

Release 2.00

AP Manager II

User Manual

Table of Contents

Getting Started	5
Requirements	
Minimum System Requirements	
Minimum Software Requirements	
Access Point Requirements	
Installation	
Install MySQL Server	
Install AP Manager II	
Using AP Manager II	
General View	
Discovering Devices	
Access Point Report	
Station Report	
Model Report	
Band Report	
Group View	
Configuration	
Set IP	
Update Configuration	
Upgrade Firmware	
Web Manage	
Telnet	
Set Password	
Sorting	
View	
Property	
Configuring 802.11a/b/g APs with AP Manager II Home > Information	
Basic > Wireless	
Basic > Wireless - Authentication	
Basic > Wireless > Access Point > WEP Encryption Basic > Wireless > Access Point > WPA/WPA2 - Enterprise	
Basic > Wireless > Access Point > WPA/WPA2 - Personal Basic > Wireless > Access Point > WPA/WPA2 - Personal	
Basic > Wireless > Access Font > wFA/ wFA2 - Fersonal Basic > Wireless > WDS	
Basic > Wireless > WDS	
Basic > LAN > Dynamic (DHCP)	
Basic > LAN > Static (Manual)	
Advanced > Performance > 802.11a	
Advanced > Performance > 802.11g	
Advanced > Filter > Wireless MAC ACL	
Advanced > Filter > Wireless MAC ACL	
Advanced > Grouping > AP Grouping Settings	
Advanced > DHCP Server > Dynamic Pool Settings	
Advanced > DHCP Server > Dynamic Fool Settings	
Advanced > DHCP Server > Current IP Mapping List	
Advanced > Multi-SSID	
Advanced > Rogue AP	
Tools > Admin	
Tools > Firmware and SSL	
Tools > Configuration File	

Tools > SNTP	
Status > Device Information	
Status > Stats	
Status > Client Information	
Status > WDS Information	
Status > Log > Log View	
Status > Log > Log Settings	
System	
Configuring 802.11n APs with AP Manager II	
Home > Information	
Basic > Wireless	
Basic > Wireless > Authentication	
Basic > Wireless > Access Point > WEP Encryption	
Basic > Wireless > Access Point > WPA/WPA2 - Enterprise	
Basic > Wireless > Access Point > WPA/WPA2 - Personal	
Basic > Wireless > WDS	
Basic > Wireless > WDS with AP	
Basic > Wireless > Wireless Client	
Basic > LAN > Dynamic (DHCP)	
Basic > LAN > Static (Manual)	
Advanced > Performance > Mixed 802.11n, 802.11g and 802.11b	
Advanced > Performance > Mixed 802.11g and 802.11b	
Advanced > Filter > Wireless MAC ACL	
Advanced > Filter > Wireless MAC ACL	
Advanced > DHCP Server > Dynamic Pool Settings	
Advanced > DHCP Server > Static Pool Settings	
Advanced > DHCP Server > Current IP Mapping List	
Advanced > Multi-SSID	
Advanced > Intrusion	
Advanced > VLAN	
Advanced > VLAN > Add/Edit VLAN	
Advanced > VLAN > PVID Setting	
Advanced > QoS	
Advanced > Schedule	
Maintenance > Admin.	
Maintenance > Firmware and SSL	
Maintenance > Configuration File	
Maintenance > SNTP	
Status > Device Information	
Status > Stats > WLAN Traffic Statistics	
Status > Stats > Ethernet Traffic Statistics	
Status > Client Information	
Status > WDS Information	
Status > Log > Log View	
Status > $Log > Log > triangle status$ Status > $Log > Log Settings$	
System	
•	
Multiconfiguration	
Create a new template	
Edit a template	
Delete a template	
Run a template	
Import or export a template	
Fault Manage	
Event settings	
Event Export	
· F	

Notice setting	
Watch list	
Tools	
Topology	
New topology view	
Background	
Grid line and rulers:	
Topology size	
Line	
Site Planning	
Collect information	
Load information	
Report	
Association	
Security	
Utilization	
Channel	
Rogue AP	
Syslog	
User Management	
System Environment	

Getting Started

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, organize and sort your APs into manageable groups.

Requirements

Minimum System Requirements

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

Minimum Software Requirements

- MySQL Server 5.0
- Mysql-connector-odbc-3.51

Access Point Requirements

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

Installation

Install MySQL Server

Before installing AP Manager II on your computer, you must first install MySQL© Server 5.0 and MySQL© ODBC Connector. During the AP Manager II install process, AP Manager II will check if these MySQL© programs have been installed. If they are not found, you will be reminded to download them.

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

MySQL© Server 5.0: http://dev.mysql.com/downloads/mysql/5.0.html.

MySQL© ODBC Connector 3.51: http://dev.mysql.com/downloads/connector/odbc/3.51.html

MySQL© 5.0 Reference Manual: http://dev.mysql.com/doc/refman/5.0/en/index.html.

Install AP Manager II

Once the MySQL Server 5.0 and MySQL ODBC Connector 3.51 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.

InstallShield Wizard
Choose Destination Location Select folder where Setup will install files.
Setup will install AP Manager II in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\D-Link\AP Manager II Browse
InstallShield
< Back Next> Cancel

Select Components

You are then given the option to select which components you want to install and which you do not. By default, the AP Manager II software and all AP modules are selected. Click **Next** to continue.

InstallShield Vizard	X
Select Components Choose the components Setup will install.	
Select the components you want to install, and clear the c install. Program DVL2700AP Module DVL2700AP Module DVL2800AP Module DVL2800AP Module DVL2590 Module DAP2590 Module	components you do not want to Description AP Manager II Components
Space Required on C: 0 K Space Available on C: 9711888 K InstallShield	k <u>N</u> ext > Cancel

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.

InstallShield Wizard		×
Select Program Folder Please select a program folder.		
Setup will add program icons to the Program Fol name, or select one from the existing folders list. Program Folders: AP Manager II Existing Folders:	Click Next to continue.	
Administrative Tools Catalyst Control Center CyberLink RowarDVDVUL-AG530 D-Link AtiPremier AG DVUL-AG530 D-Link AtiPremier AP Manager FlexibleSoft Co Games		
InstallShield.	< Back Next> Cancel]

Configure MySQL Connector

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

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

Configure	• MySQL Co	nnector				
Settin	g the connec	ting paramete	er			
confi			g file. Before you or. click Next. to			
	Server	127.0.0.1			_	
	User	root			-	
	Password	жжэ				
	Database	apm2db				
			< Back	N	ext >	Cancel
Configure MyS	QL Connec	tor				
Configure	QL Connec MySQL Co g the connec	nnector	er			
Configure Settin Setu	e MySQL Co g the connec up has comple	i nnector ting paramete	er Ig file. Before you	ı run AP M	anager II,	you must dySQL
Configure Settin Setu conf	e MySQL Co g the connec p has comple	innector ting paramete te the copyir rmation				you must dySQL
Configure Settin Setu conf	p has comple igure the connection of the connection of the connection of the connection of the connection.	innector ting paramete te the copyir rmation	g file. Before you			you must dySQL
Settin Setu conf	p has comple igure to Ser	innector ting paramete te the copyir rmation	ig file. Before you			.you must tySQL
Configure Settin Setu conf	p has comple igure to the sector. Infor Ser Use	te the copyin rmation Config	ig file. Before you			you must dySQL
Configure Settin Setu conf	p has comple igure the sector. Info Ser Use Password	te the copyin rmation Config	ig file. Before you			you must tySQL

Install Complete!

When the InstallSheild Wizard has completed, you are given the option to launch the AP Manager II program. Check the box to run AP Manager II and click **Finish** to complete the installation.



If you checked the "Run AP Manager II" box 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

-			
📀 Set Program Access and Defaults		🛅 VideoLAN	۲
💖 Windows Catalog		m D-Link AirPremier AG DWL-AG530	۲
🍓 Windows Update		🛅 VistaBootPRO 3.3	۲
츐 Program Updates			
m Accessories	•		
🛅 Administrative Tools	•		
🛅 Games	→		
🛅 D-Link	►		
🛅 D-Link AirPremier AP Manager	►		
💼 D-Link AP Manager II	•	🚊 AP Manager II	1
	-		

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

1 💽 🔊						
	1 Report Model Report		CCCESSPOINT Report			Legend Un-manage
MAC Address	IP Address	Band	Authentication	RSSI	SSID	Power Save Mode
2007-06-29 09:4	19:16 Trying to re	gister for traps	on port 162			
	AccessPoint Station Station Detail MAC Address 2007-06-29 09:4 2007-06-29 09:4	Station Detail MAC Address IP Address 2007-06-29 09:49:16 FTP Server 2007-06-29 09:49:16 Trying to re	AccessPoint Station Report Model Report Band Report Station Detail MAC Address IP Address Band 2007-06-29 09:49:16 FTP Server started on port 2007-06-29 09:49:16 FTP Server started on port	AccessPoint Report	AccessPoint Report AccessPoint Report AccessPoint Station Report Model Report Band Report Station Detail MAC Address IP Address Band Authentication ESSI 2007-06-29 09:49:16 FTP Server started on port 21. 2007-06-29 09:49:16 FTP Server started on port 162	AccessPoint Report AccessPoint Report AccessPoint Station Report Model Report Band Report Station Detail MAC Address IP Address Band Authentication ESSI SSID 2007-06-29 09:49:16 FTP Server started on port 21. 2007-06-29 09:49:16 FTP Server started on port 21. 2007-06-29 09:49:16 Trying to register for traps on port 162

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.

Standard discovery

To initiate the discovery process, right-click anywhere of the blank area 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 **AII 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.

Advance Dis	cover	
Method		
Start IP:	192 . 168 . 0 . 50	Start
End IP:	192 . 168 . 0 . 100	Cancel
Community	public	
TimeOut	30	

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 record according to its type.

Explanation of icons:

- Manageable 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-click 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.

Arre	seePoint Station Report Model Repo	ort Band Report				
	ion Detail AC Address IP Address	Band	Authentication	RSSI	SSID	Power Save Mode

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

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.

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

Station Report

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

	🗋 📊 🧟	E						
- 🛃 All Space General + 🛄 Group					Station Re	port		
MultiConfiguration For Early Manage Association Security Utilization Channel								Ligend 62.11g
		i Report Model Keport	Band Report					
	Station Detail		1		T		1	
	MAC Address	IP Address	Band	Authentication	RSSI	SSID	Power Save Mode	
	004096AF74B7	10.24.69.177	802.11g	WPA-Personal	98	Multi-SSID 1	Off	
	1100							
	2007-05-05 13:4 2007-05-05 15:4 2007-05-05 15:5	5:38 Device: 10.2 9:38 Device: 10.2 0:37 Device: 10.2	4.69.177 SNMP 4.69.177 SNMP 4.69.177 SNMP	Ping Ok! Ping TimeOut! Ping Ok!				
	2007-05-05 16:0	0:38 Device: 10.2 11:07 Device: 10.2	4.69.177 SNMP	Ping TimeOut!				
Ready	1.1.1							LogUser admin

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. It shows the numbers of every model.



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 five models of D-Link Access Points - the DAP-2590, DWL-2700AP, DWL-3200AP, DWL-7700AP, and the DWL-8200AP. 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.

Any of these 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.

Configuration

Any individual 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.

	🗎 🚺 🌌	🌆 🎽 🎦	• 🖳 • 🗟
	IP Address	Model Name MAC #	Address NetMask
All Space General Group Model DWL-7700AP	192. 168. 0. 50	D) Discover Delete Refresh Sign Rogue AP	D989810 255.255.255.0
DWL-2700AP DWL-8200AP DWL-3200AP DWL-3200AP DAP-2590 Category1 Category2 Category3		Configuration → Sorting → View By → Property	Set IP Update Config Upgrade Firmware Web manage Telnet
 MultiConfiguration Fault Manage Tool Report 			Set Password

Under the Configuration menu entry, you can select **Set IP, Update Config, Upgrade Firmware, Web manage, Telnet,** or **Set Password**. 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.

Set IP					×
IP Address	192	. 168	. 0	. 50	
Subnet Mask	255	. 255	. 255	. 0	
Default Gateway	0	. 0	. 0	. 0	
COK			Car	ncel	

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



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).

Home Basic Advanc	ed Tools Status System Help	
Home	Information -	
\$	System Information	
Information	Model Name	DWL-3200AP
	System Time	Not Available
	Up Time	0:00:25.00
	Firmware Version	v2.40
	IP address	192.168.0.50
Basic		
Advanced		
Tools		
Status		
System		
Ok!		

Note: See the section "Configuring 802.11a/b/g 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.

Firmware		
Module Name	Firmware	Edit
DWL-3200AP		Edit
	OK	Cancel

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

Open	2 🛛
Look in: 🔎	Firmware 💽 🗢 🛅 📰 -
DWL3200A	AP-firmware-v310-r0103.tfp
File name:	DWL3200AP-firmware-v310-r0103.tfp Open
Files of type:	firmware file(*.tfp)
	C Open as read-only

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

UP Firmware					×
Module Name	Firmware		Edit	[1
DWL-3200AP		ettings\Benjamin.c	Edit		
J					
	ok	Cance	1		

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 Manage

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.

Connect to 192.1	68.0.50	? 🛛
DWL-3200AP User name: Password:		
	Remember my pass	Sword

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 then 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 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 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.



Set Password

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.

Set Password	×
Set the password for AP	
User Name admin	
Password	
Ok Cancel	

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 Type - 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, Rougue 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.

Create Group					X
Basic Infor					
Group Name					
Create Date	2008- 6-11	× 7	Create By	admin	1
- Remark					
– Manager memeber – Available member				Selected member	
Everyone	-	>>		Everyone	
	Ok		Cancel		

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.

🖃 👘 All Space
General
🚊 🔄 Group
😟 🦲 Model
🖻 🦲 Category1
DH1
Category2

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

	IP Address	Model Name	MAC Address	NetMask	FW version	Lo
🖃 📳 All Space	🔿 172.18.213.35	DWL-7700AP	0050002209AA	255.255.255.0	v3.20	
General	92.168.5.82	DWL-8200AP	001CF008E630	255.255.255.0	v2.10	
🚊 🔄 Group	🤨 192.168.0.50	DAP-2590	00055D898760	255.255.255.0	2.0	
🕀 🧰 Model						

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 rightclicking the AP in the Group View window and selecting Property - as shown below.

Prope	rty							X
Basic	Informati	on						
Mode	el Name	DAP-25	90					1
MAC	Address	00055D9	9898	10	 			1
IP A	ldress	192		168	0		50	
Loca	tion				 			
	Quei	y		Set		Cano	cel	

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

Configuring 802.11a/b/g 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).

Home Basic Advance	ed Tools Status System H	elp	
Home	Information 🕶		
\$	System Information		
Information	Model Name	DWL-3200AP	
	System Time	Not Available	
	Up Time	0:00:25.00	
	Firmware Version	v2.40	
	IP address	192.168.0.50	
Basic			
Advanced			
Tools			
Status			
System			
Ok!			

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

Home	Information 🗸		
S	System Information		in in
Information	Model Name	DWL-3200AP	
	System Time	Not Available	
	Up Time	0:00:25.00	
	Firmware Version	v2.40	
	IP address	192.168.0.50	
Basic			
V/AGE/UCOMPRESS/			
Advanced			
Advanced Tools			

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 references both 802.11a and 802.11g configuration settings.

Basic > Wireless

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem Help
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode Access Point
\$	SSID dlink
LAN	SSID Broadcast
	Channel 44 🗾 5.22 GHz 🔽 Auto Channel Scan
	Authentication Open System
	Key Settings
	Encryption Enable Key Size 64 Bits
	Valid Key First 💌 Key Type HEX 💌
	First Key XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Third Key Fourth Key
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Wireless Band:	Select the wireless band to configure, 802.11a or 802.11g.
SSID:	The Service Set (network) Identifier of your wireless network.
SSID Broadcast:	Enabled by default, selecting Disable allows you to disable the broadcasting of the SSID to network clients.
Channel:	Allows you to select a channel if the Auto Channel Scan is unchecked.
	The channel of an 802.11a network may not be set manually in certain regions (e.g. Europe and USA) in order to comply with DFS (Dynamic Frequency Selection).
AP Mode:	There are 3 AP modes:
	Access Point
	WDS with AP
	WDS
	Please see the following pages for an explanation of all the AP modes.

Basic > Wireless	; >	Authenticatio	n
------------------	-----	---------------	---

Ħ	ome <u>B</u> asic <u>A</u> dvano	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
	Home	Wireless -
	Basic	Wireless Band IEEE 802.11a
	Vireless	AP Mode Access Point
		SSID dlink
	LAN	SSID Broadcast
-		Channel 40 🗾 5.2 GHz 🔽 Auto Channel Scan
1		Authentication WPA-Personal
		Key Settings Open System / Shared Key
		Encryption Disable WPA-Personal te CARia V
		Valid Key First WPA2-Enterprise pe HEX I
		First Key WPA-Auto-Personal Key
		Third Key Fourth Key
	Advanced	
	Tools	Apply
	Status	
	System	
Ge	tok.	

Open System:	The key is communicated across the network.
Shared Key:	Limited to communication with devices that share the same WEP settings.
Both:	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
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

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode Access Point
\$	SSID dlink
LAN	SSID Broadcast Enable -
	Channel 44 💌 5.22 GHz 🔽 Auto Channel Scan
	Authentication Open System 💌
	Key Settings
	Encryption Enable Key Size 64 Bits
	Valid Key First 💌 Key Type HEX 💌
	First Key Second Key
	Third Key Fourth Key
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic > Wireless > Access Point > WEP Encryption

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

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11g
Wireless	AP Mode Access Point
	SSID Broadcast Enable
	Channel 6 2.437 GHz 🔽 Auto Channel Scan
	Authentication WPA-Enterprise
	Radius Server Settings
	Cipher Type Auto Group Key Update Interval (300-9999999)
	Radius Server · · · · Radius Port (1-65535) 1312
	Radius Secre:
	Accounting Mode Disable Accounting Port Accounting Server 0.0.0.0 0
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Enterprise

Cipher Type:Select Auto, TKIP, or AES from the drop-down list.Group Key Upd
ate Interval:Select the interval during which the group key will be valid. 1800 is
the recommended setting. A lower interval may increase key update
frequency.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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11g
Wireless LAN	AP Mode Access Point SSID dlink SSID Broadcast Enable Channel 6 2.437 GHz Authentication WPA2-Personal
	PassPhrase Settings Cipher Type Auto Group Key Update Interval 1800 (300-9999999) PassPhrase
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Personal

Cipher Type:Select Auto, TKIP, or AES from the drop-down list.Group Key Upd
ate Interval:Select the interval during which the group key will be valid. 1800 is
the recommended setting. A lower interval may increase key update
frequency.PassPhrase:Enter a PassPhrase between 8-63 characters in length.

Basic > Wireless > WDS

<u>H</u> ome <u>B</u> asic <u>A</u> dvanced	1 <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp				
Home	Wireless 🔻				
Basic	Wireless Band IEEE 802.11a				
Wireless	AP Mode WDS				
	SSID dlink				
	SSID Broadcast				
	Channel 44 🔽 5.22 GHz 🗆 Auto Channel Scan				
	WDS				
	Remote AP MAC Address				
	Site Survey Type Channel Signal (%) BSSID Security SSID Scan				
	Type Channel Signal (%) BSSID Security SSID Scan				
Advanced					
Tools	Apply				
Status					
System					
Get OK.					

- **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 MA
C 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.

Basic > Wireless > WDS with AP

<u>H</u> ome <u>B</u> asic <u>A</u> dvanced	d <u>T</u> ools <u>S</u> tati	us <u>S</u> ystem	H <u>e</u> lp					
Home	Wireless 🔻							
Basic	Wireless Band IEEE 802.11a							
Wireless	AP Mode SSID		WDS with AF				-	
	SSID Broadcast		Enable 💌	l				
	Channel		44 💌	5.22 GHz 🗖 A	uto Channel Scan		≡	
	WDS with A	P						
	Remote AP	MAC Address	;					
	Site Survey	1 1	0: 1(8/)	DOOLD		0.010		
	Туре	Channel	Signal (%)	BSSID	Security	SSID	Scan	
Advanced							-	
Tools					Apply			
Status								
System								
Get OK.								

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.
	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.
Basic > LAN > Dynamic (DHCP)

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	LAN -
Basic Wireless LAN	Get IP From Dynamic (DHCP)
Advanced Tools Status System	Apply
Ok!	

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.

Basic > LAN > Static (Manual)

Home LAN - Basic LAN Settings Get IP From Static (Manual)	
Get IP From Static (Manual)	
Wireless IP address 192.168.0.50 Subnet Mask 255.255.0 Default Gateway	
Apply Advanced Tools Status System Okl	

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

Home Basic Advanced Tools Status System Help			
Home	Performance 👻		
Basic	Advanced Wireless Settin	g:	
Advanced	Wireless Band IEEE 802.11a	•	
S (1997)	Frequency	5.22 GHz	Advance Data Rate Settings
Performance	Data Rate	Auto	🔲 Enable Data Rate Control
	Beacon Interval (20 - 1000)	100	6Mb/sec Basic 💌
Filter	DTIM (1 - 255)	1	9Mb/sec Enable 💌
	Fragment Length (256 - 2346)	2346	12Mb/sec Basic 💌
S (RTS Length (256 - 2346)	2346	18Mb/sec Enable 💌
Grouping	Transmit Power	Ful	24Mb/sec Basic 💌
	Channel	44	36Mb/sec Enable 💌
DHCP Server	Radio	ON 🔽	48Mb/sec Enable 💌
DHUF Server	WMM	Enable	54Mb/sec Enable 💌
S 1	Super Mode	Disable 💌	
Multi-SSID	Antenna Diversity	Enable 🔹	
		,	
			Reset
Rogue AP 💌 Tools			
Status		Apply	
System			
Get OK.	, 		

Advanced > Performance > 802.11a

Frequency:	Displays the current frequency of the wireless band.		
Data Rate:	Set to Auto by default; use the drop-down list 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.
Auto Channel:	Enable this option to automatically select the most optimal channel available for wireless networking and to scan for the least populated channel.
Radio:	Select ON or OFF to control the signal status of the device.
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 802.1 1e WLAN QoS standard.
Super Mode	Select Super A to enable a wireless signal rate of up to 108Mbps. Super A is a group of performance enhancement features that increase end user application throughput in a 802.11a network. Super A is backwards compatible with standard 802.11 a devices. For ideal performance, all wireless devices on the network should be Super A capable.

Super A Mode	Function
Disabled	Standard 802.11a support. No enhanced capabilities.
Super A without Turbo	Capable of Packet Bursting, FastFrames, Compression. No Turbo mode.
Super A with Dynamic Turbo	Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo mode. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are configured with Super A and Dynamic Turbo enabled.
Super A with Static Turbo	Capable of Packet Bursting, FastFrames, Compression, and Static Turbo mode. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all devices on the wireless network are configured with Super A and Static Turbo enabled.

