D-Link®
Building Networks for People

DAP-3690

Version 1.0

*Air*Premier N®

Concurrent Dual Band Outdoor PoE Access Point

User Manual

Business Class Networking

Table of Contents

Package Contents

- D-Link DAP-3690 AirPremier® N Concurrent Dual Band Outdoor PoE Access Point
- CD-ROM (with Product Documentation)
- PoE Base Unit
- Four Dipole Antennas
- Grounding Wire
- Power Cord
- Power Adapter
- Mounting Kits
- Console Cable (Indoor use only)*
- Console Cable Waterproof Enclosure
- Two LAN port Waterproof Enclosures

**Do not use the console cable in an outdoor environment for long term use. We strongly recommend a type CMX console cable for outdoor use.*

Warning: Using a power adapter with different specifications than the one included with the DAP-3690 will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer 6.0, Firefox 3.0, Chrome 2.0, and Safari 3.0 and above.

Warning: This product should only be maintained by the authorized server manager.

Introduction

D-Link introduces its new AirPremier N Concurrent Outdoor Dual Band PoE Access Point (DAP-3690). With a series of versatile function, high power design[1] and weather resistant features, DAP-3690 is an ideal solution for hot spot networks to provide outdoor users with wireless Internet access. It can also be installed at manufacturing plants, industrial locations, convention halls, school campuses, airports, golf courses, marinas and other outdoor venues.

Versatile Access Point

The DAP-3690 allows network administrators to deploy a highly manageable and extremely robust concurrent dual band wireless network. All four antennas are detachable and can provide optimal wireless coverage in both 2.4GHz (802.11g and 802.11n) and 5GHz (802.11a and 802.11n) bands. Ideal for outdoor deployment, this device is built with a series of weather resistant features, such as a built in heater, to withstand all elements. For advanced installation, this new high-speed access point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation in areas where power outlets are not readily available.

Enhanced Performance

The AirPremier N Concurrent Dual Band PoE Access Point delivers reliable wireless performance with maximum wireless signal rates of up to 300Mbps[2] in either the 2.4GHz or 5GHz wireless band. This, coupled with support for Wi-Fi Multimedia™ (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications. Additionally, the DAP-3690 supports load balance features to ensure maximum performance.

Security

To help maintain a secure wireless network, the AirPremier N Concurrent Dual Band PoE Access Point provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server back end. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

The AirPremier N Concurrent Dual Band PoE Access Point includes support for up to 16 VLANs (8 VLANs per radio) for implementing multiple SSIDs to further help segment users on the network. The DAP-3690 also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

Features and Benefits

- Four different operation modes - Capable of operating in one of four different operation modes to meet your wireless networking needs: Access Point, WDS with AP, WDS, or Wireless Client.
- Faster wireless networking with the 802.11n standard to provide a maximum wireless signal rate of up to 300 Mbps[2].
- Compatible with the 802.11b standard to provide a wireless data rate of up to 11 Mbps, allowing you to migrate your system to the 802.11n and 802.11g standards on your own schedule without sacrificing connectivity.
- Compatible with the 802.11g standard to provide a wireless data rate of up to 54Mbps in the 2.4GHz frequency range.
- Compatible with the 802.11a standard to provide a wireless data rate of up to 54Mbps in the 5GHz frequency range.
- Better security with WPA (Wi-Fi Protected Access)/WPA2 - The DAP-3690 can securely connect wireless clients on the network using WPA/WPA2 to provide a much higher level of security for your data and communications than its previous versions.
- AP Manager II management software - The real-time display of the network's topology and AP's information makes network configuration and management quick and simple.
- SNMP for management - The DAP-3690 is not just fast, but also supports SNMP v.3 for better network management. Superior wireless AP manager software is bundled with the DAP-3690 for network configuration and firmware upgrade. Systems administrators can also set up the DAP-3690 easily with the Web-based configuration. D-Link D-View 6.0 module can be download to manage and real-time network traffic monitoring with multiple access points from a single location.
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing).
- Supports 802.3af Power over Ethernet.
- Supports one 10/100/1000M Ethernet port.
- Operates in the 2.4~2.5 GHz and 5.15~5.85 GHz3 frequency ranges.

[1] Maximum power setting will vary according to individual country regulations.

[2] Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

[3] Operation frequency ranges vary depending on the regulations of individual countries

Wireless Basics

D-Link wireless products are based on industry standards to provide high-speed wireless connectivity that is easy to use within your home, business or public access wireless networks. D-Link wireless products provides you with access to the data you want, whenever and wherever you want it. Enjoy the freedom that wireless networking can bring to you.

WLAN use is not only increasing in both home and office environments, but in public areas as well, such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are allowing people to work and communicate more efficiently. Increased mobility and the absence of cabling and other types of fixed infrastructure have proven to be beneficial to many users.

Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards, allowing wireless users to use the same applications as those used on a wired network.

People use WLAN technology for many different purposes:

Mobility - Productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.

Low implementation costs - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and network expansion - By avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.

Inexpensive solution - Wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-3690 saves money by providing users with multi-functionality configurable in four different modes.

Scalability - Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Standards-Based Technology

The DAP-3690 Wireless Access Point utilizes the 802.11a, 802.11b, 802.11g, and 802.11n standards.

The IEEE 802.11n standard is an extension of the 802.11a, 802.11b, and 802.1g standards that came before it. It increases the maximum wireless signal rate up to 300 Mbps* within both the 2.4 GHz and the 5 GHz bands, utilizing OFDM technology.

This means that in most environments - within the specified range of this device - you will be able to transfer large files quickly, or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then simultaneously transmitted at different frequencies to the receiver. OFDM reduces the amount of crosstalk (interference) in signal transmissions.

The D-Link DAP-3690 will automatically sense the best possible connection speed to ensure the greatest possible speed and range.

Note: *802.11n offers the most advanced network security features available today, including WPA.*

*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Installation Considerations

The D-Link DAP-3690 lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the DAP-3690 and other network devices to a minimum - each wall or ceiling can reduce your DAP-3690's range by 3-90 feet (1-30 meters). Position your devices so that the number of walls or ceilings is minimized.

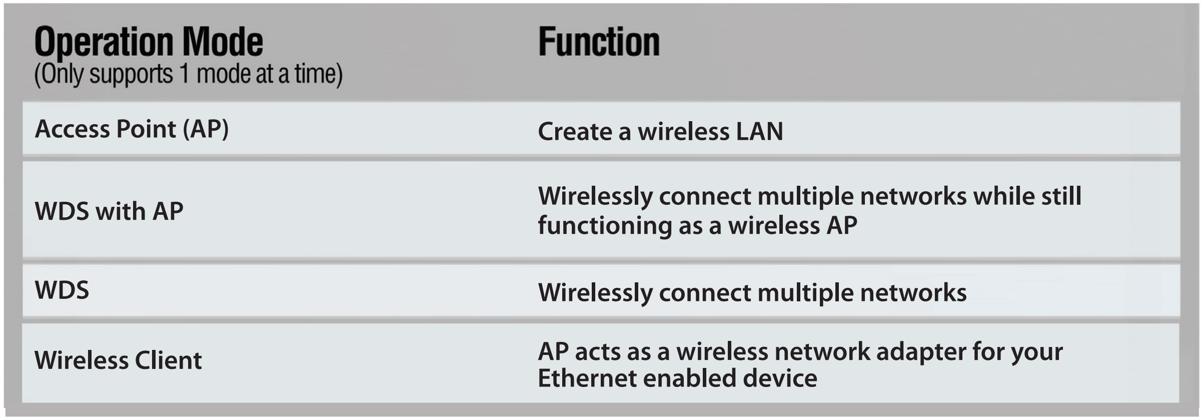
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle, the wall appears to be over 42 feet (14 meters) thick! Position your devices so that the signal will travel straight through a wall or ceiling - instead of at an angle - for better reception.

3. Building materials can impede the wireless signal - a solid metal door or aluminum studs can have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways, and not through other materials.

4. Keep your product away - at least 3-6 feet or 1-2 meters - from electrical devices or appliances that generate RF noise.

5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even when the phone is not in use.

Four Operational Modes



Operation Mode (Only supports 1 mode at a time)	Function
Access Point (AP)	Create a wireless LAN
WDS with AP	Wirelessly connect multiple networks while still functioning as a wireless AP
WDS	Wirelessly connect multiple networks
Wireless Client	AP acts as a wireless network adapter for your Ethernet enabled device

Connect to Your Network

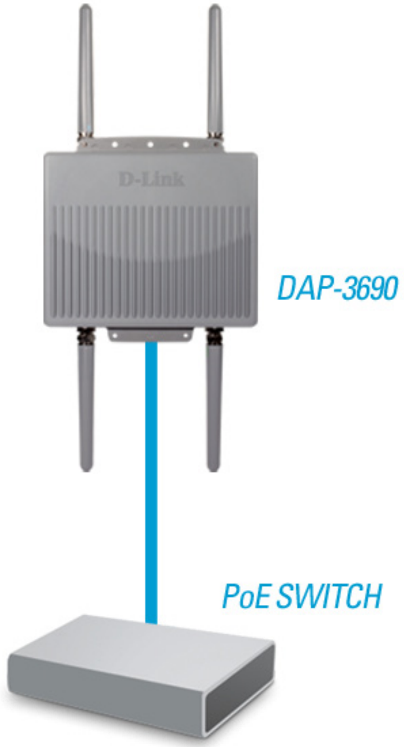
To power the access point, you can use one of the following 3 methods:

Method 1 - Use if you have a PoE switch.

Method 2 - Use if you do not have a PoE switch and do not have a power outlet near the location of the access point.

Method 1

1. Connect one end of your Ethernet cable into the LAN (PoE) port on the DAP-3690 and then connect the other end to your PoE switch.



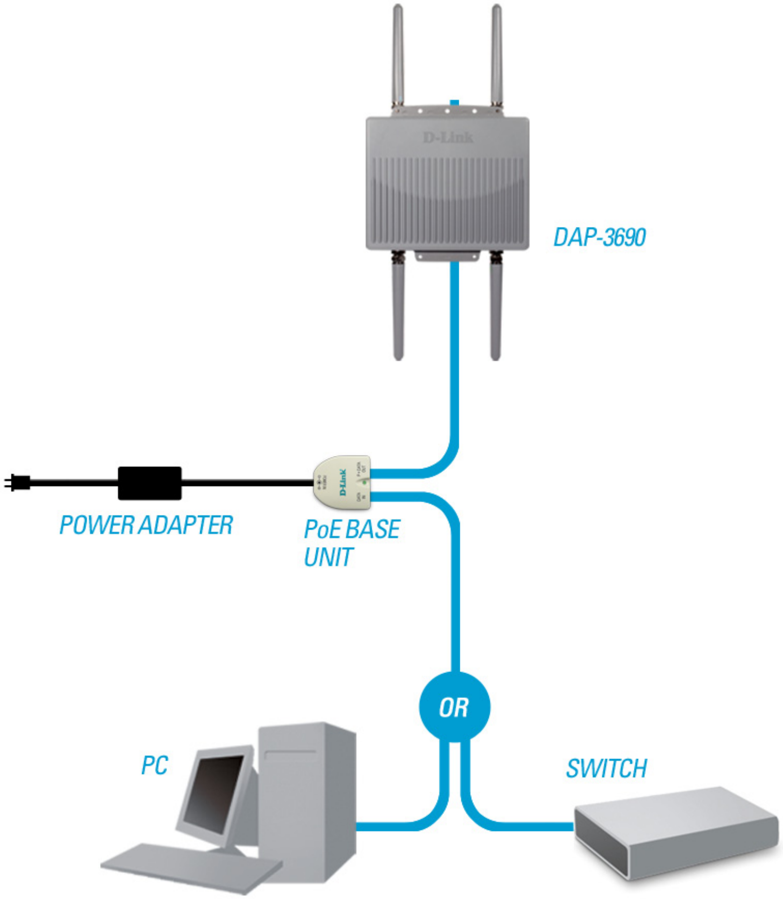
Method 2

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE base unit and the other end into one port on your switch, router, or computer.

2. Connect one end of an Ethernet cable into the **P+Data Out** port on the PoE base unit and the other end into the **LAN (PoE)** port on the DAP-3690 access point.

3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.

4. Connect the power cable to the power adapter and then connect the other end into a power outlet.



Using the Configuration Menu

To configure the DAP-3690, use a computer that is connected to the DAP-3690 with an Ethernet cable (see the *Network Layout diagram*).

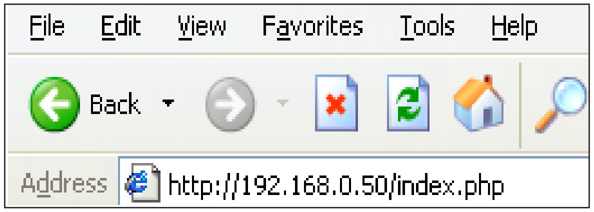
First, disable the "Access the Internet using a proxy server" function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.

Start your web browser program (I.E. Internet Explorer).

Type the IP address and http port of the DAP-3690 in the address field (**http://192.168.0.50**) and press **Enter**. Make sure that the IP addresses of the DAP-3690 and your computer are in the same subnet.

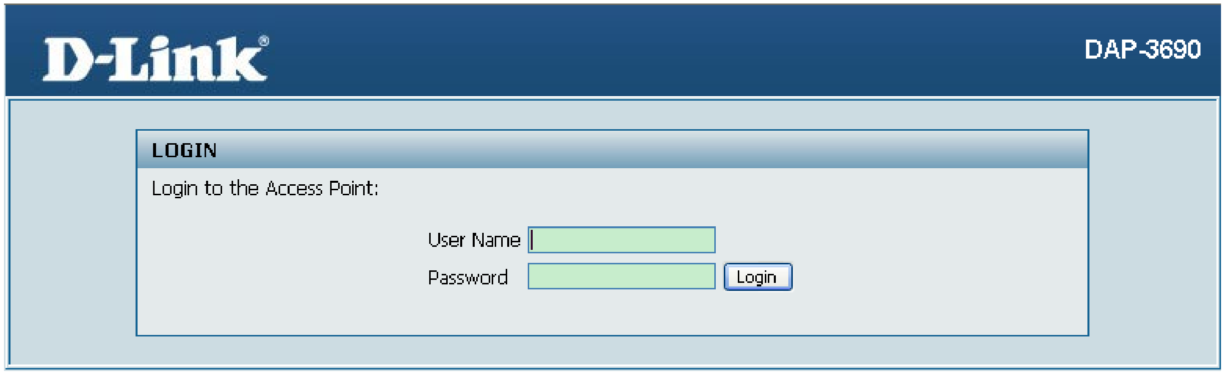
After the connection is established, you will see the user identification window as shown.

Note: *If you have changed the default IP address assigned to the DAP-3690, make sure to enter the correct IP address.*



http://192.168.0.50/index.php

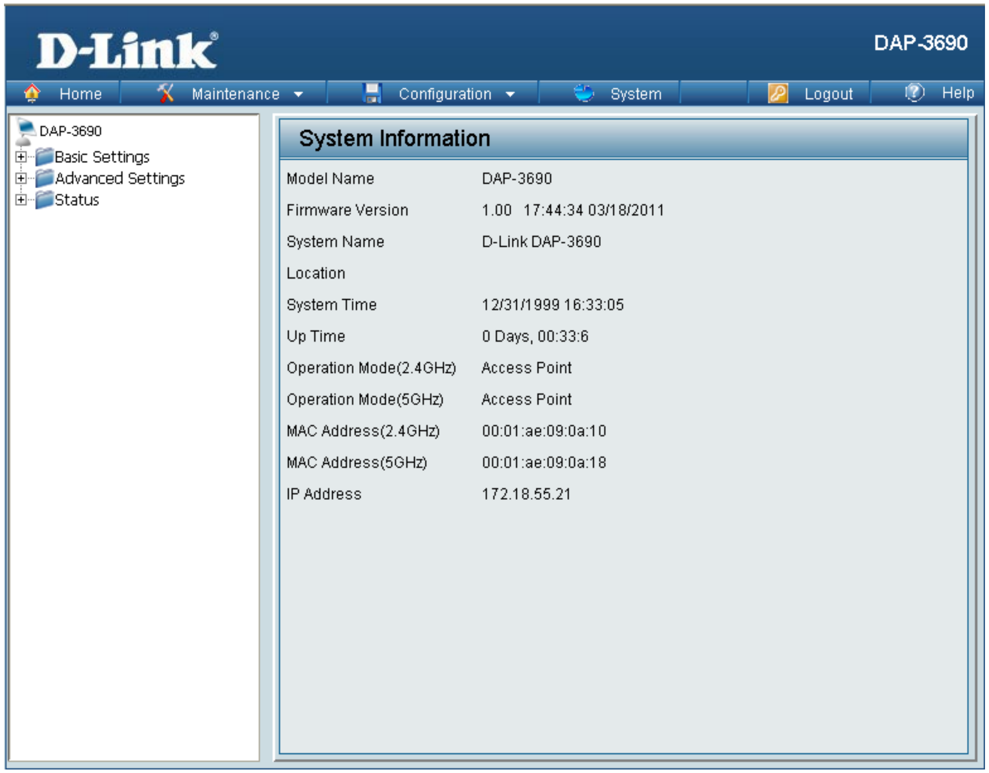
- Type "**admin**" in the User Name field.
- Leave the Password field blank.
- Click the **Login** button.



Note: *If you have changed the password, make sure to enter the correct password.*

After successfully logging into the DAP-3690 the following window will appear:

When making changes on most of the configuration windows in this section, use either the **Apply** button or the **Save** button to save your configuration changes.



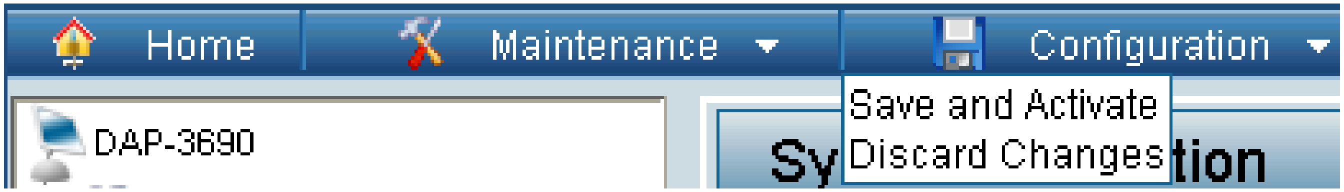
System Information

Model Name	DAP-3690
Firmware Version	1.00 17:44:34 03/18/2011
System Name	D-Link DAP-3690
Location	
System Time	12/31/1999 16:33:05
Up Time	0 Days, 00:33:6
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz)	Access Point
MAC Address(2.4GHz)	00:01:ae:09:0a:10
MAC Address(5GHz)	00:01:ae:09:0a:18
IP Address	172.18.55.21

Click the **Apply** button to configure changes.

Click the **Save** button to configure changes.

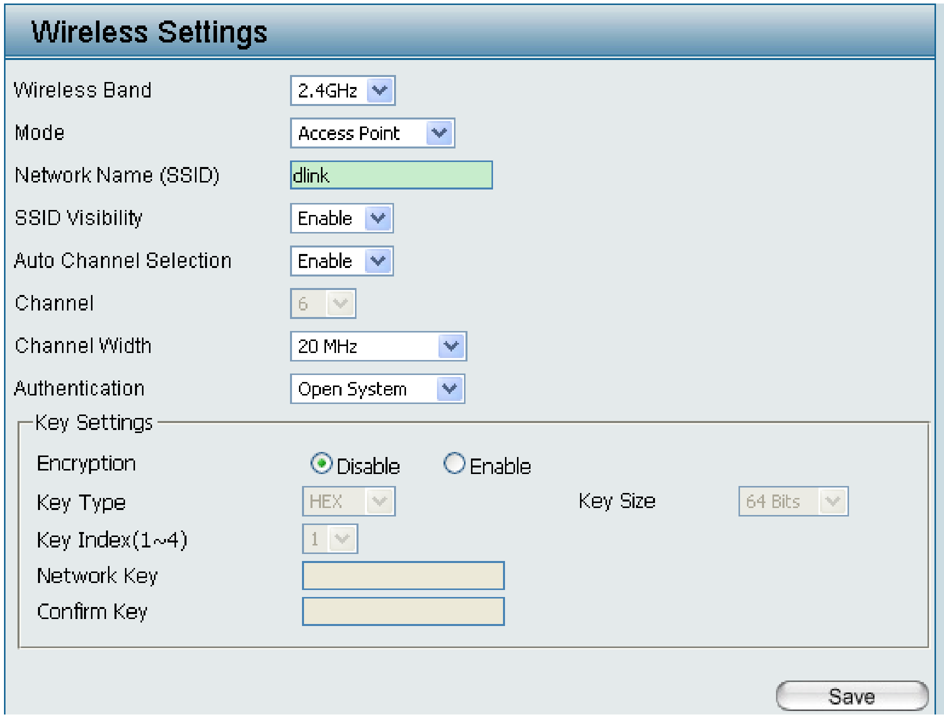
Alternatively, click the “Save and Activate” option on the Configuration drop-down menu at the top of each DAP-3690 window. This will cause the DAP-3690 to save and reboot.



Wireless Settings

Access Point Mode

In Access Point mode, the DAP-3690 functions as a wireless AP. After completing the desired settings, click the **Save** button to let your changes take effect.



Wireless Settings

Wireless Band	2.4GHz
Mode	Access Point
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	6
Channel Width	20 MHz
Authentication	Open System

Key Settings

Encryption	● Disable ○ Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

Wireless Band: Select either **2.4 GHz** or **5 GHz** from the drop-down menu.

Mode: Select **Access Point** from the drop-down menu. The other three choices are **WDS with AP**, **WDS**, and **Wireless Client**.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can easily be changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Auto Channel Selection: Enabling this feature automatically selects the channel that provides the best wireless performance. **Enable** is set by default. The channel selection process only occurs when the AP is booting up.

Channel: All devices on the network must share the same channel. To change the channel, first toggle the Auto Channel Selection setting to **Disable**, and then use the drop-down menu to make the desired selection. (***Note:*** *The wireless adapters will automatically scan and match the wireless settings.*)

Channel Width: Allows selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. When the channel width is set to **Auto 20/40 MHz**, then 802.11n wireless devices are allowed to transmit data using 40 MHz.

Authentication: Select **Open System** to communicate the key across the network.

Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.

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

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

Select **802.1X** if your network is using port-based Network Access Control.

For more information about the different types of Authentication offered on the DAP-3690 and the respective settings of each, please go to the first page of the "Authentication" explanations, which begins on page 23.

WDS with AP mode

In WDS with AP mode, the DAP-3690 wirelessly connects multiple networks while still functioning as a wireless AP. After completing the desired settings, click the **Save** button to let your changes take effect.

Wireless Band: Select either **2.4 GHz** or **5 GHz** from the drop-down menu.

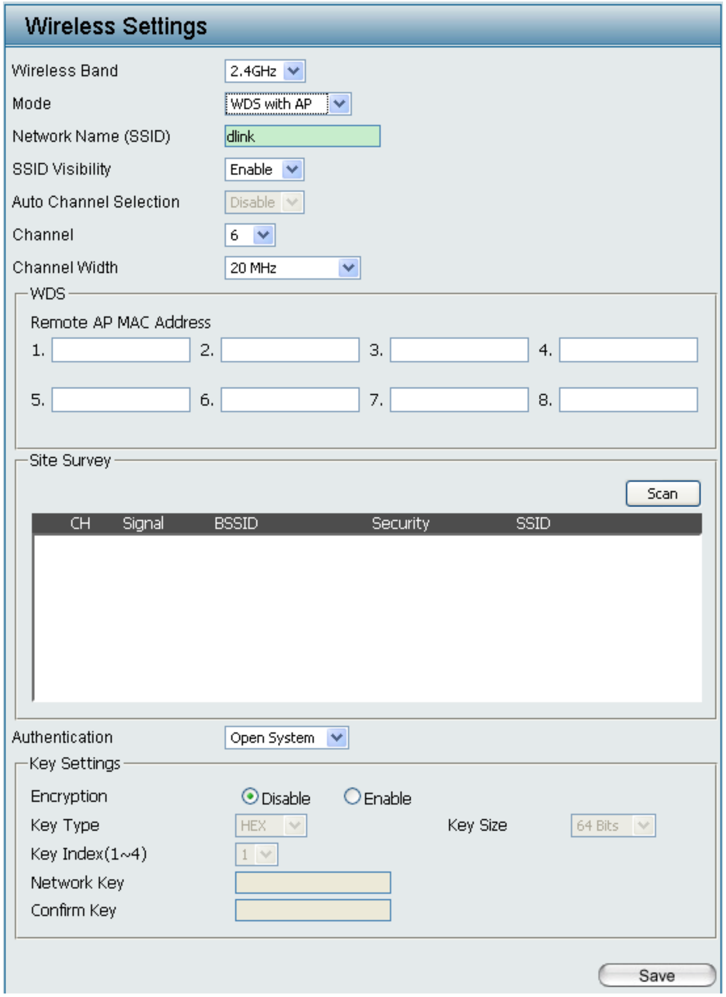
Mode: **WDS with AP** mode is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's 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.

