D-Link®

Version 2.3 | 01/11/2011

User Manual

AP Manager II

Table of Contents

Product Overview 1

System Requirements 1
Minimum Software Requirements 1
Access Point Requirements 1

Software Installation 2

Install PostgreSQL Server 2
Install AP Manager II 2

Using AP Manager II 6

General View 7
Discovering Devices 7
Advanced Discovery 8
Access Point Report 9
Station Detail 9
Station Report 11
Model Report 12
Band Report 13
Group View 14
Configuration 15
Set IP 16
Update Configuration 17
Upgrade Firmware 18
Web Management 19
Telnet 20
Change Access Password 20
SNMP Enable 21
Config Comparison 22
Sorting 23
View 25
Property 25
Configuring APs with AP Manager II 26
Home 27
Information 27
Basic 28
Wireless 28
Wireless Authentication 29
Security 30
WEP Encryption (AP Mode) 31
WPA/WPA2 Enterprise (AP Mode) 32
WPA/WPA2 Personal (AP Mode) 33
WDS Mode 34
WDS with AP Mode 35
Wireless Client (802.11n Only) 36
LAN 37
Dynamic (DHCP) 37
Static (Manual) 38
Advanced 39
Performance (802.11g) 39
Performance (802.11n) 41
Filter (Wireless MAC ACL) 43
Filter (WLAN Partition) 44
Grouping (AP Grouping Settings) 45
DHCP Server (Dynamic Pool Settings) 46
DHCP Server (Static Pool Settings) 48
DHCP Server (Current IP Mapping List) 50

Multi-SSID 52
Rogue AP 54
Intrusion (802.11n only) 55
VLAN (802.11n only) 56
Add/Edit VLAN (802.11n only) 57
PVID Setting (802.11n only) 58
QoS (802.11n only) 59
Schedule (802.11n only) 60
AP Array (802.11n only) 61
ARP Spoofing Prevention (802.11n only) 62
Internal RADIUS Server 63
Traffic Control 64
Uplink and Downlink Settings 64
QoS 65
Traffic Manager 66
Maintenance (802.11g) 67
Admin 67
Firmware and SSL 68
Configuration File 69
SNTP 70
Maintenance (802.11n) 71
Admin 71
Firmware and SSL 73
Configuration File 74
Date and Time 75
Status (802.11g) 76
Device Information 76
Stats 77
Ethernet Traffic Statistics 77
Client Information 78
Log View 79
Log Settings 80
Status (802.11n) 81
Device Information 81
WLAN Traffic Statistics 82
Ethernet Traffic Statistics 83
Client Information 84
WDS Information 85
Log View 86
Log Settings 87
System 88
Multiconfiguration 90
Template 90
Create a New Template 91
Edit a Template 94
Delete a Template 94
Import or Export a Template 94
Task Schedule 95
Config Comparison 95
Upgrade Firmware 98
MultiConfig 100
Fault Manager 102
Tools 106
Topology 106
Site Planning 113
Report 117
Association 117
By Access Point 117
By Wireless Station 118
Security 119
Utilization 120
Channel 121

Rogue AP 122
Syslog 123
Custom 123
Monitor 124
User Management 126
System Environment 127

Product Overview

AP Manager II is a convenient software tool used to manage the configuration of your wireless network from a central computer. With AP Manager II there is no need to configure devices individually.

AP Manager II allows you to configure AP settings, update the firmware, and organize and sort your APs into manageable groups.

System Requirements

- Computer with Windows® 2000/XP/2003/Vista®
- An installed Ethernet Adapter
- At least 128MB of memory and a 500MHz processor

Minimum Software Requirements

- PostgreSQL Server
- PostgreSQL © ODBC Connector (psqlodbc)

Access Point Requirements

- SNMP must be enabled on Access Points used with AP Manager II

Software Installation

Install PostgreSQL Server

Before installing AP Manager II on your computer, you must first install PostgreSQL Server and PostgreSQL© ODBC Connector. During the AP Manager II install process, AP Manager II will check if these PostgreSQL programs have been installed. If they are not found, you will be reminded to download them.

The PostgreSQL© software and documentation can be found at the following links:

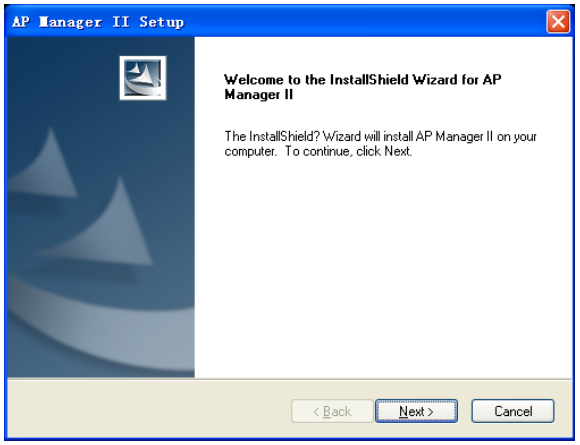
PostgreSQL© Server:
http://www.enterprisedb.com/products/pgdownload.do#windows

PostgreSQL© ODBC Connector:
http://wwwmaster.postgresql.org/download/mirrors-ftp?file=%2Fodbc%2Fversions%2Fmsi%2F

Install AP Manager II

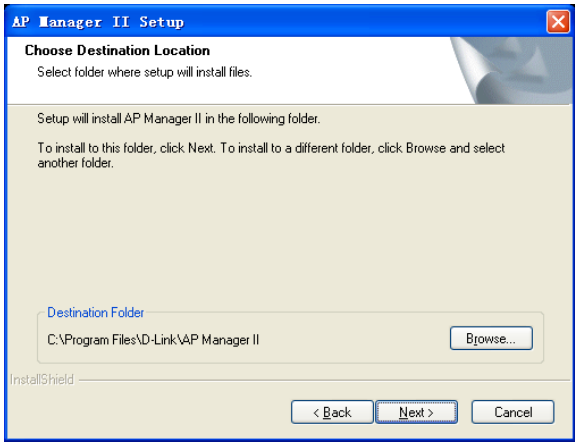
Once the PostgreSQL Server and PostgreSQL ODBC Connector programs have been installed, proceed with the AP Manager II installation. To launch the AP Manager II installation, double-click the installation package icon:

As the installation begins, a welcome screen appears and recommends you end all other programs running before continuing with the installation. Click **Next** to continue.



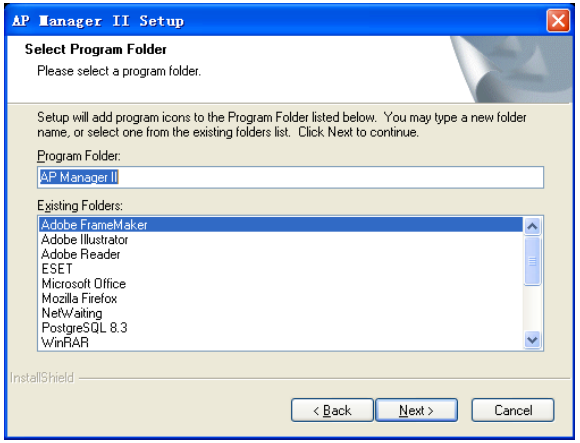
Choose Destination Location

By default, AP Manager II will be installed in the **C:\Program Files\D-Link\AP Manager II** directory. Click **Browse** to select a new location to install the software or click **Next** to continue.



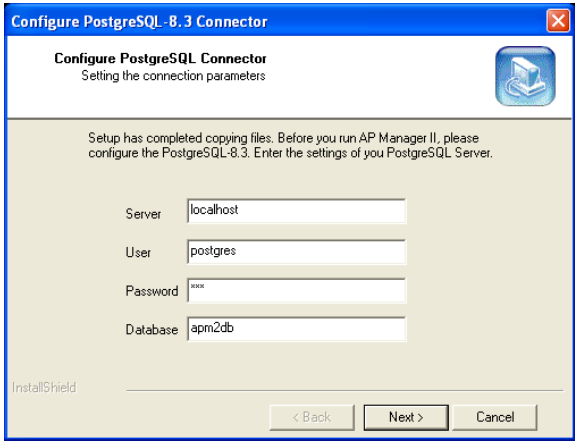
Select Program Folder

By default, the setup process will install the program in a folder called **AP Manager II.** You can keep this setting, type in a new folder name, or choose one from the list of existing folders. Click **Next** to continue.

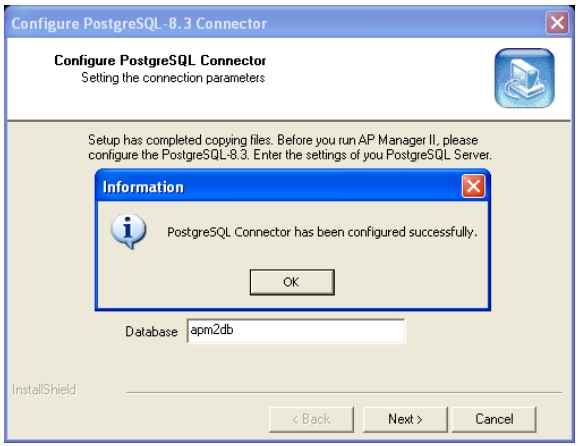


Configure PostgreSQL Connector

To configure the PostgreSQL Connector, enter the IP Address of the PC running the PostgreSQL server, the root username and password and database name. These settings are configured during the PostgreSQL Server install process. Click **Next** to continue.

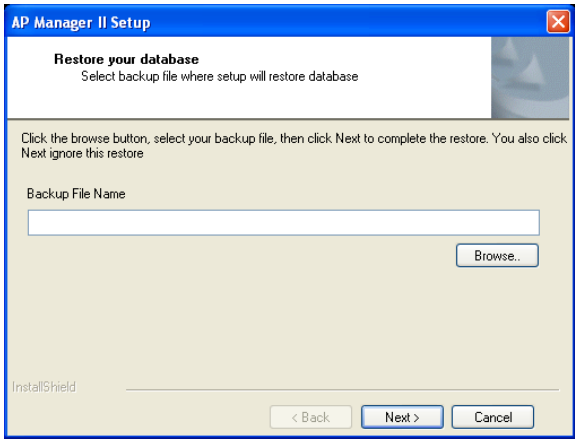


If the PostgreSQL Connector is configured properly, you will get a message confirming the setup was successful. Click **OK** to continue.



Restore your database

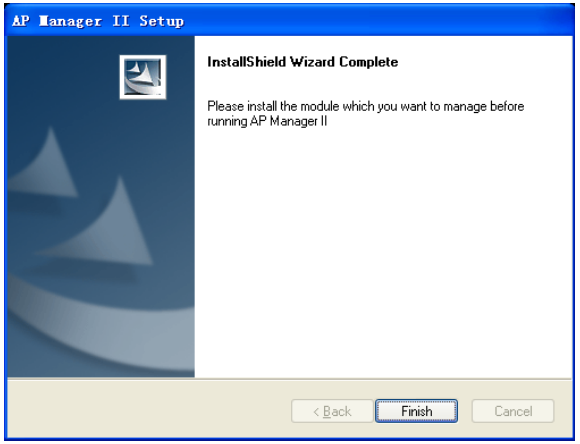
Select backup file where setup will restore database. Click **Next** to continue.



Install Complete!

When the InstallSheild Wizard has completed, Click **Finish** to complete the installation.

After the installation of AP manager II, you need to install the managed AP modules by double-click the module installation packages.

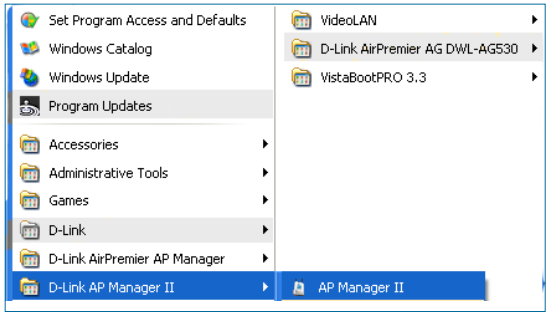


Double click the **AP Manager II** icon, the program will launch and you will be prompted with a login screen. The default user name is **admin** and the default password is **admin**. Continue to the next section in this manual, "Using AP Manager II".

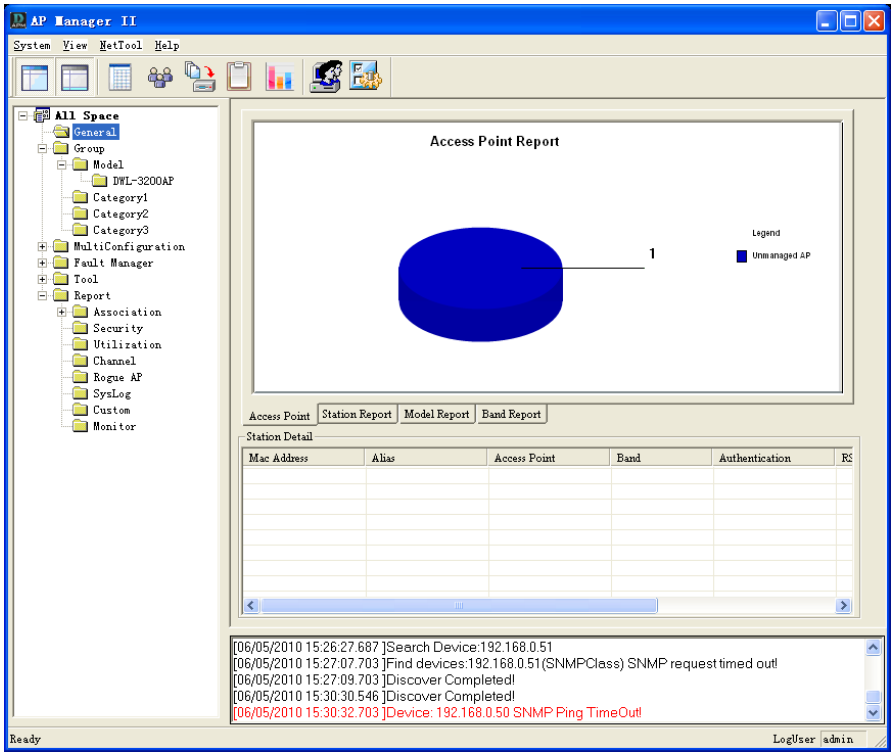
Using AP Manager II

To launch **AP Manager II**:

- Go to the **Start Menu**
- Select **Programs**
- Select **D-Link AP Manager II**
- Select **AP Manager II**



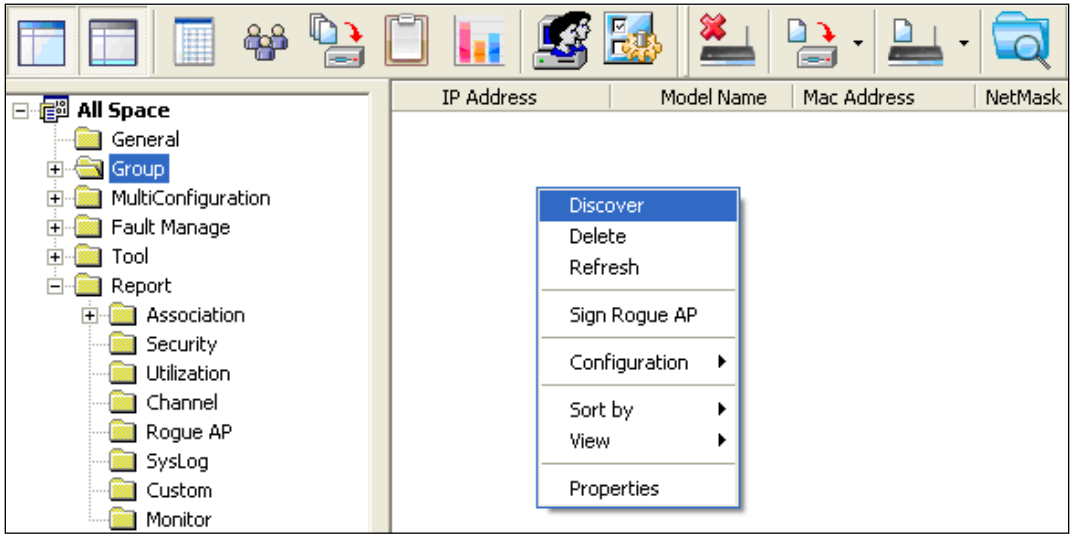
The main AP Manager II screen will appear as shown below:



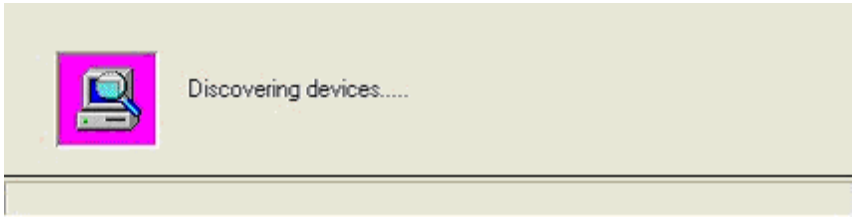
General View
Discovering Devices

Before you can manage and monitor Access Points using the AP Manager II, you must create a list of Access Points. The AP Manager can automatically search for and "discover" Access Points on your LAN using the Discovery process.

To initiate the discovery process, right-click anywhere on the **All Space** > **Group** view window and select **Discover** from the drop-down menu, as shown below.



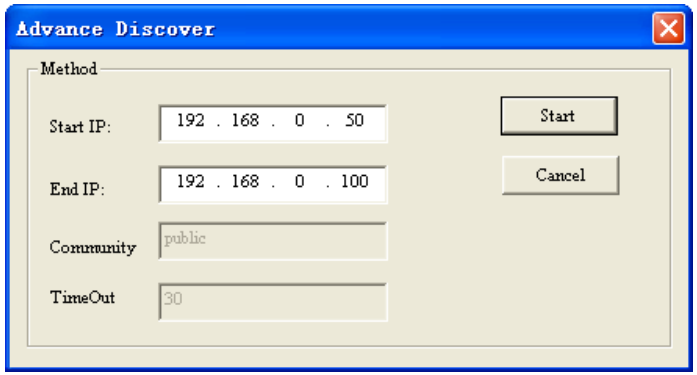
The following dialog window will appear during the Discovery process.



At the end of the Discovery process, the window will close and any Access Points discovered will be added to the **All Space > Group View** window.

Advanced Discovery

The standard discovery can only discover the APs in the same sub network. To discover the APs in the other network segments, highlight the **All Space** > **Group View** window, click the **Discover**/**Advanced Discover** icon in the tools bar and select **Advanced Discover** from the drop down menu, as shown below:



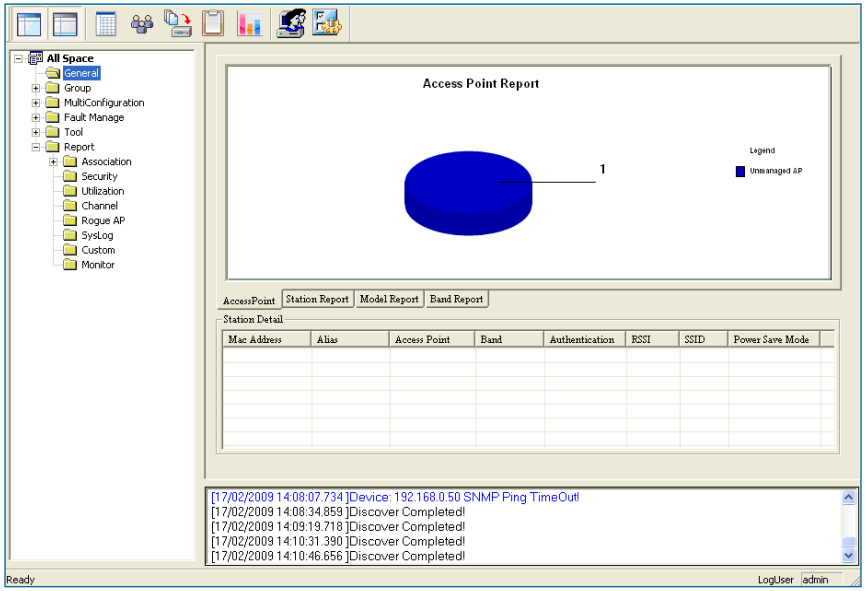
Enter the start/end IP, and then click the Start button to search the APs that can be managed by AP manager II in this IP range. Every detected AP is added an icon at the front of the record according to its type.

Explanation of icons:

Icon	Description
	New found AP.
	Managed AP.
	The AP that cannot be ping, but its IP can be modified.
	The AP is offline or its SNMP engine is off.
	The AP is specified as a Rogue AP. When the AP is online and its SNMP engine is open, the device can be specified as Rogue AP by right-clicking the AP and select the **Sign Rouge AP** item from the drop-down menu.

Access Point Report

The **General View > Access Point** window, as shown below, displays the current list of access points that the AP Manager II has discovered. These Access Points are divided into Managed APs and Unmanaged APs and the results are displayed graphically. The Managed APs are listed in the Station Detail table below the Access Point Report.



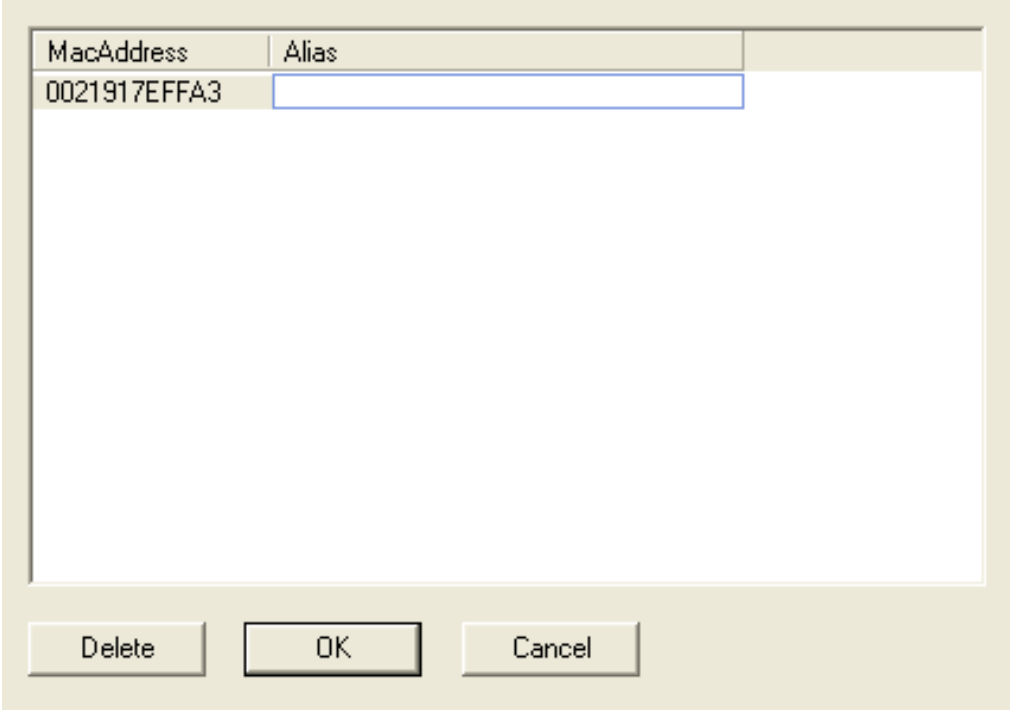
Station Detail

The Station Detail table lists the MAC Address, Alias, Access Point, IP Address, Band, Authentication type, RSSI, SSID, and Power Save Mode of all stations connected to the Managed APs.

Mac Address	Alias	Access Point	Band	Authentication	RSSI	SSID	Power Save Mode
0021917EFFA3	N/A	192.168.0.50	802.11g	OpenSystem	100	Primary-SSID	Off

The Station Detail table allows you to kick off the station from its associated AP. To remove a station from the AP, right-click the station in the **Station Detail** list and select **kick off item** from the drop-down menu.

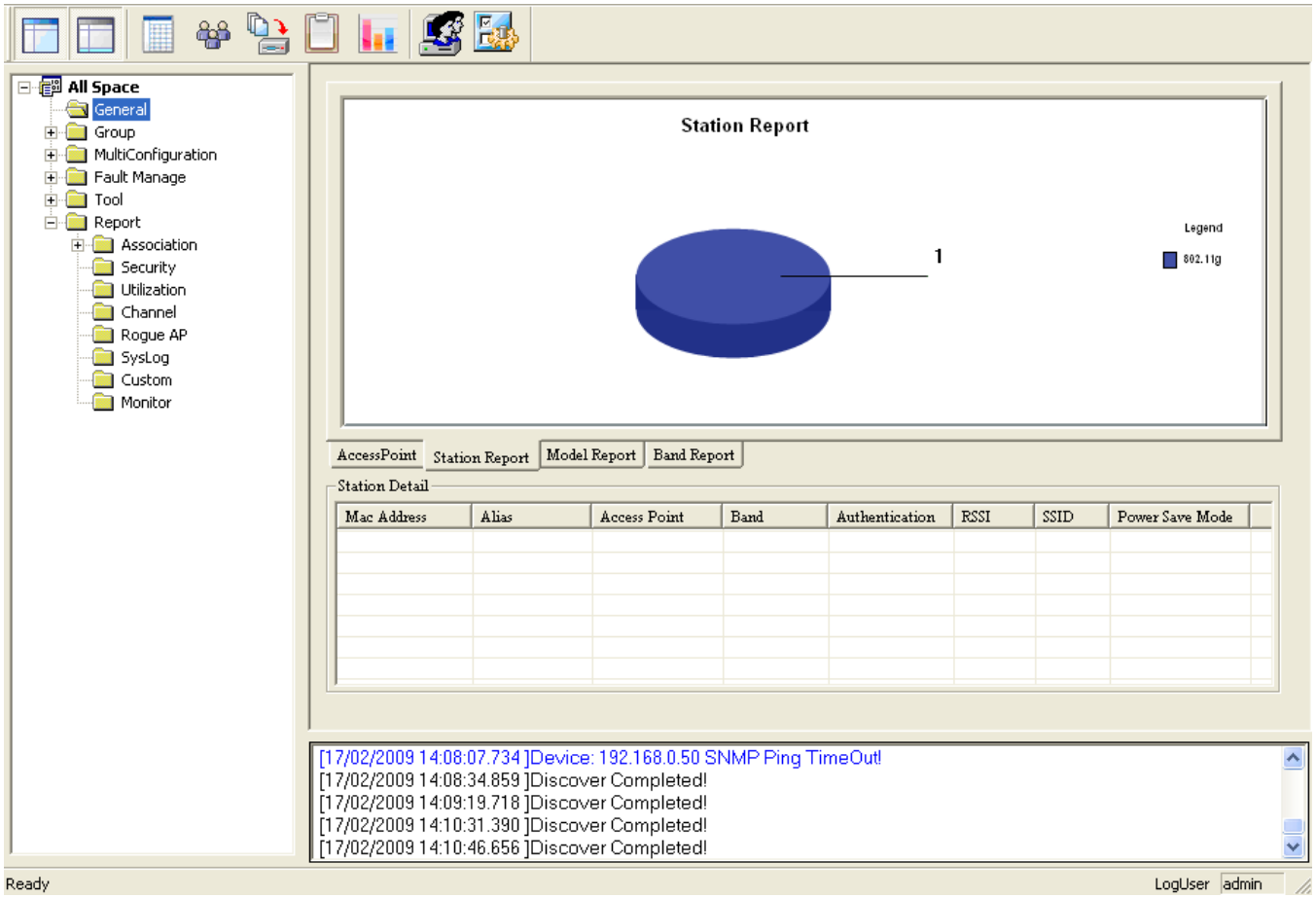
Also you can give a tag to the associated station for better identification. To create an alias, right-click the station in the Station Detail list and select Alias item from the drop-down menu. In the alias management window, double-click the records and then type the alias, shown as below:



Below the Station Report table is a real-time display of the SNMP report exchange between AP Manager II and Managed APs.

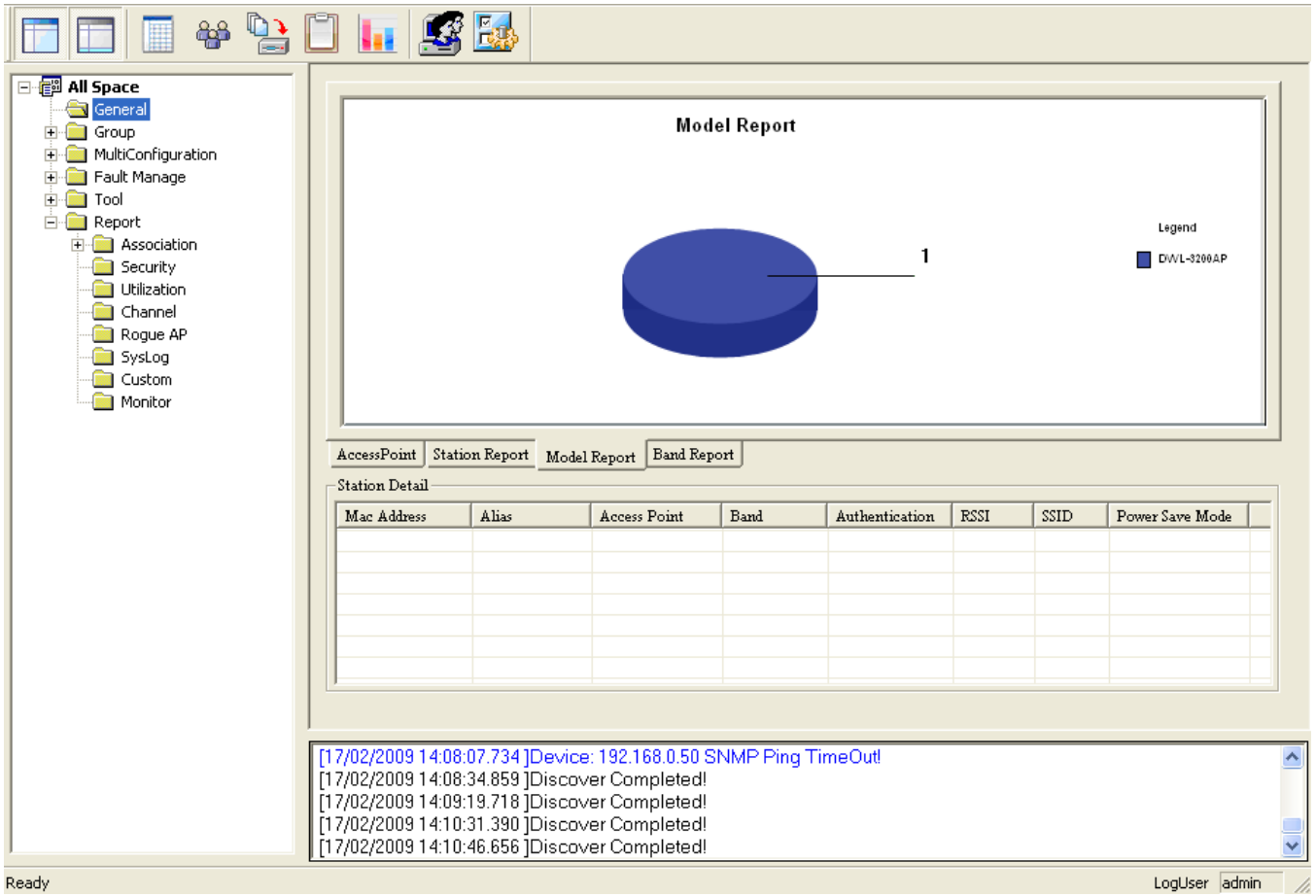
Station Report

The **General View** > **Station Report** displays a graphical representation of the associated wireless stations, as shown below. It classifies the stations by bands, and shows the station numbers of every band.



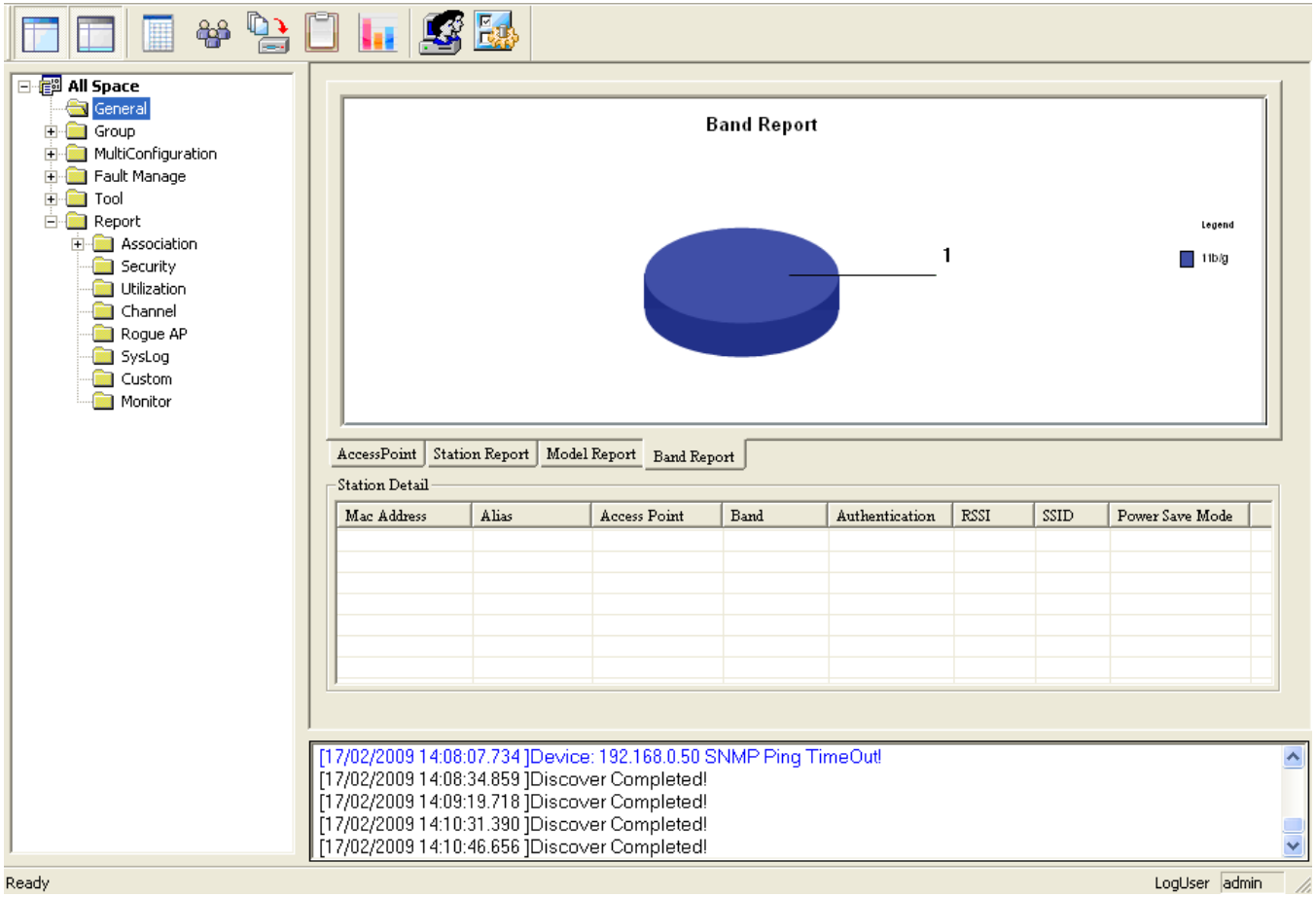
Model Report

The **General View > Model Report** displays a graphical representation of the numerical distribution of models the AP Manager II has discovered and is currently managing.



Band Report

The **General View** > **Band Report** displays a graphical representation of the distribution of WLAN bands (802.11a, 802.11b/802.11g and 802.11b/g/n) currently being used by the APs the AP Manager II is managing. It shows the AP numbers of every band.

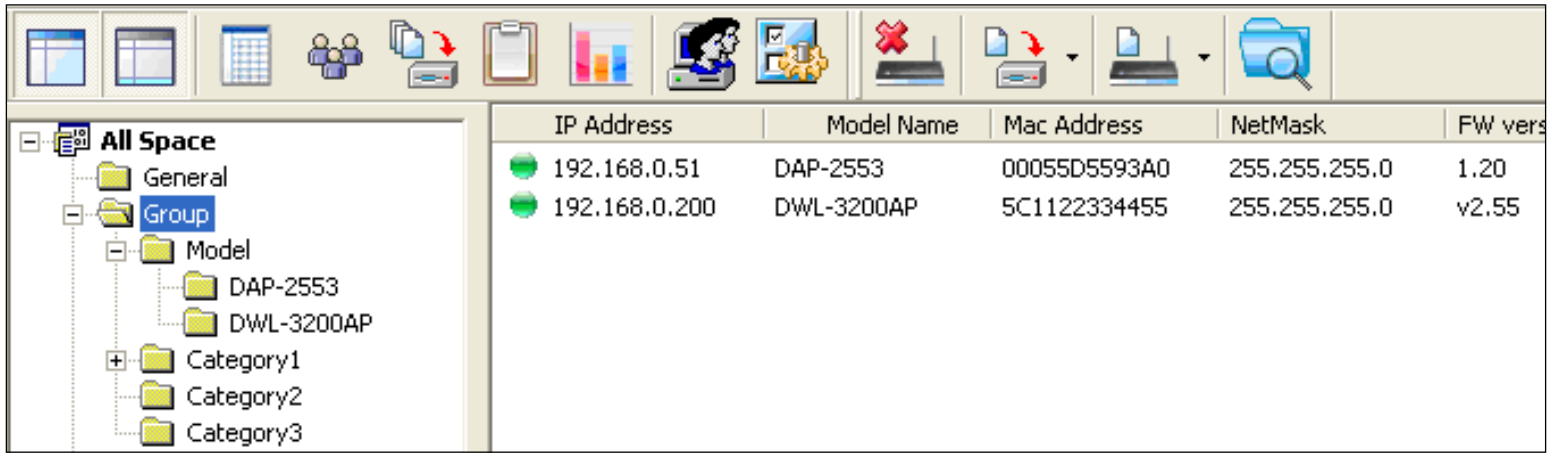


Group View

The Group window, as shown below, displays the APs the AP Manager II has discovered and is currently managing. You can group these APs by model or into categories that can make their distribution easier to visualize.

The AP Manager II can actively monitor and manage several models of D-Link Access Points. The models are installed as the form of plug-in under the installation directory of AP Manager II, it is flexible to add or remove a supported model.

APs that are detected during the discovery process will be listed in the main window of the AP Manager.

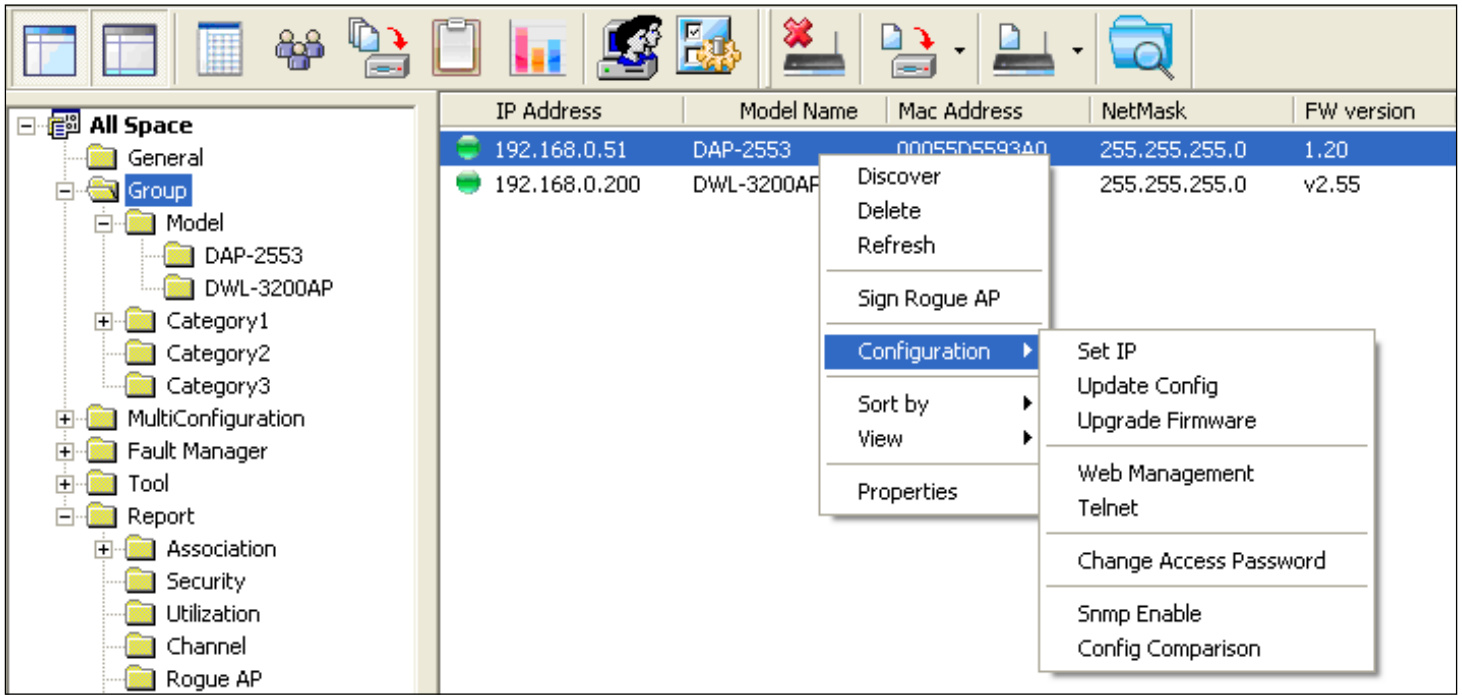


To delete the APs from the group view window, highlight the AP and select the **Delete** item from the right-click menu.

Note: To view a list of the supported access points, please go to the Frequently Asked Questions page on http://support.dlink.com/faq

Configuration

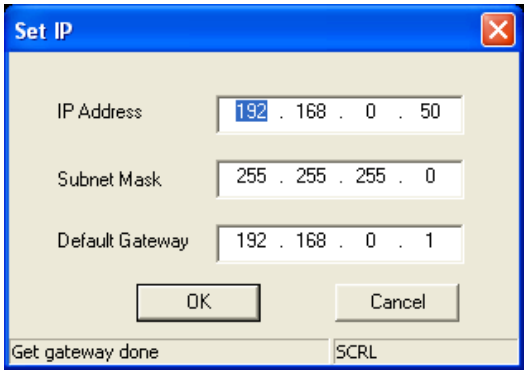
Any Access Point that the AP Manager II has discovered can be configured by right-clicking on that Access Point's icon, displayed in the Group or Category View - as shown below



Under the Configuration menu entry, you can select **Set IP**, **Update Config**, **Upgrade Firmware**, **Web manage**, **Telnet**, **Change Access Password**, Snmp Enable and **Config Comparison**. Each of these options is described in the pages that follow.

Set IP

You can manually set the IP Address of a selected Access Point. Selecting **Set IP** will open the following dialog box



For each Access Point the AP Manager II has discovered, you can use this function to assign a new IP address, Subnet Mask and Default Gateway to the device. Enter the new IP address, subnet mask and default gateway in the appropriate field and click the **OK** button.