Antenna This option is Enabled by default. When enabled, each radio will automatically switch to the antenna with the greatest RSSI value. When disabled, each radio will use its main antenna - when facing the AP, 5GHz transmits from the right antenna, while the 2.4GHz radio uses the antenna on the left.

Home Basic Advanced Tools Status System Help			
Home	Performance 👻		
Basic	Advanced Wireless Setting	ŀ	
Advanced	Wireless Band IEEE 802.11g	•	
S 1	Frequency	2.437 GHz	Advance Data Rate Settings
Performance	Data Rate	Auto 💌	Enable Data Rate Control
	Beacon Interval (20 - 1000)	100	1Mb/sec Basic 💌
Filter	DTIM (1 - 255)	1	2Mb/sec Basic 💌
Filler	Fragment Length (256 - 2346)	2346	5.5Mb/sec Basic 🔽
S	RTS Length (256 - 2346)	2346	6Mb/sec Enable 🔽
Grouping	Transmit Power	Full	9Mb/sec Enable 💌
	Channel	6	11Mb/sec Basic 💌
DHCP Server	Radio	ON 💌	12Mb/sec Enable 💌
	WMM	Enable 🔹	18Mb/sec Enable 💌
💖	Super Mode	Disable	24Mb/sec Enable 💌
Multi-SSID	Antenna Diversity	Enable	36Mb/sec Enable 💌
	Wireless B/G Mode	Mixed	48Mb/sec Enable 💌
Rogue AP 🔽	Preamble	Short and Long 🔹	54Mb/sec Enable 💌 Reset
Tools			
Status		Apply	
System			
Get OK.			

Advanced > Performance > 802.11g

Frequency:	Displays the current frequency of the wireless band.
Data Rate:	Set to Auto by default; use the drop-down list 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), mini- mum power. This tool can be helpful for security purposes if you

	wish to limit the transmission range.
Auto Channel:	Enable this option to automatically select the most optimal channel available for wireless networking and to scan for the least populated channel.
Radio:	Select ON or OFF to control the signal status of the device.
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 802.11 e WLAN QoS standard.
Super Mode:	Select Super G to enable a wireless signal rate of up to 108Mbps. Super G is a group of performance enhancement features that increase end user application throughput in a 802.1 1a network. Super G is backwards compatible with standard 802.11 g devices. For ideal performance, all wireless devices on the network should be Super G capable.
Antenna Diversity:	This option is Enabled by default. When enabled, each radio will automatically switch to the antenna with the greatest RSSI value.
Wireless B/G Mode:	Select Mixed, 11g Only, or 11b Only.
Preamble:	Select Short and Long (recommended) or Long-Only.

Advanced >	Filter >	Wireless	MAC ACL

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem <mark>Help</mark>
Home	Filter -
Basic	Wireless MAC ACL G WLAN Partition
Advanced	
	Wireless MAC ACL
Performance	Wireless Band IEEE802.11g
\$	Access Control Disable 💌
Filter	MAC Address
S	MAC Address
Grouping	ID MAC Address
\$	
DHCP Server	
\$	
Multi-SSID	
🧇 _	Del
Rogue AP 📃	
Tools	Apply
Status	
System	
Get OK.	

Wireless Band:	Select the 802.11a or 802.11g 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	iced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Filter -	
Basic	C Wireless MAC ACL	WLAN Partition
Advanced		
	WLAN Partition Settings	
Performance	Wireless Band	EE 802.11a 💌
	Internal Station Connection 🔽	Enable
Filter	Ethernet to WLAN Access	Enable
	Internal Station Connection Between 802	.11a & 802.11g
	v	Connection Enabled
Grouping		
DHCP Server		
Dirici Selvei		
Multi-SSID		
		Apply
Rogue AP 🔽		
Tools		
Status		
System		
Get OK.		

Advanced > Filter > Wireless MAC ACL

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.
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 "Connection Enabled" box to allow communication between devices on the 802.11 a network and devices on the 802.11 g network.

<u>H</u> ome	<u>B</u> asic	<u>A</u> dvanced	<u>T</u> ools	<u>S</u> tatus	<u>S</u> ystem	Help
	Home	6	iroupi	ng 👻		
	Basic		- AP Gr	ouping Se	ttinas —	
A	dvance	d				
	S		Load E	8alance		Disable
Pe	rforman	ce	User L	.imit (0 - 6	4)	10
	Filter					
(Srouping					Apply
DH	KAN Ser	ver				
Μ	W Iulti-SSII	D				
F	Kogue A	P 🔽				
	Tools					
	Status					
	System					
, Get OK.		,				

Advanced > Grouping > AP Grouping Settings

	Disabled by default, select Enable to activate load balancing among the APs.
User Limit:	Enter a user limit amount, between 0-64.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp			
Home	DHCP Server -			
Basic	DHCP Server Settings			
Advanced	Oynamic Pool Settings	Static Pool Settings	Current IP Mapping List	
\$	Function Enable/Disable	Enable		
Performance	Dynamic Pool Settings			
\$	IP Assigned From	0.0.0.0		
Filter	The Range of Pool (1-255)	0		
\$	SubMask	0.0.0.0		
Grouping	Gateway	0.0.0.0		
DHCP Server	Wins	0.0.0.0		
	DNS	0.0.0.0		
	Domain Name			
Multi-SSID	Lease Time (60 - 31536000 sec)	0		
─ 🎸 _	Status	OFF 💌		
Rogue AP 🗾				
Tools		Apply		
Status			1	
System				
Ok!				

Advanced > DHCP Server > Dynamic Pool Settings

Dynamic Pool Sett ings:	Click to enable Dynamic Pool Settings. Configure the IP address pool in the fields below.
Function Enable/D isable:	Enable or disable the DHCP server function.
Assigned IP Fro m:	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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>Tools</u> <u>Status</u> <u>System</u> H <u>elp</u>	
Home	DHCP Server -	
Basic	DHCP Server Settings	
Advanced	C Dynamic Pool Settings 📀 Static Pool Settings	Current IP Mapping List
\$	Function Enable/Disable	
Performance	Static IP Pool Adding	
- \$	Static Pool Settings	Gateway DNS Win
Filter	Assigned IP 0.0.0.0	
\$	Assigned MAC Address 00000000000	
Grouping	SubMask 0.0.0.0	
DHCP Server	Gateway 0.0.0.0	
	Wins 0.0.0.0	
Multi-SSID	DNS 0.0.0.0	
\$	Domain Name	
Rogue AP 📃	Status OFF 💌	Add Edit Del
Tools		
Status	Apply	
System		

Advanced > DHCP Server > Static Pool Settings

Static 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.
Function 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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, if applicable.

DNS:	The IP address of the DNS server, if applicable.
	Enter the domain name of the AP, if applicable.
Status:	This option turns the static pool settings on or off.

Advanced > DHCP Server > Current IP Mapping List

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	DHCP Server -
Basic Advanced	DHCP Server Settings
Aarancea	C Dynamic Pool Settings C Static Pool Settings C Current IP Mapping List
	Current DHCP Dynamic Pools
Performance	Index Current Dynamic MAC Current Dynamic Assigned IP Current Dynamic Lease
Š	
Filter	
\$	
Grouping	
\$	Current DHCP Static Pools Index Current Static MAC Current Static Assigned IP
DHCP Server	
\$	
Multi-SSID	
\$	
Rogue AP 🗾	
Tools	Refresh
Status	
System	
Ok!	

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 StaticThe current corresponding DHCP-assigned static IP address of the
device.Assigned IP:device.

Advanced > Multi-SSID

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	ed <u>T</u> ools <u>S</u> tatus	<u>S</u> ystem H <u>e</u> lp						
Home	Multi-SSID 🗸							
Basic	_ Multi-SSID Settin	gs						
Advanced	🔽 Enable Multi-S	SSID 🗖	Enable VLAN SI	ate	● both ○	11a 🔿 11g		
\$	Band	IEEE 802.11g	▼ WMM	Enable	V	VLAN ID	1	
Performance	MSSID Index	Primary SSID	 SSID 	dlink				
\$	Security	None	Ethern	et 💿 LAN	N1 C LAN2	🔽 Enable SS	ID Broadcast	
Filter	Key Settings							
	Key Size	64 Bits	🚽 Key Ind	lex	First 💌			
S (Кеу Туре	HEX	📃 Key Va	lue	*****			
Grouping					,			
DHCP Server	Multi-SSID							
	Index	SSID		Band	Encryption	VLAN ID	Ethernet	-
	Primary	dlink		11a	OFF	OFF	LAN1	
Multi-SSID	Primary	dlink		11g	OFF	OFF	LAN1	-
								-
│								1
Rogue AP 📃							Del	
Tools					1			
Status					Apply			
System								
Get OK.								

Enable Multi-SSID:	When Multi-SSID is enabled, you can configure your SSIDs for either Both, 11a only, or 11g only networks.
Enable VLAN:	Check to enable VLANs.
Band:	Select the wireless band (IEEE802.11a or IEEE802.11g).
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.
VLAN ID:	Enter a VLAN number (0 - 4094).
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.
Ethernet:	Select " LAN1 " if you wish to configure the network on LAN 1 (PoE). Select " LAN2 " to set up the network on LAN 2.
Security:	Select the security level from the drop-down menu.

SSID Broadcast:	For each SSID, select to enable or disable the broadcast of the SSID.
WEP Encryption	
Key Index:	Select which defined key is active on the selected device(s).
WEP Key:	In the first drop-down menu select HEX or ASCII . Select the level of encryption (64, 128, or 162-bit) from the second drop-down box, and then enter the WEP key in the box.
WPA/WPA2 Perso nal	
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).

Advanced > Rogue AP

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tat	us <u>S</u> yste	em H <u>e</u> lp				
Home	Rogue AP 🗸						
Basic	- Roque AP D	etection -					^
Advanced	BSS Type-	ciccion					
\$	AP BSS	6 C A	d Hoc 🗢 Both				
Performance	Band						
\$	□ 11a	1	16 🗖 11g				
Filter	Security-						_
Grouping	C OFF		P WPA-Enterp			WPA2-Enterprise	
	- Rogue AP	List					
	Туре	СН	BSSID	Security	Mode	SSID	
DHCP Server	AP BSS	36	00037F0BA7DD	WPA-Auto-Personal	802.11a	DAP-1555_mk	
	AP BSS AP BSS	48 1	001195E0FD60 00179A2DC01E	WPA-Auto-Personal WPA-Enterprise	802.11a 802.11g	dwl8220_mktg_ AP_dir625	
	AP BSS	1	00195B65745D	WEP	802.11g	12345672	
Multi-SSID	AP BSS	1	00134609E4A0	WEP	802.11g		
Multi-SSID							
🔇 🖉							
Rogue AP 📃	<						
Tools	,			Detect A	dd	Del	
Status							
System	AP List-						~
Ok!							

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 11a, 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 considering 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.

Tools > Admin

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	iced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Admin -
Basic	Login Settings
Advanced Tools	User Name admin
\$	Old Password
Admin	New Password
\$	Confirm New Password
Firmware and SSL	Console Settings
S 1	Console Protocol C None © Telnet C SSH
Configuration File	Timeout 3 Mins 💌
	Apply
SNTP	
Status	
System	
Ok!	

Login Settings	
	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 .
	l l l l l l l l l l l l l l l l l l l

Tools > Firmware and SSL

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced Tools Status System Help
Home	Firmware and SSL -
Basic	
Advanced	Update Firmware From Local Hard Drive
Tools	Firmware Version v2.01
Admin	Upload Firmware From File : Browse UpLoad
\$	Update SSL Certification From Local Hard Drive
Firmware and SSL	Upload Certificate From File: Browse UpLoad
\$	Upload Key From File : Browse., UpLoad
Configuration File	
\$	
SNTP	
Status	
System	
Get OK.	,

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.

Tools > Configuration File

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem Help
Home	Configuration File -
Basic	Update Configuration File
Advanced	
Tools	Update File OK
	Download Configuration File
Admin	
	Load settings to Local Hard Drive OK
Firmware and SSL	
Fillinware and SSE	
Configuration File	
SNTP	
Status	
System	
Get OK.	

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.

Tools > SNTP

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	SNTP -	
Basic	SNTP/NTP Information	
Advanced	SNTP/NTP Server IP	0.0.0
Tools	SNTF/NTF Serverin	0.0.0.0
	SNTP/NTP Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Admin	Local Time	
	SNTP/NTP Setting	
Firmware and SSL	SNTP/NTP Server IP	
S	SNTP/NTP Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Configuration File	Daylight Saving Time	F Enable
SNTP		
		Apply
Status		
System		
Get OK.		

	The time server IP address, time zone, and the local time will be displayed here.
Server IP Addres s:	Enter the IP address of a SNTP/NTP server.
Time Zone:	Select your time zone from the drop-down menu.
Daylight Saving Ti me:	Check the box to enable daylight savings time.

Status > Device Information

Home Device Inform						
Basic Device Informa	tion					
Advanced Firmware Vers	sion: v2.01	Ethernet MA	C Address:	001195A2EA20		
Tools WLAN0 MAC	Address:					
Status Primary:		Secondary:	001195A2EA2	21 ~ 001195A2	EA27	
WLANT MAC						
Primary:	001195A2EA28	Secondary:	001195A2EA2	29 ~ 001195A2	EA2F	
Ethernet						
Vevice Information Get IP From:	Manual					
IP address:	192.168.0.50					
Subnet Mask	255.255.255.0					
Stats Gateway:	0.0.0					
Wireless (802	.11a)					
SSID:	dlink					
Channel:	44					
Client Information Rate:	Auto					
Authentication	n: Open System					
Encrypt:	Disabled					
Super Mode:	Disabled					
WDS Information	11b/a)					
SSID:	dlink					
Channel:	ашак 6					
Log Rate:	Auto					
Authentication	: Open System					
Encrypt:	Disabled					
Super Mode:	Disabled					
System						

 $\ensuremath{\text{Device}}\xspace$ | This window displays the configuration settings of the AP, including Information: the firmware version and device MAC address. It also displays WLAN information for both the 802.11a and 802.11g wireless networks.

Status > Stats

Home	Stats -		
Basic			
Advanced	WLAN 802.11A Traffic Statistics		
	- ThroughPut		
Tools	Transmit Success Rate	100 %	
Status	Transmit Retry Rate	0 %	
	Receive Success Rate	0 %	
	Receive Duplicate Rate	0 %	
evice Information	RTS Success Count	0	
	RTS Failure Count	2	
	Transmitted Frame Count		
Stats	Transmitted Frame Count	4925	
	Multicast Transmitted Frame Count	952	
	Transmitted Error Count	0	
Client Information	Transmitted Total Retry Count	0	
	Transmitted Multiple Retry Count	0	
	Received Frame Count		
WDS Information	Received Frame Count	0	
	Multicast Received Frame Count	0	
	Received Frame FCS Error Count	2	
Log	Received Frame Duplicate Count	0	
	Ack Rov failure Count	5	
	WEP Frame Error Count		
	WEP Excluded Frame Count	0	
System	WEP ICV Error Count		

WLAN 802.11a Tra
ffic Statistics:This page displays statistics for data throughput, transmitted and
received frames, and WEP frame errors for the 802.1 1a wireless
network.WLAN 802.11g Tra
ffic Statistics:This page displays statistics for data throughput, transmitted and
received frames, and WEP frame errors for the 802.1 1g wireless
network.

Status > Client Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> yst	em H <u>e</u> lp					
Home	Client Information	-					
Basic							
Advanced	Station association wit	h 11A :	0 Station as:	sociation with	n 118/G :	0	
Tools	MAC	Band	Authentication	Signal	PSM	SSID	
Status							
\$							
Device Information							
\$							
Stats							
\$							
Client Information							
\$							
WDS Information							
\$							
Log]						
					Refresh		
System							
ok!							

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 Mo de:	Displays the status of the power saving feature.		
SSID:	Displays the SSID the client is connected to.		

Status > WDS Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem	H <u>e</u> lp				
Home	WDS Information -					
Basic						
Advanced	Station association with 11	IA: 0 9	Station associ	iation with 11B/G :	0	
Tools	SSID	MAC	Band	Authentication	Signal	Channel
Status						
\$						
Device Information						
\$						
Stats						
\$						
Client Information						
\$						
WDS Information						
\$						
Log]					
				Refresh		
System						
Ok!						

SSID:	Displays the SSID the client is connected to.
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.
Channel:	Displays the wireless channel being used.

Status > Log > Log View

<u>H</u> ome <u>B</u> asic <u>A</u> dvanced	<u>T</u> ools <u>S</u> tatus <u>S</u> ystem	H <u>e</u> lp			
Home	.og -				
Basic	Log View	C Log S	-Win		
Advanced		i Lug s	eturigs		
Tools	View Log				
Status				Total Log:	6
	Time	Туре	Message		
	Uptime 0 day 00:10:09	SYS	Web logout from 192.168.0.100		
Device Information	Uptime 0 day 00:02:29	SYS	Web login success from 192.168.0.100		
Device Information	Uptime 0 day 00:00:19 Uptime 0 day 00:00:14	WIREL	WLAN1 Normal AP ready WLAN0 Normal AP ready		
	Uptime 0 day 00:00:14	NOTICE	WEAND Normal AF ready Ethernet AE1 LINK DOWN		
	Uptime 0 day 00:00:09	SYS	-AP cold start with f/w version: v2.01		
Stats					
Stats					
Client Information					
WDS Information					
Log					
LOG	<				
			Clear		
System					
Get OK.					

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

Status > Log > Log Settings

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Log 🕶
Basic	C Log View 🕞 Log Settings
Advanced	
Tools	Log Settings
Status	Log Server / IP Address
	Log Type
Device Information	🔽 System Activity
Device micimation	Vireless Activity
Stats	I I I I I I I I I I I I I I I I I I I
	SMTP
Client Information	SMTP Enable
	SMTP Server / IP address
	SMTP Sender
WDS Information	SMTP Sender
	SMTP Recipient
Log	
	Apply
System	
ok!	

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.

System



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

Warning	
Device will rebo	oot, continue?
ОК	Cancel

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

Warning	
All of your changes will I	be discarded, continue?
ОК	Cancel

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

Configuring 802.11n 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).

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Information -	
\$	-System Information	
Information	Model Name	DAP-2590
	System Time	Fri Dec 31 16:11:12 1999
	Vp Time	0:11:13.00
	Firmware Version	1.00
	IP address	192, 168, 0, 50
	Operation Mode	Access Point
	System Name	D-Link DAP-2590
	Location	
	MAC Address	00055D989810
Basic		
Advanced		
Maintenance		
Status		
System		
0k!		

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

Home > Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Information -	
	System Information	
Information	Model Name	DAP-2590
	System Time	Fri Dec 31 16:11:12 1999
	Vp Time	0:11:13.00
	Firmware Version	1.00
	IP address	192. 168. 0. 50
	Operation Mode	Access Point
	System Name	D-Link DAP-2590
	Location	
	MAC Address	00055D989810
Basic		
Advanced		
Maintenance		
Status		
System		
0k!		

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, IP address, Operation Mode, System Name, Location and MAC Address.

Basic > Wireless

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>Maintenance</u> <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless 🕶
Basic Wireless LAN	Wireless Band 2.4GHz Mode Access Point Metwork Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel 1 Image: Channel Width 20 MHz Channel 1 Image: Channel
Advanced	
Maintenance	
Status	Apply
System	
Get OK.	

Wireless Band:	Select the wireless band to configure, 802.11a or 802.11g.
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 Width:	Select the radio width of the channel.
Channel:	Allows you to select a channel.
AP Mode:	There are 4 AP modes:
	Access Point
	WDS with AP
	WDS
	Wireless Client
	Please see the following pages for an explanation of all the AP modes.

Basic > Wireless > Authentication

Home	Wireless -
Basic Wireless LAN	Wireless Band 2.4GHz Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel I Image: Channel Width 20 MHz Channel I Image: Channel I Image: Channel Image: Channel Selection Authentication Open System Key Settings Shared Key Encryption Enable WPA-Personal Image: Channel Selection Valid Key First Valid Key First Network Key Image: Confirm Key
Advanced	
Maintenance Status	Apply
Status	

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

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

WPA-Personal: Secure your network using a password and dynamic key changes. (No RADIUS server required.)

WPA2-Personal: 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- Enterprise** to allow the client to either use **WPA-Enterprise** or **WPA2-Enterprise**.

WPA-Enterprise: Secure your network with the inclusion of a RADIUS server.

WPA2-Enterprise: Secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES).

Security

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

<u>H</u> ome <u>B</u> asic <u>A</u> dvanced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp		
Home	Wireless 🕶	
Basic	Wireless Band 2.4GHz	
Wireless	Mode Access Point	
	Network Name (SSID) dlink	
S 1	SSID Visibility Enable	
LAN	Channel Width 20 MHz 💌	
	Channel 1	✓ Auto Channel Selection
	Authentication Open System	•
	-Key Settings	
	Encryption Enable -	Key Size 64 Bits 💌
	Valid Key First 💌	Key Type HEX 💌
	Network Key	
	Confirm Key	
Advanced		
Maintenance		
Status		Apply
System		
Get OK.		

Basic > Wireless > Access Point > WEP Encryption

Authentication:	Select from the drop-down list the type of authentication to be used on the selected device(s). In this example you may select Open System or 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 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 or Shared Key .
Key Values:	Select the Key Size (64-bit or 128-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 or Shared Key .

Home	Wireless -
Basic	Wireless Band 2.4GHz
Vireless Vireless	Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel I
	Authentication WPA-Enterprise Radius Server Settings Personal / Enterprise Auto (WPA or WPA2) Group Key Update Interval (300-9999999 seconds) Cipher Type
	Primary radius server settings Radius Server Radius Port (1-65535) 1812 Radius Secret
Advanced	Backup RADIUS Server Setting (Optional)
Maintenance	
Status	Apply
System	

Basic > Wireless > Access Point > WPA/WPA2 - Enterprise

Personal/Enterprise:	Select Auto, WPA Only or WPA2 Only from the drop-down list.
Cipher Type:	Select Auto, TKIP, or AES from the drop-down list.
Group Key Update Interval:	Select the interval during which the group key will be valid. 1800 is the recommended setting. A lower interval may increase the key update frequency.
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 this box to enable accounting.
Accounting Port :	Enter the port used on the Accounting server.
Accounting Server :	Enter the IP address of the Accounting server.
Accounting Secret :	Enter the Accounting secret.
Network Protection :	Select Enable to set the VLAN mode to dynamic.
<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
---	--
Home	Wireless -
Basic	Wireless Band 2.4GHz
Wireless LAN	Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel 1 Authentication WFA-Fersonal PassPhrase Settings Personal / Enterprise Auto (WPA or WPA2) Group Key Update Interval (300-9999999 seconds) Cipher Type Auto PassPhrase
Advanced	
Maintenance	
Status	Apply
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Personal

Personal/Enterprise:	Select Auto, WPA Only or WPA2 Only from the drop-down list.
Cipher Type:	Select Auto, TKIP, or AES from the drop-down list.
	Select the interval during which the group key will be valid. 1800 is the recommended setting. A lower interval may increase the key update frequency.
PassPhrase:	Enter a PassPhrase between 8-63 characters in length.

