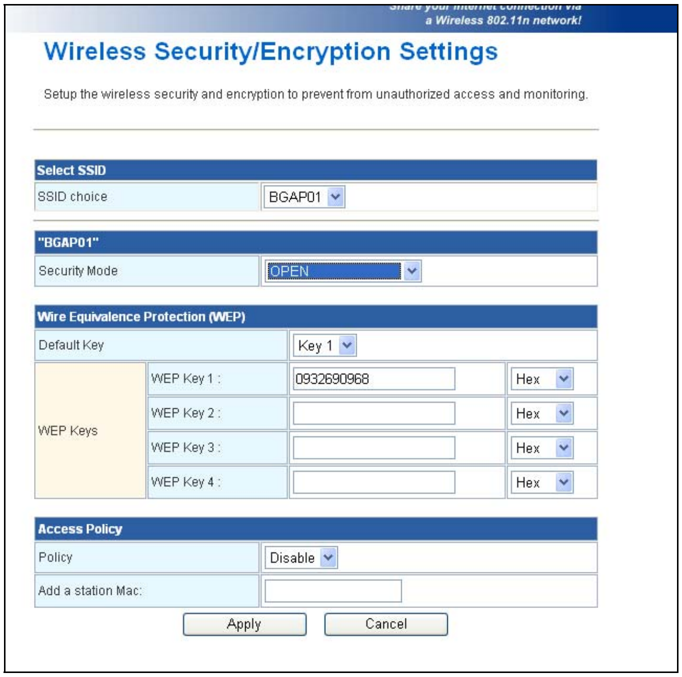
Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	wireless
"wireless"	
Security Mode	Disable
Access Policy	
Policy	Disable
Add a station Mac:	

SSID Choice: Please choose a SSID you have set for this router in the Wireless Settings > Basic Settings from the drop-down list. The SSID will be shown on the wireless network for recognizing..

Security Mode: There are 10 modes for you to select: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-PSKWPA2-PSK, WPA1WPA2, 802.1x. Please refer to the following description.

Security Mode -- Open / WEP Auto



Share your internet connection via
a Wireless 802.11n network!

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	BGAP01

"BGAP01"	
Security Mode	OPEN

Wire Equivalence Protection (WEP)			
Default Key		Key 1	
WEP Keys	WEP Key 1 :	0932690968	Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

Access Policy	
Policy	Disable
Add a station Mac:	

Default Key: Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.

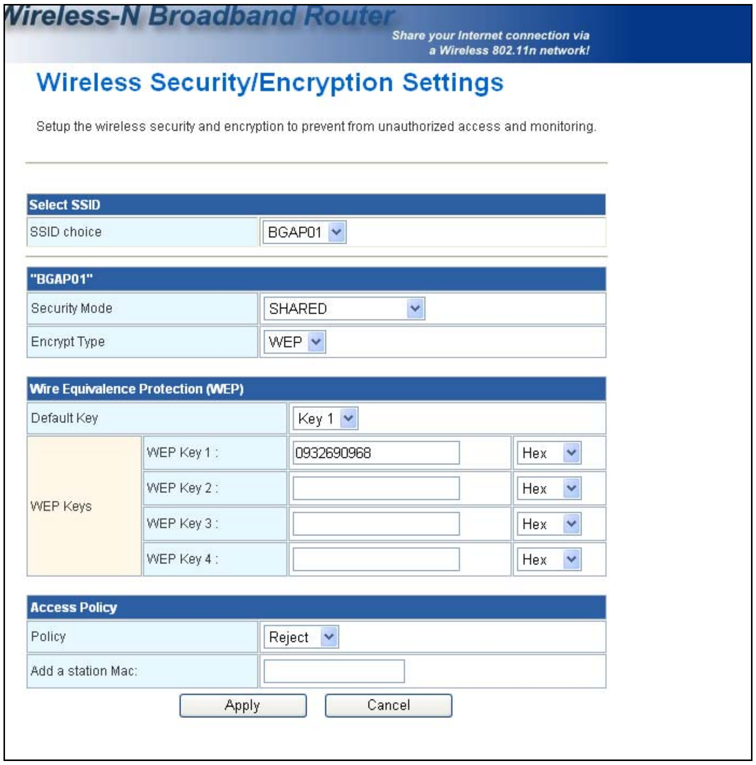
WEP Keys: Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- Shared


Wireless-N Broadband Router
Share your Internet connection via a Wireless 802.11n network!

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	BGAP01

"BGAP01"	
Security Mode	SHARED
Encrypt Type	WEP

Wire Equivalence Protection (WEP)			
Default Key	Key 1		
WEP Keys	WEP Key 1 :	0932690968	Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

Access Policy	
Policy	Reject
Add a station Mac:	

Default Key: Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.

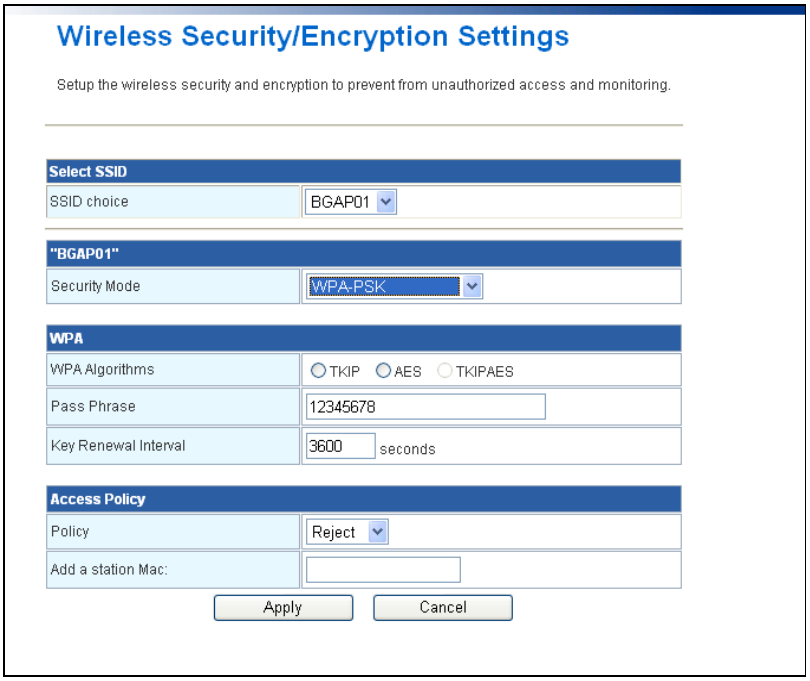
WEP Keys: Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- WPA-PSK / WPA2-PSK / WPA-PSK + WPA2-PSK



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	BGAP01

"BGAP01"	
Security Mode	WPA-PSK

WPA	
WPA Algorithms	○ TKIP ○ AES ○ TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

Access Policy	
Policy	Reject
Add a station Mac:	

WPA Algorithms: Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSK + WPA2-PSK)

Pass Phrase: Enter a pass phrase encryption key format (8~32 bytes).

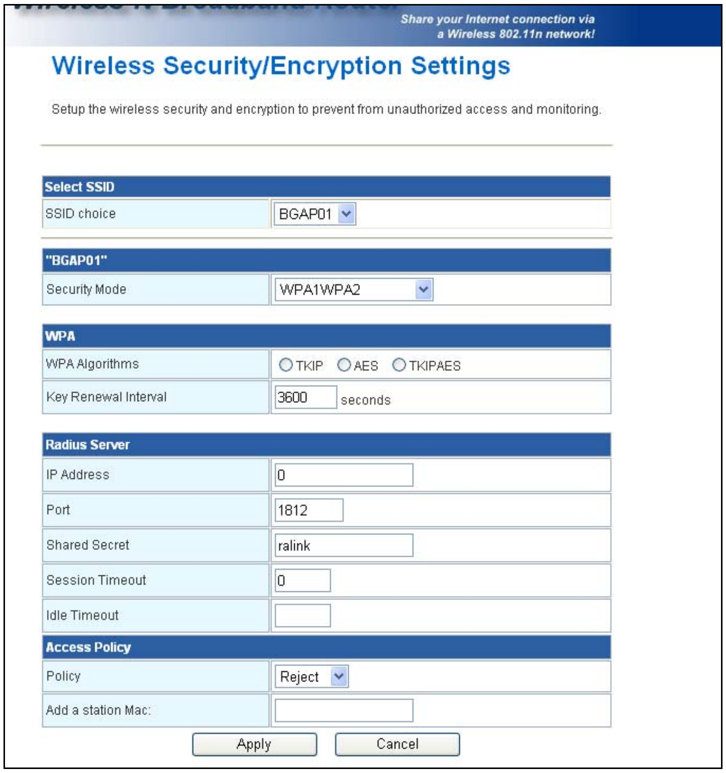
Key Renewal Interval: Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- WPA / WPA2 / WPA1 + WPA2 / 802.1x



Share your Internet connection via a Wireless 802.11n network!

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	BGAP01

"BGAP01"	
Security Mode	WPA1WPA2

WPA	
WPA Algorithms	○ TKIP ○ AES ○ TKIPAES
Key Renewal Interval	3600 seconds

Radius Server	
IP Address	0
Port	1812
Shared Secret	ralink
Session Timeout	0
Idle Timeout	
Access Policy	
Policy	Reject
Add a station Mac:	

WPA Algorithms: Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSK + WPA2-PSK)

Key Renewal Interval: Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.

Radius Server:

IP Address: Radius Server IP address.

Port: The default port number is 1812.

Shared Secret: The default is “ralink”.

Session Timeout: default is 0.

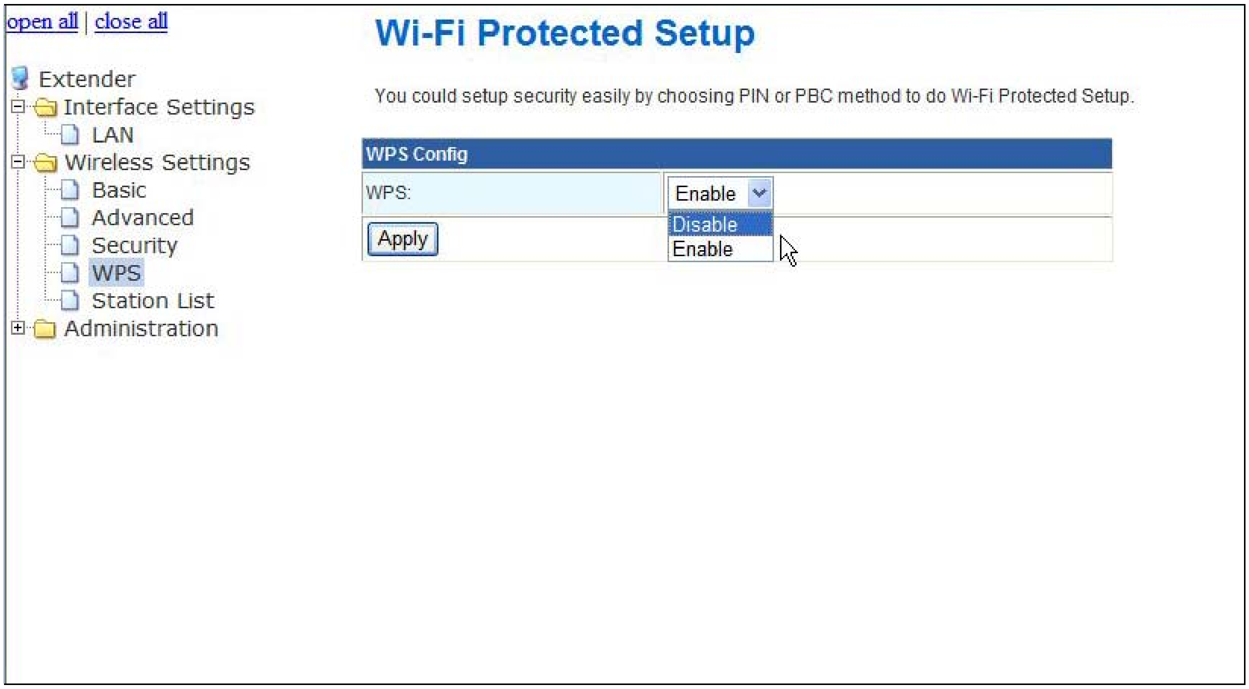
Idle Timeout: The idle timeout setting.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

3.4.4 WPS(Wi-Fi Protected Setup)



Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config

WPS: Enable

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS: Enable/Disable the WPS. Default setting is disable.

