D-Link®

DWL-2700AP

802.11b/g Access Point

Command Line Interface Reference Manual

Ver 3.20 (Feberuary 2009)

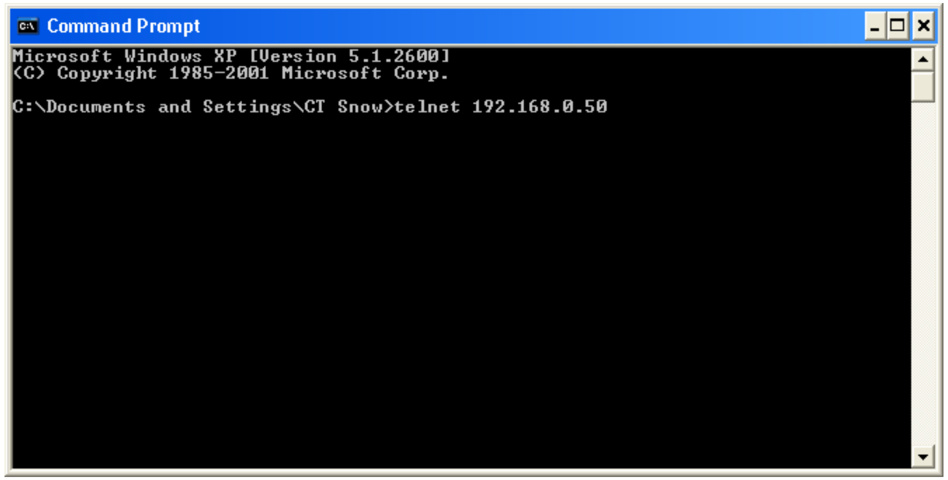
RECYCLABLE

Table of Contents

1

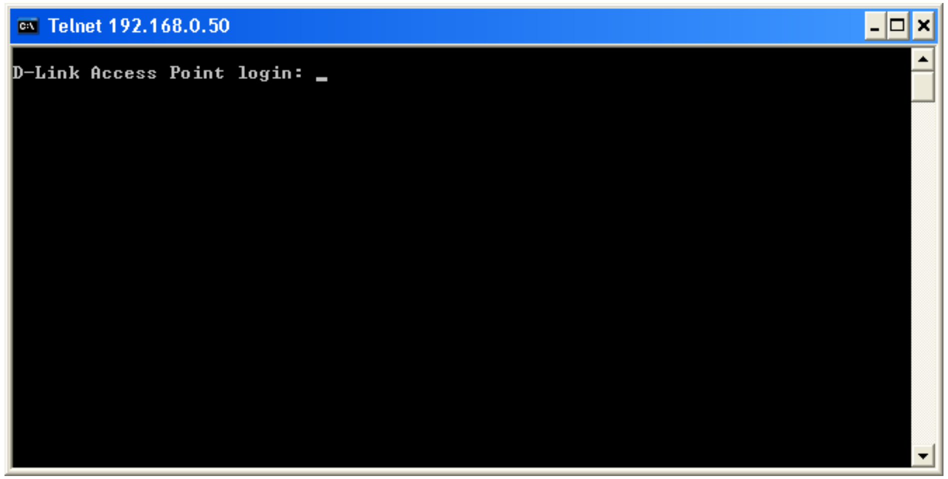
USING THE CLI

The DWL-2700AP can be accessed by Telnet. Using Microsoft Windows Operation system as example, open the Command Prompt on the computer that will be used for configuring and managing the AP and enter **telnet** and IP address of DWL-2700AP in the first line. Using the default IP address as example, enter **telnet 192.168.0.50** to cause the following screen to open:



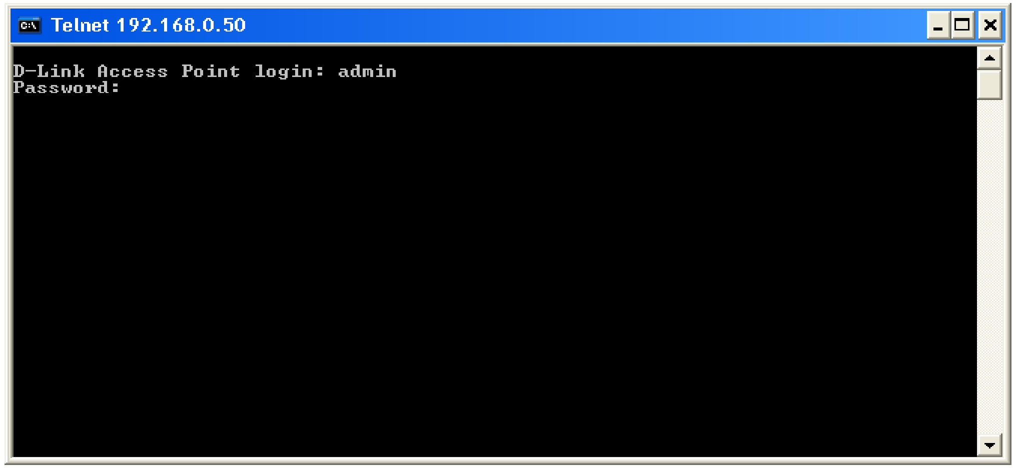
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CT Snow>telnet 192.168.0.50
```

Press **Enter** in the screen above. The following screen opens:



```
D-Link Access Point login: _
```

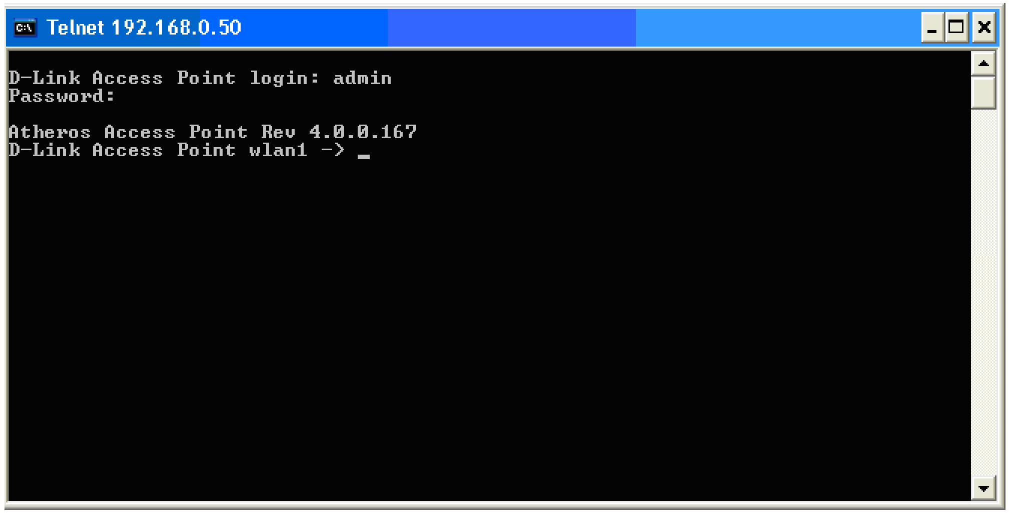
Type “**admin**” for the D-Link Access Point login username in the screen above and press **Enter**. The following screen opens:



```
D-Link Access Point login: admin
Password:
```

Press **Enter** as there is no initial password.

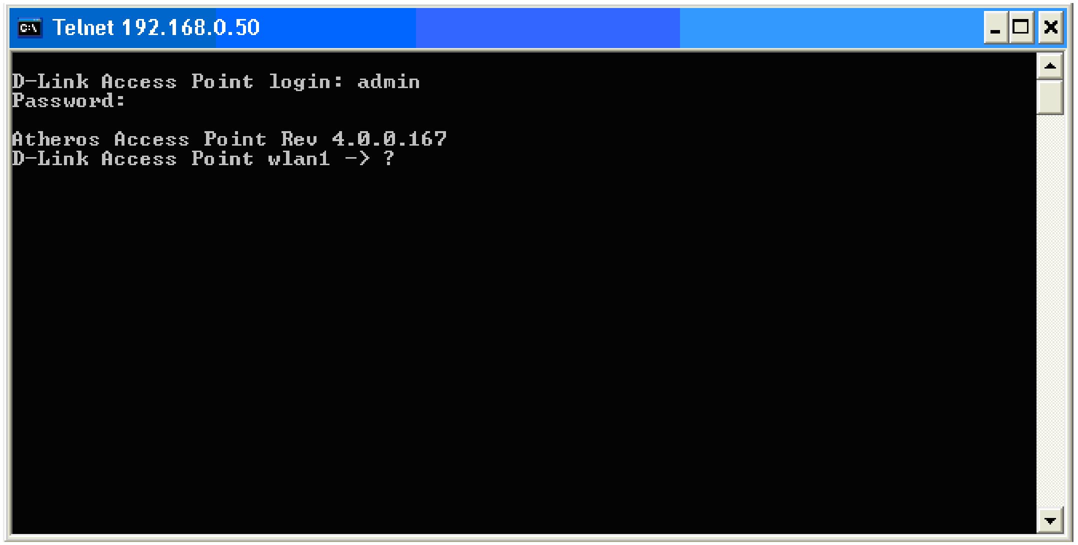
The following screen opens to indicates you have successfully logged into the DWL-2700AP.



```
D-Link Access Point login: admin
Password:

Atheros Access Point Rev 4.0.0.167
D-Link Access Point wlan1 -> _
```

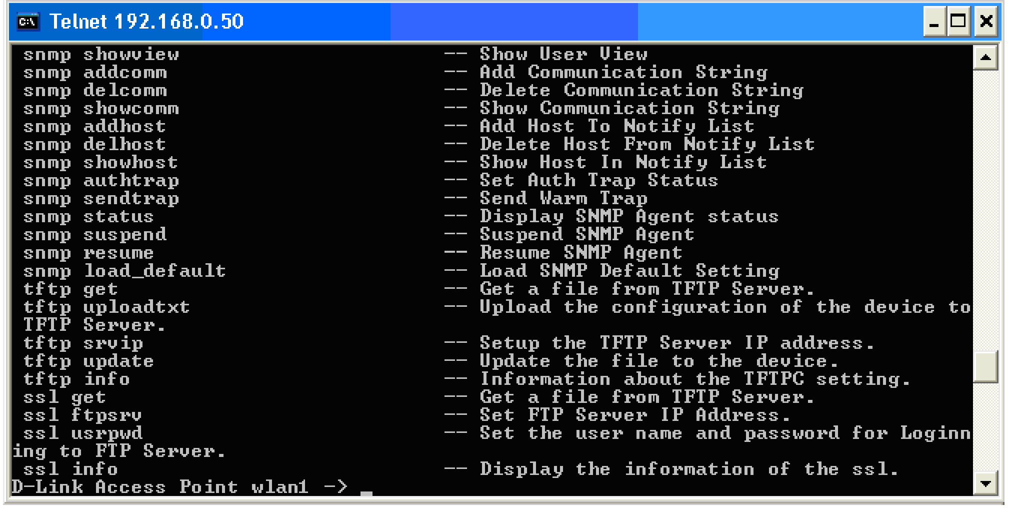
Commands are entered at the command prompt, **D-Link Access Point wlan1** – >

There are a number of helpful features included in the CLI. Entering the “**?**” command and then pressing **Enter** will display a list of all of the top-level commands. The same information can also be displayed by entering “**help**”.



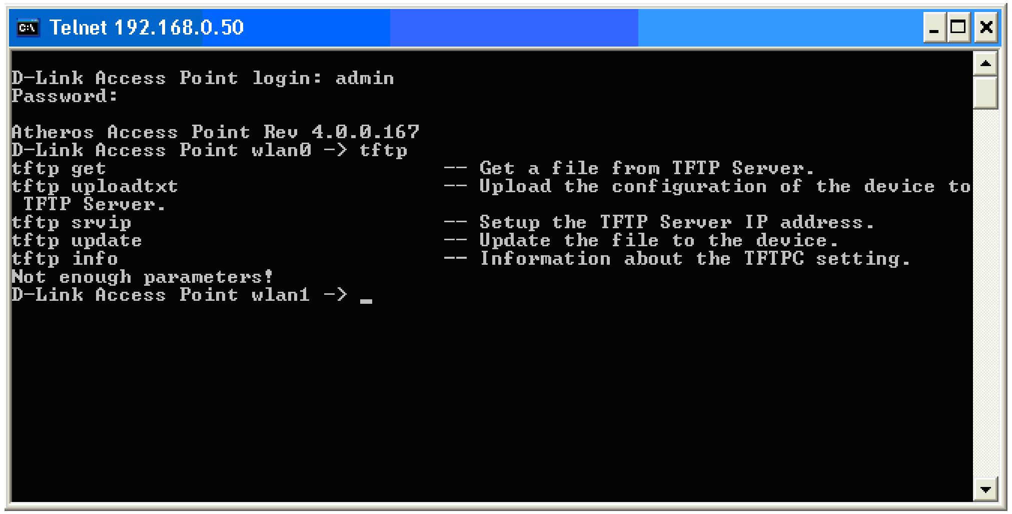
```
D-Link Access Point login: admin
Password:

Atheros Access Point Rev 4.0.0.167
D-Link Access Point wlan1 -> ?
```

Press **Enter** to see a list of all the available commands. Alternatively, you may enter “**help**” and the press **Enter**.



