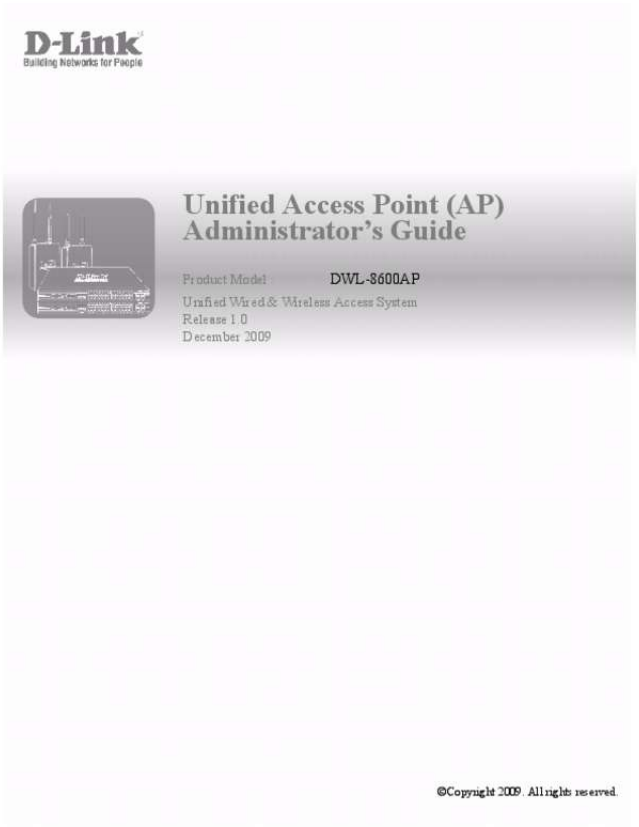

Manual abstract:

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 12 Online Help, Supported Browsers, and Limitations .....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

... 13 Section 2: Getting Started.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

14 Administrator's Computer Requirements.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....76 Page 4 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Section 6: Configuring SNMPv3 .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....77 Configuring SNMPv3 Views ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 77 Configuring SNMPv3 Groups.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

78 Configuring SNMPv3 Users .....
.....

.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

132 DiffServ Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
....134 Page 6 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP LIST OF FIGURES Figure 1: Administrator UI Online Help
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 13 Figure 2: Viewing Interface Status ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.111 Figure 39: Details for a Cluster Member AP....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....113 Page 8 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP LIST OF TABLES Table 1: Table 2: Table 3: Table 4: Table 5: Table 6: Table 7: Table 8: Table 9: Typographical Conventions ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
12 Requirements for the Administrator's Computer.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 15 Requirements for Wireless Clients .....
.....
.....
.....

.....113 Table 52: UAP Default Settings .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....114 Page 10 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP S e c t io n 1 : A b o ut Th i s D o c u m e n t This guide describes setup, configuration, administration and maintenance for the D-Link® Unified Access Point (UAP) on a wireless network. DOCUMENT ORGANIZATION The Unified Access Point Administrator's Guide contains the following sections: • • • • • • • • • • • Section 1: "About This Document" on page 11 Section 2: "Getting Started" on page 14 Section 3: "Viewing Access Point Status" on page 27 Section 4: "Managing the Access Point" on page 37 Section 5: "Configuring Access Point Services" on page 67 Section 6: "Configuring SNMPv3" on page 77 Section 7: "Maintaining the Access Point" on page 82 Section 8: "Configuring Client Quality of Service" on page 87 Section 9: "Clustering Multiple APs" on page 103 Appendix A "Default AP Settings" on page 114 Appendix B "Configuration Examples" on page 116 ADDITIONAL DOCUMENTATION The following documents are also available for the D-Link UAP. • • The Unified Access Point CLI Command Reference contains information about using the UAP command-line interface. The Unified Access Point Release Notes describe known issues and limitations.

34CSFP6XXUAP-SWUM100-D13 About This Document Page 11 D-Link UAP Software User Manual 12/10/09 DOCUMENT CONVENTIONS This section describes the conventions this document uses. Note: A note provides more information about a feature or technology and cross-references to related topics. Caution! A caution provides information about critical aspects of AP configuration, combinations of settings, events, or procedures that can adversely affect network connectivity, security, and so on. The following table describes the typographical conventions used in this guide. Table 1: Typographical Conventions Symbol Bold Blue Text Example Click Update to save your settings. See "Document Conventions" on page 12. Description Menu titles, page names, and button names Hyperlinked text. courier font courier font italics <> Angle brackets [ ] Square brackets [< >] Angle brackets within square brackets {} curly braces | Vertical bars [{}] Braces within square brackets WLAN-AP# show network Screen text, file names, commands, user-typed command-line entries value <value> [value] [<value>] {choice1 | choice2} choice1 | choice2 [{choice1 | choice2}] Command parameter, which might be a variable or fixed value. Indicates a parameter is a variable. You must enter a value in place of the brackets and text inside them.
Indicates an optional fixed parameter. Indicates an optional variable. Indicates that you must select a parameter from the list of choices. Separates the mutually exclusive choices. Indicate a choice within an optional element.
Page 12 Document Conventions 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP ONLINE HELP, SUPPORTED BROWSERS, AND LIMITATIONS Online help for the UAP Administration Web pages provides information about all fields and features available from the user interface (UI). The information in the online help is a subset of the information available in the Unified Access Point Administrator's Guide. Online help information corresponds to each page on the UAP Administration UI. For information about the settings on the current page, click the the bottom of the help panel on the UI. link on the right side of a page or the More.
.. link at The following figure shows an example of the online help available from the links on the user interface. Figure 1: Administrator UI Online Help 34CSFP6XXUAP-SWUM100-D13 Online Help, Supported Browsers, and Limitations Page 13 D-Link UAP Software User Manual 12/10/09 S e c ti o n 2 : G e t t i ng S t a r t e d The D-Link UAP provides continuous, high-speed access between wireless devices and Ethernet devices. It is an advanced, standards-based solution for wireless networking in businesses of any size. The UAP enables wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features. The UAP can operate in two modes: Standalone Mode or Managed Mode. In Standalone Mode, the UAP acts as an individual access point in the network, and you manage it by using the Administrator Web User Interface (UI), command-line interface (CLI), or SNMP. In Managed Mode, the UAP is part of the D-Link Unified Access System, and you manage it by using the D-Link Unified Switch. If an AP is in Managed Mode, the Administrator Web UI, Telnet, SSH, and SNMP services are disabled.