WPS Summary: Shows the information of WPS current status, configured, SSID, authentication mode, and pre-shared key. Click on Reset OOB button to Reset WPS AP to the OOB (out of box) configuration.

WPS Progress: Show the WPS current status.

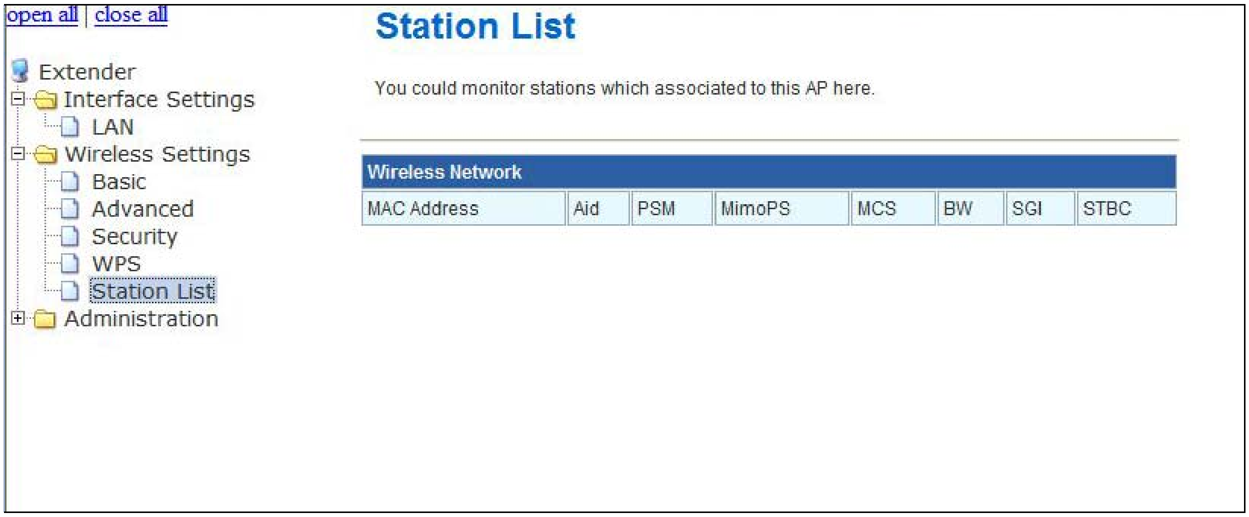
WPS mode:

PIN method (Personal Identification Number): read the PIN from either a sticker on the new STA or a display.

PBC method (Push Button Communication): in which the user simply has to push a button, either an actual or virtual one, on both the AP and the new STA. (Users can simply push the

PIN: Users have to fill in the PIN code to enrollee device if selecting PIN mode as the WPS Config method.

3.4.5 Wireless Station List



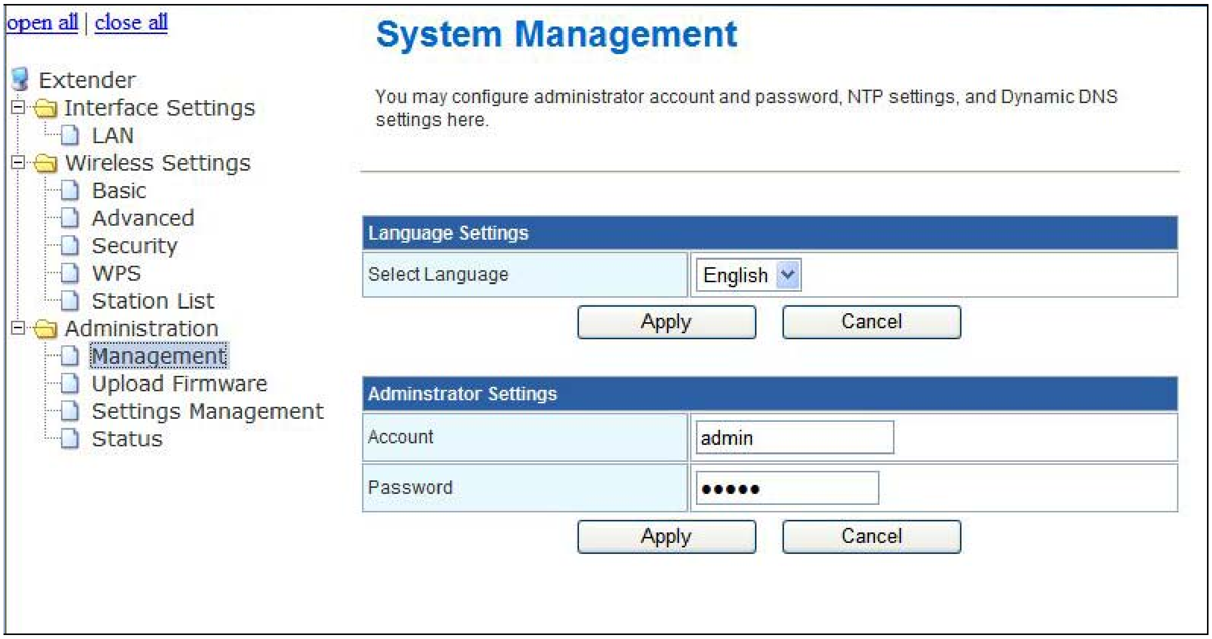
Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

Monitor Stations which associated to this AP/Router here.

3.5.1 Management



System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

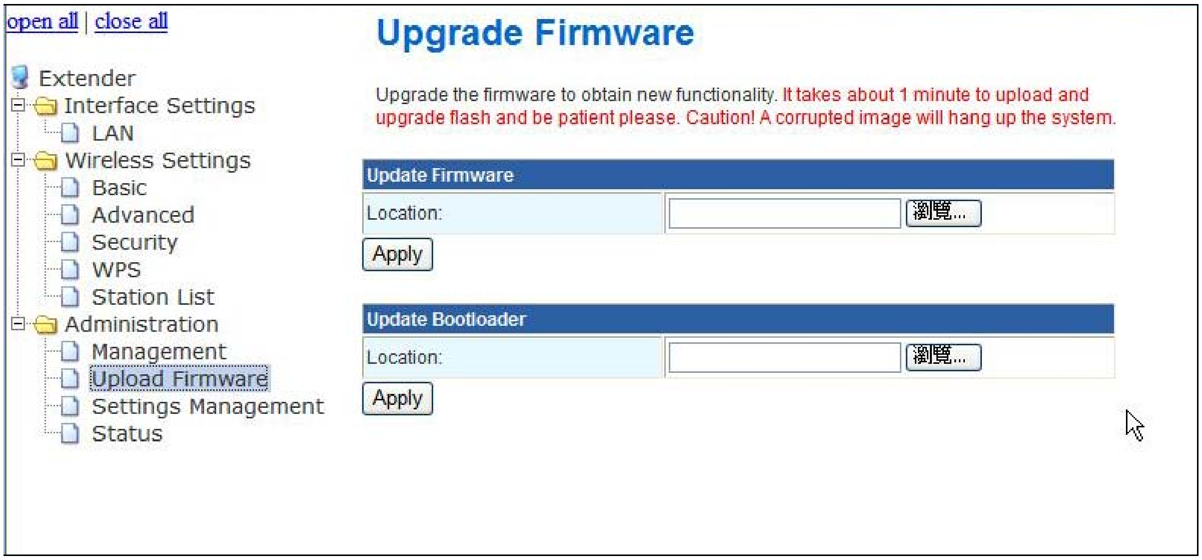
Language Settings	
Select Language	English

Adminstrator Settings	
Account	admin
Password	●●●●●

Language Settings: Can select language which you want.

Administrator Settings: Set the account and password to set and manage the Wireless Device.

3.5.2 Upgrade Firmware



Upgrade Firmware

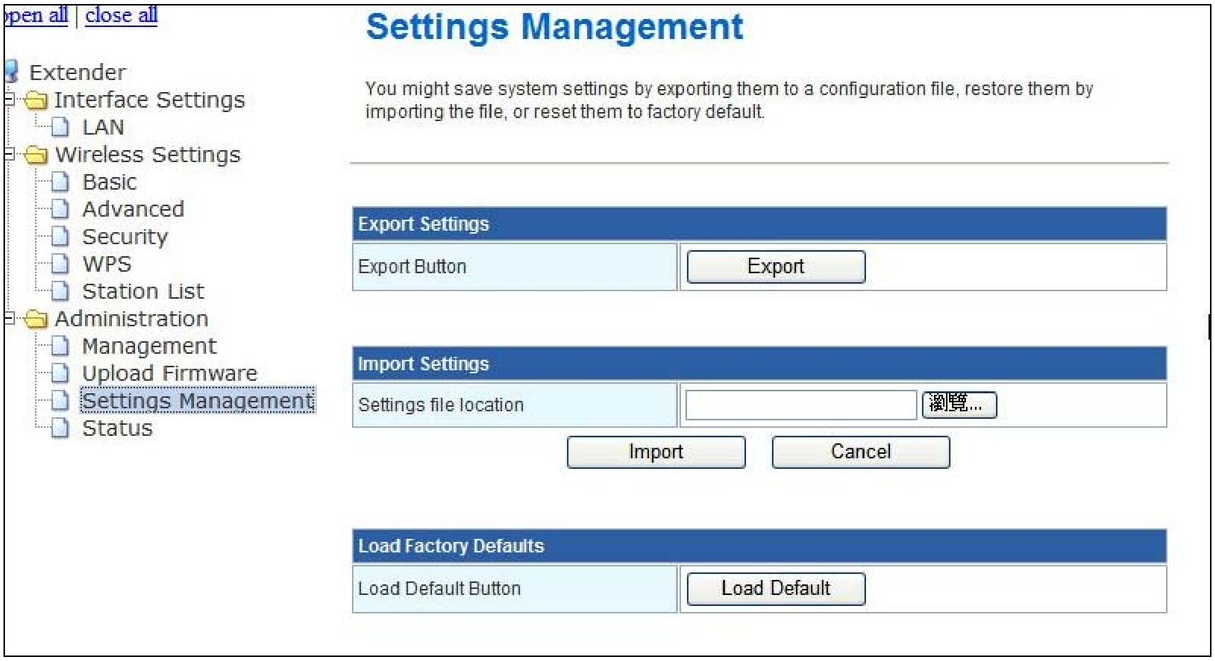
Upgrade the firmware to obtain new functionality. It takes about 1 minute to upload and upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

Update Firmware	
Location:	

Update Bootloader	
Location:	

User can upgrade the firmware in this page. Be careful, don’t power off when doing the upgrade process.