IP Address	Model Name	Mac Address	NetMask	FW version	Location	Action	Result
192.168.0.50	DWL-3200AP	001346FDB4F8	255.255.255.0	v2.50	Access Point	Reset	31%

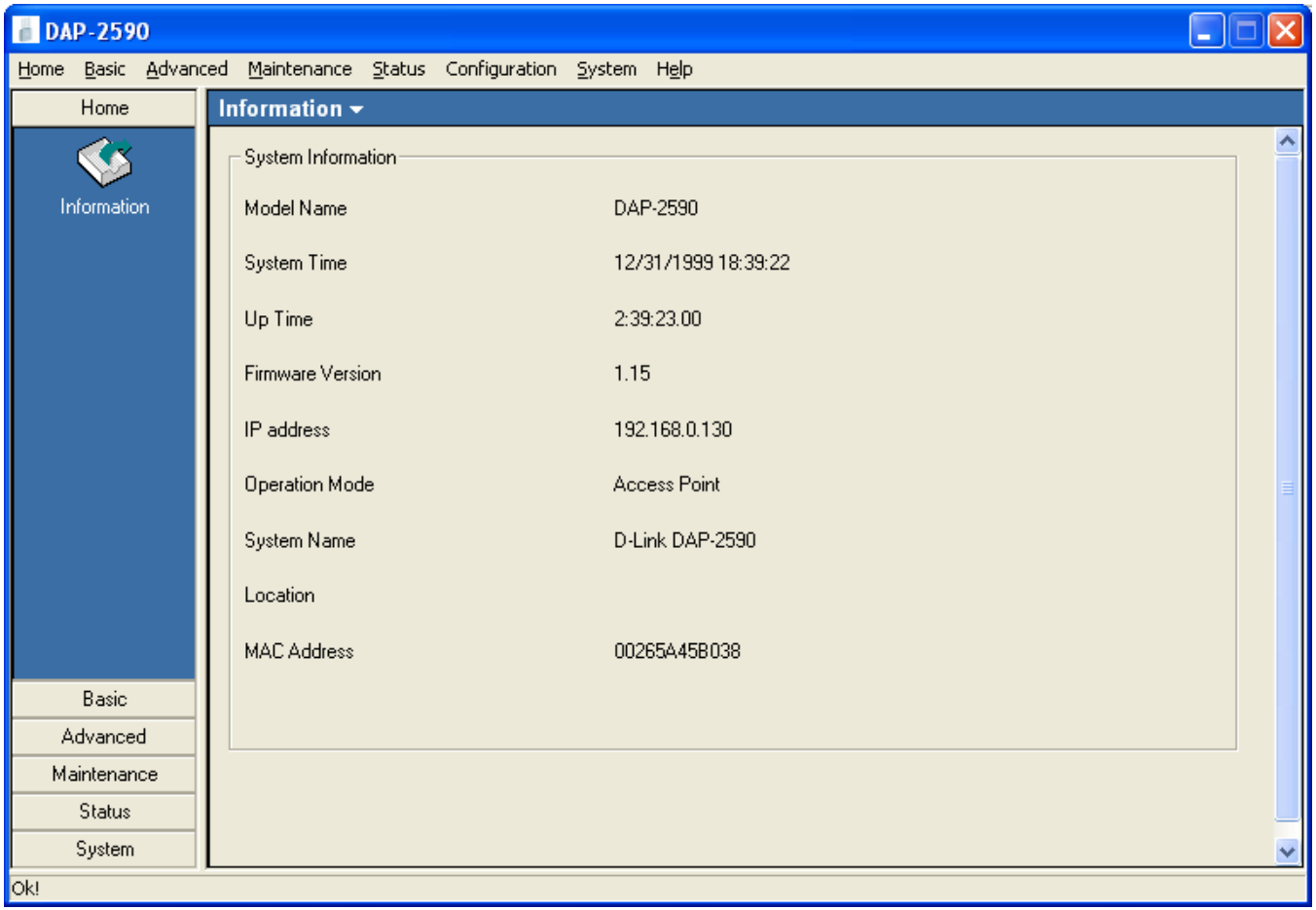
Action column shows the executing operation, for example: Set IP, Reset, and OK (Operation successful), and **Result** column shows the executive progress by percentage. You can set the IPs of multi devices at the same time.

If the operation is failed, please check whether the device and AP manager II are logically connected and the username and password are correct, for more information, refer to **Set Password** section.

When the selected Access Point's IP address has been set, this window will close and the IP address and Net Mask information presented in the Group view table will be changed to reflect the update.

Update Configuration

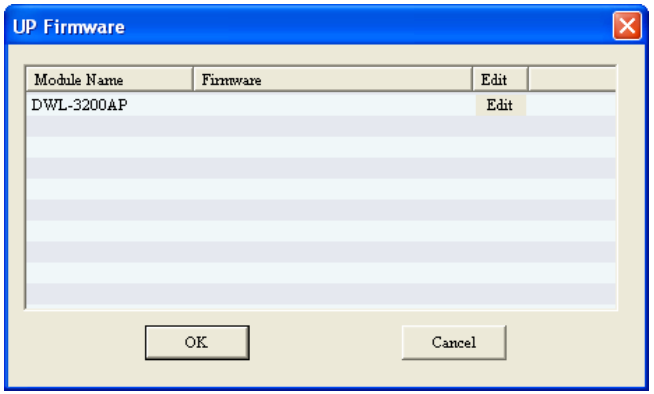
When updating the device configuration, a new window specific to the AP being updated opens, which allows you to configure settings but does not actually apply the settings to the device unless you click the **Apply** button. You can also save and load configuration files from this window. When you load a configuration file, you must click **Apply** if you want the settings to be applied to the selected device(s).



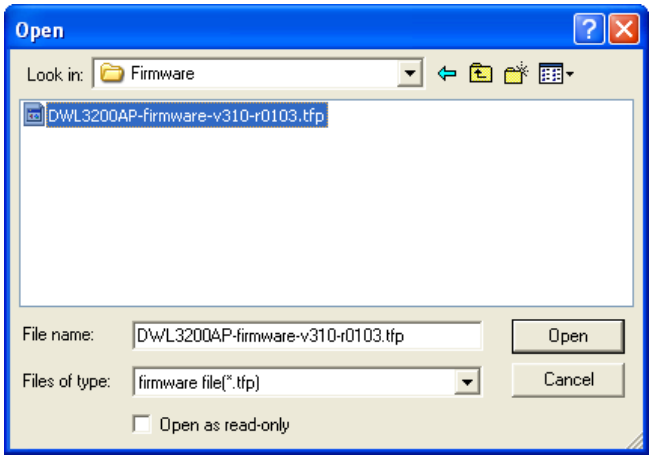
Note: See the section "Configuring 802.11g APs with AP Manager II" and "Configuring 802.11n APs with AP Manager II" for more information on updating the configuration of an AP.

Upgrade Firmware

For each Access Point the AP Manager II has discovered, you can use this function to upload a new firmware file to the device.

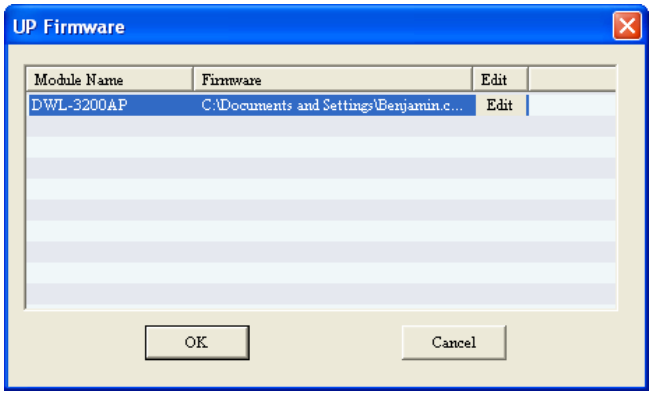


Click **Edit** to select the update firmware file from the appropriate field.



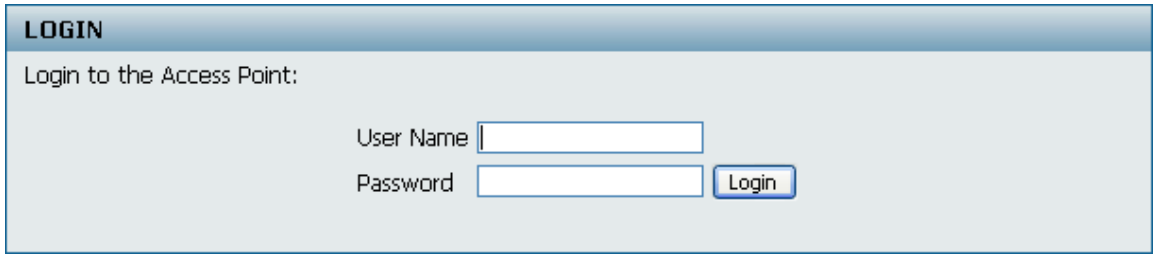
Click the **OK** button to upload the firmware.

When the selected Access Point's firmware has been updated, this window will close and the firmware version information presented in the Group view table will be changed to reflect the update.



Web Management

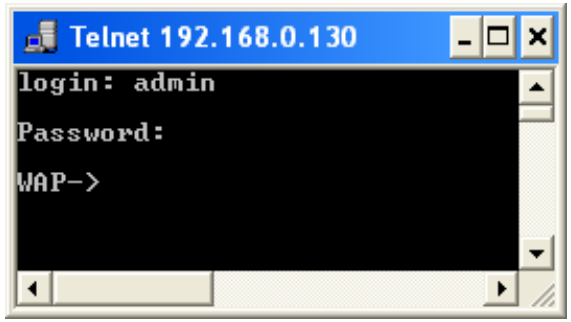
Selecting **Web Manage** from the drop-down menu will open your PC's web browser and automatically direct it to a selected Access Point's IP address. This will allow you access to the Access Point's built-in web-based manager. The first window to open will be the Windows User name and Password dialog box, as shown below.



Enter the appropriate User name and Password into the fields above and click the **OK** button. Your PC's web browser will open and the Access Point's IP address will be entered into the address field. You can the configure the Access Point using its built-in web-based manager as you would normally. There is no difference in using an Access Point's web-based manager initiated by the AP Manager II or any other method.

Telnet

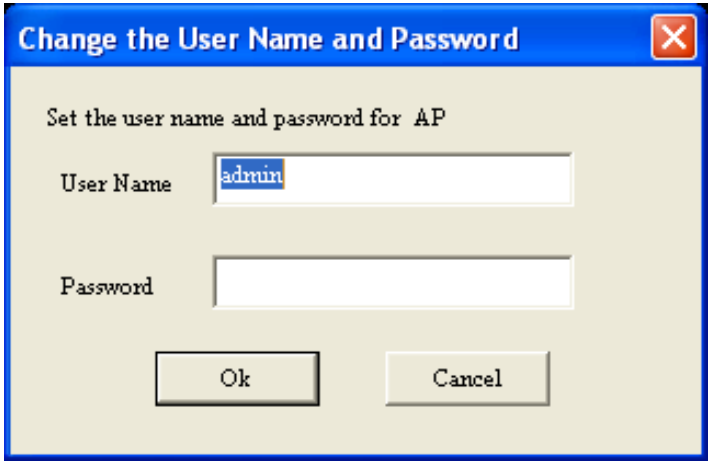
Selecting Telnet from the drop-down menu will open your PC's command line interface and automatically direct it to a selected Access Point's IP address. This will allow you access to the Access Point's built-in Telnet CLI manager. The first window to open will be the Telnet console. Enter the appropriate User name and Password and press the Enter key, as shown below.



Change Access Password

Selecting the Change Access Password option will allow you to set a new login password for the AP being configured. The screen shown below will pop up, enter a new password and click **OK**.

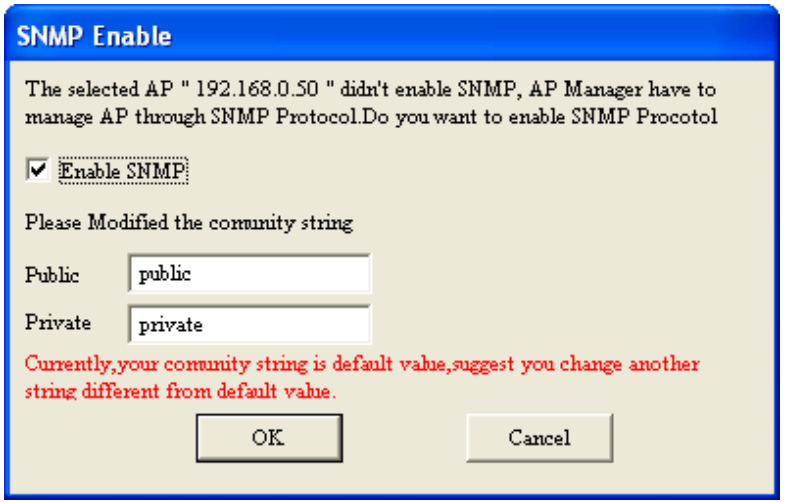
Note: The username and password must accord with the one entered in the web login, or the execution of Set IP function will be failed.



SNMP Enable

Selecting the Snmp Enable option will allow you to enable snmp function for the AP being configured. The screen shown below will pop up, check the Enable SNMP box and click **OK**.

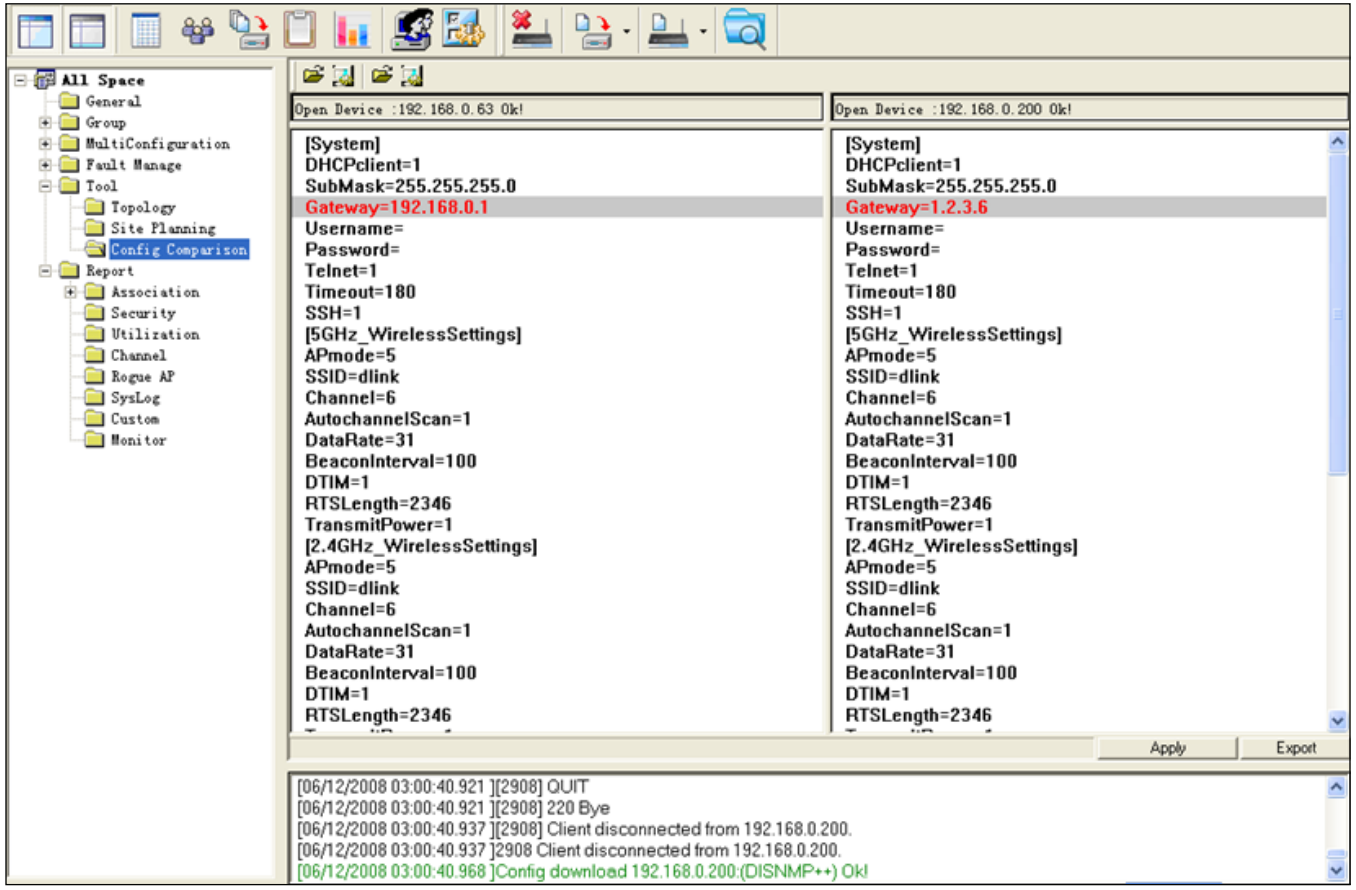
Note: You can modify the public and private strings in Public/Private textbox.



Config Comparison

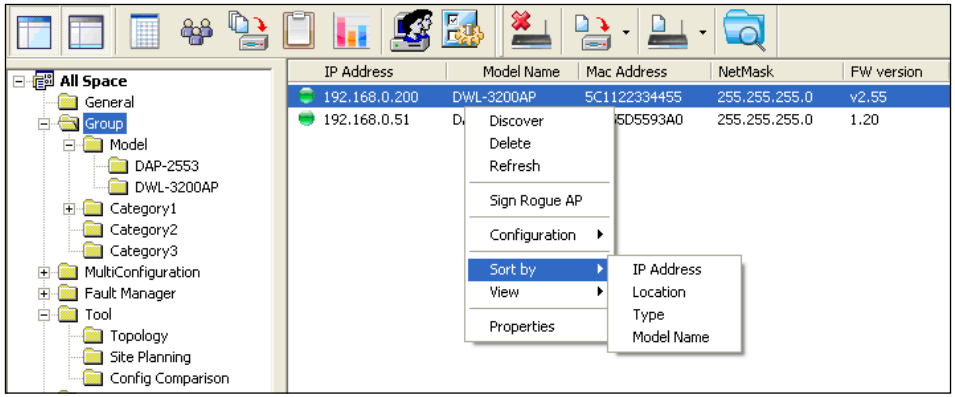
Selecting the Set Password option will allow you to set a new login password for the AP being configured. The screen shown below will pop up, enter a new password and click **OK**.

Note: The username and password must accord with the one entered in the web login, or the execution of Set IP function will be failed.



Sorting

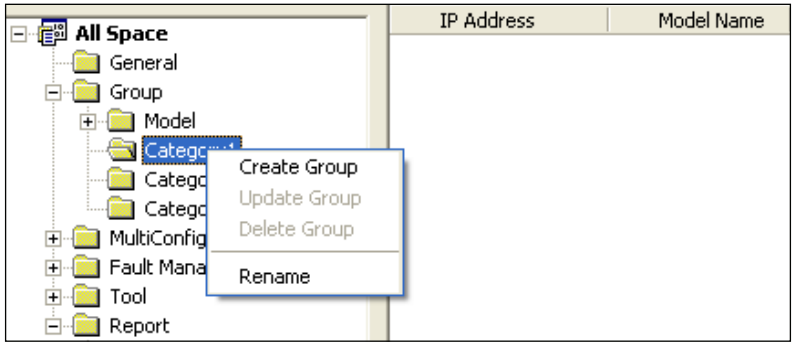
You can sort the order the Access Points that have been detected by the AP Manager II by IP address, by Location, or by Status - as necessary - by right-clicking anywhere on the Group view window and selecting Sorting followed by the sorting criteria.



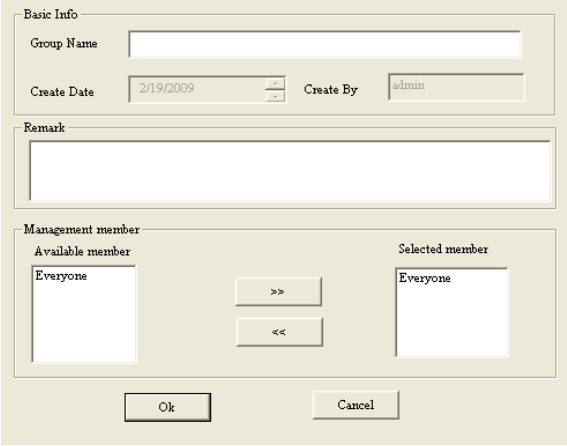
Explanation of sorting types:

- **IP Address:** Sorting by IP Address column.
- **Location:** Sorting by Location column.
- **Type:** Sorting by specified AP types, the types are: **Unmanaged**, **Managed**, and **Rogue AP**.
- **Model Name:** Sorting by Model Name of the AP.

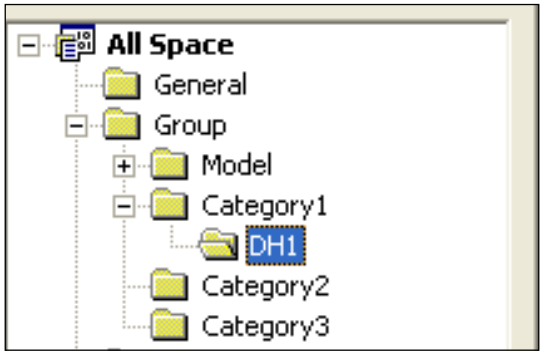
You can classify the APs to the different groups, right-click one of the three sub items category 1, category 2, or category 3 of Group, and select **Create Group** from the drop-down menu to create a new group, as shown below.



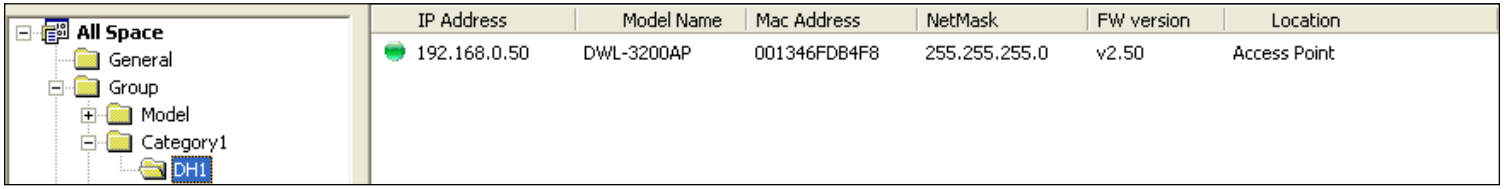
In the group creation window, enter a description in the Group Name and choose the members in the Manager members, then click **OK** button to create a new group.



You can add APs to the sub-group by dragging the APs from the main group view list to the group you created under the category sub item, as shown below.

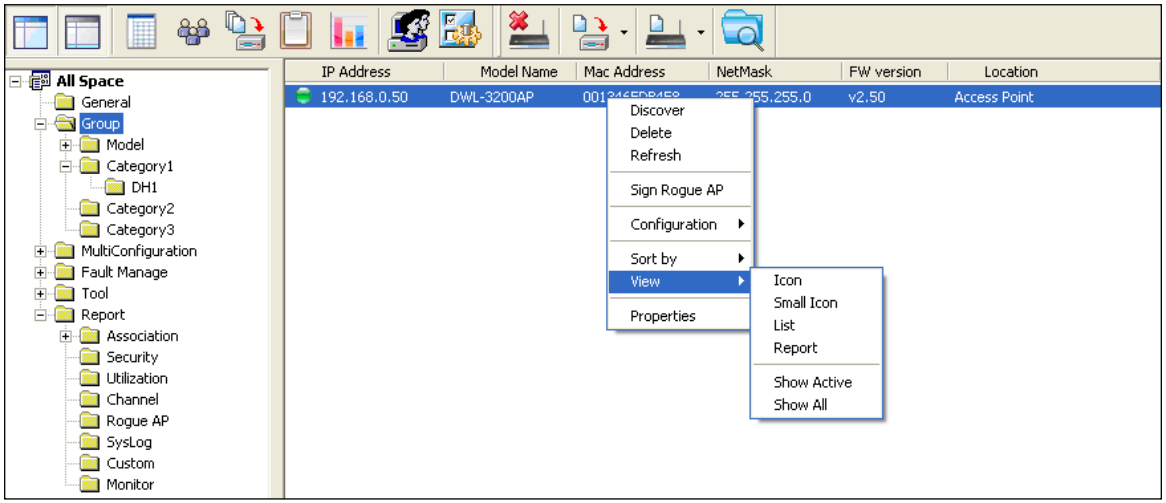


The type of the AP will be changed to Managed and the icon will be changed to .



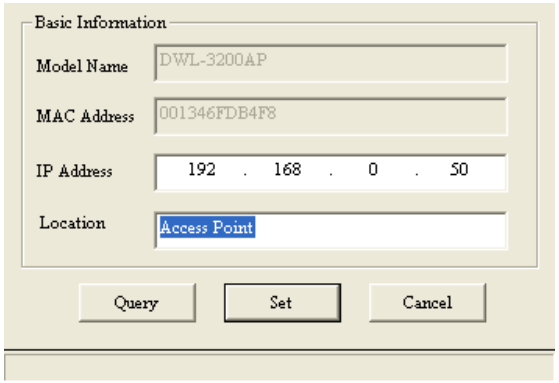
View

You can also change the way the list of Access Points detected by the AP Manager II are displayed by right-clicking anywhere in the Group View window and selecting View By followed by Icon, Small Icon, List, Report, Show Active, or Show All - as shown below.



Property

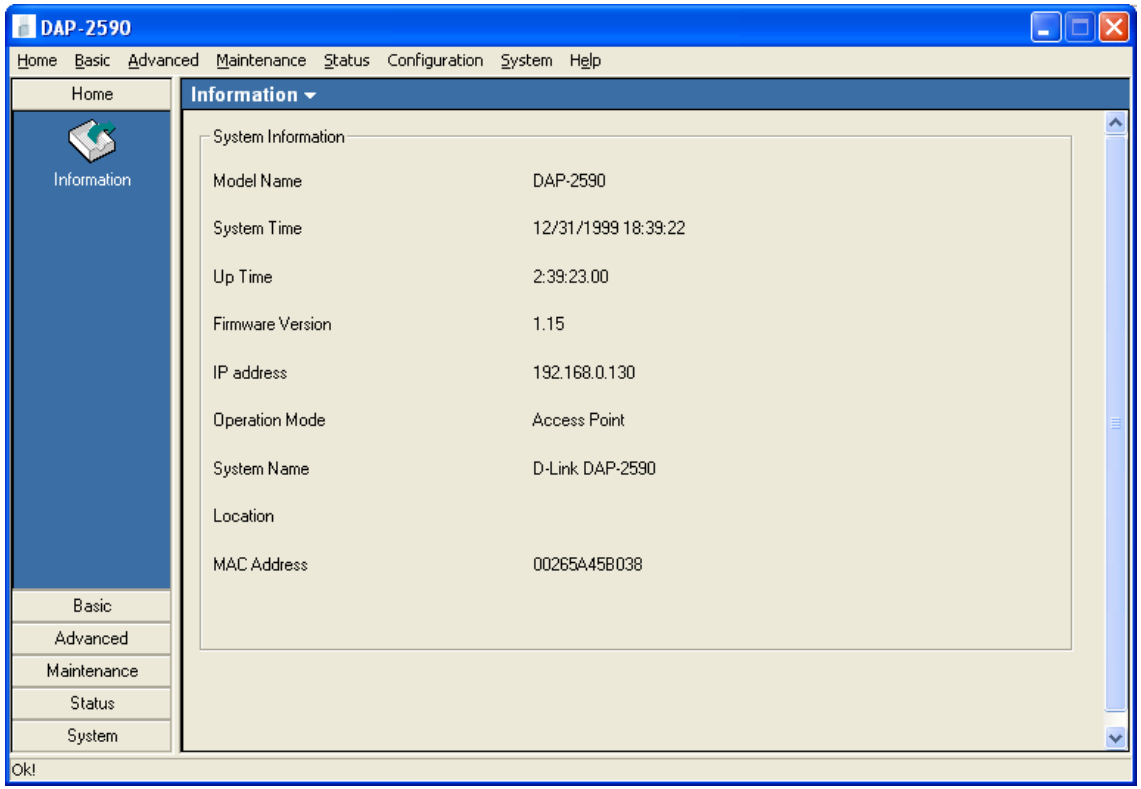
You can also view the properties of Access Points detected by the AP Manager II by right-clicking the AP in the Group View window and selecting **Property** - as shown below.



You can enter a description string in the Location textbox to describe the AP and then click the **Set** button to apply the change.

Configuring APs with AP Manager II

When updating the device configuration, a new window specific to the AP being updated opens, which allows you to configure settings but does not actually apply the settings to the device unless you click the **Apply** button. You can also save and load configuration files from this window. When you load a configuration file, you must click **Apply** if you want the settings to be applied to the selected device(s).

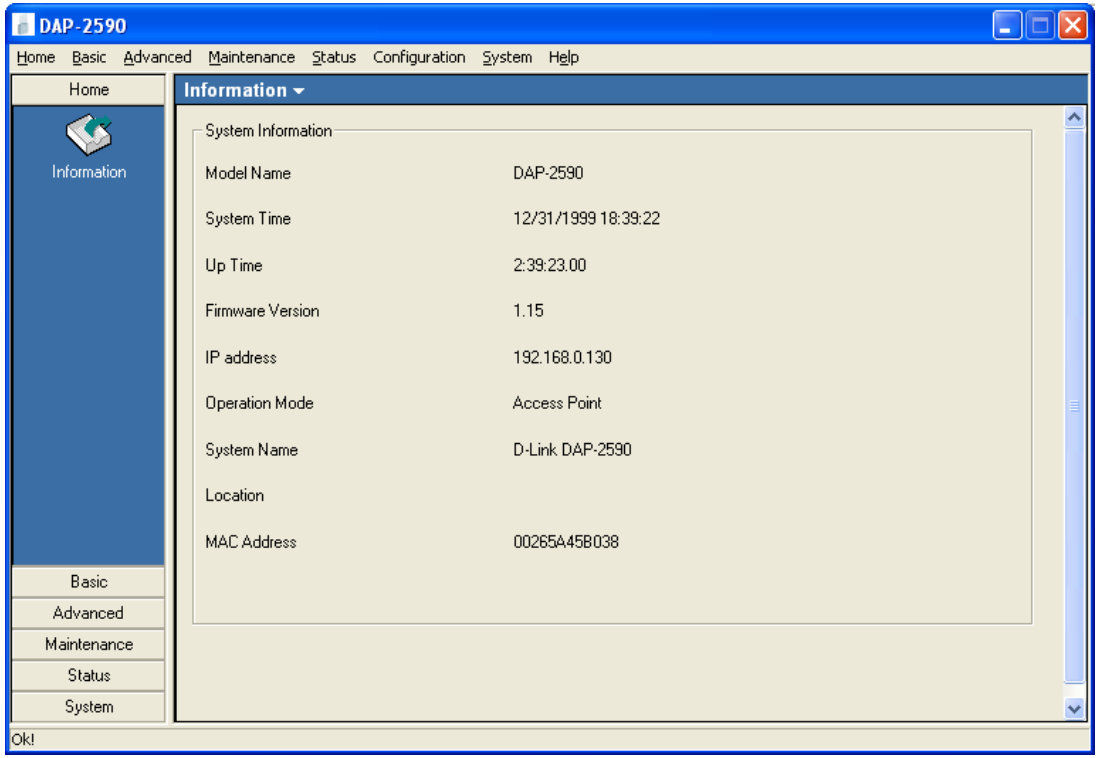


Navigate the AP configuration using the menu on the left side of the window. This menu contains the following sections, **Home**, **Basic**, **Advanced**, **Tools**, **Status**, and **System**. These sections and their menus will be discussed in detail in the following pages.

Home
Information

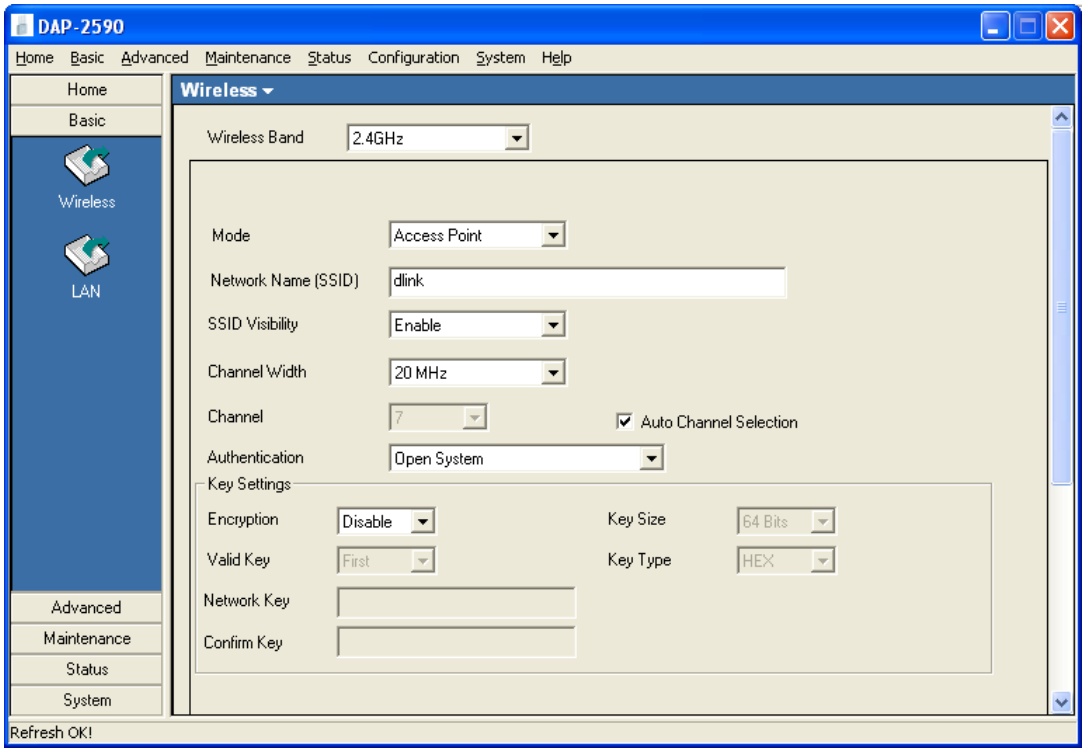
The **Home > Information** page contains basic configuration information about the access point being configured. This information includes the **Model Name**, **System Time**, **Up Time**, **Firmware Version** and **IP address**.

There will be minor differences when using AP Manager II with a single band AP and a dual band AP. This manual refernces both 802.11g and 802.11n configuration settings.



Basic

Wireless



Wireless Band: Select the wireless band to configure: **802.11g** for G access points and **5GHz or 2.4GHz** for **N** access points**.**

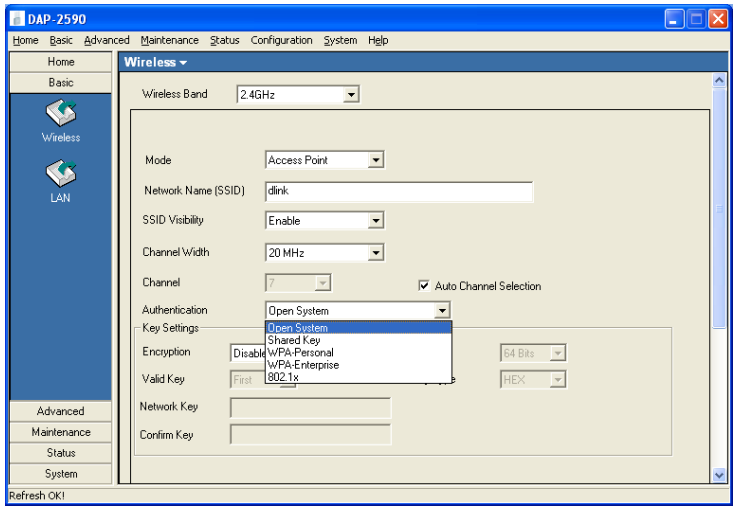
AP Mode: There are 3 AP modes: **Access Point**, **WDS with AP**, and **WDS**. IEEE 802.11n access points will also include **Wireless Client** mode.

SSID: The Service Set (network) Identifier of your wireless network.

SSID Visibility: Enabled by default, selecting **Disable** allows you to **disable** the broadcasting of the SSID to network clients.

Channel: Allows you to select a channel or set ap to auto scan the channel. The channel of an 802.11g network may not be set manually in certain regions (e.g. Europe and USA) in order to comply with DFS (Dynamic Frequency Selection).

Wireless Authentication



Open System: The key is communicated across the network.

Shared Key: Limited to communication with devices that share the same WEP settings.

Open System/Shared Key: The key is communicated and identical WEP settings are required.

Authentication: Select **Open System/Shared Key** to allow either form of data encryption.

Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.

Select **WPA-Personal** to secure your network using a password and dynamic key changes. (No RADIUS server required.)

Select **WPA2-Enterprise** to secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES).

Select **WPA2-Personal** to secure your network using a password and dynamic key changes. No RADIUS server required and encryption of data is upgraded with the Advanced Encryption Standard (AES).

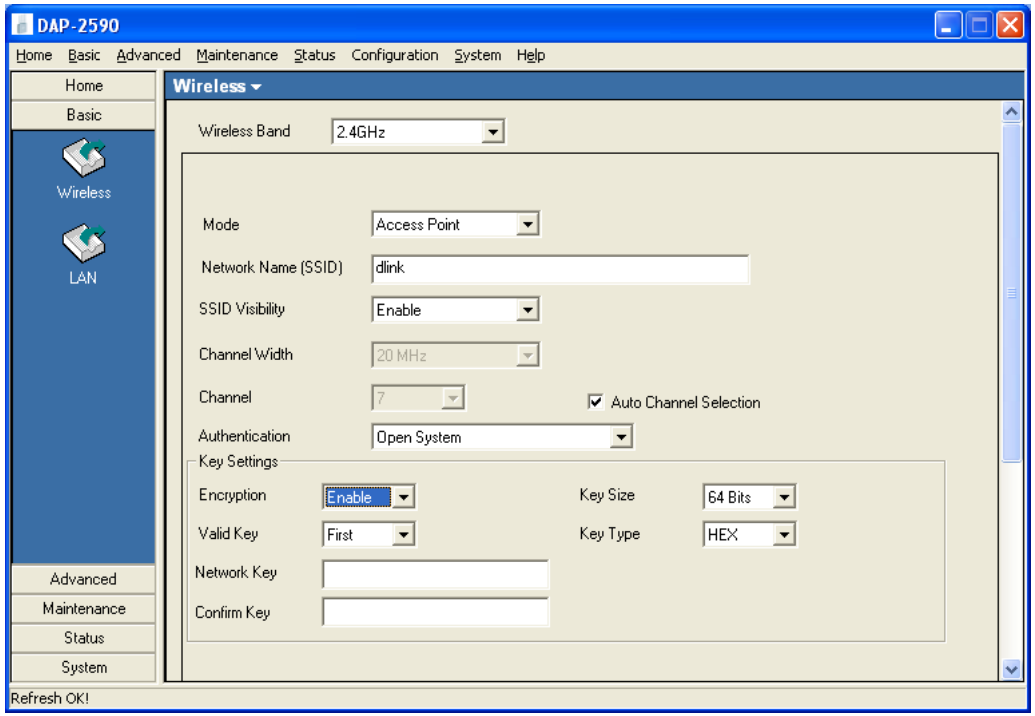
Select **WPA-Auto-Enterprise** to allow the client to either use **WPA-Enterprise** or **WPA2-Enterprise**.

Select **WPA-Auto-Personal** to allow the client to either use **WPA-Personal** or **WPA2-Personal**.

Security

AP Mode	Authentication Available
Access Point	Open System Shared Key Open System/Shared Key WPA-Enterprise WPA-Personal WPA2-Enterprise WPA2-Personal WPA-Auto-Enterprise WPA-Auto-Personal 802.1x
WDS with AP	Open System Shared Key Open System/Shared Key WPA-Personal WPA2-Personal WPA-Auto-Personal
WDS	Open System Shared Key Open System/Shared Key WPA-Personal WPA2-Personal WPA-Auto-Personal
Wireless Client	Open System WPA-Personal

WEP Encryption (AP Mode)



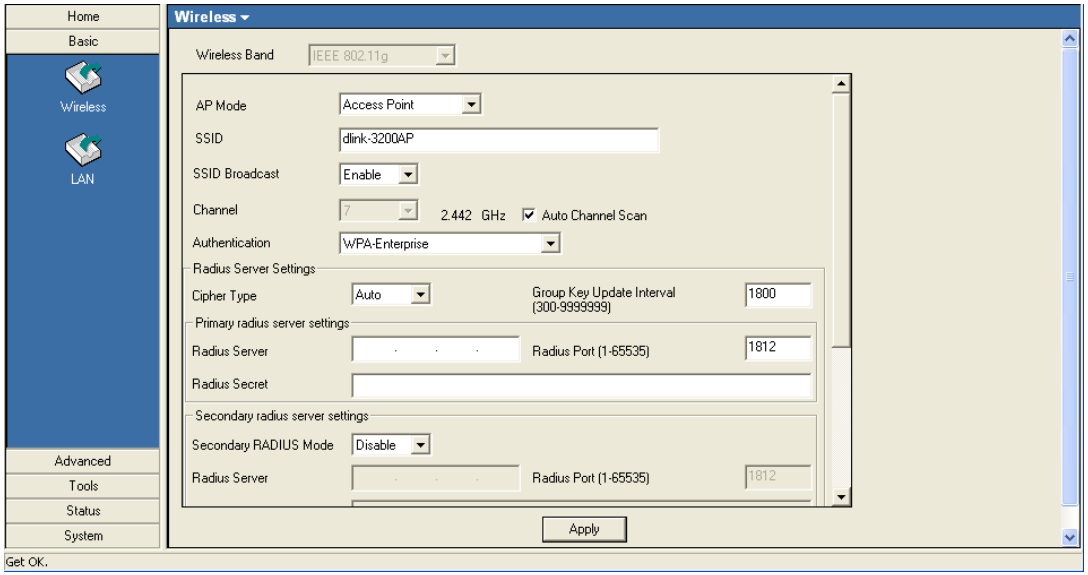
Authentication: Select from the drop-down menu the type of authentication to be used on the selected device(s). In this example you may select **Open System**, **Shared Key**, or **Open System/Shared Key**.

Encryption: **Enable** or **Disable** encryption on the selected device(s). This option will only be available when security is set to **Open System** or **Open System/Shared Key**.

Valid Key: Select which defined key is active on the selected device(s). This option will only be available when security is set to **Open System, Shared Key,** or **Open System/Shared Key**.

Key Values: Select the **Key Size** (**64-bit, 128-bit,** or **152-bit**) and **Key Type** (**HEX** or **ASCII**) and then enter a string to use as the key. The key length is automatically adjusted based on the settings you choose. This option will only be available when security is set to **Open System, Shared key,** or **Open System/Shared Key**.

WPA/WPA2 Enterprise (AP Mode)



Personal/Enterprise: Select **Auto**, **WPA** or **WPA2**.

Cipher Type: Select **Auto**, **TKIP**, or **AES** from the drop-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. **1800** is the recommended setting. A lower interval may reduce transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the port used on the RADIUS server.

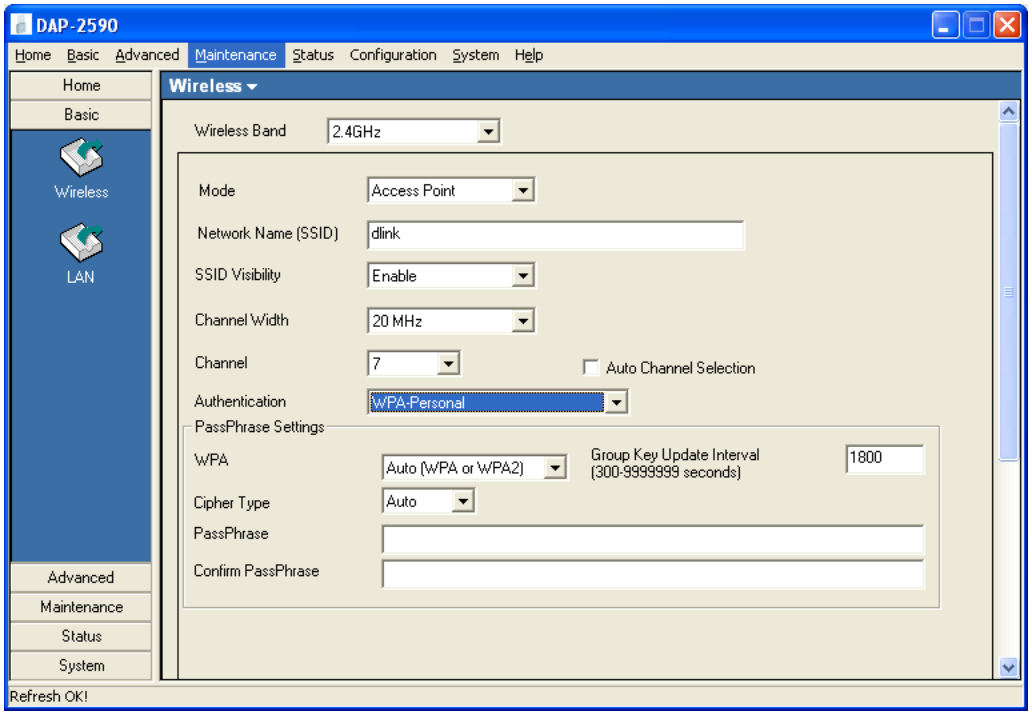
RADIUS Secret: Enter the RADIUS secret.