This document describes how to perform the setup, management, and maintenance of the UAP in Standalone Mode. For information about configuring the AP in Managed Mode by using the D-Link Unified Switch, see the Administrator Guide for the switch. Before you power on a new UAP, review the following sections to check required hardware and software components, client configurations, and compatibility issues. Make sure you have everything you need for a successful launch and test of your new or extended wireless network. This section contains the following topics: • • • • • • • • • • Administrator's Computer Requirements Wireless Client Requirements Dynamic and Static IP Addressing on the AP Installing the UAP Basic Settings Using the CLI to View the IP Address Configuring the Ethernet Settings Configuring IEEE 802.1X Authentication Verifying the Installation Configuring Security on the Wireless Access Point To manage the UAP by using the Web interface or by using the CLI through Telnet or SSH, the AP needs an IP address. If you use VLANs or IEEE 802.1X Authentication (port security) on your network, you might need to configure additional settings on the AP before it can connect to the network. Note: The WLAN AP is not designed to function as a gateway to the Internet. To connect your WLAN to other LANs or the Internet, you need a gateway device.
Page 14 Getting Started 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP ADMINISTRATOR'S COMPUTER REQUIREMENTS The following table describes the minimum requirements for the administrator's computer for configuration and administration of the UAP through a Web-based user interface (UI). Table 2: Requirements for the Administrator's Computer Required Software or Component Description Serial or

Ethernet Connection to the Access The computer used to configure the first access point must be connected to Point the access point by a serial cable or an Ethernet cable. Wireless Connection to the Network After initial configuration and launch of the first access point on your new wireless network, you can make subsequent configuration changes through the Administration Web pages using a wireless connection to the internal network.

For wireless connection to the access point, your administration device will need Wi-Fi capability similar to that of any wireless client: Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point.

Wireless client software configured to associate with the UAP. Configuration and administration of the UAP is provided through a Web-based user interface hosted on the access point. We recommend using one of the following supported Web browsers to access the access point Administration Web pages: • Microsoft® Internet Explorer® version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows® XP or Microsoft Windows 2000 • Netscape Mozilla 1.

7.x on Redhat® Linux® version 2.4 or later The administration Web browser must have JavaScript™ enabled to support the interactive features of the administration interface. Ensure that security is disabled on the wireless client used to initially configure the access point. Web Browser and Operating System Security Settings 34CSFP6XXUAP-SWUM100-D13 Administrator's Computer Requirements Page 15 D-Link UAP Software User Manual 12/10/09 WIRELESS CLIENT REQUIREMENTS The UAP provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running. The UAP supports multiple client operating systems. Clients can be laptop or desktop computers, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers. In order to connect to the access point, wireless clients need the software and hardware described in the following table. Table 3: Requirements for Wireless Clients Required Component Wi-Fi Client Adapter Description Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.

11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11n modes are supported.) Client software, such as Microsoft Windows Supplicant, configured to associate with the UAP. Security should be disabled on the client used to do initial configuration of the access point. If the Security mode on the access point is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid username and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.

1X, WPA with RADIUS server, and WPA-PSK. For information about configuring security on the access point, see "Virtual Access Point Settings" on page 46. Wireless Client Software Client Security Settings DYNAMIC AND STATIC IP ADDRESSING ON THE AP When you power on the access point, the built-in DHCP client searches for a DHCP server on the network in order to obtain an IP Address and other network information. If the AP does not find a DHCP server on the network, the AP continues to use its default Static IP Address (10.90.

90.91) until you re-assign it a new static IP address (and specify a static IP addressing policy) or until the AP successfully receives network information from a DHCP server. To change the connection type and assign a static IP address by using the CLI, see "Configuring the Ethernet Settings" on page 22 or, by using the Web UI, see "Ethernet Settings" on page 37. Caution! If you do not have a DHCP server on your internal network, and do not plan to use one, the first thing you must do after powering on the access point is change the connection type from DHCP to static IP. You can either assign a new static IP address to the AP or continue using the default address.

