# OmniAccess™ Reference AOS-W System Reference

# Copyright

Copyright © 2005 Alcatel Internetworking, Inc. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

#### Trademarks

AOS-W, OmniAccess 4304, OmniAccess 4308, OmniAccess Wireless LAN, OmniAccess 6000, OmniAccess AP60, OmniAccess AP61, and OmniAccess AP 70 are trademarks of Alcatel Internetworking, Inc. in the United States and certain other countries.

Any other trademarks appearing in this manual are owned by their respective companies.

## Legal Notice

The use of Alcatel Internetworking, Inc. switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel Internetworking, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.

	Preface	xix
	An Overview of this Manual	xix
	Related Documents	xx
	Text Conventions	xx
	Contacting Alcatel	xxi
Part 1	Overview	. 1
Chapter 1	Overview	. 3
	Key Features	. 3
	Wireless Users	. 3
	Wired Port 802.1x Authentication	. 3
	Enhanced Location Services	. 4
	Web Management Interface Enhancements	. 4
	Enhanced Network Monitoring Interface	. 4
	SNMPv3	. 4
	Remote Thin AP	. 4
	Auto-Blacklist Firewall Extended Action	. 5
	Enhanced AP-Switch Discovery and Alcatel	-
		. 5
	Multicast Configuration	. 8
Chapter 2	Management Options	. 9
	Command-Line Interface	. 9
	Web Interface	. 9
	General Screen Elements	10
	Page Elements	11
Chapter 3	Command Line Basics	13
	Connecting to the Switch	13
	Local Serial Console	13
	Local or Remote Telnet	14
	Logging In	15
	Access Modes	15
	Command Context	16
	Saving Configuration Changes.	17
	Viewing the Configuration	1/
	Command Completion	10 10
		10 12
	Command History	19
	Command Line Editing	20
	Command Syntax	20



Part 2	Design and Planning	23
Chapter 4	<b>RF Design</b> The Alcatel RF Plan Tool         Getting Started         System Requirements for Standalone RF Plan         Installing RF Plan         Launching RF Plan         RF Plan Basics         Page Summary         Page Fields         Navigation         Applying and Saving         Next Step Button         Opening Screen         Using RF Plan         Task Overview         Planning Requirements         Adding a New Building to the Plan         Planning Pages         Locating Devices	25 26 26 27 27 27 29 29 29 30 31 31 32 32 41 52
Chapter 5	Security Options Default Open Ports AOS-W Security Options User Roles Role Design Role Configuration Firewall and Traffic Policies Introduction to Firewall and Traffic Policies Configuring Traffic Policies Access Control Lists Standard ACLs Extended ACLs Extended ACLs Ethertype ACLs Authentication and Accounting Servers LDAP Internal Authentication Database Accounting	55 56 59 60 60 62 62 63 70 71 72 72 73 77 82

	Authentication Methods	. 83
	802.1x Authentication	. 84
	VPN Authentication	. 88
	Captive Portal Authentication	. 89
	MAC Address Role Mapping	. 91
	Stateful 802.1x	. 92
	SSID Role Mapping	. 94
	Encryption Type Role Mapping	. 95
	Advanced Authentication.	. 96
	Configuring VPN Settings	. 97
		. 97
	РРТР	100
	VPN Dialer Configuration	101
	VPN Server Emulation.	104
	Advanced Authentication.	105
	SecureID Token Caching	106
	Firewall Settings	107
	Advanced Security Options	109
	Service Aliases	109
	Source/Destination Aliases	110
	Bandwidth Contracts	112
	NAT Pools	112
	Time Bange	113
	Additional Information	113
	Encryption	114
	Authentication	116
	Supported VPN Clients	117
	Configuring I 2TP and IPSec	118
Chapter 6	Common Tasks	123
	Basic Network Configuration.	123
	VLANs	123
	Port Trunks	125
	Spanning Tree	125
	Making Configuration Backups	126
	Creating an On-System Backup	126
	Saving to a New Location	127
	Restoring the Configuration File	128
	Annotating Configuration Files	128
	Upgrading the AOS-W Software	129
	Reset Configuration to Defaults	133
Chapter 7	Air Management	125
Snupier 1		155
	Required Components	135
	Wireless LAN Classification	136
	AP Classifications	136
	Wireless Client Station Classifications	137



	Enforcement Policies		137
	AP Policies		137
	Wireless Client Station Policies		141
	Global Policies	•	143
	Statistics Events	•	143
	General WMS Attributes		144
	AiroPeek Support for Packet Capture		146
	Starting Packet Capture	•	146
	The AiroPeek Application	•	147
	Stopping Packet Capture	•	148
	Remediation with Sygate	·	148
Chapter 8	802.1x Client Setup		151
1	PEAP or TLS for Windows 2000		152
	Prepare the Operating System	•	152
	Configure the Service	•	152
	Validate the User Credentials	•	152
	PEAP or TLS for Windows XP	•	160
	Cisco-PEAP for Windows XP	•	162
	Prenare the Operating System	•	162
	Enable Wireless Zero Configuration	•	162
	Configure the Cisco ACU	•	164
	Configure the Wireless Network Connection	•	167
	Validate the User Credentials	:	172
01 0	Resis Continuetion		4 <del>7</del> F
Chapter 9	Basic Switch Configuration		175
	General Configuration	•	175
	Configuring the Switch Role		175
	Configuring the Switch/Loopback IP Address .		176
	Mobility Configuration		177
	Wi-Fi MUX Configuration		177
	MUX CLI Commands	•	179
	MUX Server CLI Commands	•	179
	Setting the 802.11d Regulatory Domain	•	180
	Configuring Time Zones	•	180
	Configuring NTP Servers	•	180
	Port Configuration	•	181
	Port Selection Options	•	181
	Port Selection	•	182
	Port Configuration Options	•	183
	VLAN Configuration	·	184
	View Current VLAN Configuration	•	185
		•	185
		•	186
	IP Route Configuration.	·	187
	VRRP Configuration	·	188

	Operation	190 191 191 191 192 192 194
Chapter 10	802.1x Configuration	195
	Background       Definitions and Common Abbreviations         Definitions and Common Abbreviations       Configuring the Switch for 802.1x         Creating an Authentication Server Instance       Creating an Authentication Server Instance         Assigning Default Roles       Configuring the 802.1x State Machine         Configuring the 802.1x State Machine       Configuring the 802.1x State Machine         Certificates       Certificates         Introduction to Server, Client, and CA       Certificates         Obtaining A Certification Authority (CA)       Certificate         Obtaining a Server Certificate       Obtaining a Client Cortificate	195 196 197 197 201 204 212 212 212 212 214 217 224
	802.1x Configuration under Microsoft Pocket PC.         Configuration using Pocket PC Embedded         Supplicant         Export Trusted Certification Authority         Install Certificate Authority         Configure Wireless Settings         Login to Wireless Network         Configuration using Funk Odyssey Client         Configuration function         Odyssey Client Configuration         Trusted Servers Configuration         Profile Configuration         Networks Configuration         Networks Configuration         Push to Device         Captive Portal Certificates with Intermediate         CAs	234 230 231 232 232 232 233 233 233 234 234 234 234
Chapter 11	802.1x Solution Cookbook	237
	Physical Lopology	238



	Wireless Network Operation	238
	Wireless Laptops	238
	Printers	242
	OmniAccess 6000 Switch Configuration	242
	Firewall Policies.	242
	User Role Configuration	244
	Authentication Parameters	245
	VLAN and IP Address Configuration	246
	Wireless Configuration	247
	AP Configuration	248
	Microsoft Active Directory Server Configuration	248
	Remote Access Permission	248
	Windows Group Membership Configuration	249
	Group Policy Configuration	249
	Microsoft Internet Authentication Server	
	Configuration	251
	BADIUS Client Configuration	251
	Policy Configuration	251
	Microsoft Windows XP Client Configuration	253
	Microsoft PocketPC 2003 Client Configuration	254
	Export Trusted Cartification Authority	254
	Install Cortificate Authority	254
	Configure Wireless Settings	255
	Login to Wireless Detwork	255
	Microsoft Poquiroment	250
		250
Chapter 12	Switch Management Configuration	257
	SNMP Configuration Using Web Ul.	257
	SNMP Configuration Using The CLL	259
	Configuring SNMPv3 Users	260
	Configuring Administrative Access Using	200
	Web UI	261
	Adding and Changing Administrative Access	201
	Using the CLI	265
	Adding Auth Servers	267
		267
	Configuring Logging Using Web III	268
	Configuring Logging Using Web Of	270
		270
Chapter 13	Wireless LAN Configuration	273
-	Wireless I AN Configuration	273
	Wireless LAN Network (SSID) Configuration	273
	Wireless LAN Configuration	273
	Wireless LAN Configuration	273 274 274
	Wireless LAN Comgutation         Wireless LAN Network (SSID) Configuration         Adding a New SSID         Adjusting Radio Parameters         Using ABM	273 274 279 284
	Wireless LAN Comparation	273 274 279 284 284

Chapter 14	Radio Resource Management	289
	Introduction	289
	Calibration	289
		291
	Self-Healing	291
	Client and AP DoS Protection	292
	Configuration of RF Monitoring	295
	Coverage Hole Detection	295
	Interference Detection	297
	Event Threshold Configuration	298
	Advanced Parameters	301
Chapter 15	Intrusion Detection Configuration	305
	Wireless LAN Intrusion Detection	305
	Rogue AP	307
	Denial of Service	308
	Rate Analysis.	308
		310
		311
	Station Disconnection Detection	312
	EAP Handshake Analysis	313
	Sequence Number Analysis	314
	AP Impersonation Protection	315
	Signature Detection	316
	Wireless LAN Policies	320
	Ad-hoc Network Protection	320
	Wireless Bridge Detection	321
	Wisconfigured AP Protection	321
	Multi-Tenancy Policies and Honeypot Defense	323
	MAC OUI Checking	325
Chapter 16	Authentication Server	
		327
		327
	Configuring RADIUS Servers with Web UI	328
	Configuring Attributes	330
	Configuring I DAP Servers with Web UI	333
	Adding a Server Rule	334
	Configuring the Internal Authentication Database	0.05
		335
	Configuring 802 1x Authentication with Web UI	220
	Configuring VPN Authentication with Web UI	339



	Configuring Captive Portal Authentication with
	Web UI
	Configuring MAC Address Role Mapping with
	Web UI
	Configuring Statetul 802.1x for Third Party
	Access Points
	SSID Bole Mapping 345
	Encryption Type Bole Mapping
	Configuring Advanced Conditions
	Configuring General AAA Settings Using the CLI 348
	Configuring RADIUS Servers Using the CLI 348
	Server Rules
	Configuring LDAP Servers Using the CLI 350
	Server Rules
	Configuring the Internal Authentication Database
	Configuring RADIUS Accounting Using the CLL 353
	Adding 802.1x Authentication Using the CLI 354
	Configuring VPN Authentication Using the CU 357
	Configuring Captive Portal Authentication
	Using the CLI
	Configuring MAC Address Role Mapping
	Using the CLI
	Configuring Stateful 802.1x Using the CLI 359
	AP/Server Configuration for Stateful 802.1x 360
	Role Mapping
	SSID Role Mapping
	Encryption Type Role Mapping
	Notes on Advanced AAA Features
Chattan 17	IAS Somer Configuration 267
Chapter 17	IAS Server Configuration
	Starting the IAS Server
	Creating NAS Client Entries
	Creating Remote Access Policies
	Adding a User
Chapter 18	Firewall Configuration
-	Setting Policies Using Web Ul
	Aliases
	Defining Service Aliases
	Defining Source and Destination Aliases 383
	Firewall Policies

	Defining Roles Using Web UI.       Role Design         Role Design       Configuring Roles         Configuring Roles       Setting Policies Using the CLI         Defining Service Aliases       Defining Source and Destination Aliases         Defining Roles       Setting Policies         Standard ACLs       Setting Policies	389 389 390 394 394 396 396 398 398 398 398 398
	Extended ACLs	399 399 399
Chapter 19	Captive Portal Setup         Overview         Add Users to the Database.         Configure RADIUS Server Information         Apply a Server to Captive Portal.         Customize the Logon Role         Allow Guest Access.         Configure Other User Roles         Configuring Role Derivation         Import a Server Certificate         Customize the Login Screen         Sample Configuration         Show Commands	401 402 403 404 405 408 409 410 411 413 414 415
Chapter 20	Setting Access Rights         Introduction         Defining Alias'         Defining Service Alias'         Defining Destination Alias'         Creating Session ACLs and Roles         Creating Session ACLs For Users         Creating Session ACLs For Users         How Role Derivation Works         Show Commands	419 420 420 420 421 421 421 422 422 422 424
Chapter 21	Access Point Setup.	425 426 426 426 427 427



	AP Provisioning	428
	Plug and Play	428
	Simplified AP Provisioning	429
	AP Programming Mode	430
	Manual AP Provisioning	436
	AP Reprovisioning	436
	Accessing the AP Boot Prompt.	437
	Initial Configuration	441
	Advanced AP Configuration.	444
	GRE Tunnel Configuration.	453
	Wireless LAN Switch Setup for APs	454
	Configuration Profiles	454
	AP Attribute Commands	459
	Wireless Client Station Attributes	462
	Order of Precedence for Profile Attributes	463
	CLI Configuration Examples	465
	Viewing AP Attribute Settings	469
	Viewing AP Information and Statistics	400
	AP Poprovisioning	471
		470
		400
Chapter 22		483
	Prerequisites	483
	Data Used In The Examples	484
	Network Setup	484
	RADIUS Server Setup	485
	Internal Database Setup	486
	L2TP IPSec VPN Server Setup	487
	Alcatel Switch VPN Dialer Setup	488
	VPN Dialer	490
	Before You Begin	490
	Downloading the Client	490
	Installation	494
	Connecting With VPN	497
	Alcatel VPN Dialer Features	498
	Troubleshooting	500
	Generating a Self-Distributable Alcatel Dialer	502
Chapter 23	VPN Configuration	505
	Configuring IPSec Using Web UI	506
	Adding Address Pools	508
	Adding IKE Shared Secrets	508
		509
	12TP	510
	Configuring PPTP Using Web UI	510
	Configuring The VPN Dialer Using Web UI	511
	Configuring VPN Server Emulation Using Web U	51/
	Configuring Vint Server Linuation Using Web UL.	514
	configuring becare in token caching using web UL.	515

	Configuring IPSec Using the CLI Configuring PPTP Using the CLI Configuring the VPN Dialer Using the CLI Configuring VPN Server Emulation Using the CLI Configuring SecureID Token Caching Using Web UI VPN Quick Start Guide Requirements From Customer Network Topology In Examples	516 517 518 519 520 521 521 521
	Setting Up a VPN	521 525 530 530 537
Chapter 24	Switch Maintenance	543
	Switch Level MaintenanceImage ManagementReboot SwitchReboot Peer Supervisor CardClear ConfigSynchronizeBoot ParametersBoot ParametersCopy FilesCopy LogsCopy Crash FilesBackup FlashDelete FilesWireless LAN MaintenanceRebooting Access PointsManaging the WMS DatabaseCaptive Portal MaintenanceLustomizing the Login PageUpload CertificateUpload Custom Login Pages	543 543 544 545 546 546 547 547 549 550 551 552 555 555 556
Part 3	Monitoring and Troubleshooting.	559
Chapter 25	Monitoring the Wireless         Environment         Network Monitoring         Switch Monitoring         Sample Monitoring Information         Events         Creating Custom Reports	561 562 563 564 573 575



Т

	Wireless LAN Monitoring57Debug Information57Creating Custom Logs57Reports57Example Report: Rogue APs57AP Reports57Custom Reports58
Chapter 26	Firewall Logging583Log Entries (alphabetical)583
Chapter 27	Troubleshooting AOS-W       587         Basic Connectivity       583         General       583         Client cannot find AP       583         Client finds AP, but cannot associate       593         Client associates to AP, but higher-layer       300         authentication fails       593         Client associates/authenticates, but has       593         Client associates/authenticates, but has       593         Client initially has network connectivity,       594         Client has network connectivity,       594         Client has network connectivity, then loses       597         Client experiences poor performance       593         Client experiences poor performance       594         Client experiences poor performance       597         Client experiences poor performance       597         Client experiences poor performance       597         Authentication       600         802.1x       601         Sample Packet Captures       601         Probe Response Frame       611         Broadcast Probe Request Frame       612         Probe Response Frame       613         802.11 Authenticate Frame       614         802.11 Authenticate Response (Success)
Chapter 28	Diagnostic Tools

	Network Utilities       6         Ping       6         Traceroute       6         General Information       6         Contacting Technical Support       6         Access Point Diagnostics       6         Received Configuration       6         Software Status       6         Debug Log       6         Web Diagnostic       6	527 527 528 628 628 628 628 629 629 630 630 631
Part 4	Command Reference	333
Chapter 29	AOS-W Commands 6	35
	Understanding the Command Line Interface	635 636 637 639 641 645 672



aaa Commands	675
aaa xml-api client	696
adp Commands	696
ads Commands	697
ap Commands	698
arm Commands	699
arp	701
banner motd	701
clock Commands	702
crypto Commands	703
database synchronize	712
destination	713
dot1x Commands	713
enable	720
encrypt	721
firewall Commands	721
foreign-agent	725
home-agent	726
hostname	727
Interface Commands	728
IP Commands	737
key	743
location	744
logging Commands	744
loginsession timeout	745
mac-address-table static	745
master-redundancy	746
masterip	747
mgmt-role	748
mgmt-user	749
mobagent	750
mobility	750
mobility-local	753
mobmaster primary-subnet	754
mux-address	755
mux-vlan	755
netdestination	756
newbury	757
no	757
ntp server	764
packet-capture-defaults	765
ping	767
pptp	767
program-ap	768
prompt	768
rap-wml	769
router	771
sapm	772

	shutdown	74
	site-survey	74
	snmp-server	77
	spanning-tree	78
	stm	30
	syscontact	38
	systemation	38
	telnet cli.	39
	time-range 79	30
	traceroute 70	30 31
	trusted 70	22
		22
	uup-port	ອ∠ ວວ
		92 74
		94 20
		96
		98
		98
	vpn-dialer	21
	vrrp	)3
	web-server	)5
	web-ui	7
	wms	7
Chapter 30	Action Commands 81	9
	User Mode Commands	19
	Switch Management Commands 82	20
	Layer 2/Layer 3 Commands	20
	Privileged Mode Commands	21
	Switch Management Commands 82	21
	Layer 2/Layer 3 Commands	24
	Air Management Commands	25
	Authentication Commands	28
	Clear Commands	30
	Debug Commands	31
	Panic Commands	32
	Screen Display Commands	32
Chapter 31	Show Commands 83	33
	General Switch Management	
	Commands	33
	Switch Management Commands 83	33
	Configuration Manager Commands 83	39
	Layer 2/Layer 3 Commands	40
	Layer 2 Commands	40
	Layer 3 Commands	43
	DHCP Commands	45
	Interface Commande	10



н

	Local Database Commands	853
,	VPN Commands	854
	IPSec Commands	854
	L2TP Commands	856
	VPN Dialer Commands	859
	PPTP Commands	860
	Mobility Commands	861
	Air Management Commands	872
	Air Monitor Commands	872
	WMS Commands	881
	Site Survey Commands	884
	Station Management Commands	885
	Access Point Management Commands	887
	Alcatel Soft AP Commands	887
	Authentication Commands	891
	General Authentication Commands	891
	IEEE 802.1x Commands	894
	Accounting, Authentication, Authorization	896
	Local Database Commands	902
	Dialer Commands	902
	Access Lists Commands	903
I	MUX Commands	905
I	Enhanced Show Commands	906
Part 5	Appendices	909
	Glossarv	911

# Preface

This preface includes the following information:

- An overview of the sections in this manual
- A list of related documentation for further reading
- A key to the various text conventions used throughout this manual
- Alcatel support and service information

#### An Overview of this Manual

This manual is for network administrators and operators responsible for configuring and monitoring the Alcatel Wireless LAN Switch. The manual is organized as follows:

Part 1, "Overview"

Explains the Alcatel Wireless LAN Switch interfaces, including the Command-Line Interface (CLI) and the Web UI.

Part 2, "Design"

Explains the basic network design issues in adding a Wireless LAN switch to a network.

Part 3, "Configuration"

Explains the features that can be configured for Alcatel Wireless LAN switches.

Part 4, "Monitoring"

Explains how Alcatel Wireless LAN switches are managed and maintained.

Part 5, "Common CLI Commands"

Explains the CLI syntax for commands commonly used.

Part 6, "Appendix"

Includes a glossary of terms used in this document.

#### **Related Documents**

The following items are part of the complete documentation for the Alcatel system:

- Alcatel Wireless LAN Switch Installation Guides (OmniAccess 4308, Omni-Access Wireless LAN, and OmniAccess 6000)
- Alcatel AOS-W User Guide
- Alcatel AP Installation Guides (AP60/61 and AP70)

#### **Text Conventions**

The following conventions are used throughout this manual to emphasize important concepts:

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following:
	<ul> <li>Sample screen output</li> <li>System prompts</li> <li>Filenames, software devices, and certain commands when mentioned in the text.</li> </ul>
Commands	In the command examples, this bold font depicts text that the user must type exactly as shown.
Button	The name of the object (button, link, etc.) on the interface that you click.

TABLE P-1 Text Conventions

#### TABLE P-1 Text Conventions

<arguments></arguments>	In the command examples, italicized text within angle brackets represents items that the user should replace with information appropriate to their specific situation. For example:
	<pre># send <text message=""></text></pre>
	In this example, the user would type "send" at the system prompt exactly as shown, followed by the text of the message they wish to send. Do not type the angle brackets.
[ Optional ]	In the command examples, items enclosed in brackets are optional. Do not type the brackets.
{ Item A I Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

## **Contacting Alcatel**

#### Web Site

Main Site	http://www.alcatel.com
-----------	------------------------

Support http://www.alcatel.com/enterprise

#### Telephone Numbers

- Main US/Canada (800) 995-2612
- Main Outside US (818) 880-3500



**OmniAccess Reference: AOS-W System Reference** 



# Overview





**OmniAccess Reference: AOS-W System Reference** 

# Chapter 1 Overview

The AOS-W 2.2 Interface Reference is organized by product feature for the Alcatel Wireless LAN switches and access points. This guide also includes best practice recommendations and configuration examples for a number of features.

### **Key Features**

#### **Prevention of Layer-2 Bridging between** Wireless Users

In AOS-W, a global firewall feature has been added to deny all L2 bridging between users. Because wireless users enter the switch through GRE tunnels, the feature has been labeled "Deny L2 Bridging between Untrusted GRE Tunnels", and can be configured under the global firewall settings.

#### Wired Port 802.1x Authentication

In AOS-W, 802.1x authentication has been extended to wired ports as well. This implementation is different than that found on standard Ethernet switches, as they are designed to authenticate an entire port. Alcatel's 802.1x implementation is designed to authenticate individual MAC addresses, regardless of how many MAC addresses are seen on a given port. Port-based 802.1x authentication is automatically enabled on any port configured as "untrusted", as long as global 802.1x authentication has been configured.

#### **Enhanced Location Services**

AOS-W 2.2 adds more precise position tracking of wireless devices by utilizing RF triangulation. In previous AOS-W releases, the "RF Locate" feature would display the nearest APs receiving signals from a wireless user or AP, along with the corresponding signal strength. AOS-W 2.2 adds the ability to triangulate position based on RF signal strength. This algorithm is accurate to within approximately 10 meters. Note that for triangulation to function properly, at least three sources of data are required. If three sources of data are not available, the system will revert to showing the nearest APs receiving signal from the device to be located. An additional restriction on triangulation in release 2.2 is that APs must be present in the network in order to provide live calibration data – triangulation will not function in a network with only air monitors in this release.

#### Web Management Interface Enhancements

Many sections of the Web-based management interface have been changed to improve usability. In addition, all critical features configurable from the CLI are also now available in the Web interface.

#### **Enhanced Network Monitoring Interface**

The "Monitoring" section of the Web-based management interface has been enhanced through the separation of network monitoring and switch monitoring. In a network with multiple Alcatel switches, the network monitoring section now provides an easy interface into the network view of the system. When connected to the master switch, all users in the entire network can now be located from the network monitoring section.

#### SNMPv3

Previous releases of AOS-W supported only SNMPv1 and SNMPv2c. When connecting Alcatel components to a network management platform across an insecure network, use of these protocols could lead to unintentional releases of sensitive information. SNMPv3 provides the ability to encrypt SNMP communication.

#### Remote Thin AP

Some customers reported problems when using Alcatel APs connected to a switch across a low-speed link such as a frame relay connection. The issue with this was that latency in the low-speed link would cause greater than 5ms of delay when responding to 802.11 probe request frames from wireless clients. Certain clients would only wait on a single channel for 5ms, and would be on a new channel by the time the probe response arrived. AOS-W 2.2

provides the ability to enable local probe responses for remotely connected APs. This feature may be configured under the Wireless LAN→Advanced section of the Web-based management interface, or may be configured under the "ap location" section of the CLI.

#### Auto-Blacklist Firewall Extended Action

AOS-W 2.2 provides the ability to automatically blacklist (prevent association to any AP) clients who violate a rule in a firewall policy. This is useful for protecting wireless LANs made up of devices that cannot perform authentication, such as Wi-Fi voice handsets or barcode scanners. Devices such as these should be placed into a role with an extremely restrictive firewall policy, for example allowing only SIP traffic to a SIP gateway. If an attacker were to compromise an encryption key or spoof a MAC address on such a network, a single firewall policy violation (i.e. sending an HTTP request or initiating a port scan) would cause the station to be immediately disconnected from the network. This feature may be configured by selecting it as an extended action in any firewall policy.

# Enhanced AP-Switch Discovery and Alcatel Discovery Protocol

In order for thin APs to operate, they must be able to locate and connect to a Wi-Fi switch. Alcatel APs have always had the ability to automatically locate a switch, boot from it, and become operational without requiring any configuration. In the past, this was based on APs obtaining an address through DHCP and performing a DNS lookup on the hostname "Alcatel-master". While this method of switch location is still popular, a number of customers requested alternate methods of AP configuration. AOS-W 2.2 adds "Alcatel Discovery Protocol" (ADP) to provide this functionality. ADP is present in the switch by loading AOS-W.

APs will go through the following sequence to locate a switch:

Power is applied. If AP does not already contain a pre-configured IP address, it will issue a DHCP request to obtain an address.

If DHCP response contains an Alcatel vendor-specific option (see below), it will use this vendor-specific option to contact an Alcatel switch and continue the boot process.

If the DHCP response contains a DNS server address, the AP will perform DNS lookup of the hostname "Alcatel-master.<subdomain>", where <subdomain> was learned from the DHCP server. If this request is successful, the AP will use the returned IP address to contact an Alcatel switch and continue the boot process.



If no DNS information is available, the AP will begin using Alcatel Discovery Protocol (ADP) to locate a switch. It will alternately send out ADP broadcast packets and ADP multicast packets until a response is received. The multicast packet is an IP packet directed to multicast address 224.0.82.11. If a switch is attached to the local L2 segment, it will reply to the ADP broadcast. If a switch has joined the ADP multicast group, the intervening network will forward the AP multicast packets to the switch and it will reply.

#### **DHCP** Configuration

DHCP servers may be configured to return Alcatel vendor-specific options to APs. The vendor class identifier is "AlcatelAP", and the vendor-specific option code is 43. A sample configuration for the open-source ISC DHCP server follows. In this example, the Alcatel switch is located at IP address 10.1.1.10.

```
option serverip code 43 = ip-address;
class "vendor-class" {
       match option vendor-class-identifier;
}
subnet 10.200.10.0 netmask 255.255.255.0 {
   default-lease-time 200;
  max-lease-time 200;
   option subnet-mask 255.255.255.0;
   option routers 10.200.10.1;
   option domain-name-servers 10.4.0.12;
   option domain-name "test.com";
   subclass "vendor-class" "AlcatelAP" {
        option vendor-class-identifier "AlcatelAP";
```

```
option serverip 10.1.1.10;
}
range 10.200.10.200 10.200.10.252;
}
```

To configure Microsoft's DHCP server for this feature:

1. Add an "option 43" entry to the desired DHCP scope that contains the IP address of the Alcatel switch in text. An example of this is shown in the following figure.

Sco	pe Option	s										?	×
G	ieneral Ad	lvance	ed										1
	Available	Optior	าร							D	escriptio	n 🔺	
	🗆 042 N1	[P Sei	vers						Addresses c				
	🗹 043 Ve	endor (	Spec	ific In	fo					E	mbedde	d۰	
	044 W	INS/N	IBNS	Serv	ers/					N	BNS Ad	dr	
	🗆 045 Ne	etBIOS	i ove	r TCF	71P I	NBDE	)			N	etBIOS	0V 🔻	
	•											•	
	⊏Data entr	u											
	Data:	,			Rinari	r					ASCII-		
		0.0	31	30	2도 2도	7) 	2F	31	2 ह	10	1 1	-	
	0008	31	30							10			
	I											- 1	
						OK		]_	Can	cel	A	pply	



- 2. From a command prompt, enter:
- c:\>netsh

netsh>dhcp

netsh dhcp>server \\<server machine name>

netsh dhcp>add optiondef 60 AlcatelAP String 0 comment=AlcatelSupport netsh
dhcp>set optionvalue 60 STRING AlcatelAP

netsh dhcp>exit

#### **Multicast Configuration**

A network supporting IP multicast must be in place to make use of the ADP multicast capability. To configure the Alcatel switch for multicast, enter:

(config) # adp discovery enable

(config) # adp igmp-join enable

This configuration will cause the Alcatel switch to send an IGMPv2 join message for multicast group 224.0.82.11.

# CHAPTER 2 Management Options

AOS-W provides a number of methods for managing your Alcatel Wireless LAN Switch.

#### **Command-Line Interface**

The Command-Line Interface (CLI) provides the most direct method for configuring the switch and collecting system information. The CLI has the following features:

- Accessible from a local console terminal
- Optionally available through Telnet or SSH to local management console or remote network connection
- Comprehensive, industry-standard command system

See "Command Line Basics" on page 13 for more information.

#### Web Interface

The Web interface provides an intuitive, graphical interface to special configuration and design tools. The Web interface provides the following:

- Compatible with a standard Web browser<sup>1</sup>
- Accessible from the local management console or remote network connection

<sup>1.</sup>AOS-W requires Internet Explorer 6.0 or higher. Other browsers may work but with limited functionality and are therefore not officially supported.

- Configure and manage wireless intrusion prevention and performance policies
- Monitor the state and performance of the Wireless LAN
- Perform a site survey to assist deployment of Alcatel Access Points and Air Monitors
- Monitor air interface security and performance events
- AP triangulation

Selected

#### **General Screen Elements**

When Web UI is started after a successful login, the browser window will show the default page: the Monitor Summary. For ease of navigation, all of the Web UI pages have a similar page structure:

Tool				
	Annitoring - Microsoft	t Internet Explorer		
	File Edit View Favorites	s Tools He		
	(3 Back + 6) -	2 🖒 🔎 Search 🔶 Favorites 🚱 📿 - 🚵 🕅 - 🗔 🎎		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
	Agdress () http://10.4.21.21	I/screens/vmsi/monitor.summary.html		
	Google -	👻 🛞 Search Web 🔹 🚳 🔂 31 blocked 🐄 Autor 🕅 🙀 Options 🥒		Dutton
Tool Bar	M	Ionitoring		Button
	Monitoring Configuration	on Diagnostics Maintenance Plan Events Reports	Security Summary	Page
	All WLAN Switches All Access Points	WLAN Network Status	WLAN Attack Summary	Display
	All Air Monitors	TOTAL TOTAL IPSEC IPSEC	Last 5 Min Last Hour All	Diopiay
	All WLAN Clients	WI ON Subther 2 0	Man in the Middle Attacks 0 0 0	
	Global Events	Aniha Acress Points 7 1 1 0	Signature Pattern Matches 0 0 0	
Selected	Switch Switch Summary	Aruba Air Monitors 1 1 0 0	Policy Violations Q Q Q	
Daga	Access Points	Enterprise Clients 0	Roque AP Classification Summary	
гауе	Air Monitors	RADIUS Servers 3 0	Last 5 Min Last Hour All	
	Clients	LDAP Servers 0 0	Rogue APs Detected 5 12 18	
	Blacklist Clients		Rogue APs Disabled Q Q Q	
Dago	Firewall Hits	WLAN Performance Summary	Interfering APs Detected 60 161 220	
гауе	Ports	Last 5 Min Last Hour All	Known Interfering APs 0 0	
Tree	Inventory	Load Balancing Events Q Q Q		
Tree	Local Events	Interference Events Q Q Q	Client Classification Summary	
	WLAN	Bandwidth Exceeded 0 0 0	Last 5 Min Last Hour All	
	<no found="" ssids=""></no>	Error Investigid Exceeded	Valid Clients U U U	
	Debug		Interrening Clients 4 20 22	
	Local Clients		Disabled Rogue Clients Q Q	
	Process Logs			
	Custom Logs			
	«No Custom Logs Found»			
				Reserved.   Email Support
	<b>a</b>			Internet

FIGURE 2-1 Web UI Page Elements

- Tool Bar–This contains buttons for the various tools available in the Web UI software. Click on a button to select the tool.
- Selected Tool-This displays the name of the currently selected tool.

 Page Tree-Each tool has its own information or configuration pages and sub-pages.

The page tree lists all of the pages available when using the currently selected tool. You can navigate to any of the listed pages by clicking on the page name.

**NOTE**—Some of the items in the page tree are merely headings for their sub-pages and cannot be selected. Selectable pages become highlighted when the mouse cursor is placed over them. Non-selectable items do not react.

- Selected Page-The name of the currently selected page is highlighted in the page tree.
- Page Display–This area displays all the information and/or input fields relevant to the current page of the current tool.
- Logout Button-Click on this button to end your Web UI session.

#### **Page Elements**

Each tool in the Web UI has its own unique information or configuration pages, each with specialized data and control fields. Some of the page items appear on multiple pages in multiple tools and provide a similar navigation or configuration function in each.

#### Navigation Items

- Scroll-bars-In some cases, there will be more fields than can be conveniently displayed on one window. When this occurs, standard Windows scroll-bars will be available to let you access the rest of the page.
- Page Tabs-Some pages feature a row of tabs near the top of the page display area. Each tab represents a different form available from the current page.
- Links-Items which are underlined are linked to other pages. By clicking on the item, the relevant item's configuration or information page will be displayed.

#### Fields

- Information Fields-These fields are used only for displaying information.
   The data in these fields cannot be edited directly on the displayed screen.
- Data Entry Fields-Boxed text fields contain user-configurable data. To enter or edit the information, click inside the field box.
- Pull-down Menus-These fields allow you to select an item from a preset list. The currently selected item is displayed in the box. When the arrow button is selected, a list of available options appears. You can change the current selection by clicking on any item in the options list.
- Scrolling Menus-These fields allow you to select an item from a preset list. Use the scroll arrows to view the available options. To select a specific item from the list, click on the item when displayed.



- Check Boxes-Represented as small squares in front of the item text. These fields allow you to turn items on or off by clicking on the check box. A feature or option will be turned on, selected, or enabled (as appropriate) when the box is checked. A feature or option will be turned off, unselected, or disabled when the box is empty.
- Radio Buttons-Represented as small circles in front of the item text. When a group of these items appears together, only one can be selected at any given time. An item is selected when its circle is filled. An item is unselected when the circle is empty.

#### Action Buttons

The following buttons are generally available on configuration pages.

- Apply-Accept all configuration changes made on the current page and send the completed form to the Wireless LAN switch.
- Clear-Reset all options on the current page to their last applied or saved settings.
- Add-Add a new item to the current page. This generally displays a set of relevant configuration fields for the added item.
- Edit-Edit the configuration of the selected item.
- Delete-Remove the selected item from the page configuration.
- Save Configuration-Save all applied configuration changes made since during this configuration session. Saved settings will be retained when the switch is rebooted or turned off. Unsaved configuration changes will be permanently lost.

# CHAPTER 3 Command Line Basics

The Command Line Interface (CLI) is the most direct and comprehensive method for managing the Alcatel Wireless LAN Switch. The CLI can be used to gather information about the switch configuration, collect switch performance statistics, and make configuration changes.

The CLI uses a simple, text-based interface with a Cisco-like command structure. The format is compatible with standard terminals and PC terminal emulation software, and can be accessed locally or over the network using Telnet.

## **Connecting to the Switch**

#### **Local Serial Console**

The CLI is always available using a local terminal or a computer running terminal emulation software. Attach your terminal directly to the serial port on the supervisor card and set the terminal to use the following communications setting:

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

TABLE 3	-1 C	onsole	Terminal	Settings

Press <Enter> a few times.to establish the connection and access the login prompt.

**NOTE**—The serial port accepts an RS-232 serial cable with an RJ-45 male connector (see the *Alcatel 6000 Installation Guide* for more port and cable specifications).

#### Local or Remote Telnet

If properly set up, the CLI can be accessed locally or remotely using Telnet. You can use Telnet (or SSH or the Web GUI) to access any IP interface on an Alcatel Wireless LAN switch.

#### Enabling Telnet Access

The default CLI management method is SSH. To enable Telnet, from configuration terminal mode, enter:

```
> telnet cli
```

Telnet access requires that the switch management interface and default gateway be defined. This is usually done during initial setup (see Step 3 on page 11) but can also be done manually using the local serial console:

- 1 Use the local serial console to log in as the administrator.
- 2 Enter configuration mode and select the management interface sub-mode:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Alcatel) (config) # interface mgmt
```

3 Set the management interface IP address and subnet mask:

(Alcatel) (config-mgmt) # ip address <IP address > <subnet mask>

The management interface is active by default.

#### 4 Exit the sub-mode:

(Alcatel) (config-mgmt) # exit

5 Configure the default gateway for the management interface:

(Alcatel) (config) # ip default-gateway <next hop> mgmt

**NOTE**—If no default gateway is configured, remote access is available only for devices on the same subnet as the management interface.
## Using Telnet to Connect

Use a Telnet client on your management workstation to connect to the Alcatel Wireless LAN Switch management interface IP address. The connection command may vary depending on the specific software used, but commonly appears as follows:

```
> telnet <management interface IP address>
```

When the connection is established, the login prompt will be displayed.

# Logging In

Once connected, the system displays its host name (Alcatel if not configured), followed by the log in prompts. Log in using the administrator account. For example:

(Alcatel)	
user: <b>admin</b>	
password: <b>admin</b>	(password is displayed as asterisks)

As shown above, the default administrator user name is admin, and the default password is also admin. If the password has been changed, use the correct one. When properly logged in, the user mode CLI prompt will be displayed:

(host) >

# Access Modes

Once logged in, there are two levels of access to the switch: user mode and privileged mode.

#### User Mode

User mode provides only limited access for basic operational testing, such as running ping and traceroute. User mode is entered immediately upon login and is shown with the following prompt:

(host) >

where *host* is the host name of the switch if configured, or Alcatel if not configured.

User mode commands are documented starting on page 819.



#### Privileged Mode

All configuration and management functions are available in privileged mode. To move from user mode to privileged mode requires an additional password:

```
(Alcatel) > enable <privileged passmord>
(Alcatel) #
```

When successfully promoted to privileged mode, the > prompt is replaced by the # prompt.

The numerous privileged mode commands are divided into groups according to their context as outlined in the next section.

# **Command Context**

The commands available while in the privileged mode are divided into a number of context groups:

#### Action Commands

The Action Commands take effect as soon as they are entered. They affect the current behavior or operation of the switch, but are not saved as part of the permanent configuration.

The Immediate commands are documented starting on page 819.

#### Master Commands

One Alcatel Wireless LAN Switch on the network is responsible for loading software and configuration files to the Alcatel Access Points and for managing enhanced Wireless LAN switching features (such as air management and wireless load balancing).

In a system with only one switch, the single switch always acts as the master. In a system with more than one switch, one (and only one) switch is selected as the master.

The master switch has an extended command set for handling Access Points and enhanced Wireless LAN features. The master commands are documented starting on page 797.

#### Local Commands

In a system with two or more switches, only one acts as the master. The others act as local switches with a more limited command set.

Commands on local switches mostly affect Layer 2/Layer 3 configuration (such as physical ports and routing interfaces). The local commands are documented starting on page 445.

#### Show Commands

The show commands list information about the switch configuration and performance and are invaluable for debugging system configuration. The show commands are documented starting on page 833.

# **Saving Configuration Changes**

Configuration changes made using the CLI affect only the current state of the switch. Unless saved, the changes will be lost when the system is rebooted. To save your changes so that they will be retained after a reboot, use the following privileged mode CLI command:

```
(Alcatel) # write memory
Saving Configuration...
Saved Configuration
```

# Viewing the Configuration

There are two configuration images which can be viewed from the CLI:

startup-config

This holds the configuration options which will be used the next time the system is rebooted. It contains all the options last saved using the write memory command. Presently unsaved changes are not included.

To view the startup-config, use the following command:

```
(Alcatel) # show startup-config
```

running-config

This holds the current switch configuration, including all pending changes which have yet to be saved.

To view the running-config, use the following command:

(Alcatel) # show running-config

Both configurations can also be saved to a file or sent to a TFTP server for backup or transfer to another system. See "Making Configuration Backups" on page 126 for details.



# Shortcuts

# **Command Completion**

To make command input easier, you can usually abbreviate each key word in the command. You need type only enough of each keyword to distinguish it from similar commands. For example:

```
(Alcatel) # configure terminal
```

could also be entered as:

(Alcatel) # con t

Three characters (con) represent the shortest abbreviation allowed for configure. Typing only c or co would not work because there are other commands (like copy) which also begin with those letters. The configure command is the only one that begins with con.

As you type, you can press the spacebar or tab to move to the next keyword. The system will then attempt to expand the abbreviation for you. If there is only command keyword that matches the abbreviation, it will be filled in for you automatically. If the abbreviation is too vague (too few characters), the cursor will not advance and you must type more characters or use the help feature to list the matching commands.

# **Command Help**

You can use the question mark (?) to get various types of command help.

#### List Available Commands

When typed at the beginning of a line, the question mark lists all the commands available in your current mode or sub-mode. A brief explanation follows each command. For example:

(host) > ?	
enable	Turn on Privileged commands
logout	Exit this session. Any unsaved changes are lost.
ping	Send ICMP echo packets to a specified IP address.
traceroute	Trace route to specified IP address.

## List Matching Commands

When typed at the end of a possible command or abbreviation, the question mark lists the commands that match (if any). For example:

(host) # <b>c</b> ?	
clear	Clear configuration
clock	Configure the system clock
configure	Configuration Commands
сору	Copy Files

If more than one item is shown, type more of the keyword characters to distinguish your choice. However, if only one item is listed, the keyword or abbreviation is valid and you can press tab or the spacebar to advance to the next keyword.

#### List Next Parameter

When typed in place of a parameter, the question mark list the available options. For example:

```
(host) # write ?
erase Erase and start from scratch
file Write to a file in the file system
memory Write to memory
terminal Write to terminal
<Enter>
```

The <Enter> entry ("carriage return," or the enter key) indicates that the command can be entered without additional parameters. Any other parameters are optional.

# **Command History**

The system records your most recently entered commands. You can review the history of your actions, or reissue a recent command easily, without having to retype it.

To view items in the command history, use the <up arrow> to move back through the list and <down arrow> key to forward. To reissue a specific command, press <enter> when it appears. You can even use the command line editing feature to make changes to the command prior to entering it.



## **Command Line Editing**

The command line editing feature allows you to make corrections or changes to a command without retyping. Table 3-2 lists the editing controls:

Кеу	Effect	Description
<ctrl-a></ctrl-a>	Home	Move the cursor to the beginning of the line.
<ctrl-b> or <left arrovv=""></left></ctrl-b>	Back	Move the cursor one character left.
<ctrl-d></ctrl-d>	Delete Right	Delete the character to the right of the cursor.
<ctrl-e></ctrl-e>	End	Move the cursor to the end of the line.
<ctrl-f> or <right arrow&gt;</right </ctrl-f>	Forward	Move the cursor one character right.
<ctrl-k></ctrl-k>	Kill Right	Delete all characters to the right of the cursor.
<ctrl-n> or <down arrow&gt;</down </ctrl-n>	Next	Display the next command in the command history.
<ctrl-p> or <up arrow=""></up></ctrl-p>	Previous	Display the previous command in the command history.
<ctrl-t></ctrl-t>	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
<ctrl-u></ctrl-u>	Clear	Clear the line.
<ctrl-w></ctrl-w>	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
<ctrl-x></ctrl-x>	Kill Left	Delete all characters to the left of the cursor.

TABLE 3-2 Line Editing Keys

Alpha-numeric characters are always inserted into the line at the cursor position.

# **Command Syntax**

CLI commands use basic notations for the parameters that modify a command. These include:

- Brackets []—denotes that the object(s) inside are optional.
- Braces { }-denotes that the object(s) inside are required. If more than one object is included inside a brace, one of the objects must be specified.
- Angles < >—denotes the parameter is required and must be specified.

 Pipe I —denotes a two or more parameters, separated one from the other by the I symbol.

#### For example:

#### crypto ipsec transform-set <set name> {esp-des | esp-3des }

#### {esp-md5-hmac|esp-sha-hmac}

means you have to specify the set name, then choose either esp-des or esp3des, then choose either esp-md5-hmac or esp-sha-hmac.

#### client configuration dns <server1 address> [<server2 address>|no]

means you have to specify the server1 address, but you do not have to specify anything about server2.

In general, *italics* indicates a value you have to enter. For example *address* means you have to specify an IP address or MAC address. You cannot just enter "address".

Bold, like no, means you enter that string. In this case, just type "no".



**OmniAccess Reference: AOS-W System Reference** 



# Design and Planning





**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 4 **RF Design**

# The Alcatel RF Plan Tool

RF Plan is a three-dimensional wireless deployment modeling tool that enables Network Administrators to design an efficient Wireless Local Area Network (Wireless LAN) for their corporate environment, optimizing coverage and performance, and eliminating complicated Wireless LAN network setup.

RF Plan provides the following critical functionality:

- Defines Wireless LAN coverage
- Defines Wireless LAN environment security coverage
- Assesses equipment requirements
- Optimizes radio resources
- Creates an exportable Wireless LAN profile that may be imported into an Alcatel switch and be used to configure and deploy the Wireless LAN.
- AP validation
- Rogue AP triangulation

RF Plan provides a view of each floor, allowing Network Administrators to specify how Wi-Fi coverage should be provided. RF Plan then provides coverage maps and AP/AM placement locations.

Unlike other static site survey tools that require administrators to have intricate knowledge of building materials and other potential Radio Frequency (RF) hazards, RF Plan calibrates coverage on the fly through a sophisticated RF calibration algorithm. This real-time calibration lets administrators characterize the indoor propagation of RF signals in order to determine the best channel and transmission power settings for each AP. Real-time calibration can be automatically programmed or manually undertaken at any time in order to quickly adapt to changes in the wireless environment.

# **Getting Started**

The RF Plan application is available on the Alcatel Wireless LAN switch or as a standalone Windows application. This chapter describes the functionality for both versions of RF Plan. Where there are differences in how the two difference versions are used, they are noted.

## System Requirements for Standalone RF Plan

The standalone Alcatel RF Plan application requires:

- Windows 2000 or Windows XP
- Microsoft Internet Explorer 6.0 or later<sup>1</sup>
- Macromedia Flash 6.0 or later plug-in for Internet Explorer
- Intel Pentium® III 800Mhz (min) or equivalent
- 128MB RAM
- 10MB available hard drive space

## **Installing RF Plan**

To install RF Plan, follow the three steps below:

Note-RF Plan only runs on Windows 2000 and WindowsXP.

- 1. Locate the file named Alcatel RF Plan.zip.
- 2. Unzip the file.
- 3. Launch setup.exe.

By default, the installer places the files in C:\Program Files\Alcatel RF Plan directory. To install the application in a different directory, specify the appropriate location.

<sup>1.</sup> Other browsers may work with AOS-W but with limited capability and are therefore unsupported.

# Launching RF Plan

To open RF Plan select: Start > All Programs > Alcatel Offline RF Plan> Alcatel RF Plan.

# **RF Plan Basics**

# **Page Summary**

The following is a brief summary of the functionality of each of the pages in RF Plan.

•	Building List Page	The Building List page provides a list of buildings that you have created and saved. You may use this page to add or delete buildings from you saved database. You may also import or export buildings here.
•	Building Overview Page	The Building Overview page allows you to see all the dimensional data and modeling parameters for your buildings.
•	Building Specification Page	Specify the dimensions of your building and name it in the Building Specifications page.
•	AP Modeling Page	Specify the AP Modeling parameters on this page.
•	AM Modeling Page	Specify the AM Modeling parameters on this page.
•	Import and Export	Use this page to import and export building database files.
•	Planning Floors Page	The Planning Floors page allows you to see approximate coverages of APs and AMs, as well as any floor plans you may have imported as background images.
•	Floor Editor Page	Use this page to upload background images for each floor, name the floor and delete floors.
		<b>NOTE</b> —You cannot have more than one browser window open when you are trying to upload images.



•	Area Editor Page	Use this page to specify areas on each floor where coverage is not desirable or where Access Points/Air Monitors may not be physically deployed.
•	Access Editor Page	Use this page to manually create, position, or configure Access Points or Air Monitors.
•	AP Plan	The AP Plan page is used to initialize the position of Access Points and launch RF Plan's positioning algorithm.
•	AM Plan	The AP Plan page is used to initialize the position of Air Monitors and launch RF Plan's positioning algorithm.

# **Page Fields**

Each tool in the RF Plan has its own unique information or configuration pages, each with specialized data and control fields. Some of the page items appear on multiple pages and provide a similar navigation or configuration function in each.

- Information Fields-These fields are used only for displaying information.
   The data in these fields cannot be edited directly on the displayed screen.
- Data Entry Fields-Boxed text fields contain user-configurable data. To enter or edit the information, click inside the field box.
- Pull-down Menus-These fields allow you to select an item from a preset list. The currently selected item is displayed in the box. When the arrow button is selected, a list of available options appears. You can change the current selection by clicking on any item in the options list.
- Scrolling Menus-These fields allow you to select an item from a preset list. Use the scroll arrows to view the available options. To select a specific item from the list, click on the item when displayed.
- Check Boxes-These fields are represented as small squares in front of the item text. These fields allow you to turn items on or off by clicking on the check box. A feature or option will be turned on, selected, or enabled (as appropriate) when the box is checked. A feature or option will be turned off, unselected, or disabled when the box is empty.
- Radio Buttons-These fields are represented as small circles in front of the item text. When a group of these items appears together, only one can be selected at any given time. An item is selected when its circle is filled. An item is unselected when the circle is empty.

# Navigation

The RF Plan tool is a wizard in that it logically guides you through the process of defining radio coverage for all the buildings on your campus. The left pane of the wizard screens shows the progression you follow each time you click **Apply**. The button on the top, right corner also takes you to the next logical step. You can also click the link on the left pane to go to any screen in the wizard.

Regardless of your current location, you can always return to the opening window by clicking **Plan** on the menu bar.

# Applying and Saving

When you edit information on any of the RF Plan pages you need to apply that information before it is effective. However, applying the information doesn't save it to your hard drive. You must click on the Save button to permanently save the information.

The following buttons are generally available on configuration pages.

- Apply-Accept all configuration changes made on the current page (does not save changes).
- Save-Save all applied configuration changes made since during this configuration session to a database file. Unsaved configuration changes will be lost when the RF Plan tool is exited.
- **NOTE**—Always Apply. If you advance to the next step without clicking on the Apply button the information will be lost.

# **Next Step Button**

RF Plan will sequence you through all the pages as you setup your Wireless LAN. When you have finished entering the information for each page, click **Next Step** located in the upper right-hand portion of the page.



# **Opening Screen**

When RF Plan opens, the browser window will show the default page: the RF Plan Building List page.

#### **Building List Page**

The Building list page contains all the buildings you have defined using the RF Plan software. The first time you run the application, there should be no buildings in the list.

		Plan	i.		5000	H	<del>]      </del>		
Moniti	oring Ca	nfiguration	Diagno	stics Main	tenance	Plan	n Event	s Repor	ts
Plar	n > Bui	ding Li	st						
Searc	ch Results								Search
Г	Bidg. ^	Name *	Width *	Length *	Floors	APs	Modifie	d Time	
Г	21	Campus21	200	100	1	0	19:57:44 1	/5/2005	
Г	20	Campus20	200	100	1	0	19:57:27 1	/5/2005	
Г	19	Campus19	200	100	1	0	19:57:10 1	/5/2005	
Г	18	Campus18	200	100	1	0	19:56:53 1	/5/2005	
Г	17	Campus17	200	100	1	0	19:56:37 1	/5/2005	
Г	16	Campus16	200	100	1	0	19:56:20 1	/5/2005	
	15	Campus15	200	100	1	0	19:56:02 1	/5/2005	
Г	14	Campus14	200	100	1	0	19:55:45 1	/5/2005	
	13	Campus13	200	100	1	0	19:55:29 1	/5/2005	
Г	12	Campus12	200	100	1	0	19:55:07 1	/5/2005	
			1 2 3 Nex	t   1-10 of 21	10 🗸				
Ne	ew Building	Edit	Building	Delete B	uildings	E	xport	Import	Locate

FIGURE 4-1 Building List Page

•	New Building	Use this button to create a new building. See "Adding a New Building to the Plan" on page 32.
•	Edit Buildings	Use this button to edit existing buildings in the building list. See "Adding a New Building to the Plan" on page 32
•	Delete Buildings	Use this button to delete existing buildings in the building list.
•	Export	Use this button to export a database file with all the specifications and background images of a selected building(s) in the building list. See "Import and Export" on page 39
•	Import	Use this button to import database files defining pre-existing buildings into the RF Plan building list. See "Import and Export" on page 39
•	Locate	Use this button to find the specified building.



When the database of buildings has been created, use this feature to find a specific building, on a specific campus, or search for a name string.

You may add, edit, and delete buildings using this window. You may also import and export buildings using the import and export buttons.

# **Using RF Plan**

# Task Overview

Before you begin take a minute to review this section, it explains the general steps in the order they should be taken to create a building and plan the Wireless LAN for it.

- Gather information about your building's dimensions and floor plan.
- Determine the level of coverage you want for your Access Points and Air Monitors.
- Create a new building and add its dimensions.
- Enter the parameters of your Access Point coverage.
- Enter the parameters of your Air Monitor coverage.
- Add floors to your building and import the floor plans.
- Define special areas.
- Generate suggested AP and AM tables by executing the AP/AM Plan features.
- Export the building.



## **Planning Requirements**

You should collect the following information before beginning to plan your network. Having the information below readily available will expedite your planning efforts.

- Building Dimensions
- Number of floors
- Distance between floors
- Number of users and number of users per AP
- Radio type(s)
- Overlap Factor
- Desired data rates for access points
- Desired monitoring rates for air monitors
- Areas of your building(s) that you don't necessarily want coverage
- Areas of your building(s) where you don't want to, or cannot, deploy an AP or AM
- Any area where you want to deploy a fixed AP or AM.

Building Dimensions	
Height:	Width:
Number of Floors:	
User Information	
Number of Users:	Users per AP:
Radio Types:	
Overlap Factor:	
AP Desired Rates	
802.11blg:	802.11a:
AM Desired Rates	
802.11blg:	802.11a:
Don't Care/Deploy Areas	

# Adding a New Building to the Plan

To define a new building, click **New Building**.

The Overview page shows the default values for your new building, most of which you can change in the following pages.

n Vera	Plan	5000					11.30		7.0
Plan	_								
Bulding Specification Dimension	Plan > buil	ding 1	L > 0	vervie	w			Save	Building Dimension »
Modeling: AP	Building Dimens	sions							
Modeling: AM	Building ID	1.1	Name	building 1					
Planning	Width	400 feet	Length	200 feet					
Floors	Inter Floor Height	20 feet	Floors	0					
AP Plan	Modified Time	21:40:47	7/18/200	14					
AM Plan	Access Point Me	odeling F	arame	ters					
	Radio Type	802	.11a b g	AP Type		AP-52			
	Overlap Factor	100	%						
	802.11b g Desired	Rate 1 M	bps	802.11a	Desired Rate	54 Mbps			
	Number of requir Number of APs to su Number of APs to m	ed APs: 1 upport tota eet desirec	l users: 1 1 rate: 1	l					
	Air Monitor Mo	deling Pa	arameto	ers					
	802.11b g Monitor	Rate 5.5	Mbps 8	02.11a Mo	nitor Rate 36	Mbps			
	Number of requir	ed AMs: 1							

On Building Overview Page you will be able to view the specifications for the following:

- Your buildings dimensions.
- Access Point modeling parameters.
- Air Monitor modeling parameters.

To define your building, click **Building Dimensions**. The Specification page displays.



## **Building Specification Page**

The Building Specification Page enables you to specify the identity of your building and its dimensions.

	Plan	2000		1.30		
Plan Bulding Specification Dimension	Plan > build	ing 1 > Specif	ication		Save AP Modelin	ng Spec, »
Modeling: AP Modeling: AM <b>Planning</b> Filoors AP Plan AM Plan	Edit Building ID 1 Width 4 Inter Floor Height 2 Floors 1	. 1 Name 100 Length 20 Unit L Apply	building 1 200 Teet v			

•	Building ID	This consists of two decimal numbers separated by a dot. The first is the campus ID. The campus ID will always be "1" if there is only one campus. The second is the building number.
		The valid range for these fields is any integer from 1 to 255.
•	Building Name	Enter a user friendly name for the building.
		The Building Name may be an alpha-numeric string up to 64 characters in length.
•	Width and Height	Enter the rectangular exterior dimensions of the building.
		The valid range for this field is any integer from 1 to a value corresponding to $1 \times 10^{12}$ .
•	Inter-floor Height	This is the distance between floor surfaces in the building.
		The valid range for this field is any integer from 1 to a value corresponding to $1 \times 10^{12}$ .
		<b>Note</b> —This is NOT the distance from floor to ceiling. Some buildings have a large space between the interior ceilings and the floor above.

• Floors Enter the number of floors in your building here.

The valid range for this field is any integer from 1 to a value corresponding to  $1 \times 10^{12}$ .

 Units
 Specify the units of measurement for the dimensions you specified on the page. The choices are feet and meters.

## A Word About Building Dimensions

The dimensions you specify for building width and height should be the major dimensions (maximum height and width) of the overall footprint of the building as illustrated below.



When height and width are specified, RF Plan creates a rectangular area in the Planning feature pages that represent the overall area covered by the building. You will need to import an appropriate background image (see, "Floor Editor Page" on page 44.) to aid you in defining areas that don't require coverage or areas in which you do not wish to deploy Access Points and Air Monitors (see, "Area Editor Page" on page 45).

Define your first building on this campus and click **Apply**. The AM Modeling page displays.



## AP Modeling Page

The AP Modeling page allows you to specify all the information necessary for RF Plan to determine the appropriate placement of your APs.

(	Plan			in: 39	
Plan					
Bulding Specification Dimension	Plan > Headq	uarters > <b>AP</b>	Modeling Par	ameters	Save AM Modeling Spec. >
Modeling: AP	Edit				
Modeling: AM	Radio Type	802.11 alblg 💌	AP Type	AP-52 -	
Planning Floors	Coverage   C C	apacity   🔿 Custom	Overlap Factor	100 % Low 💌	
Floor 1	Total Users	5	Users / AP	5	
Floor 2	802.11b g Desired Rate	1 V Mbps	802.11a Desired Rate	54 • Mbps	
Floor 3	APs	0			
Floor 4	Number of required Al	Ps: 184			
Floor 5	Number of APs to support Number of APs to meet de	total users: 1 sired rate: 184			
AP Plan AM Plan		A	pply		

Controls on this page allow you to select or control the following functions:

- Radio Type Use this pull-down menu to specify the radio type in the appropriate combination of a, b, and or g configuration.
- AP Type Specify AP 52 or AP 60.
- Coverage Use this option to let RF Plan automatically determine the number of APs based on desired data rates and the configuration of your building. The desired rate is selectable from 1 to 54 Mbps in both the Coverage and Capacity models.
- Capacity
   Use this option to let RF Plan determine the number of APs based upon the total number of users, ratio of users to APs, and desired data rates. The desired rate is selectable from 1 to 54 Mbps in both the Coverage and Capacity models.
- Custom Use this option to simply specify a fixed number of APs.
- Overlap Factor Use this field and pull-down to specify an overlap factor.
- Rates
   Use these pull-down to specify the data rates desired on your Access Points.
- Users/AP Selectable for Capacity or Custom models.
- APs Selectable for Capacity or Custom models.

# Radio Type

Specify the radio type(s) of your APs using the pull-down Radio Type menu on the Modeling Parameters page.

Available Radio Type Choices:

•	801.11a	5GHz, Orthogonal Frequency Division Multiplexing (OFDM) with data rates up to 54Mbps.
•	802.11b	2.4GHz, Direct Spread Spectrum (DSSS) multiplexing with data rates up to 11Mbps.
•	802.11g	2.4GHZ, OFDM/CCK (Complementary Code Keying) with data rates up to 54Mbps.

#### **Overlap Factor**

The Overlap Factor is the amount of signal area overlap that you want when the APs are operating. Overlap is important if an AP fails. It allows the network to self-heal with adjacent APs powering up to assume some of the load from the failed device. Although there may be no holes in coverage in this scenario, there will likely be a loss of throughput. Increasing the overlap will allow for higher throughputs when an AP has failed and will allow for future capacity as the number of users increases.

The valid range of values for the overlap factor are from 100% to 1000%.

#### Users

NOTE—The Users text boxes are active only when the Capacity model is selected.

Enter the number of users you expect to have on your Wireless LAN in the Users text box. Enter the number of users per access point you expect in the Users/AP text box.

The numbers entered in the these two text boxes must be no-zero integers between 1-255 inclusive.

#### Rates

**Note**—The Rate pull-down menus are active only when the Coverage or Capacity design models are selected.

Select the desired data rates from the pull-down menus for 802.11b/g and 802.11a.

High data transmission rates will require an increased number of AP to be placed in your building. You should carefully evaluate your user's data rate needs.



Click **Apply** and the AM Modeling page displays.

#### AM Modeling Page

The AM Modeling page allows you to specify all the information necessary for RF Plan to determine the appropriate placement of your AMs.

	Plan	753
Plan		
Bulding Specification Dimension	Plan > Headquarters > AM Modeling Parameters	Save Planning »
Modeling: AP	Edit	
Modeling: AM	Coverage   C Custom	
Planning	802.11blg Monitor Rate 55 V Mbns 802.11a Monitor Rate 36 V Mbns	
Floors		
Floor 1		
Floor 2	And the second s	
Floor 3	Арру	
Floor 4		
Floor 5		
AP Plan		
AM Plan		

Controls on this page allow you to select or control the following functions:

•	Monitor Rate	Use this pull-down menu to specify the desired monitor rate for your Air Monitors.
•	AMs	Use this field to manually specify the number of Air Monitors to deploy (Custom Model only).
•	Design Model	Use these radio buttons to specify a design model to use in the placement of Air Monitors.

#### Design Models

Two radio buttons on the page allow you to control the kind of model which will be used to determine the number and type of APs.

Design Model Radio Button Options:

 Coverage Use this option to let RF Plan automatically determine the number of AMs based on desired monitor rates and the configuration of your building.

Desired rate is selectable from 1 to 54 Mbps in the Coverage model.

 Custom
 Use this option to simply specify a fixed number of AMs. When the AM Plan portion of RF Plan is executed, RF Plan will make an even distribution of the AMs. **Note**—The monitor rates you select for the AMs should be less than the data rates you selected for the APs. If you set the rate for the AMs at a value equal to that specified for the corresponding PHY type AP, RF Plan will allocate one AM per AP. If you specify a monitor rate larger than the data rate, RF Plan will allocate more than one AM per AP.

## Monitor Rates

Use the drop down menus to select the desired monitor rates for 802.11b/g and 802.11a air monitors.

**NOTE**—This option is available only when the coverage design model is selected.

#### Import and Export

RF Plan allows you to import and export files that define the parameters of your buildings. The files that you import and export are XML files and depending on how many floors your buildings have, and particularly how many background images you have for your floors, the XML files may be quite large. (See "Background Images" on page 44.)

Buildings exported from RF Plan will be imported into an Alcatel switch and used by the version of RF Plan that is integrated into the Web UI Software. The exported building file contains all the data about the building(s) you created using RF Plan. The integrated RF Plan in Web UI gives you the ability to automatically configure the APs and AMs that are actually connected to the switch using the Suggested AP and Suggested AM tables created by RF Plan. (See, "AP Plan" on page 49 and "AM Plan" on page 51.)

#### Import Buildings

The Import Buildings page allows you to import configuration information from an existing Alcatel switch so you can modify it for use on another switch or in an another building.

Only XML files exported from an Alcatel switch or from Alcatel RF Plan may be imported into RF Plan.

	i	Plan	5000		
Plan					
Plan >	Import	Buildings			
Import				<u>Back</u>	
File Name					
		Import	Cancel		
File should b	e under offline	e database directo	ry, C:\Program Files\		



**NOTE**—Importing any other file, including XML files from other applications, may result in unpredictable results.

Any file you wish to import must be in the C:\Program Files\Alcatel RF Plan\data\ path. You can not specify any other path in the RF Plan Import Buildings dialog.

#### Export Buildings

The Export Buildings page allows you to export the configuration of the Wireless LAN you just created so that it may be imported into and used to automatically configure your Alcatel switches.

-	Plan	6000 geood	
Plan			
Plan > Expo	ort Buildings		
Export		Back	
Buildings	1.1: Headq	quarters	
Include Images			
File Name			
	Save C	Cancel	
File should be under o	ffline database director	ry, C:\Program Files\	

Files exported from RF Plan will be placed in the C:\Program Files\Alcatel RF Plan\data\ directory on your hard drive.

When exporting a building file it is recommended that you check the Include Images check box.

When naming your exported file, be sure to give the file the *XML* file extension.

**Example:** *My\_Building.XML* 

# **Planning Pages**

# Planning Floors Page

	RF Plan
Plan Bulding Specification Dimension Modeling: AP Modeling: AM Planning Floors Floor 1 Floor 2 Floor 3 AP Plan AM Plan	Plan > New Building > Planning       Save Add New Floor AP Planning >         Control       Image: Coverage Rate Image: N/A multiple         Floor 1   Edit Floor       Edit Floor

The Planning Floors page enables you to see what the footprint of your floors look like. You can select or adjust the following features on the Planning Floors Page.

•	Zoom	Use this pull-down menu or type a zoom factor in the text field to increase or decrease the size of the displayed floor area.
•	Approximate Cover- age Map (select radio type)	Use this pull-down to select a particular radio type for which to show estimated coverage.
•	Coverage Rate	Use this pull-down to modify the coverage areas based on a different data rate.
•	Floor Editor	Click on this link to launch the Floor Editor. See "Floor Editor Page" on page 44.
•	Area Editor	Click on this link to launch the Area Editor. See "Area Editor Page" on page 45.
•	Access Point Editor	Click on this link to launch the Access Point Editor. See "Access Editor Page" on page 46.



#### Zoom

The Zoom control sets the viewing size of the floor image. It is adjustable in finite views from 10% to 1000%. You may select a value from the pull-down zoom menu or specify a value in the text box to the left of the pull-down. When you specify a value, RF Plan adjusts the values in the pull-down to display a set of values both above and below the value you typed in the text box.



#### Coverage

Select a radio type from the Coverage pull-down menu to view the approximate coverage area for each of the APs that RF Plan has deployed in AP Plan or AM Plan. Adjusting the Coverage values will help you understand how the AP coverage works in your building.

Note—You will not see coverage circles displayed here until you have executed	either
an AP Plan or an AM Plan.	

Contr	rol						
Zoom	100 100	• %	Approx. Coverage	AP - 802.11a	•	Coverage Rate	36 💌 Mbps
Numbe Numbe Numbe	er of required r of APs to supp r of APs to meet	APs: 35 ort total u desired r	isers: 2 ate: 35	_			_
			Initialize	Start Stop	0		
Floor	1   Edit Floor						_
		सम्ब (गि.))(गि.) ()) ()) ()) ()) ()) ()) ()) ()) ()) (					

## Coverage Rate

Adjusting the coverage rate will also affect the size of the coverage circles for AMs. Adjusting the rate values will help you understand how the coverage works in your proposed building.

## Reading Coverage Maps

Under some conditions, AP or AM signal strengths show in coverage maps may not be reported accurately. One condition is a single AP or AM in the corner of a building. The coverage map may show the signal strength extending well outside the building. However, if the signal encounters nearby interference in the building, the signal strength may be much weaker in the area of the interference. This area of weakened signal strength will likely not be reflected in the coverage map.

Another condition that renders the coverage map to be somewhat inaccurate is an environment in which multiple APs or AMs differ substantially in signal strength. In this mixed environment, the coverage map will average signal strengths of the devices and may report strengths slightly less than the actual signal strength of the stronger devices and slightly greater than that of the weaker devices.

## Per Floor Recap

Between each floor display, RF Plan lists the APs and AMs defined for the floor.

Areas   Expand +   New											
Sugges	Suggested Access Points and Air Monitors   Collapse 🖃   New   Clear										
Fixed	Loc.	Name	х	Y.	o   g Type	.b g Ch/Pe	. wo	а Туре	.a Ch/Pow		
No ap's d	efined.										
Deploye	Deployed Access Points and Air Monitors   Collapse 🗆										
Loc.	Name	ΧY	AP	Туре	.b g Typ	e/Ch/Pow	.b g	Bssid	.a Type/Ch/F	wo	.a Bssid
No ap's defined.											



## Floor Editor Page

Click **Edit Floor** to display the Floor Editor which allows you to specify the background image, and name the floor.

🗿 Floor Editor ₩	eb Page Dialog		<u>? ×</u>
Floor Editor			
Level	2	Name	
Current BG Image			
New BG Image		Browse	
	Apply Car	ncel Delete	

#### Naming

You may name the floor anything you choose as long as the name is an alpha-numeric string with a maximum length of 64 characters. The name you specify appears just to the right of the Floor Number displayed just above the background image in the Planning view.

#### Background Images

A background image (floor plan image) may be imported into RF Plan for each floor. A background image is extremely helpful when specifying areas where coverage is not desired or areas where an AP/AM is not to be physically deployed.

Select a background image using the Browse button on the Floor Editor Dialog.

• File Type and Size

Background images must be JPEG format and may not exceed 2048 X 2048 pixels in size. Attempting to import a file with a larger pixel footprint than that specified here will result in the image not scaling to fit the image area in the floor display area.

**Note**—Because the background images for your floors are embedded in the XML file that defines your building you should strongly consider minimizing the file size of the JPEGs you use for your backgrounds. You can minimize the file size by selecting the maximum compression (lowest quality) in most graphics programs.

Image Scaling

Images are scaled (stretched) to fit the display area. The display area aspect ratio is determined by the building dimensions specified on the Dimension page.

## Area Editor Page

The area editor allows you to specify areas on your buildings floors where you either do not care about coverage, or where you do not want to place an AP or AM.

Open the Area Editor by clicking on the *New* link in the Areas field just below the area where the background image is displayed.

		<b></b>	— Are	a Ed	litor	"New"	L
Areas	<u>Collapse 🖃   N</u>	ew.					
Name	Туре	Left	Bottom	Right	Тор		
Area 1	Don't Care	52	7	336	101		
Area 2	Don't Deploy	55	110	335	196		

You specify these areas by placing them on top of the background image using the Area Editor.

🖉 Area Editor Web Page Dialog 🔹 🕺				
Area Edito	r			
Name	area 1	Туре	Don't Care 💌	
Left	150	Bottom	75	
Right	249	Тор	124	
Apply Cancel Delete				

## Naming

You may name an area using an alpha-numeric string of characters with a maximum length of 64 characters. You should give areas some meaningful name so that they are easily identified.

#### Locating and Sizing

You may specify absolute coordinates for the lower left corner and upper right corner of the box that represents the area you are defining. The datum for measurement is the lower left corner of the rectangular display area that represents your building's footprint. The coordinates of the upper right-hand corner of the display area are the absolute (no unit of measure) values of the dimensions you gave your building when you defined it with the dimension feature.

For example: If you defined your building to be 200 feet wide and 400 feet long, the coordinates of the upper right-hand corner would be (199, 399).

**NOTE**—Remember, the location is zero based, so the values range from 0 to (height-1 and width-1).



You may also use the drag and drop feature of the Area Editor to drag your area to where you want it and resize it by dragging one or more of the handles displayed in the corners of the area.

Don't Care areas are displayed as orange rectangles.



Don't Deploy areas are displayed as yellow rectangles.



#### Access Editor Page

The Access Editor allows you to manually create or modify a suggested access point.

🚰 Suggested Access Editor Web Page Dialog 🛛 🤶 🗙						
Suggested Access Point Editor						
Name	ap 19	Fixed	No 💌			
Location	1.1. 19	PHY Type	802.11alblg 💌			
x	200	Y	100			
802.11b g Type	Aruba AP 🔹					
802.11b g Channel	1 💌	802.11b g Power Level	2 •			
802.11a Type	Aruba AP 💽					
802.11a Channel	36 💌	802.11a Power Level	2 -			
Memo				4		
Apply Cancel Delete						

#### Naming

RF Plan automatically names APs using the default convention "a *number*". It assigns the number starting at 1 and increasing by one for each new AP. When you manually create an AP that new AP is then assigned the next "a" number in sequence and added to the bottom of the suggested AP list.

You may name an Access Point anything you wish. The name must be comprised of alpha-numeric characters and be 64 characters or less in length.

#### Location

The physical location of the AP is specified by X-Y coordinates beginning at the lower left corner of the display area. The numbers you specify in the X and Y text boxes are whole units. The X coordinates increase as a point moves up the display and the Y coordinates increase as they move from left to right across the display.



#### Fixed

Fixed APs don't move when RF Plan executes the positioning algorithm.

**Note**—You might typically set an AP as fixed when you have a specific room, such as a conference room, in which you want saturated coverage. You might also want to consider using a Fixed AP when you have an area that has an unusually high user density.

Choose Yes or No from the drop down box. Choosing Yes will lock the position of the AP as it is shown in the coordinate boxes of the Access Editor. Choosing No will allow RF Plan to move the AP as necessary to achieve best performance.

## PHY Types

The PHY Type drop down menu allows you to specify what radio mode the AP will use. You may choose from one of the following:

- 802.11a/b/g
- 802.11a
- 802.1 b/g



#### 802.11 Types

The 802.11 b/g and 802.11a Type drop down boxes allow you to choose the mode of operation for the access point. You may choose to set the mode of operation to access point (Alcatel AP) or Air Monitor.

#### 802.11 Channels

The 802.11a and 802.11b/g channel drop down menus allow you to select from the available channels.

**NOTE**—The available channels will vary depending on the regulatory domain (country) in which the device is being operated.

802.11a channels begin at channel 34 at a frequency of 5.170 MHz and increase in 20MHz steps through channel 161 at 5.805 Mhz.

802.11b/g channels begin at 1 and are numbered consecutively through 14. The frequencies begin at 2.412 MHz on channel 1 and increase in 22 MHz steps through Channel 14 at 2.484 MHz.

#### 802.11 Power Levels

The power level drop down menus allow you to specify the transmission power of the access point. Choices are OFF, 0, 1, 2, 3, and 4. A setting of 4 will apply the maximum Effective Isotropic Radiated Power (EIRP) allowed in the regulatory domain (country) in which you are operating the access point.

#### Memo

The Memo text field allows you to enter notes regarding the access point. You may enter a maximum of 256 alpha-numeric characters in the Memo field.

# AP Plan

The AP Plan feature uses the information entered in the modeling pages to locate access points in the building(s) you described.

RF Plan					
Bulding Specification Dimension Modeling: AP Modeling: AM Planning Floors	Plan > New Building > AP Planning Control Zoom 150 150 % Approx. Coverage AP - 802.11a Number of APs to support total users: 30 Number of APs to meet desired rate: 21	Add New Floor Save AM Planning » Coverage Rate 36 Mbps			
Floor 2 AP Plan AM Plan	Floor 1   Edit Floor				

## Initialize

Initialize the Algorithm by clicking on the Initialize button. This makes an initial placement of the access points and prepares RF Plan for the task of determining the optimum location for each of the APs. As soon as you click the Initialize button you will see the AP symbols appear on the floor plan. Access points are represented by this symbol.





Colored circles around the AP symbols on the floor plan indicate the approximate coverage of the individual AP and the color of the circle represents the channel on which the AP is operating. The circles appear when you select an *approximate coverage* value on one of the Floors pages. You may also use click on an AP icon and drag it to manually reposition it.



#### Start

Click on the Start button to launch the optimizing algorithm. You will see the AP symbols moving on the page as RF Plan finds the optimum location for each.

The process may take several minutes. You may watch the progress on the status bar of your browser. The algorithm will stop when the movement is less than a threshold value calculated based on the number of APs. The threshold value may be seen in the status bar at the bottom of the browser window.

#### Viewing the Results

The results of optimizing algorithm may be viewed two ways: graphically and in a table of suggested APs. You may obtain information about a specific AP by placing the cursor over its symbol. An information box appears containing information about the exact location, PHY type, channel, power, etc.

Suggested AP Information				
Name: Suggested AP: 1.12				
Location: 1.1.12,	PHY Type: 802.11ag			
X: 183, Y: 121				
.g Type: soft-ap,	.g Channel: 6, .g Power Level: 2			
.a Type: soft-ap,	.a Channel: 40, .a Power Level: 2			
Memo: <b>null</b>				
The Suggested AP Table lists the coordinates, power, location, power setting, and channel for each of the APs that are shown in the floor plan.

Sugges	ted Acc	ess Points   Collaps	<u>e</u> 🗆	New	l <u>Clea</u>	r			
Fixed	Loc.	Name	х	Y	.b ç	ј Туре	.b g Ch/Pow	.a Type	.a Ch/Pow
No	<u>1.1.1</u>	Suggested AP: 1.1	59	25		AP	1/2	AP	161 / 2
No	<u>1.1.2</u>	Suggested AP: 1.2	139	24		AP	11/2	AP	36 / 2
No	1.1.3	Suggested AP: 1.3	300	24		AP	11/2	AP	56 / 2
No	<u>1.1.4</u>	Suggested AP: 1.4	379	24		AP	6/2	AP	64 / 2
No	1.1.5	Suggested AP: 1.5	20	74		AP	6/2	AP	153 / 2
No	1.1.6	Suggested AP: 1.6	99	75		AP	6/2	AP	44 / 2
No	1.1.7	Suggested AP: 1.7	179	74		AP	11/2	AP	40/2
No	1.1.8	Suggested AP: 1.8	259	75		AP	1/2	AP	48/2
No	1.1.9	Suggested AP: 1.9	339	74		AP	1/2	AP	153 / 2
No	1.1.10	Suggested AP: 1.10	60	124		AP	6/2	AP	60/2
No	1.1.11	Suggested AP: 1.11	139	125		AP	11/2	AP	52/2
No	1.1.12	Suggested AP: 1.12	220	124		AP	6/2	AP	40/2

### AM Plan

The AM Plan feature calculates the optimum placement for your air monitors (AMs).

#### Initialize

Initialize the Algorithm by clicking on the Initialize button. This makes an initial placement of the air monitors and prepares RF Plan for the task of determining the optimum location for each of the AMs. As soon as you click the Initialize button you will see the AM symbols appear on the floor plan. Air Monitors are represented by this symbol.



### Start

Click on the Start button to launch the optimizing algorithm. You will see the AM symbols moving on the page as RF Plan finds the optimum location for each.

The process may take several minutes. You may watch the progress on the status bar of your browser. The algorithm will stop when the movement is less than a threshold value calculated based on the number of AMs. The threshold value may be seen in the status bar at the bottom of the browser window.



#### Viewing the Results

Viewing the results of the AM Plan feature is similar to that for the AP Plan feature.

The results of optimizing algorithm may be viewed two ways: graphically and in a table of suggested AMs. You may obtain information about a specific AP by placing the cursor over its symbol. An information box appears containing information about the exact location, PHY type, channel, power, etc.

Suggested AP Information	5	
Name: Suggested AM: 2.1		
Location: 1.2.1, PHY Type: 802.11ag		
X: 100, Y: 50		
.g Type: air-monitor, .g Channel: 6, .g Power	r Leve	1:2
.a Type: air-monitor, .a Channel: 64, .a Powe	er Lev	el: 2
Memo: null		

The Suggested AP Table lists the coordinates, power, location, power setting, and channel for each of the APs that are shown in the floor plan.

Sugges	Suggested Access Points   Collapse ⊡   New   Clear								
Fixed	Loc.	Name	х	Y	.b g Type	.b g Ch/Pow	.a Type	.a Ch/Pow	
No	1.2.1	Suggested AM: 2.1	100	50	Air Monitor	-1-	Air Monitor	-1-	
No	1.2.2	Suggested AM: 2.2	232	50	Air Monitor	-1-	Air Monitor	-/-	
No	1.2.3	Suggested AM: 2.3	366	49	Air Monitor	-1-	Air Monitor	-/-	
No	1.2.4	Suggested AM: 2.4	167	149	Air Monitor	-/-	Air Monitor	-/-	
No	1.2.5	Suggested AP: 2.5	40	25	AP	1/2	i AP	149 / 2	
No	1.2.6	Suggested AP: 2.6	120	24	AP	11/2	I AP	157 / 2	

# **Locating Devices**

To find a specific device by for example a MAC address or ESSID, click **Locate** on the main menu (Building List). AOS-W locates devices by the process of triangulation.



Chapter 4



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 5 Security Options

Strong network security is an absolute necessity in today's enterprise network environment. There are prying "eyes" everywhere. Some who want to gain access to your secrets, and some who are just plain malicious.

Security hinges on two important concepts. Encryption of the information traveling on the network, and authentication of users on the network. This ensures that only authorized users are using the network and that the data transmitted by them is strongly encrypted.

Cunning and devious hackers have devised ways to attack secure networks and gain unauthorized access. Therefore, cunning and inventive network security professionals have devised methods to detect, defend, and disable would-be attackers from gaining access to or disrupting the network.

One of the principle features of Alcatel AOS-W is the ability to lock the air so that unauthorized users can't even get past the antennas of a wireless access point. Alcatel's Intrusion Detection System (IDS) detects and neutralizes all the common types of intrusion attacks that might be mounted against the network.

Additionally, AOS-W deploys both Layer 2 and Layer 3 security protocols allowing a full spectrum of network security measures.

By default, Alcatel Wireless LAN Switches and Access Points treat ports as being untrusted. However, certain ports are open by default. To maintain security, these default open ports are only open on the trusted side of the network. These open ports are listed in Table 5-1 below.

Port Number	Protocol	Where Used	Description
17	ТСР	Wireless LAN Switch	This is use for certain types of VPN clients that accept a banner (QOTD). During normal operation, this port will only accept a connection and immediately close it.
21	ТСР	Wireless LAN Switch	FTP server for AP6X software download.
22	ТСР	Wireless LAN Switch	SSH
23	ТСР	AP and Wireless LAN Switch	Telnet is disabled by default but the port is still open
53	UDP	Wireless LAN Switch	Internal domain
67	UDP	AP (and Wireless LAN Switch if DHCP server is configured )	DHCP server

 TABLE 5-1
 Default (Trusted)
 Open
 Ports

Port Number	Protocol	Where Used	Description
68	UDP	AP (and Wireless LAN Switch if DHCP server is configured )	DHCP client
69	UDP	Wireless LAN Switch	TFTP
80	ТСР	AP and Wireless LAN Switch	HTTP Used for remote packet capture where the capture is saved on the Access Point. Provides access to the WebUI on the Wireless LAN Switch.
123	UDP	Wireless LAN Switch	NTP
161	UDP	AP and Wireless LAN Switch	SNMP. Disabled by default.
443	ТСР	Wireless LAN Switch	Used internally for captive portal authentication (HTTPS) and is exposed to wireless users. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing.
500	UDP	Wireless LAN Switch	ISAKMP

### TABLE 5-1 Default (Trusted) Open Ports (Continued)



Port Number	Protocol	Where Used	Description
514	UDP	Wireless LAN Switch	Syslog
1701	UDP	Wireless LAN Switch	L2TP
1723	ТСР	Wireless LAN Switch	PPTP
2300	ТСР	Wireless LAN Switch	Internal terminal server opened by telnet soe command.
3306	ТСР	Wireless LAN Switch	Remote wired MAC lookup.
4343	ТСР	Wireless LAN Switch	HTTPS. A different port is used from 443 in order to not conflict with captive portal. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing
4500	UDP	Wireless LAN Switch	sae-urn
8080	ТСР	Wireless LAN Switch	Used internally for captive portal authentication (HTTP-proxy). Not exposed to wireless users.

## TABLE 5-1 Default (Trusted) Open Ports (Continued)

Port Number	Protocol	Where Used	Description
8081	TCP	Wireless LAN Switch	Used internally for captive portal authentication (HTTPS). Not exposed to wireless users. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing.
8082	ТСР	Wireless LAN Switch	Used internally for single sign-on authentication (HTTP). Not exposed to wireless users.
8083	ТСР	Wireless LAN Switch	Used internally for single sign-on authentication (HTTPS). Not exposed to wireless users.
8088	ТСР	Wireless LAN Switch	Internal
8200	UDP	Wireless LAN Switch	Alcatel Discovery Protocol (ADP)
8211	UDP	Wireless LAN Switch	Internal

TABLE 5-1	Default	(Trusted)	Open	Ports	(Continued)
-----------	---------	-----------	------	-------	-------------

# **AOS-W Security Options**

The following security configuration options are supported in AOS-W:

- Roles
- Policies
- AAA Servers
- Authentication Methods
- VPN Settings



- Global Firewall Settings
- Advanced

These options are described in this chapter.

# **User Roles**

## **Role Design**

The *role* of a wireless user determines a number of access policies, including firewall/traffic policies, bandwidth contracts, IP address pool, VLAN assignment, and VPN dialer. The role is determined through some type of authentication mechanism, and can be as simple as "employee" versus "guest", or more granular such as "sales user, marketing user, finance user, IT staff". The selection of a role framework is an important design decision.

## **Role Configuration**

To manage user roles, navigate to **Configuration > Security > Roles**. Current roles will be displayed, as shown in the figure below.

oring Configuration	Diagnostics	Maintenance Plan Events Reports		Save Configuratio
ich neral	Security	> User Roles		
anagement	Name	Firewall Policies	Bandwidth Contract	Actions
AN	ap-role	control, ap-ad	Not Enforced	Edit Delete
Dadio	abcd	orderchangenew	Not Enforced	Edit Delete
Advanced	saqs	xsasaaaaa	Not Enforced	Edit Delete
Management	trusted-ap	allowall	Not Enforced	Edit Deicte
Calibration	default-vpn-role	allowall	Not Enforced	Edit Delete
Optimization	employee	allowall	Not Enforced	Edit Delete
Monitoring	test	$validusernew, validuser, allowall, stateful-dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, employeenew, controlnew1, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, employeenew, controlnew1, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, employeenew, controlnew1, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, employeenew, controlnew1, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, employeenew, controlnew1, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, cplogoutnew, and the stateful dot1\times/6.0.0, srcnatnew, captive portal, vpnlogon, srcnatnew, captive portal, vpnlogon, srcnatnew, captive portal, srcnatnew, $	Not Enforced	Edit Delete
Advanced	guest	control,cplogout	Not Enforced	Edit Delete
curity	stateful-dot1×	stateful-dot1×	Not Enforced	Edit Delete
Roles	stateful	control	Not Enforced	Edit Delete
Policies	logon	vpn-dst-nat.control.captiveportal.vpnlogon.remotean-1.stateful-dot1x	Not Enforced	Edit Delete
AAA Servers	Add		1	and an and an and

#### FIGURE 5-1 User Roles

To edit an existing role, click **Edit**. To add a new role, click **Add** as shown in the figure below.

Role Name NewRole
Firewall Policies
Name         Rule Count         Location         Action           Add
Re-authentication Interval
Disabled Change (0 disables re-authentication. A positive value enables authentication)
Role VLAN ID
Not Assigned Not Assigned 🗨 Change
Bandwidth Contract
Not Enforced Change
VPN Dialer
Not Assigned Not Assigned Change
L2TP Pool
Not Assigned Not Assigned Change
PPTP Pool
Not Assigned Not Assigned Change

#### FIGURE 5-2 Add New Role

User role configuration parameters are described in the following sections.



## CLI Configuration for User Roles

Sample CLI configuration follows for two different user roles. One is used for IT staff who have full access to the entire network, normally use VPN access, and have no bandwidth limitations. The other role is used for guest users. Guests must reauthenticate every 30 minutes, have a 1Mbps rate limiting policy applied, and have a restricted traffic policy that allows only Internet access.