Accounting Mode: Check to enable the accounting funtion.

Accounting Port: Enter the port used on the Accounting server.

Accounting Server: Enter the IP address of the Accounting server.

WPA/WPA2 Personal (AP Mode)



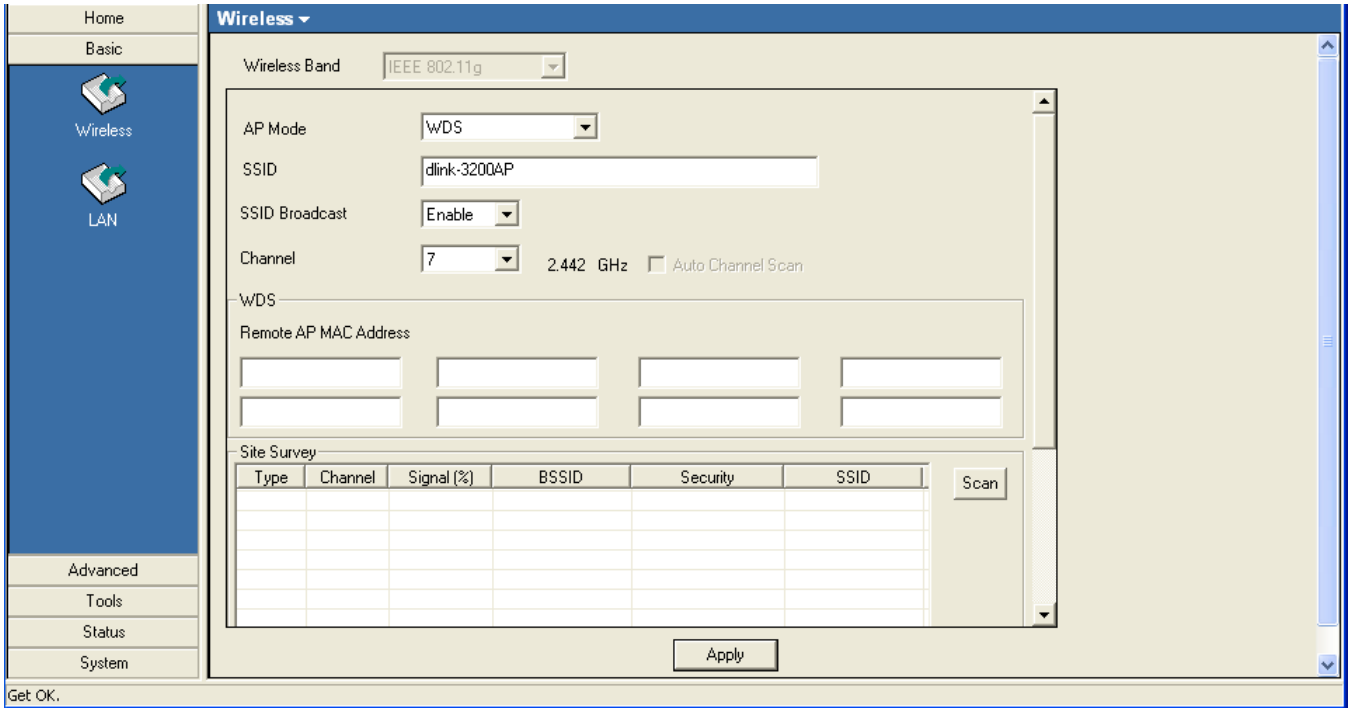
Personal/Enterprise: Select **Auto**, **WPA**, or **WPA2**.

Cipher Type: Select **Auto**, **TKIP**, or **AES** from the drop-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. **1800** is the recommended setting. A lower interval may reduce transfer rates.

Passphrase: Enter a **PassPhrase** between 8-63 characters in length.

WDS Mode

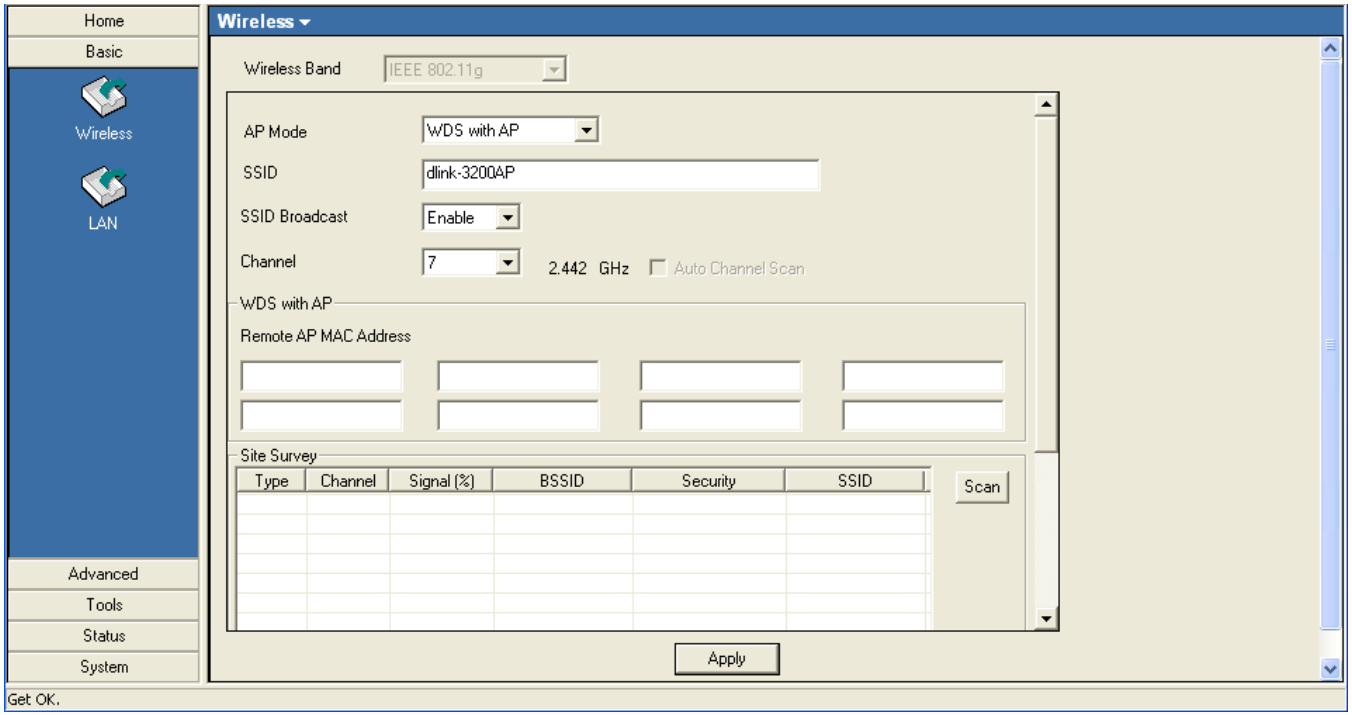


WDS: A Wireless Distribution System that interconnects so called Basic Service Sets (BSS). It bridges two or more wired networks together over wireless. The AP wirelessly connects multiple networks without functioning as a wireless AP.

Remote AP MAC Address: Enter the MAC Addresses of the other APs you want to connect to using WDS mode.

Site Survey: Click the **Scan** button to search for local APs.

WDS with AP Mode

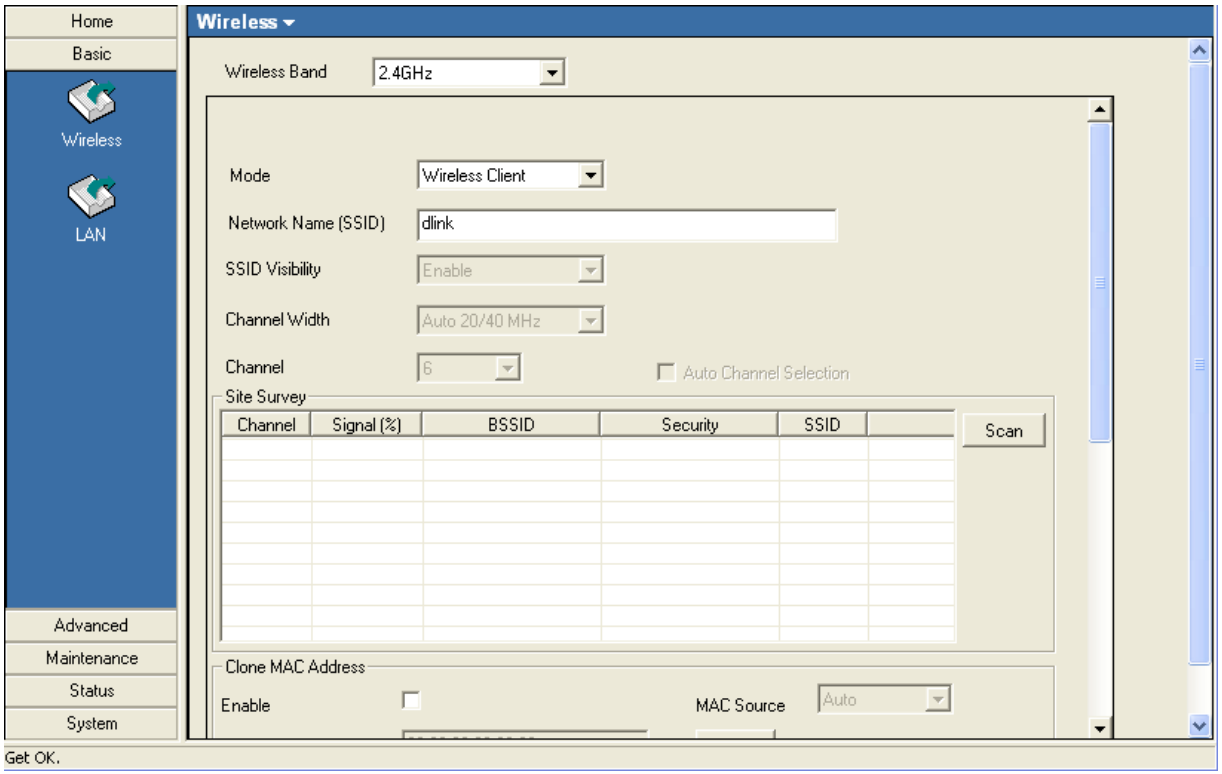


WDS with AP: Wireless Distribution System with Access Points. APs in a network are wirelessly wired together and connected via a Distribution System. The AP wirelessly connects multiple networks, while still functioning as a wireless AP.

Remote AP MAC Address: Enter the MAC Addresses of the other APs you want to connect to using WDS mode.

Site Survey: Click the **Scan** button to search for local APs.

Wireless Client (802.11n Only)



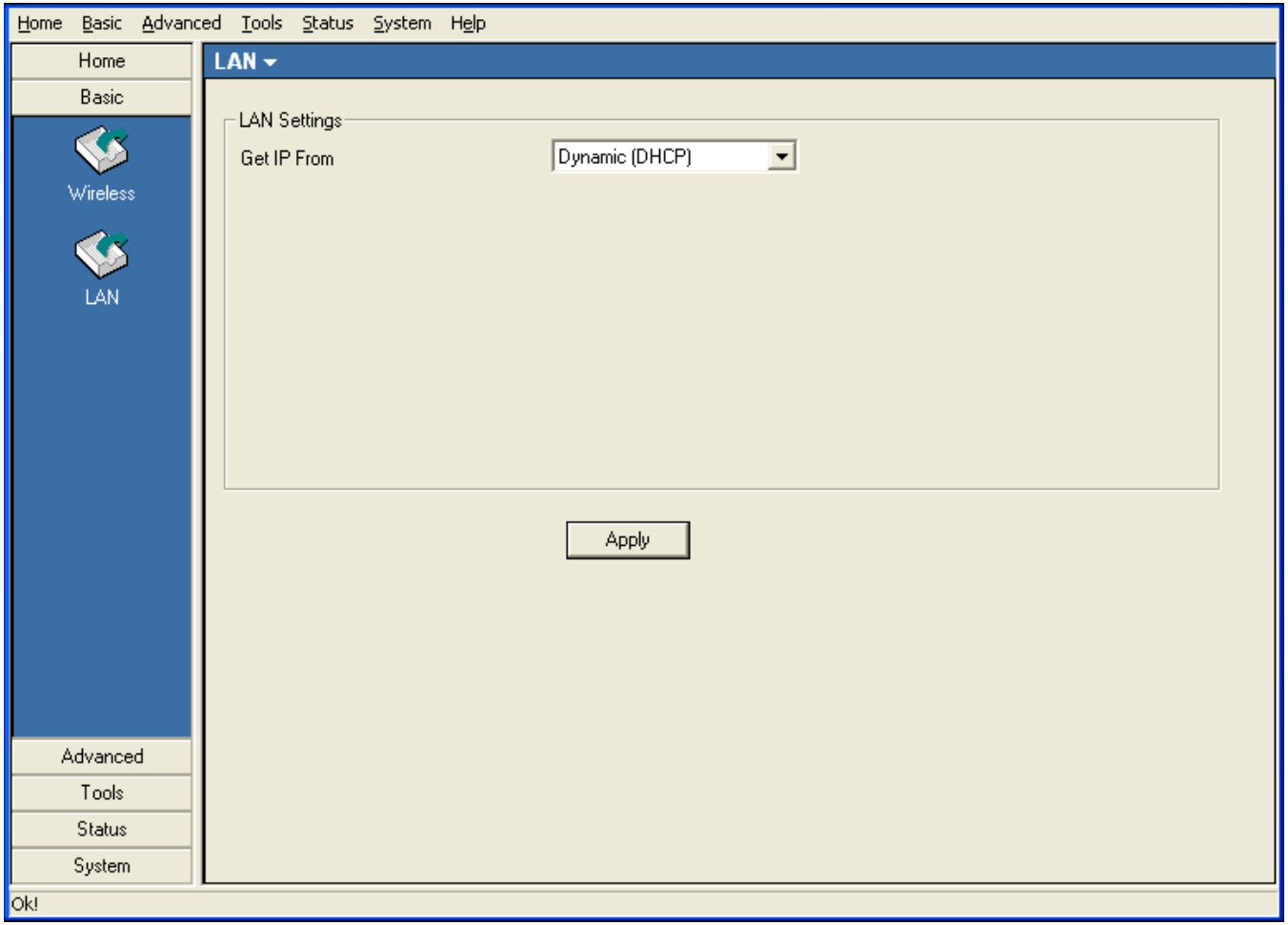
Wireless Client: The device acts as a wireless client station to connect APs. Provide a wireless connection for the non-wireless device.

Site Survey: Click the **Scan** button to search for local APs.

Clone MAC Address: Assign a mac address to the AP which is set to AP Client mode, for the communication with another AP as a network card. You can entry any address or choose an address in the scan list if select "manually". "Auto" means to assign the first mac address in that AP detected.

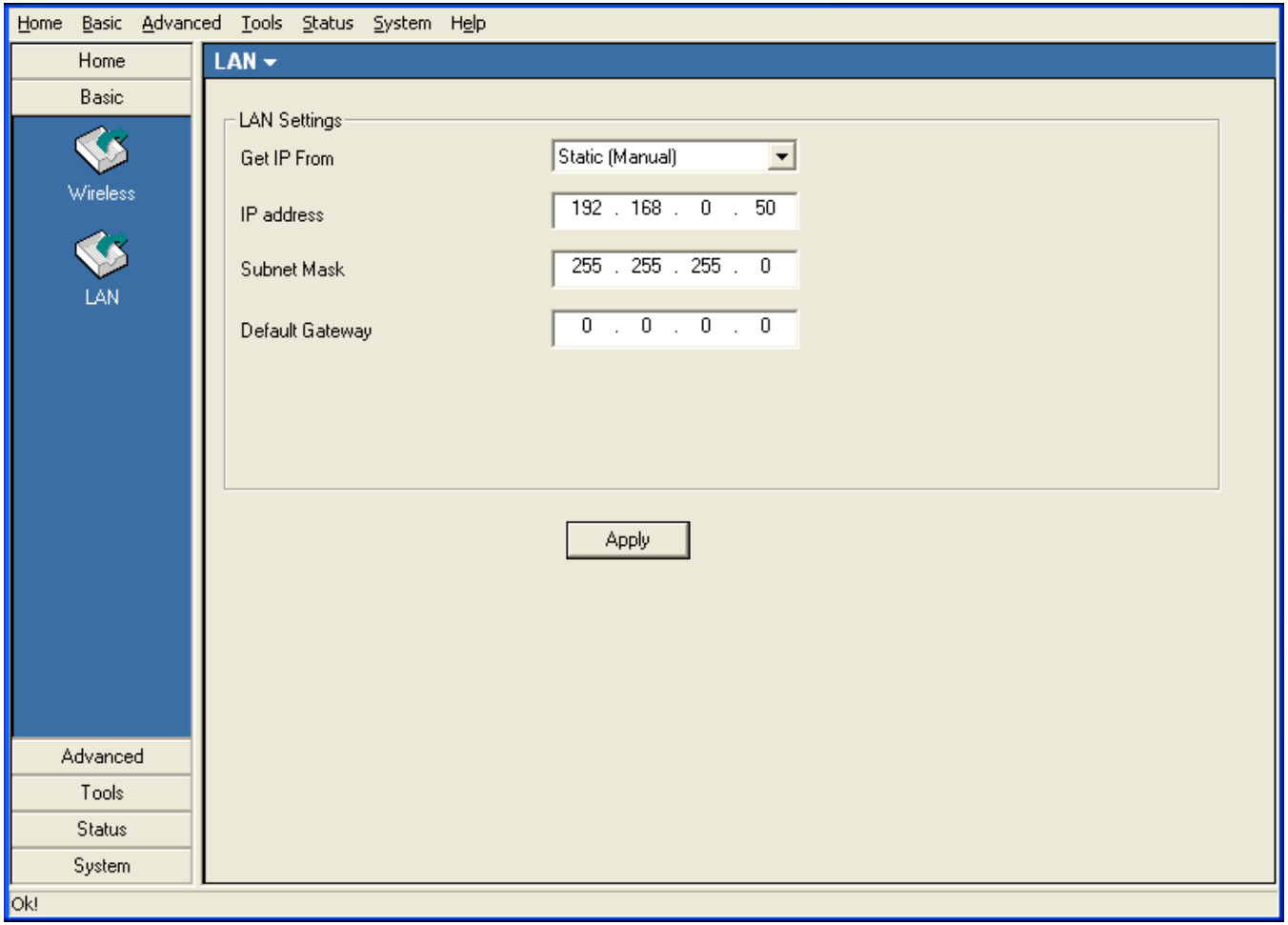
LAN

Dynamic (DHCP)



Get IP From: When set to Dynamic (DHCP) the AP(s) will function as a DHCP client(s). This allows them to receive IP configuration information from a DHCP server.

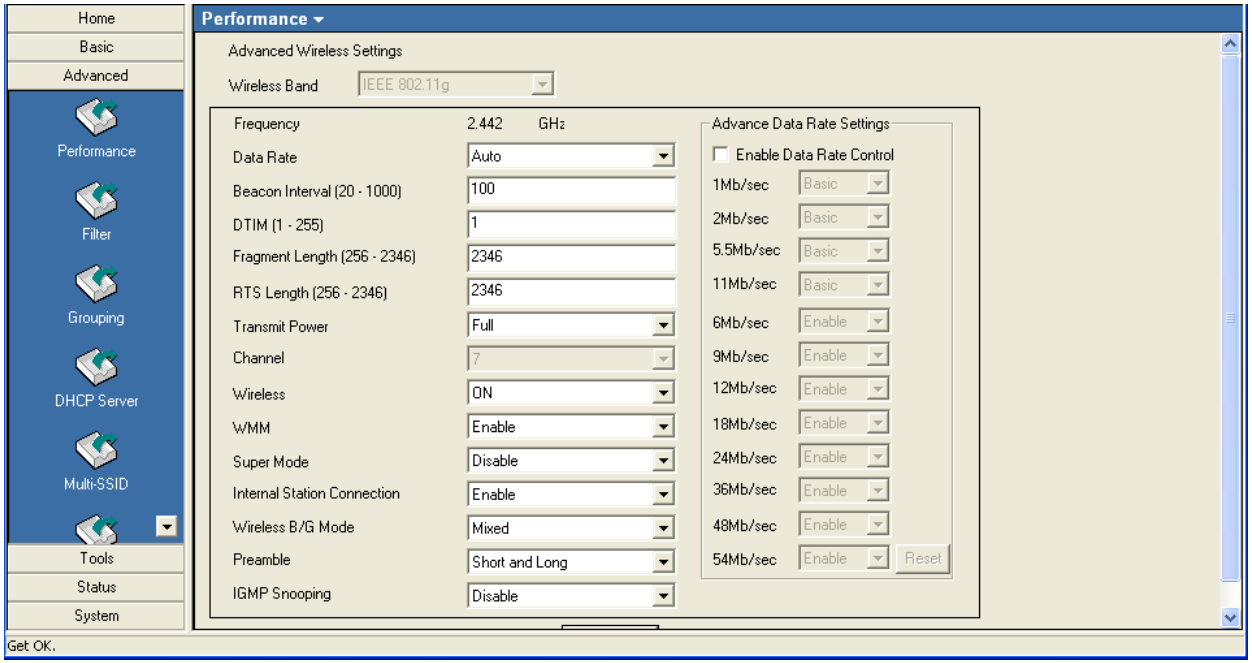
Static (Manual)



Get IP From: When set to Static (Manual) the access point(s) must have a static IP address assigned to them.

Advanced

Performance (802.11g)



Frequency: Displays the current frequency of the wireless band.

Data Rate: Set to Auto by default, use the drop-down menu to select the maximum wireless signal rate for the selected device(s).

Beacon Interval (20~1000): Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of **100** is recommended.

DTIM (1~255): DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages.

Fragment Length (256~2346): This sets the fragmentation threshold (specified in bytes). Packets exceeding the value set here will be fragmented. The default is **2346**.

RTS Length (256~2346): The RTS value should not be changed unless you encounter inconsistent data flow. The default value is **2346**.

Transmit Power: Choose **full**, **half (-3dB)**, **quarter (-6dB)**, **eighth (-9dB)**, **minimum power**. This tool can be helpful for security purposes if you wish to limit the transmission range.

Channel: **Display the** channel available for wireless networking .

Wireless: Select **ON** or **OFF**.

WMM: (Wi-Fi Multimedia) Improves the user experience for audio, video, and voice applications over a Wi-Fi network. WMM is based on a subset of the IEEE 802.11e WLAN QoS standard.

Super Mode: Select to enable a wireless signal rate of up to 108Mbps. Turbo is a group of performance enhancement features that increase end user application throughput in a 802.11g network. Turbo is backwards compatible with standard 802.11g devices. For ideal performance, all wireless devices on the network should be Turbo capable.

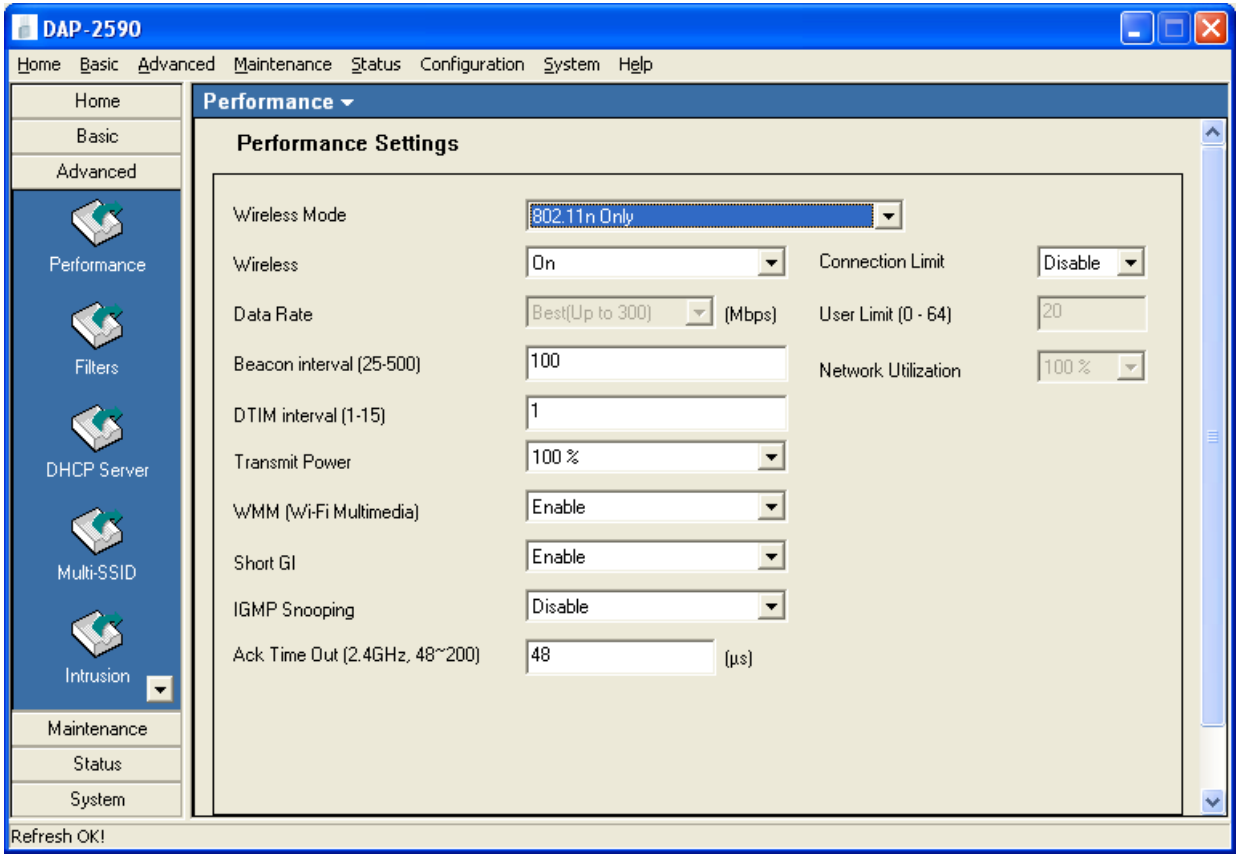
Internal Station Connection: Enabling this allows wireless clients to communicate with each other. When this option is disabled, wireless stations are not allowed to exchange data through the access point.

Wireless B/G Mode: Select **Mixed**, **11g Only**, or **11b Only**.

Preamble: Select **Short and Long** (recommended) or **Long-Only**.

IGMP Snooping: Select **Enable** to allow IGMP Snooping.

Performance (802.11n)



Wireless Mode: Select the wireless mode from the drop-down menu.

Wireless: Select **On** or **Off**.

Data Rate: Set to **Auto** by default, use the drop-down menu to select the maximum wireless signal rate for the selected device(s).

Beacon Interval (25~500): Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of **100** is recommended.

DTIM (1~15): DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages.

Transmit Power: Choose the percentage of transmit power. This tool can be helpful for security purposes if you wish to limit the transmission range.

WMM: (Wi-Fi Multimedia) Improves the user experience for audio, video, and voice applications over a Wi-Fi network. WMM is based on a subset of the IEEE 802.11e WLAN QoS standard.

Short GI: Select **Enable** to allow the Short GI.

IGMP Snooping: Select **Enable** to allow IGMP Snooping.

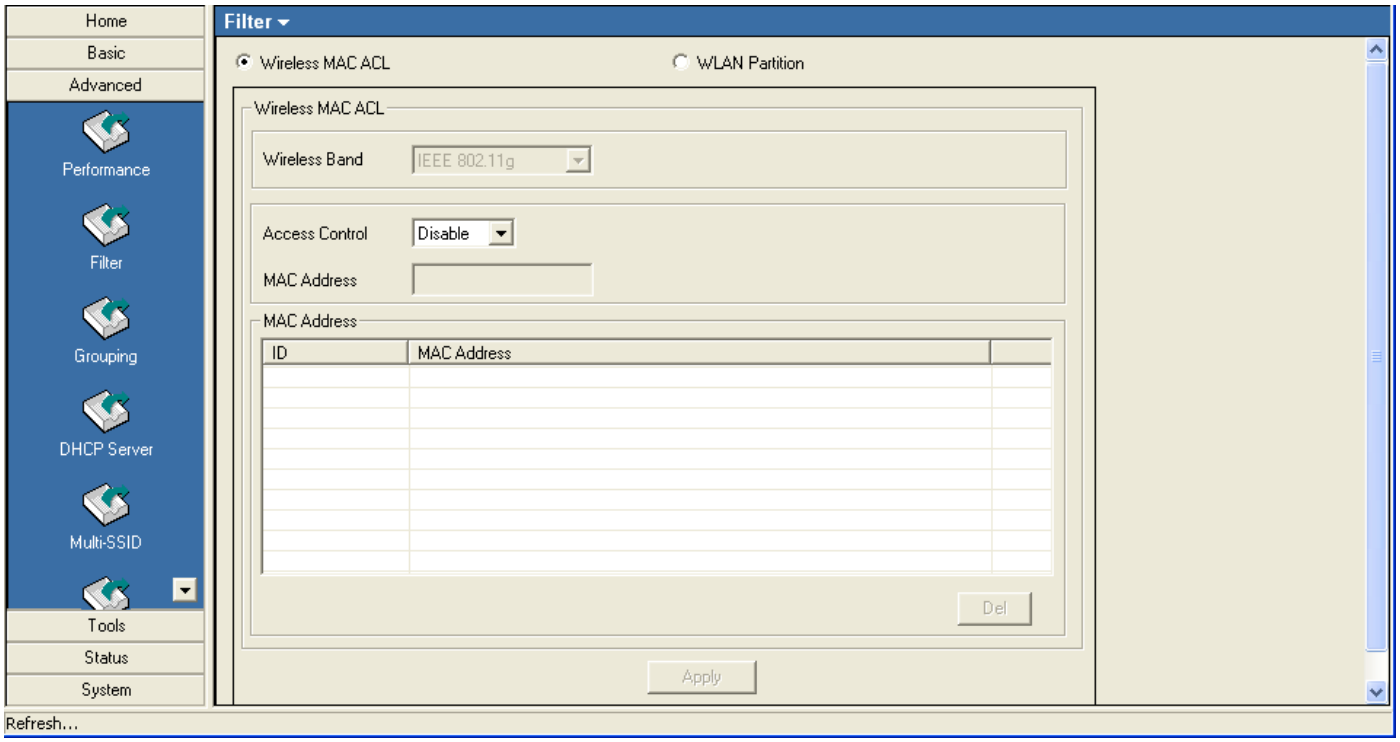
ACK Time Out: Set the maximum time of ACK session.

ConnectionLimit: Select **Enable** to limit the connections by the user limit or network utilization.

User Limit: Set the maximum users that can connect to AP. Only available when Connection Limit is enabled.

Multicast Rate for 2.4G band: Use the drop-down menu to select the maximum multicast rate for the selected device(s).

Filter (Wireless MAC ACL)



Wireless Band: Display the wireless network to apply the access control filter to.

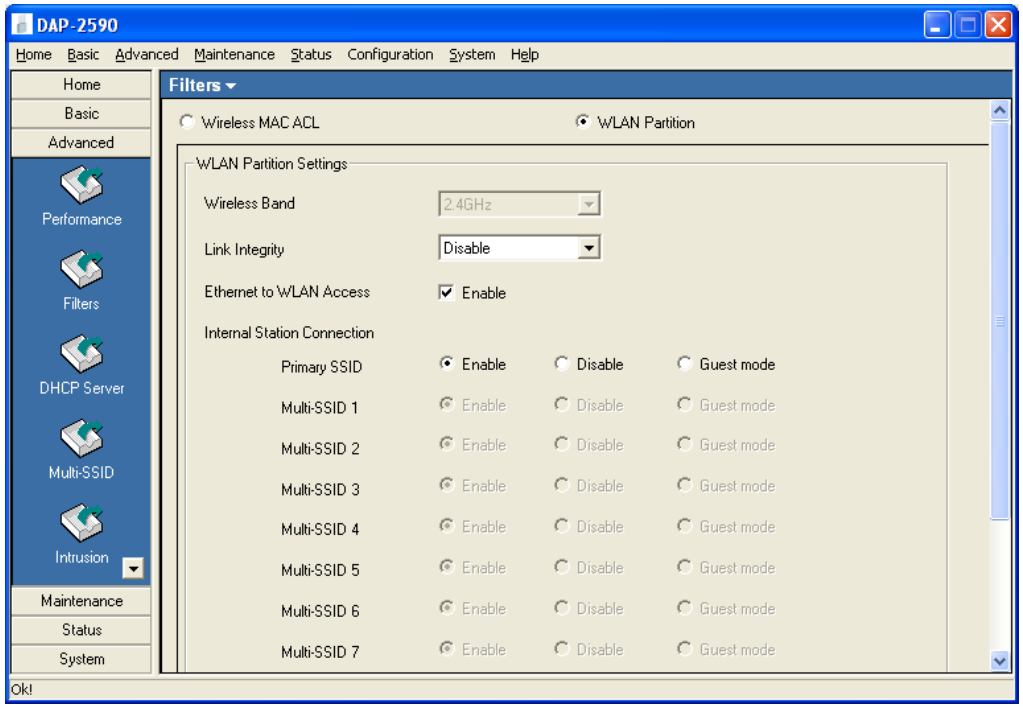
Access Control: When disabled access control is not filtered based on the MAC address. If **Accept** or **Reject** is selected, then a box appears for entering MAC addresses. When **Accept** is selected, only devices with a MAC address in the list are granted access. When **Reject** is selected, devices in the list of MAC addresses are not granted access.

Access Control List: **Add** or **Delete** MAC addresses in the Access Control List.

Current Client Information: The table lists the current associated clients. Click the **Add** button to add the client into access control list.

Upload ACL File: Use a ACL file to apply the access control filter to. Click the **Browse** buttons to locate the ACL file on your local computer. Use the **Upload** button to upload the files to the AP. Click Download button to save the ACL control settings to a configuration file.

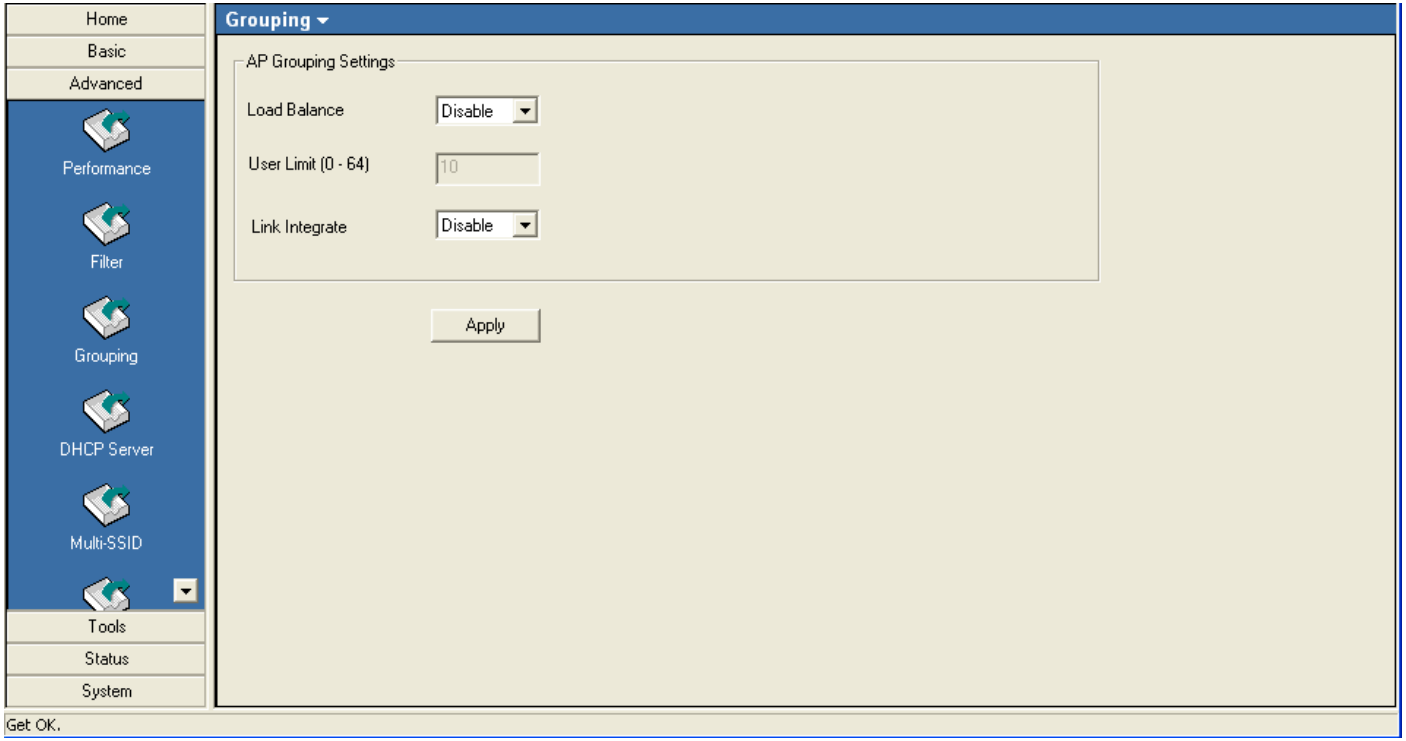
Filter (WLAN Partition)



Ethernet to WLAN Access: Enabling this option allows Ethernet devices to communicate with wireless clients. When this option is disabled, all data from Ethernet to wireless clients is blocked. Wireless devices can still send data to the Ethernet devices when this is disabled.

Internal Station Connection: Check the "Enable" box to allow communication between devices on the network.

Grouping (AP Grouping Settings)

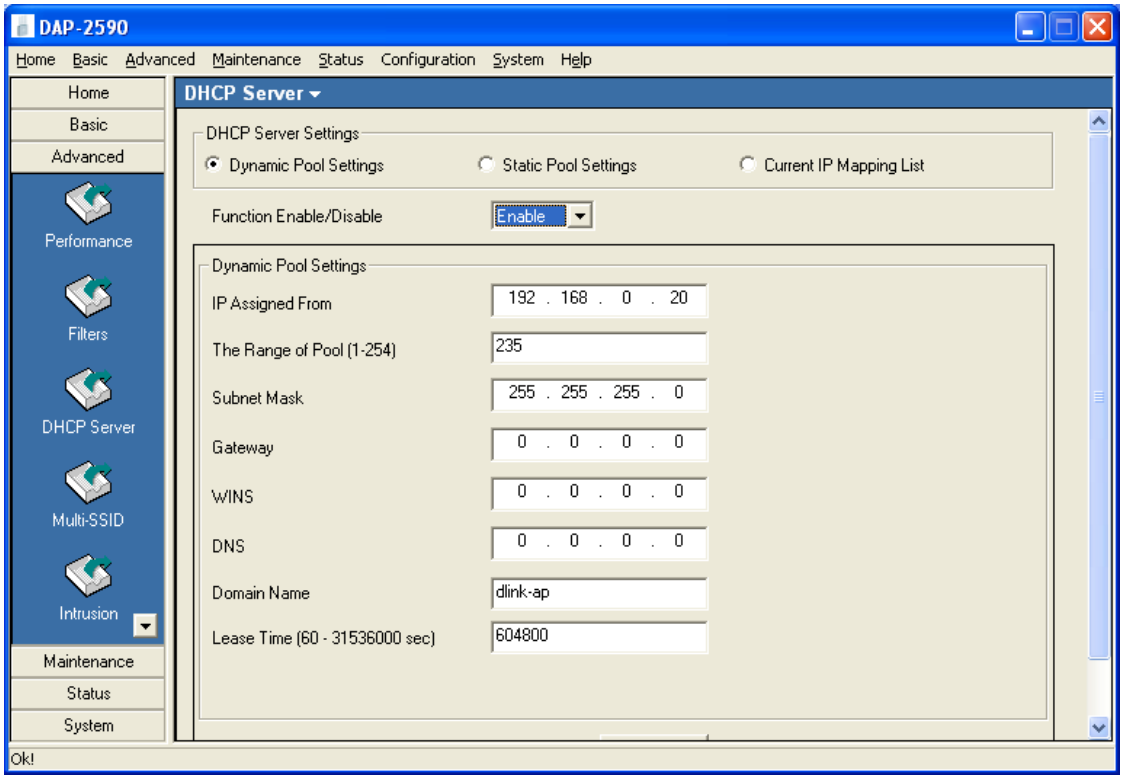


Load Balance: Disabled by default, select Enable to activate load balancing among the APs.

User Limit: Enter a user limit amount, between 0-64.

Link Integrate: If enabled, when the uplink of AP is off, the connected wireless client will be disconnected.

DHCP Server (Dynamic Pool Settings)



Dynamic Pool Settings: Click to enable Dynamic Pool Settings. Configure the IP address pool in the fields below.

Function Enable/Disable: Enable or disable the DHCP server function.

IP Assigned From: Enter the initial IP address to be assigned by the DHCP server.

Range of Pool (1~255): Enter the number of allocated IP addresses.

SubMask: Enter the subnet mask.

Gateway: Enter the gateway IP address, typically a router.

WINS: WINS (Windows Internet Naming Service) is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

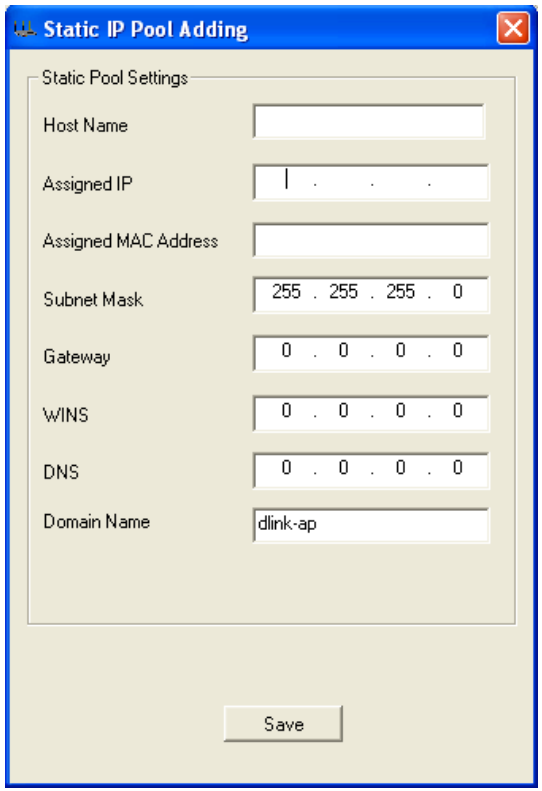
DNS: The IP address of the DNS server, if applicable.

Domain Name: Enter the domain name of the AP, if applicable.

Lease Time: The period of time that the client will retain the assigned IP address.

Status: This option turns the dynamic pool settings on or off.

DHCP Server (Static Pool Settings)



Dynamic Pool Settings: Click to enable Static Pool Settings. Use this function to assign the same IP address to a device at every restart. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool.

Enable/Disable: Enable or disable the DHCP server function.

Assigned IP: Enter the IP address to be statically assigned by the DHCP server.

Assigned MAC Address: Enter the MAC Address of the wireless client.

SubMask: Enter the subnet mask.

Gateway: Enter the gateway IP address, typically a router.