3.5.3 Settings Management



Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

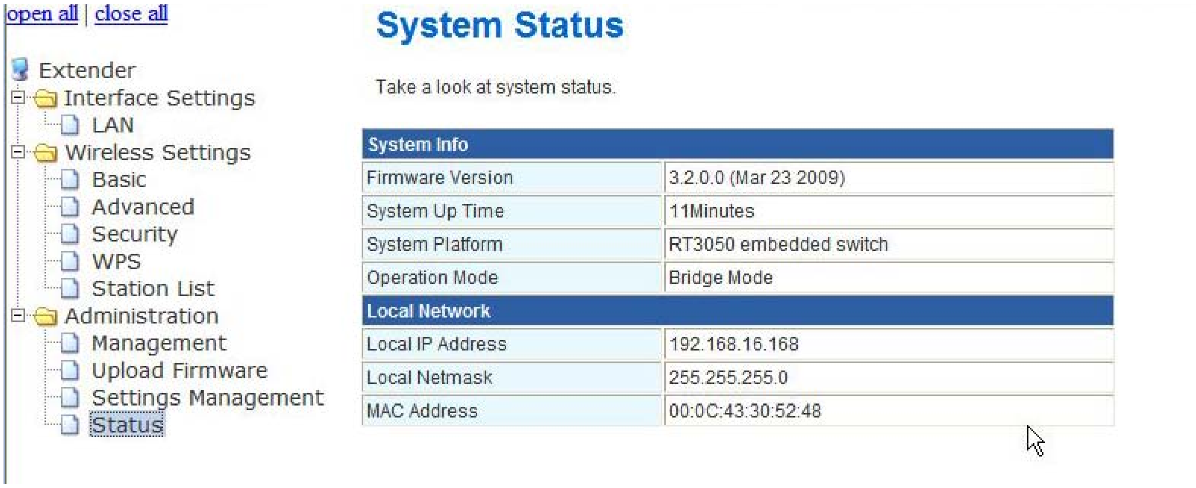
Export Settings	
Export Button	Export

Import Settings	
Settings file location	瀏覽...

Load Factory Defaults	
Load Default Button	Load Default

Users can Export Settings or Import Settings here. If want to load the factory defaults, please click the Load default button.

3.5.4 Status



System Status

Take a look at system status.

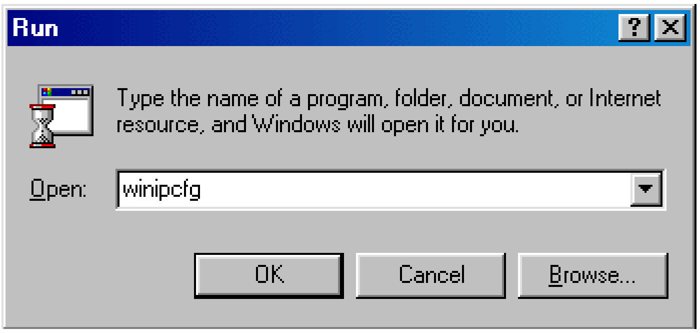
System Info	
Firmware Version	3.2.0.0 (Mar 23 2009)
System Up Time	11Minutes
System Platform	RT3050 embedded switch
Operation Mode	Bridge Mode
Local Network	
Local IP Address	192.168.16.168
Local Netmask	255.255.255.0
MAC Address	00:0C:43:30:52:48

You can check the device status in this page, The firmware version, Internet Configuration and LAN settings.

3.6.1 TCP/IP Settings for Windows Operating System

1. How can I find my IP Address in Windows 95, 98, or Me?

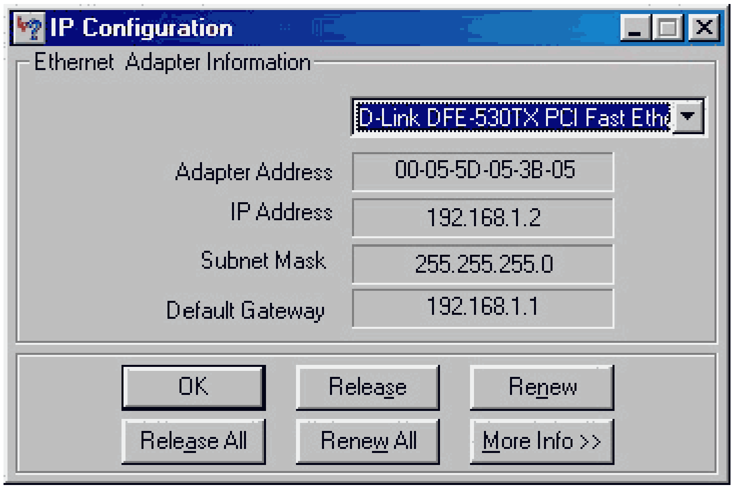
- Click on **Start**, then click on **Run**.
- The Run Dialogue Box will appear. Type **winipcfg** in the window as shown then click OK



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: winipcfg

- The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.
- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



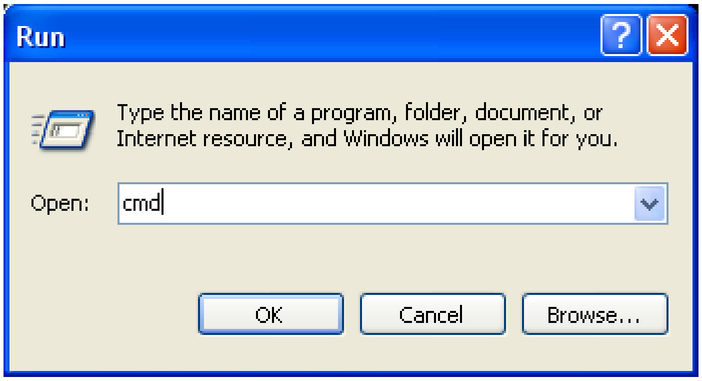
D-Link DFE-530TX PCI Fast Ethe

Adapter Address: 00-05-5D-05-3B-05
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

- After selecting your adapter, it will display your IP Address, subnet mask, and default router.
- Click **OK** to close the IP Configuration window.

2. How can I find my IP Address in Windows 2000/XP?

- Click on **Start** and select **Run**.
- Type **cmd** then click **OK**.

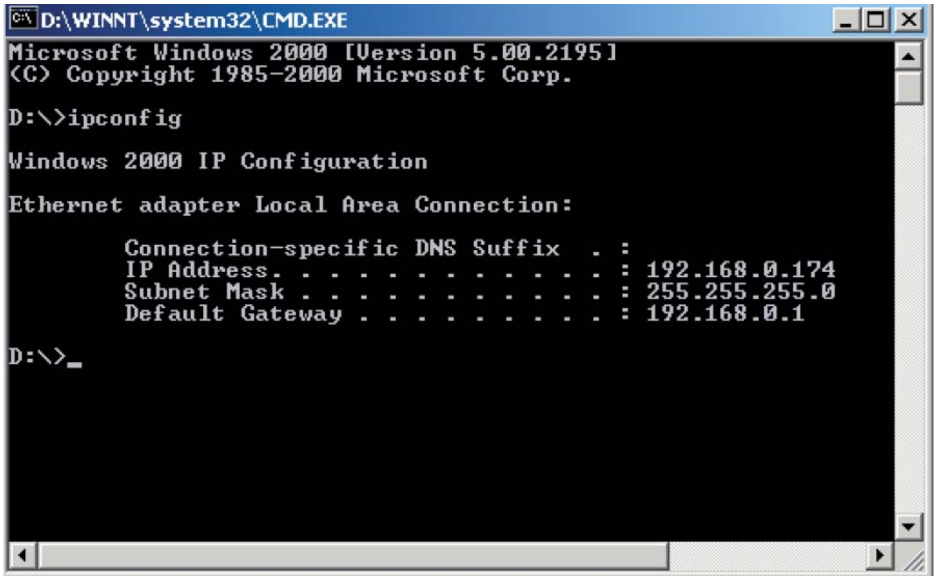


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

- From the Command Prompt, enter **ipconfig**. It will return your IP Address, subnet mask, and default router.



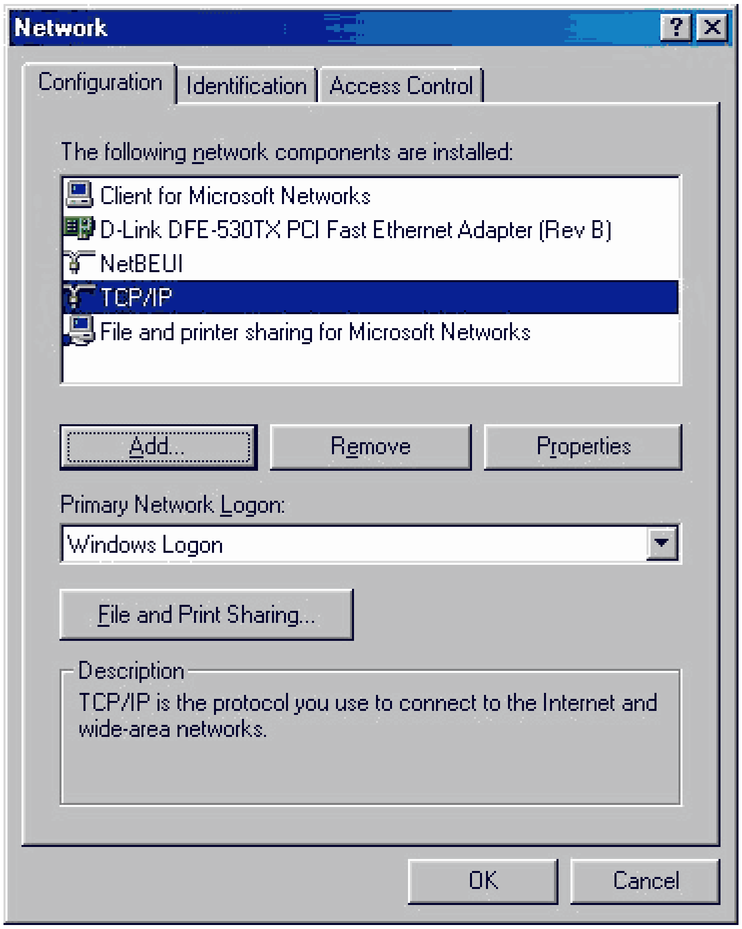
D:\WINNT\system32\CMD.EXE

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.174
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