Basic > Wireless > WDS

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless 🕶
Basic	Wireless Band 2.4GHz
Wireless	Mode WDS Network Name (SSID) dlink
	SSID Visibility Enable
	Channel Width 20 MHz Channel 1 Auto Channel Selection
	WDS Remote AP MAC Address
	Site Survey
	Channel Signal (%) BSSID Security SSID Scan
Advanced	
Maintenance	
Status	Apply
System	
Get OK.	

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.
	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.

Basic > Wireless > WDS with AP

	ireless 🔻					
Basic	Wireless H	Band 2.40	iHz 💌			
Kireless LAN	SSID Visib Channel Wi Channel WDS with A	dth	dlink Enable 20 MHz 1 v	Auto Char	mel Selection	
	Site Surve	v				
	And the second se	Signal (%)	BSSID	Security	SSID	Scan
Advanced						
	0					
Advanced hintenance Status	1			Apply		

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.
	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.

Basic > Wireless > Wireless Client

<u>H</u> ome <u>B</u> asic <u>A</u> dvanced	d <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home 🚺	Wireless 🗸
Basic	Wireless Band 2.4GHz
Wireless	Mode Wireless Client
	Network Name (SSID) dlink
	SSID Visibility Disable
LAR	Channel Width 20 MHz
	Channel 1 Auto Channel Selection
	Site Survey
	Channel Signal (%) BSSID Security SSID Scan
Advanced	Authentication Open System
Maintenance	
Status	Apply
System	
Get OK.	

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.

Basic > LAN > Dynamic (DHCP)

Home Basic Advan	nced Maintenance Status System Help
Home	LAN -
Basic Wireless LAN	LAN Settings Get IP From Dynamic (DHCP)
Advanced Maintenance Status	Apply
System	
)k!	

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.

Basic > LAN > Static (Manual)

Home LAN ~ Basic IN Settings Get IP From Static (Manual) IP address 192.168.0.50 Subnet Mask 255.255.0 Default Gateway 0.0.0.0	<u>H</u> ome <u>B</u> asic <u>A</u> dvan	nced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Wireless Get IP From Static (Manual) Wireless IP address 192.168.0.50 Subnet Mask 255.255.0 Default Gateway 0.0.0.0	Home	LAN 🗸
Apply	Basic Vireless	LAN Settings Get IP From Static (Manual) IP address 192 . 168 . 0 . 50 Subnet Mask 255 . 255 . 255 . 0 Default Gateway 0 . 0 . 0 . 0
Advanced Maintenance Status System	Maintenance Status	Apply

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

Home Dasic Havand	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem }			
Home	Performance -			
Basic	Performance Settings			
Advanced				
S	Wireless Mode	Mixed 802.11n,802.11g and 80	92.11b ▼	
Performance	Wireless	0n 💌	Connection Limit	Disable 💌
	Data Rate	Best(Up to 300) 💌 (Mbps)	User Limit (0 - 64)	20
Filters	Beacon interval (25-500)	100	Link Integrity	Disable 💌
	DTIM interval (1-15)	1	Network Utilization	100 % 🔻
N 📎 🛛	Transmit Power	100 %		
DHCP Server	WMM (Wi-Fi Multimedia)	Enable		
 	Short GI	Enable		
Multi-SSID	IGMP Snooping	Disable 💌		
\$	Ack Time Out (2.4GHz, 48~200)	48 (μ s)		
Intrusion				
Maintenance				
Status		Appl	7	
System		кррт	<u> </u>	

Wireless:	Open or close the wireless function.
Data Rate:	Set to Auto by default; use the drop-down list 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 802.1 1e 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.

Connection Limit:	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.
Link Integrity:	If enabled, when the uplink of AP is off, the connected wireless client will be disconnected.
	Set the network utilization, if the utilization is more than the setting, no clients can connect to AP. Only available when Connection Limit is enabled.

	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem :	H <u>e</u> lp		
Home	Performance -			
Basic	Performance Settings			
Advanced				
	Wireless Mode	Mixed 802.11g and 802.11b	_	
Performance	Wireless	0n 💌	Connection Limit	Disable 💌
	Data Rate	Best(Up to 54) 💌 (Mbps)	User Limit (O - 64)	20
Filters	Beacon interval (25-500)	100	Link Integrity	Disable 💌
	DTIM interval (1-15)	1	Network Utilization	100 % 💌
\sim	Transmit Power	100 %		
DHCP Server	WMM (Wi-Fi Multimedia)	Enable		
S	Short GI	Enable		
Multi-SSID	IGMP Snooping	Disable		
🤹	Ack Time Out (2.4GHz, 48~200)	48 (μ s)		
Intrusion				
<u> </u>				
Maintenance				
Status		App1:	,	
System			<u></u>	

Advanced > Performance > Mixed 802.11g and 802.11b

Wireless:	Open or close the wireless function.
Data Rate:	Set to Auto by default; use the drop-down list 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 802.1 1e 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.

Connection Limit:	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.
Link Integrity:	If enabled, when the uplink of AP is off, the connected wireless client will be disconnected.
	Set the network utilization, if the utilization is more than the setting, no clients can connect to AP. Only available when Connection Limit is enabled.

Advanced >	Filter >	Wireless	MAC	ACL
------------	----------	----------	-----	-----

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Filters -
Basic	Wireless MAC ACL O WLAN Partition
Advanced	Wireless MAC ACL Settings
V Performance	Wireless Band 2.4GHz
Filters	Access Control Disable MAC Address Add
DHCP Server	MAC Address List ID MAC Address
Multi-SSID	
Intrusi on	
<u></u>	Del
Maintenance	Current Client Information
Status	MAC Address SSID Band Authentication Signal Add 🗸
System	
0k!	

Wireless Band:	Select the 2.4GHz or 5GHz 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.

Advanced > Filter > Wireless MAC ACL

Home	Filters -		
Basic	C Wireless MAC ACL	WLAN Partition	
Advanced	WLAN Partition Settings	Tronomination	
V Performance	Wireless Band	2.4GHz ×	
	Internal Station Connection	🔽 Enable	
\$	Ethernet to WLAN Access	🔽 Enable	
Filters			
\$			
DHCP Server			
Multi-SSID			
« ×			
Intrusion			
		Apply	
Maintenance			
Status			
System			

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.
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.

Home	DHCP Server -		
Basic	DHCP Server Settings		
dvanced	Dynamic Pool Settings O	C Static Pool Settings	C Current IP Mapping List
\$	Function Enable/Disable	Enable 💌	
formance	Dynamic Pool Settings		
S	IP Assigned From	0.0.0.0	
lilters	The Range of Pool (1-255)	1	
<∕∽	Submask	0.0.0.0	
P Server	Gateway	0.0.0.0	
\$	WINS	0.0.0.0	
lti-SSID	DNS	0 . 0 . 0 . 0	
	Domain Name	Į.	
atrusion	Lease Time (60 - 31536000 sec)	604800	
ax 🖬			
intenance			
Status		Apply	
System	L		

Advanced > DHCP Server > Dynamic Pool Settings

Dynamic Pool Sett ings:	, , , , , , , , , , , , , , , , , , , ,
Function Enable/D isable:	Enable or disable the DHCP server function.
Assigned IP Fro m:	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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, 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.

Home	DHCP Server -
Basic Ivanced	DHCP Server Settings C Dynamic Pool Settings
\$	Function Enable Enable
Static II	P Pool Adding
Static Pool	Settings
Assigned IP	
Assigned MAG	C Address
Submask	255 , 255 , 255 , 0
Gateway	0.0.0.0
WINS	0.0.0
DNS	0.0.0
Domain Name	Add Edit Bel
	Apply
	Apply

Advanced > DHCP Server > Static Pool Settings

Static 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.
Function 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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, if applicable.
DNS:	The IP address of the DNS server, if applicable.
Domain Name:	Enter the domain name of the AP, if applicable.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	DHCP Server -
Basic	DHCP Server Settings
Advanced	C Dynamic Pool Settings C Static Pool Settings C Current IF Mapping List
\$	Current DHCP Dynamic Pools
Performance	Index Current Dynamic MAC Current Dynamic Assigned IP Current Dynamic Lease
\$	
Filters	
\$	
DHCP Server	Current DHCP Static Pools
\$	Index Current Static MAC Current Static Assigned IP
Multi-SSID	
\$	
Intrusion	
Maintenance	Refresh
Status	Ketresh
System	
0k!	

Advanced > 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.

Advanced > Multi-SSID

Home	Multi-SSID -					
Basic	-Multi-SSID Set	ttings				
dvanced	🔽 Enable Mult	i-SSID				
<u> </u>	Band	2.4GHz -	WMM (Wi-Fi Multim	edia) Enabl	.0 7	
	MSSID Index	Primary SSID 💌	SSID	22	19-11	
formance	Security	None *		DZ Ro	able SSID Vis	Chilline .
<u> </u>	becarty			17. 200	IVIC SOLD FIS	10141 VY
ilters	Key Settings					
	Key Size	64 Bits 💌	Key Index	irst 7		
<u> </u>	Ney Sile	01.0113	terrete construction (
P Server	Key		Key Type	EX 💌		
	Confirm Key					
S	Confirm Key	「				
\$	Confirm Key Multi-SSID	ſ				
\$		SSID	Band	Encryption	VLAN ID	
w Lei-SSID	Multi-SSID	SSID II	Band 2. 4GHz	Encryption None	VLAN ID OFF	
\$	Multi-SSID			and the state of t		
w .ti-SSID	Multi-SSID			and the state of t		
trusion	Multi-SSID			and the state of t		Tiat
ti-SSID	Multi-SSID			and the state of t		Del

Enable Multi -SSID:	When Multi-SSID is enabled, you can configure your SSIDs for networks.
Band:	Select the wireless band (2.4GHz or 5GHz).
SSID:	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.
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.
Security:	Select the security level from the drop-down menu.
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 802.11 e WLAN QoS standard.
Enable SSID Visibility:	For each SSID, select to enable or disable the broadcast of the SSID.

Advanced > Intrusion

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Intrusion -
Basic Advanced	Wireless Intrusion Protection
Multi-SSID	AP List
mui (1-331)	
S	Type Band CH SSID BSSID Last Seem Status
Intrusion	
VLAN	
QoS	
QoS	
Schedule	Set as Valid Set as Neighborhood Set as Rogue Set as New
Maintenance	C Mark All New Access Points as Rogue Access Points
Status	Apply
System	Apply
Get OK.	

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.
AP List:	The category of the APs.
	From the All list, click the corresponding Add button of AP record to classify the AP.

Advanced > VLAN

<u>H</u> ome <u>B</u> asic <u>A</u> dvand	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	VLAN -
Basic	-VLAN Settings-
Advanced	VLAN Status 🔽 Enbale
	VLAN Mode : Static
	VLAN List Port List Add/Edit VLAN PVID Setting
Multi-SSID	
	VID VLAN Name Untag VLAN Ports Tag VLAN Ports
Intrusion	
S	
VLAN	
QoS	
QoS	
Schedule	
Maintenance	
Status	
System	
Refresh	

VLAN Status:	Check this box to enable the VLAN function.
VLAN Mode:	Displays the mode of VLAN. This window lists the configured VLAN on the AP.
VLAN List:	This window lists the configured VLAN on the AP.
Port List:	This window lists the configured Port on the AP.

Advanced > VLAN > Add/Edit VLAN

Home	VLAN -									
Basic	VLAN Settings									
ivanced	VLAN Status	Enbale								
100	VLAN Mode									
🤹 🖳		e provincian	133/23	. 1/7 . 17	1					
ti-SSID	VLAN List	Port List	Add/Edi	t vlan	PVID :	Setting				
~	VID	VLAN	Name		Add					
S	1	12-12-1-1-12-12-1								
trusion	Port	Select All	Mgmt	LAN						
	Untag	ALL	•	•						
\$ \$	Tag	ALL	C	C						
VLAN	Not Member	ALL	C	0						
	MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
\$ \$	Untag	ALL	œ	•		(•	(•	ſ	(·	6
QoS	Tag	ALL.	C	C	0	C	C	C	C	C
	Not Member	ALL	C	C	C	С	0	C	С	C
\$	WDS Port	Select All	¥-1	¥-2	¥-3	¥-4	¥-5	¥-6	8-7	¥-8
hedule	Untag	ALL	œ	œ	œ	•		œ	(•	(•
	Tag	ALL	C	C	C	C	C	C	0	C
ntenance	Not Member	ALL	С	C	С	C	C	C	С	C
tatus	1					Apply	. 1			
ystem						- APPT)				

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.

Advanced > VLAN > PVID Setting

Home	VLAN -								
Basic	-VLAN Settings-								
Advanced	VLAN Status	🔽 En	bale						
	VLAN Mode	: Stati	c						
	VLAN List	Port L	ist A	dd/Edit VLAN	PVID :	Setting			
ulti-SSID		10 10 100		20-21-21-21-21-21-21-21-21-21-21-21-21-21-	2	11			
< R	PVID Auto As	sign Status	· [Enable					
V	Port	Mgmt	LAN						
Intrusion	PVID	1	1						
\$	1		3						
VLAN	MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
V LIAM	PVID								
\$	1410	11	Jr.	11]1	1.	1	μ	1
QoS	T and the set	120012	127727	127722	2017-011	1007-024	83720	102122	
	WDS Port	₩-1	¥-2	¥-3	¥-4	₩-5	¥-6	¥-7	¥-8
S	PVID	1	1	1	1	1	1	1	1
Schedule									
aintenance									
MACC IN									
Status						Apply			
System							1		

PVID Auto
Assign Status:Check this box to assign the PVID automatically.Port/MSSID
Port/WDS Port:Assign the PVID manually.

Advanced > QoS

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	iced <u>Maintenance Status S</u> ystem H <u>e</u> lp
Home	QoS -
Basic	QoS Settings
Advanced	QoS(Quality of Service) Enable 💌
🧼 🖻	Priority Classifiers HTTP Automatic (default if not matched by anything else)
Multi-SSID	Add QoS Rule
	Name Priority Protocol 💌
	Host 1 IP Range
Intrusion	
	Host 1 Port Range -
S	Host 2 IP Range
VLAN	Host 2 Port Range - Add Clear
QoS	QoS Rules List
ųoS	Name Priority Host 1 IP Range Host 2 IP Range Protocol / Ports
\$	
Schedule	
Maintenance	
Status	
System	Apply.
Refresh	

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.

Advanced > Schedule

<u>H</u> ome <u>B</u> asic <u>A</u> dvar	ced <u>M</u> aintenance <u>S</u> tatus	<u>S</u> ystem H <u>e</u> lp			
Home	Schedule 🕶				
Basic	-Wireless Schedule Sett	-			
Advanced	Wireless Schedule	Enable	•		
🧇 🏹	Add Schedule Rule			_	
Multi-SSID	Day(s)	🔿 All Week	🖲 Select Day	(z)	
Intrusi on	All Day(s)	□ Sun □	Mon 🥅 Tue 🥅	Wed 🥅 Thu 🥅	Fri 🥅 Sat
\$	Start Time End Time			ute, 24 hour time) ute, 24 hour time)	
VLAN	Wireless	Off 💌			Add Clear
\$	-Schedule Rules List				
Q₀S	Name		Day(s)	Time Frame	Wireless
			50,00	lime frame	Mireless
\$				11me frame	nirefezz
Schedule				lime frame	nireless
				lime frame	
Schedule					Edit Del
Schedule Maintenance				pply	

Wireless Schedule Settings	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.
Day(s):	Select the days that apply the schedule.
Start/End Time:	Enter the start and end times that apply the schedule.
Wireless:	Open or close the wireless function at the schedule time.
Schedule Rules List:	This window lists the configured schedule rules.

Maintenance > Admin

Home	Admin -			
Basic Advanced Maintenance	-Limit Administrator IP ☐ IP Range From To		— — — ∏ Limit Administrator VI	D I
Admin	ID IP From	IP To		Add
rnware and SSL Configuration File	Login Settings User Name Old Password New Password Confirm New Password	sdnin	=	
Date and Time	Console Settings Console Protocol Timeout	C None 🦩 I 3 Mins 💌	elnet C SSM	
	-Ping Control Settings Status	T Enable		
Status	System Nume Settings	D-Link DAP-2590		

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.
Ping Control Settings	

Status:Check this box to allow the computer ping the AP.System Name SettingsEnter a name for this device.

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

Maintenance > Firmware and SSL

Home	Firmware and SSL -	
Basic Advanced Maintenance	- Update Firmware From Local Hard Drive Firmware Version 1.00	
\$	Upload Firmware From File :	Browse UpLoad
Admin	-Update SSL Certification From Local Hard Drive	
rmware and SSL	Upload Certificate From File:	Browse UpLoad
1	Upload Key From File :	Browse, UpLoad
	The second se	
\sim		
onfiguration File		
Configuration File		
File		
Configuration File		
File		
File		
File		

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.

Maintenance > Configuration File

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Configuration File -
Basic	Update Configuration File
Advanced	Update File Browse OK
Maintenance	Update File OK
Admin	Download Configuration File
. 🐝	Load settings to Local Hard DriveOK
Firmware and SSL	
\$	
Configuration File	
\$	
Date and Time	
Status	
System	
Get OK.	

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.

Maintenance > SNTP

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	red <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Date and Time 🕶
Basic Advanced	Time Configuration
Maintenance	Time Fri Dec 31 17:18:38 1999
	Time Zone (GMT-08:00) Pacific Time (US & Canada); Tijuana 💌
Admin	Enable Daylight Saving
	Month Week Day of Week Current Time
Firmware and SSL	Daylight Saving Dates DST Start Jan 💌 1st 💌 Sun 💌 12 am 💌
\$	DST End Jan 💌 Ist 💌 Sun 💌 12 am 💌
Configuration File	Automatic Time Configuration
S	Enable NTF Server
Date and Time	NTP Server Used
	Set the Date and Time Manually
	Date And Time
	2008- 6-11 • 15:52:50 • Copy Your Computer's Time Settings
Status	
System	Apply
Get OK.	

Time Configuration	
Time:	The current local time will be displayed here.
Time Zone:	Select your time zone from the drop-down list.
Daylight Saving Tim e:	Check the box to enable daylight savings time.
Daylight Saving Offset:	Select the offset time from the drop-down list.
Daylight Saving Dates:	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 and Time Manually	
Date And Time:	Select the date and time from the box or copy your computer's time setting to AP.

Status > Device Information

Home	Device Information 🗸
Basic	Device Information
Advanced	Firmware Version: 1.00 Ethernet MAC Address: 00055D989810 Wireless MAC Address:
Maintenance	mireless MAL Address: Primary: 00055D989810 SSID 1~7: 00055D989811 ~ 00055D989817
Status	
Ś	Ethernet
Device Information	IP address: 192.168.0.50
	Subnet Mask: 255, 255, 255, 0 Gateway: N/A
\sim	Wireless (2.4GHz)
Stats	Network Name zz
	Channel: 1 Data Rate: Auto
	Security: None
Client Information	
	AP Status
WDS Information	CPU Utilization 8 %
abb intermation	Memory Utilization 68 %
Ś	
Log	
System	

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

Status > Stats > WLAN Traffic Statistics

Home	Stats -		
Basic	WLAN Traffic Statistics	C Ethernet Traffic Statistics	
Advanced	- WLAN Traffic Statistics		
laintenance	Transmitted Count		
Status	Transmitted Packet Count	73068	
	Trasmitted Bytes Count	835797	
	Dropped Packet Count	0	
Device	Transmition Retry Count	0	
nformation	Received Count		
	Received Packet Count	73069	
Stats	Received Bytes Count	13465613	
	Dropped Packet Count	0	
S	Received CRC Count	0	
	Received Decryption Error Count	0	
Client	Received MIC Error Count	0	
<<	Received PHY Error Count	0	
\checkmark			
5 Information		Refresh Clear	
de		Lieur Cleur	
Log			
System			
byseem			

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

Home	Stats -		
Basic	C WLAN Traffic Statistics	Ethernet Traffic Statistics	
Advanced	-Ethernet Traffic Statistics		
Maintenance	- Transmitted Count		
Status	Transmitted Packet Count	51	
1	Trasmitted Bytes Count	31426	
\sim	Dropped Packet Count	0	
Device Information	Received Count		
	Received Packet Count	51	
	Received Bytes Count	6236	
Stats	Dropped Packet Count	0	
	Received Multicast Packet Count	0	
Client	Received Broadcast Packet Count	34	
Information	Len 64 Packet Count	28	
	Len 65~127 Packet Count	13	
Log	Len 128~255 Packet Count	4	
- Murey	Len 256°511 Packet Count	6	
	Len 512~1023 Packet Count	0	
	Len 1024~1518 Packet Count	0	
	Len 1519 ^{MAX} Packet Count	0	
System	1-2-	Refresh Clear	

Status > Stats > Ethernet Traffic Statistics

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

Status > Client Information

Home	Client Information	ė.					
Basic	-						
Advanced	Station associati	on (2.4GHz)	: 1				
Maintenance	MAC	Band	Authentication	Signal	PSM	SSID	ę.
Status	001CBF4F4E5F	G	Open System	30 %	Off	Primary SSID	
S							
Device Information							
\$							
Stats							
\$							
Client Information							
\$							
5 Information							
\$							
Log					Refresh]	
System							

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.

Status > WDS Information

Home	WDS Information	1 -				
Basic						
Advanced	WDS Information	Channel: 2 (2.4GHz):				
Maintenance	Name	MAC	Authentication	Signal	Status	
Status	₩-1	06055D989810	Shared Key	54 %	on	
\$						
Device Information						
\$						
Stats						
\$						
Client Information						
\$						
MDS Information						
\$						
Log			Ref	resh		
System						

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 client.