We recommend assigning a new static IP address so that if you bring up another WLAN AP on the same network, the IP address for each AP will be unique. RECOVERING AN IP ADDRESS If you experience trouble communicating with the access point, you can recover a static IP address by resetting the AP configuration to the factory defaults (see "Resetting the Factory Default Configuration" on page 84), or you can get a dynamically assigned address by connecting the AP to a network that has a DHCP server. Page 16 Wireless Client Requirements 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP DISCOVERING A DYNAMICALLY ASSIGNED IP ADDRESS If you have access to the DHCP server on your network and know the MAC address of your AP, you can view the new IP address associated with the MAC address of the AP. If you do not have access to the DHCP server that assigned the IP address to the AP or do not know the MAC address of the AP, you might need to use the CLI to find out what the new IP address is. For information about how to discover a dynamically assigned IP address, see "Using the CLI to View the IP Address" on page 21. INSTALLING THE UAP To access the Administration Web UI, you enter the IP address of the AP into a Web browser. You can use the default IP address of the AP (10.90.90.91) to log on to the AP and assign a static IP address, or you can use a DHCP server on you network to assign network information to the AP.

The DHCP client on the AP is enabled by default. To install the UAP, use the following steps: 1. Connect the AP to an administrative PC by using a LAN connection or a direct-cable connection. • To use a LAN connection, connect one end of an Ethernet cable to the network port on the access point and the other end to the same hub where your PC is connected, as shown in the following figure. The hub or switch you use must permit broadcast signals from the access point to reach all other devices on the network. • To use a direct-cable connection, connect one end of an Ethernet straight-through or crossover cable to the network port on the access point and the other end of the cable to the Ethernet port on the PC, as shown in the following figure. You can also use a serial cable to connect the serial port on the AP to a serial port on the administrative computer. For initial configuration with a direct Ethernet connection and no DHCP server, be sure to set your PC to a static IP address in the same subnet as the default IP address on the access point. (The default IP address for the access point is 10.90.

90.91.) If you use this method, you will need to reconfigure the cabling for subsequent startup and deployment of the access 34CSFP6XXUAP-SWUM100-D13 Installing the UAP Page 17 D-Link UAP Software User Manual 12/10/09 point so that the access point is no longer connected directly to the PC but instead is connected to the LAN (either by using a hub or directly). Note: It is possible to detect access points on the network with a wireless connection. However, we strongly advise against using this method.

In most environments you may have no way of knowing whether you are actually connecting to the intended AP. Also, many of the initial configuration changes required will cause you to lose connectivity with the AP over a wireless connection.

2. Connect the power adapter to the power port on the back of the access point, and then plug the other end of the power cord into a power outlet. 3. Use your Web browser to log on to the UAP Administration Web pages. If the AP did not acquire an IP address from a DHCP server on your network, enter 10.90.90.91 in the address field of your browser, which is the default IP address of the AP. If you used a DHCP server on your network to automatically configure network information for the AP, enter the new IP address of the AP into the Web browser. If you used a DHCP server and you do not know the new IP address of the AP, use the following procedures to obtain the information: a. Connect a serial cable from the administrative computer to the AP and use a terminal emulation program to access the command-line interface (CLI). b. At the login prompt, enter admin for the user name and admin for the password.

At the command prompt, enter get management The command output displays the IP address of the AP. Enter this address in the address field of your browser. For a more detailed explanation about how to log on to the CLI by using the console port, see "Using the CLI to View the IP Address" on page 21. 4. When prompted, enter admin for the user name and admin for the password, then click OK. When you first log in, the Basic Settings page for UAP administration is displayed, as the following figure shows. This page is also accessible from the Tools > Basic Settings menu. Page 18 Installing the UAP 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP 5. Verify the settings on the Basic Settings page. • •Review access point description and provide a new administrator password for the access point if you do not want to use the default password, which is admin.
Click the Update button to activate the wireless network with these new settings. Note: The changes you make are not saved or applied until you click Update. Changing some access point settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.
For more information about the fields and configuration options on the Basic Settings page, see "Basic Settings" on page 20. 6. If you do not have a DHCP server on the management network and do not plan to use one, you must change the Connection Type from DHCP to Static IP. You can either assign a new Static IP address to the AP or continue using the default address. We recommend assigning a new Static IP address so that if you bring up another UAP on the same network, the IP address for each AP will be unique.
To change the connection type and assign a static IP address, see "Configuring the Ethernet Settings" on page 22 (CLI) or "Ethernet Settings" on page 37 (Web). 34CSFP6XXUAP-SWUM100-D13 Installing the UAP Page 19 D-Link UAP Software User Manual 12/10/09 7. If your network uses VLANs, you might need to configure the management VLAN ID or untagged VLAN ID on the UAP in order for it to work with your network. For information about how to configure VLAN information, see "Configuring the Ethernet Settings" on page 22 (CLI) or "Ethernet Settings" on page 37 (Web). 8. If your network uses IEEE 802.1X port security for network access control, you must configure the 802.1X supplicant information on the AP. For information about how to configure the 802.1X user name and password, see "Configuring IEEE 802.

1X Authentication" on page 24. BASIC SETTINGS From the Basic Settings page, you can view various information about the UAP, including IP and MAC address information, and configure the administrator password for the UAP. Table 4 describes the fields and configuration options on the Basic Settings page. Table 4: Basic Settings Page Field IP Address IPv6 Address IPv6 Link Local Address MAC Address Description Shows the IP address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCP, or statically through the Ethernet Settings page). Shows the IPv6 address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCPv6, or statically through the Ethernet Settings page). Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process. Shows the MAC address of the AP.
The address shown here is the MAC address associated with the management interface. This is the address by which the AP is known externally to other networks. Shows version information about the firmware currently installed on the AP. As new versions of the WLAN AP firmware become available, you can upgrade the firmware on your APs. Identifies the AP hardware model.
Identifies the AP hardware version. Generic name to identify the type of hardware. Provides information about the product hardware. Enter the current administrator password. You must correctly enter the current password before you are able to change it.
Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type. The administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. Note: As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default. Re-enter the new administrator password to confirm that you typed it as intended. Firmware Version Product Identifier Hardware Version Device Name Device Description Current Password New Password Confirm New Password Page 20 Basic Settings 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 4: Basic Settings Page Field Baud Rate Description Select a baud rate for the serial port connection. The baud rate on the AP must match the baud rate on the terminal or terminal emulator to connect to the AP command-line interface (CLI) by using a serial (console) connection. The following baud rates are available: • 9600 • 19200 • 38400 • 57600 • 115200 Enter a name for the AP. This name appears only on the Basic Settings page and is a name to identify the AP to the administrator.