D:\>_
```

- Type exit to close the command prompt.
- Make sure you take note of your computer´s Default Router IP Address. The Default Router is the IP Address of the router. By default, it should be **192.168.16.168**

3. How can I assign a Static IP Address in Windows 98/Me?

- From the desktop, right-click on the **Network Neighborhood** icon (Win ME - My Network Places) and select **Properties**.
- Highlight **TCP/IP** and click the **Properties** button. If you have more than 1 adapter, then there will be a TCP/IP “Binding” for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



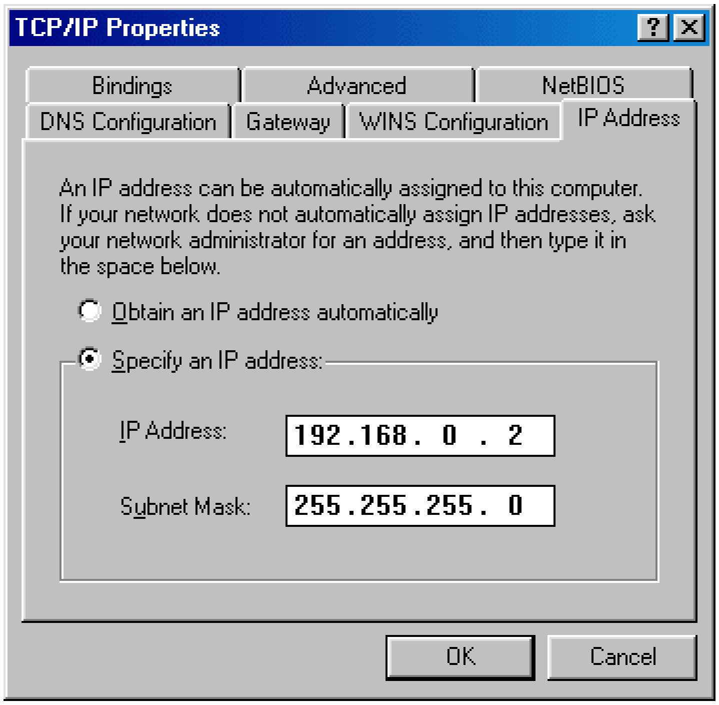
The following network components are installed:

Client for Microsoft Networks
D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)
NetBEUI
TCP/IP
File and printer sharing for Microsoft Networks

Primary Network Logon:
Windows Logon

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

- Click **Specify an IP Address**.
- Enter in an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.16.168, make your IP Address 192.168.16.X where X is between 2-99. Make sure that the number you choose is not in use on the network.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

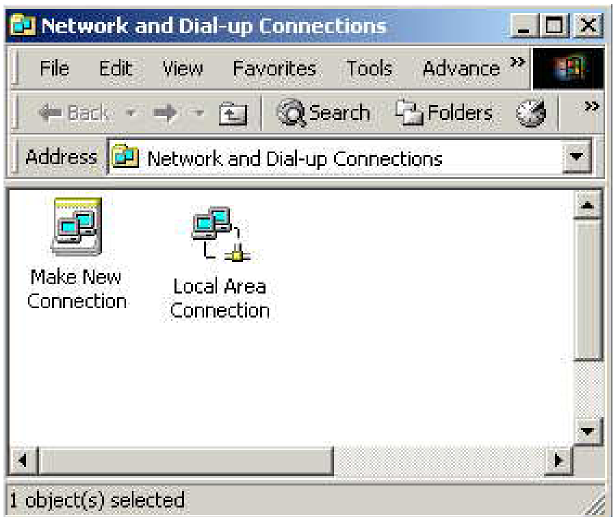
IP Address: 192.168. 0 . 2

Subnet Mask: 255.255.255. 0

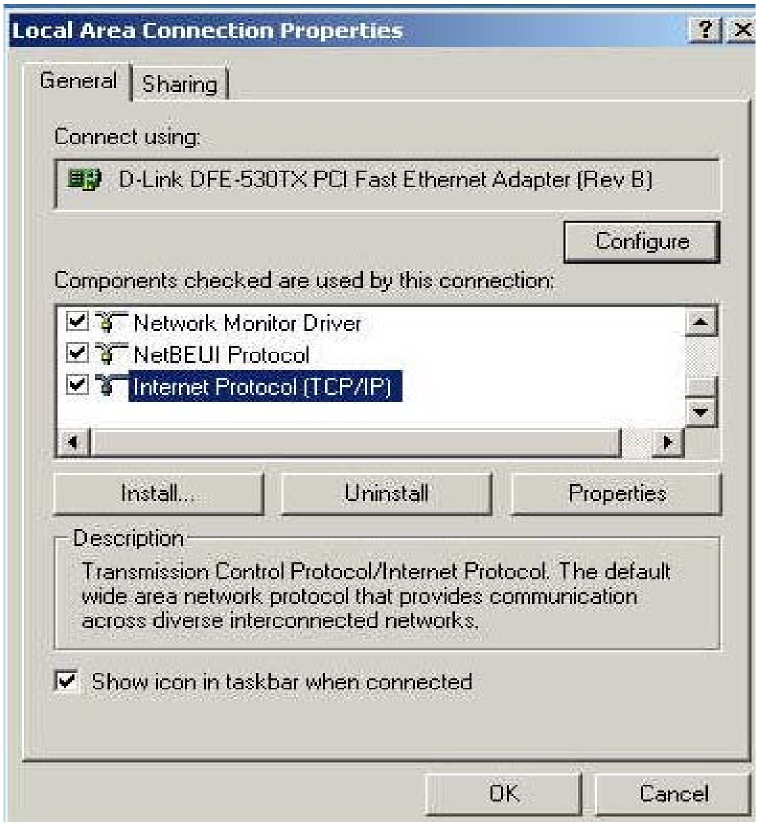
- Click **OK** twice.
- When prompted to reboot your computer, click **Yes**. After you reboot, the computer will now have a static, private IP Address.

4. How can I assign a Static IP Address in Windows 2000?

- Right-click on **My Network Places** and select **Properties**.
- Right-click on the **Local Area Connection** which represents your network card and select **Properties**.


Network and Dial-up Connections
File Edit View Favorites Tools Advance
Back Search Folders
Address Network and Dial-up Connections
Make New Connection
Local Area Connection
1 object(s) selected

- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.



Connect using:

D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)

Components checked are used by this connection:

☑ Network Monitor Driver
☑ NetBEUI Protocol
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

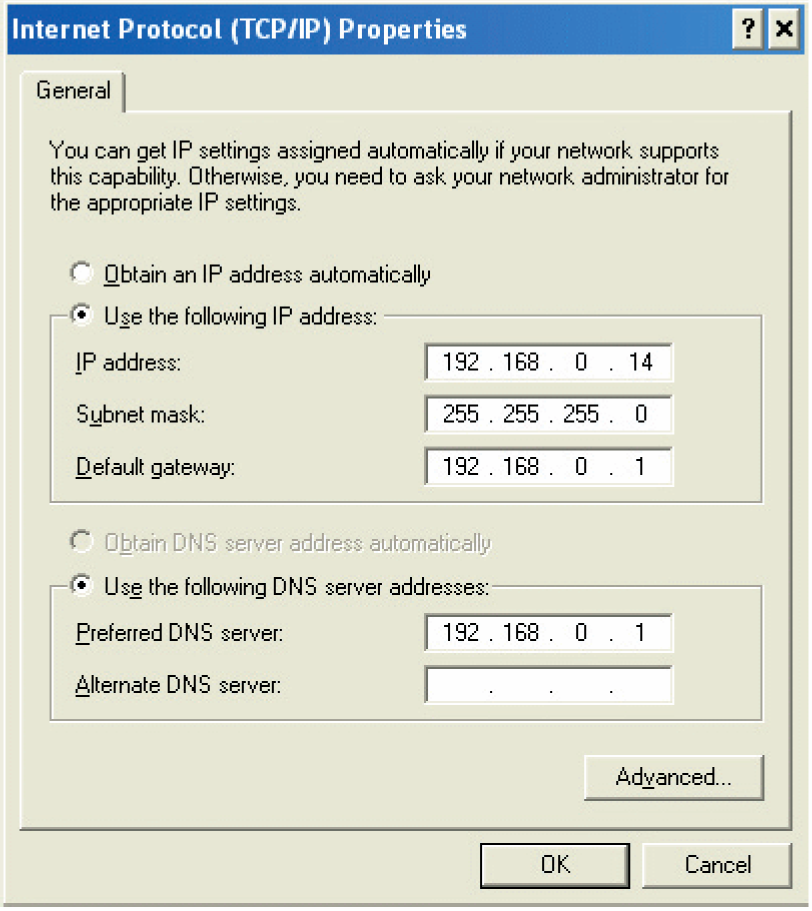
- Click **Use the following IP Address** and enter an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.16.168, make your IP Address 192.168.16.X where X = 2-99. Make sure that the number you choose is not in use on the network.

.

- Click **OK** twice. You may be asked if you want to reboot your computer. Click **Yes**.

5. How can I assign a Static IP Address in Windows XP?

- Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
- See the steps for assigning a static IP address in Windows 2000 and continue from there.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 0 . 14
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 0 . 1
Alternate DNS server:	. . .

- Access the Web management. Open your Web browser and enter the IP Address of your router device in the address bar. This should open the login page for the Web management. Follow instructions to login and complete the configuration.

Chapter 4. Powerline Networking Utility

Note. The Powerline Device can auto detect the other powerline bridges which plug in the same power circuit, you don't need to use this powerline utility except you want to encryption all the powerline devices as the same group or you can not access the other computers.

Introduction of Configuration Utility

The Configuration Utility for Windows OS enables the user to find Powerline Ethernet devices on the Powerline network; measures data rate performance, ensures privacy, performs diagnostics and secures Powerline networks.

Before install the utility, please check the windows edition of your computer. For vista 64, it need to install the vista 64 utility, you can easy to see it in the CD auto run screen. Please use the correct utility to install; otherwise it can not work properly.

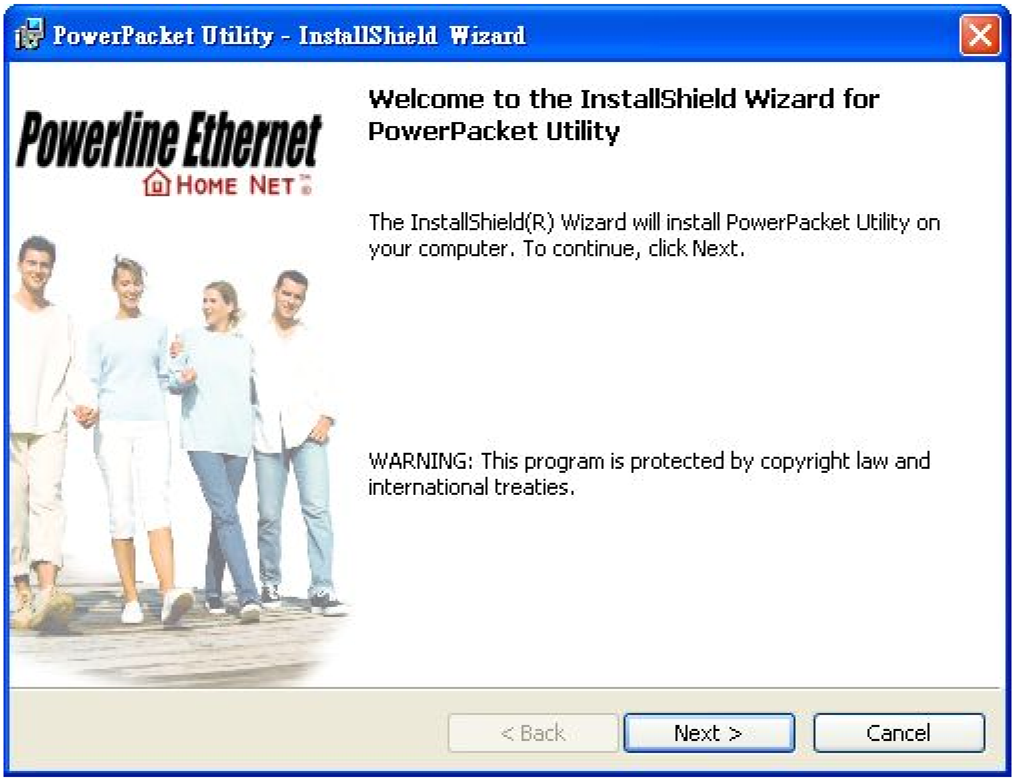
4.1 Configuration Utility Setup

4.1.1 Installation of the Utility

Please verify that no other Powerline Management Utilities are installed before installing this product. If other utilities are installed, uninstall them and restart before installing this software.

To install, insert the Windows OS Configuration Utility Setup utility CD-ROM into the computer's CD-ROM drive. The Setup utility shall run automatically. Choose the correct one utility to install or user can manually install by double clicking the setup.exe file when browse the folder. The CD will launch an installation utility similar to the one shown in *Figure 1*.