```
user-role IT-staff
dialer IT-staff
pool 12tp pool3
pool pptp pool3
session-acl allowall
!
user-role guest
bandwidth-contract guest-1M
vlan 2
reauthentication-interval 30
session-acl Internet Only
```

# **Firewall and Traffic Policies**

## Introduction to Firewall and Traffic Policies

A "traffic policy" is a term used to describe a stateful flow-classification rule. In other words, a traffic policy identifies specific characteristics about a data packet passing through the switch, then takes some action based on that identification. In an Alcatel switch, the action could be a firewall-type action such as permitting or denying the packet, an administrative action such as logging the packet, or a quality of service (QoS) type action such as setting Diffuser or 802.1p bits or placing the packet into a priority queue. Traffic policies can be applied to *users*, giving differential treatment to different users on the same network, or to *physical ports*, applying the same policy to all traffic through that port.

Traffic policies are often confused with access control lists (ACLs), but the two have some major differences:

Traffic policies are *stateful*, meaning they understand flows in a network and keep track of the state of sessions. If a policy is enabled to allow *telnet* outbound from a client, a traffic policy will understand that inbound traffic associated with that session should be allowed. ACLs have no memory of

what came before – at best, ACLs can look at the "SYN" flag in a TCP packet, treating the session as new if the flag is set and treating the session as "established" if it is not. This works for "normal" traffic but is ineffective against many types of attack traffic.

Traffic policies in an Alcatel Wi-Fi switch are *dynamic*, meaning that address information in the rules can change as the policies are applied to users. For example, a traffic policy containing the alias "*user*" can be created. After the policy is applied to a particular user, this alias is automatically changed to match the IP address assigned to the user. An ACL is typically a static packet filter, with IP addresses hard coded into the rule.

Traffic policies are *bi-directional*. While ACLs are normally applied either to traffic inbound to an interface or outbound from an interface, traffic policies automatically work in both directions. Traffic policy configuration can be simpler than ACL configuration for this reason, since the administrator does not need to worry about building consistent input and output ACLs.

## **Configuring Traffic Policies**

To configure traffic policies, navigate to **Configuration > Security > Policies** as shown in the figure below.

Name	Rule Count	Policy Usage	Action	
control	5	ap-role stateful logon	Edit Delete	2
Internet_Only	0	guest	Edit Delete	•
captiveportal	3	logon	Edit Delete	•
allowall	1	trusted-ap employee default-vpn-role IT-staff	Edit Delete	•
test	1	Not Assigned	Edit Delete	•
srcnat	1	Not Assigned	Edit Delete	•
vpnlogon	5	logon	Edit Delete	•
cplogout	1	Not Assigned	Edit Delete	•
guest	0	Not Assigned	Edit Delete	2
stateful-dot1×	0	Not Assigned	Edit Delete	2
ap-acl	5	ap-role	Edit Delete	•
stateful-kerberos	5 1	Not Assigned	Edit Delete	2
Add				

FIGURE 5-3 Traffic Policies



To edit or delete existing policies, click the appropriate button. Note that some policies are system policies and cannot be deleted. The Policy Usage column will display which user roles currently have a policy applied – if a policy is in use, it cannot be deleted. To delete a policy that is in use, first edit the user role and delete the policy, then return to the policies screen to delete it.

To add a new policy, click the Add button. The "Add New Policy" screen appears, as shown in the figure below. Supply a descriptive name for the new policy, and click **Add** under **Rules** to begin adding rules.

Policy Name						I	nternet_Only
Rules							
Source	Destination	Service	Action Log	Queue	Action		
Add							
Source	Destination	Service	Action	Log	Queue		
any -	any 🔹	any _	permit 💌		⊙Low ◯ High		
				Can	cel Add		
							Appl



#### Source/Destination

Identical parameters are available for both source and destination selection. Traffic policies are bi-directional, and will match traffic in either direction. A packet will match a particular rule in the traffic policy only if the rule is matched exactly, meaning that source address, destination address, and service all match. However, traffic policies are stateful. For example, when a wireless user generates a DNS request to a DNS server, the traffic policy will automatically create a session entry for the response so that the response will be permitted. Because traffic policies are stateful, it is not necessary to configure separate rules for inbound and outbound traffic. All packets that match an identified flow will receive the same treatment by the traffic policy.

Five choices exist for both source and destination.

Any - Alias that represents any IP address.

**User** -Alias that represents the user's IP address. When a traffic policy containing the "user" alias is applied to an authenticated user, this alias is replaced by the IP address assigned to that user. With this alias, generic traffic policies can be configured that will automatically be customized at the time of user login.

Host - A single IP address.

**Network -** An IP subnet, consisting of a network number and subnet mask.

**Alias –** When Alias is selected, allows selection of a pre-defined source/destination alias, or creation of a new one. See the section of this guide entitled "Source/Destination Aliases" for more information on these aliases.

#### Service

Traffic flows are identified in part by their service type. A service type may be defined by IP protocol number, TCP port number(s), or UDP port number(s). Four options are available for service selection:

Any – Represents any service.

**TCP** – Matches TCP packets destined to the specified port(s). To specify a single port, enter it in the Port1 field. To specify a range of ports, enter the lower port number in the Port1 field, and the upper port number in the Port2 field.

**UDP** – Matches UDP packets destined to the specified port(s). To specify a single port, enter it in the Port1 field. To specify a range of ports, enter the lower port number in the Port1 field, and the upper port number in the Port2 field.

**Service** – Matches a pre-defined service alias, and also provides the ability to create a new service alias by clicking the "New" button. The use of a service alias allows for a more easily readable and understandable policy. For more information about service aliases, please see the section of this guide entitled "Service Aliases".

**Protocol** – Matches an IP protocol number. For example, IPSec ESP uses protocol number 50 (IPSec ESP is also a pre-defined service alias called "svc-esp".)

#### Action

The traffic policy action defines what the disposition of packets matching the rule will be. Five options are available:

**Permit –** Forwards the packet unmodified

**Deny –** Silently drops the packet



**Src-nat** – Changes the source IP address of the packet. If no source NAT pool is specified, the packet will be given the source IP address of the Alcatel switch. If a NAT pool is specified, the packet will be given an IP address from the NAT pool. Add a new NAT pool by clicking **New**, or manage NAT pools by navigating to **Configuration > Security > Advanced > NAT Pools**.

**Dst-nat** – Changes the destination IP address of the packet to that of the Alcatel switch. Used primarily for intercepting VPN sessions to outside VPN concentrators or for captive portal authentication.

**Redirect** – The redirect action does not modify the packet, but changes the internal destination of the packet. This action is configured automatically by the system when Stateful 802.1x is enabled. This action can also be configured by the administrator to redirect packets to tunnel interfaces.

#### Log

If the "Log" option is checked, all packets matching the rule will be recorded in the system logfile. Use caution when enabling this option for high-volume traffic, since the logfile will quickly grow very large.

#### Queue

Select this action to place packets outbound to wireless users in either a high or low priority queue. AOS-W uses strict queueing, meaning that any time packets are waiting in the high priority queue, they will be transmitted ahead of packets in the low priority queue.

#### Rule Ordering

After rules have been defined the order of rules may be changed by clicking on the up arrow or down arrow next to each rule, as shown in the figure below. The order of rules is important, since policies are executed from the first rule sequentially to the last rule.

Policy Name	e						Internet_Only
Rules							
Source	Destination	Service	Action	Log	Queue	Action	
user	alias "Internal_Network"	"svc-dhcp"	permit		low	Delete 🔺 🔻	
user	alias "Internal_Network"	"svc-dns"	permit		low	Delete 🔺 🔻	
user	alias "Internal_Network"	any	deny		low	Delete 🔺 🔻	
user	any	"svc-http"	permit		low	Delete 🔺 🔻	
user	any	"svc-https"	permit		low	Delete 🔺 🔻	
user	any	"svc-ike"	permit		low	Delete 🔺 🔻	
user	any	"svc-ike"	permit		low	Delete 🔺 🔻	
user	any	any	deny		low	Delete 🔺 🔻	
Add							
							Apply

FIGURE 5-5 Rule Ordering

## **CLI** Configuration

All CLI configuration for traffic/firewall policies is done under the ip access-list session command. Equivalent CLI configuration for the example shown above is:

```
ip access-list session Internet_Only
user alias Internal_Network svc-dhcp permit
user alias Internal_Network svc-dns permit
user any svc-http permit
user any svc-https permit
user any svc-ike permit
user any any deny
```

Applying Traffic Policies to Physical Ports

Traffic policies can be applied either to user roles, as described below in the **User Roles** section, or to physical ports. To apply traffic policies to a physical port, navigate to **Configuration > Switch > Port**. Select the port to which the policy should be applied, then select the policy under **Firewall Policy** as shown in the figure below.



Configure Selected Ports	
Enable Port	V
Enable 802.3af Power Over Ethernet	
Enable Cisco Power Over Ethernet(Enabling this option will disable 802.3af Power Over Ethernet)	
Make Port Trusted	
Port Mode	⊙ Access O Trunk
Enter VLAN(s)	< 1 -
Firewall Policy	guest 🗨
Enable MUX	

#### FIGURE 5-6 Applying Traffic Policies to Ports

To add traffic policies to ports using the CLI, use the following format:

interface fastethernet 2/13
ip access-group guest session

#### **Firewall Policies**

This section provides an ordered list of traffic policies applied to the user role. Traffic policies are executed in order, with an implicit "**deny all**" after the final policy. For more information on firewall and traffic policies, see the section entitled "**Firewall and Traffic Policies**."

To apply a new policy to the user role, click Add.

Choose from Configured Policies control	Location 0.0.0
C Create New Policy From Existing Policy control	Create
C Create New Policy Create	
	Done

FIGURE 5-7 User Role Traffic Policies

Three options are available when adding new traffic policies to a user role:

**Choose from Configured Policies** – Select this option to apply a traffic policy already configured in the system. By default, the policy will be applied to the user role regardless of where the user is physically located (indicated by Location 0.0.0). However, if the policy only applies while the user is associated to a particular AP or is located in a particular building or floor, fill in the

"Location" field on this line. See the chapter entitled "Wireless LAN Configuration – Advanced Location-Based AP Configuration" for more information on location codes.

**Create New Policy From Existing Policy** – Select this option to create a new traffic policy by copying an existing one. The next screen will allow modification of the newly created policy as well as selection of a location code. See the section entitled "Firewall and Traffic Policies" for information on building traffic policies.

dc=AlcateInetworks, dc=com

**Create New Policy –** Create an entirely new traffic policy. The next screen will allow editing of the newly created policy as well as selection of a location code. See the section entitled "Firewall and Traffic Policies" for information on building traffic policies.

Multiple traffic policies may be applied to a user role. When multiple traffic policies are applied, they behave as a single policy – that is, once a rule is matched in the policy and action is taken, no further rules are processed in the policy. Rules are executed from top to bottom, so the placement of rules within a policy and of policies within a user role is important. When multiple traffic policies are applied to a user role, their position within the role may be adjusted using the up and down arrows, as shown in the figure below.

Firewall Policies									
Name	Rule Count	Location	Action						
control	5	0.0.0	Edit Delete 🔺 🔻						
guest	0	0.0.0	Edit Delete 🔺 🔻						
Add	Add								

FIGURE 5-8 Multiple Policies

### Other Role Parameters

**Re-authentication Interval** – By default, once a user has been authenticated that user will remain authenticated until the login session is terminated. If this parameter is set, re-authentication will be required on a periodic basis. If re-authentication is unsuccessful, the user will be denied access to the network.



Security Options | 69

**Role VLAN ID** –This parameter allows the user to be mapped to a particular VLAN based on the role assigned. This parameter only works when using L2 authentication such as 802.1x, MAC address role mapping, ESSID role mapping, or encryption type role mapping, because these happen before an IP address has been assigned. If a user authenticates using a L3 mechanism such as VPN or captive portal, this parameter has no effect.

**Bandwidth Contract** – Applies a bandwidth contract, or rate limiting policy, to the user role to prevent any one user from monopolizing network resources. Bandwidth contracts may be viewed or edited by navigating to **Configuration > Security > Advanced > Bandwidth** Contract. A new bandwidth contract may also be created while adding or editing a user role – to do this, select **Add New**, supply a name for the bandwidth contract, and fill in the desired bandwidth limit either in kilobits per second or in megabits per second. Bandwidth contracts are part of the user role, but are applied independently on a per-user basis. For example, if two users are active on the network and both are part of the same role with a 500kbps bandwidth contract, then each user will be able to use up to 500kbps.

**VPN Dialer –** If VPN is used is an access method, a user may login using captive portal and download a customized VPN "dialer". This dialer is a Windows application that configures the VPN client built into Microsoft Windows 2000 and Windows XP. The VPN dialer may be customized based on the user role. This parameter specifies which customization profile should be available for download to users who are part of this user role. See the section entitled "**Configuring VPN Settings**" for more information on setting up VPN dialers.

L2TP Pool – If VPN is used as an access method, specifies which address pool the user's IP address should be assigned from when the user negotiates an L2TP/IPSec session. Address pools are configured under **Configuration >** Security > VPN Settings > IPSec > Address Pools. See the section entitled "Configuring VPN Settings" for more information on setting up L2TP/IPSec.

**PPTP Pool** – If VPN is used as an access method, specifies which address pool the user's IP address should be assigned from when the user negotiates a PPTP session. Address pools are configured under **Configuration > Security > VPN Settings > PPTP > Address Pools**. See the section entitled "**Configuring VPN Settings**" for more information on setting up PPTP.

## Access Control Lists

Access Control Lists (ACLs) are a common way of restricting certain types of traffic on a physical port. (ACLs can be applied on a per user, per group, as well as a per port basis.) Standard and extended ACLs are both available for compatibility with router software from other popular vendors. However, traffic policies provide equivalent and greater function than standard and extended ACLs, and should be used instead. When filtering non-IP traffic on a

physical port basis, MAC address ACLs and Ethertype ACLs are both available. All ACL configuration is done through the CLI – because these options are not often used, no GUI configuration is available.

ACLs are applied to interfaces using the *ip* access-group command. The direction of traffic to which the ACL is applied must also be specified, using either the keywords *in* or *out*. For example:

```
interface FastEthernet 1/21
ip access-group IP-only in
```

## Standard ACLs

A standard ACL permits or denies traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range of 1 to 99 and 1300 to 1399. Standard ACLs use a bitwise mask (sometimes inaccurately called an "inverse netmask") to specify which portion of the address should be matched.

Sample configuration:

```
ip access-list standard 1
    permit 1.0.0.0 0.255.255.255
    permit host 10.1.1.3
    deny any
```

The example above permits any traffic from the subnet 1.0.0.0/8. It also permits traffic from a host with IP address 10.1.1.3. All other traffic is denied.

## Extended ACLs

Extended ACLS permit or deny traffic based on source or destination IP address, source or destination port number, or IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range of 100 to 199 and 2000 to 2699. The command syntax follows standard Cisco IOS conventions, and extensive context-sensitive help is available by pressing the ? key after each keyword entry.

Sample configuration:

```
ip access-list extended 101
    permit tcp any host 1.1.1.1 range 67 69
```



permit icmp 1.1.1.0 0.0.0.255 any echo-reply

The example above permits TCP traffic from any host to 1.1.1.1 on ports 67 through 69. It also permits ICMP echo-replies from the 1.1.1.0/24 subnet to any network.

## MAC ACLs

A MAC ACL is used to filter on a specific source MAC address or range of MAC addresses. MAC ACLs can be either named or numbered, with valid numbers in the range of 700 to 799 and 1200 to 1299.

Sample configuration:

ip access-list mac 700
permit host 00:01:01:04:cf:b2
permit 00:03:01:00:00 ff:ff:ff:00:00:00

The sample above permits a specific host with MAC address 00:01:01:04:cf:b2. Also permits any MAC address with the prefix of 00:03:01.

## **Ethertype ACLs**

Ethertype ACLs are used to filter based on the ethertype field in the frame header. These ACLs could be used, for example, to permit IP while blocking other non-IP protocols such as IPX or AppleTalk. Ethertype ACLs can be named or numbered, with valid numbers in the range of 200 to 299.

Sample configuration:

ip access-list eth IP-only permit 2048

The above ACL permits only IP traffic. IP is ethertype 0x800 (hex) or 2048 (decimal). The ethertype can also be entered in hex using "0x" to precede the ethertype value.

## **Authentication and Accounting Servers**

All strong authentication methods (meaning that the user identity is validated) must use some type of authentication server. In an Alcatel switch, the authentication server may be an internal database, or may be an external RADIUS or LDAP server. MAC address "authentication" also can make use of an authentication server, simplifying access control when many MAC-authenticated devices (such as VoIP handsets) are used in a network. To configure general authentication server settings, navigate to **Configuration > Security > AAA Servers > General**, as shown in the figure below.

Authentication Timers	
User Idle Timeout (minutes)	5
Authentication Server Dead Time (minutes)	10
	Apply

FIGURE 5-9 AAA General Parameters

Configuration parameters for this section are:

**User Idle Timeout** – Determines the maximum amount of time a user may remain idle before being deauthenticated and removed from the system. The default is 5 minutes.

Authentication Server Dead Time – Determines the maximum amount of time an authentication server may remain unresponsive before it is considered down. Multiple authentication servers may be configured for each authentication method – if the first server in the list is down, the request will be sent to the second server.

The equivalent CLI configuration for the example above is:

aaa timers idle-timeout 5 aaa timers dead-time 10

## RADIUS

RADIUS is the most commonly used type of authentication server. RADIUS is flexible, extensible, and has a high degree of interoperability. To configure RADIUS server settings navigate to **Configuration > Security > AAA Servers > RADIUS**, as shown in the figure below.



Name	IP Address	Authentication Port	Accounting Port	Status	Action
test	1.1.1.1	1812	1813	Enabled	Edit Delete
Add					

#### FIGURE 5-10 RADIUS Server Configuration

A list of currently configured RADIUS servers appears in this section. To edit or delete an existing server, click the appropriate button. To add a new RADIUS server, click the "Add" button as shown in the figure below.

Server Name		Auth2
IP Address		192.168.24.2
Shared Secret		•••••
Verify Shared Secret		•••••
Authentication Port		1812
Accounting Port		1813
Num Retries		3
Timeout		5
Mode		Enable 💌
Server Rules		
Rule Action Attribute Condition Matching Value	Value Action	
Add		
		Apply

FIGURE 5-11 Add RADIUS Server

Available configuration parameters when adding a RADIUS server are:

**Server Name** – Supply a human-readable name for the RADIUS server. This name will be referenced in other parts of the configuration when this RADIUS server is used.

**IP Address -** Specifies the IP address of the RADIUS server.

**Shared Secret** – Each RADIUS client-server pair must use a shared secret. Treat this shared secret as a password, and ensure that it is not an easily-guessed word. Ensure that the shared secret is configured identically on the RADIUS server.

**Authentication Port –** Specifies the UDP port number over which RADIUS exchanges will take place. The default is 1812 – this value is typically used by most modern RADIUS implementations.

**Accounting Port –** When RADIUS accounting is enabled, this value specifies the UDP port number over which RADIUS accounting exchanges will take place. The default is 1813 – this value is typically used by most modern RADIUS implementations.

**Num Retries –** Specifies the number of times that the Alcatel switch will send authentication requests without receiving a reply

**Timeout -** Specifies how long, in seconds, the Alcatel switch will wait for a response from the RADIUS server for each request sent.

**Mode** – Enables or disables use of this RADIUS server. A server may be disabled, for example, when the server will be offline for maintenance.

The equivalent CLI configuration for the example above is:

aaa radius-server "Auth2" host 192.168.24.2 key abc123

authport 1812 acctport 1813 retransmit 3 timeout 5

mode "enable"

Server Rules

For each authentication server used by the system, a server rule may be configured to specify how role and VLAN information is determined. Role and VLAN determination may be done simply by specifying a default value per authentication type, or the information may be learned from the authentication server through a RADIUS attribute. Any attribute may be used – the server rule specifies how that attribute is mapped into a role or VLAN. Server rules are executed in order, and multiple server rules may be configured for each authentication server. To add a new server rule, click the "Add" button.



Rule Type	Role Assignment 💌
Attribute	Framed-Compression Framed-MTU Filter-Id Framed-Routing
Condition	value-of 💌
Value	
Role/Vlan	ap-role 🗾

FIGURE 5-12 Add RADIUS Server Rule

Available configuration parameters are:

**Rule Type** – Specifies if the server rule is used to determine role assignment or VLAN assignment.

**Attribute** – Specifies a RADIUS attribute that will contain role or VLAN information.

**Condition** – Specifies how the system will match the attribute. If the condition is set to "value-of", the contents of the attribute will be treated literally as the role or VLAN assignment. For example, if the attribute is set to "Filter-ID" and the condition is set to "value-of", the RADIUS server will return the value of "IT-Staff" in side the Filter-ID attribute to set the user's role to "IT-Staff".

**Value** – If the condition is set to any option other than "value-of", the value specifies what the contents of the attribute should be in order to match the rule. For example, if the attribute is set to "Filter-ID", the condition is set to "equals", and the value is set to "IT", a role can be selected when the RADIUS server returns the Filter-ID attribute containing the value "IT".

Role/VLAN - Specifies the role or VLAN that will be set if the rule is matched.

The equivalent CLI configuration for the example above is:

aaa derivation-rules server Auth2 set role condition

"Filter-Id" value-of

## LDAP

LDAP (Lightweight Directory Access Protocol) is a lightweight protocol for accessing directory services. A directory is a specialized database optimized for searching, reading and browsing. Directories tend to contain descriptive, attribute-based information. LDAP is specifically geared towards X.500 based directory services and runs over TCP/IP.

## LDAP Background

The LDAP information model is based on *entries*, where an entry is a collection of *attributes*. An attribute has a *type* and one or more *values*. A type is typically a mnemonic string, for example, "cn" for *Common Name*, or "mail" for *Email Address*. The syntax of an attribute's value depends on the type of the attribute. It can be a string, for example, the value "John Doe" for "cn", or a binary JPEG format value for an attributes in an entry through the use of a special attribute called *objectClass*. An objectClass defines the attributes for an entry, and specifies which attributes are required, and which ones are optional. In addition to the attributes that comprise an entry, protection and privacy mechanisms for an entry can be specified in LDAP. Access rights for performing the *read/write/search* operations on the entry can be defined for each entry.

In LDAP, the directory entries are organized in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries. For example, entries representing countries appear at the top of the tree. Below them are entries representing states and national organizations. Below them may be entries representing organizational units, people, printers, documents etc. An example LDAP directory for an organization is shown below.





FIGURE 5-13 LDAP Directory Structure

An entry at a given level in the directory's tree structure is identified by a Relative Distinguished Name (or RDN). For example, the RDN of a user "John Doe" in an NIS based organization is "uid=jdoe" or "cn=John Doe". The attribute that is used to specify the Login ID in the RDN is called the *key attribute*. The Distinguished Name is used to identify an entry uniquely in a global namespace. It identifies an entry in the entire tree. It is built by incorporating the names in the tree along the path that lead up to the entry. For example, the DN for the entry corresponding to user "John Doe", in our example, would be: "uid=jdoe, ou=People, dc=AlcateInetworks, dc=com". There is usually one entry in the directory that has special privileges: the *root/admin* entry. This entry usually has read/write/search privileges over all the entries in the directory.

LDAP provides an API for interrogating and updating the directory. Although LDAP supports operations to add, delete and update an entry, it is primarily used to search for information in the directory. The LDAP search operation allows the user to specify the portion of the directory that should be searched. In addition, a *search filter*, can be used to specify the criteria that should be looked for in the entries that are being searched for.

In addition to the above operations, LDAP supports access control by providing a mechanism for a client to authenticate itself to the server. Typically, a **root** or **admin** entry in the directory has access privileges to all the entries in the directory. Some implementations, like Active Directory for example, do not allow even the **root** entry to read the password attribute of another entry in order to protect the privacy of an entry. During client authentication, the client should supply the distinguished name of the entry that it is trying to connect as, and the password for the entry.

and server is a TCP connection, there is a possibility for a third party to snoop the password from the connection. LDAP supports a more secure connection mechanism through SSL/TLS.

There are a number of LDAP server implementations that are deployed by organizations including the OpenLDAP server, the Netscape Directory Server and the Microsoft Active Directory.

#### Configuring LDAP Servers

To configure LDAP servers, navigate to **Configuration > Security > AAA Servers > LDAP Servers**, as shown in the figure below.

Security	> AAA S	Servers	> LDAP Ser	vers >	> Add	LDAP Sei	rver
Server Name							
Is Server Activ	ve Directory						
IP Address							
Authentication	n Port						
Base DN							
Admin DN							
Admin Passwo	rd						
Verify Admin P	assword						
Key Attribute							
Filter							
Timeout							
Mode						Enable 🔽	
Server Rule	s						
Rule Type Add	Attribute	Condition	Matching Value	¥alue	Action		
							Apply

FIGURE 5-14 LDAP Server Configuration

Available configuration parameters are:



**Server Name –** Specifies a human-readable name to reference the LDAP server.

Host Name/IP Address - Specifies the IP address of the LDAP server.

**Authentication Port –** The port on which the LDAP server is configured. The default value is 389.

**Base DN** - The Distinguished Name of the node which contains the entire user database that should be used for user authentication.

Admin DN - A user who has read/search privileges across all the entries in the LDAP database. The user need not have write privileges – the user should be able to search the database and read attributes of other users in the database.

Admin Password - The password of the "Admin" user defined above.

**Key Attribute -** The attribute that contains the unique key for the LDAP object. This is the name of the attribute that contains the login ID of the users.

**Filter -** The filter that should be applied to search of the user in the LDAP database. The default filter string is: "(objectclass=\*)".

**Timeout –** The amount of time that an LDAP request can go unanswered by the LDAP server before that server is considered down.

Mode - Administratively enables or disables use of this LDAP server.

The equivalent CLI configuration for the example above is:

```
aaa ldap-server LDAP1
host 10.1.1.214
authport 389
base-dn "cn=Users,dc=lm,dc=Alcatelnetworks,dc=com"
admin-dn "cn=Alcatel
Admin,cn=Users,dc=lm,dc=Alcatelnetworks,dc=com"
admin-passwd abc10
key-attribute sAMAccountName
filter "(objectclass=*)"
timeout 20
mode enable
```

#### Server Rules

For each authentication server used by the system, a server rule may be configured to specify how role and VLAN information is determined. Role and VLAN determination may be done simply by specifying a default value per authentication type, or the information may be learned from the authentication server through an attribute. Any attribute may be used – the server rule specifies how that attribute is mapped into a role or VLAN. Server rules are executed in order, and multiple server rules may be configured for each authentication server. To add a new server rule, click **Add**.

Rule Type	Role Assignment 💌
Attribute	Role
Condition	value-of 💌
Value	
Role/Vlan	ap-role 💌
	Done

#### FIGURE 5-15 Add LDAP Server Rule

Available configuration parameters are:

**Rule Type** – Specifies if the server rule is used to determine role assignment or VLAN assignment.

Attribute - Specifies an attribute that will contain role or VLAN information.

**Condition** – Specifies how the system will match the attribute. If the condition is set to "value-of", the contents of the attribute will be treated literally as the role or VLAN assignment. For example, if the attribute is set to "Filter-ID" and the condition is set to "value-of", the LDAP server will return the value of "IT-Staff" in side the Filter-ID attribute to set the user's role to "IT-Staff".

**Value** – If the condition is set to any option other than "value-of", the value specifies what the contents of the attribute should be in order to match the rule. For example, if the attribute is set to "Filter-ID", the condition is set to "equals", and the value is set to "IT", a role can be selected when the LDAP server returns the Filter-ID attribute containing the value "IT".

Role/VLAN – Specifies the role or VLAN that will be set if the rule is matched.

The equivalent CLI configuration for the example above is:

aaa derivation-rules server LDAP1 set role condition
 "role" value-of



## **Internal Authentication Database**

AOS-W supports an internal authentication database that can be used when an external authentication server is unavailable or undesirable. This database is available when using VPN, captive portal, or MAC-based authentication. 802.1x requires an external RADIUS server, and is not capable of utilizing the internal database. To configure the internal database, navigate to **Configuration > Security > AAA Servers > Internal Database**, as shown in the figure below.

Server Rules	3					
Rule Action	Attribu	ite Condi	tion M	atching Valu	je Value	Action
Role Assignm	ent Role	value-c	of			Delete 🔺 🔻
Add						
Users						
Licer Name	Daccword	Dolo	E-mail	Enabled	Action	
demo	*****	employee	L-IIIdii	Yes	Delete	
Add User						

#### FIGURE 5-16 Internal Authentication Database

The internal database contains fields for username, password, role, email address, and administrative status. A role assignment rule is automatically configured by the system to enable role assignment by the internal database. If additional role or VLAN assignment rules are desired, click **Add**.

To add users, click the "**Add User**" button and fill in appropriate details for each user. The internal database supports up to 4000 user entries.

CLI configuration to add a user to the internal database is done from command mode, rather than configuration mode:

local-userdb	add	username	demo	password	abc123	role
employee						

## Accounting

AOS-W supports standard RADIUS accounting for tracking user login/logout times. Accounting will track logins accurately, but logouts may not be tracked accurately since the user may roam out of range without logging out. To configure accounting, navigate to Configuration→Security→AAA Servers→Accounting, as shown in the figure below.

Enable Accounting							
Name	IP Address	Accounting Port	Status	Actions			
test	1.1.1.1	1812	Enabled	Delete			
Choose an Authentication Server							
Add Cancel							

FIGURE 5-17 RADIUS Accounting

Configuration parameters are:

Enable Accounting – Specifies whether or not accounting will be enabled.

**Server** – Specifies a list of configured RADIUS servers to which accounting data will be sent. Servers must be configured under **Configuration > Security > AAA Servers > RADIUS** before they appears as available options.

The equivalent CLI configuration for the example above is:

aaa radius-accounting mode enable aaa radius-accounting auth-server test

# **Authentication Methods**

Authentication provides a way to identify a user and provide appropriate access to the network for that user. By default, all wireless users in an Alcatel network start in the "logon" role, and use an authentication method to move to an identified, authenticated role. One or more authentication methods may be used, ranging from secure authentication methods such as 802.1x, VPN, and captive portal to less secure "role mapping". Role mapping should always be combined with firewall policies to provide enhanced security.



Once an authentication method has been enabled on the switch, it is automatically available for all ESSIDs configured on that switch.

## 802.1x Authentication

802.1x is an IEEE standard designed to provide authentication before any L2 access to the network is permitted. 802.1x provides a framework inside of which multiple authentication protocols may operate. A number of authentication protocols, including EAP-TLS, PEAP, and TTLS are ideally suited for wireless network, most notably because they allow the client to authenticate the network as well as allowing the network to authenticate the client. The authentication protocols are all based on EAP (Extensible Authentication Protocol) and are also known as "EAP types".

An 802.1x system consists of three parts. The *supplicant*, or client, is the device attempting to gain access to the network. The *authenticator* is the "gatekeeper" to the network, either permitting or denying access to supplicants. Finally, the *authentication server* provides a database of authentication information and signals the authenticator whether or not access should be permitted. An Alcatel switch acts as an authenticator, relaying authentication requests between the supplicant and the authentication server. The Alcatel switch implements the 802.1x framework, but is transparent to different authentication protocols within 802.1x. As long as the supplicant and authentication server support compatible authentication protocols, the Alcatel switch will interoperate with all EAP types.

To configure 802.1x, navigate to **Configuration > Security > Authentication Methods > 802.1x** as shown in the figure below.

Configuration							
Faitch	Ulagnostics Maintenance Main Events Reports Save Comingulation Logiout						
General	Security > Authentication Methods > Captive Portal Authentication						
Management WLAN	802.1x VPN Captive Portal MAN	C Address Stateful 802.1x	SSID L2 Encryption Advanced				
Network	Authentication Enabled						
Radio	Defe & Dala						
RF Management Calibration	Enable Guest Logon	Г					
Optimization	Enable User Logon	<b>v</b>					
Protection	Enable Logout Popup Window						
Monitoring Advanced	Protocol Type	C http @ https					
	Redirect Pause Time(secs)	10					
Roles	Welcome Page Location	/auth/welcome.html					
Policies	Logon Wait Interval	5 - 10 seconds					
AAA Servers	CPU Utilization Threshold	60 %					
VPN Settings	Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)					
Firewall Settings							
Advanced							
WLAN Intrusion Protection	Authentication Servers						
Rogue AP	Name Type IP Address Authentication Port Status Actions						
Man In the Middle	radon Radius 10.4.0.21 1812	Enabled Delete * *					
Signatures	Add	Apply					
Policies							
	Announce of the second s						
	Commands	View Con	mands				

#### FIGURE 5-18 802.1x Configuration

To enable 802.1x authentication with minimal configuration:

- 1. Click the "Enable Authentication" checkbox.
- 2. Select a default role.
- 3. Add an authentication server.

Available configuration parameters are:

**Default Role** – If a client authenticates using 802.1x, and the authentication server does not provide role information, the default role will be given to the client.

Enable authentication - Enables or disables 802.1x authentication.

**Authentication Server Timeout –** Specifies the delay period between authentication retries. The value can be between 1-65535 seconds. The default is 30 seconds.

**Client Response Timeout** – Sets the period between each identity request sent to the supplicant by the authenticator. The ID request is sent when a client associates or reassociates with an AP or when the reauthentication time expires. The value can be between 1-65535 seconds. The default is 30 seconds.



**Authentication Failure Timeout** – After authentication fails, the 802.1x state machine enters a quiet period specified by this value, during which the authenticator will make no attempt to acquire the supplicant. The value can be between 1-65535 seconds. The default is 30 seconds.

**Client Retry Count** – Sets the maximum number of attempts the switch will make to authenticate a supplicant. The value can be between 0 and 10. The default value is 3.

**Server Retry Count** – Specifies the number of attempts the switch may make to obtain authentication from the server after an initial attempt times out. The value can be between 0 and 3. The default value is 2.

**Enable Reauthentication –** Forces supplicants to reauthenticate after the reauthentication time interval has elapsed since the last authentication. Unicast keys are updated after each reauthentication. The default is disabled.

**Reauthentication Time Interval –** If reauthentication is enabled, specifies the time interval since the last successful authentication after which the client will be forced to reauthenticate. The value can be between 1 and 4,294,967,295 seconds. The default value is 3600 seconds.

**Enable Multicast Key Rotation –** Enables periodic rotation of multicast encryption keys. Multicast keys are used to encrypt broadcast and multicast frames that must be sent to all wireless clients. The default is disabled.

**Multicast Key Rotation Time Interval –** When multicast key rotation is enabled, specifies the amount of time that must elapse since the last key rotation until a new multicast key rotation is done. The value can be between 1 and 4,294,967,295 seconds. The default value is 1200 seconds.

**Enable Unicast Key Rotation –** Enables periodic rotation of unicast encryption keys. The default is disabled.

**Unicast Key Rotation Time Interval –** When unicast key rotation is enabled, specifies the amount of time that must elapse since the last key rotation until a new unicast key rotation is done. The value can be between 1 and 4,294,967,295 seconds. The default value is 240 seconds.

**Reset 802.1x Parameters to Factory Defaults –** Check this box to reset all 802.1x settings back to default values. The equivalent CLI configuration command is "dot1x default".

Authentication Failure Threshold for Station Blacklisting – If a station fails 802.1x authentication by this number of times in a row, the station will be "blacklisted" and will not be allowed to associate to the network. Enter 0 to disable blacklisting.
The equivalent CLI configuration for the example above is:

```
aaa dot1x default-role "employee"
aaa dot1x mode enable
dot1x server server-timeout 30
dot1x timeout idrequest-period 30
dot1x timeout quiet-period 30
dot1x max-req 3
dot1x server server-retry 2
dot1x re-authentication
dot1x timeout reauthperiod 3600
dot1x multicast-keyrotation
dot1x timeout mcastkey-rotation-period 1200
dot1x unicast-keyrotation
dot1x timeout ucastkey-rotation-period 240
aaa dot1x max-authentication-failures 0
```

#### 802.1x Authentication Server

802.1x authentication requires the use of an authentication server that supports the same EAP type as that used by the client. 802.1x authentication servers may be configured below the 802.1x configuration screen, as shown in the figure below.

Authentication Servers								
Name	Туре	IP Address	Authentication Port	Status	Actions			
test	Radius	1.1.1.1	1812	Enabled	Delete 🔺 🔻			
Choose	an Authe	ntication Server			Apply			
	Add C	ancel						

FIGURE 5-19 802.1x Authentication Server

To add an authentication server, click the "Add" button. One or more servers may be added to the list. To change the order in which servers are used by the system, click the up or down arrows next to the appropriate server name.

The equivalent CLI command to add the server shown above is:

```
aaa dot1x auth-server test
```



## **VPN** Authentication

When the use of IPSec or PPTP is desired, Alcatel switches provide full VPN termination capabilities using hardware acceleration. All encryption protocols are run in hardware, with encryption hardware being appropriately sized to handle a full load of access points. The majority of VPN settings are configured under a dedicated VPN section below. VPN backend authentication parameters are configured under **Configuration > Security > Authentication Methods > VPN**, as shown in the figure below.

Authent	ication En	abled					
Default	Role		default-vpn-role 💌				
Authent	ication Fa	ilure Threshold f	0 (0 disa	ables blacklisting)			
Auther	Authentication Servers						
Name	Туре	IP Address	Authentication P	ort Status	Actions		
Internal	Local	172.16.1.100	n/a	Enabled	Delete 🔺 🔻		
Add					Apply		

#### FIGURE 5-20 VPN Authentication

Available configuration parameters are:

Authentication Enabled - Enables or disables VPN termination.

**Default Role** – If a client authenticates using VPN, and the authentication server does not provide role information, the default role will be given to the client.

**Authentication Failure Threshold for Station Blacklisting –** If a station fails VPN authentication by this number of times in a row, the station will be "blacklisted" and will not be allowed to associate to the network. Enter 0 to disable blacklisting.

**Authentication Servers** – An ordered list of authentication servers to be used when VPN clients attempt to authenticate.

The equivalent CLI configuration for the example above is:

```
aaa vpn-authentication mode enable
aaa vpn-authentication default-role "vpn-role"
```

```
aaa vpn-authentication auth-server Internal
aaa vpn-authentication max-authentication-failures 0
```

# **Captive Portal Authentication**

Captive portal authentication allows a wireless client to authenticate using a web-based portal. Captive portal authentication can be done over SSL, but provides no encryption for user data once authentication has taken place. Therefore, it should be used in environments where encryption is not required, such as when providing Internet access for guest users. To configure captive portal authentication, navigate to **Configuration > Security > Authentication Methods > Captive Portal**, as shown in the figure below. Additional captive portal customization may be done under Maintenance→Captive Portal (see "Captive Portal Maintenance" on page 555).



FIGURE 5-21 Captive Portal Authentication

Available configuration parameters are:

Authentication Enabled – Enables or disables captive portal authentication.

**Default Role –** If a client authenticates using captive portal, and the authentication server does not provide role information, the default role will be given to the client.



**Enable Guest Logon –** When this option is selected, the captive portal page will display a field for guest users to enter their email address. The email address is not validated or authenticated, but can be used to keep track of user identity. When a user enters an email address in the guest logon field, the switch will assign the "guest" role to the user.

**Enable User Logon** – When this option is selected, the captive portal page will display a field for a registered user to enter a username and password. The user will be authenticated against the selected authentication server and will be assigned a role according to either the authentication server role information, or the captive portal default role.

**Enable Logout Popup Window –** If this option is selected, a second web browser window appears after captive portal authentication succeeds. This browser window will contain a button to allow the user to logout of the system.

**Protocol Type –** Selects whether the captive portal page will be transmitted using HTTP or HTTPS (SSL). The default is HTTPS. If HTTP is selected, then usernames and passwords would be transmitted with no encryption, making it possible for anyone to intercept them.

**Redirect Pause Time** – After captive portal authentication succeeds, an "authentication succeeded" page will display, with additional options for downloading a VPN dialer. The page will be displayed for this time interval, after which the browser will be redirected to the original URL requested when the captive portal action took place.

**Logon Wait Interval** – If the switch control CPU is in a high load condition, rendering the captive portal page could cause other higher-priority tasks to slow down. This parameter specifies how long the logon process will be delayed if the CPU is in a highly loaded condition.

**CPU Utilization Threshold -** If the switch control CPU is in a high load condition, rendering the captive portal page could cause other higher-priority tasks to slow down. This parameter specifies the CPU load that must be exceeded in order for captive portal delay to take effect.

Authentication Failure Threshold for Station Blacklisting – If a station fails captive portal authentication by this number of times in a row, the station will be "blacklisted" and will not be allowed to associate to the network. Enter 0 to disable blacklisting.

**Authentication Servers** – An ordered list of authentication servers to be used when clients attempt to authenticate using captive portal.

The equivalent CLI configuration for the example above is:

```
aaa captive-portal default-role "employee"
aaa captive-portal guest-logon
aaa captive-portal user-logon
aaa captive-portal logout-popup-window
no aaa captive-portal protocol-http
aaa captive-portal redirect-pause 10
aaa captive-portal logon-wait range 5 10
aaa captive-portal logon-wait cpu-utilization 60
aaa captive-portal max-authentication-failures 0
aaa captive-portal auth-server Internal
```

# MAC Address Role Mapping

MAC Address "Role Mapping" provides identification of clients based on MAC address and subsequent mapping to a role. This feature should not be considered "authentication", since no secure password is used. Additionally, MAC addresses are not a secure form of identification, since they can easily be modified by client devices. This feature should always be combined with L2 encryption and appropriately restrictive firewall policies. To configure MAC address role mapping, navigate to **Configuration > Security > Authentication Methods > MAC Address**, as shown in the figure below.

Authent	ication En	abled						
Default	Role		guest	•				
Authent	ication Fa	ilure Threshold f	0 (0 dis	ables blacklisting)				
Authentication Servers								
Name	Туре	IP Address	Authentication P	ort Status	Actions			
Internal	Local	172.16.1.100	n/a	Enabled	Delete 🔺 🔻			
Add					Apply			

FIGURE 5-22 MAC Address Role Mapping

Available configuration parameters are:

Authentication Enabled – Enables or disables MAC address role mapping.



**Default Role** – If a client is identified by MAC address, and the authentication server does not provide role information, the default role will be given to the client.

Authentication Failure Threshold for Station Blacklisting – If a station fails MAC address authentication by this number of times in a row, the station will be "blacklisted" and will not be allowed to associate to the network. Enter 0 to disable blacklisting.

**Authentication Servers** – An ordered list of authentication servers to be used when VPN clients attempt to authenticate. The authentication server should be populated with MAC addresses, with no separating characters, in the field normally used for usernames. Passwords should also be the MAC address with no separating characters.

The equivalent CLI configuration for the example above is:

```
aaa mac-authentication mode enable
aaa mac-authentication default-role "guest"
aaa mac-authentication auth-server Internal
aaa mac-authentication max-authentication-failures 0
```

# Stateful 802.1x

#### Third-party Access Points

When third-party access points are used in the network, and those third-party access points act as 802.1x authenticators, AOS-W provides the ability to intercept communication between the AP and the authentication server in order to learn username information and apply appropriate role and traffic policies. This assumes that the Alcatel switch is located in the data path between the third-party AP and the authentication server. To configure stateful 802.1x, navigate to **Configuration > Security > Authentication Methods > Stateful 802.1x**, as shown in the figure below.

Authentication Enabled			•				
Default Role			guest 💌				
Request/Response timeout			20				
Authentication Servers							
Name	Туре	IP Addr	ess	Authentication Port	Status	Actions	
test	Radius	1.1.1.1	1	812	Enabled	Delete 🔺 🔻	
Add							

FIGURE 5-23 Stateful 802.1x Configuration

Available configuration parameters are:

Authentication Enabled - Enables or disables stateful 802.1x authentication.

**Default Role** – If a client authenticates using stateful 802.1x, and the authentication server does not provide role information, the default role will be given to the client.

**Request/Response Timeout** – Specifies the maximum time to wait for a response from the RADIUS server after seeing a RADIUS request from the AP.

**Authentication Servers** – An ordered list of authentication servers to be used when clients attempt to authenticate through stateful 802.1x.

The equivalent CLI configuration for the example above is:

```
aaa stateful-authentication dot1x mode enable
aaa stateful-authentication dot1x timeout "20"
aaa stateful-authentication dot1x auth-server test
aaa mac-authentication max-authentication-failures 0
```

#### **AP/Server Configuration**

After enabling stateful 802.1x as shown above, a list of each third-party AP for which stateful 802.1x should be performed must be entered as shown in the figure below.



AP Server Configuration List						
Cfg-Name	AP-IP	Server	Actions			
Add new AP Serve	r					
Configuration Name	Cisco22	Cisco22				
IP Address	192.168.3	192.168.3.22				
Choose an Radius Serv	er (Server Ty	(Server Type:Radius(test) IP Address:1.1.1.1) 💌				
Кеу	radius-ke	radius-key				
Add Cancel						
Apply						

FIGURE 5-24 Stateful 802.1x AP/Server Configuration

Available configuration parameters are:

**Configuration Name –** Choose a human-readable name to identify the third-party AP.

IP Address - Specify the IP address of the third-party AP.

**RADIUS Server –** Choose the RADIUS server with which the third-party AP will communicate.

**Key –** Specify the RADIUS secret used between the third-party AP and the RADIUS server.

The equivalent CLI configuration for the example above is:

```
aaa stateful-authentication dot1x ap-config Cisco22
ap-ipaddr 192.168.3.22 radius-server-name test key
radius-key
```

#### SSID Role Mapping

SSID Role Mapping allows a role to be assigned based entirely on the ESSID with which the client associates. This is typically used for guest access to completely bypass authentication. Because authentication is bypassed, this method should always be combined with a firewall policy. To configure SSID role mapping, navigate to **Configuration > Security > Authentication Methods > SSID** as shown in the figure below.

Condition	equals 💌
Value	Guest-SSID
Role Name	guest 💽
Apply	

FIGURE 5-25 SSID Role Mapping

Available configuration options are:

**Condition –** Specifies how the value should be matched.

Value - Specifies the SSID that should be matched.

Role Name - Specifies the role that will be applied when the SSID is matched.

Equivalent CLI configuration for the example above is:

```
aaa derivation-rules user
set role condition essid equals "Guest-SSID" set-
value "guest"
```

**NOTE**—When using the CLI to enter ESSID values, the name string may include space characters only if the string is placed within quotes. When spaces are not used, quotes are not required. For example, the following ESSIDs are valid

CompanyESSID#1 "Company ESSID #1" When using the Web Interface, spaces may be used without adding quotes

# **Encryption Type Role Mapping**

Encryption Type Role Mapping allows a role to be assigned based entirely on the L2 encryption type used by the client. This is typically used for guest access to completely bypass authentication. Because authentication is



bypassed, this method should always be combined with a firewall policy. To configure encryption type role mapping, navigate to **Configuration > Security > Authentication Methods > L2 Encryption** as shown in the figure below.

Condition	equals 💽		
Value	Open System 💌		
Role Name	guest 💽		
Apply			

FIGURE 5-26 Encryption Type Role Mapping

Available configuration options are:

Condition - Specifies how the value should be matched.

Value - Specifies the encryption type that should be matched.

**Role Name –** Specifies the role that will be applied when the encryption type is matched.

Equivalent CLI configuration for the example above is:

```
aaa derivation-rules user
set role condition encryption-type equals open set-
value "guest"
```

#### **Advanced Authentication**

To configure advanced security options, navigate to **Configuration > Security > Authentication Methods > Advanced**. The Advanced tab appears in the figure below.

Security > Authentication Methods > Advanced Authentication											
_	802.1x	VPN	Captive P	Portal M/	AC Address		Stateful 802.1x	SS	ID	L2 Encryption	Advanced
	Rule Type	Conditio	n Value	Role Name	Actions						
	Add										

Click Add to create security rules.

# **Configuring VPN Settings**

When the use of IPSec or PPTP is desired, Alcatel switches provide full VPN termination capabilities using hardware acceleration. All encryption protocols are run in hardware, with encryption hardware being appropriately sized to handle a full load of access points. Additionally, built into each switch is a "VPN dialer" Windows application that pre-configures supported Windows systems to work with Alcatel VPN services.

# IPSec

AOS-W supports termination of IPSec tunnels using both L2TP/IPSec (supported natively by Windows 2000, XP, and PocketPC 2003) and IPSec/XAUTH (supported by most 3<sup>rd</sup>-party VPN clients). To configure IPSec, navigate to **Configuration > Security > VPN Settings > IPSec**, as shown in the figure below.



L2TP and	I XAUTH Par	ameters				
Enable L21	"P	V				
Authentica	ation Protocols	PAP		5CHAP 🔽 MSC	HAPv2	
Primary DI	IS Server	0.0.0.0				
Secondary	DNS Server	0.0.0.0				
Primary W	INS Server	0.0.0.0				
Secondary	WINS Server	0.0.0.0				
Address	Pools					
Pool Nan	ne Start Ad	Idress	End Address	Actions		
estl2tppoc	l 10.4.21.80	) 1	0.4.21.100	Edit Delet	e	
Add						
Source N	AT					
Enable So	urce NAT					
NAT Pool		~				
IKE Aggre	ssive Group Nar	me char	igeme (Only r	needed for XAU	TH)	
IKE Shar	ed Secrets					
Subnet	Subnet Mas	sk Lengtl	n Key	Actions		
0.0.0.0	0		***** Ed	lit Delete		
Add						
IKE Polic	ies					
Priority	Encryption	Hash	Authenticati	ion Group	Lifetime	Action
10	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete
Default	3DES	SHA	RSA	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete
Add						
						Apply

FIGURE 5-27 IPSec Configuration

Available configuration parameters are:

**Enable L2TP –** Enables termination of L2TP/IPSec tunnels. This is required when supporting native Windows 2000/XP VPN clients.

**Authentication Protocols –** Configures which authentication protocols will be allowed. The client, Alcatel switch, and backend RADIUS server must all support at least one of these authentication protocols. Generally, it is safe to leave all protocols enabled.

**Primary/Secondary DNS Server –** Configures the list of DNS servers that will be passed to clients after authentication. These parameters are optional.

**Primary/Secondary WINS Server –** Configures the list of WINS servers that will be passed to clients after authentication. These parameters are optional.

**Address Pools** - IPSec tunnel endpoints are assigned IP addresses. The Alcatel switch endpoint will always use the switch IP address, while client addresses are assigned from a pool. To add a new address pool, click the Add button and fill in the pool name and the starting and ending addresses for the pool. Multiple pools may be configured.

**Enable Source NAT** – If the address range included in the VPN address pool is not routable by the rest of the network, source NAT can be enabled. When this is enabled, the source address of all user traffic emerging from a VPN tunnel will be changed to the switch IP address. This checkbox configures a traffic policy for the VPN default role – if multiple roles are being used with VPN, a source-NAT traffic policy will need to be configured for each of them.

NAT Pool - Specifies the name of the NAT pool.

**IKE Aggressive Group Name –** When configuring IPSec XAUTH, enter the group name. This group name must match the group name configured on each client.

**IKE Shared Secrets –** Specifies IKE pre-shared keys for different IP address ranges. This option is only used when IKE pre-shared key authentication is in use. To configure a single IKE pre-shared key for all clients, enter a subnet of 0.0.0.0 with a mask length of 0. The IKE pre-shared key must be identically configured on all clients. The shared secret should be treated as a password, and should not be composed of common dictionary words or phrases.

**IKE Policies –** Specifies encryption, hash, and authentication parameters for IKE. The default policy configures IKE for triple-DES encryption, SHA1 hash, and RSA public/private key authentication. To enable IKE pre-shared keys, add a policy as shown in the example to enable pre-shared key authentication.

The equivalent CLI configuration for the example above is:

```
vpdn group 12tp
  client configuration dns 1.1.1.1 2.2.2.2
  client configuration wins 3.3.3.3 4.4.4.4
  ppp authentication PAP
  ppp authentication CHAP
  ppp authentication MSCHAP
  ppp authentication MSCHAPv2
!
ip local pool 1t2p-pool 172.16.2.1 172.16.2.24
!
crypto isakmp groupname changeme
!
crypto isakmp key test123 address 0.0.0.0 netmask 0.0.0.0
!
```



```
crypto isakmp policy 10
authentication pre-share
```

#### PPTP

PPTP provides an alternative to IPSec that is supported by MacOS, Linux, PocketPC, Windows 2000, Windows XP, and many other platforms. PPTP is considered to be less secure than IPSec, but also requires less configuration. To configure PPTP, navigate to **Configuration > Security > VPN Settings > PPTP** as shown in the figure below.

PPTP Param	eters						
Enable PPTP		◄					
PPTP Echo Tim	eout(secs)	60					
Authentication Protocols		MS MS	MSCHAPv2				
Primary DNS S	erver	1.1.1	1				
Secondary DN	S Server	2.2.2	2.2.2.2				
Primary WINS	Primary WINS Server 3.3		3				
Secondary WI	Secondary WINS Server 4.4		4				
Address Poo	Address Pools						
Pool Name	Start Ad	dress	End Address	Actions			
pptp-pool1	172.16.18.	1	172.16.18.24	Edit Delete			
Add							

#### FIGURE 5-28 PPTP Configuration

Available configuration parameters are:

Enable PPTP	Enables or disables termination of PPTP (Point to Point Tunneling Protocol) clients.
PPTP Echo Timeout	Amount of time, in seconds, that the system will wait for a PPTP echo response from the client before considering the client down. After this interval with no response, the client will be disconnected
Authentication Protocols	Configures the PPTP authentication protocol. Currently, only MS-CHAPv2 is supported.

Primary/Secondar y DNS Server	Configures the list of DNS servers that will be passed to clients after authentication. These parameters are optional.
Primary/Secondar y DNS Server	Configures the list of WINS servers that will be passed to clients after authentication. These parameters are optional.
Address Pools	PPTP tunnel endpoints are assigned IP addresses. The Alcatel switch endpoint will always use the switch IP address, while client addresses are assigned from a pool. To add a new address pool, click the Add button and fill in the pool name and the starting and ending addresses for the pool. Multiple pools may be configured

The equivalent CLI configuration for the example above is:

```
vpdn group pptp
client configuration dns 1.1.1.1 2.2.2.2
client configuration wins 3.3.3.3 4.4.4.4
!
pptp ip local pool "pptp-pool1" "172.16.18.1" "172.16.18.24"
```

# **VPN Dialer Configuration**

AOS-W includes a "VPN dialer" Windows application that pre-configures supported Windows systems to work with Alcatel VPN services. This dialer can be customized for each role, and is downloaded through the captive portal authentication page. After a user authenticates via captive portal, a link appears to allow download of the VPN dialer if a dialer has been configured for the user's role. To configure one or more VPN dialers, navigate to **Configuration > Security > VPN Settings > Dialers**, as shown in Figure 5-29.

Name	Action		
default-dialer	Edit	Delete	
test	Edit	Delete	
Add			

FIGURE 5-29 VPN Dialer List



As shown in the figure, two VPN dialers are currently configured. "Default-dialer" is pre-configured by the system, while "test" was added manually. Each dialer can be applied to a particular user role, and multiple user roles may use the same dialer. To add a new VPN dialer, click the Add button. Dialer parameters are shown as in the figure below.

Dialer Name	
Enable PPTP	
Enable L2TP	<b>v</b>
Send Direct Network Traffic In Clear(Split Tunneling)	
Disable Wireless Devices When Client is Wired	
Enable SecurID New and Next Pin Mode	
Authentication	▼ PAP ▼ CHAP ▼ MSCHAP ▼ MSCHAPv2 □ Cache SecurID Token
IKE Lifetime (secs)	28800
IKE Encryption	€ 3DES C DES
IKE Diffie Hellman Group	€ 2 ∩ 1
IKE Hash Algorithm	€ SHA C MDS
IKE Authentication	C RSA Signatures 📀 Preshared Key Password
IPSEC Lifetime (secs)	7200
IPSEC Mode Group	€ 2 C 1
IPSEC Encryption	€ ESP-3DES C ESP-DES
IPSEC Hash Algorithm	€ ESP-SHA-HMAC C ESP-MD5-HMAC
	Apply

FIGURE 5-30 VPN Dialer Configuration

The minimum required configuration for a VPN dialer is to specify a dialer name and an IKE pre-shared key. Specifying these two parameters and leaving all other parameters at default values will allow most implementations to work.

Available configuration parameters are:

Dialer Name	Enter a human-readable name for the dialer so that it may be easily referenced.
Enable PPTP	Allows the dialer to negotiate a PPTP tunnel with the Alcatel switch.
Enable L2TP	Allows the dialer to negotiate an L2TP/IPSec tunnel with the Alcatel switch.
Send Direct Network Traffic In Clear	Enables "split tunneling" functionality so that traffic destined for the internal network will be tunneled, while traffic for the Internet will not. For security reasons, this option is not recommended.

Disable Wireless Devices when Client is Wired	Allows the VPN dialer to detect when a wired network connection is in use. If this option is enabled, the wireless interface will be shut down while a wired connection exists.
Enable SecurID New and Next Pin Mode	ТВС
Authentication	Specifies the list of authentication protocols to be supported. This list should match the switch IPSec or PPTP configuration, and should also contain at least one protocol supported by the authentication server. It is generally safe to leave all protocols enabled. If SecureID Token Caching is enabled (see the SecureID Token Caching section of this guide below), the system will cache SecureID tokens so that users do not need to reauthenticate every time a network connection is lost.
IKE Lifetime	Specifies how long an IKE security association lasts, in seconds. This parameter must match the IKE lifetime configured in the IPSec IKE policy. The default value is 28,800 seconds.
IKE Encryption	Specifies the IKE encryption protocol. This parameter must match the IKE encryption protocol configured in the IPSec IKE policy. The default value is triple-DES.
IKE Diffie-Hellman Group	Specifies whether IKE will use Diffie-Hellman group 1 or group 2. This parameter must match the IKE Diffie-Hellman group configured in the switch. The default is group 2.
IKE Hash Algorithm	Specifies the hash algorithm used by IKE – either SHA or MD5. This parameter must match the IKE hash algorithm configured in the IPSec IKE policy. The default is SHA.
IKE Authentication	Specifies whether RSA signatures or pre-shared keys should be used for IKE authentication. This parameter must match the "IKE Shared Secrets" configuration. The default is for pre-shared key authentication. Make sure the pre-shared key specified here matches the pre-shared key specified in the IKE shared secrets policy.
IPSec Lifetime	Specifies how long an IPSec security association lasts, in seconds. The default is 7200 seconds.
IPSec Mode Group	Specifies the IPSec Perfect Forward Secrecy (PFS) mode. The default is Group 2.
IPSec Encryption	Specifies the encryption type used for IPSec. The default is triple-DES.



IPSec Hash	Specifies the hash algorithm used by IPSec.	The default
Algorithm	is to use SHA.	

The equivalent CLI configuration for the example above is:

```
vpn-dialer dialer2
enable l2tp
ppp authentication PAP
ppp authentication CHAP
ppp authentication MSCHAP
ppp authentication MSCHAPv2
ike lifetime 28800
ike encryption 3des
ike group 2
ike hash sha
ike authentication pre-share test123
ipsec lifetime 7200
ipsec pfs group2
ipsec encryption esp-3des
ipsec hash esp-sha-hmac
```

#### **VPN Server Emulation**

In multi-campus environments, it may be common for employees to move between campuses with their laptop computers. When this happens, the VPN dialer installed on the laptop will be configured with the IP address of the "home" Alcatel switch. When the user activates the VPN dialer, it will form a connection back to the home office, resulting in sub-optimal performance. The VPN Server Emulation feature configures the Alcatel switch to intercept VPN sessions destined for configured IP addresses, and terminate them locally instead. To configure VPN Server Emulation, navigate to **Configuration > Security > VPN Settings > Emulate VPN Servers**, as shown in Figure 5-31.

IP Address	Action		
1.2.3.4	Delete		
IP Address			
Add Cancel			

FIGURE 5-31 VPN Server Emulation

Configure a list containing the switch IP addresses of all Alcatel switches that could potentially result in the situation described above.

The equivalent CLI configuration for the example above is:

```
ip access-list session vpn-dst-nat
  any host 1.2.3.4 svc-ike dst-nat
  any host 1.2.3.4 svc-esp dst-nat
  any host 1.2.3.4 svc-l2tp dst-nat
  user-role logon
  session-acl vpn-dst-nat position 1
```

# Advanced Authentication

To configure advanced authentication options, select **Configuration > Security > Authentication Methods > Advanced Authentication**.



FIGURE 5-32 Advanced Authentication

To add an advanced authentication method, click **Add** to display the Add Condition screen.

Security > Authentication Methods > Advanced Authentication > Add Condition



FIGURE 5-33 Adding Advanced Authentication Condition

where:

Parameter	Description
Rule Type	Specifies the type of rule to be created.



Condition	Specifies the logical relationship.
Value	Specifies the rule type value.
Role Name	The role name description.

To add the new condition, click Apply.

#### SecureID Token Caching

SecureID Token Caching allows the Alcatel switch to cache SecureID tokens when the user logs in for the first time. For a configurable time interval after initial authentication, the switch will use the cached token any time a user loses and then reestablishes a VPN link. This helps users avoid having to perform a new SecureID authentication procedure each time a network connection is lost.

To configure SecureID Token Caching, navigate to **Configuration > Security > VPN Settings > Advanced**, as shown in Figure 5-34.

IPSEC	PPTP Dia	lers	Emulate VPN Servers	Advanced	
L2TP Hello Timeout(secs)					
SecurID Token Persistence Enabled					
SecurID Token	Persistence Timeo	out(minut	es)		
IPSEC Maximum MTU Size					1500
IPSEC Transf	orm Sets				
Name	Encryption	Hash	Action		
default-transfor Add	m 3DES	SHA	Edit Delėte		Apply
					- iddu
Commands				View Commands	

#### FIGURE 5-34 SecureID Token Caching

To apply the advanced VPN settings, click Apply.

The equivalent CLI configuration for the example above is:

```
vpdn group l2tp
ppp authentication CACHE-SECURID
ppp securid cache 1440
```

## Adding IPSec Transform Sets

To create IPSec transform sets, click **Add**. The Add Transform Set screen appears.

Security > V	PN Settings > Advanced > Add Transform Set
Transform Set Name	
Encryption	3DES 💌
Hash Algorithm	SHA 🔽
	Apply

where:

Description
The name of the transform set.
Specifies the type of encryption to be applied.
Specifies the type of hash to be applied.

To add the new transform set, click Apply.

# **Firewall Settings**

To configure global firewall settings select **Configuration > Security > Firewall Settings**.

Cont	figuration		2,30			
Monitoring Configuration	Diagnostics Maintenance Plan	Events Reports			Save Configuration	Logout
Switch General	Security > Firewall Settin	gs				
Management	Monitor Ping Attack ( per sec)					
Network	Monitor TCP SYN Attack rate (per sec)					
Radio	Monitor IP Session Attack (per sec)					
Advanced	Prevent L2 Bridging between Wireless Users					
Calibration	Enforce TCP Handshake Before Allowing Data	П				
Optimization	Prohibit IP Spoofing					
Protection	Prohibit RST Replay Attack					
Monitoring Advanced	Log ICMP Errors					
Security	Disable stateful SIP Processing	Г				
Roles	Allow Tri-session with DNAT	<b>—</b>				
AAA Servers	Session Mirror Destination					
Authentication Methods	Disable FTP server					
VPN Settings						-
Firewall Settings	Community.					Apply
Advanced	commanus		view Commands			





#### where:

Parameter	Description
Monitor Ping Attack	Monitors incoming pings.
Monitor TCP SYN Attack	Monitors SYN attacks.
Monitor IP Session Attack	Monitors IP session attacks.
Prevent L2 Bridging between Wireless Users	Prevents wireless users from creating ad hoc networks.
Drop All IP Fragments	Deletes all IP fragment packets.
Enforce TCP Handshake Before Allowing Data	Requires completion of TCP session negotiation before allowing incoming packets.
Prohibit IP Spoofing	Prevents IP spoofing.
Prohibit RST Replay Attack	Prevents RST replay attacks.
Log ICMP Errors	Logs ICMP (for example, ping) errors.
Disable stateful SIP Processing	ТВС
Allow Tri-session with DNAT	ТВС
Session Mirror Destination	ТВС
Disable FTP server	Prevents FTP transfers.

To apply the new firewall settings, click **Apply**.

### **Service Aliases**

Service aliases aid in policy configuration by applying a human-readable label to protocols numbers or groups of protocol numbers. To manage service aliases, navigate to **Configuration > Security > Advanced > Services**, as shown in the figure below.

Name	Protocol	Port	End Port	Action	
svc-snmp-trap	udp	162	N/A	Edit	Delete
svc-syslog	udp	514	N/A	Edit	Delete
svc-l2tp	udp	1701	N/A	Edit	Delete
svc-ike	udp	500	N/A	Edit	Delete
svc-https	tcp	443	N/A	Edit	Delete
svc-smb-tcp	tcp	445	N/A	Edit	Delete
svc-dhcp	udp	67	68	Edit	Delete

FIGURE 5-36 Service Aliases

To edit or delete an alias, click the appropriate button. To add a new service alias, click **Add**. The Add Service window is shown in the figure below.

Protocol • TCP • UDP • Protocol	
Starting Port	
End Port	
	Apply

#### FIGURE 5-37 New Service Definition

Configuration parameters for new service definition are:



**Service Name** – A human-readable name to identify the service alias. Default service aliases begin with "svc-" followed by the protocol name. This convention may be used if desired, or a new one may be used.

**Protocol –** Services can be defined by TCP port numbers, UDP port numbers, or IP protocol number. If a particular service can operate over both TCP and UDP, create two separate services aliases.

**Starting Port –** For TCP or UDP services, specifies the lower port number of a port range. To specify a single port, enter the same number in both the starting and ending field.

**End Port** – For TCP or UDP services, specifies the upper port number of a port range. To specify a single port, enter the same number in both the starting and ending field.

The equivalent CLI configuration for the example above is:

netservice svc-newservice tcp 1024 1026

#### Source/Destination Aliases

Source and destination aliases aid in policy configuration by applying a human-readable label to IP addresses and groups of IP addresses. Source/destination aliases are used in traffic policies to specify either the source of a packet or the destination of a packet. To manage source/destination aliases, navigate to **Configuration > Security > Advanced > Destinations**, as shown in the figure below.

Name	Rule Count	Invert	Action		
user	1	No	Edit	Delete	
mswitch	1	No	Edit	Delete	
any	1	No	Edit	Delete	
Add					

FIGURE 5-38 Source/Destination Alias

Three pre-defined aliases exist and should not be deleted or edited:

**User** – When a traffic policy containing the "user" alias is applied to an authenticated user, this alias is replaced by the IP address assigned to that user. With this alias, generic traffic policies can be configured that will automatically be customized at the time of user login.

**Mswitch –** This policy represents the switch IP address (loopback address or VLAN 1 address) of the Alcatel switch on which the traffic policy is running. This alias is used in the captive portal policy, as well as in many destination NAT policies.

Any - Represents any IP address.

To add a new source/destination alias, click **Add**, as shown in the figure below. Configuration options are:

**Destination Name -** A human-readable name for the alias. This name appears in all traffic policies making use of this source/destination alias.

**Invert –** Specifies that the inverse of the addresses entered should be used. For example, if a network of 172.16.0.0/16 is entered, the "invert" option specifies that the policy should match everything *except* 172.16.0.0/16.

Destinatio	on Name			Internal_Network
Invert				
Туре	IP Address	NetMask/Range	Actions	
host	10.14.1.22		Delete 🔺	T
network	172.16.0.0	255.255.0.0	Delete 🔺	T
range	192.168.1.1	192.168.1.17	Delete 🔺	T
Add				
			Appl	У
Add Rule	2			
Rule Typ	)e	host 💌		
IP Addre	ess			
Network	.Mask/Range			
		Cancel Add		

FIGURE 5-39 Add Source/Destination Alias



Source/destination aliases contain one or more IP addresses or ranges of IP addresses. To add a new address or address range, click the Add button. Three choices are available:

**Host** - A single IP address. When entering a single IP address, do not fill in the netmask/range field.

Network - An IP subnet, consisting of a network number and subnet mask.

**Range –** A range of IP addresses consisting of all sequential addresses between a lower value and an upper value. Enter the lower value in the "IP Address" field, and the upper value in the "Network Mask/Range" field. The maximum number of addresses in the range is 16 – if larger ranges are needed, please convert the range into a network number with a subnet mask and use the "Network" option.

The equivalent CLI configuration for the example above is:

```
netdestination Internal_Network
host 10.14.1.22
network 172.16.0.0 255.255.0.0
range 192.168.1.1 192.168.1.17
```

#### **Bandwidth Contracts**

To configure bandwidth contracts, go to **Configuration > Security > Bandwidth Contracts**.

You can create a bandwidth contract on a VLAN to rate limit only multicast and broadcast packets. The syntax is:

(config) # interface vlan <x>
(config-subif) # bandwidth-contract <name>

# NAT Pools

To create the collection of IP addresses that are assigned to users inside the firewall, go to **Configuration > Security > NAT Pools**.

# **Time Range**

To define a time range select **Configuration > Security > Advanced > Time Range**. The Time Range screen appears.

Con	figuration			20	7.8		0
Monitoring Configuration	Diagnostics Maintenanc	e Plan Events Repo	orts			Save Configuration	Logout
Switch General	Security > Advance	ed > Time Range					
Management	Services Destination	s Bandwidth Contracts	NAT Pools	Time Range			
WLAN Network Radio	Name Type Action Add						

FIGURE 5-40 Time Range

To add a time range, click Add.

Security > Advanced > TimeRange > A	Add Time Range
Name	
Туре	
Start Date (mm/dd/yyyy)	
Start Time(hh:mm)	
End Date (mm/dd/yyyy)	
End Time(hh:mm)	
	Apply

FIGURE 5-41 Adding a Time Range

Complete the information requested on the  ${\bf Add}\ {\bf Time}\ {\bf Range}\ {\bf screen}\ {\bf and}\ {\bf click}\ {\bf Apply}.$ 

# **Additional Information**

This section contains background information on key concepts discussed in this chapter.



# Encryption

Encrypting the transmitted data is only one part of the security process. Although this affords some security, all the common data encryption schemes such as WEP (Wired Equivalent Privacy) have been broken and anyone with the software can read your data in plain text.

#### IKE (Internet Key Exchange) Encryption

IKE encryption is based on establishing a contract between the two computers (or servers) that are exchanging data. This security method is accomplished in two phases, the first establishes the identity of the computers and authenticates the security contract between them. The second phase is the establishment of the encryption of the payload data. The negotiations during phase II are protected by the methods established in phase I.

#### Phase I Negotiations

The negation of a contract initially involves three basic steps:

- Policy negotiation
- DH public value exchange
- Authentication

Policy negotiation consists of four mandatory parameters: encryption algorithm (DES, 3DES), hash algorithm, authentication method, and Diffie-Hellman (DH) group.

During the DH exchange only the base information required to generate the actual key's is exchanged.

Authentication of the DH key exchange is done to assure that the keys were generated and correctly passed.

#### Phase II Negotiations

Phase II is the negotiation of the algorithms used to encrypt the payload data. This is comprised of 3 steps:

- Policy Negotiation
- Session key materials are exchanged or renewed
- As (Security Associations), keys, and SPI (Security Parameters Index) are passed to the IPSec driver.

#### **IPSec**

IP was originally developed within a highly restricted, secure network. Therefore, IP did not have security features built in. Once the Internet became a public forum, security became a critical need. This need has been, and continues to be addressed by the IETF which had developed a suite of security protocols under the umbrella of IP Security, or IPSec. IPSec defines two encryption modes: Transport mode (which only encrypts the data in a packet) and Tunnel mode (which encrypts the entire packet).

All encrypted traffic must be decrypted upon receipt. Therefore, the receiving node (which also must be IPSec compliant) uses a decryption device called a key, which it shares with the encrypting node. The key, known as a public key, is shared between the two communicating nodes by means of the Internet Security Association and Key Management Protocol (ISAKMP).

#### WEP Encryption

WEP encryption comes in two basic flavors 64-bit and 128-bit encryption. Obviously, the 128-bit version offers stronger encryption. When using WEP both sender and receiver must be using the same key to decrypt the transmitted data. WEP allows for rotation of keys and most equipment will allow you to have as many as 4 keys.

Some equipment supports WEP Mapped Keys which are MAC keyed pairwise keys. In this scheme each unique pair of MAC address share a unique WEP key. The pairing is stored in a MIB table.

#### The Problem With WEP

The problem with WEP is that from a design standpoint, it's basically broken. There are actually many flaws in WEP that allow ingenious attackers to break the codes and get to the data. The Internet Security, Applications, Authentication and Cryptography (ISAAC) Group at the University of California at Berkeley has published a report based on their analysis of the WEP standard which can be found at

http://www.isaac.cs.berkeley.edu/isaac/wep-fag.html.

#### TKIP (Temporal Key Integrity Protocol)

TKIP is a replacement for WEP, and along with 802.1x, forms the basis for Wi-Fi Protected Access (WPA). TKIP generates per packet keys, greatly decreasing the likelihood of unauthorized decryption.

TKIP is used in two modes, WPA and PSK (pre-shared key). The WPA mode requires the use of an authentication server and is described below.



The PSK mode uses a pre-shared key (password) which is shared by all clients on the network to establish the initial communication with the access point. After the initial data exchange is complete and the user is authenticated, the key is rotated such that each client uses a different key.

#### WPA (Wi-Fi Protected Access)

Enterprise mode: requires an authentication server and uses RADIUS protocols for authentication and key distribution. The use of a RADIUS server centralizes the management of user credentials.

# Authentication

Authentication of users is critical to protect network resources and data. There are a number of methods for authenticating users/clients. Authentication verifies the identity of users attempting to associate with the network. Authentication in and of itself is not secure. Authentication requests as with all data transmitted over wireless should be encrypted with a form of strong encryption.

Authentication should always be coupled with strong firewall policies and/or Access Control Lists (ACLs) which carefully define user roles. Authenticated users should be carefully classified and assigned roles according to their legitimate business needs for access to various resources and data on the network.

Alcatel AOS-W supports 3 basic types of authentication

- RADIUS
- LDAP
- MAC

#### RADIUS

RADIUS (Remote Authentication Dial In User Service) originally developed in 1992 is probably the most widely deployed method of client authentication. The RADIUS protocol is described in RFC 2138 (1). It is a highly extensible UDP client/server application protocol. A full implementation of the protocol consists of a RADIUS server and a separate RADIUS Accounting server bound to UDP ports 1812 and 1813 respectively. Usually, both services are combined into a single server daemon.

RADIUS servers support several authentication methods, including:

- PPP
- PAP

- CHAP
- UNIX Login
- Others

RADIUS authentication is based on the exchange of shared secrets between a client and the authentication server. The client issues an Access Request packet which contains an encrypted shared secret.

The servers checks to see if it has a shared secret for the client, if not then the packet is silently dropped. If it has a shared secret for the client, the shared secret in the decrypted packet is compared to the shared secret stored on the server.

When the server receives the packet is decrypts the shared secret and compares it to the shared secret for the requesting client, stored on the server.

The server may also validate other parameters such as time of day, NAS, or access ports before it will authenticate the user.

#### LDAP

LDAP (Lightweight Directory Access Protocol) is defined by RFC 1777 (1995). Originally designed at the University of Michigan to adapt a highly complex directory system to the internet. LDAP provides a means to access complex directory structures to verify user name and password information for authentication.

#### MAC

MAC authentication uses the MAC address of the client device to establish an identity for authentication.

The actual authentication may be done by RADIUS, LDAP, or Local Database on the switch.

# Supported VPN Clients

The following third-party VPN clients are supported in release 2.0.6 or higher:

- Microsoft Windows XP with built-in PPTP VPN and L2TP/IPSec support
- Microsoft Windows 2000 with built-in PPTP VPN and L2TP/IPSec support
- Microsoft Windows NT 4.0
- Microsoft Windows ME
- Microsoft Windows 98SE



- Microsoft Windows Mobile 203/CE 4.2 with built-in L2TP/IPSec VPN support (PDA)
- Apple MacOS 10.x with built-in PPTP and L2TP/IPSec VPN support
- PalmOS 5.x with built-in PPTP VPN
- Mergic PPTP VPN for PalmOS 3.5—4.x
- Movian VPN for PalmOS 3.5—5.x
- Movian VPN for Microsoft Windows Mobile/CE
- Linux VPNC

#### **Configuring L2TP and IPSec**

This procedure applies to configuring L2TP/IPSec on Windows 2003 PDAs.

To configure L2TP/IPSec for generic Windows 2003 PDAs:

1. Exit your browser.

Do not just click **OK**, you must actually exit the browser. Depending on your PDA, you may not be able to easily exit applications. If necessary, press the reset button and start over.

- 2. Set up a wireless connection with static WEP.
- 3. Navigate to Start > Settings > Connections > Edit my VPN servers.
- 4. Select Add a new server.

Use the following settings:

host IP IP of Alcatel MX loopback address VPN type IPsec/L2TP

- 5. Click **Next** and select **A pre-shared key** and type the IPSEC pre-shared key (not the securID that you configured on the switch).
- 6. Follow the rest of the instructions (your password is the securID).
- 7. Navigate to Settings > Connections.
- 8. Select the Advanced tab.
- 9. Select Select Networks.
- 10. Click Exceptions.
- 11. Click Add new URL.
- 12. Type \*/\* and click OK.

By default Windows mobile 2003 uses unencrypted frames to pass browser data unless it matches the exception list.

If you have a proxy server:

- Navigate to Settings > Connections > Set up my proxy server.
- Follow the on-screen instructions.

At this point, if you have wireless connectivity, you should be able to click on the icon at the top of the screen with the two arrows pointing left and right next to the speaker icon.

#### 13. Select Connect VPN.

You should be connected and every thing should be working.

**NOTE**—With AOS-W 2.2 or lower, L2TP/IPSEC clients terminating on anything other than the switch IP (loopback or VLAN 1) required the server IP to be in the emulate servers table for dest-natting purposes.

With AOS-W 2.3.0.0 and higher, this restriction has been removed. The only IPs needed in the emulate servers table are the IPs not present on the current switch itself.

#### Configuring L2TP and IPSec with SecureID

The AlcatelReg.exe program is required to modify a registry setting in Windows Mobile 2003. By default, Windows Mobile 2003's IPSec client works with most RADIUS servers except one time password servers such as RSA SecurID. This is because the Mobile 2003 client requires MSCHAPv2 for user authentication. Since RSA does not support MSCHAPv2 for one-time passwords, Alcatel has developed the following procedure to remove this restriction on mobile 2003 so it behaves like normal Windows clients. To run it:

- 1. Create an L2TP/IPSec entry for the user on mobile 2003.
- 2. Copy AlcatelReg.exe from your desktop into mobile 2003. This can be done from Microsoft ActiveSync and selecting **Explore**.
- 3. It is recommended that the file be copied to:

Mobile Device/\My Pocket PC/\AlcatelReg.exe

(this corresponds to "My Device" on the PDA).

- 4. After copying, open the File Explorer on the PDA.
- 5. Locate where the file was copied to. If following the previous suggestions, it would be under "My Device".
- 6. Run **AlcatelReg.exe**. A message should show the status of all the L2TP/IPSec entries.

The program only needs to be run once after a new entry is created. It will modify the registry in the entries for all L2TP/IPSec entries present in the PDA.



**OmniAccess Reference: AOS-W System Reference** 



# **Switch Configuration**





**OmniAccess Reference: AOS-W System Reference**
# CHAPTER 6 Common Tasks

## **Basic Network Configuration**

### VLANs

Virtual Local Area Networks (VLANs) are used to divide LAN traffic into manageable broadcast domains. Using VLANs, the LAN can be divided into smaller, logical networks, such as to segregate wireless traffic from the rest of the LAN.

VLANs are created in two parts: first the network interface for the VLAN must be defined on the switch, and then physical switch ports must be added to the VLAN.

Creating a VLAN Interface

If you wish to allow routing between VLANs, you must assign a routing interface to the VLAN, and provide it an IP address on the VLAN subnet. You can skip this procedure if routing among VLANs is not needed. (If no VLANs are configured in the startup dialog script, then all ports are assigned to VLAN 1 by default.)

- 1 Log in as the administrator and enter privileged mode.
- 2 Select a VLAN.

In this example, VLAN 2 will be used for wireless traffic:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Alcatel) (config) # vlan 2
```

Provide a routing interface for the VLAN.

```
(Alcatel) (config) # interface vlan 2
(Alcatel) (config-subif)# ip address 172.16.2.254 255.255.255.0
```

4 Set the DHCP server for relaying DHCP requests for the interface:

(Alcatel) (config-subif) # ip helper-address 172.16.14.9

If the DHCP server is on the same subnet as the VLAN interface, then you do not need to create an IP helper address.