Use up to 64 alphanumeric characters, for example My AP. Enter the name, e-mail address, or phone number of the person to contact regarding issues related to the AP. Enter the physical location of the AP, for example Conference Room A. System Name System Contact System Location CONNECTING TO THE AP WEB INTERFACE BY USING THE IPV6 ADDRESS To connect to the AP by using the IPv6 global address or IPv6 link local address, you must enter the AP address into your browser in a special format. Note: The following instructions and examples work with Microsoft Internet Explorer 7 (IE7) and might not work with other browsers.

To connect to an IPv6 global address, add square brackets around the IPv6 address. For example, if the AP global IPv6 address is 2520::230:abff:fe00:2420, type the following address into the IE7 address field: http://[2520::230:abff:fe00:2420]. To connect to the iPv6 link local address, replace the colons (:) with hyphens (-), add the interface number preceded with an "s," then add ".ipv6-literal.net.

" For example, if the AP link local address is fe80::230:abff:fe00:2420, and the Windows interface is defined as "%6," type the following address into the IE7 address field: http://fe80--230-abff-fe00-2420s6.ipv6literal.net. USING THE CLI TO VIEW THE IP ADDRESS The DHCP client on the UAP is enabled by default. If you connect the UAP to a network with a DHCP server, the AP automatically acquires an IP address.

To manage the UAP by using the Administrator UI, you must enter the IP address of the access point into a Web browser. If a DHCP server on your network assigns an IP address to the UAP, and you do not know the IP address, use the following steps to view the IP address of the UAP: 1. Using a null-modem cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port. If you attached a PC, Apple, or UNIX workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm. 2.

Configure the terminal-emulation program to use the following settings: 34CSFP6XXUAP-SWUM100-D13 Using the CLI to View the IP Address Page 21 D-Link UAP Software User Manual 12/10/09 • • • • • Baud rate: 115200 bps Data bits: 8 Parity: none Stop bit: 1 Flow control: none 3. Press the return key, and a login prompt should appear. The login name is admin. The default password is admin. After a successful login, the screen shows the (Access Point Name)# prompt. 4. At the login prompt, enter get management. Information similar to the following prints to the screen. CONFIGURING THE ETHERNET SETTINGS The default Ethernet settings, which include DHCP and VLAN information, might not work for all networks. By default, the DHCP client on the UAP automatically broadcasts requests for network information.

If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information. The management VLAN is VLAN 1 by default. This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the access point. For information about using the Web interface to configure the Ethernet settings, see "Ethernet Settings" on page 37. You can also use the CLI to configure the Ethernet settings, which the following section describes. Page 22 Configuring the Ethernet Settings 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP USING THE CLI TO CONFIGURE ETHERNET SETTINGS Use the commands shown in the following table to view and set values for the Ethernet (wired) interface. For more information about each setting, see the description for the field in Table 12 on page 38. Table 5: CLI Commands for Ethernet Setting Action Get the DNS Name Set the DNS Name Command get host id set host id <host_name> For example: set host id vicky-ap get management set management vlan-id <1-4094> get untagged-vlan set untagged-vlan status up set untagged-vlan status down set untagged-vlan vlan-id <1-4094> get management dhcp-status set management dhcp-client status up set management dhcp-client status down set management static-ip <ip_address> Example: set management static-ip 10.10.

12.221 set management static-mask <netmask> Example: set management static-mask 255.255.255.0 set static-ip-route gateway <ip_address> Example: set static-ip-route gateway 10.

10.12.1 get host dns-via-dhcp set host dns-via-dhcp down set host static-dns-1 <ip_address> set host static-dns-2 <ip_address> Example: set host static-dns-1 192.168.23.

45 set host dns-via-dhcp up Get Current Settings for the Ethernet (Wired) Internal Interface Set the management VLAN ID View untagged VLAN information Enable the untagged VLAN Disable the untagged VLAN Set the untagged VLAN ID View the connection type Use DHCP as the connection type Use a Static IP as the connection type Set the Static IP address Set a Subnet Mask Set the Default Gateway View the DNS Nameserver mode Dynamic= up Manual=down Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode) Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode) 34CSFP6XXUAP-SWUM100-D13 Configuring the Ethernet Settings Page 23 D-Link UAP Software User Manual 12/10/09 In the following example, the administrator uses the CLI to set the management VLAN ID to 123 and to disable the untagged VLAN so that all traffic is tagged with a VLAN ID. D-Link-WLAN-AP# set management vlan-id 123 D-Link-WLAN-AP# set untagged-vlan status down D-Link-WLAN-AP# get management Property Value ----------vlan-id 123 interface brvlan123 static-ip 10.90.90.91 static-mask 255.0.0.0 ip 10.254.24.