This Utility is designed for Powerline 85M/200M Ethernet bridges. Click the **Next** button to continue.



PowerPacket Utility - InstallShield Wizard

Welcome to the InstallShield Wizard for PowerPacket Utility

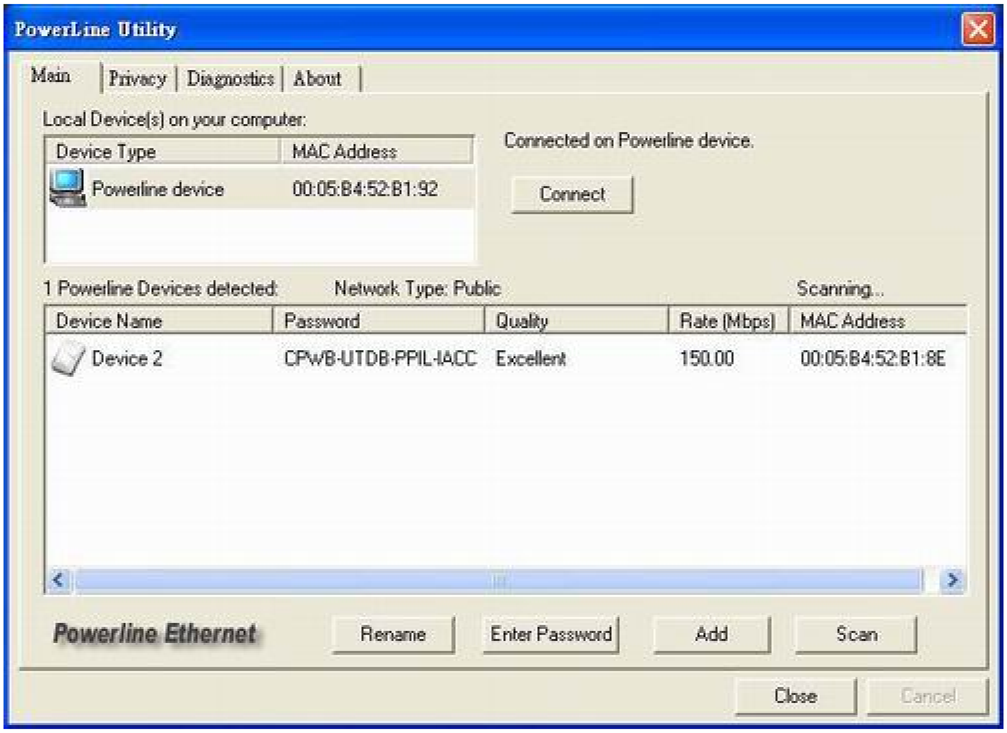
The InstallShield(R) Wizard will install PowerPacket Utility on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 1: Install Shield Screen

4.2 Windows Configuration Utility

In order to run the utility, double-click the utility icon. *Figure 2* shows the main screen of the configuration utility. This screen shot shows a Powerline Ethernet device connected as a local device and other Powerline Ethernet devices as remote devices.



Local Device(s) on your computer:

Device Type	MAC Address
Powerline device	00:05:B4:52:B1:92

Connected on Powerline device.

1 Powerline Devices detected: Network Type: Public Scanning...

Device Name	Password	Quality	Rate (Mbps)	MAC Address
Device 2	CPWB-UTDB-PPIL-IACC	Excellent	150.00	00:05:B4:52:B1:8E

Figure 2: Main Screen with High-Speed Powerline Ethernet device Local

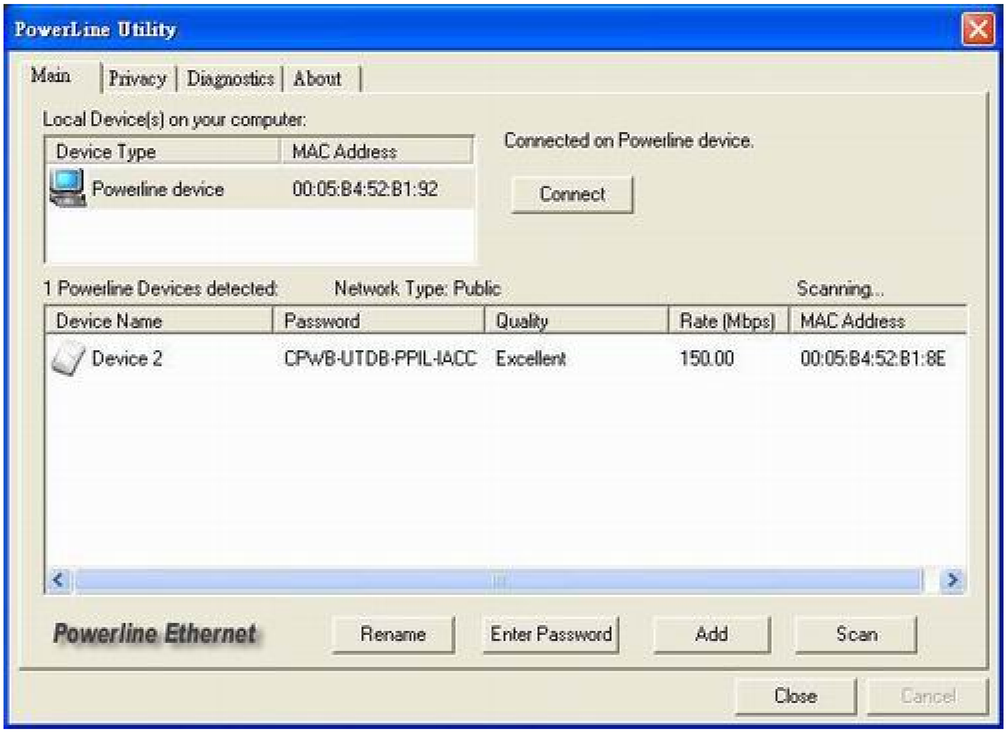
4.3 User Interface

4.3.1 Main Screen

The **Main** screen essentially provides a list of all Powerline Ethernet devices logically connected to the computer where the utility is running.

The top panel shows all local Powerline Ethernet devices found connected to the computer's NIC (Network Interface Card). In most cases, only one device will be seen. In situations where there are more than one device connected, such as a USB and also an Ethernet device, the user may click to select the one to manage through and then click the **Connect** button to its right. The status area above the button indicates that your PC is connected to that same device. Once connected to the chosen local device, the utility will automatically scan the powerline periodically for any other Powerline Ethernet devices. If no local Powerline Ethernet devices are discovered, the status area above the connect button will indicate that accordingly.

Figure 3 illustrates the presence of two local devices in the computer.



Local Device(s) on your computer:

Device Type	MAC Address
Powerline device	00:05:B4:52:B1:92

Connected on Powerline device.

1 Powerline Devices detected: Network Type: Public Scanning...

Device Name	Password	Quality	Rate (Mbps)	MAC Address
Device 2	CPWB-UTDB-PPIL-IACC	Excellent	150.00	00:05:B4:52:B1:8E

Figure 3: Multiple Local Device Connection

The **lower panel** displays all the Powerline Ethernet devices, discovered on the current logical network (remote devices). Displayed immediately above this panel is the number of remote devices found, the type of logical network (Public or Private), and a message area that reports connectivity

and scan status. The following information is displayed for each of the devices discovered that appear in the lower panel:

Device Name column shows the default device name, which may be user re-defined. A user may change the name by clicking on the name and editing in-place, or by using the rename button. An icon is optionally shown with the name. A distinction in icons is made between low-speed and high-speed devices . By default, the icon is displayed with the name.

MAC Address column shows the device's MAC address.

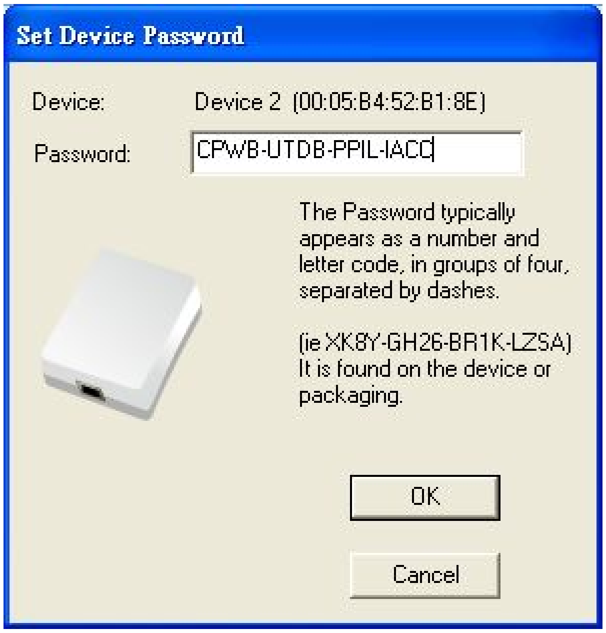
Password column shows the user-supplied device password (initially left blank).

A user may enter the password by using the Enter Password button.

To set the **Password** of the device (required when creating a private network), first select the device by clicking on its name in the lower panel and then click on the Enter Password button.

A dialog box will appear as shown in Figure 4 to type the password. The selected device name is shown above the field for entering the password. Hit OK after entering the new password. A confirmation box will appear if the password was entered correctly.

If a device is not found, the user will be notified and suggestions to resolve common problems will be presented.



Device: Device 2 (00:05:B4:52:B1:8E)

Password: CPWB-UTDB-PPIL-IACC

The Password typically appears as a number and letter code, in groups of four, separated by dashes.

(ie XK8Y-GH26-BR1K-LZSA) It is found on the device or packaging.

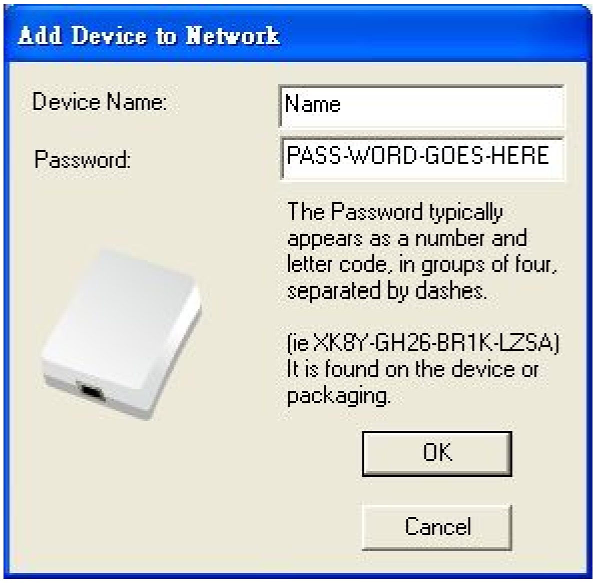