```
 snmp showview                      -- Show User View
 snmp addcomm                       -- Add Communication String
 snmp delcomm                       -- Delete Communication String
 snmp showcomm                      -- Show Communication String
 snmp addhost                       -- Add Host To Notify List
 snmp delhost                       -- Delete Host From Notify List
 snmp showhost                      -- Show Host In Notify List
 snmp authtrap                      -- Set Auth Trap Status
 snmp sendtrap                      -- Send Warm Trap
 snmp status                        -- Display SNMP Agent status
 snmp suspend                       -- Suspend SNMP Agent
 snmp resume                        -- Resume SNMP Agent
 snmp load_default                  -- Load SNMP Default Setting
 tftp get                           -- Get a file from TFTP Server.
 tftp uploadtxt                     -- Upload the configuration of the device to
 TFTP Server.
 tftp srvip                         -- Setup the TFTP Server IP address.
 tftp update                        -- Update the file to the device.
 tftp info                          -- Information about the TFTPC setting.
 ssl get                            -- Get a file from TFTP Server.
 ssl ftpsrv                         -- Set FTP Server IP Address.
 ssl usrpwd                         -- Set the user name and password for Loginn
ing to FTP Server.
 ssl info                           -- Display the information of the ssl.
D-Link Access Point wlan1 -> _
```

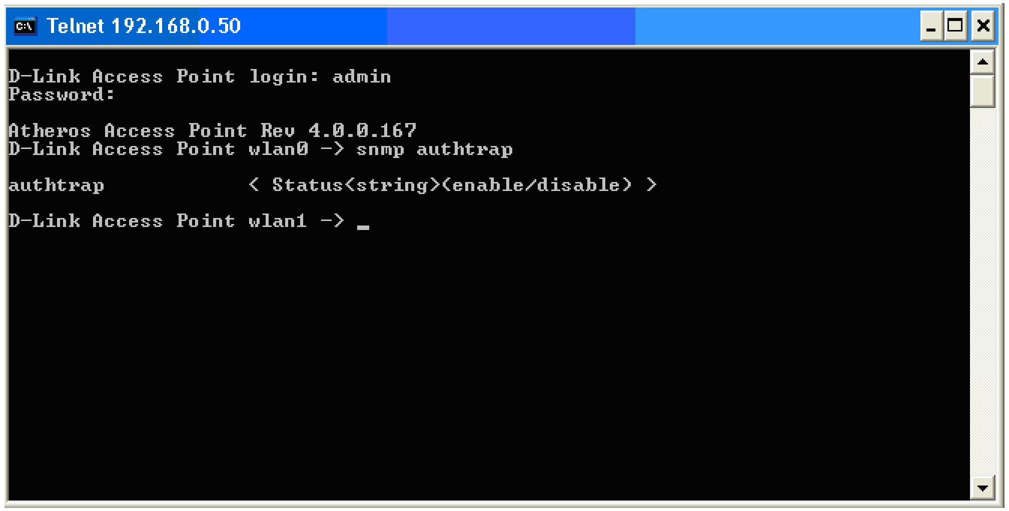
When you enter a command without all of its required parameters, the CLI will prompt you with a list of possible completions. For example, if “**tftp**” was entered, the following screen opens:



```
D-Link Access Point login: admin
Password:

Atheros Access Point Rev 4.0.0.167
D-Link Access Point wlan0 -> tftp
tftp get                            -- Get a file from TFTP Server.
tftp uploadtxt                      -- Upload the configuration of the device to
 TFTP Server.
tftp srvip                          -- Setup the TFTP Server IP address.
tftp update                         -- Update the file to the device.
tftp info                           -- Information about the TFTPC setting.
Not enough parameters!
D-Link Access Point wlan1 -> _
```

This screen displays all the possible command completions for “**tftp**”

When you enter a command without a variable or value that needs to be specified, the CLI will prompt you with further information about what is needed to complete the command. For example, if “snmp authtrap” was entered, the following screen opens:



```
D-Link Access Point login: admin
Password:

Atheros Access Point Rev 4.0.0.167
D-Link Access Point wlan0 -> snmp authtrap

authtrap             < Status<string><enable/disable> >

D-Link Access Point wlan1 -> _
```

The missing value for the “snmp authtrap**”** command, “enable/disable,” is displayed in the screen above.

2

COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.

Note: All commands are case-insensitive.

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**set login <username>**
Description	In the above syntax example, you must specify the **username**. Do not type the angle brackets.
Example Command	**set login accounting**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	**get multi-authentication [index]**
Description	In the above syntax example, you must specify an **index** to be created. Do not type the square brackets.
Example Command	**get multi-authentication 2**

: colon	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	**set antenna [1:2:best]**
Description	In the above syntax example, you must specify either **1**, **2** or **best**. Do not type the colon.
Example Command	**set antenna best**

3

UTILITY COMMANDS

Help Command:	**Function**	**Syntax**
help	Display CLI Command List	help or ?
Ping Command:	**Function**	**Syntax**
ping	Ping	ping <xxx.xxx.xxx.xxx>
Restart and Exit Commands:	**Function**	**Syntax**
set factorydefault	Restore to Default Factory Settings	set factorydefault
reboot	Reboot Access Point. It is necessary to reboot the AP after making configuration changes for those changes to take effect.	reboot
quit	Logoff	quit
Version Display Command:	**Function**	**Syntax**
version	Displays the currently loaded firmware version	version
System Status Command:	**Function**	**Syntax**
get bdtempmode	Display Monitor Board Temperature Mode	get bdtempmode
set bdtempmode	Set Monitor Board Temperature Mode (In Centigrade)	set bdtempmode [enable:disable]
get bdalarmtemp	Display Monitor Board Temperature Alarm Limitation (In Centigrade)	get bdalarmtemp
set bdalarmtemp	Set Monitor Board Temperature Alarm Limitation (In Centigrade)	set bdalarmtemp <temperature>
get bdcurrenttemp	Display Current Board Temperature (In Centigrade)	get bdcurrenttemp
set detectlightmode	Set HW Detect Light Mode	set detectlightmode [enable:disable]
Addminstration Command:	**Function**	**Syntax**
get login	Display Login User Name	get login
get uptime	Display UpTime	get uptime
set login	Modify Login User Name	set login <username>
set password	Modify Password	set password
get wlanManage	Display manage AP with WLAN Mode	get wlanManage
set wlanmanage	Set manage AP with WLAN Mode	set wlanmanage [enable:disable]
get systemname	Display Access Point System Name	get systemname
set systemname	Specify Access Point System Name	set systemname <name>
Other Command:	**Function**	**Syntax**
radar!	Simulate radar detection on current channel	radar!

4

ETHERNET COMMANDS

Get Command:	**Function**	**Syntax**
get ipaddr	Display IP Address	get ipaddr
get ipmask	Display IP Network/Subnet Mask	get ipmask
get gateway	Display Gateway IP Address	get gateway
get lcp	Display Link Integrate state	get lcp
get lcplink	Display Ethernet Link State	get lcplink
get dhcpc	Display DHCP Client State of enabled or disabled	get dhcpc
get domainsuffix	Display Domain Name Server Suffix	get domainsuffix
get nameaddr	Display IP Address Of Name Server	get nameaddr
Set Command:	**Function**	**Syntax**
set hostipaddr	Set Boot Host IP Address	set hostipaddr <xxx.xxx.xxx.xxx> Explanation:<xxx.xxx.xxx.xxx>is IP address
set ipaddr	Set IP Address	set ipaddr <xxx.xxx.xxx.xxx> Explanation: <xxx.xxx.xxx.xxx> is IP address
set ipmask	Set IP Network/Subnet Mask	set ipmask < xxx.xxx.xxx.xxx> Explanation: <xxx.xxx.xxx.xxx> is Network mask
set lcp	Set Lcp State	set lcp [0:1] Explanation:0=disable 1=enable
set gateway	Set Gateway IP Address	set gateway <xxx.xxx.xxx.xxx> Explanation: <xxx.xxx.xxx.xxx> is Gateway IP address
set dhcpc	Set DHCP Clinet State of enable or disabled	set dhcp[disable:enable]
set domainsuffix	Set Domain Name Server Suffix	set domainsuffix <suffix>
set nameaddr	Set Name Server IP Address	set nameaddr [1:2] <xxx.xxx.xxx.xxx>
set ethctrl	ethernet control Speed and FullDuplex	set ethctrl[0:1:2:3:4] Explanation: 0: Auto 1: 100M FullDuplex 2: 100M HalfDuplex 3: 10M FullDuplex 4: 10M HalfDuplex

5

WIRELESS COMMANDS

Fundamental		
Config Commands:	**Function**	**Syntax**
config wlan	Select WLAN Adapter to configure. DWL-2700AP only WLAN 1 is available for configuration. This command is not necessary.	config wlan [0:1]
Find Commands:		
find bss	Perform Site Survey, Wireless service will be disrupted	find bss
find channel	Channel spanning to select the Preferred Channel	find channel
find all	Perform Site Survey including Super G and Turbo, Wireless service will be disrupted	find all
find rogue	Find Rogue BSS	find rogue
Get Command:	**Function**	**Syntax**
get apmode	Display current AP Mode	get apmode
get ssid	Display Service Set ID	get ssid
get ssidsuppress	Display SSID Suppress Mode is enabled or disabled	get ssidsuppress
get station	Display Client Station Connection Status	get station
get wdsap	Display WDS Access Point List	get wdsap
get remoteAp	Display Remote AP's Mac Address	get remoteAp
get association	Display Association Table that indicates the information of associated client devices	get association
get autochannelselect	Display state of Auto Channel Selection feature (enabled, disabled)	get autochannelselect
get channel	Display Radio Frequency (MHz) and Channel Designation	get channel
get availablechannel	Display available Radio channels	get availablechannel
get rate	Display current Data Rate selection. Default is best.	get rate
get beaconinterval	Display Beacon Interval	get beaconinterval
get dtim	Display Delivery Traffic Indication Message Beacon Rate	get dtim
get fragmentthreshold	Display Fragment Threshold in bytes	get fragmentationthreshold
get rtsthreshold	Display RTS/CTS Threshold	get rtsthreshold
get power	Display Transmit Power Setting: Full, half, quarter, eighth, min	get power
get wlanstate	Display Wireless LAN state status (enabled or disabled)	get wlanstate
get shortpreamble	Display Short Preamble Usage state: enabled or disabled	get shortpreamble
get wirelessmode	Display Wireless LAN Mode (11b or 11g)	get wirelessmode

get 11gonly	Display 11g Only Mode operational state of enabled or disabled	get 11gonly
get antenna	Display Antenna Diversity of 1, 2, or best	get antenna
get sta2sta	Display wireless STAs to wireless STAs connect state	get sta2sta
get eth2sta	Display ethernet to wireless STAs connect state	get eth2sta
get trapsevers	Get trap server state	get trapsevers
get eth2wlan	Display Eth2Wlan Broadcast packet filter state	get eth2wlan
get macaddress	Display Mac Address	get macaddress
get config	Display Current AP Configuration Settings	get config
get countrycode	Display Country Code setting	get countrycode
get hardware	Display Hardware Revisions of WLAN Components	get hardware
get aging	Display Aging Interval in seconds	get aging
get MulticastPacketControl	Display Multicast Packet Control state	get MulticastPacketControl
get MaxMulticastPacketNumber	Display Max Multicast Packet Number	get MaxMulticastPacketNumber
get 11goptimize	Display 11g Optimization Level	get 11goptimize
get 11goverlapbss	Display Overlapping BSS Protection	get 11goverlapbss
get assocnum	Display Number Of Association STA	get assocnum
get eth2wlanfilter	Display Eth2WLAN BC & MC filter type	get eth2wlanfilter
get extendedchanmode	Display Extended Channel Mode	get extendedchanmode
get iapp	Display IAPP State	get iapp
get iapplist	Display IAPP Group List	get iapplist
get iappuser	Display IAPP User Limit Number	get iappuser
get minimumrate	Display Minimum Rate	get minimumrate
get dfsinforshow	Display DFS infor	get dfsinforshow
get wdsrssi	Display WDS Access Point RSSI	get wdsrssi
get ackmode	Display Variable Ack Time Mode	get ackmode
get acktimeout	Display Ack Time Out Number	get acktimeout
Set Command:	**Function**	**Syntax**
set apmode	Set AP Mode to Normal AP, WDS with AP Mode,WDS without AP Mode or AP Client	set apmode [ap:wdswithap:wds:apc]