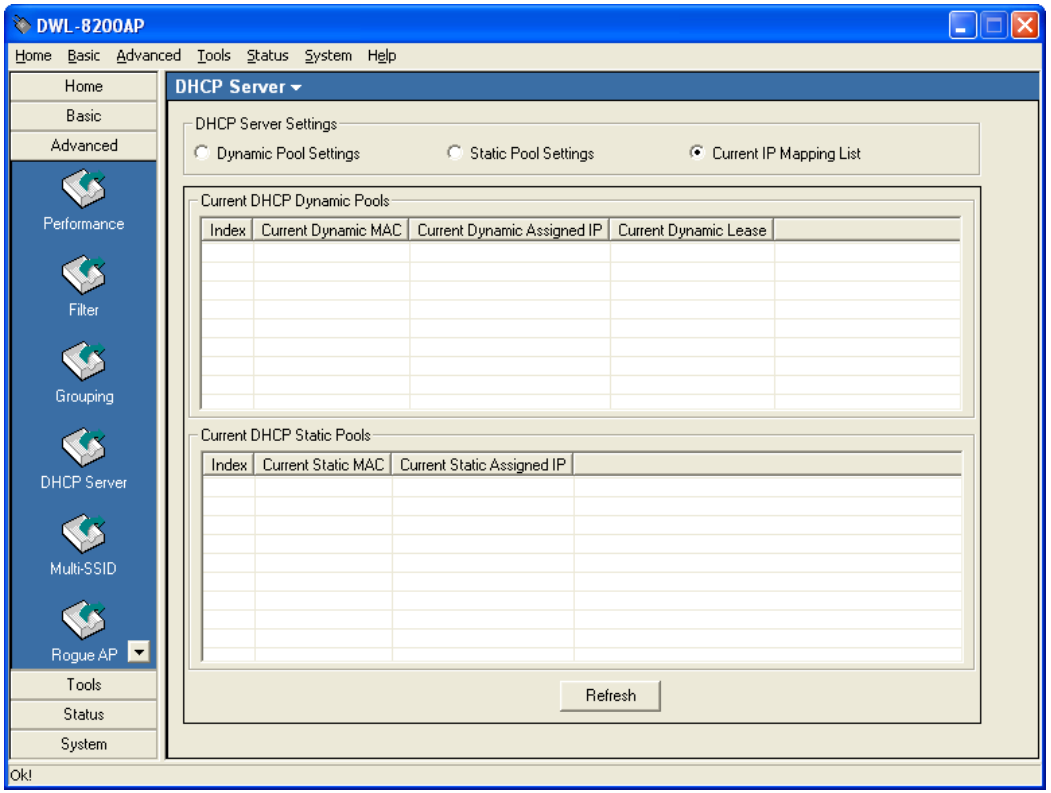
WINS: WINS (Windows Internet Naming Service) is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS: The IP address of the DNS server, if applicable.

Domain Name: Enter the domain name of the AP, if applicable.

Status: This option turns the static pool settings on or off.

DHCP Server (Current IP Mapping List)



This screen displays information about the current DHCP dynamic and static IP address pools. This information is available when you enable the DHCP function of the AP and assign dynamic and static IP address pools.

Current DHCP Dynamic Pools: These are IP address pools to which the DHCP server function has assigned dynamic IP addresses.

Current Dynamic MAC: The MAC address of a device on the network that is within the DHCP dynamic IP address pool.

Current Dynamic Assigned IP: The current corresponding DHCP-assigned dynamic IP address of the device.

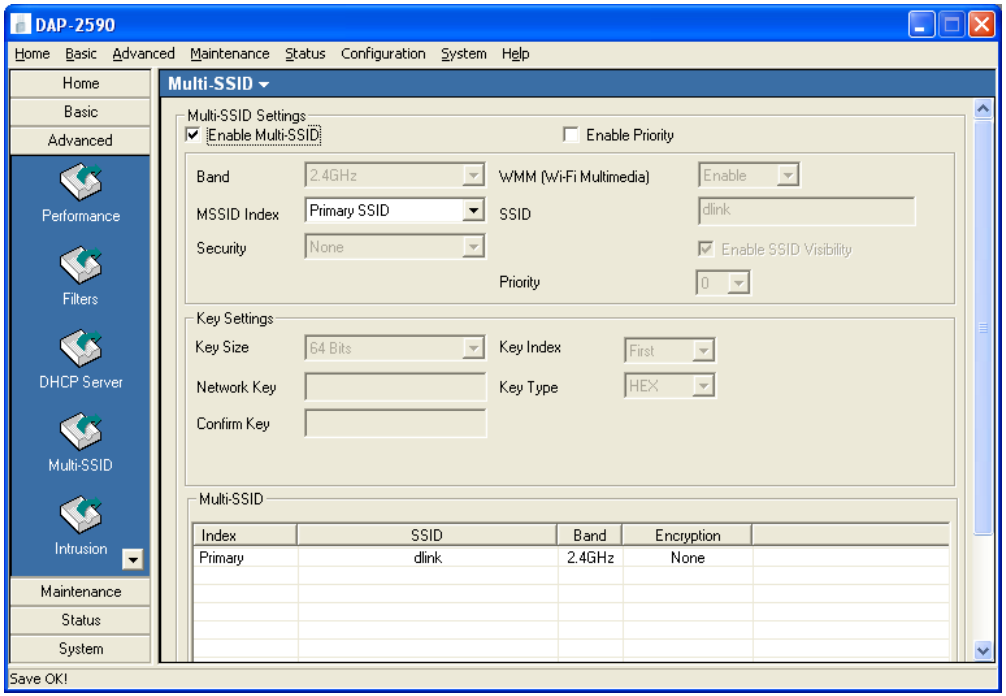
Current Dynamic Lease: The length of time that the dynamic IP address will be valid.

Current DHCP Static Pools: These are IP address pools to which the DHCP server function has assigned static IP addresses.

Current Static MAC: The MAC address of a device on the network that is within the DHCP static IP address pool.

Current Static Assigned IP: The current corresponding DHCP-assigned static IP address of the device.

Multi-SSID



Enable Multi-SSID: When Multi-SSID is enabled, you can configure your SSIDs for 1**1g** networks.

Enable VLAN State: Check to enable VLANs.

Enable Priority: Check to enable priority.

Band: Select the wireless band. When configuring an 802.11n access point, select **2.4GHz** or **5GHz**.

MSSID Index: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Ethernet Without Tag: Check to set ethernet without tag. Only available when VLAN State is enabled.

VLAN ID: Enter a VLAN number (0 - 4094). Only available when VLAN State is enabled.

MSSID Index: You can select up to 7 MSSIDs per band, the default MSSID is the primary, which puts the total to 8 MSSIDs per band.

SSID: The Service Set (network) Identifier of your wireless network.

Security: Select the security level from the drop-down menu.

Enable SSID Broadcast: For each SSID, select to enable or disable the broadcast of the SSID.

VLAN Tag Mode: Dispalys the VLAN tag mode.

WMM: Check to enable WMM.

Priority: Select a priority level for the selected SSID. Only available when Priority is enabled.

WEP Encryption

Key Index: Select which defined key is active on the selected device(s).

WEP Key: In the Key Type drop-down menu select **HEX** or **ASCII**. Select the level of encryption (64, 128, or 162-bit) from the key Size drop-down box, and then enter the WEP key in the box.

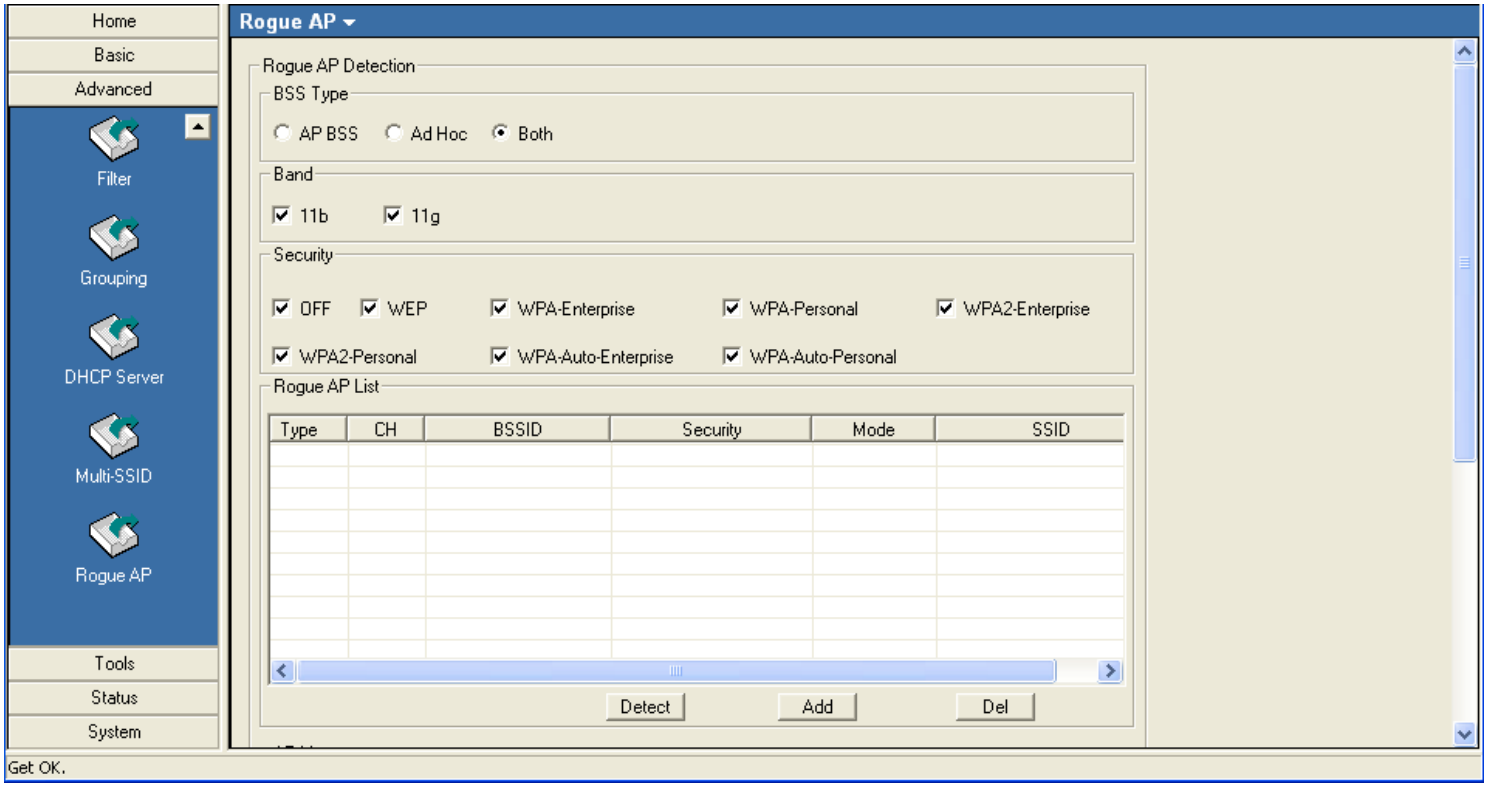
WPA/WPA2 Personal

Cipher Type: Select **Auto**, **AES**, or **TKIP**.

Group Key Update Interval: Enter the Group Key Interval (1800 is default).

Passphrase: Enter the WPA passphrase (between 8-63 characters).

Rogue AP



BSS Type: The Basic Service Set Type allows you to select from **AP BSS**, **Ad Hoc**, or **Both**.

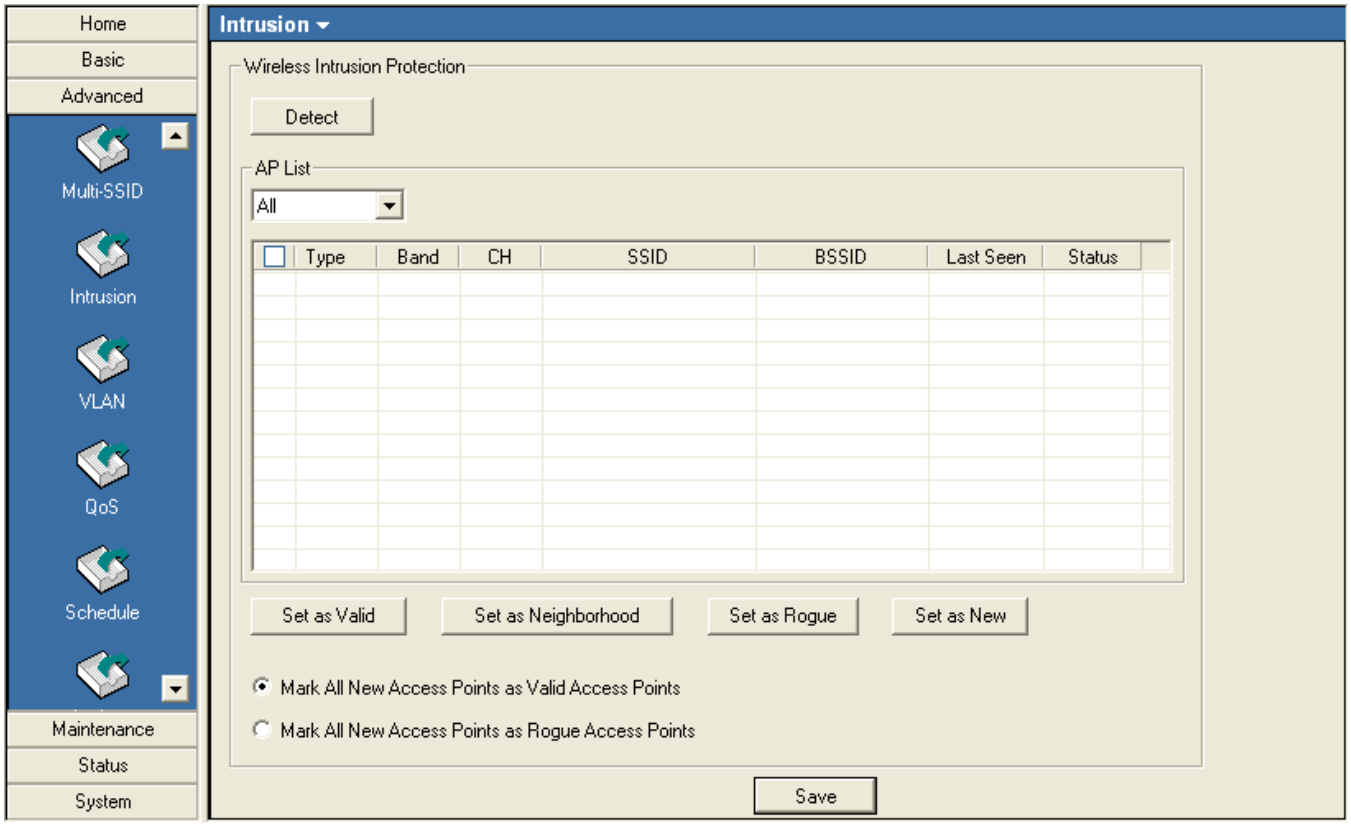
Band: Select the type of network (bands **11b**, and **11g)** that you would like the AP detection to search on.

Security: Select the Security type - **Off**, **WEP**, **WPA-Enterprise**, **WPA-Personal, WPA2 Enterprise, WPA2-Personal, WPA-Auto-Enterprise, and WPA2-Auto-Personal** that you would like to be consider during AP detection.

Rogue AP List: This window shows all of the neighbor APs detected, which is based on your criteria from above (BSS Type, Band, and Security). If the AP is in the same network, or if you know the AP, just click on "**Add**" to save it to the AP list.

AP List: This window shows all of the APs that are allowed access on the network.

Intrusion (802.11n only)

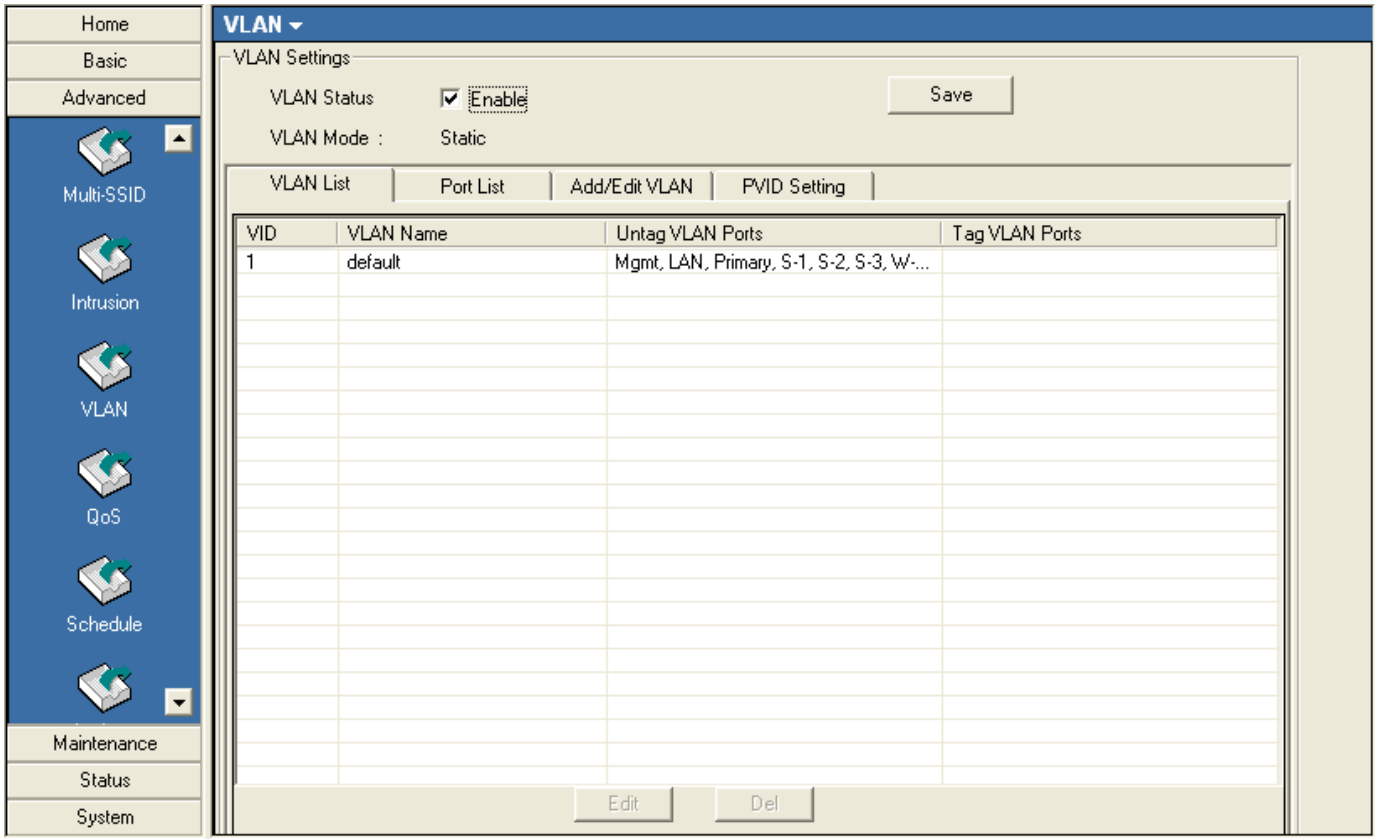


Wireless Intrusion Protection: It is used to classify the surrounding APs.

Detect: Click the button to detect the surrounding APs. The results will show in the AP list. The category of the APs.

AP List: From the All list, click the corresponding **Set** button of AP record to classify the AP. Or mark all new access points as valid/rogue access poins.

VLAN (802.11n only)



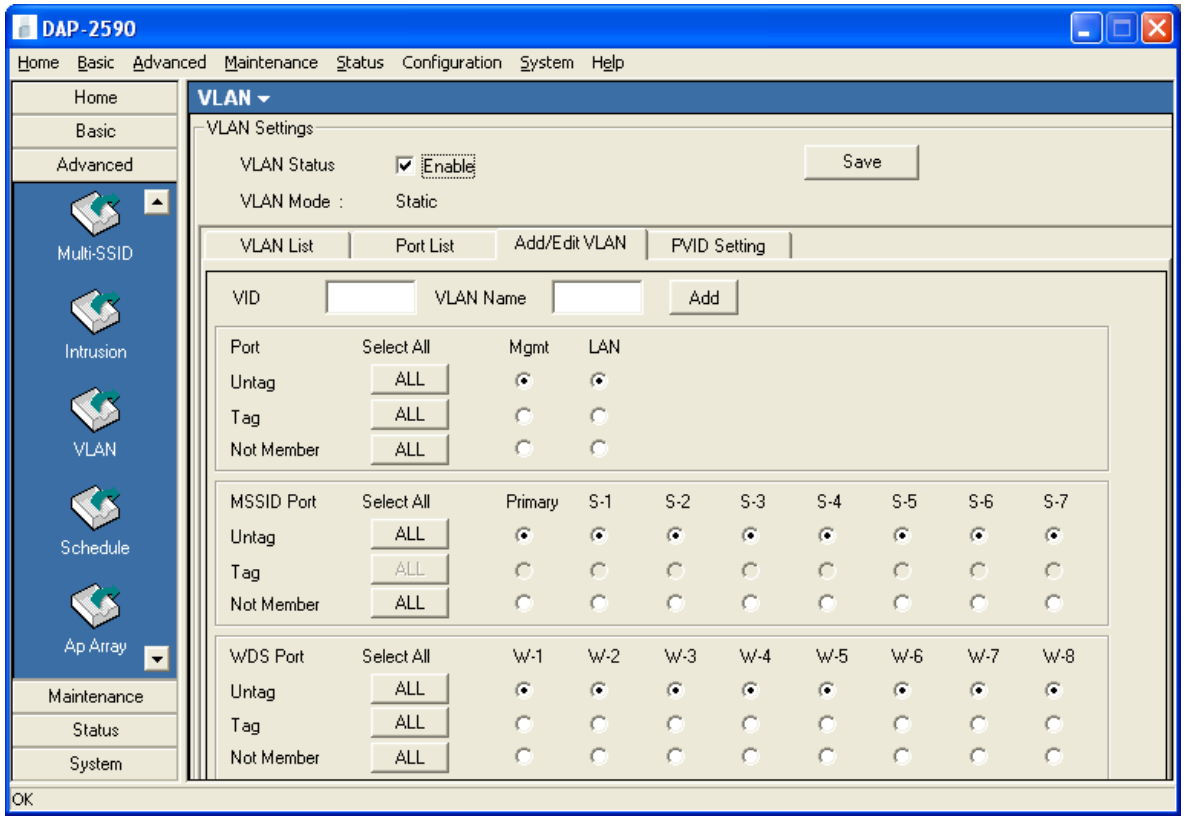
VLAN Status: Check this box to enable the VLAN function.

VLAN Mode: Displays the mode of VLAN.

VLAN List: This window lists the configured VLAN on the AP.

Port List: This window lists the configured Port on the AP.

Add/Edit VLAN (802.11n only)

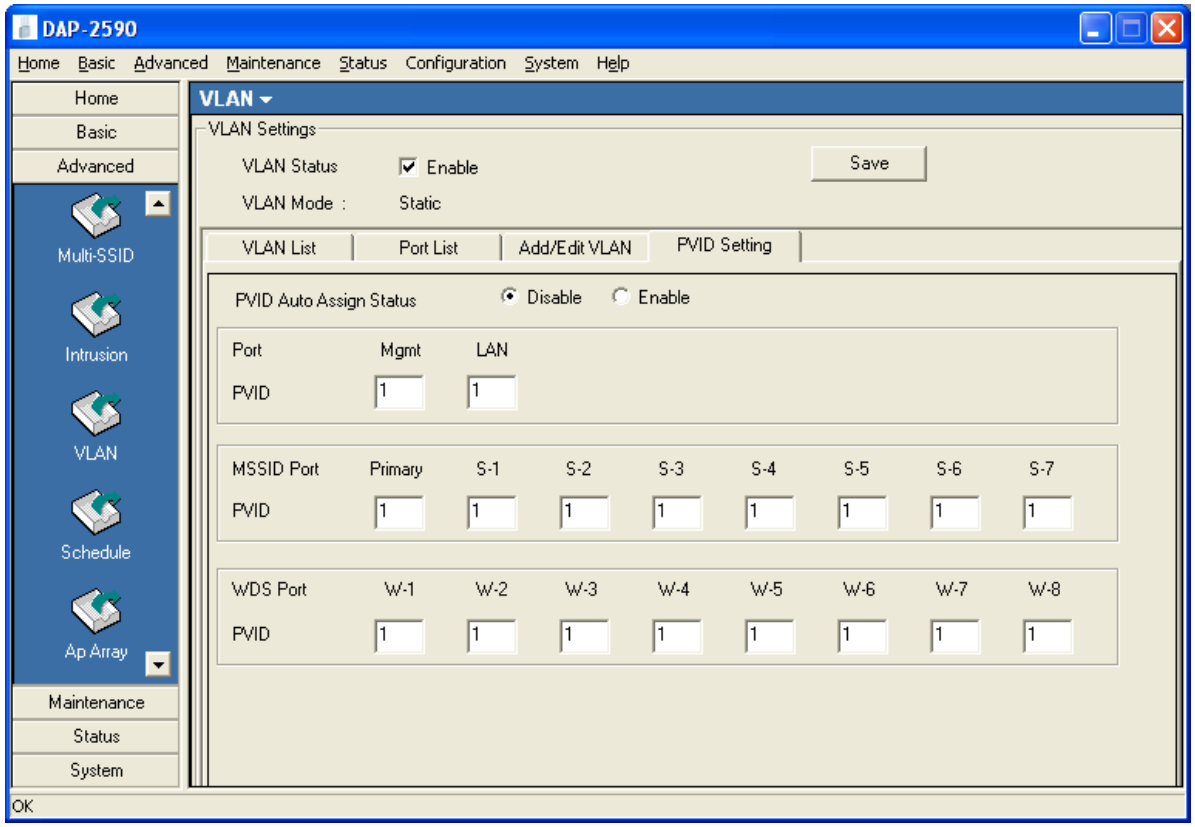


VID: Enter a VID number in this box.

VLAN Name: Enter a VID description string in this box.

Port/MSSID Port/WDS Port: Select and assign the VLAN members from Port/MSSID Port/WDS Port.

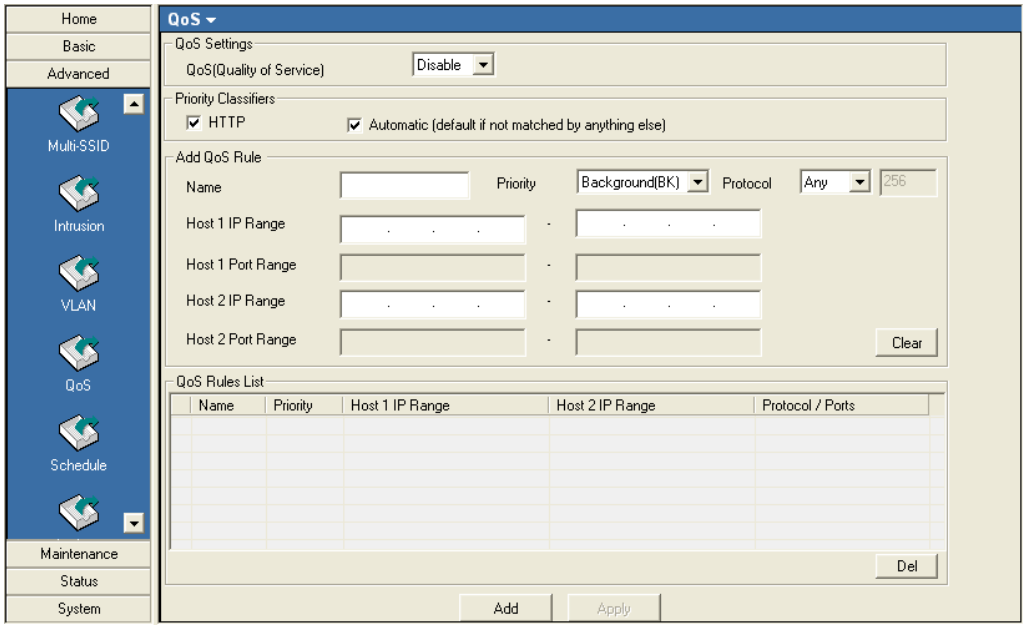
PVID Setting (802.11n only)



PVID Auto Assign Status: Check this box to assign the PVID automatically.

Port/MSSID Port/WDS Port: Assign the PVID manually.

QoS (802.11n only)



Qos Settings: Check the box to enable the QoS function.

Priority Classifiers: Check the HTTP box to apply the rule to http packets. Check Automatic box to apply the rule to all the packets.

Add QoS Rule Name: Enter a name for this QoS rule.

Priority: Select a priority level from the drop-down list. There are four types of priority: **Background**, **Best Effort**, **Video** and **Voice**.

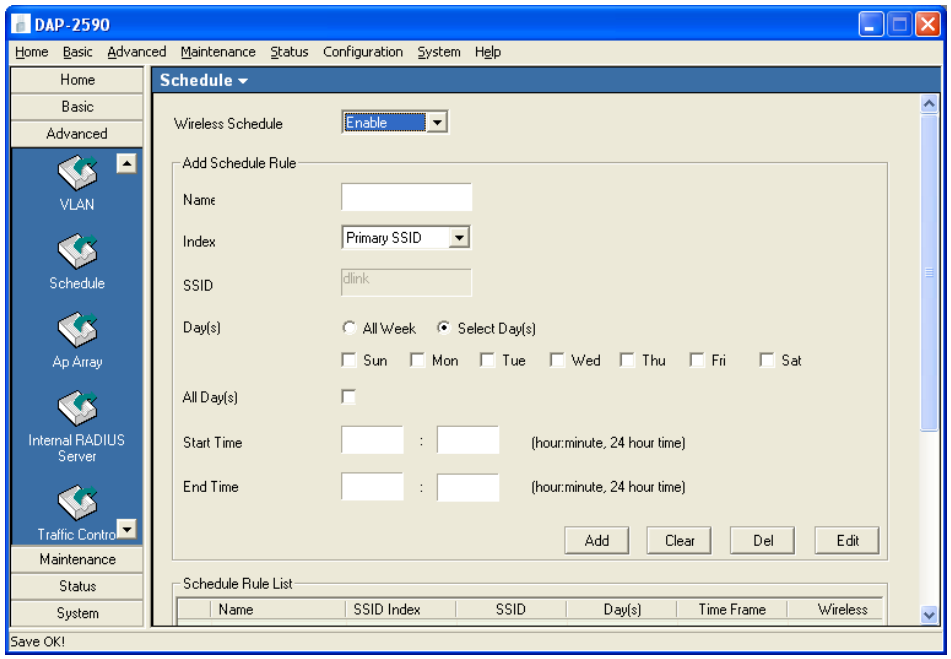
Protocol: Select the protocol from the drop-down list.

Host IP Range: Enter the IP range that applies the rule.

Host Port Range: Enter the Port range that applies the rule.

QoS Rules List: This window lists the configured QoS rules.

Schedule (802.11n only)



Wireless ScheduleSettings: The schedule is used to open or close the wireless function of the AP at the specified time.

Wireless Schedule: Select **Enable** from the drop-down list to enable this function.

Add Schedule Rule Name: Enter a name for this schedule rule.

Index: Select the SSID index.

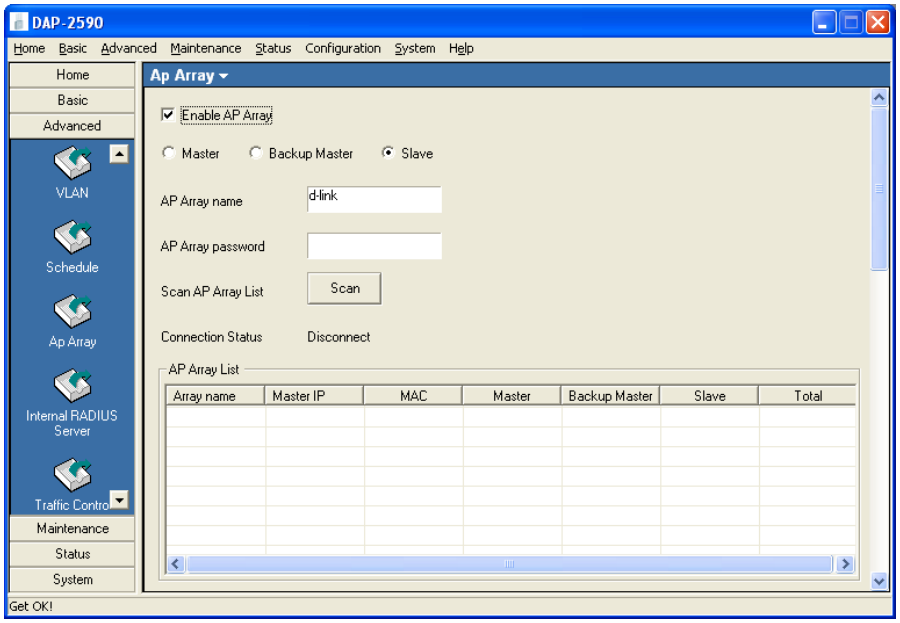
SSID: Dispaly the SSID you selected.

Day(s): Select the days that apply the schedule.

Start/End Time: Enter the start and end times that apply the schedule.

Schedule RulesList: This window lists the configured schedule rules.

AP Array (802.11n only)



AP Array: An AP array is a set of devices on a network that are organized into a single group to increase ease of management.

Enable AP Array: This check box allows the user to enable the AP array function. The three modes that are available are Master, Backup Master, and Slave. APs in the same array will use the same configuration. The configuration will sync the Master AP to the Slave AP and the Backup Master AP when a Slave AP and a Backup Master AP join the AP array.

AP Array Name: Enter a user-selected name for the AP array you have created.

AP Array Password: Enter a user-selected password that will be used to access the AP array you have created.

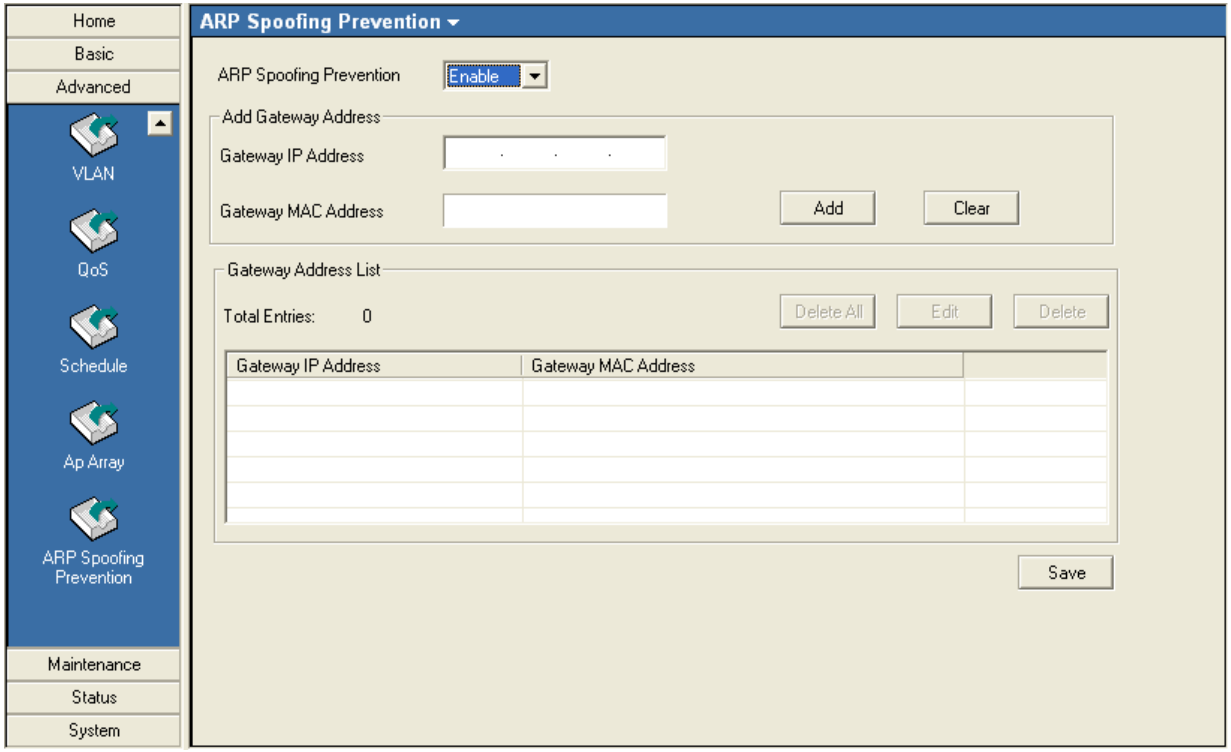
Scan AP Array List: Click this button to initiate a scan of all the available APs currently on the network.

AP Array List: This table displays the current AP array status for the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.

Current Members: This table displays all the current array members. The DAP-2553 AP array feature supports up to eight AP array members.

Synchronized Parameters: Choose Synchronized Parameters of AP Array. Click "Clear all " button to clear all Synchronized Parameters .

ARP Spoofing Prevention (802.11n only)



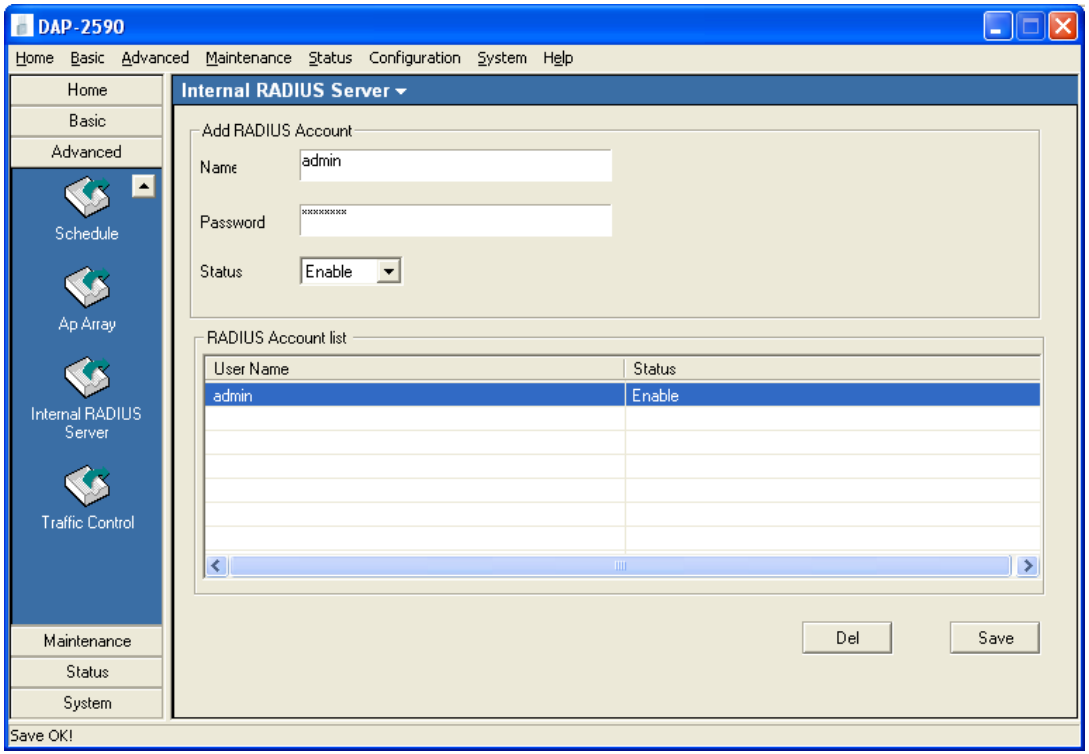
ARP Spoofing Prevention: The ARP Spoofing Prevention feature allows users to add IP/MAC address mapping to prevent arp spoofing attack.

ARP Spoofing Prevention: This check box allows you to enable the arp spoofing prevention function.

Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.

Internal RADIUS Server



Name: Enter a username.

Password: Enter a password.

Status: Select **Enable** or **Disable** from the drop-down menu.

RADIUS Account List: Displays all the created RADIUS accounts and the status.

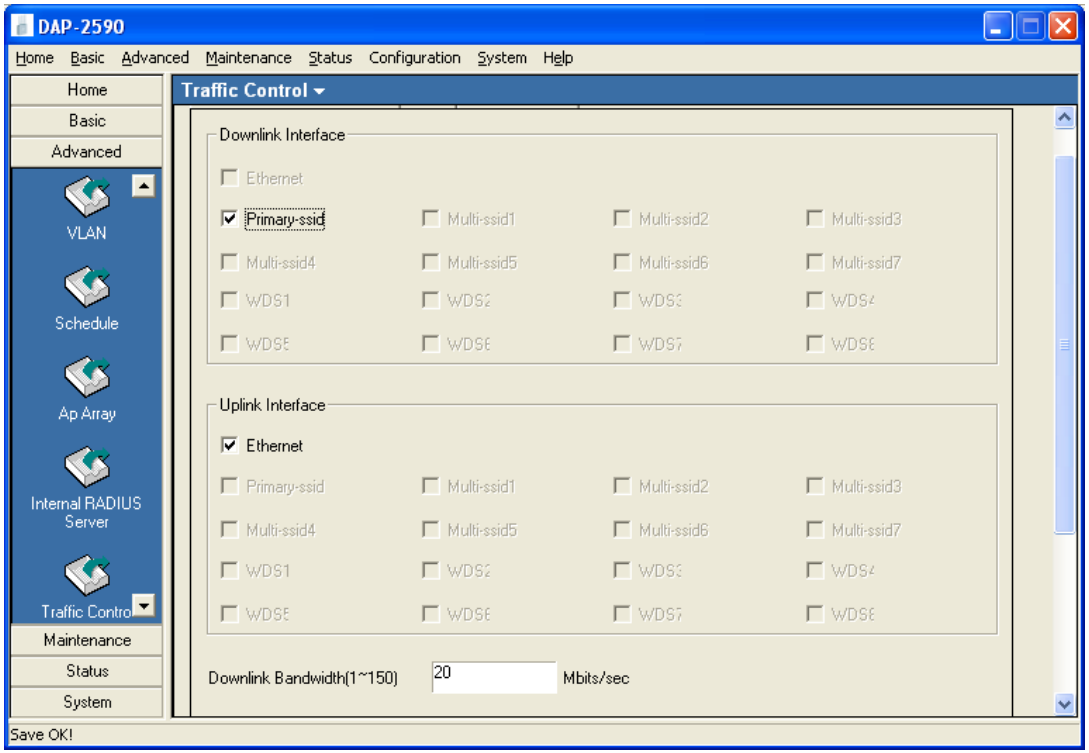
Del: Select an account from the RADIUS Account list and click **Del** to delete the account.

Save: To save your settings after creating an account or changing the status, click **Save**.

Traffic Control

Uplink and Downlink Settings

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows. Once the desired uplink and downlink settings are finished, click the Save button to let your changes take effect.

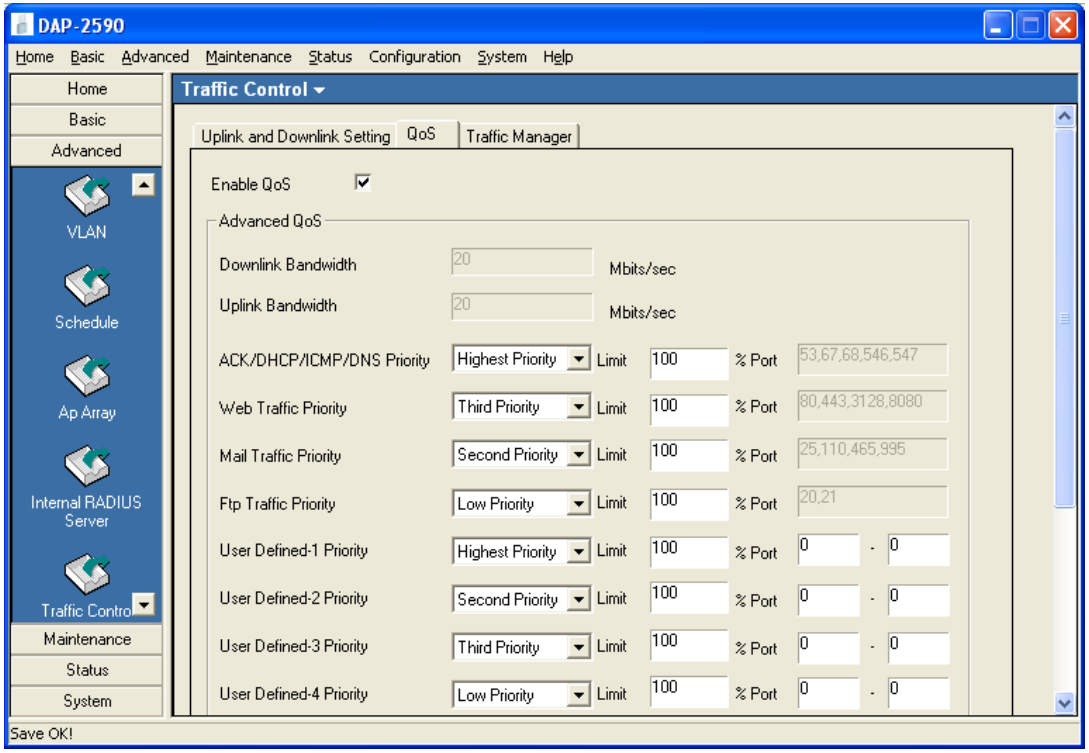


Downlink Interface: The downlink bandwidth in Mbits per second.