Figure 4: Set Device Password

The **Add** button is used to add a remote device to your network that is not on the displayed list in the lower panel, for example, a device currently on another logical network. Users are advised to locate the passwords for all devices they wish to manage and add them to the local logical network by clicking on the Add button.

A dialog box will appear as seen below. The dialog box allows the user to enter both a device name and the password.

A confirmation box will appear if the password was entered correctly and if the device was found.

If a device is not found, the user will be notified and suggestions to resolve common problems will be presented.



Add Device to Network

Device Name: Name

Password: PASS-WORD-GOES-HERE

The Password typically appears as a number and letter code, in groups of four, separated by dashes.

(ie XK8Y-GH26-BR1K-LZSA) It is found on the device or packaging.

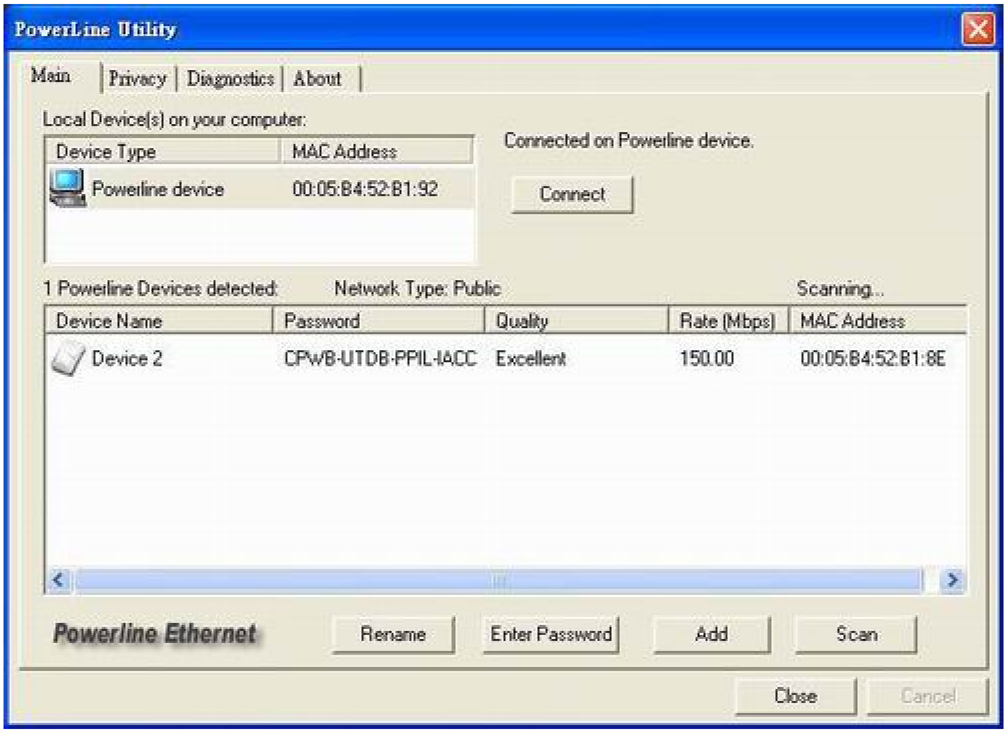
Figure 5: Add Remote Device

Note: The device must be present on the power line (plugged in) in order for the password to be confirmed and added to the network. If the device could not be located, a warning message will be shown.

The **Scan** button is used to perform an immediate search of the Powerline Ethernet devices connected to the computer.

By default the utility automatically scans every few seconds and updates the display.

A typical screen after naming and supplying passwords might appear as in *Figure 6*.



Local Device(s) on your computer:

Device Type	MAC Address
Powerline device	00:05:B4:52:B1:92

Connected on Powerline device.

1 Powerline Devices detected: Network Type: Public Scanning...

Device Name	Password	Quality	Rate (Mbps)	MAC Address
Device 2	CPWB-UTDB-PPIL-IACC	Excellent	150.00	00:05:B4:52:B1:8E

Figure 6: Main Screen of the Configuration Utility

4.3.2 Privacy Screen

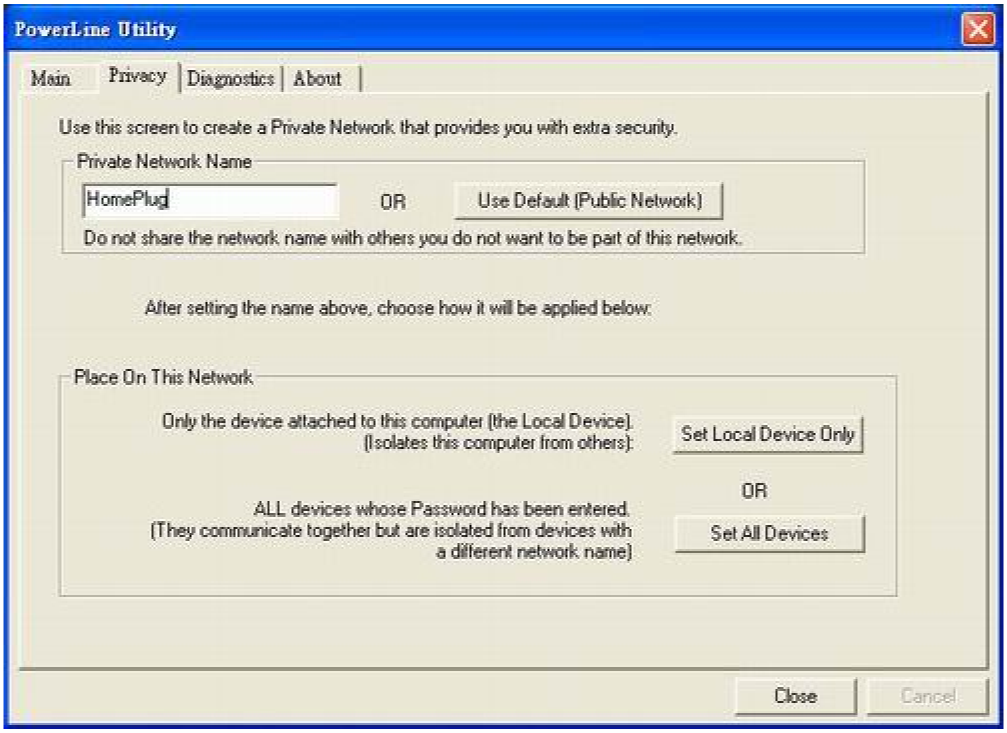
The Privacy dialog screen provides a means for managing the local network and providing additional security.

All Powerline Ethernet devices are shipped using a default logical network (network name), which is normally “**HomePlug**”.

The **Privacy** dialog screen allows user to make the network private by changing the network name (network password) of devices.

The user can always reset a Powerline Ethernet network to the universal one (public) by entering “HomePlug” as the network name or by clicking on the **Use Default** button.

Note: Changing the network name to any other name other than HomePlug will show the network type on the main screen as Private.



Use this screen to create a Private Network that provides you with extra security.

Private Network Name

HomePlug OR

Do not share the network name with others you do not want to be part of this network.

After setting the name above, choose how it will be applied below:

Place On This Network

Only the device attached to this computer (the Local Device).
(Isolates this computer from others):

OR

ALL devices whose Password has been entered.
(They communicate together but are isolated from devices with
a different network name)

Figure 7: Privacy Screen

The **Set Local Device** Only button is used to change the network name (network password) for the local device only.

After doing this, all the devices seen on the Main panel prior to this will no longer be able to communicate or respond to the computer, as they will be on a different logical network. Devices previously set up with the same logical network (same network name) will appear in the device list afterward selecting this option.

The **Set All Devices** button is used to change the logical network of all devices that appear on the Main panel.

The user must have entered the device's Password in order to set it to the new logical network. A notification message will appear to report the success of this operation.

4.4 Diagnostics Screen

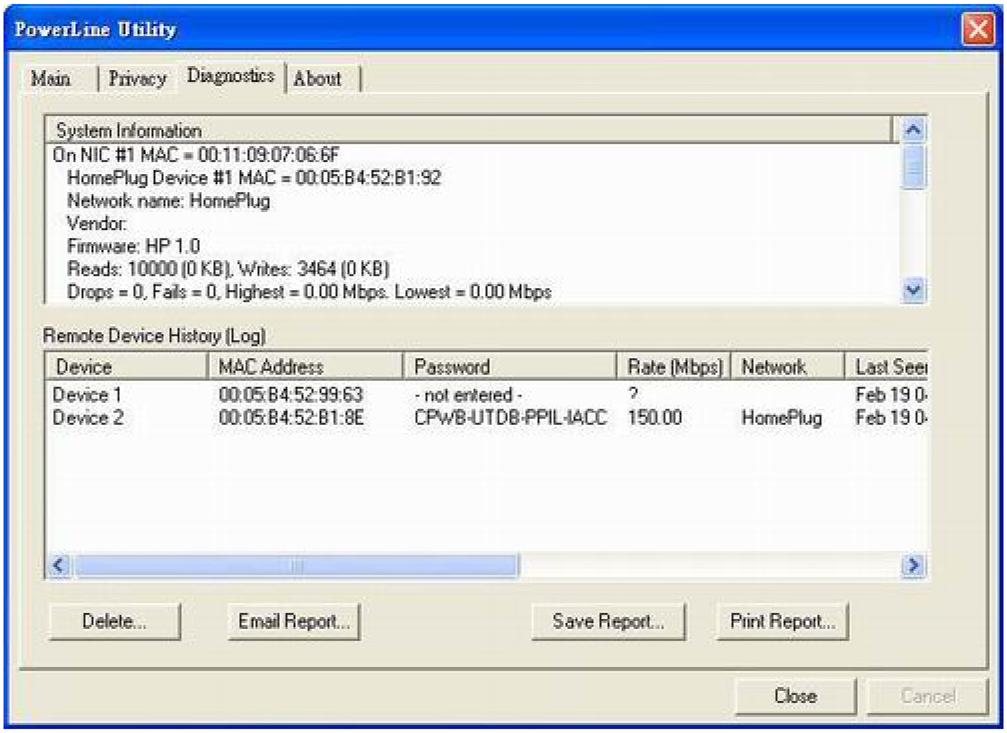
The **Diagnostics** screen shows system information and a history of all devices seen.

The appearance is shown in *Figure 8*.

The **upper panel** shows technical data concerning software and hardware on the host computer used to communicate over Powerline Ethernet Network.

It shall include the following:

- Operating System Type/Version
- Host Network Name
- User Name
- MAC Address of all NICs (network interface card)
- Identify versions of all Driver DLLs and Libraries used (NDIS) and optionally
- MAC Firmware Version



System Information