set ssid	Set Service Set ID	set ssid <SSID>
set ssidsuppress	Set SSID Suppress Mode enable or disable	set ssidsuppress [disable:enable]
set autochannelselect	Set Auto Channel Selection to enable or disable	set autochannelselect [disable:enable]
set rate	Set Data Rate	set rate [best:1:2:5.5:6:9:11:12:18:24:36:48:54]
set beaconinterval	Modify Beacon Interval 20-1000	set beaconinterval [20-1000]

set dtim	Set Delivery Traffic Indication Message Beacon Rate. Default is 1	set dtim [1-255]
set fragmentthreshold	Set Fragment Threshold	set fragmentationthreshold [256-2346]
set rtsthreshold	Set RTS/CTS Threshold in bytes	set rtsthreshold [256-2346f]
set power	Set Transmit Power in predefined increments	set power [full:half:quarter:eighth:min]
set roguestatus	Set Rogue AP status	set roguestatus [enable:disable]
set roguebsstypestatus	Set Rogue AP BSS type status	set roguebsstypestatus [enable:disable]
set roguebsstype	Set ROGUE AP BSS Type	set roguebsstype [apbss:adhoc:both']
set roguesecuritystatus	Set Rogue AP Security Type status	set roguesecuritystatus [enable: disable]
set roguesecurity	Set ROGUE AP Security Type	set roguesecurity
set roguebandselectstatus	Set Rogue AP Band Select status	set roguebandselectstatus [enable:disable]
set roguebandselect	Set ROGUE AP Band Select	set roguebandselect
set wlanstate	Select the operational state of wlan: enabled or disabled	set wlanstate [disable:enable]
set shortpreamble	Set Short Preamble	set shortpreamble [disable: enable]
set wirelessmode	set wirelessmode to 11b/11g.	set wirelessmode [11a:11b:11g] NOTE:11a is not supported.
set 11gonly	Only 802.11g clients will be Allowed to connect to this BSS	set 11gonly [disable:enable]
set antenna	Set Antenna selection of 1, 2, or best	set antenna [1:2:best]
set aging	Set Aging Interval	set aging <seconds>
set channel	Select Radio Channel of Operation	set channel [1:2:3:4:5:6:7:8:9:10:11]
set eth2wlan	Enable or Disable the Eth2Wlan Broadcast packet filter feature	set eth2wlan [0:1] Explanation: 0=disable:1=enable
set sta2sta	Set wireless STAs to wireless STAs connect state (WLAN Partition)	set sta2sta [disable: enable]
set eth2sta	Set ethernet to wireless STAs connect state	set eth2sta [disable: enable]
set trapsevers	Set trap server state	set trapsevers [disable:enable]
set MulticastPacketControl	Enable or Disable Multicast Packet Control	set MulticastPacketControl [0:1] Explanation: 0=disable:1=enable
set MaxMulticastPacketNumber	Set Max Multicast Packet Number	set MaxMulticastPacketNumber [0-1024]
set extendedchanmode	Set Extended Channel Mode	set extendedchanmode [disable:enable]
set eth2wlanfilter	Set Eth2WLAN Broadcast & Multicast Filter type	set eth2wlanfilter [1:2:3] Explanation: 1=Broadcast filter: 2=Multicast filter: 3=Both of BC and MC.
set ackmode	Set Ack Mode	set ackmode [enable:disable]
set acktimeout	Set Ack Timeout Number	set acktimeout <timeout>
set iapp	Set IAPP State.	set iapp [0:1] Explanation: 0=close 1=open
set iappuser	Set IAPP User Limit Number	set iappuser [0-64]

Security		
Del Command:	**Function**	**Syntax**
del key	Delete Encryption key	del key [1-4]
Get Command:	**Function**	**Syntax**
get encryption	Display (WEP) configuration state (enabled or disabled)	get encryption
get authentication	Display Authentication Type	get authentication
get cipher	Display Encryption cipher type Explanation: Response WEP for choosing WEP Response Auto for choosing WPA-Auto Resopnse AES for choosing WPA-AES Response TKIP for choosing WPA-TKIP	get cipher
get keysource	Display Source Of Encryption Keys: Explanation: Response Flash Memory for static key Response Key Server for dynamic key Response mixed for mix static and dynamic key	get keysource
get key	Display specified WEP encryption Key	get key [1-4]
get keyentrymethod	Display Encryption Key Entry Method ASCII or Hexadecimal	get keyentrymethod
get groupkeyupdate	Display WPA Group Key Update Interval (in Seconds)	get groupkeyupdate
get defaultkeyindex	Display Active Key Index	get defaultkeyindex
get dot1xweptype	Display 802.1x Wep Key Type	get dot1xweptype
get reauthperiod	Display Manual Reauthentication Period	get reauthperiod
Set Command:	**Function**	**Syntax**
set encryption	Enable or Disable Encryption Mode	set encryption [disable: enable]
set authentication	Set Authentication Type	set authentication [open-system: shared-key: auto:8021x: WPA: WPA-PSK: WPA2: WPA2-PSK:WPA-AUTO:WAP2-AUTO-PSK]
set cipher	Set Cipher of wep, aes, tkip, or auto negotiate	set cipher [wep:aes:tkip:auto]
set groupkeyupdate	Set Group Key Update Interval (in Seconds) for TKIP	set groupkeyupdate <seconds>
set key	Used to set the specified wep key value and size	set key [1-4] default set key [1-4] [40:104:128] < value>
set keyentrymethod	Select Between ASCII or HEX encryption key format	set keyentrymethod [asciitext : hexadecimal]
set keysource	Select Source of Encryption Keys: static(flash), dynamic (server), mixed	set keysource [flash:server:mixed]
set passphrase	Modify Passphrase	set passphrase <new passphrase>
set dot1xweptype	Set 802.1x Wep Key Type	set dot1xweptype [static: dynamic]
set reauthperiod	Set Manual Reauthentication Period	set reauthperiod <xxxx> Explanation: <xxxx> is new priod.

WMM		
Get Command:	**Function**	**Syntax**
get wmm	Display WMM mode status (enabled or disabled)	get wmm
get wmmParamBss	Display WMM parameters used by STA in this BSS	get wmmParamBss
get wmmParam	Display WMM parameters used by this AP	get wmmParam
Set Command:	**Function**	**Syntax**
set wmm	Enable or Disable WMM Features	set wmm [disable:enable]
set wmmParamBss ac	Set WMM (EDCA) parameters used by STAs in this BSS	set wmmParamBss ac [AC number] [logCwMin] [logCwMax] [aifs] [txOpLimit] [acm] Explanation: AC number: 0->AC_BE 1->AC_BK 2->AC_BK 3->AC_BK Exampble: set wmmParamBss ac 0 4 10 3 0 0
set wmmParam ac	Set WMM (EDCA) parameters used by this AP	set wmmParamBss ac [AC number] [logCwMin] [logCwMax] [aifs] [txOpLimit] [acm] [ack-policy] Explanation: AC number: 0->AC_BE 1->AC_BK 2->AC_BK 3->AC_BK

6

MULTI-SSID AND VLAN COMMANDS

Get Command:	Function	Syntax
get vlanstate	Display Vlan State status (enabled or disabled)	get vlanstate
get vlanmanage	Display manage AP with VLAN Mode	get vlanmanage
get nativevlan	Display Native Vlan tag	get nativevlan
get Vlantag	Display Vlan tag	get Vlantag
get multi-state	Display Multi-SSID Mode (enabled or disabled)	get multi-state
get multi-ind-state [index]	Display Individual Multi-SSID State	get multi-ind-state [index]
get multi-ssid [index]	Display SSID of the specify Multi-SSID	get multi-ssid [index]
get multi-ssidsuppress [index]	Display SSID Suppress Mode of the specify Multi-SSID	get multi-ssidsuppress [index]
get multi-authentication [index]	Display Authentication Type for Multi-SSID	get multi-authentication [index]
get multi-cipher [index]	Display Encryption cipher for Multi-SSID	get multi-cipher [index]
get multi-encryption [index]	Display Encryption Mode for Multi-SSID	get multi-encryption [index]
get multi-keyentrymethod	Display Encryption Key Entry Method for Multi-SID	get multi-keyentrymethod
get multi-vlantag [index]	Display Vlan tag for Multi-SSID	get multi-vlantag [index]
get multi-key [index]	Display Encryption Key for Multi-SSID	get multi-key [index]
get multi-keysource [index]	Display Key Source for Multi-SSID	get multi-keysource [index]
get multi-config [index]	Display AP Configuration for Multi-SSID	get multi-config [index]
get multi-passphrase [index]	Display Passphrase for Multi-SSID	get multi-passphrase [index]
get multi-dot1xweptype [index]	Display 802.1x Wep Key Type For Multi-SSID	get multi-dot1xweptype [index]
Set Command:	**Function**	**Syntax**
set vlanstate	Enable or Disable VLAN	set vlanstate [disable:enable] Note: Must Enable Multi-SSID firstly
set vlanmanage	Set Enabled or Disable manage AP with VLAN	set vlanmanage [disable:enable] Note: Must Enable vlanstate firstly
set nativevlan	Set Native Vlan Tag	set nativevlan [1-4096]
set Vlantag	Set VLAN Tag	set vlantag <tag value>
set Vlanpristate	Set Vlan Priority State	set Vlanpristate [enable:disable]