5 Enable the interface and exit the sub-mode.

```
(Alcatel) (config-subif)# no shutdown
(Alcatel) (config-subif)# exit
```

Adding Ports to a VLAN

 In configuration mode, select the physical switch port interface or range.

In this example, slot 2/port 0 is selected:

(Alcatel) (config) # interface fastethernet 2/0

You can also select a range of consecutive ports in a specific slot using the following command:

```
interface range <interface> <slot>/<start port>-<end port>
```

For example, to select slot 2, ports 0 through 23, enter the following:

(Alcatel) (config) # interface range fastethernet 2/0-23

You can also use a comma separated list of consecutive ports, for example:

(Alcatel) (config) # interface range fastethernet 2/0-12,2/27-23,3/1-17

2 Set the port for access to the VLAN.

(Alcatel) (config-if) # switchport access vlan 2



3 Define whether the port is trusted (LAN) or untrusted (wireless).

If connected to the trusted LAN (to an upstream router for example), enter the following:

```
(Alcatel) (config-if) # trusted
```

Otherwise if a port is connected to wireless access points, skip this step.

Enable the port interface and exit the sub-mode.

```
(Alcatel) (config-if) # no shutdown
(Alcatel) (config-if) # exit
```

Repeat this procedure for each port or port range being added to the VLAN.

### **Port Trunks**

Port trunks allow multiple VLANs on one interface. For example, to configure a Fast Ethernet port interface as an 802.1q trunk, the following configuration commands could be used:

```
(Alcatel) (config)# interface fastethernet 2/5(Select slot and port)(Alcatel) (config-if)# switchport trunk allowed vlan 4-5(Set VLAN 4 and 5)(Alcatel) (config-if)# switchport mode trunk(Activate trunk)(Alcatel) (config-if)# no shutdown(Enable port)
```

## **Spanning Tree**

Alcatel Wireless LAN switches support Common Spanning Tree (CST), Multiple instance STP (MISTP), and Rapid Spanning Tree (RSTP) protocols.

**Global Spanning Tree** 

```
(Alcatel) (config) # spanning-tree <option...>
```

Where the following *options* can be configured:

- forward-time <interval>
   Set the spanning tree forward interval.
- hello-time <interval> Set the spanning tree hello interval.



- max-age <interval>
   Set the spanning tree maximum age interval.
- priority <level>
   Set the spanning tree priority level.

### Per Interface Spanning Tree

Per interface spanning tree is configured from the interface sub-mode:

```
(Alcatel) (config) # interface <interface type> <slot>/<port>
(Alcatel> (config-if) # spanning-tree <options...>
```

Where the following *options* can be configured:

- cost <path cost>
   Set the interface's spanning tree path cost.
- port-priority <value>
   Set the interface's spanning tree priority.
- portfast
   Change the interface from blocking to forwarding mode.

# **Making Configuration Backups**

The Alcatel Wireless LAN Switch configuration information is stored in a system file which can be backed up, restored, and even transferred to another system.

The configuration image includes four files:

- Configuration file (for example default.cfg)
- wmf database
- RF plan database
- Local user database

A backup requires that all four files be copied and placed on a external system. To recover or restore a configuration to the Wireless LAN switch, these four files must be copied to the switch from the external system.

### **Creating an On-System Backup**

The configuration file is stored in flash memory in the /flash/config directory. Use the following procedure to place a copy of the configuration file in the same location:

#### Save any current configuration changes.

```
(Alcatel) # write memory
Saving Configuration...
Saved Configuration
```

2

Determine the name of the current configuration file.

```
(Alcatel) # show boot
Config File: default.cfg
Boot Partition: PARTITION0
```

In this example, default.cfg is the name of the configuration file.

3 Copy the configuration to a new file.

The format for the CLI command is:

**copy flash:** <*source filename>* **flash:** <*destination filename>* 

For example:

(Alcatel) # copy flash: default.cfg flash: default-backup.cfg

where default-backup.cfg is the name of the new file.

Verify the creation of you backup copy.

```
(Alcatel) # dir
-rw-r--r-- 1 root root 1333 Apr 20 00:19 default-backup.cfg
-rw-r--r-- 1 root root 1333 Apr 20 14:59 default.cfg
```

You should see the configuration file and any backup you created.

**NOTE**—In AOS-W 2.2.1.0, you can also use **tar flash** and **wms export-db** commands to make backups.

### Saving to a New Location

The configuration file can also be copied to an FTP or TFTP server. This requires the IP address of a working FTP or TFTP server that has a valid IP route to the switch. The format for the CLI command is:

**copy flash:** <source filename> **tftp:** <*TFTP server address>* <*destination filename>* 



For example:

```
(Alcatel) # copy flash: default.cfg tftp: 10.5.10.21 default.cfg
```

Here, the configuration file is downloaded to a TFTP server with IP address 10.5.10.21.

**NOTE**—A placeholder file with the destination filename must exist on the FTP or TFTP server prior to executing the copy command.

### **Restoring the Configuration File**

To restore a backup configuration file, copy the backup over the original source.

To restore an on-system backup, the format for the CLI command is:

copy flash: <backup filename> flash: <original filename>

For example:

```
(Alcatel) # copy flash: default-backup.cfg flash: default.cfg
```

To restore a copy stored on an FTP or TFTP server, the command is:

**copy tftp:** <*TFTP server address*> <*backup filename*> **flash:** <*original filename*>

For example:

(Alcatel) # copy tftp: 10.5.10.21 default.cfg flash: default.cfg

### **Annotating Configuration Files**

You can insert comments into configuration files by inserting a pound sign (#) as the first character of the line.

# Upgrading the AOS-W Software

The Alcatel AOS-W software can be upgraded as new releases become available.

1 Obtain a valid Alcatel Wireless LAN Switch software image.

Contact Alcatel Customer Support for software availability. In this example, the file OmniAccess 6000\_2.0.6.0 holds the new software image.

2 Upload the new software image to an FTP or TFTP server on your network and verify the network connection.

Place the software image file in the root directory of your FTP or TFTP server.

The switch must have a valid network route to the FTP or TFTP server. You can verify the route using the ping command from the switch CLI:

ping <destination IP address>

For example, if the TFTP server IP address is 10.1.1.234:

```
(Alcatel) # ping 10.1.1.234
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.1.1.234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- 3 Backup your switch configuration (see page 126).
- 4 Determine which memory partition will be used to hold the new software image.

Of the switch's four memory partitions, two are used to hold switch software images. One of the partitions holds the active software image and the other generally holds a backup.

When loading new software, it is recommended to load the new image into the backup partition. In this way, if there is a failure during the download process, the active partition is not compromised. Later, after the download is confirmed, the partition with the new software image is automatically selected for active use, keeping the old image as a backup.



(Alcatel) # show image version -----: 0:0 (/dev/hda1) \*\*Default boot\*\* Partition Software Version : 1.0.0.0 Build number : 1654 Built on : Tue Apr 15 04:52:19 PDT 2003 -----Partition : 0:1 (/dev/hda2) /dev/hda2: Image not present -----Partition : 1:0 (/dev/hdc1) Not plugged in. \_\_\_\_\_ : 1:1 (/dev/hdc2) Partition Not plugged in.

Use the following command to check the memory partitions:

In this example, partition 0 contains the active image and partition 1 is empty. To protect the active image, in the following steps we will load the new image into partition 1.

5 Load the new image into the Alcatel Wireless LAN Switch.

Use the copy command to place the image file into the switch:

```
copy tftp: <server address> <image filename> system: partition{0|1}
```

For example:

```
(Alcatel) # copy tftp: 10.1.1.234 OmniAccess 6000_2.0.6.0 system:
partition1
Upgrading partition1
.....Copied image successfully.
The system will boot from partition1 during the next reboot.
```

6 Verify that the new image is loaded.

Use the following command to check the memory partitions:

```
(Alcatel) # show image version
------
Partition
                : 0:0 (/dev/hda1)
Software Version : 1.0.0.0
Build number
                : 1654
Built on
              : Tue Apr 15 04:52:19 PDT 2003
-----
Partition
               : 0:1 (/dev/hda2) **Default boot**
Software Version : 1.5.0.0
Build number
                : 412
Built on
               : Tue May 15 08:01:24 PDT 2003
_____
Partition
                : 1:0 (/dev/hdc1)
Not plugged in.
-----
Partition
                : 1:1 (/dev/hdc2)
Not plugged in.
```

In this example, the new image can be seen in partition 1.

7 Reboot the switch.

```
(Alcatel) # reload
Do you really want to reset the system(y/n): y
System will now restart!
```

If there are any unsaved changes, the switch will prompt you about saving the changes.



8 When the boot process is complete, verify the upgrade.

```
(Alcatel) # show version
Switch version
Alcatel Switch Operating System Software.
AOS Switch Software (MODEL: Alcatel6000), Version 2.4.0.0
Website: http://www.alcatel.com/enterprise
Copyright (c) 2003 by Alcatel, Inc.
Compiled on Wed Apr 23 17:34:31 PDT 2003 (#412) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.3 (Apr 21 2003 - 00:27:10)
Switch uptime is 1 minutes 26 seconds
Alcatel Supervisor Card
Alcatel Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of
memory.
Assembly#:2000004D Rev:01.00 Serial#:P00000254 Date:03/14/03
Crypto Assembly#:2000005B Rev:02.00 Serial#:P00000346
32K bytes of non-volatile configuration memory.
128M bytes of Supervisor Card System flash (model=128MB CHH).
```

In this example, Version 2.4.0.0 is loaded and running, indicating that the upgrade is complete.

## **Reset Configuration to Defaults**

Under some conditions, like when reassigning a switch to a new environment, it may be helpful to first return the switch configuration to its factory default state. Use the following procedure to reset the switch configuration.

1 Log in as the administrator and enter privileged mode.

2 Erase the switch configuration.

```
(Alcatel) # write erase
Write Erase successful
(Alcatel) # _
```

Performing a **write erase** will also remove the certificate that was uploaded for the Web UI.

Reconfigure the switch.

Once the switch configuration is erased, you can continue to use the CLI to make new configuration changes, or you use the build-in setup dialog to perform initial setup. To use the setup dialog, first reboot the switch:

```
(Alcatel) # reload
```

When the switch reboots, perform initial setup as described in Chapter 2 on page 9.



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 7 Air Management

This chapter explains the main elements of wireless intrusion prevention.

Alcatel Access Points (AP60, AP61, and AP70) support Air Monitor functionality in a wide range of configurations including:

- Static Access Point (AP) configuration
- Static Air Monitor (AM) configuration
- Access Point Monitor (APM) until needed to recover for a failed device.

## **Required Components**

An Alcatel Access Point acting as an Air Monitor (AM) When acting as an AM, the Alcatel Access Point works with the Alcatel Wireless LAN Switch to analyze Wireless LAN traffic in order to classify and enforce security policies.

The Alcatel Access Point can be configured as a full-time, dedicated AM. It can also be configured to act as AM unless a network failure requires it to automatically become an Access Point (AP).

 An Alcatel Wireless LAN Switch running Wireless LAN Management Server (WMS) software

The WMS software on Alcatel Wireless LAN Switch allows you to configure and manage the air management features and the AMs registered with switch.

## Wireless LAN Classification

The WMS continually monitors wireless traffic to detect any new AP or wireless client station that tries to connect to the network. When an AP or wireless client is detected, it is classified and its classification is used in order to determine the security policies which should be enforced on the device.

#### **AP Classifications**

AP are classified as one of the following:

Valid AP (VAP)

An AP that is part of the enterprise providing Wireless LAN services is a valid AP. An AP will be classified as valid under the following circumstances:

- The Alcatel AP successfully connects with the switch and loads its software and configuration, or
- The AP is manually classified as valid by the administrator, or
- If AP learning is enabled (see page 137), every new AP is classified as valid.
- Interfering AP (IAP)

An AP that is part of a foreign network in a multi-tenancy environment is an Interfering AP. An AP will be classified as interfering under the following circumstances:

- An AP can be manually classified as IAP by the administrator, or
- If AP learning is disabled (see page 137), every new AP is classified as Interfering.
- Unsecure AP (UAP)

An AP that is part of the enterprise by illegally connected to the network is an Unsecure AP. An AP will be classified as unsecure under the following circumstances:

- An AP can be manually classified as UAP by the administrator, or
- The WMS analyzes MAC addresses from the IAPs and the LAN to determine whether an IAP should be classified as a UAP.

If the AM is segregated from the LAN, wired-side MAC addresses can be manually configured (see "Wired-Side MAC Addresses" on page 138).

DoS AP (DAP)

An AP through which administrator does not want any access to the network is a DoS AP.

### Wireless Client Station Classifications

A wireless client station (STA) is classified as one of the following:

• Valid STA (VSTA)

A station that is part of the enterprise is a valid station. When an interfering station receives 802.11 data frames from a VAP that is encrypted or is 802.11 unencrypted but VPN encrypted, it is marked as a VSTA.

Interfering STA (ISTA)

A station that is not part of the enterprise is marked as an Interfering STA. Every new STA is marked as ISTA.

Dos STA (DSTA)

A station that should not be allowed any access to the Wireless LAN is marked as a DoS STA. A station must be manually marked as a DSTA by the administrator.

## **Enforcement Policies**

Enforcement policies control how the Alcatel Wireless LAN Switch handles IAPs, UAPs, and various kinds of suspicious traffic. Specific enforcement policies can be enabled or disabled based on your security needs. All policies are configured from the WMS configuration sub-mode, which is accessible as follows:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Alcatel) (config) # wms
(Alcatel) (wms) # _
```

## **AP** Policies

The following policies provide control for AP behavior.

### AP Learning

Learning affects the way APs are classified (see "AP Classifications" on page 136). To enable or disable learning, use the following command:

```
(Alcatel) (wms) # ap-policy learn-ap {enable disable}
```



#### Wired-Side MAC Addresses

If an AM is segregated from the LAN (by a firewall for example), it cannot use LAN information to help classify APs. In such a configuration, MAC addresses from the LAN can be manually entered as follows:

(Alcatel) (wms) # wired-mac <MAC address> mode {enable disable}

#### Protect Unsecure AP

If this policy is enabled, WMS prevents any wireless client station from accessing the Wireless LAN by connecting through a UAP. The policy is configured as follows:

```
(Alcatel) (wms) # ap-policy protect-unsecure-ap {enable disable}
```

#### Protect Misconfigured AP

The administrator can specify the configuration attributes that are part of a VAP. Then, if this policy is enabled, WMS prevents any wireless client station from accessing the Wireless LAN by connecting to a misconfigured AP.

#### Valid Configuration Attributes

There are a number of related commands for specifying VAP configuration attributes:

• To specify DCF, PCF, WEP privacy, and short-preamble attributes:

(Alcatel) (wms) # ap-config <attribute> {enable | disable}

where the following *attributes* are available:

Attributes	Description
wpa	Wired Protected Access
privacy	WEP privacy key
short-preamble	Short preamble

• Organizationally Unique Identifier (OUI) of valid MAC addresses:

(Alcatel) (wms) # valid-oui <0UI>:FF:FF:FF mode {enable disable}

where the OUI address is the first half of the MAC address, formatted as  $AA:BB:CC.^{1}$ 

• Valid channel list for 802.11a channels:

(Alcatel) (wms) # valid-11a-channel <*channel*> mode {enable | disable}

• Valid channel list for 802.11b channels:

(Alcatel) (wms) # valid-11b-channel <channel> mode {enable | disable}

SSID list:

(Alcatel) (wms) # valid-ssid <SSID> mode {enable disable}

#### Enabling the Policy

Once the VAP configuration attributes are defined, the policy can be configured as follows:

(Alcatel) (wms) # ap-policy protect-misconfigured-ap {enable disable}

#### Protect Multi-Tenancy Channel Split

The administrator can configure a set of reserved wireless communication channels for which their network has exclusive access. If an AM detects an IAP on a reserved channel and this policy is enabled, the AM will perform denial of service against the IAP.

#### Specify Reserved Channels

The following command can be used to reserved channels:

For 802.11a channels:

```
(Alcatel) (wms) # reserved-11a-channel <channel> mode
{enable|disable}
```

For 802.11b channels:

```
(Alcatel) (wms) # reserved-11b-channel <channel> mode
{enable|disable}
```

1. When entered as a command parameter, Organizationally Unique Identifiers (OUIs) must use the following hexadecimal format:

xx:yy:zz:**ff:ff**:**ff** 

where xx:yy:zz is the organization ID, and ff:ff:ff is the required mask. For example:

00:0b:86:ff:ff:ff



#### Enabling the Policy

Once the reserved channels are defined, the protection policy can be configured as follows:

(Alcatel) (wms) # ap-policy protect-mt-channel-split {enable disable}

#### Protect Multi-Tenancy SSID Split

If the AM detects an IAP with an SSID that is in the valid SSID list and this policy is enabled, the AM will perform denial of service against the IAP.

#### Valid SSID Addresses

Valid SSIDs can be configured as follows:

```
(Alcatel) (wms) # valid-ssid <SSID> mode {enable | disable}
```

#### Enabling the Policy

Once the valid SSIDs are defined, the protection policy can be configured as follows:

```
(Alcatel) (wms) # ap-policy protect-mt-ssid {enable disable}
```

#### AP Load Balancing

The AP load balancing feature allows the system to balance wireless traffic across adjacent APs. Load balancing can be triggered based on the number of users or degree of utilization on an AP. When traffic reaches the configured thresholds on an AP where load balancing is allowed, any new wireless client station attempting to associate with the saturated AP will be directed to an adjacent AP instead. Stations which are already associated with the AP not affected.

For Alcatel Access Points, load balancing is implemented by station management on the Alcatel Wireless LAN Switch. For third party APs, it is implemented by AMs.

#### Load Balancing Options

High and low watermarks must configured if load balancing is enabled. For example, if load balancing is done based on the number of users per AP, when the number of users is equal to or greater than the high watermark value, load balancing is enabled. It is disabled only when number of users on the AP is less than the low watermark. Use the following commands to configure watermarks.

• To set high and low watermarks for number of users per AP:

(Alcatel) (wms) # ap-lb-user-high-wm <number of users>(for high matermark)
(Alcatel) (wms) # ap-lb-user-low-wm <number of users>(for low matermark)

• To set high and low watermarks for AP utilization level:

(Alcatel)	(wms)	#	ap-lb-util-high-wm <level></level>	(for high watermark)
(Alcatel)	(wms)	#	ap-lb-util-low-wm <level></level>	(for low watermark)

Maximum number of retries must also be configured for load balancing. The maximum retries is the number of times a new station is encouraged to move to an adjacent access point. If the station still attempts to associate with the AP after that, association is allowed.

Use the following commands to configure maximum retries:

```
(Alcatel) (wms) # ap-lb-max-retries <number of retries>
```

#### Enabling the Policy

Once thresholds and retries are defined, use the following command to configure AP load balancing:

(Alcatel) (wms) # ap-policy ap-load-balancing {enable disable}

### **Wireless Client Station Policies**

The following policies provide control for wireless client station (STA) behavior.

#### Valid STA

If a station is classified as VSTA and connects to an IAP, the AM will disrupt the connection if this policy is enabled. The policy is configured as follows:

(Alcatel) (wms) # station-policy protect-valid-sta {enable disable}



#### **STA Impersonation Detection**

If the AM detects two stations with the same MAC address while this policy is enabled, a syslog event is generated. The policy is configured as follows:

```
(Alcatel) (wms) # station-policy detect-sta-impersonation
{enable|disable}
```

## **Global Policies**

### Weak WEP

If the AM detects a station or AP encrypting 802.11 frames with weak WEP, a syslog event is generated if this policy is enabled. The policy is configured as follows:

```
(Alcatel) (wms) # global-policy detect-bad-wep {enable disable}
```

#### Interference Detection

WMS can be used to detect interference near a wireless client station or AP based on an increase in the Frame Receive Error Rate and Frame Fragmentation Rate. If this policy is enabled, an increase in the expected rates will generate a syslog event. The policy is configured as follows:

```
(Alcatel) (wms) # global-policy detect-interference {enable disable}
```

Interference detection can be tuned using the following options:

Interference Wait Time

The amount of time an AM inspects traffic to create a baseline for normal values for retry rate and receive error rate.

(Alcatel) (wms) # global-policy interference-wait-time <seconds>

Interference Increase Threshold

The percentage increase in retry rate or receive error rate caused by interference.

```
(Alcatel) (wms) # global-policy interference-inc-threshold <increase>
```

Interference Increase Time

The amount of time in seconds that the increased rate should be present before an event is generated.

```
(Alcatel) (wms) # global-policy interference-inc-time <seconds>
```

# **Statistics Events**

WMS can generate events when particular statistics exceed configured thresholds. Both high and low watermark values can be specified for each statistic. When the statistic exceeds the high watermark, an event is



generated. No new events are generated until the statistic value falls below the low watermark. If a statistic watermark value is set to 0, event generation is disabled for that statistic. Statistics events can be generated for the following:

Frame Retry Rate (FRR)

This is generated for APs and valid wireless client stations.

(Alcatel) (wms) # event-threshold frr-high-wm <high threshold> (Alcatel) (wms) # event-threshold frr-low-wm <low threshold>

Frame Fragmentation Rate (FFR)

This is generated for valid APs and valid wireless client stations.

```
(Alcatel) (wms) # event-threshold ffr-high-wm <high threshold>
(Alcatel) (wms) # event-threshold ffr-low-wm <low threshold>
```

Frame Receive Error Rate (FRER)

This is generated for wireless client stations only.

(Alcatel) (wms) # event-threshold frer-high-wm <high threshold> (Alcatel) (wms) # event-threshold frer-low-wm <low threshold>

#### Bandwidth Utilization (BUR)

This is generated for wireless client stations only.

```
(Alcatel) (wms) # event-threshold bwr-high-wm <high threshold>
(Alcatel) (wms) # event-threshold bwr-low-wm <low threshold>
```

#### Frame Non Unicast Rate (FNUR)

This is generated for wireless client stations only.

```
(Alcatel) (wms) # event-threshold fnur-high-wm <high threshold>
(Alcatel) (wms) # event-threshold fnur-low-wm <low threshold>
```

#### Frame Low Speed Rate (FLSR)

This is generated for wireless client stations only.

(Alcatel) (wms) # event-threshold flsr-high-wm <high threshold> (Alcatel) (wms) # event-threshold flsr-low-wm <low threshold>

## **General WMS Attributes**

The following options affect the general WMS behavior:

#### Poll interval

This defines the interval in milliseconds for communication between the Alcatel Wireless LAN Switch and the Alcatel Access Points and AMs. The WMS will contact the AP or AM every poll-interval to download AP to STA associations, update policy configuration changes, and download AP and STA statistics. By default, the interval is set 60000 milliseconds. This can be set to a lower value if the number of AMs deployed is small.

(Alcatel) (wms) # general poll-interval <milliseconds>

#### Poll retries

This defines the maximum number of failed polling attempts before the polled AP is declared down.

(Alcatel) (wms) # general poll-retries <number of retries>

#### • Grace time

This defines the buffer time for the WMS to AM communication in milliseconds. By default, this is set 2000 milliseconds.

(Alcatel) (wms) # general grace-time <milliseconds>

#### Laser beam

The AM sends "*laser beams*" to APs or wireless stations to enforce policies. For policy enforcement, this feature must be enabled.

(Alcatel) (wms) # general laser-beam {enable disable}



#### Laser beam debug

When an AM generates a laser beam, it impersonates an AP or wireless client station. Normally, it is not possible to determine which AM generated the laser beam by examining the packet. However, when laser beam debug is enabled, the AM will place its BSSID in the packet header to assist in debugging.

To enable laser beam debugging, use the following command:

```
(Alcatel) (wms) # general laser-beam-debug {enable disable}
```

When enabled, the AM will place its BSSID in the packet header as follows:

#### AP to STA

If the laser beam is impersonated as from the AP to the wireless client station (packet header ToDS = 1 and FromDS = 0), the AM's BSSID appears in the 802.11 Addr1 (BSSID) field.

STA to AP

If the laser beam is impersonated as from the wireless client station to the AP (packet header ToDS = 0 and FromDS = 1), the AM's BSSID appears in the 802.11 Addr1 (DA) field.

**NOTE**—When laser beam debug is enabled, policies may not be enforced in some cases, as 802.11 headers are no longer standards compliant.

### AiroPeek Support for Packet Capture

The Alcatel Air Monitor (AM) can be configured to capture packets and send then to a remote client station running Wildpackets' AiroPeek monitoring software. This requires the Alcatel remote adapter plug-in (available from Wildpackets) installed on the monitoring station.

#### **Starting Packet Capture**

1 Start the AiroPeek software on the monitoring client station.

Start the software manually, or by using the link on the Alcatel Web Interface.

**NOTE**—The Web Interface can only be used to launch the AiroPeek software (if not already running). It will not automatically open a capture window for an AM.

2 Open a capture window for a target Air Monitor.

Either start a capture on an already configured remote adapter, or create a new remote adapter by assigning the name and IP address of the Air Monitor for which will be forwarding the packets.

3 On the Alcatel Wireless LAN switch, configure the AM to send captured packets to the monitoring client station.

**NOTE**—The AiroPeek software cannot issue commands to start the AM sending captured packets. Use the Alcatel Web Interface or CLI instead.

The following CLI command can be used to start the AM packet capture:

pcap raw-start <AM IP address> <client IP address> <UDP port> <format> [bssid <radio BSSID>]
[channel <channel>]

With the following parameters:

AM IP address	The IP address of the Air Monitor collecting packets.
Client IP address	The IP address of the client station running the AiroPeek monitoring software.
UDP port	The UDP port number on the client station where the captured packets are expected to be received.
	<b>NOTE</b> —Multiple AMs can send packets to the same UDP port or different UDP ports on the client station. How- ever, if sent to different UDP ports, the AiroPeek appli- cation can display only packets collected on one UDP port at any given time.
format	The format for the captured packets:
	<ul> <li>0: For pcap clients such as Ethereal</li> <li>1: For the AiroPeek client</li> </ul>
radio BSSID	Optional. Each wireless radio protocol (802.1a or 802.1b/g) on the Air Monitor uses a different BSSID. If you wish to restrict packet capture to a specific radio protocol enter the desired BSSID.
channel	Optional. If you wish to restrict packet capture to a spe- cific wireless radio channel, enter the desired channel number.

### The AiroPeek Application

The AiroPeek application cannot be used to control the flow or type of packets coming from the Alcatel Air Monitors. Starting, stopping, or restricting the radio or channel for captured packets can only be done using the switch Web Interface or CLI.

The AiroPeek application listen for all Air Monitor packets for the configured client IP address and UDP port. All packets are processed, however, you can apply display filters on the capture window to control the number and type of packets being displayed.



In the capture window, the absolute time stamps that are displayed correspond to the time that the packet was received by the client station. This time is not synchronized in any manner with the time on the Air Monitor.

### **Stopping Packet Capture**

The AiroPeek application cannot be used to start or stop the flow packets coming from the Alcatel Air Monitors. To stop the packet capture, use the switch Web Interface or the following CLI command:

pcap stop <AM IP address> <pcap ID> [bssid <radio BSSID>]

The *pcap ID* can be found using the show pcap status command to list active packet captures.

### **Remediation with Sygate**

AOS-W 2.4 users who rely on Sygate Technologies for firewall and virus scanning protection need to install the XML 4 Active X Control file (MSXML-install.zip) which can be obtained on the Alcatel support website. The file is in the Tech Tips directory under Support Bulletins.

Responding to error message:

MS XML4 Active X Control is not installed on this machine.

If you are using Windows XP Service Pack 2, and there is a warning box above, click on it, then choose "Install". Once installation is done, click here to proceed.

Click the link and following the installation instructions.

🖆 http://192.168.200.1/clilib/msxml4-installer.html - Microsoft Internet Explorer	
<u>File Edit View Favorites Tools Help</u>	
🚱 Back 🝷 💿 🕤 📓 🐔 🔑 Search 📌 Favorites 😵 Media 🛷 🎰 🗟	
Address 🗃 http://192.168.200.1/clilib/msxml4-installer.html	*
MS XML4 Active X Control is not installed on this machine. If you're using Windows XP Service Pack 2, and there is a warning box above, click on it, then choose "Insta Once installation is done, click <u>here</u> to proceed.	all ActiveX Control"
Opening page http://192.168.200.1/cilib/msxml4-installer.html	Stocal 😌

Additional information TBC.



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 8 802.1x Client Setup

This chapter describes how to configure your wireless client station for 802.1x authentication using the Extensible Authentication Protocol (EAP).

The Alcatel Wireless LAN Switch supports the following:

- EAP-PEAP and EAP-TLS under Windows 2000 (see page 152)
- EAP-PEAP and EAP-TLS under Windows XP (see page 160)
- Cisco-PEAP under Windows XP (see page 162)

Additional information can be found at the Microsoft Web site:

http://www.microsoft.com/windowsxp/pro/techinfo/administration/wir elesssecurity/default.asp

# PEAP or TLS for Windows 2000

### Prepare the Operating System

- 1 Install Windows 2000 with Service Pack 3.
- 2 Download and apply Windows 2000 patch Q313664.

The required patch can be found at the following Web site:

http://www.microsoft.com/windows2000/downloads/recommen ded/q313664/default.asp

#### **Configure the Service**

1 Set the wireless service for automatic operation.

From the Windows 2000 Control Panel, select Administrative Tools, then Services. The following window appears:

🍇 Services						
] <u>A</u> ction ⊻iew ] ← →	🖿 🖬 🖬 🕏 🗟	🔮   🕨		>		
Tree	Name 🛆	Description	Status	Startup Type	Log On As	
Services (Local)	Routing and Remot	Offers rout		Disabled	LocalSystem	
SNS	RunAs Service	Enables st	Started	Automatic	LocalSystem	
	Security Accounts	Stores sec	Started	Automatic	LocalSystem	
	Server 🖏	Provides R	Started	Automatic	LocalSystem	
	🆏 Smart Card	Manages a		Manual	LocalSystem	
	🦓 Smart Card Helper	Provides s		Manual	LocalSystem	
	System Event Notifi	Tracks syst	Started	Automatic	LocalSystem	
	🍓 Task Scheduler	Enables a	Started	Automatic	LocalSystem	
	🖏 TCP/IP NetBIOS Hel	Enables su	Started	Automatic	LocalSystem	
	🆓 Telephony	Provides T	Started	Manual	LocalSystem	
	🦓 Telnet	Allows a re		Manual	LocalSystem	
	Wuninterruptible Pow	Manages a		Manual	LocalSystem	
	🍓 Utility Manager	Starts and		Manual	LocalSystem	_
	🦓 Windows Installer	Installs, re		Manual	LocalSystem	
	🦓 Windows Managem	Provides s	Started	Automatic	LocalSystem	
	🦓 Windows Managem	Provides s	Started	Manual	LocalSystem	
	🆓 Windows Time	Sets the co		Manual	LocalSystem	
	Wireless Configuration	Provides a		Manual	LocalSystem	
	🦓 Workstation	Provides n	Started	Automatic	LocalSystem	
	WZCBDL Service		Started	Automatic	LocalSystem	
	<u></u>					-

#### If necessary, enable the Wireless Configuration service for automatic startup.

If the Wireless Configuration item in the Service window is not already set for automatic startup, right click on the entry and select the properties option from the pop-up menu. The following window appears:

Wireless Configura	tion Properties (Local Computer)
General Log On	Recovery Dependencies
Service name:	WZCSVC
Display <u>n</u> ame:	Wireless Configuration
Description:	Provides authenticated network access control using IE
Pat <u>h</u> to executabl C:\WINNT\Syste	e: m32\svchost.exe -k netsvcs
Startup typ <u>e</u> :	Automatic
Service status:	Started
<u>S</u> tart	Stop Pause Resume
You can specify th from here.	he start parameters that apply when you start the service
Start para <u>m</u> eters:	
	OK Cancel Apply

Under Startup type, select Automatic from the pull-down menu. If the service has not already been started (as shown under Service status), click on the Start button.

Once the service has started, click on the OK button to close the window.



3 Select the Wireless Network Connection properties.

From the Windows Start menu, select Control Panel | Network Connections.

Setwork Connections			
Eile Edit View Favorites Tools Adva	anced <u>H</u> elp		A
🕞 Back 👻 📀 👻 🏂 🔎 Search 🛛	🄁 Folders 🛛 📴 🏂	× 🍤 💷-	
Address 💊 Network Connections			💌 🎅 Go 🛛 Links 🌺
Name	Туре	Status	Device Name
LAN or High-Speed Internet			
Local Area Connection	LAN or High-Speed Inter	Enabled	Accton EN2242 Series MiniPCI Fast
🕹 1394 Connection	LAN or High-Speed Inter	Enabled	1394 Net Adapter
$\uparrow$ Wireless Network Connection	LAN or High-Speed Inter	Enabled	Cisco Systems 340 Series PCMCIA
Virtual Private Network			
- Boingo Wireless VPN	Virtual Private Network	Disconnected	WAN Miniport (L2TP)
I VPN - Home	Virtual Private Network	Disconnected	WAN Miniport (PPTP)
Wizard			
New Connection Wizard	Wizard		

In the Network Connections window, right-click on the Wireless Network Connection entry and select the properties option from the popup menu.



Wireless network properties	? ×
Association Authentication	
Network name (SSID): My-AP	
└ Wireless network key	
This network requires a key for the following:	
Network Authentication: Open	•
Data encryption: WEP	•
Network <u>k</u> ey:	
C <u>o</u> nfirm network key:	
Key inde <u>x</u> (advanced):	
✓ The key is provided for me automatically	
This is a computer-to-computer (ad hoc) network; wir access points are not used	eless
ОК	Cancel

In the Wireless network properties window, select the Association tab and set the following properties:

- Network Authentication: Select Open from the pull-down menu.
- Data encryption: Select WEP from the pull-down menu.
- The key is provided to me automatically:

If using dynamic WEP, check this box. Otherwise uncheck the box and enter the WEP keys manually.



5 Configure the Authentication attributes.



**NOTE**—To configure settings on the Authentication tab, you must be a member of the local Administrators group.

In the Wireless network properties window, select the Authentication tab and set the following properties:

- Enable IEEE 802.1x authentication for the network: Check this box to enable 802.1x authentication.
- EAP type: This setting depends on the type of authentication required.
  - If using EAP-PEAP, select Protected EAP (PEAP).
  - If using EAP-TLS, select Smart Card or Other Certificate.
- Uncheck the other two authentication boxes.

### 6 Configure the Authentication Properties.

Click on the Properties button. Depending on the authentication type selected, one of the following windows appears:

If using EAP-PEAP:

If using EAP-TLS:

Protected EAP Properties	<u>? ×</u>	Smart Card or other Certificate Properties	? ×
When connecting:         ✓ Yalidate server certificate         Connect to these servers:         IPS SERVIDORES         Microsoft Root Authorities:         IPS SERVIDORES         Microsoft Root Authority         Microsoft Root Certificate Authority         NetLock Expressz (Class C) Tanusitvanykiado         NetLock Kozjegyzoi (Class A) Tanusitvanykiado         NetLock Uzleti (Class B) Tanusitvanykiado         NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.         PTT Post Root CA         Image: Secured password (EAP-MSCHAP v2)         Center Context	nfigure	When connecting:       Use my gmart card         Use a getificate on this computer         Use signle certificate selection (Recommended)         Instruct to these servers:         Instruct to the servers:         Instrest to the servers: <tr< td=""><td>A Cancel</td></tr<>	A Cancel

Set the following parameters (valid for either authentication type):

- Validate server certificate: Check this box. This will verify that the server certificate presented to your computer is still valid.
- Connect to these servers: (Optional) Specify whether to connect only if the server resides within a particular domain.
- Trusted Root Certification Authority: Select the appropriate authority. Make sure you have retrieved the CA Certificate from the Root CA Server. For more details on certificates for 802.1x Authentication refer to Certificates for 802.1x.

For EAP-TLS authentication, set the following:

 When connecting: Select the options to Use a certificate on this computer, and to Use simple certificate Selection. This will set the client certificate from the local computer to be used as the user credentials for authentication.



For EAP-PEAP authentication, set the following:

- Enable Fast Reconnect: This enables wireless clients to ROAM between wireless access points on the same network without being re-authenticated each time they associate with the new access point. To enable fast reconnect (recommended), check this box.
- Select Authentication Method: Set as Secured Password (EAP-MSCHAP V2) and click on the Configure button. The following properties window will be displayed:

EA	P MSCHAPv2 Properties	×
١	When connecting:	
	Automatically use my Windows logon name and password (and domain if any).	ł
	OK Cancel	

Check the box if you want to automatically use the Windows logon name and password as your user credentials. Otherwise, you will have to enter the user credentials manually. If you check this box make sure your windows name and password are the user credentials configured on the Authentication Server (e.g., IAS).

### Validate the User Credentials

After the Wireless connection is configured, the station will try to associate with the configured AP. If the 802.11 association is successful, the system will attempt to validate the user credentials. If this is configured to be done manually, the following message appears above the Windows system tray:

🔱 Wireless Network Connection	×
Click here to select a certificate or other creden connection to the network	tials for

This informs you that a certificate or other credentials are required to access the network. Click on the message to open the user credentials entry window. Specify your user credentials and click on the OK button.
The wireless client station adapter should now use EAP authentication and the following type of message appears:

alidate Server (	Certificate		
The Root Certific	ation Authority for th	e server's ce	ertificate is:
If this is the correct certificate, click OK to connect and you will not see this message again. Click CANCEL to drop connection.			
			View Server Certificate
	ОК	Cancel	

This message indicates the root certification authority for the server's certificate. If this indicates the correct certification authority, click on the OK button to accept the connection. Otherwise, click Cancel.

Upon successful logon, the status of your Wireless Network Connection will indicate Authentication succeeded:

SNetwork Connections			
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools Adva	anced <u>H</u> elp		n
🕞 Back 👻 🕥 👻 🏂 Search 👔	🄁 Folders 🛛 🔯 🍞 🔰	× 🍤 💷 ·	
Address 💊 Network Connections			💌 🄁 Go 🛛 Links 🎽
Name	Туре	Status	Device Name
LAN or High-Speed Internet			
🕹 1394 Connection	LAN or High-Speed Inter	Enabled	1394 Net Adapter
🕹 Local Area Connection	LAN or High-Speed Inter	Enabled	Accton EN2242 Series MiniPCI Fast
Y Wireless Network Connection	LAN or High-Speed Inter	Authentication succeeded	Cisco Systems 340 Series PCMCIA
Virtual Private Network			
Boingo Wireless VPN	Virtual Private Network	Disconnected	WAN Miniport (L2TP)
PVPN - Home	Virtual Private Network	Disconnected	WAN Miniport (PPTP)
Wizard			
New Connection Wizard	Wizard		
			Þ



# PEAP or TLS for Windows XP

**NOTE**—If using Cisco-PEAP with Windows XP, see the instructions on page 162 instead.

- Install Windows XP with Service Pack 1a.
- Enable the Wireless Network Connection.

From the Windows Start menu, select Control Panel | Network Connections.



If not already enabled, right-click on the Wireless Network Connection entry and select the enable option from the popup menu. **3** Select the Access Point for association.

- In the Network Connections window, right-click on the Wireless Network Connection entry and select the properties option from the popup menu.
- From the properties window, select the Wireless Networks tab.

, Wireless Network Connection Properties
General Wireless Networks Advanced
✓ Use Windows to configure my wireless network settings Available networks:
To connect to an available network, click Configure.
i wildcard <u>Configure</u>
i aruba-alpha-ap
below: Move.up
Move_down
Add <u>H</u> emove Properties
Learn about <u>setting up wireless network</u> Ad <u>v</u> anced

- Select the option to Use Windows to configure my wireless network settings. This will ensure that Windows is in charge of the wireless connection properties.
- In the Available networks list, select the AP to which you wish to associate, and click on the Configure button. This will open the Wireless Network properties window.
- 4 Continue the configuration

The rest of the configuration instructions are identical to the Windows 2000 procedure. Go to Step 4 on page 155 to continue the configuration.



# **Cisco-PEAP for Windows XP**

Presently, only EAP-PEAP is supported with the Cisco ACU for Windows XP. For EAP-TLS, use the Microsoft supplicant as described on page 160.

#### Prepare the Operating System

- Install Windows XP with Service Pack 1/1a.
- Install the Cisco ACU (version 5.05.001 and higher) which includes the Cisco-PEAP supplicant.
  - **Note**—Although Windows XP-SP1/SP1a includes the Microsoft PEAP supplicant, it is not compatible with the Cisco PEAP supplicant. To use the Cisco PEAP supplicant, you must install the Cisco-ACU *after* SP1/SP1a for Windows XP.

The latest drivers for the Cisco Wireless Network Adapter can be found at:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

## **Enable Wireless Zero Configuration**

The wireless zero configuration service provides automatic configuration for 802.11 adapters. To enable the service:

- From the Start menu, select Control Panel | Administrative Tools | Services.
- 2 In the Services window, locate and double-click on the Wireless Zero Configuration item.

Services				_	
<u>File Action View</u>	Help				
⇐ ⇒ 💽 🖻	🖸 🖪 😫 🕨 ■ 🗉 ■				
🍓 Services (Local)	Name 🔺	Description	Status	Startup Type	Lo 🔺
	🏶 Windows Time	Maintains date	Started	Automatic	Lo
	🎇 Wireless Zero Configuration	Provides autom		Automatic	Lo
	🦓 WMI Performance Adapter	Provides perfor		Manual	Lo
	Workstation	Creates and ma	Started	Automatic	Lo
	WZCBDL Service		Started	Automatic	Lo 💌
	Extended A Standard /				

This will launch the Properties window for the Wireless Zero Configuration service.



On the General properties tab, set the Startup type to Automatic.

Wireless Zero Con	figuration Properties (Local Computer)	? ×
General Log On	Recovery Dependencies	
Service name:	WZCSVC	
Display <u>n</u> ame:	Wireless Zero Configuration	
Description:	Provides automatic configuration for the 802.11	
Pat <u>h</u> to executab C:\WINDOWS\S	le: jystem32\svchost.exe -k netsvcs	
Startup typ <u>e</u> :	Automatic	] [
Service status:	Stopped	-
<u>S</u> tart	Stop <u>P</u> ause <u>R</u> esume	] [
You can specify t from here.	he start parameters that apply when you start the service	
Start para <u>m</u> eters:		
	OK Cancel Appl	y

4 If necessary, start the service by clicking on the Start button.

**NOTE**—If the service is already running, the Start button may not be available.

#### **Configure the Cisco ACU**

The Cisco ACU must be configured to use Host-Based EAP in order to support Cisco-PEAP. Use the following procedure to create a profile with Host-Based EAP. In this example, we will create a profile named Office and associate it with an AP whose SSID is My-AP.

- 1 Launch the Cisco ACU.
- 2 Add a new profile.

Click on Add profile and provide the profile name (Office in this example).

3 Specify the System Parameters.

340 Series Properties - [Office]			×
System Parameters RF Network	Advanced (Infrastructure)	Network Security	
System Parameters RF Network 4 Client Name: SSID1: SSID2: SSID3: Power Save Mode: © CAM (Constantly A © Max PSP (Max Pow © East PSP (Power S	Advanced (Infrastructure)   My-Station My-AP   wake Mode) wer Savings) ave Mode)	Network Security	Defaults
		OK Car	ncel Help

On the System Parameters tab, specify the following:

- Client Name: Specify the name of the wireless client station (My-Station in this example).
- SSID1: Specify the SSID of the associated AP (My-AP in this example).
- Network type: Select the Infrastructure option.



4 Specify the Network Security parameters.

340 Series Properties - [Office]	X
System Parameters   RF Network   Advanced (Infrastructure)	Network Security
Network Security Type: Host Based EAP Configure	WEP C No WEP C Use Static WEP Keys C Use Dynamic WEP Keys
Static WEP Keys	
WEP Key Entry Method: C Hexadecimal (0:9, A:F) ASCII Text Already Transmit Set ? Key WEP Key 1: C WEP Key 2: C WEP Key 3: C WEP Key 4: C	Access Point Authentication: © Open Authentication © Shared Key Authentication WEP Key Size 40 128 © O © O © O © O
Allow Association To Mixed Cells	<u>D</u> efaults
	OK Cancel Help

On the Network Security tab, specify the following:

- Network Security Type: Select Host Based EAP from the pull-down menu.
- WEP: Select the Use Dynamic WEP Keys option.

When finished, click the OK button to close the window.

5 In the profile manager, select Use Selected Profile and choose the Office profile.

## **Configure the Wireless Network Connection**

1 Enable the Wireless Network Connection.

From the Windows Start menu, select Control Panel | Network Connections.

Network Connections					
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools Adva	a <u>n</u> ced <u>H</u> elp		🥂		
🕞 Back 👻 🕥 👻 🏂 Search 👔	🄁 Folders 🛛 🗟 🎯 🔰	× 🍤 💷 -			
Address 💊 Network Connections			💌 🋃 Go 🛛 Links 🌺		
Name	Туре	Status	Device Name		
LAN or High-Speed Internet					
🕹 Local Area Connection	LAN or High-Speed Inter	Enabled	Accton EN2242 Series MiniPCI Fast		
🕹 1394 Connection	LAN or High-Speed Inter	Enabled	1394 Net Adapter		
$m{\Upsilon}$ Wireless Network Connection	LAN or High-Speed Inter	Enabled	Cisco Systems 340 Series PCMCIA		
Virtual Private Network					
Boingo Wireless VPN	Virtual Private Network	Disconnected	WAN Miniport (L2TP)		
PVPN - Home	Virtual Private Network	Disconnected	WAN Miniport (PPTP)		
Wizard					
New Connection Wizard	Wizard				
•			•		

If not already enabled, right-click on the Wireless Network Connection entry and select the enable option from the popup menu.



- 2 Select the Access Point for association.
  - In the Network Connections window, right-click on the Wireless Network Connection entry and select the properties option from the popup menu.
  - From the properties window, select the Wireless Networks tab.

🚣 Wirele	ss Network Connection Properties	? ×
General	Wireless Networks Advanced	
🔽 Use	e <u>W</u> indows to configure my wireless network set	tings
_ Availa	able <u>n</u> etworks:	
To co	onnect to an available network, click Configure.	
Å	wildcard	onfigure
i.	aruba-alpha-ap	Refresh
<u> </u>	new1	<u>ienesn</u>
Profe	wad waturaka:	
Autor	matically connect to available networks in the or	der listed
belov	M:	
	M	ove <u>u</u> p
	Ma	ve <u>d</u> own
	Add <u>R</u> emove Properties	
Learn <u>confic</u>	about <u>setting up wireless network</u> guration.	Advanced
	ОК	Cancel

- Select the option to Use Windows to configure my wireless network settings. This will ensure that Windows is in charge of the wireless connection properties.
- In the Available networks list, select the AP to which you wish to associate, and click on the Configure button. This will open the Wireless Network properties window.

	3	Configure t	he Association	attributes.
--	---	-------------	----------------	-------------

Wireless network propertie	:5	<u>? ×</u>		
Association Authentication				
Network name (SSID):	My-AP			
Wireless network key				
This network requires a ke	ey for the following:			
Network <u>A</u> uthentication:	Open	•		
Data encryption:	WEP	•		
Network <u>k</u> ey:				
Confirm network key:				
Key inde <u>x</u> (advanced);	1 -			
The key is provided fo	r me automatically			
This is a <u>c</u> omputer-to-computer (ad hoc) network; wireless access points are not used				
	ОК	Cancel		

In the Wireless network properties window, select the Association tab and set the following properties:

- Network Authentication: Select Open from the pull-down menu.
- Data encryption: Select WEP from the pull-down menu.
- The key is provided to me automatically: Check this box.



Gonfigure the Authentication attributes.



**NOTE**—To configure settings on the Authentication tab, you must be a member of the local Administrators group.

In the Wireless network properties window, select the Authentication tab and set the following properties:

- Enable IEEE 802.1x authentication for the network: Check this box to enable 802.1x authentication.
- EAP type: Select Protected EAP (PEAP).

Note—EAP-TLS is not currently supported using the Cisco ACU.

Uncheck the other two authentication boxes.

#### 5 Configure the Authentication Properties.

On the Authentication tab, click on the Properties button and set the following:

PEAP Properties	×
Validate server certificate	
Connect only if server name <u>ends</u> with:	
Irusted root certificate authority: Microsoft Root Authority	
Second Phase EAP Type: Generic Token Card	
<u> </u>	

- Validate server certificate: Check this box. This will verify that the server certificate presented to your computer is still valid.
- Connect to these servers: (Optional) Specify whether to connect only if the server resides within a particular domain.
- Trusted Root Certification Authority: Select the appropriate authority. Make sure you have retrieved the CA Certificate from the Root CA Server. For more details on certificates for 802.1x Authentication refer to Certificates for 802.1x.



 Second Phase EAP Type: Select the Generic Token Card option and click on properties.

In the Generic Token Card Properties window, select either Static Password or One Time Password (OTP).

<ul> <li>Support <u>H</u>ardwareToken</li> <li>Support Software Toker</li> <li>Supported <u>Type</u>:</li> <li>Secure Computing SofToken II 2.0</li> </ul>	<ul> <li><u>Static</u> P</li> <li><u>O</u>ne Tim</li> </ul>	assword (Wind ne Password	ows NT/2000,	LDAP)	
Support Software Toker Supported Type: Secure Computing SofToken II 2.0	🔽 Suppo	rt <u>H</u> ardwareTo	ken		
Secure Computing SofToken II 2.0	Suppor	rt So <u>f</u> tware Tol ted <u>T</u> ype:	ter		
	Secure	Computing So	fToken II 2.0		~

For OTP (hardware token), the appropriate support must be installed on the Authentication Server (for example: Cisco-ACS + RSA ACE Server Agent).

#### Validate the User Credentials

After the Wireless connection is configured, the station will try to associate with the configured AP. If the 802.11 association is successful, the following message appears above the Windows system tray:



This informs you that a certificate or other credentials are required to access the network. Click on the message to configure user credentials. Depending on whether a Static Password or OTP was chosen, one of the following appears: Static Password:

Please enter y	our password.	
User <u>N</u> ame:		
<u>P</u> assword:		
<u>D</u> omain:		

OTP:

Please enter y	your password.
User <u>N</u> ame:	
Password:	
	dware Token 🔿 Software Token

For OTP, select either the Hardware Token or Software Token option. If you select Software Token, the Password field on the One Time Password screen becomes the PIN field.

Enter your PEAP authentication user name and password (which are registered with the RADIUS server). If using a Static Password, select your domain name from the drop-down list (or type it in if applicable).

When finished, click on the OK button. The wireless client station adapter should now use EAP authentication.



In some cases, the following type of message appears:

۷	alidate Server Certificate				
	The Root Certification Authority for the server's certificate is:				
	If this is the correct certificate, click OK to connect and you will not see this message again. Click CANCEL to drop connection.				
	y View Server Certificate				
	Cancel				

This message indicates the root certification authority for the server's certificate. If this indicates the correct certification authority, click on the OK button to accept the connection. Otherwise, click Cancel.

Upon successful logon, the status of your Wireless Network Connection will indicate Authentication succeeded:

Setwork Connections			
<u>File Edit View Favorites Tools Adva</u>	anced <u>H</u> elp		💦 🖉
🕞 Back 👻 🕥 👻 🏂 🔎 Search 🛛	🄁 Folders 🛛 📴 🎾 🔰	× 🍤 💷 ·	
Address 💊 Network Connections			💽 🄁 Go 🛛 Links 🌺
Name	Туре	Status	Device Name
LAN or High-Speed Internet			
🕹 1394 Connection	LAN or High-Speed Inter	Enabled	1394 Net Adapter
🕹 Local Area Connection	LAN or High-Speed Inter	Enabled	Accton EN2242 Series MiniPCI Fast
	LAN or High-Speed Inter	Authentication succeeded	Cisco Systems 340 Series PCMCIA
Virtual Private Network			
Boingo Wireless VPN	Virtual Private Network	Disconnected	WAN Miniport (L2TP)
PVPN - Home	Virtual Private Network	Disconnected	WAN Miniport (PPTP)
Wizard			
New Connection Wizard	Wizard		
4			Þ

# CHAPTER 9 Basic Switch Configuration

This chapter explains how to configure the Alcatel Wireless LAN switch using the AOS-W Command Line Interface (CLI) and the web-based Web UI management tool. The tasks described in this chapter are all found on the **Configuration** tab of Web UI.

# **General Configuration**

#### **Configuring the Switch Role**

The switch role (either master or local) is generally set at the time of initial configuration through the setup dialog. Should the need arise to change the switch role, it may be done through the GUI by navigating to **Configuration > Switch > General** as shown in the figure below.

Switch Role	Master 💌
Master IP Address	172.16.1.100

FIGURE 9-1 Switch Role Configuration

If the switch role is master, the Master IP Address field will be automatically filled in. If the switch role is set to local, fill in the Master IP Address field with the loopback or switch IP address of the master switch. To set the switch role from the CLI, use the command masterip from configuration mode. If this is configured as 127.0.0.1, the switch is a master. If this is configured as any other value, the switch becomes a local switch.

#### Configuring the Switch/Loopback IP Address

The switch IP address is used for different administrative purposes, such as terminating VPN tunnels, terminating GRE tunnels, originating RADIUS requests, and accepting administrative communication. The switch IP address is typically configured through the initial setup dialog, and may be set in two different ways:

If a loopback address is configured in the switch, the loopback address will be used as the switch IP address. A loopback address is not bound to any specific interface and is operational at all times. The loopback address is always configured as a host address, with a 32-bit netmask (255.255.255.255) and should be routable from all external networks.

If a loopback address is not configured, the IP address of VLAN 1 will be used as the switch IP address. Note that if the VLAN 1 address is used as the switch address, all GRE tunnels, RADIUS requests, etc. will fail in the event that VLAN 1 goes down.

To set the loopback IP address through the GUI, navigate to **Configuration > Switch > General** as shown in the figure below.

taufaca				
LOOPDACK Internate				
00:0B:86:00:F2:00				
10.30.30.30				
Switch IP Details (Loopback)				
00:0B:86:00:F2:00				
10.30.30.30				
255 255 255 255				
	terface 00:08:86:00:F2:00 10.30.30.30 etails (Loopback 00:08:86:00:F2:00 10.30.30.30			

FIGURE 9-2 Loopback Interface Configuration

To set the loopback address through the CLI, enter the following command:

interface loopback

ip address 10.1.1.1

## **Mobility Configuration**

To enable mobility, select the Enable Mobility checkbox.

Mobility Conf	iguration
Enable Mobility	

FIGURE 9-3 Mobility Configuration

## Wi-Fi MUX Configuration

An Alcatel switch operating as a Wi-Fi MUX does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as MUX ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central Alcatel switch for processing.

An Alcatel switch licensed and configured for Wireless LAN switching is automatically configured to accept GRE tunnels from MUX switches. However, it must be configured to know which VLANs traffic from the MUX will contain. When terminating tunnels from MUX switches, this Alcatel switch is known as the *MUX Server*.

On the Wi-Fi MUX switch, the first step in enabling MUX operation is to configure VLANs that will be transported to the MUX server. These VLANs can either be local port-based VLANs used for segmentation, or tagged VLANs originating from 3<sup>rd</sup>-party APs attached to the MUX switch. Create new VLANs by navigating to **Configuration > Switch > VLAN**. Click **Add** to add a new VLAN. Configure a VLAN ID and assign ports as shown in the figure below. An IP address may be configured for the VLAN if desired, but it is not required.



	DHCP Helper Addresses			
ID 22	No Helper Addresses C			
dress	Add			
lask				
ort Selection Options				
ise any of the selection criteria to choose port r manually select one or more ports by clicking ou can also select all the ports using the 'Sele	s for configuration g on the ports. ct All' checkbox.			
C Administrative State	perational State 🛛 🗹 F	Port Mode		
VLAN Association 2	rusted			
Assign this VI AN to Ports				
Assign this VLAN to Ports Silot 2 224 0	25 <b>Slot 3</b>	0 1 st All Clear All		
Assign this VLAN to Ports	25 <b>Slot 3</b>	0 1 ct AllClear All		
Assign this VLAN to Ports	25 Slot 3 22 3 Sele 4 Slot 1	0 1 ct AllClear All		
Assign this VLAN to Ports Slot 2 24 0	25 Slot 3 22 22 3 See 4 Slot 1	0 1 ct Al Clear All		
Assign this VLAN to Ports Slot 2 24 0	25 Slot 3 22 22 3 23 5ele 4 Slot 1 5ele	0 1 ct All Clear All 0 1 ct All Clear All		
issign this VLAN to Ports iot 2 24 1	solo ander the mouse cursor will be	0 1 1 ct Al Clear All		
Assign this VLAN to Ports Siot 2	25 Slot 3 22 22 Sole 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	0 1 t Al Clear All 0 1 t Al Clear All ct Al Clear All s displayed N/A		
Assign this VLAN to Ports Slot 2	Solo 1 So	0 1 ct Al (Ger All 0 1 ct Al (Ger All e displayed N/A		
Assign this VLAN to Ports Slot 2	25 Slot 3 22 3 5 5 5 5 5 5 5 5 5 5 5 5 5	0 1 ct Al (Ceer Al 0 1 ct Al Ceer Al etisplayed N/A N/A N/A		
Assign this VLAN to Ports	sele N/A Port Policy N/A Port Policy N/A	0 1 t Al Clear All 0 1 t Al Clear All 0 1 t All Clear All 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1		
Assign this VLAN to Ports Slot 2  Current configuration of the port u Administrative State Power Over Ethernet Is Port an Access or a Trunk Port Spanning Tree VLAN(s)	Solo 1 So	0 1 1 ct All Clear All 0 1 1 ct All Clear All e displayed N/A N/A N/A		



To enable mux ports in the CLI, enter commands in the following format:

```
interface fastethernet 1/7
muxport
```

Finally, enable Wi-Fi MUX operation in the GUI by navigating to **Configuration > Switch > General**. Under the **MUX Configuration** section, enable MUX operation as shown in the figure below. The MUX Server IP address is the loopback or switch IP address of the MUX Server. On the Wi-Fi MUX itself, do not configure the "MUX VLANs" section.

To enable MUX Server operation, VLANs should be created on the switch as described above. Conceptually, the GRE tunnel from the MUX will be treated as a tagged VLAN port. To specify which VLANs are extended to the MUX,

navigate to **Configuration > Switch > General** and specify them in the MUX VLANs section. In the example below, the MUX Server is configured to terminate VLANs 22 and 23 from remote MUXes.

MUX Configuration	
Enable MUX	
MUX Server IP Address	
Enable MUX Server	
MUX VLANs	<ul><li>&lt; 1 ♥</li><li>Delete</li></ul>

FIGURE 9-5 MUX Server Configuration

To configure Wi-Fi MUX operations using the CLI, the corresponding commands are as follows. Please see the CLI Command Reference Guide for more details on these commands.

## **MUX CLI Commands**

```
interface fastethernet 1/7
  switchport mode trunk
    switchport trunk native vlan 22
    switchport trunk allowed vlan 22-23
    muxport
!
mux-address 172.16.1.102
```

## **MUX Server CLI Commands**

mux-vlan 22 mux-vlan 23



## Setting the 802.11d Regulatory Domain

The 802.11d regulatory domain controls which channels and power levels may be used by a radio. The regulatory domain is set at the time of installation using the initial setup dialog. To view the regulatory domain from the GUI, navigate to **Configuration > Switch > General**.

802.11d Regu	latory Domain
Country United 9	States
Time Zone	
Offset from UTC	Name PST Hours(-23 to 23) -8 Minutes(0-59)

FIGURE 9-6 Regulatory Domain

#### **Configuring Time Zones**

To set the local time zone for the switch location, complete the Time Zone information as shown below.

Time Zone				
Offset from UTC	Name	PST	Hours(-23 to 23) -8	Minutes(0-59)

FIGURE 9-7 Setting Time Zone Information

#### **Configuring NTP Servers**

NTP (Network Time Protocol) is used to synchronize network devices to a central time source. Configure the switch to set its system clock using NTP by adding one or more NTP servers under Configuration $\rightarrow$ Switch $\rightarrow$ General as shown in the figure below.

NTP Servers					
NTP Servers	172.16.1.25				
		Delete	Add		

#### FIGURE 9-8 NTP Configuration

The equivalent CLI configuration for the example above is:

ntp server 172.16.1.25

**NOTE**—Do not change the time after you have started NTP. NTP will take care of any time adjustments automatically. If you manually adjust the time more than 1024 seconds, NTP will fail because it cannot adjust for time discrepancies of this size or large.

# **Port Configuration**

To configure physical ports on the Alcatel switch, navigate to **Configuration > Switch > Port.** 

## **Port Selection Options**

Ports must be selected before they can be configured. Two methods for port selection exist. Using the first method, ports may be selected using broad categories as shown in the figure below.



Port Selection				
Slot 2 24 [ 0		25 Slot 3 22 23 Select	0 AllClear All	1
		Slot 1		
Supervisor Card		Select .	0 Clear All	1
Supervisor Card Current configuration of the port und	ler the n	Select	0 Clear All	1
Supervisor Card Current configuration of the port und Administrative State	ler the n N/A	Select	0 Clear All	1
Supervisor Card Current configuration of the port und Administrative State Power Over Ethernet	ler the n N/A N/A	Select nouse cursor will be d Operational State Is Port Trusted	0 All Clear All Iisplayed N/A N/A	1
Supervisor Card Current configuration of the port und Administrative State Power Over Ethernet Is Port an Access or a Trunk Port	ler the n N/A N/A N/A	Select a Select of Select of Select of Select of Select of Operational State Is Port Trusted Port Policy	0 Clear All Iisplayed N/A N/A N/A	1
Supervisor Card Current configuration of the port und Administrative State Power Over Ethernet Is Port an Access or a Trunk Port Spanning Tree	ler the n N/A N/A N/A N/A	Select . Douse cursor will be d Operational State Is Port Trusted Port Policy	0 Clear All Iisplayed N/A N/A N/A	1

FIGURE 9-9 Port Selection Options

Ports may be selected based on their administrative state, operational state, port mode, VLAN association, or trusted state. To select ports based on one of these parameters, click on the appropriate radio button, then select the desired state from the drop-down menu. Ports selected in this way will be shown in the **Port Selection** section with an X.

#### **Port Selection**

To select ports manually, click on the appropriate port(s) in the **Port Selection** section. Positioning the mouse over each port will show the current status for that port in the **Configuration Details** section. Multiple ports may be selected for configuration by clicking on each port once.

Port Selection	on	
Slot 2		Slot 3
	24 25	24 25
0	22	0
1	23	1
	Select All Clear All	Select All Clear All
	Supervisor Card	Empty Slot

FIGURE 9-10 Port Selection

To select multiple ports from the CLI, enter commands in the form:

interface range FastEthernet 2/12-23

This will select ports 2/12 through 2/23.

## **Port Configuration Options**

After one or more ports have been selected, configure the selected port(s) under the **Configure Selected Ports** section as shown in the figure below. The checkbox on the left side of the window specifies which parameters should be updated (useful when multiple ports have been selected for configuration).

Configure Selected Ports	
Enable Port	V
Enable 802.3af Power Over Ethernet	Г
Enable Cisco Power Over Ethernet(Enabling this option will disable 802.3af Power Over Ethernet)	Г
Make Port Trusted	
Port Mode	
Enter VLAN(s)	< 1 💌
Firewall Policy	🔽 🔽 Delete
Enable MUX	Г
Spanning Tree	Enabled      19     Port Cost      128     Priority      Port Fast

FIGURE 9-11 Port Configuration Options

The port configuration options are as follows:

Enable Port - Set the administrative state of the port.

Enable Power Over Ethernet – Enable 802.3af power over Ethernet.

**Enable Cisco Power Over Ethernet –** Enable support for Cisco pre-standard power over Ethernet. Use this option with certain types of Cisco access points.

**Make Port Trusted** – Trusted ports are typically connected to internal controlled networks. Untrusted ports connect to 3<sup>rd</sup>-party access points, public areas, conference rooms, or any other network to which the Alcatel switch should provide access controls. When Alcatel APs are attached directly to the switch, always set the port to be trusted.



**Port Mode –** Sets the mode of the port with respect to VLAN tagging. If the port is set to access, untagged frames will be sent and received on the port, and all traffic will be part of a single VLAN. If the port is set to trunk, tagged frames will be sent and received.

#### VLAN

- If the port is set to access mode, a single port-based VLAN will be configured here.
- If the port is set to trunk mode, a native VLAN and a list of allowed VLANs can be configured. The native VLAN specifies the VLAN to which untagged ingress traffic will be mapped. In addition to the native VLAN, the port may be configured to allow all other VLANs in the switch, or to allow only a specific list of VLANs.

**Firewall Policy** – Applies a firewall policy to the physical port. Firewall policies are created under **Configuration > Security > Policies**.

**Enable MUX –** Specifies that this port connects to a third-party AP for which the switch will perform the Wi-Fi MUX function. See the section on configuring Wi-Fi MUX for more details.

Spanning Tree – TBC

CLI configuration of interfaces is done using the *interface* command. An example interface configuration is:

```
interface fastethernet 2/12
    description "To-Bldg4"
    trusted
    poe cisco
    switchport access vlan 4
```

# **VLAN Configuration**

VLANs configuration on an Alcatel switch is similar to that of a standard L2/L3 switch. VLANs can exist locally only, or can be extended to other devices in the network through VLAN tagging. VLANs can exist purely for L2 segmentation, or can have IP addresses assigned. When IP addresses are assigned, the switch will automatically act as a router and perform L3 forwarding between VLANs.

VLAN 1 is the default VLAN. All ports are part of VLAN 1 until configured otherwise. VLAN 1 cannot be deleted.

## View Current VLAN Configuration

To view the current VLAN configuration, navigate to **Configuration > Switch > VLAN** as shown in the figure below. The current VLANs, along with their IP address parameters and port members, are displayed. To edit an existing VLAN, click **Edit**.

VLAN ID	IP Address	Net Mask	Associated Ports	ρ	ctions
1	172.16.1.1	255.255.255.0	1/0,1/1,1/2,1/3,1/4,1/5,1/6,1/7,1/8,1/9,1/10,1/11,1/12,1/13,1/14,1/15,1/16,1/17,1/18,1/19,	Edit	Delete
			1/20,1/21,1/22,1/23,1/24,1/25,2/0,2/1,2/2,2/3,2/4,2/5,2/6,2/7,2/8,2/9,2/10,2/11,2/12,2/13,		
			2/14,2/15,2/16,2/17,2/18,2/19,2/20,2/21,2/22,2/23,2/24,2/25,3/0,3/1,3/2,3/3,3/4,3/5,3/6,3/7,		
			3/8,3/9,3/10,3/11,3/12,3/13,3/14,3/15,3/16,3/17,3/18,3/19,3/20,3/21,3/22,3/23,3/24,3/25		
Add					

#### FIGURE 9-12 Current VLAN Configuration

The equivalent CLI command is show vlan.

## Add New VLAN

To add a new VLAN, navigate to **Configuration > Switch > VLAN** and click the Add button. Specify a VLAN ID, between 2 and 4096<sup>1</sup>. If desired, specify an IP address and netmask. This IP address will exist as a virtual interface within the VLAN, and will be available to all IP stations within the VLAN.

If desired, a DHCP helper may be configured for the VLAN. If this option is enabled, all DHCP broadcasts on the VLAN will be unicast-forwarded to the specified DHCP server. When using this option, ensure that there is only one DHCP helper on the VLAN and that the Alcatel switch has not been configured as a DHCP server.

The figure below shows the addition of a new VLAN with VLAN ID 26. The Alcatel switch interface in the VLAN has IP address 10.26.1.1/24, and a DHCP helper has been configured with all DHCP requests forwarded to 10.4.1.22.

<sup>1.</sup>AOS-W supports up to 128 concurrent VLANs.



and the second	Drice neiper Addresses			
ID 22	No Helper Addresses C			
ldress	Add			
Aask				
Port Selection Options Jse any of the selection criteria to choose po ir manually select one or more ports by clickin You can also select all the ports using the Sel	ts for configuration g on the ports. sct All' checkbox.			
C Administrative State	Operational State 🔗 🔿 Po	rt Mode		
C VLAN Association	Trusted 📉 😭			
VLAN Association 2	rrusted 4 25 Slot 3 22 23Selec	01 AliClear Ali		
VLAN Association 2 Assign this VLAN to Ports Stot 2 2 3 Select All Clear	1 25 Slot 3	0 1 Al Clear Al		
VLAN Association	frusted Y	0 1 Al Cear Al 0 1 : Al Cear Al		
VLAN Association 2	frusted 4 25 Slot 3 2 22 2 3 Select N Slot 1 Select ander the mouse cursor will be	01 AlCear Al 01 :AlCear Al :AlCear Al :tisplayed		
VLWN Association       2       C         Assign this VLAN to Ports       Sint 2       2         1	trusted t 25 Slot 3 22 22 23 Select A Slot 1 Select IV/A Operational State	0 1 Al Clear All 0 1 Al Clear All displayed N/A		
VLAN Association       2       C         Assign this VLAN to Ports       Slot 2       2         1	Inusted 25 Stot 3 4 225 Stot 3 22 Stot 1 Stot 1 Select N/A Operational State N/A Is Port Trusted	0 1 1 Al Clear Al 0 1 : Al Clear Al Clear Al Clear Al Clear Al NA N/A		
VLAN Association       2       C         Assign this VLAN to Ports       2         Stot 2       2         1       3         Select All       Clear         Current configuration of the port in Administrative State       Power Over thermet         Is Port an Access or a Trunk Port       Is Port an Access or a Trunk Port	Inusted State	0 1 1 Al Clear Al Al Clear Al Al Clear Al Al Clear Al N/A N/A N/A		
VLAN Association       2         Assign this VLAN to Ports         Slot 2       2         1       3         Supervisor Card         Current configuration of the port i         Administrative State         Power Over thermet         Is Port an Access or a Trunk Port         Spanning Tree	Invated Selection of the selection of th	0 1 Al Cear Al 0 1 Al Cear Al displayed N/A N/A N/A		



The equivalent CLI configuration for the example above is:

```
vlan 26
interface vlan 26
    ip address 10.26.1.1 255.255.255.0
    ip helper-address 10.4.1.22
```

## Tunnels

To configure generic tunnels for the switch, navigate to **Configuration > Switch > Tunnels**.



FIGURE 9-14 Tunnels

To create a tunnel, click **Add** and define the tunnel.

## **IP Route Configuration**

Alcatel AOS-W supports configuration of static IP routes. To configure these, navigate to **Configuration > Switch > IP Routing**. On the OmniAccess 6000, two default routes can be configured – one for the management Ethernet port only, and one for the rest of the switch. On other models, a single default gateway may be configured. Costs may be specified on routes to specify priority for multiple routes to the same destination – a lower cost equals a higher priority.

To configure a static route other than the default route, click **Add** button and fill in the required parameters as shown in the figure below.

Destination IP Address	172.16.0.0
Destination Network Mask	255.255.0.0
Next Hop IP Address	10.1.1.200
Cost	
Add Cancel	

FIGURE 9-15 Static Route Configuration

The equivalent CLI configuration for the example above is:

ip route 172.16.0.0 255.255.0.0 10.1.1.200



# **VRRP** Configuration

AOS-W 2.2 supports redundant switch configurations using Virtual Router Redundancy Protocol (VRRP) as the backup mechanism. Please see the Redundancy Design Guide for more information on creating redundant configurations.

**NOTE**—Alcatel recommends that the redundant master switches be of the same type (for example, OmniAccess 6000 to OmniAccess 6000) and configured with the same version of AOS-W. The same applies to redundant local switches (same class of switch running same version of AOS-W.

To enable VRRP, navigate to **Configuration > Switch > VRRP**. The Virtual Router Table will display all redundant networks in which the switch currently participates.

Switch >	Virtual Ro	uter				
General	Port VLAN	T	unnels II	P Routing	VRRP	DHCP Serve
Virtual Router	r Table					
Router Name	IP Address	VLAN	Admin Stat	e Opera	ational State	Action
Add						
Database Sync	chronization P	aramet	ers			
Enable periodic da	atabase synchroni	zation				
Database synchro	onization period in	minutes	0			
Include RF Plan d	lata					
Commanda					01	ew Commande

FIGURE 9-16 Configuring VRRP

To add a new VRRP instance, click Add. Parameters available are the following:

**Virtual Router ID** – A unique identifier of the VRRP instance, also known as VRID. This number should match the VRID on the other member of the redundant pair, and must be between 1 and 255.

**Advertisement Interval** – This specifies how frequently VRRP announcements are sent out. The default value is 1 second, or 1000 milliseconds. This value must be the same on both members of the redundant pair.

Authentication Password – This password must be the same on both members of the redundant pair. The password is sent in plain-text on the wire and therefore should not be treated as a security mechanism. Rather, its purpose is to guard against misconfiguration in the event that other VRRP devices exist on the same network. **Description** – An optional description of the VRRP instance that can be used for administrator convenience.

**IP Address** – The virtual IP address that will be created and used by the VRRP instance. This is the IP address that will be redundant – it will be active on the VRRP master, and will become active on the VRRP backup in the event that the VRRP master fails. This IP address must be part of the IP subnet configured on the VLAN, and must be unique – the address cannot be the loopback address of the switch, or the address of any VLAN interface. This is the IP address to which Access Points will connect, and should be the address configured as the LMS for an AP Group (see the Wireless LAN-Advanced section of this guide for more information.)

**Enable Router Pre-emption** – When enabled, a switch with a higher VRRP priority will always become active while a switch with the lower VRRP priority will always be backup. While this may be desirable in stateless routers, it is recommended that pre-emption be disabled in Alcatel switches to avoid excessive interruption to users, or "flapping" if a problematic switch is cycling up and down.

**Priority –** Defines which switch will become VRRP master if pre-emption has been enabled. These values should be different on each member of the redundant pair. A higher number specifies higher priority. This value must be between 1 and 254.

Admin State – Can be set either up or down. When down, VRRP is not active, although the configuration information is retained.

**VLAN** – Specifies the VLAN on which VRRP is active. If the redundant switch pair is connected to more than one VLAN, each VLAN should have a VRRP configuration.



The figure below shows a sample VRRP configuration. In this example, the switch has an IP address of 172.16.4.254 configured on VLAN 4. The other switch in the redundant pair also has VLAN 4 configured, with an IP address of 172.16.4.253. The Virtual IP address managed by VRRP is 172.16.4.252.

Virtual Router Id	1
Advertisement Interval (msecs)	1000
Authentication Password	Floor2
Description	Floor 2 Switch2
IP Address	172.16.4.252
Enable Router Pre-emption	
Priority	1
Admin State	UP 💽
VLAN	4 💌

FIGURE 9-17 VRRP Configuration

The equivalent CLI configuration is shown below:

```
vrrp 1
priority 1
authentication Floor2
ip address 172.16.4.252
description "Floor 2 Switch1"
vlan 4
no shutdown
```

#### **Dual Supervisor Card (Virtual Switch) Operation**

The Alcatel OmniAccess 6000 Switch supports dual Supervisor Cards. This allows the OmniAccess 6000 to operate as a Wireless LAN switch as well as a virtual switch. (As a virtual switch, it must be configured as a local switch pointing to a master switch.)

To operate the OmniAccess 6000 as a virtual switch:

 Install the Supervisor Cards (SC) in the OmniAccess 6000. Use SC revisions 2.2 (build 8037) or higher. 2. Follow the rules of operation below.

## Rules of Operating a Virtual Switch

1. When a single SC is present in the chassis, it will try to use all the line cards present. SC-0 can use any combination of Line Cards (LCs), for example: LC-1, LC-2 or LC3.

SC-1 can use any combination of LC-2 and LC-3.

2. When two SCs are present in the chassis, SC-0 is dedicated to LC-2 only and SC-1 is dedicated to LC-3 only. In this case, there are two Gigabits of bandwidth available between each LC and SC pairs.

## Hot Swapping Support

Hot swapping is fully supported. Any cards can be removed or added at any time. For example: If SC-0, and LC-2 and LC-3 are installed, then SC-0 uses all the LC-2 and LC-3 ports. When SC-1 is inserted, SC-0 immediately releases control of LC-3, and SC-1 will boot and take over control of LC-3.

Traffic between SC-0 and LC-2 is not interrupted.

If SC-0 is then removed, SC-1 takes over LC-2 and controls LC-2 and LC-3, again without traffic interruption.

**NOTE**—Port numbering is fixed by slot numbers. This means that in a fully loaded system, SC-0 will use ports 2/ and SC-1 will use ports 3/.

#### **Dual SC Operation Example**

To illustrate this dual SC operation:

1. Install SC-0, LC-2 and LC-3. Configure Layer-2 and Layer-3 on ports 2/ and 3/.

- 2. Remove SC-0.
- 3. Install SC-1, LC-2 and LC-3. Configure Layer-2 and Layer-3 on ports 2/ and 3/.
- 4. Install all the cards. SC-0 will use only LC-2 and SC-I will use only LC-3. However, if one of the SC is removed, the other SC will take over an use the previously set configuration.

## **Resetting the Other SC**

The **reload-peer-sc** command allows one SC to reset the other SC in a dual SC configuration. This does not affect the SC on which the command is executed (and the LC it controls).



When the reset button is pushed on a SC, it will reset the SC and only the line cards it controls. This also applies to **reload** and **reload-peer-SC** commands. On a fully loaded system, each side can be reset/reloaded independently.

#### **DHCP Server Configuration**

IP address assignment for wireless clients is normally done through DHCP, although static addresses can also be used. Alcatel switches provide the ability to use an internal DHCP server for address assignment, in the event that an external server is not available or not desirable.

CLI commands to configure DHCP server functionality can be found in the CLI Command Reference Guide under "service dhcp", "ip dhcp pool", and "ip dhcp excluded-address".

#### DHCP Server Operation

To enable the DHCP server, navigate to **Configuration > Switch > DHCP Server**. The DHCP server state is shown at the top of the window, as shown in the figure below.



FIGURE 9-18 DHCP Server State

To enable the DHCP server, click on the start button. To disable the DHCP server, click on the stop button. The equivalent CLI commands are:

service dhcp no service dhcp

#### **DHCP Pool Configuration**

To view DHCP pools, navigate to **Configuration > Switch > DHCP Server**. To edit an existing DHCP pool, click the corresponding Edit button.

Pool Configuration							
Name	Default Router	Network	Range	A	iction		
vlan18		192.168.18.0	192.168.18.2-192.168.18.254	Edit	Delete		
vlan4	172.16.4.254	172.16.4.0	172.16.4.1-172.16.4.253	Edit	Delete		
vlan5	172.16.5.254	172.16.5.0	172.16.5.1-172.16.5.253	Edit	Delete		
Add							

#### FIGURE 9-19 VLAN Pool Configuration

A different DHCP pool must be created for each IP subnet for which DHCP services should be provided. DHCP pools are not specifically tied to VLANs – the DHCP server exists on every VLAN. When a DHCP request comes in, the switch examines the origin of the request to determine if it should answer. If the IP address of the VLAN matches a subnet for which the DHCP server is configured, it will answer the request.

To add a new DHCP pool, click **Add**. Fill in parameters as shown in the figure below. Only those parameters shown are supported by the DHCP server. If additional DHCP options are required, an external DHCP server should be used. In the example shown, a DHCP pool has been created for network 10.26.1.0/24. The default router for the subnet is 10.26.1.1, and the primary DNS server is 192.168.1.10.

Cont	figuration		
Monitoring Configuration	Diagnostics Maintenance Plan Events Reports S	lave Configuration	Logou
Switch General	Switch > DHCP Server		
Management	General Port VLAN Tunnels IP Routing VRRP DHCP Server		
WLAN Network	DHCP Server Sterr Stop		
Radio	Pool Configuration		
Advanced	Name Default Router Network Range Action		
RF Management	testpol 10.4.21.254 10.4.21.0 10.4.21.2-10.4.21.9 10.4.21.12-10.4.21.19 10.4.21.22-10.4.21.29 10.4.21.31-10.4.21.233 10.4.21.235-10.4.21.253 Edit Delete	l .	
Calibration	Add		
Optimization			
Protection	Excluded Address Range		
Monitoring	104211		
Advanced	Evoluted Address		
Security Roles	10.4.21.11 10.4.21.20 Delete		
Policies			
AAA Servers			Apply

#### FIGURE 9-20 DHCP Server

The equivalent CLI configuration for the example above is:



```
ip dhcp pool vlan26-pool
  default-router 10.26.1.1
  dns-server 192.168.1.10
  domain-name net26.test.com
  lease 0 8 0
  network 10.26.1.0 255.255.255.0
```

## **DHCP Excluded Address Configuration**

If DHCP should specifically exclude some addresses from DHCP assignment, configure them in the excluded address section as shown in the figure below. Although most DHCP client implementations will check to see if an address is in use before taking it, it is good practice to exclude statically assigned addresses from the DHCP pool.

kcluded Addres	s Range	
Excluded Address	192.168.18.1	Add Delete

FIGURE 9-21 DHCP Excluded Addresses

The equivalent CLI configuration for the example above is:

ip dhcp excluded-address 192.168.18.1 192.168.18.1
# CHAPTER 10 802.1x Configuration

# Introduction

This chapter will explain the process of configuring the server for 802.1x and using CA Certificates for authorization.