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS with AP mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (***Note:*** *The wireless adapters will automatically scan and match the wireless settings.*)



Wireless Settings

Wireless Band	2.4GHz
Mode	WDS with AP
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Disable
Channel	6
Channel Width	20 MHz

WDS

Remote AP MAC Address

1. 2. 3. 4.

5. 6. 7. 8.

Site Survey

Scan

CH	Signal	BSSID	Security	SSID

Authentication: Open System

Key Settings

Encryption	● Disable ○ Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

Save

Channel Width: Allows selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. 802.11n wireless devices are allowed to transmit data using 40 MHz when the channel width is **Auto 20/40 MHz**.

Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Site Survey: Click the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose **Open System**, **Shared Key**, or **WPA-Personal**.

Select **Open System** to communicate the key across the network.

Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.

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

For more information about the different types of Authentication offered on the DAP-3690 and the respective settings of each, please go to the first page of the “Authentication” explanations, which begins on page 23.

WDS mode

In WDS mode, the DAP-3690 wirelessly connects multiple networks, without functioning as a wireless AP. After completing the desired settings, click the **Save** button to let your changes take effect.

Wireless Band: Select either **2.4 GHz** or **5 GHz** from the drop-down menu.

Mode: **WDS** is selected from the drop-down menu.

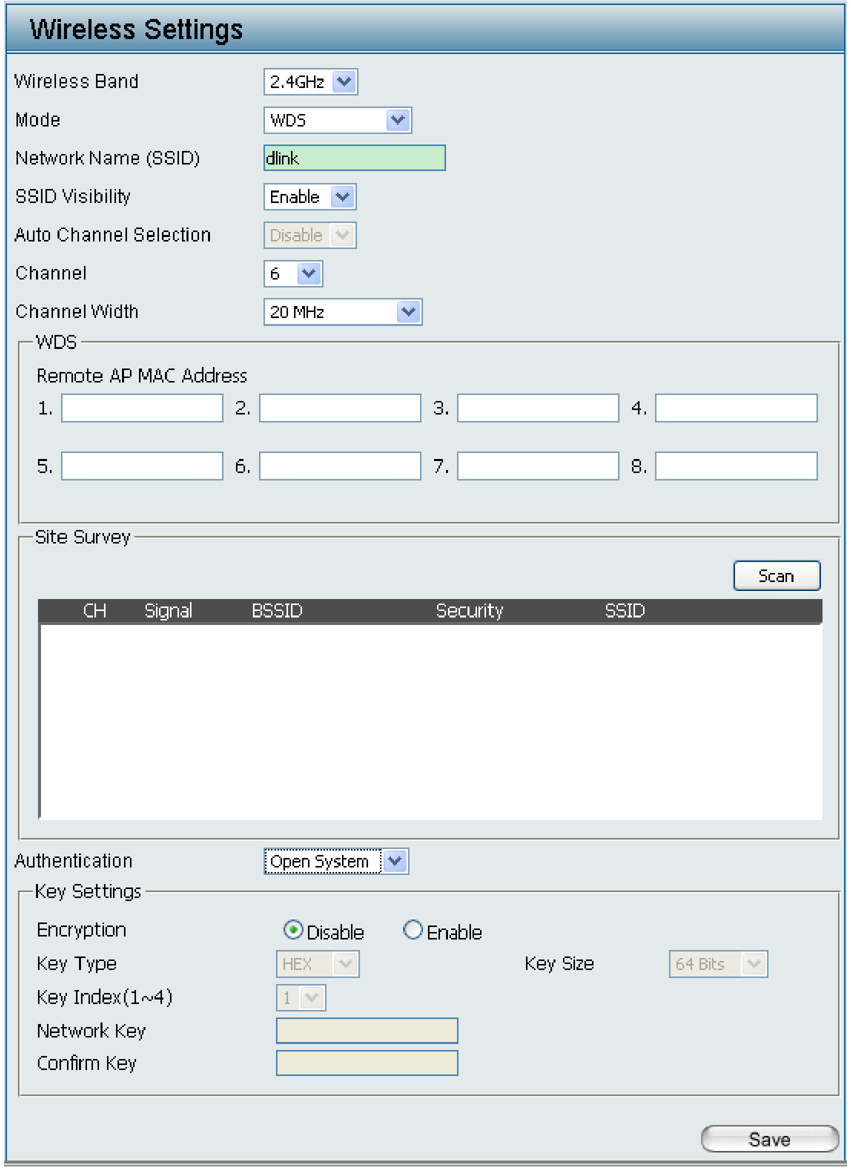
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection.

Channel Width: Allows selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. 802.11n wireless devices are allowed to transmit data using 40 MHz when the channel width is **Auto 20/40 MHz**.



Wireless Settings

Wireless Band: 2.4GHz
Mode: WDS
Network Name (SSID): dlink
SSID Visibility: Enable
Auto Channel Selection: Disable
Channel: 6
Channel Width: 20 MHz

WDS

Remote AP MAC Address
1. 2. 3. 4.
5. 6. 7. 8.

Site Survey

Scan

CH	Signal	BSSID	Security	SSID

Authentication: Open System

Key Settings

Encryption: ● Disable ○ Enable
Key Type: HEX
Key Size: 64 Bits
Key Index(1~4): 1
Network Key
Confirm Key

Save

Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Site Survey: Click the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose **Open System**, **Shared Key**, or **WPA-Personal**.

Select **Open System** to communicate the key across the network.
Select **Shared Key** to limit communication to only those devices that share the same WEP settings.
Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.

For more information about the different types of Authentication offered on the DAP-3690 and the respective settings of each, please go to the first page of the Authentication explanations which begins on page 23.

Wireless Client mode

In Wireless Client mode, the DAP-3690 functions as a wireless client on a wireless network in which an AP already exists. After completing the desired settings, click the **Save** button to let your changes take effect.

Wireless Band: Select either **2.4 GH**z or **5 GHz** from the drop-down menu.

Mode: **Wireless Client** is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network.

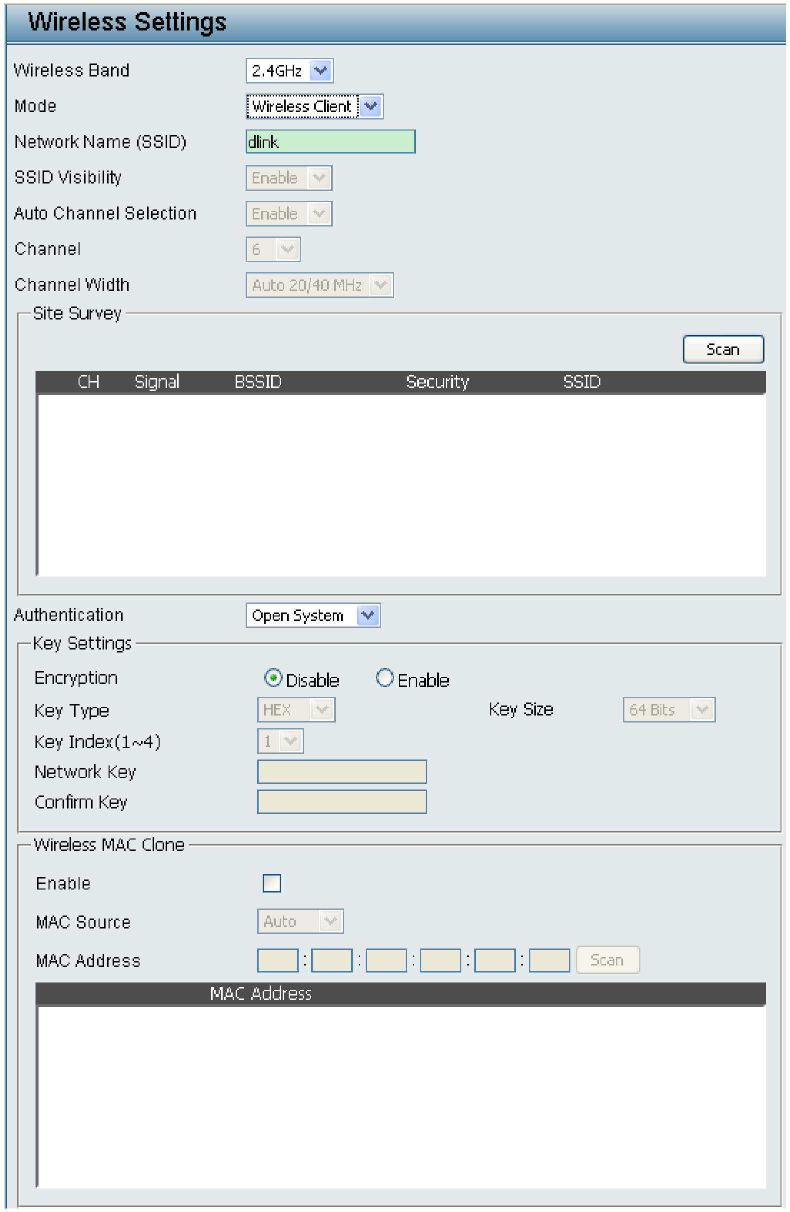
SSID Visibility: This option is unavailable in wireless client mode.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in Wireless Client mode.

Channel: The channel used will be displayed, and follow the root AP.

Channel Width: This option is unavailable in wireless client mode.

Site Survey: Click the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.



Wireless Settings

Wireless Band	2.4GHz
Mode	Wireless Client
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	6
Channel Width	Auto 20/40 MHz

Site Survey

Scan

CH	Signal	BSSID	Security	SSID

Authentication: Open System

Key Settings

Encryption ● Disable ○ Enable

Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

Wireless MAC Clone

Enable □

MAC Source: Auto

MAC Address: : : : : : Scan

MAC Address

Authentication: Use the drop-down menu to choose **Open System** or **WPA Personal**.

Select **Open System** to communicate the key across the network.

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

For more information about the different types of Authentication offered on the DAP-3690 and the respective settings of each, please go to the first page of the Authentication explanations which begins on page 23.

Wireless MAC Clone

Enable: Click the box to enable the Wireless MAC Clone feature. Enabling this option allows the user to manually assign the source MAC address to packets forwarded by the DAP-3690. If disabled, the packet's source MAC address field will be automatically selected as the DAP-3690's MAC address.

MAC Source: Use the drop-down menu to select either **Auto** or **Manual**.

MAC Address: If you selected **Manual** for the MAC Source above, you can either click the **Scan** button to search for all available devices connected to your DAP-3690's Ethernet port or manually enter a MAC address in the space provided.

Open System or Shared Key Authentication

Encryption: Use the radio button to disable or enable encryption.

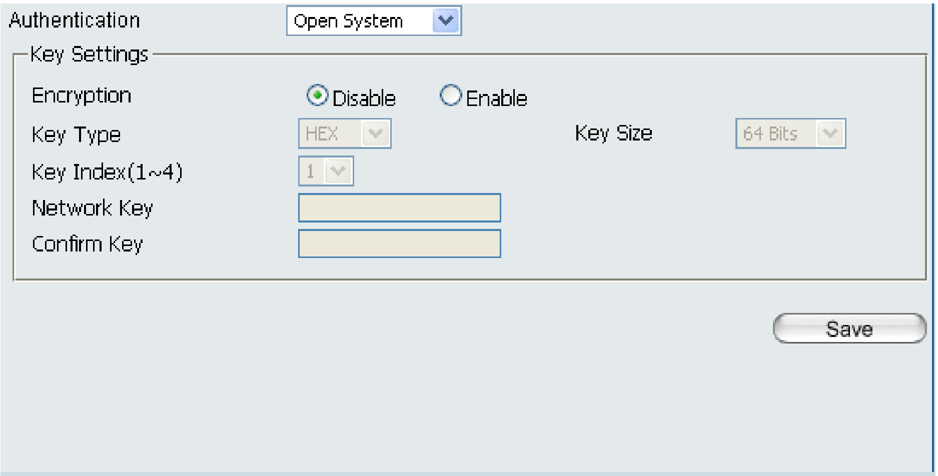
Key Type: Select **HEX**** or **ASCII***.

Key Size: Select **64 Bits** or **128 Bits**.

Key Index (1~4): Select the 1st through the 4th key to be the active key.

Network Key: Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

Confirm Key: Retype the Network Key entered above in the corresponding field.



Authentication: Open System

Key Settings

Encryption ● Disable ○ Enable

Key Type: HEX

Key Size: 64 Bits

Key Index(1~4): 1

Network Key

Confirm Key

**ASCII (American Standard Code for Information Interchange) is a code that represents English letters using numbers ranging from 0-127.*

***Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.*

WPA-Personal Authentication

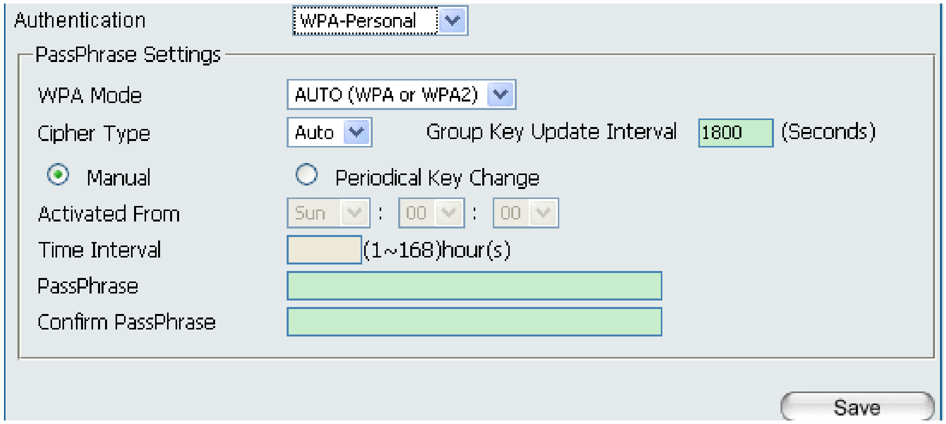
WPA Mode: When **WPA-Personal** is selected for Authentication type, you must also select a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2.

Cipher Type: When you select WPA-Personal, you must also select **AUTO**, **AES**, or **TKIP** from the drop-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. The default value of **1800** is recommended.

PassPhrase: When you select WPA-Personal, please enter a PassPhrase in the corresponding field.

Confirm PassPhrase: Retype the PassPhrase entered above in the corresponding field.



Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: AUTO (WPA or WPA2)

Cipher Type: Auto   Group Key Update Interval: 1800 (Seconds)

● Manual   ○ Periodical Key Change

Activated From: Sun : 00 : 00

Time Interval: (1~168)hour(s)

PassPhrase:

Confirm PassPhrase:

WPA-Enterprise Authentication

WPA Mode: When **WPA-Enterprise** is selected, you must also select a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: **Auto**, **AES**, or **TKIP**.

Group Key Update Interval: Select the interval during which the group key will be valid. The recommended value is **1800**, as a lower interval may reduce data transfer rates.

Network Access Protection: Enable or disable Microsoft Network Access Protection.

RADIUS Server: Enter the IP address of the RADIUS server. Click External if the RADIUS server is on your network or Internal if you are using the RADIUS server on the DAP-3690.

RADIUS Port: Enter the RADIUS port (**1812** is the default).

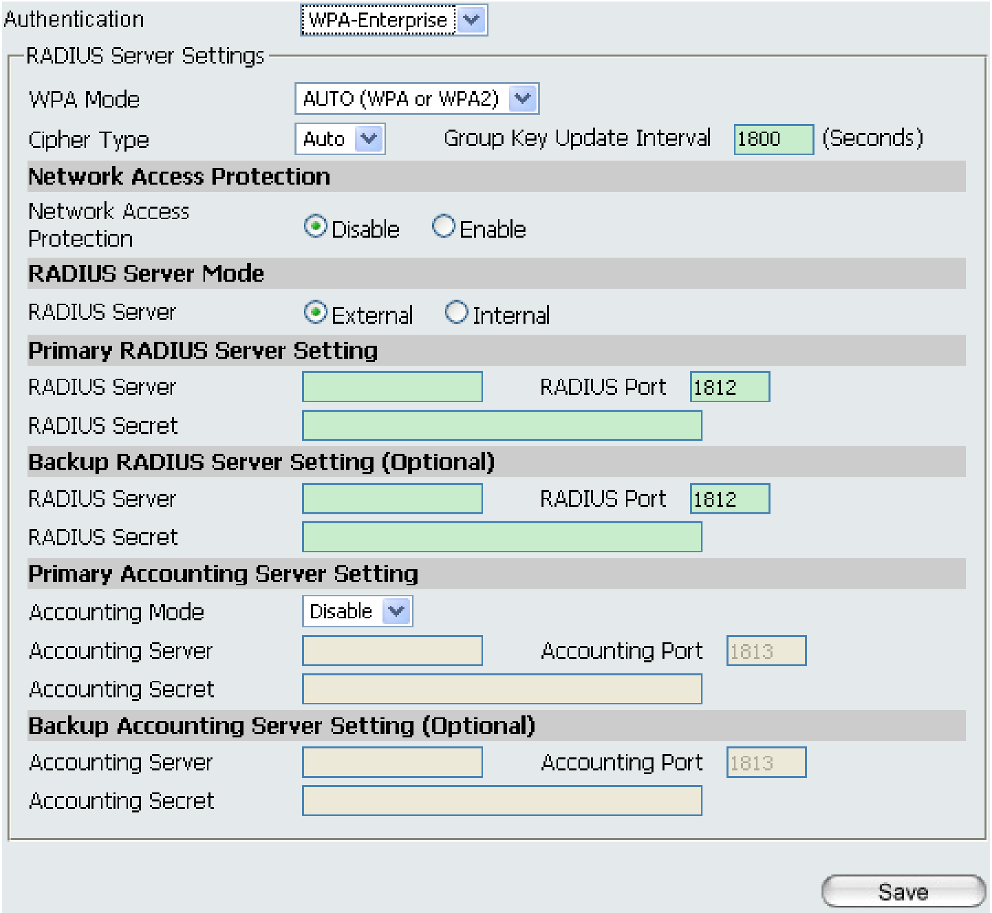
RADIUS Secret: Enter the RADIUS secret.

Accounting Mode: Select if you want to use a different server for accounting.

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

Accounting Port: Enter the Accounting port (**1813** is the default).

Accounting Secret: Enter the Accounting secret.



Authentication: WPA-Enterprise

RADIUS Server Settings

WPA Mode: AUTO (WPA or WPA2)

Cipher Type: Auto — Group Key Update Interval: 1800 (Seconds)

Network Access Protection

Network Access Protection: ● Disable ○ Enable

RADIUS Server Mode

RADIUS Server: ● External ○ Internal

Primary RADIUS Server Setting

RADIUS Server: — RADIUS Port: 1812

RADIUS Secret:

Backup RADIUS Server Setting (Optional)

RADIUS Server: — RADIUS Port: 1812

RADIUS Secret:

Primary Accounting Server Setting

Accounting Mode: Disable

Accounting Server: — Accounting Port: 1813

Accounting Secret:

Backup Accounting Server Setting (Optional)

Accounting Server: — Accounting Port: 1813

Accounting Secret:

***Note:** You can input the secondary RADIUS server and accounting server settings if you have a backup RADIUS and accounting server.*

802.1X Authentication

Key Update Interval: Select the interval (in seconds) during which the key will be valid.

RADIUS Server: Enter the IP address of the RADIUS server. Click **External** if the RADIUS server is on your network or **Internal** if you are using the RADIUS server on the DAP-3690.

RADIUS Port: Enter the RADIUS port (**1812** is the default).

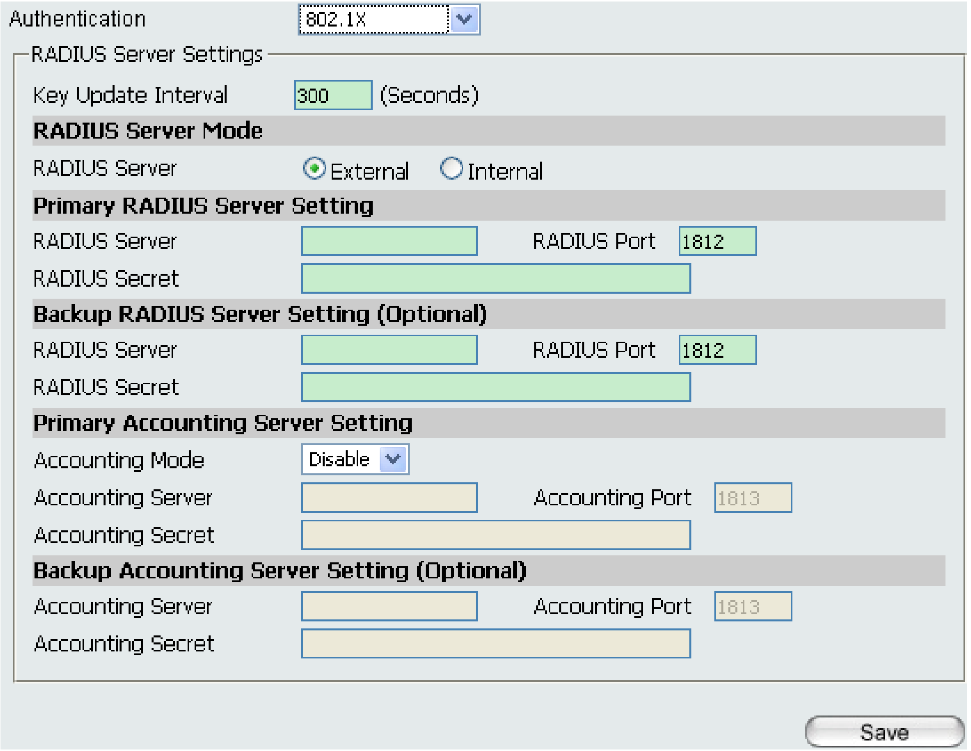
RADIUS Secret: Enter the RADIUS secret.

Accounting Mode: Select if you want to use a different server for accounting.

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

Accounting Port: Enter the Accounting port (**1813** is the default).

Accounting Secret: Enter the Accounting secret.

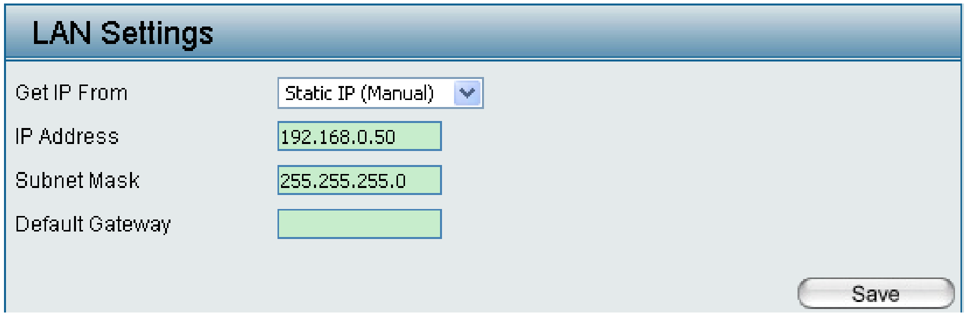


Authentication	802.1X		
RADIUS Server Settings			
Key Update Interval	300 (Seconds)		
RADIUS Server Mode			
RADIUS Server	● External ○ Internal		
Primary RADIUS Server Setting			
RADIUS Server		RADIUS Port	1812
RADIUS Secret			
Backup RADIUS Server Setting (Optional)			
RADIUS Server		RADIUS Port	1812
RADIUS Secret			
Primary Accounting Server Setting			
Accounting Mode	Disable		
Accounting Server		Accounting Port	1813
Accounting Secret			
Backup Accounting Server Setting (Optional)			
Accounting Server		Accounting Port	1813
Accounting Secret			

Note: *You can input the secondary RADIUS server and accounting server settings if you have a backup RADIUS and accounting server.*

LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-3690. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. After completing the desired LAN settings, click the **Save** button to let your changes take effect.



LAN Settings

Get IP From	Static IP (Manual)
IP Address	192.168.0.50
Subnet Mask	255.255.255.0
Default Gateway	

Get IP From: Choose **Static IP (Manual)** if you do not have a DHCP server on your network, or if you wish to assign a static IP address to the DAP-3690. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: The default IP address is **192.168.0.50**. Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Default Gateway: Enter the IP address of the gateway in your network. If there is a gateway in your network, please enter an IP address within the range of your network.