set Vlanpri	Modify Vlan Priority	set Vlanpri [0-7]
set ethnotag	Set Primary Eth No Tag Stat	set ethnotag [enable:disable]
set multi-vlantag	Set VLAN Tag for Multi-SSID	set multi-vlantag <tag value> [index]

set multi-ethnotag	Set Individual Eth No Tag State	set multi-ethnotag [index] [disable:enable]
set multi-vlanpri	Set Vlan-Priorityi for Multi-SSID	set multi-vlanpri [pri value] [index]
set VlantagType	Modify Vlantag Type	set VlantagType [1:2]
set multi-vlantagtype	Set Vlan-Tag Typefor Multi-SSID	set multi-vlantagtype [tagType value] [index]
set multi-state	Enable or Disable Multi-SSID Features	set multi-state [disable:enable]
set multi-ind-state	Enable or Disable specifically Mulit-SSID	set multi-ind-state [disable:enable] [index]
set multi-ssid	Set Service Set ID for Multi-SSID	set multi-ssid [index] <ssid name>
set multi-ssidsuppress	Enable or Disable to broadcast SSID of Multi-SSID	set multi-ssidsuppress [disable:enable]
set multi-authentication	Set Authentication Type for Multi-SSID	set multi-authentication [open-system:shared-key:wpa:wpa-psk:wpa2:wpa2-psk:wpa-auto:wpa-auto-psk:8021x] [index]
set multi-cipher	Set Cipher for Multi-SSID	set multi-cipher [wep:aes:tkip:auto] [index]
set multi-encryption	Set Encryption Mode for Multi-SSID	set multi-encryption [disable:enable] [index]
set multi-keyentrymethod	Select Encryption Key Entry Method for Multi-SSID	set multi-keyentrymethod [hexadecimal:asciitext] [index]
set multi-vlantag [tag value] [index]	Set VLAN Tag For Multi-SSID	set multi-vlantag [tag value] [index]
set multi-key	Set Encryption Key for Multi-SSID	set multi-key default [key index] [Multi-SSID index]

set multi-keysource	Set Source Of Encryption Key For Multi-SSID	set multi-dot1xweptype [flash:server:mixed] [index]
		Explanation:
		flash=Set All Keys Will Be Read From Flash:
		server=Set All Keys Will Be Derived From Authentication Server
		mixed= Set Keys Read From Flash Or Derived From Authentication Server

set multi-passphrase	Set PassPhrase for Multi-SSID	set multi-passphrase [index] <passphrase>
set multi-dot1xweptype	Set 802.1x Wep Key Type For Multi-SSID	set multi-dot1xweptype [static: dynamic] [index]

Routing Commands (Spaning Tree Protocol)		
Set Command:	**Function**	**Syntax**
rstp getstate	Show Spanning Tree State	rstp getstate
rstp getstp	Show Spanning Tree Settings	rstp getstp
rstp getport	Show STP Port Settings	rstp getport

7

ACCESS CONTROL LIST COMMANDS

Del Command:	Function	Syntax
del acl	Delete specified Access Control List entry	del acl [1-16]
del wdsacl	Delete specified WDS ACL entry: 1-8	del wdsacl [1-8]
Get Command:	**Function**	**Syntax**
get acl	Display Access Control Setting of Enabled or disabled	get acl
get wdsacl	Display WDS Access Control List	get wdsacl
Set Command:	**Function**	**Syntax**
set acl enable	Select ACL restricted access to specified MAC addresses	set acl enable
set acl disable	Select Unrestricted access	set acl disable
set acl allow	Add specified MAC address to the allow ACL	set acl allow <xx:xx:xx:xx:xx:xx>
set acl deny	Add specified MAC address to the deny ACL	set acl deny <xx:xx:xx:xx:xx:xx>
set acl strict	Select Restricted Access, only clients with authorized MAC will communicate	set acl strict
set acl keymap	Add WEP Encryption Key mapping for MAC Address	set acl keymap <xx:xx:xx:xx:xx:xx> [1-4] set acl keymap <xx:xx:xx:xx:xx:xx> default set acl keymap <xx:xx:xx:xx:xx:xx> [40:104:128] < value>
set wdsacl allow	Add MAC Address to WDS List	set wdsacl allow <xx:xx:xx:xx:xx:xx>
IPfilter Command:	**Function**	**Syntax**
ipfilter state	Display or Set Remote IP Acl State	ipfilter state ipfilter state [accept:disable:reject]
ipfilter add	Add a IP Entry	ipfilter add <xxx.xxx.xxx.xxx>
ipfilter del	Del a IP Entry	ipfilter del <xxx.xxx.xxx.xxx>
ipfilter clear	Clear IP Pool	ipfilter clear
Ipfilter list	Display IP Pool	ipfilter list
Ethacl Command:	**Function**	**Syntax**
ethacl state	Display Or Set Ethernet Acl State	ethacl state ethacl state [accept:off:reject]
ethacl add	Add Mac <xx:xx:xx:xx:xx:xx> Entry	ethacl add < xx:xx:xx:xx:xx:xx >
ethacl del	Del Mac <xx:xx:xx:xx:xx:xx> Entry	ethacl del < xx:xx:xx:xx:xx:xx >
ethacl clear	Clear MAC Pool	ethacl clear
ethacl list	Display MAC Pool	ethacl list

Ipmanager Command:	**Function**	**Syntax**
ipmanager state	Display Or Set Remote IP Management State	ipmanager state ipmanager state [on:off]
ipmanager add	Add a IP Entry	ipmanager add <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
ipmanager del	Del a IP Entry	ipmanager del <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
ipmanager clear	Clear IP Pool	ipmanager clear
ipmanager list	Display IP Pool	ipmanager list
IGMP snooping Command:	**Function**	**Syntax**
igmp state	IGMP snooping state	igmp state [enable,disable]
igmp enable	IGMP snooping enable	igmp enable
igmp disable	IGMP snooping disable	igmp disable
igmp dump	IGMP MDB dump	igmp dump
igmp setrssi	set igmp snp rssi threshold	igmp setrssi [0-100]
igmp getrssi	get igmp snp rssi threshold	igmp getrssi
igmp setportagingtime	set igmp snp port aging time	igmp setportagingtime [0-65535]
igmp getportagingtime	get igmp snp port aging time	igmp getportagingtime
rogue Command:	**Function**	**Syntax**
rogue add	Add a Rogue Access Point Result <index> Entry	rogue add [index]
rogue del	Del a Rogue Access Point Result <index> Entry	rogue del [index]
rogue deleep	Del a Rogue Access Point Result <index> Entry	rogue deleep [index]
rogue list	Display Rogue Access Point Detection Result	rogue list
rogue listeep	Display Rogue Access Point Detection Result	rogue listeep

8

RADIUS SERVER COMMANDS

Get Command:	**Function**	**Syntax**
get radiusname	Display RADIUS server name or IP address	get radiusname
get radiusport	Display RADIUS port number	get radiusport
get accountingstate	Display Accounting Mode	get accountingstate
get accountingname	Display Accounting server name or IP address	get accountingname
get accountingport	Display Accounting port number	get accountingport
get accounting2ndstate	Display second Accounting Mode	get accounting2ndstate
get accounting2ndname	Display second Accounting server name or IP address	get accounting2ndname
get accounting2ndport	Display second Accounting port number	get accounting2ndport
get accountingcfgid	Display the configuration of Accounting now	get accountingcfgid
Set Command:	**Function**	**Syntax**
set radiusname	Set RADIUS Server name or IP address	set radiusname <DNS name::xxx.xxx.xxx.xxx> Explanation: <xxx.xxx.xxx.xxx> is IP address
set radiusport	Set RADIUS port number	set radiusport <xxxxx> Explanation: <xxxxx> is port number, default value is 1812
set radiussecret	Set RADIUS shared secret	set radiussecret
set accountingstate	Set Accounting Mode	set accountingstate [enable:disable]
set accountingname	Set Accounting name or IP address	set accountingname [xxx.xxx.xxx.xxx : servername]
set accountingport	Set Accounting port number	set accountingport <xxxxx> Explanation: <xxxxx> is port number, default value is 1813.
set accounting2ndstate	Set second Accounting Mode	set accounting2ndstate [enable:disable]
set accounting2ndname	Set second Accounting server name or IP address	set accounting2ndname [xxx.xxx.xxx.xxx : servername]
set accounting2ndport	Set second Accounting port number	set accounting2ndport <xxxxx>
set accountingcfgid	Set the configuration of Accounting now	set accountingcfgid

9

DHCP SERVER COMMANDS

Command:	Function	Syntax
dhcps help	Display DHCP Server Command Help	dhcps help
dhcps state	get DHCP Server state	dhcps state
dhcps state <on:off>	turn on or turn off DHCP Server	dhcps state [on:off]
dhcps dynamic info	get current settings	dhcps dynamic info
dhcps dynamic ip	set start ip	dhcps dynamic ip <x.x.x.x>
dhcps dynamic mask	set netmask	dhcps dynamic mask <x.x.x.x>
dhcps dynamic gw	set gateway	dhcps dynamic gw <x.x.x.x.>
dhcps dynamic dns	set dns	dhcps dynamic dns <x.x.x.x>
dhcps dynamic wins	set wins	dhcps dynamic wins <x.x.x.x>
dhcps dynamic range	set range	dhcps dynamic range [0-255]
dhcps dynamic lease	set lease time (sec)	dhcps dynamic lease [60- 864000]