#### Background

The IEEE 802.1x standard defines a Layer 2, port-based network access control scheme that provides authenticated network access on wireless Ethernet networks. The ability of a device to transmit and receive data over an Ethernet switch port is denied if the authentication process is unsuccessful. This standard was originally developed for traditional wired networks and has been successfully adapted for use with wireless networks.

#### **Definitions and Common Abbreviations**

#### Authentication server

An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. Example: Microsoft IAS is an Authentication Server.

#### Authenticator

An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. Example: Alcatel-6000 is an 802.1x Authenticator.

#### Certificates

Certificates are digital documents which are commonly used for authenticating users, computers and for securing information on open networks. Certificates bind public keys to the entity that possesses the private key and are digitally signed by the issuing certification authority (CA).

#### Certification authority (CA)

A certification authority is an entity which is responsible for establishing and vouching for the authenticity of public keys belonging to subjects (usually users or computers) or other certification authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and certificate revocation.

#### EAP

(Extensible Authentication Protocol) is a general protocol for PPP authentication which supports multiple authentication mechanisms.

#### EAP-TLS

(EAP-Transport Level Security) is used in certificate-based security environments. It provides the strongest authentication and key determination method. EAP-TLS provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the client and the authenticator.

#### EAP-TTLS

(EAP- Tunnelled TLS Authentication Protocol) is an EAP protocol that extends EAP-TLS. In EAP-TLS, a TLS handshake is used to mutually authenticate a client and server. EAP-TTLS extends this authentication negotiation by using the secure connection established by the TLS handshake to exchange additional information between client and server. In EAP-TTLS, the TLS handshake may be mutual; or it may be one-way, in which only the server is authenticated to the client.

#### PEAP

(Protected EAP) is an authentication protocol that uses TLS to enhance the security of other EAP authentication methods. PEAP for Microsoft 802.1X Authentication Client provides support for EAP-TLS, which uses certificates for both server authentication and client authentication, and Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MS-CHAP v2), which uses certificates for server authentication and password-based credentials for client authentication.

#### RADIUS

(Remote Authentication Dial-In User Service) is a distributed client/server system that secures networks against unauthorized access. Alcatel-6000 can be configured as a RADIUS Client and send authentication requests to the configured RADIUS servers that contains all user authentication and network service access information.

#### Supplicant

An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link. Example: Win-XP/2K Wireless station is a supplicant.

#### TLS

(Transport Layer Security) provide privacy and data integrity between two communicating applications.

# Configuring the Switch for 802.1x

#### **Creating an Authentication Server Instance**

This section of the chapter will guide you through the process of specifying an authentication server for use with your OmniAccess 6000 switch. The commands used for configuring the switch are explained in Chapter 30.

Authentication Server for 802.1x authentication is a RADIUS Server which is configured to support EAP infrastructure. In this example we will configure a Microsoft IAS server as the Authentication server. The name of the server instance is IAS-RADIUS, the IP address is 10.1.1.214 and the shared secret between the Alcatel-6000 and the IAS server is a12u13a. The default authentication port is 1812 and the default accounting port is 1813.Retrasmit determines the number of times the RADIUS packet will be sent to the server before dropping that request. The default value of the retransmit is 3.The timeout is the time period between each retries and the default value is 5 seconds.



**NOTE**—To configure an SSID to support 802.1x, set its opmode to dynamicWep or dynamicTkip. Failure to do so will prevent clients from implementing 802.1x.

Enter the following commands at an attached terminal or via Telnet to the switch.

1 Login using the appropriate administrator username/password pair

2 Enter the enable mode.

Type enable <cr>, then input the cr>, then input the cr> and press <Enter>

3 Enter the configuration mode

Type configure terminal <Enter>

4 Enable the dot1x mode.

Type aaa dot1x mode enable <Enter>.

5 Verify that the dot1x enable was successful.

Type show aaa dot1x <Enter>.

6 Enter Configuration commands, one per line. End with CNTL Z.

**NOTE**—The command reference for this action may be found in "RADIUS Commands" on page 830.

# aaa radius-server <name of RADIUS server> <acctport portnumber>...<mode enable | disable> <Enter>

The parameters and defaults for this command are:

acctport	Port number used for accounting	default = 1813
authport	Port number used for authentication	default = 1812
host	The IP address of the RADIUS server.	default = 0.0.0.0
inservice	Bring server in service immediately.	default = Y
key	Shared secret text string	default = "changeme"
mode	Enable or Disable as an authentication server	default = disabled
retransm it	Maximum times a RADIUS request is retried	default = 3
timeout	Specify time period between RADIUS requests.	default = 10

7 Verify that the radius server was created. RADIUS server is created with the default values, unless otherwise specified.

Type show aaa radius-server <Enter>

A list of authorization servers and their parameters will be displayed.

 Auth Server List

 ----- 

 Pri
 Host IP addr
 Port Acct Retries Timeout Secret
 Status
 Inservice

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

 1
 IAS
 10.1.1.214
 1812
 1813
 3
 5
 tamales
 Enabled
 Yes



Assigning a Server to 802.1x Authentication

Each instance of a RADIUS server, as created above, must be explicitly assigned as an authentication server.

1 Verify that the server you created above is enabled as a do1x authentication server and that it is assigned the correct priority.

```
Type show aaa dot1x <Enter>.
```

The system will display a screen similar to this:

The order in which servers are queried is determined by their priority. The server with the highest priority (priority = 1) is queried first.

2 If the priority of the server is too low, change the priority with the aaa dot1x auth-server command.

Type aaa dot1x auth-server <server name> <priority> <number> <Enter>.

# **Assigning Default Roles**

A role is a broad classification of users and is associated with a specific set of permissions. The role function is a method by which a user may be associated with specific Access Control Lists (ACLs).

Create an Access Control List (ACL)

Before a role can be created, the ACLs that will be associated with the role must be created. The following procedures will walk you through the process of creating an ACL named *TestEmpl-acl* and creating a User Role named *TestEmployee*.

Enter the following commands at an attached terminal or via Telnet to the switch.

- Login using the appropriate administrator username/password pair
- 2 Enter the enable mode.

Type enable <Enter>, then type cpassword> <Enter>

3 Enter the configuration mode

Type configure t <Enter>

4 Enter Configuration commands, one per line. End with CNTL Z.

**NOTE**—The command reference for this action may be found in "Access Control List Commands" on page 835.

The system will display a screen similar to this:

```
(Alcatel) #configure t
Enter Configuration commands, one per line. End with CNTL/Z
```

(Alcatel) (config) #

5 Create an ACL with the name TestEmpl-acl (you may choose any name you wish).

Type ip access-list session TestEmpl-acl <Enter>

The system will display a screen similar to this:

```
(Alcatel) (config) #ip access-list session TestEmpl-acl
(Alcatel) (config-sess-TestEmpl-acl)#
```



6 Specify any for the source, destination, and port parameters and permit for the action parameter.

Type any any any permit <Enter>

Create a User Role

In this example we will create a user role and apply the session-acl TestEmpl-acl to that role.

1 Create a user role named TestEmployee.

Type user-role TestEmployee <Enter>

The system will display a screen similar to this:

```
(Alcatel) (config) #user-role TestEmployee
(Alcatel) (config-role) #
```

2 Associate (assign) the session-acl, *TestEmpl-acl*, created in the steps above.

Type session-acl TestEmpl-acl <Enter>

The system will display a screen similar to this:

```
(Alcatel) (config) #user-role TestEmployee
(Alcatel) (config-role) #session-acl TestEmpl-acl
```

```
(Alcatel) (config-role) #
```

Type exit<Enter> to exit the config-role mode.

```
(Alcatel) (config) #user-role TestEmployee
(Alcatel) (config-role) #session-acl TestEmpl-acl
(Alcatel) (config-role) #exit
(Alcatel) (config) #
```

3 Assign the TestEmployee role as the default role for all users authenticated using 802.1X

Type aaa dot1x default-role TestEmployee <Enter>

The system will display a screen similar to this:

```
(Alcatel) (config) #aaa dot1x default-role TestEmployee
```

```
(Alcatel) (config) #
```

4 Verify that the authorization server and default roles were correctly assigned.

Type show and dot1x <Enter>. The system will display a screen similar to this:

You may also view the rights that are assigned to the user (TestEmployee)

Type show rights TestEmployee <Enter>.

The system will display a screen similar to this:



#### Configuring the 802.1x State Machine

Dot1x CLI Commands

This section describes the commands and variables that may be adjusted to tune the 802.1x state machine. In most cases, the default settings should be used.

The following is a description of the 802.1x commands used to configure the state machine.

Commands in the dot1x group may be reset to their default values or disabled by using the *no* form of the command as shown below.

(Alcatel) (config) # no dot1x re-authentication <Enter>

#### dot1x default

The *dot1x default* command resets the dot1x state machine configuration to its default values.

#### dot1x max-req <retry>

The *dot1x max-req* command sets the maximum number of attempts the server will make to authenticate a supplicant.

Default: 5

Valid Range: 0 - 10

#### dot1x multicast-keyrotation

The *dot1x multicast-keyrotation* command enables the rotation of multicast keys. Multicast keys are used to encrypt multicast packets generated for each AP. Multicast keys are associated with each essid.

Default: Disabled

#### dot1x re-authentication

The *dot1x re-authentication* command enables the re-authentication of supplicants. Re-authorization occurs after a specific amount of time has elapsed from the last authentication. The time period is specified using the *dot1x timeout reauthperiod* command (see below). Unicast keys are updated after each re-authorization.

Default: Disabled

#### Dot1x server

The dot1x server commands are used for setting the back-end authentication server configuration.

#### dot1x server server-retry <retry>

The *dot1x server server-retry* command sets the number of attempts the switch may make to obtain an authentication from the server.

Default: 2

Valid Range: 0 - 3

#### dot1x server server-timeout <timeout>

The *dot1x server server-timeout* command sets the delay period between radius requests.

Default: 30 (seconds)

Valid Range: 1 - 65535

#### dot1x timeout

The dot1x timeout commands are used for setting the periods of the timers used in the 802.1x authenticator.

### dot1x timeout idrequest-period <IDR period>

The *dot1x timeout idrequest-period* command sets the period between each identity request sent to the supplicant by the authenticator. The identity request is sent when a client associates or re-associates with an AP or when the re-authentication timer expires (see *dot1x re-authentication*, above).

Default: 30 (seconds)

Valid Range: 1 - 65535

#### dot1x timeout mcastkey-rotation-period <MKR period>

The *dot1x timeout mcastkey-rotation-period* command sets the time between each multicast key rotation. A key message is sent by the authenticator to all the stations associated with an AP at the expiration of the period.

Default: 1200 (seconds)

Valid Range: 1-4294967295



#### dot1x timeout quiet-period <quiet period>

The state machine enters a quiet period when authentication fails. The *dot1x timeout quiet-period* command sets the time interval during which the authenticator will make no attempt to acquire the supplicant.

Default: 60 (seconds)

Valid Range: 0 - 65535

#### dot1x timeout reauthperiod {<RA period>|server}

The *dot1x timeout reauthperiod* command sets the period between re-authorization and the last authorization. This period may also be driven by the *Session-Timeout* attribute from the authentication server.

Default: 60 (seconds)

Valid Range: 1-2147483647

#### 802.1x Show Commands

This sections describes the show commands applicable to 802.1x.

#### show dot1x config

The show dot1x config command displays the current values the 802.1x authenticator's parameters.

When the command is executed the system will display a screen similar to the one below.

```
(OmniAccess 6000) #show dot1x config
Authentication Server Timeout: 30 Seconds
Client Response Timeout: 30 Seconds
Fail Timeout: 30 Seconds
Client Retry Count: 3
Server Retry Count: 2
Key Retry Count: 1
Reauthentication: Disabled
Reauthentication Time Interval: 86400 Seconds
Multicast Key Rotation: Disabled
Multicast Key Rotation Time Interval: 1800 Seconds
Unicast Key Rotation: Disabled
Unicast Key Rotation Time Interval: 900 Seconds
Countermeasure: Disabled
Wired Clients: Enabled
Enforce Machine Authentication: Disabled
Machine Auth Cache Timeout: 24 Hours
Machine Auth Default Role: guest
User Auth Default Role: quest
WPA Key Retry Count: 3
WPA Key Timeout: 1
Ignore EAPOL-Start after Authentication: Disabled
(OmniAccess 6000) #
```



#### show dot1x ap-table

The show dot1x ap-table command and its variants display information about access points connected to the switch.

When the show dot1x ap-table command is executed the systems displays a screen similar to the one below.

# show dot1x ap-table list-aps [static-wep|dynamic-wep|tkip]

Options:

static-wep	Displays the static wep keys of all the APs. The information includes:
	AP MAC Address
	<ul> <li>WEP Key and Size for each of the four keys.</li> </ul>
dynamic wep	Displays the dynamic wep keys of all the APs. The information includes:
	AP MAC Address
	<ul> <li>WEP Key, Size, and Slot for the two keys.</li> </ul>
tkip	Displays the tkip keys for all APs.

#### show dot1x supplicant-info list-all

The show dot1x supplicant-info list all command displays details about the supplicants associated with the switch.

When this command is executed the system returns a screen containing a table the includes the following information about each of the supplicants.

MAC Address of the supplicant

- User Name
- Authentication Status (yes/no)
- AP MAC
- Encryption Key
- Authorization Mode
- EAP type

#### show dot1x supplicant-info statistics

The show dot1x supplicant-info statistics command displays statistical information about each supplicant.

When this command is executed the system returns a screen containing a table that includes the following statistical information about each of the supplicants.

•	MAC	The supplicant's MAC Address
•	Name	User name
•	Auth-Succs	The number of times the supplicant has been successfully authenticated.
•	Auth-Fails	The total number of times the supplicant sent invalid user credentials and/or entered an incorrect password.
•	Auth-Tmout	The number of times authorization requests timed out.
•	Reauths	The number of times the supplicant has successfully reauthenticated.
•	Supp-Naks	The number of times a Supplicant NAK occurred. This may be due to an EAP mismatch between the supplicant and authentication server, or if the server has been configured for multiple EAP types.
•	UKeyRota- tions	The number of times the Unicast key associated with the supplicant has been rotated.
•	MKeyRota- tions	The number of times the Multicast key associated with the supplicant has been rotated.



#### show aaa dot1x

The show aaa dot1x commands displays which servers are configured for 802.1x authentication, the priority of each server, and the default role assigned to all users authenticated under 802.1x.

When the command is executed the system will display a screen similar to the one below.



• Inservice This field indicates the status of connectivity between the switch and the server.

#### Debug Commands

The commands in this section are used for debugging the authentication module. Debugging is accomplished through a telnet monitor.

A two step process is required to enter the debugging mode. First, enter the configure terminal mode, then enter the debug mode.

Exit debugging using the *no debug* command, see "Debug Commands" on page 831.

1 Enter the configuration command mode.

Type configure t <Enter>

The system will display a screen similar to the one shown here.

```
(Alcatel) #configure t
Enter Configuration commands, one per line. End with CNTL/Z
```

2 Enter the debugging mode

Type logging monitor debugging authmgr <Enter>

This command enables monitoring of authorization debugging messages on a telnet terminal.

Options for the debugging authmgr command are:

•	dot1xcfg	Debug 802.1x configuration items.
•	dot1xeapol	Debug EAPOL messages from supplicants to authenticator.
•	dot1xkeymgt	Debug Key messages from the 802.1x authenticator to the supplicant.
•	dot1xradius	Debug messages between the radius server and the authenticator.
•	dot1xspmgt	Debug 802.1x authenticator SAP context management.
•	dot1xsapmmsg	Debug messages between the 802.1x authenticator the STM.
•	dot1xxsm	Debug the 802.1x state machine.



#### RF Deauthentication Debugging

Using Alcatel Air Management features, Alcatel APs can identify other APs and client stations that violate configured protection policies. The Alcatel APs can also be configured to send deauthentication frames (or laser-beams) to prevent the offending AP or client station behavior (refer to the Alcatel AOS-W User's Guide).

Since deauthentication frames are spoofed on behalf of the AP or client station, the true source of packet is not evident. However, deauthentication debugging reveals the source of these packets to help verify that enforcement policies are behaving as expected. To enable or disable this feature, use the following CLI configuration command:

```
(config) # wms general laser-beam-debug {enabledisable}
```

When enabled, Alcatel APs alter their deauthentication frames to include their own MAC address. This identifies the source of the laser-beam to packet capture software or inspection equipment ("sniffers") and nullifies the deauthentication effect.

Because debugging disables the intended deauthentication, is should be turned off except when debugging is required.

## Certificates

This section of the chapter deals with authentication certificates. Certificates provide strong security when authenticating users and computers and eliminate the need for less secure password based authentication schemes.

Three authentication methods use certificates: Extensible Authentication Protocol-Transport Level Security (EAP-TLS), Protected Extensible Authentication Protocol (PEAP), and TTLS. Alcatel AOS-W employs all three.

This section will describe the process of acquiring certificates for authenticating servers (server certificates) and for authenticating clients (client certificates).

#### Introduction to Server, Client, and CA Certificates

**Client Certificates and Certificate Verification** 

Clients as well as the servers to which they attach may hold authentication certificates that validate their identity. When a client connects to a server for the first time, or the first time since its previous certificate has expired or been revoked, the server will request that the client transmit its authentication certificate. The client's certificate is then verified against the CA certificate of the authority which issued it (Clients do not have to validate the Server certificate in order for 802.1x to function).

#### Server Certificates and Certificate Verification

Similar to client certificates, a server has a certificate which authenticates its identity. The first time a client associates with a server, or the first time after the server's certificate has expired or been revoked, the client makes a request for the server's authentication certificate. The server's certificate is then verified against the CA certificate of the authority which issued it.

#### Certification Authority (CA) Certificates

A certification authority issues authentication certificates to both servers and clients. The only way to assure that a certificate issued to a client or server is valid is to examine the digital signature. This is done by comparing it to the digital signature on the issuing certification authority's CA certificate. Therefore, to complete the authentication process for either a server or client the parties must have both the CA and the client/server certificate.



#### **Obtaining A Certification Authority (CA) Certificate**

CA Certificates are obtained from the corporate CA server. Download the certificate using the following procedure.

1 Open a web browser and point it at the corporate CA server. For example:

http://<ip address>/crtserv

The following page should appear in your browser.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	×
File Edit View Favorites Tools Help	7
🚱 Back 🔹 🕥 🔸 📓 🐔 🔎 Search 🤺 Favorites 🜒 Media 🤣 🍰 🌲	»
Address 🕘 http://10.1.1.2/certsrv/	•
	*
Microsoft Certificate Services aruba-server Home	
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	
Select a task: © Retrieve the CA certificate or certificate revocation list	
<ul> <li>Request a certificate</li> <li>Check on a pending certificate</li> </ul>	
Next >	
	-
🕘 Done 👘 🔮 Internet	//.



Select the *Retrieve the CA Certificate or certificate revocation list* option, then click Next. The following screen should appear in your browser.



3 Click on the Install this CA certification path link.



You may receive one or both of the following warnings. In either case click **Yes**.

Potentia	Scripting	Violation
1	This Web site could	site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you w	ant this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
		Yes No
		tificate Store
		Issuer : Self Issued Time Validity : Monday, July 29, 2002 through Sunday, July 29, 2007 Serial Number : 7C+4054D 59A933BD 466F47A0 428E0B42 Thumbprint (sha1) : 90E52E7 717D8898 A51BASFF 4F5A1BFB D3610334 Thumbprint (md5) : FDFAD3D9 00028DBA 0944285A 88E29DB6 Yes

The installation should proceed automatically and the following screen should appear.

Microsoft Certificate Services - Microsoft Internet Explore	ar _ 🗆 🗙
File Edit View Favorites Tools Help	an 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 19
🚱 Back 👻 🕤 👻 😫 🏠 🔎 Search 🤺 Fav	orites 🔮 Media 🧭 🏾 🎽
Address 🙆 http://10.1.1.2/certsrv/certrmpn.asp	🔽 🋃 Go 🛛 Links » 📆 🗸
	A
Microsoft Certificate Services	<u>Home</u>
CA Contificate In stalled	
The CA certificate has been successfully installe	d
	u.
	-
	🔡 Internet

# **Obtaining a Server Certificate**

The following steps will guide you through the process of obtaining and installing an authentication certificate on your server.

1 Open a web browser and point it at the corporate CA server

(http://<ip address>/crtserv).

The webpage below should appear in your browser window.

File       Edit       View       Favorites       Tools       Help         Start       Start       Start       Favorites       Media       So       <
Stack <ul> <li></li></ul>
Address Address http://10.1.1.2/certsrv/
Microsoft Certificate Services Home
Welcome
weicome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate C Check on a pending certificate
Next >
Done



2 Select the *Request a certificate* option, then click **Next**.

The web page below should appear in your browser window.



3 Select Advanced request, then click **Next**.

The following web page should appear in your browser window.





4 Select the Submit a certificate request to this CA using a form option, then click Next.

You may receive one of the security warnings shown below. Click Yes.



The web page form below should appear in your browser window.

🎒 Microsoft Certifi	ate Services - Microsoft Internet Explorer			<u>_ 0 ×</u>
File Edit View	Favorites Tools Help			<b>.</b>
🕞 Back 👻 🕥	🛛 📓 🏠 🔎 Search 🤺 Favorites 🜒 Media 🧭 🔗 - 🌭	W.	· 🔁	
Address 🙆 http://10	0.1.1.2/certsrv/certrqma.asp		💌 🔁 Go	Links » 📆 🗸
Microsoft Certifi	cate Services			Home
Advanced Ce	rtificate Request			
ldentifying Infor	mation:			
Name:				
E-Mail:				
Company:	Aruba Networks			
Department:				
City:	San Jose			
State:	CA			
Country/Region:	US			
Intended Purpo	se:			
	Client Authentication Certificate			
	<b>_</b> _			
Key Options:				
USP:	Cryptographic Provider VI.U			
Key Usage:	Exchange C Signature Both			
rtey olize.	Max:1024			
	Create new key set			
	Cilise evisting key set			
	Enable strong private key protection			
	Invaria Reys as exportable			
	You must be an administrator to generate			
	a key in the local machine store.			
Additional Optic	ns:			
Hash Algorithm:	SHA-1			
	Uniy used to sign request.			
	L Save request to a PKCS #10 file			
Attributes:				
			0	unit > 1
Dana			Sut	
Done			Three The States of the States	BL .

5 Enter the following information in the *Identity Information* section of the form:

- Name (the authentication server's fully qualified name)
- The administrator's email address
- The name of the company
- The department within the company to which the server belongs
- The city, state, and country where the company is located.



6 Select *Server Authentication Server Certificate* under the Intended Purpose section.

Set the following options under the Key Options section:

- CSP Select the *Microsoft Base Cryptographics Provider v1.0* option from the drop down box.
- Key Usage Select Both
- Key Size
   Set the key size to 1024
- Create new key set Select
- Use local machine Check use *local machine store* option store
- 7 Click Submit after you have correctly entered all the information.

You may see the warning text box pictured below appear on the screen, Click **Yes**.

Potential	Scripting Violation
1	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

The web page shown below should appear in your browser window.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	<b>R</b>
🚱 Back 🔹 🕥 – 💌 😰 🏠 🔎 Search 🐈 Favorites 🜒 Media 🤗	»
Address 🙆 http://10.1.1.2/certsrv/certfnsh.asp 🔽 🎅 Go Links 🎽	<b>D</b> -
	<u> </u>
Microsoft Certificate Services Home	
Certificate Issued	
	-
The certificate you requested was issued to you.	
Install this certificate	
	-
🔊 Done 🖉 🖉 Internet	_/_

8 Click the Install this certificate button.

You may see the warning text box pictured below appear on the screen, Click **Yes**.

Pot	ential	Scripting Violation
4	1	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
		Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
		Yes No

The certificate should now be installed on the authentication server.



#### **Obtaining a Client Certificate**

The following steps will guide you through the process of obtaining and installing an authentication certificate on your client station/computer.

1 Open a web browser and point it at the corporate CA server

(http://<ip address>/crtserv).

The webpage below should appear in your browser window.

🚰 Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help 🥂
🚱 Back 🔹 🕥 👻 🛃 🚮 🔎 Search 👷 Favorites 🜒 Media 🧭 🔗 - 🌺 🎽
Address 🗃 http://10.1.1.2/certsrv/
Microsoft Certificate Services Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate C Check on a pending certificate
Next >
Done Done Done

2 Select the *Request a certificate* option, then click Next.

The web page below should appear in your browser window.

🖉 Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
🕞 Back 🔹 🕥 - 💌 😰 🏠 🔎 Search 🤺 Favorites 🔇 Media 🤗 👘
Address 🙆 http://10.1.1.2/certsrv/certrqus.asp 💽 🕤 Go Links » 📆 🗸
Microsoft Certificate Services Home
Choose Request Type
Please select the type of request you would like to make:
O User certificate request:
Web Browser Certificate E-Mail Protection Certificate
<ul> <li>Advanced request</li> </ul>
Next >
🗃 Done 🛛 👘 👘 Internet

**3** Select Advanced request, then click **Next**.



The following web page should appear in your browser window.



# Select the Submit a certificate request to this CA using a form option, then click Next.

You may receive one of the security warnings shown below. Click Yes.





The web page form below should appear in your browser window.

🎒 Microsoft Certifica	ate Services - Microsoft Internet Explorer			>
File Edit View F	avorites Tools Help			
😋 Back 🔹 🕥 🗸	🖹 😰 🏠 🔎 Search 🤺 Favorites 🜒 Media 🥝 🍰 🌜		-	
Address 餐 http://10.	1.1.2/certsrv/certrqma.asp		💌 🄁 Go	Links » 📆 🗸
Microsoft Certific	ate Services			<u>Home</u>
Advanced Cer	tificate Request			
ldentifving Inforn	nation:			
Name:		-		
E-Mail:				
E-man. [				
Company:	Aruba Networks			
Department:				
City:	San Jose			
State:	CA			
Country/Region:	US			
Intended Purpos	2.			
	Client Authentication Certificate	-		
I				
Key Options:		-		
CSP:	Microsoft Base Cryptographic Provider v1.0	]		
Key Usage:	C Exchange C Signature 👁 Both			
Key Size:	512 Min: 384 (common key sizes: <u>512 1024</u> ) Max:1024 (			
	Create new key set			
	□ Set the container name			
	O Use existing key set			
	Enable strong private key protection			
	□ Mark keys as exportable —			
	Use local machine store You must be an administrator to generate a key in the local machine store.			
Additional Option	IS:			
Hash Algorithm:	SHA-1	-		
,	ony assure sign request. □ Save request to a PKCS #10 file			
I				
Attributes:	T T			
			Sub	omit >
Done			intern	et

5 Enter the following information in the *Identity Information* section of the form:

- Name (the authentication server's fully qualified name)
- The User's email address
- The name of the company
- The department within the company to which the server belongs
- The city, state, and country where the company is located.

6 Select Server Authentication Server Certificate under the Intended Purpose section.

Set the following options under the Key Options section:

- CSP Select the *Client Authentication Certificate* option from the drop down box.
- Key Usage Select Both
- Key Size Set the key size to 1024
- Create new key set Select
- Use local machine Check use *local machine store* option store

7 Click **Submit** after you have correctly entered all the information.

You may see the warning text box pictured below appear on the screen, click **Yes**.

Potential	Scripting Violation
1	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No



The web page shown below should appear in your browser window.

🚰 Microsoft Certificate Services - Microsoft Internet Explorer 📃 📃	
File Edit View Favorites Tools Help	1
🚱 Back 🔹 🕥 - 💌 😰 🔥 🔎 Search 🤺 Favorites 🔮 Media 🚱	»
Address 🙆 http://10.1.1.2/certsrv/certfnsh.asp 💽 🕞 Go 🛛 Links 🄌 🦿	1 -
Microsoft Certificate Services Home	4
Certificate Issued	
The certificate you requested was issued to you.	
🕘 Done	-

8 Click the *Install this certificate* button.

You may see the warning text box pictured below appear on the screen, Click Yes.

Potentia	al Scripting Violation
1	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	Yes No

The certificate should now be installed on the client station/computer.

# 802.1x Configuration under Microsoft Pocket PC

Pocket PC 2003 includes built-in support for wireless networks and 802.1x authentication. Some PDA vendors, including HP, have also produced system updates to enable support for WPA and TKIP, assuming the NIC driver also supports TKIP. Section 1 of this document explains how to configure Pocket PC devices using either the built-in 802.1x supplicant. Section 2 explains how to perform the same configuration using the Funk Odyssey client.
## **Export Trusted Certification Authority**

The first step in enabling 802.1x authentication on Pocket PC devices is to install a trusted certification authority, if required. If the RADIUS server uses a certificate with a certification path already trusted by the Pocket PC devices, then this step is not necessary. Certificates purchased from large certificate authorities such as Verisign, for example, will already be trusted by the clients. If a self-signed certificate is used, the certification path will need to be installed on the client. To do this, first export the certificate for the root certificate authority into a standard X.509 file format. This step can be accomplished on any Windows computer where the trusted certification path has already been installed. Launch the Microsoft Management Console by selecting **Start > Run**, and entering "mmc" in the box.

In the management console, select **File > Add/Remove Snap-in**. Select the Certificates snap-in.

Typically, a trusted certificate authority certificate can be found in both the user certificate store and the computer certificate store. When prompted to select the certificate snap-in, choose "My user account".

Next, locate the certificate for the trusted certificate authority, right-click on it, select "All tasks", then select "Export".

When prompted, export the key as a DER-encoded binary X.509 file,w.

If given the option, do not export the private key. This option only appears on the certificate authority itself. Save the file somewhere accessible on the hard drive.

### Install Certificate Authority

The next step of the process is to copy the previously generated X.509 certificate to the Pocket PC client device. To do this, place the X.509 certificate on a machine running ActiveSync that has a partnership arrangement with a Pocket PC device. The Pocket PC device's filesystem should appear under Windows Explorer, and a folder entitled "<mobile device name> My Documents" should appear on the Windows desktop. Copy the X.509 certificate file from the host computer to the "My Documents" directory on the Pocket PC device.

Next, install the certification authority in the Pocket PC device's certificate store. To do this, run the Pocket PC File Explorer and navigate to "My Documents".



To install the certificate authority, simply tap on the certificate file. The system will ask for confirmation before installing the certificate. Select "Yes".

The certification path has now been installed. It can be verified by navigating on the Pocket PC device to **Settings > System > Certificates > Root**.

### **Configure Wireless Settings**

The next step will be to configure wireless settings. If required, install the appropriate NIC card and drivers. Ensure that the drivers are specific to Pocket PC 2003 – earlier versions of Pocket PC and Windows CE did not contain native support for wireless.

Configure wireless settings by navigating to **Settings > Connections > Connections > Advanced > Network Card > Wireless**.

If the appropriate ESSID is not already shown in the list, add it by selecting "Add new".

After filling in the ESSID in the **Network Name** field, select the **Authentication** tab. The authentication settings screen appears.

Configure the screen. In the EAP type field, select PEAP. Do not click **Properties** – this is used to configure certificate-based authentication. A warning message will be generated if **Properties** is clicked – this warning message may be ignored.

### Login to Wireless Network

Once the wireless network has been configured, the Pocket PC device will associate with an Access Point and begin 802.1x authentication. Once this has begun, the user will be prompted for a username and password.

Supply the necessary login credentials, and the process will complete.

### **Configuration using Funk Odyssey Client**

The Funk Odyssey client is a commercial software application available on a number of Windows platforms, including Pocket PC 2002 and 2003. The software acts as both a radio manager and an 802.1x supplicant, and supports several different methods of EAP authentication using 802.1x. The software also supports multiple profiles, simplifying mobility between public and private wireless networks.

Configuration of the Funk Odyssey client can be performed either on the host PC or on the Pocket PC device. All permanent configuration should be done on the host PC, which will then push the configuration to the mobile device. This document will describe configuration on the host PC.

### **Certificate Configuration**

During the operation of 802.1x authentication, a digital certificate will be passed from the authentication server to the client. This certificate will be used by the client to authenticate the network infrastructure, so that connections to untrusted networks are not made. To authenticate the network, the client checks the certification path of the server certificate and compares it with trusted root certification authorities for which the client has been configured. Microsoft Windows and Pocket PC come with a number of large public certification authorities pre-installed, including authorities such as VeriSign, SecureSign, GTE, C&W, and others. An organization may also use a self-signed server certificate, generated by a local certificate server.

The Funk Odyssey client will automatically push required certificates to the mobile device. However, this assumes that the certificate information – including trusted certification paths – is already available on the host PC. If a server certificate's certification path includes of these pre-installed certificate authorities, no further action is required on the client. If a self-signed certificate is used, the organization's certificate authority server must be configured on the client device so that it is trusted. For instructions on installing a certification authority (CA) certificate on the host PC, please consult the Alcatel AOS-W User's Guide and look for the section entitled "Obtaining a Certification Authority (CA) Certificate."

### **Odyssey Client Configuration**

To configure the Odyssey client, navigate on the host PC to **Start > Programs > Funk Software > Odyssey Client for Pocket PC** and select the Configuration Manager. The Configuration Manager appears.

### **Trusted Servers Configuration**

The first configuration step is to specify which 802.1x authentication servers should be trusted. Click **Trusted Servers**.

The server trust configuration may be done in two different ways. One method instructs the client to trust any server that provides a certificate ultimately signed by a specified certification authority (CA). This option is not recommended if the CA is a public CA, since the client would then trust any certificate that was also signed by that same CA. To configure this method, click **Advanced**.



The second and more secure method specifies the domain name of the authentication server. Only servers with this domain name that send a valid trusted certificate will be authorized. To configure a trusted server, click **Add** on the **Trusted Servers** screen.

### Profile Configuration

To use 802.1x authentication, a profile must be created to configure the appropriate EAP type, as well as other authentication details. Profiles are configured in the **Profiles** screen.

The first step of profile configuration is to establish the user information and type of authentication credentials. In this example, a username and password is required to access the network. The password can be saved on the device, if desired.

Next, the authentication EAP type must be selected. In this case, PEAP is used in this network. The "Validate server certificate" option should always be enabled for security reasons.

Finally, settings for PEAP must be configured. MS-CHAP v2 is used to hash the user's password. This is the default PEAP mode of operation for most RADIUS servers, including Microsoft IAS.

### **Networks Configuration**

Once a profile has been configured, the SSID with which the device should connect must be configured. This is done in the "Networks" screen.

In the example below, the SSID "Wireless LAN-01" will be used. Open authentication is used with WEP encryption. The previously-created "Wireless LAN" authentication profile will be used to authenticate to the network, and WEP keys will be generated automatically during 802.1x authentication.

### **Connection Configuration**

Finally, the default network should be specified. Although multiple networks may be configured under the "Networks" screen, only one of them will be the default network.

### **Push to Device**

After all configuration has been completed in the Funk Odyssey Configuration Manager, the configuration must be pushed out to the mobile device. After establishing an ActiveSync connection, select **Commands > Push To Device** from the Odyssey Configuration Manager.

### **Captive Portal Certificates with Intermediate CAs**

To install certificates for captive portal installations that have intermediate CAs:

1. Concatenate the certificates in the following order with every certificate followed by whatever signed it:

- server certificates
- intermediate certificates
- 2. The very last intermediate certificate must be signed by the CA that is present on the client.

All certificates are formatted x509 PEM unencrypted.



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 11 802.1x Solution Cookbook

This chapter describes the theory, configuration, and operation of a wireless network based on Microsoft Windows client and server components and utilizing the 802.1x authentication protocol. This design is based on an actual deployment in a K-12 school district located in the United States. The key features of this design include:

- Two-phase authentication based on both computer and user authentication
- Role-based authorization to segment student, faculty, and IT staff network access
- Laptops and client devices that are shared by multiple users throughout the day
- Secure guest access
- Link-layer encryption using per-user dynamic WEP keys

The school system has deployed a wireless network consisting of an OmniAccess 6000 Wireless LAN system, over two hundred laptops with integrated 802.11 network interface cards running Microsoft Windows XP, several dozen HP iPAQ 2215 PDAs running Microsoft PocketPC 2003, and a Microsoft server infrastructure. The laptops are shared by students during the instructional day to provide Internet access and access to central storage on a Windows 2003 Server machine. PDAs are used by the faculty only. Approximately one hundred Alcatel 52 Access Points have been deployed throughout the initial building to provide wireless coverage. The building is several decades old and constructed with concrete interior walls, so a higher than required number of APs was deployed to ensure both coverage and performance. 802.1x authentication based on PEAP is used to provide both computer and user authentication. Domain credentials are used for computer authentication, and the user's Windows login and password are used for user authentication. A single user sign-on facilitates both authentication to the wireless network and access to the Windows server resources. WEP is used as a link-layer encryption technology, with dynamic per-user WEP keys being provided through the 802.1x authentication process. A migration to either WPA or 802.11i is planned for this network, which will be automated through group policy objects.

# Physical Topology

A map of the network, excluding individual APs, is shown below. The OmniAccess 6000 switch has been deployed in the main server room, with half of the APs directly attached to the switch via Cat5 cabling from the classrooms. The Alcatel switch provides power over Ethernet (POE) for these APs. The rest of the APs are home run to a wiring closet on the second floor, where they connect to a standard Ethernet switch supporting POE. The second floor wiring closet connects to the first floor server room through a fiber link connected to a router port.

The OmniAccess 6000 switch connects to the rest of the network through a port on the main routing switch. This port is part of the 10.1.1.0 subnet, on which most of the servers also exist.

Redundancy was not a primary design concern in the wireless network, since other parts of the network are not redundant.

# Wireless Network Operation

Normal wireless network operation is defined by the following processes.

### Wireless Laptops

1. Wireless laptop boots Windows XP and comes up with a Windows domain login screen.

2. In order to gain network connectivity to the domain controller, the Windows laptop associates and authenticates to the wireless network.

- a The laptop searches for the wireless ESSID "Wireless LAN-01", chooses the AP with the best signal strength, and attempts to associate to it.
  - i. The laptop will send 802.11 broadcast probe-requests to search for any ESSID.
  - •ii. All APs in range will respond with probe-responses containing the ESSID "Wireless LAN-01". A load balancing feature has been enabled on the Alcatel switch that will limit the number of users on a single AP to 20. If the load-balancing high watermark has been reached on a given AP, this AP will not respond to probe-responses. From the laptop's perspective, it appears as though the AP does not exist.
  - •iii. The laptop will choose the best AP among the list of responses. This decision is typically based on measured signal strength.
  - iv. The laptop will initiate an 802.11 association process with the chosen AP.
- b The laptop will initiate 802.1x authentication by transmitting an EAPOL-Start message to the AP. An 802.1x authentication sequence using PEAP will follow. The Alcatel switch will convert all 802.1x EAPOL messages on the wireless network into EAPOL-over-RADIUS messages on the wired network, and will transmit them to the Microsoft IAS server. All 802.1x communication is between the client and the IAS server, with the Alcatel components acting as pass-through devices.
  - •i. The laptop will transmit a username of "host\computer\_name" where "computer\_name" is replaced by the actual configured computer name of the laptop. The Alcatel switch will recognize the username information, record it, and map it to the MAC address of the client in an internal table.
  - •ii. The IAS server will compare the transmitted username with a list of computers and users in the Active Directory database. Because the username represents a computer in the domain, the IAS server will process the authentication request according to a policy matching all domain computers.
  - •iii. The IAS server will transmit a digital certificate to the client. This digital certificate was issued and signed by the local Windows certificate authority. Each laptop has been configured to trust the local certificate authority. Because of this trust relationship, the client accepts the certificate and allows authentication to proceed. If an invalid certificate were presented (for example, from an intruder attempting to gain access to the network by running a separate AP and authentication server), the client would halt the authentication process at this point.
  - •iv. During the encrypted PEAP exchange, the client will again transmit a username corresponding to its computer name. Using MS-CHAP v2, the computer will next transmit a password. In this case, the password is the domain SID (security identifier) previously exchanged between the laptop and the domain controller the first time the laptop joined the domain. The SID is stored on each laptop automatically.
  - v. If the computer name and SID match those stored in the Active Directory database, authentication is granted. The IAS server transmits a RADIUS "Accept" message to the Alcatel switch. The Alcatel switch transmits an EAPOL "Success" message to the wireless client. This concludes 802.1x authentication.



The IAS server has also been configured to transmit an RADIUS attribute called "Class" to the Alcatel switch. The value of this attribute is set to "computer" to identify the authenticated device as a computer. The Alcatel switch is configured to recognize this RADIUS attribute, and maps the wireless client to a "computer" role.

- •vi. Using information from the 802.1x authentication exchange, the wireless client and Alcatel switch derive dynamic keys for use in the encryption process. After key derivation, both the client and the Alcatel switch begin using the WEP encryption protocol to encrypt data on the wireless network.
- c The laptop transmits a DHCP request. The Alcatel switch intercepts this DHCP request and forwards it to an external DHCP server running on a Windows server. The server assigns an IP address to the wireless laptop and issues a DHCP response. The Alcatel switch learns the IP address assigned to the client and stores this information in an internal table.
- d The wireless laptop now has IP connectivity to the network, and can contact the domain controller for authentication requests and group policy updates. At this point, the laptop is still displaying a Windows domain login screen.
- 3 A user enters a username and password in the Windows domain login screen on the wireless laptop. A standard Windows authentication procedure follows between the client and the domain controller.
- 4. If the Windows logon is successful, the laptop will perform another 802.1x re-authentication to the wireless network using the user's authentication credentials. This behavior is the default for Windows, and is configurable through a registry setting or through group policy.

- a The laptop will transmit an EAPOL-Start message to the Alcatel switch. The Alcatel switch will then proceed with 802.1x authentication by transmitting an EAPOL "Request identity" message to the laptop.
- b b. The laptop will transmit the user's username. The Alcatel switch will recognize the username information, record it, and map it to the MAC address of the client in an internal table. The new username will replace the previously-learned computer name.
- c The IAS server will compare the transmitted username with a list of computers and users on the Active Directory server. Because the username represents a user in the domain, the IAS server will process the authentication request according to a policy matching the group to which the user belongs (faculty, student, or system administrator.)
- d The IAS server will transmit a digital certificate to the client. This digital certificate was issued and signed by the local Windows certificate authority. Each laptop has been configured to trust the local certificate authority. Because of this trust relationship, the client accepts the certificate and allows authentication to proceed. If an invalid certificate were presented (for example, from an intruder attempting to gain access to the network by running a separate AP and authentication server), the client would halt the authentication process at this point.
- e During the encrypted PEAP exchange, the client will again transmit a username. Using MS-CHAP v2, the computer will next transmit the user's password entered during the Windows logon process. Note that this exchange is MS-CHAP v2, so the actual password is not transmitted.
- f If the username and password match those stored in the Active Directory database, authentication is granted. The IAS server transmits a RADIUS "Accept" message to the Alcatel switch. The Alcatel switch transmits an EAPOL "Success" message to the wireless client. This concludes 802.1x authentication.
  - •i. The IAS server has also been configured to transmit an RADIUS attribute called "Class" to the Alcatel switch. The value of this attribute is set to either "student", "faculty", or "sysadmin" to identify the user's group. The Alcatel switch is configured to recognize this RADIUS attribute, and maps the wireless client to the appropriate role. Different firewall policies are configured for different groups on the Alcatel switch, primarily to limit student access to approved uses of the network.
- g The wireless laptop and Alcatel switch derive new encryption keys for WEP.
- h The wireless laptop maintains the same IP address.
- 5 The user now has network access consistent with the user's group privileges.
- 6. If the user moves to another room where the wireless association can no longer be maintained, the laptop will search for a new AP and re-initiate the association process. After each association, the 802.1x authentication process will repeat. While a user is logged in to the laptop, the 802.1x authentication will be performed using the user's credentials. If 802.1x



authentication takes place when a user is not logged in to the laptop, the computer's authentication credentials will be used to perform the authentication process.

7. When a user logs out of Windows, the laptop will again perform 802.1x authentication using computer credentials, as described in 2(b) above. This places the wireless device back into the "computer" role in the Alcatel switch.

### Printers

Separate to the process above, support for wireless-attached printers is also provided. The printers connect to the wireless network using a hidden ESSID of "Wireless LAN-01-printer". Because the wireless adapters for the printers do not support strong authentication or encryption, this ESSID utilizes WEP encryption with no authentication. For security reasons, printers are automatically mapped to a special "printer" role in the Alcatel switch, are placed into a special VLAN, and have restricted access to the network. In the event that the printer WEP key were compromised, the potential damage an attacker could do would be very limited, and the breach would be quickly discovered by the network administrator.

### **OmniAccess 6000 Switch Configuration**

The configuration of the OmniAccess 6000 switch is available through the Alcatel Command Line Interface (CLI) or through the graphical web-based Web UI management software. Either tool can be used to configure the system – both tools modify the same configuration file. This section will explain various pertinent sections of the configuration file and discuss their operational importance. Please refer to the *Alcatel AOS-W AOS-W Configuration Guide* for full documentation of the entire system.

### **Firewall Policies**

Several firewall policies have been configured in the Alcatel switch, and are mapped to user roles. These firewall policies are designed to control access only to the internal

network. The school district implements other firewall technology for the connection to the Internet to further limit district-wide Internet traffic.

#### **Firewall Destination Aliases**

To simplify configuration of firewall policies, an alias representing all internal network addresses has been defined. The actual IP addresses used by the school district have been changed here for security and privacy reasons. netdestination district-network network 10.0.0.0 255.0.0.0 network 172.16.0.0 255.255.0.0

### Student Policy

The policy below prevents students from using telnet, POP3, FTP, SMTP, SNMP, or SSH to the wired portion of the network. Telnet, FTP, SNMP, and SSH are used by the IT staff to maintain network devices, but are not permitted for other classes of users. POP3 and SMTP are permitted for faculty and staff members to access email. All students use Microsoft Exchange to access email.

```
ip access-list session student
user alias district-network svc-telnet deny
user alias district-network svc-pop3 deny
user alias district-network svc-ftp deny
user alias district-network svc-smtp deny
user alias district-network svc-snmp deny
user alias district-network svc-ssh deny
```

### Faculty Policy

The faculty policy is similar to the student policy above in restricting use of maintenance protocols to the internal network. However, faculty members are allowed the use of POP3 and SMTP. Faculty laptops have email clients configured to use these protocols as they were deemed more efficient than the Exchange protocol when laptops were taken home and used with VPN remote access. Students did not have this same requirement, since they are not permitted to use VPN remote access.

```
ip access-list session faculty
user alias district-network svc-telnet deny
user alias district-network svc-ftp deny
user alias district-network svc-snmp deny
user alias district-network svc-ssh deny
```

### Allow All Policy

The following policy allows unrestricted access to any network. This policy is used for members of the IT staff.

```
ip access-list session allowall
any any any permit
```



### **Printer Policy**

The following policy is used for the printer role. It restricts printers to communicating only with the print server, and only on specific port numbers. Any violation of the printer policy will trigger a log message, notifying the system administrator that a possible network security breach had occurred.

ip access-list session printer-acl user host 172.16.31.26 svc-windows-printing permit user host 172.16.31.27 svc-windows-printing permit any any any deny log

### **Guest Policy**

The following policies permit guest access only to the Internet, and only during daytime working hours.

```
time-range working-hours periodic
weekday 07:30 to 17:00
ip access-list session guest
user host 10.1.1.25 svc-dhcp permit time-range working-hours
user host 10.1.1.25 svc-dns permit time-range working-hours
user alias district-network any deny
user any svc-http permit time-range working-hours
user any svc-https permit time-range working-hours
user any any deny
```

### **User Role Configuration**

The following configuration establishes the user roles in the switch, and maps firewall policies to user roles. Additionally, guest traffic is limited to 1Mbps.

```
user-role printer
session-acl printer-acl
!
user-role student
session-acl student
session-acl allowall
!
user-role sysadmin
session-acl allowall
!
user-role faculty
session-acl faculty
session-acl allowall
!
```

```
user-role computer
session-acl allowall
!
user-role guest
session-acl guest
bandwidth-contract guest-1M
```

### **Authentication Parameters**

The following configuration statements are related to user authentication.

### **RADIUS** Configuration

The following statements configure the available RADIUS servers, including the IP address of the RADIUS server and the key.

```
aaa radius-server IAS1 host 10.1.1.21 key |*a^t%183923!
aaa radius-server IAS2 host 10.1.1.25 key |*a^t%312213!
```

#### **Role Derivation Rules**

The following statements determine how the switch maps wireless users into roles. The first statement instructs the switch to examine the "Class" RADIUS attribute returned from the authentication server, and to take the literal value of that attribute as the role name.

```
aaa derivation-rules server IAS set role condition Class value-of
```

The second statement instructs the switch to place any clients associating with the ESSID "Wireless LAN-01-printer" into the "printer" role. There is currently no authentication for printers – only the static WEP key and firewall policy protects the printer network from unauthorized users.

```
aaa derivation-rules user
set role condition essid equals "Wireless LAN-01-printer" set-
```

The third statement instructs the switch to place any clients associating with the ESSID "Guest" into the "guest" role. Guests are not required to authenticate, but are only permitted very limited network access and only during daytime working hours.

```
aaa derivation-rules user
set role condition essid equals "Guest" set-value guest
```

For more information on the role derivation process, refer to: "Setting Access Rights" on page 419.



### 802.1x Configuration

The following statements enable 802.1x authentication. It also establishes which RADIUS server to use for 802.1x authentication, and determines the default role that an 802.1x client will get in the absence of a "Class" attribute from the RADIUS server.

aaa dot1x mode enable aaa dot1x default-role student aaa dot1x auth-server IAS1 aaa dot1x auth-server IAS2

### Machine Authentication Enforcement

Because students do not always choose strong passwords, the school district wished to ensure that only authorized computers were allowed on the wireless network. This would prevent someone from bringing their own computer to the building and logging in through guessed or stolen credentials. The following statements enforce machine authentication before user authentication—if a user attempts to login without machine authentication first taking place, the user will be placed in the "guest" role and will have the same access rights as any other guest.

```
aaa dot1x enforce-machine-authentication
mode enable
machine-authentication default-role computer
user-authentication default-role quest
```

### VLAN and IP Address Configuration

The following statements set up VLANs, assign IP addresses to each VLAN, and establish a "helper-address" to which DHCP requests will be forwarded. Wireless clients will be assigned to either VLAN 60 or 61, and printers will be assigned to VLAN 62. The client's default gateway will be the Alcatel switch, which will route the traffic out to the 10.1.1.0 subnet. The VLANs are used to split up users into smaller IP subnets, improving performance by decreasing broadcast traffic. The VLANs are internal to the Alcatel switch only, and do not extend into other parts of the wired network. VLAN 63 is used for guest access.

```
vlan 60
vlan 61
vlan 62
vlan 63
!
interface vlan 1
ip address 10.1.1.251 255.255.255.0
```

```
1
interface vlan 60
ip address 10.1.60.1 255.255.255.0
ip helper-address 10.1.1.25
1
interface vlan 61
ip address 10.1.61.1 255.255.255.0
ip helper-address 10.1.1.25
interface vlan 62
ip address 10.1.62.1 255.255.255.0
ip helper-address 10.1.1.25
interface vlan 63
ip address 10.1.63.1 255.255.255.0
ip helper-address 10.1.1.25
ip default-gateway 10.1.1.254
```

### Wireless Configuration

The following statements set up the default AP parameters for the entire network. This establishes the encryption mode as dynamic TKIP (WPA) and the default ESSID as "Wireless LAN-01". In addition, a second ESSID called "Wireless LAN-01-printer" is established with the encryption mode set to static WEP, and the static WEP key is defined. The "Wireless LAN-01-printer" ESSID does not respond to broadcast probe requests, preventing clients from seeing it. Note that a hidden ESSID name is used for convenience and to reduce confusion among the users – not as a security mechanism. Simple attack tools are available that will quickly reveal a hidden ESSID name.

```
ap location 0.0.0
weptxkey 1
wepkey1 c4f32001f1c25ab20f838312f2
phy-type a
opmode dynamicWep
essid "Wireless LAN-01"
virtual-ap "Wireless LAN-01-printer" vlan-id 62 opmode
staticWep deny-bcast enable
virtual-ap "Guest" vlan-id 63 opmode opensystem deny-
bcast disable
phy-type g
opmode dynamicWep
essid "Wireless LAN-01"
virtual-ap "Wireless LAN-01-printer" vlan-id 62 opmode
```



```
staticWep deny-bcast enable
virtual-ap "Guest" vlan-id 63 opmode opensystem deny-
bcast disable
```

### **AP Configuration**

Users associating to each AP are mapped into a VLAN. For scalability purposes and to prevent broadcast issues caused by too many users on a single network, two different user VLANs have been set up. Membership in the VLAN is determined by the initial AP to which the user associates. As users roams between different APs, they will keep their original VLAN assignment regardless of which AP they are currently associated with. Currently, APs are mapped to VLANs based on the floor on which the AP has been deployed.

Guest users have an ESSID-specific VLAN configuration which overrides the default config below. Guest users will be mapped into VLAN 63.

```
ap location 1.1.0
vlan-id 60
!
ap location 1.2.0
vlan-id 61
```

# **Microsoft Active Directory Server Configuration**

The Active Directory database serves as the master authentication database for both the wired and wireless networks. The IAS authentication server bases all authentication decisions on information in the Active Directory database. The server is configured in a conventional fashion as a domain controller.

Wireless authentication depends on two specific parameters in Active Directory:

- 1. Remote access permission
- 2. Windows group membership configuration

### **Remote Access Permission**

Microsoft IAS is normally used as an authentication server for remote access (dialup or VPN) and thus looks to the Active Directory "Remote Access" property to determine whether authentication requests should be allowed or denied. This property is set on a per-user or per-computer basis. For a user or computer to be allowed access to the wireless network, the remote access property must be set to "Allow access".

### Windows Group Membership Configuration

The authentication policy configured in IAS depends on the group membership of the computer or user in Active Directory. These policies are responsible for passing group information back to the Alcatel switch for use in assigning computers or users to the correct role and thus determining their network access privileges. Only computers or users that are members of the following groups are allowed access to the wireless network:

- Domain Computers this group is used for all computers to authenticate to the network.
- Student this group is used for all student users
- Faculty this group is used for all faculty users
- Sysadmin this group is used for system administrators

### **Group Policy Configuration**

Windows 2003 Server contains support for Group Policy Objects to configure client wireless settings. Because there are a number of wireless settings that must be made on each client device, use of a GPO ensures that each client is correctly configured. The GPO push must be done from a wired network the first time, since a chicken-and-egg problem would result if wireless were used for network connectivity. To initiate a group policy update manually, issue the "gpupdate" command from the client computer.

Within the policy, several different settings are available. The information below appears on each client device as long as the domain policy has been updated.

#### Sets up general properties for the policy.

- Specifies that each client should check for policy updates every 60 minutes.
- Clients should only connect to Access Points. Clients should not connect to or form ad-hoc networks.
- Clients will use the built-in Wireless Zero Configuration service to configure wireless settings.
- Clients should not connect to non-preferred networks.

#### Sets up preferred ESSIDs that clients should connect to.

The only ESSID clients should connect to is "Wireless LAN-01".

#### Sets up general network properties for the ESSID.

The ESSID name is "Wireless LAN-01".



- The encryption type is WEP
- Open authentication should be used (this refers to 802.11 "basic" authentication, not to 802.1x)
- Each client will use a dynamically-generated WEP key that will be automatically derived during the 802.1x process.
- The network is not ad-hoc APs are required to be used.

#### Sets up 802.1x authentication parameters for the ESSID.

- Enables 802.1x
- Specifies that the client will initiate the 802.1x exchange (default)
- Establishes default timing parameters for 802.1x
- Specifies the EAP type as PEAP
- Clients will not attempt to authenticate as a guest
- Clients will perform computer authentication when a user is not logged in.
- After a user logs in, clients will re-authenticate to the wireless network

#### Sets up client PEAP properties

- Server certificate will be validated. This option instructs the client to check the validity of the server certificate from an expiration, identity, and trust perspective.
- The District-CA certificate authority is the only trusted CA that can issue server certificates for the wireless network.
- The PEAP "inner authentication" mechanism will be a password through MS-CHAP v2.
- Fast reconnect has not been enabled on the client. This option can speed up authentication in some cases.

#### Sets up the behavior of MS-CHAP v2 within PEAP.

The user's Windows logon information will be used for authentication to the wireless network. This option enables single sign-on, allowing the same logon to be used for access to the Windows domain as well as the wireless network.

# Microsoft Internet Authentication Server Configuration

Microsoft Internet Authentication Server (IAS) provides all authentication functions for the wireless network. IAS implements the RADIUS protocol, which is used between the Alcatel switch and the server. IAS uses Active Directory as the database for looking up computers, users, passwords, and group information.

### **RADIUS Client Configuration**

Each device in a network that needs to authenticate to a RADIUS server must be configured as a RADIUS client. In this case, the Alcatel switch must be configured as a RADIUS client.

For each RADIUS client configured, a shared secret must be configured. The shared secret is configured on the RADIUS server and client, and ensures that an unauthorized client cannot perform authentication against the RADIUS server

### **Policy Configuration**

The heart of IAS configuration is the policy configuration screen. From this screen, all policies related to wireless access can be defined – including time of day restrictions, session length, authentication type, and group-related policies. The essential policy settings for wireless access are described here - for detailed explanations of all IAS policy settings, please see Microsoft's official documentation.

### **Policy Matching Conditions**

When the IAS server receives a request for authentication, it compares the request with the list of remote access policies. The first policy to match the request will be executed, after which additional policies will not be searched. Each of the first four policies listed above corresponds to a group within the Active Directory database.

The policies above are designed to work by examining the username portion of the authentication request, searching the Active Directory database for a matching name, and then examining the group membership for a computer or user entry that matches. The following policy-group matches are made:

• The Wireless-Computers policy matches the "Domain Computers" group. This group contains the list of all computers that are members of the domain.



- The Wireless-Student policy matches the "Student" group.
- The Wireless-Faculty policy matches the "Faculty" group.
- The Wireless-Sysadmin policy matches the "Sysadmin" group.

In addition to matching the group, the policy also specifies that the request must be from an 802.11 wireless device. The policy above instructs IAS to grant remote access permission if all the conditions specified in the policy match, a valid username/password was supplied, and the user's or computer's remote access permission was set to "Allow".

By clicking **Edit Profile** in the policy screen above, additional authentication parameters can be selected. Two such parameters are of interest: the authentication method, which is common to all policies, and the advanced attributes, which are different for each policy.

#### Authentication Methods

To enable 802.1x authentication, an appropriate EAP type must be selected under the Authentication tab.

The only EAP method that should be selected is Protected EAP (PEAP). By click **Edit** in the screen above, additional properties for PEAP can be selected.

On this screen, a server certificate must be chosen, and the "inner" authentication method must be chosen. The list of available certificates is taken from the computer certificate store on which IAS is running. In this case, a self-signed certificate was generated by the local certificate authority and installed on the IAS machine. The local certificate authority has been added as a trusted certificate authority on each wireless client device, thus allowing this certificate to be trusted.

The authentication method shown here is MS-CHAP v2. Because password authentication is being used on this network, this is the only EAP authentication type that should be selected.

Fast reconnect can be enabled in this screen also. If fast reconnect is enabled here and also on client devices, additional time can be saved when multiple authentications take place (such as when clients are roaming between APs often) because the server will keep alive the PEAP encrypted tunnel. For this application, fast reconnect was not desired.

### Advanced Attributes

One of the principles in this network is that the Alcatel switch will restrict network access privileges based on the group membership of the computer or user. In order for this to work, the Alcatel switch must be told to which group the user belongs. This is accomplished using RADIUS attributes. To configure these attributes, select the Advanced tab from the policy profile.

An attribute called "Class" has been added here. The Alcatel switch has been configured to interpret the "Class" attribute and use it to determine group membership. The example above is for the "Wireless-Computers" policy, and upon successful completion will return the "Class" attribute to the Alcatel switch containing the value "computer".

The "Wireless-Student" policy for example will return a RADIUS attribute called "Class" containing the value "student" upon successful completion.

# Microsoft Windows XP Client Configuration

Client configuration should be automatic through group policy updates described above. However, client configuration can also be done manually through Windows XP's built-in "Wireless Zero Configuration" service.

Windows will connect to preferred networks in the order in which they appear in this list.

By clicking "Advanced", the "Networks to access" screen is displayed. This screen determines what types of wireless networks can be accessed. By default, Windows will connect to any type of wireless network. In the configuration at the left, Windows has been configured to connect only with Access Points.

#### Sets up general network properties for the ESSID.

- The ESSID name is "Wireless LAN-01".
- Open authentication should be used.
- The encryption type is WEP
- Each client will use a dynamically-generated WEP key that will be automatically derived during the 802.1x process.
- The network is not ad-hoc APs are required to be used.

#### Sets up 802.1x authentication parameters for the ESSID.

Enables 802.1x



- Specifies the EAP type as PEAP
- Clients will not attempt to authenticate as a guest
- Clients will perform computer authentication when a user is not logged in.

#### Sets up client PEAP properties

- Server certificate will be validated. This option instructs the client to check the validity of the server certificate from an expiration, identity, and trust perspective.
- The District-CA certificate authority is the only trusted CA that can issue server certificates for the wireless network.
- The PEAP "inner authentication" mechanism will be a password through MS-CHAP v2.
- Fast reconnect has not been enabled on the client. This option can speed up authentication in some cases.

#### Sets up the behavior of MS-CHAP v2 within PEAP.

• The user's Windows logon information will be used for authentication to the wireless network. This option enables single sign-on, allowing the same logon to be used for access to the Windows domain as well as the wireless network.

## Microsoft PocketPC 2003 Client Configuration

PocketPC 2003 includes built-in support for wireless networks and 802.1x authentication. Some PDA vendors, including HP, have also produced system updates to enable support for WPA and TKIP, assuming the NIC driver also supports TKIP. This deployment uses dynamically-generated WEP keys, but has a future upgrade path to WPA/TKIP.

### **Export Trusted Certification Authority**

The first step in enabling 802.1x authentication on PocketPC devices is to install a trusted certification authority, if required. If the RADIUS server uses a certificate with a certification path already trusted by the PocketPC devices, then this step is not necessary. Certificates purchased from large certificate authorities such as Verisign, for example, will already be trusted by the clients. If a self-signed certificate is used, the certificate for the root certificate authority into a standard X.509 file format. This step can be accomplished on any Windows computer where the trusted certification path has already been installed. Launch the Microsoft Management Console by selecting **Start > Run**, and entering "mmc" in the box.

In the management console, select **File > Add/Remove Snap-in**. Select the Certificates snap-in.

Typically, a trusted certificate authority certificate can be found in both the user certificate store and the computer certificate store. When prompted to select the certificate snap-in, choose "My user account".

Next, locate the certificate for the trusted certificate authority, right-click on it, select "All tasks", then select "Export".

When prompted, export the key as a DER-encoded binary X.509 file.

If given the option, do not export the private key. This option only appears on the certificate authority itself. Save the file somewhere accessible on the hard drive.

### **Install Certificate Authority**

The next step of the process is to copy the previously generated X.509 certificate to the PocketPC client device. To do this, place the X.509 certificate on a machine running ActiveSync that has a partnership arrangement with a PocketPC device. The PocketPC device's filesystem should appear under Windows Explorer, and a folder entitled "<mobile device name> My Documents" should appear on the Windows desktop. Copy the X.509 certificate file from the host computer to the "My Documents" directory on the PocketPC device.

Next, install the certification authority in the PocketPC device's certificate store. To do this, run the PocketPC File Explorer and navigate to "My Documents".

To install the certificate authority, simply tap on the certificate file. The system will ask for confirmation before installing the certificate. Select "Yes".

The certification path has now been installed. It can be verified by navigating on the PocketPC device to **Settings > System > Certificates > Root**.

### **Configure Wireless Settings**

The next step will be to configure wireless settings. If required, install the appropriate NIC card and drivers. Ensure that the drivers are specific to PocketPC 2003 – earlier versions of PocketPC and Windows CE did not contain native support for wireless.

Configure wireless settings by navigating to **Settings > Connections > Connections > Advanced > Network Card > Wireless**.



If the appropriate ESSID is not already shown in the list, add it by selecting "Add new".

After filling in the ESSID in the "Network Name" field, tap the "Authentication" tab. The authentication settings screen appears.

Configure the screen. In the EAP type field, select PEAP. Do not click **Properties** – this is used to configure certificate-based authentication. A warning message will be generated if **Properties** is clicked – this warning message may be ignored.

**NOTE**—Maintain the battery on PDA at operating levels. Should you allow the battery to run low, your configuration may become corrupted. If this happens, delete the configured ESSID. Create the exact same ESSID as you just deleted. Then enable PEAP for this configuration.

### Login to Wireless Network

Once the wireless network has been configured, the PocketPC device will associate with an Access Point and begin 802.1x authentication. Once this has begun, the user will be prompted for a username and password.

Supply the necessary login credentials, and the process will complete.

### Microsoft Requirement

For 802.1x, Microsoft requires that you specify the subject Alt Name.

# CHAPTER 12 Switch Management Configuration

This Chapter discusses how to use the various management features of Alcatel Switches using the AOS-W Web UI software and the command line interface (CLI).

The management feature in Web UI are available on the **Configuration > Management** pages. Those features include:

- SNMP
- Access Control
- Logging

### **SNMP Configuration Using Web UI**

#### Entering SNMP system information

Standard SNMP system information may be recorded for your Alcatel switch. Standard SNMP information includes:

- System Name System Name is an alpha-numeric string with a maximum length of 32 characters.
- System Contact System Contact is an alpha-numeric string with a maximum length of 32 characters.
- System Location System location is an alpha-numeric string with a maximum length of 128 characters.
- Read Community String
   Kead Community Strings are alpha-numeric strings with a maximum length of 16 characters. You may enter an unlimited number of strings.

1 Navigate to the **Configuration > Management > SNMP** page. Add system information in the System Group section of the SNMP page.

Management > S	NMP
SNMP Access Cont	rol Logging
System Group	
Host Name	
System Contact	
System Location	Aruba Networks
Read Community Strings	Add
Enable Trap Generation	
Trap Receivers	
IP Address SNMP Version	on Community String UDP Port Action
SNMPV3 Users	
User Authentication Pr	otocol Privacy Protocol Action
Add	
	Apply

- 2 Type a user friendly name in the System Name field.
- 3 Type a name or system administrator contact information in the System Contact field.
- **4** Type the location of the Alcatel switch in the System Location field.

**Configuring Trap Receivers** 

Navigate to Configuration > Management > SNMP page. (Additional SNMP configuration settings are set on the Configuration > Network > General page.

Click **Add** in the Trap Receivers section of the SNMP page.

Trap Receivers							
IP Address	SNMP Version	Community String	UDP Port	Action			
Add							

The Add Host page appears on the screen.

Co	nfiguration				123
Monitoring Configuration	n Maintenance Pla	n Events Reports		Save Configuration	Logout
Switch	Management	> SNMP Configu	ration > Trap Receivers	> Add	« Back
Management	Host		-		
WLAN					
Network	IP Address				
Radio	Version	SNMPv1 -			
Advanced					
RF Spectrum Mgmt	SNMP Community String				
Calibration	UDP Port				
Optimization		Apply			
Protection					

- 3 Enter the IP address of the SNMP server host in the IP Address field.
- 4 Chose the appropriate SNMP version from the Version pull-down menu.
- 5 Enter a valid SNMP Community String in the SNMP community String field.
- 6 Enter the UDP port for the trap in the UDP Port field.

### **SNMP** Configuration Using The CLI

SNMP configuration commands must be executed from the config prompt in the privileged mode.

# Entering SNMP system information

Use the following CLI commands to configure and store SNMP system information.

**1** Create a system name entry using the hostname *<name>* command.



2

**NOTE**—The console will revert to the immediate (non-privileged mode) when you change the system name. You will need to re-execute the enable and configure terminal commands before you can proceed.

2 Create a System Contact entry using the syscontact <name> command.

```
(UrsaMinor) (config) #syscontact AniceGuy
(UrsaMinor) (config) #
```

3 Create a System Location entry using the systemation *<location* > command.

```
(UrsaMinor) (config) #syslocation Server_Room
(UrsaMinor) (config) #
```

4 Create a Read Community String entry using

```
(UrsaMinor) (config) #snmp-server community Security
(UrsaMinor) (config) #
```

#### **Configuring Trap Receivers**

**1** Define a SNMP Trap Receiver using the snmp-server host <*IPaddr*> version <*l* | 2*c* | 3> <*CommunityString*> command.

```
(UrsaMinor) (config) #snmp-server host 191.168.1.1 version 2c security (UrsaMinor) (config) #
```

### Configuring SNMPv3 Users

To configure SNMP version 3 users, navigate to **Configuration > Management SNMP Configuration**.

User Authentication Pro	tocol Privacy Protocol	Action
user1 md5	DES	Delete
Muu		
User Name		
Authentication Protocol	×	
Authentication Protocol Passwo	ord	
Privacy Protocol	*	
Privacy Protocol Password		
	Add Cancel	

### **Configuring Administrative Access Using Web UI**

AOS-W allows different levels of access for administrative users based on assigned roles.



Manag	jeme	ent > Acc	ess Control		
SNMP	Ac	cess Control	Logging		
Manage	ment U	sers			
Name	Role	Action			
admin i	root	Edit Delete			
Add					
Manage	ment R	oles			
Name	Act	ion			
root	Edit	Delete			
Add					
A		<b>.</b>			_
Authen	tication	1 Servers			
Name	Туре	IP Address	Authentication Port	Status	Actions
Add					

Navigate to the **Configuration > Management > Access Control** page.

You can view, add, delete, or edit Management Users and Roles from this page.

### Adding and Editing Management Users

Adding and editing users is accomplished in the Management Users section of the page

Con	figuration		
Monitoring Configuration	Maintenance Plan Events Reports	Save Configuration	Logout
Switch	Management > Access Control		
Management			
WLAN	SNMP Access Control Logging		
Network	Management Users		
Radio	Name Role Action		
Advanced	admin root Edit Delete		
RF Spectrum Mgmt	administrator root Edit Delete		
Calibration	rale rest Edit Delete		
Optimization			
Protection	sean root Edit Delete		
Monitoring	Add		
Security			
Roles			
Policies	Management Roles		
AAA Servers	Name Action		
Authentication Methods	guest Edit Delete		
VPN Settings	root Edit Delete		
Advanced	Add		
WLAN Intrusion Detection			
Rogue AP			

Add a Management user by clicking on **Add** in the Management Users portion of the Access Control page. The **Add User** page appears.

- 1 Enter a name in the User Name field. The name you enter must be 1 16 alpha-numeric characters in length.
- 2 Enter a password in the Password field. The password you enter must be 1 16 alpha-numeric characters in length.
- **3** Retype the password in the Confirm Password field.
- 4 Choose a role from the Role pull-down menu.
- 5 Click **Add Role** to apply the selected role to the user.
- 6 Click **Apply** to activate the new entries.
- 7 Click on **Save Configuration** near the top of the page to save the changes to the configuration file.



### Adding and Editing Management Roles

Add or edit Management Role by clicking **Add** in the Management Roles section of the Access Control page. The Add Role page appears.

	Conf	iguration	5000				20		
Monitoring Co	nfiguration	Maintenance	Plan	Events	Reports			Save Configuration	Logout
Switch		Access Con	trol	> Add F	Role				« Back
Management			_						
WLAN		Role Name							
Network		Modules							
Radio		Management Me	odule	Access Pe	rmissions	Action			
Advanced						Add			
RF Spectrum Mgi Calibration	mt					Apply			

#### 1 Click **Add**, the Add Module page appears.

Configuration								
Monitoring Configuration	Maintenance Plan Events Reports	Save Configuration	Logout					
Switch	Access Control > Roles > Add Role > Add Module		« Back					
Management WLAN Network Radio	Management-Module     Access Permissions       am     read       Add							

- 2 Select a Management Module using the pull-down menu.
- 3 Select an Access Permission using the pull-down menu.
- 4 Click **Add**, the Add Role page is again displayed and shows the added module and permission.
- 5 Click the Apply button to activate the new entries.
- 6 Click the Save Configuration button near the top of the page to save the changes to the configuration file.

**Note**—The Web GUI includes a View only Role. When a role is made view-only, all module permission information is ignored.

# Adding and Changing Administrative Access Using the CLI

Viewing Management Users

You may view currently configured management users and their assigned roles by executing the show mgmt-users command from the CLI.

### Adding and Editing Management Users

Add a management user and assign a role with the mgmt-user <username> <role> command in CLI.

```
(Alcatel) (config) #mgmt-user test_manager temp_mgr
passwd:*****
Re-Type passwd:*****
(Alcatel) (config) #
```



### Viewing Management Roles

You may view currently configured management roles and their assigned roles by executing the show mgmt-roles command from the CLI.

# Adding and Editing Management Roles

Add or edit management roles in the CLI by executing the mgmt-role *<rolename>* command. Executing the mgmt-role command will place the console in the mgmt-role sub-mode.

```
(Alcatel) (config) #mgmt-role foo_test
(Alcatel) (mgmt-role)#?
```

Add a permission to the role using the permit <moduleID> command.

```
(Alcatel) (mgmt-role)#permit am read write
(Alcatel) (mgmt-role)#
```
# **Adding Auth Servers**



# Logging

The logging feature in Alcatel AOS-W allows permanent system logs to be stored externally on one or more logging servers.



# **Configuring Logging Using Web UI**

Begin configuring logging servers by navigating to the **Configuration > Management > Logging** page.

Con	liguration			
Monitoring Configuration	Maintenance Plan	Events Repor	ts	Save Configuration L
Switch	Management >	ogging		
Management	Management >	ogging		
WLAN	SNMP Access Cor	ntrol Logging		
Network	Logging Servers			
Radio	No Server Addresses C			
Advanced	Add			
RF Spectrum Mgmt	Logging Levels			
Optimization	Module	Logging Level		
Protection	Management AAA	informational		
Monitoring		informational		
Security				
Roles	Configuration Manager	r informational		
Policies	VPN Server	informational		
AAA Servers	DHCP Server	informational		
VPN Settings	Switching	informational		
Advanced	Mobility	informational		
WLAN Intrusion Detection	User User	informational		
Rogue AP Desial of Service	Access Point Manager	informational		
Man-In-the-Middle	Station Manager	informational		
Signatures	Traffic	informational		
Policies	RE Director	informational		
	Apply			
	Commands		View Co	ommands

Add a logging server by clicking **Add**.

	Cor	nfiguration	
Monitoring Configu	uration	Maintenance Plan Events Reports Save Configuration Logou	t
Switch		Management >Logging	
Management			
WLAN		SNMP Access Control Logging	
Network		Logging Servers	
Radio		No Server Addresses d	
Advanced			
RF Spectrum Mgmt		172.16.1.254 Add Cancel	
- 14 - 14		Logging Lovelo	

An additional text field appears.

Enter the address of a logging server and click the Add button next to the text field.

Select a check box of a module for which you want to do logging. The logging level menu appears.



Select the appropriate logging level and click on the apply button.

There are a total of eight logging levels, each having it's own distinct characteristics:

- Emergency Panic conditions that occur when the system becomes unstable.
- Alert Any condition requiring immediate attention and correction.
- Critical Any critical conditions such as, hard drive errors.
- Errors Error conditions
- Warning Warning messages.
- Notice Significant events of a non-critical and normal nature.
- Informational Messages of general interest to system users.
- Debug Messages containing information useful for debugging purposes.

#### Hierarchy of Logging Levels

When logging levels are set for any module, that level and messages with higher logging levels appears in the logs. The list of logging levels above are shown in hierarchal order.



# **Configuring Logging Using The CLI**

#### Adding A Logging Server

Add a logging server using the logging <IPAddress> command from the CLI.

```
(Alcatel) (config) #logging 192.168.25.25
(Alcatel) (config) #
```

#### Setting Logging Levels

Set a logging level using the logging level <*level>* <*module>* command from the CLI.

```
(Alcatel) (config) #logging level alert aaa
(Alcatel) (config) #
```

#### Viewing Current Logging Levels

View the current logging levels using the show logging level command from the CLI.

(Alcatel)	(config) #show logging level	
LOGGING LE'	VELS	
Applicatio	n Level	
authmgr	informational	
crypto	informational	
l2tp	informational	
pptp	informational	
wms	informational	
mmgr	informational	
mobagent	informational	
master	informational	
stm	informational	
localdb	informational	
sapm	informational	
fpapps	informational	
cfgm	informational	
suser	informational	
intuser	informational	
aaa	informational	
traffic	informational	
dhcpd	informational	
processes	informational	
publisher	informational	
(Alcatel)	(config) #	



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 13 Wireless LAN Configuration

This chapter discussed how to configure all the standard 802.11 features of an Alcatel Wireless LAN switch. The features discussed in this chapter are:

- SSID
- Radio Parameters
- Encryption
- AP Parameters

# Wireless LAN Configuration

This Wireless LAN configuration chapter explains setup and configuration of all standard 802.11 settings, including SSID, radio parameters, and encryption. This guide also explains how to configure system-wide parameters, per-building AP parameters, per-floor AP parameters, and per-AP parameters.

# Wireless LAN Network (SSID) Configuration

Before wireless users can gain access to the network, they must associate to an access point using a particular ESSID. AOS-W supports up to 16 ESSIDs – 8 each for 802.11a and 802.11b/g. In the Alcatel Access Point, each ESSID uses a separate BSSID (MAC address) for 802.11b/g radios, while all ESSIDs share the same BSSID (MAC address) for 802.11a radios. To view, add, and modify SSIDs, navigate to **Configuration > Wireless LAN > Network**, as shown in the figure below.

WLAN > Network > SSID							
SSID	General						
SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Period	Actions		
ар	802.11a/b/g	Default	No Encryption	1	Edit		
Add							

#### FIGURE 13-1 SSID Configuration

The first SSID configured is primary and can be edited, but cannot be deleted. Other SSIDs can be edited or deleted.

**NOTE**—Note: These parameters affect all APs in the network, unless a more specific configuration applies. Configuration in this section corresponds to the CLI configuration for "ap location 0.0.0".

#### Adding a New SSID

To add a new SSID, click the Add button. The figure below will be displayed.

WLAN > Networl	Add SSID				
Add SSID					
SSID					
Radio Type	802.11 a 💌				
Hide SSID		Encryption Type	• NULL C WEP	C TKIP C AES-CCM C Mixed TKIP/AES-CCM	
SSID Default VLAN	0 < None 💌	Encryption Type 1002 112			
Ignore Broadcast Probe Reque	st 🗂				
DTIM Period	1				
Commands			View Commands		
				Apply	

FIGURE 13-2 Add SSID

Available parameters are:

**SSID** – Fill in the name of the ESSID. Clients will use this ESSID to associate to the correct network.

**Radio Type –** SSIDs may appear on only 802.11a radios, only 802.11b/g radios or on both types of radios.

**SSID Default VLAN –** If desired, a given SSID may be mapped to a particular VLAN. See the "VLAN Mapping" section below for more details.

**Ignore Broadcast Probe-Request** – When a client sends a broadcast probe-request frame to search for all available SSIDs, controls whether or not the system will respond for this SSID. When enabled, no response will be sent – clients will have to know the SSID in order to associate. When disabled, a probe-response frame will be sent for this SSID.

**NOTE**—When using multiple SSIDs on Alcatel Access Points, the 802.11a radio may respond with multiple probe responses using the same BSSID (MAC address). Some clients will report only a single ESSID per BSSID and may not be able to associate. If this problem occurs, enable this option to suppress responses to broadcast probe requests.

**Encryption Type** – Specify open, WEP, TKIP, AES-CCM, or Mixed TKIP/AES-CCM. See below for discussion on each type.

#### VLAN Mapping

AOS-W supports a concept known as "crypto-VLANs" whereby clients may access the same network using different encryption types. Good security practices require that different L2 encryption types be mapped to different L2 subnets – otherwise, broadcast and multicast frames from a less secure encryption such as static WEP may lead to the compromise of a more secure encryption type such as TKIP. When using multiple encryption types on separate SSIDs, make sure that each SSID is mapped to a different VLAN inside the Alcatel switch.

SSID-based VLAN mapping may also be used for separation of traffic. For example, traffic from a guest SSID may be mapped to a guest VLAN, while traffic from employee SSIDs may be mapped to an internal network.

#### WEP Encryption

Two types of WEP encryption are available: static WEP and dynamic WEP. When static WEP is used, one WEP key will be configured for the SSID. All users on the network must use the same key, and no key rotation is possible. Static WEP is generally considered to provide less-than-ideal security and should be supplemented with Alcatel's built-in firewall protection when used.

Dynamic WEP (used with 802.1x) provides somewhat better protection, particularly when combined with AOS-W Wireless Intrusion Detection features. When using dynamic WEP, the authentication server provides an individual encryption key to each client at the time of 802.1x authentication.



The 802.1x framework also allows the encryption key to be rotated at specific intervals. By allowing each user to have a different key, and by allowing key rotation, dynamic WEP provides a much better level of security than static WEP.

Dynamic WEP (used with 802.1x) provides somewhat better protection, particularly when combined with AOS-W Wireless Intrusion Detection features. When using dynamic WEP, the authentication server provides an individual encryption key to each client at the time of 802.1x authentication. The 802.1x framework also allows the encryption key to be rotated at specific intervals. By allowing each user to have a different key, and by allowing key rotation, dynamic WEP provides a much better level of security than static WEP.

**NOTE**—802.1x authentication is required when using dynamic WEP. Clients using dynamic WEP will not be able to access the network until 802.1x configuration is also completed.

To configure WEP encryption, click on the WEP radio button in the Add SSID screen as shown in the figure below.

SSID		NewSSID	]	
Radio T	уре	802.11 a/b/g 💌		CNULL <sup>©</sup> WEP C TKIP
SSID D	efault VLAN	0 < 1 -	Encryption Type	WEP
Allow S	SID Broadcast to Asso	ociate		Static WEP Dynamic WEP
WEP K	eys			
S. No	Use as Tx Key	WEP Key	Size	
1	$\odot$	*****	*** 26 Hex	•
2	0		26 Hex	•
3	0		26 Hex	•
4	0		26 Hex	•
	Enter 40-bit WEP key	/s as 10 hexadecimal digits(0-9.a-f,	, or A-F)	
	Enter 128-bit WEP ke	eys as 26 hexadecimal digits(0-9.a-	f, or A-F)	

#### FIGURE 13-3 WEP Configuration

If static WEP is selected, fill in one or more keys. WEP keys must be entered in hex, and must be either 10 characters (for 64-bit WEP) or 26 characters (for 128-bit WEP). If dynamic WEP is selected, no keys need to be configured. Both static WEP and dynamic WEP may be enabled at the same time. The equivalent CLI configuration to add the SSID shown above is:

ap location 0.0.0 phy-type a virtual-ap "NewSSID" vlan-id 0 opmode staticWep,dynamicWep deny-bcast enable ap location 0.0.0 phy-type g virtual-ap "NewSSID" vlan-id 0 opmode staticWep,dynamicWep deny-bcast enable

#### WPA, TKIP, and AES Encryption

TKIP (Temporal Key Integrity Protocol) is a replacement for WEP, and along with 802.1x forms the basis for WPA (Wi-Fi Protected Access). TKIP provides a number of advantages over WEP, including per-frame key rotation, a longer initialization vector, and a cryptographically-secure message integrity check. TKIP may be configured in two different ways: Pre-Shared Key (PSK) or WPA. PSK TKIP is designed for very small networks that do not contain an authentication server and cannot use 802.1x. In PSK TKIP, a pre-shared key is used by all clients in the network to establish initial communication. Once an initial exchange has taken place, standard TKIP key rotation begins so that each client uses a different key.