Status > Log > Log View



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

Status > Log > Log Settings

Home	Log 🕶			
Basic	C Log View @	Log Settings		
dvanced				
ntenance	Log Settings	2		
Status	Log Server / IP Address			
14	Log Type			1
\$	System Activity			
Device ormation	V Wireless Activity			
CONTRACTOR OF T				
\$	✓ Notice			
Stats	Email Notification			
14	Email Notification	T Enable	SMTP Port	25
$\langle \rangle$	Email Server address			
lient ormation				
1x	From Email Address		Password	
Log	To Email Address		Confirm Password	
	-Email Log Schedule			
	Schedule	0 • hours or	when Log is full	
		Appl	у	
System				

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 NotificationImage: Server you would like to send the AP log to.
three types: System, Wireless and Notice.
Email Notification
Email Notification: Check the box to enable email notification.
Email ServerEnter the IP address of the SMTP server.Address:
From EmailEnter the e-mail address of the SMTP sender.Address:
To Email Address: Enter the e-mail address of the SMTP recipient.
SMTP Port: Enter the port of the SMTP server.
User Name: Enter the username of the SMTP server.
Password: Enter the password of the SMTP server.
Email LogSelect an interval time from drop-down list to send the logs to mail recipient.

System

Home	System -
Basic Advanced	- System Settings
Maintenance	Apply Settings and Restart Restart
Status	Restore to Factory Default Settings Restore
System	
\sim	
System	

Click **Restart** to restart the AP and save 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.

Warning 🔀
Device will rebcot and module will be disconnected, continue?
OK Cancel

Multiconfiguration

Administrator can manage the configuration of APs that AP Manager II has detected by using the 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		General X
Basic Info	Enter a name for this template.	Basic Info Name : dlink Creator : admin
Content Selection	Check the box to select the configuration contents included in this template. Then configure the settings in the following page.	Time : 2008- 6-11 Content Selection Image: System Image: System <
		< Back Next > Cancel
System	Check the box to select the configuration contents included in this template.	System
LAN Settings	Set the subnet mask and default gateway of the Access Point.	Subnet Mask 255 . 255 . 0 Default Gateway
Admin	Enter the username and password of administrator for AP.	Password Misc Console Protocol Timeout 5 Mins
Misc	Set the console type.	
		< Back Next > Cancel

Wireless

Check the box to select the configuration contents included in this template. For how to configure wireless settings, please refer to page 29 and 41.

Check the box to select the configuration contents included in this template. For how to configure security settings, please refer to page 69.

Wireless 11g	
Wireless 11g Wireless Settings([EEE802.11g) SSID Channel SSID Broadcast Data Rate RTS Length(256-2346) Beacon Interval(20-1000) Fragment Length(256-2346) DTIM(1-255) Radio	Check All Clear All dlink Auto Clear All Clear All dlink Auto Clear All Clear All
	<back next=""> Cancel</back>
Security 11g	
Authentication Open System Key Settings Encryption Enable Key Type HEX Key Value WPA Cipher Type AUTO Grou PassPhrase Radius Server Radius Secret	Key Size 64 Bits Valid Key First up Key Update interval 1800 Port 1812 Key Back Next > Cancel
Filter 11g	X
IEEE802.11g Wireless MAC ACL Sett Access Control Accept MAC Address	
	< Back Next > Cancel

MAC Filter

Check the box to select the configuration contents included in this template. For how to configure MAC filter settings, please refer to page 83.

Device By Group: By IP:	The APs that belong to the group will apply the template. Select the APs by IP that will	Device Image: Constraint of the system Image: By Group By Group By Group Image: Sort Image: DAP-2530 Model Image: DWL-2700AP Model Image: DWL-3200AP Image: DWL-3200AP Image: DWL-3200AP Image: DWL-3200AP Image: DWL-3200AP Image: DWL-3200AP Image: DWL-3200AP Image: DWL-320AP <
	apply the template.	
		< Back Next> Cancel
Update	To configure the runtime of	Sahadula 💎
opullo	template, please choose the device object first.	C Disable C Disable Specify Time C Snerifu Interval
Specify Time:	template, please choose the device object first. Specify the day time that will apply the template. The template will run at certain	⊂ Disable
	template, please choose the device object first. Specify the day time that will apply the template. The template will run at certain day(s) of every week. Specify the interval time to	⊂ Disable
Specify Time:	template, please choose the device object first. Specify the day time that will apply the template. The template will run at certain day(s) of every week.	 C Disable Interval Specify Interval Specify Date Monday □ Tuesday □ Wednesday □ Thursday Friday □ Saturday □ Sunday

After the configuration, the template will be listed in the template window. The **NextRun Time** column shows the running time of the template. When the running time arrived, the template will apply the configured parameters to the devices selected in the **Device** selection window. If multi-APs are selected, AP Manager II will apply the template to all the APs that selected at the same time.

Template Name	Creator	Create Date	Activity Status	Next Run Time	Status	Result
😑 Default Template	System	2008/01/10	Disabled	Unknown		
😑 Test	admin	2008/06/13	Enabled	2008/07/13 14:02:16		

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.

Update						×
General	System	Wireless 11g S	ecurity 11g F	Filter 11g Dev	rice Schedule	L,
Basic	: Info					
Nam	ie:	<u>dlink</u>				
Crea	ator :	admin				
Time	e:	2008- 6-11	_			
	ent Selecti	on				
	System					
▼ \	Wireless	11A 🗖	11G 🗹			
	Security	11A 🗖	11G 🗹			
I I F	Filter	11A 🗖	11G 🗹			
				OK	Cancel	

For how to configure the items in this page, please refer to page 109.

Delete a template

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

Run a template

If you want to apply the template immediately, right-click the template, and select **Run** item from the drop-down menu. The **Status** column will show the progress of this operation, and the **Result** column show the operation result.

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 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.

Fault Manage

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

	Event Name	Event Type	Event Level	Date Time	Source	Description
- 💼 All Space	🧇 PollingFailed	System	Notice	2008-06-11 14:4	192.168.0.50	Indicate th
General	🧇 PollingFailed	System	Notice	2008-06-11 14:4	192.168.0.50	Indicate th
🕂 🦲 Group	🧇 PollingFailed	System	Notice	2008-06-11 14:4	192.168.0.50	Indicate th
Ŧ 🦲 MultiConfiguration	🧇 PollingFailed	System	Notice	2008-06-11 14:4	192, 168, 0, 50	Indicate th
🖹 🔄 Fault Manage						
StandardTrap						
- System						
Threshold						
Private						
🔁 🛄 Tool						
- C Report Association						
Security						
Utilization						
Channel						
Rogue AP						
SysLog						

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 128.
- Threshold: The Threshold view window displays the threshold notice data. To enable the threshold notice, please refer to page 128
- 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.

vent				
- Event Type	SnmpVersion	SNMP VI		~
- StandardTxap ColdStart WarmStart	Event Name	StandardTrap		
LinkDown LinkUp AuthenticationFailure	Trap Generic	ColdStart(0)		~
EgpNeighborLoss ColdStart(snmpv2)	Status	C Disable	Enable	
WarmStart(snmpv2) LinkDown(snmpv2)	OID			
- LinkUp(snmpv2) - AuthenticationFailure(snmpv2) - System Event	Description			
PollingFailed PollingOk	Level	Critical		•
Threshold Event	Threshold Enab	le		
TransmitThreshold	Ascending	0		
	Descending	0		
	New	Save	Delete	Close

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

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

Event Settings		×
Event		
- Event Type	SnmpVersion	SNMP V2C
- StandardTrap		·
ColdStart	Event Name	
WarmStart		
LinkDown		
LinkUp	Trap Generic	EnterpriseSpecific(6)
- AuthenticationFailure		
EgpNeighborLoss	Status	C Disable 💿 Enable
ColdStart(snmpv2)		
WarmStart(snmpv2)	OID	
LinkDown(snmpv2)		
LinkUp(snmpv2)	Description	
AuthenticationFailure(snmpv2)		
- System Event	Level	Critical
PollingFailed PollingOk	Tever	
Threshold Event	Threshold Enab	•
TransmitThreshold	✓ I hreshold Enab	
+ Private	Ascending	0
	Descending	0
		1 1 1
	New	Save Delete Close

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 **Line** 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.

Notice Settings	
Warning Level	- Notice Settings
Critical	Play sound
Error Warning Notice	Sound File Browse
	🔲 Show Pop Message
	🔲 Send Email
	To Email Address
	From Email Address
	SMTP Server
	User Name
	Password [Optional]
	Subject
	Message
	Ok Apply Cancel

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.

🖳 🎑 🥥 💭 · 🔂 🛃 ·					
ent Type	Event Level	Date Time	Create Watchlist	ription	
stem	Notice	2008-06-04 10:58:09	Update Watchlist	ate the	
stem	Notice	2008-06-04 10:58:09	Delete Watchlist	ate the	
stem	Notice	2008-06-04 09:49:09	192.168.0.50 Indi	cate the	
stem	Notice	2008-06-04 09:33:20	192.168.0.50 Indi	cate the	
chom	Notico	2000 02 02 10,40,21	102 149 0 42 Toda	anto the	

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

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

Notes: 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 **Delete watch list** item under the icon it 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.



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.

Open	2 🗙
Look in: 📋 My Documents 💽 🔶 🖻 👩	* 💷 •
My Music	
Scan AP	
武接收到的文件 冠 我的共享文件夹	
File name:	Open
Files of type: JPEG File (*.jpg)	Cancel
Picture Display Style Adjust the size of the canvas to fit the pict	
	//

After the successful loading:



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

Grid line and rulers:

To hide the grid line or ruler, click the **Grid** or **Ruler** item from the right-click menu, as shown below.



To show the grid and ruler, click the **Grid** or **Ruler** item from the right-click menu again.

Topology size

To change the topology size, click the **Topology Size** item from the right-click menu, as shown below.

Can¥as Setting	×
Canvas Width:	300
Canvas Height:	300
(OK)	Cancel

The area in the textbox is the valid area.

Line

You can insert lines into map to more efficiently organize the APs. To insert a line, click the **Insert line** item from the 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.

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.

Y ScanAP			
File View Help			
Scan Information			Chait
BSSID	SSID Chann	el Aul	
			Total
			100
			80
			8 60 8 240
			20
<	1	>	16:48 16:49 16:50 16:51 16:52 16:53 16:54 16:55 16:56 16:57 16:58 16:59
Wireless Adapters			
Location ID	Location4		
Interval Time	6		
	720 Seconds		
Total Time	720 Seconds		
Description	LocationA		
Wireless Adapters	1		
Last Scan At			
	1900-01-01 00:00:01		
Scheduled Next Sca	n 1900-01-01 00:00:01		
1			
Start	Stop		
eady			2008-6-11 16:47:40

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

Select			*
Please select APs-			
BSSID	SSID	Channel	Authentication
00:e0:4c:8c:86:71	ella_test_333	10	Yes
00:03:7f:be:ef:11	3200_test	6	No
00:0c:43:28:60:d8	C300BRS4	6	No
00:03:7f:be:f1:98	ChinaNetwww	3	No
00:03:7f:be:f0:43	dlink	13	No
00:1c:f0:18:fb:69	dlink	11	No
00:27:41:72:25:01	dlink-kwest	6	No
00:80:c8:19:1c:11	dlink	6	No
00:60:b3:27:fc:16	KangTe-11g	8	Yes
<	Ш		>
	-		
Select		Cancel	

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:

Save in	: 🔁 Scan AP		•	(= 🗈 💣 📰	-
My Recent Documents Desktop My Documents					
My Computer	File name:	LocationA.stp		-	Save
					Cancel

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.

Open			? 🗙
Look in: 隘	Scan AP	• 🔁 🕐	* 💷 *
LocationA.			
File name:			Open
Files of type:	SitePlanning Files (*.stp)	•	Cancel
	🔲 Open as read-only		

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

ocalID(BSSID)	Start Time(Band)	Interval Time(avgRSSI)	Lenth(MaxRSSI)	Description(MinRS	SI)
🔄 🔄 LocationA	2008-2-21 14:24:42	6 seconds	00:12:12(732 seconds)	LocationA	
🔄 🔁 LocationB	2008-2-21 14:38:47	10 seconds	00:20:20(1220 seconds)	LocationB	
1					
y DateTime					
y DateTime		LocationB			
		LocationB			Legend
100		LocationB			Legend
100		LocationB		~	00:50:00:22:09:10 11A
100		LocationB		$\overline{\Lambda}$	00:50:00:22:09:10 11A 00:1c:f0:18:fb:69 11G
		LocationB			00:50:00:22:09:10 11A 00:16:f0:18:fb:69 11G 00:05:5d:51:31:99 11G 00:50:00:23:10:14 11G
2 ₄₀		LocationB			00:50:00:22:09:10 11A 00:10:f0:18:fb:69 11G 00:05:5d:51:31:99 11G 00:50:00:23:10:14 11G 00:13:46:e5:30:b2 11G
		LocationB			00:50:00:22:09:10 11A 00:10:f0:18:fb:69 11G 00:05:5d:51:31:99 11G 00:50:00:23:10:14 11G 00:13:46:e5:30:b2 11G
					Legend 00:50:00:22:09:10 11A 00:16:10:18 fb:58 116 00:05:5d:51:31:39 116 00:50:00:23:10:14 116 00:13:46:s5:36:b2 116 00:03:7f:bef2:16 116
	14:42 14:44 14:45	LocationB		14:57	00:50:00:22:09:10 11A 00:10:f0:18:fb:69 11G 00:05:5d:51:31:99 11G 00:50:00:23:10:14 11G 00:13:46:e5:30:b2 11G

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



Report

Association

The association window shows the managed APs and their associated client stations. Highlight an Access Point and the details of the client stations that associated with the AP list. The detail information include: DateTime, SSID, MAC Address, Band, Authentication, RSSI and Power save mode.

	MAC Address	IP A	ldress	SSID	Status		
WL-3200AP	001346FDB4F8	172.1	18.215.50		Done		
	001346FDB4F8	172.1	18.215.50	DWL-3200AP	802.11b/g		
WL-8200AP	001195F1C110		168.0.50		Done		
	001195F1C110		168.0.50	8200g	802.11b/g		
	001195F1C110	192.1	168.0.50	8200a	802.11a		
itation Detail DateTime	SSID		MAC Address	5 Band	Authentication	RSSI	Power Sa
•							Þ

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

To list the APs according to the detected date, choose the date range from the **From/To** drop-down menu, and click the **Search** 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.

All Space	2008- 6-11 💌	Co 2008- 6-11 💌	Search							Export Text
🗧 General 🕈 🦲 Group	DateTime	IP Address	Мая	STA's Number	UpTime	Trasmitted Packets	Trasmitted Success Rate	Trasmitted Retry Rate	Band	
+ 🛄 MultiConfiguration + 🛄 Fault Manage										
+ 🛄 Tool										
- Report										
Security										
- Channel		Se	leet							
Rogue AP		-								
Of an of			DAP-2590	00055D9898	10 192.168.	0.50 255.255.25	5.0			
					Select	Cancel	1			
		1	🗌 Selete from (CustomGroup —		1	_			
		-								
	- Polling Detail									
	Polling Interval 5	minutes Change	Scheduled N	ext Poll 2008-06-	11 15:20:38	Enable Thresho	ld Notice	Start		
			_		11 15:20:38	Threshold Column	TransSuccessRal -	End		
	Dependency	one Change	2 Call offer	AT 2000-00-	.11 15.20.50		1			
	1									
	2008-06-11 15:2	0:05 FTP Server	started on po	rt 21.						
	2008-06-11 15:2 2008-06-11 15:2	0:06 SnmpTrap in 0:19 Discourse Co	nitializtion suc	cessi						
	2000-00-11 15.2	0:20 Device: 192.	mpieleui							

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.

9				SSID	RSSI		_
	001CF008E638	WPA-Auto-Personal	802.11g		80 %		-
9	001CF008E639	WPA-Auto-Personal	802.11g	wireless test team	76 %		
8	0060B327FC16	WEP	802.11g	KangTe-11g	28 %		- In
		OFF					- 11
							- 11
							- 11
							- 11
							- 11
							- 11
							- 11
							- 11
							- 11
6	001B118C494C	OFF	802.11g		86 %		
6	00119594EB80	WPA-Personal	802.11g	gabriel	66 %		
6	0050F1121210	OFF	802.11g	E1131	40 %		
1	0060B38E51A8	OFF	802.11g	UNICOM	18 %		
1	00030F0ED78F	OFF	802.11g	DCW-BR54+	26 %		Ŧ
	ODAOEDEOEEEA		000.44	allia Leine A	(4.0)		<u> </u>
Channel	BSSID	Security	Mode	SSID	RSSI		
13	00037FBEF043	OFF	802.11g	dlink	42 %		
							-1
							-11
							-11
							-11
							-#
							-11
							-11
							=1
	1	1				Detect Delete	
	3 13 11 11 11 11 11 11 11 16 6 6 6 6 6 6 6 6 6 6 6 6 6	3 001195F1C118 13 000375EF035 11 001811A8A608 11 001811A8A608 11 001871A8A608 11 001874010AA2 11 0018707972C0 10 0018707972C0 10 0018707972C0 10 00550559312 10 00550559352 10 00550559352 10 005505555 10 00550555 10 0055055 10 0055055 10 00550555 10 0055055 10 0055055 10 00550555 10 00550555 10 0055055 10 00550555 10 00550555 10 0055055 10 0055055 10 00550555 10 0055055	3 001195FLC118 OFF 13 00037FBEFG03F OFF 11 00181LA8Ac08 WEP 11 00038FEFACF OFF 11 001038FEFACF OFF 11 001038FEFACF OFF 11 001038FEFACF OFF 11 00161/346350037 OFF 6 01346350037 OFF 6 00050559312 OFF 6 00050859312 OFF 6 00508A10004 OFF 6 00201330A1 WEP 6 001B11904FE WEP 6 001B11904FE WEP 6 001B11904FE WEP 6 001B11904FE OFF 1 006083851A8 OFF 1 005071121210 OFF	3 0011997+[C118] OFF 802.11g 13 000379EF030 OFF 802.11g 11 001811A8A608 WEP 802.11g 11 00038FEFAC70 OFF 802.11g 11 001038FEFAC70 OFF 802.11g 11 001038FEFAC70 OFF 802.11g 11 0015709720 OFF 802.11g 6 013709720 OFF 802.11g 6 00350539312 OFF 802.11g 6 000550539312 OFF 802.11g 6 0055063010004 OFF 802.11g 6 00550639312 OFF 802.11g 6 0055063010004 OFF 802.11g 6 005064010004 OFF 802.11g 6 005064218606 OFF 802.11g 6 00506418606 OFF 802.11g 6 00507112120 OFF 802.11g 6 005071121210 OFF 802.11g	3 001195FLC118 OFF 802.11g at200g 13 000375FEFG05 OFF 802.11g dirk.p 11 00036FEFAC05 OFF 802.11g USEC-CNC 11 00036FEFAC05 OFF 802.11g USEC-CNC 11 001036FEFAC05 OFF 802.11g SCAC-MOT-CD-SL. 11 001036FEFAC7 OFF 802.11g SCAC-MOT-CD-SL. 11 001074010AA2 WEP 802.11g SCAC-MOT-CD-SL. 16 0130749720C0 OFF 802.11g Hink.ACD 6 01055059312 OFF 802.11g Hink.ACD 6 00055059312 OFF 802.11g dHink.ACD 6 00055059312 OFF 802.11g dHink.ACD 6 00055059312 OFF 802.11g dHink.ACD 6 0005905622 OFF 802.11g dHink.ACD 6 0005905620 OFF 802.11g dHink.hoo0000000. 6 00059119032FE<	3 001195FLC118 OFF 802.11g 8200g 20 % 13 000375FEFG05 OFF 802.11g dikk.p.p 48 % 11 001811A8A08 WEP 802.11g USEE-CNC 44 % 11 00038FEFACF0 OFF 802.11g USEE-CNC 44 % 11 001038FEFACF0 OFF 802.11g SCCAV-(MOT-CD-SL) 10 % 11 00103707972C0 OFF 802.11g SCCAV-(MOT-CD-SL) 10 % 6 013707972C0 OFF 802.11g dink. 50 % 10 % 6 00055053912 OFF 802.11g dink.4000-41a 24 % 6 00055053912 OFF 802.11g dink.4000-41a 24 % 6 00055053912 OFF 802.11g dink.4000-41a 24 % 6 005505A100004 OFF 802.11g dink.4000-41a 24 % 6 005605A100004 OFF 802.11g dink.4000-40a 28 % 6 0056046318	3 001195F1C118 OFF 802.119 8200g 20% 13 000175FEF035 OFF 802.119 dink, p.0 48 % 11 001811A8A08 WEP 802.119 USEF-CNC 44 % 11 00103FFEF035 OFF 802.119 USEF-CNC 44 % 11 00103FFEF035 OFF 802.119 CVC-SC2 8 % 11 001074010AA2 WEP 802.119 SCCAC-MOT-CD-SX 10 % 11 00157079720 OFF 802.119 SCCAC-MOT-CD-SX 10 % 6 01054058051 WEP 802.119 Perta CD 18 % 6 00055053912 OFF 802.119 HT_APD 42 % 6 00550640004 OFF 802.119 dink-dio-04a 10 % 6 00550640004 OFF 802.119 dink-brossocooco 28 % 6 00560403626 OFF 802.119 dink-brossocooco 28 % 6 00511002FF

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 106.

	Facility	Priority	Timestamp	Sender	Message
6	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
6	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]WLANO Normal AP ready
S	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
6	1	5	2008-5-9 11:11:05	172.18.215.50	[SYS]Web logout from 172.18.215.111

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.

Iser Lanage			
User User Name	Password	Privilege	Creat Date
admin	admin	Administrator	
<			>
Add	Update	Delete	
Name	Passw	ord	
Privilege Manager	•		
Resume			
Resume			

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 **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.

tion		×					
Logon Setting • To use the sy • Please selec	ystem, user shou	Id input name		sword			
User Name	Privilege	Creat Date			Resum	в	
admin	Administra						
<u><</u>						>	
SNMP Setting				161			
Public Community		public	Port	161			
Private Communi		private					
SNMP Response	e TimeOut	30					
Polling Setting		<u> </u>					
Polling type Interval time	Oisable	🔿 Enable	9				
	30	(10-60sec)					
Discover Retry	1	TimeOut	5		(5-60sec	:)	
L							
			OK		Cance	1	Apply

Logon SettingSet 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 SettingSet the Public/Private Community String, Port number and SNMP
Response Timeout.Polling SettingDisable by default. When this function is enabled, you must set the
polling interval time, it is 30 seconds by default.DiscoverEnter the Retry number and the time of timeout when discovering.

Option			
General Module Database Maintenance Advance			
Select firmware file			
Model Name	Firmware file		
DAP-2590 DWL-2700AP			
DWL-3200AP	Save	Brow	vse
DWL-7700AP DWL-8200AP	Module Information-		
	Model Name	DAP-2590	
	Description	AP Manager II Module v1.00r05 (200)8-6-4)
	Version:	1.00	
	Support Band:	11b/g/n	
		OK Cancel	Apply

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.