43 mask 255.255.248.0 mac 00:02:BC:00:14:E8 dhcp-status up D-Link-WLAN-AP# get untagged-vlan Property Value ----------vlan-id 1 status down D-Link-WLAN-AP# CONFIGURING IEEE 802.1X AUTHENTICATION On networks that use IEEE 802.1X, port-based network access control, a supplicant (client) cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information that the AP can supply to the authenticator.

If your network uses IEEE 802.1X see "Configuring 802.1X Authentication" on page 65 for information about how to configure 802.1X by using the Web interface. USING THE CLI TO CONFIGURE 802.

1X AUTHENTICATION INFORMATION The following table shows the commands used to configure the 802.1X supplicant information using the CLI. Table 6: CLI Commands for the 802.1X Supplicant Action View 802.1X supplicant settings Enable 802.

1X supplicant Disable 802.1X supplicant Set the 802.1X user name Set the 802.1s password Command get dot1x-supplicant set dot1x-supplicant status up set dot1x-supplicant status down set dot1x-supplicant user <name> set dot1x-supplicant password <password> In the following example, the administrator enables the 802.1X supplicant and sets the user name to wlanAP and the password to test1234. Page 24 Configuring IEEE 802.1X Authentication 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP D-Link-WLAN-AP# set D-Link-WLAN-AP# set D-Link-WLAN-AP# set D-Link-WLAN-AP# get Property Value ----------status up user wlanAP dot1x-supplicant status up dot1x-supplicant user wlanAP dot1x-supplicant password test1234 dot1x-supplicant VERIFYING THE INSTALLATION Make sure the access point is connected to the LAN and associate some wireless clients with the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune the AP by modifying advanced configuration features.

1. Connect the access point to the LAN.

• • If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN. The next step is to test some wireless clients. If you configured the access point by using a direct cable connection from your computer to the access point, do the following procedures: a. Disconnect the cable from the computer and the access point. b. Connect an Ethernet cable from the access point to the LAN. c. Connect your computer to the LAN by using an Ethernet cable or a wireless card. 2. Test LAN connectivity with wireless clients.

Test the UAP by trying to detect it and associate with it from some wireless client devices. For information about requirements for these clients, see "Wireless Client Requirements" on page 16. 3. Secure and configure the access point by using advanced features. Once the wireless network is up and you can connect to the AP with some wireless clients, you can add in layers of security, create multiple virtual access points (VAPs), and configure performance settings. Note: The WLAN AP is not designed for multiple, simultaneous configuration changes. If more than one administrator is logged onto the Administration Web pages and making changes to the configuration, there is no guarantee that all configuration changes specified by multiple users will be applied. By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN. An important next step is to configure security, as described in "Virtual Access Point Settings" on page 46. 34CSFP6XXUAP-SWUM100-D13 Verifying the Installation Page 25 D-Link UAP Software User Manual 12/10/09 CONFIGURING SECURITY ON THE WIRELESS ACCESS POINT You configure secure wireless client access by configuring security for each virtual access point (VAP) that you enable.

You can configure up to 16 VAPs per radio that simulate multiple APs in one physical access point. By default, only one VAP is enabled. For each VAP, you can configure a unique security mode to control wireless client access. Each radio has 16 VAPs, with VAP IDs from 0-15. By default, only VAP 0 on each radio is enabled. VAP0 has the following default settings: • • • • • • VLAN ID: 1 Broadcast SSID: Enabled SSID: dlink1 Security: None MAC Authentication Type: None Redirect Mode: None All other VAPs are disabled by default. The default SSID for VAPs 1–15 is dlinkx where x is the VAP ID. To prevent unauthorized access to the UAP, we recommend that you select and configure a security option other than None for the default VAP and for each VAP that you enable. For information about how to configure the security settings on each VAP, see "Virtual Access Point Settings" on page 46. Page 26 Configuring Security on the Wireless Access Point 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP S e c t io n 3 : V i ew in g A c c e s s Po in t S t a t us This section describes the information you can view from the tabs under the Status heading on the navigation tree of the UAP Web UI.

This section contains the following subsections: • • • • • • Viewing Interface Status Viewing Events Viewing Transmit and Receive Statistics Viewing Associated Wireless Client Information Viewing Neighboring Access Points Viewing Managed AP DHCP Information VIEWING INTERFACE STATUS To monitor Ethernet LAN and wireless LAN (WLAN) settings, click the Interfaces tab. Figure 2: Viewing Interface Status This page displays the current settings of the UAP. It displays the Wired Settings and the Wireless Settings. WIRED SETTINGS (INTERNAL INTERFACE) The Internal interface includes the Ethernet MAC Address, Management VLAN ID, IP Address (IPv4 and IPv6), Subnet Mask, and DNS information. If you want to change any of these settings, click the Edit link. After you click Edit, you are redirected to the Ethernet Settings page. 34CSFP6XXUAP-SWUM100-D13 Viewing Access Point Status Page 27 D-Link UAP Software User Manual 12/10/09 For information about configuring these settings, see "Configuring the Ethernet Settings" on page 22. WIRELESS SETTINGS The Radio Interface includes the Radio Mode and Channel. The Wireless Settings section also shows the MAC address (read-only) associated with each radio interface. If you want to change the Radio Mode or Channel settings, click the Edit link.

After you click Edit, you are redirected to the Wireless Settings page. For information about configuring these settings, see "Wireless Settings" on page 40 and "Modifying Radio Settings" on page 43. VIEWING EVENTS The Events page shows real-time system events on the AP such as wireless clients associating with the AP and being authenticated. To view system events, click the Events tab. Figure 3: Viewing Events From the Events page, you can view the most recent events generated by this AP and configure logging settings.