dhcps dynamic domain	set domain name	dhcps dynamic domain <string>
dhcps dynamic state	set state	dhcps dynamic state [on:off]
dhcps dynamic map	get mapping list	dhcps dynamic map
dhcps static info	get setting from <0-255> to <0-255>	dhcps static info [0-255] [0-255]
dhcps static ip	set static <id> pool start ip	dhcps static <id> ip <x.x.x.x>
dhcps static mask	set static <id> pool netmask	dhcps static <id> mask <x.x.x.x>
dhcps static gw	set static <id> pool gateway	dhcps static <id> gw <x.x.x.x.>
dhcps static dns	set static <id> pool dns	dhcps static <id> dns <x.x.x.x>
dhcps static wins	set static <id> pool wins	dhcps static <id> wins <x.x.x.x>
dhcps static domain	set static <id> pool domain name	dhcps static <id> domain <string>
dhcps static mac	set static <id> pool mac	dhcps static <id> mac <xx:xx:xx:xx:xx:xx>
dhcps static state	set static <id> pool state	dhcps static <id> state [on:off]
dhcps static map	get static <id> pool mapping list	dhcps static map

Note: The DHCP server function is to assign Dynamic IP to Wireless Client devices. It doesn’t assign IP to Ethernet port.

10

SNMP COMMANDS

Command	Function	Syntax
snmp adduser	Add User To SNMP Agent	snmp adduser <Username> <GroupName> [AuthProtocol] [Authkey] [PrivProtocol] [PrivKey] Explanation: AuthProtocol: 1 Non, 2 MD5, 3 SHA Autheky: Key string or none PrivProtocl:1 none, 2 DES PrivKey: Key string or none
snmp deluser	Delete User From SNMP Agent	snmp deluser <username>
snmp showuser	Show User list In SNMP Agent	snmp showuser
snmp setauthkey	Set User Auth Key	snmp setauthkey <username> <Authkey>
snmp setprivkey	Set User Private Key	snmp setauthkey <username> <Privkey>
snmp addgroup	Add User Group	snmp addgroup <GroupName> [Security Level] <ReadView> <WriteView> <NotifyView> Explanation: Security Level:1 no_auth no_priv, 2 auth no_priv, 3 auth priv ReadView: <string> or NULL for None WriteView: <string> or NULL for None NotifyView: <string> or NULL for None
snmp delgroup	Delete User Group	snmp delgroup <GroupName >
snmp showgroup	Show SNMP Group Settings	snmp showgroup
snmp addview	Add User View	snmp addview <ViewName> <OID > [Type] Explanation: ViewName: <string> OID:<string> Type:1: included, 2: excluded
snmp delview	Delete User View	snmp delview <ViewName> <OID > Explanation: ViewName: <string> OID: <string> or all for all OID
snmp showview	Show User View	snmp showview
snmp editpubliccomm	Edit public communication String	snmp editpubliccomm <publicCommunityString>
snmp editprivatecomm	Edit private communication String	snmp editprivatecomm <privateCommunityString>

snmp addcomm	Add Communication String	snmp addcomm <CommunityString> <ViewName> [Type] Explanation: CommunityString: <string> ViewName:<string> Type:1: Read-Only, 2: Read-Write
snmp delcomm	Delete Community String	snmp delcomm <CommunityString>
snmp showcomm	Show Community String Table	snmp showcomm
snmp addhost	Add Host To Notify List	snmp addhost TrapHostIP<string> [SnmpType] [AuthType] <AuthString> Explanation: TrapHostIP: <string> SnmpType: 1: v1 2: v2c 3: v3 AuthType: 0: v1_v2c 1: v3_noauth_nopriv 2: v3_auth_nopriv 3 v3_auth_priv> AuthString: <string>, CommunityString for v1,v2c or UserName for:v3
snmp delhost	Delete Host From Notify List	snmp delhost <TrapHostIP >
snmp showhost	Show Host In Notify List	snmp showhost
snmp authtrap	Set Auth Trap Status	snmp authtrap [enable:disable]
snmp sendtrap	Send Warm Trap	snmp sendtrap
snmp status	Display SNMP Agent status	snmp status
snmp lbsstatus	Show the status of LBS	snmp lbsstatus
snmp lbsenable	Enable the function of LBS	snmp lbsenable
snmp lbsdisable	Disable the function of LBS	snmp lbsdisable
snmp lbstrapsrv	Set the LBS trap server ip	snmp lbstrapsrv <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> is the lbs trap server ip.
snmp showlbstrapsrv	Show the LBS trap server ip	snmp showlbstrapsrv
snmp suspend	Suspend SNMP Agent	snmp suspend
snmp resume	Resume SNMP Agent	snmp resume
snmp load_default	Load SNMP Default Settings	snmp load_default
get trapstate	Get trap server state	get trapstate
set trapstate	Set trap server state	set trapstate [disable:enable]

11

TIME DISPLAY & SNTP COMMANDS

Command:	Function	Syntax
timeofday	Displays the Current Time of Day	timeofday Note: Need to set up SNTP/NTP server firstly
Get Command	**Function**	**Syntax**
get sntpserver	Display SNTP/NTP Server IP Address	get sntpserver
get tzone	Display Time Zone Setting	get tzone
Set Command	**Function**	**Syntax**
set sntpserver	Set SNTP/NTP Server IP Address	set sntpserver <xxx.xxx.xxx.xxx> Explanation: <xxx.xxx.xxx.xxx> is IP address
set tzone	Set Time Zone Setting	set tzone [0=GMT]

12

TELNET & SSH COMMANDS

TFTP&FTP Commands:

Command:	Function	Syntax
tftp get	Get a file from TFTP Server.	tftp get Filename<string>
tftp uploadtxt	Upload the configuration of the device to TFTP Server.	tftp uploadtxt Filename<string>
tftp srvip	Setup the TFTP Server IP address.	tftp srvip <xxx.xxx.xxx.xxx>
tftp update	Update the file to the device.	tftp update
tftp info	Information about the TFTPC setting.	tftp info
get telnet	Display Telnet Status of current login, number of login attempts, etc.	get telnet
get timeout	Display Telnet Timeout in seconds	get timeout
set telnet	Set Telnet Access/SSL Mode to enabled or disabled	set telnet <0:1:2> Explanation: 0=disable telnet and enable SSL 1=enable telnet and disable SSL 2=disable both telnet and SSL
set timeout	Set Telnet Timeout in seconds, 0 is never and 900 seconds is the maximum <0-900>	set timeout <0-900>
ftp	Software Update TFP File Via FTP	ftp <xxx.xxx.xxx.xxx>
ftpcon srvip	Set The FTP Server IP Address	ftpcon srvip <xxx.xxx.xxx.xxx>
ftpcon downloadtxt	Update configure file From FTP Server	ftpcon downloadtxt
ftpcon uploadtxt	Set The File And Upload To Server in text File	ftpcon uploadtxt
ssl srvip	Set FTP Server IP Address	ssl srvip <xxx.xxx.xxx.xxx>
ssl usrpwd	Set The User Name And Password For Loginning To FTP Server	ssl usrpwd <usrname> <password>
ssl ftpget	Display File From FTP Server	ssl ftpget <cert file> <key ca file>
ssl info	Display The Information Of The SSL	ssl info

SSH Commands

Command:	Function	Syntax
ssh showuser	Show SSH User	ssh showuser
ssh loaddefault	Load SSH Default Setting	ssh loaddefault
ssh showalgorithm	Show SSH Algorithm	ssh showalgorithm

ssh setalgorithm	Set SSH Algorithm	ssh setalgorithm [0 -12] [enable/disable] Explanation: Algorithm: 0:3DES 1:AES128 2:AES192 3:AES256 4:Arcfour 5:Blowfish 6:Cast128 7:Twofish128 8:Twofish192 9:Twofish256 10:MD5 11:SHA1 12:Password) Example: 1. Disable 3DES algorithm support ssh setalgorithm 0 disable

13

SYSTEM LOG & SMTP COMMAND

SYSTEM LOG Commands		
Get Command	**Function**	**Syntax**
get syslog	Display Syslog Information	get syslog
Set Command	**Function**	**Syntax**
set syslog	Set sysLog setting	set syslog remoteip <xxx.xxx.xxx.xxx> set syslog remotestate [0:1] set syslog localstate [0:1] set syslog clear all Explanation: 0=disable:1=enable
Log Command	**Function**	**Syntax**
pktLog	Display Packet Log	pktLog

SMTP Commands		
Command	**Function**	**Syntax**
smtp	SMTP Clicient Utility	smtp <xxx.xxx.xxx.xxx>
Get Command	**Function**	**Syntax**
get smtplog	Display SMTP With Log Status	get smtplog
get smtpserver	Display SMTP Server(IP Or Name)	get smtpserver
get smtpsender	Display Sender Account	get smtpsender
get smtprecipient	Display Recipient Email Address	get smtprecipient
Set Command	**Function**	**Syntax**
set smtplog	Set SMTP With Log Status	set smtplog [0:1] Explanation: 0=disable 1=enable
set smtpserver	Set SMTP Server	set smtpserver <xxx.xxx.xxx.xxx>
set smtpsender	Set Sender Account	set smtpsender <sender>
set smtprecipient	Set Recipient Email Address	set smtprecipient <emailaddr>

14

FIRST-TIME CONFIGURATION EXAMPLES

The following AP configuration examples are provided to help first-time users get started. The user commands are in **bold** for easy reference.

Many users will want to set a new IP address for the DWL-2700AP. This will also require setting an IP mask and a Gateway IP address. The following is an example in which the AP's default IP address of 192.168.0.50 is changed to 192.168.0.55.