Option	
General Module Database Maintenance Advance	
Select Fault Notice By Records To ensure the database efficient, Please notice user to clear the database Notice user when records	
Clear Rule Clear Bule Clear Bule Delete all records Records: 100 Delete these records before the datetime Datetime: 2008- 6-11	
	Clear
OK Cancel	Apply

Select Choose the type of records.

Notice By Recor d Set the number that record reach to notice the user to clear the database.

Clear RuleDelete 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.

Option	X
General Module Database Maintenance	Advance
TimeOut Settings	
Set Timeout(s)	5
Reboot Timeout(s)	50
Configuration Flash Update Time(s)	60
Factory Reset Time(s)	60
F/W Download Time(s)	60
F/W Flash Update Time(s)	80
Timing Tolerance Time(s)	5 Defaul
FTP Server © Enable Local FTP Server © Enable Remote FTP Server Remote Server IP Address User Name Password Port Language Default (English)	0.0.0.0 admin xxxxxx 21 Trest
	OK Cancel Apply

TimeOut Setting | Configure the system time out settings.

Select Enable Local FTP Server to run an ftp server on the local computer. The ftp server will run when AP Manager II starts. Select Enable Remote FTP Server if all the system logs are stored in a lone ftp server. You should configure the ftp server parameters here.
 Language Select an interface language for AP Manager II. It only supports English now.

Contacting Technical Support

Technical Support

You can find software updates and user documentation on the D-Link website.

U.S. and Canadian customers can contact D-Link Technical Support through our website, or by phone.

Tech Support for customers within the United States: D-Link Technical Support over the Telephone: (877) 354-6555

> *D-Link Technical Support over the Internet:* http://support.dlink.com

Tech Support for customers within Canada: D-Link Technical Support over the Telephone: (877) 354-6560

> *D-Link Technical Support over the Internet:* http://support.dlink.com

> > Version 2.0 June 18, 2008



Release 2.00

AP Manager II

User Manual

Table of Contents

Getting Started	
Requirements	
Minimum System Requirements	
Minimum Software Requirements	
Access Point Requirements	
Installation	
Install MySQL Server	
Install AP Manager II	
Using AP Manager II	
General View	
Discovering Devices	
Access Point Report	
Station Report	
Model Report	
Band Report	
Group View.	16
Configuration	
Set IP	
Update Configuration	
Upgrade Firmware	
Web Manage	
Telnet	
Set Password	
Sorting	
View	
Property	
Configuring 802.11a/b/g APs with AP Manager II	
Home > Information	
Basic > Wireless	
Basic > Wireless > Authentication	
Basic > Wireless > Access Point > WEP Encryption	
Basic > Wireless > Access Point > WPA/WPA2 - Enterprise	
Basic > Wireless > Access Point > WPA/WPA2 - Personal	
Basic > Wireless > WDS	
Basic > Wireless > WDS with AP	
Basic > LAN > Dynamic (DHCP)	
Basic > LAN > Static (Manual)	
Advanced > Performance > 802.11a	
Advanced > Performance > 802.11g	
Advanced > Filter > Wireless MAC ACL	
Advanced > Filter > Wireless MAC ACL	
Advanced > Grouping > AP Grouping Settings	
Advanced > DHCP Server > Dynamic Pool Settings	
Advanced > DHCP Server > Static Pool Settings	
Advanced > DHCP Server > Current IP Mapping List	
Advanced > Multi-SSID	
Advanced > Rogue AP	
Tools > Admin	
Tools > Firmware and SSL	
Tools > Configuration File	

Tools > SNTP	
Status > Device Information	
Status > Stats	
Status > Client Information	
Status > WDS Information	
Status > Log > Log View	
Status $> Log > Log$ Settings	
System	
Configuring 802.11n APs with AP Manager II	
Home > Information	
Basic > Wireless	
Basic > Wireless > Authentication	
Basic > Wireless > Access Point > WEP Encryption	
Basic > Wireless > Access Point > WPA/WPA2 - Enterprise	
Basic > Wireless > Access Point > WPA/WPA2 - Personal	
Basic > Wireless > WDS	
Basic > Wireless > WDS with AP	
Basic > Wireless > Wireless Client	
Basic > LAN > Dynamic (DHCP)	
Basic > LAN > Static (Manual)	
Advanced > Performance > Mixed 802.11n, 802.11g and 802.11b	
Advanced > Performance > Mixed 802.11g and 802.11b	
Advanced > Filter > Wireless MAC ACL	
Advanced > Filter > Wireless MAC ACL	
Advanced > DHCP Server > Dynamic Pool Settings	
Advanced > DHCP Server > Static Pool Settings	
Advanced > DHCP Server > Current IP Mapping List	
Advanced > Multi-SSID	
Advanced > Intrusion	
Advanced > VLAN	
Advanced > VLAN > Add/Edit VLAN	
Advanced > VLAN > PVID Setting	
Advanced > QoS	
Advanced > Schedule	
Maintenance > Admin	
Maintenance > Firmware and SSL	
Maintenance > Configuration File	
Maintenance > SNTP	
Status > Device Information	
Status > Stats > WLAN Traffic Statistics Status > Stats > Ethernet Traffic Statistics	
Status > Client Information	
Status > WDS Information	
Status > $Log > Log View$	
Status > Log > Log Settings	
System	
Multiconfiguration	
Create a new template	
Edit a template	
Delete a template	
Run a template	
Import or export a template	
Fault Manage	114
Event settings	
Event Settings	
Event Export	

Notice setting	
Watch list	
Tools	
Topology	
New topology view	
Background	
Grid line and rulers:	
Topology size	
Line	
Site Planning	
Collect information	
Load information	
Report	
Association	
Security	
Utilization	
Channel	
Rogue AP	
Syslog	
User Management	
System Environment	

Getting Started

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, organize and sort your APs into manageable groups.

Requirements

Minimum System Requirements

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

Minimum Software Requirements

- MySQL Server 5.0
- Mysql-connector-odbc-3.51

Access Point Requirements

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

Installation

Install MySQL Server

Before installing AP Manager II on your computer, you must first install MySQL© Server 5.0 and MySQL© ODBC Connector. During the AP Manager II install process, AP Manager II will check if these MySQL© programs have been installed. If they are not found, you will be reminded to download them.

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

MySQL© Server 5.0: http://dev.mysql.com/downloads/mysql/5.0.html.

MySQL© ODBC Connector 3.51: http://dev.mysql.com/downloads/connector/odbc/3.51.html

MySQL© 5.0 Reference Manual: http://dev.mysql.com/doc/refman/5.0/en/index.html.

Install AP Manager II

Once the MySQL Server 5.0 and MySQL ODBC Connector 3.51 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.

InstallShield Wizard
Choose Destination Location Select folder where Setup will install files.
Setup will install AP Manager II in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\D-Link\AP Manager II Browse
nstallShield

Select Components

You are then given the option to select which components you want to install and which you do not. By default, the AP Manager II software and all AP modules are selected. Click **Next** to continue.

InstallShield Wizard		
Select Components Choose the components Setup will install.		
Select the components you want to instal install. Program DWL.770AP Module DWL270AP Module DWL8200AP Module DWL8200AP Module DWL8200AP Module DWL8200AP Module	I, and clear the c	omponents you do not want to Description AP Manager II Components
Space Required on C: Space Available on C: InstallShield	0 K 9711888 K	
	< <u>B</u> ack	< <u>N</u> ext> Cancel

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.

InstallShield Wizard		
Select Program Folder Please select a program folder.		R.
Setup will add program icons to the Program F name, or select one from the existing folders lis Program Folders: [AP Manager I]]	older listed below. You may type a x. Click Next to continue.	new folder
Existing Folders: Administrative Tools Catabust Control Center Catabust Control Center O-Link, ProwerDVD O-Link, ProwerDVD D-Link AirPermier AG D/vL-AG530 D-Link AirPermier AP Managet FlexibleSoft Co- Games		<
InstallShield	< Back Next >	Cancel
Configure MySQL Connector

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

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

Configure MySQL Connector							
	Configure MySQL Connector Setting the connecting parameter						
Setup config conne	gure the MyS	te the copying file. Before you run AP Manager II, you must iQL Connector. click Next. to start configure the MySQL					
	Server	127.0.0.1					
	User	root					
	Password	200					
	Database	aբm2db					
InstallShield							
		< Back Next > Cancel					
Configure MySC							
configure myse	ir Connec	tor					
Configure	MySQL Co						
Configure Setting Setup config	MySQL Co g the connect o has comple gure the	onnector					
Configure Setting Setup config	MySQL Co g the connect o has comple gure the	ennector titing parameter ete the copying file. Before you run AP Manager II, you must MySQL					
Configure Setting Setup config	MySQL Co g the connect o has comple gure the ector. Info	ting parameter					
Configure Setting Setup config	MySQL Co g the connect o has comple gure the sector. Info Ser Use Password	ennector ting parameter ting parameter te the copying file. Before you run AP Manager II, you must mation Configure MySQL Connector successII OK					
Configure Setting Setup config	MySQL Ca g the connect of has complet gure to the gure to the sector. Info Ser Use	ting parameter ting parameter te the copying file. Before you run AP Manager II, you must mation Configure MySQL Connector success!!					
Configure Setting Setup config	MySQL Co g the connect o has comple gure the sector. Info Ser Use Password	ennector ting parameter ting parameter te the copying file. Before you run AP Manager II, you must mation Configure MySQL Connector successII OK					

Install Complete!

When the InstallSheild Wizard has completed, you are given the option to launch the AP Manager II program. Check the box to run AP Manager II and click **Finish** to complete the installation.



If you checked the "Run AP Manager II" box 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

😵 Set Program Access and Defaults		🛅 VideoLAN	×
😻 Windows Catalog		m D-Link AirPremier AG DWL-AG530	۲
🌯 Windows Update		🛅 VistaBootPRO 3.3	۲
去 Program Updates			
m Accessories	•		
🛅 Administrative Tools	×		
🛅 Games	•		
🛅 D-Link	٠		
🛅 D-Link AirPremier AP Manager	•		
🛅 D-Link AP Manager II	•	🚊 - AP Manager II	

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

AP Manager II								
≦ystem ⊻iew <u>H</u> elp								
	🗎 🔝							
All Space General + Group + MultiCcnfiguration + Fault Manage Report Association Security Utilization Channel	AccessPoint Station	n Report Model Repor		1			Legend Un-manage	•
	MAC Address	IP Address	Band	Authentication	RSSI	SSID	Power Save Mode	
								_
	2007-06-29 09:4	49:16 FTP Server 49:16 Trying to re 49:16 SnmpTrap i	gister for traps	on port 162		1		
Ready	22 E		T				LogUser adm	in

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.

Standard discovery

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

	🗎 🚺 🛃	3 🔜 🚢	•	-
All Space General General General General Group Fault Manage Group Fault Manage Group Report Association Gecurity Utilization Channel Rogue AP SysLog	IP Address	Model Name Discover Delete Refresh Sign Rogue AP Configuration Sorting View By Property	MAC Address	NetMask

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.

Advance Dis	cover	X
_Method		
Start IP:	192 . 168 . 0 . 50	Start
End IP:	192 . 168 . 0 . 100	Cancel
Community	public	
TimeOut	30	
L		

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 record according to its type.

Explanation of icons:

- Manageable 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-click 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.

								^
All Space General Group Group Group Group Group Group Group Group Group Grout Group Grout Grout	AccessPoint Statio	n Report Model Repor		ccessPoint Report			Legend Un-en anage	
	MAC Address	IP Address	Band	Authentication	RSSI	SSID	Power Save Mode	
	2007-06-29 09:	49:16 FTP Server 49:16 Trying to re 49:16 SnmpTrap i	gister for traps	on port 162				

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

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.

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

Station Report

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

🗖 🗖 🗍 🏶 🄮									
									-
- All Space		Station Report							
+ MultiConfiguration + Report - Report - Security - Utilization - Channel									Ligand B22.11g
	AccessPont Station	n Report Model Keport	Band Report						
	Station Detail				2.2	200			
	MAC Address	IP Address	Band	Authentication	RSSI	SSID	Power Save Mode		
	004096AF74B7	10.24.69.177	802.11g	WPA-Personal	98	Multi-SSID 1	Off		
	1. L.								
	2007-05-05 13:4	15:38 Device: 10.2	4.69.177 SNMP	Ping Ok!					
	2007-05-05 15:4	19:38 Device: 10.2	4.69.177 SNMP	Ping TimeOut!					
	2007-05-05 15:0	50:37 Device: 10.2 10:38 Device: 10.2	4.69.177 SNMP	Ping TimeOut!					
	2007-05-05 16:0	11:07 Device: 10.2	4.69.177 SNMP	Ping Ok!					
Readv									LooUser admin

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. It shows the numbers of every model.



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 five models of D-Link Access Points - the DAP-2590, DWL-2700AP, DWL-3200AP, DWL-7700AP, and the DWL-8200AP. 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.

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

🔲 🔲 🔲 🍪 🎦	🗎 🖬 🥵	🛃 🕌	🕒 - 🔛 ·		
	IP Address	Model Name	MAC Address	NetMask	FW version
All Space General Group Model DWL-7700AP DWL-2700AP DWL-8200AP DWL-8200AP DWL-3200AP DAP-2590 + Category1 Category2 Category3	🥌 192. 168. 0. 50	DAP-2590	00055D989810	255. 255. 255. 0	1.00

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

Configuration

Any individual 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.

	🗎 🚺 🌌	🔝 🚢 🕒	• 🖳 • 🟹
	IP Address	Model Name MAC A	Address NetMask
 All Space General Group Model DWL-7700AP DWL-2700AP DWL-8200AP DWL-3200AP DWL-3200AP DAP-2590 Category1 Category2 Category3 MultiConfiguration Fault Manage Tool Report 	192. 168. 0. 50	DA Discover Delete Refresh Sign Rogue AP Configuration > Sorting View By Property	D989810 255.255.0 Set IP Update Config Upgrade Firmware Web manage Telnet Set Password

Under the Configuration menu entry, you can select **Set IP, Update Config, Upgrade Firmware, Web manage, Telnet,** or **Set Password**. 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.

Set IP					X	
IP Address	192	. 168	. 0	. 50		
Subnet Mask	255	. 255	. 255	. 0	1	
Default Gateway	0	. 0	. 0	. 0]	
OK Cancel						

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



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).

Home Basic Advance	ed Tools Status System Help		
Home	Information 👻		(
\$	System Information		
Information	Model Name	DWL-3200AP	
	System Time	Not Available	
	Up Time	0:00:25.00	
	Firmware Version	v2.40	
	IP address	192.168.0.50	
Basic			
Advanced			
Tools			
Status			
System			
Ok!			

Note: See the section "**Configuring 802.11a/b/g 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.

ι	JP Firmware					×
	Module Name	Firmware		Edit	[-
	DWL-3200AP	riniware		Edit		
	·					
		ок	Cancel	1		

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

Open	? 🔀
Look in: 隘) Firmware 💽 🗢 🛅 📰 -
DWL3200	AP-firmware-v310-r0103.tfp
File name:	DWL3200AP-firmware-v310-r0103.tfp Open
Files of type:	firmware file(*.tfp)
	C Open as read-only

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

UP Firmware				X
Module Name	Firmware		Edit	
DWL-3200AP	C:\Documents and Set	tings\Benjamin.c	Edit	
	ок	Cancel		

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 Manage

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.

Connect to 192.16	8.0.50 🛛 🛛 🔀
R	GA
DWL-3200AP User name: [Password: [
ſ	Remember my password

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 then 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 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 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.

Press Enter to login
D-link Corp. Access Point login: admin Password:
Atheros Access Point Rev 4.1.2.56 D-link Corp. Access Point wlan1 ->

Set Password

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.

Set Passwor	d		
Set the password	for AP		
User Name	admin		-
Password			
	Ok	Cancel	

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 Type - 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, Rougue 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.

Create Group					×
Basic Infor					
Group Name					
Create Date	2008- 6-11	* *	Create By	admin	
- Remark					
– Manager memeber –					
Available member	:			Selected member	
Everyone	-	>>		Everyone	
		<<	_		
[Ok		Cancel		

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 💌.

	IP Address	Model Name	MAC Address	NetMask	FW version	Lo
🖃 📳 All Space	🔿 172.18.213.35	DWL-7700AP	0050002209AA	255.255.255.0	v3.20	
General	92.168.5.82	DWL-8200AP	001CF008E630	255.255.255.0	v2.10	
🚊 🔄 Group	192.168.0.50	DAP-2590	00055D898760	255.255.255.0	2.0	
🕀 🦲 Model						

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 rightclicking the AP in the Group View window and selecting Property - as shown below.

P	roperty		X
	-Basic Informati	on	
	Model Name	DAP-2590	
	MAC Address	00055D989810	
	IP Address	192 . 168 . O . SO	
	Location		
	Quer	y Set Cancel	

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

Configuring 802.11a/b/g 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).

Home Basic Advan	ced Tools Status System H	elp	1
Home	Information 👻		
S	System Information		
Information	Model Name	DWL-3200AP	
	System Time	Not Available	
	Up Time	0:00:25.00	
	Firmware Version	v2.40	
	IP address	192.168.0.50	
Basic			
Advanced			
Tools			
Status			
System			
Ok!			

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
--------	-------------

Home Basic Advar	nced Tools Status System H	elp	
Home	Information 👻		
\$	System Information		
Information	Model Name	DWL-3200AP	
	System Time	Not Available	
	Up Time	0.00:25.00	
	Firmware Version	v2.40	
	IP address	192.168.0.50	
Basic			
Advanced			
Tools			
Status			
System			
Ok!			

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 references both 802.11a and 802.11g configuration settings.

Basic > Wireless

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode Access Point
Š	SSID dlink
LAN	SSID Broadcast Enable -
	Channel 44 💌 5.22 GHz 💌 Auto Channel Scan
	Authentication Open System 💌
	Key Settings
	Encryption Enable Key Size 64 Bits
	Valid Key First Key Type HEX
	First Key Second Key
	Third Key Fourth Key
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Wireless Band:	Select the wireless band to configure, 802.11a or 802.11g.			
SSID:	The Service Set (network) Identifier of your wireless network.			
SSID Broadcast:	······································			
Channel:	Allows you to select a channel if the Auto Channel Scan is unchecked.			
	The channel of an 802.11a network may not be set manually in certain regions (e.g. Europe and USA) in order to comply with DFS (Dynamic Frequency Selection).			
AP Mode:	There are 3 AP modes:			
	Access Point			
	WDS with AP			
	WDS			
	Please see the following pages for an explanation of all the AP modes.			

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless LAN	AP Mode Access Point SSID dlink SSID Broadcast Enable Channel 40 40 5.2 GHz Auto Channel Scan Authentication WPA-Personal Key Settings Open System / Shared Key Encryption Disable WPA-Personal WPA-Personal WPA-Enterprise Pe HEX WPA-Personal WPA-Enterprise WPA-Personal WPA-Enterprise WPA-Personal WPA-Enterprise Valid Key First Key WPA-Auto-Personal WPA-Auto-Enterprise It Key Third Key Fourth Key
Advanced	
Tools	Apply
Status	
System	
Get OK,	

Basic > Wireless > Authentication

Open System: The key is communicated across the network. Shared Key: Limited to communication with devices that share the same WEP settings. Both: The key is communicated and identical WEP settings are required. Select Open System/Shared Key to allow either form of data Authentication: 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
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
	WFA-AULO-FEISUIIdi

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode Access Point
	SSID dlink
LAN	SSID Broadcast
	Channel 5.22 GHz 🔽 Auto Channel Scan
	Authentication Open System
	Key Settings
	Encryption Enable Key Size 64 Bits
	Valid Key First Key Type HEX
	First Key XXXXXXXX Second Key
	Third Key Fourth Key
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic >	Wireless	>	Access	Point >	WEP	Encryptic	n

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

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	red Tools Status System Help
Home	Wireless -
Basic	Wireless Band IEEE 802.11g
Wireless	AP Mode Access Point
	SSID dlink
LAN	SSID Broadcast
	Channel 🛛 🔂 🗹 2.437 GHz 🔽 Auto Channel Scan
	Authentication WPA-Enterprise
	Radius Server Settings
	Cipher Type Auto Group Key Update Interval 1300 (300-9999999)
	Radius Serve: · · · · Radius Port (1-65535)
	Radius Secre:
	Accounting Mode Disable Accounting Port 1313
	Accounting Server 0.0.0.0
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Enterprise

Cipher Type:Select Auto, TKIP, or AES from the drop-down list.Group Key Upd
ate Interval:Select the interval during which the group key will be valid. 1800 is
the recommended setting. A lower interval may increase key updateRADIUS 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11g
Wireless	AP Mode Access Point 💌
	SSID dlink
LAN	SSID Broadcast
	Channel 6 🗹 2.437 GHz 🔽 Auto Channel Scan
	Authentication WPA2-Personal
	PassPhrase Settings
	Cipher Type Auto Group Key Update Interval (300-9999999)
	PassPhrase
Advanced	
Tools	
	Apply
Status	
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Personal

Cipher Type:Select Auto, TKIP, or AES from the drop-down list.Group Key Upd
ate Interval:Select the interval during which the group key will be valid. 1800 is
the recommended setting. A lower interval may increase key update

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

frequency.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode
	SSID dlink
	SSID Broadcast
	Channel 44 💽 5.22 GHz 🗆 Auto Channel Scan
	WDS
	Remote AP MAC Address
	Site Survey Type Channel Signal (%) BSSID Security SSID Scan
	Scan
Advanced	
Tools	
Status	Apply
System	
Get OK,	
aut en	

Basic > Wireless > WDS

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 MA C Addresses of the other APs you want to connect to using WDS mode.
 Site Survey: Click the Scan button to search for local APs.

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>I</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band IEEE 802.11a
Wireless	AP Mode WDS with AP 💌
	SSID dlink
	SSID Broadcast Enable 💌
	Channel 44 💽 5.22 GHz 🗆 Auto Channel Scan
	WDS with AP
	Remote AP MAC Address
	Site Survey
	Type Channel Signal (%) BSSID Security SSID Scan
Advanced	
Tools	Apply
Status	
System	
Get OK.	

Basic > Wireless > WDS with AP

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.

Home	<u>B</u> asic	<u>A</u> dvanced	<u>T</u> ools	<u>S</u> tatus	<u>S</u> ystem	H <u>e</u> lp	
	Home	L	AN 👻				
	Basic						
				ettings-			
	· · · ·		Get IF	' From			Dynamic (DHCP)
	Wireless	3					
	\$						
	LAN						
	LAN						
							Apply
	4 I						
′	Advance	:d					
	Tools						
	Status						
L	System						
Ok!							