You can enable and configure persistent logging to write system event logs to non-volatile memory so that the events are not erased when the system reboots. This page also gives you the option of enabling a remote log relay host to capture all system events and errors in a Kernel Log. Page 28 Viewing Events 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Note: The AP acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as Greenwich Mean Time). You need to convert the reported time to your local time. For information on setting the network time protocol, see "Enabling the Network Time Protocol Server" on page 76. CONFIGURING PERSISTENT LOGGING OPTIONS If the system unexpectedly reboots, log messages can be useful to diagnose the cause. However, log messages are erased when the system reboots unless you enable persistent logging. Caution! Enabling persistent logging can wear out the flash (non-volatile) memory and degrade network performance. You should only enable persistent logging to debug a problem. Make sure you disable persistent logging after you finish debugging the problem. To configure persistent logging on the Events page, set the persistence, severity, and depth options as described in Table 7, and then click Update. Figure 4: Persistent Logging Options Table 7: Logging Options Field Persistence Description Choose Enabled to save system logs to non-volatile memory so that the logs are not erased when the AP reboots. Choose Disabled to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.

Specify the severity level of the log messages to write to non-volatile memory. For example, if you specify 2, critical, alert, and emergency logs are written to non-volatile memory. Error messages with a severity level of 3–7 are written to volatile memory. • 0—emergency • 1—alert • 2—critical • 3—error • 4—warning • 5—notice • 6—info • 7—debug You can store up to 128 messages in non-volatile memory.

Once the number you configure in this field is reached, the oldest log event is overwritten by the new log event. Severity Depth 34CSFP6XXUAP-SWUM100-D13 Viewing Events Page 29 D-Link UAP Software User Manual 12/10/09 Note: To apply your changes, click Apply. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low. CONFIGURING THE LOG RELAY HOST FOR KERNEL MESSAGES The Kernel Log is a comprehensive list of system events (shown in the System Log) and kernel messages such as error conditions, like dropping frames.

You cannot view kernel log messages directly from the Administration Web UI for an AP. You must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. Then, you can configure the UAP to send syslog messages to the remote server. Remote log server collection for AP syslog messages provides the following features: • • • Allows aggregation of syslog messages from multiple APs Stores a longer history of messages than kept on a single AP Triggers scripted management operations and alerts To use Kernel Log relaying, you must configure a remote server to receive the syslog messages. The procedure to configure a remote log host depends on the type of system you use as the remote host.

Note: The syslog process will default to use port 514. We recommend keeping this default port. However; If you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process. ENABLING OR DISABLING THE LOG RELAY HOST ON THE EVENTS PAGE To enable and configure Log Relaying on the Events page, set the Log Relay options as described in the following table, and then click Apply. Figure 5: Log Relay Host Table 8: Log Relay Host Field Relay Log Relay Host Description Select Enabled to allow the UAP to send log messages to a remote host. Select Disabled to keep all log messages on the local system. Specify the IP Address or DNS name of the remote log server. Page 30 Viewing Events 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 8: Log Relay Host Field Relay Port Description Specify the Port number for the syslog process on the Relay Host. The default port is 514. Note: To apply your changes, click Apply. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low. If you enabled the Log Relay Host, clicking Apply will activate remote logging. The AP will send its kernel messages realtime for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you disabled the Log Relay Host, clicking Apply will disable remote logging. VIEWING TRANSMIT AND RECEIVE STATISTICS The Transmit/Receive page provides some basic information about the current AP and a real-time display of the transmit and receive statistics for the Ethernet interface on the AP and for the VAPs on both radio interfaces. All transmit and receive statistics shown are totals since the AP was last started. If you reboot the AP, these figures indicate transmit and receive totals since the reboot. To view transmit and receive statistics for the AP, click the Transmit/Receive tab. Figure 6: Viewing Traffic Statistics 34CSFP6XXUAP-SWUM100-D13 Viewing Transmit and Receive Statistics Page 31 D-Link UAP Software User Manual 12/10/09 Table 9: Transmit/Receive Field Interface Status MAC Address Description The name of the Ethernet or VAP interface. Shows whether the interface is up or down. MAC address for the specified interface. The UAP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.

Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same AP. The VLAN ID is set on the VAP tab. (See "Configuring Load Balancing" on page 62.) Wireless network name.

Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP tab. (See "Configuring Load Balancing" on page 62.) VLAN ID Name (SSID) Transmit and Receive Information Total Packets Total Bytes Total Drop Packets Total Drop Bytes Errors Indicates total packets sent (in Transmit table) or received (in Received table) by this AP. Indicates total bytes sent (in Transmit table) or received (in Received table) by this AP.

Indicates total number of packets sent (in Transmit table) or received (in Received table) by this AP that were dropped. Indicates total number of bytes sent (in Transmit table) or received (in Received table) by this AP that were dropped. Indicates total errors related to sending and receiving data on this AP. VIEWING ASSOCIATED WIRELESS CLIENT INFORMATION To view the client stations associated with a particular access point, click the Client Associations tab. Figure 7: Viewing Client Association Information The associated stations are displayed along with information about packet traffic transmitted and received for each station. Table 10 describes the fields on the Client Associations page. Page 32 Viewing Associated Wireless Client Information 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 10: Associated Clients Field Network Description Shows which VAP the client is associated with. For example, an entry of wlan0vap2 means the client is associated with Radio 1, VAP 2. An entry of wlan0 means the client is associated with VAP 0 on Radio 1. An entry of wlan1 means the client is associated with VAP 0 on Radio 2.