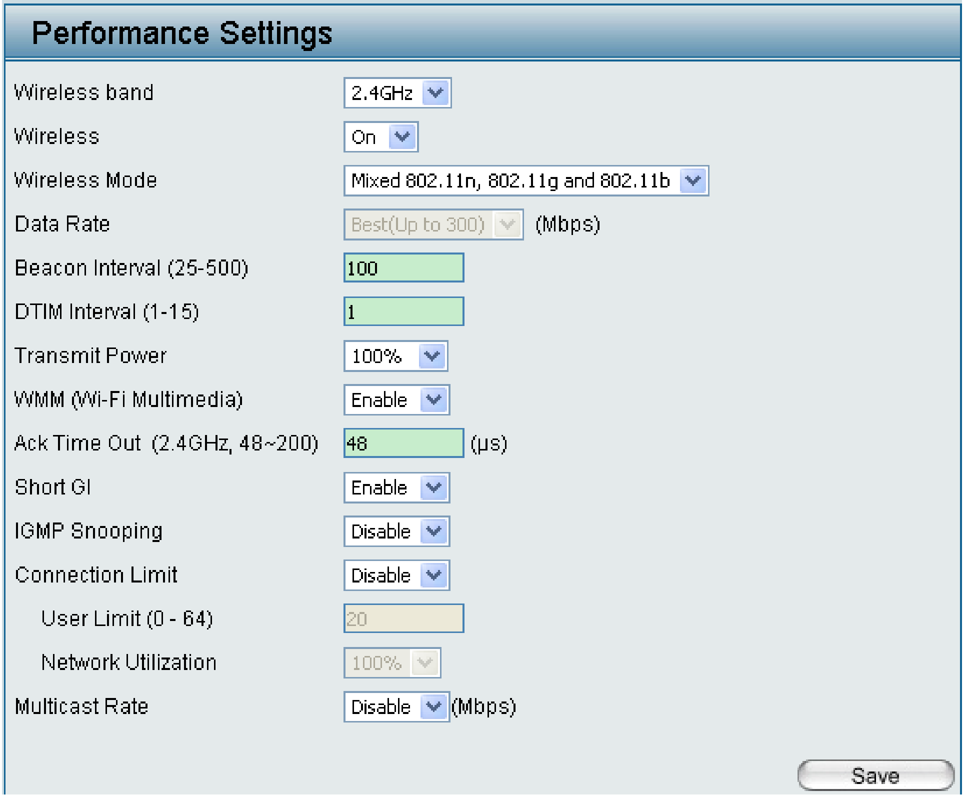
Advanced Settings

Performance

The Performance Settings window offers a number of user-controlled settings designed to optimize the performance of the DAP-3690. After completing the desired settings, click the Save button to let your changes take effect.

Wireless: Use the drop-down menu to turn the wireless function **On** or **Off**.

Wireless Mode: The different combination of clients that can be supported include **Mixed 802.11n, 802.11g and 802.11b**, **Mixed 802.11g and 802.11b**, and **802.11n Only** in the 2.4 GHz band and **Mixed 802.11n and 802.11a**, **802.11a only**, and **802.11n Only** in the 5 GHz band. Please note that when backwards compatibility is enabled for legacy (802.11a/g/b) clients, degradation of 802.11n wireless performance is expected.



Performance Settings

Wireless band	2.4GHz	
Wireless	On	
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b	
Data Rate	Best(Up to 300)	(Mbps)
Beacon Interval (25-500)	100	
DTIM Interval (1-15)	1	
Transmit Power	100%	
WMM (Wi-Fi Multimedia)	Enable	
Ack Time Out (2.4GHz, 48~200)	48	(µs)
Short GI	Enable	
IGMP Snooping	Disable	
Connection Limit	Disable	
User Limit (0 - 64)	20	
Network Utilization	100%	
Multicast Rate	Disable	(Mbps)

Data Rate*: Indicate the base transfer rate of wireless adapters on the wireless LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will step down the rate. This option is enabled in Mixed 802.11g and 802.11b mode (for 2.4 GHz) and 802.11a only mode (for 5 GHz). The choices available are **Best (Up to 54)**, **54**, **48**, **36**, **24**, **18**, **12**, **9**, and **6** for 5 GHz and **Best (Up to 54)**, **54**, **48**, **36**, **24**, **18**, **12**, **9**, **6**, **11**, **5.5**, **2** and **1** for 2.4 GHz.

Beacon Interval (25-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (**100**) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

DTIM Interval (1-15): Select a Delivery Traffic Indication Message setting between **1** and **15**. **1** is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Transmit Power: This setting determines the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area, then select 50% as the option. Use the drop-down menu to select **100%**, **50%**, **25%**, or **12.5%**.

WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.

Ack Time Out (2.4 GHZ, 48~200) or Ack Time Out (5 GHZ, 25~200): To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between **25** and **200** microseconds for 5 GHz or from **48** to **200** microseconds in the 2.4 GHz in the field provided.

Short GI: Select **Enable** or **Disable**. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.

IGMP Snooping: Select **Enable** or **Disable**. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.

Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-3690 will not allow clients to associate with the AP.

User Limit (0 - 64): Set the maximum amount of users that are allowed access (zero to 64 users).To use this feature, the Connection Limit above must be enabled. For most users, a limit of **10** is recommended. The default setting is **20**.

Network Utilization: Set the maximum utilization of this access point for service. The DAP-3690 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between **100%**, **80%**, **60%**, **40%**, **20%**, or **0%**. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

Multicast Rate: Adjust the multicast packet data rate here. The multicast rate is supported in **AP mode**, (2.4 GHZ and 5 GHZ) and **WDS with AP mode**, including Multi-SSIDs.

Multi-SSID

The device supports up to eight multiple Service Set Identifiers. You can set the Primary SSID in the **Basic > Wireless** section. The SSID's 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. When the information for the new SSID is finished, click the **Add** button. Click the **Save** button to let your changes take effect.

Enable Multi-SSID: Check to enable support for multiple SSIDs.

Enable Priority: Check to enable the priority feature.

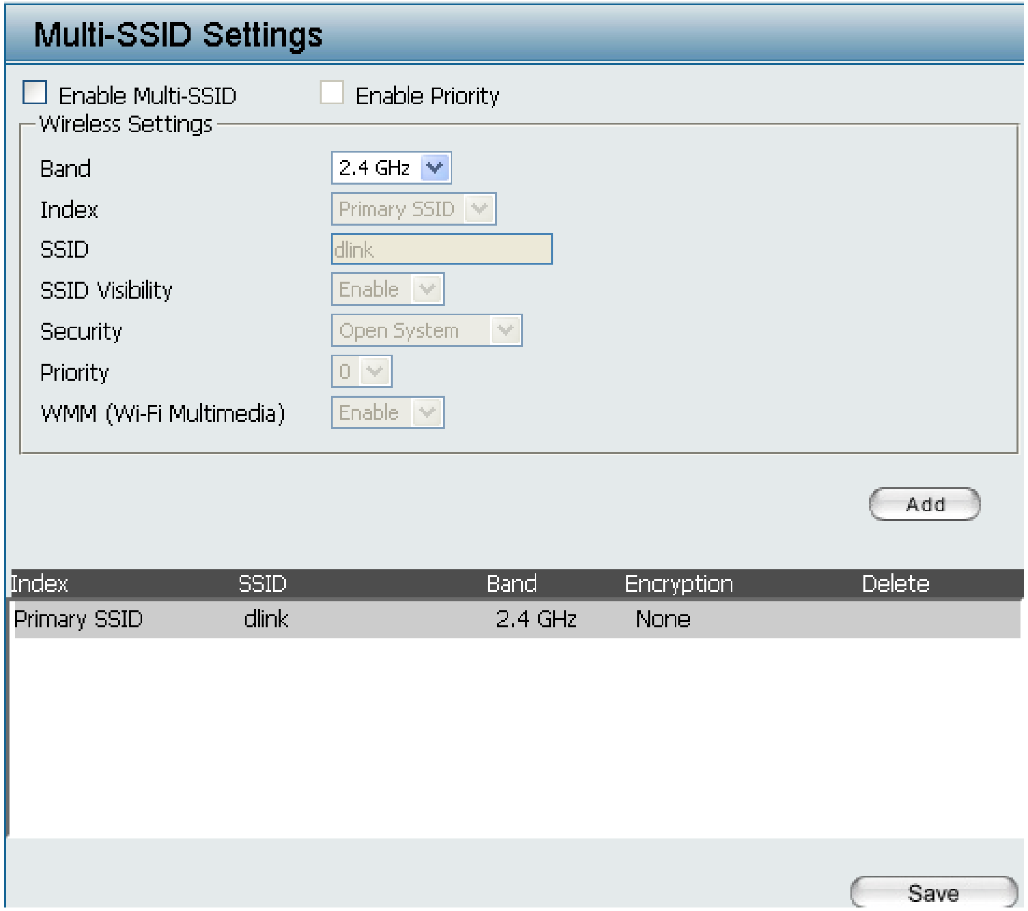
Band: This read-only value is the current band setting.

Index: You can select up to seven multi-SSIDs. With the Primary SSID, you have a total of eight multi-SSIDs.

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

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Security: The Multi-SSID security can be **Open System**, **WPA-Personal, WPA-Enterprise**, or **802.1X**. For a detailed description of the Open System parameters please go to page 23. For a detailed description of the WPA-Personal parameters please go to page 24. For a detailed description of the WPA-Enterprise parameters please go to page 25. For a detailed description of the 802.1X parameters please go to page 26.



Multi-SSID Settings

□ Enable Multi-SSID □ Enable Priority

Wireless Settings

Band	2.4 GHz
Index	Primary SSID
SSID	dlink
SSID Visibility	Enable
Security	Open System
Priority	0
WMM (Wi-Fi Multimedia)	Enable

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Priority: When the Enable Priority check box is checked at the top of this window, this drop-down menu is used to select a priority between **0** and **7**.

WMM (Wi-Fi Multimedia): Select **Enable** to provide basic Quality of Service features.

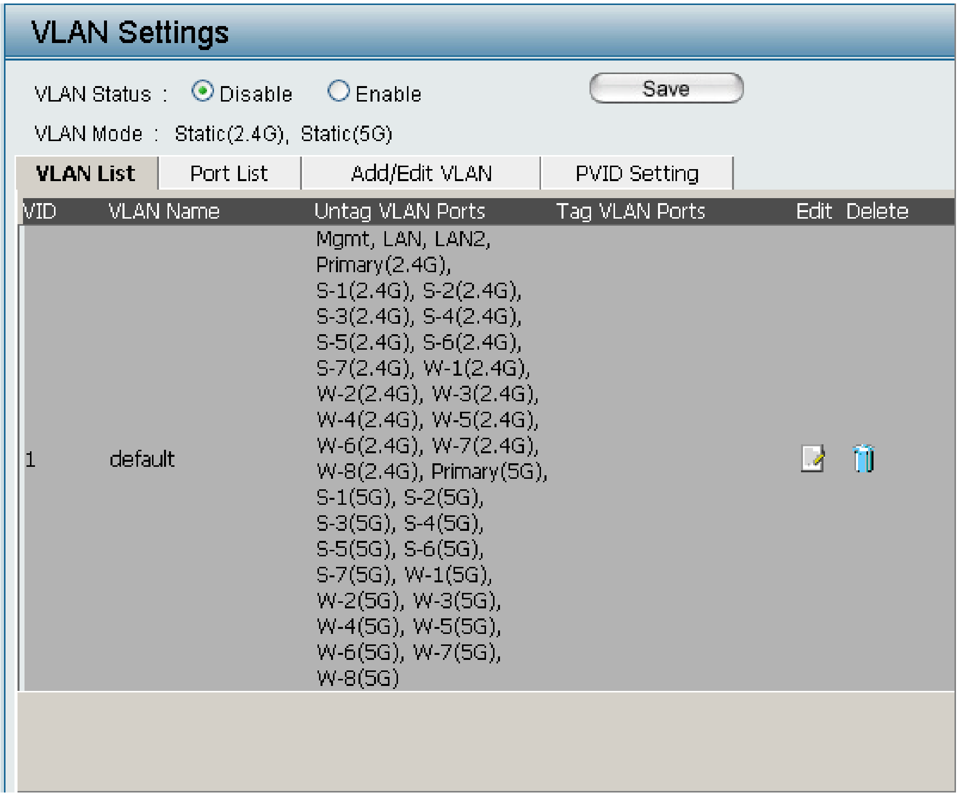
VLAN Settings > VLAN List

The DAP-3690 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-3690 without a VLAN tag will have a VLAN tag inserted with a PVID. Once you have made the desired settings, click the **Save** button to let your changes take effect.

The VLAN List tab displays the current VLANs.

VLAN Status: Use the radio button to toggle to Enable. Next, go to the **Add/Edit** VLAN tab to add or modify an item on the VLAN List tab.

VLAN Mode: The current VLAN mode is displayed.



VLAN Status : ● Disable ○ Enable

VLAN Mode : Static(2.4G), Static(5G)

VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	Edit	Delete
1	default	Mgmt, LAN, LAN2, Primary(2.4G), S-1(2.4G), S-2(2.4G), S-3(2.4G), S-4(2.4G), S-5(2.4G), S-6(2.4G), S-7(2.4G), W-1(2.4G), W-2(2.4G), W-3(2.4G), W-4(2.4G), W-5(2.4G), W-6(2.4G), W-7(2.4G), W-8(2.4G), Primary(5G), S-1(5G), S-2(5G), S-3(5G), S-4(5G), S-5(5G), S-6(5G), S-7(5G), W-1(5G), W-2(5G), W-3(5G), W-4(5G), W-5(5G), W-6(5G), W-7(5G), W-8(5G)		✎	🗑

Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard. Once you have made the desired settings, click the **Save** button to let your changes take effect.

VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.

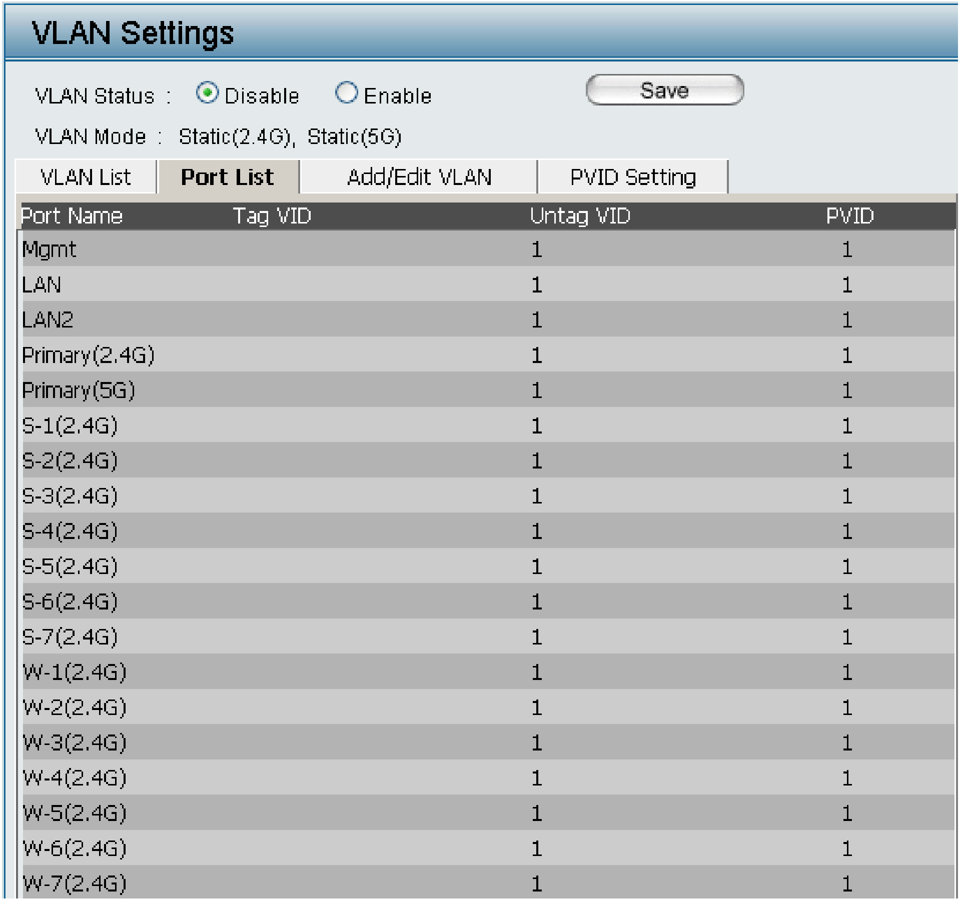
VLAN Mode: The current VLAN mode is displayed.

Port Name: The name of the port is displayed in this column.

Tag VID: The Tagged VID is displayed in this column.

Untag VID: The Untagged VID is displayed in this column.

PVID: The Port VLAN Identifier is displayed in this column.



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static(2.4G), Static(5G)

Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN		1	1
LAN2		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1
S-1(2.4G)		1	1
S-2(2.4G)		1	1
S-3(2.4G)		1	1
S-4(2.4G)		1	1
S-5(2.4G)		1	1
S-6(2.4G)		1	1
S-7(2.4G)		1	1
W-1(2.4G)		1	1
W-2(2.4G)		1	1
W-3(2.4G)		1	1
W-4(2.4G)		1	1
W-5(2.4G)		1	1
W-6(2.4G)		1	1
W-7(2.4G)		1	1

Add/Edit VLAN

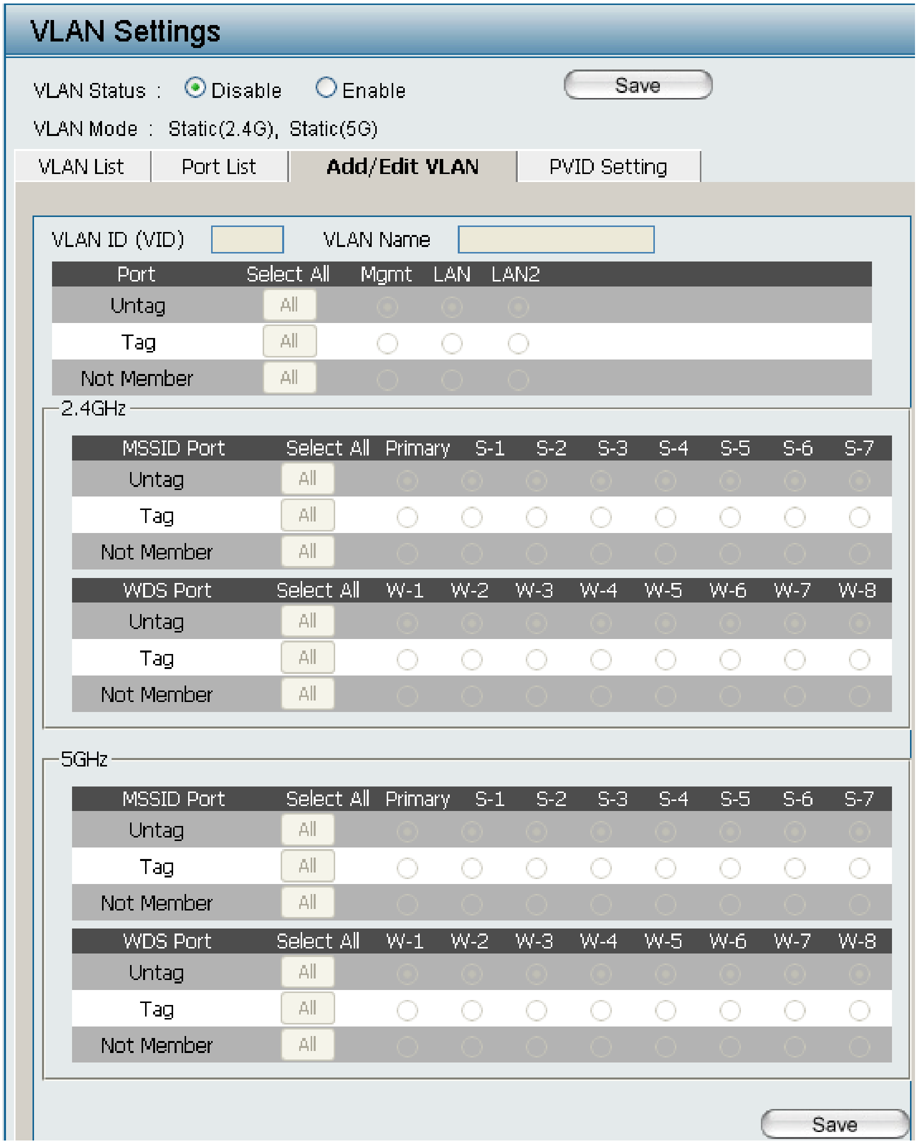
The Add/Edit VLAN tab is used to configure VLANs. Once you have made the desired settings, click the **Save** button to let your changes take effect.

VLAN Status: Use the radio button to toggle to Enable.

VLAN Mode: The current VLAN mode is displayed.

VLAN ID (VID): Provide a number between **1** and **4094** for the Internal VLAN.

VLAN Name: Enter the VLAN to add or modify.



VLAN Settings

VLAN Status : ● Disable ○ Enable Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN ID (VID) VLAN Name

Port	Select All	Mgmt	LAN	LAN2
Untag	All	●	●	●
Tag	All	○	○	○
Not Member	All	○	○	○

2.4GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

5GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

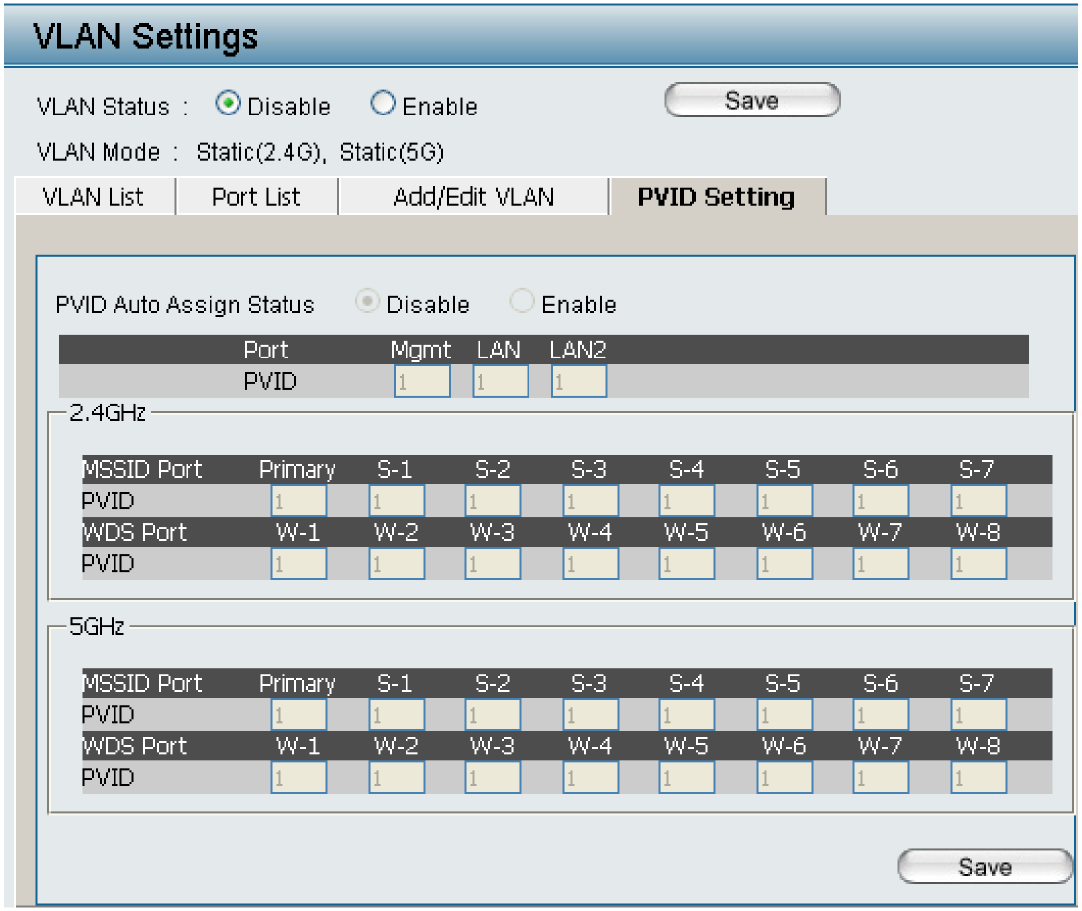
PVID Setting

The PVID Setting tab is used to enable/disable the Port VLAN Identifier Auto Assign Status as well as to configure various types of PVID settings. Once you have made the desired settings, click the **Save** button to let your changes take effect.

VLAN Status: Use the radio button to toggle to Enable.

VLAN Mode: The current VLAN mode is displayed.

PVID Auto Assign Status: Use the radio button to toggle PVID auto assign status to Enable.



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static(2.4G), Static(5G)

PVID Auto Assign Status ● Disable ○ Enable

Port	Mgmt	LAN	LAN2
PVID	1	1	1

2.4GHz

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
WDS Port	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
PVID	1	1	1	1	1	1	1	1

5GHz

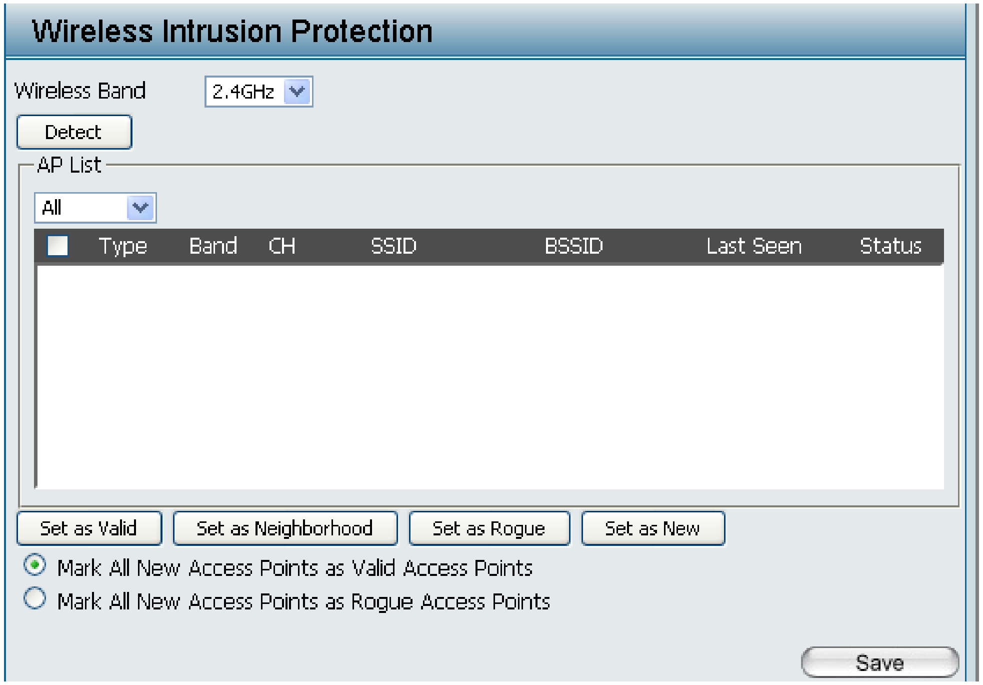
MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1
WDS Port	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
PVID	1	1	1	1	1	1	1	1

Intrusion

The Wireless Intrusion Protection window is used to set APs as All, Valid, Neighborhood, Rogue, and New. Once you have made the desired settings, click the **Save** button to let your changes take effect.