Uplink Interface: The uplink bandwidth in Mbits per second.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.



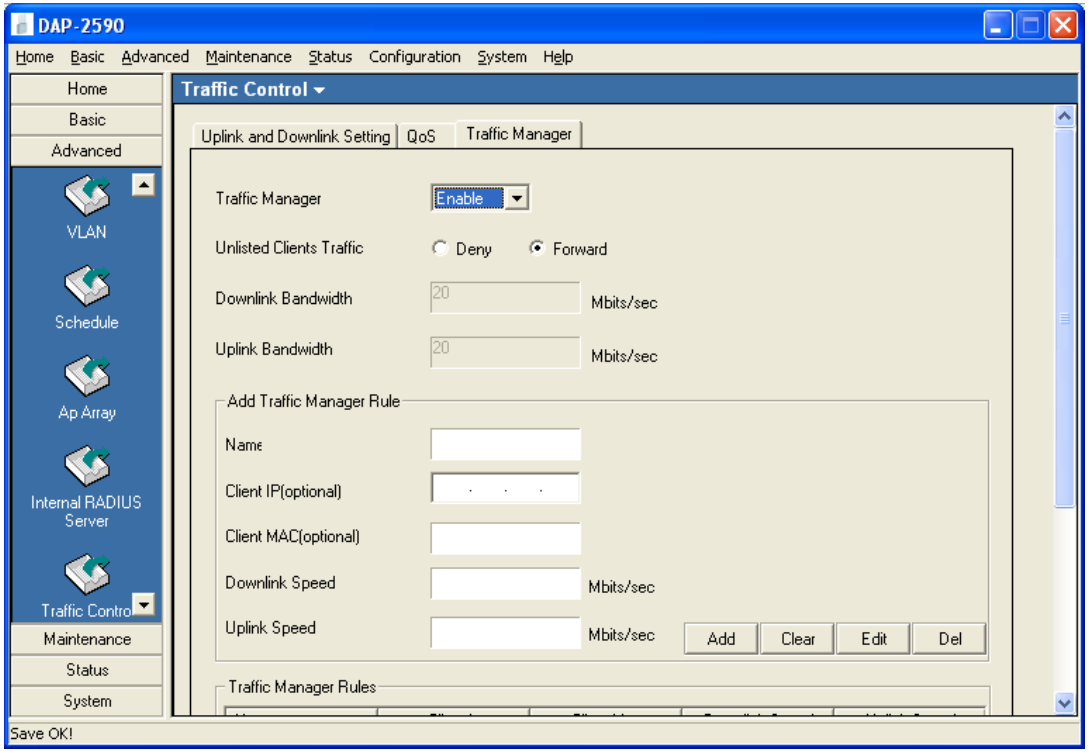
Enable QoS: Check this box to allow QoS to prioritize traffic. Use the drop-down menus to select the four levels of priority. Click the **Save** button when you are finished.

Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Traffic Manager

The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink and uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.



Traffic Manager: Select **Enable** or **Disable** from the drop-down menu.

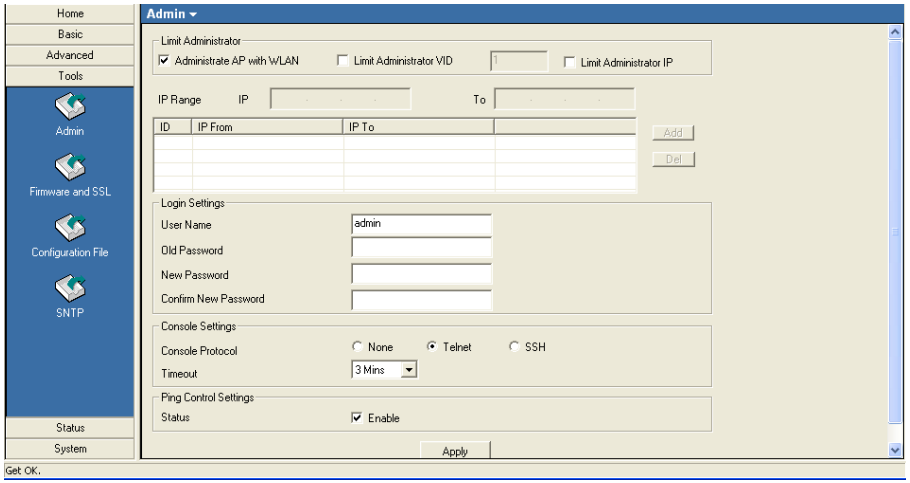
Unlisted Clients Traffic: Select **Deny** to block unlisted clients from accessing the network, or select **Forward** to allow all clients access to the network.

Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Maintenance (802.11g)

Admin



Administrate AP with WLAN: Check this box to allow only the computers within wlan can manage the AP.

Limit Administrator IP: Check this box to allow only the computers within the IP range can manage the AP.

Limit Administrator VID: Check this box to allow only the computers within the VID can manage the AP.

Login Settings

User Name: Enter a user name. The default is **admin**.

Old Password: When changing your password, enter the old password here.

New Password: When changing your password, enter the new password here.

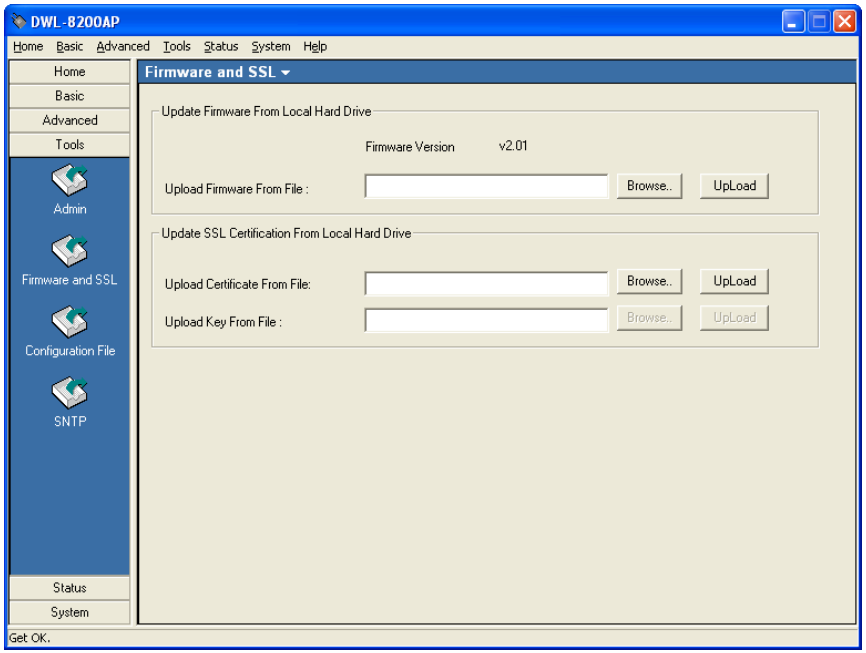
Confirm New Password: Confirm your new password here.

Console Settings

Status: Status is Enabled by default. Select "**None**" to disable the console.

Console Protocol: Select the type of protocol you would like to use, **Telnet** or **SSH**.

Firmware and SSL



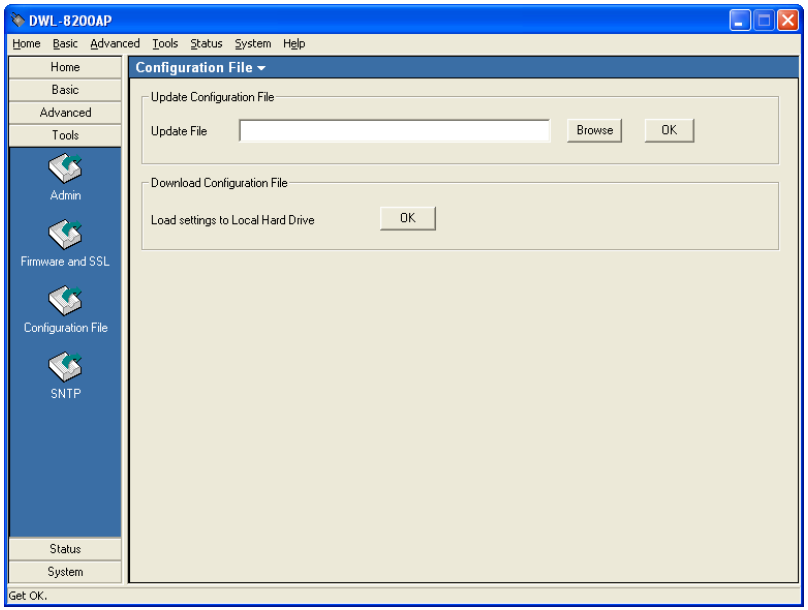
Upgrade Firmware from Local Hard Drive

- Download the latest firmware upgrade from http://support.dlink.com to an easy to find location on your hard drive.
- Click on the **Browse** button as shown above.
- A popup window will appear. Locate the firmware upgrade file and click **Open**.
- The path to the file will be displayed in the "Upgrade Firmware File From" field. Click the **Upload** button to upload the file to the AP.

Update SSL Certification from Local Hard Drive

To update the SSL Certification on the AP, use the **Browse** buttons to locate the SSL certificate and key files on your local computer. Use the **Upload** buttons to upload the files to the AP.

Configuration File



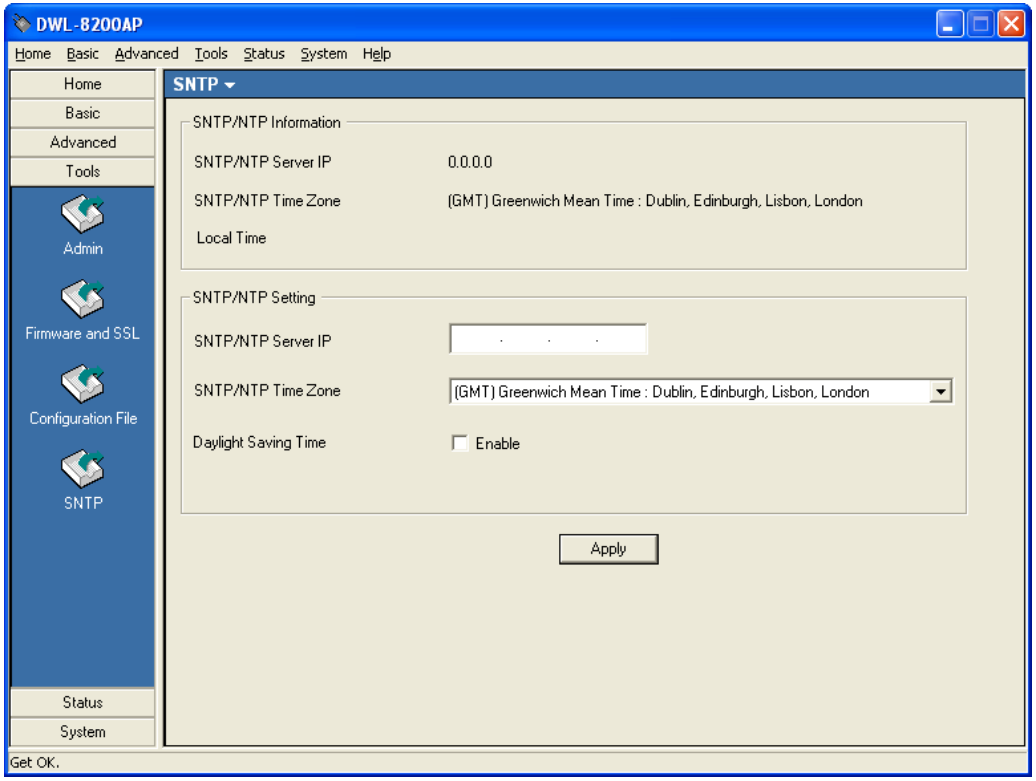
The AP Manager II software allows you to save the device settings to a configuration file. To save a configuration file follow these steps:

- Select a device from the Device List on the main screen of AP Manager II.
- Browse to the **Tools** > **Configuration** page of AP Manager II.
- Click the **OK** button under **Download Configuration File** after you have all the settings as you want them.
- A popup window will appear prompting you for a file name and location. Enter the file name, choose a file destination, and click **Save**.

To load a previously saved configuration file, follow these steps:

- Click **Browse** to locate the device configuration file on your computer.
- A popup window will appear prompting you to locate the configuration file. Locate the file and click **Open**.
- The path to the file will be displayed in the "Upgrade File" field. Click the **OK** button to upload the configuration file to the AP.

SNTP



SNTP/NTP Information: The time server IP address, time zone, and the local time will be displayed here.

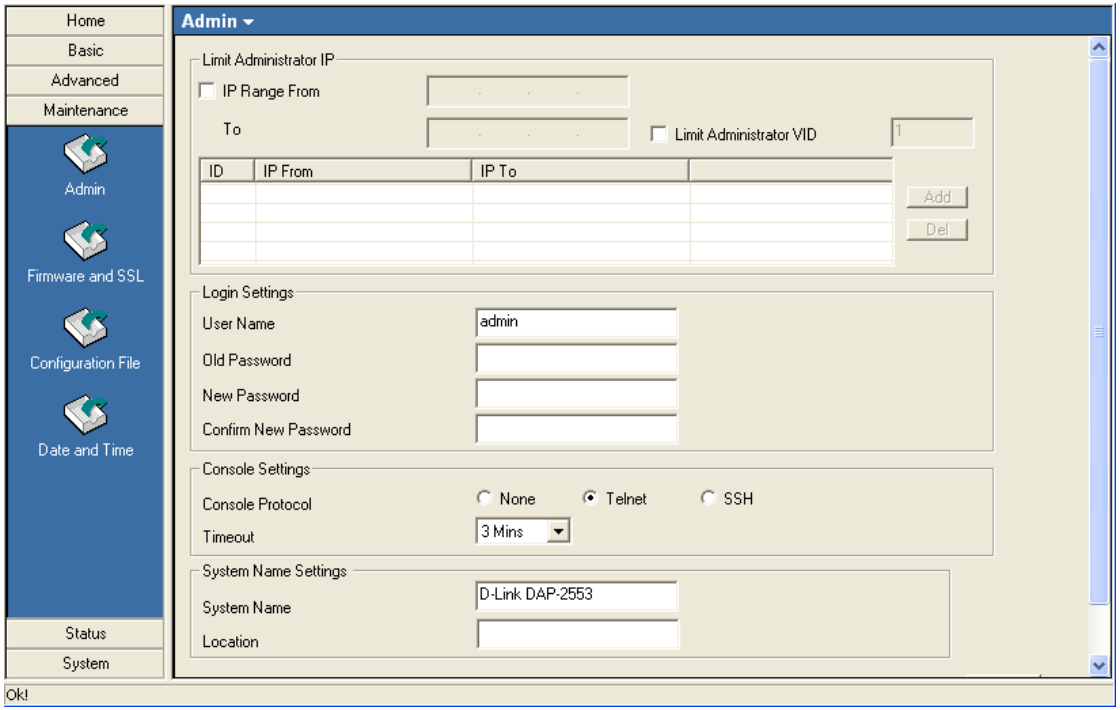
Server IP: Enter the IP address of a SNTP/NTP server.

Time Zone: Select your time zone from the drop-down menu.

Daylight Saving Time: Check the box to enable daylight savings time.

Maintenance (802.11n)

Admin



Limit Administrator IP

IP Range From: Check this box to allow only the computers within the IP range can manage the AP.

Limit Administrator VID: Check this box to allow only the computers within the VID can manage the AP.

Login Settings

User Name: Enter a user name. The default is **admin**.

Old Password: When changing your password, enter the old password here.

New Password: When changing your password, enter the new password here.

Confirm New Password: Confirm your new password here.

Console Settings

Console Protocol: Select the type of protocol you would like to use, Telnet or SSH or select "None" to disable the console.

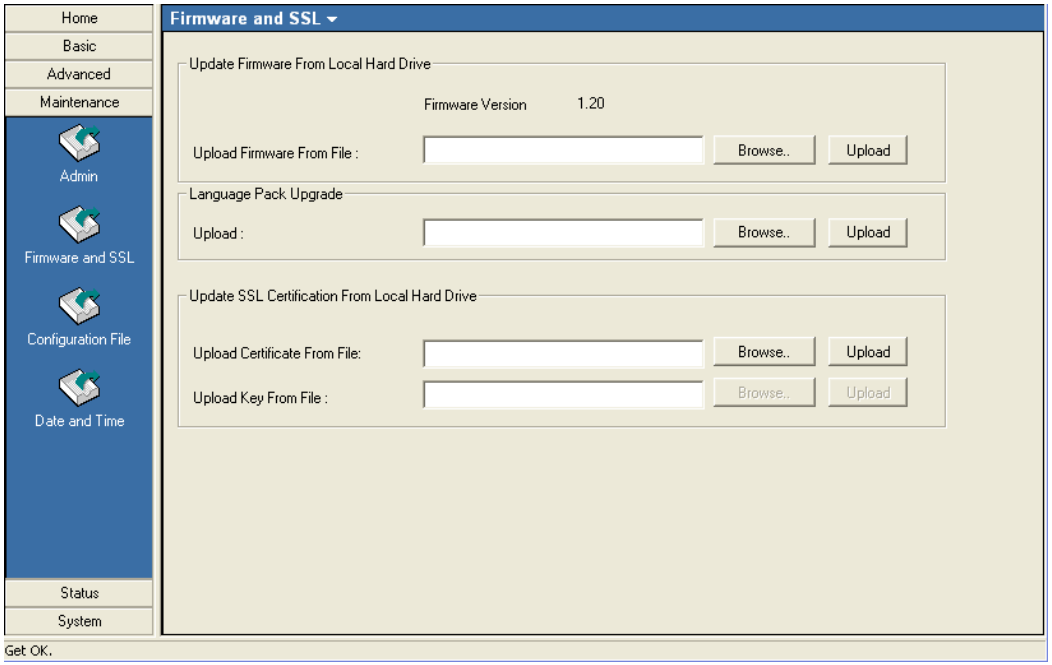
Timeout: Select the expired time from the drop-down list.

System Name Settings

System Name: Enter a name for this device.

Location: Enter a string to describe the location of device.

Firmware and SSL



Upgrade Firmware from Local Hard Drive

- Download the latest firmware upgrade from http://support.dlink.com to an easy to find location on your hard drive.
- Click on the **Browse** button as shown above.
- A popup window will appear. Locate the firmware upgrade file and click **Open**.
- The path to the file will be displayed in the "Upgrade Firmware File From" field. Click the **Upload** button to upload the file to the AP.

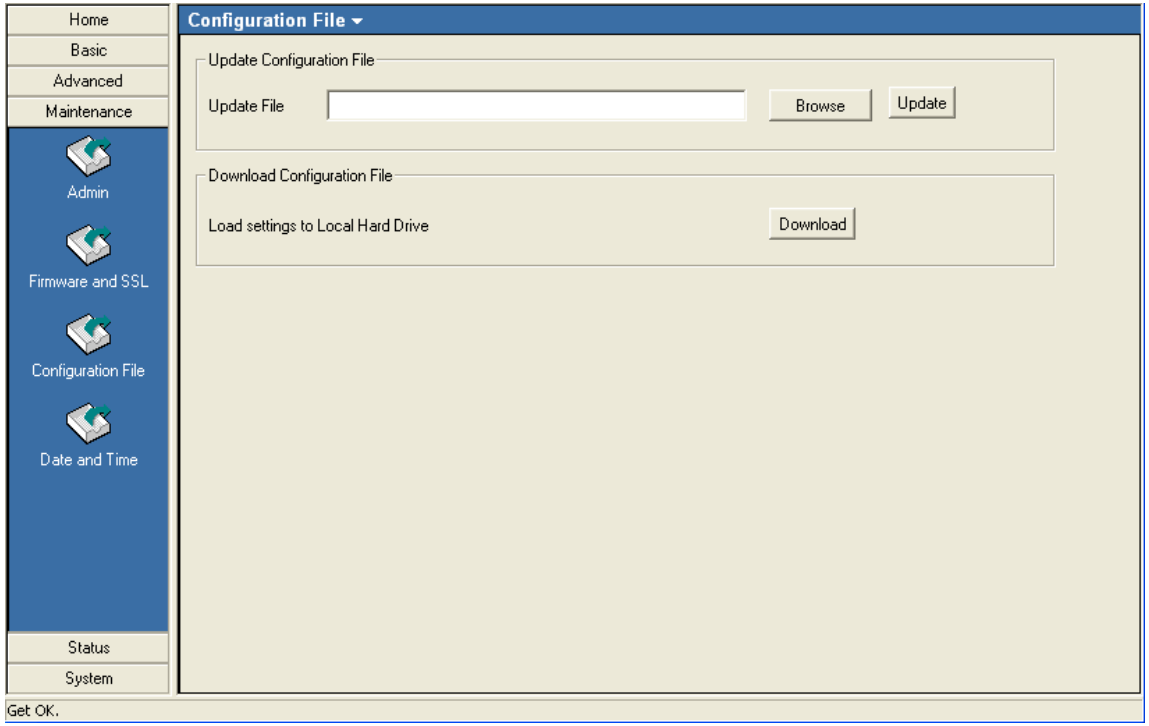
Language Pack Upgrade

To update the language on the AP, use the **Browse** buttons to locate the language pack on your local computer. Use the **Upload** button to upload the files to the AP.

Update SSL Certification from Local Hard Drive

To update the SSL Certification on the AP, use the **Browse** buttons to locate the SSL certificate and key files on your local computer. Use the **Upload** buttons to upload the files to the AP.

Configuration File



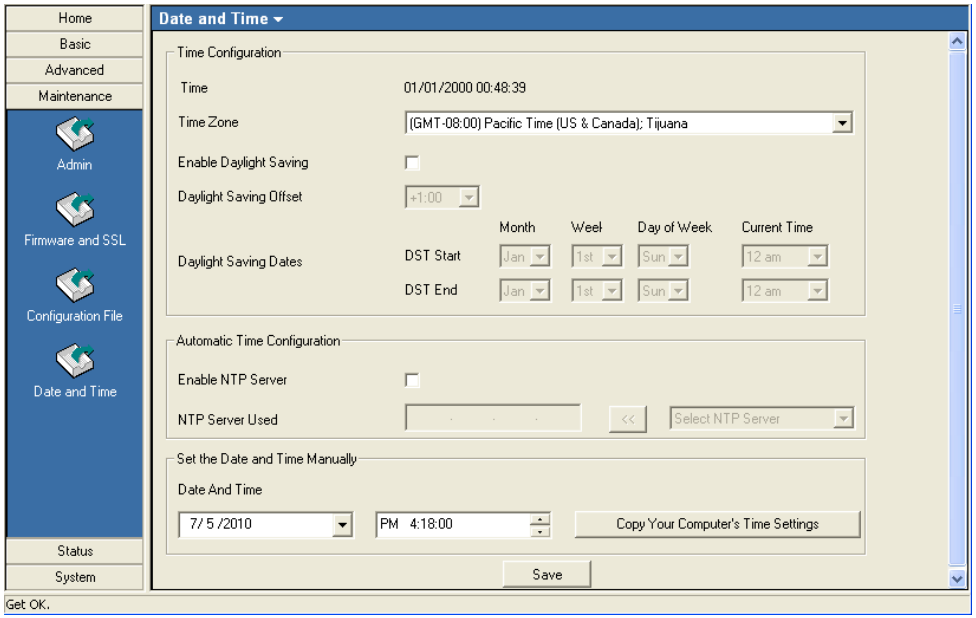
The AP Manager software allows you to save the device settings to a configuration file. To save a configuration file follow these steps:

- Select a device from the Device List on the main screen of AP Manager.
- Browse to the **Tools** > **Configuration** page of AP Manager.
- Click the **OK** button under **Download Configuration File** after you have all the settings as you want them.
- A popup window will appear prompting you for a file name and location. Enter the file name, choose a file destination, and click **Save**.

To load a previously saved configuration file, follow these steps:

- Click **Browse** to locate the device configuration file on your computer.
- A popup window will appear prompting you to locate the configuration file. Locate the file and click **Open**.
- The path to the file will be displayed in the "Upgrade File" field. Click the **OK** button to upload the configuration file to the AP.

Date and Time



Time Configuration

Time: The current local time will be displayed here.

Time Zone: Select your time zone from the drop-down list.

Daylight Saving: Check the box to enable daylight savings time.

Daylight Saving Offset: Select the offset time from the drop-down list.

Daylight SavingDates: Select the start and end date of daylight saving.

Automatic Time Configuration

Enable NTP Server: Check this box to synchronize the time with NTP server.

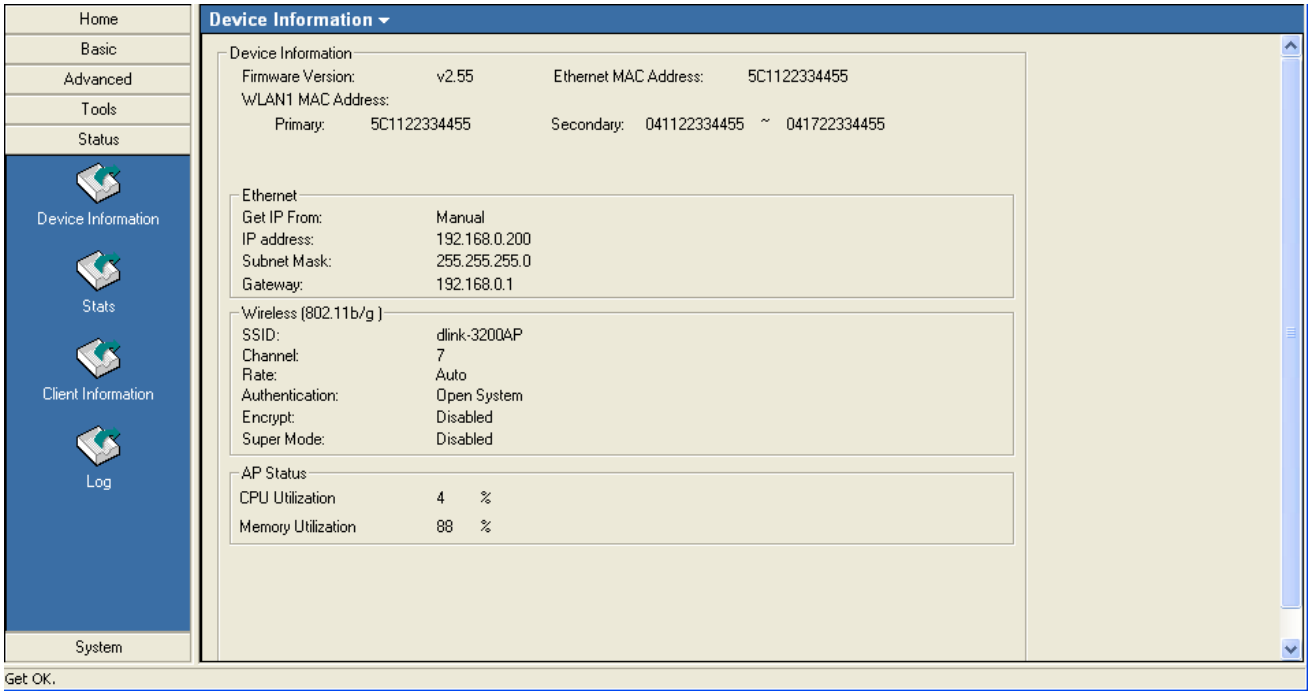
NTP Server Used: Select one NTP server from the drop-down list.

Set the Date andTime Manually

Date And Time: Select the date and time from the box or copy your computer's time setting to AP.

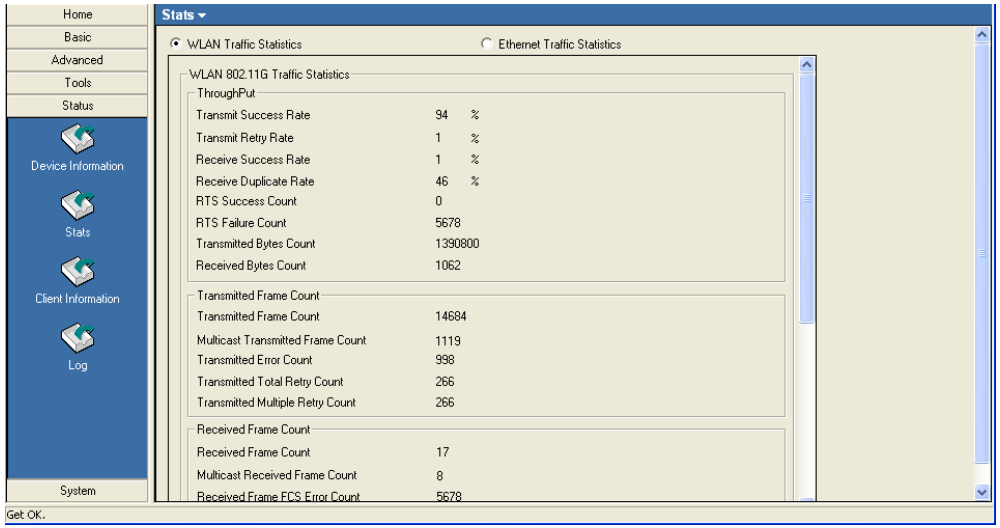
Status (802.11g)

Device Information



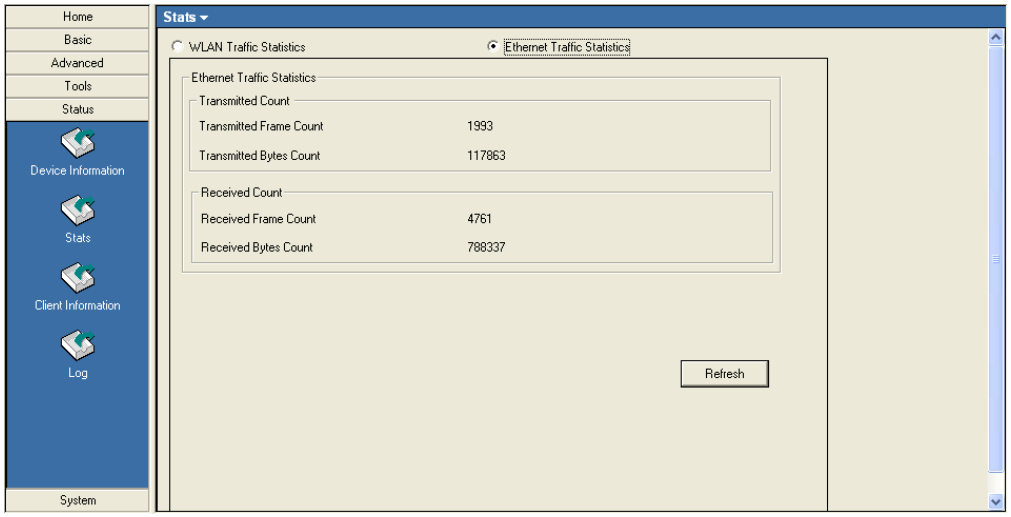
Device Information: This window displays the configuration settings of the AP, including the firmware version and device MAC address. It also displays WLAN information for both the 802.11b and 802.11g wireless networks.

Stats



WLAN Traffic Statistics: This page displays statistics for data throughput, transmitted and received frames, and WEP frame errors for the wireless network.

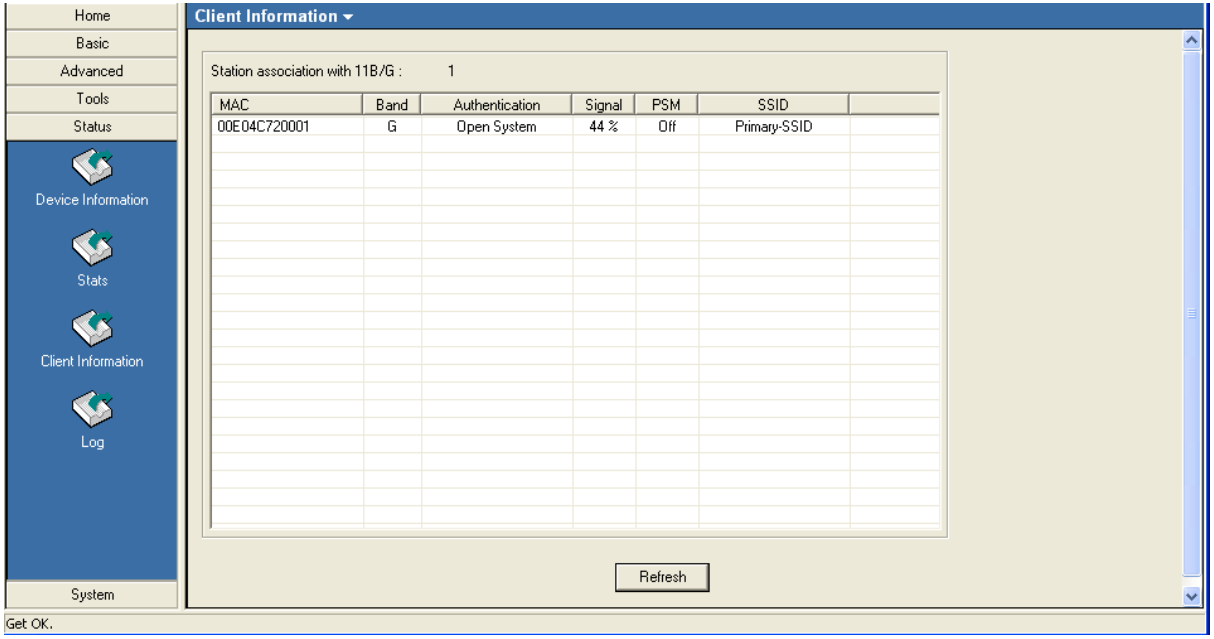
Ethernet Traffic Statistics



Ethernet Traffic Statistics: This page displays statistics for data throughput, transmitted and received frames for the Ethernet port of AP.

Client Information

This window displays the wireless client information for clients currently connected to the AP. The following information is available for each client communicating with the AP.



MAC: Displays the MAC address of the client.

Band: Displays the wireless band the client is connected on.

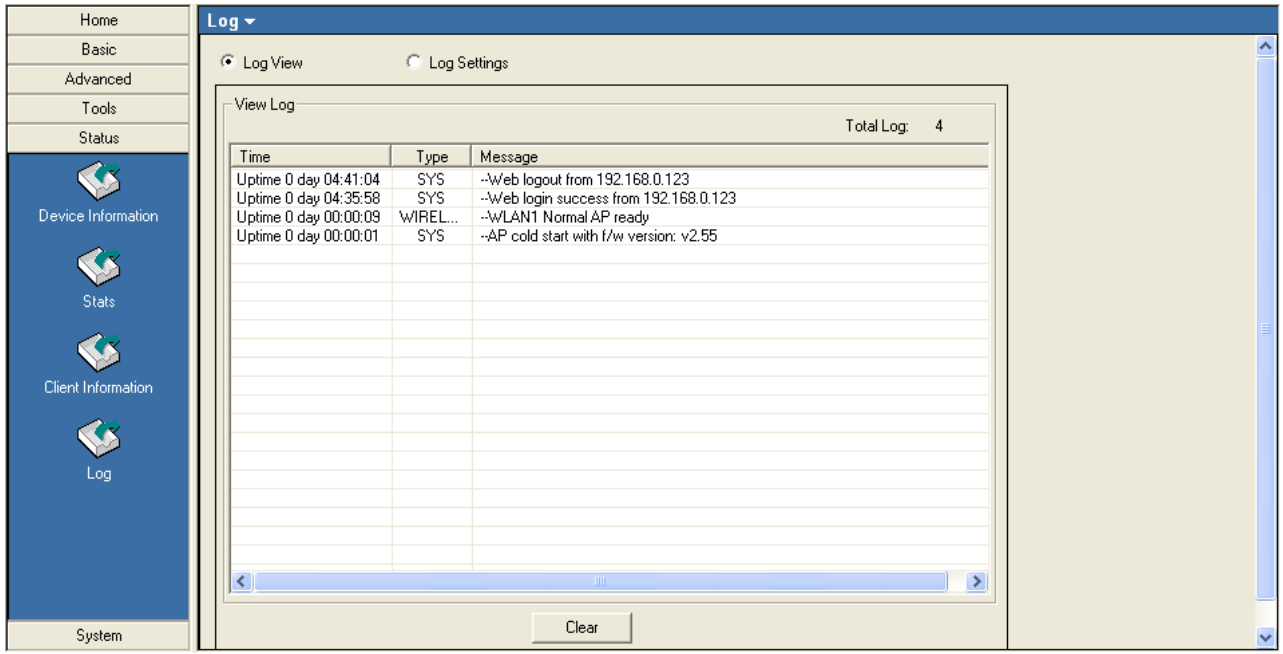
Authentication: Displays the type of authentication being used.

Signal: Displays the strength of the clients signal.

Power Saving Mode: Displays the status of the power saving feature.

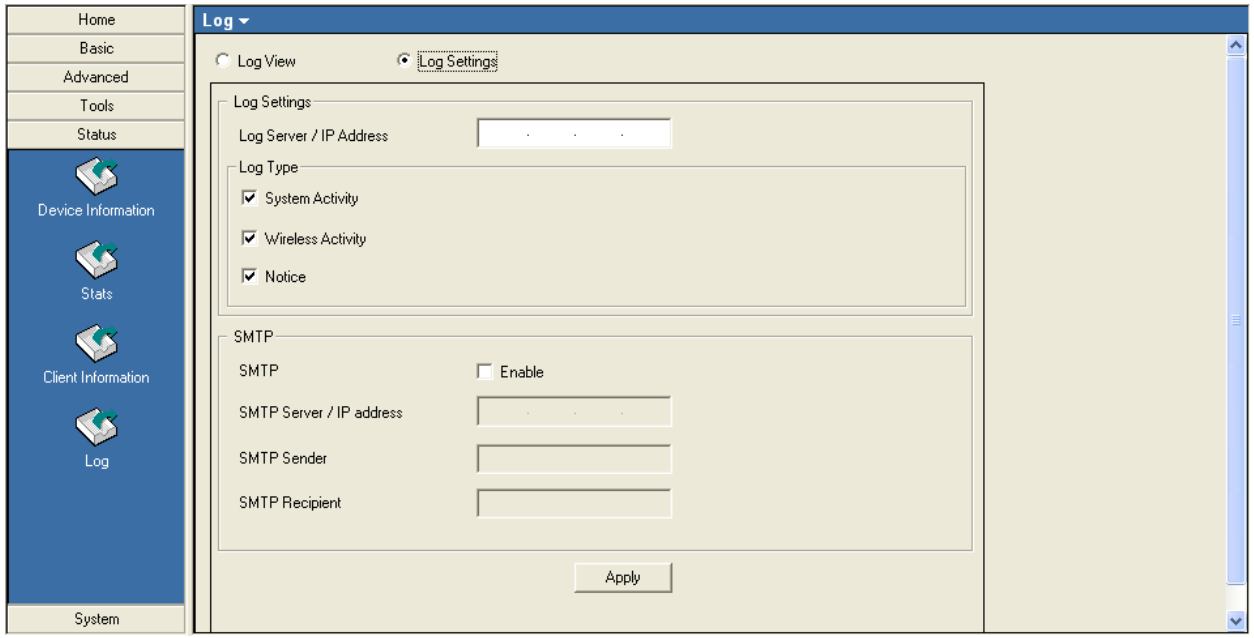
SSID: Displays the SSID the client is connected to.

Log View



View Log: The log displays system and network messages including a time stamp and message type.

Log Settings



Log Settings

Log Server / IP Address: Enter the IP address of the server you would like to send the AP log to.

Log Type: Check the box for the type of activity you want to log. There are three types: **System**, **Wireless** and **Notice**.

SMTP Settings

SMTP: Check the box to enable SMTP.

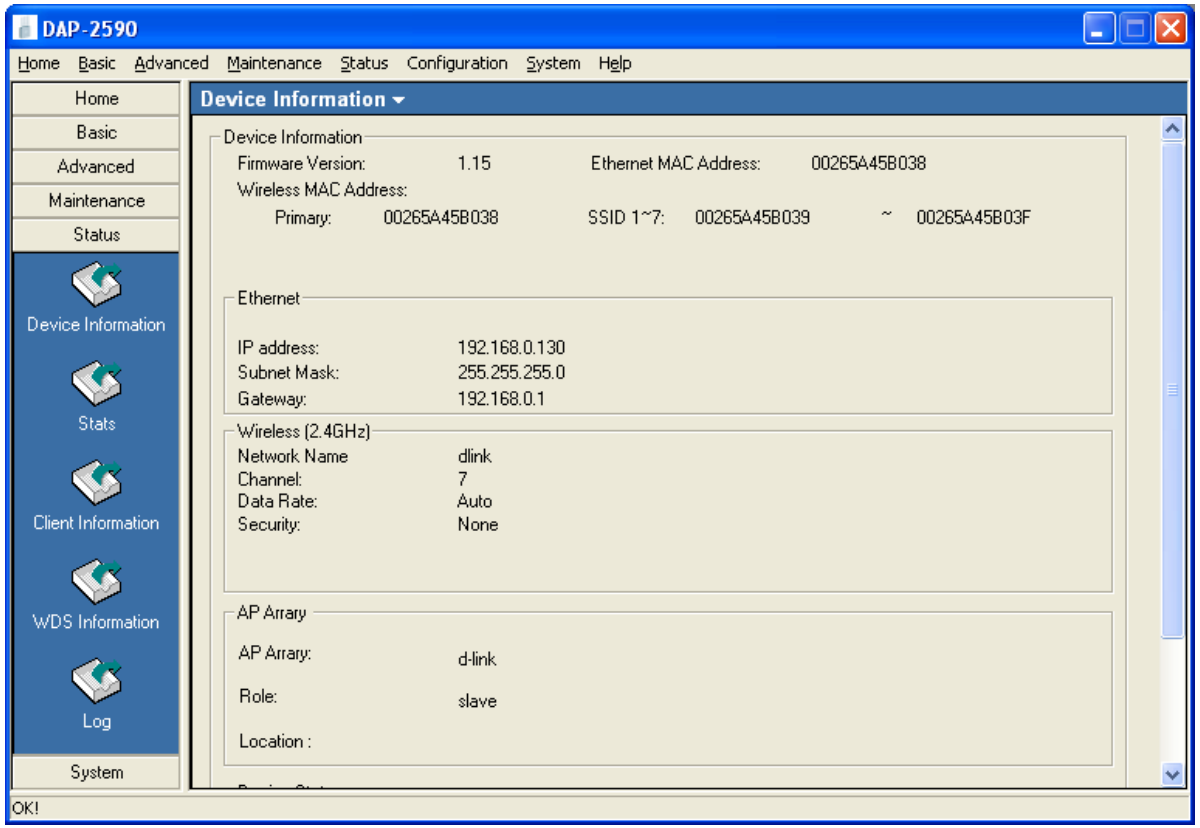
SMTP Server / IP Address: Enter the IP address of the SMTP server.

SMTP Sender: Enter the e-mail address of the SMTP sender.

SMTP Recipient: Enter the e-mail address of the SMTP recipient.