WPA TKIP requires the use of 802.1x for authentication and, similar to dynamic WEP, provides a mechanism for the authentication server to assign a unique encryption key to each client. WPA TKIP provides the best available L2 encryption available today.

To enable TKIP, select the appropriate radio button as shown in the figure below.



	Confi	guration	1			00	
Monitoring C	onfiguration	Maintenance Plan	Eve	nts Reports			
Switch		WLAN > Netwo	rk >	Edit SSID			
Management							
WLAN		Edit SSID					
Network		SSID		VAP001-10.3.17.75	]		
Radio		Radio Type		802.11 a/b/g 🗸		CNUL	CWED @ TVID
Advanced		Hide SSTD			Fearmelies Ture	TKID	
RF Managemen	nt				Encryption type	G DEV TV	
Calibration		SSID Default VLAN		64 < None 💙		IN PSK IK	
Optimization		Ignore Broadcast Probe Re	quest	$\checkmark$			
Protection		DTIM Period		1	1		
Monitoring					-		
Advanced		Apply Globally (Always	applied	(globally)			
Security		PSK TKIP Key/Passobrase			Format PSK Pass	enhrase 🔽	
Policies		The DSK TKID I	lav Kas	, chould be a 64 character b	evadecimal string	priidse 💌	
000 Servers		The PSK TKIP Passo	hrase s	bould be an ASCII string 8-i	63 characters in lend	nth	
Authentication I	Methoda			in the second		<b>J</b>	
VDN Settings	nourous						
Firewall Setting	-	Commands				View Comn	hands
Secure Access	2						
Secure Service	Toterfaces					Apply	
Adupped	Inconaces						

FIGURE 13-4 TKIP Configuration

If PSK TKIP is selected, fill in the pre-shared key. To enter the key directly in hex, enter 64 hex characters. To enter the key as a passphrase, select "PSK Passphrase" from the drop-down menu and enter a passphrase between 8 and 63 characters in the box on the left. When configuring clients, enter the same key or passphrase.

If WPA TKIP is selected, no further configuration is required. All key generation will be done by the authentication server.

**NOTE**—802.1x authentication is required when using WPA TKIP. Clients using WPA TKIP will not be able to access the network until 802.1x configuration is also completed.

The equivalent CLI configuration to add the SSID shown above is:

ap location 0.0.0 phy-type a virtual-ap "NewSSID" vlan-id 0 opmode staticTkip deny-bcast enable ap location 0.0.0 phy-type g virtual-ap "NewSSID" vlan-id 0 opmode staticTkip deny-bcast enable ap location 0.0.0 wpa-hexkey abc123abc123abcdefabcdef12345678abc123abc123abcdefabcdef12345678 **NOTE**—AOS-W versions 2.4.0.0 and later support different staticWep and staticTkip keys per SSID. In earliers releases, the staticWep and staticTkip keys applied to each Access Point.

WEAN > NECOUR	- Add 331D					
Add SSID						
SSID			C NULL C	C WEP C TKIP @ AES-CCM C Mixed TKIP/AES-CCM		
Radio Type	802.11 a 💌					
Hide SSID		Encryption Type	WPA2			
SSID Default VLAN	0 < None 🗸		PSK AES	PSK AES-CCM ○ WPA2 AES-CCM		
Ignore Broadcast Probe Reque	st 🔽		Enable P	Enable Pre-authentication		
DTIM Period	1	]				
Apply Globally						
PSK AES Key/Passphrase		Format PSK Pass	phrase 💌			
The P5K AES Hex	Key should be a 64 character h	exadecimal string				
The PSK AES Passphras	e should be an ASCII string 8-	63 characters in lenç	gth			
Commands			View Comma	mands		
				Apply		

FIGURE 13-5 AES-CCM Configuration

WLAN > Netwo	rk > Add SSID			1	« Back
Add SSID					
SSID			CINIT		
Radio Type	802.11 a 💌		HOLL		
Hide SSID		Encryption Type	Mixed TK	KIP/AES-CCM	
SSID Default VLAN	0 < None 🗸		PSK TK	PSK TKIP/AES-CCM C WPA/2 TKIP/AES-CCM	
Ignore Broadcast Probe Rei	quest $ agric land land land land land land land land$		Enable	e Pre-authentication	
DTIM Period	1				
Apply Globally					
P5K AES Key/Passphrase	•••••	Format PSK Pass	phrase 🔽		
The PSK AES H	ex Key should be a 64 character h	exadecimal string			
The PSK AES Passph	rase should be an ASCII string 8-	63 characters in lenç	jth		
Commands			View Comn	mands	
				Apply	

FIGURE 13-6 Mixed TKIP and AES-CCM Configuration

# **Adjusting Radio Parameters**

To view and edit default radio parameters for all APs, navigate to **Configuration** > **Wireless LAN** > **Radio** as shown in the figure below. Radio parameters for both 802.11b/g radios and 802.11a radios are available by selecting the appropriate tab.



RTS Threshold (bytes)	2333	Ageout (secs)	1000
Hide SSID		Deny Broadcast	C Enable 🖲 Disable
Max Retries	4	DTIM Period	1
Max Clients	5	Beacon Period (ms)	100
Initial Radio State	€ Up C Down	Mode	Access Point C Air Monito
Default Channel	1 💌	Initial Transmit Power	14 dBm(25.119 mW) 💌
Short Preamble	<b>v</b>		
Basic Rates (Mbps)		Г9 Г11 Г12 Г18	3 🗖 24 🗖 36 🗖 48 🗖 54
Supported Rates (Mbps)	<b>▼</b> 1 <b>▼</b> 2 <b>▼</b> 5 <b>▼</b> 6	▼ 9 ▼ 11 ▼ 12 ▼ 18	3 🔽 24 🔽 36 🔽 48 🔽 54
ARM Assignment	Disabled 🔽	ARM Client Aware	
ARM Scanning	Г	ARM Scan Time (msecs)	110
ARM Scan Interval (secs)	10	1	

FIGURE 13-7 802.11b and g Radio Parameters

RTS Threshold (bytes)	2333	Ageout (secs)	1000
Hide SSID		Deny Broadcast	C Enable 🤄 Disable
Max Retries	4	DTIM Period	1
Max Clients	5	Beacon Period (ms)	100
Initial Radio State		Mode	Access Point C Air Monito
Default Channel	52 💌	Initial Transmit Power	12 dBm(15.849 mW) 💌
Basic Rates (Mbps)	<b>₽</b> 6 <b>□</b> 9 <b>₽</b> 12 <b>□</b> 18	₩ 24 1 36 1 48 1	54
Supported Rates (Mbps)	<b>▼</b> 6 <b>▼</b> 9 <b>▼</b> 12 <b>▼</b> 18	▼ 24 ▼ 36 ▼ 48 I	₹ 54
ARM Assignment	Disabled 💌	ARM Client Aware	<b>v</b>
ARM Scanning	Г	ARM Scan Time (msecs)	110
ARM Scan Interval (secs)	10		

FIGURE 13-8 802.11a Radio Parameters

**NOTE**—Note: These parameters affect all APs in the network, unless a more specific configuration applies. Configuration in this section corresponds to the CLI configuration for "ap location 0.0.0".

Available parameters are:

**RTS Threshold** – Wireless clients transmitting frames larger than this threshold will issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting. An Alcatel network normally consists of a larger number of APs with a smaller footprint, reducing the likelihood of this "hidden node" problem. The default is 2333 bytes.

**Ageout -** Specifies the amount of time a client is allowed to remain idle before being aged out. The default is 1000 seconds.

**Hide SSID –** Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.

**Deny Broadcast** – When a client sends a broadcast probe-request frame to search for all available SSIDs, this option controls whether or not the system will respond for this SSID. When enabled, no response will be sent – clients will have to know the SSID in order to associate. When disabled, a probe-response frame will be sent for this SSID.

**Max Retries –** Specifies the maximum number of retries allowed for the AP to send a frame. The recommended range is between 3 and 7. The default is 3.

**DTIM Period** – Specifies the interval between sending DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to received broadcasts. The default is 2.

**Max Clients** – Specifies the maximum number of wireless clients for a radio on an AP. The default is 0, but is set to 64 if the initial setup dialog is used to configure the switch.

**Beacon Period –** Specifies the time between successive beacons being transmitted. The default is 100 ms.

Initial Radio State - Used to enable or disable the radio.

**Mode –** Specifies whether the AP should act as an access point or an air monitor. The default is AP.



**Default Channel** – Sets the default channel on which the AP will operate, unless a better choice is available – either from calibration or from RF Plan.

**Initial Transmit Power** - Sets the initial transmit power on which the AP will operate, unless a better choice is available – either from calibration or from RF Plan.

**LMS IP** – Specifies the Local Management Switch that the AP will use in multi-switch networks. The LMS is responsible for terminating user traffic from the APs, processing it, and forwarding it to the wired network. Setting the option in this screen will set an LMS for the entire network, which is probably not desirable.

When using redundant switches as the LMS, set this parameter to be the VRRP IP address. This will ensure that APs always have an active IP address with which to terminate sessions.

**Short Preamble –** Enables or disables short preamble for 802.11b/g radios. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Network performance is higher when short preamble is enabled. Legacy client devices that use only long preamble can generally be updated to support short preamble. The default is enabled.

**Basic Rates** – Specifies the a list of supported rates that will be advertised in beacon frames and probe responses.

**Supported Rates –** Specifies the set of rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.

The default CLI configuration for ap location 0.0.0 is:

(Alcatel6000)	config) # <b>ap location 0.0.0</b>	
(Alcatel6000)	<pre>sap-config location 0.0.0) #?</pre>	
ageout	Seconds of inactivity after which client is ag out	jed
ap-enable	One of enable or disable	
ap-logging	Set logging levels for AP facilities	
arm	Adaptive Radio Management configuration	
authalgo	Only opensystem is supported. No support for sharedkey	
beacon-period	Beacon Period for the AP. Typically 100	
bkplms-ip	The IP addr of the backup LMS for APs at this location	
bootstrap-thres	hold Number of heartbeat misses before AP re-bootstraps	

deny	Deny wireless access according to timerange argument
deny-bcast	enable to suppress responses to probe requests with broadcast SSID
disable	disable this feature or mode
dns-name	DNS Name for the AP. Can contain a \$L substring that is replaced with the location of the AP
double-encrypt	Encrypt 802.11 data frames using IPSec
dtim-period	Interval between sending DTIMs in beacon
dump-server	Core dump server (for debugging)
enable	enable this feature or mode
essid	ESSID for the AP. Should be a string of max. 32 characters
hide-ssid	enable or disable hiding the SSID in beacons
hostname	Change the system name
lms-ip	The IP addr of the LMS that should be assigned to APs
	at this location
local-probe-response	The AP (not the switch) generates probe response
max-clients	Max wireless chients for AP. U thru 256
max-retries	a packet
max-tx-fail	Maximum transmit failures before client gives up
mode	One of am_mode or ap_mode (air monitor or access point)
mode mtu	One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes)
mode mtu no	One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command
mode mtu no opmode	One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of
mode mtu no opmode	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk</pre>
mode mtu no opmode phy-type	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1</pre>
mode mtu no opmode phy-type power-mgmt	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management</pre>
<pre>mode mtu no opmode phy-type power-mgmt radio-off-threshold</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off</pre>
<pre>mode mtu no opmode phy-type power-mgmt radio-off-threshold restore-default</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem, staticWep, dynamicWep, staticTkip, dy namicTkip, wpa2-aes, wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off Restore default configs for this location</pre>
<pre>mode mtu no opmode phy-type power-mgmt radio-off-threshold restore-default rf-band</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off Restore default configs for this location The RF Band that the AP should operate in (g=2.4GHz, a=5GHz)</pre>
<pre>mode mtu no opmode phy-type power-mgmt radio-off-threshold restore-default rf-band rts-threshhold</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off Restore default configs for this location The RF Band that the AP should operate in (g=2.4GHz, a=5GHz) The RTS threshold. Packets bigger than this use RTS and CTS</pre>
<pre>mode mtu mtu no opmode phy-type power-mgmt radio-off-threshold restore-default rf-band rts-threshhold snmp-server</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off Restore default configs for this location The RF Band that the AP should operate in (g=2.4GHz, a=5GHz) The RTS threshold. Packets bigger than this use RTS and CTS Enable SNMP; Modify SNMP parameters</pre>
<pre>mode mtu mtu no opmode phy-type power-mgmt radio-off-threshold restore-default rf-band rts-threshhold snmp-server syscontact</pre>	<pre>One of am_mode or ap_mode (air monitor or access point) The MTU on the wired link for the AP (1024-1576 bytes) Delete Command Can be a comma separated list of opensystem,staticWep,dynamicWep,staticTkip,dy namicTkip,wpa2-aes,wpa2-aes-psk Specify either .a or .g for physical layer type, or enet1 for ethernet port 1 'enable': Enable power management Number of heartbeat misses before radio is turned off Restore default configs for this location The RF Band that the AP should operate in (g=2.4GHz, a=5GHz) The RTS threshold. Packets bigger than this use RTS and CTS Enable SNMP; Modify SNMP parameters Change the system contact</pre>



telnet tx-power virtual-ap vlan-id	Enable or disable telnet to the AP A number from 0 thru 4 Configure a virtual AP with its own essid The ID of the VLAN assigned to this AP's or
	range: 0-4094)
wepkeyl	Specify static WEP key 1 of 4 (length 5 or 13 bytes)
wepkey2	Specify static WEP key 2 of 4 (length 5 or 13 bytes)
wepkey3	<pre>Specify static WEP key 3 of 4 (length 5 or 13     bytes)</pre>
wepkey4	Specify static WEP key 4 of 4 (length 5 or 13 bytes)
weptxkey	Specify an index from 1 thru 4
wpa-hexkey	Set a WPA Pre-Shared Key (PSK)
wpa-passphrase	Set a WPA passphrase to generate PSK
wps	Enable Windows Provisioning Service

(Alcatel6000) (sap-config location 0.0.0) #

## Using ARM

If you enable ARM in AOS-W 2.3 and later, disable healing based on calibration. To do this, enter:

(host) #configure terminal
(host) (config) #wms
(host) (wms) #site-survey ha-compute-time 0
(host) (config) #

# **Advanced Location-Based AP Configuration**

The previous two sections have described default SSID and radio configuration for the global network. If differing configuration is required for specific buildings, floors, or APs, this can be set in the Advanced Location-Based

configuration section. To view or modify location-based configuration, navigate to **Configuration > Wireless LAN > Advanced**, as shown in the figure below

WLAN	> Advance	d		
Location	Default ESSID	802.11 a Channel	802.11 b/g Channel	Actions
1.1.2	shinjuku	36	1	Edit Delete
Add				

FIGURE 13-9 Advanced Location-Based Configuration

To add a new location configuration, click **Add**. After specifying the location to configure, select which parameters should be different from the default for that location. Parameters that can be changed for a particular location include supported SSIDs, 802.11b/g radio parameters, and 802.11a radio parameters. In the example below, all APs in building 2 will be configured to support 128 users, rather than the default of 64:

In the example above, a specific AP (1.1.2) has been configured with parameters that differ from the default.

AP configuration is hierarchical, with a location code of 0 being used as a wildcard. For example, location code "1.0.0" specifies all APs in building 1, regardless of floor or location. Location code "2.1.0" specifies all APs in building 2, floor 1. The effective configuration used by an AP starts with the most specific and moves to the least specific.



WLAN > Advanced > 802.11b/g (4.5.6)				
SSID 802.11b/g	802.11a General			
RTS Threshold (bytes)	1111	Ageout (secs)	1000	
Hide SSID		Deny Broadcast	C Enable 💿 Disable	
Max Retries	8	DTIM Period	1	
Max Clients	0	Beacon Period (ms)	100	
Initial Radio State	⊙ Up C Down	Mode	• Access Point C Air Monitor	
Default Channel	1 💌	Initial Transmit Power	14 dBm(25.119 mW) 💌	
Short Preamble				
Basic Rates (Mbps)	<b>▼</b> 1 <b>▼</b> 2 <b>▼</b> 5 <b>□</b> 6 <b>□</b>	9 🗹 11 🗆 12 🗆 1	8 🗆 24 🗖 36 🗖 48 🗖 54	
Supported Rates (Mbps)	<b>▼</b> 1 <b>▼</b> 2 <b>▼</b> 5 <b>▼</b> 6 <b>▼</b>	9 🗹 11 🔽 12 🔽 1	8 🔽 24 🔽 36 🔽 48 🔽 54	

FIGURE 13-10 Location 2.0.0 Configuration

Assuming that the same change is made for the 802.11a tab, the equivalent CLI configuration for the example above is:

```
ap location 2.0.0
phy-type g
max-clients 128
phy-type a
max-clients 128
```

The configuration could also be done by entering:

```
ap location 2.0.0
max-clients 128
```

The following is new and needs to be added to this discussion.

Monitoring Configuration	Diagnosti	cs Maintenan	e Plan Event	s Reports	
Switch General	WLAN	> Advance	d		
Management	Location	Default ESSID	802.11 a Channel	802.11 b/g Channel	Actions
WLAN	1.1.3	qa_Test_Gui	52	1	Edit Delete
Radio	1.1.10	qa_Test_Gui	52	1	Edit Delete
Advanced	43.33.4444	qa_Test_Gui	52	1	Edit Delete
RF Management			1   1-3 of	3	
Calibration					
Optimization	Add				

#### FIGURE 13-11 Advanced Wireless LAN Configuration

Click **Add** to display the four categories of advanced Wireless LAN configuration:

- SSID—Equivalent to Configuration > Wireless LAN > Network > SSID.
- 802.11b/g—See Figure 13-7.
- 802.11a—See Figure 13-8.
- General—Equivalent to **Configuration > Wireless LAN > Network > General**.

#### **General Wireless LAN Settings**

To configure other Wireless LAN settings, click **Configuration > Wireless LAN > Network > General**. The following screen displays.



VLAN > N	letwork > Genera	I	
SSID Ge	eneral		
LMS IP		Backup LMS IP	
Tunnel MTU		If no value is specified, the MTU will be negotiated	
Power Managem	ient 🔽	Double Encrypt (IPSEC AP)	Г
Radio Off Threst	nold 3	Bootstrap Threshold	8
RF Band 🛛 g 💌			
Disable Radio Fo	r Time Range 🛛 💌		
Restore configur	ration to factory default		
AP Debuggin	g and Logging		
Dump Server			
AP Module	Logging Level		
SAP	Informational 🐱		
АМ	Warnings 👻		
5NMP	Informational 🐱		
SNMP System	Information		
Host Name	TestAP		
System Location			
System Contact			
Enable SNMP Tra	aps 🔽		
Communities	public testcomm1 Add Delete		
Trap Receiver	s		
Server IP V	ersion Community Strings	UDP Port Actions	
Add			
NMPV3 Users	Authentication Protocol P	ivacy Protocol Actions	
Add		nacy monoton menons	

#### FIGURE 13-12 General Wireless LAN Settings

# CHAPTER 14 Radio Resource Management

This chapter discusses the process of configuring the Radio Resource Management features of AOS-W. This feature has two primary functions, configuring and calibrating the radio settings for the network, and then monitoring and dynamically managing those same radio resources.

## Introduction

The goal of RF Management is to initially configure and calibrate radio settings for the network. After the radio network is operational, the goal of RF Management is to tune and adjust radio parameters to ensure that performance remains acceptable for users. RF Management is largely automatic in an Alcatel network, requiring little configuration or intervention from the administrator.

# Calibration

Calibration is a process generally run once at the time of network installation and at additional times if the physical environment changes significantly. Calibration is run on a per-building, per-radio type basis, so that all 802.11a radios in a given building are calibrated at the same time, and all 802.11g radios are calibrated at the same time. Calibration is an active process, requiring all APs and Air Monitors (AMs) in a building to shut down temporarily while the calibration process takes place. During calibration, all APs and AMs communicate with each other at different data rates and different transmit power levels. This process allows the Alcatel switch to build an RF-based map of the network topology, learning about environmental characteristics such as attenuation, interference, and reflection. When calibration has completed, the switch will automatically configure AP/AM mode of the APs, transmit power levels, and channel selection to minimize interference and maximize coverage and throughput.

To initiate calibration from the GUI, navigate to **Configuration > RF Management > Calibration**. Two parameters can be set from this screen, as shown in the figure below.

Maximum Packets per Transmit Power and Transmit Rate	256
Maximum Time for Channel Plan Computation (secs)	600000
Calibrate Radio Network Clear	Apply

FIGURE 14-1 Radio Calibration Configuration

These parameters should not typically be adjusted unless directed by Alcatel Technical Support.

To calibrate the network, click on the "Calibrate Radio Network" button. (See also **Maintenance > Calibrate**.)

Radio Calibi	ration Status			
<b>Building ID</b>	802.11 b/g Status		802.11 a Status	
1	# APs:7 # AMs:1 Calibration Previously Done	Calibrate	# APs:7 # AMs:1 Calibration Previously Done	Calibrate
255	# APs:0 # AMs:1 Calibration Not Done Before	Calibrate	# APs:0 # AMs:0 Calibration Not Done Before	Calibrate
127	# APs:0 # AMs:1 Calibration Not Done Before	Calibrate	# APs:0 # AMs:0 Calibration Not Done Before	Calibrate

#### FIGURE 14-2 Radio Calibration

To begin calibration, click on the calibrate button for each building and each radio type. Perform calibration on only one building and one radio type at a time. Depending on the number of APs in the building, calibration may take between one and forty-five minutes. While calibration is in progress, the message "Calibration in progress" will be displayed on the Radio Calibration Status screen. When calibration has completed, the message "Calibration Previously Done" will be displayed. To view the results of calibration, click on this message. Results similar to the figure below will be displayed.

WLAN > Calibrate Radio Network > Calibration Results(1/802.11 b/g)					
Location	BSSID	Default Channel	Current Channel	Default Power Level	Current Power Level
1.1.4	00:0b:86:9d:61:40	11	11	4/18	4/18
1.1.1	00:0b:86:9d:5c:00	1	1	4/18	4/18
1.1.6	00:0b:86:9d:62:f0	6	6	4/18	4/18
1.1.8	00:0b:86:9d:5b:80	6	6	4/18	4/18
1.1.9	00:0b:86:9d:5b:90	1	1	2/12	2/12

#### FIGURE 14-3 Calibration Results

The equivalent CLI command to perform calibration is "site-survey calibrate".

# Optimization

#### **Self-Healing**

After calibration has taken place, the Alcatel switch has an RF-based topology map of the entire wireless network. This allows the switch to understand which APs are within range of each other. In the event that an AP fails, surrounding APs will increase their transmit power level to fill in any gaps. Self-healing is enabled by default, and can be configured in the GUI by navigating to **Configuration > RF Management > Optimization > Self Healing**.

Self Healing	Load Balancing		
Self Healing			
Maximum HA Neighb	ors to participate in Self-healing		3
Maximum Power Lev	el Increase		2
Self-healing wait Tim	e after AP Failure		60000
		Clear	Apply

FIGURE 14-4 Self Healing Configuration

It is typically not necessary to adjust these parameters. The available parameters are:



**Maximum neighbors to participate in self-healing** – The maximum number of neighboring APs that will increase their power level after a failure.

**Maximum power level increase –** The number of power levels a neighbor AP will increase after a failure.

**Self-Healing Wait Time –** The time after a failure, in milliseconds, after which the self-healing algorithm will begin. This should be set sufficiently high so that an AP reboot, rather than a failure, will not trigger the self-healing algorithm.

The equivalent CLI configuration for the above example is:

```
site-survey max-ha-neighbors 3
site-survey neighbor-tx-power-bump 2
site-survey ha-compute-time 60000
```

# Load Balancing

When multiple APs are available to service users in the same area, load balancing ensures that a single AP does not become overloaded. Load balancing works by keeping track of user count and bandwidth utilization for each AP in the network. If an AP reaches a configured performance threshold, that AP will attempt to force new clients to a different AP by temporarily rejecting association attempts. If no other AP is able to pick up the load, eventually the client will be allowed to associate after a configured interval has passed.

To configure load balancing in the GUI, navigate to Configuration  $\rightarrow$  RF Management  $\rightarrow$  Optimization  $\rightarrow$  Load Balancing, as shown in the figure below.

Self Healing	Load Balancing	
Load Balancing		
Enable Load Balancir	ig	Г
Wait Time before ap	plying Load Balancing (secs)	30
Max Association Ret	ries	8
Maximum User Coun	t - High Watermark	255
Maximum User Coun	t - Low Watermark	230
Bandwidth Utilization	Threshold - High Watermark (%)	90
Bandwidth Utilization	Threshold - Low Watermark (%)	80
		Clear Appl

FIGURE 14-5 Load Balancing Configuration

Available parameters are:

Enable Load Balancing - Enables or disables load balancing.

Wait Time before applying Load Balancing (secs) – Specifies the number of seconds to wait before performing load balancing processing.

**Max Association Retries –** Specifies the number of association attempts that will be rejected before a client is allowed to associate to an AP that has reached a performance threshold.

**Maximum User Count High Watermark –** The maximum number of client associations on a single AP, after which load balancing will begin.

**Maximum User Count Low Watermark –** After load balancing has begun, the number that the current association count must go below for load balancing to stop.

**Bandwidth Utilization Threshold High Watermark** – The maximum percentage of available bandwidth that must be consumed before load balancing will begin. The value represents percentage of maximum for a given radio. For 802.11b, the theoretical maximum bandwidth is 7 Mbps. For 802.11a and g, the theoretical maximum is 30 Mbps.

**Bandwidth Utilization Threshold Low Watermark –** After load balancing has begun, the percentage of available bandwidth below which the utilization must drop before load balancing will end.



The equivalent CLI configuration for the above example is:

```
ap-policy ap-load-balancing disable
ap-policy ap-lb-max-retries 8
ap-policy ap-lb-util-high-wm 90
ap-policy ap-lb-util-low-wm 80
ap-policy ap-lb-user-high-wm 255
ap-policy ap-lb-user-low-wm 230
```

# **Client and AP DoS Protection**

Configure station and AP Denial of Service attack protection by navigating to Configuration > RF Management > Protection as shown in the figure below.

RF Management > <b>Protection</b>		
DoS Protection		
Enable Access Point DoS Protection		
Enable Client DoS protection		
DoS Client Block Time (secs)	3600	
Authentication Failure Block Time (secs)('0' blocks stations indefinitely)	0	
		Clear Apply
Commands		<u>View Commands</u>

FIGURE 14-6 Client and AP Protection

Available parameters are:

**Enable AP DoS Protection** – Instructs APs to ignore deauthenticate frames seen from clients. This prevents a successful deauth attack from being carried out against the AP. A client that has shut down or left the network will time out naturally after a configured ageout interval, by default 30 minutes.

**Enable Client DoS Protection –** Enables detection of a deauth attack initiated against a client associated to an Alcatel AP. When such an attack is detected, the client can be quarantined from the network to prevent a man-in-the-middle attack from being successful.

**DoS Client Block Time –** Specifies the number of seconds a client will be quarantined from the network after a deauth attack against the client has been detected. This is used to prevent man-in-the-middle attacks.

The equivalent CLI configuration for the above example is:

stm dos-prevention enable
stm sta-dos-prevention enable
stm sta-dos-block-time 3600

# **Configuration of RF Monitoring**

#### **Coverage Hole Detection**

The way we implemented CHD is slightly different. We will generate a CHD event only if the RSSI of the client is low during association phase.

We don't do any CHD based on the RSSI of data packets. The way I test is associate a client (I used CISCO-350) to the AP and moved to around 180ft.

Then Cisco started sending out probe-request around 180ft. And the AP noticed low RSSI on the probe request and generated CHD event.

You will see now a coverage hole detection (CHD) event in the log.

Our CHD works only when the client is not able to associate.

Coverage hole detection looks for clients unable to associate to any AP, associating at very low data rates, or associating with low signal strength. These symptoms indicate areas of a building where holes in radio coverage exist. When the system detects such coverage holes, the administrator is notified of the condition via the event log. To configure coverage hole detection, navigate to **Configuration > RF Management > Monitoring > Coverage Hole Detection** as shown in the figure below.



RF Management > Monitoring > Coverage Hole Detection					
Coverage Hole Detection	Interference Detection	Event Thresholds			
Enable Coverage Hole Detection					
High RSSI Threshold for Hole Detection				20	
Low RSSI Threshold for Hole Detection				10	
Ageout Time for Good RSSI Station (secs)				30	
Delay Time for Hole Detection Event Generation (secs)				180	
Idle Time for Bad RSSI station (secs)				90	
			Clear	Apply	
Commands		View Con	nmands		

FIGURE 14-7 Coverage Hole Detection

Other than enabling or disabling the feature, these parameters should generally not be changed unless directed by Alcatel Technical Support. Available parameters are:

**Enable Coverage Hole Detection –** Enables or disables coverage hole detection.

**High RSSI Threshold for Hole Detection –** Stations with signal strength above this value are considered to have good coverage.

**Low RSSI Threshold for Hole Detection –** Stations with signal strength below this value will trigger detection of a coverage hole.

**Ageout time for Good RSSI Station -** Amount of time, in seconds, after which a station with good RSSI will be aged out.

**Delay Time for Hole Detection Event Generation –** The amount of time after a coverage hole is detected until another coverage hole event notification is generated.

**Idle Time for Bad RSSI Station -** Amount of idle time, in seconds, after which a station in a poor coverage area will be aged out.

The equivalent CLI configuration for the above example is:

```
stm coverage-hole-detection disable
stm good-rssi-threshold 20
```

```
stm poor-rssi-threshold 10
stm hole-detection-interval 120
stm good-sta-ageout 30
stm idle-sta-ageout 90
```

## **Interference Detection**

Interference detection notifies the administrator when localized interference becomes sufficient to cause performance degradation. Enable interference detection in the GUI by navigating to **Configuration > RF Management > Monitoring > Interference Detection** as shown in the figure below.

RF Management > Monitoring > Interference Detection					
Coverage Hole Detection	Interference Detection	Event Thresholds			
Enable Interference Detection					
Interference Retry Increment Threshold(%)			100		
Interference Wait Time (secs)			30		
Interference Quiet Time (secs)			30		
			Clear Apply		
Commands		View Com	mands		

FIGURE 14-8 Interference Detection

Available parameters are:

Enable Interference Detection - Enables or disables interference detection.

**Interference Retry Increment Threshold** – Interference monitoring will begin on a given channel when the local frame retry rate or frame receive error rate increases by this percentage.

**Interference Wait Time –** Specifies the amount of time that the frame retry rate of frame receive error rate must be continuously above the threshold in order for an interference detection event to be generated.

**Interference Quiet Time -** The amount of time, in seconds, that the AP should listen to establish a baseline error rate.

The equivalent CLI configuration for the above example is:



```
wms
global-policy detect-interference disable
global-policy interference-inc-threshold 100
global-policy interference-inc-timeout 30
global-policy interference-wait-time 30
```

## **Event Threshold Configuration**

AOS-W provides the ability to configure event thresholds to notify the administrator when certain RF parameters are exceeded. These events can signal excessive load on the network, excessive interference, or faulty equipment. Configure event thresholds by navigating to **Configuration > RF Management > Monitoring > Event Thresholds** as shown in the figure below. Events generated by these thresholds being exceeded are found in the system event log under the Events heading in the GUI.

**NOTE**—Every environment is different, and administrators should plan to tune these parameters for optimal monitoring. Alcatel provides recommended values for these parameters for an average environment. If these thresholds are too high or too low, it could lead to too many false alarms or could lead to error conditions being missed.

5	5		
Coverage Hole Detection	Interference Detection	Event Thresholds	
Bandwidth Rate-High Watermark(%	)		0
Bandwidth Rate-Low Watermark (%)			
Frame Error Rate-High Watermark (%)			0
Frame Error Rate-Low Watermark (%)			0
Frame Fragmentation Rate-High Wa	termark (%)		16
Frame Fragmentation Rate-Low Wa	termark (%)		8
Frame Low Speed Rate-High Waterr	nark (%)		16
Frame Low Speed Rate-Low Watern	nark (%)		8
Frame Non Unicast Rate-High Water	mark(%)		0
Frame Non Unicast Rate-Low Water	mark(%)		0
Frame Receive Error Rate-High Wat	ermark (%)		16
Frame Receive Error Rate-Low Wate	ermark(%)		8
Frame Retry Rate-High Watermark (	(%)		16
Frame Retry Rate-Low Watermark (	%)		8
			Clear Apply
Commands		View Com	mands

## RF Management > Monitoring > Event Thresholds

#### FIGURE 14-9 Event Threshold Configuration

To disable detection for any parameter, set the value to 0. Available parameters are:

**Bandwidth Rate High Watermark** – If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents percentage of maximum for a given radio. For 802.11b, the theoretical maximum bandwidth is 7 Mbps. For 802.11a and g, the theoretical maximum is 30 Mbps. The recommended value is 85%.

**Bandwidth Rate Low Watermark** – After a bandwidth exceeded condition exists, the condition will persist until bandwidth drops below this value. The recommended value is 70%.



**Frame Error Rate High Watermark –** If the frame error rate, as a percentage of total frames, in an AP exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%.

**Frame Error Rate Low Watermark –** After a frame error rate exceeded condition exists, the condition will persist until the frame error rate drops below this value. The recommended value is 8%.

**Frame Fragmentation Rate High Watermark –** If the frame fragmentation rate, as a percentage of total frames, in an AP exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%.

**Frame Fragmentation Rate Low Watermark –** After a frame fragmentation rate exceeded condition exists, the condition will persist until the frame fragmentation rate drops below this value. The recommended value is 8%.

**Frame Low Speed Rate High Watermark** – If the rate of low-speed frames, as a percentage of total frames, in an AP exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%.

**Frame Low Speed Rate Low Watermark –** After a low-speed rate exceeded condition exists, the condition will persist until the percentage of low-speed frames drops below this value. The recommended value is 8%.

**Frame Non-Unicast Rate High Watermark** – If the non-unicast rate, as a percentage of total frames, in an AP exceeds this value, a non-unicast rate exceeded condition exists. The default value for this parameter is 0, indicating that it is disabled. This value largely depends on applications used on the network.

**Frame Non-Unicast Rate Low Watermark –** After a non-unicast rate exceeded condition exists, the condition will persist until the non-unicast rate drops below this value. The default value for this parameter is 0, indicating that it is disabled.

**Frame Receive Error Rate High Watermark –** If the frame receive error rate, as a percentage of total frames, in an AP exceeds this value, a frame receive error rate exceeded condition exists. The recommended value is 16%.

**Frame Receive Error Rate Low Watermark –** After a frame receive error rate exceeded condition exists, the condition will persist until the frame receive error rate drops below this value. The recommended value is 8%

**Frame Retry Rate High Watermark –** If the frame retry rate, as a percentage of total frames, in an AP exceeds this value, a frame retry rate exceeded condition exists. The recommended value is 16%.

**Frame Retry Rate Low Watermark –** After a frame retry rate exceeded condition exists, the condition will persist until the frame retry rate drops below this value. The recommended value is 8%.

The equivalent CLI configuration for the above example is:

```
wms
event-threshold fer-high-wm 16
event-threshold fer-low-wm 8
event-threshold frr-high-wm 16
event-threshold frr-low-wm 8
event-threshold flsr-high-wm 16
event-threshold flsr-low-wm 8
event-threshold fnur-low-wm 0
event-threshold frer-high-wm 16
event-threshold frer-low-wm 8
event-threshold ffr-high-wm 16
event-threshold ffr-high-wm 16
event-threshold ffr-low-wm 8
event-threshold ffr-low-wm 8
event-threshold bwr-low-wm 0
```

### **Advanced Parameters**

To access RF management advanced parameters, navigate to **Configuration > RF Management > Advanced**.

The advanced RF management parameters are shown in the figure below.



RF Management > Advanced	
AP Ageout Interval (millisecs)	30
(Enter 0 to disable AP Ageout)	
AP Scan Inactivity (seconds)	5
AM Grace Time (milli seconds)	2000
Force Station Deauthentication for Policy Enforcement	
Enable Force Station Deauthentication Debug	
AM Poll Interval(milli seconds)	60000
Number of AM Poll Retries	2
Station Ageout Interval(minutes)	30
(Enter 0 to disable Station Ageout)	
Station Scan Inactivity(seconds)	60
Enable Statistics Update in DB	
Commands	View Commands

#### FIGURE 14-10 RF Management Advanced Parameters

The advanced parameters are:

**AP Ageout Interval -** The number of millisecs TBC.

AP Scan Inactivity - The number of seconds TBC.

**AM Grace Time-** The number of milliseconds TBC

Force Station Deauthentication for Policy Enforcement- was laser beamTBC.

Enable Force Station Deauthentication- TBC.

AM Poll Internal- TBC.

Number of AM Poll Retries- TBC.

Station Ageout Interval - TBC.
#### Station Scan Inactivity- TBC.

#### Enable Statistics Update in DB- TBC:

```
auto-rra scan-interval 10
auto-rra scan-time 110
auto-rra beacon-discovered-ageout 4
auto-rra data-discovered-ageout 8
auto-rra error-rate-threshold 0
auto-rra good-channel-index 75
auto-rra channel-update-trigger-interval 60
auto-rra channel-update-dampen-interval 300
auto-rra compute-tree-depth 1
auto-rra min-scan-time 4
auto-rra scanning disable
```



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 15 Intrusion Detection Configuration

This chapter discusses the various kinds of intrusion and Wireless LAN attack methods. It also describes how to configure the switch to detect and guard against the various kinds of intrusion attempts.

AOS-W protects against numerous types of intrusion methods and tools, including:

- Probing and Network Discovery
- Denial of Service (DoS)
- Surveillance
- Impersonation
- Client Intrusion
- Network Intrusion

## Wireless LAN Intrusion Detection

The nature of wireless networks makes them attractive targets for intruders. Many intruders are only searching for free Internet access, and use a number of different probe tools to find it. Others, however, are intent on gaining access to an enterprise network for malicious purposes – either to steal data, disrupt legitimate communication, or damage data. Wireless LAN intrusion can be classified into several broad categories:

Probing and Network Discovery

Network discovery is a normal part of 802.11, and allows client devices to discover APs and also to learn about available services provided by APs. While network discovery itself does not necessarily lead to security problems, it is the first step that an attacker needs to accomplish before moving on to more serious intrusion attempts.

Denial of service (DoS) attack

DoS attacks are designed to prevent or inhibit legitimate users from accessing the network. This includes blocking network access completely, degrading network service, and increasing processing load on clients and network equipment.

#### Surveillance

Surveillance allows an attacker to monitor and capture data from a wireless network. The primary means of overcoming the risk of surveillance is the use of encryption – either link-layer encryption such as WEP or TKIP, or network-layer encryption such as IPSec.

Impersonation

Impersonation attacks in a wireless network typically involve an attacker taking on the address of a valid client or AP and trying to obtain access or services typically reserved for those valid clients or APs. Because wireless devices are not at the end of a physical cable, it can be difficult to detect such an attack taking place. In a worst-case scenario, an impersonating AP could fool a client into connecting with it, and then obtain that client's authentication credentials.

Client Intrusion

Client intrusion attacks attempt to exploit vulnerabilities in client devices to gain access to a network resource. Often the attacks involve a combination of DoS and impersonation.

Network Intrusion

A network intrusion attack implies that an attacker is able to gain full access to enterprise network resources.

The following sections explain configuration of the Wireless LAN intrusion detection and prevention of Alcatel AOS-W.

## Rogue AP

Rogue APs represent perhaps the largest threat to enterprise network security because they bypass all other security provisions and open a network up to the outside world. Rogue APs are normally placed by employees who do not understand the risks their actions represent.

A rogue AP is defined as one that is a) unauthorized, and b) plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered "interfering" – it has the potential to cause RF interference, but is not connected to the enterprise wired network and thus does not represent a direct threat. Alcatel is unique in providing the classification function to ensure that valid, interfering, and rogue APs are accurately and automatically classified.

To configure rogue AP detection and protection capabilities, navigate to **Configuration > Wireless LAN Intrusion Detection > Rogue AP** as shown in the figure below.

Disable Users from Connecting to Rogue Access Points	₹
Mark All New Access Points as Valid Access Points	
Mark Unknown Access Points as Rogue Access Points	

FIGURE 15-1 Rogue AP Configuration

Rogue AP detection and classification is enabled by default. To view AP classification reports, navigate to **Reports > AP Reports** as described in "Monitoring the Wireless Environment".

Available configuration parameters are:

**Disable Users from Connecting to Rogue APs –** By default, rogue APs are only detected, but are not automatically disabled. Enable this option to automatically shut down rogue APs. When this option is enabled, clients attempting to associate to a rogue AP will be disconnected from the rogue AP through a denial of service attack.



**Mark All New APs as Valid** – When installing an Alcatel switch in an environment with an existing 3<sup>rd</sup>-party wireless network, it is necessary to manually classify existing enterprise APs as valid – a time-consuming process if a large number of APs are installed. Enable this option to mark all detected APs as valid. Leave this option enabled until all enterprise APs have been detected and classified as valid. After this process has completed, disable this option and re-classify any unknown APs as interfering.

**Mark Unknown APs as Rogue –** In an environment where no interfering APs should exist—for example, a building far away from any other buildings or an RF shielded building —enable this option to turn off the classification process. Any AP detected that is not classified as valid will be marked as rogue.

**NOTE**—*Note:* Use caution when enabling both "Mark Unknown APs as Rogue" and "Disable Users from Connecting to Rogue APs". If the system is installed in an area where APs from neighboring locations can be detected, these two options will disable all APs in the area.

The equivalent CLI configuration for the able example is:

```
wms ap-policy protect-unsecure-ap enable
wms ap-policy learn-ap disable
wms ap-policy classification enable
```

## **Denial of Service**

Denial of Service attack detection encompasses both rate analysis and detection of a specific DoS attack known as FakeAP.

### **Rate Analysis**

Many DoS attacks flood an AP or multiple APs with 802.11 management frames. These can include authenticate/associate frames, designed to fill up the association table of an AP. Other management frame floods, such as probe request floods, can consume excess processing power on the AP. To configure rate analysis, navigate to **Configuration > Wireless LAN Intrusion Detection > Denial Of Service > Rate Analysis** as shown in the figure below.

Rate Analysis					
Enable Rate Anomaly Checking					
Detection Pa	rameters				
Frame Type	Channel Thresh	old Channel T	ïme(sec)	Channel Quiet Time(sec)	
Association	30	3		900	
Probe Request	30	3		900	
Probe Response	30	3		900	
Disassociation	30	3		900	
Authentication	30	3		900	
Deauthentication	30	3		900	
		Edit Cance	el		
F	N- d- 76	N			_
Association	Node Inresnoid	Node Time(s)	ec) Node	e Quiet Time(sec)	
Probe Request	50 60	60	900		
	60	60	900		
Disassociation	20	60	900		
Authoritics	30	00	900		
Authentication	30	60	900		
Deauthentication	150	15	900		
	E	dit Cancel			

### FIGURE 15-2 Rate Analysis Configuration

Configuration is divided into two sections: Channel thresholds and node thresholds. A channel threshold applies to an entire channel, while a node threshold applies to a particular client MAC address. All frame types are standard management frames as defined by the 802.11 standard. Configuration parameters are:

**Channel/Node Threshold –** Specifies the number of a specific type of frame that must be exceeded within a specific interval to trigger an alarm.

**Channel/Node Time –** Specifies the time interval in which the threshold must be exceeded in order to trigger an alarm.

**Channel/Node Quiet Time –** After an alarm has been triggered, specifies the amount of time that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the logfile.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy rate-frame-type-param assoc channel-threshold 30
ids-policy rate-frame-type-param assoc channel-inc-time 3
```



```
ids-policy rate-frame-type-param assoc channel-quiet-time 900
ids-policy rate-frame-type-param assoc node-threshold 30
ids-policy rate-frame-type-param assoc node-time-interval 60
ids-policy rate-frame-type-param assoc node-quiet-time 900
ids-policy rate-frame-type-param disassoc channel-threshold 30
ids-policy rate-frame-type-param disassoc channel-inc-time 3
ids-policy rate-frame-type-param disassoc channel-quiet-time 900
ids-policy rate-frame-type-param disassoc node-threshold 30
ids-policy rate-frame-type-param disassoc node-time-interval 60
ids-policy rate-frame-type-param disassoc node-quiet-time 900
ids-policy rate-frame-type-param deauth channel-threshold 30
ids-policy rate-frame-type-param deauth channel-inc-time 3
ids-policy rate-frame-type-param deauth channel-quiet-time 900
ids-policy rate-frame-type-param deauth node-threshold 150
ids-policy rate-frame-type-param deauth node-time-interval 15
ids-policy rate-frame-type-param deauth node-quiet-time 900
ids-policy rate-frame-type-param probe-request channel-threshold 30
ids-policy rate-frame-type-param probe-request channel-inc-time 3
ids-policy rate-frame-type-param probe-request channel-quiet-time 900
ids-policy rate-frame-type-param probe-request node-threshold 60
ids-policy rate-frame-type-param probe-request node-time-interval 60
ids-policy rate-frame-type-param probe-request node-quiet-time 900
ids-policy rate-frame-type-param probe-response channel-threshold 30
ids-policy rate-frame-type-param probe-response channel-inc-time 3
ids-policy rate-frame-type-param probe-response channel-quiet-time 900
ids-policy rate-frame-type-param probe-response node-threshold 60
ids-policy rate-frame-type-param probe-response node-time-interval 60
ids-policy rate-frame-type-param probe-response node-quiet-time 900
ids-policy rate-frame-type-param auth channel-threshold 30
ids-policy rate-frame-type-param auth channel-inc-time 3
ids-policy rate-frame-type-param auth channel-quiet-time 900
ids-policy rate-frame-type-param auth node-threshold 30
ids-policy rate-frame-type-param auth node-time-interval 60
ids-policy rate-frame-type-param auth node-quiet-time 900
```

### **FakeAP Detection**

FakeAP is a tool originally created to thwart wardrivers by flooding beacon frames containing hundreds of different addresses. This would appear to a wardriver as though there were hundreds of different APs in the area, thus concealing the real AP. While the tool is still effective for this purpose, a newer purpose is to flood public hotspots or enterprises with fake AP beacons to confuse legitimate users and to increase the amount of processing client operating systems must do. To configure detection of FakeAP, navigate to **Configuration > Wireless LAN** Intrusion Detection > Denial of Service > FakeAP as shown in the figure below.

Fake AP	
Enable Fake AP Flood Detection	
Flood Inc Time (secs)	3
Flood Threshold	50
Quiet Time (secs)	900

FIGURE 15-3 FakeAP Detection

Configuration parameters are:

Enable Fake AP Flood Detection - Enables or disables the feature.

**Flood Inc Time –** The time period in which a configured number of FakeAP beacons must be received.

**Flood Threshold –** The number of FakeAP beacons that must be received within the Flood Inc Time in order to trigger an alarm.

**Quiet Time -** After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy ap-flood-check disable
ids-policy ap-flood-threshold 50
ids-policy ap-flood-inc-time 3
ids-policy ap-flood-quiet-time 900
```

# Man-in-the-Middle

A successful man-in-the-middle attack will insert an attacker into the data path between the client and the AP. In such a position, the attacker can delete, add, or modify data, provided he has access to the encryption keys.



Such an attack also enables other attacks that can learn a user's authentication credentials. Man-in-the-middle attacks often rely on a number of different vulnerabilities.

### MAC Spoofing

MAC address spoofing is a typical attack on a wireless LAN in which an attacker will spoof the MAC address of a currently active valid client in an attempt to be granted that client's access privileges. The AirJack driver for Linux allows easy access to such an attack.

To configure detection of MAC address spoofing, navigate to **Configuration > Wireless LAN Intrusion Detection > Man-in-the-Middle > MAC Spoofing** as shown in the figure below.

MAC Spoofing				
Enable MAC Address Spoof Detection				
	Clear	Арр	ly -	

FIGURE 15-4 MAC Spoofing

The equivalent CLI configuration for the above example is:

wms

```
station-policy detect-sta-impersonation enable
```

### **Station Disconnection Detection**

Spoofed deauthenticate frames form the basis for most denial of service attacks, as well as the basis for many other attacks such as man-in-the-middle. A Linux driver called AirJack typically forms the basis for this type of attack, with tools such as Wireless LAN-Jack and Fata-Jack actually carrying out the attack. In a station disconnection attack, an attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association.

To configure detection of station disconnection, navigate to **Configuration > Wireless LAN Intrusion Detection > Man-in-the-Middle > Disconnect Station**, as shown in the figure below.



FIGURE 15-5 Detect Station Disconnection

Configuration parameters are:

Enable Disconnect Station Analysis - Enables or disables the feature

**Disconnect Station Detection Quiet Time** – After a station disconnection is detected, the amount of time that must pass before another identical alarm can be generated.

Equivalent CLI configuration for the above example is:

wms ids-policy dsta-check enable ids-policy dsta-quiet-time 900

FIGURE 15-6 Disconnect Station Settings

## EAP Handshake Analysis

EAP (Extensible Authentication Protocol) is a component of 802.1x used for authentication. Some attacks, such as "ASLEAP" (used to attack Cisco LEAP) send spoofed deauthenticate messages to clients in order to force the client to re-authenticate multiple times. These attacks then capture the authentication frames for offline analysis. EAP Handshake Analysis detects a client performing an abnormal number of authentication procedures and generates an alarm when this condition is detected. To configure EAP Handshake Analysis, navigate to **Configuration > Wireless LAN Intrusion Detection > Man-in-the-Middle > EAP Handshake**, as shown in the figure below.



EAP Handshake Analysis	
Enable EAP Handshake Analysis	
EAP Handshake Threshold	10
EAP Time Interval (secs)	60
EAP Rate Detection Quiet Time (secs)	900

FIGURE 15-7 EAP Handshake Analysis

Configuration parameters are:

Enable EAP Handshake Analysis - Enables or disables the feature.

**EAP Handshake Threshold –** The number of EAP handshakes that must be received within the EAP Time Interval in order to trigger an alarm.

**EAP Time Interval –** The time period in which a configured number of EAP handshakes must be received.

**EAP Rate Detection Quiet Time** – After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy eap-check enable
ids-policy eap-rate-threshold 10
ids-policy eap-rate-time-interval 60
ids-policy eap-rate-quiet-time 900
```

### Sequence Number Analysis

During an impersonation attack, the attacker will generally spoof the MAC address of a client or AP. If two devices are active on the network with the same MAC address, their 802.11 sequence numbers will not match – since the sequence number is usually generated by the NIC firmware, even a custom driver will not generally be able to modify these numbers. Sequence number analysis will detect possible impersonation attacks by looking for anomalies between sequence numbers seen in frames in the air. To configure sequence number analysis, navigate to **Configuration > Wireless LAN Intrusion Detection > Man-in-the-Middle > Sequence Number**, as shown in the figure below.

Sequence Number Analysis	
Enable Sequence Number Discrepancy Checking	
Sequence Number Difference Threshold	100
Sequence Number Checking Time Tolerance (secs)	500
Sequence Number Checking Quiet Time (secs)	900

FIGURE 15-8 Sequence Number Analysis

Configuration parameters are:

**Enable Sequence Number Discrepancy Checking –** Enables and disables the feature.

**Sequence Number Difference Threshold –** The maximum allowable tolerance between sequence numbers within a specific time interval.

**Sequence Number Checking Time Tolerance –** The time interval in which sequence numbers must exceed the sequence number difference threshold in order for an alarm to be triggered.

**Sequence Number Checking Quiet Time** – After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy sequence-check enable
ids-policy sequence-diff 100
ids-policy sequence-time-tolerance 500
ids-policy sequence-quiet-time 900
```

## **AP Impersonation Protection**

AP impersonation attacks can be done for several purposes, including as a Man-In-the-Middle attack, as a rogue AP attempting to bypass detection, and as a possible honeypot attack. In such an attack, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. To configure AP Impersonation Detection and Protection, navigate to **Configuration > Wireless LAN Intrusion Detection > Man-in-the-Middle > AP Impersonation** as shown in the figure below.





FIGURE 15-9 AP Impersonation Protection

Configuration parameters are:

Enable AP Impersonation Detection - Enables detection of AP impersonation.

**Enable AP Impersonation Protection –** When AP impersonation is detected, both the legitimate and the impersonating AP will be disabled using a denial of service attack.

**Beacon Rate Increment Threshold –** The percentage increase in beacon rate that will trigger an AP impersonation event.

The equivalent CLI configuration for the above example is:

```
wms
ap-policy detect-ap-impersonation enable
ap-policy protect-ap-impersonation enable
ap-policy beacon-diff-threshold 50
```

## Signature Detection

Many Wireless LAN intrusion and attack tools generate characteristic signatures that can be detected by the Alcatel network. The system comes pre-configured with several known signatures, and also includes the ability for network managers to create and edit new signatures. To configure signature detection, navigate to **Configuration > Wireless LAN Intrusion Detection > Signatures**, as shown in Figure 15-10.

Intrusion Prevention > Signatures					
Signature Analysis					
Enable Signature Analysis	Γ				
Signature Analysis Quiet T	ime (secs) 9	00			
Name	Category	Active	Action		
ASLEAP	Pre-Defined	Yes	Edit Delete		
Null-Probe-Response	Pre-Defined	Yes	Edit Delete		
AirJack	Pre-Defined	Yes	Edit Delete		
NetStumbler Generic	Pre-Defined	Yes	Edit Delete		
NetStumbler Version 3.3.0x	Pre-Defined	Yes	Edit Delete		
Deauth-Broadcast	Pre-Defined	Yes	Edit Delete		
Add					
Commands				<u>View Commands</u>	

FIGURE 15-10 Signature Analysis

Configuration parameters are:

Enable Signature Analysis - Enables and disables the feature.

**Signature Analysis Quiet Time** - After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy signature-check enable
ids-policy signature-quiet-time 900
```

### **Pre-Defined Signatures**

Pre-defined signatures as of AOS-W 2.0 are listed below. These signatures may be supplemented or changed as additional software versions are released.



**Null-Probe-Response** - An attack with the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. A number of popular NIC cards will lock up upon receiving such a probe response.

**AirJack –** Airjack is a popular NIC driver for Linux that allows manipulation of many 802.11 parameters. Airjack also includes AP functionality that by default generates beacons with an ESSID of "AirJack". This signature detects the AP functionality using the default configuration.

**NetStumbler Generic** – NetStumbler is a popular wardriving application used to locate 802.11 networks. When used with certain NICs (such as Orinoco), NetStumbler generates a characteristic frame that can be detected.

**NetStumbler 3.3.0x –** Version 3.3.0 of NetStumbler changed the characteristic frame slightly. This signature detects the updated frame.

**Deauth-broadcast** – A deauth broadcast attempts to disconnect all stations in range – rather than sending a spoofed deauth to a specific MAC address, this attack sends the frame to a broadcast address.

CLI configuration for the pre-defined signatures is:

```
wms
ids-signature "Null-Probe-Response"
  mode enable
  frame-type probe-response ssid-length 0
ids-signature "AirJack"
  mode enable
  frame-type beacon ssid AirJack
 1
ids-signature "NetStumbler Generic"
  mode enable
  payload 0x00601d 3
  pavload 0x0001 6
 1
ids-signature "NetStumbler Version 3.3.0x"
  mode enable
  payload 0x00601d 3
  payload 0x000102 12
 L
ids-signature "Deauth-Broadcast"
  mode enable
  frame-type deauth
   dst-mac ff:ff:ff:ff:ff:ff
```

### Adding New Signatures

To add new signatures, click the Add button. The Add IDS Signature screen is shown in the figure below.

Signature Name	New_Signature
Signature Mode	
Signature Rul	es
Attribute Va	alue Action
Add	
	Apply
Add Condition	า
Attribute bssic	Value
Add Ca Dssid dst-m frame paylo	ac ⊳type ad
Comman( src-m	ium iac

FIGURE 15-11 Add IDS Signature

Configuration parameters are:

Signature Name – A user-defined name for the new signature

**Signature Mode –** A checkbox in this field indicates that the signature is enabled.

To add signature rules, click **Add**. Available attributes for signature matching include BSSID, destination MAC address, frame type, payload, sequence number, and source MAC address. If desired, multiple attributes may be configured for each rule. When finished adding new rules, click **Apply**.



# **Wireless LAN Policies**

### Ad-hoc Network Protection

As far as network administrators are concerned, ad-hoc wireless networks are uncontrolled. If they do not use encryption, they may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad-hoc network may also function like a rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities. For these reasons, many administrators choose to prohibit ad-hoc networks. The Alcatel system can perform both ad-hoc network detection and also disable ad-hoc networks when they are found. To configure ad-hoc network protection, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Adhoc Network**, as shown in the figure below.

Adhoc Network	
Enable Adhoc Networks Activity Detection	
Enable Adhoc Network Protection	•
Adhoc Detection Quiet Time (secs)	900

FIGURE 15-12 Ad-Hoc Network Protection

Configuration parameters are:

**Enable Adhoc Network Activity Detection** – Enable detection of Ad-hoc networks.

**Enable Adhoc Network Protection –** When Ad-hoc networks are detected, they will be disabled using a denial of service attack.

Adhoc Detection Quiet Time - After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the above example is:

```
wms
ids-policy adhoc-check enable
ap-policy protect-ibss enable
ids-policy adhoc-quiet-time 900
```

## Wireless Bridge Detection

Wireless bridges are normally used to connect multiple buildings together. However, an attacker could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges – in these networks, the presence of a bridge is a signal that a security problem exists. To configure detection of wireless bridges, navigate to Configuration > Wireless LAN Intrusion Detection > Policies > Wireless Bridge, as shown in the figure below.

Wireless Bridge	
Enable Wireless Bridge Detection	
Wireless Bridge Detection Quiet Time (secs)	900

FIGURE 15-13 Wireless Bridge Detection

Configuration parameters are:

Enable Wireless Bridge Detection - Enable or disable the feature.

Wireless Bridge Detection Quiet Time - After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

Equivalent CLI configuration for the example above is:

```
wms
ids-policy wbridge-check enable
ids-policy wbridge-quiet-time 900
```

## **Misconfigured AP Protection**

If desired, a list of parameters can be configured that defines the characteristics of a valid AP. This is primarily used when non-Alcatel APs are being used in the network, since the Wireless LAN switch cannot configure the 3<sup>rd</sup>-party APs. These parameters can include preamble type, WEP configuration, OUI of valid MAC addresses, valid channels, DCF/PCF configuration, and ESSID. The system can also be configured to detect an AP using a weak WEP key. If a valid AP is detected as misconfigured, the system will deny access to the misconfigured AP. In cases where someone gains configuration access to a 3<sup>rd</sup>-party AP and changes the configuration, this



policy is useful in blocking access to that AP until the configuration can be fixed. To configure protection of misconfigured APs, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Misconfigured AP**, as shown in Figure 15-14.

Adhoc Network	Wireless Bridge	Misconfigu	ared AP	Weak WEP	Multi Tenancy	MAC OUI
Misconfigured Acce	ess Points					
Detect Misconfigured A	ccess Points					
Disable Detected Misco	nfigured Access Points					
Valid Enterprise 802.11	b/g Channels		2 🗆 3 🗆 4	5 16 7 7	8 🗆 9 🗖 10 🔽 11	
Valid Enterprise 802.11	a Channels	☞ 36 ☞ 40 ☞ 44 ☞ 48 ☞ 52 ☞ 56 ☞ 60 ☞ 64 □ 149 □ 153 □ 157 □ 161 □ 165			□ 153 □ 157 □ 161 □ 165	
Enforce Short Preamble						
Prevent valid clients fro	om roaming to interfering AF	APS				
Enforce WEP Encryptio	n for all Traffic	<b>V</b>				
Enforce WPA Encryptio	n for all Traffic					
Valid Access Point Manu (OUIs must be entered the format xx:xx:xx:x is a hexadecimal numbe	ufacturers OUI List in «xx:xx where x r, f being the wildcard)		Delete (	dding/Deleting to/	from the OLIT list will imm	wadiataku undata tha suitch confiniuration

FIGURE 15-14 Misconfigured AP Protection

Configuration parameters are:

#### **Detect Misconfigured Access Points-TBC**

**Disable Misconfigured Access Points –** When valid APs are found that violate the list of allowable parameters, prevents clients from associating to those APs using a denial of service attack.

Valid Enterprise 802.11 b/g Channels – Defines the list of valid 802.11b/g channels that 3<sup>rd</sup>-party APs are allowed to use.

Valid Enterprise 802.11a Channels–Defines the list of valid 802.11a channels that 3<sup>rd</sup>-party APs are allowed to use.

#### Enforce Short Preamble as invalid AP configuration-TBC

**Prevent valid clients from roaming to interfering APs –** If a valid enterprise client attempts to associate with an AP classified as "interfering", the system will break the association using a denial of service attack.

**Enforce WEP Encryption for all Traffic –** Any valid AP not using WEP will be flagged as misconfigured.

**Enforce WPA Encryption for all Traffic –** Any valid AP not using WPA will be flagged as misconfigured.

Valid Access Point Manufacturers OUI List – A list of MAC address OUIs that define valid AP manufacturers. Any valid AP with a differing OUI will be flagged as misconfigured.

Equivalent CLI configuration for the example above is:

```
wms
ap-policy protect-misconfigured-ap enable
valid-11b-channel 6 mode enable
valid-11b-channel 1 mode enable
valid-11b-channel 11 mode enable
valid-11a-channel 36 mode enable
valid-11a-channel 60 mode enable
valid-11a-channel 52 mode enable
valid-11a-channel 64 mode enable
valid-11a-channel 48 mode enable
valid-11a-channel 44 mode enable
valid-11a-channel 40 mode enable
valid-11a-channel 56 mode enable
station-policy protect-valid-sta enable
ap-config privacy enable
ap-config wpa disable
```

### Entering New Valid OUIs

To add a new valid OUI, click the Add button. Specify all MAC OUIs in the form:

xx:xx:ff:ff:ff

where xx:xx:xx is the desired OUI.

## Weak WEP Detection

The primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. Most modern 802.11 devices do not generate such weak IVs, but many legacy devices are still in use today that do. AOS-W will monitor for devices using weak WEP implementations and generate reports for the administrator of which devices require upgrades. To



configure detection of weak WEP implementations, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Weak WEP**, as shown in the figure below.



### FIGURE 15-15 Weak WEP Detection

Equivalent CLI configuration for the example above is:

wms global-policy detect-bad-wep enable

## **Multi-Tenancy Policies and Honeypot Defense**

AOS-W provides the ability to configure reserved channel and SSID lists, and disable unrecognized APs using these reserved resources. This feature can be used in a multi-tenant building where different enterprises must share the RF environment. This feature can also be used to defend against "honeypot" APs. A "honeypot" AP is an attacker's AP that is set up in close proximity to an enterprise, advertising the ESSID of the enterprise. The goal of such an attack is to lure valid clients to associate to the honeypot AP. From that point, a MITM attack can be mounted, or an attempt can be made to learn the client's authentication credentials. Most client devices have no way of distinguishing between a valid AP and an invalid one – the devices only look for a particular ESSID and will associate to the nearest AP advertising that ESSID. To configure multi-tenancy policies, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Multi Tenancy**, as shown in the figure below.

Multi Tanangu	
Multi-renancy	
Disable Access Points Violating Enterprise SSID List	
Valid Enterprise SSID List	Add Delete
Disable Access Points Violating Channel Allocation Agreements	
Reserved Enterprise 802.11b/g Channels	☑ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11
Reserved Enterprise 802.11a Channels	□ 36 □ 40 □ 44 □ 48 □ 52 □ 56 □ 60 □ 64 □ 149 □ 153 □ 157 □ 161 □ 165

### FIGURE 15-16 Multi-Tenancy Configuration

Available parameters are:

**Disable APs Violating Enterprise SSID List** – When an unknown AP is detected advertising a reserved SSID, the AP will be disabled using a denial of service attack.

Valid Enterprise SSID List - A list of reserved SSIDs.

**Disable APs Violating Channel Allocation Agreements –** When an unknown AP is detected using a reserved channel, the AP will be disabled using a denial of service attack.

Reserved Enterprise Channels - A list of reserved channel numbers.

The equivalent CLI configuration for the example shown above is:

```
wms
ap-policy protect-mt-ssid enable
valid-ssid OurSSID mode enable
ap-policy protect-mt-channel-split enable
reserved-11b-channel 1 mode enable
```

## MAC OUI Checking

AOS-W provides the ability to match MAC addresses seen in the air with known manufacturers. The first three bytes of a MAC address are known as the MAC OUI (Organizationally Unique Identifier) and are assigned by the IEEE. Often, clients using a spoofed MAC address will not use a valid OUI, and instead use a randomly generated MAC address. By enabling MAC OUI checking, administrators will be notified if an unrecognized MAC address is in use. To enable MAC OUI checking, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > MAC OUI**, as shown in the figure below.





FIGURE 15-17 MAC OUI Checking

Available parameters are:

Enable MAC OUI Check - Enables or disables the feature.

**MAC OUI Quiet Time** - After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

The equivalent CLI configuration for the example shown above is:

wms
ids-policy mac-oui-check enable
ids-policy mac-oui-quiet-time 900

# CHAPTER 16 Authentication Server Configuration

## Introduction

Strong authentication methods use authentication servers as the basis of their methodology. Alcatel switches allow you to use either an internal authentication database or an external RADIUS or LDAP server.

Authentication provides a way to identify a user and provide appropriate network access to that user. By default, all wireless users on an Alcatel network begin in the logon role. The users role is reassigned after authenticating, and the role is sometimes dependent upon what kind of authentication was used.

Begin configuring authentication servers by navigating to the **Configuration > Security > AAA Servers > General** page.

Switch	Security > AAA Servers > General
Management	
WLAN	General Radius LDAP Internal DB Accounting
Network	Authentication Timers
Radio	
Advanced	
RF Spectrum Mgmt	User Idle Timeout (minutes) 5
Calibration	Authentication Server Dead Time (minutes) 10
Optimization	Apply
Protection	
Monitoring	
Security	Commands View Commands
Roles	

You may configure 2 general parameters here, they are:

•	User Idle Timeout	Sets the maximum time, in seconds, that a user may be idle before the user is deauthenticated and dropped from the system. The default is 5 minutes.
•	Authentication Server Deat Time	Sets the maximum amount of time, in minutes, that an authentication server may remain unresponsive before it is considered down.

## **Configuring RADIUS Servers with Web UI**

RADIUS authentication servers are the most often used servers. They are flexible, extensible, and possess a high degree of interoperability.

Configure a RADIUS server using Web UI by navigating to the **Configuration > Security > AAA Servers > Radius** page.

Switch	Security >	AAA Se	rvers > Radius	Servers			
Management WLAN	General	Radius	LDAP Internal DB	Accounting	_	_	
Network	Name	IP Address	Authentication Port	Accounting Port	Status	A	ction
Radio	rad-radius-server	192.168.200.1	1812	1813	Enabled	Edit	Delete
Advanced	Add	_		_	_	_	_
RF Spectrum Mgmt	-						

The RADIUS Servers page displays all the currently configured RADIUS servers. You may use the Edit and Delete buttons to change the configuration or delete it all together. Add a new server by clicking the Add button.

The Add RADIUS Server page appears. Enter information about a RADIUS server on this page then click **Apply** and **Save** configuration when you are finished.

Add	Un
Server Rules Bule Action Attribute Condition Matching Value Value Acti	ion
Mode	Enable 😪
frim FQDN	
Match FQDN	Add Delete
Match ESSID	Add Delete
Fimeout	5
Vum Retries	3
Accounting Port	1813
Authentication Port	1812
/erify Shared Secret	
Shared Secret	
IP Address	
Server Name	

The following parameters and options may be configured through Web UI.

Server Name	A plain language meaningful name for the RADIUS server.
IP Address	The IP address of the RADIUS server.
Shared Secret	The secret work (password) shared between the client and the server.
Verify Shared Secret	твс



Authentication Port	Specifies the UDP port used for RADIUS exchanges.
Accounting Port	Specifies the UDP port used for RADIUS accounting, when it is enabled.
Num Retries	The maximum number the Alcatel switch will issue authentication requests without receiving a reply.
Timeout	The maximum time, in seconds, that the switch will wait for a response from the RADIUS server after each authentication request is transmitted.
Match ESSID	ТВС
Match FQDN	ТВС
Trim FQDN	ТВС
Mode	This parameter enables or disables the RADIUS server.

## **Server Rules**

Server rules may be defined for each server to determine role and VLAN assignments. Multiple rules may be defined for each server and each is executed in order.

Server rules are displayed at the bottom of the Edit RADIUS Server page.

Monitoring Security	Num Retries	3
Roles	Timeout	5
Policies	Mode	Enable -
AAA Servers Authentication Methods VPN Settings Advanced	Server Rules Rule Action Attribute Condition Matching Value Value Action Add	Anniv
WLAN Intrusion Detection		
Denial of Service	Commands	<u>View Commands</u>

Add a rule by clicking the add button.

Rule Type	Role Assignment 💌	
Attribute	Aruba-Admin-Role Aruba-Priv-Admin-User Aruba-User-Vlan Aruba-Vlan	
Add Att	ribute Delete Attribute	
Condition	contains 💌	
Value		
Role/Vlan	ap-role 💟	
	Done	

The following parameters may be configured for server rules using Web UI:

Rule Type	Sets the rule type to either a role assignment or a VLAN assignment rule.
Attribute	Specifies which RADIUS attribute to examine for the value.
Condition	Specifies how the rule will match the attribute information to the specified value.
Value	Specifies the value for which the rule will test the specified attribute.
Role/VLAN	Specifies the role or VLAN to be assigned to the user if the rule tests true.

### **Configuring Attributes**

To add an attribute, from the Add Server Rule page click Add Attribute. The following screen appears.



Rule Type	Role Assignment 💌	
Attribute	Aruba-Admin-Role Aruba-Priv-Admin-User Aruba-User-Vlan Aruba-Vlan	×
Add Att	ibute Delete Attri	bute
Attribute Na	ne	
Attribute ID		
Attribute Ty	oe Date 💌	
Vendor Nam	•	
Vendor ID		
	Done Cance	.1
Condition	contains 💌	
Value		
Role/Vlap	ap-role	

where:

Attribute Name TBC

Attribute ID TBC

Attribute Type TBC

Vendor Name TBC

Vendor ID TBC

# **Configuring LDAP Servers with Web UI**

Alcatel switches allow for authentication using LDAP servers. Configure LDAP servers from the **Configuration > Security > AAA Servers > LDAP** page in Web UI

Switch	Security	> AAA Se	ervers > LDAP	Server	's
Management					
WLAN	General	Radius	LDAP Internal DB	Acco	unting
Network	Name	HostName	Authentication Port	Status	Action
Radio	Horseradish_1	192.168.200.25	0 389	Enabled	Edit Delete
Advanced	Add				

You may add, edit, or delete an LDAP server from the LDAP page. When the Add or Edit button is clicked the following page is displayed.

Server Name		
Is Server Active Directory		
IP Address		
Authentication Port		
Base DN		
Admin DN		
Admin Password		
Verify Admin Password		
Key Attribute		
Filter		
Timeout		
Mode		Enable 🐱
Server Rules		
Rule Type Attribute Condition Matchin	g Value Value Action	

Server Name

A plain language name to identify the server.



TBC
The IP address of the LDAP server.
The port on which the server is configured. Default=389.
The Distinguished Name of the node containing the entire user database to be used for user authentication.
The name of the user who has read/search privileges across all entries in the LDAP database.
The password for the Admin defined in Admin DN.
Reenter the password entered for Admin Password.
The attribute containing the unique key for the LDAP object.
The filter to apply to searches for users in the LDAP database.
The amount of time, in seconds, an LDAP may go unanswered before the server is considered "down".
Enables or disables the server.

## Adding a Server Rule

To add a server rule, click **Add** on the Add LDAP Server page. The following screen displays.

#### Security > AAA Servers > Add LDAP Server > Add Server Rule Rule Type Role Assignment 💟 Attribute Condition Y contains contains Value ends-with equals Role/Vlan × not-equals starts-with Done value-of

where:

### Rule type is Role Assignment or Vlan Assignment.TBC

Attribute is TBC

Condition is TBC

Value is TBC

Role/Vlan is TBC



## **Configuring the Internal Authentication Database with Web UI**

Alcatel AOS-W supports an internal authentication database. The internal database is available with using VPN, Captive Portal, or MAC based authentication, it is not usable for 802.1z type authentication.

You may configure the internal database by navigating to the **Configuration >** Security > AAA Servers > Internal DB page.

General	Radius	LDAP	LDAP Internal DB			unting		
Server Rules								
Rule Action	Attribut	e Condi	ition M	latching	Value	Value	Action	
Role Assignm	ent Role	value-	of				Delete	•
Add								
Maintenanco	è							
Export Import Delete All Users Repair Databa							;e	
Users								
User Name	Password	Role E	-mail	Enabled	Expiry	/ Actio	n	

The internal database enables you to store information for user name, password, role, and email.

You may also allow the switch to configure the role or you may create additional role or VLAN assignments using the interface on this page.

Maintenance information TBC

# **Configuring RADIUS Accounting with Web UI**

Alcatel AOS-W supports RADIUS accounting, tracking login and logout times.

Configuration of RADIUS accounting is done by navigating to the **Configuration > Security > AAA Servers > Accounting** page.

Switch	Security >	> AAA Sei	rvers > Acco	untin	g		
WLAN	General	Radius	.DAP Internal I	DB Ad	counting		
Network	Enable Accountin	ng 🗖					
Radio		_			_		
Advanced	Name	IP Address	Accounting Port	Status	Actions		
RF Spectrum Mgmt Calibration	rad-radius-server	192.168.200.1	1812	Enabled	Delete		
Optimization	Add	_		_	_		
Protection							
Monitoring							Apply
Security Roles	Commands					<u>View Commands</u>	

Add configured servers by clicking **Add** then selecting a server from the pull-down menu.



# Configuring 802.1x Authentication with Web UI

802.1x authentication is designed to provide authentication before the user is granted any Layer 2 access to the network, and provides a framework in which multiple authentication protocols may be employed.

Several protocols are well suited for wireless networks and include:

- EAP-TLS
- PEAP
- TTLS

Begin configuring 802.1x Authentication by navigating to the **Configuration > Security> Authentication Methods > 802.1x** page.

802	1x	VPN	Canti	ve Portal	MAC AN	dress	Stateful 802.1x	SSID	1.2 Encryption	Advanced		
002.	1/	VI 14	Caba	ver er er er			0000101002.11	0010	Le cheryption	Aurancea		
Default	Role er	nployee	~	Ĩ								
Enable Authentication												
Enable Reauthentication					Г							
Enable (	Opportuni	stic Key (	Caching (	(WPA2)	Г							
Enforce	Machine	Authentic	ation		F							
Machine	Authenti	cation De	fault Ro	le	gu	guest						
User Au	thenticati	on Defau	lt Role		gu	iest	~					
Authent	ication Fa	ilure Thr	eshold fo	or Station Blac	klisting 0	(O dis	ables blacklisting)					
Advanc	ed Con	figurat	ion									
Auther	nticatio	n Serve	ers									
Name	Туре	IP Ad	dress	Authentic	ation Port	Status	Actions					
adon	Radius	10.4.0.	21	1812		Enabled	Delete 🔺 🔻					
add							Apply					

You may choose to enable 802.1x Authentication with a minimum of effort. Follow the steps below.
- 1 Click the Enable Authentication checkbox.
- 2 Select a default role from the pull-down menu
- 3 Add an authentication server using the ADD button at the bottom of the page.

The following options/features may be configured for 802.1x authentication using Web UI:

Default Role	The default role assigned to an 802.1x authenticated client if the role is not provided by the server.
Enable authentication	Enables/disables 802.1x authentication.
Enable Opportunistic Key Caching (WPA2)	ТВС
Enforce Machine Authentication	ТВС
Machine Authentication Default Role	ТВС
User Authentication Default Role	ТВС
Authentication Failure Threshold for Station Blacklisting	Specifies the number of time a station may fail 802.1x authentication before it is placed on a blacklist and not allowed to authenticate.
	Enter 0 to disable blacklisting.



# **Configuring VPN Authentication with Web UI**

Alcatel switches provide full VPN termination capabilities, using hardware acceleration. All encryption protocols are executed in hardware, with the hardware sized appropriately to handle a full compliment of access points.

Configure VPN authentication by navigating to the **Configuration > Security > Authentication Method > VPN** page.

-			
Switch	Security > Authenticati	ion Methods > VPN Authentic	ation
Management			
WLAN	802.1x VPN Captive Port	tal MAC Address Stateful 802.1x	SSID L2 Encryption
Network			
Radio	Authentication Enabled		
Advanced	Defeate Dele	a such	
RF Spectrum Mgmt	Derault Role	guest	
Calibration	Authentication Failure Threshold for Statio	n Blacklisting 0 (0 disables blacklisting)	
Optimization			
Protection	Authoratication Servers		
Monitoring	Authentication betvers		
Security	Name Type IP Address Auth	entication Port Status Actions	
Roles	Internal Local 192.196.10.1 n/a	Enabled Delete 🔺 🔻	
Policies	Add	Apply	
AAA Servers	_		
Authentication Methods			
VPN Settings	Commands	View Comman	ds
Adversed			

You may configure the following VPN options and parameters using Web UI.

Authentication Enabled	Check or uncheck this box to enable or disable VLAN Authentication.
Default Role	Use this pull-down menu to select the default role for the client when authenticated. This role is assigned if the authentication server does not provide role information.
Authentication Failure Threshold for Station Blacklisting	Specifies the number of time a station may fail authentication before it is placed on a blacklist and not allowed to authenticate.
	Enter 0 to disable blacklisting.
Authentication Servers	Use the Add button to create ordered list of authentication servers.

# Configuring Captive Portal Authentication with Web UI

Alcatel switches provide the ability to allow wireless users to authenticate through a web-based portal. Captive portal authentication may be completed over an SSL connection, however it provides no security for user data after authentication has occurred. Captive Portal authentication should only be used in environments where encryption id not required.

Configure Captive Portal Authentication by navigating to the **Configuration >** Authentication Methods > Captive Portal page.

Authentication Enabled Procedure row of an inverse statistic doz. 12 SSD L2 End youth Authentice Authentication Enabled Enable Guest Logon Enable User Logon Enable Logout Popup Window Protocol Type Redirect Pause Time(secs) 10 Welcome Page Location Logon Wait Interval Compared to the statistic for Station Blacklisting Show FQDN List Capture Three Redirect Pause Times (Secs) Authentication Failure Threshold for Station Blacklisting Show FQDN List Capture Three Redirect Pause Times (Secs) Show FQDN List Capture Threshold For Station Blacklisting Show FQDN List Capture Three Redirect Pause Times (Secs) Capture Threshold For Station Blacklisting Compared For Station Blacklisting Capture Threshold For Station For Stat	202	1v	VPN C:	ontivo Portal	MAC Ad	frace	Stateful 902 1v	COL	1.2 Encryption	Advancer
Authentication Enabled   Default Role   employee   Enable Guest Logon Enable Logout Popup Window Fotocol Type C http      https Redirect Pause Time(secs) C http      https Redirect Pause Time(secs) I0 Vetcome Page Location Vetcome Page Location Vetcome Page Location Vetcome Page Location C U Utilization Threshold C U Utilization Threshold Foto Station Blacklisting Show FQDN List	002.	TV		apuve rortar	MAC AU	ui ess	Staterur 002.1X	3310		Auvanceu
Default Role mployee ▼ Enable Guest Logon □ □ Enable Guest Logon □ □ Enable User Logon □ □ □ Enable Logout Popup Window □ Fotocol Type □ □ □ □ □ Redirect Pause Time(secs) □ □ □ Welcome Page Location □ /auth/welcome.html Logon Wait Interval □ □ □ 0 (0 disables blacklisting) Show FQDN List □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Authent	ication Er	nabled 🔽							
Enable Guest LogonImage: Comparison of the comparison of th	Default	Role	emp	loyee 🔽						
Enable User LogonIEnable Logout Popup WindowIProtocol TypeC http f httpsRedirect Pause Time(secs)10Welcome Page Location/auth/welcome.htmlLogon Wait Interval5 - 10 secondsCPU Utilization Threshold For Station Blacklisting0 (0 disables blacklisting)Show FQDN ListI	Enable (	Guest Log	on		Γ					
Enable Logout Popup Window       I         Protocol Type       C http C https         Redirect Pause Time(secs)       10         Welcome Page Location       /auth/welcome.html         Logon Wait Interval       5 - 10 seconds         CPU Utilization Threshold       60 %         Authentication Failure Threshold for Station Blacklisting       0 (0 disables blacklisting)         Show FQDN List       I	Enable (	Jser Logo	n		~					
Protocol Type     C http f https       Redirect Pause Time(secs)     10       Welcome Page Location     /auth/welcome.html       Logon Wait Interval     5 - 10 seconds       CPU Utilization Threshold     60 %       Authentication Failure Threshold for Station Blacklisting     0 (0 disables blacklisting)       Show FQDN List     Image: Page Page Page Page Page Page Page Page	Enable L	.ogout Po	pup Window		~					
Redirect Pause Time(secs)     10       Welcome Page Location     /auth/welcome.html       Logon Wait Interval     5 - 10 seconds       CPU Utilization Threshold     60 %       Authentication Failure Threshold for Station Blacklisting     0 (0 disables blacklisting)       Show FQDN List	Protoco	Туре			C	http 📀 ht	tps			
Welcome Page Location     /auth/welcome.html       Logon Wait Interval     5 - 10 seconds       CPU Utilization Threshold     60 %       Authentication Failure Threshold for Station Blacklisting     0 (0 disables blacklisting)       Show FQDN List <ul> <li>Image: Comparison of the state of</li></ul>	Redirect	: Pause Ti	me(secs)		10					
Logon Wait Interval     5     - 10     seconds       CPU Utilization Threshold     60     %       Authentication Failure Threshold for Station Blacklisting     0     (0 disables blacklisting)       Show FQDN List     •     •	Welcom	e Page Lo	cation		/au	th/welco	me.html			
CPU Utilization Threshold     60 %       Authentication Failure Threshold for Station Blacklisting     0 (0 disables blacklisting)       Show FQDN List	Logon V	vait Inter	val		5	- 10	seconds			
Authentication Failure Threshold for Station Blacklisting     0     (0 disables blacklisting)       Show FQDN List	CPU Util	ization Th	reshold		60	ı_%				
Show FQDN List	Authent	ication Fa	ailure Thresho	ld for Station Bla	cklisting 0	(0 dis	ables blacklisting)			
	Show F	QDN List			F					
	Authe	nticatio	n Servers							
Authentication Servers	Name	Туре	IP Addre	ss Authentic	ation Port	Status	Actions			
Authentication Servers           Name         Type         IP Address         Authentication Port         Status         Actions	adon	Radius	10.4.0.21	1812		Enabled	Delete 🔺 🔻			
Authentication Servers       Name     Type     IP Address     Authentication Port     Status     Actions       adon     Radius     10.4.0.21     1812     Enabled     Delete     *	hdd						Apply			

The following options and parameters may be configured using Web UI.

Authentication Enabled

Check or uncheck this box to enable or disable Captive Portal Authentication.



Default Role	Use this pull-down menu to select the default role for the client when authenticated. This role is assigned if the authentication server does not provide role information.
Enable Guest Logon	When selected, this option enables the display of a guest user field where the user may enter their email address as a user ID. The email address is not authenticated or validated, but it is tracked.
Enable User Logon	When selected, this option enables the display of a registered user field wherein the user may enter their user ID and Password.
Enable Logout Popup Window	When selected, this option enables a second small browser window to appear, facilitating a single click logout by the user.
Protocol Type	Use the radio buttons to select the browser protocol type, HTTP or HTTPS. If HTTP is selected user names and passwords are NOT encrypted.
	Default = HTTPS
Redirect Pause Time	The length of time in seconds during which the browser will display the "Authorization Succeeded" page containing additional options do download the VPN dialer. After the pause the browser will be redirected to the originally requested URL.
Logon Wait Interval	This parameter specifies the maximum time the logon process will be delayed if the CPU is occupied with a large load of high priority traffic.
CPU Utilization Threshold	This parameter specifies the CPU load which must be exceeded before a captive portal delay takes effect.

Authentication FailureThreshold for Station Blacklisting	Specifies the number of time a station may fail authentication before it is placed on a blacklist and not allowed to authenticate.
	Enter 0 to disable blacklisting.
Authentication Servers	Use the Add button to create ordered list of authentication servers.
Show FQDN List	ТВС



# Configuring MAC Address Role Mapping with Web UI

MAC Address role mapping provides identification and role mapping based on the Client MAC Address. This feature should not be considered an authentication method because no secure password is employed. This feature should ALWAYS be combined with L2 encryption and appropriate firewall policies.

Configure MAC Address Role Mapping by navigating to the **Configuration > Security > Authentication Methods > MAC Address** page.

Switch	Security > Authentication Methods > MAC Authentication
Management WLAN Network	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption
Radio	Authentication Enabled
Advanced	Default Role guest
RF Spectrum Mgmt Calibration	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Optimization	
Protection	Authentication Servers
Monitoring	Name Type IP Address Authentication Port Status Actions
Security Roles	Internal Local 192.196.10.1 n/a Enabled Delete
Policies	Add
AAA Servers	

The following options and parameters may be configured with Web UI.

Authentication Enabled	Check or uncheck this box to enable or disable MAC Address Role Mapping.
Default Role	Use this pull-down menu to select the default role for the client when authenticated. This role is assigned if the authentication server does not provide role information.
Authentication Failure Threshold of Station Blacklisting	Specifies the number of time a station may fail authentication before it is placed on a blacklist and not allowed to authenticate.
	Enter 0 to disable blacklisting.
Authentication Servers	Use the Add button to create ordered list of authentication servers.

# Configuring Stateful 802.1x for Third Party Access Points

This feature allows the switch to intercept communications between third-party APs and the authentication server so that it can learn the username and apply appropriate role and traffic policies. This assumes that the Alcatel switch is located in the datapath between the AP and the authentication server.

Configure Stateful 802.1x by navigating to **Configuration > Security >** Authentication Methods > Stateful 802.1x.

Switch Management	Security > Authentication Methods > Stateful 802.1x Authentication
Network	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption
Radio	
Advanced	Authentication Enabled
RF Spectrum Mgmt Calibration	Default Role guest
Optimization	Request/Response timeout 30
Protection	
Monitoring	Authoritization Contorn
Security	Authentication Servers
Roles	Name Type IP Address Authentication Port Status Actions
Policies	rad-radius-server Radius 192.168.200.1 1812 Enabled Delete *
AAA Servers	Add

The following options and parameters may be configured with Web UI.

Authentication Enabled	Check or uncheck this box to enable or disable stateful 802.1x authentication.
Default Role	Use this pull-down menu to select the default role for the client when authenticated. This role is assigned if the authentication server does not provide role information.
Request/Response Timeout	Specifies the maximum wait time for a response from the RADIUS server after seeing a RADIUS request from the AP.
Authentication Servers	Use the Add button to create ordered list of authentication servers.



# **Role Mapping**

From the Web UI, you can perform role mapping based on SSID and encryption. These two methods are discussed in the following sections. From the CLI, you can perform role mapping on BSSID, location, and MAC address in addition to SSID and encryption. To access role mapping from the CLI, enter:

```
(OmniAccess 6000) (config) #aaa derivation-rules user
(OmniAccess 6000) (user-rule) #?
no
                        Delete Command
set
                        The action for the rule
(OmniAccess 6000) (user-rule) #set ?
role
                       The action of the rule is to set to role
vlan
                       The action of the rule is to set to vlan
(OmniAccess 6000) (user-rule) #set role condition ?
bssid BSSID of access point
encryption-type Encryption method used by station
essid
                       ESSID of access point
location
                       location of user in building.floor.location format
                       MAC address of user
macaddr
```

### **SSID Role Mapping**

This feature enables roles to be assigned based solely on the ESSID to which a client associates.

This method of role assignment bypasses authentication and should therefore be combines with a strong firewall policy.

Configure SSID Role Mapping by navigating to the **Configuration > Authentication Methods > SSID** page.

Switch	Securit	v > Authent	tication N	lethods > S	SID Authen	ticatior	ı
Management							
WLAN	802.1x	VPN Capt	ive Portal	MAC Address	Stateful 802.1x	SSID	L2 Encryption
Network	Condition	Matching Value	Role Name	Actions		-	
Radio	SSID equals	MYFOOESSID	foo-user	Delete 🔺 🔻			
Advanced	Add						
RF Spectrum Mgmt							
Calibration	_						
Optimization							

Adding a Role Map

- 1 Click Add.
- Select a match condition from the Condition pull-down menu box.
- 3 Enter a value for the ESSID you wish to match to a role.
- 4 Select a role from the Role Name pull-down menu box.

### **Encryption Type Role Mapping**

This feature enables roles to be assigned based solely on the Layer 2 encryption type used by the client.

This method of role assignment bypasses authentication and should therefore be combines with a strong firewall policy.

Configure SSID Role Mapping by navigating to the **Configuration >** Authentication Methods > L2 Encryption page.

Switch Management	Security > Au Authenticatio	ithentication I	Methods > L	2 Encryption	1	
WLAN						
Network	802.1x VPN	Captive Portal	MAC Address	Stateful 802.1x	SSID	L2 Encryption
Radio	Condition	Value Role Nan	ne Actions			
Advanced	Encryption Type equals	Dynamic WEP foo-user	Delete 🔺 🔻			
RF Spectrum Mgmt Calibration	Add					

# **Configuring Advanced Conditions**

This feature enables TBC.

Configure SSID Role Mapping by navigating to the **Configuration > Authentication Methods >Advanced** page.

recourtey r	- Autu	entica	ation Me	thods >	Advanced Au	thenti	cation	
802.1x	VPN	Captive F	Portal M	AC Address	Stateful 802.1x	SSID	L2 Encryption	Advanced
Rule Type (	Condition	Value	Role Name	Actions				



### Adding a Condition

### твс

Securit	y > Authentio	cation Methods	> Advanced	Authentication	> Add Condition
Rule Type	Mac Address 💌				
Condition	equals 💌				
Value					
Role Name	ap-role 💌				
Apply					

where:

Rule Type-specifies what rule will apply such as on MAC addresses, BSSIDs, or location.

Condition-specifies how the rule type is treated, for example a MAC address equal to a value.

Value-specifies the value of the condition, for example when location is not equal to Headquarters.

Role Name is the name of the role affected by the condition.

When you finish defining the condition, click **Apply**.

# **Configuring General AAA Settings Using the CLI**

Configure the general AAA settings using the aaa timers command

```
(Alcatel) (config) #aaa timers idle-timeout 5
(Alcatel) (config) #aaa timers dead-time 10
```

View the general authentication server settings using the show aaa timers command.