```
On NIC #1 MAC = 00:11:09:07:06:6F
  HomePlug Device #1 MAC = 00:05:B4:52:B1:92
  Network name: HomePlug
  Vendor:
  Firmware: HP 1.0
  Reads: 10000 (0 KB), Writes: 3464 (0 KB)
  Drops = 0, Fails = 0, Highest = 0.00 Mbps, Lowest = 0.00 Mbps
```

Remote Device History (Log)

Device	MAC Address	Password	Rate (Mbps)	Network	Last Seei
Device 1	00:05:B4:52:99:63	- not entered -	?		Feb 19 0
Device 2	00:05:B4:52:B1:8E	CPWB-UTDB-PPIL-IACC	150.00	HomePlug	Feb 19 0

Figure 8: Diagnostics Screen

The **lower panel** contains a history of all remote devices seen on the computer, over time. Devices are shown here regardless of whether or not they are on the same logical network. Devices that are active on the current logical network will show a transfer rate in the Rate column; devices on other networks, or devices that may no longer exist are shown with an "?" in the Rate column.

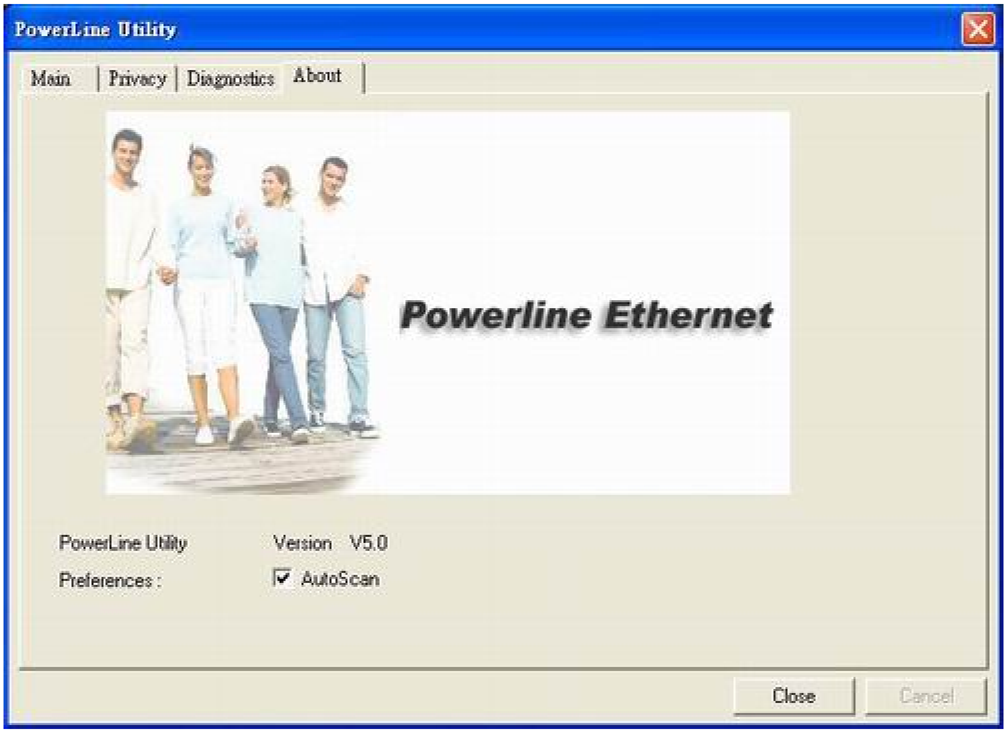
The following remote device information is available from the diagnostics screen:

- Adapter Alias Name
- Adapter MAC Address
- Adapter Password
- Adapter Last known rate
- Adapter Last Known Network
- Date device last scanned
- MAC Firmware Version

The diagnostics information displayed may be saved to a text file for later emailing to technical support of a manufacturer or printed for reference during a technical support call. Devices no longer part of the network can be deleted using the delete button.

4.4.1 About Screen

The screen shows the software release date.



PowerLine Utility Version V5.0

Preferences : ☑ AutoScan

Figure 9: About dialog screen

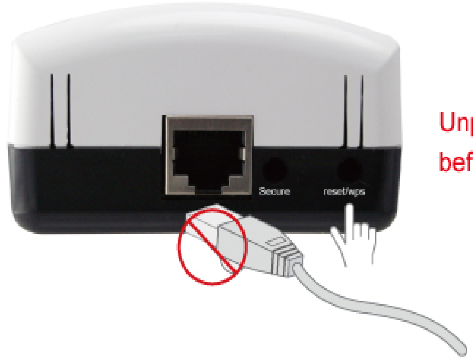
4.4.2 Preferences

The lower part of the panel may display options for user preferences (such as turning the auto-scan feature on or off) as shown *Figure 9* above.

5. Push Button Setting

There are 2 buttons in this device, one is Reset button the other is Secure button.

Reset: Push this button can reset to the factory default settings. **Be careful, when you press the reset button, please make sure unplug (remove) the Ethernet cable (RJ-45cable) first, and then press the reset button. After press the reset button (the time need < 3 sec) and then wait the PWR LED light again. Don't power off when the device is in reset process.**



Unplug the Ethernet Cable first
before press the Reset button.

Secure button can auto secure and group the Powerline devices, the follow is the scenario for secure button.

Two Push Button trigger state conditions

"Adder state" for a device providing the NMK for an existing AVLN

"Joiner state" for a device that will join an AVLN

Pushing buttons on any two devices results in one of them becoming an "adder" and the other one a "joiner"

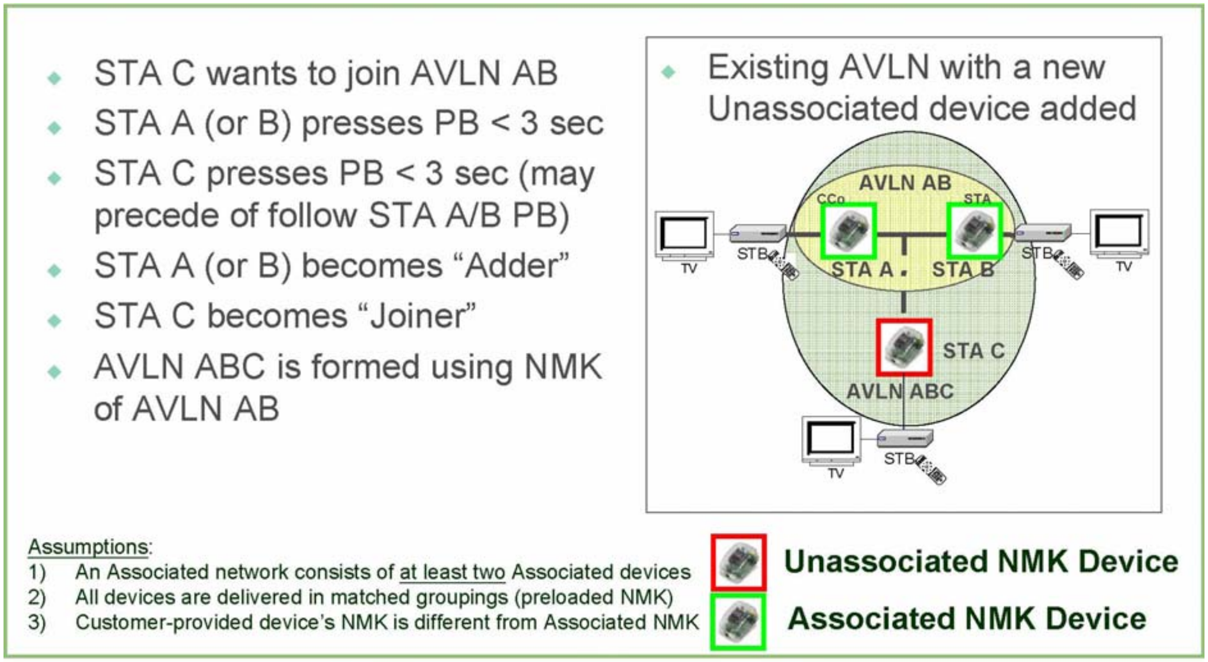
Three possible scenarios

Unassociated device joining an existing AVLN

- Two Unassociated devices joining to form a new AVLN
- Special case: one device is a CCo, the other is a STA

Two Associated devices joining to form an AVLN with a new NMK

Possible Use Case Scenario 1: Unassociated device joining existing AVLN



- STA C wants to join AVLN AB
- STA A (or B) presses PB < 3 sec
- STA C presses PB < 3 sec (may precede of follow STA A/B PB)
- STA A (or B) becomes "Adder"
- STA C becomes "Joiner"
- AVLN ABC is formed using NMK of AVLN AB

- Existing AVLN with a new Unassociated device added

Assumptions:

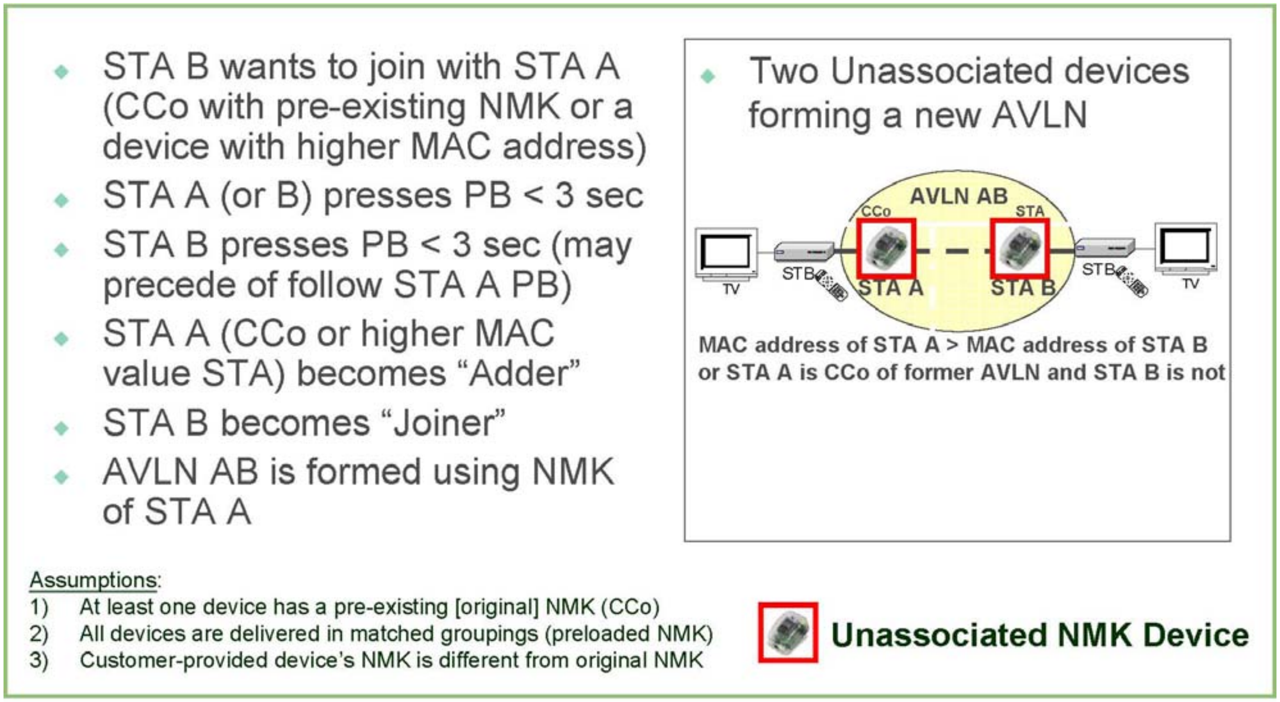
1) An Associated network consists of at least two Associated devices
2) All devices are delivered in matched groupings (preloaded NMK)
3) Customer-provided device's NMK is different from Associated NMK

🟥 Unassociated NMK Device

🟩 Associated NMK Device

Possible Use Case Scenario 2: Two devices joining to form new AVLN

Before this scenario begin, please make sure to press each device secure button > 10 sec till all LEDs re-flash to generate the random network password key first.



- STA B wants to join with STA A (CCo with pre-existing NMK or a device with higher MAC address)
- STA A (or B) presses PB < 3 sec
- STA B presses PB < 3 sec (may precede of follow STA A PB)
- STA A (CCo or higher MAC value STA) becomes "Adder"
- STA B becomes "Joiner"
- AVLN AB is formed using NMK of STA A

- Two Unassociated devices forming a new AVLN

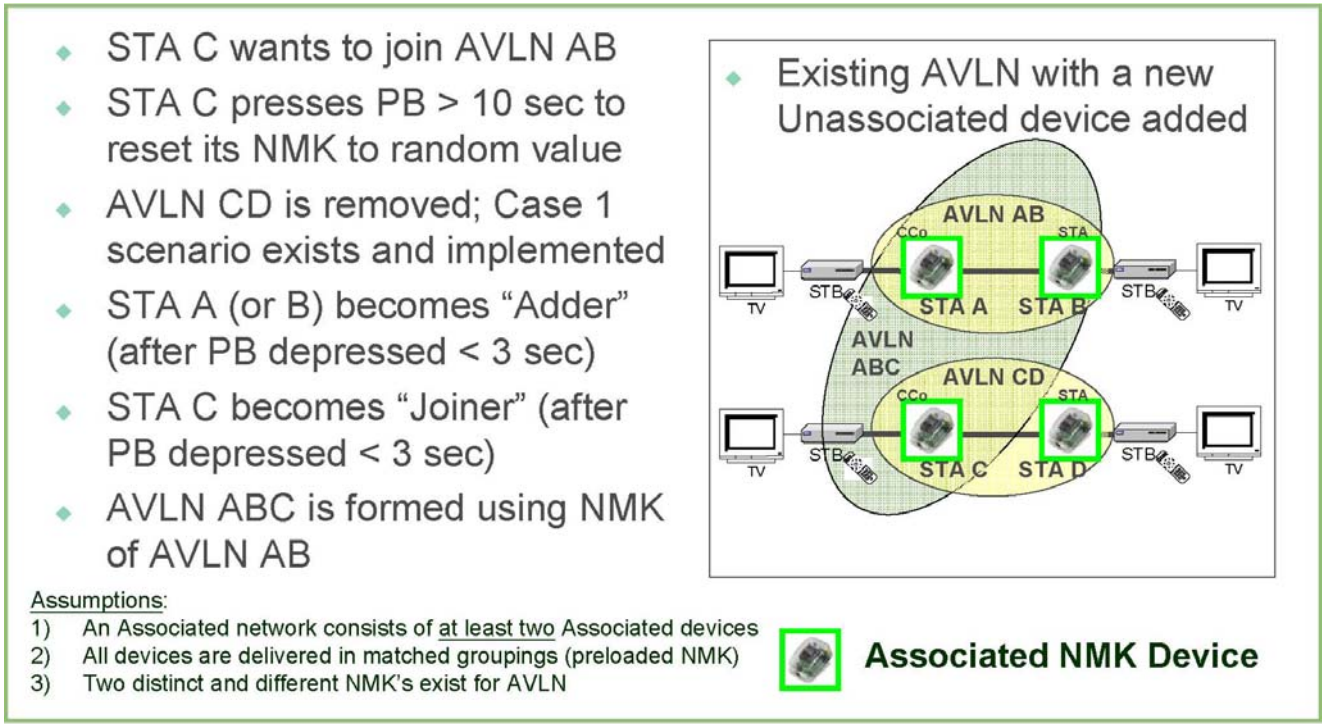
MAC address of STA A > MAC address of STA B or STA A is CCo of former AVLN and STA B is not

Assumptions:

1) At least one device has a pre-existing [original] NMK (CCo)
2) All devices are delivered in matched groupings (preloaded NMK)
3) Customer-provided device's NMK is different from original NMK

🟥 Unassociated NMK Device

Possible Use Case Scenario 3: Reset



- STA C wants to join AVLN AB
- STA C presses PB > 10 sec to reset its NMK to random value
- AVLN CD is removed; Case 1 scenario exists and implemented
- STA A (or B) becomes “Adder” (after PB depressed < 3 sec)
- STA C becomes “Joiner” (after PB depressed < 3 sec)
- AVLN ABC is formed using NMK of AVLN AB

- Existing AVLN with a new Unassociated device added

Assumptions:

1) An Associated network consists of at least two Associated devices
2) All devices are delivered in matched groupings (preloaded NMK)
3) Two distinct and different NMK’s exist for AVLN

Associated NMK Device

6. Trouble Shooting

1. Why my utility can not work properly after finish install steps?

Ans:

Please follow the steps to check the problem.

1. Check the Windows version, the utility only can support windows 2000, XP, 2003, vista 32, Vista 64.