Basic > 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem Help
Home	LAN -
Basic Wireless LAN	LAN Settings Get IP From Static (Manual) IP address 192.168.0.50 Subnet Mask 255.255.0 Default Gateway 0.0.0.0
Advanced Tools Status System Ok!	Apply

Basic > LAN > Static (Manual)

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

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	ced <u>T</u> ools <u>S</u> tatus <u>System</u> H <u>e</u> lp	62.11	
Home	Performance -		
Basic	Advanced Wireless Settin	10:	
Advanced	Wireless Band IEEE 802.11		
S 1	Frequency	5.22 GHz	Advance Data Rate Settings
Performance	Data Rate	Auto	🔲 Enable Data Rate Control
	Beacon Interval (20 - 1000)	100	6Mb/sec Basic 💌
Filter	DTIM (1 - 255)	1	9Mb/sec Enable 💌
Filler	Fragment Length (256 - 2346)	2346	12Mb/sec Basic 👻
S (RTS Length (256 - 2346)	2346	18Mb/sec Enable 💌
Grouping	Transmit Power	Full	24Mb/sec Basic 💌
	Channel	44	36Mb/sec Enable 💌
	Radio	ON 🔹	48Mb/sec Enable
DHCP Server	WMM	Enable 💌	54Mb/sec Enable
S	Super Mode	Disable 🔹	
Multi-SSID	Antenna Diversity	Enable	
<i>(</i> 1)			
			Reset
Rogue AP 🔽			
Tools Status		Apply	
System		Apply	
Get OK.	J		

Advanced > Performance > 802.11a

Frequency:	Displays the current frequency of the wireless band.
Data Rate:	Set to Auto by default; use the drop-down list 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.

- Auto Channel: Enable this option to automatically select the most optimal channel available for wireless networking and to scan for the least populated channel.
 - **Radio:** Select **ON** or **OFF** to control the signal status of the device.
 - 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 802.1 1e WLAN QoS standard.
 - Super ModeSelect Super A to enable a wireless signal rate of up to 108Mbps.
Super A is a group of performance enhancement features that
increase end user application throughput in a 802.11a network.
Super A is backwards compatible with standard 802.11 a devices.
For ideal performance, all wireless devices on the network should be
Super A capable.

Super A Mode	Function
Disabled	Standard 802.11a support. No enhanced capabilities.
Super A without Turbo	Capable of Packet Bursting, FastFrames, Compression. No Turbo mode.
Super A with Dynamic Turbo	Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo mode. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are configured with Super A and Dynamic Turbo enabled.
Super A with Static Turbo	Capable of Packet Bursting, FastFrames, Compression, and Static Turbo mode. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all devices on the wireless network are configured with Super A and Static Turbo enabled.

AntennaThis option is Enabled by default. When enabled, each radio will
automatically switch to the antenna with the greatest RSSI value.
When disabled, each radio will use its main antenna - when facing
the AP, 5GHz transmits from the right antenna, while the 2.4GHz
radio uses the antenna on the left.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	_	
Home	Performance 🕶		
Basic	Advanced Wireless Setting	g:	
Advanced	Wireless Band IEEE 802.11g		
S (1997)	Frequency	2.437 GHz	Advance Data Rate Settings
Performance	Data Rate	Auto	Enable Data Rate Control
	Beacon Interval (20 - 1000)	100	1Mb/sec Basic 💌
Filter	DTIM (1 - 255)	1	2Mb/sec Basic 💌
Filler	Fragment Length (256 - 2346)	2346	5.5Mb/sec Basic 👻
S (RTS Length (256 - 2346)	2346	6Mb/sec Enable 💌
Grouping	Transmit Power	Full	9Mb/sec Enable 💌
	Channel	6	11Mb/sec Basic 💌
DHCP Server	Radio	ON 💌	12Mb/sec Enable 💌
	WMM	Enable	18Mb/sec Enable 💌
	Super Mode	Disable 💌	24Mb/sec Enable 🔽
Multi-SSID	Antenna Diversity	Enable	36Mb/sec Enable 💌
	Wireless B/G Mode	Mixed	48Mb/sec Enable 💌
Rogue AP 📃	Preamble	Short and Long 🔹	54Mb/sec Enable 💌 Reset
Tools			
Status		Apply	
System			
Get OK.			

Frequency:	Displays the current frequency of the wireless band.
Data Rate:	Set to Auto by default; use the drop-down list 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), mini- mum power. This tool can be helpful for security purposes if you

	wish to limit the transmission range.
Auto Channel:	Enable this option to automatically select the most optimal channel available for wireless networking and to scan for the least populated channel.
Radio:	Select ON or OFF to control the signal status of the device.
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 802.11 e WLAN QoS standard.
Super Mode:	Select Super G to enable a wireless signal rate of up to 108Mbps. Super G is a group of performance enhancement features that increase end user application throughput in a 802.1 1a network. Super G is backwards compatible with standard 802.11 g devices. For ideal performance, all wireless devices on the network should be Super G capable.
Antenna Diversity:	This option is Enabled by default. When enabled, each radio will automatically switch to the antenna with the greatest RSSI value.
Wireless B/G Mode:	Select Mixed, 11g Only, or 11b Only.
Preamble:	Select Short and Long (recommended) or Long-Only.

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>I</u> ools <u>S</u> tatus <u>S</u> ystem <mark>Help</mark>
Home	Filter -
Basic	Wireless MAC ACL
Advanced	
	Wireless MAC ACL
Performance	Wireless Band IEEE802.11g
renonnance	
S (S)	Access Control Disable
Filter	
	MAC Address
S 🚳 🛛	MAC Address
Grouping	ID MAC Address
📎	
DHCP Server	
Multi-SSID	
	Del
Rogue AP 🗾	
Tools	
Status	
System	
Get OK.	

Advanced > Filter > Wireless MAC ACL

Wireless Band:	Select the 802.11a or 802.11g 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.


Advanced > Filter > Wireless MAC ACL

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.
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 "Connection Enabled" box to allow communication between devices on the 802.11 a network and devices on the 802.11 g network.

<u>H</u> ome <u>B</u> asic <u>A</u> dva	nced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem	Help	
Home	Grouping -		
Basic	AP Grouping Settings		
Advanced			
	Load Balance	Disable 💌	
Performance	User Limit (0 - 64)	10	
r choimance			
Filter			
S		Apply	
Grouping			
DHCP Server			
Multi-SSID			
S 1			
Rogue AP 👱			
Tools			
Status			
System			
Get OK.			

Advanced > 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp			
Home	DHCP Server -			
Basic	DHCP Server Settings			
Advanced	Oynamic Pool Settings	C Static Pool Settings	C Current IP Mapping List	
Performance	Function Enable/Disable	Enable 💌		
renoimance	Dynamic Pool Settings			
S (19 1	IP Assigned From	0.0.0.0		
Filter	The Range of Pool (1-255)	0		
S	SubMask	0.0.0.0		
Grouping	Gateway	0.0.0.0		
S	Wins	0.0.0.0		
DHCP Server	DNS	0.0.0.0		
	Domain Name		1	
Multi-SSID	Lease Time (60 - 31536000 sec)	0		
	Status	OFF		
Rogue AP 💌				
Tools		Apply		
Status				
System				
Ok!				

Advanced > DHCP Server > Dynamic Pool Settings

Dynamic Pool Sett ings:	Click to enable Dynamic Pool Settings. Configure the IP address pool in the fields below.			
Function Enable/D isable:	Enable or disable the DHCP server function.			
Assigned IP Fro m:	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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, 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.

Home	DHCP Server -				
Basic	DHCP Server Settings				
Advanced	C Dynamic Pool Settings	Static Pool Settings	C Current IP	Mapping List	
Š	Function Enable/Disable	Enable 💌			
Performance	E Static IP Pool Adding	: 🔀			
S	Static Pool Settings		Gateway	DNS	Win
Filter	Assigned IP	0.0.0.0			
Š	Assigned MAC Address	00000000000			
Grouping	SubMask	0.0.0.0			
DHCP Server	Gateway	0.0.0.0			
	Wins	0.0.0.0			
Multi-SSID	DNS	0.0.0.0			
\$	Domain Name				>
Rogue AP 🔽 Tools	Status	OFF 💌	Add Edit	Del	
I OOIS Status			<u> </u>		
System		Apply			

Advanced > DHCP Server > Static Pool Settings

Static 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.				
Function 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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, if applicable.				

DNS:	The IP address of the DNS server, if applicable.
	Enter the domain name of the AP, if applicable.
Status:	This option turns the static pool settings on or off.

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	rd Tools Status System Help
Home	DHCP Server -
Basic	DHCP Server Settings
Advanced	C Dynamic Pool Settings C Static Pool Settings C Current IP Mapping List
Performance	Current DHCP Dynamic Pools
Feironnance	Index Current Dynamic MAC Current Dynamic Assigned IP Current Dynamic Lease
S 🚳	
Filter	
S 🚳	
Grouping	
	Current DHCP Static Pools
	Index Current Static MAC Current Static Assigned IP
DHCP Server	
Multi-SSID	
Rogue AP	
Tools Status	Refresh
Status	
Ok!	

Advanced > 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 StaticThe current corresponding DHCP-assigned static IP address of the
device.Assigned IP:device.

Advanced > Multi-SSID

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	ed <u>T</u> ools <u>S</u> tatus	<u>S</u> ystem H <u>e</u> lp					
Home	Multi-SSID 👻						
Basic	_ Multi-SSID Settin	gs					
Advanced	🔽 Enable Multi-S	SID 🗌 Enable	VLAN State	🖲 both i C	11a 🔿 11g		
\$	Band	IEEE 802.11g 🗨	WMM Enable	V	VLAN ID		
Performance	MSSID Index	Primary SSID 🔹	SSID dlink				
\$	Security	None	Ethernet 🛞 LA	VI C LAN2	🔽 Enable SS	ID Broadcast	
Filter	Key Settings Key Size	64 Bits	Key Index	First 💌			1
Grouping	Кеу Туре	HEX	Key Value	****			
DHCP Server	- Multi-SSID						
		SSID	Band	Encryption	VLAN ID	Ethernet	
	Primary	dlink		OFF	OFF	LAN1	
Multi-SSID	Primary	dlink	11g	OFF	OFF	LAN1	
\$							
Rogue AP 🔽						Del	
Tools							-
Status				Apply			
System							
Get OK.							

Enable Multi-SSID:	When Multi-SSID is enabled, you can configure your SSIDs for either Both, 11a only, or 11g only networks.
Enable VLAN:	Check to enable VLANs.
Band:	Select the wireless band (IEEE802.11a or IEEE802.11g).
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.
VLAN ID:	Enter a VLAN number (0 - 4094).
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.
Ethernet:	Select " LAN1 " if you wish to configure the network on LAN 1 (PoE). Select " LAN2 " to set up the network on LAN 2.
Security:	Select the security level from the drop-down menu.

SSID Broadcast:	For each SSID, select to enable or disable the broadcast of the SSID.
WEP Encryption	
Key Index:	Select which defined key is active on the selected device(s).
WEP Key:	In the first drop-down menu select HEX or ASCII . Select the level of encryption (64, 128, or 162-bit) from the second drop-down box, and then enter the WEP key in the box.
WPA/WPA2 Perso nal	
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).

Advanced > Rogue AP

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tat	us <u>S</u> yste	em H <u>e</u> lp				
Home	Rogue AP 🗸						
Basic	- Roque AP D	etection-					. 🔼
Advanced	-BSS Type						
\$	AP BSS	AP BSS C Ad Hoc C Both					
Performance	Band						
\$	Security-	☐ 1 ⁻	16 🗌 11g				
Filter Grouping			P I WPA-Enterp			WPA2-Enterprise	
		CH	BSSID	Security	Mode	SSID	
DHCP Server	AP BSS	36	00037F0BA7DD	WPA-Auto-Personal	802.11a	DAP-1555_mk	
	AP BSS AP BSS	48 1	001195E0FD60 00179A2DC01E	WPA-Auto-Personal WPA-Enterprise	802.11a 802.11g	dwl8220_mktg_ AP_dir625	
	AP BSS	1	00195B65745D	WEP	802.11g	12345672	
Multi-SSID	AP BSS	1	00134609E4A0	WEP	802.11g		
\$							
Rogue AP 📃	<					>	
Tools				Detect A	.dd (Del	
Status							
System	-AP List-						~
ok!							

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 11a , 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 considering 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.

Tools > Admin

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	nced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Admin -
Basic	Login Settings
Advanced	
Tools	User Name admin
\$	Old Password
Admin	New Password
S	Confirm New Password
Firmware and SSL	Canada Callinga
	Console Settings
Conferentian File	Console Protocol C None © Telnet C SSH
Configuration File	Timeout 3 Mins 💌
SNTP	Apply
Status	
System	
Ok!	

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 .

Tools > Firmware and SSL

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	iced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp				
Home	Firmware and SSL -				
Basic	Update Firmware From Local Hard Drive				
Advanced					
Tools	Firmware Version v2.01				
Admin	Upload Firmware From File : UpLoad				
\$	Update SSL Certification From Local Hard Drive				
Firmware and SSL	Upload Certificate From File: Browse UpLoad				
\$	Upload Key From File : Browse UpLoad				
Configuration File					
SNTP					
0.111					
Status					
System					
Get OK.					

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.

Tools > Configuration File

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Configuration File -
Basic	Update Configuration File
Advanced	
Tools	Update File Browse OK
	Download Configuration File
Admin	
	Load settings to Local Hard Drive OK
Firmware and SSL	
Configuration File	
Conliguration rile	
SNTP	
Status	
System	
Get OK.	

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.

Tools > SNTP

<u>H</u> ome <u>B</u> asic <u>A</u> dvano	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	SNTP -	
Basic	SNTP/NTP Information	
Advanced		
Tools	SNTP/NTP Server IP	0.0.0.0
	SNTP/NTP Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
	Local Time	
Admin		
	SNTP/NTP Setting	
Firmware and SSL		
Filliwale and SSL	SNTP/NTP Server IP	
	SNTP/NTP Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Configuration File		
	Daylight Saving Time	F Enable
SNTP		
		Apply
Status		
System		
, Get OK,		

SNTP/NTP Informa tion:	The time server IP address, time zone, and the local time will be displayed here.
Server IP Addres s:	Enter the IP address of a SNTP/NTP server.
Time Zone:	Select your time zone from the drop-down menu.
Daylight Saving Ti me:	Check the box to enable daylight savings time.

Home	Device Information 🕶					
Basic	Device Information					
Advanced	Firmware Version:	v2.01	Ethernet MA	C Address:	001195A2EA20	
Tools	WLAN0 MAC Address:					
	Primary: 001	195A2EA20	Secondary:	001195A2EA	21 ~ 001195A2EA27	
Status	WLAN1 MAC Address:					
	Primary: 001	195A2EA28	Secondary:	001195A2EA	29 ~ 001195A2EA2F	
\sim	Ethernet					
Device Information	Get IP From:	Manual				
	IP address:	192.168.0.50				
	Subnet Mask:	255.255.255.0				
Stats	Gateway:	0.0.0.0				
Stats	- Wireless (802.11a)					
	SSID:	dlink				
\sim	Channel:	44				
Client Information	Rate:	Auto				
	Authentication:	Open System				
	Encrypt:	Disabled				
	Super Mode:	Disabled				
WDS Information	Wireless (802.11b/g)-					
	SSID:	dlink				
	Channel:	6				
Log	Rate:	Auto				
	Authentication:	Open System				
	Encrypt:	Disabled				
	Super Mode:	Disabled				
System						

Status > 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 802.11a and 802.11g wireless networks.

Status > Stats

	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp		
Home	Stats -		
Basic	WLAN 802.11A Traffic Statistics		
Advanced	ThroughPut		
Tools	Transmit Success Rate	100 %	
Status	Transmit Retry Rate	0 %	
	Receive Success Rate	0 %	
\sim	Receive Duplicate Rate	0 %	
evice Information	RTS Success Count	0	
	RTS Failure Count	2	
	Transmitted Frame Count		
Stats	Transmitted Frame Count	4925	
	Multicast Transmitted Frame Count	952	
	Transmitted Error Count	0	
Client Information	Transmitted Total Retry Count	0	
	Transmitted Multiple Retry Count	0	
\sim	Received Frame Count		
WDS Information	Received Frame Count	0	
	Multicast Received Frame Count	0	
\sim	Received Frame FCS Error Count	2	
Log	Received Frame Duplicate Count	0	
	Ack Rcv failure Count	5	
	WEP Frame Error Count		
	WEP Excluded Frame Count	0	
System	WER ICV Error Count	0	

WLAN 802.11a Tra
ffic Statistics:This page displays statistics for data throughput, transmitted and
received frames, and WEP frame errors for the 802.1 1a wireless
network.WLAN 802.11g Tra
ffic Statistics:This page displays statistics for data throughput, transmitted and
received frames, and WEP frame errors for the 802.1 1g wireless
network.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Client Information 👻
Basic	
Advanced	Station association with 11A : 0 Station association with 11B/G : 0
Tools	MAC Band Authentication Signal PSM SSID
Status	
Device Information	
Device monnation	
S	
Stats	
\$	
Client Information	
\$	
WDS Information	
Ś	
Log	
	Refresh
System	
Ok!	

Status > Client Information

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 Mo de:	Displays the status of the power saving feature.
SSID:	Displays the SSID the client is connected to.

Status > WDS Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced <u>T</u> ools <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp				
Home	WDS Information -				
Basic					
Advanced	Station association with 11A :	0 Station asso	ciation with 11B/G :	0	
Tools	SSID	MAC Band	Authentication	Signal	Channel
Status					
S					
Device Information					
Stats					
\$					
Client Information					
WDS Information					
\$					
Log					
			Refresh		
System					
Ok!					

SSID:	Displays the SSID the client is connected to.
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.

Channel: Displays the wireless channel being used.

Status > Log > Log View

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>T</u> ools <u>S</u> tatus <u>S</u> ystem	H <u>e</u> lp			
Home	Log v				
Basic	C. Lan View	<u></u>			
Advanced	Log View	O Log S	ettings		
Tools	View Log				
Status				Total Log:	6
	Time	Туре	Message		
	Uptime 0 day 00:10:09	SYS	Web logout from 192.168.0.100		
	Uptime 0 day 00:02:29	SYS	Web login success from 192.168.0.100		
Device Information	Uptime 0 day 00:00:19	WIREL	WLAN1 Normal AP ready		
	Uptime 0 day 00:00:14 Uptime 0 day 00:00:09	WIREL NOTICE	WLAN0 Normal AP ready Ethernet AE1 LINK DOWN		
	Uptime 0 day 00:00:09	SYS	Ethernet AET LINK DOWN AP cold start with f/w version: v2.01		
	Optime o day 00.00.03	313	-AF cold start with t/w version, v2.01		
Stats					
S 1					
Client Information					
S 🚳					
WDS Information					
Log					
	<				
			Clear		
System					
)					
Get OK.					

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

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>T</u> ools <u>S</u> tatus <u>System</u> H <u>elp</u>
Home	Log 🗸
Basic	C Log View 📀 Log Settings
Advanced	
Tools	Log Settings
Status	Log Server / IP Address
Device Information	Log Type System Activity
Stats	✓ Wireless Activity ✓ Notice
	SMTP
Client Information	SMTP 🔽 Enable
\$	SMTP Server / IP address
WDS Information	SMTP Sender
\$	SMTP Recipient
Log	
	Apply
System	
Ok!	

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 > Log > Log Settings

System



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

Warning	
Device will rebo	ot, continue?
ОК	Cancel

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

Warning	
All of your changes will	be discarded, continue?
ок	Cancel

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

Configuring 802.11n 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).

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Information -	
	System Information	
Information	Model Name	DAP-2590
	System Time	Fri Dec 31 16:11:12 1999
	Vp Time	0:11:13.00
	Firmware Version	1.00
	IP address	192. 168. 0. 50
	Operation Mode	Access Point
	System Name	D-Link DAP-2590
	Location	
	MAC Address	00055D989810
Basic		
Advanced		
Maintenance		
Status		
System		
0k!		

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

Home > Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Information -	
	System Information	
Information	Model Name	DAP-2590
	System Time	Fri Dec 31 16:11:12 1999
	Up Time	0:11:13.00
	Firmware Version	1.00
	IP address	192. 168. 0. 50
	Operation Mode	Access Point
	System Name	D-Link DAP-2590
	Location	
	MAC Address	00055D989810
Basic		
Advanced		
Maintenance		
Status		
System		
0k!		

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, IP address, Operation Mode, System Name, Location and MAC Address.

Basic > Wireless

Home Wireless > Basic Wireless Band 2.4GHz Wireless Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz
Wireless Band 2.4GHr Wireless Mode Access Point Network Name (SSID) Glink SSID Visibility
Wireless Network Name (SSID) LAN SSID Visibility
SSID Visibility Enable
LAN
Channel 1 🔽 🔽 Auto Channel Selection
Authentication Open System 💌
- Key Settings
Encryption Disable 💌 Key Size 64 Bits 💌
Valid Key First V Key Type HEX V
Network Key
Confirm Key
Advanced
Maintenance
Status Apply
System
Get OK.

Wireless Band:	Select the wireless band to configure, 802.11a or 802.11g.
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 Width:	Select the radio width of the channel.
Channel:	Allows you to select a channel.
AP Mode:	There are 4 AP modes:
	Access Point
	WDS with AP
	WDS
	Wireless Client
	Please see the following pages for an explanation of all the AP modes.

Home	Wireless 🕶	
Home Basic Wireless LAN	Wireless Band 2.4GHz Mode Access Point Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel 1 Muthentication Open System Key Settings Shared Key	
Advanced Maintenance Status System	Encryption Enabl WFA-Personal WFA-Enterprise e 64 Bits V Valid Key First V Key Type HEX V Network Key Confirm Key	

Basic > Wireless > Authentication

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

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

WPA-Personal: Secure your network using a password and dynamic key changes. (No RADIUS server required.)

WPA2-Personal: 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- Enterprise** to allow the client to either use **WPA-Enterprise** or **WPA2-Enterprise**.

WPA-Enterprise: Secure your network with the inclusion of a RADIUS server.

WPA2-Enterprise: Secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES).

Security

Open System
Shared Key
WPA- Enterprise
WPA- Personal
Open System
Shared Key
WPA-Personal
WPA2-Personal
Open System
Shared Key
WPA-Personal
WPA2-Personal
Open System
WPA-Personal
WPA2-Personal

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Wireless 🕶	
Basic	Wireless Band 2.4GHz	
Wireless	Mode Access Point 💌 Network Name (SSID) dlink	
	SSID Visibility Enable	
	Channel Width 20 MHz	
	Channel 1	🔽 Auto Channel Selection
	Authentication Open System	•
	Key Settings	
	Encryption Enable -	Key Size 64 Bits 💌
	Valid Key First 💌	Key Type HEX 💌
	Network Key	
	Confirm Key	
Advanced		
Maintenance		
Status		Apply
System		
Get OK.		