```
(Alcatel) (config) #show aaa timers
User idle timeout = 5 minutes
Auth Server dead time = 10 minutes
```

# **Configuring RADIUS Servers Using the CLI**

Configure RADIUS servers using the aaa radius-server command.

```
(Alcatel) (config) #aaa radius-server rad2-radius-server
(Alcatel) (config) #aaa radius-server rad2-radius-server host
192.168.200.2
(Alcatel) (config) #aaa radius-server rad2-radius-server authport
1812
(Alcatel) (config) #aaa radius-server rad2-radius-server acctport
1813
(Alcatel) (config) #aaa radius-server rad2-radius-server key
AbcdE12345
(Alcatel) (config) #aaa radius-server rad2-radius-server retransmit 3
(Alcatel) (config) #aaa radius-server rad2-radius-server timeout 5
(Alcatel) (config) #aaa radius-server rad2-radius-server timeout 5
(Alcatel) (config) #aaa radius-server rad2-radius-server mode
"enable"
```



The configured RADIUS server settings may be viewed using the show aaa radius-server server-name <*name*> command.

### **Server Rules**

Define server rules for deriving roles or VLANS using the aaa derivation-rules command from the CLI.

Enter the server-rule sub-mode using the aaa derivation-rules <ServerName> command.

```
(Alcatel) (config) #aaa derivation-rules server rad2-radius-server
(Alcatel) (server-rule) #
```

Define the rules using the form

set [role] vlan] condition <Attribute> <CONDITIONAL> <value> set-value [RoleName | VLAN]

Conditionals:

- contains
- ends-with
- equals
- not-equals
- starts-with
- value-of

```
(Alcatel) (server-rule) #set role condition User-Name contains foo set-value foo-user
```

You may view the rule you create using the show aaa derivation-rules command from the CLI.

# **Configuring LDAP Servers Using the CLI**

Configure LDAP servers using the aaa ldap-server command from the CLI.



Enter the config-Idapserver submode by executing the aaa ldap-server command with the name of the server you wish to configure as the argument.

```
(Alcatel) (config) #aaa ldap-server horseradish_2_ldap
(Alcatel) (config-ldapserver-horseradish 2 ldap)#
```

2 Enter the LDAP server's IP address.

```
(Alcatel) (config-ldapserver-horseradish_2_ldap)#host
192.168.200.251
```

3 Specify the authentication port number.

```
(Alcatel) (config-ldapserver-horseradish 2 ldap) #authport 389
```

4 Specify a base distinguished name under which the server to search for all users.

```
(Alcatel) (config-ldapserver-horseradish_2_ldap)#base-dn "cn=Users,
dc=lm, dc=Alcatelnetworks, dc=com"
```

5 Specify an admin distinguished name to establish the user with administrative rights.

```
(Alcatel) (config-ldapserver-horseradish_2_ldap)#admin-dn
"cn=Users, dc=lm, dc=Alcatelnetworks, dc=com"
```

6 Specify the admin password.

```
(Alcatel) (config-ldapserver-horseradish_2_ldap)#admin-passwd
ABC123
```

7 Specify the key attribute to use when searching for the server.

(Alcatel) (config-ldapserver-horseradish\_2\_ldap)#key-attribute sAMAaccountName

8 Select a filter

```
(Alcatel) (config-ldapserver-horseradish-2-ldap)#filter
"(objectclass=*)"
```

#### 9 Set the server timeout in seconds.

(Alcatel) (config-ldapserver-horseradish-2-ldap) #timeout 20

Set the mode, enable or disable LDAP.

(Alcatel) (config-ldapserver-horseradish-2-ldap) #mode enable

View the LDAP server settings using the show aaa ldap-server <*Name*> command from the CLI.

(Alcatel) (config) # sl	now aaa ldap-server horseradish_2_ldap
LDAP Server Table	
LDAP Server Attribute V	Value
Priority	5
Name	horseradish_2_ldap
Hostname	192.168.200.251
AuthPort	389
Retries	3
Timeout	20
AdminDN	cn=Users, dc=lm, dc=Alcatelnetworks, dc=com
AdminPasswd	****
BaseDN	cn=Users, cd=lm, dc=Alcatelnetworks, dc=com
KeyAttribute	sAMAaccountName
Filter	(objectclass=*)
Status	Enabled
InService	no
InitDone	no
AdminBound	no
Marked For Delete	no
In Use Callback Set	no
RefCount	0
RebindTimerSet	yes
RebindCount	19

### **Server Rules**

The steps and commands for deriving roles and VLANs for LDAP are exactly the same as for RADIUS servers, above.



Authentication Server Configuration | 353

10

# **Configuring the Internal Authentication Database Using the CLI**

An internal authentication database may be configured using the local-userdb command from the CLI. Users are added to the local database from the command rather than the configuration prompt.

```
(Alcatel) #local-userdb add username NewGuy password NewFoo role
foo-user
```

Users may be deleted using the local-userdb delete option from the CLI.

```
(Alcatel) #local-userdb del username foolishGuy
```

The users in the local database may be viewed using the show local-userdb command from the CLI.

```
(Alcatel) #show local-userdb
User Details
_____
      Password Role E-Mail Enabled
Name
____
       _____ _
                       _____ ____
       ******* foo-user
NewGuy
                              Yes
OldGuy
       ******* foo-user
                             Yes
BIGGuy
       ******* foo-user
                             Yes
Peonski ******* foo-user
                            Yes
User Entries: 4
```

# Configuring RADIUS Accounting Using the CLI

Configure RADIUS accounting using the aaa radius-accounting command from the CLI.



#### 1 Enable RADIUS accounting

(Alcatel) (config) #aaa radius-accounting mode enable



Assign an accounting server.

```
(Alcatel) (config) #aaa radius-accounting auth-server rad2-radius-server
```

### Configuring 802.1x Authentication Using the CLI

802.1x configuration is accomplished using 2 families of commands from the CLI, the aaa general accounting commands and the dotlx commands.

 Select a default role for users authenticating through 802.1x. This is the role that will be assigned unless the authentication server provides another role for the user.

(Alcatel) (config) #aaa dot1x default-role foo-user

2 Enable or disable 802.1x authentication.

(Alcatel) (config) #aaa dot1x mode enable

3 Set the authentication server timeout, in seconds. (1 - 65535)

(Alcatel) (config) #dot1x server server-timeout 30

4 Set the authentication failure timeout, in seconds. (1-65535)

(Alcatel) (config) #dot1x timeout idrequest-period 30

5 Set the quiet time (time between authentication attempts), in seconds (1 - 65535).

(Alcatel) (config) #dot1x timeout quiet-period 30

Set the maximum number of authentication attempts (1 - 10).

```
(Alcatel) (config) #dot1x max-req 5
```

7 Set the maximum number of attempts to contact the server before it is considered down (0 - 3)

(Alcatel) (config) #dot1x server server-retry 3





(Alcatel) (config) #dot1x re-authentication (Alcatel) (config) #no dot1x re-authentication

9 Set the reauthentication time interval, in seconds (60-2147483647). You may also specify that the interval provided by the server be used.

```
(Alcatel) (config) #dot1x timeout reauthperiod 3600
```

#### 10 Enable multicast key rotation.

```
(Alcatel) (config) #dot1x multicast-keyrotation
```

1) Set the multicast key rotation interval, in seconds (60-2147483647).

(Alcatel) (config) #dot1x timeout mcastkey-rotation-period 1200

#### 12 Enable unicast key rotation.

(Alcatel) (config) #dot1x unicast-keyrotation

13 Set the unicast key rotation interval, in seconds (5-2147483647)

(Alcatel) (config) #dot1x timeout ucastkey-rotation-period 240

**14** Set the authentication failure threshold for station blacklisting

(Alcatel) (config) #aaa dot1x max-authentication-failures 0

You may view the 802.1x configuration settings using the show aaa dot1x command from the CLI.

```
(Alcatel) (config) #show aaa dot1x
Mode = 'Enabled'
Default Role = 'foo-user'
Max authentication failures = 0
Auth Server Table
_____
Pri Name Type IP addr AuthPort Status Inservice Applied Users
 (Alcatel) (config) #show dot1x ?
                      Show 802.1X AP Table
ap-table
config
                     Show 802.1X Authenticator Configuration
supplicant-info Show details about supplicant(s)
(Alcatel) (config) #show dot1x config
Authentication Server Timeout: 30 Seconds
 Client Response Timeout: 30 Seconds
 Fail Timeout: 30 Seconds
 Client Retry Count: 5
 Server Retry Count: 3
 Key Retry Count: 1
 Reauthentication: Disabled
 Reauthentication Time Interval: 3600 Seconds
 Multicast Key Rotation: Enabled
 Multicast Key Rotation Time Interval: 1200 Seconds
 Unicast Key Rotation: Enabled
 Unicast Key Rotation Time Interval: 240 Seconds
 Countermeasure: Disabled
 Wired Clients: Disabled
 Enforce Machine Authentication: Disabled
Machine Auth Cache Timeout: 24 Hours
 Machine Auth Default Role: guest
 User Auth Default Role: guest
```



### Adding 802.1x Authentication Servers

Add an existing configured 802.1x authentication server.

(Alcatel) (config) #aaa dot1x auth-server foo-dot1auth-server

# Configuring VPN Authentication Using the CLI

VPN authentication maybe configured when IPSec or PPTP is in use on the switch. VPN authentication is configured using the aaa vpn-authentication commands from the CLI.

Enable VPN authentication.

(Alcatel) (config) #aaa vpn-authentication mode enable

Set the VPN Default role. This role will be assigned to the client if no other role is supplied by the authentication server.

(Alcatel) (config) #aaa vpn-authentication default-role foo-user

**NOTE**—You may view the roles currently defined on the switch using the show rights command from the CLI.

3 Specify the authentication server.

> (Alcatel) (config) #aaa vpn-authentication auth-server rad2-radius-server

Set the authentication failure threshold for station blacklisting parameter.

```
(Alcatel) (config) #aaa vpn-authentication
max-authentication-failures 0
```

# **Configuring Captive Portal Authentication Using** the CLI

Captive Portal authentication may be configured when clients wish to authenticate using a web-based portal. Captive Portal authentication may be accomplished via SSL, however it provides no encryption after authentication is completed.

Configure Captive Portal using the aaa captive-portal commands from the CLI.

 Set the default role. This is the role which will be assigned to the client if the authentication server provides no role information about the client when they authenticate.

(Alcatel) (config) #aaa captive-portal default-role foo-user

2 Enable guest logon - optional.

(Alcatel) (config) #aaa captive-portal guest-logon

3 Enable user logon - optional.

(Alcatel) (config) #aaa captive-portal user-logon

4 Enable logout popup menu - optional.

(Alcatel) (config) #aaa captive-portal logout-popup-window

5 Select the protocol type. The default protocol is HTTPS.

(Alcatel) (config) #no aaa captive-portal protocol-http

6 Set the pause time before redirect.

(Alcatel) (config) #aaa captive-portal redirect-pause 10

#### 7 Set the logon wait time range

(Alcatel) (config) #aaa captive-portal logon-wait range 5 10

#### 8 Set the CPU utilization threshold.

(Alcatel) (config) #aaa captive-portal logon-wait cpu-utilization 60

9 Set the authentication failure threshold for station blacklisting.

(Alcatel) (config) #aaa captive-portal max-authentication-failures 0

#### Specify an authentication server.

(Alcatel) (config) #aaa captive-portal auth-server internal



### **Configuring MAC Address Role Mapping Using** the CLI

MAC Address Role Mapping is a method of identifying clients based on their MAC address and assigning an appropriate role based on the MAC Address. This method should not be considered a true authentication method, since no password is associated with the method. This method should always be coupled with Layer 2 encryption and strict firewall policies.

#### 1 Enable MAC Address Role Mapping

(Alcatel) (config) #aaa mac-authentication mode enable

2 Set the default role. This is the role which will be assigned to the client if the authentication server provides no role information about the client when they authenticate.

(Alcatel) (config) #aaa mac-authentication default-role foo-user

#### Specify an authentication server. 3

(Alcatel) (config) #aaa mac-authentication auth-server internal

Set the authentication failure threshold for station blacklisting.

```
(Alcatel) (config) #aaa mac-authentication
max-authentication-failures 0
```

You may see the MAC Address Role Mapping settings by using the show aaa mac-authentication command from the CLI.

### Configuring Stateful 802.1x Using the CLI

This procedure configures stateful 802.1x for third-party Access Points using the CLI.

#### Enable stateful 802.1x.

(Alcatel) (config) #aaa stateful-authentication dot1x mode enable

#### Set the Request/Response time out, in seconds. 2

(Alcatel) (config) #aaa stateful-authentication dot1x timeout 20



```
(Alcatel) (config) #aaa stateful-authentication dot1x auth-server
```

### AP/Server Configuration for Stateful 802.1x

When stateful 802.1x authentication is used with third-party APs, a list of those APs must be maintained. The list is automatically generated when configuring 802.1x stateful authentication through Web UI (Web Interface). However, for legacy support it may be done manually through the CLI.

Define the configuration. This must contain all the elements shown in the example below.

```
(Alcatel) (config) #aaa stateful-authentication dot1x ap-config foo
ap-ipaddr 192.168.150.1 radius-server-name rad2-radius-server key
fooword
```

# **Role Mapping**

### SSID Role Mapping

Enter the user-rule sub-mode in the CLI.

```
(Alcatel) (config) #aaa derivation-rules user
(Alcatel) (user-rule) #
```

```
2
```

Specify the rule for assigning a role based on the client SSID

(Alcatel) (user-rule) #set role condition essid equals foo set-value foo-user

### Encryption Type Role Mapping

Enter the user-rule sub-mode in the CLI.

(Alcatel) (config) #aaa derivation-rules user (Alcatel) (user-rule) #



(Alcatel) (user-rule) #set role condition encryption-type equals open set-value foo-user



### Notes on Advanced AAA Features

The Advanced AAA feature pack for AOS-W unlocks a number of extended authentication and authorization features for enterprise and service provider networks. With the Advanced AAA feature pack, the standard AOS-W authentication features are augmented with the following:

- Per-SSID selection of authentication server for wireless networks
- Domain and realm selection of authentication server
- Dynamic authorization and authentication API using RFC 3576

### The Problem

Most enterprise networks have a single authentication infrastructure, typically based on directory services such as Microsoft Active Directory or Novell NDS. For these enterprise networks, the standard authentication capabilities of AOS-W are sufficient because all users on the system can be found in the same authentication database. However, a number of occasions arise where multiple distinct authentication infrastructures must be supported. For example, when two companies merge it often takes months or even years for the IT infrastructure to consolidate, meaning that user identity is often contained in multiple different user databases. For these networks, the ability to support multiple authentication systems is critical.

For service providers, there also exists a requirement for multiple authentication systems. Service providers often provide wholesale access service for many different companies – for example, a virtual hotspot service provider that resells service for three different national ISPs. Service providers also typically offer roaming agreements with other service providers, whereby customers of one service provider are able to connect to the networks of other service providers using their own access credentials. For these service providers, the ability to authenticate against multiple databases is essential.

Finally, some enterprise networks also require the ability to provide fine-grained authorization (meaning what a user is permitted to do on the network) control on a per-user basis, where that authorization may change dynamically during a session. For example, an enterprise may wish to enable guest access to the network, but have the ability to shut off guest access to a given user as soon as that user checks out with the front lobby receptionist. In this situation, the lobby receptionist would log the user out through visitor log software, which would then dynamically instruct the Alcatel grid controller to disconnect the user. For this application, a standard API (Application Programming Interface) is required to interface the grid controller to a number of different software packages.

# The AOS-W Solution

All the problems outlined above are solved using the Advanced AAA feature pack for Alcatel AOS-W. The feature pack is a collection of authenticationand authorization-related enhancements conveniently packaged together. The feature pack includes the following solutions:

### Per-SSID Selection of Authentication Server

In wireless networks, the SSID (Service Set Identifier) is used to differentiate between different types of services. For example, corporate users may connect to an SSID labeled "Corp" while guest users may connect to "Guest". Each SSID may support different authentication and encryption schemes, and may provide access to different wired networks as well.

The per-SSID selection of authentication server feature in AOS-W permits one or more authentication servers to be mapped to each SSID configured in the system. All users connecting to one SSID will be authenticated against one set of servers, while all users connecting to second SSID will be authenticated against a different set of servers. One application for this in enterprise networks is the ability to set up test networks or migration networks, where users must be supported on an existing authentication database while new authentication databases are set up on alternate SSIDs. The two systems can operate concurrently without interfering with each other.

Another major application for this feature is in service provider networks, where each SSID represents a completely different userbase. Many wireless hotspot providers resell their access services to national service providers. The national providers own the customers and handle billing and marketing of their service, while local hotspot companies provide the "pipes" to the network, managing and installing physical equipment at hotspot premises. These service providers can use a different SSID for each national ISP, and then authenticate the users against each respective provider's own authentication servers.

### Domain and Realm Selection of Authentication Servers

Realms and domains are commonly used in authentication systems. A realm is normally the first part of a username, separated from the actual username by a leading slash. In a Windows Active Directory network, the Active Directory domain is used as the realm. For example, Acme Corporation's domain may be "ACME", and a user named Bob within that domain may be identified on the network as "ACME/bob". Usernames also often appear in fully-qualified domain name (FQDN) format. These addresses appear similar to an email address, for example "bob@acme.com". For either format, Alcatel's Advanced AAA feature pack enables AOS-W to select different authentication servers based on domain or realm.



In an enterprise network, this capability can be used to authenticate users from different organizational units. As an example, Acme Corporation may use Windows Active Directory to store user information, and may authenticate users in this network against Microsoft's Internet Authentication Server. Acme Corporation merges with Consolidated Widgets, Inc. which uses Novell Directory Services (NDS) to manage the userbase. Depending on the size of the two companies, it may take months or years to merge the IT infrastructure, if it ever happens at all. For this company, realm-based selection of authentication servers allows the users of both companies to use the same network infrastructure while their identity information continues to be managed by two different directory services. The figure below illustrates this principle.



In service provider networks, the same access wholesaling described in the previous section can be enabled by this feature with much greater scalability. SSID-based authentication server selection described above permits up to 16 services on a given AP, limited by AP hardware. Domain or realm based authentication server selection, on the other hand, allows nearly an unlimited

number of different services to be provided. All users can connect to the network using the same method, and the domain name supplied when the user authenticates will be used to determine which ISP has authentication data for that user. This method has the additional benefit of applying to wired networks as well as wireless networks.

### Dynamic Authorization and Authentication API using RFC 3576

RFC 3576 is an IETF standard that defines how the RADIUS protocol may be extended to provide dynamic authorization of user activity in addition to basic authentication. Alcatel AOS-W implements this standard as an API (Application Programming Interface) that allows fine-grained control of users by the authentication server. This control of users includes disconnection from the network, role re-assignment, and dynamic updates of user policies.

One application for this API is in providing guest access. Nearly all corporate locations receive visitors, in the form of meeting attendees, vendors, customers, training class attendees, and so on. These visitors are increasingly equipped with mobile computing devices such as laptops, and often request or require access to their home office network or to the Internet. Corporate IT managers wish to be flexible in providing such access, but at the same time want to minimize the risk of unauthorized access because of concerns over legal liability. The ideal goal is to provide customized guest access, allowing only those services required by each individual visitor and only for the exact period of time the access is actually required.

One of Alcatel's financial services customers has implemented this customized access approach using the RFC 3576 API. The company has visitor log software running at computers used by lobby receptionists. Each visitor to the office is issued an electronically-printed visitor badge that must be worn in the building. When the software prints the visitor badge, it dynamically provisions a RADIUS server with a temporary username and password, and prints this information on the visitor's badge. The visitor can access either the wireless network through a guest SSID, or the wired network through any conference room or public area Ethernet jack. The visitor enters the username and password provided through a Web-based captive portal page, and is granted restricted access to the Internet. When the visitor leaves the office, the visitor badge must be returned to the lobby receptionist. The lobby receptionist logs the time the visitor left, and the visitor log software dynamically deletes the user from the RADIUS server. As soon as this happens, the RADIUS server signals the Alcatel grid controller using the RFC 3576 API and causes the user to be disconnected from the network.



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 17 **IAS Server Configuration**

This chapter describes how to configure your IAS server for Extensible Authorization Protocol (EAP). It will cover the following 4 topics.

- Starting the IAS Server Creating NAS clients Remote Access Policies Adding Users

# Starting the IAS Server

1 Click **Start** on task bar, click **Settings**, click **Administrative Tools**, click **Services**, select and double-click on **Internet Authentication** (See Figure). The Internet Authentication Service Properties dialog box appears.

🍇 Services						<u>_   ×</u>
] Action ⊻iew  ] ← →						
Tree	Name 🛆	Description	Status	Startup Type	Log On As	
Services (Local)	🏶 File Server for Macintosh	Enables Ma	Started	Automatic	LocalSystem	
ave	Service 1		Started	Automatic	LocalSystem	
	Service Publishing Service	Provides F	Started	Automatic	LocalSystem	
	🆏 IIS Admin Service	Allows adm	Started	Automatic	LocalSystem	_
	🆏 Indexing Service	Indexes co		Manual	LocalSystem	
	intel(R) Active Monitor		Started	Automatic	LocalSystem	
	Internet Authentication Service	Enables au	Started	Automatic	LocalSystem	
	anternet Connection Sharing	Provides n		Manual	LocalSystem	
	🆏 Intersite Messaging	Allows sen	Started	Automatic	LocalSystem	
	iPSEC Policy Agent	Manages I	Started	Automatic	LocalSystem	
	Kerberos Key Distribution Center	Generates	Started	Automatic	LocalSystem	
	Cicense Logging Service		Started	Automatic	LocalSystem	
	🆏 Logical Disk Manager	Logical Disk	Started	Automatic	LocalSystem	
	🏶 Logical Disk Manager Administrative	Administrat		Manual	LocalSystem	
	🆓 Message Queuing	Provides a	Started	Automatic	LocalSystem	
	Senter Messenger	Sends and	Started	Automatic	LocalSystem	
	🆏 Net Logon	Supports p	Started	Automatic	LocalSystem	
	🏶 NetMeeting Remote Desktop Sharing	Allows aut		Manual	LocalSystem	
	Network Connections	Manages o	Started	Manual	LocalSystem	
	🖏 Network DDE	Provides n		Manual	LocalSystem	
	Network DDE DSDM	Manages s		Manual	LocalSystem	-

2 Click the **General** tab at the top of the IAS Properties dialog box.



### 3 Change the Startup type to Automatic.

# **Creating NAS Client Entries**

Open the IAS Administration Tool



1 Click **Start** on the task bar, click **Programs**, then **Administrative Tools**, and then **Internet Authentication Service**. The Internet Authentication Service (IAS) window appears.



Create a new NAS Client.

2 Right-click on the Clients folder icon.



3 Select **New Client**. The Add Client Dialog window appears.

l ype a friendly name	and protocol for the	e client.		
Friendly name:	Туре	e a user friendly n	ame here	
Protocol:	RAD	IUS		•

Enter a meaningful name in the Friendly name box.

- 4 Use the Protocol pull-down menu to select RADIUS for the protocol.
- 5 Click Next. The Add RADIUS client dialog appears.

Client address (IP or D	NS):				
10.1.1.20					⊻erify
Client-Vendor:					
RADIUS Standard					
🔲 Client must always	send the signal	ture attribute	in the reque	st	
Shared secret:	NHN N	00			
Confirm shared secret	XXX	***			

6 Enter the IP address of the RADIUS client.

Select the appropriate vendor from the Client-Vendor pull-down box.



7 Enter a word in the Shared secret text box, then re-enter the same word in the Confirm shared secret text box.

A shared secret is a text string that serves as a password between client and server, client and proxy, or a proxy and a server.

Observe the following conventions when creating a shared secret:

- The shared secret must be the same case-sensitive text string on both devices.
- Use any standard alphanumeric and special characters.
- Limit the length of the shared secret to 128 or less characters.
- Create shared secrets of at least 22 characters and include numbers and punctuation marks in a random order.
- Use difference shared secrets for each radius server/client pair.

**NOTE**—Additional information regarding security and shared secrets, go to the Microsoft TechNet website.

http://www.microsoft.com/technet

8 Click Finish.

### **Creating Remote Access Policies**

Creating remote access policies consists of 3 basic steps.

- Naming the policy
- Setting the remote access policies and granting permission
- Creating/editing a user profile

Remote access policies are created using the IAS Administration Tool. If the IAS Administration Tool is not already open, open it by Clicking Start on the task bar, then Programs, then Administrative Tools, and then Internet Authentication Service.



- 1 Right-click on the Remote Access Policies icon in the IAS window.
- 2 Click on New Remote Access Policy. The Add Remote Access Policy dialog appears.

A Remote Acce meeting certain	ss Policy is a set of act conditions.	ions which can be a	pplied to a group o	of users
Analogous to ru specify a set of You can then sr	les you can apply to inc conditions that must be necify actions to be tak	coming mail in an e-r matched for the Re en when the conditi	nail application, you mote Access Polic ons are met	u can ;y to apply.
Policy friendly n	ame:		one die mot	

Type a name for the policy in the Policy friendly name text box.



3 Click Next. The Select Attribute dialog window appears.

pecity the co Conditions:	nditions to match.		

4 Click the Add button. The Select Attribute list window appears.

Name	Description			
Called-Station-Id	Phone number dialed by user			
Calling-Station-Id	Phone number from which call originated			
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only			
Client-IP-Address	IP address of RADIUS client. (IAS only)			
Client-Vendor Manufacturer of RADIUS proxy or NAS. (IAS				
Day-And-Time-Restric	Time periods and days of week during which			
Framed-Protocol	The protocol to be used			
NAS-Identifier	String identifying the NAS originating the reque			
NAS-IP-Address	IP address of the NAS originating the request			
NAS-Port-Type	Type of physical port used by the NAS origina			
Service-Type	Type of service user has requested			
Tunnel-Type	Tunneling protocols to be used			
Windows-Groups	Windows groups that user belongs to			
4				

5 Select the attributes (s) to add to the policy, then click the Add button. The NAS-IP-Address dialog box appears.

NAS-IP-Address		<u>? ×</u>
Type a word or a wild card (for example	e, abc.*):	
	OK	Cancel

Type the NAS-IP-Address in the text box and click OK.

**NOTE**—Add additional conditions by clicking the Add button, just below the conditions list, at the bottom of the Add Remote Access Policy window. Repeat the step above.
When finished adding conditions, click the Next button on Add Remote Access Policy dialog.

6 Select the Grant remote access permission radio box.



7 Click Next. The Add Remote Access Policy User Profile dialog appears.

Add Remote Access Policy	×
User Profile Specily the user profile.	
You can now specify the profile for users who matched the conditions you have specified.	
Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.	
Edit <u>Profile</u>	
< <u>B</u> ack Finish Canc	.el



R Click the Edit Profile button. The Edit Dial-In Profile window appears.



9 Click on the Authentication tab.

Check the **Extensible Authentication Protocol** check box.

If the authentication server needs to be configured for EAP-TLS, then select either Smart Card or Other Certificate from the EAP drop-down menu.

If the authentication servers needs to be configured for Protected EAP (PEAP), then select Protected EAP (PEAP) from the EAP drop-down dialog

After the EAP type is selected, click **OK** and the **Finish** to set the properties.

## Adding a User

Adding users to the active directory is accomplished in the following manner.

1 Click **Start**, then **Run**, then type **mmc** and press **Enter**. The Console window appears.



2 Click **Console** and select **Add/Remove Snap-in**. The **Add/Remove Snap-In dialog** appears.

🚡 Console1	
🛛 🖸 🖸 🖾 🔚 💷	
Open Ctrl+0	
Add/Remove Snap-in Ctrl+M	
1 C:\WINNT\System32\las.msc	
2 C: (WINNI (System32) doste.msc 3 C: (WINNI (System32) domain msc	
4 C:\WINNT\system32\services.msc	

Click the Standalone Tab.



3 Select the Active Directory User and Computer item in the Add Standalone Snap-in list window.

Click Add, then the Close at the bottom of the list window.

d/Remove Snap-in	? ×		
Standalone Extensions			
Use this page to add or remove a standalone Snap-in from the console.	-		
Shap-ins added to: Console Root	Add Standalone Snap-in		?
	Available Standalone Snap-ins:		
	Snap-in	Vendor	-
	Exclive Directory Domains and Trusts	Microsoft Corporation	
	Active Directory Sites and Services	Microsoft Corporation	
	Active Directory Users and Computers	Microsoft Corporation	
	🛍 ActiveX Control		
	🗐 Certificates	Microsoft Corporation	
	📴 Certification Authority	Microsoft Corporation	
	Component Services	Microsoft Corporation	
Description	📃 🔜 Computer Management	Microsoft Corporation	
	🔜 Device Manager	Microsoft Corporation	
	Р	Microsoft Corporation	j
	Description		
Add Remove About	You can use the Active Directory Domain manage Active Directory domains and tr	ns and Trusts snap-in to usts.	
	[	Add Clo	se

Right-click the Users folder in the tree pane of the Console window.

**NOTE**—You may find the Users folder along the path Console Root/Active Director Users and Computers/network name/Users.

4 Click **New**, then **User**. The New Object - User dialog appears

v Object - User	
Create in: Im.an	ubanetworks.com/Users
First name:	Initials:
Last name:	
Full name:	
User logon name:	
	@lm.arubanetworks.com
User logon name (pre-Window	ws 2000):
LM\	

Type the user's name information in the appropriate text fields., then click **Next**.

New Ubject - User
Create in: Im.arubanetworks.com/Users
Pessword:
User must change password at next logon
Password never expires
C Account is disabled
<u>&lt;₿</u> ack <u>N</u> ∰t> Cancel

Enter the password in the Password text field and re-enter it in the Confirm Password text field.

5 Click **Next**. The New Object - User dialog below appears, then click **Finish**.

New Object - User		X
Create in: Im.arut	banetworks.com/Users	
When you click Finish, the follo	owing object will be created:	
Full name: Harold Angel		
User logon name: hangle@lm.		
The password never expires.		
,		
	< Back [Finish]	Cancel

## **Configuring ACS**

твс



# **Configuring SBR**

твс

# **Configuring Funk**

твс

# CHAPTER 18 Firewall Configuration

# **Setting Policies Using Web UI**

## Aliases

Aliases are a convenient way to associate a human understandable name with a specific object. AOS-W enables administrators to assign easily understandable names to network ports (services) and specific IP Addresses or groups of IP Addresses

## **Defining Service Aliases**

Service aliases apply to protocol/port numbers. Service aliases may be configured in Web UI.

Normally only one alias need be defined for a particular service, however some services use more than one protocol. In the case where a service uses multiple protocols, a separate alias must be defined for each protocol.

Services	Destin	ations	Bandwid	lth Contr	racts	NAT Pools	Time Range
Name	Protocol	Port	End Port	A	ction		
svc-syslog	udp	514	N/A	Edit	Delete	•	
svc-l2tp	udp	1701	N/A	Edit	Delete	•	
svc-ike	udp	500	N/A	Edit	Delete	,	
svc-https	tcp	443	N/A	Edit	Delete	•	
svc-smb-tcp	tcp	445	N/A	Edit	Delete	•	
svc-dhcp	udp	67	68	Edit	Delete	•	
svc-pptp	tcp	1723	N/A	Edit	Delete	,	
svc-telnet	tcp	23	N/A	Edit	Delete	•	
abcd	tcp	2222	N/A	Edit	Delete	•	
svc-tftp	udp	69	N/A	Edit	Delete		

Navigate to the **Configuration > Security > Advanced > Services** page.

Add a new Service Alias. Click Add. The Add Service page appears.

End Port	Apoly
Starting Port	
Protocol	
Service Name	

The options and parameters available for configuration on the Add Service page are:

Service Name

A plane language name that identifies the alias.

**NOTE**—Default service aliases begin with *svc*- followed by the name of the protocol.

Protocol	Specify the protocol, either by using the radio buttons or by entering the protocol number (0 - 255).
Starting Port	Sets the lower port number of a protocol port range.
End Port	Sets the upper port number of a protocol port range.
	<b>Note</b> —If the service uses a single port, enter the starting port number here also.

- 1 Enter a name in the Service Name text field.
- 2 Check the appropriate Protocol radio button.
- 3 Enter the Starting Port.
- 4 Enter the End Port (If this service uses only a single port, enter the starting port number here).
- 5 Click Apply and Save Configuration

## **Defining Source and Destination Aliases**

Source and destination aliases may be configured in Web UI.

Source and destination aliases apply to specific IP addresses or groups of IP addresses. The alias is a convenient method to identify these addresses in easily readable way. They are used with traffic policies to specify the source or destination of a packet.

Navigate to the **Configuration > Security > Advanced > Destinations** page.

Serv	lices	Dest	tinations	Band	width Contracts	NAT Pools	Time Range
Name	Rule	Count	Invert	A	ction		
iser	1		No	Edit	Delete		
nswitch	1		No	Edit	Delete		
any	1		No	Edit	Delete		



You may add, delete, or modify source and destination aliases on this page.

Alcatel provides 3 pre-defined aliases which should not be altered or deleted.

User	When applied to an authenticated user the alias is replaced by an IP Addressed assigned to that user.
Mswitch	Represents the IP Address, loopback address, or VLAN 1 address of the switch upon which the policy is running.
Any	Represents any IP Address

Add a new alias by clicking **Add**, the Add Destinations page appears.

estination Name				
nvert			Г	
Type IP Address	NetMask/Range	Actions		
bbA				
		0 D D D V L		
		мрріу		
		Whhile		
dd Rule				
<b>idd Rule</b> Rule Type	host 💌			
<b>idd Rule</b> Rule Type IP Address	host 💌			_
a <b>dd Rule</b> Rule Type IP Address Network Mask/Range	host 💌	Αμμιγ		
<b>dd Rule</b> Rule Type IP Address Network Mask/Range	host	Αμμιγ		

- Click Add to expand the page and expose the Add Rule section, near the bottom.
- 2 Enter a name for the new destination in the Destination Name text box.
- 3 Select a rule type using the Rule Type pull-down menu.

The choices for rule types are:

Host	Use this selection to specify a single address. Do not enter anything in the Network Mask/Range field.
Network	Use this selection when specifying an IP subnet. It comprises a
Range	Use this selection when specifying an sequential range of IP Addresses. When specifying a range enter the upper address in the Network Mask/Range field.
	The maximum number of addresses is 16 when specifying a range.

- 4 Enter an IP Address in the IP Address field.
- 5 Enter a netmask or upper address of an IP range in the Network Mask/Range field.

**Note**—If you wish to specify a range with more than 16 addresses, select the Network Rule Type then enter network number and subnet mask in the IP Address and Network Mask fields.

6 Click Add, then click Apply and Save Configuration.

Other tabs: Bandwidth Contracts, NAT Pools, Time Range - TBC

## **Firewall Policies**

Alcatel AOS-W firewall policies are stateful and bi-directional. Stateful policies mean that when a packet matches a rule, they must match exactly, the policy will create a session entry so that the session may continue in both directions.

Firewall policies consist of a set of rules that are applied in a specific order against network traffic presented at the firewall. The rule at the top of the list is applied first.



Rules are organized in top-down lists where the first rule applied to the traffic is at the top of the list. Traffic is tested against each rule in order until a match is found. When a match occurs the rule is applied and no other testing occurs.

Policies can be applied to physical ports or to user roles.

Navigate to the <b>Configuration &gt; Security &gt; Policies</b> page	Navigate to the	Configuration >	Security >	Policies page
---	-----------------	-----------------	------------	---------------

Name	Rule Count	Policy Usage	A	ction
control	6	guest stateful logon	Edit	Delete
validuser	1	Not Assigned	Edit	Delete
remoteap	1	logon	Edit	Delete
abcd	1	Not Assigned	Edit	Delete
captiveportal	3	logon	Edit	Delete
allowall	1	trusted-ap employee default-vpn-role	Edit	Delete
555	1	Not Assigned	Edit	Delete
test	2	Not Assigned	Edit	Delete
srcnat	1	Not Assigned	Edit	Delete
vpnlogon	5	logon	Edit	Delete
cplogout	1	guest	Edit	Delete
guest	0	Not Assigned	Edit	Delete
stateful-dot1×	0	Not Assigned	Edit	Delete
ap-acl	5	Not Assigned	Edit	Delete
stateful-kerberos	1	Not Assigned	Edit	Delete

From the Firewall Policies page you may Edit, Delete, or Add policies.

#### Rules in Firewall Policies

Rules in firewall policies are applied to traffic that presents itself to the switch. Rules examine the source address, destination address, and the kind of information (service) the packet contains. The Source and Destination elements of a rule have the same 5 options. Those options are:

1.	any	This option will test true for traffic from any source or to any destination.
2.	user	This option will test true only for traffic to or from a known user.
3.	host	This option will test true only for traffic to or from a specific IP Address.
4.	network	This option will test true only for traffic to or from a network specified by a network address and subnet mask
5.	alias	This option will test true only for traffic to or from the address or addresses defined in a specified alias, see "Defining Source and Destination Aliases" on page 383.

The Service element of a rule has 5 options. Those options are:

1.	any	This option will test true for any type of traffic.
2.	tcp	This option will test true for only tcp traffic.
3.	udp	This option will test true for only udp traffic.
4.	service	This option will test true for only traffic to or from a specified service alias.
5.	protocol	This option will test true for only traffic with a specified protocol number.

The Action element of a rule has 5 options. Those options are:

1.	Permit	Forward the packet without modification.
2.	Deny	Drop the packet with no notification.
3.	src-nat	Change the source IP address of the packet and forward it. If no source NAT pool is specified the IP address of the Alcatel switch will be substituted for the original source address.
4.	dst-net	Change the destination IP address of the packed and to the switch IP address and forward it.



5. redirect

Add a policy by clicking Add, the Add New Policy page appears.

Security > Firewall Policies > Add New Policy Policy Name Rules Source Destination Service Action Log Mirror Queue Time Range BlackList TOS 802.1p Priority Action Add Destination Service Action Log Mirror Queue Time Range Black List TO5 802.1p Priority 🖌 any 🖌 any 🖌 permit 💌 🗖 Log 🎵 Mirror 💽 Low C High 🔛 Г \* \* Cancel Add Apply Commands View Commands

The Add New Policy page is where you name your new policy and define rules for that policy.

- Enter a meaningful name in the Policy Name field at the right hand side of the page.
- 2 Select a traffic source from the Source pull-down menu.
- 3 Select a traffic destination from the Destination pull-down menu.
- 4 Select an action from the Action pull-down menu.
- 5 Select Log in you wish each packet matching this rule to be recorded in the system logfile.
- 6 Set a queue priority, high or low by selecting the corresponding Queue radio button.

Queue priority sets the priority of outbound wireless traffic.

- 7 Click Add.
- 8 When you are done adding rules, click **Apply** and **Save Configuration**.

Applying Policies to Physical Ports

Policies may be applied to either physical ports or user roles.

General Port VLAN Tunne	IS IP R	outing VRRP E	HCP Server		
Port Selection Options Use any of the selection criteria to choose port or manually select one or more ports by clicking You can also select all the ports using the 'Seler	s for configu on the ports	ration 			
C Administrative State C Ope VLAN Association 78 C Trus	rational State	Port Mod	e		
Port Selection					
		7 7 7 22			
1		23 24		25	
Current configuration of the port u	nder the n	nouse cursor will be d	isplayed		
Administrative State	N/A	Operational State	N/A		
Fower uver Etnernet	N/A N/A	Is Port Trusted	N/A		
Spapping Tree	N/A	PortPolicy	NVA		
VI AN(c)	N/A				
Enable Port					
Enable 802 3af Power Over Ethernet					,
Enable Cisco Power Over Ethernet/Enabling th	is option will	disable 802 3af Power Over	r Ethernet)		Г.
Make Port Trusted	no operari min		Contract,		Г. Г
Port Mode					C Access C Trur
				_	
Enter VLAN(S)				-	
Firewall Policy				_	
Enable MUX					
					Enable     19     Port Cos
Spanning Tree					128 Priori
					Port Fa
					Apply

Navigate to the **Configuration > Switch > Port** page.

Select the port to which you wish to apply a policy, then use the pull-down menu to select a policy to apply.

#### Click Apply and Save Configuration.

More information TBC



# **Defining Roles Using Web UI**

### **Role Design**

A role is assigned to a user when they connect to the network, and possibly again after they are authenticated.

Roles determine what network resources the user may access. Roles may be very broad-based, allowing access to many resources or they may be very narrow in scope, allowing access to very limited resources. Sometimes, a role is used to grant a particular user, or group of users, access to a specific resource that other users are not.

## **Configuring Roles**

Navigate to the **Configuration > Security > Roles** page to view roles.

Name	Firewall Policies	Bandwidth Contract	Actions
ap-role	control,ap-acl	Not Enforced	Edit Delete
visitor	Not Configured	Not Enforced	Edit Delete
trusted-ap	allowall	Not Enforced	Edit Delete
employee	allowall	Not Enforced	Edit Delete
default-vpn-role	e allowall	Not Enforced	Edit Delete
guest	control,cplogout	Not Enforced	Edit Delete
stateful-dot1×	Not Configured	Not Enforced	Edit Delete
stateful	control	Not Enforced	Edit Delete
ogon	control,captiveportal,vpnlogon,remoteap	Not Enforced	Edit Delete

Click **Add** to begin adding a new role to the list. The Add Role page appears.

Role Name		
Firewall Policies		
Name         Rule Count           Add	Location Action	
Re-authentication In	terval	
Disabled Change	(0 disables re-authentication. A pos	tive value enables authentication
Role VLAN ID		
Not Assigned Not Assigne	d 💙 Change	
Bandwidth Contract		
Not Enforced	Change 🔽 Per User	
VPN Dialer		
Not Assigned Not Assigne	d ⊻ Change	
L2TP Pool		
Not Assigned Not Assigne	d 💙 Change	
PPTP Pool		
Not Assigned Not Assigne	d ⊻ Change	
Commands		View Commands
Commands		<u>View Commar</u>



### Adding Firewall Policies

Add firewall policies, begin by clicking the Add button under the Firewall Policies header on the page. The Configure Firewall Policy page then appears.

Role Nam	e			
Firewall F	olicies			
Name	Rule Count Loca	ation Action		
Add				
	80 DA DE 88	0		
Choose	from Configured Pol	licies control	Location 0.0.	0
C Create	New Policy From Exis	sting Policy control	💌 Creat	te
		And a second	and the second sec	

You may choose one of three options on this page:

- Specify an existing policy.
- Create a new policy using an existing policy as a model.
- Create a new policy from scratch.

#### Specify an Existing Policy

- 1 Select the Choose from Configured Policies radio box.
- 2 Specify a particular AP (if you wish to apply this policy only when using the specified AP) by entering the its location in the Location text box.
- 3 Click Done.

Create a New Policy From an Existing Policy

**1** Select Create New Policy From Existing Policy.

Security > User Roles > Add Role > Add Policy

2 Click Create. The Add New Policy page appears.

Policy Nam	e		сог	itrolnev	V.)								
Location			0.0	.0									
Rules													
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Actio	on	
any	any	svc-icmp	permit			low					Delete	*	
any	any	svc-dns	permit			low					Delete	*	
any	any	svc-papi	permit			low					Delete	•	
any	any	svc-adp	permit			low					Delete		
any	any	svc-tftp	permit			low					Delete		
any	any	svc-dhcp	permit			low					Delete		
Add													

3 Create a new policy in exactly the same way you would in "Firewall Policies" on page 385.

Create a New Policy from Scratch

- 1 Select the Create New Policy radio button.
- 2 Click Create. The Add New Policy page appears.
- 3 Create a new policy in exactly the same way you would in "Firewall Policies" on page 385.

**Configuring Other Policy Options** 

In addition to creating new policies for a role, you may add or adjust 6



additional options.

•	Re-authentication Inter- val	By default a user will remain authenticated until the login session is terminated. Use this option to force periodic re-authentication.
•	Role VLAN ID	When a VLAN is specified for this option, the user will be mapped to that VLAN.
		<b>Note</b> —This option only applies if authentication is done at Layer 2.
•	Bandwidth Contract	This option applies a bandwidth contract to the role.
•	VPN Dialer	Use this option to assign a specific VPN dialer to a user role. For more information about configuring VPN dialers, see "VPN Configuration" on page 505.
•	L2TP Pool	Use this option to specify the address pool from which a VPN user will be assigned an IP address when the user negotiates an L2TP/IPSec session. For more information see "VPN Configuration" on page 505.
•	PPTP Pool	Use this option to specify the address pool from which a VPN user will be assigned an IP address when that user negotiates a PPTP session. For more information see "VPN Configuration" on page 505.

# **Setting Policies Using the CLI**

This portion of the chapter describes the process of configuring firewall (traffic) policies using the Command Line Interface. The processed describe here mirror the processes in the first part of the chapter which describes firewall configuration using Web UI, a web-based graphical user interface.

## **Defining Service Aliases**

**Define a service alias using the** netservice *<name>* {ProtocolNum | TCP *<startAddr> <endAddr>* | UDP *<startAddr> <endAddr>* } command from the CLI.

You may define a service alias by giving it a name, then choosing to specify one of three options:.

UDP	Use this option to specify UDP as the service. Specify a port for the service by including a single value after the UDP specifier or a range of ports by including two values representing <i>startAddr</i> and <i>endAddr</i> . The valid range for ports is 0-65535.
ТСР	Use this option to specify TCP as the service. Specify a port for the service by including a single value after the UDP specifier or a range of ports by including two values representing <i>startAddr</i> and <i>endAddr</i> . The valid range for ports is 0-65535.
Protocol Number	Use this option to specify the service by its protocol number. No port or port range may be specified when using this option.

Define the service alias.

```
(Alcatel) (config) #netservice svc-foo-udp udp 7066 7165
(Alcatel) (config) #netservice svc-foo-tcp tcp 10555
(Alcatel) (config) #netservice svc-foo-chaos 16
```

The current service alias configurations may be viewed using the show netservice command from the CLI.

```
(Alcatel) (config) #show netservice
Services
_____
            Protocol Ports
Name
____
             _____ ____
svc-snmp-trap udp 162
svc-syslog udp
                    514
svc-l2tp udp
svc-ike udp
                    1701
                     500
svc-https tcp
svc-smb-tcp tcp
                     443
                     445
svc-dhcp
                    67 68
        udp
```



#### **Defining Source and Destination Aliases**

Define a source/destination alias and enter the config-dest mode using the netdestination *<name>* command from the CLI.

After entering the config-dest mode you may specify one of 3 types of destinations for your alias:

host	Use this command to specify a specific host IP address for the alias.
network	Use this command to specify a network or sub-net as a source or destination. Specify a network number followed by a subnet mask.
range	Use this command to specify a range of valid IP addresses. Specify the lower address followed by the higher.

1 Enter the config-dest mode and define the name for the alias

(Alcatel) (config) #netdestination dest-foo-any

2 Configure the alias as host with an IP address of 192.196.10.200.

(Alcatel) (config-dest) #host 192.196.10.200

#### **Firewall Policies**

Firewall policies are configured using the ip access-list session <name> command from the CLI.

#### 1 Enter the config-sess-*aclname* mode.

```
(Alcatel) (config) #ip access-list session foo-acl
(Alcatel) (config-sess-foo-acl)#
```



#### Enter rules in the order you wish them to be applied.

```
(Alcatel) (config-sess-foo-acl) # user alias Int net svc-dhcp permit
(Alcatel) (config-sess-foo-acl) # user alias Int net svc-dns permit
(Alcatel) (config-sess-foo-acl) # user any svc-http permit
(Alcatel) (config-sess-foo-acl) # user any svc-https permit
(Alcatel) (config-sess-foo-acl) # user any svc-ike permit
(Alcatel) (config-sess-foo-acl) # user any any deny
```

If you wish to change the position of a rule in the list, use the position option to move the rule to a specific line.

```
(Alcatel) (config-sess-foo-acl) # user any svc-ike permit position 3
```

Use the show access-list <aclName> command from the CLI to view a specific firewall policy.

Use the show access-list brief command to see a listing of the current ACLs

(Alcatel) (config)	#show ac	cess-list k	orief			
Access list table						
Name	Туре	Use Count	Roles			
control	session ·	4	logon	ap-role	stateful	guest
captiveportal	session i	1	logon			
allowall	session i	1	truste	ed-ap		
vpnlogon	session i	1	logon			
cplogout	session i	1	guest			
guest	session	0				
stateful-dot1x	session	0				
ap-acl	session i	1	ap-rol	.e		
stateful-kerberos	session 0					

#### Applying Policies to Physical Ports

Add a policy to a specific port from the CLI using the interface fastethernet mode commands.



#### Enter the config-if mode.

```
(Alcatel) (config) #interface fastethernet 1/22
(Alcatel) (config-if)#
```



2 Assign a policy to a the port used when entering the config-if mode.

```
(Alcatel) (config-if) #ip access-group guest session
```

# Defining Roles Using the CLI

### **Configuring Roles**

Roles are configured in the CLI using the config-role mode commands.

Define a user role and enter the config-role mode.

(Alcatel) (config) #user-role foo-user (Alcatel) (config-role) #

Begin to enter the role parameters.

(Alcatel) (config-role) #dialer default-dialer (Alcatel) (config-role) #pool pptp-pool-1

## **Defining Access Control Lists in the CLI**

ACLs are applied to physical interfaces<sup>1</sup> using the *ip* access-group command in the CLI.

```
(Alcatel) (config) #ip access-list standard foo-1
(Alcatel) (config-std-foo-1)#
```

## Standard ACLs

Create standard ACLs using the standard option of the access-list command.

```
(Alcatel) (config-std-foo-1)# permit 192.168.10.0 255.255.255
(Alcatel) (config-std-foo-1)# permit host 192.168.20.15
(Alcatel) (config-std-foo-1)# deny any
```

1.All Alcatel Wireless LAN switches support up to 128 IP interfaces.

## Extended ACLs

Create extended ACLs using the extended option of the access-list command.

```
(Alcatel) (config) #ip access-list extended foo-ext-1
(Alcatel) (config-ext-foo-ext-1)# permit tcp any host 1.1.1.1 range
67 69
(Alcatel) (config-ext-foo-ext-1)#permit icmp 1.1.1.0 0.0.0.255 any
echo-reply
```

## MAC ACLs

Create MAC ACLs using the mac option of the access-list command.

```
(Alcatel) (config) #ip access-list mac foo-mac-1
(Alcatel) (config-mac-foo-mac-1)# permit host 00:01:01:03:04:05
(Alcatel) (config-mac-foo-mac-1)# permit 00:0a:ff:02:ad:01
ff:ff:ff:00:00:00
```

## Ethertype ACLs

Create Ethertype ACLs using the eth option of the access-list command.

```
(Alcatel) (config) #ip access-list eth foo-eth-1
(Alcatel) (config-eth-foo-eth-1)# permit 2048
```



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 19 Captive Portal Setup

## **Overview**

The following outline lists the steps used to configure captive portal authentication. Each of the outlined steps is covered in detail in the sections that follow.

- 1 Add users to the authentication database.
- Configure the server information on Wireless LAN switch.
- 3 Apply an authentication server for captive portal authentication.
- 4 Customize the logon role.

Identify what traffic is to be permitted to authenticate the user.

- 5 If guest access is to be allowed, enable the guest login and customize the guest role.
- 6 Configure other user roles as needed.
- 7 Configure server rules to derive the role for various users.
- 8 Import a server certificate
- 9 Customize the captive portal login screen, if desired.

## Add Users to the Database

Authentication can be provided using one of the following:

- An internal database on the Wireless LAN switch
- An external RADIUS server attached to your network

If using an external RADIUS server, refer to your server documentation for adding users and skip to the next section.

Otherwise, users must be added to the Wireless LAN switch internal database. The internal database includes a default guest account. If no other specialized accounts are needed, no further server configuration is required and you can skip to the next section.

If specialized accounts are needed, use the following CLI configuration commands:

```
(config) # local-userdb add username <name> password <password> role <role-name>
```

For example:

```
(config) # local-userdb add username dave password sssHHH role employee
```

**NOTE**—The specified role must also be defined on the authentication server. See "Configuring Role Derivation" on page 410 for more information.

To see all the users configured in the database:

(config) # **show local-userdb** 

To delete a user from the database:

```
(config) # local-userdb del username <name>
```

## **Configure RADIUS Server Information**

If using a Wireless LAN switch internal server, skip to the next section.

Otherwise, if using an external RADIUS server use the following CLI configuration commands to provide information about the external server:

(config) # aaa radius-server <name> [host <IP address>] [key <shared secret>]
[authport <port number>] [acctport <port-number>] [timeout <seconds>]
[inservice] [retransmit <retries>] [mode {enable|disable}]

Parameters:

<name></name>	Specify the name assigned to the RADIUS server.
<pre>host <ip address=""></ip></pre>	Specify the IP address of the remote RADIUS server host.
key <shared key=""></shared>	Specify the shared secret text string used between the Wireless LAN switch and the RADIUS server.
<pre>authport <port number=""></port></pre>	Optional. Specify the authentication destination port number. The default is 1812.
acctport <port number=""></port>	Optional. Specify the accounting destination port number. The default is 1813.
timeout <seconds></seconds>	Optional. Specify the length of time to wait for a reply from the RADIUS server before retransmitting the request. The default is 5 seconds.
inservice	Optional. If the server has timed out, this option will set it a back in service immediately.
retransmit <retries></retries>	Optional. Specify the number of times the Wireless LAN switch transmits an unacknowledged RADIUS request to the server. The default is 3.
<pre>mode {enable disable}</pre>	Optional. Enable or disable the server. The default is enabled.

For example:

(config) # aaa radius-server IAS host 10.1.1.214 key nocat



Use the no prefix to remove the server information from the database. For example:

```
(config) # no aaa radius-server IAS
```

## Apply a Server to Captive Portal

Associate the authentication server to the captive portal using the following command:

(config) # aaa captive-portal auth-server <server name>

Where *server name* is one of the following:

 If using a Wireless LAN switch internal database, specify Internal (the name is preset and cannot be changed)

(config) # aaa captive-portal auth-server Internal

**Note**—The name of Wireless LAN switch internal database server (Internal) cannot be changed.

• If using an external RADIUS server, use the name specified in the aaa radius-server command. For example:

```
(config) # aaa captive-portal auth-server IAS
```

## **Customize the Logon Role**

The logon role is intended only to allow clients to access the captive portal logon page. Typically, the logon role should be configured with two session Access Control Lists (ACLs): one to allow general control traffic (such as DNS and DHCP) and another to allow captive portal authentication.

#### Modify the Control ACL

A default control ACL is already configured to allow generic traffic, but may be modified as necessary. You can view the rules in the control ACL as follows:

```
(Alcatel) # show ip access-list control
ip access-list session control
control
_____
Priority Source Destination Service Action Opcode Log Queue
       any any svc-dhcp permit
user any svc-nbns permit
1
                                                            Low
2
                                                            Low
3
        user any
                            svc-dns permit
                                                           Low
                           svc-tftp permit
svc-gre permit
        user any
4
                                                           Low
5
        user any
                                                           Low
                           svc-bootp permit
svc-icmp permit
6
        any any
                                                            Low
7
                                                            Low
        user any
```

**NOTE**—Netbios Name Server Lookup (NBNS), shown as rule 2 above, is required if using a WINS server with Microsoft Windows.

You can add rules to the control ACL as follows:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CTRL/Z
(Alcatel) (config) # ip access-list session control
(Alcatel) (config-sess-control) # <source> <destination> <service> <action>
```

You can remove rules using the no form of the same command

(Alcatel) (config-sess-control) # no <source> <destination> <service> <action>



#### Modify the Captive Portal ACL

A default captiveportal ACL is already configured to allow captive portal authentication traffic. You can view the rules in the captive portal ACL as follows:

```
(Alcatel) # show ip access-list captiveportal
ip access-list session captiveportal
captiveportal
_____
Priority Source Destination Service Action Opcode Log Queue
   user mswitch svc-https permit
user any svc-http dst-nat 8080
1
                                                LOW
      user any
2
                                                Low
                     svc-https dst-nat 8081
3
      user any
                                               Low
```

Normally, the captive portal ACL need not be modified. However, you can add rules to ACL the if necessary:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CTRL/Z
(Alcatel) (config) # ip access-list session captiveportal
(Alcatel) (config-sess-captiveportal) # <source> <destination> <service> <action>
```

You can remove rules using the no form of the same command:

```
(Alcatel) (config-sess-captiveportal) # no <source> <destination> <service>
<action>
```

## Modify the Logon Role

The logon role should have only the control and captive portal ACLs assigned. ACLs that allow other forms of authentication (such as VPN) should be removed from the logon role.

To view the ACLs assigned to the various roles, use the following command:

In this case, the logon role shown at the bottom of the list has three ACLs: control, vpnlogon, and captiveportal. The vpnlogon ACL should be removed:

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CTRL/Z
(Alcatel) (config) # user-role logon
(Alcatel) (config-role) # no session-acl vpnlogon
```



### Allow Guest Access

By default, guest access is disabled. To allow guest access, first the guest logon must be enabled, and then the guest role must be configured with appropriate ACLs.

#### Enable the Guest Logon

By default, the guest login option is disabled. This means that the guest option is not shown on the login page. Only users with valid user names and passwords are allowed. To explicitly enable the guest login, use the following configuration command:

```
(Alcatel) (config) # aaa captive-portal allow-guest-logon
```

To disable the guest logon, use the no form of the command:

```
(Alcatel) (config) # no aaa captive-portal allow-guest-logon
```

#### Customize the Guest Role

By default, the guest role denies all traffic except as needed for logging out (using the default cplogout ACL). To enable other forms of guest access, you must assign ACLs which permit appropriate guest traffic.

For example, to deny guests all access to the internal class B network but allow access to the internet, the following configuration commands could be used:

```
(Alcatel) (config) # ip access-list session guest
(Alcatel) (config-sess-guest) # user network 172.5.0.0 255.255.255
deny
(Alcatel) (config-sess-guest) # user any any permit
(Alcatel) (config-sess-guest) # exit
(Alcatel) (config) # user-role guest
(Alcatel) (config) # user-role guest
(Alcatel) (config-role) # session-acl guest
```

In the example above, the guest ACL denies internal network access and allows all else. The guest ACL is then assigned to the guest role.

Another way to achieve the same results is as follows:

(Alcatel) (config) # destination internet network 172.5.0.0 255.255.0.0 invert
(Alcatel) (config) # ip access-list session guest
(config-sess-guest) # user alias internet permit

In the example above, a destination alias is created that represents all IP addresses *except* the internal network (by selecting the internal network and using the invert option). The guest user is then permitted access to the resources in the alias.

## **Configure Other User Roles**

You can configure other user roles as needed. For each role, first create the session ACLs. Then, apply the session ACLs to the appropriate user role.

In the following example, we will create two session ACLs (noilabs and nonoc) and then use them to configure three user roles.

```
ip access-list session noilabs
                                                   (This policy denies access to the iLabs network)
any network 45.128.0.0 255.128.0.0 any deny
exit
ip access-list session nonoc
                                                   (This policy denies access to the NOC network)
user host 45.0.12.20 dns permit
 any network 45.0.0.0 255.255.0.0 any deny
 any network 45.2.0.0 255.255.0.0 any deny
 any network 45.125.0.0 255.255.0.0 any deny
 any network 45.120.0.0 255.255.0.0 any deny
 any network 192.16.170.0 255.255.255.0 any deny
exit
user-role ilabs
                                                   (iLabs users do not have access to the NOC network)
 session-acl nonoc
 session-acl allowall
exit
user-role quest
                                                   (Guest users do not have access to either NOC or iLabs)
no session-acl control
no session-acl quest
 session-acl nonoc
 session-acl noilabs
 session-acl allowall
exit
user-role noc
                                                   (NOC users have complete access)
 session-acl allowall
```



### **Configuring Role Derivation**

The simplest option for role derivation is to configure a default role for the captive portal user. This role will be assigned to the user after successful authentication. This should be used when there is only one role to be configured and can be done as follows:

1 Create the captive portal role:

(config) # aaa captive-portal default-role employee

2 If using the Wireless LAN switch internal database, define the role condition:

If using an external RADIUS server, skip this step.

Otherwise, if the internal database is used and the role configured in the database is to be used as the role after authentication, the following server rule must be configured:

(config) # aaa server-rule Internal
(server-rule) # set role condition Role value-of

This means that if the Role attribute is present, its value is used for the role.

If using an external RADIUS server, define the role conditions:

If using the switch internal database, skip this step.

Otherwise, if using an external RADIUS server, server rules must be configured to examine attributes returned by the server. Any attribute can be used, but one common attribute is Filter-Id. To use the attribute the server must first be configured to return this attribute with the right role.

The following commands can be used to allow the Wireless LAN switch to derive the role from a valid server attribute:

```
(config) # aaa server-rule IAS
(server-rule) # set role condition Filter-Id value-of
```

This means that if the Role attribute is present, its value is used for the role.

There are various other operators in addition to value-of such as contains, equals and not-equals which can be used in the commands above.

If no role value is found, the default role for the captive portal will remain guest.
For more information on how role derivation works, refer to "Setting Access Rights" on page 419.

## Import a Server Certificate

Unless an appropriate server certificate is in place, wireless client stations using captive portal may get a security warning message after logging in. For example:



FIGURE 19-1 Windows XP Security Alert

To prevent the warning message, use the Alcatel Web Interface to import a valid x509 PEM server certificate.

1 Access the Alcatel Web interface

To use the Alcatel Web interface, the following is required:

- A Wireless LAN switch configured with a management interface IP address.
- A PC with a standard Web browser and access to the Wireless LAN switch IP address.

To access the certificate import page, enter the following URL in your Web browser:

http://<switch IP address or hostname>/screens/certificate\_import.html

If your PC has access to the appropriate interface, you will be prompted to login.



#### 2 Log in using the admin account

When successful, the following page appears:

<u>Wireless Network Management</u> Import Certificate for Web Server		
The certificate should be in X.509 PEM format. After the certificate is uploaded, the management module of the switch will restart. This will shutdown all the CLI and Web Server connections		
File to be imported	Browse	
Upload		

FIGURE 19-2 Import Certificate Page

3 Select the valid server certificate.

Type the filename or use the Browse button to the locate a properly formatted x509 PEM server certificate file that includes both public and private key information.

4 Upload the server certificate file.

Click on the upload button to load and install the certificate. Once the certificate is installed, the Alcatel Web Interface will automatically restart (this could take a few moments). When ready, clients using captive portal should no longer receive the security warning message.

The same certificate may be installed in multiple switches. The switch will parse the FQDN (Fully Qualified Domain Name) in the certificate and use that as the redirection URL for captive portal users.

When the user's machine issues a DNS query for that FQDN upon receiving the redirection URL, the switch will intercept that DNS request and reply to it with the FQDN and switch loopback IP address.

The user's browser will be redirected to a captive portal page with a valid FQDN address after the switch receives the DNS reply.

**NOTE**—For information on installing certificates with an intermediate CA, see "Captive Portal Certificates with Intermediate CAs".

# **Customize the Login Screen**

If desired, the background image shown on the captive portal login screen can be replaced with a custom GIF, JPG, or PNG graphic file.



Enter the following URL in your Web browser:

http://<switch IP address or hostname>/screens/auth/captiveportal\_customize.html

If your PC has access to the appropriate interface, you will be prompted to login.

2 Log in using the admin account

When successful, the following page appears:

<u>Wireless Network Management</u> Import Background for CaptivePortal Login page		
The background image can be a .gif,.png or .jpg file.The size of the background image should match the size of the captive portal page.		
Background Image	Browse	
Upload		

FIGURE 19-3 Import Background Graphic

3 Select the valid graphic file.

Type the filename or use the Browse button to the locate a valid GIF, JPG, or PNG formatted graphic file.

- **NOTE**—Because different client stations may use different screen resolutions to view the captive portal login screen, the relative size of the background graphic may be different for different users. In cases where the graphic is smaller than the available screen dimensions, the background graphic will be repeated as tiles. In cases where the graphic is larger than the available screen, only a portion of the graphic will be displayed. You should design your graphic with these factors in mind.
- 4 Upload the graphic file.

Click on the upload button to load and install the graphic. Once installed, new logins using captive portal should see the new background graphic.

**NOTE**—To revert to the default image, use the CLI del command to remove the cp image file.



# **Sample Configuration**

Listed below are the commands relevant to the captive portal configuration on an actual Alcatel Wireless LAN Switch places on an N+I network:

```
ip access-list session noilabs
any network 45.128.0.0 255.128.0.0 any deny
exit
ip access-list session nonoc
 user host 45.0.12.20 dns permit
 any network 45.0.0.0 255.255.0.0 any deny
 any network 45.2.0.0 255.255.0.0 any deny
 any network 45.125.0.0 255.255.0.0 any deny
 any network 45.120.0.0 255.255.0.0 any deny
 any network 192.16.170.0 255.255.255.0 any deny
exit
ip access-list session captiveportal
user any http dst-nat 8080
user host 45.1.14.1 https permit
user any https dst-nat 8081
exit
user-role ilabs
 session-acl nonoc
 session-acl allowall
exit
user-role quest
no session-acl control
no session-acl quest
 session-acl nonoc
 session-acl noilabs
 session-acl allowall
exit
user-role noc
no session-acl noc
 session-acl allowall
exit
user-role logon
no session-acl control
no session-acl logon
session-acl nonoc
 session-acl noilabs
 session-acl captiveportal
session-acl allowall
exit
```

```
user-role ap
session-acl nonoc
session-acl noilabs
exit
aaa captive-portal default-role noc
aaa captive-portal auth-server infoblox priority 1
aaa captive-portal auth-server infoblox
aaa radius-server infoblox host 45.0.12.60 key infoblox
aaa server-rule server infoblox
set role condition User-Name starts-with ilab set-value ilabs
exit
interface vlan 1
ip address 45.1.14.1 255.255.0.0
exit
ip default-gateway 45.1.0.1
```

# Show Commands

The following show commands will help you obtain information important for configuring and debugging captive portal features.

#### show rights

This command gives an overview of all configured roles. It shows the component session ACL of each role.



#### show rights <role-name>

This command details the access rights associated with a role.

```
(Alcatel) # show rights employee
Derived Role = 'employee'
Bandwidth = No Limit
Session ACL count = 1
Session ACL List = employee
ACL = 11
VPN Dialer name = default-dialer
employee
------
Source Destination Service Action Opcode TimeRange Log Expired
------
any any permit
Expired Policies (due to time constraints) = 0
```

#### show access-list <acl-name>

Use this command to see individual session ACL filters.

#### show aaa captive-portal

This command shows the complete captive portal configuration:

#### show user-table

This command shows all the users currently known to the system:

```
      (OmniAccess 6000) # ahow user-table

      Users

      IP
      MAC
      Name
      Role
      Age(d:h:m)
      Auth
      VPN link
      location
      Roaming
      Essid/Bssid/Phy

      ID.2.15.4
      00:01:24:60:03:99
      pdedhia
      employee
      00:09:52
      VPN
      10.3.25.169
      52.1.3
      Associated
      Alcatel-alpha-ap/00:0b:8

      6:80:60:78/a
      (OmniAccess 6000) #
```

The meaning for the various columns is as follows:

- IP: IP address of the user
- MAC: MAC address of the user
- Name: Name of the user
- Role: Role assigned to the user
- Age: How long the user has been known to the switch (days:hours:mins)
- Auth: Authentication method (Web, VPN, 802.1x, MAC)
- VPN link: Cross reference between inner and outer IP address of VPN user.
- Location: The location code (building.floor.device) for the AP being used for the connection.

# **Using Microsoft Certificate Authority**

More information TBC



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 20 Setting Access Rights

This chapter will describe how to set access rights on the OmniAccess 6000 switch using the AOS-W software application.

# Introduction

User rights are controlled by the ACL assigned to the user's role. User roles are derived from information about the user obtained through the authentication process.

A session ACL is comprised of one or more traffic filtering rules.

The process of setting access rights involves the following 5 basic steps:

- 1 Define service and destination Alias
- 2 Create one or more session ACLs
- 3 Define a role(s) and apply a session ACL
- 4 Configure a default role for authentication.
- 5 Configure rules from which to derive roles.

# **Defining Alias'**

## **Defining Service Alias'**

Alias' are useful when creating filters, giving service definitions a friendly name. Creating an alias is accomplished using the **netservice** command, See "Authentication Commands" on page 817.

```
(Alcatel) (config) #netservice HTTP tcp 80
(Alcatel) (config) #
```

# **Defining Destination Alias'**

Define a destination alias using the destination command.See "Authentication Commands" on page 817.

```
(Alcatel) (config) # destination Internet 192.168.1.120 255.255.255
(Alcatel) (config) #
```

# **Creating Session ACLs and Roles**

# **Creating A Session ACL for Logon**

A session ACL must first be created for the Logon role. That ACL will contain filters that control the user's access during the logon process, before the user is authenticated.

Session ACLs are created or modified using the **ip** access-list session command. See "Access Control List Commands" on page 835.

### **Predefined ACLs**

A predefined session ACL named control, the predefined filters for the default control ACL are shown below:

- svc-icmp
- svc-dns
- svc-dhcp
- svc-papi
- svc-tftp
- svc-bootp

If a WINS server is configured then the following filter should be added to the control ACL:

svc-nbns

Another predefined ACL named captive portal allows only that traffic necessary for captive portal authentication. The filters associated with this ACL are:

- scv-http dst-nat 8080
- svc-https
- svc-https dest-nat 8081

A separate ACL(s) should be created for use after the user has been authenticated and assigned a role.

# **Creating Session ACLs For Users**

Access rights for successfully authenticated users are granted by creating session ACLs that are assigned to a user subsequent to authentication.

After a Session ACL has been created it must be assigned to a role(s) using the user-role command. See "Role Sub-Mode" on page 819.



# **Role Derivation**

The simplest way to assign a role is to create a default role for the authentication method being used, then assign that role to all or most of the users when they are authenticated.

Create a role using the aaa captive-portal command. See "AAA Commands" on page 823.

## How Role Derivation Works

Roles are derived in the following order:

- 1. The default role for a new user is always logon.
- 2. Prior to authentication, derivation rules based on user attributes (SSID, BSSID, user MAC, location and encryption type) can change the role. This will override the default logon role. User derivation rules are configured with the aaa derivation-rules user command.
- 3. After a successful authentication, if there is a default role assigned for the authentication method, AOS-W will override the role derived from step 1 or step 2 with it.
- 4. Derivation rules based on returned attributes from the authentication server (and some user attributes) can change the role after successful authentication. Server rules are configured with the aaa derivation-rules server command. This will override all previous roles. Starting with AOS-W 2.3.2.0, rules based on SSID and location (user attributes) can also be created under server rules even though these attributes are not returned by server.
- Alcatel VSA. If authentication server returns Alcatel VSA for role (Vendor id 14823, Attribute id 1) it takes highest precedence. In fact, server rules are not even checked if Alcatel role VSA is present.

The following flow illustrates how roles are derived.

FIGURE 20-1 Role Derivation Flow Chart





# **Show Commands**

The Show Commands associated with user rights are:

- show rights
- show rights rolename
- show rights derive-role authentication\_method
- show access-list aclname
- show aaa captive-portal
- show user-table

A full description of the Show Commands may be found in the Show Commands chapter.

# CHAPTER 21 Access Point Setup

This chapter covers the following topics for the Alcatel Wireless Access Point (AP):

- Overview of the system components and supported network topology
- Description of AP setup, including requirements, boot access, initial configuration, and advanced configuration.
- Description of switch setup for new APs, including profiles and setting attributes.

Because Access Points are broadcast radio devices, their operation is subject to governmental regulation. Therefore, it is important that you correctly configure each AP for the location of its intended use. This means, you must select the proper channel assignments antenna gain values, and the like, before you activate the AP. (If you do not configure the antenna gain value, the AP will not function.) It is your responsibility to determine what these proper values are for each location in which you plan to install APs.

To protect the AP configuration from unauthorized misconfiguration of these broadcast parameters, the country code can only be set during the initial setup script. To prevent other values from being changed improperly, Alcatel Networks recommends that you change the default administrator password to something you and no one else will remember.

# System Overview

## Components

The Alcatel Wireless LAN solution consists of the three major components:

- The Alcatel Wireless LAN Switch. This is an enterprise-class switch into which multiple wireless Access Points (APs) are connected and controlled.
- The Alcatel Wireless Access Point. This is a next-generation wireless transceiver which functions as AP or Air Monitor (AM). Although third-party APs can be used with the Alcatel Wireless LAN system, the Alcatel AP provides the best features and easiest integration.
- The Alcatel AOS-W Switch Software. This software intelligently integrates the Wireless LAN switch and APs to provide load balancing, rate limiting, self healing, authentication, mobility, security, centralization for monitoring and upgrades, and more.

## **Supported Network Topologies**

The Alcatel Wireless LAN Switch can be deployed in the wiring closet with direct physical connection to the APs it controls, or in the backbone where it controls APs attached to the wired LAN.



FIGURE 21-1 Alcatel Deployment Options

### **Direct Connection**

The Alcatel AP can be connected directly to one of the FE ports on Alcatel Wireless LAN Switch. In this topology, the port on which the AP is connected is considered *untrusted*; all users associating with the AP are untrusted and must be authenticated, and all traffic is checked against per-user firewall rules.

APs with a direct connection to the Wireless LAN switch can also utilize optional Serial and Power Over Ethernet (SPOE) and support the Wireless LAN switch Access Point Status LEDs .(When multiple APs are connected to a port indirectly, the LEDs provide information about the aggregate connection, not about a specific AP.)

**NOTE**—To use SPOE, the AP must be connected to the Alcatel Wireless LAN Switch without any intervening hubs, routers, or other networking equipment.

#### Indirect Connection

The Alcatel AP can be also be connected to the Alcatel Wireless LAN Switch through a Layer 2/Layer 3 network. In this topology, the Wireless LAN switch port connected to the network is considered *trusted*; the traffic is verified to ensure it is a recognized part of the internal network. Indirect deployment results in minimal disruption to existing infrastructure.

Indirect deployment requires that there are no Network Address Translation (NAT) devices in the path between the AP and the Alcatel Wireless LAN Switch. Also, if there is a firewall between AP and switch, the following protocols/ports should be allowed to pass between them:

- GRE
- UDP 8211
- DHCP
- DNS

# **Access Point Setup**

## Requirements

You must have the following:

- An operational Alcatel Wireless LAN Switch with a valid IP route to the LAN segment to which the AP will be connected.
- An appropriate physical location for the new AP.

We recommend an up-to-date site survey using the Web UI's RF Plan tool to help determine the optimal location for your AP.

• An Alcatel AP physically installed and connected to the network according to the appropriate hardware installation guide.



# **AP Provisioning**

There are several methods for setting up and configuring Alcatel APs for use with the Wireless LAN switch. Depending on your network configuration, the following methods are available, each of which is explained in greater detail below:

- Plug and Play-A limited situation where APs can be connected to the Wireless LAN switch and brought into operation with only default configuration settings.
- AP Programming Mode-AP configuration parameters are set using the switch CLI or Web interface and then pushed to APs connected to specially designated switch ports. This method is useful for adding Alcatel APs to a highly customized network. See page 430.
- Simplified AP Provisioning-A streamlined example for specifying only the IP address of the AP's host Wireless LAN switch. This is the most common customizing. See page 429.
- Manual Provisioning–APs can be individually provisioned using a terminal connected directly to the AP serial port. This method should be used only as a last resort. For more information, refer to the Alcatel AP Installation Guide and the Alcatel AOS-W User's Guide.
- Reprovisioning–This method allows you to make configuration changes to APs which are already configured and deployed. See page 436.

## Plug and Play

Alcatel APs and Wireless LAN switches are shipped with default settings that allow them to be connected together with no extra configuration. This is a limited scenario, however, and requires the following conditions:

- DNS must be available on your network and must be configured to resolve the default Alcatel-master hostname to the Wireless LAN switch IP address.
- DHCP must be available on your network.
- The Alcatel AP must begin with factory default values.

If the AP and your network meet these requirements, you can connect the AP to the switch with no further configuration. When the AP boots, it will be assigned a default location ID of 255.255.65535.