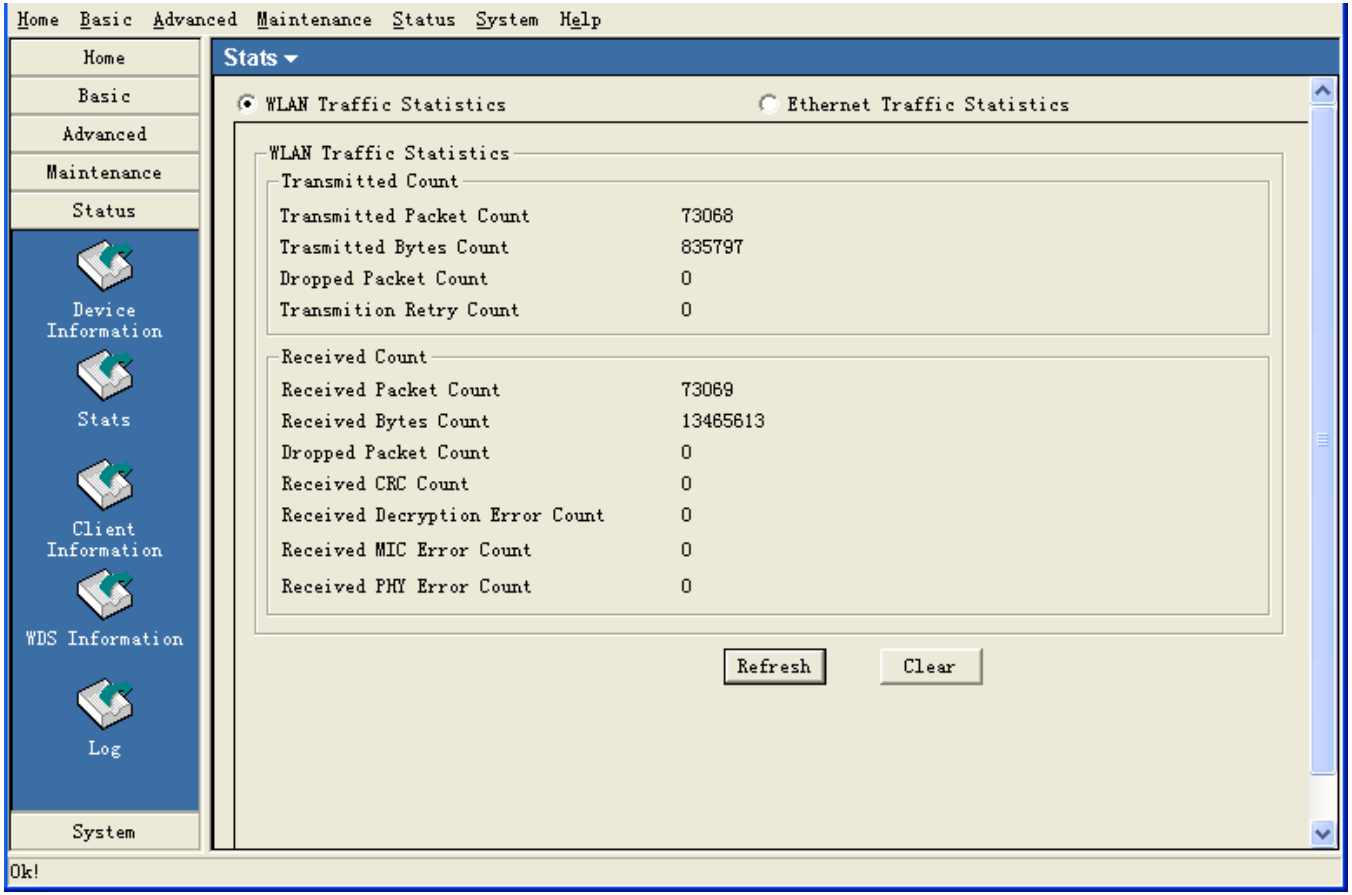
Status (802.11n)

Device Information



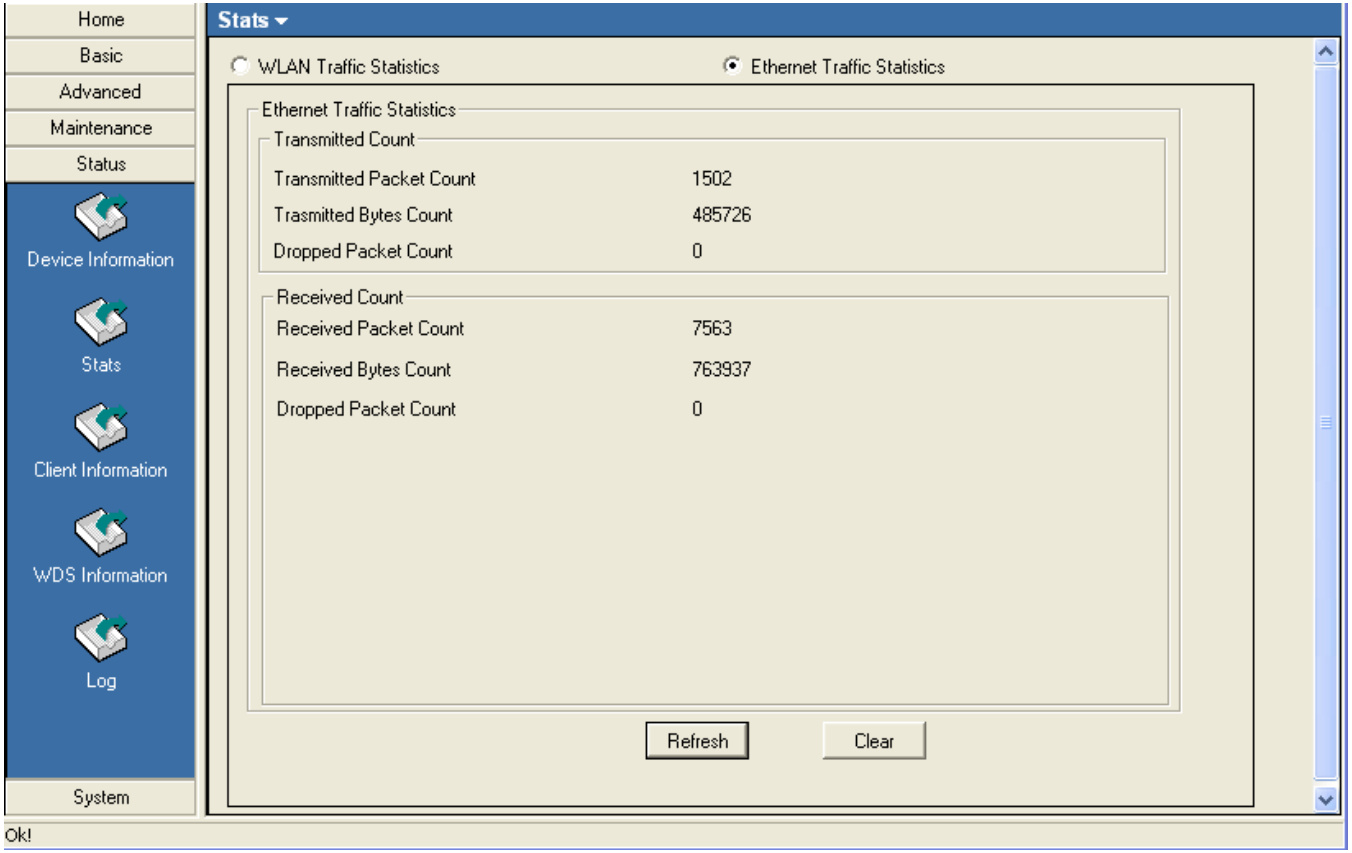
Device Information: This window displays the configuration settings of the AP, including the firmware version and device MAC address. It also displays WLAN information for either the 2.4GHz or the 5GHz wireless networks.

WLAN Traffic Statistics



WLAN Traffic Statistics: This page displays statistics for data throughput, transmitted and received frames for the wireless network.

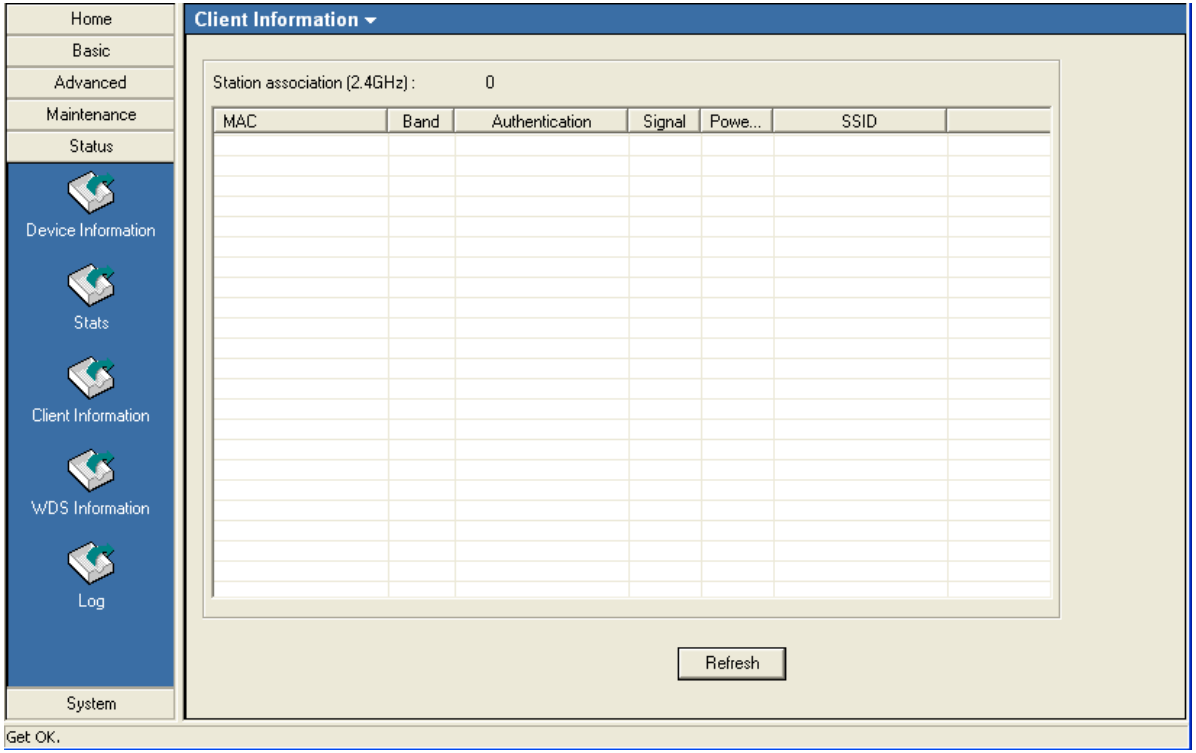
Ethernet Traffic Statistics



Ethernet Traffic Statistics: This page displays statistics for data throughput, transmitted and received frames for the Ethernet port of AP.

Client Information

This window displays the wireless client information for clients currently connected to the AP. The following information is available for each client communicating with the AP.



MAC: Displays the MAC address of the client.

Band: Displays the wireless band the client is connected on.

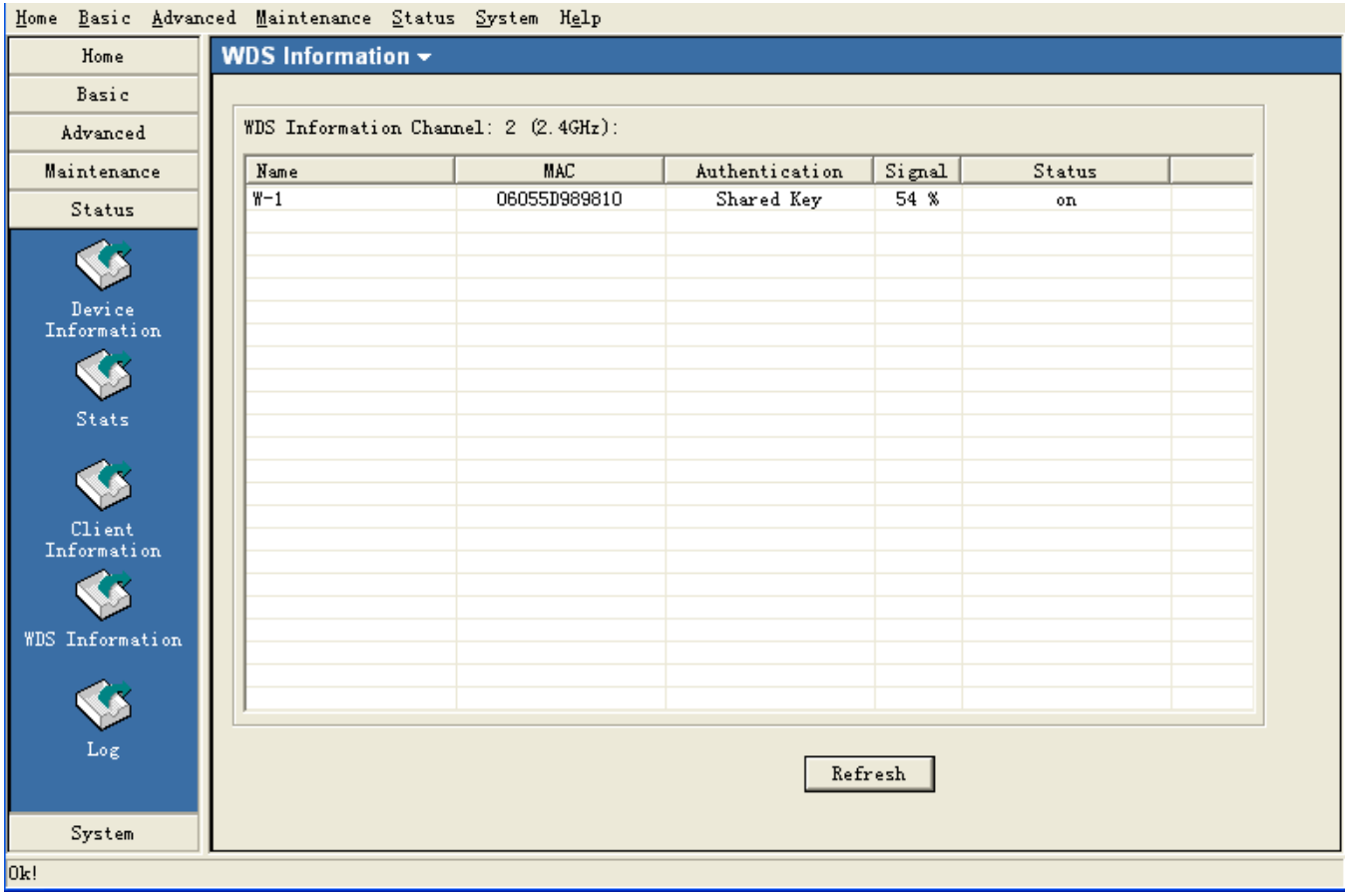
Authentication: Displays the type of authentication being used.

Signal: Displays the strength of the clients signal.

Power Saving Mode: Displays the status of the power saving feature.

SSID: Displays the SSID the client is connected to.

WDS Information



Name: Displays the name of the client.

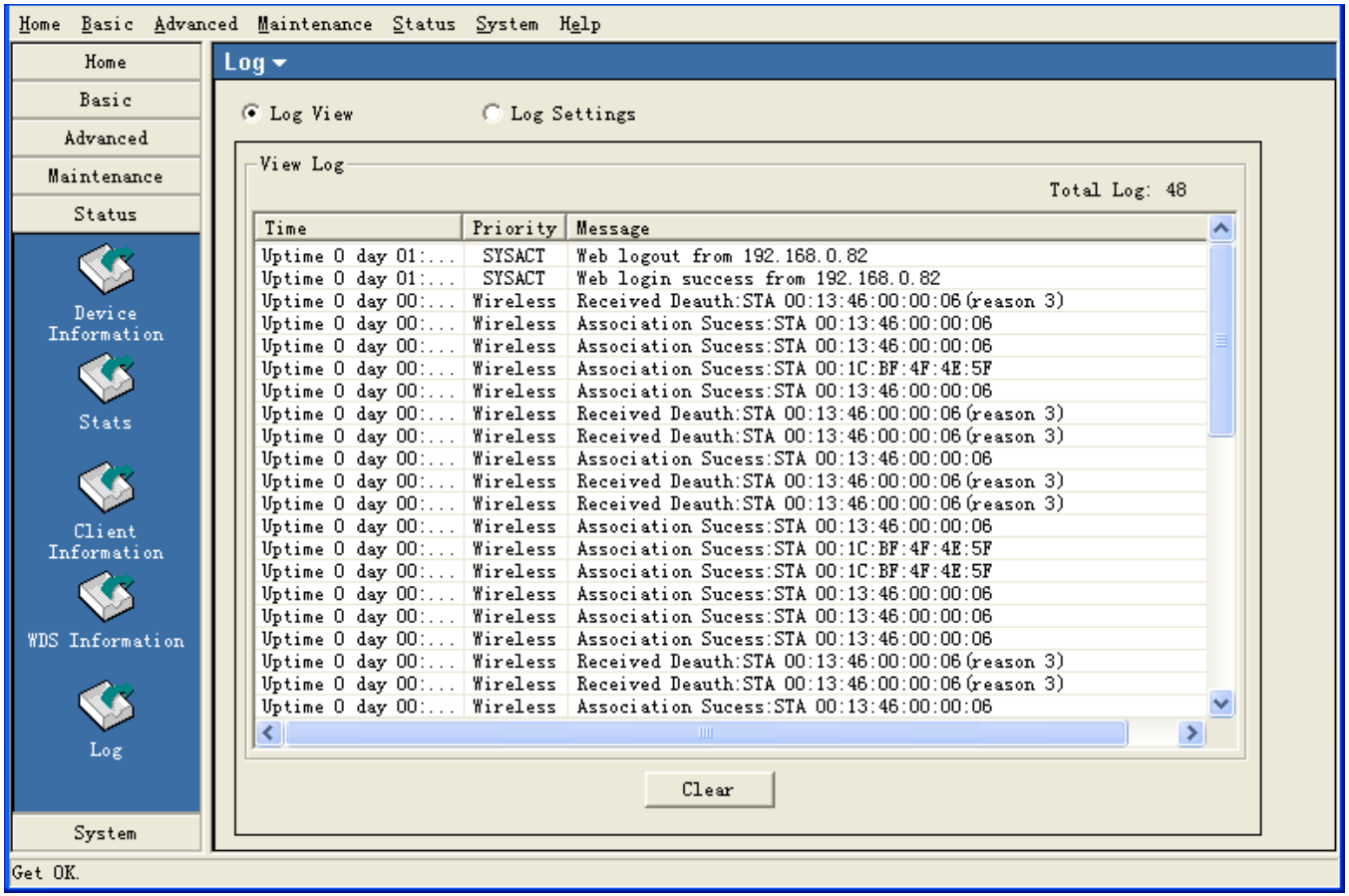
MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the strength of the clients signal.

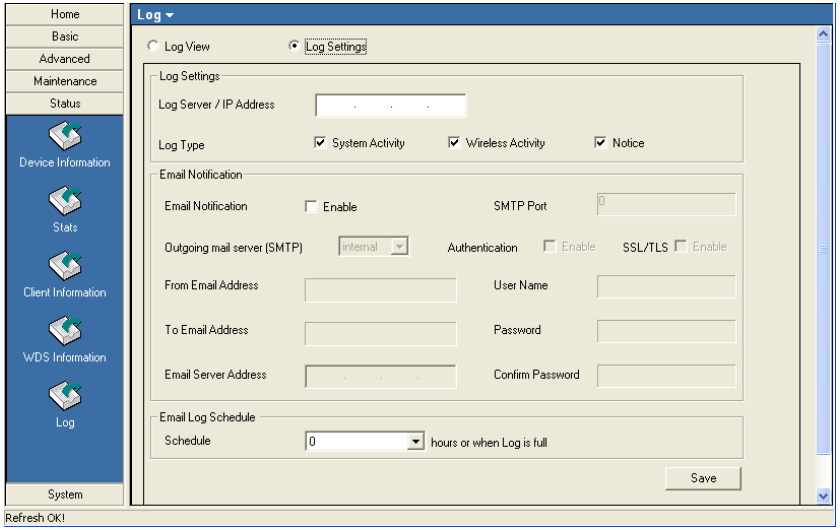
Status: Displays the status of the wireless.

Log View



View Log: The log displays system and network messages including a time stamp and message type.

Log Settings



Log Settings

Log Server / IP Address: Enter the IP address of the server you would like to send the AP log to.

Log Type: Check the box for the type of activity you want to log. There are three types: **System**, **Wireless** and **Notice**.

Email Notification

Email Notification: Check the box to enable email notification.

Outgoing mail server: Select the outgoing server type. There are three types: Internal, gmail, hotmail.

SMTP Port: Enter the SMTP port of the outgoing server.

From Email Address: Enter the e-mail address of the SMTP sender.

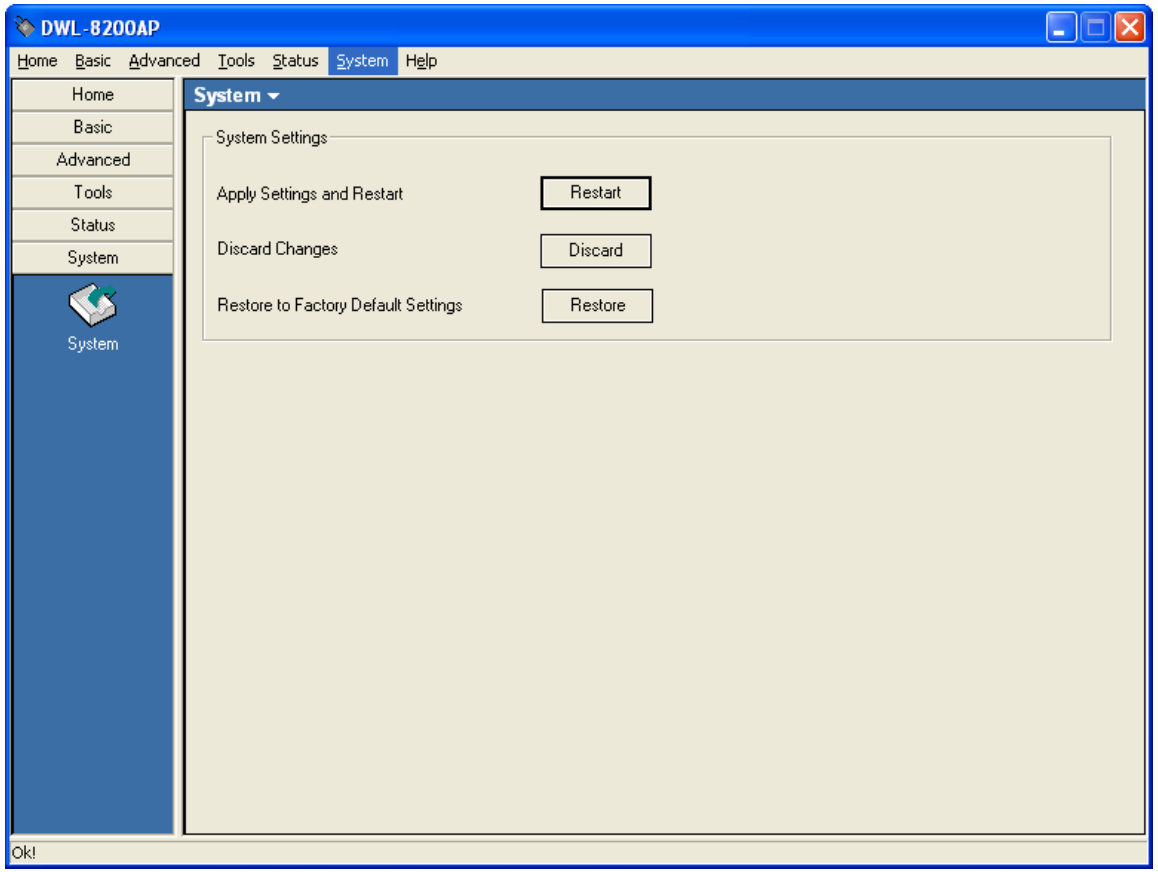
To Email Address: Enter the e-mail address of the SMTP recipient.

Username / Password: Enter the user name and password of the SMTP server.

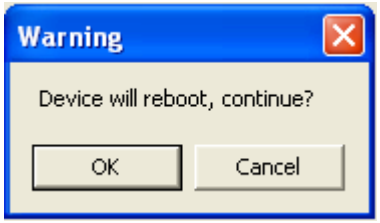
Email Server Address: Enter the IP address of the SMTP server.

Email Log Schedule: Select an interval time from drop-down list to send the logs to mail recipient.

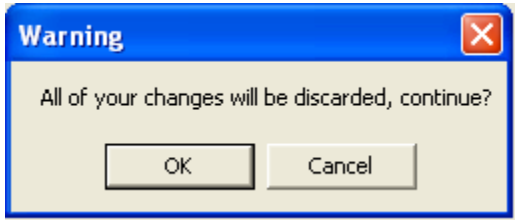
System



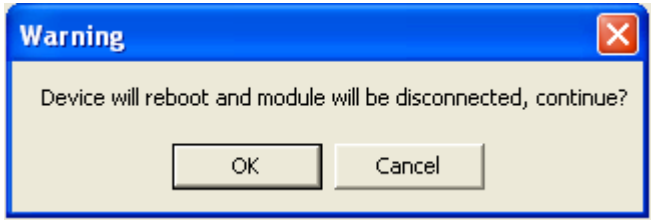
Click **Apply Settings and Restart** to restart the AP and save the configuration settings. You will receive the following prompt.



Click **Discard Changes** to cancel any changes made to the configuration settings. You will receive the following prompt.

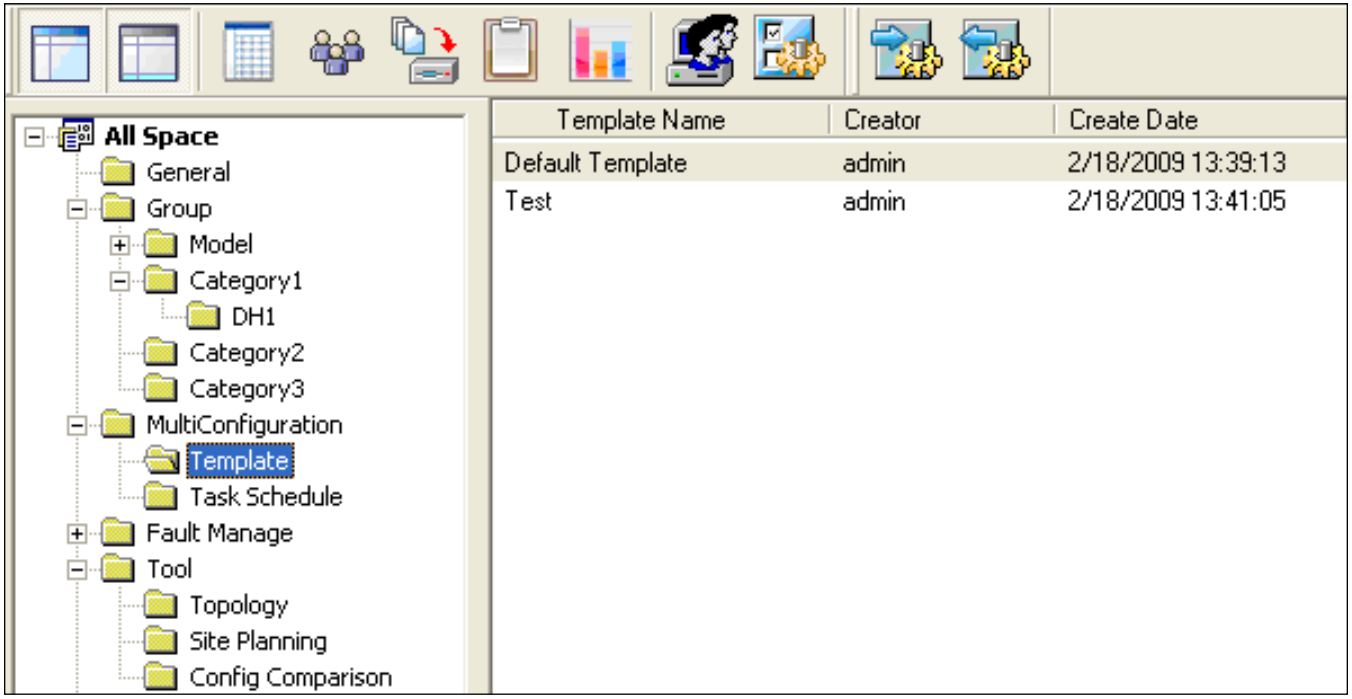


Click **Restore** to restore the AP back to factory default settings. You will receive the following prompt.



Multiconfiguration
Template

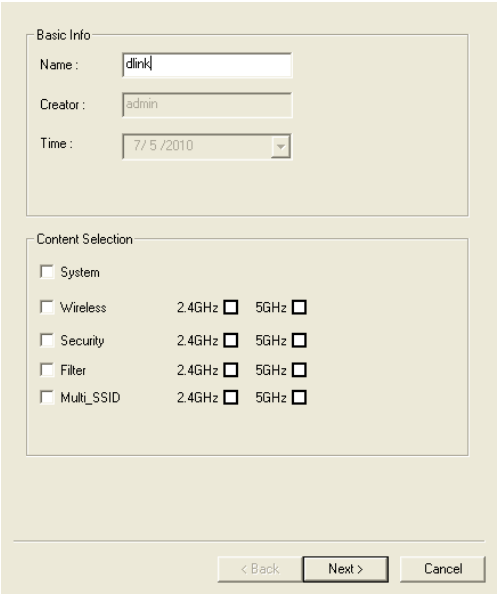
Administrators can manage the configuration of APs that AP Manager II has detected by using a template. The same profile can be used for multiple APs. Each template profile can has unique settings for the access point features which include System, Wireless, Security and Filter settings.



Create a New Template

To create a new template, right-click anywhere on the template view window and select the **New** item. Each of these items is described in the pages that follow:

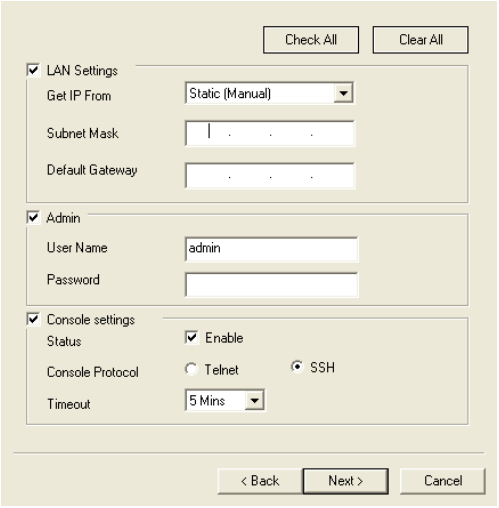
General



Basic Info: Enter a name for this template.

Content Selection: Check the box to select the configuration contents included in this template. Then configure the settings in the following page.

System



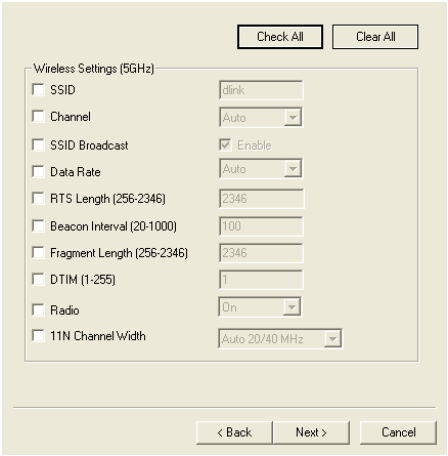
LAN Settings: Enter the IP settings for this template.

Admin: Check the box to select the configuration contents included in this template.

Console Settings: Then configure the settings in the following page.

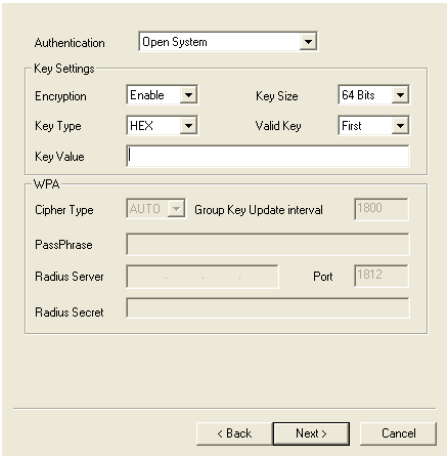
Wireless

Check the box to select the configuration contents included in this template.



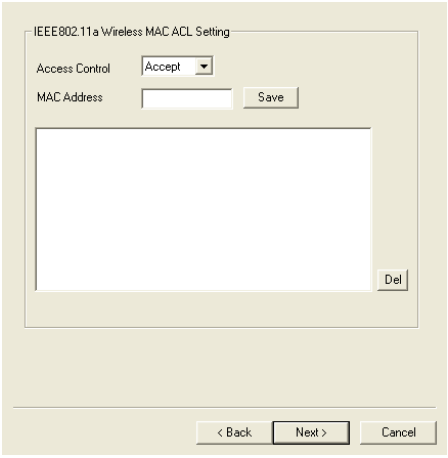
Security

Check the box to select the configuration contents included in this template.



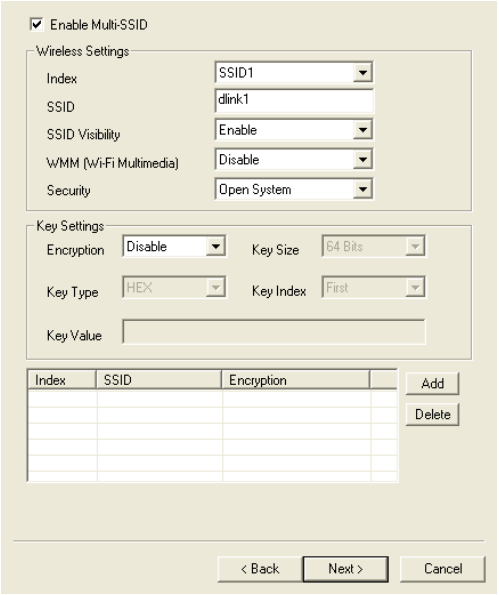
MAC Filter

Check the box to select the configuration contents included in this template.



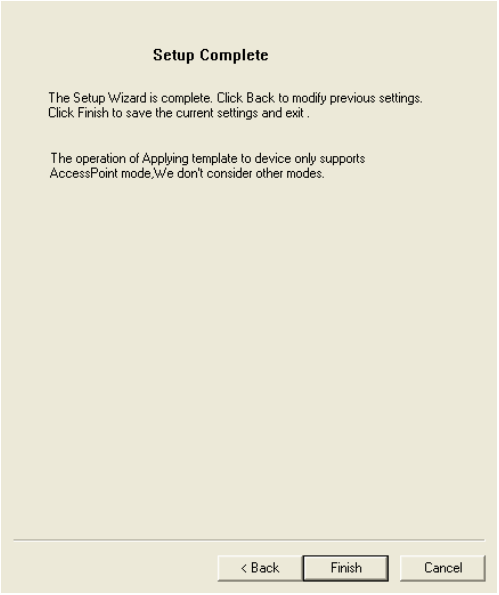
Multi-SSID

Check the box to select the configuration contents included in this template.



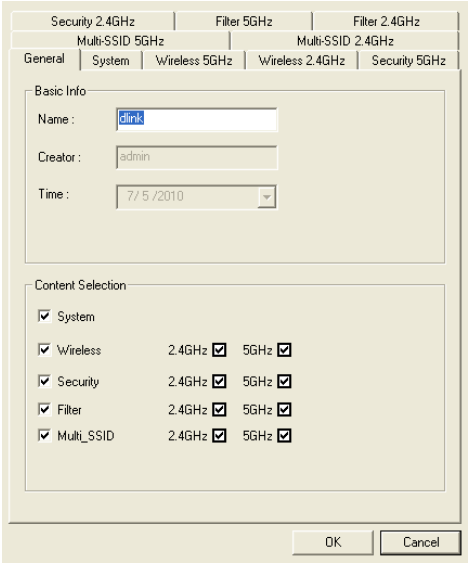
Setup Complete

Click the **Finish** button to complete the template.



Edit a Template

To edit a template, double-click the template or right-click the template and select **Edit** item from the drop-down menu, the configuration page shown as below.



Delete a Template

To delete an exit template, right-click the template, and select the Delete item from the drop-down menu.

Import or Export a Template

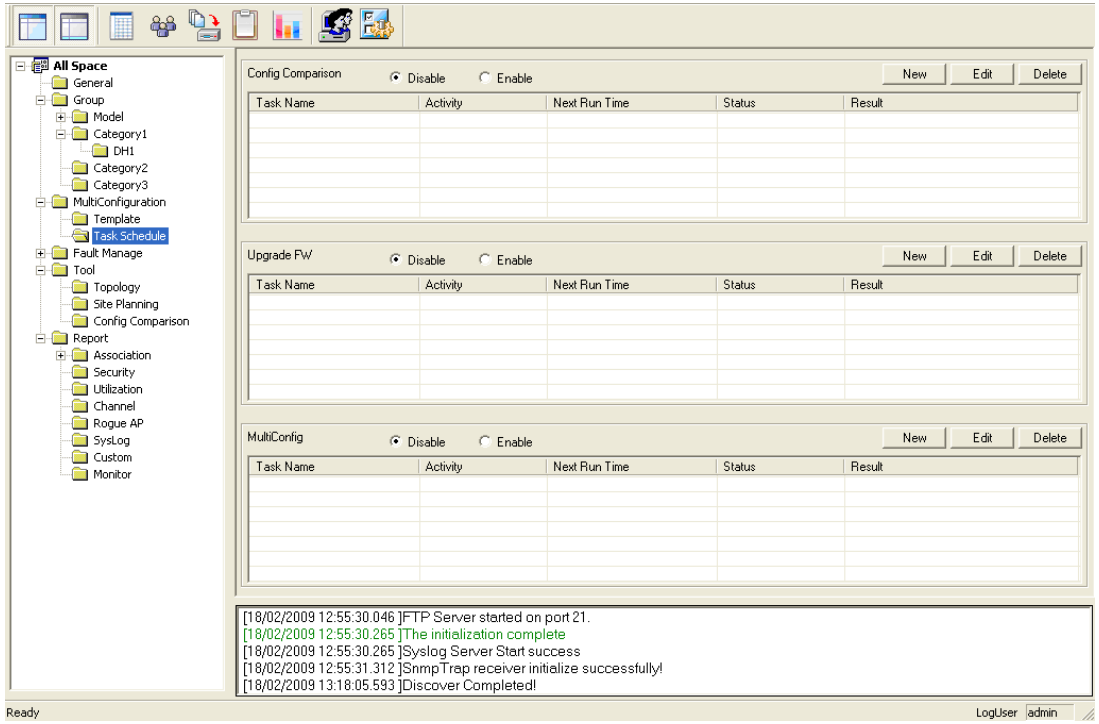
AP Manager II allows you to export the template to a profile saved in the disk or import a template from the profile.

To import a template profile, right-click anywhere on the **All Space** > **MultiConfiguration** view window, and select **Import** item from the drop-down menu or click the icon from the tools bar. Then select the template file in the opening window and click the **Open** button to import this template.

To export a template, right-click the template on the **All Space** > **MultiConfiguration** view window, and select **Export** item from the drop-down menu or click the icon from the tools bar. Then enter a profile name for this template in the File Name textbox and click the **Save** button to export the template to a file.

Task Schedule

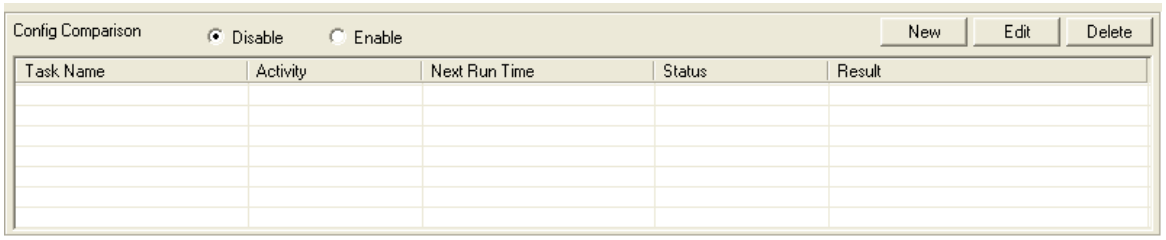
In this page, Administrator can compare the devices, upgrade the firmware and upload the template to device in batches



Each of these options is described in the pages as shown below.

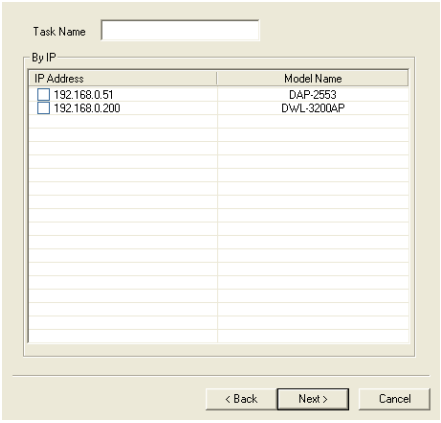
Config Comparison

You can compare the configurations of a template and AP to point out their differences, the steps shown as below.



Click the **New** button to open the following windows.

Device

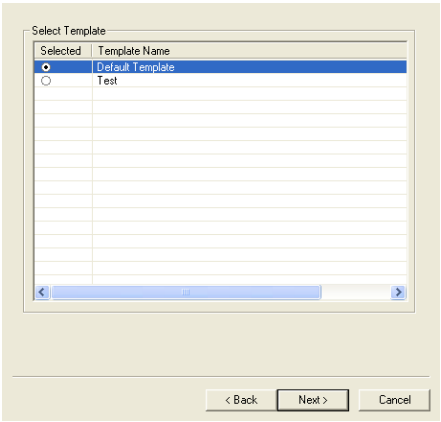


Task Name: Enter a string to describe the task.

By Group: Select the APs by group. The APs that belong to the group will apply the comparison.

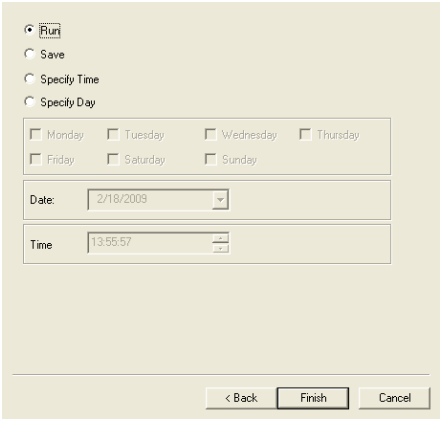
By IP: Select the APs by IP that will apply the comparison.

Select Template



Choose a template for comparing.

Schedule



Run: Compare the devices immediately.

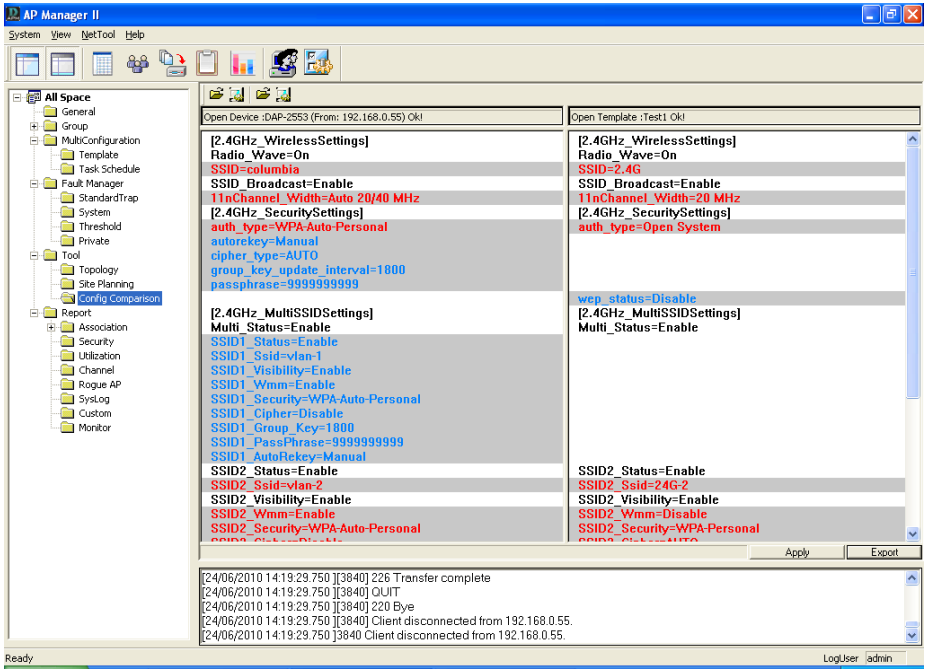
Save: Just save this comparison record.