Basic > Wireless > Access Point > WEP Encryption

Authentication:	Select from the drop-down list the type of authentication to be used on the selected device(s). In this example you may select Open System or 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 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 or Shared Key .
Key Values:	Select the Key Size (64-bit or 128-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 or Shared Key .

Home	Wireless -		
Basic	Wireless Band 2.4GHz		
Wireless EAN	Mode Access Point Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel 1 Y Auto Channel Selection		1
	Authentication WPA-Enterprise Radius Server Settings Personal / Enterprise Auto (WPA or WPA2) Group Key Update Interval (300-9999999 seconds) Cipher Type	1800	
	Primary radius server settings Radius Server Radius Port (1-65535) Radius Secret	1812	
Advanced	Backup RADIUS Server Setting (Optional)		
Maintenance			-
Status	Apply		
System			

Basic > Wireless > Access Point > WPA/WPA2 - Enterprise

Personal/Enterprise:	Select Auto, WPA Only or WPA2 Only from the drop-down list.
Cipher Type:	Select Auto, TKIP, or AES from the drop-down list.
Group Key Update Interval:	Select the interval during which the group key will be valid. 1800 is the recommended setting. A lower interval may increase the key update frequency.
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 this box to enable accounting.
Accounting Port :	Enter the port used on the Accounting server.
Accounting Server :	Enter the IP address of the Accounting server.
Accounting Secret :	Enter the Accounting secret.
Network Protection :	Select Enable to set the VLAN mode to dynamic.

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic Wireless	Wireless Band 2.4GHz
LAN	Network Name (SSID) dlink SSID Visibility Enable Channel Width 20 MHz Channel 1 Channel 1 Auto Channel Selection Authentication WPA-Personal PassPhrase Settings Personal / Enterprise Auto (WPA or WPA2) Group Key Update Interval (300-9999999 seconds) Cipher Type Auto PassPhrase
Advanced Maintenance	
	Apply
Status	TPP 1
System	
Get OK.	

Basic > Wireless > Access Point > WPA/WPA2 - Personal

Personal/Enterprise:	Select Auto, WPA Only or WPA2 Only from the drop-down list.
Cipher Type:	Select Auto, TKIP, or AES from the drop-down list.
Group Key Update Interval:	Select the interval during which the group key will be valid. 1800 is the recommended setting. A lower interval may increase the key update frequency.
PassPhrase:	Enter a PassPhrase between 8-63 characters in length.

Basic > Wireless > WDS

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band 2.4GHz
Wireless	Mode WDS Network Name (SSID) dlink
LAN	SSID Visibility Enable
	Channel Width 20 MHz Channel 1 Auto Channel Selection
	WDS Remote AP MAC Address
	-Site Survey
	Site Survey Signal (%) BSSID Security SSID Scan
Advanced	
Maintenance	
Status	Apply
System	
Get OK.	

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 MA C Addresses of the other APs you want to connect to using WDS mode.

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

Basic	reless v						
Wireless LAN	SSID Visid Channel Wi Channel WDS with <i>i</i>	Name (SSID) bility idth	Hz WDS with AP dlink Enable 20 MHz 1	Auto Chan	nel Selection		
	Site Surve	ey					
	Channel	Signal (%)	BSSID	Security	SSID	Scan	
	-						
Advanced							
							-
Advanced				Apply			•

Basic > Wireless > WDS with AP

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.
	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.

Basic > Wireless > Wireless Client

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Wireless -
Basic	Wireless Band 2.4GHz
Wireless	Mode Wireless Client 🔽
	Network Name (SSID) dlink
S	SSID Visibility Disable
LAN	Channel Width 20 MHz 💌
	Channel 1 🔽 Auto Channel Selection
	Site Survey
	Channel Signal (%) BSSID Security SSID Scan
Advanced	Authentication Open System
Maintenance	
Status	Apply
System	
Get OK.	

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.

Home Basic Advan	ced Maintenance Status Sys	stem H <u>e</u> lp	2
Home	LAN -		
Basic Vireless LAN	LAN Settings Get IP From	Dynamic (DHCP)	
Advanced Maintenance Status System		Apply	
Ok!	J		

Basic > 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.

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	iced <u>Maintenance</u> <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	LAN 🕶
Basic Wireless LAN	LAN Settings Get IP From Static (Manual) IP address 192 . 168 . 0 . 50 Subnet Mask 255 . 255 . 0 Default Gateway 0 . 0 . 0 . 0
Advanced Maintenance Status System	Apply
0k!	

Basic > LAN > Static (Manual)

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

Home	Performance 👻			
Basic	Performance Settings			
Advanced				
	Wireless Mode	Mixed 802.11n,802.11g and 80	2.11b 💌	
Performance	Wireless	0n 💌	Connection Limit	Disable 💌
	Data Rate	Best(Up to 300) 💌 (Mbps)	User Limit (O - 64)	20
Filters	Beacon interval (25-500)	100	Link Integrity	Disable 💌
	DTIM interval (1-15)	1	Network Utilization	100 %
V	Transmit Power	100 %		
DHCP Server	WMM (Wi-Fi Multimedia)	Enable		
S	Short GI	Enable		
Multi-SSID	IGMP Snooping	Disable 💌		
S	Ack Time Out (2.4GHz, 48~200)	48 (μ _s)		
Intrusion				
¬				
Maintenance				
Status		Appl		
System			<u>у</u>	

Advanced > Performance > Mixed 802.11n, 802.11g and 802.11b

Wireless:	Open or close the wireless function.
Data Rate:	Set to Auto by default; use the drop-down list 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 802.1 1e 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.
Connection Limit:	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.
Link Integrity:	If enabled, when the uplink of AP is off, the connected wireless client will be disconnected.
Network Utilization:	Set the network utilization, if the utilization is more than the setting, no clients can connect to AP. Only available when Connection Limit is enabled.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H	{ <u>e</u> lp		
Home	Performance 🕶			
Basic	Performance Settings			
Advanced				
	Wireless Mode	Mixed 802.11g and 802.11b		
Performance	Wireless	0n 💌	Connection Limit	Disable 💌
	Data Rate	Best(Up to 54) 💌 (Mbps)	User Limit (0 - 64)	20
Filters	Beacon interval (25-500)	100	Link Integrity	Disable 💌
rifters	DTIM interval (1-15)	1	Network Utilization	100 %
S	Transmit Power	100 %		
DHCP Server	WMM (Wi-Fi Multimedia)	Enable		
\$	Short GI	Enable		
Multi-SSID	IGMP Snooping	Disable 💌		
\$	Ack Time Out (2.4GHz, 48~200)	48 (μ s)		
Intrusion				
<u>~</u>				
Maintenance				
Status		Appl	<i>"</i>	
System			<i>4</i>	
Get OK.				

Advanced > Performance > Mixed 802.11g and 802.11b

Wireless:	Open or close the wireless function.
Data Rate:	Set to Auto by default; use the drop-down list 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 802.1 1e 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.

Connection Limit:	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.
Link Integrity:	If enabled, when the uplink of AP is off, the connected wireless client will be disconnected.
Network Utilization:	Set the network utilization, if the utilization is more than the setting, no clients can connect to AP. Only available when Connection Limit is enabled.

<u>H</u> ome <u>B</u> asic <u>A</u> dvance	red <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp	
Home	Filters 🕶	
Basic	Wireless MAC ACL WLAN Partition	
Advanced	Wireless MAC ACL Settings	
Performance Filters	Access Control Disable MAC Address Add	
DHCP Server	MAC Address List	III
Multi-SSID		
Intrusi on		
Maintenance	Del	
Status		-
System	The Address SSID Band Addrentication Signal Add	
Ok!		

Advanced > Filter > Wireless MAC ACL

Wireless Band:	Select the 2.4GHz or 5GHz 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.

Advanced > Filter > Wireless MAC ACL

	ced Maintenance Status System	Help	
Home	Filters -	the Western Device and	
Basic	C Wireless MAC ACL	NLAN Partition	
Advanced	-WLAN Partition Settings		
Performance	Wireless Band	2.4GHz 💌	
reriormatice	Internal Station Connection	🔽 Enable	
Filters	Ethernet to WLAN Access	🔽 Enable	
DHCP Server			
Multi-SSID			
\$			
Intrusion		Apply	
Maintenance			
Status			
System			
Get OK.			

	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.
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.

Home DHCP Server	V						
Basic DHCP Server	Settings			_			
dvanced (* Dynamic)	ool Settings C	Static	Pool	Set	ting	5	C Current IP Mapping List
	able/Disable	Enable	•				
-Dynamic Po	l Settings						
IP Assigned	l From	0.	0	. 0	- W	0	
	of Pool (1-255)	1		_			
Submask Submask	ſ	0,	0	. 0	6	0	
P Server Gateway	ſ	0,	0	. 0	8 x	0	
WINS VINS	ſ	0.	0	. 0	6 a	0	
Iti-SSID DWS	ſ	0.	0	. 0	s	0	
Comain Name	. I	I					
trusion Lease Time	(60 - 31536000 sec)	604800		_		_	
<u>a</u> 🗖							
intenance							
Status					Appl	y	
System							

Advanced > DHCP Server > Dynamic Pool Settings

Dynamic Pool Sett ings:	Click to enable Dynamic Pool Settings. Configure the IP address pool in the fields below.
Function Enable/D isable:	Enable or disable the DHCP server function.
Assigned IP Fro m:	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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, 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.

fome DHCP	Server -			
Marking Colored	DHCP Server Settings C Dynamic Pool Settings			
S Fun	nction Enable Enable			
Static IP Pool	Adding X			
tatic Pool Settings	s /			
ssigned IP				
ssigned MAC Address	s			
ubmask	255 . 255 . 255 . 0			
iateway	0.0.0			
INS	0.0.0			
ONS	0.0.0			
lomain Name	dlink-ap Add Edit Del			
	Apply			
	Apply			

Advanced > DHCP Server > Static Pool Settings

Static 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.
Function 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 Name Service) is a system that register and query the mapping between IP and NetBios dynamically, if applicable.
DNS:	The IP address of the DNS server, if applicable.
Domain Name:	Enter the domain name of the AP, if applicable.

<u>H</u> ome <u>B</u> asic <u>A</u> dvanc	ed <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	DHCP Server -
Basic	_DHCP Server Settings
Advanced	C Dynamic Pool Settings C Static Pool Settings 💽 Current IP Mapping List
	-Current DHCP Dynamic Pools-
Performance	Index Current Dynamic MAC Current Dynamic Assigned IP Current Dynamic Lease
S 1	
Filters	
DHCP Server	Current DHCP Static Pools
	Index Current Static MAC Current Static Assigned IP
Multi-SSID	
WIT (1-22TD	
\$	
Intrusion	
Maintenance	
Status	Refresh
System	
0k!	

Advanced > 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.

Advanced > Multi-SSID

Home	Multi-SSID -						
Basic	-Multi-SSID Set						
vanced	🔽 Enable Mult	i-SSID					
<u> </u>	Band	2.4GHz	× 1	MMM (Wi-Fi Multin	edia) Enab	le 💌	
	MSSID Index	Primary SSID	•	SSID	22		
formance	Security	None	v.		E Es	able SSID Vis	ibility
\$ \$							
lters	Key Settings						
1.	Key Size	64 Bits	- 1	Key Index [First 💌		
>	Key			Key Type	HEX		
Server	22.2						
	Confirm Key						
< <u>.</u>	Confirm Key						
ti-SSID							
ti-SSID	Multi-SSID					VIAN TO	
SSID		SSII		Band 2.4GHz	Encryption None	VLAN ID	
ti-SSID	- Multi-SSID Index			Band	Encryption		
\$	- Multi-SSID Index			Band	Encryption		
virusi on	- Multi-SSID Index			Band	Encryption		Del
vusion	- Multi-SSID Index			Band	Encryption		Del

Enable Multi -SSID:	When Multi-SSID is enabled, you can configure your SSIDs for networks.
Band:	Select the wireless band (2.4GHz or 5GHz).
SSID:	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.
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.
Security:	Select the security level from the drop-down menu.
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 802.11 e WLAN QoS standard.
Enable SSID Visibility:	For each SSID, select to enable or disable the broadcast of the SSID.

Advanced > Intrusion

<u>Home Basic Advar</u>	nced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Intrusion 🗸
Basic	Wireless Intrusion Protection
Advanced	Detect
No. 10	
	AP List
Multi-SSID	
	Type Band CH SSID BSSID Last Seem Status
Intrusion	
VLAN	
- 🌾 -	
QoS	
	Set as Valid Set as Neighborhood Set as Rogue Set as New
Schedule	
	• Mark All New Access Points as Valid Access Points
Maintenance	🦳 Mark All New Access Points as Rogue Access Points
Status	
System	Аррту
	Apply

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.
AP List:	The category of the APs.
	From the All list, click the corresponding Add button of AP record to classify the AP.

Advanced > VLAN

Home	VLAN 👻				
Basic	-VLAN Sett	ings			
Advanced	VLAN S	Status 🔽 Enbal	e		
🔺 🔊	VLAN I	Mode : Static			
	VLAN L	ist Port List	Add/Edit VLAN PVID	Setting	
Multi-SSID			<u> </u>		
	VID	VLAN Name	Untag VLAN Ports	s Tag VLAN Ports	
\sim					
Intrusion					
\$					
VLAN					
QoS					
QoS					
\sim					
Schedule					
Maintenance					
Status					

VLAN Status:	Check this box to enable the VLAN function.
	Displays the mode of VLAN.
	This window lists the configured VLAN on the AP.
Port List:	This window lists the configured Port on the AP.

Home VLAN -										
asic -VLAN Se	ttings									
vanced VLA	N Status	F Enbale								
VLA 🗖	N Mode :	Static								
VLAY	List	Port List	Add/Edi	t VLAN	PVID S	etting	r.			
ti-SSID						-1				
		VLAN 1	Name		Add	<u> </u>				
Port		Select All	Mgmt	LAN						
rusion Unta	ε	ALL	œ	(•						
Tag		ALL	C	C						
	Wember	ALL	C	С						
MSSI	D Port :	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
🐼 Unta	g	ALL	(•	•	(•		(•	(•	(•	(•
QoS Tag		ALL	C	C	C	C	C	C	C	С
Not	llember	ALL	0	C	C	C	C	C	C	C
WDS :	Port :	Select All	W-1	¥-2	¥-3	W-4	¥-5	₩~6	¥-7	¥-8
hedule Unta	z	ALL	G	(•	•		(•		œ	G
Tag		ALL	C	C	C	C	C	C	C	C
	llember	ALL	C	C	C	C	С	C	С	С
tatus						Apply	. 1			
ystem					2					

Advanced > VLAN > Add/Edit VLAN

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.

D-Link AP Manager II Software User Manual

Home	VLAN -								
Basic	-VLAN Settings-								
wanced	VLAN Status	🔽 En	bale						
	VLAN Mode	: Stati	c						
	VLAN List	Port Li	ist A	dd/Edit VLA	N PVID	Setting			
ti-SSID						~ *			
<u> </u>	PVID Auto As	sign Status	• J.	Enable					
trusion	Port	Mgmt	LAN						
truston	PVID	1	1						
<s></s>		-	-						
VLAN	MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
	PVID	1	1	1	1	1	1	1	1
\$		10	1	1	1-	J.	J	I. S.	E.
QoS	WDS Port	₩ - 1	₩-2	¥-3	₩-4	¥-5	¥-6	₩ - 7	¥-8
100						_			
\$	PVID	1]1	1	1	1	1	1	1
hedule									
ntenance									
tatus						Apply	1		
ystem									

Advanced > VLAN > PVID Setting

PVID AutoCheck this box to assign the PVID automatically.**Assign Status:**Assign the PVID manually.

Port/WDS Port:

Advanced > QoS

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	QoS -
Basic	QoS Settings
Advanced	QoS (Quality of Service) Enable
🤹 😵	-Priority Classifiers HTTP Automatic (default if not matched by anything else)
Multi-SSID	Add QoS Rule
**	Name Priority Protocol 💌
Intrusion	Host 1 IP Range
S	Host 1 Port Range
VLAN	Host 2 Port Range - Add Clear
\$	QoS Rules List
QoS	Name Priority Host 1 IP Range Host 2 IP Range Protocol / Ports
\$	
Schedule	
Maintenance	
Status	
System	Apply
Refresh	

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.

Advanced > Schedule

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	red <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Schedule 🗸
Basic	Wireless Schedule Settings
Ådvanced	Wireless Schedule Enable 💌
🧼 🍯	Add Schedule Rule
Multi-SSID	Day(s) C All Week © Select Day(s)
\$	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat All Day(s) □
Intrusion	Start Time : (hour:minute, 24 hour time)
\$	End Time : Chour:minute, 24 hour time)
VLAN	Wireless Off 💌 Add Clear
S	-Schedule Rules List
QoS	Name Day(s) Time Frame Wireless
\$	
Schedule	
Maintenance	Edit Del
Status	
System	Apply
0k!	

Wireless Schedule Settings	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.
Day(s):	Select the days that apply the schedule.
Start/End Time:	Enter the start and end times that apply the schedule.
Wireless:	Open or close the wireless function at the schedule time.
Schedule Rules List:	This window lists the configured schedule rules.

Maintenance > Admin

Home	Admin 🔫			
Basic Advanced wintenance	- Limit Administrator IP — □ IP Range From To		- - └ Limit Administrator VI	co 1
Admin.	ID IP From	IP To		Add
eare and SSL	Login Settings User Name Old Password New Password Confirm New Password	edmin		
e and Time	Console Settings Console Protocol Timeout	C None (* Ta 3 Mins 💌	elnet C SSH	
	Ping Control Settings Status	T Enable		
Status System	-System Name Settings	D-Link DAP-2590		

Limit Administrator IP

Check this box to allow only the computers within the IP range can manage the AP.
Check this box to allow only the computers within the VID can manage the AP.
Enter a user name. The default is admin.
When changing your password, enter the old password here.
When changing your password, enter the new password here.
Confirm your new password here.
Select the type of protocol you would like to use, Telnet or SSH or select " None " to disable the console.
Select the expired time from the drop-down list.

Status:	Check this box to allow the computer ping the AP.
System Name Settings	
System Name:	Enter a name for this device.
Location:	Enter a string to describe the location of device.

Maintenance > Firmware and SSL

Home	Firmware and SSL 🕶		
Basic Advanced	- Update Firmware From Local Hard Drive		
Maintenance	Firmware Version 1.00		
\$	Upload Firmware From File :	Browse	UpLoad
Admin	Update SSL Certification From Local Hard Drive		
irmware and SSL	Upload Certificate From File:	Browse	UpLoad
<u> </u>	Upload Key From File :	Browse	UpLoad
Configuration File			
S			
Date and Time			
Date and Time			
Date and Time			
Date and Time Status			

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.

Maintenance > Configuration File

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>Maintenance S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Configuration File 🕶
Basic	Update Configuration File
Advanced	Update File Browse OK
Maintenance	opuate rite
\$	Download Configuration File
Admin	Load settings to Local Hard Drive OK
\$	Load settings to Local Hard Drive OK
Firmware and SSL	
\$	
Configuration File	
\$	
Date and Time	
Status	
System	
Get OK.	

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.

Maintenance > SNTP

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	nced <u>M</u> aintenance <u>S</u> tatus <u>S</u> ystem H <u>e</u> lp
Home	Date and Time -
Basic Advanced	Time Configuration
Maintenance	Time Fri Dec 31 17:18:38 1999
	Time Zone (GMT-08:00) Pacific Time (US & Canada); Tijuana 💌
Admin	Enable Daylight Saving
	Daylight Saving Offset +1:00 💌
- S	Month Week Day of Week Current Time
Firmware and SSL	Daylight Saving Dates DST Start Jan 🔻 1st 🔽 Sun 💌 12 am 💌
\$	DST End Jan V Ist V Sun V 12 am V
Configuration File	Automatic Time Configuration
S	Enable NTP Server
Date and Time	NTP Server Used Select NTP Server
	Set the Date and Time Manually
	Date And Time
	2008- 6-11
Status	
System	Apply
Get OK.	

Time Configuration	
Time:	The current local time will be displayed here.
Time Zone:	Select your time zone from the drop-down list.
Daylight Saving Tim e:	Check the box to enable daylight savings time.
Daylight Saving Offset:	Select the offset time from the drop-down list.
Daylight Saving Dates:	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 and Time Manually	
Date And Time:	Select the date and time from the box or copy your computer's time setting to AP.

Status > Device Information

<u>H</u> ome <u>B</u> asic <u>A</u> dvan	ced <u>Maintenance</u> <u>Status</u> <u>System</u> H <u>e</u> lp
Home	Device Information -
Basic	Device Information
Advanced	Firmware Version: 1.00 Ethernet MAC Address: 00055D989810 Wireless MAC Address:
Maintenance	Primary: 00055D989810 SSID 1~7: 00055D989811 ~ 00055D989817
Status	
\$	Ethernet
Device Information	IP address: 192.168.0.50 Subnet Mask: 255.255.255.0
	Gateway: N/A
Stats	Wireless (2.4GHz) Network Name zz Channel: 1
\$	Data Rate: Auto Security: None
Client Information	
S 1	AP Status CPU Utilization 8 %
WDS Information	Memory Utilization 68 %
Log	
System	
Get OK.	

Information:

Device 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 2.4GHz and 5GHz wireless networks.

Status > Stats > WLAN Traffic Statistics

Home	Stats -		
Basic	WLAN Traffic Statistics	C Ethernet Traffic Statistics	^
Advanced	-WLAN Traffic Statistics		
Maintenance	Transmitted Count		
Status	Transmitted Packet Count	73068	
	Trasmitted Bytes Count	835797	
	Dropped Packet Count	0	
Device	Transmition Retry Count	0	
Information		•	
	Received Count		
	Received Packet Count	73069	
Stats	Received Bytes Count	13465613	
	Dropped Packet Count	0	
	Received CRC Count	0	
Client	Received Decryption Error Count	0	
Information	Received MIC Error Count	0	
	Received PHY Error Count	0	
WDS Information	1	Refresh Clear	
S			
Log			
System			
-,			

WLAN TrafficThis page displays statistics for data throughput, transmitted and
received frames for the wireless network.

Home Basic Advanced Maintenance Status System Help Stats -Home Basic WLAN Traffic Statistics Ethernet Traffic Statistics Advanced **Ethernet Traffic Statistics** Maintenance Transmitted Count Status Transmitted Packet Count 51 31426 \$ Trasmitted Bytes Count Dropped Packet Count 0 Device Information Received Count Received Packet Count 51 3 Received Bytes Count 6236 0 **Dropped Packet Count** Received Multicast Packet Count 0 Received Broadcast Packet Count 34 Information Len 64 Packet Count 28 Len 65~127 Packet Count 13 Len 128~255 Packet Count 4 Log Len 256~511 Packet Count 6 Len 512~1023 Packet Count 0 Len 1024~1518 Packet Count 0 Len 1519 MAX Packet Count 0 System Refresh Clear 0k!