**NOTE**—If the AP has been previously used in another network and configured with settings compatible to the new Wireless LAN switch, plug and play may function correctly. However, if the AP uses settings incompatible with the new network (wrong hostname or static IP address), plug and play will fail. If the AP does not work with the new Wireless LAN switch, return the AP to its original network and reset the AP to its factory defaults before moving it again, or perform manual provisioning.

# Simplified AP Provisioning

This is a streamlined example of the AP Programming Mode. This procedure represents the most typical customization: setting the master Wireless LAN switch IP address on the AP. In this example, DNS is not required.

**NOTE**—If you would like more control over AP configuration settings, or for more details on any of the commands in the procedure, see "AP Programming Mode" on page 430.

To perform simplified AP provisioning through the CLI, use the following procedure:

1 Enter the AP programming sub-mode on the switch:

```
(Alcatel) # config terminal(Enter configuration mode)(Alcatel) (config) # program-ap(Enter AP programming sub-mode)
```

2 Enable AP programming mode on an available switch port or port range:

```
(Alcatel) (program-ap) # port-range <slot>/<start[-end]>(Specify AP programming port range)
(Alcatel) (program-ap) # enable (Enable AP programming on the ports)
```

- 3 Connect the target APs to the specified AP programming ports on the switch and power up the APs.
- 4 Verify that all target APs are detected by the switch.

(Alcatel) (program-ap) # show provisioning-ap-list

Detected APs will be shown on the provisioning list. It may take a couple minutes for all APs to be detected. Repeat the command until all expected APs appear on the list.

5 Configure the IP address of the host (master Wireless LAN switch) for the AP.

```
(Alcatel) (program-ap) # hostip <Wireless LAN switch IP address>
(Alcatel) (program-ap) # masterip <Wireless LAN switch IP address>
```

6 Verify the AP configuration settings.

```
(Alcatel) (program-ap) # show ap-params
```

This command displays the settings that are ready to be uploaded to the APs. Make any changes necessary before proceeding.



Once the settings are correct, push the configuration to the APs.

(Alcatel) (program-ap) # **config all** (Upload configuration to the APs)

8 Disable the AP Programming Mode:

(Alcatel) (program-ap) # **disable** (*Return ports to normal operation*)

## **AP Programming Mode**

The AP Programming Mode offers extended provisioning for adding Alcatel APs to a highly customized network. To perform extended provisioning through the CLI, use the following procedure:

1 Enter the AP programming sub-mode on the switch:

```
(Alcatel) # config terminal(Enter configuration mode)
(Alcatel) (config) # program-ap(Enter the AP programming sub-mode)
```

2 Enable AP programming mode on the port(s) you will use for configuring Alcatel APs:

Any switch port (or range) can be placed in AP Programming Mode. While in AP Programming Mode, normal network traffic on the designated ports is suspended. When AP configuration is complete, the AP Programming Mode must be disabled so that the ports can resume their normal network functions.

**NOTE**—Before enabling AP programming mode on any port, make sure that the port is available and is not connected to working APs or other networking equipment.

The CLI command to set a port or port range for AP provisioning is as follows:

port-range <Physical Switch Slot>/<Port>[-<End port of range)>]

For example, to set slot 2 port 1 for AP Programming Mode:

```
(Alcatel) (program-ap) # port-range 2/1(Specify an AP Programming port)
(Alcatel) (program-ap) # enable(Enable AP programming on the port)
```

Or to set a range of ports (slot 2 ports 1 through 3):

```
(Alcatel) (program-ap) # port-range 2/1-3(Specify a port range)
(Alcatel) (program-ap) # enable(Enable AP programming on the range)
```

3 Connect the Alcatel APs that require configuration to one of the specified AP programming ports on the switch.

**NOTE**—Although a direct Ethernet connection between the AP and Wireless LAN switch is preferred, a Layer 2 hub can be used to connect more than one Alcatel AP to any specific AP programming port.

4 Power up the connected APs.

5 Verify that the APs connected to the AP programming ports are detected by the switch.

Use the following command to list the APs detected on the AP programming ports:

```
(Alcatel) (program-ap) # show provisioning-ap-list
```

Depending on each AP's status, the following is displayed:

- Unprovisioned APs-For APs which have never been configured or have been reset to factory default settings, the APs MAC address is shown, the hostname is shown as Alcatel-master, and the state is shown as unprovisioned.
- Previously Configured APs–For APs witch have been previously configured prior to being connected to an AP provisioning port, the AP's current settings are shown and the *state* is shown as unprovisioned.
- In Progress–For APs which are in the process of uploading configuration settings (after the AP programming mode config command is issued), the state is in progress.
- Provisioned APs-For APs which have been successfully configured though the AP provisioning port, the AP's provisioned settings are shown and the state is provisioned.
- **NOTE**—It may take a couple of minutes for all APs to be detected. Repeat the command until all expected APs appear on the list.

If expected APs do not appear on the list, check the following troubleshooting points:

- Make sure there is no Layer 3 routing device between the AP and Wireless LAN switch.
- Make sure that the correct Wireless LAN switch ports are set for AP programming mode and that the enable command has been executed (see Step 2).
- Make sure that the AP is powered on and connected to the correct Wireless LAN switch port.



- Disconnect and reconnect the AP from the switch port. If the AP list had previously been cleared using the clear-provisioning-ap-list command, the AP should now reappear.
- If the AP was previously configured on a different network with settings incompatible with the current network (wrong hostname or static IP address), return the AP to its old network and reset the AP to its factory defaults before moving it again (see "AP Reprovisioning" on page 436).
- If the AP still cannot be detected on the Wireless LAN switch, manual provisioning may be required for the AP.

#### 6 Configure the Host information, if necessary.

In order to provide centralized management of the APs, each Alcatel AP downloads its software image and configuration files from the master Alcatel Wireless LAN Switch.

Setting the correct host information depends on the following:

- Does your network use direct IP addresses or DNS with host names?
- If using host names, is Alcatel-master acceptable for the master Wireless LAN switch, or do you need to define a different name?

Depending on your answers, select one of the following lettered steps.

#### A My network uses DNS. The Alcatel-master host name is acceptable.

This is the default. This requires that your DNS be configured to resolve the "Alcatel-master" host name to the IP address of the master Alcatel Wireless LAN Switch. Unless your system has been previously configured for different settings, you can skip to Step 3 on page 443.

Otherwise, if your system was previously configured for a different setup, you should manually set the host name to its default value:

(Alcatel) (program-ap) # hostname Alcatel-master

**NOTE**—The masterip and hostip commands (below) also affect how source files are selected and if previously set should be cleared when using this approach. To clear settings, use the no masterip and no hostip commands.

When finished, proceed to Step 3 on page 443.

# B My network uses DNS, but I want to use a different host name for the Wireless LAN switch.

This requires that the hostname setting be configured with your chosen host name for the master Alcatel Wireless LAN Switch and that your DNS be configured to resolve the specified host name to the IP address of the master Alcatel Wireless LAN Switch.

To change the host name, use the following command:

(Alcatel) (program-ap) # hostname < Wireless LAN switch host name >

**NOTE**—The masterip and hostip commands also affect how source files are selected and if previously set should be cleared when using this approach. To clear settings, use the no masterip and no hostip commands.

When finished, proceed to Step 3 on page 443.

## (C) My network uses direct IP addresses instead of DNS.

If using direct IP addresses in your network, use the following commands:

(Alcatel) (program-ap) # hostip <Wireless LAN switch IP address>
(Alcatel) (program-ap) # masterip <Wireless LAN switch IP address>

**NOTE**—If the hostname setting is configured in this scenario, it will be ignored.

#### 75 Specify an IP address for a specific AP, if necessary.

If using DHCP, the AP will obtain its IP address automatically and you can skip this step. Otherwise, configure the AP with a static IP address using the following commands:

```
(Alcatel) (program-ap) # ipaddr <static IP address for the AP>
(Alcatel) (program-ap) # netmask <static IP address mask>
(Alcatel) (program-ap) # gateway (Alcatel) (program-ap) # gateway (Alcatel) (program-ap) # gateway // IP address
```

Set the location for the specific AP, if necessary.

Location settings depend on how much control you want over configuring logical groups of APs in the future.

Default Locations

If you wish all APs to be treated as a single entity for configuration and accounting purposes, you can use the default location profile (255.255.65535) and skip to Step 11 on page 435.

#### Specific Locations

By setting specific location IDs for each AP, you can later apply configuration changes or collect statistics and information for specific groups of APs (for example, all APs on a particular floor in a particular building).

To set a specific location for an individual AP, the following command is used:

**location** *<building number>.<floor number>.<device number>* where the following fields are required:

Building Number	A unique number (1-254) is required for each building in your campus.
Floor Number	Within any building, a unique number (1-254) is required for each floor.
Device Number	Within any floor, a unique number (1-65534) is required for each access point or air monitor.

If you performed the recommended site survey using the Alcatel RF Plan tool, the location data for all access points and air monitors can be found on the tool's deployment screen.



If you prefer to manually generate the location data, record the location you set for each access point and air monitor along with the following:

Device Description Note the intended function of the device (access point or dedicated air monitor) and a brief description of its service location.

X, Y Coordinates For each access point and air monitor, measure its X and Y position (in feet) relative to the bottom-left corner of the building plan as seen from overhead. For example:



Use the same fixed point and orientation for all floors in a building.

10 Verify the configuration settings targeted for the APs.

Use the following command to examine the settings which will be used for provisioning:

```
(Alcatel) (program-ap) # show ap-params
```

Any items listed as NA are blank and will erase the corresponding item from the AP when provisioning is executed. Make any necessary changes to the settings before proceeding.

## **115** Push the configuration to the APs.

Depending on how specific your AP configuration must be applies, use one of the following commands to upload configuration settings to the APs.

Using default IP address and location settings.

If you are using default DHCP setting (Step 3) and default location settings (Step 8), you can configure all APs simultaneously using the following command:

(Alcatel) (program-ap) # config all

Using specific IP address or location information.

If using specific settings for individual APs, use the following command to configure the AP:

config <AP index>

where *AP* index is the AP's entry in the list generated using the show provisioning-ap-list command. For example, to push current configuration settings to the first AP in the list:

(Alcatel) (program-ap) # config 1

Once configured, the *state* of the APs (shown using show provisioning-ap-list command) will be shown as provisioned. The configured APs can then be disconnected from the switch, deployed to their final locations, and reconnected to the network.

- If configuring specific settings for individual APs, repeat Step 6 through Step 11 of this procedure for each Alcatel AP that requires configuration.
- 14 If configuring multiple sets of APs, prepare for the next set.

Disconnect the provisioned APs from the Wireless LAN switch, set them aside for deployment, and use the following command to clear the AP provisioning list:

```
(Alcatel) (program-ap) # clear-provisioning-ap-list
```

Then collect the next set of APs to be provisioned and repeat this procedure from Step 3 on page 431.



If no other APs are to be configured, disable the AP programming mode:

```
(Alcatel) (program-ap) # disable
```

This will return all AP programming ports to their previously defined network settings.

**NOTE**—If the AP programming mode is not disabled after provisioning is complete, the affected switch ports will not work properly for normal network operations.

## Manual AP Provisioning

APs can be individually provisioned using a terminal connected directly to the AP serial port. This method should be used only as a last resort, as it provides no command error feedback and can result in misconfiguring the AP if not performed correctly.

Details on manually performing initial setup and configuration of the AP can be found in the Alcatel AP Installation Guide and the Alcatel AOS-W User's Guide.

## **AP** Reprovisioning

The following reprovisioning commands can be used to make configuration changes to APs which are already configured and deployed.

- **NOTE**—Reprovisioning does not require AP programming mode to be enabled on the Wireless LAN switch ports. Do not use the AP programming sub-mode port-range or enable commands for reprovisioning, as this will disrupt normal network operation.
- 1 Enter the AP programming sub-mode on the switch:

(Alcatel)	<pre># config</pre>	terminal	(Enter configuration mode)
(Alcatel)	(config)	<pre># program-ap</pre>	(Enter AP programming sub-mode)

# 2 Read the current information from the deployed APs you wish to reprovision.

(Alcatel) (program-ap) # read-bootinfo <AP IP address>

You can repeat this command for as many deployed APs as you wish. The configuration information for each AP will be added to the AP provisioning list, which can be displayed using show provisioning-ap-list command.

#### If desired, you can reset a deployed AP to its factory default settings:

(Alcatel) (program-ap) # reset-bootinfo <*AP* index>

where *AP index* is the AP's entry in the list generated using the show provision-ing-ap-list command.

**NOTE**—The reset-bootinfo command takes effect immediately and does not require use of the AP programming mode config or reprovision commands.

4 Otherwise, use the provisioning commands to set new parameters.

See the commands under "AP Programming Mode" on page 430 for details (hostname, hostip, masterip, ipaddr, netmask, gateway, and location).

You can list current provisioning settings using the show ap-params command.

5 Push the new provisioning parameters to the appropriate deployed AP:

(Alcatel) (program-ap) # reprovision <*AP* index>

# Accessing the AP Boot Prompt

Initial configuration of the AP is done from the AP boot prompt (apboot). The AP boot prompt can be accessed either by connecting a terminal directly to the AP serial console port, or using Telnet to connect to the AP via the Wireless LAN switch Serial-Over-Ethernet (SOE) interface.

1St If using a direct terminal connection, access the AP serial interface.

**NOTE**—If using the SOE interface for remote connection, skip this step and see Step 2 on page 438.

Otherwise, attach your local terminal to the AP serial console port. See the *Alcatel AP Installation Guide* for port and cable characteristics.

Set the terminal or terminal emulation software to use the following communication settings:

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

Once attached, press <Enter> a few times to establish communication between the AP and the terminal.



```
Proceed to Step 3 on page 439.
```

2St If using Telnet to connect to the AP remotely, access the AP through the Wireless LAN switch Serial and Power Over Ethernet (SPOE) interface.

**NOTE**—If using a terminal directly connected to the AP, see Step 1 on page 437 instead.

By default, the Wireless LAN switch does not permit Telnet access to the serial portion of the SPOE interface. To enable the serial interface for remote access to APs, log in to the Alcatel Wireless LAN Switch as the administrator and perform the following configuration command:

```
(Alcatel) (config) # telnet soe
```

Then, use a Telnet client on your management workstation to connect to the Alcatel Wireless LAN Switch IP address using logical port 2300. The connection command may vary depending on the specific software used, but commonly appears as follows:

> telnet <smitch IP address> 2300

When prompted, log in to the Alcatel Wireless LAN Switch as the administrator:

user: admin
password: <administrator password (not displayed)>

This will present you with the Alcatel Wireless LAN Switch SOE console prompt:

```
Available commands:
  baud [9600|19200|38400|57600|115200]
  connect <slot/port>
  exit (no args)
  soe>
```

Connect to the Alcatel Wireless LAN Switch port to which the OmniAccess Reference is physically attached:

```
soe> connect <slot number>/<port number>
```

where *slot number* is the physical slot of the line card in the Wireless LAN switch, and *port number* is the physical port.

3St Interrupt the AP boot process.

Depending on how far the AP boot has booted, use one of the following lettered steps:



When power is first connected, the AP will begin its initialization process. At any time before the autoboot timer expires, you can press any key to interrupt this process. For example:

```
APBoot 1.0.1 (Mar 7 2003 - 16:20:28)
     MPC8245 Revision 16.20 at 192 MHz: 16 kB I-Cache 16 kB D-Cache
CPU:
      Watchdog enabled
Board: ASAP Local Bus at 96 MHz
DRAM: 16 MB
POST: passed
FLASH: 4 MB
PCI: scanning bus0 ...
      dev fn venID devID class rev MBAR0
                                       MBAR1
                                               MBAR2
                                                       MBAR3
      00 00 1057 0006 060000 12 0000008 0000000 0000000 0000000
      12 00 1260 3873 028000 01 f0000008 0000000 0000000 0000000
     13 00 1317 0985 020000 11 fe000001 f0001000 0000000 0000000
     serial
In:
Out: serial
Err: serial
Net: an983b#0
Hit any key to stop autoboot: 3 <Enter><Enter>
apboot>
apboot>
```

From the AP boot prompt, proceed to "Initial Configuration" on page 441.



### (B) If the AP has completed booting.

If no key is pressed before the autoboot timer expires (default of 3 seconds), the AP will resume normal software loading and initialization functions:

Once the AP has booted and the # prompt appears, you must turn the AP off and back on, and then press any key while the AP is initializing (see Step 3-A on page 439).

To turn the AP off, disconnect its power by either unplugging its power adapter (if used) or disconnecting the FE cable (if Power Over Ethernet is used).

#### C If the AP is in a continual boot cycle.

If the AP cannot connect to the Wireless LAN switch, the AP will remain in a boot cycle looking for a switch from which to download its software and configuration:

```
BOOTP broadcast 1

DHCP IP address: 10.3.9.172

DHCP subnet mask: 255.255.255.0

DHCP def gateway: 10.3.9.254

DHCP DNS server: 10.1.1.2

ARP broadcast 1 for 10.3.9.254

TFTP from server 10.10.10.10; our IP address is 10.3.9.172; sending

through gateway 10.3.9.254

Filename 'sap.bin'.

Load address: 0x100000

Loading: T T T T T T T T T

Retry count exceeded; starting again
```

Press <Control-C> at any time to interrupt the boot cycle. You will be presented with the AP boot prompt (apboot>).

From the AP boot prompt, proceed to "Initial Configuration" on page 441.

# Initial Configuration

The Alcatel AP requires some initial configuration before it will operate. All direct configuration of the AP is done using the AP boot prompt (see page 437). Once connected to the AP boot prompt, configure the AP as follows:

From the AP boot prompt, set the intended location for the AP:

apboot> **setenv location** <br/> *setenv location <br/>
wilding number>.<floor number>.<device number>* 

If you performed the recommended site survey using the built-in RF Plan tool, the location data for all access points and air monitors can be found on the tool's deployment screen.

If you plan to manually generate the location data, record the following information for each access point and air monitor. It will be required when configuring the Alcatel Wireless LAN Switch.

- *Building Number* A unique number (1-254) is required for each building in your campus.
- *Floor Number* Within any building, a unique number (1-254) is required for each floor.
- *Device Number* Within any floor, a unique number (1-65534) is required for each access point or air monitor.
- Device Note the intended function of the device (access point or dedicated air monitor) and a brief description of its service location.
- X, Y For each access point and air monitor, measure its X and Y position (in feet) relative to the bottom-left corner of the building plan as seen from overhead. For example:



Use the same fixed point and orientation for all floors in a building.



#### 2 Specify host information, if necessary.

In order to provide centralized management of the APs, each OmniAccess Reference AP downloads its software image and configuration files from the master Alcatel Wireless LAN Switch.

Setting the correct host information depends on the following:

- Does your network use DNS with host names, or direct IP addresses?
- If using host names, is Alcatel-master acceptable for the master Wireless LAN switch, or do you want to define a different name?

Depending on your answers, select one of the following lettered steps.

#### A My network uses DNS. The Alcatel-master host name is acceptable.

This is the default. This requires that your DNS be configured to resolve the "Alcatel-master" host name to the IP address of the master Alcatel Wireless LAN Switch.

By default, the AP is configured to use the Alcatel-master host name. However, if the AP was previously configured for a different setup, you should manually set the host name on the AP to its default value:

apboot> setenv servername Alcatel-master

**Note**—The master and serverip environment variables also affect how source files are selected and if previously set should be cleared when using this approach. To clear a variable, enter the setenv *variable* command with no host or address value.

When finished, proceed to Step 3 on page 443.

#### B My network uses DNS. I want to use a different host name for the Wireless LAN switch.

This requires that the servername environment variable be configured with your chosen host name for the master Alcatel Wireless LAN Switch and that your DNS be configured to resolve the specified host name to the IP address of the master Alcatel Wireless LAN Switch.

To change the host name, configure the AP as follows:

apboot> setenv servername < Wireless LAN switch host name>

**Note**—The master and serverip environment variables also affect how source files are selected and if previously set should be cleared when using this approach. To clear a variable, enter the setenv *variable* command with no host or address value.

When finished, proceed to Step 3 on page 443.

#### O My network uses direct IP addresses instead of DNS.

If using direct IP addresses in your network, use the following commands:

apboot> **setenv serverip** <Wireless LAN switch IP address> apboot> **setenv master** <Wireless LAN switch IP address> Note-If the servername environment variable is configured in this scenario, it will be ignored.



#### Specify an IP address, if necessary.

If using DHCP, the OmniAccess Reference will obtain its IP address automatically and this step can be skipped. Otherwise, the AP must be manually configured with a static IP address using the following commands:

apboot> **setenv** ipaddr <static IP address for the AP> apboot> **setenv netmask** <*static IP address mask*> apboot> setenv gatewayip <default gateway IP address>

4 Save the configuration and reboot the OmniAccess Reference.

apboot> **save** apboot> **boot** 

Once the AP has been configured with initial settings, the Wireless LAN switch must be configured with the appropriate AP settings (see "Wireless LAN Switch Setup for APs" on page 454).



# **Advanced AP Configuration**

The following sections cover the following:

- How to access the Alcatel AP configuration prompt
- Commands and settings that can be configured
- Example configurations for common scenarios

#### **APBoot Commands**

The following commands are available from the apboot prompt:

🗕 help

List the available commands and a brief explanation of each.

printenv

List the environment variables and their current settings. The environmental variables represent the APs configurable parameters See page 445 for a list of variables.

#### setenv <environmental variable> [<new value>]

Set the specified environmental variable to a new value. This is used for changing the AP configuration. If the value is omitted, the variable is reset to its default value. See page 445 for a list of configurable variables.

saveenv

Save the environment variables to persistent storage. Make sure to save configuration changes before rebooting the AP.

#### boot

Boot the AP using the currently saved environmental variables. Any unsaved changes to the variables will be lost.

#### ping <IP address>

Ping the specified IP address. This is useful for testing network access.

reset

Restart the AP. This is similar to cycling the power on the AP.

## **APBoot Environment Variables**

The following environment variables can be configured using the setenv command and listed using the printenv command (see page 444):

**NOTE**—Spelling is critical when defining environment variables. The AP may not function properly if environment variables are misspelled or misconfigured.

Variable	Description
bootdelay	The length of time (in seconds) of the autoboot timer. This is the delay during which the user can interrupt the boot process and access the apboot prompt (see page 437).
	Default = 3
location	The location where the AP will be permanently installed, specified as:
	  ding number>. <floor number="">. <device number=""></device></floor>
	The location specifies which configuration profile will be downloaded to the AP from the Wireless LAN switch. See page 451 for more location information.
	Default = -111 (unconfigured)
master	This is the IP address or hostname of the Alcatel Wireless LAN Switch that controls the AP. The AP downloads its configuration from the specified switch.
	If a hostname is specified, your DNS server must be configured to resolve the hostname to the master Alcatel Wireless LAN Switch.
	The master variable overrides the value of serverip and servername (below) if configured.

TABLE 21-2	Configurable	Environment	Variables
	Conngarabio		• an abroo



Variable	Description
servername	This is the hostname of the Alcatel Wireless LAN Switch (or TFTP server) that holds the AP software image and/or configuration files.
	When using this variable, your DNS server must be configured to resolve the specified hostname to the appropriate location. The default value is Alcatel-master.
	If not using DNS, use the master and serverip variables instead.
	The servername variable overrides the value of serverip (for both software and configuration) and is overridden by the master variable (for configuration only) if configured.
serverip	This is the IP address of the Alcatel Wireless LAN Switch (or TFTP server) where the AP software and/or configuration files are stored. This variable is usually set when DNS is not used.
	The serverip variable is overridden by the servername variable (for both software and configuration) and the master variable (for configuration only) if configured.
ipaddr	This is the IP address of the AP, specified in dotted decimal notation. If specified, the AP uses this address instead of obtaining one using DHCP.
netmask	This is the IP address mask of the AP. This is used in conjunction with the ipaddr variable to define the subnet of the AP.
gatewayip	This is the IP address of the default gateway for the IP. This is used in conjunction with ipaddr when using static addresses instead of DHCP.

#### TABLE 21-2 Configurable Environment Variables

The following environmental variables should be kept at their default values unless directed otherwise by Alcatel support:

Variable	Description
autostart	Default = yes
baudrate	<b>Default =</b> 9600
bootcmd	Default = localflash

 TABLE 21-3
 Preset Environment Variables
Variable	Description	
bootfile	This is the file name of the AP image.	
	Default = sap.bin	
ethaddr	This is the MAC address of the Ethernet interface in the AP. This is unique for each AP.	
stderr	Default = serial	
stdin	Default = serial	
stdout	Default = serial	

TABLE 21-3 Preset Environment Variables

## **AP** Configuration Examples

## Factory Default Values

By default, the environmental variables are as follows:

```
apboot> printenv
bootcmd=localflash<sup>a</sup>
bootdelay=2
baudrate=9600
servername=Alcatel-master
bootfile=sap.bin
autostart=yes
ethaddr=00:30:f1:71:d6:1d
stdin=serial
stdout=serial
stderr=serial
Environment size: 165/131068 bytes
apboot>
```

a.As of AOS-W 2.2.1, after an Access Point loads a local image, it will compare that image with the booted image. It the images differ, the AP will attempt to download the latest image using FTP. If FTP fails, the AP will attempt to download the latest image using TFTP.

NOTE—Variables not listed have no effect on this configuration.

With these settings:

- DHCP is used to obtain the APs IP address.
- DNS is used to resolve Alcatel-master for the OmniAccess 6000 IP address.



• The AP location is set to -1.-1.-1 (unconfigured) and uses the default location profile.

## Set AP Software & Configuration Source

By default, the AP downloads its software image and configuration files from a TFTP service on the Wireless LAN switch. The AP locates the switch by issuing a DNS request for the IP address of the Alcatel-master. This default requires your DNS system to be configured with the appropriate Wireless LAN switch IP address information for the Alcatel-master name.

You can, however, specify different TFTP sources (with or without DNS) for downloading the software and/or configuration files. In the following example, mytftp is the DNS name of the TFTP server to be used by the AP:

```
apboot> setenv servername mytftp
apboot> saveenv
apboot> printenv
bootcmd=tftpboot
bootdelay=2
baudrate=9600
servername=mytftp
bootfile=sap.bin
autostart=yes
ethaddr=00:30:f1:71:d6:1d
stdin=serial
stdout=serial
stdout=serial
stderr=serial
```

When booted normally (without entering APBoot mode), the AP will use the new settings and the AP console will display the following kind of information:



If DNS is not used or if you need to assign different TFTP servers for the software and configuration files, the following environment variables can be configured:

Variable	Software Image Source	Configuration File Source
master	Not applicable.	IP address or DNS name of the Alcatel Wireless LAN Switch that holds the AP configuration file.
		Highest priority. Overrides servername and serverip.
servername	DNS name of the TFTP server that holds the AP software image. Usually resolves to the Wireless LAN switch.	DNS name of TFTP server that holds the AP configuration. Usually resolves to the Wireless LAN switch.
	Highest priority. Overrides serverip.	Overridden by master. Overrides serverip.
serverip	IP address of the TFTP software server. For use instead of DNS.	IP address of the TFTP configuration server. For use instead of DNS.
	Overridden by servername.	Lowest priority. If master and servername are not configured, serverip is used.

 TABLE 21-4
 AP Download Preferences

**NOTE**—Spelling is critical when defining environment variables. The AP may not function properly if environment variables are misspelled or misconfigured.

## Set AP with Static IP Address

The AP usually obtains its IP address using DCHP. If DHCP is not used, the IP address, network mask, and default gateway environment variables should be configured manually. For example:

```
apboot> setenv ipaddr 10.3.3.3
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 10.3.3.254
apboot> saveenv
```

## Set AP with Specific Location

The location variable can be used to specify where the AP will be permanently installed. The location specifies which configuration profile will be downloaded to the AP from the Wireless LAN switch.

The location of the AP can be set manually, using the following APBoot command:

setenv location <building number>.<floor number>.<device number>

For example:

```
apboot> setenv location 1.2.1
apboot> saveenv
```

If you performed a site survey using the Alcatel Wireless LAN Switch planning tools, the location data for all access points and air monitors can be found on the tool's deployment screen.

If you plan to manually generate the location data, record the following information for each access point and air monitor. It will be needed later when configuring the Alcatel Wireless LAN Switch.

Building number

A unique number (1-255) is required for each building in your campus.

*Floor number* 

Within any building, a unique number (1-255) is required for each floor.

Device number

Within any floor, a unique number (1-65535) is required for each access point or air monitor.

### Device description

Although not strictly required, we recommend that you note the intended function of the device (access point or dedicated air monitor) and a brief description of its service location.

X, Y coordinates

For each access point and air monitor, measure its X and Y position (in feet) relative to the bottom-left corner of the building plan as seen from overhead.

Use the same fixed point and orientation for all floors in a building.



## **GRE** Tunnels

Regardless of the network topology between the AP and the Wireless LAN switch, the AP will open one GRE tunnel per radio interface to the Wireless LAN switch.

One end of the GRE tunnel will be the IP address of the AP. The other end of the GRE tunnel is specified (in descending order of priority) by the master, servername, and then serverip variables. If these variables are left to default values, the AP will use DNS to look up the well known name Alcatel-master to discover the OmniAccess 6000 Wireless LAN Switch.

Once the IP address is discovered, the AP uses its closest address (in terms of router hops) as the GRE tunnel end point at the Wireless LAN switch. You can determine the Wireless LAN switch tunnel end-point using the following AP console commands:

<pre># enable Password: <privileged password=""> # Spawning Enable Shell. Typ # show config</privileged></pre>	(Enter the AP privileged command mode) (Same as Wireless LAN switch enable password) be Ctrl-D to exit enable mode.
11G config	(Displayed first for 802.11g and then 802.11a)
essid piyer-wep-ap channel 6 txpower 0 rates 0x0	(ESSID) (Channel that the AP is on) (Transmit power set on the interface)
bssid 00:30:f1:70:49:70 beacon_interval 0 dtim period 0	(MAC address of the Wireless LAN interface)
<pre>mode monitor sensitivity 0 frag_threshold 0 rts_threshold 0 retry 255</pre>	(monitor for air monitor, or master for AP)
lms_address 10.3.3.1	(IP address of the OmniAccess 6000 GRE endpoint)
<pre>short_preamble 0 power_mgmt 0 calibrate 0 encryption 0</pre>	(shown for 802.11g only) (Set to 1 if power management is enabled on the interface) (Set to 1 if calibration is in progress)
location 1.2.1 walkabout 0 mtu 1564 ageout 300 heartbeat 40	(Location configured for the AP) (Set to 1 if walkabout is in progress) (Result of MTU discovery) (Ageout for inactive STA in seconds) (Number of successful heartbeats on tunnel to the switch)

The value of lms\_address is the Wireless LAN switch tunnel end point in use by AP.

## Wireless Client IP Address

The wireless clients associating with the AP will get an IP address in the VLAN that contains the Wireless LAN switch GRE tunnel end-point IP address.

## **GRE Tunnel Configuration**

This release supports GRE tunneling between the Alcatel Wireless LAN Switch and other GRE-capable devices. Up to four tunnels can be configured.

- Log in as the administrator and access the switch configuration mode.
- 2 Configure a tunnel interface.

The tunnel interface defines the local and remote end-points for the GRE tunnel, as well as the IP address (or range) of the tunnel network. The following commands are used to configure a tunnel on the Wireless LAN switch:

```
(Alcatel) (config) # interface tunnel <tunnel ID>
(Alcatel) (config-if) # ip address <tunnel IP address> <tunnel netmask>
(Alcatel) (config-if) # tunnel source <local end-point>
(Alcatel) (config-if) # tunnel destination <remote end-point>
(Alcatel) (config-if) # tunnel mode gre ip
```

where the following parameters apply:

tunnel ID	The local ID (1-2147483647) of the tunnel being defined on the switch.		
tunnel IP address	The base IP address of the tunnel. This represents the entrance to the tunnel. Static routes direct traffic into the tunnel through this address.		
tunnel netmask	The subnet mask used with the <i>tunnel IP address</i> to create a tunnel network range.		
local end-point	The local end-point of the tunnel on the Alcatel Wireless LAN switch. The local end-point can be one of the fol- lowing:		
	<pre><interface address="" ip=""> vlan <vlan id=""> loopback</vlan></interface></pre>		
remote end-point	The IP address of the remote end-point of the tunnel on the other GRE device.		



### 3 Direct traffic into the tunnel.

Traffic can be directed into the tunnel using static routes and/or ACLs:

Using the tunnel as the next hop for a static route.

(Alcatel) (config) # ip route <dest. address> <dest. netmask> <tunnel IP address>

where the following parameters apply:

destination address	The base IP address of the destination on the other side of the tunnel.
destination netmask	The subnet mask used with the <i>destination address</i> to create an address range.
tunnel IP address	An IP address on the tunnel network defined in the previous step. This is used as the next hop for traffic destined for the remote network.

Using an ACL to redirect traffic into a specified tunnel:

A session-based Access Control List (ACL) can be used to redirect selected traffic into a tunnel. In the following example, an ACL rule named redirguest is used to send traffic defined by the guest role into tunnel 1:

```
(Alcatel) (config) # ip access-list session redirguest
(Alcatel) (config-sess-redirguest) # user any any redirect tunnel 1
(Alcatel) (config-sess-redirguest) # any user any permit
(Alcatel) (config-sess-redirguest) # user-role guest
(Alcatel) (config-role) # session-acl redirguest
(Alcatel) (config-role) # no session-acl control
(Alcatel) (config-role) # no session-acl cplogout
```

**NOTE**—This example assumes that the guest user-role has already been defined.

# Wireless LAN Switch Setup for APs

The following sections cover the following:

- The different types of AP configuration profiles stored on the Wireless LAN switch
- Commands and settings that can be configured
- Example configurations for common scenarios

## **Configuration Profiles**

Many AP attributes are configured and stored in profiles on the Wireless LAN switch. The profiles can be based on location index or BSSID.

## Location-Based Profiles

AP configuration profiles can be based on the unique location index (*building.floor.device*) assigned to each AP during its initial setup (see page 451). These location-based configuration profiles are stored on the Wireless LAN switch and are downloaded to the appropriate APs during their startup process.

## Accessing the AP Location Sub-Mode

To configure AP attributes based on location, use the following commands from the privileged mode:

(Alcatel) # configure terminal Enter Configuration commands, one per line. End with CNTL/Z (Alcatel) (config) # ap location <br/>
configure terminal

Once in the location configuration sub-mode, use the AP Attribute Commands (see page 459) to set AP attributes.



## Using AP Location Wildcards

The location profiles allow zero (0) to be used as a wildcard in the location index. This allows you to configure AP attributes for the entire system, a particular building, or a single floor.

The profile system is also hierarchical: the attributes in more generic profiles (those with more wildcards) are overridden by the attributes in the more specific profiles (those with fewer wildcards). This lets you create a set of default attributes for all APs, and then add layers of attribute overrides for each building, floor, and AP.

### • The Base Profile

The base profile uses location index 0.0.0 (all wildcards). This special profile holds the default attributes used for all APs in the system, but can be overridden by any other profile.

Building Profiles

A building profile uses the location index *<building>*.0.0 (wildcards for *floor* and *device*). Attributes configured in building profiles override those in the base profile. Unless overridden by floor or individual profiles, these attributes affect all APs in the specified building.

Floor Profiles

A floor profile uses the location index *<building>.<floor>.*0 (wildcard for *device*). Attributes configured in floor profiles override those in the base and building profiles. Unless overridden by individual profiles, these attributes affect all APs on the specified floor.

### Individual AP Profiles

Attributes configured for an individual AP (no wildcards) always override those in the base, building, and floor profiles.

Attributes in the various profiles are treated individually. Only the attributes which are specifically configured in one profile will override the more generic profiles. For example:

System Default	Base 0.0.0 Profile	AP 1.2.1 Profile	Result AP 1.2.1 Configuration
ageout 1000			ageout 1000
ap-enable enable			ap-enable enable
beacon-period 100	beacon-period 300		beacon-period 300
dtim-period 2	dtim-period 0		dtim-period 0
essid (blank)		essid lab1b	essid lab1b
max-clients 0	max-clients 30	max-clients 15	max-clients 15
max-retries 3			max-retries 3
mode ap-mode			mode ap-mode
opmode opensystem			opmode opensystem
power-mgmt enable			power-mgmt enable
rts-threshhold 2333			rts-threshhold 2333
short-preamble enable			short-preamble enable
tx-power 2			tx-power 2
phy-type a: channel 36 rates 6,9,12,18,24,36,48,5 4			phy-type a: channel 36 rates 6,9,12,18,24,36,48,5 4
phy-type g: channel 1 rates 1,2,5,11			phy-type g: channel 1 rates 1,2,5,11

The highlighted attributes override those in the other profiles.

Also, when an attribute in a more specific profile is cleared (see the no command on page 460), the result configuration uses value from the next more generic profile. For example, if the max-clients value in the AP 1.2.1 profile above is cleared (no max-clients), the base profile value would be used—not the system default.



## The Unconfigured AP Profile

APs are typically assigned a unique location code when first installed. If this is not done, the AP will use the default location index -1.-1.-1 to indicate that it is not configured. You can define a configuration profile for location -1.-1.-1 to be used for any unconfigured AP.

For example, if you wanted to be sure that unconfigured APs were disabled, you could specify the ap-enable disable attribute in the profile. See page 459 for attribute details.

### **BSSID-Based Profiles**

AP profiles can also be specified for a BSSID. There is no hierarchical lookup for BSSID-based profiles. Each specific BSSID profile is applied to the AP radio interface with a matching BSSID.

The following Wireless LAN switch commands are issued to enter the AP BSSID configuration sub-mode:

(Alcatel) # configure terminal Enter Configuration commands, one per line. End with CNTL/Z (Alcatel) (config) # ap bssid <BSSID>

# **AP Attribute Commands**

## AP Configuration Mode

The following commands are available from the AP location or BSSID configuration sub-modes:

ageout <number of seconds>
 Specify the amount of time a client is allowed to remain idle before being aged out. The default is 1000 seconds.

### ap-enable {enable|disable}

Enable or disable the AP. The default is enabled.

 beacon-period <number of milliseconds> Specify the beacon period for the AP. The beacon advertises the APs presence, identity and radio characteristics to wireless clients. The default is 100 milliseconds.

dtim-period <number of beacons>

Specify the interval between sending DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to *sleep*, the client must revive at least once during the DTIM period to receive broadcasts. The default is 2.

essid <ESSID string (31 characters maximum)>

Specify the ESSID for the AP. This names the network or collection of APs to which the AP belongs. Other APs in the same network can have the same ESSID.

max-clients <number of clients (0-255)>

Specify the maximum number of wireless clients for the AP. The default is 0. This ensures that the AP does not begin associating wireless clients until explicitly allowed.

max-retries <number of retries>

Specify the maximum number of retries allowed for the AP to send a packet. The recommended range is between 3 and 7. The default is 3.

### mode {ap\_modelam\_mode}

Specify the mode for the AP:

- ap\_mode The AP provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. This is the default.
- am\_mode The device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.



no <command>

Clear the specified command attributes in the current profile.

**NOTE**—If using location-based profiles, any specific AP will use the first defined (non-cleared) attribute in profile hierarchy: favoring AP, floor, building, base, or system default profile (in order of descending priority).

#### opmode <encryption mode list>

Specify a comma separated list from the following:

opensystem	No encryption. Traffic is sent in the clear. This is the default.
staticWep	Use Wireless Equivalent Privacy (WEP) protocol for encryption with administratively defined keys. See the wep-key commands.

dynamicWep Use WEP with keys negotiated when joining the network.

### phy-type {alg}

Enter the configuration sub-mode for either the 802.11a or 802.11g physical layer type. Subsequent configuration commands apply only the selected physical layer type. In addition to the regular location and BSSID mode commands, channel and rate can be set (see page 462).

### power-mgmt {enable|disable}

Enable or disable power management. The default is enabled. Disabling power management can provide a slight increase in network performance, but should be done only in networks where power management is disabled on all wireless clients.

• rts-threshhold <size of packets>

Specify the RTS threshold. Wireless clients transmitting packets larger than the threshold will issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air packet collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting. The default is 2333 bytes.

#### tkip-key{1|2|3|4} <key string (16 or 32 characters hexidecimal)>

Used when opmode is set for staticTkip. This command specifies one of four static TKIP keys. The specific key to be used is selected using the tkip-transmitkey command.

#### tkip-transmitkey <key index (1-4)>

Used when <code>opmode</code> is set for <code>staticTkip</code>. Specify which static TKIP key to use. The default is 1.

#### tx-power <level (1-4)>

This is usually set automatically during network calibration. It specifies the transmit power level for the AP. The pre-calibration default is 2.

• wep-key{1|2|3|4} <key string (5 or 13 characters hexidecimal)>

Used when opmode is set for staticWep. This command specifies one of four static WEP keys. The specific key to be used is selected using the wep-transmitkey command.

wep-transmitkey <key index (1-4)>

Used when <code>opmode</code> is set for <code>staticWep</code>. Specify which static WEP key to use. The default is 1.



### Physical Layer Sub-mode

In addition to the regular AP attribute commands, the following commands are also available from the AP 802.11a or 802.11g physical layer configuration sub-modes:

**channel** <*channel number*>

Set the channel number for the AP physical layer.

- For 80211.a: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, or 161. The default is 36.
- For 80211.g: 1 through 11. The default is 1.

#### rates <list of rates>

Set the rates available for the AP physical layer.

- For 802.11a: Specify from a comma separate list of 6, 9, 12, 18, 24, 36, 48, and 54.
- For 802.11g: Specify from a comma separate list of 1, 2, 5 and 11.

By default, all rates are enabled.

#### short-preamble {enable disable}

For 802.11g. Enable or disable short preamble. The default is enabled. In a mixed radio environment, some wireless client stations operating 802.11g radios in 802.11b mode may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble.

## **Wireless Client Station Attributes**

Station management can be configured to enable DOS-prevention features or WECA compliance features for wireless clients.

#### stm dos-prevention {enabledisable}

If enabled, the Alcatel APs will ignore de-authentication packets from client stations. This does not affect third-party APs. The default is disabled.

stm strict-compliance {enable|disable}

If enabled (the default), the AP will deny the client association request if the AP and client station have no common rates defined. Some legacy client station which are not fully 802.11 compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.

# **Order of Precedence for Profile Attributes**

## Channel and Transmit Power

Settings for the AP channel and transmit power attributes are obtained using the following priorities (highest to lowest):

- 1 Matching BSSID specific profile
- Matching location specific profile (exact match, without any wildcards)
- **3** Results of a site survey stored in the WMS database.
- Result from initial AP placement configuration in the WMS database.
- 5 Hierarchical lookup to find the closest match between the AP location and profile.

## Mode

The AP can operate in three modes:

- ap Operating as an access point for wireless clients
- am Operating as a dedicated air monitor
- apm Operating as an air monitor which can transition to an access point if a neighboring AP goes down

The setting for the AP mode is obtained using the following priorities (highest to lowest):



- 1 Matching BSSID specific profile
- Matching location specific profile (exact match, without any wildcards)
- 3 Results of a site survey stored in the WMS database. If an AP is initially configured to be off (due to overbuilding the network coverage for example), the device will operate in apm mode instead.
- 4 Result from initial AP placement configuration in the WMS database.
- 5 Hierarchical lookup to find the closest match between the AP location and profile.

### Other Attributes

The setting for all other AP attributes is obtained using the following priorities (highest to lowest):

- 1 Matching BSSID specific profile
- 2 Hierarchical lookup to find the closest match between the AP location and profile.

# **CLI Configuration Examples**

This section has typical commands for configuring AP attributes on the Wireless LAN switch. The following sections assume you are logged-on to the Wireless LAN switch as the administrator in privileged mode.

## Disable WEP for Base Location Profile

**NOTE**—In this example, the built-in help function is used to show available options before the actual configuration commands are issued. The help commands (those ending with a question mark "?") are not strictly necessary.

### Access the configure mode.

```
(Alcatel) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

## 2 Access the AP configuration sub-mode for base location 0.0.0.

```
(Alcatel) (config) # ap ?
bssid Specify the BSSID
location Specify location as bldg.floor.location(0 is wildcard)
(Alcatel) (config) # ap location ?
    Specify location as bldg.floor.location(0 is wildcard)
(Alcatel) (config) # ap location 0.0.0
```

The 0.0.0 location index uses wildcards (0) in all the location fields. This selects all APs (regardless of the building, floor, or device number) for configuration in the commands that follow.



### 3

## Set the opmode to opensystem.

(Alcatel) (sap-config	location 0.0.0) # ?	
ageout	Seconds of inactivity after which client is aged out	
ap-enable	One of enable or disable	
authalgo	Only opensystem is supported. No support for sharedkey	
beacon-period	Beacon Period for the AP. Typically 100	
dtim-period	Interval between sending DTIMs in beacon	
essid	$\ensuremath{ESSID}$ for the AP. Should be a string of max. 32 characters	
max-clients	Max Wireless CLients for AP. 0 thru 256	
max-retries	Maximum number of retries allowed for AP to send a packet	
mode	One of am_mode or ap_mode (air monitor or access point)	
no	Delete Command	
opmode	Can be a comma separated list of opensystem, staticWep, dyn-	
phy-type	Specify either .a or .g for physical layer type	
power-mgmt	'enable': Enable power management	
rts-threshhold	The RTS threshold. Packets bigger than this use RTS and $\ensuremath{C}\xspace$	
short-preamble	Can be one of enable or disable	
tkip-keyl	Specify static TKIP key 1 of 4 (length 16 or 32 bytes)	
tkip-key2	Specify static TKIP key 2 of 4 (length 16 or 32 bytes)	
tkip-key3	Specify static TKIP key 3 of 4 (length 16 or 32 bytes)	
tkip-key4	Specify static TKIP key 4 of 4 (length 16 or 32 bytes)	
tkip-transmitkey	Specify an index from 1 thru 4	
tx-power	A number from 0 thru 4	
wep-key1	Specify static WEP key 1 of 4 (length 5 or 13 bytes)	
wep-key2	Specify static WEP key 2 of 4 (length 5 or 13 bytes)	
wep-key3	Specify static WEP key 3 of 4 (length 5 or 13 bytes)	
wep-key4	Specify static WEP key 4 of 4 (length 5 or 13 bytes)	
wep-transmitkey	Specify an index from 1 thru 4	
(Alcatel) (san-config	location $(0, 0, 0)$ # oppose opensystem	
(meacer) (sup coming		

### **Resetting the Base Location Profile**

The base location 0.0.0 profile cannot be deleted from the switch as other profiles can. In order to reset the base location profile to its factory defaults, enter the following commands:

```
(Alcatel) (config) # ap location 0.0.0
(Alcatel) (sap-config location 0.0.0) # restore-default
```

## Enable Static WEP for a Specific Building

To select all APs in a specific building for configuration changes, the building number is specified, but wildcards (0s) are used for the floor and device fields. For example, to select building 1:

(Alcatel) (config) # ap location 1.0.0

To enable static WEP for all APs in the specified building, the following commands are issued:

## Change ESSID for all 802.11g APs

(Alcatel) (config) # ap location 0.0.0 (Alcatel) (sap-config location 0.0.0) # phy-type g (Alcatel) (sap-config location 0.0.0 : phy-type g) # essid bap

In this example, all APs are first selected using the base location index (0.0.0). Then the selection is narrowed by entering the sub-mode for the 802.11g physical layer type. The final essid command affects all 802.11g APs.

## Set the Channel for a Specific AP

(Alcatel) (config) # ap bssid 01:02:03:04:05:06 (Alcatel) (sap-config bssid 01:02:03:04:05:06) # channel 6

In this example, only one AP is selected. The AP with the matching BSSID is set to channel 6.



# **Viewing AP Attribute Settings**

## Show a Location Profile

(Alcatel) # show ap config location 1.0.0			
CONFIG AP RESULT			
PARAMETER	802.11b/g	802.11a	
Location (Bldg.Flr.Loc)	1.0.0	1.0.0	
BSSID	N/A	N/A	
Channel	1	36	
ESSID	alpha-guest	alpha-guest	
Encryption	staticWep	staticWep	
Device Type	ap_mode	ap_mode	
Authentication	opensystem	opensystem	
Short Preamble	Enabled	N/A	
RTS Threshold (Bytes)	2333	2333	
Transmit Power (Level)	2	2	
Retry Limit	8	8	
DTIM Interval (beacon periods)	1	1	
Max Associations	64	64	
Beacon Period (millisecs)	100	100	
Basic Rates	1,2	6,9,12,18,24,36,48,54	
Transmit Rates	1,2,5,11	6,9,12,18,24,36,48,54	
AP Radio	Enabled	Enabled	
Power Management	Enabled	Enabled	
Station Ageout Time (secs)	1000	1000	
VLAN ID	7	7	
Hidden SSID	Disabled	Disabled	
Deny_Broadcast Probes	Disabled	Disabled	
b/g Mode	mixed	N/A	
Country Code	US	US	
WPA Hexkey	N/A	N/A	
WPA Passphrase	N/A	N/A	
LMS IP	N/A	N/A	
Backup LMS	0.0.0.0	0.0.0	

**NOTE**—Channel and transmit power values are determined as described on page 463.

# Show a BSSID Profile

(Alcatel) # show ap config bssid 01:	02:03:04:05:06			
CONFIG_AP_RESULT				
PARAMETER	Value			
Location (Bldg.Flr.Loc)	1.0.0			
BSSID	01:02:03:04:05:06			
Channel	6			
ESSID	alpha-guest			
Encryption	staticWep			

Show Encryption Keys for a Location

**NOTE**—For security, passwords and keys are encrypted by default. Where displayed in show commands, encrypted items appear only as asterisks (\*). To turn the encryption feature off and display passwords and keys as plain text, the encrypt disable command is available in the configuration mode.



## Show Effective Config for a Specific AP

This example shows the actual configuration that will be applied to a BSSID of a specific physical layer type at a specific location. The command traverses the configuration tree and site survey database to compile the configuration:

```
(Alcatel) # show ap effective-config bssid 01:02:03:04:05:06 location 1.0.0
phy-type g
CONFIG AP RESULT
_____
PARAMETER
                                Value
_____
                                ____
                                1.0.0
Location (Bldg.Flr.Loc)
BSSID
                                01:02:03:04:05:06
Channel
                                6
ESSID
                                alpha-guest
                                staticWep
Encryption
. . .
```

### Show Client Management Configuration

Station management can be configured to enable DOS-prevention features or WECA compliance features for wireless clients.

```
(Alcatel) (config) # stm ?
dos-prevention strict-compliance Enable/Disable STM DoS prevention capabilities
(Alcatel) (config) # stm dos-prevention {enable|disable}
(Alcatel) (config) # stm strict-compliance {enable|disable}
```

To view the station management configuration:

# **Viewing AP Information and Statistics**

List Bootstrapped APs

(Alcatel) # show ap registered location 0.0.0					
AP_REGIS	STRATIONS_P	RESULT			
LOC S	SAP_IP	LMS_IP	.b_MAC	.a_MAC	STATE
1.1.1 10 1.1.2 10 1.1.3 10 1.1.4 10 1.2.1 10 1.2.2 10 1.2.3 10 Num APs:	0.2.13.194 0.2.12.253 0.1.1.56 0.2.12.212 0.3.25.252 0.3.25.237 0.3.25.253 :7	10.2.13.254 10.2.12.254 10.3.25.1 10.2.12.254 10.3.25.1 10.3.25.1 10.3.25.1	00:30:f1:70:49:93 00:30:f1:70:49:4c 00:30:f1:70:49:4c 00:30:f1:70:49:65 00:30:f1:70:49:70 00:30:f1:70:49:72 00:30:f1:70:49:73	00:30:f1:71:93:8f 7 00:30:f1:71:93:7d 7 6f 00:30:f1:71:93:3d5 00:30:f1:71:93:54 7 e 00:30:f1:71:93:53 7 1 00:30:f1:71:93:55 7 d 00:30:f1:71:94:08 7	7 7 7

For STATE, the expected value is 2 (sent tunnel response) or 7 (steady state)



```
List Management Registered APs
```

## List AP Association Table

## List Wireless STA State

```
(Alcatel) # show stm state 00:08:21:31:b1:17
STA Table
_____
bssid
              auth assoc aid
____
              ____ ___
00:30:f1:70:49:93 y n
00:30:f1:70:49:65 y y 6
Association Info
_____
bssid
              aid
____
               ____
00:30:f1:70:49:65 6
```

## List AP Status LED State

(Alcate	<pre>1) # show ap-leds 2</pre>	(View LED states for the line card in slot 2)	
LED Stat	e -		
s/p le	d reason		
2/0 1	unsecure ap found		
2/1 1	unsecure ap found		
2/2 1	unsecure ap found		
2/3 6	no ap connected		
2/4 6	no ap connected		
2/5 6	no ap connected		
2/6 6	no ap connected		
2/7 6	no ap connected		
2/8 6	no ap connected		
2/9 6	no ap connected		
2/10 6	no ap connected		
2/11 6	no ap connected		
2/12 1	unsecure ap found		
2/13 6	no ap connected		
2/14 5	ok		
2/15 5	ok		
2/16 6	no ap connected		
2/17 6	no ap connected		
2/18 6	no ap connected		
2/19 6	no ap connected		
2/20 6	no ap connected		
2/21 6	no ap connected		
2/22 6	no ap connected		
2/23 5	ok		

Use the following command to view the state of the Access Point Status LED for a specific line card:



## List Configuration Applied on an AP

```
      (Alcatel) # show am config 10.1.1.56

      Wireless LAN Configuration

      ------

      bssid
      essid

      tx-pwr chan lms
      encr

      mode
      rat+

      -----
      -----

      00:30:f1:70:49:6f Alcatel-alpha-ap 4
      6
      10.3.25.1 s-wep/ master f +

      00:30:f1:71:93:d5 Alcatel-alpha-ap 4
      52
      10.3.25.1 s-wep/ master ff0+
```

## List Statistics for an AP or STA

```
(Alcatel) # show ap stats 10.2.12.212 00:30:f1:70:49:65
Frame rates
-----
retry low-speed non-unicast recv-error frag bwidth
----- 0 33 100 0 0 8
RSSI
----
cur-signal low-signal high-signal cur-noise low-noise high-noise
----- 100 100 165 13 9 39
```

Chapter 21

Frame rates \_\_\_\_\_ retry low-speed non-unicast recv-error frag bwidth ----- ----- ------ ------0 9 100 0 0 7 RSSI \_\_\_\_ cur-signal low-signal high-signal cur-noise low-noise high-noise 100 100 165 12 9 39 Raw Stats \_\_\_\_\_ tx-pkt tx-byte rx-pkt rx-byte tx-retry-pkt rx-retry-pkt tx-frag-pkt rx+ 247960 19878186 27075 4577596 18 3559 0 0 + Tx Frame Type Stats \_\_\_\_\_ mgmt-pkt mgmt-byte ctrl-pkt ctrl-byte data-pkt data-byte ----- ----- ------ ------ -------247568 19804838 0 0 392 73348 Rx Frame Type Stats \_\_\_\_\_ mqmt-pkt mqmt-byte ctrl-pkt ctrl-byte data-pkt data-byte ----- ------ ------ ------548 25264 0 0 26527 4552332 Dest Addr Type Stats \_\_\_\_\_ bcast-pkt bcast-byte mcast-pkt mcast-byte ucast-pkt ucast-byte \_\_\_\_\_ \_\_\_ \_\_\_\_\_ 247684 19833378 7 975 269 43833 Frame Size Packet Stats \_\_\_\_\_ type 0-63 64-127 128-255 256-511 512-1023 1024+ ---- ---- ------ ------ -----tx 96 134 114 42 3 3 rx 10397 9292 4241 1982 66 549 Tx Frame Rate Stats \_\_\_\_\_ pkt-1m byte-1m pkt-2m byte-2m pkt-5.5m byte-5.5m pkt-11m byte-11m \_\_\_\_\_ \_\_\_\_\_ 14 518 0 0 0 0 34 2949 Rx Frame Rate Stats \_\_\_\_\_ pkt-1m byte-1m pkt-2m byte-2m pkt-5.5m byte-5.5m pkt-11m byte-11m \_\_\_\_\_ \_\_\_\_\_\_ 1568 135551 5699 768444 5736 924896 14072 2748705



## List Status for an AP

(OmniAccess 6000) #show ap status 10.1.1.114

```
Station Table
MAC BSSID Assoc_State AID PS_State Tx_Pkts Rx_Pkts PS_Pkts Tx_Retries Tx_Rate Rx_Rate Last_ACK_SNR Last_Rx_SNR Tx_Times
tamp Rx_Timestamp
_____
-----
Descriptor Usage
Interface Queue Alloc Free In-use Max Failed
----- ---- ----- ----- ----
Interface counters
Interface Rx_pkts Rx_errors Rx drops Tx_pkts Tx_errors Tx_drops Resets
                                          - - -
wifi0 112364636 1715080 2037663 311285 105368 0
wifi1 9519548 90112 51 381002 21652 0
                                                                  41
                                                                  1506
ARP Cache
 -----
             HW type Flags HW address Mask Device
IP address
 10.1.1.254 0x1 0x2
                                   00:0B:86:00:0B:00 *
                                                                 eth0
Kernel Log
Alcatel Model AP60
AOS-W Version 2.4.0.0 (build 10150 / label #8041)
Built by p4build@speedy on 2005-06-25 at 19:22:19 PDT (gcc version 3.2)
0: offset=0x0,size=0x20000,blocks=32
Linux Tulip driver version 0.9.15-pre9 (Nov 6, 2001)
eth0: ADMtek Comet rev 17 at 0xc240dc00, 00:0B:86:C0:06:B5, IRQ 18.
wifi0: Atheros AR5212 PCI (v3): 00:0b:86:80:6b:50, irq 19, mode G
wifil: Atheros AR5211 PCI: 00:0b:86:80:6b:58, irg 17
Alcatel AP (c) 2002-2004 Alcatel, Inc.
Registering handlers for Atheros abg Atheros a
Process Table
PID Size State Command
---
             -----
1 1096 kB S
44 552 kB S
                    init
                    udhcpc

        61
        424 kB
        S

        62
        652 kB
        S

        73
        568 kB
        S

        76
        536 kB
        S

                    utelnetd
                    boa
                 nanny
                    wdg
   588 kB R
1524 kB S
                 msgHandler
77
79
                   sapd
85 1352 kB S
                  snmpd_sap
init
96 1096 kB S
416 1236 kB R
                  am
1599 1100 kB S
                  syslogd
Memory Usage
     total: used: free: shared: buffers: cached:
Mem: 14995456 14401536 593920 0 323584 7233536
Swap: 0 0
MemTotal: 14644 kB
                           0
MemSharee.
Buffers: 310 ~~
3. 7064 kB
Nu...
Buffers:
Cached:
SwapCached:
of kB
2492 kB
0 kB
               0 kB
HighFree:
                   0 kB
HighFree: 0 kB
LowTotal: 14644 kB
LowFree: 580 kB
SwapTotal: 0 kB
               0 kB
0 kB
SwapFree:
(OmniAccess 6000) #
```

# List Information for Technical Support

(Alcatel) # show tech-support



# **AP** Reprovisioning

If the AP is already configured and you want to change the AP parameters, use the **Reprovisioning** option. (You must have a network connection between the AP and the configured Alcatel Wireless LAN Switch.

1. Go to Maintenance > Program AP page

The Provisioning and Reprovisioning tabs display.

2. Click **Reprovisioning** 

This page displays all the APs currently configured DHCP pool of the Alcatel Wireless LAN Switch.

3. Select the AP to be reprovisioned.



FIGURE 21-2 Provisioned APs

4. Click Enable.

The selected AP should be seen in the Provisioning list.

Switch Image Management	WLAN >	Progra	m AP > R	e-Provi	ision > <b>IP</b>	10.100.1	15.12	21			« Back	
Reboot Switch	AP Parame	ters										
Clear Config	Location											
Boot Parameters File	Host Switch I	P Address/Nam	e ?		Master Sw	itch IP Address 🧃						
Copy Files	Obtain IF	Address Using	DHCP									
Copy Logs	C Use the f	ollowing IP Add	ress									
Copy Crash Files Delete Files	IP Address						Sub	onet Mask				
WLAN	Gateway IP 4	ddress										
Calibrate Radio Network												
Program AP	AP List										Refrest	1
Reboot AP	Index	Slot/Port	AP MAC/IP	Location	Master IP	Host Switch IP	/Name	IP	Gateway IP	State		
Captive Portal	□ 1	N/A	10.100.115.121	1.1.3	10.100.115.100	10.100.115.100/	I/A	N/A/N/A	N/A	Provisioned		
Customize Login Page Upload Certificate											Apply Cancel	

FIGURE 21-3 Selecting an AP for Reprovisioning

5. Configure the location, Host IP/Name, Master IP.

If the AP is going to be assigned a static IP, enter IP address, Net mask, and Gateway IP.

If the AP will use DHCP for its IP address information, select DHCP.

6. After configuring the required parameters, select the entry from the list (the AP to which the configuration is to be applied) and click **Apply**.

Switch Image Management	WLA	$\mathbb{N} > \mathbb{I}$	Progra	m AP > F	le-Prov	ision > IP	10.100.11	5.121	L			« Back
Reboot Switch	AP Par	ramete	rs									
Clear Config	Locatio	n		1.1.10								
Boot Parameters File	Host Sv	vitch IP A	Address/Nam	e ? 10.100	.115.200	Master Sw	10.100.115.200					
Copy Files	🖲 об	tain IP A	ddress Using	DHCP								
Copy Logs	C Use	e the folk	owing IP Add	tress								
Copy Crash Files	IP Addr	ress						Subne	et Mask			
WLAN	Gatewa	ay IP Ado	dress									
Calibrate Radio Network												
Program AP	AP Lis	t										Refresh
Reboot AP	Ir	ndex	Slot/Port	AP MAC/IP	Location	Master IP	Host Switch IP/	Name	IP	Gateway IP	State	
aptive Portal	<b>▼</b> 1	N	/A	10.100.115.121	1.1.3	10.100.115.100	10.100.115.100/N/	4 N	V/A/N/A	N/A	Provisioned	
Customize Login Page												
Upload Certificate												Apply Cancel
												1.10.10.10

FIGURE 21-4 Entering Updated Provisioning Information

The State shows In Progress.

Switch Image Management	WL	AN > I	Program	n AP > Re	-Provis	ion > IP :	LO.100.11	5.121				« Back
Reboot Switch	AP P	aramete	rs									
Clear Config	Locat	ion.		1.1.10								
Boot Parameters File	Host Switch IP Address/Name			10.100.115.200		Master Switch IP Address 🕥		10.100.115.200				
Copy Files	•	obtain IP A	ddress Using Di	HCP								
Copy Logs	СL	Jse the folk	wing IP Addre	55								
Copy Crash Files	IP Ad	ldress						Subne	t Mask			
WLAN	Gate	way IP Ado	lress									
Calibrate Radio Network												
Program AP	AP L	ist										Refresh
Reboot AP		Index	Slot/Port	AP MAC/IP	Location	Master IP	Host Switch I	P/Name	IP	Gateway IP	State	
Captive Portal		1	N/A	10.100.115.121	1.1.3	10.100.115.100	10.100.115.100/	N/A	N/A/N/A	N/A	In Progress	
Customize Login Page						Clear Table						
upioad Certificate												
												Apply Cancel
							© Copyright 20	003 Aruba	Wireless I	Networks, Inc.,	All Rights Res	erved.   Email Support

FIGURE 21-5 Processing Updates

7. Click the **Refresh** link after 10 seconds and the **State** is changed to **Provisioned**.

The Configured Parameters should be reflect in the AP list entry.



Switch Image Management	WLAN > Program AP > Re-Provision > IP 10.100.115.121    
Reboot Switch Clear Config	AP Parameters
Boot Parameters File	Host Switch IP Address/Name () 10.100.115.200 Master Switch IP Address () 10.100.115.200
Copy Files	Obtain IP Address Using DHCP
Copy Crash Files	© Use the following IP Address IP Address Subnet Mask
Delete Files WLAN	Gateway IP Address
Calibrate Radio Network Program AP	AP List Refresh
Reboot AP	Index Slot/Port AP MAC/IP Location Master IP Host Switch IP/Name IP Gateway IP State
Captive Portal	□ 1 N/A 10.100.115.121 1.1.10 10.100.115.100 10.100.115.100/N/A N/A/N/A N/A Provisioned
Customize Login Page Upload Certificate	Apply Cancel
	© Copyright 2003 Aruba Wireless Networks, Inc., All Rights Reserved.   Email Support

FIGURE 21-6 Updated Configuration

Click **Back** to go into the previous page and see that the entry of the AP is still selected.

8. Click **Disable** to disable AP Reprovisioning.

The entry will be deselected.

Now the AP is configured with the Parameters given

9. Reboot the AP to allow the AP to come up with the new configured parameters.

The AP should not be connected to any ports on which provisioning is currently active, or it will come up with the newly configured parameters.

Chapter 21



**OmniAccess Reference: AOS-W System Reference**
# CHAPTER 22 VPN Setup

The Alcatel Virtual Private Network (VPN) connection consists of the wireless user, the Access Point, and the Alcatel Wireless LAN switch. The wireless user is connected to the Wireless LAN switch via a captive portal which allows the wireless user to download the Alcatel dialer which makes the VPN connection. The relationship between the wireless user and the Wireless LAN switch is illustrated in the figure below.





# Prerequisites

You will need to make sure the following prerequisites are met before attempting to setup your VPN.

- Obtain a valid RADIUS server IP Address (if you are not using an internal database)
- RADIUS password and access port number, typically UDP port 1645
- A routable IP Pool for VPN.

The pool must not conflict with any other VLAN subnet.

This item is not required if you are using source NAT. Contact Alcatel support to setup source NAT.

- VLAN topology and switch loopback IP.
- Windows 2000 or Windows XP are required to run the VPN Dialer.

# Data Used In The Examples

Throughout this document you will find IP addresses and names of servers, users, passwords, etc. Do not use the values given in the examples, use actual values from the network to which you are connecting the switch.

## **Network Setup**

If your network is already setup, SKIP this section and GO TO the appropriate authentication server setup (RADIUS or Internal Database).

The process involves the following 4 steps:

- Creating the VLAN
- Configuring the port the VLAN will use
- Setting the default gateway
- Testing the connectivity to the default gateway and RADIUS server

1 Create a VLAN using the following CLI commands.

```
(Alcatel) (config) # vlan 1 <Enter> [This creates VLAN 1]
(Alcatel) (config) # interface vlan 1 <Enter> [Configure VLAN 1]
(Alcatel) (config-subif) # ip address 3.3.3.1 255.255.255.0 <Enter>
[Sets the IP address and subnet mask for VLAN 1]
(Alcatel) (config-subif) # exit <Enter>
```

2 Configure the VLAN port using the following CLI commands.

3 (Set the default gateway using the following CLI command.

(Alcatel) (config) # ip default-gateway 3.3.3.254 <Enter>

Test the connectivity to the default gateway and RADIUS server.

(Alcatel) (config) # ping 3.3.3.254 <Enter>
(Alcatel) (config) # ping 4.4.4.1 <Enter>

## **RADIUS Server Setup**

This section describes the steps necessary to setup the Alcatel switch to use a RADIUS server for authentication.

**NOTE**—If you are using an internal database for authentication, SKIP THIS SEC-TION.

Setup the RADIUS server using the following CLI commands.

**CAUTION**—Make sure you use the same name (RADIUS server) in each step.

Set the authport, host IP, and RADIUS server key for a named RADIUS server.

(Alcatel) (config) #aaa radius-server name authport 1645 host 4.4.4.1
key Alcatel <Enter>

2 Set a named server as the VPN authentication server.

(Alcatel) (config) # aaa vpn-authentication auth-server name <cr

3 Set a named server as the Captive Portal authentication server.

(Alcatel) (config) # aaa captive-portal auth-server name <Enter>



Exit the RADIUS server setup.

(Alcatel) (config) # exit <Enter>

5 Test the RADIUS server setup using the following CLI command.

```
(Alcatel) (config) # aaa test-server name username password <Enter>
```

If the authentication fails check the following:

- Connectivity ping the RADIUS server
- Confirm that the RADIUS server key from above is correct
- Confirm that the RADIUS authport was set correctly
- Username and password
- Verify that the Alcatel switch is allowed to access the RADIUS server (NAS IP on RADIUS)

#### **Internal Database Setup**

**NOTE**—If you are using RADIUS for authentication, SKIP THIS SECTION

Setup and test an internal database for authentication by using the following CLI commands.

**CAUTION**—Make sure you use the same server name for both the VPN and Captive Portal authentication servers.

Select a named internal server to use as the VPN authentication server.

(Alcatel) (config) # aaa vpn-authentication auth-server name <Enter>

 Select a named internal server to use as the Captive Portal authentication server.

(Alcatel) (config) # aaa captive-portal auth-server name <Enter>

3 Exit the setup.

(Alcatel) (config) # exit <Enter>

Create a test user.

(Alcatel) # local-userdb add username name password pmd role rolename
<Enter>

**5** Test the setup using the following CLI Commands

(Alcatel) # aaa test-server servername username password <Enter>

# L2TP IPSec VPN Server Setup

This section describes the steps necessary to configure the Alcatel switch as a VPN server.

1 Enter the policy sub-mode and define a policy with a specified priority.

(Alcatel) (config) # crypto isakmp policy num <Enter>

Specify the authentication method (pre-shared key) using the following CLI command.

(Alcatel) (config-isakmp) #authentication pre-share <Enter>

3 Exit the policy sub-mode.

(Alcatel) (config) # exit <Enter>

4 Set the value (string) of the IKE key to be used. This command also specifies a group IP address and subnet mask. The IP address and mask should be set as shown in the example below (IP = 0.0.0.0, netmask = 0.0.0.0) as these values will make the key global.

```
(Alcatel) (config) #crypto isakmp key KeyString address 0.0.0.0 netmask 0.0.0.0 <Enter>
```

5 Specify the range of IP addresses to use an a VPN address pool. The n.n.n.n and x.x.x.x arguments specify the starting and ending IP addresses for the pool.

(Alcatel) (config) # **ip local pool** *PoolName n.n.n. x.x.x.x* <Enter>

6 Enter the VPN L2TP Sub-Mode using the following CLI command.

(Alcatel) (config) # vpdn group 12tp <Enter>

7 Set the PPP authentication type using the following CLI command.

(Alcatel) (config-vpdn-l2tp) # ppp authentication PAP <Enter>



8 Turn off the default mschapv2 authentication using the following CLI command.

```
(Alcatel) (config-vpdn-l2tp) # no ppp authentication mschapv2 <Enter>
```

9 Specify the DNS IP address that will be pushed to the VPN Dialer using the following CLI command.

(Alcatel) (config-vpdn-l2tp) # client configuration dns n.n.n. < Enter>

Specify the WINS IP address that will be pushed to the VPN Dialer using the following CLI command.

(Alcatel) (config-vpdn-l2tp) # client configuration wins n.n.n.n <Enter>

**11** Exit the VPN L2TP Sub-Mode.

```
(Alcatel) (config-vpdn-l2tp) # exit <Enter>
```

## **Alcatel Switch VPN Dialer Setup**

This section describes the steps necessary to configure the Alcatel switch as a VPN Dialer.

 Enter the VPN dialer mode using the following CLI command. This command creates a VPN dialer with the name specified in the DialerName argument.

**NOTE**—Because the dialer name will be displayed on the client machine (laptop, etc), care should be taken to choose an appropriate and meaningful name.

(Alcatel) (config) # **vpn-dialer** DialerName <Enter>

2 Specify the IKE authentication key to be used with this VPN dialer. It should be the same key string specified above.

```
(Alcatel) (config-vpn-dialer) # ike authentication pre-share KeyString
<Enter>
```

3 Specify the SecurID authentication method.

**NOTE**—Use this only if RSA SecurID is being implemented.

```
(Alcatel) (config-vpn-dialer) # ppp authentication CACHE-SECURID <Enter>
```



Apply a default role to Captive Portal authentication using the following CLI command.

(Alcatel) (config) # aaa captive-portal default-role RoleName <Enter>



# **VPN** Dialer

#### **Before You Begin**

- Make sure you have wireless connectivity.
   You can check the connectivity by "pinging" the switch.
- Make sure you aren't currently running a VPN dialer. If you are, quit the application.

#### **Downloading the Client**

1 Open a browser. Your browser should be redirected to the switch's captive portal, shown below.

REGISTERED USER	
USERNAME	
PASSWORD	
Log In	

2 Enter your username and password, then click the Log In button.

**NOTE**—You might see a Security Alert Dialog appear. If this happens it probably means that the server certificate is either expired or not signed. The client is shipped with a self-signed certificate. You will need to purchase a certificate for your server that is signed by a well known CA.



After you have been authenticated two browser windows appears, the larger will remain for approximately 10 seconds to allow you to download the VPN Dialer. The smaller of the two appears in the lower right corner of your screen and has a link that allows you to log out of the switch.



Click to Log	<u>gout</u>
/PN Users:	Click to download VPN dialer
in 10 secor http://www	nds you will be automatically redirected to yourhomepage.com/.
Click <u>here</u> t	o go there directly.
E users: C	lick <u>here</u> to bookmark this page.
Other brow	sers: Press control-d to bookmark this page.
/ou can coi	me back to this page later to logout or download VPN dialer



**NOTE**—If you close the Alcatel Logout window you can access it again to logout of the switch by opening a browser and going to the following URL https://switch IP Address/logout.html.

The File Download dialog box appears.

4 Click the Open button.

The download process will begin and installation will begin automatically.





#### Installation

When the setup file is finished downloading the Dialer Setup Wizard will open.

1 Click the Next button.



The License Agreement dialog appears.

#### 2 Select I accept and click on the Next button.



The Choose Setup Type dialog appears.



;₩	VPN Dialer Se	tup X
C	hoose Setup Type Choose the setup ty	pe that best suits your needs
	<b>N</b>	Complete Complete Installation of Aruba VPN Dialer.
		< <u>B</u> ack Mext > Cancel

The Ready to Install dialog appears.

#### 4 Click the Install button.

👘 VPN Dialer Setup	×
Ready to Install The Setup Wizard is ready to begin the Complete installation	$\mathfrak{S}$
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
< <u>B</u> ack [	cel



The Installation Progress dialog appears, when the installation is finished the "Completing the Alcatel VPN Setup Wizard" dialog appears.

🚼 VPN Dialer Setup		×
Ð	Completing the VPN Dialer Setup Wizard	
	Click the Finish button to exit the Setup Wizard.	
	< Back Finish Cancel	

5 Click the Finish button.

The Alcatel VPN Dialer dialog will launch and the dialog appears.

VPN Dialer - default-d	lialer 🔀
	ER
	the second
User name:	
Password:	
Save Pass	word
Connect	HangUp
Not Connected.	Launch at Boot Up     Connect At Launch     Wait For Wireless     Hide After Connect      Network Info

## **Connecting With VPN**

You are now ready to connect to the network using VPN. The Alcatel VPN icon appears in the Startup tray at the right hand side of the Windows Task Bar.



You may launch the VPN Dialer by double-clicking on the icon or you may launch it from the Windows Start Menu.

The VPN Dialer window appears as soon as the application is launched.

1 Type your username and password in the text boxes on the VPN Dialer dialog and click the Connect button.

VPN Dialer - default-d	ialer 🔀
User name:	
Password:	
🔲 Save Pass	word
Connect	HangUp
Not Connected.	Launch at Boot Up     Connect At Launch     Wait For Wireless     Hide After Connect      Network Info

The dialer will connect automatically.



#### Alcatel VPN Dialer Features

The Dialer has 4 features that may be selected.

- Launch at Boot-Up
- Connect at Launch
- Wait For Wireless
- Hide After Connect.
- Network Info

#### Launch at Boot-up

When selected, this feature will cause the VPN Dialer to launch automatically each time you start or restart your computer.

#### Connect at Launch

When selected, this feature allows the Dialer to automatically connect every time the application is launched. When you select this feature the Save Password check box will be automatically checked, however you may elect to enter your password manually each time you login by unchecking the Save Password box.

#### Wait For Wireless

When this feature is enabled the client waits for wireless connectivity and waits do detect an Alcatel switch before it attempts to login.

#### Hide After Connect

This feature will automatically hide the Dialer window when the login process is completed. You may open the window again by double-clicking the dialer lcon in the Task Tray.

#### Network Info

This feature will display a static window showing important network information.

Dial							×
	Instant Wireless Network PC ( Physical Address: DHCP Enabled: IP Address: Subnet Mask: Default Gateway: BSSID: SSSD: RSSI: BeaconPeriod: Channel: WEP: AUTHMODE: 3Com 3C920 Integrated Fast Physical Address: DHCP Enabled: IP Address: Subnet Mask: Default Gateway: WAN (PPP/SLIP) Interface: Physical Address: DHCP Enabled: IP Address: Subnet Mask: Default Gateway: DNS Servers: Scanned Access Points (11):	Card V3.0 - Packet Sc 00:06:25:17:90:8C YES 10.1.1.122 255:255.255.255.0 10.0.1.254 00:08:66:20:27:10 ethersphere -54 100 858516 Enabled Open Ethernet Controller ( 00:08:74:94:37:DD YES 0.0.0.0 00:53:45:00:00:00 NO 00:53:45:00:00:00 NO 00:55:255.255.255 10.5.10.55 10.1.1.2 BSSID 00:08:66:90:65:10 00:08:66:90:55:10 00:08:66:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:86:90:55:10 00:00:62:25:80:67:05 00:80:62:07:6E:1F CA:50:95:1E:BE:C52 CA:50:95:1E:BE:C52 CA:50:95:1E:BE:C52 CA:50:95:1E:BE:C52 00:08:66:20:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00:08:80:27:10 00	Control (2005) (3C905)	RSSI -TX Compa -TX Compa -TX Compa -7X -72 -73 -76 -78 -75 -70 -78 -70 -79 -70 -70 -30	Channel 858516 858516 858516 858516 858516 858516 858516 858516 858516 858516	SSID swep-ap test parag-b1 qa_linksys_wrt5 auth-sap qa_cisco_ap350 qa_link_di614 qa_linksys_wrt5 adinc_die14 qa_linksys_wrt5 adinca ethersphere	X tu
		OK					



#### Troubleshooting

#### **Common Dialer Error Messages**

#### Interface is down or no route.

This message indicates that there is a wireless connectivity problem.

#### Route to destination is not wireless

This message indicates that the computer (laptop) is connected through a wired connection. If you wish to connected through the wired side of the network, uncheck the Wait For Wireless box on the Dialer window. Otherwise, unplug the network cable from the computer.

#### No Alcatel switches detected... will retry

This message indicates that the computer is unable to automatically detect the presence of an Alcatel switch. Do not uncheck this box unless you think the error is invalid, this message us usually a strong indication that something is setup incorrectly in the network.

#### Wired. Wireless disabled ... will retry.

This message indicates that the wirednowifi function is enabled on the switch and wireless connection is not allowed.

#### **Common Problems**

#### Dialer does not connect to server

If the dialer seems to stall while attempting to connect (as indicated by a persistent *Connecting* status, are several possible causes for the failure. The following steps will help you to identify and correct the problem. Those causes include:

- Make sure you have the latest dialer. You can download the latest dialer from your switch by going to the captive portal login (http:// smitchIP/login.html).
- Make sure connectivity is in place by pinging the switch.
- The ISAKMP shared key may be misconfigured on the client.
- The client may be failing to encrypt properly.
- The VPN IP Address pool may be exhausted.

1 Use the show crypto isakmp sa command on the switch to make sure the user is authenticating.

```
(Alcatel) (config) #show crypto isakmp sa
Responder IP 10.1.1.158
Initiator IP 10.1.1.122
Initiator cookie ce91845e68f75026 Responder cookie 9635499cf2dad66e
Life secs 28800
transform: 3DES - Secure Hash Standard
Authentication method: Pre-Shared Key
```

If the initiator and client IP match, then the client has successfully started IPSec authentication. Otherwise, make sure that the pre-shared keys in the vpn-default dialer. You may see the key by using the vpn-dialer command, page 833. Be sure that the encrypt feature is disabled, page 446.