```
D-Link Access Point wlan1 -> set ipaddr 192.168.0.55
IP Address: 192.168.0.55
D-Link Access Point wlan1 -> set ipmask 255.255.255.0
IP Subnet Mask: 255.255.255.0
D-Link Access Point wlan1 -> set gateway 192.168.0.254
Gateway IP Address: 192.168.0.254
D-Link Access Point wlan1 -> set channel 6
Radio Frequency: 2437 MHz (IEEE 6)
D-Link Access Point wlan1 -> set ssid myAP-2700
```

Once the user has determined what type of authentication is best for their wireless network, follow the appropriate instructions below.

The following is an example in which authentication is set to Open System.

```
D-Link Access Point wlan1 -> set authentication open-system
Authentication Type: Open-System
D-Link Access Point wlan1 -> set encryption disable
Encryption: Disabled
```

The following is an example in which the authentication is set to Shared-Key.

```
D-Link Access Point wlan1 -> set authentication shared-key
Authentication Type: Shared-Key
D-Link Access Point wlan1 -> set key 1 40 1234567890
Shared Key 1, size 40: 1234567890
D-Link Access Point wlan1 -> set key 1 default
Default Key: 1
D-Link Access Point wlan1 -> set encryption enable
Encryption: Enabled
```

The following is an example in which the authentication is set to WPA-PSK.

```
D-Link Access Point wlan1 -> set authentication wpa-psk
Authentication Type: WPA-PSK
D-Link Access Point wlan1 -> set encryption enable
Encryption: Enabled
D-Link Access Point wlan1 -> set cipher auto
Cipher selection: AUTO
D-Link Access Point wlan1 -> set passphrase
Old Passphrase->
New Passphrase-> **********
Type passphrase again to confirm-> **********
Passphrase confirmed
```

The following is an example in which the authentication is set to WPA.

```
D-Link Access Point wlan1 -> set authentication wpa
Authentication Type: WPA
D-Link Access Point wlan1 -> set encryption enable
Encryption: Enabled
D-Link Access Point wlan1 -> set cipher auto
Cipher selection: AUTO
D-Link Access Point wlan1 -> set radiusname 192.168.0.99
RADIUS server name: 192.168.0.99
D-Link Access Point wlan1 -> set radiussecret
Old RADIUS shared secret->
New RADIUS shared secret-> **********
Type RADIUS secret again to confirm-> **********
RADIUS shared secret confirmed
D-Link Access Point wlan0 -> set keysource server
Key Source: server
```

Once the user has set up the AP to their satisfaction, the device must be rebooted to save settings.

```
D-Link Access Point wlan1 -> reboot
```