AP List: The choices include **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

Detect: Click this button to initiate a scan of the network.



Wireless Intrusion Protection

Wireless Band 2.4GHz

AP List

All

□	Type	Band	CH	SSID	BSSID	Last Seen	Status

● Mark All New Access Points as Valid Access Points

○ Mark All New Access Points as Rogue Access Points

Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. When the information for the new schedule rule is finished, click the **Add** button. To discard the new schedule rule settings, click the **Clear** button. Click the **Save** button to let your changes take effect.

Wireless Schedule: Use the drop-down menu to **Enable** the device's scheduling feature.

Name: Enter a name for the new scheduling rule in the field provided.

Index: Use the drop-down menu to select the desired SSID.

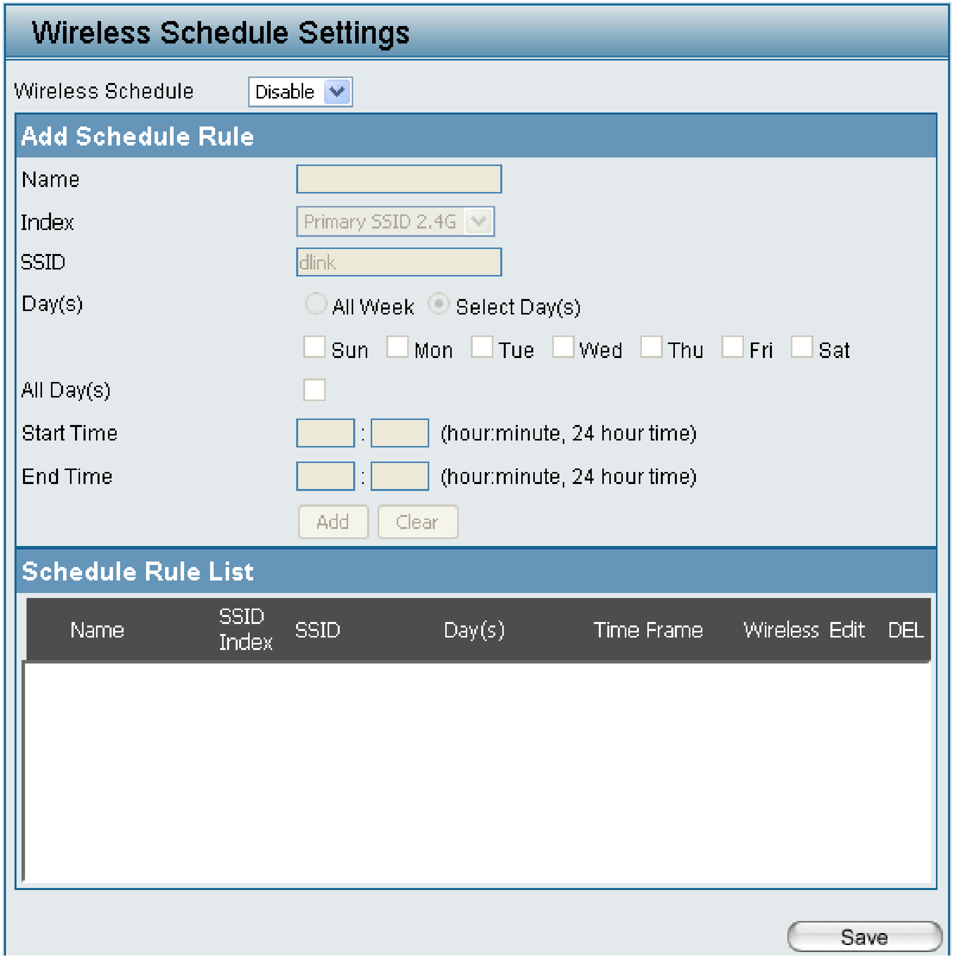
SSID: This read-only field indicates the current SSID in use. To create a new SSID, go to the Wireless Settings window (**Basic Settings > Wireless)**.

Day(s): Toggle the radio button between **All Week** and **Select Day(s)**. If the second option is selected, check the specific days you want the rule to be effective on.

All Days(s): Check this box to have settings apply 24 hours a day. If the settings are not to apply 24 hours a day, enter the desired starting and ending times in the next two fields.

Start Time: Enter the beginning hour and minute, using a 24-hour clock.

End Time: Enter the ending hour and minute, using a 24-hour clock.



Wireless Schedule Settings

Wireless Schedule: Disable

Add Schedule Rule

Name:

Index: Primary SSID 2.4G

SSID: dlink

Day(s): ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day(s): □

Start Time: : (hour:minute, 24 hour time)

End Time: : (hour:minute, 24 hour time)

Add Clear

Schedule Rule List

Name	SSID Index	SSID	Day(s)	Time Frame	Wireless	Edit	DEL

Save

AP Array

The AP Array window allows users to create a set of devices on a network that are organized into a single group in order to increase ease of management. Once a user has made the desired settings, click the **Save** button to let the changes take effect.

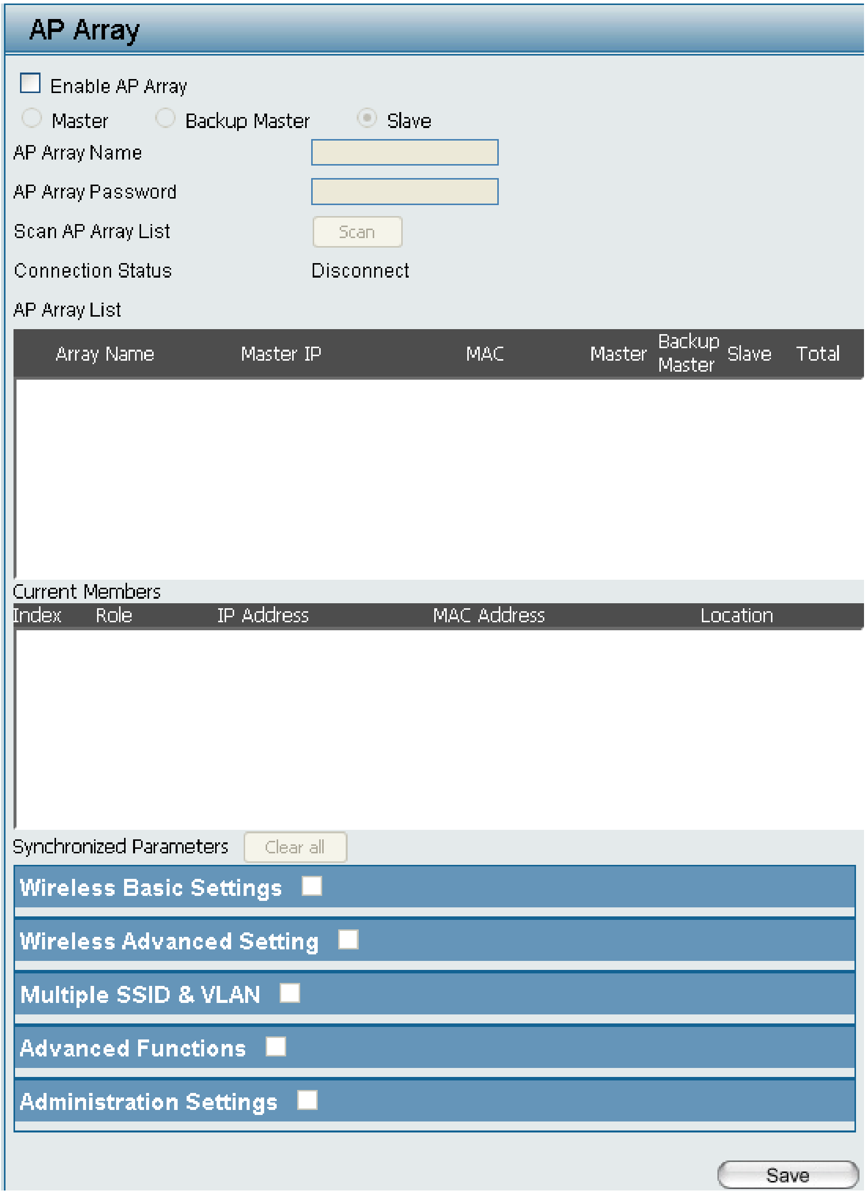
Enable AP Array: Check this box to enable the AP array function. The three modes that are available are Master, Backup Master, and Slave. APs in the same array will use the same configuration. The configuration will sync the Master AP to the Slave AP and the Backup Master AP when a Slave AP and a Backup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

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

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

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

Connection Status: This displays the status of the current AP array.



AP Array

□ Enable AP Array

○ Master ○ Backup Master ● Slave

AP Array Name

AP Array Password

Scan AP Array List [Scan]

Connection Status Disconnect

AP Array List

Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

Synchronized Parameters [Clear all]

Wireless Basic Settings □

Wireless Advanced Setting □

Multiple SSID & VLAN □

Advanced Functions □

Administration Settings □

[Save]

Web Redirection

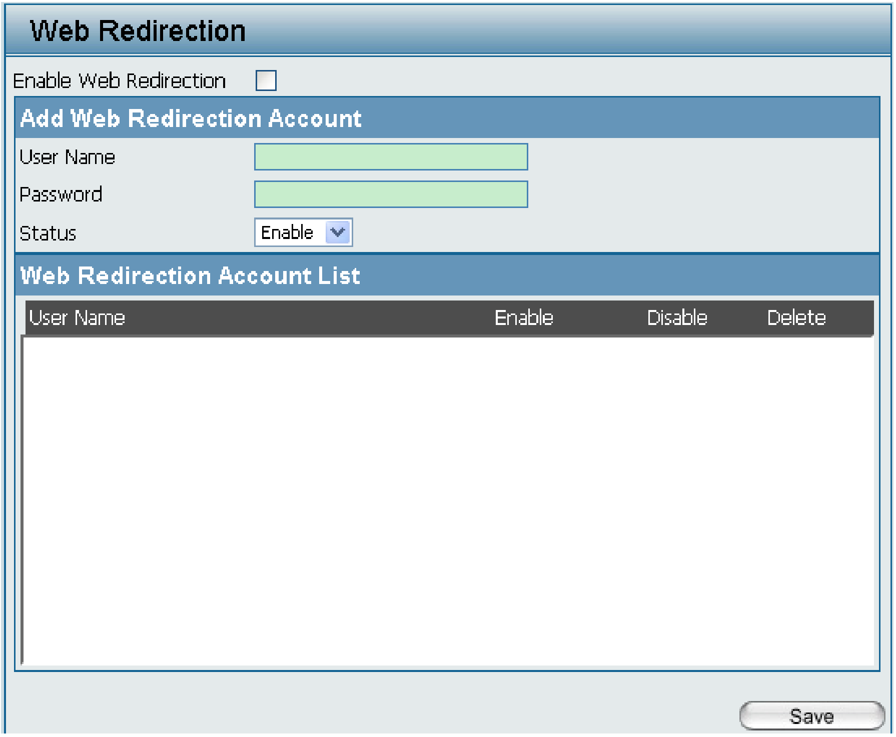
Web redirection allows you to be redirected to the appointed page, but only those who passed the authentication can access via AP.

Username: Enter a name to authenticate user access to the appointed page.

Password: Enter a password to authenticate user access to the appointed page.

Status: Toggle the drop-down menu between Enable and Disable.

Web Direction Account List: A list of accounts will be displayed here. Highlight a username to edit it or click the Delete icon to remove it from this list.



Web Redirection

Enable Web Redirection □

Add Web Redirection Account

User Name

Password

Status: Enable

Web Redirection Account List

User Name	Enable	Disable	Delete

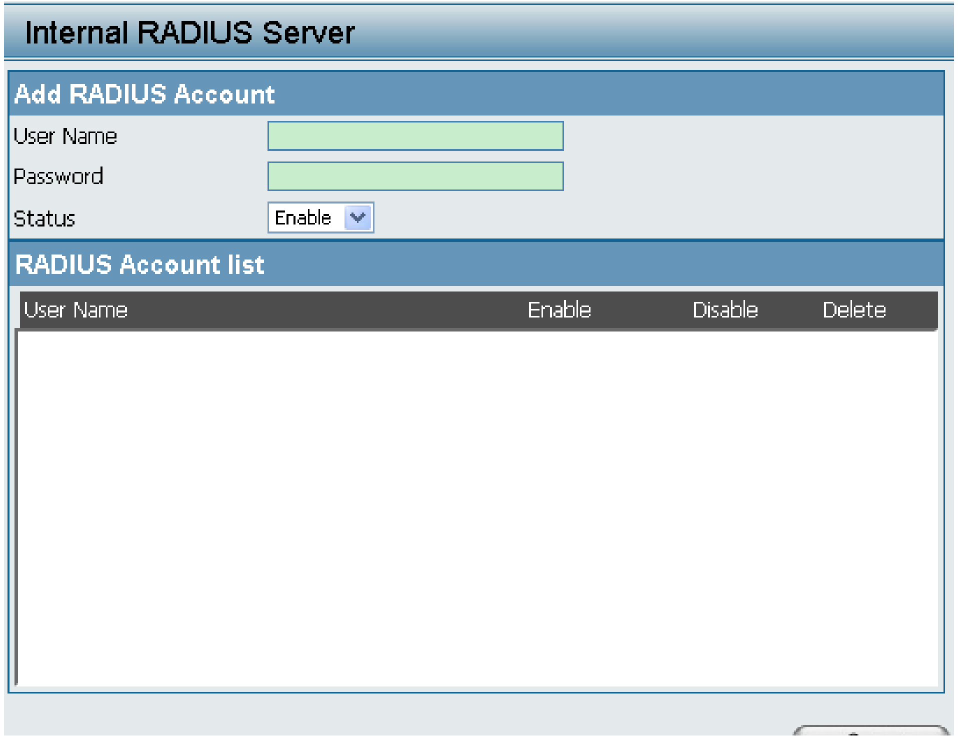
Internal RADIUS Server

The DAP-3690 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

User Name: Enter a name to authenticate user access to the internal RADIUS server.

Password: Enter a password to authenticate user access to the internal RADIUS server. The length of your password should be 8~64.

Status: Toggle the drop-down menu between **Enable** and **Disable**.



Internal RADIUS Server

Add RADIUS Account

User Name

Password

Status: Enable

RADIUS Account list

User Name	Enable	Disable	Delete

ARP Spoofing Prevention Settings

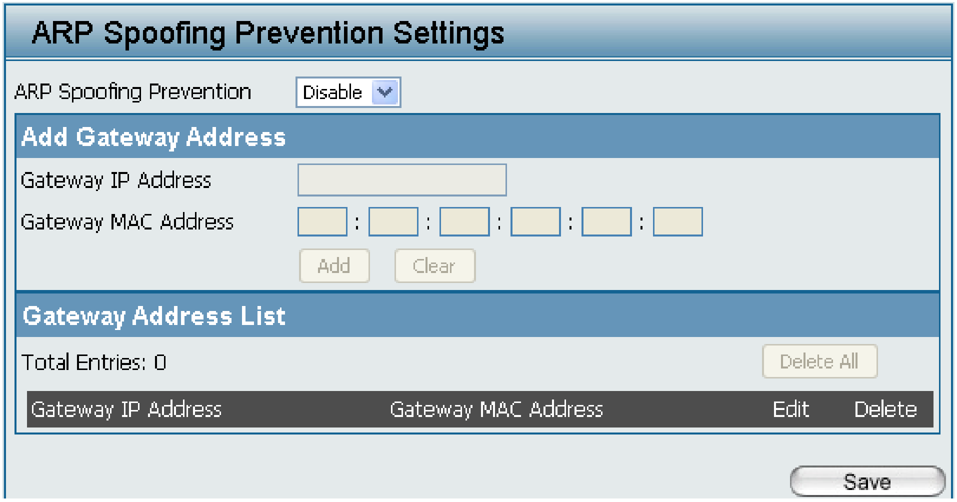
ARP Spoofing Prevention allows you to add IP/MAC address mapping for preventing ARP spoofing attack.

ARP Snooping Prevention: Check to enable ARP Snooping Prevention.

Gateway IP Address: Enter the IP address of your gateway.

Gateway MAC Address: Enter the MAC address of your gateway.

Gateway Address List: A list of gateway addresses will be displayed here. Highlight an IP address to edit it or click the Delete icon to remove it from this list.



ARP Spoofing Prevention Settings

ARP Spoofing Prevention: Disable

Add Gateway Address

Gateway IP Address

Gateway MAC Address : : : : :

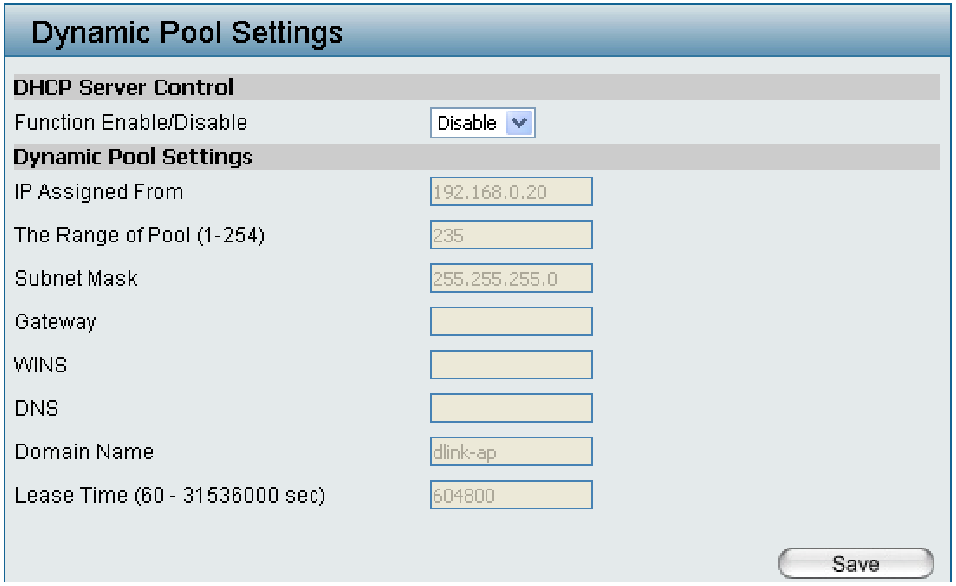
Gateway Address List

Total Entries: 0

Gateway IP Address	Gateway MAC Address	Edit	Delete

DHCP Server (Dynamic Pool Settings)

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. Once a user is finished, click the **Save** button to let the changes take effect.



Dynamic Pool Settings

DHCP Server Control

Function Enable/Disable: Disable

Dynamic Pool Settings

IP Assigned From: 192.168.0.20

The Range of Pool (1-254): 235

Subnet Mask: 255.255.255.0

Gateway:

WINS:

DNS:

Domain Name: dlink-ap

Lease Time (60 - 31536000 sec): 604800

Function Enable/ Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select **Enable** to allow the DAP-3690 to function as a DHCP server.

IP Assigned From: Input the first IP address available for assignment on your network.

The Range of Pool (1-254): Enter the number of IP addresses available for assignment. IP addresses are increments of the IP address specified in the "IP Assigned From" field.

SubMask: All devices in the network must have the same subnet mask to communicate. Enter the submask for the network here.

Gateway: Enter the IP address of the gateway on the network.

WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer that has a dynamically assigned IP address.

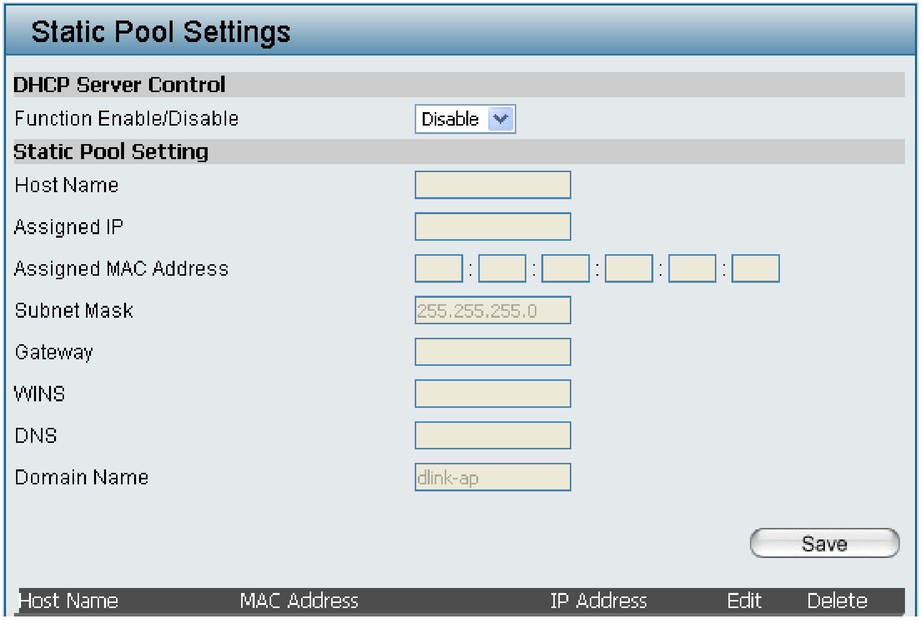
DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name: Enter the domain name of the network, if applicable. (An example of a domain name is: www.dlink.com.)

Lease Time (60-31536000 sec): The lease time is the period of time before the DHCP server will assign new IP addresses.

DHCP Server (Static Pool Setting)

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control.
Once a user is finished, click the **Save** button to let the changes take effect.



Static Pool Settings

DHCP Server Control

Function Enable/Disable	Disable

Static Pool Setting

Host Name	
Assigned IP	
Assigned MAC Address	: : : : :
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap

Host Name	MAC Address	IP Address	Edit	Delete

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select **Enable** to allow the DAP-3690 to function as a DHCP server.

Host Name: Enter the name of the host computer in this text box.

Assigned IP: Use the Static Pool Settings to assign the same IP address to a device every time you start up. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool. After you have assigned a static IP address to a device via its MAC address, click **Save**; the device will appear in the Assigned Static Pool at the bottom of the window. You can edit or delete the device in this list.

Assigned MAC Address: Enter the MAC address of the device requesting association here.

Subnet Mask: Define the subnet mask of the IP address specified in the "IP Assigned From" field.

Gateway: Specify the Gateway address for the wireless network.

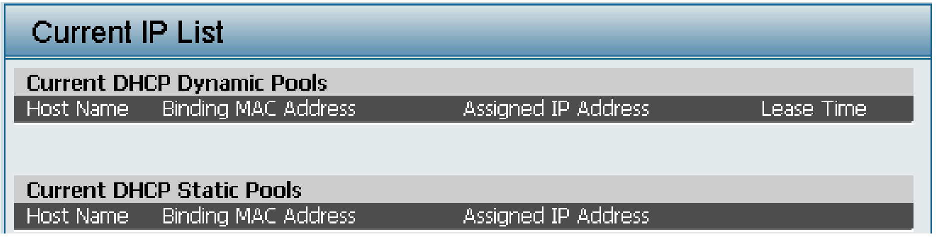
WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS: Enter the Domain Name System (DNS) server address for the wireless network. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name: Specify the domain name for the network.

DHCP Server (Current IP Mapping List)

This window displays information about the current assigned DHCP dynamic and static IP address pools. This information is available when you enable DHCP server on the AP and assign dynamic and static IP address pools.



Current IP List

Current DHCP Dynamic Pools

Host Name	Binding MAC Address	Assigned IP Address	Lease Time

Current DHCP Static Pools

Host Name	Binding MAC Address	Assigned IP Address

Current DHCP Dynamic Pools: These are IP address pools the DHCP server has assigned using the dynamic pool setting.

Binding MAC Address: The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

Assigned IP Address: The current corresponding DHCP-assigned IP address of the device.

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

Current DHCP Static Pools: These are the IP address pools of the DHCP server assigned through the static pool settings.

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

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

Filters (Wireless MAC ACL)

The DAP-3690 features a wireless MAC Access Control List filter. Once a user is finished with these settings, click the **Save** button to let the changes take effect.