Shows the MAC address of the associated wireless client. The Authenticated and Associated Status shows the underlying IEEE 802.11 authentication and association status, which is present no matter which type of security the client uses to connect to the AP. This status does not show IEEE 802.1X authentication or association status. Some points to keep in mind with regard to this field are: • If the AP security mode is None or Static WEP, the authentication and association status of clients showing on the Client Associations tab will be in line with what is expected; that is, if a client shows as authenticated to the AP, it will be able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.) • If the AP uses IEEE 802.1X or WPA security, however, it is possible for a client association to show on this tab as authenticated (via the IEEE 802.

11 security) but actually not be authenticated to the AP via the second layer of security. Shows the number of packets and bytes received from the wireless client and the number of packets and bytes that were dropped after being received. Shows the number of packets and bytes transmitted from the AP to the wireless client and the number of packets and bytes that were dropped upon transmission.

Station Status From Station To Station LINK INTEGRITY MONITORING The UAP provides link integrity monitoring to continually verify its connection to each associated client. To do this, the AP sends data packets to clients every few seconds when no other traffic is passing.

This allows the AP to detect when a client goes out of range, even during periods when no normal traffic is exchanged. The client connection drops off the list within 300 seconds if these data packets are not acknowledged, even if no disassociation message is received. 34CSFP6XXUAP-SWUM100-D13 Viewing Associated Wireless Client Information Page 33 D-Link UAP Software User Manual 12/10/09 VIEWING NEIGHBORING ACCESS POINTS The status page for Neighboring Access Points provides real-time statistics for all APs within range of the AP on which you are viewing the Administration Web pages. Click Apply to refresh the screen and display the most current information. To view information about other access points on the wireless network, click the Neighboring Access Points tab.

Figure 8: Viewing Neighboring Access Points You must enable the AP detection on the AP in order to collect information about other APs within range. Page 34 Viewing Neighboring Access Points 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 11 describes the information provided on neighboring access points. Table 11: Neighboring Access Points Field AP Detection MAC Radio Description To enable neighbor AP detection and collect information about neighbor APs, click Enabled. To disable neighbor AP detection, click Disabled. Shows the MAC address of the neighboring AP. The Radio field indicates which radio detected the neighboring AP: • wlan0 (Radio One) • wlan1 (Radio Two) Shows the Beacon interval being used by this AP. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on the Radio tab page.(See "Modifying Radio Settings" on page 43.

) Indicates the type of device: • AP indicates the neighboring device is an AP that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. • Ad hoc indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). The Service Set Identifier (SSID) for the AP. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name. The SSID is set on the VAP tab.

(See "Configuring Load Balancing" on page 62.) Indicates whether there is any security on the neighboring device. • Off indicates that the Security mode on the neighboring device is set to None (no security). • On indicates that the neighboring device has some security in place. Security is configured on the AP from the VAP page.

Indicates whether WPA security is on or off for this AP. This indicates the IEEE 802.11 mode being used on this AP. (For example, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.) The number shown indicates the mode according to the following map: • 2.4 indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes) • 5 indicates IEEE 802.11a or 802.11n mode (or both modes) Shows the Channel on which the AP is currently broadcasting. The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.

The channel is set in Radio Settings. (See "Modifying Radio Settings" on page 43.) Shows the rate (in megabits per second) at which this AP is currently transmitting. The current rate will always be one of the rates shown in Supported Rates. Indicates the strength of the radio signal emitting from this AP. If you hover the mouse pointer over the bars, a number appears and shows the strength in decibels (dB). Shows the total number of beacons received from this AP since it was first discovered. Shows the date and time of the last beacon received from this AP. Beacon Int. Type SSID Privacy WPA Band Channel Rate Signal Beacons Last Beacon 34CSFP6XXUAP-SWUM100-D13 Viewing Neighboring Access Points Page 35 D-Link UAP Software User Manual 12/10/09 Table 11: Neighboring Access Points (Cont.

) Field Rates Description Shows supported and basic (advertised) rate sets for the neighboring AP. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the Radio Settings page. (See "Modifying Radio Settings" on page 43.

) VIEWING MANAGED AP DHCP INFORMATION The UAP can learn about D-Link Unified Switches on the network through DHCP responses to its initial DHCP request. The Managed AP DHCP page displays the DNS names or IP addresses of up to four D-Link Unified Switches that the AP learned about from a DHCP server on your network. For information about how to configure a DHCP server to respond to AP DHCP requests with the switch IP address information, see the Administrator Guide for the switch. Page 36 Viewing Managed AP DHCP Information 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Sec tion 4: Managing the A cce ss Po int This section describes how to manage the UAP and contains the following subsections: • • • • • • Ethernet Settings Modifying Radio Settings Virtual Access Point Settings Configuring Load Balancing Controlling Access by MAC Authentication Configuring Load Balancing The configuration pages for the features in this section are located under the Manage heading on the navigation tree of the UAP Web UI. ETHERNET SETTINGS The default wired interface settings, which include DHCP and VLAN information, might not work for all networks.

By default, the DHCP client on the UAP automatically broadcasts requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information. The management VLAN is VLAN 1 by default. This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the AP. To configure the LAN settings, click the Ethernet Settings tab. 34CSFP6XXUAP-SWUM100-D13 Managing the Access Point Page 37 D-Link UAP Software User Manual 12/10/09 Figure 9: Ethernet Settings The following table describes the fields to view or configure on the Ethernet Settings page. Table 12: Ethernet Settings Page Field DNS Name Description Enter the DNS name (host name) for the AP in the text box. The DNS name has the following requirements: • Maximum of 20 characters • Only letters, numbers and dashes • Must start with a letter and end with either a letter or a number Shows the MAC address for the LAN interface for the Ethernet port on this AP.