Status > Stats > Ethernet Traffic Statistics

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

Status > Client Information

Home	Client Information	~						
Basic								
Advanced	Station association (2.4GHz) : 1							
Maintenance	MAC	Band	Authentication	Signal	PSM	SSID		
Status	001CBF4F4E5F	Ģ	Open System	30 %	Off	Primary SSID		
\$								
Device Information								
\$								
Stats								
\$								
Client Information								
\$								
5 Information								
\$								
Log				I	lefresh]		
System								

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.

Status > WDS Information

Home	WDS Information	17				
Basic						
Advanced	WDS Information	Channel: 2 (2.4GHz):				
Maintenance	Name	MAC	Authentication	Signal	Status	
Status	₩-1	06055D989810	Shared Key	54 %	on	
Ś						
Device Information						
\$						
Stats						
\$						
Client Information						
\$						
)S Information						
Š						
Log			Ref	resh		
System						

Displays the name of the client.
Displays the name of the client. Displays the MAC address of the client.
Displays the type of authentication being used.
Displays the strength of the clients signal.
Displays the status of the client.

Status > Log > Log View

Home Basic	Log 🗸	
	🖲 Log View 🕜 Log Settings	
Advanced		
laintenance	-View Log	: 48
Status	Time Priority Message	~
	Uptime O day O1: SYSACT Web logout from 192.168.0.82	
	Uptime 0 day 01: SYSACT Web login success from 192.168.0.82	
	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
Device	Uptime O day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
Information	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:1C:BF:4F:4E:5F	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
Stats	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
Stats	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
<u></u>	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
Client	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
Information	Uptime 0 day 00: Wireless Association Sucess:STA 00:1C:BF:4F:4E:5F	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:1C:BF:4F:4E:5F	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
S Information	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	
	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
	Uptime 0 day 00: Wireless Received Deauth:STA 00:13:46:00:00:06 (reason 3)	
	Uptime 0 day 00: Wireless Association Sucess:STA 00:13:46:00:00:06	×
	<	>
Log	1 ²	
	Clear	

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

Home	Log 🗸			
Basic	C Log View	Log Settings		
lvanced		bog bettings		
ntenance	- Log Settings			
Status	Log Server / IP Address	10. 10		
14	Log Type			
\$	🔽 System Activity			
)evice ormation	Vireless Activity			
Store and a store of the				
\$	V Notice			
Stats	Email Notification			
\$	Email Notification	T Enable	SMTP Port	25
	Email Server address		User Name	
lient ormation	From Email Address		Password	
\$	from Email Address	1	rassword	
Log	To Email Address	1	Confirm Password	
	-Email Log Schedule			
	Schedule	0 💌 hour	s or when Log is full	
			Apply	
ystem				

Log Settings Log Server/IP Enter the IP address of the server you would like to send the AP Address: log to. Check the box for the type of activity you want to log. There are Log Type: three types: System, Wireless and Notice. **Email Notification** Email Notification: Check the box to enable email notification. Email Server Enter the IP address of the SMTP server. Address: From Email Enter the e-mail address of the SMTP sender. Address: To Email Address: Enter the e-mail address of the SMTP recipient. SMTP Port: Enter the port of the SMTP server. Enter the username of the SMTP server. User Name: Password: Enter the password of the SMTP server. Email Log Select an interval time from drop-down list to send the logs to mail Schedule: recipient.

Status > Log > Log Settings

System

Home	System -
Basic Advanced	System Settings
Maintenance	Apply Settings and Restart Restart
Status	
System	Restore to Factory Default Settings Restore
\$	
System	

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

Warning	
Device will rebo	ot, continue?
ОК	Cancel

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

Warning	
Device will rebcot and module v	vill be disconnected, continue?
ОК	Cancel

Multiconfiguration

Administrator can manage the configuration of APs that AP Manager II has detected by using the 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.

	🗋 🚺 🌌	强 强			
	Template Name Cr	eator	Create Date	Activity Status	Next Run Time
 All Space General Group MultiConfiguration Template Fault Manage Tool Report Association Security Utilization Channel Rogue AP SysLog 	🔁 Default Template Sy	<u>N</u> ew Delete Edit <u>R</u> un E <u>x</u> port <u>I</u> mport	2008/01/10	Disabled	Unknown

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		General X
Basic Info Content Selection	Enter a name for this template. Check the box to select the configuration contents included in this template. Then configure the settings in the following page.	Basic Info Name : dlink Creator : admin Time : 2008- 6-11 ✓ 2008- 6-11 ✓ System ✓ System ✓ Vireless 11A ✓ Security 11A ✓ Filter 11A
System	Check the box to select the configuration contents included in this template.	System Check All Check All Clear All
LAN Settings	Set the subnet mask and default gateway of the Access Point.	✓ LAN Settings Subnet Mask 255 . 255 . 0 Default Gateway ✓ Admin User Name admin
Admin	Enter the username and password of administrator for AP.	Password Misc Console Protocol Timeout 5 Mins Timeout
Misc	Set the console type.	< Back Next > Cancel

Wireless

Check the box to select the configuration contents included in this template. For how to configure wireless settings, please refer to page 29 and 41.

Security

Check the box to select the configuration contents included in this template. For how to configure security settings, please refer to page 69.

MAC Filter

Check the box to select the configuration contents included in this template. For how to configure MAC filter settings, please refer to page 83.

reless 11g		
	Check All Clear A	dl
Wireless Settings(IEEE802.11g)		
	dlink	
Channel	Auto	
SSID Broadcast	Enable	
Data Rate	Auto 🔽	
RTS Length(256-2346)	2346	
Beacon Interval(20-1000)	100	
Fragment Length(256-2346)		
DTIM(1-255)	1	
🗖 Radio	On 🔽	
	<back next=""> C</back>	ancel
urity 11g		
inty rig		
Authentication Open Sys	stem	
Key Settings		
Encryption Enable	 Key Size 64 Bits 	•
Key Type HEX	 Valid Key 	•
Key Value		=
WPA		
	Group Key Update interval	_
PassPhrase	,	_
,	- 1010	_
Radius Server	• • • Port 1812	_
Radius Secret		
	<back next=""> C</back>	ancel
er 11g		
er rig		Ľ
IEEE802.11g Wireless MAC ACL	L Setting	
Access Control Accept	•	
MAC Address	Save	
	[Del
	<back next=""> C</back>	ancel

Device By Group:	one AP group or AP, AP Manager II will apply the template to all the selected APs at the same time.	Device Image: Constraint of the system Image: By Group By Group By Group Group Name Group Name Sort Image: DAP-2530 Model DWL-2700AP Model DWL-3200AP Model DWL-3200AP Model Image: DAWL-3200AP Model
By IP:	Select the APs by IP that will apply the template.	< Back Next > Cancel
Update	To configure the runtime of	Schedule
	template, please choose the device object first.	C Disable © Specify Time
Specify Time:	template, please choose the device object first. Specify the day time that will apply the template. The template will run at certain	 Specify Time Specify Interval Specify Date Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Specify Time: Specify Interval: Specify Date:	template, please choose the device object first. Specify the day time that will apply the template. The	 ⑦ Specify Time ⑦ Specify Interval ⑦ Specify Date ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday

After the configuration, the template will be listed in the template window. The **NextRun Time** column shows the running time of the template. When the running time arrived, the template will apply the configured parameters to the devices selected in the **Device** selection window. If multi-APs are selected, AP Manager II will apply the template to all the APs that selected at the same time.

Template Name	Creator	Create Date	Activity Status	Next Run Time	Status	Result
😑 Default Template	System	2008/01/10	Disabled	Unknown		
😑 Test	admin	2008/06/13	Enabled	2008/07/13 14:02:16		
-						

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.

Update						X
General	System	Wireless 11g	Security 11g F	Filter 11g D	evice 9	chedule
Basic	Info					
Nam	e:	dlink				
Creat	tor :	admin				
Time	:	2008- 6-11				
		,				
Conte	ent Selecti	on				
🔽 S	iystem					
▼ ∨	Vireless	11A 🗖	11G 🗹			
💌 S	ecurity	11A 🗖	11G 🗹			
🗹 F	ïlter	11A 🗖	11G 🗹			
				OK		Cancel

For how to configure the items in this page, please refer to page 109.

Delete a template

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

Run a template

If you want to apply the template immediately, right-click the template, and select **Run** item from the drop-down menu. The **Status** column will show the progress of this operation, and the **Result** column show the operation result.

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 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.

Fault Manage

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

	Event Name	Event Type	Event Level	Date Time	Source	Description
- 🗗 All Space	🚸 PollingFailed	System	Notice	2008-06-11 14:4	192, 168, 0, 50	Indicate th
General General	🚸 PollingFailed	System	Notice	2008-06-11 14:4	192, 168, 0, 50	Indicate th
🛨 🦲 Group	🚸 PollingFailed	System	Notice	2008-06-11 14:4	192, 168, 0, 50	Indicate th
🗄 🦲 MultiConfiguration	🚸 PollingFailed	System	Notice	2008-06-11 14:4	192, 168, 0, 50	Indicate th
🖻 🔄 Fault Manage						
- StandardTrap						
- System						
Threshold						
Private						
Tool						
E E Report						
Association						
Security						
Utilization						
Channel 						
SysLog						
əysLog						

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 128.
- Threshold: The Threshold view window displays the threshold notice data. To enable the threshold notice, please refer to page 128
- 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.

Event Settings		X
Event		
Event Type	SnmpVersion	SNMP VI
ColdStart WarmStart	Event Name	StandardTrap
LinkDown LinkUp AuthenticationFailure	Trap Generic	ColdStart(0)
- EgpNeighborLoss 	Status	C Disable 💿 Enable
	OID	
LinkUp(snmpv2) AuthenticationFaihre(snmpv2)	Description	
 System Event PollingFailed PollingOk 	Level	Critical
Threshold Event	Threshold Enab	le
TransmitThreshold + Private	Ascending	0
	Descending	0
<	New	Save Delete Close

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

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

Event Settings		
Event		
🖃 Event Type	Snmp Version	SNMP V2C
 StandardTrap ColdStart WarmStart 	Event Name	
LinkDown LinkUp AuthenticationFailure	Trap Generic	EnterpriseSpecific(6)
EgpNeighborLoss ColdStart(snmpv2)	Status	C Disable 💿 Enable
	OID	
- LinkDown(snmpv2) - LinkUp(snmpv2) - AuthenticationFailure(snmpv2)	Description	
 System Event PollingFailed PollingOk 	Level	Critical
Threshold Event	Threshold Enab	le
Transmit Threshold	Ascending	0
	Descending	0
	New	Save Delete Close
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 **use** in the tools bar, as shown below.

Notice Settings	\mathbf{X}
Notice Settings Warning Level Critical Error Warning Notice	Notice Settings Play sound Sound File Show Pop Message Show Pop Message Send Email To Email Address From Email Address SMTP Server User Name Password [Optional] Subject Message
	Ok Apply Cancel

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.

	🧋 🎑 🔇	Q 📿 - 🛃	-	
ent Type	Event Level	Date Time	Create Watchlist	ription
stem	Notice	2008-06-04 10:58:09	Update Watchlist	ate the
stem	Notice	2008-06-04 10:58:09	Delete Watchlist	ate the
stem	Notice	2008-06-04 09:49:09	192.168.0.50 India	cate the
stem	Notice	2008-06-04 09:33:20	192.168.0.50 India	cate the
chore	Mohico	2000 02 02 10,40,21	102 149 0 42 Toda	asto the

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

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

Notes: 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 **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 **AII** topology view window and selecting the new topology under the **Copy Component To** item, as shown below.



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.

Open	? 🔀
Look in: 📋 My Documents 💽 🖛 🖻 🖿	* ⊞-
My Music	
Scan AP	
□ 我接收到的文件 □ 我有些我的共享文件夹	
File name:	Open
Files of type: JPEG File (*.jpg)	Cancel
Picture Display Style: Adjust the size of the canvas to fit the pict.	

After the successful loading:



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

Grid line and rulers:

To hide the grid line or ruler, click the **Grid** or **Ruler** item from the right-click menu, as shown below.



To show the grid and ruler, click the **Grid** or **Ruler** item from the right-click menu again.

Topology size

To change the topology size, click the **Topology Size** item from the right-click menu, as shown below.

Can¥as Setting	×
Canvas Width:	300
Canvas Height:	300
OK	Cancel

The area in the textbox is the valid area.

Line

You can insert lines into map to more efficiently organize the APs. To insert a line, click the **Insert line** item from the 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.

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.

Y ScanAP			
File View Help			
8			
Scan Information		, Chart	
BSSID	SSID Channel	Au	
00010	Solo Channel	Total	
		100	
		80	
		$\overline{\sigma}_{e0}$	
		20	
	(16:48 16:49 16:50 16:51 16:52 16:53 16:54 16:55 16:56 16:57 16:58	16:59
<			
- Wireless Adapters			
Location ID	LocationA		
Location in	1 martine and a second s		
Interval Time	6 Seconds(63600)		
Total Time	720 Seconds		
Description	LocationA		
Wireless Adapters	Ē		
	1		
Last Scan At	1900-01-01 00:00:01		
Scheduled Next Scar	1900-01-01 00:00:01		
Start	Stop		
Ready		2008-6-11 16:47:40	

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

BSSID	SSID	Channel	Authentication
DO:eO:4c:8c:86:71	ella_test_333	10	Yes
D0:03:7f:be:ef:11	3200_test	6	No
00:0c:43:28:60:d8	C300BRS4	6	No
D0:03:7f:be:f1:98	ChinaNetwww	3	No
00:03:7f:be:f0:43	dlink	13	No
00:1c:f0:18:fb:69	dlink	11	No
00:27:41:72:25:01	dlink-kwest	6	No
D0:80:c8:19:1c:11	dlink	6	No
D0:60:b3:27:fc:16	KangTe-11g	8	Yes
<			

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:

				?
🔁 Scan AP		<u> </u>	🗢 🖻 💣 📰	•
File name:	LocationA.stp		•	Save
rile riditie.				
	: 🔁 Scan AP			

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.

Open	? 🛛
Look in: 隘	Scan AP 💽 🗢 🛅 🐨
LocationA.	stp
File name:	Open
Files of type:	SitePlanning Files (*.stp)
	C Open as read-only

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

Model Name	MAC Address	IP Ad	ldress	SSID		Status		
DWL-3200AP	001346FDB4F	8 172.1	8.215.50			Done		
	001346FDB4F	8 172.1	8.215.50	DWL-3	3200AP	802.11b/g		
OWL-8200AP	001195F1C110		68.0.50			Done		
	001195F1C110		68.0.50	8200g		802.11b/g		
	001195F1C110) 192.1	68.0.50	8200a		802.11a		
DateTime SSID			MAC Address Band		Band	Authentication	RSSI	Power Sa
•								►

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

To list the APs according to the detected date, choose the date range from the **From/To** drop-down menu, and click the **Search** 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

				Security Report		
12			Wrelesz Retwork/(SSI	D)		 Legend 8200x-802.11a 8200x902.11b/g DWL-3200AP-802.11b/g
Security Details	Model Name	MAC Address	IP Address	Authentication	Band	
8200a 8200g DWL-3200AP	DWL-8200AP DWL-8200AP DWL-3200AP	001195F1C110 001195F1C110 001346FDB4F8	19 Address 192.168.0.50 192.168.0.50 172.18.215.50	Open System Open System Open System	Bana 802.11a 802.11b/g 802.11b/g	
						Refresh

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.

General Group Group Full Manage Total Manage Total Manage Total Report Security Ministion Channel Repue AF	Transmit Detail									
Group MultiConfiguration Fault Manage Tool	DateTime	IP Address	Max STA	's Number UI)Time T	rasmitted Packets	Trasmitted Success Rate	Trasmitted Retry Rate	Band	
+ Group + MultiConfiguration + Fault Manage + Tool - Report Association Security - Utilization - Chamel		Selec	at l							
					IP Address 192.168.0.5	Netmask 255.255.25	5.0			
		ت s	elete from Custo	Sel	lect	Cancel				
	Polling Detail			Poll 2008-06-11 1	15.20.29	Enable Thresho	11 11 12	Start		
	Polling Interval 5 n		cheduled Next . Last Polled At	2008-06-11 1			TransSuccessRal 💌	End		
	2008-06-11 15:20 2008-06-11 15:20):05 FTP Server star):06 SnmpTrap initial):19 Discover Compl):20 Device: 192.168.	iztion succe: eted!	ssl						

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.

Туре	Channel	BSSID	Security	Mode	SSID	RSSI		
P BSS	9	001CF008E638	WPA-Auto-Personal	802.11g		80 %		
P BSS	9	001CF008E639	WPA-Auto-Personal	802.11g	wireless test team	76 %		
P BSS	8	0060B327FC16	WEP	802.11g	KangTe-11g	28 %		
P BSS	3	001195F1C118	OFF	802.11g	8200g	20 %		
AP BSS	13	00037FBEF03F	OFF	802.11g	dlink p	48 %		
AP BSS	11	001B11A8A608	WEP	802.11g	USEE-CNC	44 %		
AP BSS	11	000D3BFEFACF	OFF	802.11g	CNC-SC2	8%		
AP BSS	11	081074010AA2	WEP	802.11g	scdcte	16 %		
AP BSS	11	0015707972C0	OFF	802.11g	SCCNC-MOT-CD-SX	10 %		
AP BSS	11	00E04C8186D1	WEP	802.11g	dink	50 %		
AP BSS	6	00134635DD37	OFF	802.11g	Penta CD	18 %		
AP BSS	6	00055D559312	OFF	802.11g	HT AP0	42 %		
AP BSS								
AP BSS	6	000027418948	OFF	802.11g	dink-dir300-ella	24 %		
	6	0050BA010004		802.11g	ChinaNet-DTG800HA			
AP BSS	6	0019E093F622	OFF	802.11g	TP-LINK	16 %		
AP BSS	6	00E04C8C8671	OFF	802.11g	dlink	26 %		
AP BSS	6	00E04C8186D6	OFF	802.11g	dink_hoooooooooo	28 %		
AP BSS	6	00CD013306A1	WEP	802.11g	dlink	44 %		
AP BSS	6	001B119D3EFE	WEP	802.11g	USEE-CT	44 %		
AP BSS	6	001B118C494C	OFF	802.11g	dlink	86 %		
AP BSS	6	00119594EB80	WPA-Personal	802.11g	gabriel	66 %		
AP BSS	6	0050F1121210	OFF	802.11g	E1131	40 %		_
AP BSS	1	0060B38E51A8	OFF	802.11g	UNICOM	18 %		
AP BSS	1	00030F0ED7BF	OFF	802.11g	DCW-BR54+	26 %		-
AD DCC		00105050555	055	000.11-	allaL/D()	64.04		
Туре	Channel	BSSID	Security	Mode	SSID	RSSI		
AP BSS	13	00037FBEF043	OFF	802.11g	dlink	42 %		
								-
							DUL DU	
							Detect Delete	

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 106.

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	[5Y5]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]WLANO 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

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.

er Lanage User ———						
User Name	Password	Privilege	Creat Date			
admin	admin	Administrator				
<			>			
Ad	l Update	Delete				
Name	Pas	sword				
Privilege Mana	lege Manager					
Resume						

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 **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.

	To use the system, user should input name and password Please select the user to use the system Jser Name Privilege Creat Date Resume				_
admin	Privilege Administra	Creat Date		Resume	
<					>
,)	
SNMP Setting				~	
Public Communit	y String	public	Port 1	61	
Private Commun	ity String	private			
SNMP Response	e TimeOut	30			
– Polling Setting –					
Polling type	💿 Disable	🔿 Enable			
Interval time	30	(10-60sec)			
Discover		,			
Retry	1	TimeOut	5	(5-60sec)	

Logon Se	etting	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 S	etting	Set the Public/Private Community String, Port number and SNMP
		Response Timeout.
Polling So	etting	Disable by default. When this function is enabled, you must set the
-	-	polling interval time, it is 30 seconds by default.
Dis	cover	Enter the Retry number and the time of timeout when discovering.

Option							
General Module Database Maintenance Advance							
Select firmware file for model							
Model Name	Firmware file						
DAP-2590 DWL-2700AP							
DWL-3200AP DWL-7700AP	Save	Browse					
DWL-9700AP DWL-8200AP	Module Information-						
	Model Name	DAP-2590					
	Description	AP Manager II Module v1.00r05 (2008-6-4)					
	. ·	1.00					
	Version: Support Band:	1.00 11b/g/n					
	Support Bana.	Tib/g/n					
		OK Cancel Apply					

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.

Option					
General Module Database Maintenance Advance					
Select Fault Notice By Records To ensure the database efficient, Please notice user to clear the database Notice user when records Clear Rule Clear Rule To Delete all records					
C Delete these top records					
Records: 100					
O Delete these records before the datetime					
Datetime: 2008- 6-11 💌					
	Clear				
OK Cancel	Apply				

SelectChoose the type of records.Notice By RecorSet the number that record reach to notice the user to clear the
database.Clear RuleDelete 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.

Option			×
General Module Database Maintenance	Advance		
TimeOut Settings			
Set Timeout(s)	5		
Reboot Timeout(s)	50		
Configuration Flash Update Time(s)	60		
Factory Reset Time(s)	60		
F/W Download Time(s)	60		
F/W Flash Update Time(s)	80		
Timing Tolerance Time(s)	5	Defaul]
FTP Server Enable Local FTP Server Enable Remote FTP Server Remote Server IP Address User Name Password Port	0.0 admin xxxxxx 21	. 0 . 0	
⊢Language ☐ Default (English)			
	OK	Cancel	Apply

TimeOut Setting Configure the system time out settings.

Select Enable Local FTP Server to run an ftp server on the local computer. The ftp server will run when AP Manager II starts. Select Enable Remote FTP Server if all the system logs are stored in a lone ftp server. You should configure the ftp server parameters here.
 Language Select an interface language for AP Manager II. It only supports English now.

Contacting Technical Support

Technical Support

You can find software updates and user documentation on the D-Link website.

U.S. and Canadian customers can contact D-Link Technical Support through our website, or by phone.

Tech Support for customers within the United States: D-Link Technical Support over the Telephone: (877) 354-6555

> *D-Link Technical Support over the Internet:* http://support.dlink.com

Tech Support for customers within Canada: *D-Link Technical Support over the Telephone:* (877) 354-6560

> *D-Link Technical Support over the Internet:* http://support.dlink.com

> > Version 2.0 June 18, 2008