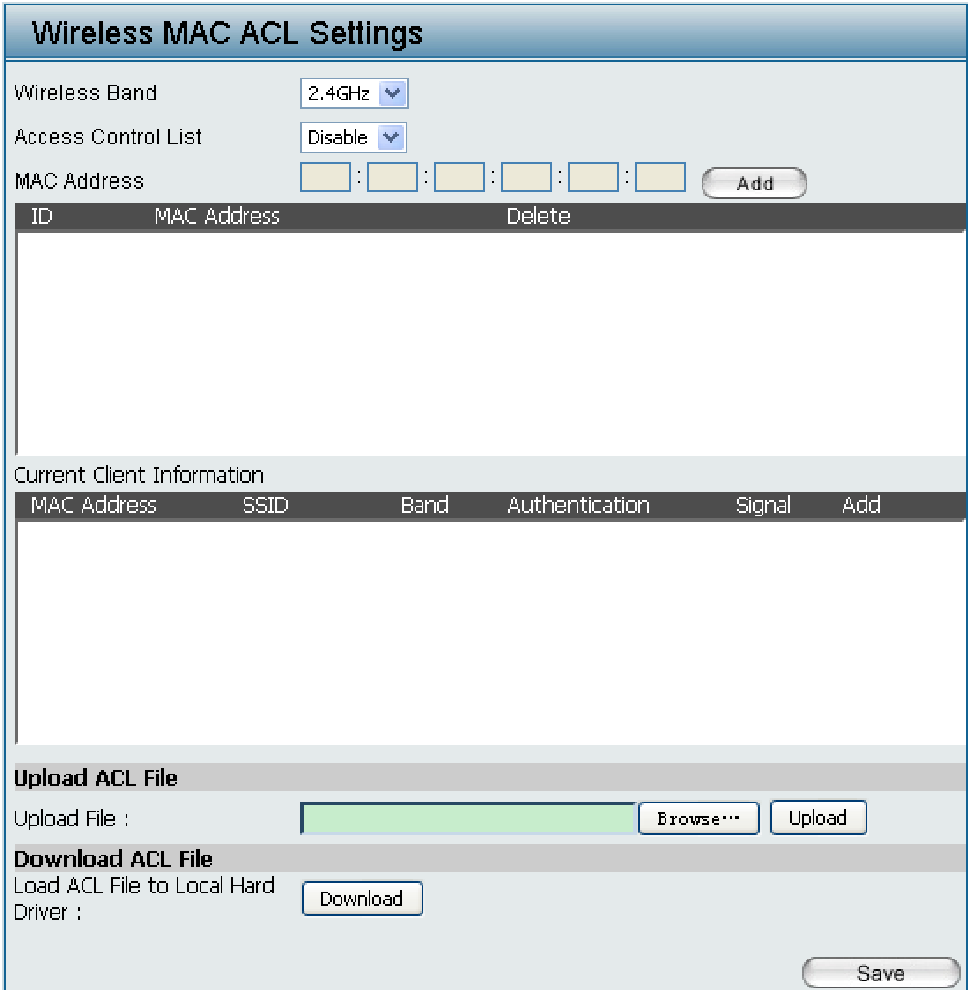
Wireless Band: Displays the current wireless band rate.

Access Control List: Select **Disable** to disable the filters function. Select **Accept** to accept only those devices with MAC addresses in the Access Control List. All other devices not on the list will be rejected. Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

MAC Address: Enter each MAC address that you wish to include in your filter list, and click **Add**.

MAC Address List: When a MAC address is entered, it appears in this list. Highlight a MAC address and click the Delete icon to remove it from this list.

Current Client Information: This table displays information about all the current connected stations.



Wireless MAC ACL Settings

Wireless Band: 2.4GHz

Access Control List: Disable

MAC Address: _ : _ : _ : _ : _ : _

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add

Upload ACL File

Upload File :

Download ACL File

Load ACL File to Local Hard Driver :

Filters (WLAN Partition)

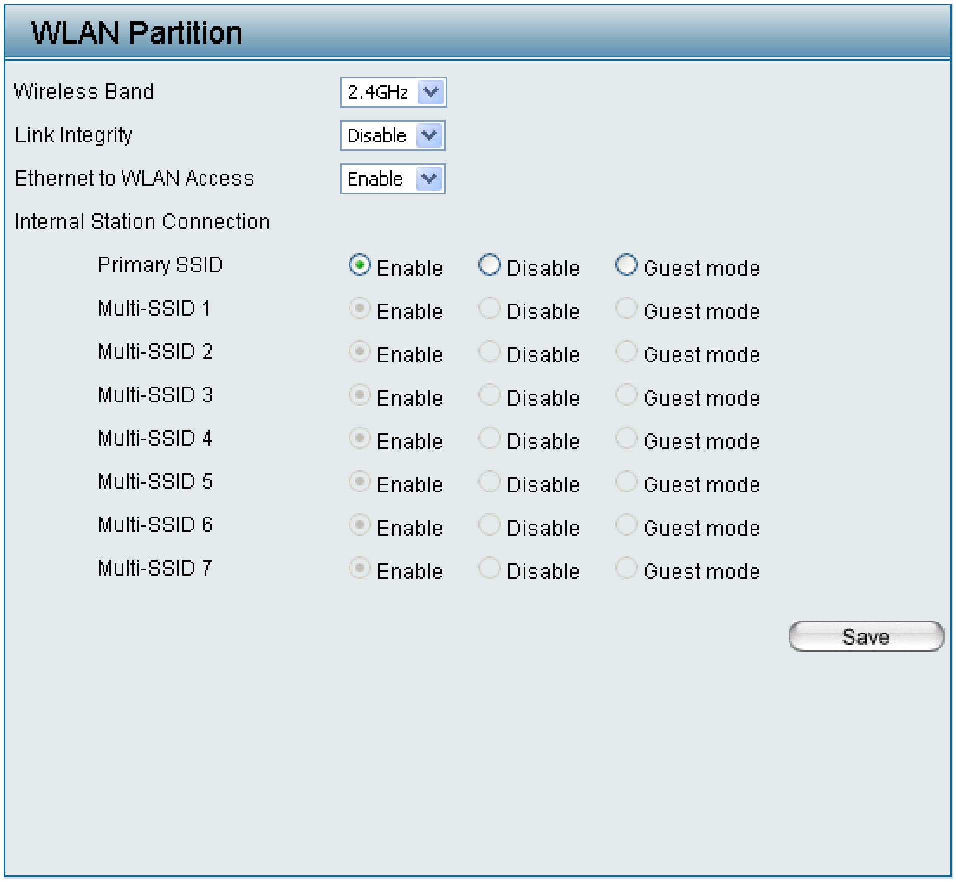
The DAP-3690 features a wireless partition. Once a user is finished with these settings, click the **Save** button to let the changes take effect.

Wireless Band: Displays the current wireless band.

Link Integrity: Select **Enable** or **Disable**. If the Ethernet connection between the LAN and the AP is disconnected, enabling this feature will cause the wireless segment associated with the AP to be disassociated from the AP.

Ethernet to WLAN Access: The default is **Enable**. When disabled, all data from the Ethernet to associated wireless devices will be blocked. Wireless devices can still send data to the Ethernet.

Internal Station Connection: The default value is **Enable**, which allows stations to intercommunicate by connecting to a target AP. When disabled, wireless stations cannot exchange data on the same Multi-SSID. In Guest mode, wireless stations cannot exchange data with any station on your network.



WLAN Partition

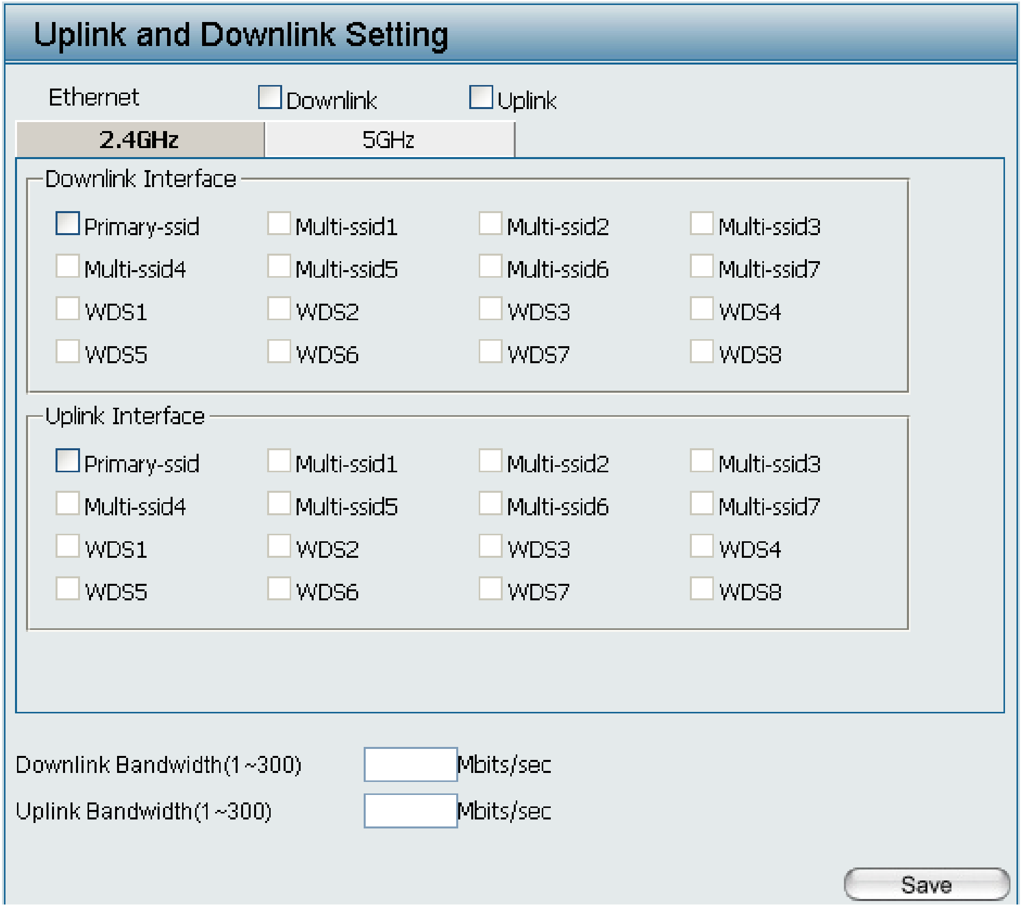
Wireless Band	2.4GHz		
Link Integrity	Disable		
Ethernet to WLAN Access	Enable		
Internal Station Connection			
Primary SSID	● Enable	○ Disable	○ Guest mode
Multi-SSID 1	● Enable	○ Disable	○ Guest mode
Multi-SSID 2	● Enable	○ Disable	○ Guest mode
Multi-SSID 3	● Enable	○ Disable	○ Guest mode
Multi-SSID 4	● Enable	○ Disable	○ Guest mode
Multi-SSID 5	● Enable	○ Disable	○ Guest mode
Multi-SSID 6	● Enable	○ Disable	○ Guest mode
Multi-SSID 7	● Enable	○ Disable	○ Guest mode

Traffic Control (Uplink/Downlink Setting)

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

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: The uplink bandwidth in Mbits per second.



Uplink and Downlink Setting

Ethernet □ Downlink □ Uplink

2.4GHz | 5GHz

Downlink Interface

□ Primary-ssid	□ Multi-ssid1	□ Multi-ssid2	□ Multi-ssid3
□ Multi-ssid4	□ Multi-ssid5	□ Multi-ssid6	□ Multi-ssid7
□ WDS1	□ WDS2	□ WDS3	□ WDS4
□ WDS5	□ WDS6	□ WDS7	□ WDS8

Uplink Interface

□ Primary-ssid	□ Multi-ssid1	□ Multi-ssid2	□ Multi-ssid3
□ Multi-ssid4	□ Multi-ssid5	□ Multi-ssid6	□ Multi-ssid7
□ WDS1	□ WDS2	□ WDS3	□ WDS4
□ WDS5	□ WDS6	□ WDS7	□ WDS8

Downlink Bandwidth(1~300) ____ Mbits/sec

Uplink Bandwidth(1~300) ____ Mbits/sec

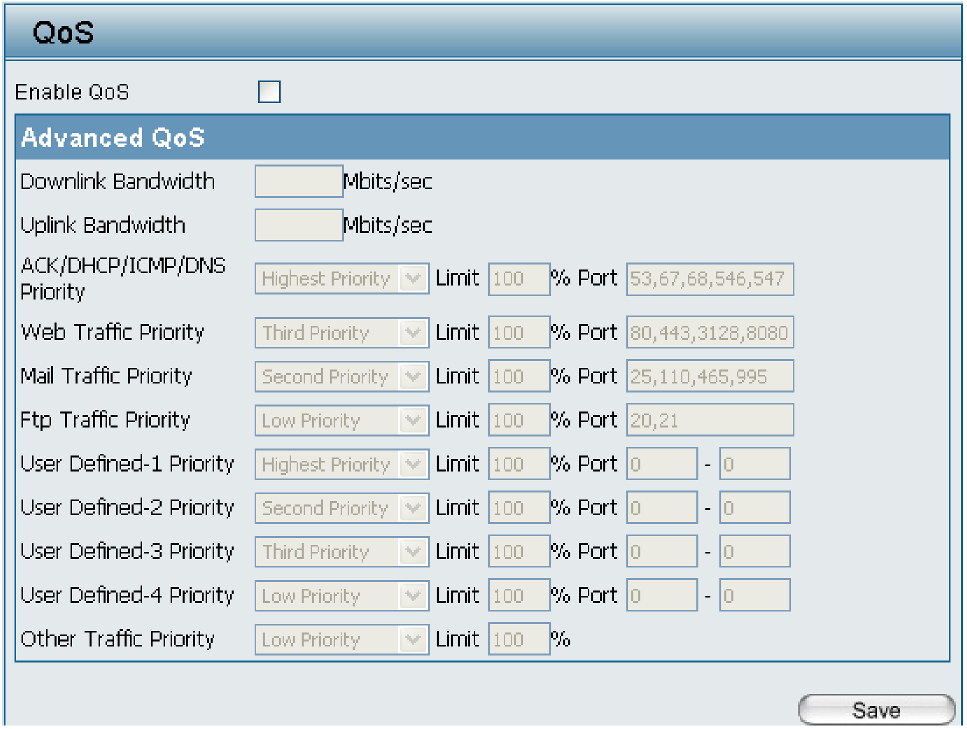
Traffic Control (QoS)

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-3690 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.

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

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

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



QoS

Enable QoS □

Advanced QoS

Downlink Bandwidth	Mbits/sec				
Uplink Bandwidth	Mbits/sec				
ACK/DHCP/ICMP/DNS Priority	Highest Priority	Limit	100 %	Port	53,67,68,546,547
Web Traffic Priority	Third Priority	Limit	100 %	Port	80,443,3128,8080
Mail Traffic Priority	Second Priority	Limit	100 %	Port	25,110,465,995
Ftp Traffic Priority	Low Priority	Limit	100 %	Port	20,21
User Defined-1 Priority	Highest Priority	Limit	100 %	Port	0 - 0
User Defined-2 Priority	Second Priority	Limit	100 %	Port	0 - 0
User Defined-3 Priority	Third Priority	Limit	100 %	Port	0 - 0
User Defined-4 Priority	Low Priority	Limit	100 %	Port	0 - 0
Other Traffic Priority	Low Priority	Limit	100 %		

Traffic Control (Traffic Manager)

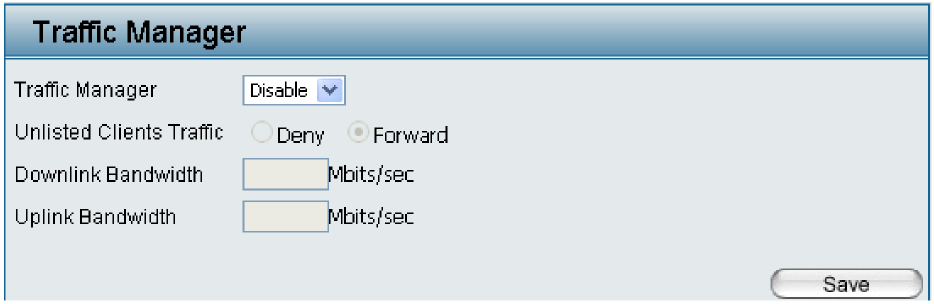
The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.

Traffic Manager: Use the drop-down menu to **Enable** the traffic manager feature.

Unlisted Client Traffic: Toggle the radio buttons between Deny and Forward to determine how to deal with unlisted client traffic.

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

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



Traffic Manager

Traffic Manager: Disable

Unlisted Clients Traffic: ○ Deny ● Forward

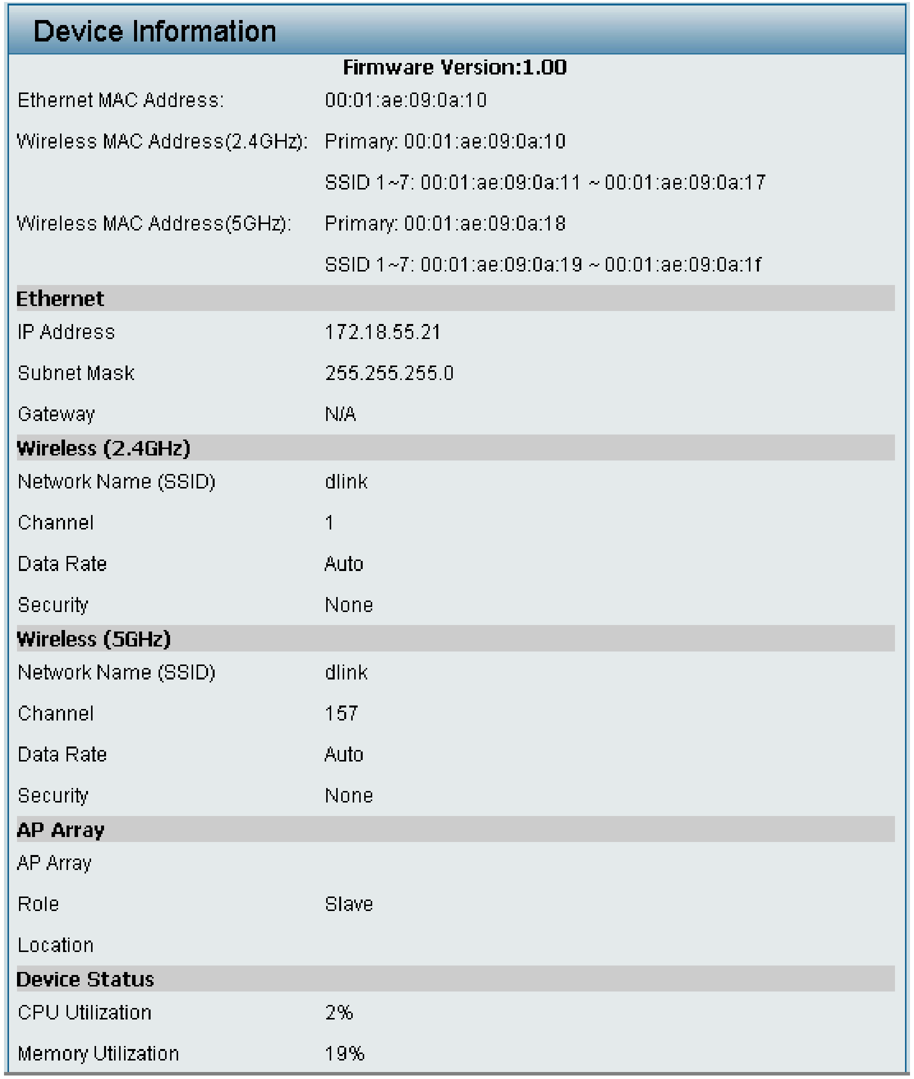
Downlink Bandwidth: Mbits/sec

Uplink Bandwidth: Mbits/sec

Home > Status

Device Information

Device Information: This read-only window displays the configuration settings of the DAP-3690, including the firmware version and the device's MAC address.



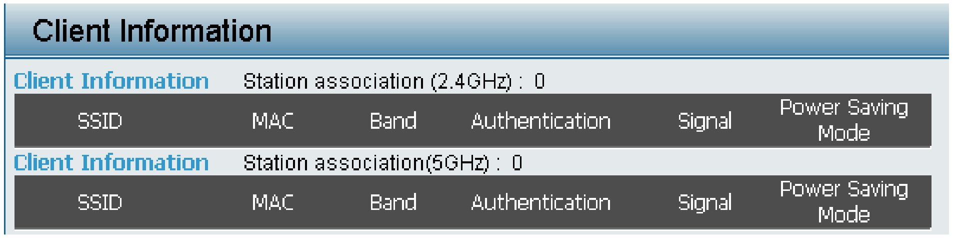
Device Information

Firmware Version:1.00

Ethernet MAC Address:	00:01:ae:09:0a:10
Wireless MAC Address(2.4GHz):	Primary: 00:01:ae:09:0a:10
	SSID 1~7: 00:01:ae:09:0a:11 ~ 00:01:ae:09:0a:17
Wireless MAC Address(5GHz):	Primary: 00:01:ae:09:0a:18
	SSID 1~7: 00:01:ae:09:0a:19 ~ 00:01:ae:09:0a:1f
Ethernet	
IP Address	172.18.55.21
Subnet Mask	255.255.255.0
Gateway	N/A
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	1
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	157
Data Rate	Auto
Security	None
AP Array	
AP Array	
Role	Slave
Location	
Device Status	
CPU Utilization	2%
Memory Utilization	19%

Client Information

Client Information: This window displays the wireless client information for clients currently connected to the DAP-3690.


Client Information

Client Information Station association (2.4GHz) : 0

SSID	MAC	Band	Authentication	Signal	Power Saving Mode

Client Information Station association(5GHz) : 0

SSID	MAC	Band	Authentication	Signal	Power Saving Mode

The following information is available for each client communicating with the DAP-3690.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Band: Displays the wireless band that the client is connected to.

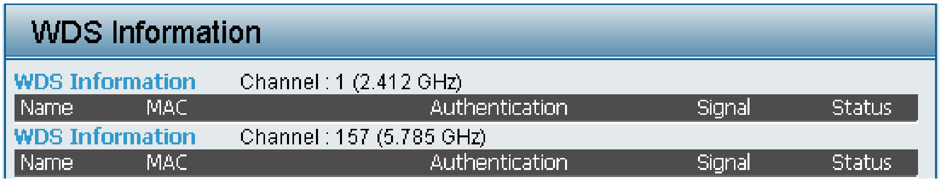
Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

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

WDS Information

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-3690.



WDS Information

WDS Information Channel : 1 (2.412 GHz)

Name	MAC	Authentication	Signal	Status

WDS Information Channel : 157 (5.785 GHz)

Name	MAC	Authentication	Signal	Status

The following information is available for each client communicating with the DAP-3690.

Name: Displays the name of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

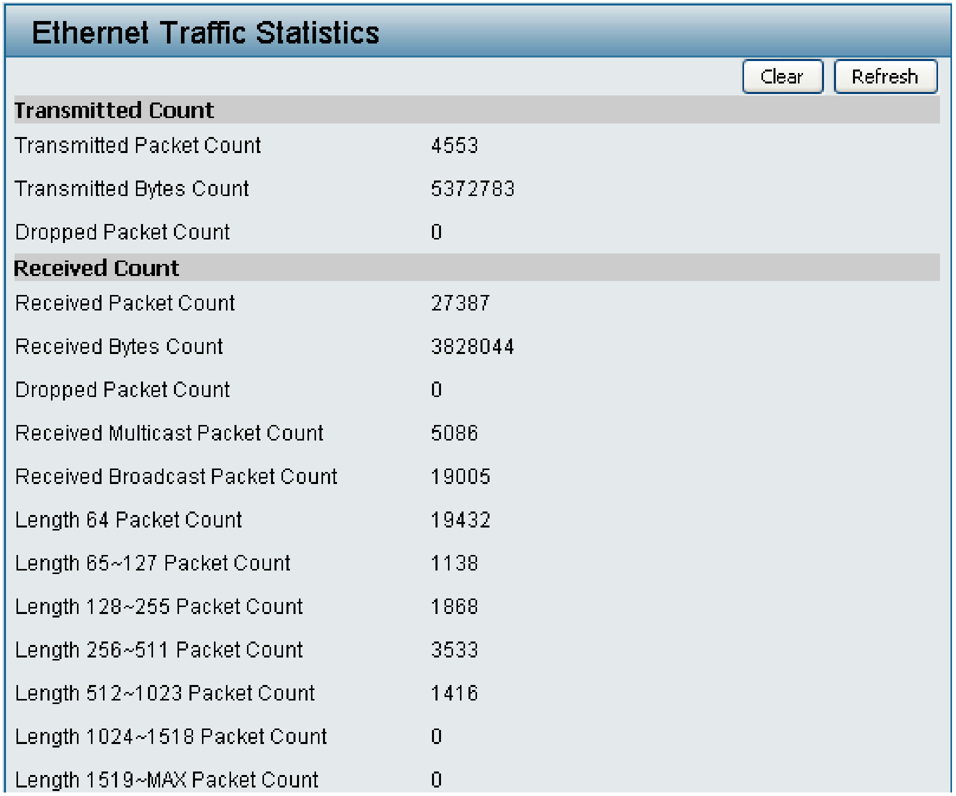
Signal: Displays the WDS link signal strength.

Status: Displays the status of the power saving feature.

Home > Status

Stats > Ethernet

Ethernet Traffic Statistics: This window displays transmitted and received count statistics for packets and bytes.