Specify Time: Specify the day time that will apply the comparison. The comparison will run at certain day(s) of every week.

Specify Day: Specify the date that will apply the comparison. It only applies the comparison at a time.

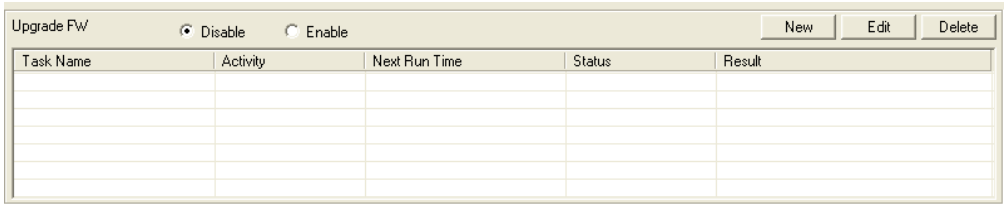
Enable Comparison

After establish the comparison record, highlight the record and then click **Enable** to implement the compare action. The results will show in a new window.



Upgrade Firmware

For all Access Points that the AP Manager II discovered, you can use this function to upload a new firmware file to devices in batches at a specified time, the steps shown as below.



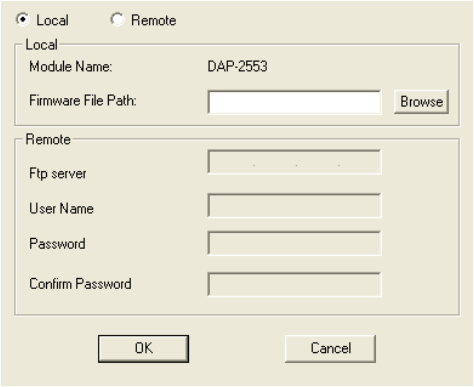
Click the **New** button to open the following windows.

Device

Task Name: Enter a string to describe the task.

By Group: Select the APs by group. The APs that belong to the group will upgrade their firmware.

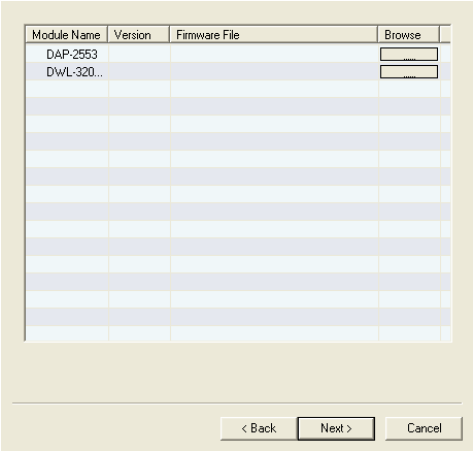
By IP: Select the APs by IP that will apply the firmware upgrade.



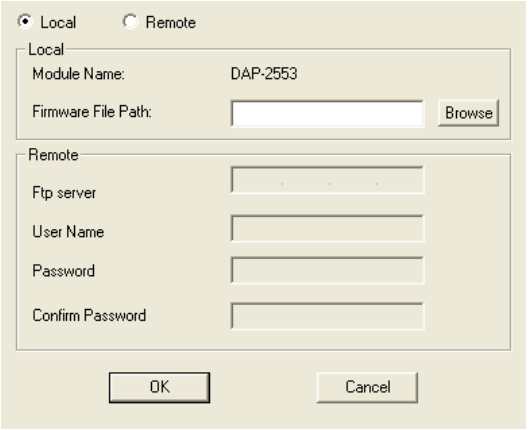
Firmware File Setting

Firmware File Setting: Double-click the module name to configure its firmware location.

Notification: Take this action when device's version is lower than the upgrading version.



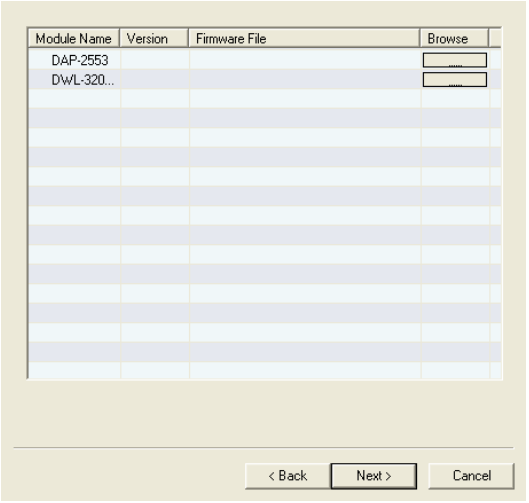
Firmware File Setting



Local: Select the update firmware file from the local hard drive.

Remote: Load the firmware from a remote ftp server. To implement this function, you need to type appropriate values in the Remote column.

Schedule



Run: Upgrade the firmware immediately.

Save: Just save this upgrade record.

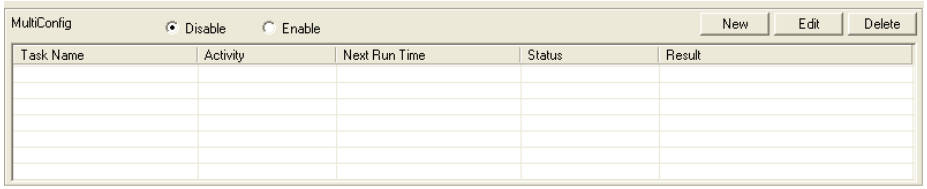
Specify Time: Specify the day time that will apply the upgrade. The upgrade action will run at certain day(s) of every week.

Specify Day: Specify the date that will apply the upgrade.

After establish the upgrade record, highlight the record and then click **Enable** to implement the firmware upgrade action.

MultiConfig

For all Access Points that the AP Manager II discovered, you can use this function to upload a previously created template to devices in batches at a specified time, the steps shown as below.



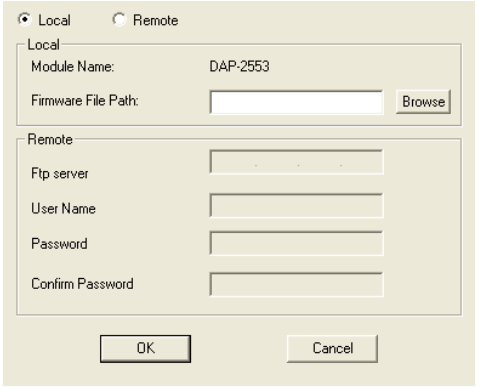
Click the **New** button to open the following windows.

Device

Task Name: Enter a string to describe the task.

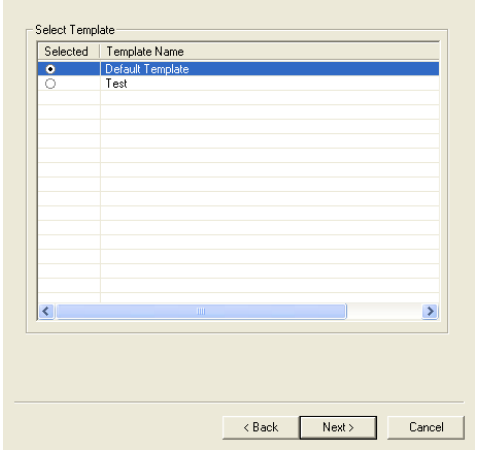
By Group: Select the APs by group. The APs that belong to the group will upgrade their firmware.

By IP: Select the APs by IP that will apply the firmware upgrade.



Select Template

Choose a template for uploading.



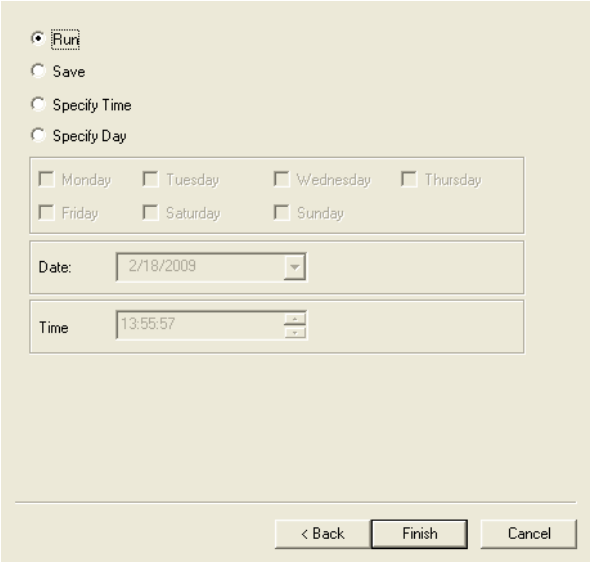
Schedule

Run: Upgrade the firmware immediately.

Save: Just save this upgrade record.

Specify Time: Specify the day time that will apply the upgrade. The upgrade action will run at certain day(s) of every week.

Specify Day: Specify the date that will apply the upgrade.

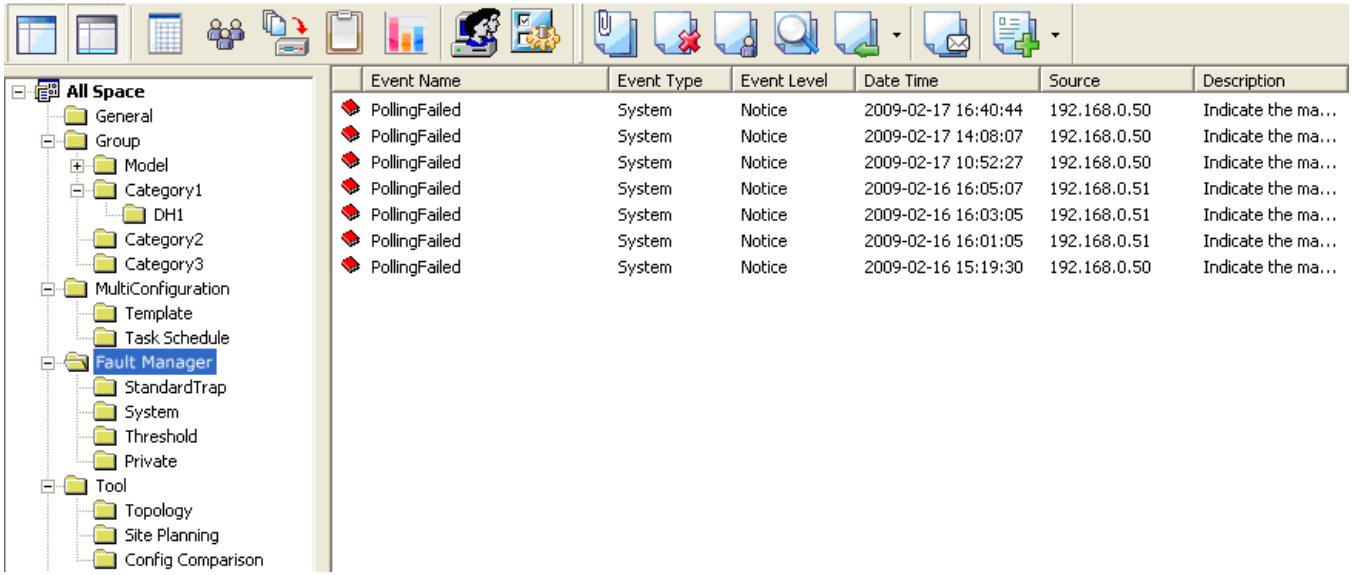


After establish the upload record, highlight the record and then click **Enable** to implement the configuration upload action.

```
[19/02/2009 14:00:40.705 ]SSID=3200
[19/02/2009 14:00:40.705 ]Show the Comparison result (different): end
[19/02/2009 14:10:12.798 ]Apply Config to Device
[19/02/2009 14:10:17.173 ]192.168.0.50  Apply Config file :Ok
[19/02/2009 14:10:17.173 ]Reboot Devices :192.168.0.50
```

Fault Manager

Fault Manager window shows the trap data received from AP and polling data.

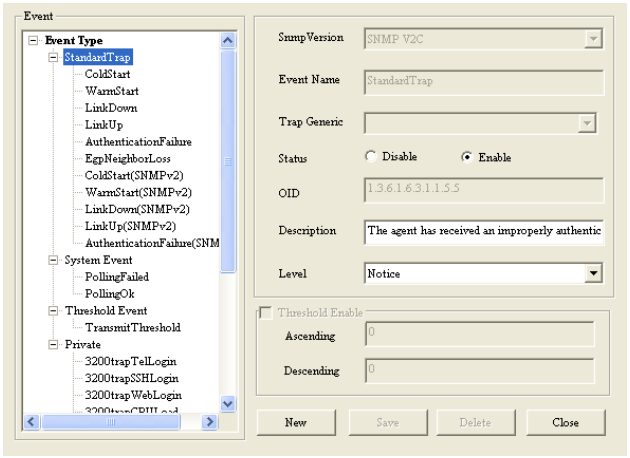


There are four types of events:

- **StandardTrap:** The standard trap view window displays the standard trap data received from APs.
- **System:** The system view window displays the polling results. To start the polling, please refer to page 116.
- **Threshold:** The Threshold view window displays the threshold notice data. To enable the threshold notice, please refer to page 116.
- **Private:** The Private view window displays the Private trap data received from APs.

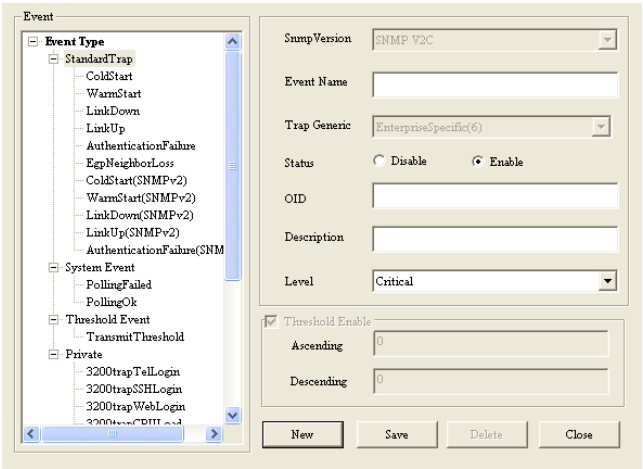
Event settings

To configure the trap condition, click the icon in the tool bar to set the event settings, as shown below.



To modify an event setting, select the event from the Event Type list and then change the items. After the setting, click **Save** button to apply the changes.

To add a new event, click **New** button, and configure the settings in the event creation window as shown below.

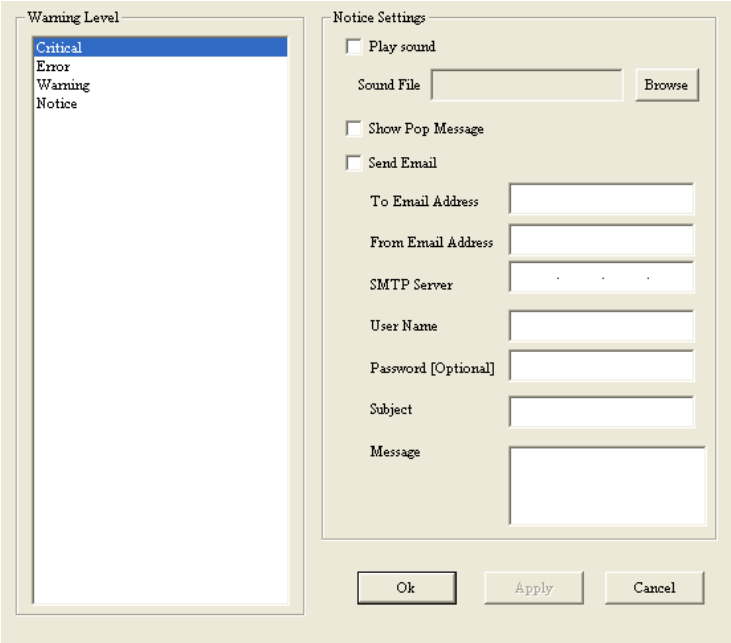


Event Export

AP Manager II can export the event results to the files in the format of Text/Excel/PDF. To save event results, highlight the event record in the event window and click the **Event Export icon** in the tools bar, then select the file format you want to save, AP Manager II will save all the records of that type to file.

Notice setting

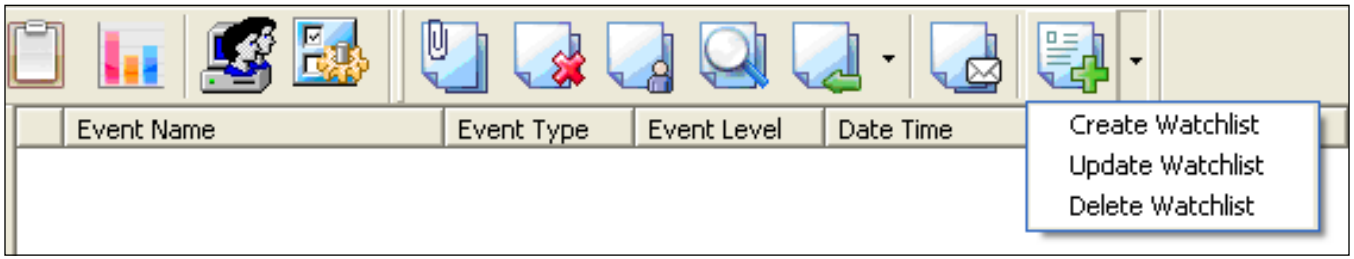
AP Manager II can set the corresponding actions when some level of events occurs. To configure the notice setting, click the **Notice Settings** icon in the tools bar, as shown below.



- **Play sound:** Click Browse to select the sound file. AP Manager II will play the sound file when this level of event occurs.
- **Show Pop Message:** AP Manager II will pop a message window when this level of event occurs.
- **Send Email:** Enter the Email information of To/From email address, SMTP server, User Name/Password [Optional], Subject and Message in the respective column. AP Manager II will send this email when this level of event occurs.

Watch List

AP manager II allows user to add custom watch list which only shows the specified devices and events.



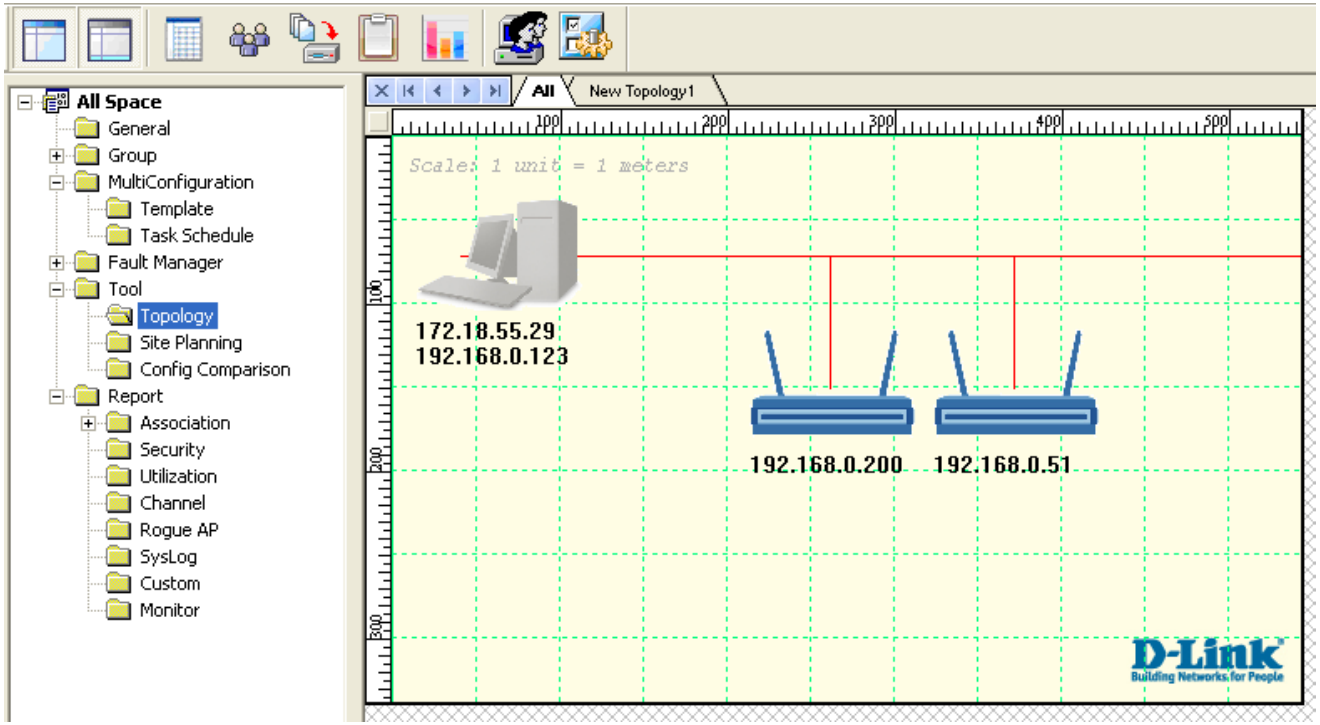
To create a watch list, please follow the steps below:

- Click the **Create Watchlist** item under the icon of the tools bar, and enter the Watch list Name in Create list form.
- Click the **Add** button to insert the events into event list, and select the events that need to be added in Select Event form, click the **Select** button, then click the **OK** button.
- Click the **Add** button to insert the devices into device list, and select the devices that need to be added in Select Device form, click the **Select** button, then click the **OK** button.

Note: The watch list name must be different from others; the event type of creating new event folder belongs to system event.
To delete a watch list, select the watch list item, and then click the **Delete watch list** item under the icon of the tools bar.

Tools
Topology

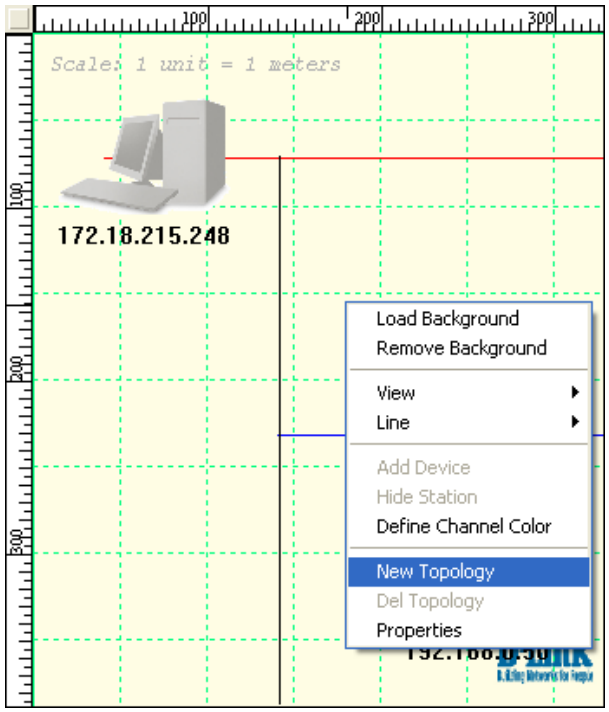
You can create a topology map to graphically represent planned or existing networks to aid network design, and also AP Manager II will periodically polling network devices to monitor the status. You can further customize their diagrams with selected icons and bitmap files used for the background. When a topology map is opened, AP Manager II will discover the devices connected on the network and display their icons on the map.



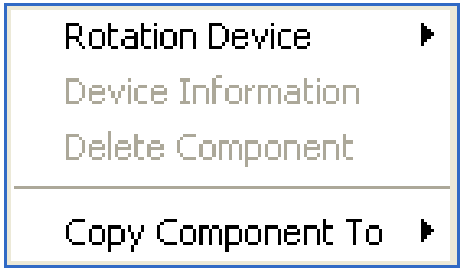
New Topology View

In the new topology, you can layout the APs according to the actual deployment. When an AP is failed, the administrator has a visual sight of which AP is failed, and substitutes it quickly.

To create a new topology view, right-click the blank place of the Topology view window and select New Topology item, as shown below.

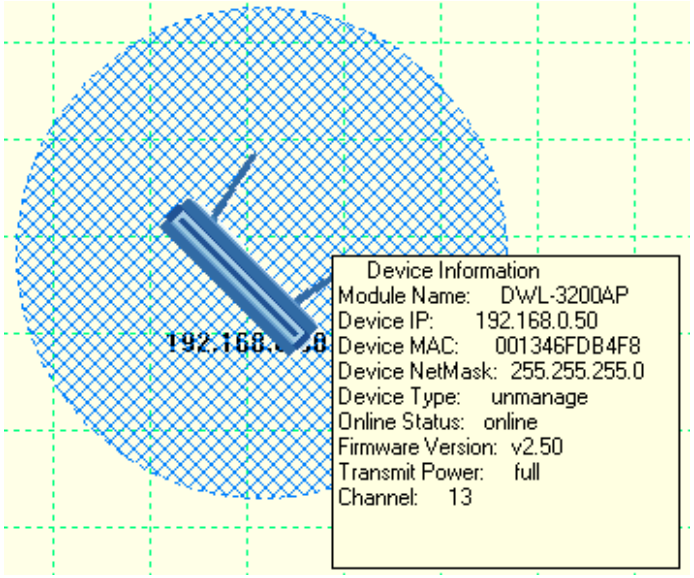


Firstly, you should import APs into the new topology by right-clicking the APs in the All topology view window and selecting the new topology under the Copy Component To item, as shown below.

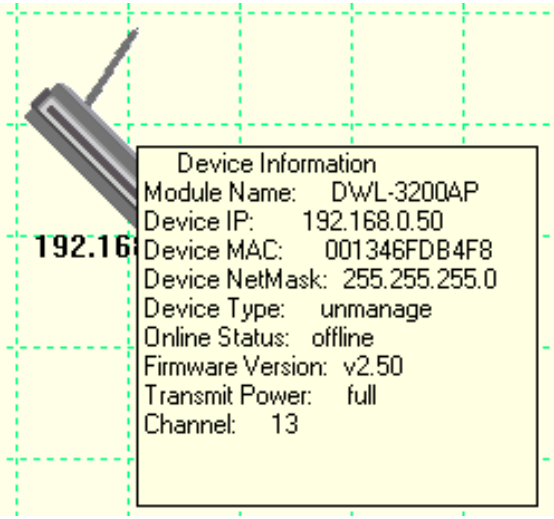


Show RF Range

The new topology view displays the device's RF range. RF range is based on the transmit power, and its color is related to the channel.

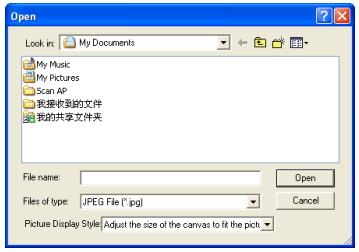


If AP is power off, it doesn't show the RF range.

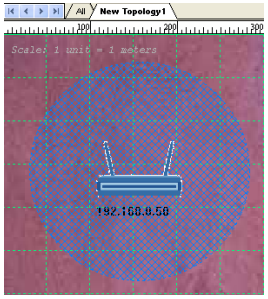


Background

To load a background for the new topology, right-click the blank place of the Topology view window and click the Load Background item.



After the successful loading:



To remove the background, right-click the blank place of the Topology view window and select Remove Background item.

View

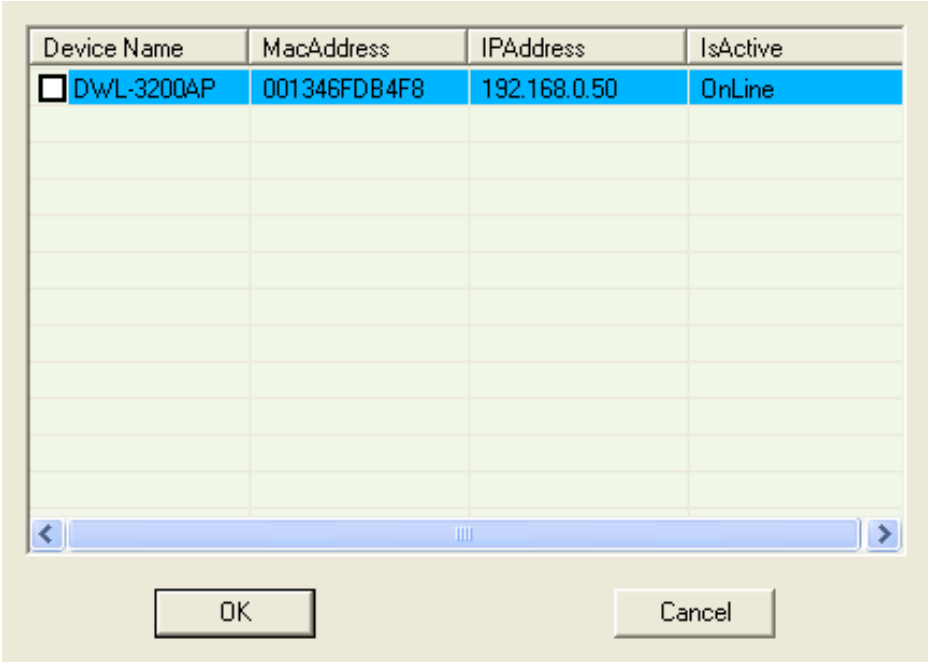
The view option provides the functions of showing the grid and ruler in topology configuring the size of topology, and displaying the AP with small or large icon. To show/hide the grid and ruler, click Grid or Ruler item from the right-click menu. To change the topology size and display ratio, click Topology Size item from the right-click menu, as shown below.

Line

You can insert lines into map to organize the APs more efficiently. To insert a line, click the Insert line item from the Line option of right-click menu, and use the mouse point to paint a line in the map. After insert a line, you can delete line/set line color/set line width/hide line by right-clicking the line and then select the corresponding item from the drop-down menu.

Add/Hide Device

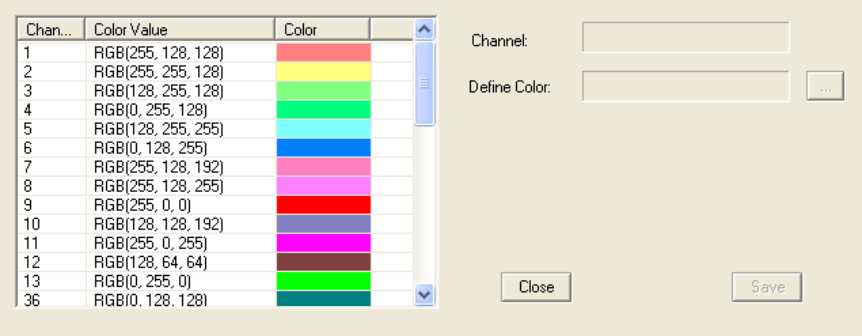
You can add station to the map by click Add Device item from the right-click menu, the window shown as below.



To hide a device in the topology view, right-click the device and then select Hide Device item from the drop-down menu.

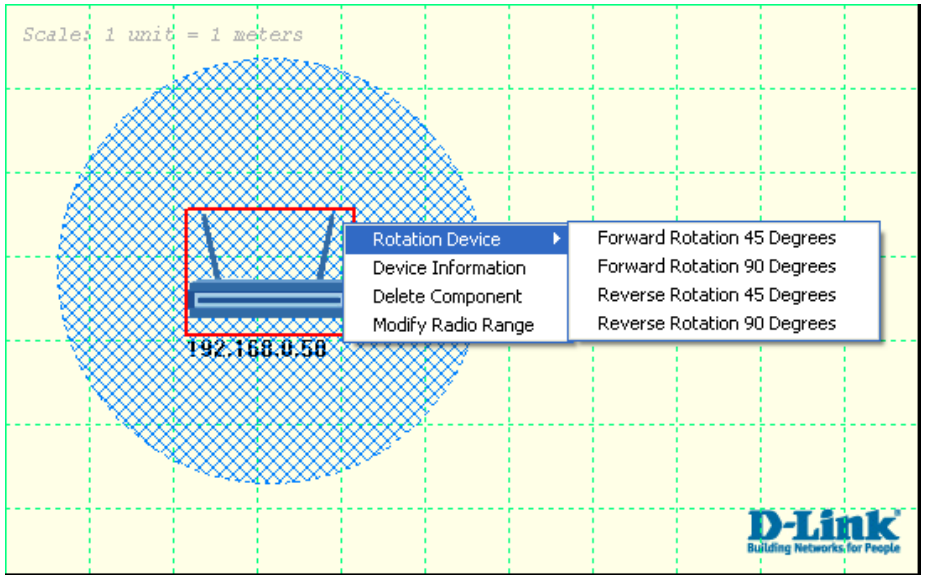
Define Channel Color

The topology view can show the channel in different colors. To set channel color, click Define Channel Color item from the right-click menu, the window shown as below.

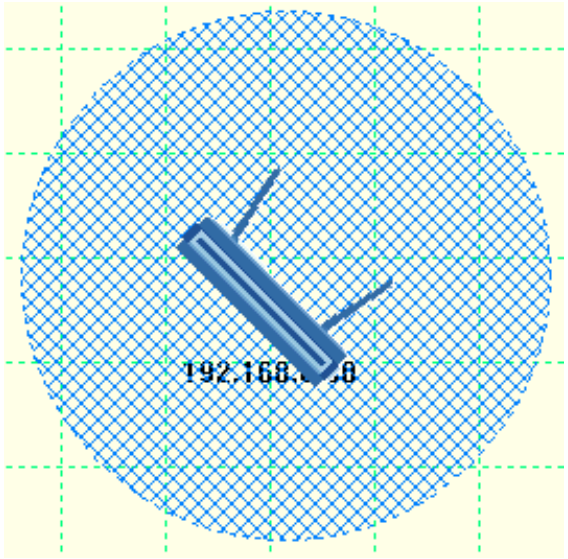


Rotation Device

You can change the device angle by right-clicking the device, the window shown as below.



To rotate the device at 45 degree clockwise, click Forward Rotation 45 Degrees item from Rotation Device option, shown as below.

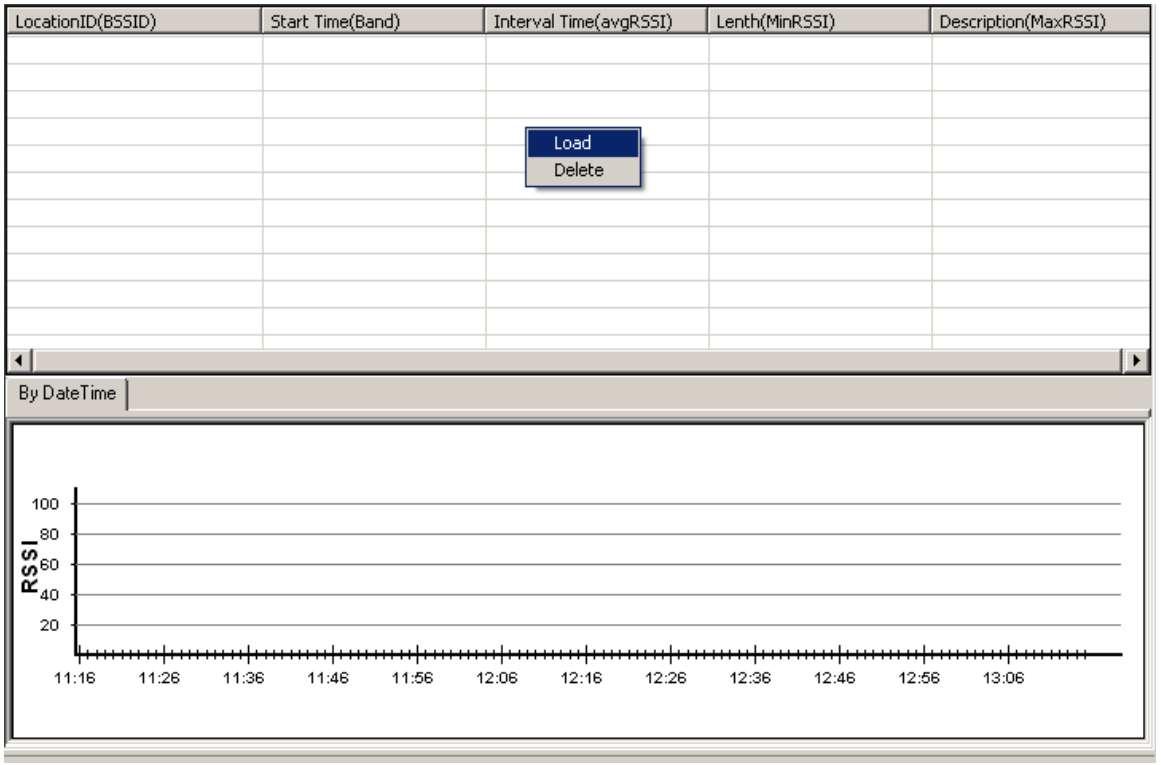


Site Planning

The Site Planning is designed to help user to layout the wireless network. Before establishing a wireless network, user needs to plan and evaluate at first. Normally, user locates some APs in the different places, and uses a notebook computer running scan AP program to test which places can reach the highest radio effort. After record the data, they can be import into AP Manager II for analyzing.

To run the scan AP program in a notebook computer, copy the ScanAP.exe from the installation directory of AP Manager II of the computer which has been installed AP Manager II to notebook and then double click ScanAP.exe.

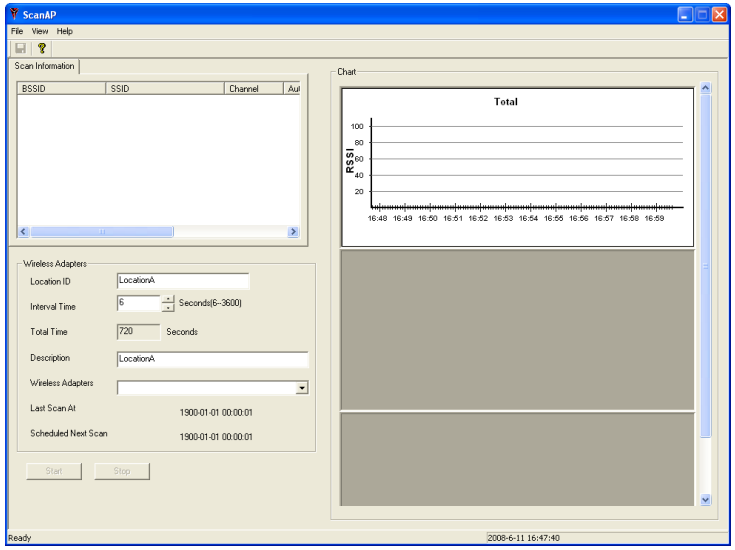
The Site Planning shows the results that tested by scan AP tool. Please first run the ScanAP.exe and save the scan result into the file and then right-click the Site Planning view window to load the file.



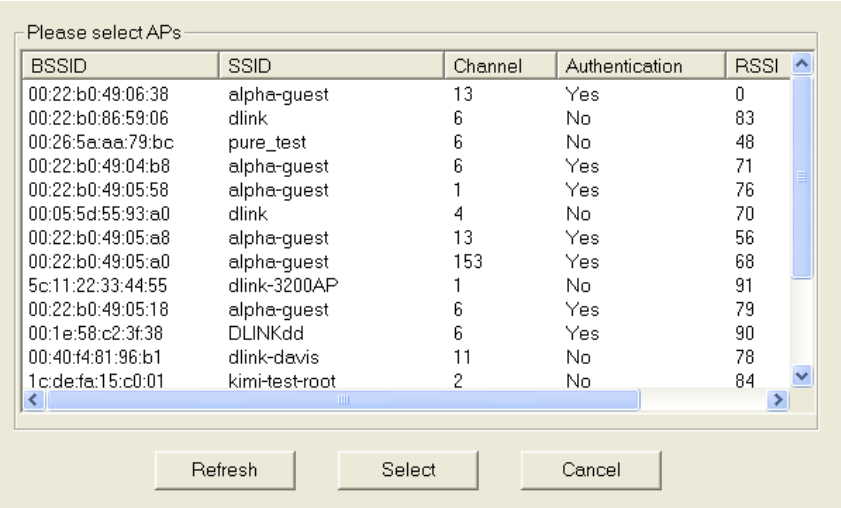
The Site Planning window shows BSSID, Start Time, Interval Time, Length, Description data of the site planning results.

Collect information

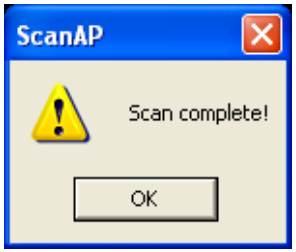
To collect the AP's RF information, please click the Scan item under the Tools menu or double click scanAP.exe in the notebook, the scanning program will run, as shown below.



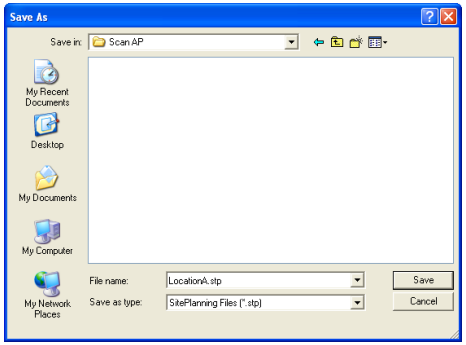
Enter the Location ID, Description, and select the interval Time and wireless adapter, and then click the Start button. At first, you must select target AP, as shown below.



Then ScanAP will start to collect the AP's RF information. The scan information table shows any information in details. When the scanning finished, the window shows:



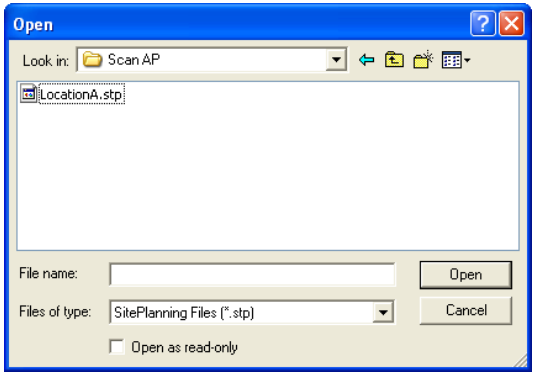
When you scan again or close the ScanAP, it prompts to save the information into disk:



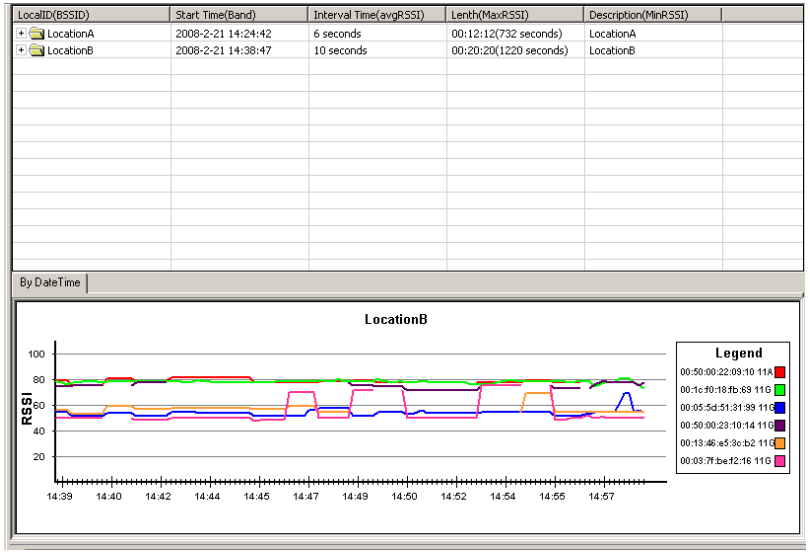
Note: ScanAP can run on the laptop computer singly.

Load information

To load the result file into Site Planning application, click the Load button from the Site Planning window, as shown below.



Select the scanning result file. AP Manager II shows the data in line by time, as shown below.



Click the + icon front the scanning record to expand the item and view the details.