2. Reinstall the utility again, you can remove it and reinstall the utility again.
3. If the OS is vista 64, make sure you install the correct utility for vista 64. You can see it in CD auto run utility page.

2. What kind of windows OS can install the Powerline utility?

Ans:

Now the Powerline utility only supports Windows 2000, XP and 2003, Vista 32/64.

3. Why the throughput of Powerline 200M bridge is bad?

Ans:

Please follow the steps to check the problem.

1. Due to the master/slave structure, you need to avoid plugging two Powerline bridge in the same time, so you had better plug the Powerline to the power outlet sequence.
2. Please unplug the Powerline bridge and plug again, please remember plug them in sequence. Check the Powerline utility and check the throughput again.

4. Why the Powerine 200M device can not work stable?

Ans:

In some respects, User had better to adjust the NB/PC NIC's connection type setting to 100MBaseTx half duplex while connect to powerline 200M device. It will keep the performance to the best status and stable. When user found the link is unstable or not good, please change the NIC's connection type setting to half duplex.

Appendix A Glossary

Address mask

A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

AAL5

ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ADSL

Asymmetric digital subscriber line.

ATM

Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation.
ATM offers fast packet technology, real time; demand led switching for efficient use of network resources.

AWG

American Wire Gauge - The measurement of thickness of a wire.

Bridge

A device connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

Broadband

Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO

Central Office. Refers to equipment located at a Telco or service provider's office.

CPE

Customer Premises Equipment located in a user's premises.

DHCP (Dynamic Host Configuration Protocol)

DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT

Discrete Multi-Tone frequency signal modulation

Downstream rate

The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM

Digital Subscriber Line Access Multiplex

Dynamic IP Addresses

A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

Encapsulation

The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

Ethernet

One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP

File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

Hop count

A measure of distance between two points on the Internet. It is equivalent to the number of routers that separate the source and destination.

HTML

Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http

Hypertext Transfer Protocol - The protocol used to carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP

Internet Control Message Protocol - The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP

Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC

Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB

Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT

Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT

Network Virtual Terminal

PAP

Password Authentication Protocol

PORT

The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS

Plain Old Telephone Service - This is the term used to describe basic telephone service.

PPP

Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE

PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server

A network computer allows a user to log on to the network from a distant location.

RFC

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org..

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many routers and many physical networks. In the Internet, each datagram is routed separately.

Router

A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing table

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET

(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.

(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When three or more LAN's segments are connected via bridges, a loop can occur. Because a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at either end

Static IP Addresses

A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet

For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP

Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP

Trivial File Transfer Protocol - A simple file transfer protocol (a simplified version of FTP) that is often used to boot diskless workstations and other network devices such as routers over a network (typically a LAN).

Telnet

The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging

So named because the intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding; learning workstation addresses and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP

User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling

User Network Interface signaling for ATM communications.

Virtual Connection (VC)

A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

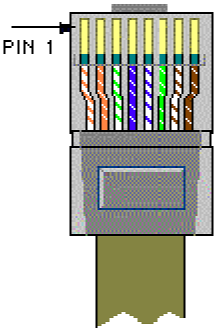
Appendix B Cabling / Connection

Network cables connect PCs in an Ethernet network Category 5, called "Cat5" for short is commonly used type of network cable today.

Cat 5 cables are tipped with RJ-45 connectors, which fit into RJ-45 port.

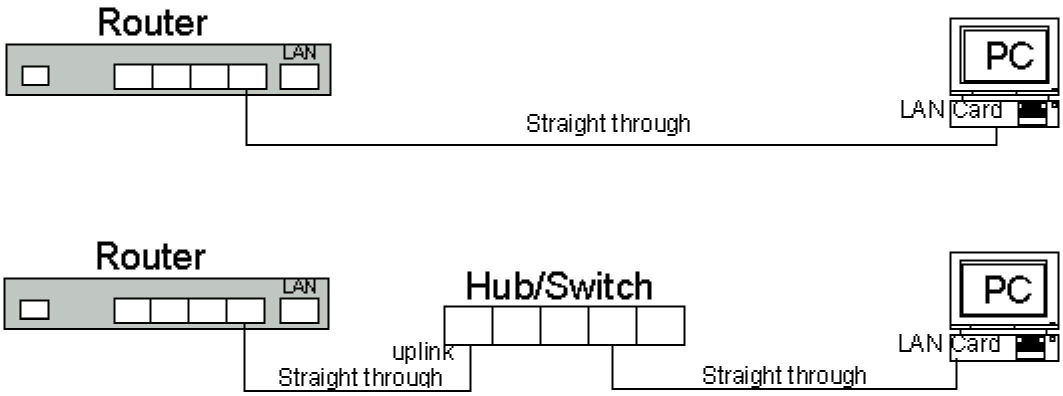
Straight-through vs. Crossover Cables:

Straight-through	
Wire	**Becomes**
1	1
2	2
3	3
6	6



Straight-through	
Wire	**Becomes**
1	1
2	2
3	3
6	6

LAN Connection:



To check LEDs light up when you finish connecting two pieces of hardware.