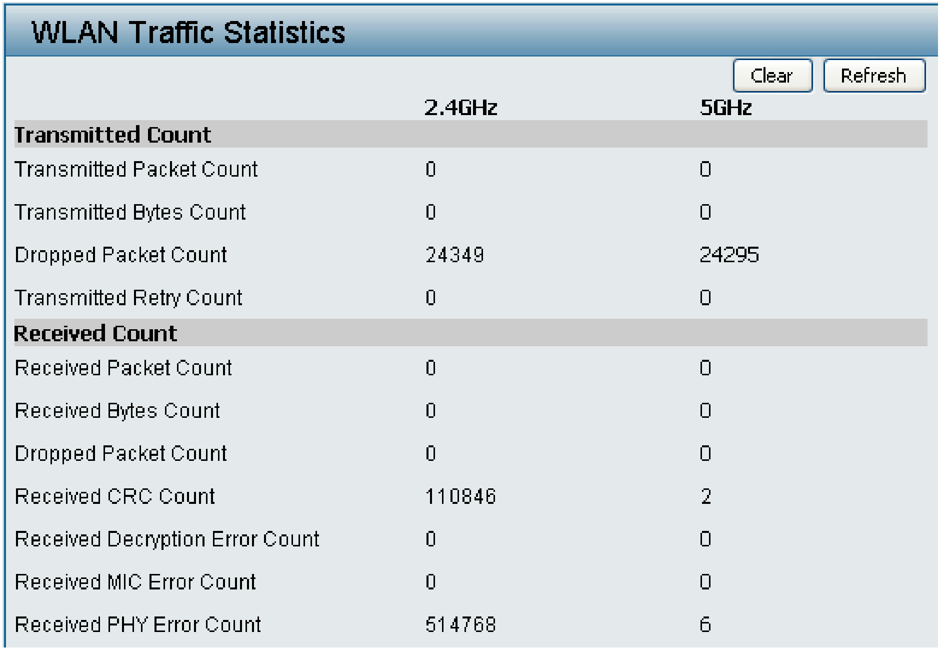


Ethernet Traffic Statistics

Transmitted Count	
Transmitted Packet Count	4553
Transmitted Bytes Count	5372783
Dropped Packet Count	0
Received Count	
Received Packet Count	27387
Received Bytes Count	3828044
Dropped Packet Count	0
Received Multicast Packet Count	5086
Received Broadcast Packet Count	19005
Length 64 Packet Count	19432
Length 65~127 Packet Count	1138
Length 128~255 Packet Count	1868
Length 256~511 Packet Count	3533
Length 512~1023 Packet Count	1416
Length 1024~1518 Packet Count	0
Length 1519~MAX Packet Count	0

Stats > WLAN

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

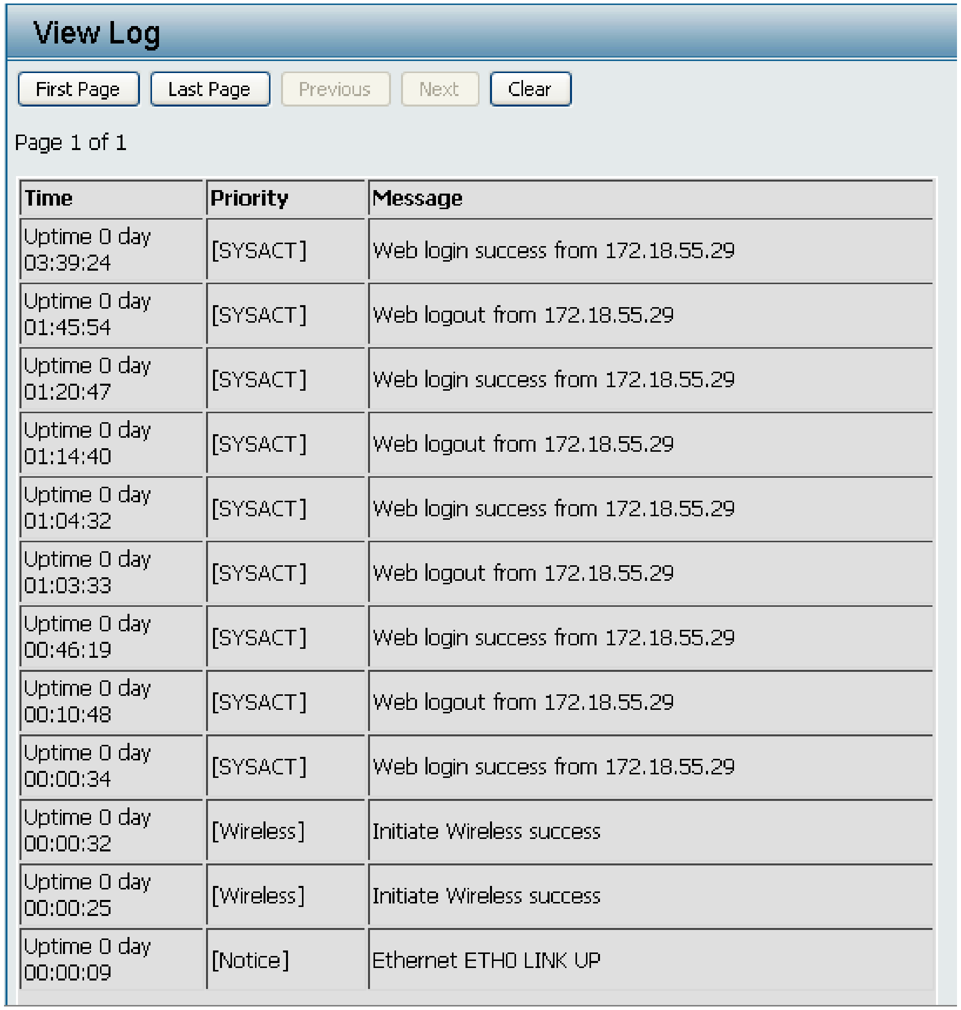


WLAN Traffic Statistics

	2.4GHz	5GHz
Transmitted Count		
Transmitted Packet Count	0	0
Transmitted Bytes Count	0	0
Dropped Packet Count	24349	24295
Transmitted Retry Count	0	0
Received Count		
Received Packet Count	0	0
Received Bytes Count	0	0
Dropped Packet Count	0	0
Received CRC Count	110846	2
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	514768	6

Log > View Log

View Log: The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.



Page 1 of 1

Time	Priority	Message
Uptime 0 day 03:39:24	[SYSACT]	Web login success from 172.18.55.29
Uptime 0 day 01:45:54	[SYSACT]	Web logout from 172.18.55.29
Uptime 0 day 01:20:47	[SYSACT]	Web login success from 172.18.55.29
Uptime 0 day 01:14:40	[SYSACT]	Web logout from 172.18.55.29
Uptime 0 day 01:04:32	[SYSACT]	Web login success from 172.18.55.29
Uptime 0 day 01:03:33	[SYSACT]	Web logout from 172.18.55.29
Uptime 0 day 00:46:19	[SYSACT]	Web login success from 172.18.55.29
Uptime 0 day 00:10:48	[SYSACT]	Web logout from 172.18.55.29
Uptime 0 day 00:00:34	[SYSACT]	Web login success from 172.18.55.29
Uptime 0 day 00:00:32	[Wireless]	Initiate Wireless success
Uptime 0 day 00:00:25	[Wireless]	Initiate Wireless success
Uptime 0 day 00:00:09	[Notice]	Ethernet ETH0 LINK UP

Log > Log Settings

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-3690 log to.

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

Email Notification: Check the box to enable Simple Mail Transfer Protocol.

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

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

Email Server Address: Enter the IP address of the e-mail/SMTP server.

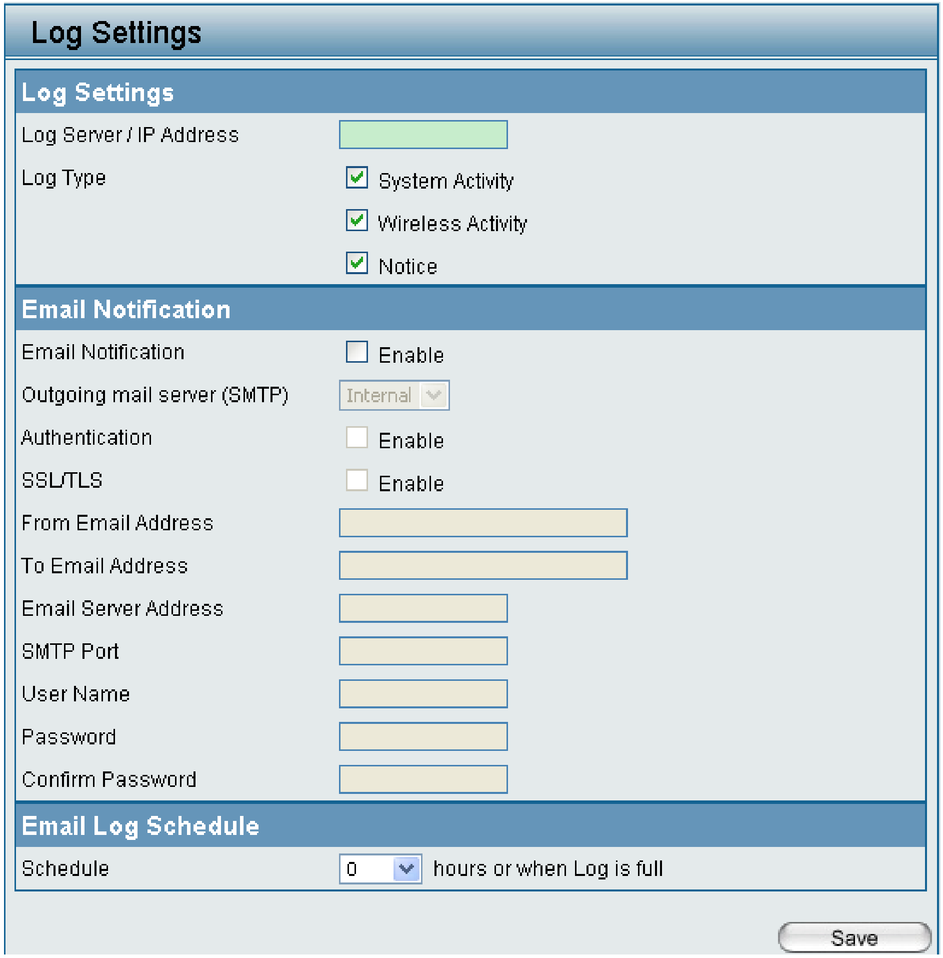
SMTP Port: Enter the desired SMTP port number. The default value is 25.

User Name: Enter a user name for the SMTP server.

Password: Enter a password for the SMTP server.

Confirm Password: Confirm the password for the SMTP server by retyping it.

Schedule: Use the drop-down menu to set the e-mail log schedule.

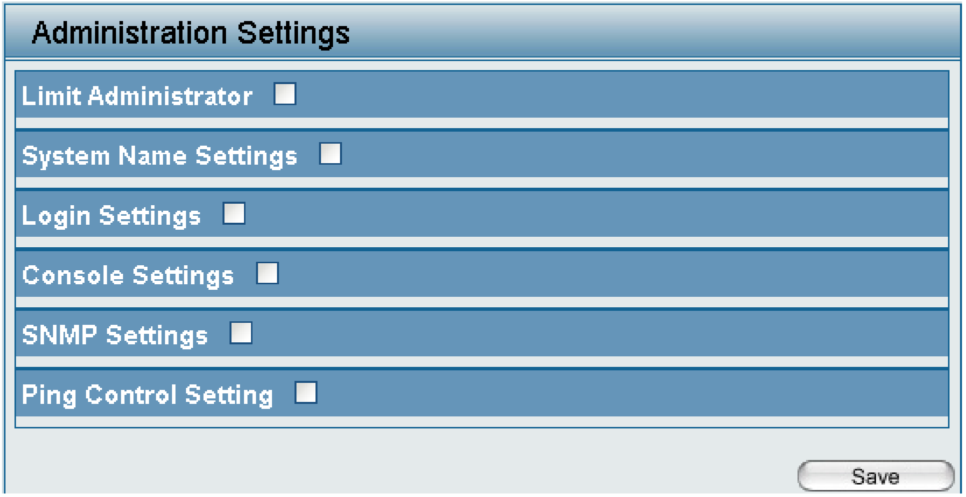


Log Settings

Log Settings	
Log Server / IP Address	
Log Type	☑ System Activity ☑ Wireless Activity ☑ Notice
Email Notification	
Email Notification	☐ Enable
Outgoing mail server (SMTP)	Internal
Authentication	☐ Enable
SSL/TLS	☐ Enable
From Email Address	
To Email Address	
Email Server Address	
SMTP Port	
User Name	
Password	
Confirm Password	
Email Log Schedule	
Schedule	0 hours or when Log is full

Maintenance > Administrator Settings

Check one or more of the six main categories to display the various hidden administrator parameters and settings displayed on the next six windows.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Limit Administrator

Confirm New Password: Confirm by re-entering your new password here.

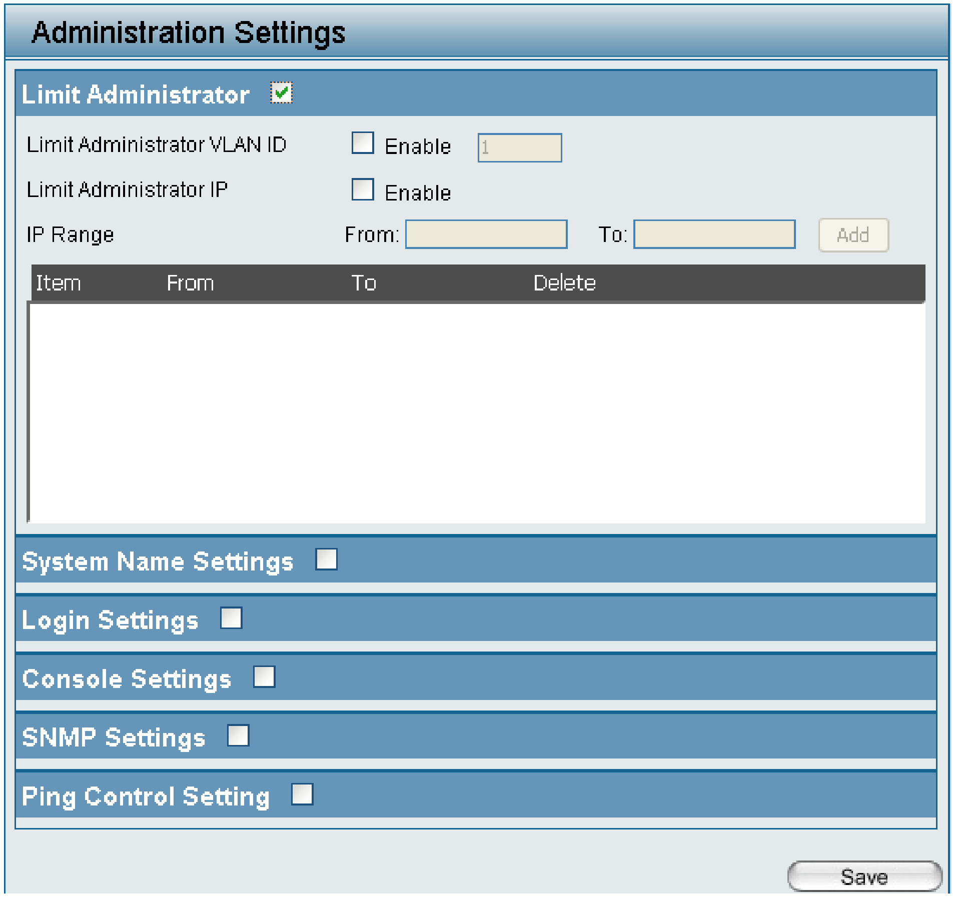
Each of the six main categories display various hidden administrator parameters and settings.

Limit Administrator

Limit Administrator VLAN ID: Check the box provided and the enter the specific VLAN ID that the administrator will be allowed to log in from.

Limit Administrator IP: Check to enable the Limit Administrator IP address.

IP Range: Enter the IP address range that the administrator will be allowed to log in from and then click the **Add** button.



Administration Settings

Limit Administrator ☑

Limit Administrator VLAN ID □ Enable 1

Limit Administrator IP □ Enable

IP Range From: To: Add

Item	From	To	Delete

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Save

System Name Settings

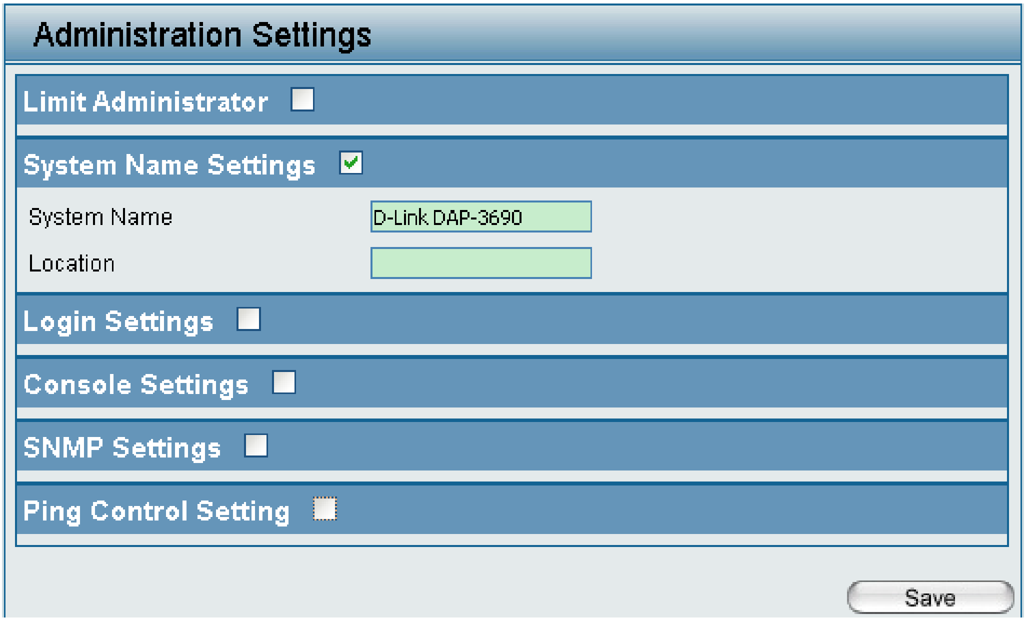
Confirm New Password: Confirm by re-entering your new password here.

Each of the six main categories display various hidden administrator parameters and settings.

System Name Settings

System Name: The name of the device. The default name is **D-Link DAP-3690**.

Location: The physical location of the device, e.g. "office".



Administration Settings

Limit Administrator □

System Name Settings ☑

System Name: D-Link DAP-3690

Location:

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Login Settings

Confirm New Password: Confirm by re-entering your new password here.

Each of the six main categories display various hidden administrator parameters and settings.

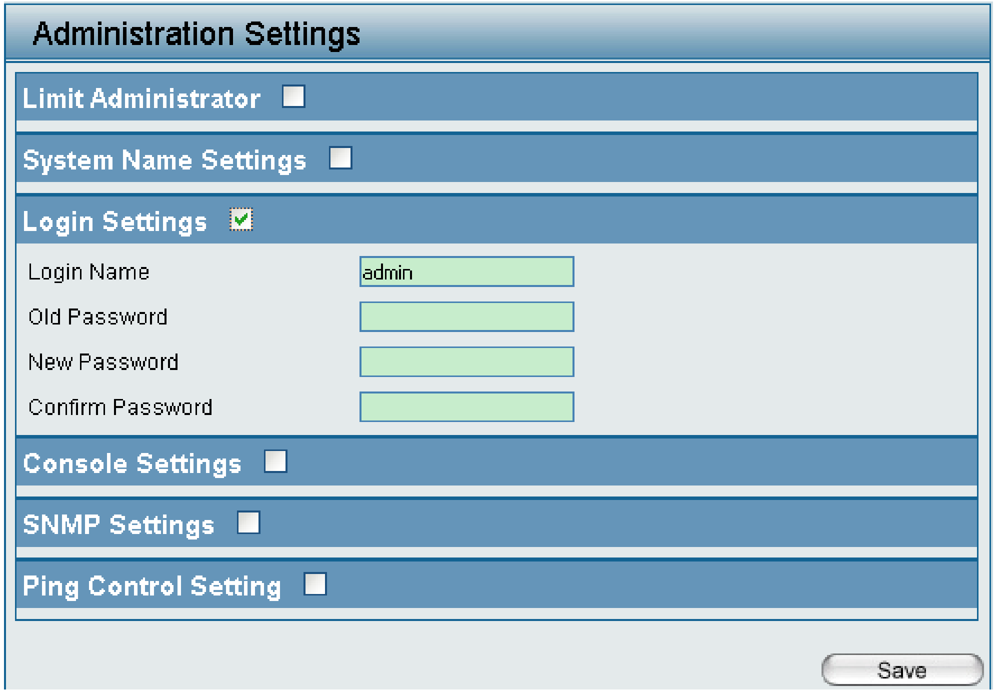
Login Settings

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. The password is case-sensitive. "A" is a different character than "a." The length should be between 0 and 12 characters.

Confirm Password: Enter the new password a second time for confirmation purposes.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings ☑

Login Name: admin

Old Password:

New Password:

Confirm Password:

Console Settings □

SNMP Settings □

Ping Control Setting □

Console Settings

Confirm New Password: Confirm by re-entering your new password here.

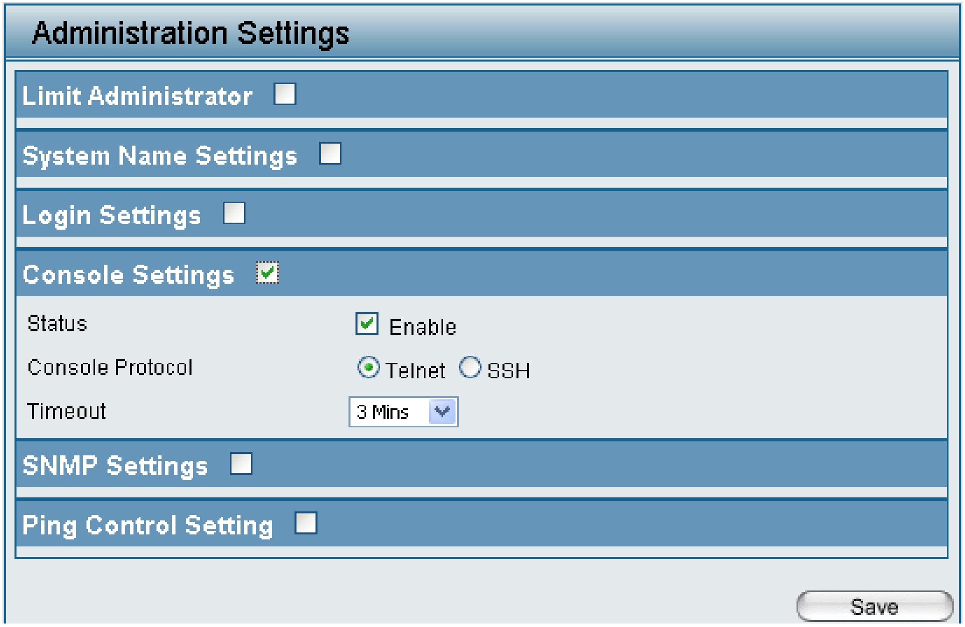
Each of the six main categories display various hidden administrator parameters and settings.

Console Settings

Status: Status is enabled by default. Uncheck the box to disable the console.

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

Timeout: Set to **1 Min**, **3 Mins**, **5 Mins**, **10 Mins**, **15 Mins** or **Never**.



Status ☑ Enable

Console Protocol ● Telnet ○ SSH

Timeout 3 Mins

SNMP Settings

Confirm New Password: Confirm by re-entering your new password here.

Each of the six main categories display various hidden administrator parameters and settings.

SNMP Settings

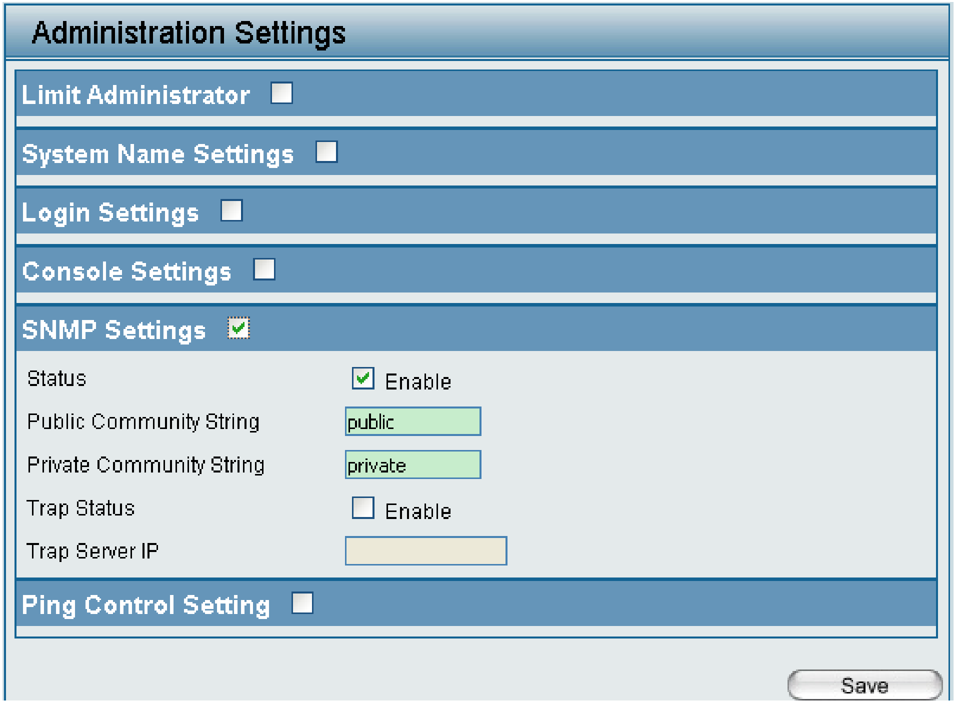
Status: Check the box to enable the SNMP functions. This is enabled by default.