This is a read-only field that you cannot change.

MAC Address Management VLAN ID The management VLAN is the VLAN associated with the IP address you use to access the AP. The default management VLAN ID is 1. Provide a number between 1 and 4094 for the management VLAN ID. Untagged VLAN If you disable the untagged VLAN, all traffic is tagged with a VLAN ID. By default all traffic on the UAP uses VLAN 1, which is the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS. Provide a number between 1 and 4094 for the untagged VLAN ID. Traffic on the VLAN that you specify in this field will not be tagged with a VLAN ID. Untagged VLAN ID Page 38 Ethernet Settings 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 12: Ethernet Settings Page (Cont.) Field Connection Type Description If you select DHCP, the UAP acquires its IP address, subnet mask, DNS, and gateway information from a DHCP server.

If you select Static IP, you must enter information in the Static IP Address, Subnet Mask, and Default Gateway fields. Enter the static IP address in the text boxes. This field is disabled if you use DHCP as the connection type. Enter the Subnet Mask in the text boxes. Enter the Default Gateway in the text boxes. Select the mode for the DNS. In Dynamic mode, the IP addresses for the DNS servers are assigned automatically via DHCP. This option is only available if you specified DHCP for the Connection Type. In Manual mode, you must assign static IP addresses to resolve domain names. Enable or disable IPv6 management access to the AP Enable or disable IPv6 auto address configuration on the AP.

When IPv6 Auto Config Mode is enabled, automatic IPv6 address configuration and gateway configuration is allowed by processing the Router Advertisements received on the LAN port. The AP can have multiple auto configured IPv6 addresses. Enter a static IPv6 address. The AP can have a static IPv6 address even if addresses have already been configured automatically. Enter the static IPv6 prefix length, which is an integer in the range of 0–128. Static IP Address Subnet Mask Default Gateway DNS Nameservers IPv6 Admin Mode IPv6 Auto Config Admin Mode Static IPv6 Address Static IPv6 Address Prefix Length IPv6 Autoconfigured If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed. Global Addresses IPv6 Link Local Address Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process. Default IPv6 Gateway Enter the default IPv6 gateway. 34CSFP6XXUAP-SWUM100-D13 Ethernet Settings Page 39 D-Link UAP Software User Manual 12/10/09 WIRELESS SETTINGS Wireless settings describe aspects of the LAN related specifically to the radio device in the AP (802.

11 Mode and Channel) and to the network interface to the AP (AP MAC address). To configure the wireless interface, click the Wireless Settings tab. Figure 10: Wireless Interface Configuration Note: Radio interface settings apply to both Radio Interface One and Radio Interface Two. Page 40 Wireless Settings 34CSFP6XXUAP-SWUM100-D13 Software User Manual 12/10/09 D-Link UAP Table 13 describes the fields and configuration options available on the Wireless Settings page. Table 13: Wireless Settings Field Description 802.11d Regulatory Enabling support for IEEE 802.11d (World Mode) on the AP causes the AP to broadcast which Domain Support country it is operating in as a part of its beacons and probe responses. This allows client stations to operate in any country without reconfiguration. Disabling 802.11d prevents the country code setting from being broadcast in the beacons.

However, this only applies to radios configured to operate in the g band (2.4 GHz band). For radios operating in the a band (5 GHz band), the AP software configures support for 802.11h. When 802.

11h is supported, the country code information is broadcast in the beacons. To enable 802.11d regulatory domain support, click Enabled. To disable 802.11d regulatory domain support, click Disabled.

IEEE 802.11h Support The Administration UI shows whether IEEE 802.11h regulatory domain control is in effect on the AP. IEEE 802.11h cannot be disabled by an end user Administrator. For more information, see "Using the 802.11h Wireless Mode" on page 42. IEEE 802.11h is a standard that provides two services required to satisfy certain regulatory domains for the 5-GHz band. These two services are Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS).

Note: The 802.11h mode is automatically enabled if the AP is configured to work in any country that requires 802.11h as a minimum standard. This standard is currently only required by those countries which fall into the European Telecommunications Standard Institute (ETSI) category. 802.11h is also enabled for Japan. To enable station isolation, select the check box directly beside it. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same VAP. The AP still allows data traffic between its wireless clients and wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among wireless clients.

Specify whether you want the radio interface on or off. Indicates the Media Access Control (MAC) addresses for the interface. This page shows the MAC addresses for Radio Interface One and Radio Interface Two. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer.

You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. The Mode defines the Physical Layer (PHY) standard the radio uses. Note: The modes available on your AP depend on the country code setting. Select one of the following modes for each radio interface: • IEEE 802.

11a—Only 802.11a clients can connect to the AP. • IEEE 802.11b/g—802.11b and 802.11g clients can connect to the AP. • IEEE 802.11a/n—802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP.

• IEEE 802.11b/g/n (default)—802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the AP. • 5 GHz IEEE 802.11n—Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.

• 2.4 GHz IEEE 802.11n—Only 802.11n clients operating in the 5-GHz frequency can connect to the AP. Station Isolation Radio Interface MAC Address Mode 34CSFP6XXUAP-SWUM100-D13 Wireless Settings Page 41 D-Link UAP Software User Manual 12/10/09 Table 13: Wireless Settings (Cont.