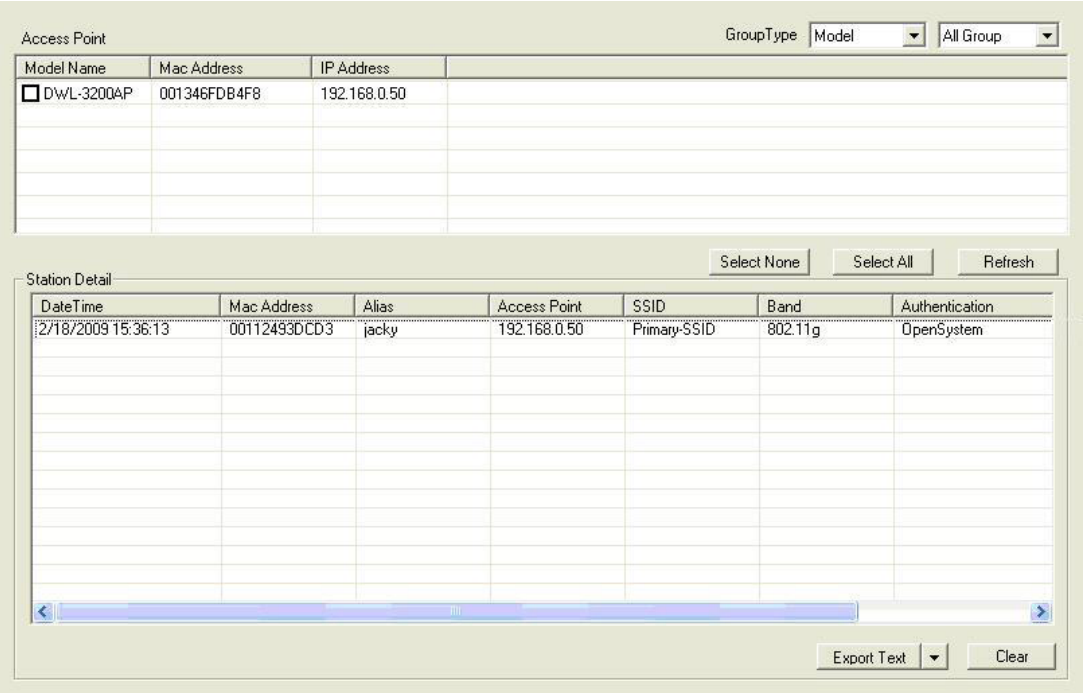
Report

Association

The association window shows managed APs and their associated client stations in two ways – By Access Point and By Wireless Station.

By Access Point

Highlight an Access Point and the details of client stations that associated with the AP list. The detail information includes, DateTime, MAC Address, Alias, Access Point, SSID, Band, Authentication, RSSI and Power save mode.

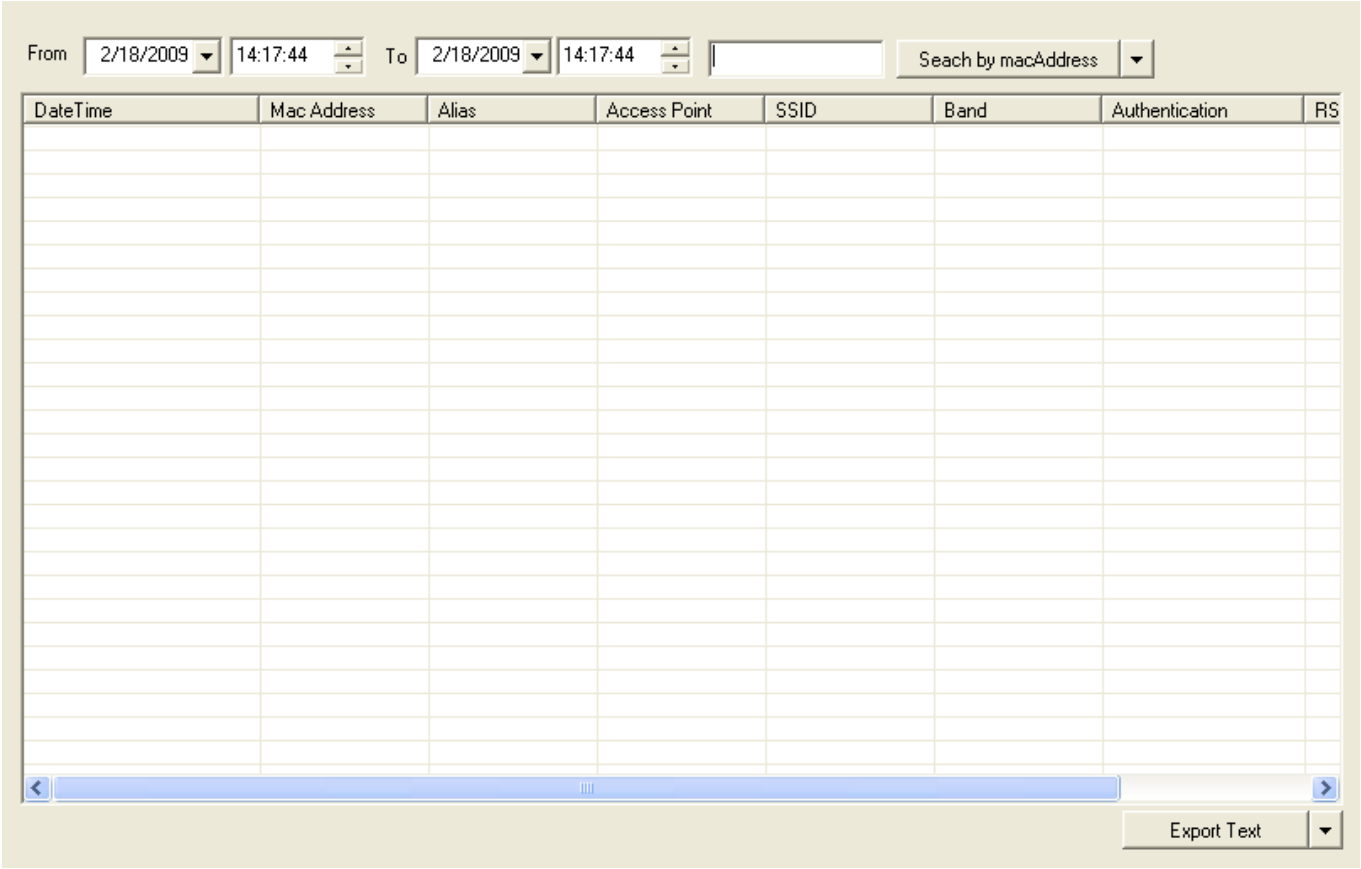


From the **Group Type**, you can specify that the window show the data according to specified model or group.

To export the AP data to file, click a file type from the **Export Text** drop-down menu or click the Export Text button, and then enter a file name in the Export window, click the **Save** button to save the AP data.

By Wireless Station

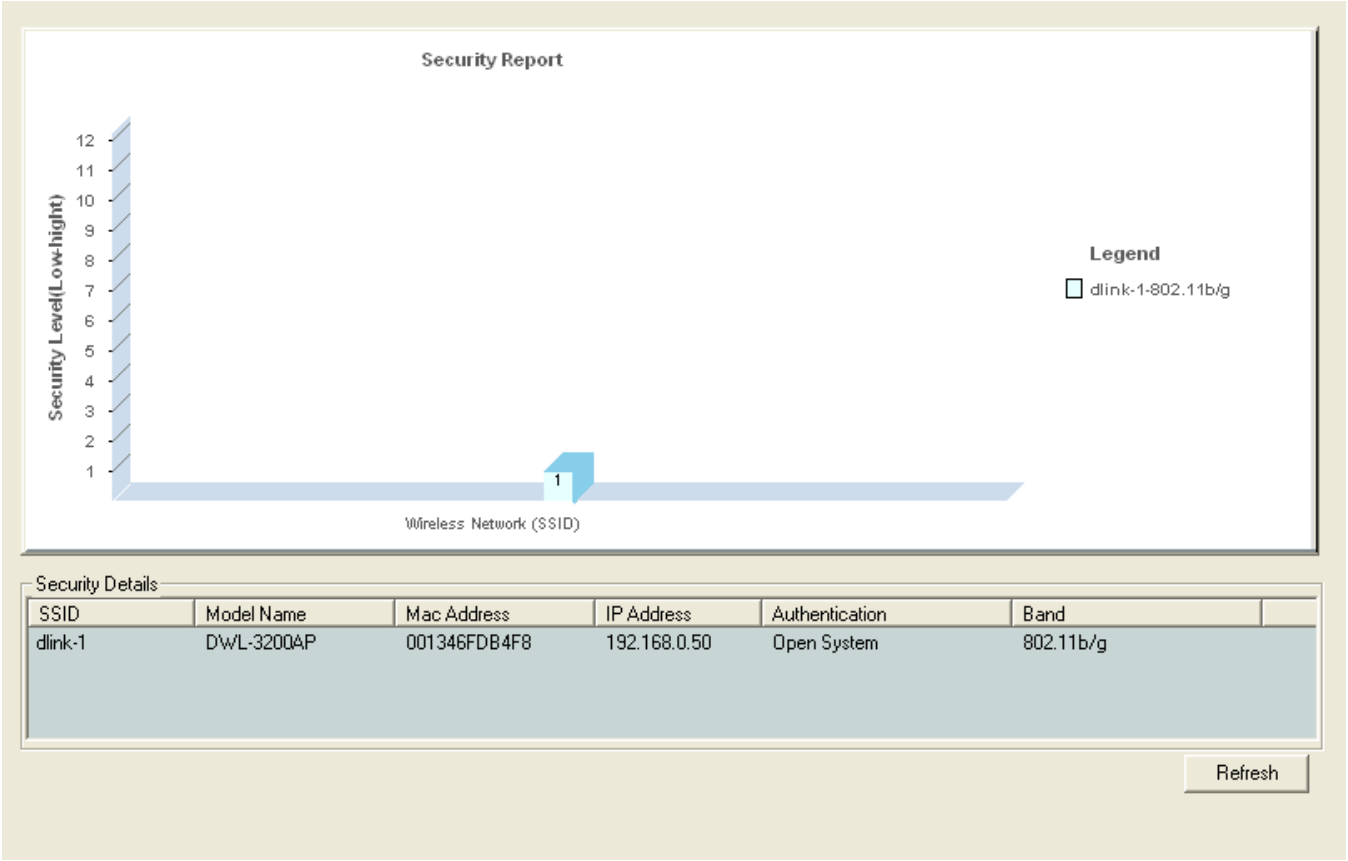
To list the APs according to the specified station and detected date, choose the date range from **From/To** drop-down menu, and type Mac address or alias of the device, then click **Search By …** button.



To export the AP data to file, click a file type from the **Export Text** drop-down menu or click the **Export Text** button, and then enter a file name in the Export window, click the **Save** button to save the AP data.

Security

The security window graphically lists the security level of the managed APs.

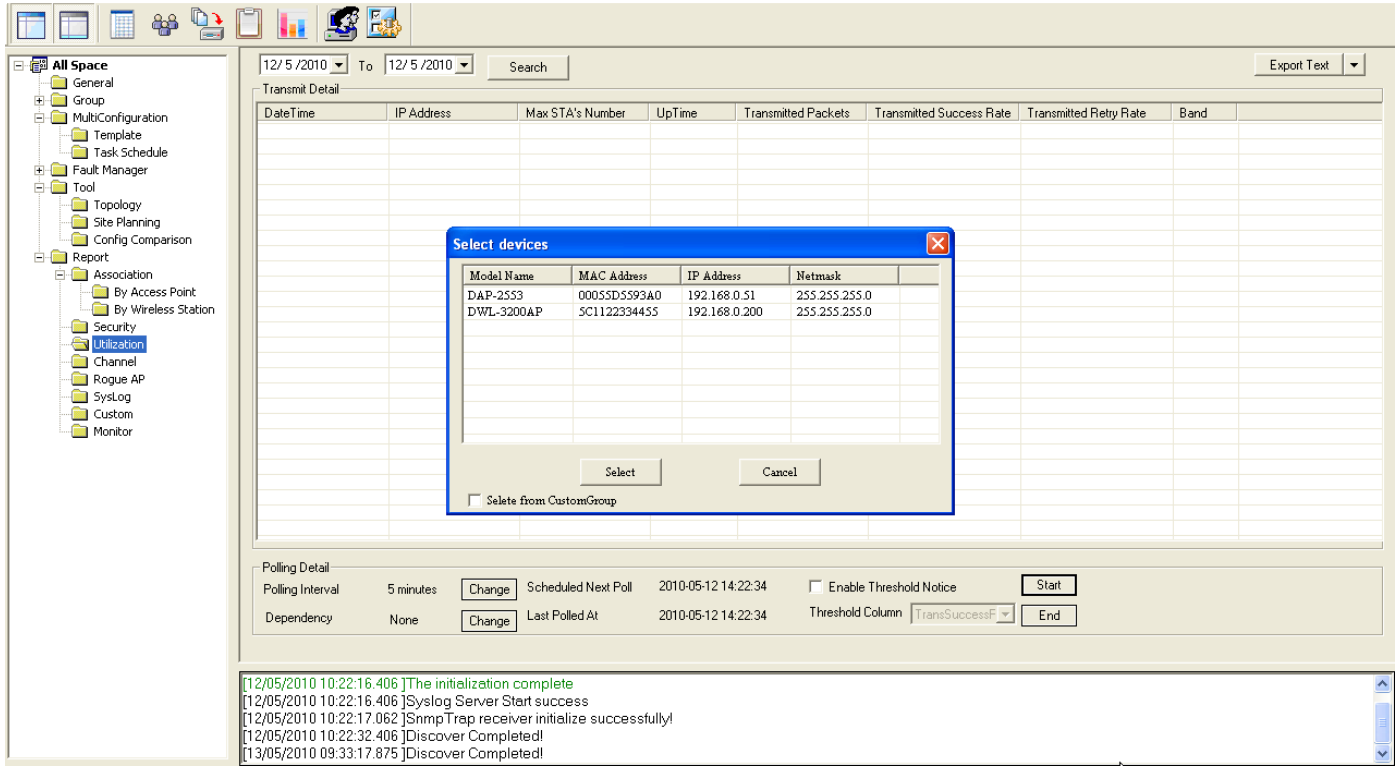


The security levels from the lowest to highest are: **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, **WPA2-Personal**, and **WPA2-Enterprise**.

The security details window shows the **SSID**, **Mode Name**, **MAC Address**, **IP Address**, **Authentication**, and **Band** information of APs.

Utilization

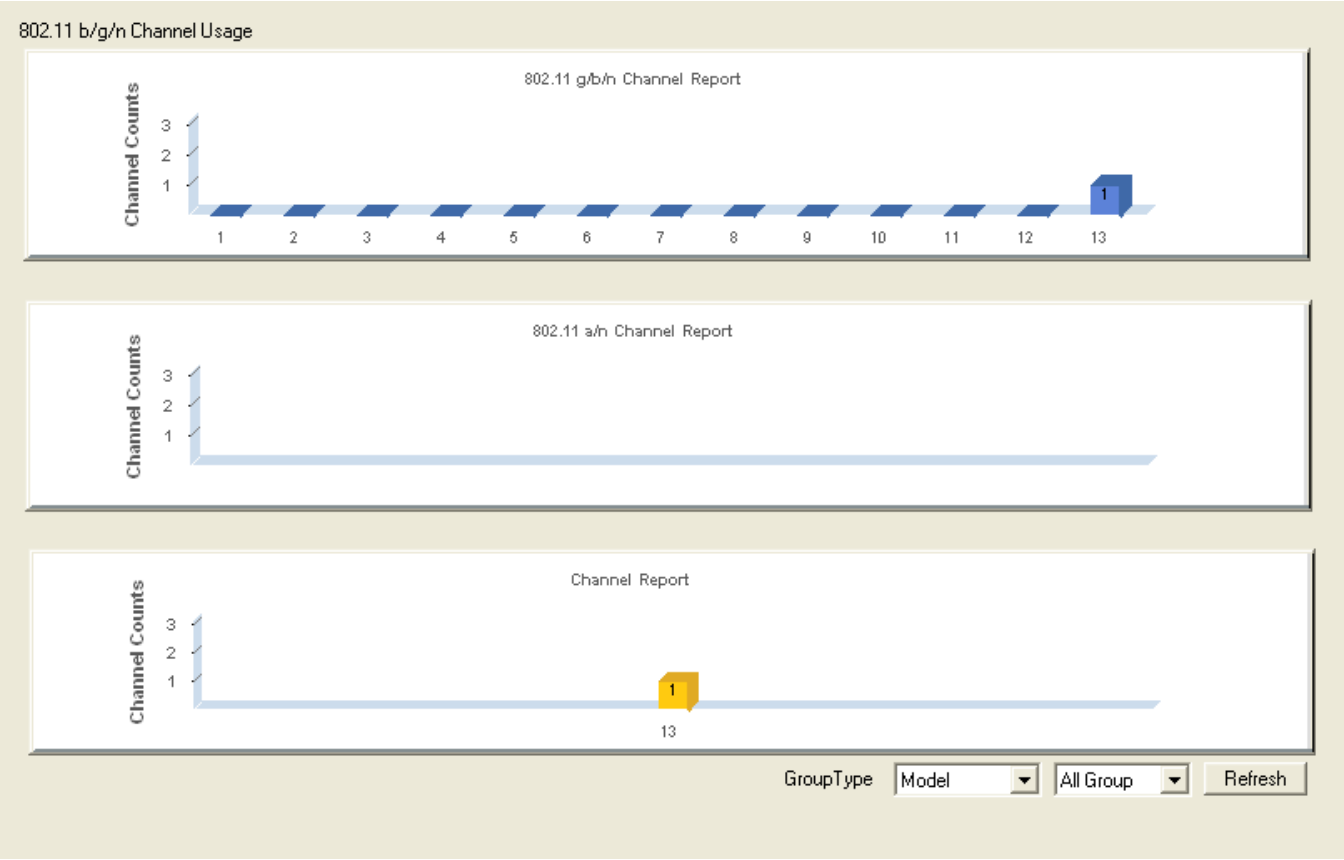
Utilization window shows the band usage of specified APs. To show the usage, AP Manager II should poll the APs.



To start the polling, you should select the APs that AP Manager II will polling from the **Select** window by clicking the **Change** button of **Dependency** and then click **Start** button. You can also enable the threshold notice by clicking the **Enable Threshold Notice** and select the type of **Threshold Column**.

Channel

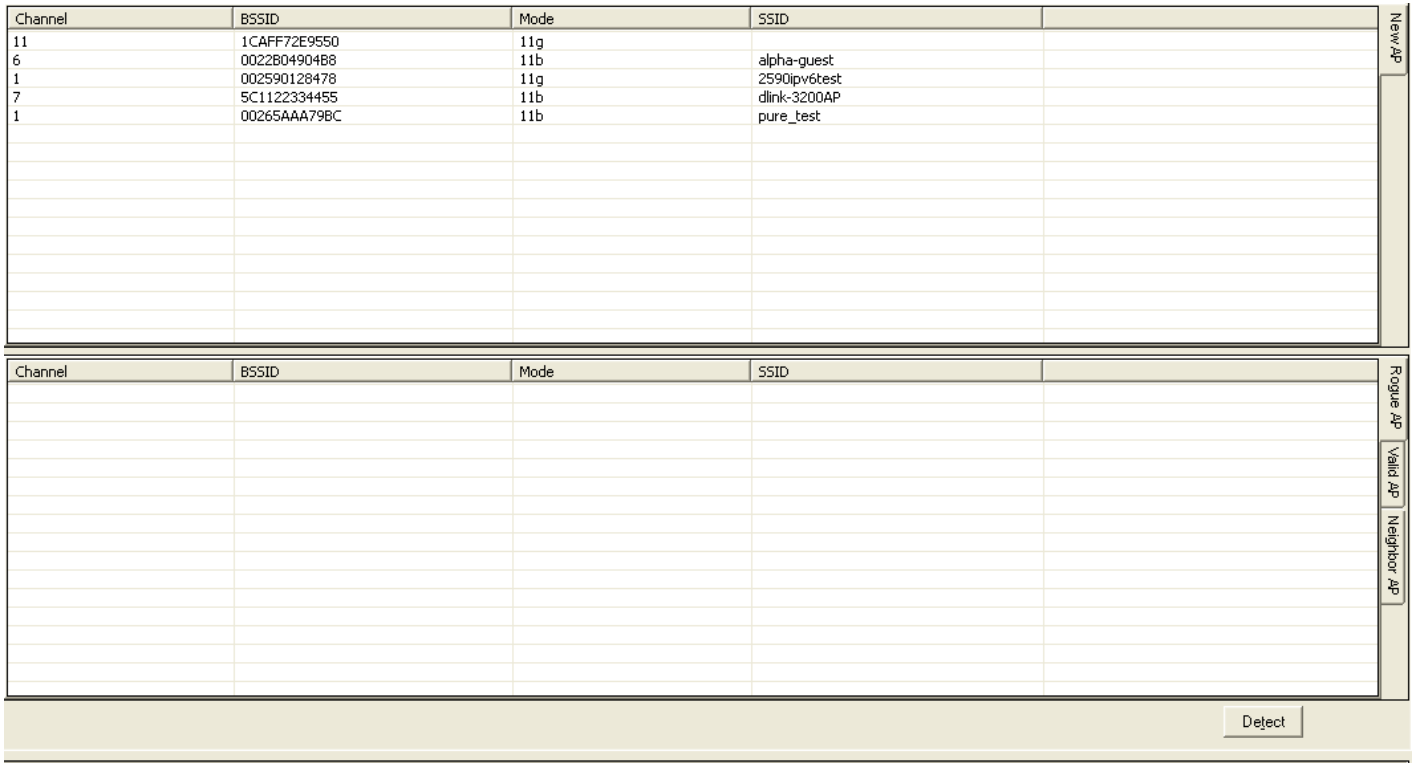
The channel window graphically lists the channel usage of the managed APs.



From the Group Type, you can specify that the graph shows the data according to specified model or group.

Rogue AP

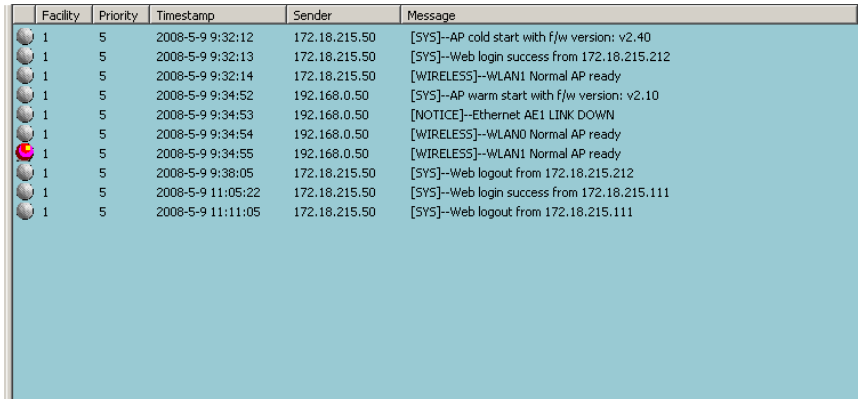
The rogue AP window lists the APs scanned by AP Manager II. You can specify which AP is valid, rogue or neighbor AP.



To categorize the APs, click the **Detect** button to scan the APs around, and click the category at the right side of window, then drag the AP from top window to bottom window.

Syslog

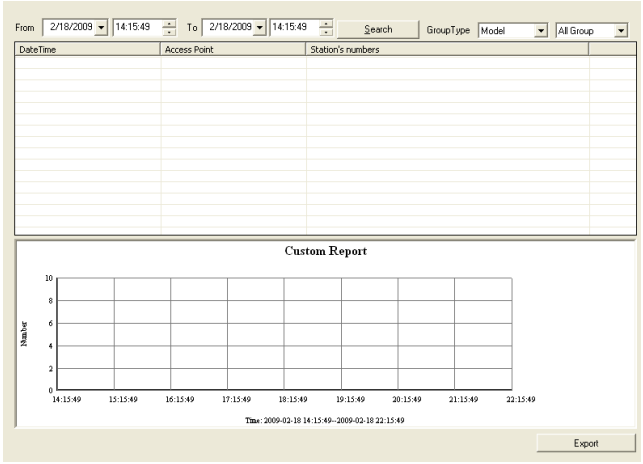
The syslog window shows the system log information sent by the managed APs. Please configure the APs to send the syslog to AP Manager II first, for how to configure the log setting of AP, refer to page 80.



Facility	Priority	Timestamp	Sender	Message
1	5	2008-5-9 9:32:12	172.18.215.50	[SYS]--AP cold start with f/w version: v2.40
1	5	2008-5-9 9:32:13	172.18.215.50	[SYS]--Web login success from 172.18.215.212
1	5	2008-5-9 9:32:14	172.18.215.50	[WIRELESS]--WLAN1 Normal AP ready
1	5	2008-5-9 9:34:52	192.168.0.50	[SYS]--AP warm start with f/w version: v2.10
1	5	2008-5-9 9:34:53	192.168.0.50	[NOTICE]--Ethernet AE1 LINK DOWN
1	5	2008-5-9 9:34:54	192.168.0.50	[WIRELESS]--WLAN0 Normal AP ready
1	5	2008-5-9 9:34:55	192.168.0.50	[WIRELESS]--WLAN1 Normal AP ready
1	5	2008-5-9 9:38:05	172.18.215.50	[SYS]--Web logout from 172.18.215.212
1	5	2008-5-9 11:05:22	172.18.215.50	[SYS]--Web login success from 172.18.215.111
1	5	2008-5-9 11:11:05	172.18.215.50	[SYS]--Web logout from 172.18.215.111

Custom

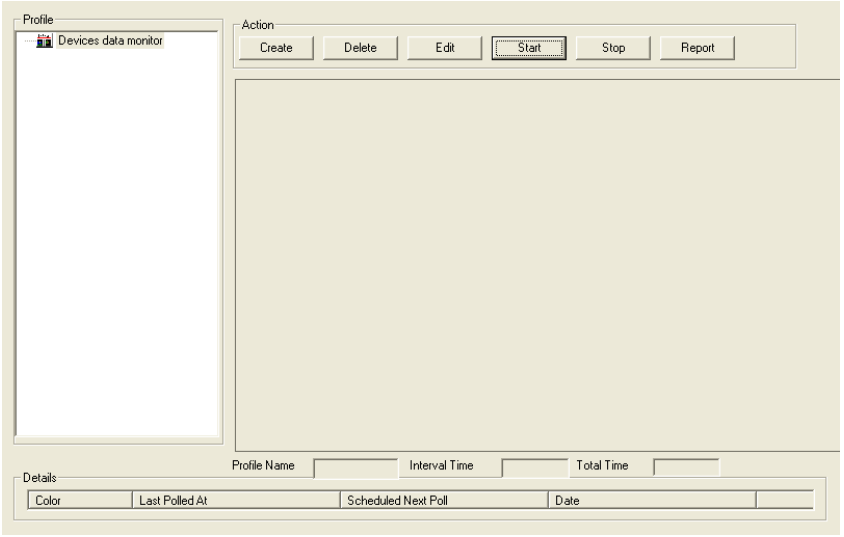
The Custom window shows summarized information about the associated station numbers of APs in a specified interval. To list the stations according to the detected date, choose the date range from From/To drop-down menu, and click **Search** button.



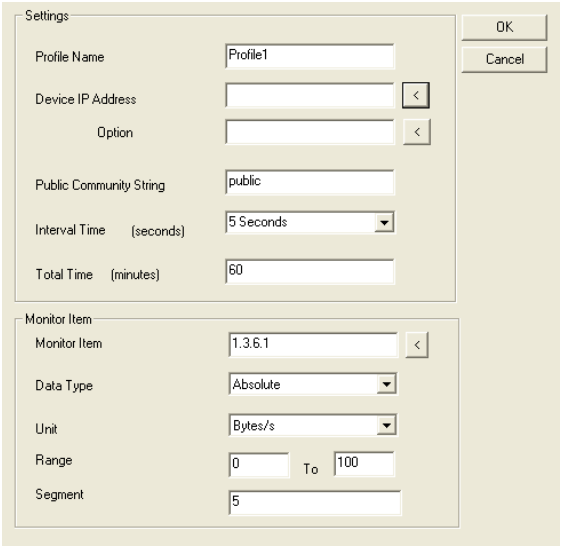
From the **Group Type**, you can specify that the window show the data according to specified group.

Monitor

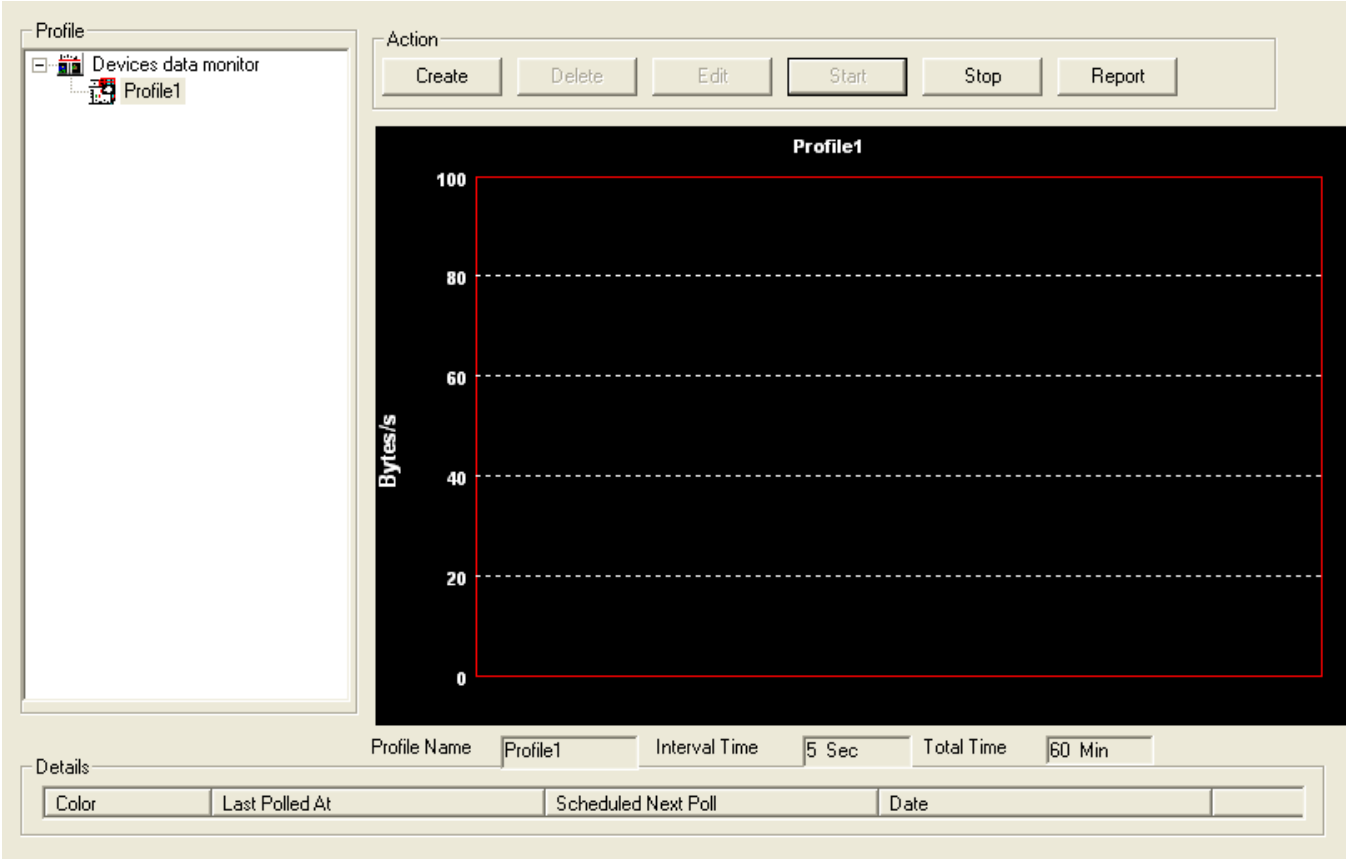
The Monitor window shows the performance of a specified AP in real-time, the window shown as below.



To create a new surveillance profile, click **Create** button to open the following window.

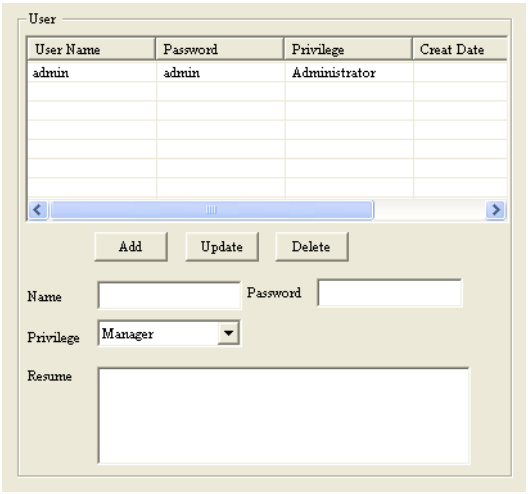


Enter the profile name, public community string and select the device IP address, scan interval time, total display time and monitor items. Then click **Start** button to monitor the AP's received or transmitted data in visualized way.



User Management

AP Manager II allows you to manage the user profiles. To manage the users, click the **User Manage** item under the System menu or click the icon in the tools bar. The configuration page is shown as below.



Explanation of privilege levels:

- **Administrator:** Owns all the rights of AP Manager II.
- **Manager:** Owns all the rights except user manage.
- **Guest:** Only can view the information.

To add a new user, follow the steps below:

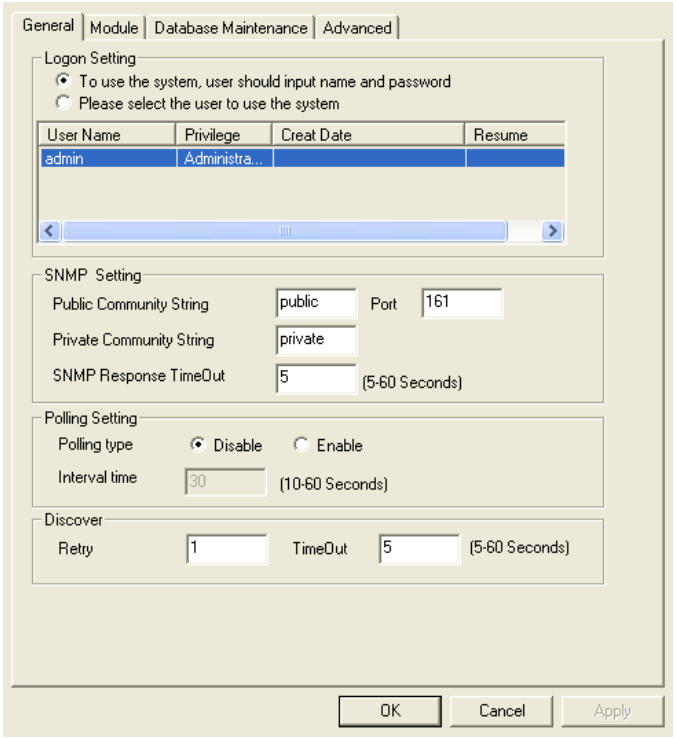
- Enter the username and password in the Name and Password textbox.
- Choose the right level in the Privilege drop-down menu.
- Enter the description about this user in the Resume textbox.
- Click the **Add** button to add this user to AP Manager II.

To modify a user, highlight the record line of that user, modify the contents in the corresponding textbox, and then click the **Update** button to apply the changes.

Note: The changes will take effect at next login. To delete a user, highlight the record line of that user, and then click the **Delete** button to remove the user from AP Manager II.

System Environment

You can change the software operation environment of AP Manager II. To configure the system environment, click the **Options** item under the System menu or click the icon in the tools bar. The configuration page is shown as below.

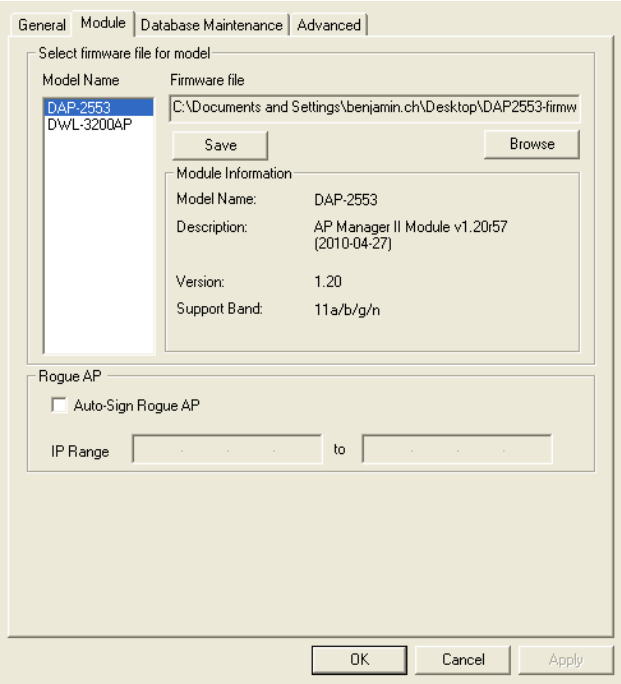


Logon Setting: Set whether login the system automatically or by hand. To login automatically, you should select a user used to login the system from the user list.

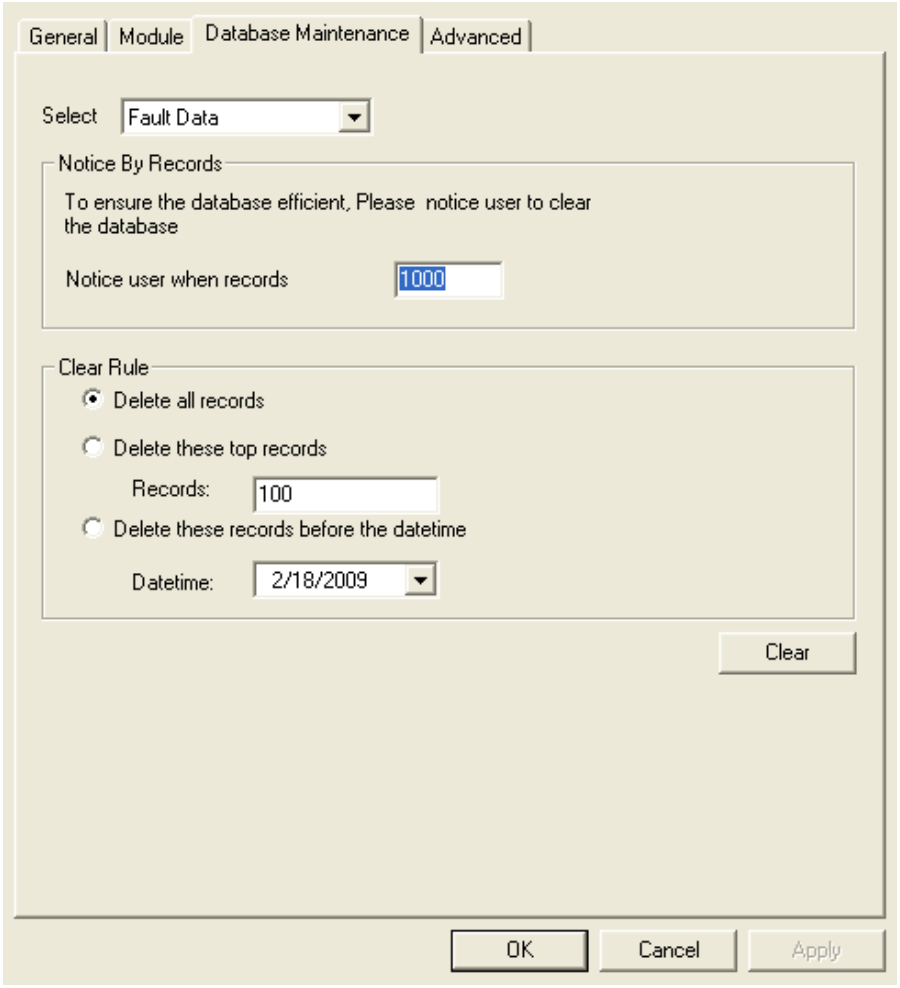
SNMP Setting: Set the Public/Private Community String, Port number and SNMP Response Timeout.

Polling Setting: Disable by default. When this function is enabled, you must set the polling interval time, it is 30 seconds by default.

Discover: Enter the Retry number and the time of timeout when discovering.



Module: For updating the firmware of AP, you can specify a default firmware file for each model of AP. Highlight one type of AP, and click the **Browse** button to choose the firmware file then click the **Save** button to apply the changes.

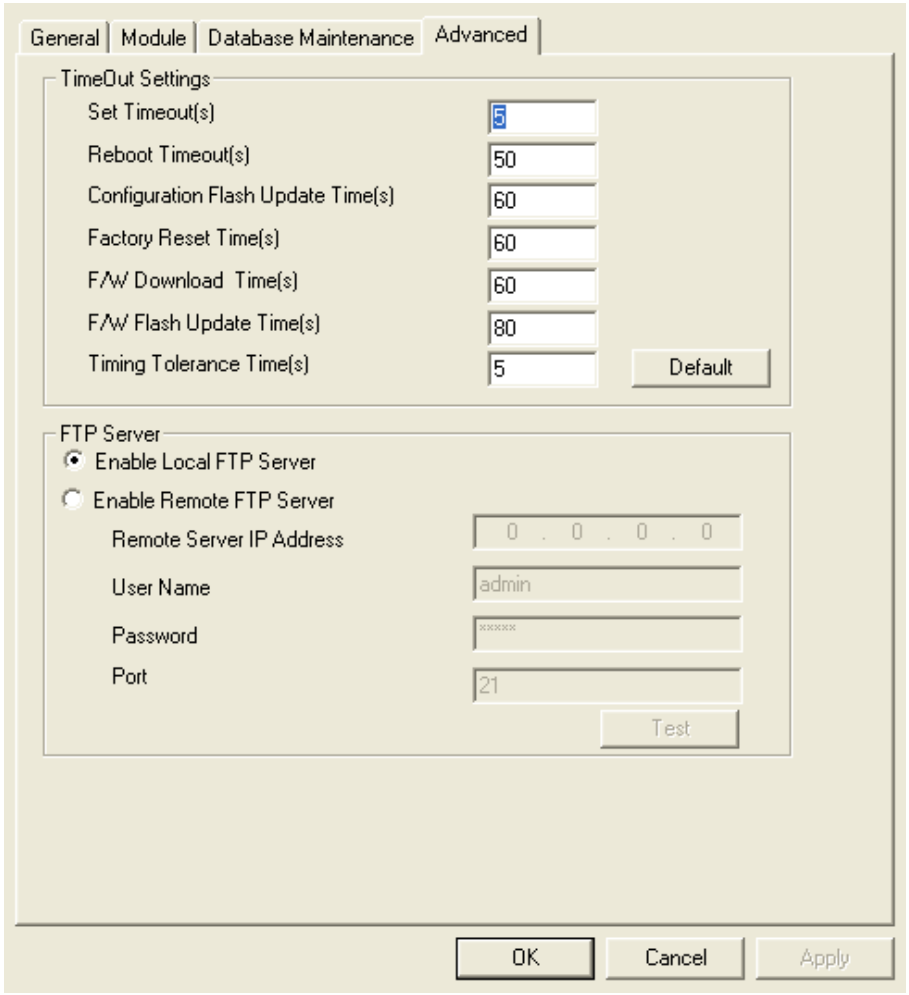


Select Choose: the type of records.

Notice By Record: Set the number that record reach to notice the user to clear the database.

Clear Rule:

- **Delete all records:** select this option to clear all the records.
- **Delete these top records:** select this option to clear the specified number of top records.
- **Delete these records before the date time:** select this option to clear the records that recorded before the specified time. Click the **Clear** button to apply the change.



TimeOut Settings: Configure the system time out settings.

FTP Server: Click **Enable Local FTP Server** to run an ftp server on the local computer. The ftp server will run when AP Manager II starts. Click **Enable Remote FTP Server** if all the system logs are stored in a lone ftp server. You should configure the ftp server parameters here.