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

Trap Status: Check the box to enable the trap status.

Trap Server IP: Enter the trap server IP address. This is the IP address of the SNMP manager to receive traps sent from the wireless access point.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings ☑

Status ☑ Enable

Public Community String public

Private Community String private

Trap Status □ Enable

Trap Server IP

Ping Control Setting □

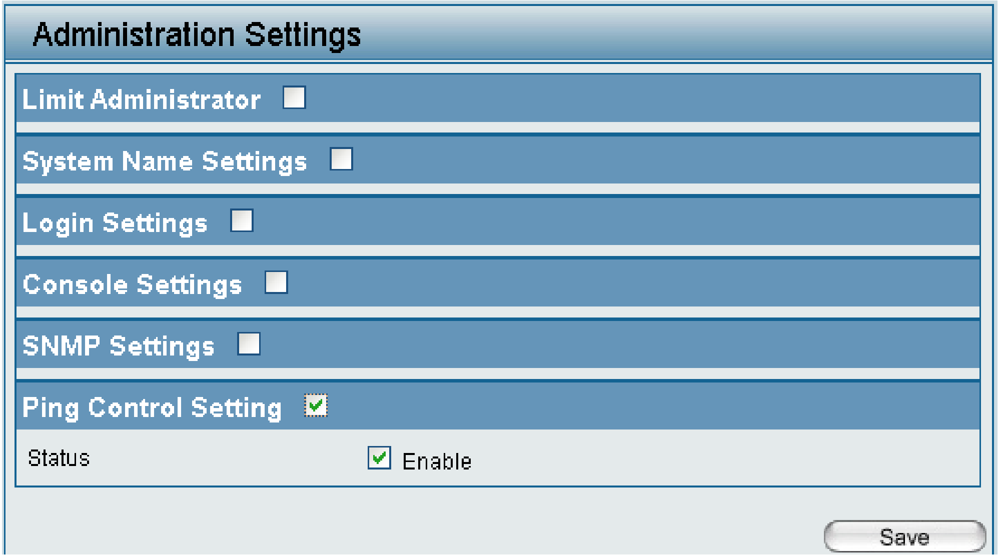
Ping Control Setting

Confirm New Password: Confirm by re-entering your new password here.

Each of the six main categories display various hidden administrator parameters and settings.

Ping Control Setting

Status: Check the box to enable Ping control. Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP echo response replies. The default is enabled.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

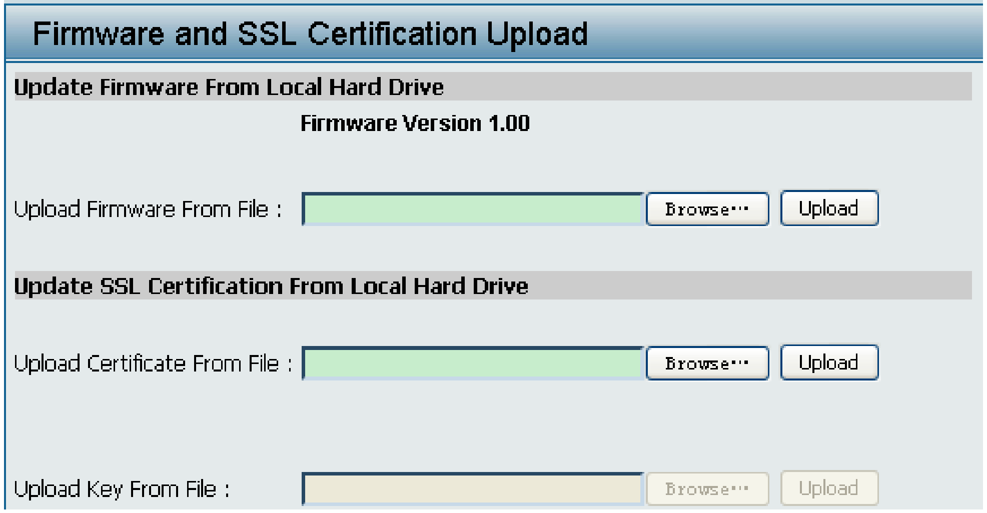
SNMP Settings □

Ping Control Setting ☑

Status ☑ Enable

Firmware and SSL Certification Upload

Upload Firmware From Local Hard Drive: The current firmware version is displayed above the file location field. After downloading the most recent version of firmware for the DAP-3690 from http://dlink.com//support to your local computer, use the **Browse** button to locate the firmware file on your computer. Click **Upload** to update the firmware version. Please don't turn the power off while upgrading.



Firmware and SSL Certification Upload

Update Firmware From Local Hard Drive

Firmware Version 1.00

Update SSL Certification From Local Hard Drive

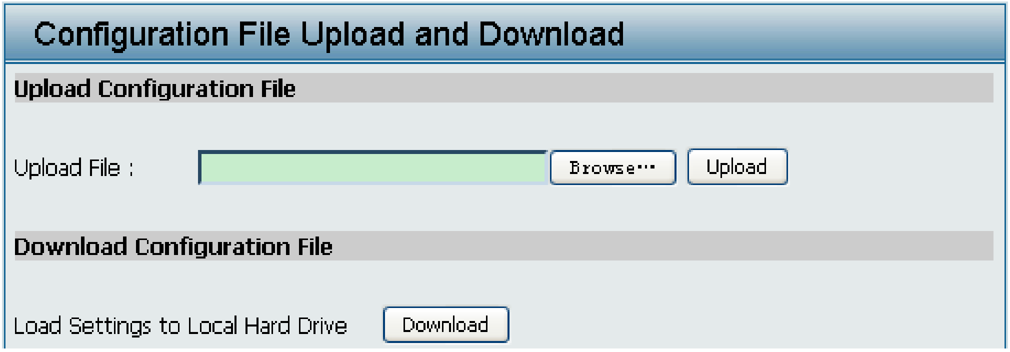
Language Pack Upgrade: Click **Browse** to locate the language pack upgrade on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-3690.

Upload SSL Certification From Local Hard Drive: Click **Browse** to locate the SSL Certification file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-3690.

Maintenance > Configuration File

Upload File: Click the **Browse** button to locate a previously saved configuration file on your local computer. After selecting the file, click **Upload** to apply the configuration settings to the DAP-3690.

Download Configuration File: Click **Download** to save the current DAP-3690 configuration to your local computer. Note that if you save one configuration with the administrator's password now, after resetting your DAP-3690, and then updating to this saved configuration file, the password will be gone.


Configuration File Upload and Download

Upload Configuration File

Upload File :

Download Configuration File

Load Settings to Local Hard Drive

Maintenance > Time and Date

Current Time: Displays the current time and date settings.

Time Zone: Use the drop-down menu to select your correct Time Zone.

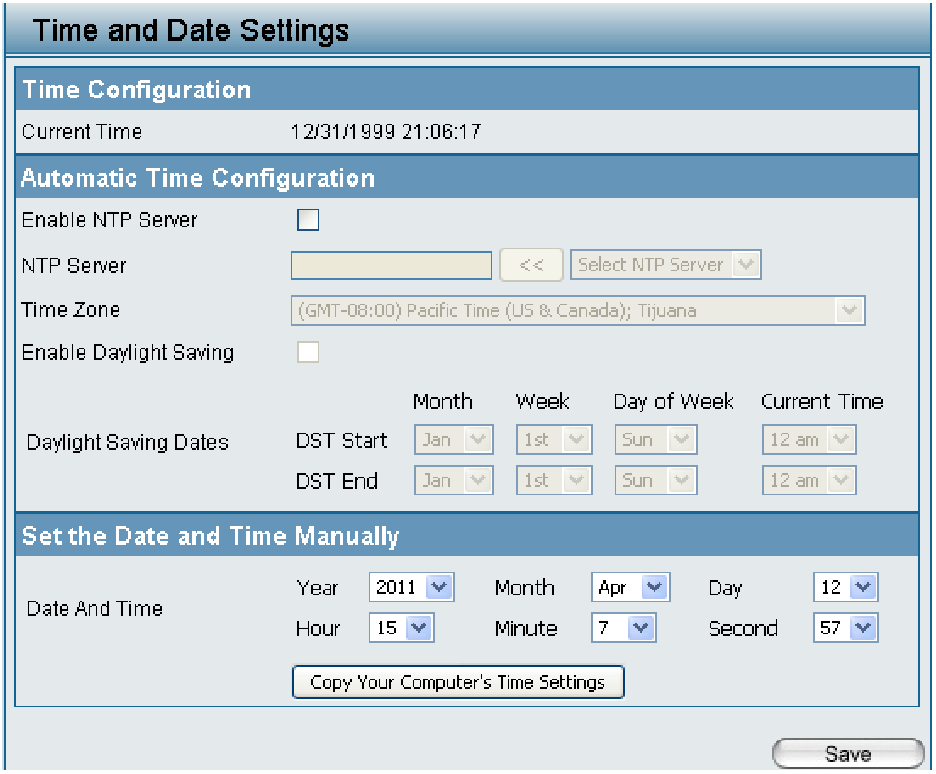
Enable NTP Server: Check to enable the AP to get system time from an NTP server.

NTP Server: Enter the NTP server IP address.

Enable Daylight Saving: Check the box to Enable Daylight Saving Time.

Daylight Saving Dates: Use the drop-down menu to select the correct Daylight Saving offset.

Set the Date and Time Manually: A user can either manually set the time for the AP here, or click the **Copy Your Computer's Time Settings** button to copy the time from the computer in use (Make sure that the computer's time is set correctly).



Time and Date Settings

Time Configuration

Current Time 12/31/1999 21:06:17

Automatic Time Configuration

Enable NTP Server □

NTP Server [ ] << Select NTP Server

Time Zone (GMT-08:00) Pacific Time (US & Canada); Tijuana

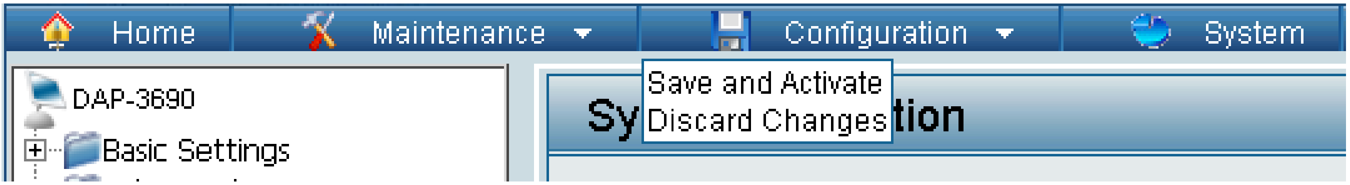
Enable Daylight Saving □

Daylight Saving Dates		Month	Week	Day of Week	Current Time
	DST Start	Jan	1st	Sun	12 am
	DST End	Jan	1st	Sun	12 am

Set the Date and Time Manually

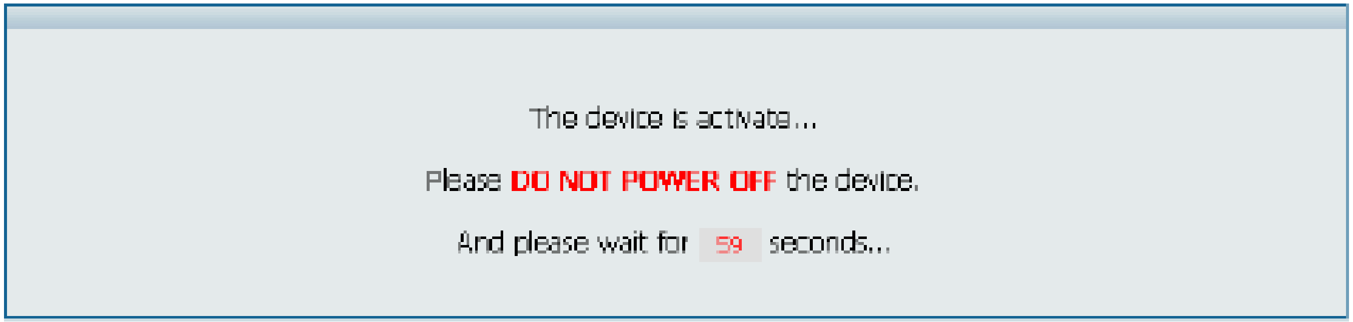
Date And Time	Year	2011	Month	Apr	Day	12
	Hour	15	Minute	7	Second	57

Configuration > Save and Activate



The drop-down Configuration menu allows users to save the current changes and reboot the DAP-3690 by clicking "Save and Activate".

If the "Save and Activate" option is selected, the following window will appear to display how many seconds remain before the save settings and reboot system action is completed.

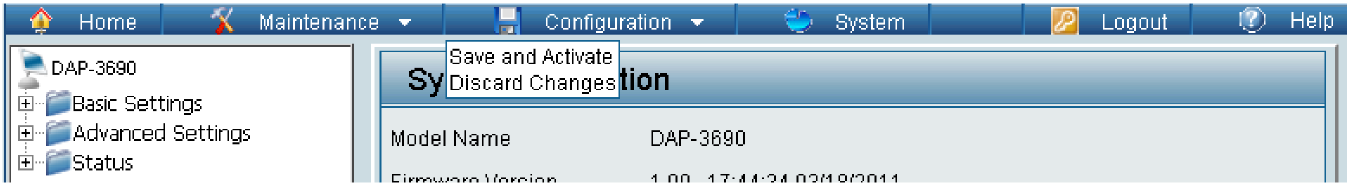


The device is activate...

Please DO NOT POWER OFF the device.

And please wait for 59 seconds...

Configuration > Discard Changes



Model Name DAP-3690

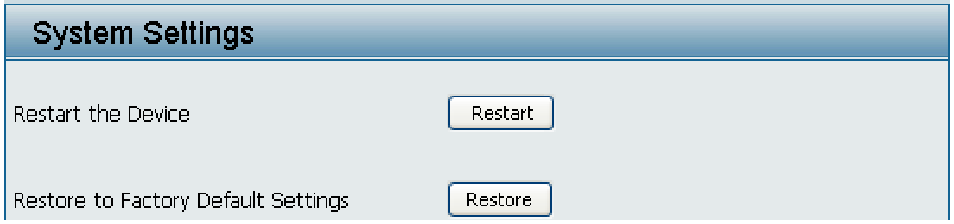
The drop-down Configuration menu allows users to drop the latest changes by clicking "Discard Changes."

System > System Settings

Restart the Device: Click **Restart** to restart the DAP-3690.

Restore to Factory Default Settings: Click **Restore** to restore the DAP-3690 back to factory default settings.

Clear Language Pack: Click **Clear** to remove the DAP-3690 language pack.

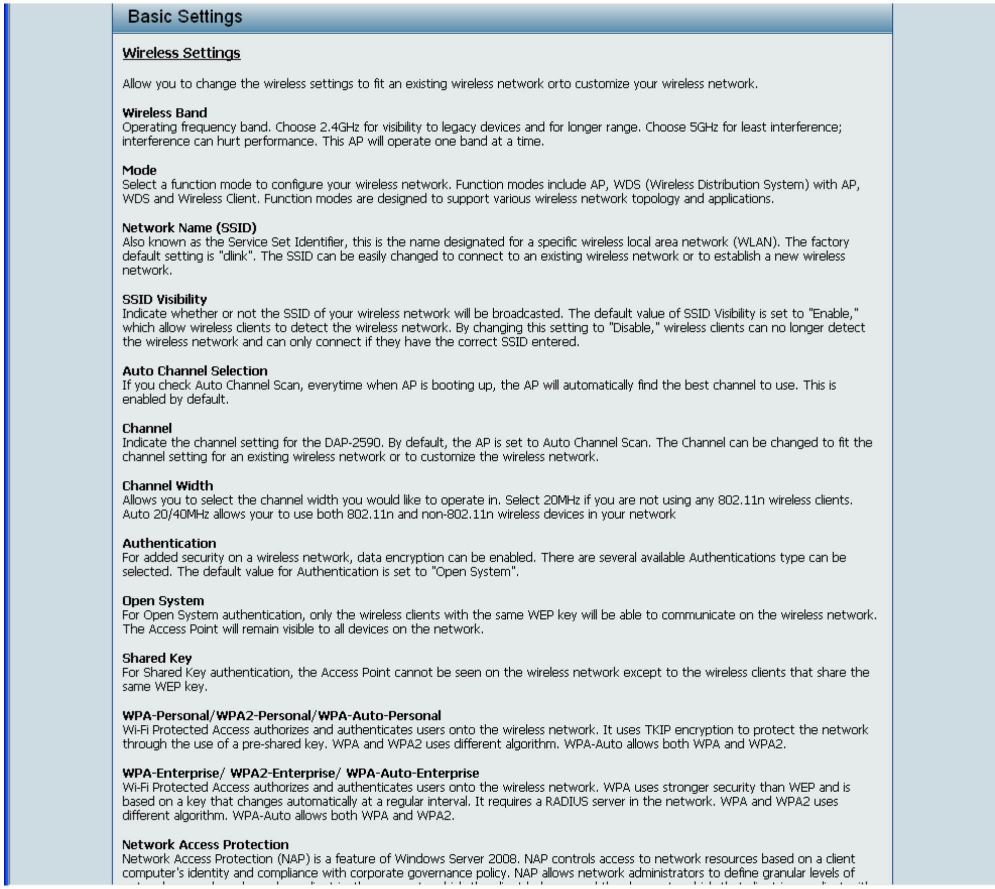


System Settings

Restart the Device [Restart]

Restore to Factory Default Settings [Restore]

Help



Wireless Settings

Allow you to change the wireless settings to fit an existing wireless network orto customize your wireless network.

Wireless Band
Operating frequency band. Choose 2.4GHz for visibility to legacy devices and for longer range. Choose 5GHz for least interference; interference can hurt performance. This AP will operate one band at a time.

Mode
Select a function mode to configure your wireless network. Function modes include AP, WDS (Wireless Distribution System) with AP, WDS and Wireless Client. Function modes are designed to support various wireless network topology and applications.

Network Name (SSID)
Also known as the Service Set Identifier, this is the name designated for a specific wireless local area network (WLAN). The 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.

SSID Visibility
Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Visibility is set to "Enable," which allow wireless clients to detect the wireless network. By changing this setting to "Disable," wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

Auto Channel Selection
If you check Auto Channel Scan, everytime when AP is booting up, the AP will automatically find the best channel to use. This is enabled by default.

Channel
Indicate the channel setting for the DAP-2590. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Channel Width
Allows you to select the channel width you would like to operate in. Select 20MHz if you are not using any 802.11n wireless clients. Auto 20/40MHz allows your to use both 802.11n and non-802.11n wireless devices in your network

Authentication
For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to "Open System".

Open System
For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

Shared Key
For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

WPA-Personal/WPA2-Personal/WPA-Auto-Personal
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. It uses TKIP encryption to protect the network through the use of a pre-shared key. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

WPA-Enterprise/ WPA2-Enterprise/ WPA-Auto-Enterprise
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

Network Access Protection
Network Access Protection (NAP) is a feature of Windows Server 2008. NAP controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of

Help: Scroll down the Help page for topics and explanations.

Using the AP Array

The deployment of wireless local area network (WLAN) in a small office environment is often hindered by the lack of simplicity, stability and affordability. Multiple access points (APs) will require more effort in configuration and management, and the complexity of security settings adds to the burden. With limited resources in a small office, solutions provided for bigger organizations will be too complicated and not economical.

D-Link's AP Array is an ideal WLAN management tool for the small office. The WLAN management feature is built within the firmware, making configuration for multiple APs an effortless process. All AirPremier 11n Business APs support this tool, which can manage up to eight stand-alone APs. This will make WLAN deployment easier and more affordable.

Simple WLAN Management Tool

When one needs to set up a wireless local area network (WLAN) in a small office with limited IT resources, D-Link's AP Array is the answer. It allows the efficient deployment of a secured WLAN and easier administration from a single point; thus, minimizing the effort to maintain the wireless network.

Easy Deployment and Management

With D-Link's AP Array, deployment and management of APs are made simple. The following steps show how straightforward it is to deploy the array of APs:

Step 1 - Deployment of Master AP:

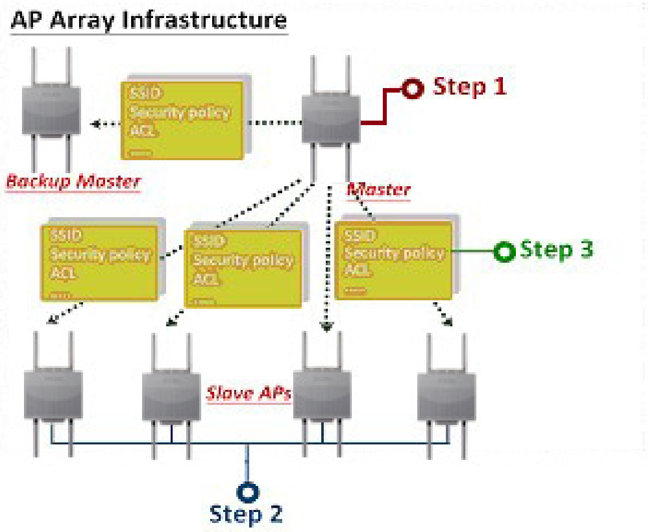
- Designate one AP as Master
- Set up Array ID & password
- Configure the AP

Step 2 - Deployment of Slave APs:

- Specify Array ID & password of Master in Slave APs.

Step 3 - Settings Are Synchronized:

- Backup Master & all Slave APs will follow configuration from Master automatically.

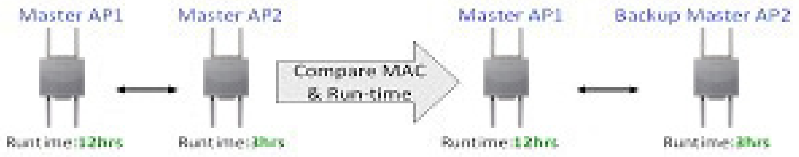


Up to eight stand-alone APs can be managed in an array. Members in the same AP Array group must be on the same subnet of the same model, and each AP is assigned with a unique IP address.

Situations Encountered with the Different Implementations:

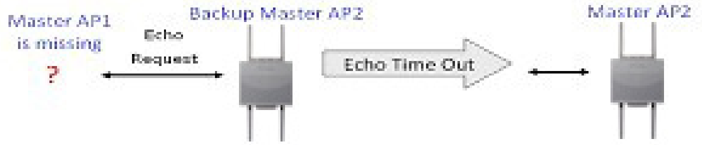
- **Multiple Master APs**: If there are two or more Master APs assigned in an array, the AP with the longest run-time will become the Master AP.

  Note: *The other Master APs will become Backup Master APs.*



- **Manually Configured Slave AP**: At intervals of one minute, the Master AP will send out a beacon to check the status of the Slave APs. If any changes are done to the slave APs manually, the Master AP will automatically synchronize its configuration to the slave AP and overwrite it.

- **Master AP Crashed**: In a situation where the Master AP becomes unavailable to the array, the Backup Master AP will take over the Master role and synchronize the configuration to the Slave APs.



- **No Backup Master AP Available**: If the Master AP crashes and there are only Slave APs in the array, the Slave APs will work as stand-alone APs until a new Master joins the array. The administrator may want to configure two Master APs for the array, so that there is always a Backup Master AP available.

Whenever the user makes any changes in the Master AP and selects "Save & Activate", the Master AP in an array will automatically synchronize its configuration to all Slave APs.

Settings that can be synchronized are:

- Wireless Settings
- Multiple SSID & VLAN
- WiFi Schedule
- MAC Filter
- WLAN Partition
- DHCP Server
- Log Settings
- Time & Date
- QoS Settings
- Performance Settings
- All Administrator Settings

Settings that are not synchronized are:

- Operation Mode
- Radio Channel
- LAN Settings

If required, settings that are not synchronized will have to be configured individually for each AP.

Different AP Roles in an Array

There are three modes for the administrator to define the role of each AP.

- **Master AP**
  The Master AP can do all the management settings for members in an array. Each array can only have one Master AP.

- **Backup Master AP**
  In an event when the Master AP crashes, the Backup Master AP will take over the Master AP function. Each array can have up to two Backup Master APs.

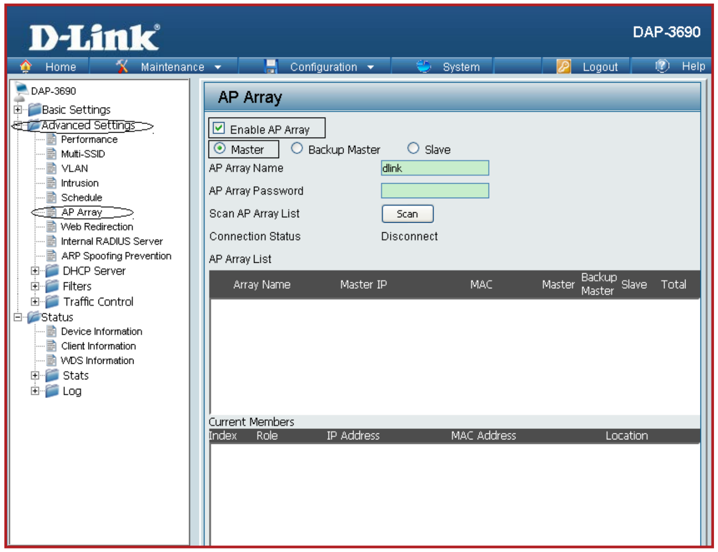
- **Slave AP**
  The Slave AP follows all the settings in the Master AP.

Easy Configuration of D-Link AP Array

The following section shows how simple it is to configure the D-Link AP Array for the different AP roles:

Master AP Role
Click **Advanced Settings** > **AP Array** to view and edit the information on the AP in an array.

Step 1:
Click **Enable AP Array** and select the **Master role**.



AP Array

☑ Enable AP Array

● Master ○ Backup Master ○ Slave

AP Array Name: dlink

AP Array Password:

Scan AP Array List

Connection Status: Disconnect

AP Array List

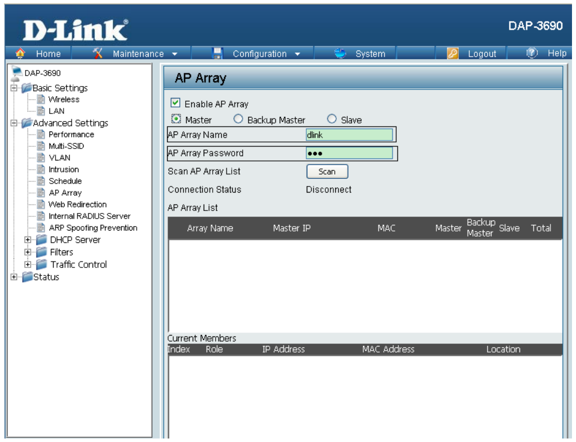
Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

Step 2:
Set up the AP Array **name** and **password**. Click the **Save** button located on the lower right hand side.

Note: *Remember to select "Save & Activate". The AP will not become master until you select "Save & Activate".*



AP Array

☑ Enable AP Array

● Master ○ Backup Master ○ Slave

AP Array Name: dlink

AP Array Password: •••

Scan AP Array List

Connection Status: Disconnect

AP Array List

Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

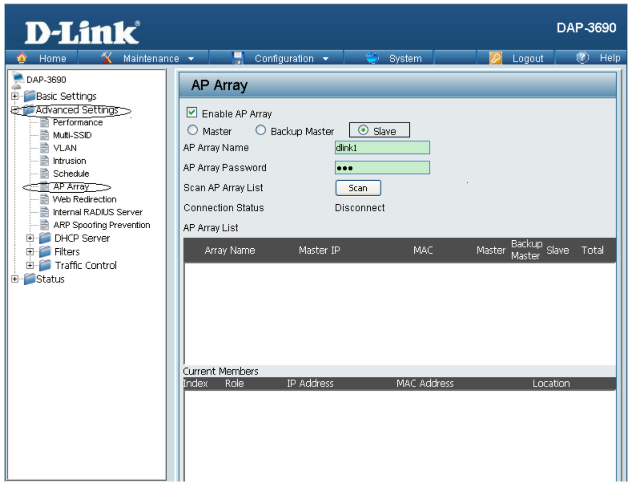
Current Members

Index	Role	IP Address	MAC Address	Location

Slave AP Role

Click **Advanced Settings** > **AP Array** to view and edit the information on the AP in an array.

Step 1:
Click **Enable AP Array** and select the **Slave role**.



AP Array

☑ Enable AP Array

○ Master ○ Backup Master ● Slave

AP Array Name: dlink1

AP Array Password: •••

Scan AP Array List

Connection Status: Disconnect

AP Array List

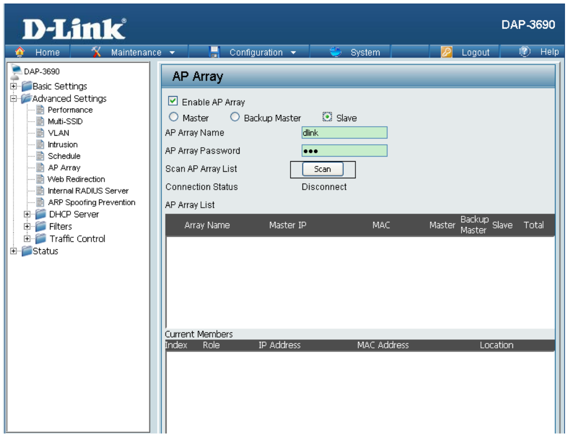
Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

Step 2:
Click the **Scan** button to search for an existing array, and enter the array password to join it. Click the **Save** button located on the lower right hand side.

Note: *Remember to select "Save & Activate". The AP will not become slave until you select "Save & Activate".*



AP Array

☑ Enable AP Array

○ Master ○ Backup Master ● Slave

AP Array Name	dlink
AP Array Password	●●●
Scan AP Array List	Scan
Connection Status	Disconnect

AP Array List

Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

Supported in all D-Link 11n Business APs

D-Link AP Array is supported in all D-Link 11n business APs.

Note: *Please refer to your local D-Link website for any new models of D-Link 11n business APs. You may also get the latest AP Array function by doing a firmware update.*

Reliable WLAN Management Tool

When you need a reliable WLAN management tool for your small office, the D-Link AP Array will be the ideal choice to provide you with the simplicity to configure and manage an array of APs. Being a free software module that is built in D-Link 11n business APs, it eliminates the need for an extra software or PC.

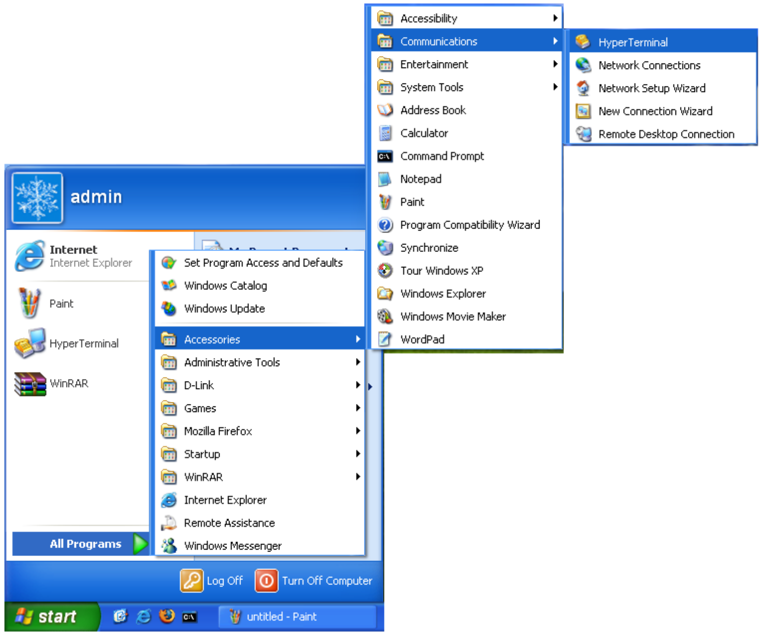
With auto-synchronization, it means that configuration will only need to be done on the Master AP, and it will automatically be synchronized to the Slave APs.

As AP configuration and management are done within only one Master AP, you will be able to view the deployment of APs as a single wireless network rather than a series of separate wireless devices.

Using the Console Port

You can connect to the DAP-3690 console port to configure device settings via the command line.

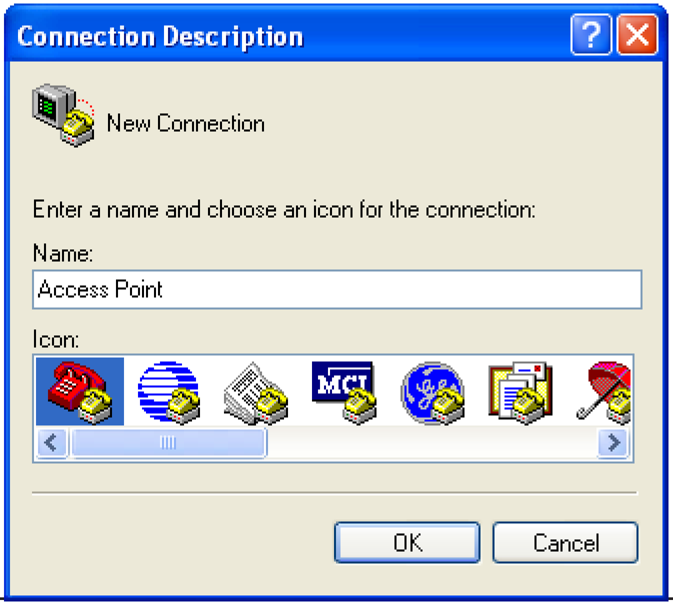
1. Connect one end of the provided serial console cable to the console port on the DAP-3690, and the other to an available serial port on the PC you wll use to connect to the device.



2. Run HyperTerminal on the PC:

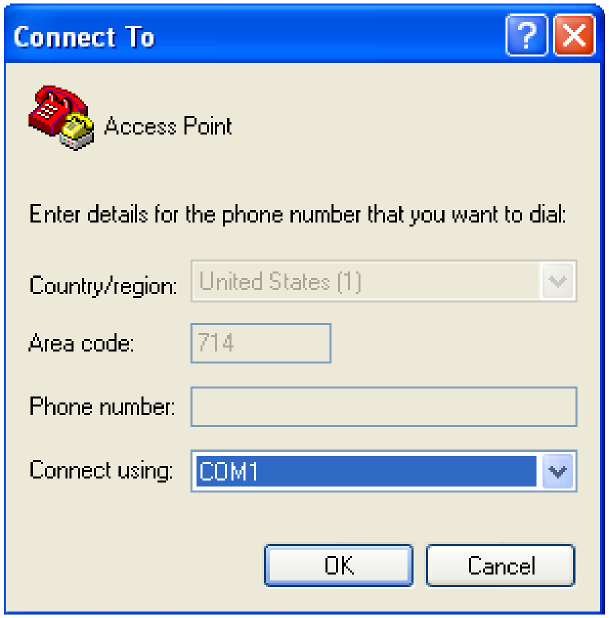
- Go to the Start Menu
- Select All Programs
- Select Accessories
- Select Communications
- Select HyperTerminal

3. Enter a New Connection name:



Name: Access Point

4. Select the appropriate COM port:


Connect To

Access Point

Enter details for the phone number that you want to dial:

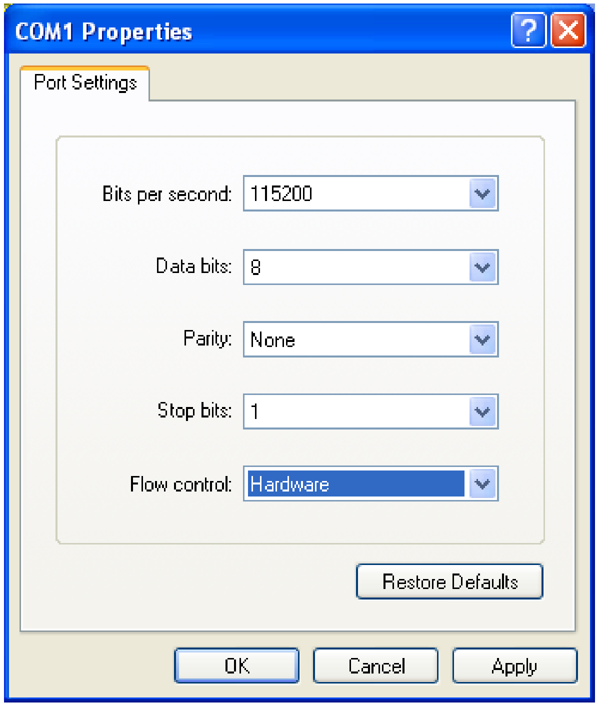
Country/region: United States (1)

Area code: 714

Phone number:

Connect using: COM1

5. Configure the Port Settings:


COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

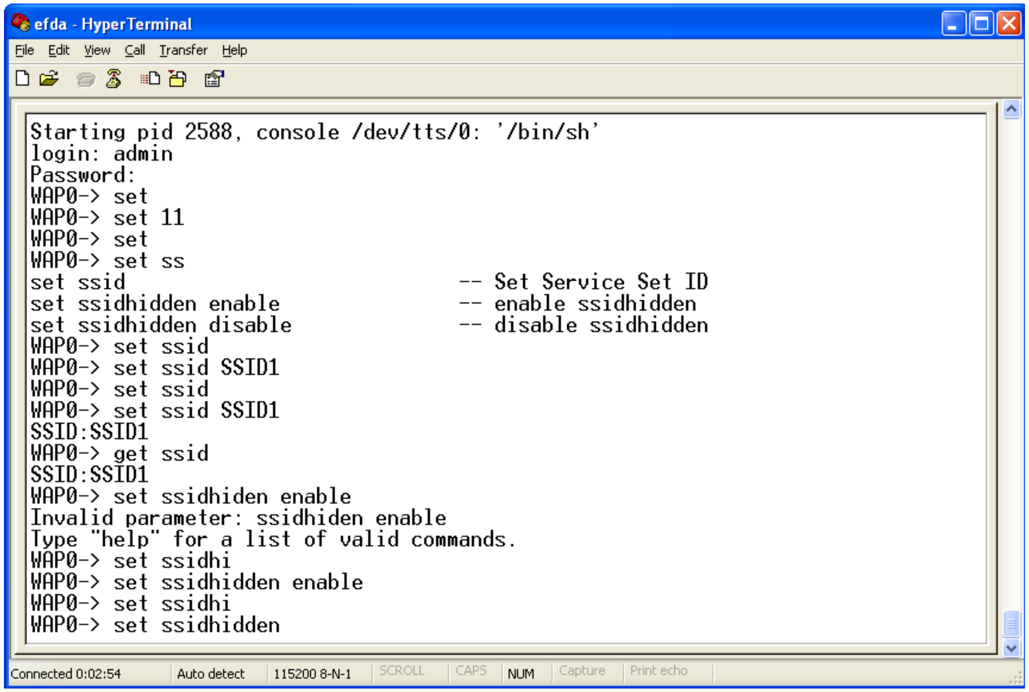
Flow control: Hardware

Note: Your terminal emulation must be set to 115200 bits per second.

6. Enter the Login Name and Password:

Once logged in, you will be able to run configuration commands from the command line prompt.

You can type in a letter and press tab to see the available command**s.**



```
Starting pid 2588, console /dev/tts/0: '/bin/sh'
login: admin
Password:
WAP0-> set
WAP0-> set 11
WAP0-> set
WAP0-> set ss
set ssid                            -- Set Service Set ID
set ssidhidden enable               -- enable ssidhidden
set ssidhidden disable              -- disable ssidhidden
WAP0-> set ssid
WAP0-> set ssid SSID1
WAP0-> set ssid
WAP0-> set ssid SSID1
SSID:SSID1
WAP0-> get ssid
SSID:SSID1
WAP0-> set ssidhiden enable
Invalid parameter: ssidhiden enable
Type "help" for a list of valid commands.
WAP0-> set ssidhi
WAP0-> set ssidhidden enable
WAP0-> set ssidhi
WAP0-> set ssidhidden
```

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3690 Wireless Access Point. We will cover various aspects of the network setup, especially the network adapters. Please read the following if you are having any technical difficulties.

Note: *It is recommended that you use an Ethernet connection to configure the DAP-3690.*

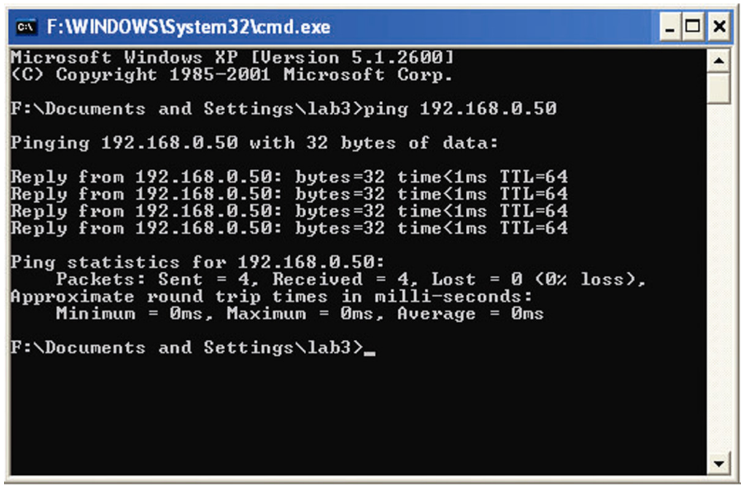
1. The computer used to configure the DAP-3690 cannot access the Configuration menu.

- Check if the LAN LED on the DAP-3690 is ON. If the LED is not ON, check if the cable for the Ethernet connection is securely inserted.
- Check if the Ethernet adapter is working properly. Please see item 3 of this Troubleshooting section to check that the drivers for the network adapters are loaded properly.
- Check if the IP address is in the same range and subnet as the DAP-3690.

Note: *The default IP address of the DAP-3690 is 192.168.0.50. All the computers on the network must have a unique IP address in the same range, e.g. 192.168.0.x. Any computers that have identical IP addresses will not be visible on the network. They must all have the same subnet mask, e.g. 255.255.255.0.*

- Do a Ping test to make sure that the DAP-3690 is responding. Go to **Start>Run**>Type "Command"and at the DOS prompt, type"ping 192.168.0.50". A successful ping will show four replies.

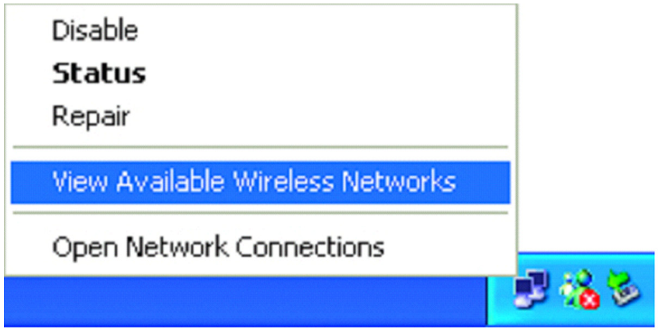
Note: *If you have changed the default IP address, make sure to ping the correct IP address assigned to the DAP-3690.*

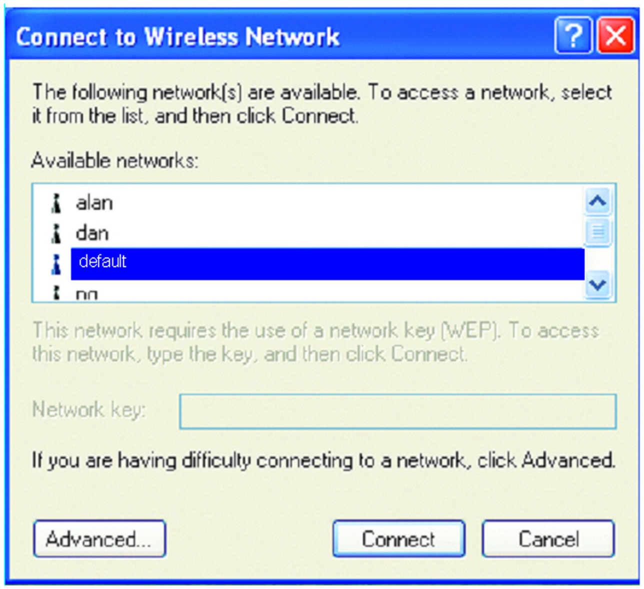


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab3>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

F:\Documents and Settings\lab3>_
```

2. The wireless client cannot access the Internet within Infrastructure mode.

Make sure the wireless client is associated and joined with the correct access point. To check this connection, right-click on the Local Area Connection icon in the taskbar and select View Available Wireless Networks. The Connect to Wireless Network screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.





The following network(s) are available. To access a network, select it from the list, and then click Connect.

Available networks:

- alan
- dan
- default
- nn

This network requires the use of a network key (WEP). To access this network, type the key, and then click Connect.

Network key:

If you are having difficulty connecting to a network, click Advanced.

- Check that the IP address assigned to the wireless adapter is within the same IP address range as the access point and gateway. Since the DAP-3690 has an IP address of 192.168.0.50, wireless adapters must have an IP address in the same range, e.g. 192.168.0.x. Each device must have a unique IP address; there may be no two devices with the same IP address. The subnet mask must be the same for all the computers on the network. To check the IP address assigned to the wireless adapter, double-click the Local Area Connection icon in the taskbar, then select the Support tab and the IP address will be displayed.

- If it is necessary to assign a Static IP Address to the wireless adapter. If you are entering a DNS Server address, you must also enter the Default Gateway Address. *Remember that if you have a DHCP-capable router, you will not need to assign a static IP address.*

3. What variables may cause my wireless products to lose reception?

D-Link products let you access your network from virtually anywhere you want, however, the positioning of the products within your environment will affect its wireless range.

4. Why does my wireless connection keep dropping?

- Antenna Orientation - try different antenna orientations for the DAP-3690. Try to keep the antenna at least 6 inches away from the wall or other objects.
- If you are using 2.4 GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or even drop. Try changing the channel of your router, access point and wireless adapter to a different channel to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

5. Why can’t I get a wireless connection?

If you have enabled encryption on the DAP-3690, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- Make sure that the SSID on the AP and the wireless client are exactly the same. If they are not, wireless connection cannot be established.
- Move the DAP-3690 and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Turn off your DAP-3690 and the client. Turn the DAP-3690 back on again, and then turn on the client.
- Make sure that all devices are set to Infrastructure mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network.
- If you are using 2.4 GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your DAP-3690, and on all the devices in your network to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

Technical Specifications

Standards
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3af

Network Management
- Web Browser interface
  - HTTP
  - Secure HTTP (HTTPS)
- AP Array
- AP Manager II
- SNMP Support
  - D-View Module
  - Private MIB
- Command Line Interface
  - Telnet
  - Secure SSH Telnet

Data Rates*

For 802.11a:
- 54, 48, 36, 24, 18, 12, 9, and 6 Mbps

For 802.11b:
- 11, 5.5, 2, and 1 Mbps

For 802.11g:
- 54, 48, 36, 24, 18, 12, 9, and 6 Mbps

For 802.11n : HT20/HT40
- 144.4/300, 130/270, 117/243, 104/216, 78/162, 66/135, 58.5/121.5, 52/108, 39/81, 26/54, 19.5/40.5, 12/27, and 6.5/13.5 Mbps

Security
- WPA™ Personal/Enterprise
- WPA2™ Personal/Enterprise
- WEP™ 64-/128-bit
- SSID Broadcast Disable
- MAC Address Access Control

Wireless Frequency Range
- 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz**

Operating Voltage
- 48V 0.4A PoE

Radio and Modulation Type

For 802.11a/g/n:
BPSK, QPSK, 16QAM, and 64QAM with OFDM

For 802.11b:
DQPSK, DBPSK, DSSS, and CCK

Operating Frequency*

For 802.11a:
5.15 ~ 5.85 GHz

For 802.11b/g:
2400 ~ 2483.5 MHz ISM band

For 802.11n:
2.4 GHz Band: 2.4 ~ 2.4835 GHz
5 GHz Band: 5.15 ~ 5.85 GHz

Dipole Antenna
5dBi Gain @2.4 GHz
7dBi Gain @5 GHz

*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

**Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3690 isn’t supported in the 5.25~5.35 GHz and 5.47 ~ 5.725 GHz frequency ranges in some regions.

LEDs

- Power
- LAN
- 2.4 GHz
- 5 GHz

Temperature

- -40°C~60°C*

* The product is capable of continuous reliable operation when operating in ambient temperature of -30°C to +60°C, and could be extended to -40°C to +60°C when heater is in operation.

Humidity

- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

Certifications

- FCC
- CE
- IC
- C-Tick
- UL
- WiFi
- NCC
- IP67

Dimensions

- L = 197 mm
- W = 190 mm
- H = 35 mm

*Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3690 isn't supported in the 5.25~5.35 GHz and 5.47 ~ 5.725 GHz frequency ranges in some regions.

Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DAP-3690)
- Hardware Revision (located on the label on the bottom of the Access Point (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the Access Point).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

For customers within the United States:

Phone Support:
(877) 354-6555

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(877) 354-6560

Internet Support:
http://support.dlink.ca

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects.

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support (USA 1-877-453-5465 or Canada 1-800-361-5265), who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form. Enter the assigned Case ID Number at https://rma.dlink.com/ (USA only) or https://rma.dlink.ca (Canada only).
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc.

- **USA residents** send to 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- **Canadian residents** send to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:
Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement:

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

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

FCC Caution:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

Industry Canada Notice:

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

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

This device has been designed to operate with an antenna having a maximum gain of 6 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Registration

Register your product online at registration.dlink.com

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
June 21, 2011