```
(Alcatel)(config) #show vpn-dialer
default-dialer
-------
Attribute Value
------ -----
PPTP disabled
...
IKEPASSWD *******
.
IPSecAUTH ESP-SHA-HMAC
```





```
(Alcatel)(config) #show crypto ipsec sa
Responder IP 10.1.1.158
Initiator IP 10.1.1.122
Initiator cookie ce91845e68f75026 Responder cookie 9635499cf2dad66e
Life secs 7200
transform: esp-3des esp-sha-hmac
```

If the initiator IP matches the client IP, then IPSec encryption is good.

3 Use the show vpdn I2tp pool command on the switch to check the availability of VPN IP addresses.

Dialer connects and authenticates, but doesn't logon.

This is indicates that either the username/password combination is wrong or the RASIUS server is unreachable.

RSA SecurID users having this problem may nave been locked out, check the RSA SecurID server. For more information, see <a href="http://rsasecurity.agora.com/rsasecured/detail.asp?product\_id=1404">http://rsasecurity.agora.com/rsasecured/detail.asp?product\_id=1404</a>

Dialer connects but no traffic moves from applications.

This indicates that the L2TP/PPTP IP pool is not routable.

## Generating a Self-Distributable Alcatel Dialer

To generate a self distributable Alcatel dialer, you need to:

1. Download and save the set (using winzip for example). Be sure to maintain the directory structure.

2. In the same directory where dialer.Msi has been uncompressed, create a file named config.htm with the following contents:

```
"DIALER_NAME"="Company Name"
"PPTP"=DWORD:0
```

"L2TP"=DWORD:1

```
"DNETCLEAR"=DWORD:0
```

- "MSCHAPV2"=DWORD:0
- "CACHE-SECURID"=DWORD:1
- "IKESECS"=DWORD:28800
- "IKEENC"="3DES"
- "IKEGROUP"="TWO"
- "IKEHASH"="SHA"
- "IPSECSECS"=DWORD:7200
- "IPSECGROUP"="GROUP2"
- "IPSECENC"="ESP-3DES"
- "IPSECAUTH"="ESP-SHA-HMAC"
- "PAP"=DWORD:1
- "CHAP"=DWORD:0
- "MSCHAP"=DWORD:0
- "IKEPASSWD"="changeme"
- "IKEAUTH"="PRE-SHARE"
- "WIREDNOWIFI"=DWORD:1
- "SETUPIP"="1.1.1.1"

```
"NovellLogin"=DWORD:0
```

- 3. Modify IKEPASSWD to the pre-shared key you use and SETUPIP to the IP address of the switch. Quotes below are important. "DIALER\_NAM" will be the name displayed on the window title bar.
- 4. After creating config.htm, zip all the files including the new config.htm into a self-extracting package. Maintain the directory structure as the .msi file expects the same directory hierarchy.
- **NOTE**—The WIRENOWIFI option configures the dialer to automatically enable/disable wireless when the wired port is plugged in and is functional on the laptop.



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 23 VPN Configuration

Alcatel switches provide full support for Virtual Private Network (VPN) termination using IPSec and PPTP. Encryption protocols run in hardware appropriately sized to process a full complement of access points.

# Configuring IPSec Using Web UI

Switch	Security > VPN Settings > IPSEC
Management WLAN	IPSEC PPTP Dialers Emulate VPN Servers Advanced
Network	L2TP and XAUTH Parameters
Radio	Enable L2TP 🔽
Advanced	
RF Spectrum Mgmt	
Calibration	Primary DNS Server U.U.U.U
Optimization	Secondary DNS Server 0.0.0.0
Protection	Primary WINS Server 0.0.0.0
Monitoring	Secondary WINS Server 0.0.0.0
Security	
Rules	Address Pools
POlicies	Pool Name Start Address End Address Actions
AAA bervers	944
VDN Settings	
Advanced	Source NAT
WI AN Intrusion Detection	Enable Source NAT
Roque AP	IKE Aggressive Group Name changeme (Only needed for XAUTH)
Denial of Service	
Man-In-the-Middle	IKE Shareu Secrets
Signatures	Subnet Subnet Mask Length Key Actions
Policies	Add
	IKE PUILLIES           Description         Hach         Authoratication         Excurption         Action
	Default 3DES SHA DSA GDOLLD 2 [300 - 86400] caronda no volume limit Edit. Delete
	Add
	Apply
	Commands View Commands

The following parameters and options may be configured through Web UI.

•	Enable L2TP	Enable or disable L2TP authentication functionality
•	Authentication Proto- cols	Use these check boxes to select the
•	Primary DNS Server	Specify the IP address of the Primary DNS server in the text box.
•	Secondary DNS Server	Specify the IP address of the Secondary DNS server in the text box.
•	Primary WINS Server	Specify the IP address of the Primary WINS server in the text box.

•	Secondary WINS Server	Specify the IP address of the Secondary WINS server in the text box.
•	Address Pools	IPSec tunnel endpoints are assigned discrete IP addresses. The client is assigned an address from one of the pools specified in this option. The IP address at the switch endpoint will always be either one of the IP address on the switch or the Emulate Server IP address.
•	Enable Source NAT	Enable or disable NAT (Network Address Translation). When selected, a traffic policy is created for the VPN default role.
		Source NAT may be enabled when the address range in the VPN address pool is not routable by the remainder of the network.
		When Source NAT is enabled the source address of packets from the client will be changed to that of the switch as they pass outbound from the switch to the server.
•	IKE Aggressive Group	(Only required for third party VPNs)
	Name	Enter the name of the IKE Aggressive Group when XAUTH is used.
		The group name must exactly match the group name configured on each client.
•	IKE Shared Secrets	Specify the IKE pre-shared keys for various IP address ranges.
		Keys may be from 1 to 64 characters in length.
•	IKE Policies	Define IKE policies in this section of the page.



#### Adding Address Pools

Add Address Pools by clicking **Add** under the address pool section.

Address Pools			
Pool Name	Start Address	End Address	Actions
remoteappool	10.4.21.101	10.4.21.110	Edit Delete
Add			

#### The Configuration > VPN Settings > IPSec > Add Address Pool page appears.

Switch	Security > VPN Settings > IPSEC > Add Address Pool	« Back
Management		
WLAN	Pool Name	
Network	Start Address	
Radio Advanced	End Address	
RF Spectrum Mgmt	Done	

- 1 Enter a unique name for the address pool you are defining.
- 2 Enter the start and end addresses for the pool.
- 3 Click done.
- 4 Click Save configuration on the **Configuration > VPN Settings IPSec** page.

#### Adding IKE Shared Secrets

Add Shared Secrets by clicking **Add** at the bottom of the IKE Shared Secrets portion of the page.

IKE Shar	ed Secrets			
Subnet	Subnet Mask Length	Key	Act	ions
0.0.0.0	0	****	Edit	Delete
Add				

Switch	Security > VPN Setti	nas > IPSEC> Add IKE Secret	« Back
Management			
WLAN	Subnet	0.0.0.0	
Network	Subnet Mask	0.0.0	
Radio	(Please use the defaults 0.0.0.0 for t	the Subnet and Subnet mask if you do not intend to have multiple pre-shared	i keys)
Advanced	IKE Shared Secret		
Calibration	Verify IKE Shared Secret		
Optimization			Done
Protection			

The Configuration> Security > VPN Settings > IPSec > Add IKE Secret page appears.

- 1 Type the secret in the IKE Shared Secret field.
- 2 Re-type the secret in the Verify Shared Secret field.
- 3 Enter a subnet and subnet mask if you are using multiple keys.

#### **Adding IKE Policies**

Add IKE policies by clicking the Add button at the bottom of the IKE Policies portion of the page.

Priority	Encryption	Hash	Authentication	Group	Lifetime	A	ction
10	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400] seconds, no volume limit	Edit	Delete
Default	3DES	SHA	RSA	GROUP 2	[300 - 86400] seconds, no volume limit	Edit	Delete

#### The Configuration> Security > VPN Settings > IPSec > Add Policy page appears.

Switch	Security > V	<b>PN</b> Setting	IS > IPSEC > Add Policy	« Back
Management			· · · · · · · · · · · · · · · · · · ·	
WLAN	Priority			
Network	Encryption	DES 👤		
Radio Advanced	Hash Algorithm	SHA 🗸		
RF Spectrum Mgmt	Authentication	PRE-SHARE 💌		
Calibration	Diffie Hellman Group	GROUP 2 💌		
Optimization	Life Time(secs)			
Protection		1 noly		
Monitoring		Арріу		
Security				



- 1 Specify a priority.
- 2 Select an encryption type from the Encryption pull-down box.
- 3 Select a hash algorithm from the Hash Algorithm pull-down box.
- 4 Select an authentication type from the Authentication pull-down box.
- 5 Select a Diffie-Hellman group from the Diffie Hellman pull-down box.
- 6 Specify a lifetime (in seconds).

# L2TP

#### **Configuring PPTP Using Web UI**

To configure PPTP, go to the **Configuration > Security > VPN Settings > PPTP** page.

Switch	Security	> VPN S	settings >	PPTP	
Management WLAN	IPSEC	PPTP C	)ialers Emu	late VPN Servers	Advanced
Network	PPTP Param	eters			
Radio	Enable PPTP	l.	•		
Advanced	PPTP Echo Tim	eout(secs) 6	1		
RF Spectrum Mgmt	Authoptication	Destocale E			
Calibration	Addrendcadon	IPROCOCOIS IN	MSCHAPV2		
Optimization	Primary DNS S	erver 0	.0.0.0		
Monitoring	Secondary DN	5 Server 0	0.0.0		
Security	Primary WINS	Server 0	.0.0.0		
Roles	Secondary WI	NS Server 0	.0.0.0		
Policies	Address Por	nls			
AAA Servers					
Authentication Methods	Pool Name	Start Addre	ess End Addre	ss Actions	
VPN Settings	pptp-pool-1	192.168.10.50	192.168.10.5	9 Edit Delete	
Advanced	Add				
WLAN Intrusion Detection Rogue AP					Apply
Denial of Service	Commands				View Commands
Man-In-the-Middle					

The following parameters and options may be configured through Web UI.

Enable PPTP

Enables and disables PPTP client termination.

•	PPTP Echo Timeout	The period of time, in seconds, the system for a PPTP echo response from a client before dropping the client.
•	Authentication Proto- col	Determines the PPTP authentication protocol. At this time only MS-CHAPv2 is supported.
•	Primary DNS Server	Specify the Primary DNS server IP Address.
•	Secondary DNS Server	Specify the Secondary DNS server IP Address.
•	Primary WINS Server	Specify the Primary WINS server IP Address
•	Secondary WINS Server	Specify the Secondary WINS server IP Address
•	Address Pools	Add address pools using this section of the page.

Add address pools by clicking **Add** in the Address Pools section of the PPTP page. The PPTP > Add Address Pool page appears.

Pool Name		
Start Address		
End Address		

# Configuring The VPN Dialer Using Web UI

Alcatel AOS-W includes a configurable Windows VPN dialer application. The dialer will pre-configure supported Windows systems to operate with Alcatel VPN services.



You may configure the VPN dialer by navigating to the **Configuration > VPN Settings > Dialers** page.

IPSEC	PPTP	Dialers	Emulate VPN Servers	Advanced	
Name	Act	ion			
default-dialer	Edit	Delete			

Add a new dialer by clicking **Add**. The **Configuration > VPN Settings > Dialers > Add Dialers** page appears.

Switch	Security > VPN Settings > Dia	alers > Add Dialer
Management	, 3	
WLAN	Dialer Name	
Network	Enable PPTP	
Radio	Enable L2TP	<b>v</b>
Advanced RE Epocheuro March	Send Direct Network Traffic In Clear(Split Tuppeling)	
Calibration	Send Direct Network trainc in clear(Split Turineiing)	
Optimization	Disable Wireless Devices When Client is Wired	
Protection	Enable SecurID New and Next Pin Mode	
Monitoring	Authentication	PAP CHAP MSCHAP MSCHAPv2 Cache SecureID Token
Security	IKE Lifetime (secs)	28800
Policies	IKE Encryption	⊙ 3DES O DES
AAA Servers	IKE Diffie Hellman Group	© 2 O 1
Authentication Methods	IKE Hash Algorithm	⊙ SHA C MDS
VPN Settings	IKE Authentication	C RSA Signatures ⊙ Preshared Key Password
Advanced	IDSEC Lifetime (cerc)	7200
WLAN Intrusion Detection		2.00
Royale AP Depial of Service	IPSEC Mode Group	0201
Map-Ip-the-Middle	IPSEC Encryption	© ESP-3DES ○ ESP-DES
Signatures	IPSEC Hash Algorithm	● ESP-SHA-HMAC ○ ESP-MD5-HMAC
Policies		Apply
, ender		

The following parameters and options may be configured through Web UI.

Dialer Name

Specify a name for the dialer.

Enable PPTP Enable PPTP tunneling to the Alcatel switch.

**Note**—You may check both PPTP and L2TP, however they will not run simultaneously. When both are checked, the client will attempt the more secure method, L2TP, first.

• Enable L2TP Enable L2TP tunneling to the Alcatel switch.

**Note**—You may check both PPTP and L2TP, however they will not run simultaneously. When both are checked, the client will attempt the more secure method, L2TP, first.

 Send Direct Network Traffic In Clear
 This option enables Split Tunneling. Split Tunneling tunnels traffic destined for the internal network while allowing internet bound traffic to travel outside the secure tunnel.

**NOTE**—For reasons of security this option is not recommended.

- Disable Wireless
   Devices When Client is
   Wired
   When enabled, this option allows the
   dialer to detect a wired connection and
   shut down the wired connection.
- Authentication
   This option allows you to specify a list of protocols to be supported by the dialer. The list should match the IPSec or PPTP configuration on the switch and contain a minimum of one protocol supported by the authentication server.
- IKE Lifetime (seconds) The value entered specifies the length of the IKE security association, in seconds.
- IKE Encryption
   Specifies the IKE encryption protocol to be used for the dialer. The choice in the dialer must match the protocol specified in the IPSec IKE policy on the switch.
- IKE Diffie Hellman Group
   Specifies which Diffie-Hellman grout IKE will use. The choice in the dialer must match the D-H group specified in the IPSec IKE policy on the switch. The default is Group 2.



•	IKE Hash Algorithm	Specifies which hash algorithm will be used by IKE. The choice in the dialer must match the algorithm specified in the IPSec IKE policy on the switch. The default is SHA.
•	IKE Authentication	Specifies wither RSA signatures or a Pre-shared key for IKE authentication and must match that specified in the IPSec IKE policy on the switch.
		The shared secret must match that specified in the IKE share secret policy on the switch.
•	IPSec Lifetime (sec- onds)	The value entered specifies the length of the IPCEC security association, in seconds. The default is 7200 (2 hours).
•	IPSec Mode Group	Choose the IPSEDC Perfect Forward Secrecy (PFS) mode. The default is Group 2.
•	IPSec Encryption	Specifies the encryption type for IPSec. The default is ESP-3DES.
•	IPSec Hash Algorithm	Specifies which hash algorithm will be used by IKE. The choice in the dialer must match the algorithm specified in the IPSec IKE policy on the switch. The default is SHA.

# **Configuring VPN Server Emulation Using Web UI**

It is sometimes common for users in multi-campus environments to move between campuses with their laptops. When this occurs there may be a loss of optimization of the user's connection because the dialer is configured with the IP address of the home switch.

The VPN Server Emulation feature negates this loss of optimization by intercepting the sessions destined for the home switch and provides them with a local termination.

The number of IP addresses which may be added to the list of server addresses is limited to approximately 650. The exact number of IP addresses may be calculated by the following:

Maximum Number of IP Addresses = 
$$\frac{\text{Number of ACLs}}{3}$$

VPN Server Emulation may be configured by navigating to the **Configuration > VPN Settings Emulate VPN Servers** page.

Serve	gs > Emulate VPI	Settin	> VPN	ecurity
Advanc	Emulate VPN Servers	Dialers	PPTP	IPSEC
			Action	IP Address
			ALLIUN	Add
nc	N Ser Advar	<b>gs &gt; Emulate VPN Ser</b> Emulate VPN Servers Adva	Settings > Emulate VPN Ser           Dialers         Emulate VPN Servers         Advantage	> VPN Settings > Emulate VPN Ser           PPTP         Dialers         Emulate VPN Servers         Advantage           Action         Action         Advantage

Add a server IP address

Click on the Add box.

- 1 Type the IP Address in the text box.
- 2 Click the Add button again.
- 3 Click the Save Configuration tab near the top of the page.

# Configuring SecureID Token Caching Using Web UI

Alcatel AOS-W allows caching of SecureID tokens so that the user doesn't need to perform a new authentication procedure each time a network connection is lost.



SecureID Token Ring Caching may be configured by navigating to the **Configuration > Security > VPN Settings > Advanced** page.

IPSEC	PPTP D	ialers	Emulate VPN Servers	Advanced	
L2TP Hello Timeout(secs)					60
SecurID Token Persistence Enabled					
SecurID Token Persistence Timeout(minutes)					1440
IPSEC Maximum MTU Size					1500
IPSEC Transf	form Sets				
Name	Encryptic	n Hash	Action		
default-transfor	m 3DES	SHA	Edit Delete		
Add					
					Apply
Commands View Corr					hands

- 1 Check the SECUREID Token Persistence Enabled check box.
- 2 Set the SECUREID Token Persistence Timeout in minutes by typing a value in the text box.

## **Configuring IPSec Using the CLI**

IPSec is configured from the config-vpdn-l2tp prompt in the CLI.

1 Enter the config-vpdn-l2tp submode using the vpdn group 12tp command from the CLI.

```
(Alcatel) (config) #vpdn group l2tp
(Alcatel) (config-vpdn-l2tp) #
```

2 Specify the primary and secondary DNS servers.

```
(Alcatel) config-vpdn-l2tp)# client configuration dns 192.168.29.1
192.168.29.2
```



Specify the primary and secondary WINS servers

```
(Alcatel)(config-vpdn-l2tp)# client configuration wins 192.168.30.1 192.168.30.2
```

#### Select authentication protocols

```
(Alcatel) (config-vpdn-l2tp)# ppp authentication PAP
(Alcatel) (config-vpdn-l2tp)# ppp authentication CHAP
(Alcatel) (config-vpdn-l2tp)# ppp authentication MSCHAP
(Alcatel) (config-vpdn-l2tp)# ppp authentication MSCHAPv2
```

5 Define an address pool for VPN users. This is done from the config prompt. If the CLI is still in the config-vpdn-l2tp submode, type exit to return to the config prompt.

(Alcatel) (config) #ip local pool 12tp-pool 192.168.99.1 192.168.99.100

6 Specify a group name for IKE (required only if using XAUTH).

(Alcatel) (config) #crypto isakmp groupname fooname

7 Specify an IKE Shared Secret for clients connecting through the specified subnet. This allows multiple shared secrets to be employed.

8 Define a crypto policy and assign it a priority. Begin by entering the config-isakmp submode.

(Alcatel) (config) #crypto isakmp policy 10
(Alcatel) (config-isakmp)#

9 Specify the authentication method.

(Alcatel) (config-isakmp) # authentication pre-share

## Configuring PPTP Using the CLI

PPTP is configured from the config-vpdn-pptp prompt in the CLI.



# 1 Enter the config-vpdn-pptp submode using the vpdn group pptp command from the CLI

(Alcatel) (config) #vpdn group pptp (Alcatel) (config-vpdn-pptp)#

2 Specify the IP addresses of the primary and secondary DNS servers

```
(Alcatel) (config-vpdn-pptp)# client configuration dns
192.168.29.1 192.168.29.2
```

3 Specify the IP addresses of the primary and secondary WINS servers.

```
(Alcatel) (config-vpdn-pptp)# client configuration wins
192.168.30.1 192.168.30.2
```

```
4
```

Exit the config-vpn-pptp submode.

(Alcatel) (config-vpdn-pptp)# exit

#### 5 Define an IP address pool for PPTP users.

(Alcatel) (config) #pptp ip local pool pptp-pool 192.168.200.1 192.168.200.100

# **Configuring the VPN Dialer Using the CLI**

1 Enter the config-vpn-dialer submode.

(Alcatel) (config) #vpn-dialer foo-dialer-2
(Alcatel) (config-vpn-dialer)#

2 Select a tunneling method (L2TP, PPTP)

(Alcatel) (config-vpn-dialer) #enable 12tp

#### 3 Select one or more authentication methods

(Alcatel) (config-vpn-dialer) #ppp authentication PAP (Alcatel) (config-vpn-dialer) #ppp authentication CHAP (Alcatel) (config-vpn-dialer) #ppp authentication MSCHAP (Alcatel) (config-vpn-dialer) #ppp authentication MSCHAPv2
#### Set the IKE lifetime.

4

(Alcatel) (config-vpn-dialer)#ike lifetime 28800

#### 5 Select an encryption type.

(Alcatel) (config-vpn-dialer) #ike encryption 3des

#### 6 Specify a Diffie-Hellman group.

(Alcatel) (config-vpn-dialer) #ike group 2



(Alcatel) (config-vpn-dialer) #ipsec hash esp-sha-hmac

# **Configuring VPN Server Emulation Using the CLI**





VPN Configuration | 519

2 Define rules.

```
(Alcatel) (config-sess-vpn-dst-nat)#any host 192.68.8.1 svc-ike
dst-nat
(Alcatel) (config-sess-vpn-dst-nat)#any host 192.68.8.1 svc-esp
dst-nat
(Alcatel) (config-sess-vpn-dst-nat)#any host 192.68.8.1 svc-l2tp
dst-nat
```

3 Return to the config prompt.

```
(Alcatel) (config-sess-vpn-dst-nat) #!
```

4 Apply a role for VPN users.

(Alcatel) (config) #user-role logon

5 Set the position of the ACL defined above.

(Alcatel) (config-role) #session-acl vpn-dst-nat position 1

# Configuring SecureID Token Caching Using Web UI

1 Enter the config-vpdn-l2tp sub-mode.

(Regulus) (config) #vpdn group 12tp

2 Enter the following two commands to enable caching and set the period for which a token will be cached.

(Regulus) (config-vpdn-l2tp)# ppp authentication CACHE-SECURID (Regulus) (config-vpdn-l2tp)# ppp securid cache 1440

**NOTE**—When testing securID caching on a VPN with multiple laptops, be sure the same PIN+token is used on all the laptops. If more than one PIN+token is used, only the last one will work properly.

# **VPN Quick Start Guide**

#### **Requirements From Customer**

The user must provide the following:

- RADIUS server IP (if not using internal database)
- RADIUS password and access port number (typically UDP port 1645)
- Routable IP pool for VPN. Pool MUST NOT conflict with any other VLAN subnet (may skip if using source NAT, contact support to setup source NAT)
- Desired IPSec pre-shared key (global, not per user), use something long with capital letters and numbers.
- VLAN topology and switch loopback IP.
- This document only covers Win2k and WinXP.

## **Network Topology In Examples**

The following values are used in this section:

- 2.2.2.x is the pool of private addresses for VPN (2.2.2.1 2.2.2.254)
- 3.3.3.x is the trusted side of the network going to the router, assume port 2/0 vlan 1
- Default router's IP: 3.3.3.254
- RADIUS server IP: 4.4.4.1, authport is 1812, password is Alcatel
- Valid user and passwords in radius server: user: foo, password: bar
- IPSec pre-shared key is f00xYz123BcA
- DNS and WINS servers for VPN users: 10.1.1.2, 10.1.1.3

#### Setting Up a VPN

Perform the following steps:

- 1 Set up network
- 2 Set up and test RADIUS Server
- 3 Set up VPN server on Alcatel Switch
- 4 Set up roles and VPN Dialer on Alcatel Switch



#### 5 Set up client

The following sections explain each step in detail.

## 1. Set up Network

The steps necessary to set up a network are:

```
(Alcatel6000) (config) # vlan 1
(Alcatel6000) (config) # interface vlan 1
(Alcatel6000) (config-subif) # ip address 3.3.3.1 255.255.255.0
(Alcatel6000) (config-subif) # exit
(Alcatel6000) (config) # interface fastethernet 2/0
(Alcatel6000) (config-if) # trusted
(Alcatel6000) (config-if) # switchport access vlan 1
(Alcatel6000) (config-if) # exit
(Alcatel6000) (config) # ip default-gateway 3.3.3.254
(test connectivity to default gateway and RADIUS)
(Alcatel6000) (config) # ping 3.3.3.254
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
(Alcatel6000) (config) # ping 4.4.4.1
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

## 2. Set up and Test RADIUS the Server

If you are using a local database skip this step and proceed with Step 3.

On the RADIUS server):

```
(Alcatel6000) (config) # aaa radius-server ias authport 1812 host
4.4.4.1 key Alcatel
(Alcatel6000) (config) # aaa vpn-authentication auth-server ias
(Alcatel6000) (config) # aaa captive-portal auth-server ias
(Alcatel6000) (config) # exit
```

Test the RADIUS server with username: foo, password bar

(Alcatel6000) # aaa test-server ias foo bar Authentication successful

If this test fails, troubleshoot the RADIUS server by checking:

- Connectivity problem, try pinging radius server
- RADIUS server key is wrong
- RADIUS server authport is wrong

- Username and/or password is wrong
- Alcatel switch is not allowed to access RADIUS server (NAS IP on RADIUS)

# 2(b). Set up and Test Internal Database

Skip this step if you are using RADIUS. Proceed to Step 3.

To configure the local database:

(Alcatel6000) (config) # aaa vpn-authentication auth-server Internal (Alcatel6000) (config) # aaa captive-portal auth-server Internal (Alcatel6000) (config) # exit

Add a user to the internal database.

(Alcatel6000) # local-userdb add username foo password bar role employee

Test the internal server with username: foo, password bar.

(Alcatel6000) # aaa test-server Internal foo bar Authentication successful

# 3. Set up L2TP IPSec VPN Server on OmniAccess 6000

To configure a Layer 2 Tunneling Protocol, IP Security Virtual Private Network Server:

(Alcatel6000) (config) # crypto isakmp policy 10
(Alcatel6000) (config-isakmp) # authentication pre-share
(Alcatel6000) (config-isakmp) # exit

Set up IKE with a customer provided pre-shared key, keep 0.0.0.0 as is:

(Alcatel6000) (config) # crypto isakmp key f00xYz123BcA address 0.0.0.0 netmask 0.0.0.0

Using a customer provided VPN IP pool):

(Alcatel6000) (config) # ip local pool vpnaddr 2.2.2.1 2.2.2.254

Set up L2TP:

(Alcatel6000) (config) # vpdn group 12tp

PAP will work with most RADIUS servers, use "CACHE-SECURID" if using RSA SecurID):



(Alcatel6000)	(config-vpdn-12tp)	#	ppp authentication PAP
(Alcatel6000)	(config-vpdn-l2tp)	#	no ppp authentication mschapv2
(Alcatel6000)	(config-vpdn-l2tp)	#	client configuration dns 10.1.1.2
(Alcatel6000)	(config-vpdn-l2tp)	#	client configuration wins 10.1.1.2
(Alcatel6000)	(config-vpdn-l2tp)	#	exit

## 4. Set up VPN Dialer and Roles for Users

Set up the dialer. The name will display on the client's machine, so choose something appropriate - spaces are not allowed.

```
(Alcatel6000) (config) # vpn-dialer Default-dialer
(Alcatel6000) (config-vpn-dialer) # ike authentication pre-share
f00xYz123BcA
```

For RSA SecurID only enter:

```
(Alcatel6000) (config-vpn-dialer) # ppp authentication CACHE-SECURID
(only for SecurID)
(Alcatel6000) (config) # exit
```

Set up a role (here the role is called employee) for VPN and the captive portal:

```
(Alcatel6000) (config) # user-role employee
(Alcatel6000) (config-role) # dialer Default-dialer
(Alcatel6000) (config-role) # session-acl allowall
(Alcatel6000) (config-role) # exit
```

Apply roles to the VPN and captive portal:

(Alcatel6000) (config) # aaa vpn-authentication default-role employee
(Alcatel6000) (config) # aaa captive-portal default-role employee

## 5. Set Up the Client (All steps are on client laptop.)

To set up the client:

- 1. Make sure that wireless connectivity is available (ping the switch IP).
- 2. Quit VPN dialer if there's already one running.
- Open browser, user should be redirected to switch's captive portal which should look like this, if user is not for whatever reason, type URL: https://switchip/auth/index.html



Type in username **foo**, password **bar**. You should see a page with the link to **download VPN-dialer**. Select that link and open **setup.exe**.

Follow the onscreen instructions. For more information refer to "VPN Setup" on page 483

If the laptop receives a notice to reboot, comply. Once the laptop is back and the dialer is running, type in username **foo** and password **bar**. The user should connect.

#### Verification and Troubleshooting

Client Side Issues:

If the dialer stays at **Connecting**, make sure wireless connectivity is still up by pinging the switch:

on the switch, enter:

```
(Alcatel6000) #show crypto isakmp sa
Responder IP 3.3.3.1
Initiator IP 1.1.1.1
Initiator cookie 5ea3c79a7492a65d Responder cookie 506acc2482185e1c
Life secs 7200
```



```
transform: esp-3des esp-sha-hmac
```

If there is an initiator IP that matches the client's IP, it means the client successfully started IPSec authentication. Otherwise, check the IKE pre-shared key on the **crypto isakmp key** command and **vpn-dialer default-dialer** command. The two must match.

On the switch, enter:

(Alcatel6000) #show crypto ipsec sa

Responder IP 10.1.1.158 Initiator IP 10.1.1.103 Initiator cookie 0a6c4974a8538522 Responder cookie dc42860c619f3ac4 Life secs 7200 transform: esp-3des esp-sha-hmac

If there is an initiator IP that matches the client's IP, then that means the client is successfully doing IPSec encryption but may have trouble authenticating the actual user **foo**.)

On the switch, enter:

(Alcatel6000) #show vpdn 12tp pool

IP addresses used in pool vpnaddr 2.2.2.1 1 IPs used - 253 IPs free

If there are no IP addresses free, then you've run out of IP addresses for VPN.

If the dialer continues **Logging On** but then fails, the username/password is either incorrect or the RADIUS server is unreachable. If you are using a RSA SecurID, then the user's ID may have been locked out. Check the RSA SecurID server.

If the dialer connects, but no traffic goes through from applications, make sure the inner IP pool is routable. The only way to check this is to sniff between the router and switch.

**NOTE**—Just because the switch IP can ping the default router doesn't mean the VPN IP pool is routable. Check the router. There may be OSPF or other issues.

#### Common Dialer Messages:

#### Interface is down or no route

There is a basic wireless connectivity problem.

#### Route to destination is not wireless

The laptop is connected through a wired link. Uncheck **Wait for Wireless** if that's how you want to connect, or disconnect the wire.

#### No Alcatel switches detected...will retry

The laptop cannot automatically detect the presence of an Alcatel switch. Uncheck **Wait for Wireless** if you think this is an error.

#### Wired. Wireless disabled...will retry

Only when **wirednowifi** is enabled.

#### Verifications:

Use the following commands to verify functionality:

#### (Alcatel6000) (config) #show aaa vpn-authentication

```
Mode = Enabled

Default Role = 'employee'

Dialer download location = /auth/dialer.html

Auth Server List

------

Pri Name Type Status Inservice Applied

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

1 ias RADIUS Enabled Yes 3 ←IMPORTANT LINE
```

#### (Alcatel6000) (config) #show aaa captive-portal

Default role	employee
Guest logon	Disabled
User logon	Enabled
Auto redirect delay	10 seconds
Welcome page location	/auth/welcome.html
Logout popup window	Enabled
Authentication protocol	https
Logon page Theme	default1
Logon wait range	5-10 seconds



(Alcatel6000) (config) #show crypto isakmp policy

```
ISAKMP ENABLED
Protection suite priority 10
    encryption algorithm: 3DES - Triple Data Encryption Standard
(168 bit keys)
    hash algorithm: Secure Hash Algorithm
    authentication method: Pre-Shared Key ←IMPORTANT
    Diffie-Hellman Group: #2 (1024 bit)
    lifetime: [300 - 86400] seconds, no volume limit
Default protection suite
    encryption algorithm: 3DES - Triple Data Encryption Standard
    (168 bit keys)
    hash algorithm: Secure Hash Algorithm
    authentication method: Rivest-Shamir-Adelman Signature
    Diffie-Hellman Group: #2 (1024 bit)
    lifetime: [300 - 86400] seconds, no volume limit
```

#### (Alcatel6000) (config) #encrypt disable

(Alcatel6000) (config) #show crypto isakmp key

ISAKMP Pre-Shared keys configured by Address IP address of the host Subnet Mask Length Key 0.0.0.0 0 f00xYz123BcA ←IMPORTANT

#### (Alcatel6000) (config) #show vpdn l2tp configuration

Enabled

#### (Alcatel6000) (config) #show vpn-dialer Default-dialer

default-dialer		
Attribute	Value	
PPTP L2TP DNETCLEAR WIREDNOWIFI PAP CHAP MSCHAP MSCHAPV2 CACHE-SECURID IKESECS IKEENC IKEGROUP	disabled enabled disabled enabled enabled disabled disabled 28800 3DES TWO	
IKEGROOF IKEHASH IKEPASSWD IPSecSECS IPSecGROUP IPSecENC IPSecAUTH	SHA PRE-SHARE <b>f00xYz123BcA</b> 7200 GROUP2 ESP-3DES ESP-SHA-HMAC	←IMPORTANT ←IMPORTANT



# **Example VPN Configurations**

This section includes sample VPN clients terminating on Alcatel Wireless LAN switches.

### **Using Cisco VPN Client on Alcatel Switches**

If you are terminating a Cisco VPN client on an Alcatel switch, refer to the information below for help in managing this connection.

#### Requirements

The following requirements apply to Cisco VPN clients terminating on Alcatel Wireless LAN switches.

- Release 2.4.0.0 and higher will support Cisco VPN client, version 4.0.2b
- Native Cisco profiles, (151.151.1.1 is your Cisco VPN concentrator)
- Direct Cisco VPN termination, (10.10.1.1 is your Alcatel loopback IP address)

**NOTE**—The DNS server and the DHCP server can not be the same host.

If you are using the native Cisco VPN profile, Alcatel can emulate the Cisco concentrator.

When you select Emulate VPN Servers, as shown below, a **vpn-dst-nat** ACL is added to your logon role.

Switch	Security > VPN Settings > Emulate VPN
Management	Servers
WLAN	
Network	IPSEC PPTP Dialers Emulate VPN Servers Advanced
Radio	IP Address Action
Advanced	151.151.1.1 Delete
RF Spectrum Mgmt Calibration	Add
Optimization	
Protection	
Monitoring	
Security Roles	
Policies	
AAA Servers	
Authentication Methods	
VPN Settings	
Advanced	
WLAN Intrusion Detection	
Rogue AP	
Denial of Service	
Man-In-the-Middle	
٤	🥥 Internet

FIGURE 23-1 Emulating VPN Servers

Go to **Configuration > Security > Roles > Edit Role** (logon) to verify that the **vpn-dst-nat** ACL is associated with the log on role.



Switch	Security > User	Roles >	Edit Role(k	oaon)	
Management	,		``	5,	
WLAN					« Back
Network					
Radio	Firewall Policies				
Advanced	Name Rule Count	Location	Action		-
RF Spectrum Mgmt	vpn-dst-nat 3	0.0.0	Edit Delete 🔺		
Calibration	control 5	0.0.0	Edit Delete 🔺		
Optimization	cantivenortal 3	0.0.0	Edit Delete 🔺		
Protection	upplagen E	0.0.0	Edit Delete		
Monitoring	vpniogon 5	0.0.0	Eult Delete		
Security	Add				
Roles					
Policies					-
AAA Servers	Re-authentication Inte	rval			_
Authentication Methods	Disabled Change	(0 disables re	-authentication, A po	ositive value enables authenticatio	n)
VPN Settings					
Advanced	Role VLAN ID				
WLAN Intrusion Detection Rogue AP	Not Assigned Not Assigned	V Change	е		
Denial of Service					
Man-In-the-Middle	Bandwidth Contract				
Signatures	Not Enforced	<ul> <li>Change</li> </ul>	e		
Policies					
	uniuni I				×
é)					🌍 Internet

FIGURE 23-2 Verifying the Logon Role ACL

Make sure the IKE shared secrets match by going to **Configuration > Security > VPN Settings > IPSec**.

Switch	Securit	y > VPN	l Setti	ings > <b>I</b>	PSEC				
Management	IPSEC PPTP Dialers Emulate VPN Servers Advanced								
Network	L 2TD and		amotore	Entaid		Advanced			
Radio	EziP and Addin Parameters								
Advanced	LINDUG LZ II		•		_				
RF Spectrum Mgmt	Authentical	tion Protocols	PAP	🗹 СНАР 🗆	MSCHAP 🗆 MSC	HAPv2			
Calibration	Primary DN	S Server	10.10.1	.1					
Optimization	Secondary DNS Server 0.0.0.0								
Protection	Primary WI	NS Server	10.10.1	.1					
Monitoring	Canandam.		0.0.0.0						
Security	Secondary	wills server	0.0.0.0						
Roles	Address F	Pools							
Policies AAA Servers	Pool Nam	e Start Ad	ldress	End Address	a Actions				
Authentication Methods	lt2p-pool	10.10.38.1	. 1	0.10.38.254	Edit Delete	9			
VPN Settings	Add								
Advanced	Source M	АТ							
WLAN Intrusion Detection	Cashla Cau	NAT							
Rogue AP	Enable Sou	rteniai							
Denial of Service	IKE Aggres	sive Group Nar	ne cisco	(On	y needed for XAU	TH)			
Man-In-the-Middle	IKE Share	d Secrets							
Signatures Policies	Subnet	Subnet Mas	ik Length	Key	Actions				
	0.0.0.0	0		*****	Edit Delete				
	Add								
	we put t								
	IKE POIICI	es Formulation	1 to all	Authoritie	-Non Current	Life blass	A		
	Prioricy	Encryption	riasn	Authentic	ación Group	Liretime	Edit		
	10	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400] seconds, no volume limit	Delete		
	Default	3DES	SHA	RSA	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete		
	Add								
							Apply		
	Command	is				View Commands			
3							Internet		

FIGURE 23-3 Matching the IKE Shared Secret

The IKE Aggressive Group Name is the same as the Cisco dialog box Authentication tab Group Authentication Name. The IKE Shared Secret is the same as the Cisco dialog box Authentication tab Group Authentication Password.



Connection Entry:
Host: 10.10.1.1
Authentication Transport Backup Servers Dial-Up
Group Authentication
Name: cisco
Password: +++++
Confirm Password:
C Certificate Authentication
Name:
Send CA Certificate Chain
Erase User Password Save Cancel

FIGURE 23-4 Matching IKE Parameters

#### **Default Values**

The following figures show the default values for the Cisco dialog box Transport, Backup Servers and Dial Up tabs

## Default Transport Values

Connection Entry:
Description:
Host: 10.10.1.1
Authentication Transport Backup Servers Dial-Up
Enable Transparent Tunneling
IPSec over UDP (NAT / PAT)
C IPSec over TCP TCP Port: 10000
Allow Local LAN Access
Peer response timeout (seconds): [90
Erase User Password Save Cancel

FIGURE 23-5 Default Transport Tab Values



Default Backup Servers Values

Connection Entry:	
Host: 10.10.1.1	
Authentication   Iransport   Backup Servers   Dial-Up	[
	Add Remove
Erase User Password Save	Cancel

FIGURE 23-6 Default Backup Servers Tab Values

## Default Dial Up Values

Connection Entry:
Description:
Host: 10.10.1.1
Authentication Transport Backup Servers Dial-Up
Connect to Internet via dial-up
Microsoft Dial-Up Networking
Phonebook Entry: Aruba VPN 💌
Third party dial-up application     Application:     Browse
Erase User Password Save Cancel

FIGURE 23-7 Default Dial-Up Tab Values

## **Typical Third-Party VPN Clients**

The steps required to terminate typical VPN clients on an Alcatel Wireless LAN switch are:

- Configure the Alcatel GUI for basic VPN connection
- Configure the VPN client wizard (if applicable)
- Logon using the VPN client dialog box

#### **Basic Alcatel Configuration**

Configure the group name by selecting **Configuration > Security > VPN Settings > IPSec**.



VPN Configuration | 537

Management										
WLAN	IPSEC	PPTP	Dialers	Emul	ate VPN	Servers	Advanced			
Network	L2TP and XAUTH Parameters									
Radio	Enable L2TP 🔽									
Advanced	Authentical	tion Protocols	PAP	CHAP T	MSCHA	MSCI	HAPv2			
Calbration	Primary DN	5 Server	10.10.1	.1						
Optimization	Secondary	DNS Server	0.0.0.0							
Protection	Primary WI	NS Server	10.10.1	1						
Monitoring	Secondary	WINS Server	0.0.0.0							
Security	Secondary	naio su to	0101010	_						
Policies	Address F	200ls								
AAA Servers	Pool Nam	e Start Ad	dress	End Addres	5 /	ctions				
Authentication Methods	k2p-pool	10.10.38.1	1	0.10.38.254	Edit	Delete	9			
VPN Settings	Add									
Advanced	Source NAT									
WLAN Intrusion Detection	Enable Source NAT									
Denial of Service	IKE Aggres	sive Group Nan	ne norte	d (0	ily neede	d for XAU	THO			
Man-In-the-Middle	IVE Chare	d Cocrote								
Signatures	INE OTHER	userets			1000	2011				
Policies	Subnet	Subnet Mas	k Length	Key	Act	ons				
	0.0.0.0	0		*******	Edit	Delete				
	Add									
	<b>IKE Polici</b>	es								
	Priority	Encryption	Hash	Authentie	ation	Group	Lifetime	1	Action	
	10	3DES	SHA	PRE-SHARE	10	SROUP 2	[300 - 86400] seconds, no volume I	mit Edit	Delete	
	Default	3DES	SHA	RSA	9	SROUP 2	[300 - 86400] seconds, no volume l	mit soort	Delete	
	Add									
									No. of Concession, Name	
									Apply	
	Command	İs					View Commands			

FIGURE 23-8 Configuring a Group Name

Verify the IKE policy settings by selecting **Configuration > Security > VPN Settings > IPSec > Edit**. Make sure the IKE key matches, that the IKE policy is pre-shared key, and that the Group ID is defined.

Policies	© Copyr	right 2003 Aruba Wireless Networks, Inc., All Rights Reserved.   Email Support
Signatures		
Man-In-the-Middle		
Denial of Service		
Rogue AP		
Advanced		
VPN Settings		
Authentication Methods		
AAA Servers		
Policies		
Roles		
Monitoring	and the second second	Apply
Protection	Life Time	
Optimization	Diffie Hellman Group	GROUP 2 💌
Calibration	Authentication	PRE-SHARE V
RF Spectrum Mgmt	Hash Algorithm	SHA 👻
Kadio Advanced	Encryption	3DES 👻
Network	Priority	10
WLAN	(10)	
Management	(10)	r a securitys > 1 Sec > Luit



Verify the basic logon role by selecting **Configuration > Security > Roles > Edit Role** (logon).



Management WLAN	5							« Back
Network.								
Radio	Firewall Po	licies						
Advanced	Name	Rule Count	Location	Darrant I	Action	CONTRACTOR OF		
Calbration	control	6	0.0.0	Edit	Delete			
Optimization	captiveportal	3	0.0.0	Edit	Delete	•		
Protection	vpnlogon	5	0.0.0	Edit	Delete	▲ ▼		
Monitoring	Add							
iecunity								
Roles								
Policies	Re-authen	tication Int	erval					
AAA Servers Authentication Methods	Disabled	Change	0 disables n	e-authe	ntication. A	positive	value enables authentication)	
Advanced	Role VLAN	ID	-					
WLAN Intrusion Detection Rogue AP	Not Assigned	Not Assigned	Chang	90				
Denial of Service	Bandwidth	Contract	-					
Man-In-the-Hiddle Not Enforced Change								
Policies	<b>VPN Dialer</b>							
	Not Assigned	Not Assigned	Chang	pe				
	L2TP Pool		())errie					
	default-l2tp-p	ool Not Assign	ned V Chi	ange				
	PPTP Pool							
	default-pptp-	Not Assig	ned 🛩 Ch	hange	]			
	Commands						View Commands	
	Apply							

FIGURE 23-10 Basic Logon Role

Modify the basic logon role by adding an ACL to allow TCP on port 17 by selecting **Configuration > Security > Roles > Edit Role (logon) > Edit Policy** (Control).

Switch Management WLAN Network Radio	Securi (contr	ity > Usei ol)	r Roles	> Edi	t Rol	le(logo	on) > <b>f</b>	Edi	t Po	olicy	« Back
Advanced	Location	0.0.0	)	1							
RF Spectrum Mgmt	Rules	0.00									
Calibration	Source	Destination	Service	Action	Log	Queue	Acti	ion			
Optimization	any	any	svc-icmp	permit		low	Delete		T		
Protection	any	any	svc-dns	permit		low	Delete		V		
Monitoring	any	any	svc-papi	permit		low	Delete		V		
Roles	any	any	svc-tftp	permit		low	Delete		V		
Policies	any	any	svc-dhcp	permit		low	Delete		T		
AAA Servers	any	any	tcp 17	permit		low	Delete		V		
Authentication Methods	Add										
Advanced								App	ly		
WLAN Intrusion Detection Rogue AP Denial of Service Man-In-the-Middle											
Signatures Policies											
				© Copyrig	HL 2003	3 Aruba Win	eless Netwo	eks,	Inc., i	All Rights Reserve	1.   Email Support
				_			_			😴 Inter	net

FIGURE 23-11 Allowing TCP on Port 17

#### Configuring a Third-Party VPN Client

Complete the VPN client wizard with source and destination information to configure the VPN client.



#### Troubleshooting the Connection

If you have trouble connecting to the Alcatel Wireless LAN switch using a typical third-party VPN client, check the following:

- Verify the ACL groups in the "logon" role.
- Verify that TCP port 17 is allowed (this solves a banner problem).
- Verify the IKE key is matching.
- Verify that Group ID is defined.
- Verify that the IKE policy is pre-shared key.

If you need further assistance, see "Contacting Alcatel" on page xxi for support.

The setup for Cisco is actually the same as for Alcatel VPN (w/o dialer). You can ignore input of the XAuth groupname (that's just for show). To include AES-256, you need to (assuming GUI):

- 1. Navigate to Configuration->Security->VPN Settings->IPSEC:
- 2. Add an IKE policy with AES-256, pre-share, and SHA.
- 3. Navigate to Configuration->Security->VPN Settings->Advanced.
- 4. Add or change the IPSec transform to AES-256 and SHA.

NOTE—Cisco does not support AES-192 (only 128 and 256.

# CHAPTER 24 Switch Maintenance

Alcatel switches provide full support for maintenance at the switch level, the file level, the wireless LAN level, and at the captive portal level. All maintenance functions are available from the Maintenance tab on the toolbar.

## Switch Level Maintenance

To access the switch level maintenace functions, click **Maintenance > Switch**. The five switch maintenance functions are:

- Image Management
- Reboot Switch
- Reboot Peer Supervisor Card
- Clear Config
- Boot Parameters

#### Image Management

Navigate to **Maintenance > Switch > Image Management** to access the image management screen:

Switch > Image Manage	ement
Upgrade using IFTP C FTP	
Server IP Address	
Image File Name	
Partition to Upgrade	Partition 0     Partition 1
Boot Partition	Partition 0     Partition 1
Reboot Switch After Upgrade	C Yes 🖲 No
Save Current Configuration Before Reboot	G Yes C No

Image management options are.

Upgrade using	Specify how you are going to copy an image onto the server. Both TFTP and FTP are supported.
Server IP Address	Specify the IP address of the TFTP or FTP server which contains the image to download onto the switch.
Image File Name	Enter the name of the image file.
Partition to Upgrade	You can copy the image into Partition 0 or 1. Specify the location here.
Boot Partition	Specify which partition the switch will use when it reboots.
Reboot Switch After Upgrade	To use the new image once it has been downloaded, specify <b>Yes</b> to reboot the switch. To keep using the current boot image, click <b>No</b> .
Save Current Configuration Before Reboot	Click <b>Yes</b> to write the current configuration to file so changes will not be lost upon reboot. Click <b>No</b> to leave the configuration file unchanged.

## **Reboot Switch**

To reboot the switch, typically after an image update, click **Maintenance > Switch > Reboot Switch**.

Switch > Reboot Switch	
Confirm	
Save Current Configuration Before Reboot ?	€ Yes C No
Continue	Cancel

To save any changes to the current switch configuration, click **Yes**. To leave the configuration file unchanged, click **No**.

To proceed with the switch reboot, click **Continue** and follow any prompts.

## **Reboot Peer Supervisor Card**

The Maintenance > Switch > Reboot Peer Supervisor Card option requires an Alcatel Wireless LAN switch with a supervisor card installed.

## **Clear Config**

To reset the switch configuration to factory default settings, use the Maintenance > Switch > Clear Config option.

Switch > Clear Config		
Confirm	an and the state of the state	
and a second sec		
This erases the Switch Configuration and will default state. This action does not remove th the switch and reboots the switch after erasi	return the Switch to its f ne persistent state data r ing the configuration.	actory naintained ir

The current configuration is erased and the factory default configuration is set as the boot configuration. This option forces the switch to reboot using the factory default configuration. (The persistent state data maintained in the switch is preserved.)



When ready to revert to the original, factory configuration, click **Continue** and follow any prompts.

From the CLI, enter:

write erase all reload

Make sure you do this from the serial console as this removes all IP and port configurations. The switch will reboot and display the Setup Dialog.

#### Synchronize

This feature is only valid in redundant Master-Master configurations.

To synchronize the database with the other master, use the Maintenance > Switch > Synchronize Database option and click Sync.

Synchronization Status		
Last synchronization time: Not synchronized since last reboot Periodic synchronization is disabled Synchronization includes RF plan data		
	Sync	< <back< th=""></back<>

The system will prompt you to confirm that you want to synchronize the database.

#### **Boot Parameters**

The boot parameters are the name of the boot file and its boot partition location. Access these parameters by accessing **Maintenance > Switch > Boot Parameters**.

Boot Partition	Partition 1	C Partition 0	Partition 1
Configuration File	default.cfg	default.cfg	~

The following parameters and options may be configured through Web UI.

Boot Partition	Specify which partition the switch will use when it reboots.
Configuration File	Select the name of the saved configuration file from the drop down menu.

When finished, click Apply.

# **File Maintenance**

The four options available in the **Maintenance > File** menu are:

- Copy Files
- Copy Logs
- Copy Crash Files
- Delete Files

## **Copy Files**

You can copy files on the switch to off-switch locations by selecting **Maintenance > File > Copy Files**.



Source Selection	
🔹 Flash File System	abcd 💌
C TFTP Server	
C Running Configura	ition
C Startup Configura	tion
C FTP Server	
Destination Selection	1
📀 Flash File System	File Name
C	
1FIP Server	

The options are.

Source Selection	Select <b>Flash File System</b> and select the name of a file from the drop-down menu.
	To use a TFTP server, click <b>TFTP</b> and enter the IP address of the TFTP server.
	To copy the running configuration, click <b>Running Configuratio</b> n.
	To copy the startup configuration, click <b>Startup Configuration</b> .
	To use a use an FTP server, click <b>FTP</b> and enter the IP address of the FTP server

Destination Selection	If you are copying a flash file system, select <b>Flash File System</b> and specify the name of a file.
	To use a TFTP server, click <b>TFTP</b> and enter the IP address of the TFTP server.
	To use a use an FTP server, click <b>FTP</b> and enter the IP address of the FTP server.

#### **Copy Logs**

To copy logs from the switch to another system, go to **Maintenance > File > Copy Logs**.

File > Copy	Logs		
Destination			
• TFTP Server	IP Address	File Name	
C FTP Server			
Technical Support	Include technical supp	port information	

You can copy the logs using an FTP server or TFTP server. Once you have specified the transfer protocol, specify the IP address and file name to be used for the log file.

## **Copy Crash Files**

To copy crash files from the switch to another system, go to **Maintenance > File** > **Copy Crash Files**.



File > Copy	Crash Files		
Destination			
• TFTP Server	IP Address	File Name	
C FTP Server			

You can copy the crash files using an FTP server or TFTP server. Once you have specified the transfer protocol, specify the IP address and file name to be used for the crashfile.

#### **Backup Flash**

To copy the files in flash, go to **Maintenance > File > Backup Flash**.

contents of the	e flash to flashbackup.tar.gz		
Once the backup is complete, it can be copied elsewhere for safe-keeping.			
up Cor	py Backup		
k	kup Co		

Click **Create Backup** to start the backup process. The system will report the backup being created when finished. Clicking **Copy Backup** is the same as selecting **"Copy Files"**.

#### **Restore Flash**

To restore Flash files which have previously been backed up, go to **Maintenance** > File > Restore Flash.

File > Restore Flash	
	This will restore the contents of flashbackup.tar.gz
	A reboot will be required once this is completed.
	Restore

The system must reboot before it can use the restored Flash files.

## **Delete Files**

To keep from running out of flash file space, you should delete files you no longer need. You can also delete files that you have copied off the switch. To remove unwanted or no longer needed files, go to **Maintenance > File > Delete Files**.

le List	
abod Ib_dump.sql Ib_dump_pre_2_0_2 Jefault.ofg-setup-bk	.sql
lashbackup.tar.gz	~

Click the file(s) to be deleted, and click **Delete**. To select multiple files:

Shift-click file names that form a continuos block of file names.

Ctrl-click individual file names that are not continuous.

# Wireless LAN Maintenance

The maintenance-level commands that you can perform on an Alcatel Wireless LAN switch are:



- Calibrate the Radio Network—See "Calibration" on page 289.
- Program Access Points—See "AP Reprovisioning" on page 478.
- Reboot Access Points—See below.
- WMS Database—See below.

#### **Rebooting Access Points**

To reboot an Access Point, go to Maintenance > Wireless LAN > Reboot AP.

Sear	th				
Г	Location	AP IP 🔺	Wired MAC Address *	AP Type 🔺	
Г	1.1.6	10.4.21.212	00:0b:86:c2:04:39	60	
Г	1.1.7	10.4.21.101	00:0b:86:c2:04:8a	OR-61	
F	1.1.7	10.4.21.102	00:0b:86:c2:04:8a	OR-61	
		1   1	-3 of 3 10 💌		

Click the Access Point(s) you want to reboot, and click **Reboot**. To find an AP, click **Search** and enter any information you have (such as location, IP or MAC address). To organize the display to make finding APs easier, you can sort (ascending or descending) on location, IP and MAC address.

The display is limited to ten APs per page. Use the page navigator to scroll through the listings of APs controlled by this switch.

#### Managing the WMS Database

You can import a new WMS database, export this one, clean, or re-initialize it.

Information on cleaning and re-initializing TBC.

#### Exporting a WMS Database

твс

port	Import	Clean old entries	Re-initialize Database	< <back< th=""></back<>
Ex	plorer User	Prompt		X
Si Pl	cript Prompt: lease enter the	name of the file to export		OK Cancel

## Importing a WMS Database

твс

Export Im	iport	Clean old entries	Re-initialize Database	< <back< th=""></back<>
1	Microso	ft Internet Explorer		
	?	This will overwrite the WMS	DB. Proceed?	

## **Removing Old Entries**

твс



VLAN > WMS	Clean old entries	Re-initialize Database	<back< th=""></back<>
<b>•</b>	icrosoft Internet Explore	er 🔀	
	This will clean the WI	MS DB. Proceed?	

#### Re-initializing a WMS Database

твс

Export Imp	oort Clear	n old entries	Re-initialize Database	< <back< th=""></back<>
		Micros	oft Internet Explorer	
		2	This will re-create the database.	Proceed?
			OK Cancel	
# **Captive Portal Maintenance**

The captive portal is the screen users see when their wireless device connects to the network through the switch. This screen allows network administrators to control what users and guests see, and what they can do once they log in and are authenticated.

Maintenance on the captive portal consists of two options:

- Customize Login Page
- Upload Certificate

## **Customizing the Login Page**

To change what Wireless LAN users see when they connect through the Alcatel Wireless LAN switch, go to **Maintenance > Captive Portal > Customize Login Page**.

Captive Portal > Customize Login Page	
Eustomize the look of your Captive Portal	
Page Design: (Click your choice.)	
Page text (n HTML format): (Size limited to s6k)	
Additional options	
More options will be made available here when you have chosen a page design from the choices above.	
Edit your Acceptable Use Policy	
Policy Text (In HTML formal): (Used only when Guest Access is enabled. Size limited to 16K)	
Submit Reset Vew CaptivePortal	

From this screen you can select a background login page or upload your own login page. You can also edit your policy for guests. When you are finished customizing the login page, click **Submit**. To erase any changes without saving them, click **Reset**. To see what the captive portal will look like with the changes you have made, click the **View CaptivePortal** link.



## **Upload Certificate**

To manually upload a authentication certificate for the captive portal, go to **Maintenance > Captive Portal > Upload Certificate**.

The certificate should be in X.	509 PEM format. After the certificate odule of the switch will restart. This
shutdown all Web Server con	ections.

Specify the name of the certificate file to be imported in the **File to be imported field**. You can click **Browse** to search for the file. When ready, click **Upload**.

As the onscreen notice advises, the switch expects the certificate file to be an X.509 PEM file. The onscreen notice also warns that the uploading of a new certificate will cause the switch to shutdown all Web Server connections while the certificate is being installed.

## **Upload Custom Login Pages**

To manually upload a custom login page for the captive portal, go to **Maintenance > Captive Portal > Upload Custom Login Pages**.

File to be imported		Browse.
Page Type:	Content	~
Revert to factory default set	tings 🔽	

твс

Chapter 24



**OmniAccess Reference: AOS-W System Reference** 



# Monitoring and Troubleshooting





**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 25 Monitoring the Wireless Environment

The Web UI Monitoring tab contains information on the wireless network, the Alcatel Wireless LAN switch, and the Wireless LAN. If you have created custom logs, you can view them here.

#### **Network Summary**

	TOTAL	TOTAL	IPSEC	IPSEC
	UP	DOWN	UP	DOWN
WLAN Switches	1	0		
Aruba Access Points	3	4	1	1
Aruba Air Monitors	0	1	0	0
Unprovisioned Aruba APs	0			
Enterprise Clients	0			
RADIUS Servers	1	0		
LDAP Servers	Q	<u>0</u>		
WLAN Performance S	ummar	Y		
	Last 5	Min Las	t Hour	All
Load Balancing Events	0	0		0
Interference Events	0	Q		0
	0	Q		0
Bandwidth Exceeded	and the second se			

WLAN Attack Summ	nary			
	La	st 5 Min	Last Ho	ur Al
Denial of Service Attack	s <u>0</u>		0	0
Man in the Middle Attack	s Q		0	0
Signature Pattern Match	ies Q		0	Q
Policy Violations	Q		0	0
Rogue APs Detected	Last	5 Min	u y Last Hour 0	All 3
	Last	5 Min	Last Hour	All
Rogue APs Detected Rogue APs Disabled Interfering APs Detected	Last Q Q d 6	5 Min	u <b>y</b> Last Hour 0 0 25	All 3 0 45
Rogue APs Detected Rogue APs Disabled Interfering APs Detecter Known Interfering APs	Last Q Q d <u>6</u> Q	5 Min	25 0 0 25	All 3 0 45 0
Rogue APs Detected Rogue APs Disabled Interfering APs Detecter Known Interfering APs Client Classification	Last 0 0 0 0 0 Sumr Last 5	5 Min nary Min La	Last Hour 0 25 0 st Hour	All 3 0 45 0
Rogue APs Detected Rogue APs Disabled Interfering APs Detecter Known Interfering APs Client Classification Valid Clients	Last 0 0 0 0 0 5 0 Last 5 0	5 Min nary Min La Q	Last Hour 0 25 0 st Hour	All 3 45 0 All
Rogue APs Detected Rogue APs Disabled Interfering APs Detecte Known Interfering APs Client Classification Valid Clients Interfering Clients	Last 0 0 0 0 5 0 Last 5 0 2	5 Min nary Min La 2	Last Hour 0 0 25 0 st Hour	All 2 45 0 All 2

FIGURE 25-1 Monitoring the wireless environment

# **Network Monitoring**

To see a summary of the status of the wireless network, click Monitoring. **Network Summary** is displayed by default. Wireless LAN Network Status shows the number of operational Wireless LAN switches, Access Points, Air Monitors, unprovisioned APs, enterprise clients, RADIUS servers, and LDAP servers.

Wireless LAN Performance Summary shows throughput metrics (the last five minutes, the past hours, and overall) for Load Balancing Events, Interference Events, Bandwidth Exceeded, and Error Threshold Exceeded.

The Security Summary statistics shows the last five minutes, last hour, and overall summaries for Wireless LAN Attack statistics, Rogue AP Classification Summary, and Client Classification Summary data. Wireless LAN Attack Summary data includes: Denial of Service Attacks, Man in the Middle Attacks, Signature Pattern Matches, and Policy Violations statistics.

Rogue AP Classification Summary statistics include: Rogue APs Detected, Rogue APs Disabled, Interfering APs Detected, and Known Interfering APs.

Client Classification Summary statistics include: Valid Clients, Interfering Clients, and Disabled Rogue Clients.

Select **Monitoring > Network > All Wireless LAN Switches** to see details about each Wireless LAN switch. Details include IP address, location (from RF Plan), Type (Master or local), and AOS-W version running.

Select **Monitoring > Network > All Access Points** to see details about each Access Point. Details include Name, Location, IP Address, Type, IP address of the Wireless LAN switch, number of, and channels used by, 802.11b and g clients, and number of 802.11a clients and the channels they are using.

Select **Monitoring > Network > All Air Monitors** to see details about air monitors. Details include Name, Location, IP Address, Type, Switch IP, Last Seen, and Status.

Select **Monitoring > Network > All Wireless LAN Clients** to see details about wireless clients. Details include MAC Address, Name, IP Address, Role, Authentication Method, Home Switch, and Current Switch.

Select **Monitoring > Network > Global Events** to see details about wireless activity. Event details include Event ID, Type, Info(mation), Device type, MAC Address, Count (which is a count of how many times the event has occurred), and Occurred Time. Selecting **Global Events** is the same as clicking **Events** on the toolbar.

# Switch Monitoring

The **Monitoring > Switch** screens provide details about the Wireless LANs in the wireless network.

Select **Monitoring > Switch Summary** to see details about the Wireless LAN switch including its Model, AOS-W Version, IP Address, and MAC Address.

Select **Monitoring > Switch > Access Points** to see details about the APs connected to this Wireless LAN switch. Details include Name, Location, IP address, Type, 802.11b and g Clients, 802.11a clients, the Channel Power Levels for these a, b, and g client, and the uptime for each AP.

Click:

Status	To display dynamic data including number of packets and number of associated clients.
Profile	To show static data such as AP configurations.
AP Activity	To show overall AP status.
Packet Capture	To display the packet capture screen.
Locate	To display the RF Plan page and perform a triangulation.
Ping	Issues a ping.

Select **Monitoring > Switch > Air Monitors** to see details about air monitors connected to this Wireless LAN switch. Details include NAme, Location, IP address, Type, and Uptime for each AM. Click **Overview, Channel, APs, Clients,** and **Packet Capture** for additional information.

Select **Monitoring > Switch > Clients** to see details about wireless clients. Details include User Name, MAC Address, Client IP address, User Role, Access Method, Age, and Status.

Select **Monitoring > Switch > Blacklist Clients** to see details about users who are not welcome. Details include Client MAC address, Reason, and Block Time. (Block Time is the time in seconds that a blacklisted user is blocked from attempting to connect.) Click **Enable** to turn on DoS prevention. Click **Remove from Blacklist** to allow the selected user to access the wireless network without restriction.

Select **Monitoring > Switch > Firewall Hits** to see details about attacks on the switch. Details include User Role Hits (including Role, Policy, source and destination addresses, Service, Action, Dest/Opcode, New Hits, Total Hits, and Index), Port Based Session ACL Hits (including Policy, source and destination addresses, Action, Dest/OPcode, New Hits, Total Hits, and Index),



and Port ACL Hits (including ACL, ACE, New Hits, Total Hits, and Index. ACE is the individual permit or deny rule that makes up an ACL. The index number is the priority of each ACE starting with 1.)

Select **Monitoring > Switch >Ports** to see details about port activity. Details include Admin State, Operational State, Port Mode, VLAN Association, Trusted or untrusted. Click **Status**, **Profile**, **Activity**, or **Diagnostics** for additional information.

Select **Monitoring > Switch > Inventory** to see details about switch components, software, and environment. Details for Supervisor cards include Status, FPGA Revision, SC Assembly Number, SC Serial Number, Crypto Assembly Number, Crypto Serial Number, management Port NW MAC Address, Switch Base MAC Address, Peer Supervisor Card. Details for line cards are reported for each slot occupied by a line card and include: FPGA Revision Number, Gigabitethernet Daughter Card, SPOE<sup>1</sup> Daughter Card, Supervisor Card 0, and Supervisor Card 1. Fan and Power Supply details include status for Fan 0, Fan 1, and Fan 2 as well as for Power Supply 0, Power Supply 1, and Power Supply 2.

Environmental Readings includes Internal Temperature, System 5.0V status, System 3.3V status, System 2.5V status, and CPU 2.0V status.

Software Information includes General information on Switch Model, AOS-W Version, Complied date and build number, ROM version, Switch Uptime, and Alcatel Firmware versions. Information on Licenses includes Max AP Limit, Max Mux Limit, Wireless LAN Switch, Wireless LAN IDS, Web UI, and VPN/Firewalls.

Select **Monitoring > Switch** to see the switch log. Selecting the **Events** tab displays the same screen. (See "Events" below.)

## Sample Monitoring Information

This section includes sample screens of monitoring information available through AOS-W.

<sup>1.</sup>SPOE stands for Serial Power over Ethernet.

## Sample Air Monitor Screens

To display a typical screen for Air Monitors, select **Monitoring > Switch > Air Monitors**.

Network Network Summary	Switch > Air Monitors	
All WLAN Switches	Local Air Monitors	Search
All Access Points	AM Name Location AM IP A	P Type A Uptime A
All Air Monitors	C 255.255.65535 192.168.64.101 AP-	-60 1d:18h:40m
All WLAN Clients	C 255.255.65535 192.168.64.163 AP-	-60 1d:18h:40m
Global Events Switch	C 255.255.65535 192.168.64.173 AP-	-60 1d:18h:40m
Switch Summary	C 255.255.65535 192.168.64.175 AP-	-60 1d:18h:40m
Access Points	C 255.255.65535 192.168.64.176 AP-	-60 1d:18h:40m
Air Monitors	C 255.255.65535 192.168.64.177 AP-	-60 1d:18h:40m
Clients Blacklist Clients	C 255.255.65535 192.168.64.180 AP-	-60 1d:18h:40m
Firewall Hits	C 255.255.65535 192.168.64.184 AP-	-60 1d:18h:40m
Ports	1   1-8 of 8 10 💌	
Inventory		
Local Events	Overview	Channel APs Clients Packet Capture
WLAN		

#### FIGURE 25-2 Monitoring Air Monitors

From the screen shown in Figure 25-2, you can select to view information on:

- Overview—see Figure 25-3.
- Channel—see Figure 25-4 and Figure 25-5.
- **APs**—see Figure 25-6.
- Clients—see Figure 25-7
- Packet Capture—see Figure 25-8.



## **Overview** Information

Click **Overview** to see the following information.



FIGURE 25-3 Overview Information

## **Channel Information**

Click Channel to see the following information.



## FIGURE 25-4 Channel Information



The details on the selected change are shown in the figure below.

Aggreg	ate Sta	tistics	-									
Bandwidt	h Rate		7 kbj	os								
Retry Pa	ckets		0%									
Low Spee	ed Packet	s	100	%								
Multicast	/Broadca:	st Packe	ets 100	%								
Fragmen	ted Packe	ets	0 %									
PHY Erro	rs		0 %									
MAC Erro	ors		0%									
Raw Co	unters		-									
Packets		930	04709									
Bytes		842	2391243									
Retry Pa	ckets	450	06									
Fragmen	ted Packe	ets O										
PHY Erro	rs	0										
MAC Erro	ors	586	591									
802.11	Packet	Туре	Distrib	ution	-							
	Manag	gemen	t Con	trol E	ata							
Packets	8862657		30439	97 789	164							
Bytes	8056915	73	42624	152 324	37218							
002.11	Data D	ockot	Dictribu	rtion	-							
002.11	Broad	cast	Multica	ation act Un	icaet							
Dackate	23907		334	5412	3							
Bytes	5790631		219174	2642	7413							
0,000	0, 20001			2012								
Packet	Size Dis	tribut	ion					-				
0-63 by	tes 6	4-127	128-3	255 23	56-511	512	-1023	1024-	+			
21394	19	263	7321	704	5	13106		10835				
Packet	Rate Di	stribu	tion									-
	1M	2M	5.5M	11M	6M	9M	12M	18M	24M	36M	48M	54M
Packets	30435	210	384	47932	0	0	3	0	0	0	0	Ø
Bytes	6429419	97275	143435	2576524	10	0	1848	0	0	0	0	0

FIGURE 25-5 Overview Information

## AP Information

Click APs to see the following information.



FIGURE 25-6 AP Information

## **Client Information**

Click Clients to see the following information.



FIGURE 25-7 Client Information



### Packet Capture Information

Click **Packet Capture** to see the following information.

Network Network Summary	Mor	ito	ring >	> Air I	Ionitor	: 192.1	.68.64	.184 >	Pack
All WLAN Switches	Searc	h Re	sult						
All Access Points		ID	Туре	Radio	Channel	Packets	Status	Target	Filter
All Air Monitors	None f	ound.							
All WLAN Clients			Refresh	Ston	Delete	Pause	Resume	New	
Global Events		- 1	Ne	w Raw F	acket Cant	ure	(Q) Launch i	NiroPeek	
Switch			140	AT INGTO I	dokot Capt			AILOFCON	
Switch Summary									

#### FIGURE 25-8 Packet Capture Information

### **Example Port Information**

To see monitoring information on ports, select Monitoring > Switch > Ports.

Network Network Summary All WLAN Switches	Switch > Ports
All Access Points	Port Selection Options
All Air Monitors	C Admin State
All WLAN Clients Global Events	C Port Mode C VLAN Association
Switch Switch Summary	C Trusted
Access Points	Port Selection
Air Monitors	24 25 24 25
Clients Blacklist Clients	
Firewall Hits	
Ports	Select All Clear All
Inventory	Empty Slot
Local Events	Supervisor Caru
WLAN <no found="" ssids=""></no>	
Debug Local Clients	Status Profile Activity Diagnostics

FIGURE 25-9 Monitoring Ports

The following types of information are available:

Status—see Figure 25-10.

Profile—see Figure 25-11.

Activity—see Figure 25-12.

Diagnostics—see Figure 25-13.

Port Status Information

Click Status to see the following types of information.

Network Network Summary	Port 2/14 > St	atus		
All WLAN Switches	General		Spanni	ng Tree
All Access Points	Operational Status	Up	Status	DISABLED
All Air Monitors	Line Protocol	Down		
All WLAN Clients	Counters Last Cleared	5 day 23 hr 50 min 0 sec		
Global Events	Link Status Last Changed	5 day 19 hr 49 min 42 sec		

## FIGURE 25-10 Port Status Information

## Port Profile Information

Click **Profile** to see the following types of information.

Network Network Summary	Port 2/1	4 > <b>Pr</b>	ofile
All WLAN Switches	General		
All Access Points	Port Type	FastEthern	iet
All Air Monitors	MAC Address	00:0B:86:0	0:F2:0F
All WLAN Clients	Description	10/100 Co	pper-Level
Global Events	Encapsulation	ARPA	
Switch	Loopback	Not set	
Switch Summary	Duplex	AUTO	
Access Points	Speed	AUTO	
Air Monitors	MTU	1500bytes	
Clients	Bandwidth	200 Mbits	
Blacklist Clients	Trusted	Yes	
Eirawall kite	POE	On	
Deute	Mode	Access	
Ports			
Inventory	Spanning Tr	ee	
Local Events	Port Path Cost		19
WLAN	Port Priority		128
<no 22105="" found=""></no>	Designated Ro	ot Priority	32768
Debug Local Clients	Designated Ro	ot Address	00:0b:86:00:f2:0
Local clients	Designated Pol	rt Priority	32768
Process Logs	Designated Pol	rt Address	00:05:86:00:12:0
Lustom Logs	Designated Por	rt	41
<no cuscoiii="" loys="" pound=""></no>	Path Cost		0
	Message Time	Timer	0
	Forward Delay	Timer	0
	Hold (imer		U

#### FIGURE 25-11 Port Profile Information



## Port Activity Information

Click Activity to see the following types of information.

Network Network Summary	Port 2/14 >	> Activity « Back
All WLAN Switches	In Counters	
All Access Points	Octets	3243923
All Air Monitors	Unicast Packets	20078
All WLAN Clients	Multicast Packets	7
Global Events	Broadcast Packets	34
Switch		
Switch Summary	Out Counters	
Access Points	Octets	5811311
Air Monitors	Unicast Packets	20584
Clients	Multicast Packets	1092
Blacklist Clients	Broadcast Packets	5440
Firewall Hits		Clear Counters
Ports		

FIGURE 25-12 Port Activity Information

#### Port Diagnostic Information

Click **Diagnostics** to see the following types of information.

Network Network Summary	Port 2/14 >	Diag	nostics	« Back
All WLAN Switches	Error Counters			
All Access Points	Input Error Bytes	248		
All Air Monitors	CRC Errors	8		
All WLAN Clients	Frames	0		
Global Events	Output Error Bytes	0		
Switch	Deffered	0		
Switch Summary	Collisions	0		
Access Points	Late Collisions	0		
Air Monitors	Throttles	0		
Clients				
Blacklist Clients			Clear Counters	

FIGURE 25-13 Port Diagnostics Information

## Status Information

Click Status to see the following types of information.

Network Network Summary	Port 2/14 > Sta	itus	
All WLAN Switches	General		Spanning Tree
All Access Points	Operational Status	Up	Status DISABLED
All Air Monitors	Line Protocol	Down	
All WLAN Clients	Counters Last Cleared	5 day 23 hr 50 min 0 sec	
Global Events	Link Status Last Changed	5 day 19 hr 49 min 42 sec	

#### FIGURE 25-14 Port Status Information

# **Events**

As mentioned above, selecting **Monitoring** > **Switch** is equivalent to selecting the **Events** tab.

No Custom Reports>	Searc	h Results						Search
	Group	By None	~					
		Event ID 🔻	Туре 🕇	Info	Device	MAC Address 🔺	Count 🝷	Occurred Time
		1540 🥐	Rogue AP		AP	00:0b:86:80:12:b8	381	14:03:55 7/26/2004
		913 🅐	Rogue AP		AP	00:0b:86:80:1f:58	516	14:03:55 7/26/2004
		52 🥐	Rogue AP		AP	00:0b:86:80:60:71	4436	14:03:40 7/26/2004
		919 🍞	Rogue AP		AP	00:0b:86:80:1f:50	772	14:02:54 7/26/2004
		487 🍞	Rogue AP		AP	00:0b:86:80:60:72	3510	14:01:22 7/26/2004
		1632 🍞	Rogue AP		AP	00:0b:86:81:07:f8	533	14:01:07 7/26/2004
		1900 🥐	Rogue AP		AP	00:0b:86:80:9e:c8	39	13:59:35 7/26/2004
		1933 🍞	Rogue AP		AP	00:0b:86:80:6b:58	3	13:56:32 7/26/2004
		908 🕐	Rogue AP		AP	00:0b:86:80:12:b0	1578	13:56:32 7/26/2004
		70 🥐	Rogue AP		AP	00:0b:86:80:0b:d0	3750	13:54:46 7/26/2004
				1 2 3	4 Next	1-10 of 35 10 💌		
					Delete Sel	lected Events		

FIGURE 25-15 Events

Events consists of	
Event ID	A system generated identifier for this event.
Туре	The type of event.
Info	An optional field with additional event details.



Device	The type of device involved in the event.
MAC Address	The MAC address of the device.
Count	The number of packets involved in the event.
Occurred Time	The timestamp when the event occurred.

You can sort the events on any of these categories by using the **Group By** drop-down menu. Click **Search** to find a specific event, or use the page navigation links to display additional pages of events. To manage the number of events reported, you can delete events that are no longer of interest. To delete unwanted events, click the selection box to the left of each event to be removed, and click **Delete Selected Events**.

# **Creating Custom Reports**

Additionally, the **Events** tab allows you to create custom reports by going to **Events > Create Custom Reports**.

vent Id								
a second s		MAC						
hoose Category Clea	•	💉 Choose	9					
AP Impersonation	🗖 AP Loa	ad Balancing		🗆 Bandwidth Rate Exce	eded			
Frame Fragmentation Rate Excee	eded 「 Frame	Low Speed Rate Exce	eded	Frame Non-Unicast R	ate Exceeded			
Frame Receive Error Rate Excee	ded 🛛 🗖 Frame	Retry Rate Exceeded		IBSS Violation				
IDS: Ad-hoc Network Bridge Dete	cted 🗖 IDS: A	d-hoc Network Detecte	ed	TIDS: Channel Rate A	nomaly			
IDS: Disconnect Station Attack	TDS: E	AP Handshake Rate Ar	iomaly	TIDS: Fake AP Flood D	etected			
IDS: Invalid MAC OUI	TDS: N	ode Rate Anomaly		TIDS: Sequence Numb	er Anomaly			
IDS: Signature Match	TDS: W	/ireless Bridge Detecte	а	Interference Detected				
Misconfigured Channel Violation	Miscon	figured DCF-Only Viola	Misconfigured DCF-PCF Violation					
Misconfigured OUI Violation	Miscon	figured PCF-Only Viola	Misconfigured Privacy Violation					
Misconfigured SSID Violation	Miscon	figured Short Preamble	Misconfigured WPA V	iolation				
Reserved Channel Violation	Reserv	ved SSID Violation	Rogue AP					
Station Failed	🗖 ValidS1	rA Violation	WEP Repeat Key IV					
🗆 WEP Weak Key IV								
Number of results per page:	10 🗸 Se	arch Reset S	ave As	Export Del	ete			
Number of results per page.								
earch Results				<u>Search</u>				
roup By None 🛛 💌								
Event ID • Type •	Info Device	MAC Address *	Count	Occurred Time				
🖵 5 🕐 Rogue AP	AP	00:0b:86:c0:01:21	1	17:27:07 1/13/2005				
🗖 4 🕐 🛛 Rogue AP	AP	00:0b:86:c0:17:a1	1	17:27:07 1/13/2005				
🗂 3 🕐 🛛 Rogue AP	AP	00:0b:86:c0:01:20	17	14:39:53 1/13/2005				
🗖 2 🕐 🛛 Rogue AP	AP	00:0b:86:c0:17:a0	25	14:39:53 1/13/2005				
🕅 1 🕐 🛛 Rogue AP	AP	00:0b:86:9d:62:b0	1	18:05:32 1/12/2005				

FIGURE 25-16 Custom Reports

The **Custom Reports** option allows you to tailor event reports to suit your needs. For example, you can create a report that just shows Rogue APs, or track times when bandwidth rates were exceeded.

To create a custom report, click **Search** and enter the criteria and click **Save As** to name the report.



# Wireless LAN Monitoring

Displays network information for each Wireless LAN based on the SSID of each Wireless LAN.

# Debug Information

You can set debugging levels on an Alcatel Wireless LAN switch to capture information on local clients. To enable this feature, select **Monitoring > Debug > Local Clients**. Wireless users will have their MAC Address, IP Address, and User Name recorded

To view the resulting debug activity, select **Monitoring > Debug > Process Logs**. Log details are shown in Figure 25-17.

Debug > Process Logs
Logs
Time Log
Jan 13 17:32:15 am: process_eif_packet MAC = 00:0b:86:c4:01:0c, IP = 10.4.21.42
Jan 13 17:32:16 am: New AP B 00:0b:86:80:11:43 C 1 P 1 W 0 DCF 1 PCF 0 PD 0 SP 1 BI 100
Jan 13 17:32:16 am: New AP Detected Channel = 1 SSID = newap3 BSSID = 00:0b:86:80:11:43
Jan 13 17:32:16 am: in msgr_papi_receive_callback
Jan 13 17:32:16 am: AM 00:0b:86:a0:48:a0-1.1.7: AP with BSSID 00:0b:86:80:11:43 SSID newap3 for detect_jap
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):Inside snmpReceiveCallBack, Processing Messages
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):Processing Trap 48 newTrap flag 0, isApTrap Flag 0
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):Mapped Trap Number is 48
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):valLen is 6
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):valLen is 5
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):valLen is 4
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):valLen is 74
Jan 13 17:32:16 snmp[294]: 10.4.21.102(1.1.7):Inside Initializing Traps
Jan 13 17:32:16 am: rap_message: RAP Type set to 1 for AP 00:0b:86:80:11:43
Jan 13 17:32:16 am: Untagged Frame Received 806 806
Jan 13 17:32:16 am: Parsed ARP Frame
Jan 13 17:32:16 am: Untagged Frame Received 806 806
Jan 13 17:32:16 am: process_eif_packet MAC = 00:0b:86:c4:01:0c, IP = 10.4.21.42
Jan 13 17:32:16 am: Parsed ARP Frame
Jan 13 17:32:16 am: process_eif_packet MAC = 00:0b:86:c4:01:0c, IP = 10.4.21.42
Jan 13 17:32:17 am: Untagged Frame Received 806 806
Jan 13 17:32:17 am: Parsed ARP Frame
Jan 13 17:32:17 am: Untagged Frame Received 806 806
Jan 13 17:32:17 am: process_eif_packet MAC = 00:0b:86:c4:01:0c, IP = 10.4.21.42
Jan 13 17:32:17 am: Parsed ARP Frame
Jan 13 17:32:17 am: process_elf_packet MAC = 00:0b:86:c4:01:0c, IP = 10.4.21.42
Jan 13 17:32:18 am: New AP B 00:0b:86:80:11:64 C 1 P 1 W 0 DCF 1 PCF 0 PD 0 SP 1 BI 100
Jan 13 17:32:18 am: New AP Detected Channel = 1 SSID = newap4 BSSID = 00:0b:86:80:11:64
Jan 13 17:32:18 am: in msgr_papi_receive_callback
Jan 13 17:32:18 am: AM 00:0b:86:a0:48:a0-1.1.7: AP with BSSID 00:0b:86:80:11:64 SSID newap4 for detect_jap
Jan 13 17:32:18 snmp[294]: 10.4.21.102(1.1.7):Inside snmpReceiveCallBack, Processing Messages
Jan 13 17:32:18 snmp[294]: 10.4.21.102(1.1.7):Processing Trap 48 newTrap flag 0, isApTrap Flag 0

FIGURE 25-17 Debugging Logs

Using the information collected by the logging process, you can tailor custom logs that suit your needs.

# Reports

The reporting capability of AOS-W is located in the **Reports** tab. The most commonly used types of reports are prepackaged and include:

- Active rogue Access Points (Active Rogue APs)
- All rogue Access Points (All Rogue APs)
- All active and valid Access Points (Active Valid APs)
- All inactive and valid Access Points (**Inactive Valid APs**)
- All valid Access Points active and inactive (All Valid APs)
- All Access Points that are interfering with other Access Points (Active Interfering APs)
- All Access Points that are causing interference (All Interfering APs)
- All active interfering Access Points (Active Known Interfering APs)
- All known interfering Access Points (All Known Interfering APs)
- The most congested Access Points (**Top Congested APs**)
- Active interfering wireless clients (Active Interfering Clients)
- All interfering wireless clients active or not (All Interfering Clients)
- All valid and active wireless clients (Active Valid Clients)
- All valid wireless client active or not (All Valid Clients)
- The wireless clients using the most bandwidth (Top Talker Clients)

A typical report screen looks like:



AP Reports Active Rogue APs	Rep	orts > Ac	tive Rogu	e APs						
All Rogue APs	Searc	h Result								Search
Active Valid APs	Group	Ru None	~							
Inactive Valid APs	Group	by None								
All Valid APs		AP Type 🔺	Manufacturer	Radio 🕈	Channel 🕈	SSID *	BSSID *	Clients	Last Seen	Status 🕈
Active Interfering APs		ROGUE	a Networks	802.11a	56	ethersphere	00:0b:86:80:9e:c8	0	14:09:31 7/26/2004	up
All Interfering APs		ROGUE	a Networks	802.11a	161	aruba-alpha-ap-wpa	00:0b:86:80:33:c8	0	14:09:16 7/26/2004	up
Active Known Interfering APs	П	ROGUE	a Networks	802.11a	157	aruba-alpha-ap	00:0b:86:80:62:f8	1	14:07:59 7/26/2004	up
All Known Interfering APs		ROGUE	a Networks	802.11a	161	aruba-aloba-an	00:05:86:80:60:78	0	14:07:44 7/26/2004	un
Top Congested APs	-		a Nocison d	002.110			00.00.00.00.00.70	-	11.07.117/20/2001	op
Client Reports		ROOUE	a Networks	802.11a	149	aruba-alpha-ap	00:0b:86:80:6b:58	0	14:04:56 7/26/2004	up
Active Interfering Clients		ROOUE	a Networks	802.11a	153	aruba-alpha-ap	00:0b:86:80:61:18	0	14:04:26 7/26/2004	up
All Interfering Clients		ROOUE	a Networks	802.11g	1	aruba-alpha-ap-wpa	00:0b:86:80:60:71	0	14:03:40 7/26/2004	up
Active Valid Clients		ROOUE	a Networks	802.11a	1	alpha-psk-tkip	00:0b:86:80:60:72	0	14:01:22 7/26/2004	up
All Valid Clients	-		- Mahuradar	000.11-	-		00.01.02.01.07.50	-	14-01-07 7/06/0004	
Top Talker Clients	1.1	MODDE	a Networks	602.11a	44	ethersphere	00:00:06:01:07:F0	1	14:01:07 7)26)2004	up
Custom Reports		ROOUE	a Networks	802.11b	1	demoswitch	00:0b:86:80:0b:d0	0	13:54:46 7/26/2004	up
Create AP Report					1 <u>2 3 4 N</u>	lext   1-10 of 34 10	~			
Create Client Report	Cta	tur Sata	c Valid S	at ac Interfe	ring	Set as Known In	terfering	Set ac D	Dicable	Clear
<no custom="" report=""></no>	Sta	581.8	s valia Si	st as interne	anng	Sec as Known In	contorning	Souds P	Disable	Clear

FIGURE 25-18 Sample Report

You can change the status of a rogue or interfering device by clicking **Set as Valid**, **Set as Interfering**, **Set as Known Interfering**, etc. If necessary, you can also turn off any device by clicking **Disable**.

## **Example Report: Rogue APs**

To analyze active rogue AP activity, go to **Reports > Active Rogue APs** to display the screen shown above. You can examine the list and determine if you want to mark any APs as interfering as opposed to rogue. You can also change the status of any AP displayed from rogue to interfering or to valid. You can also shut down any AP by clicking **Disable**.

# **AP Reports**

To see a typical AP report, select **Reports > AP > Active Valid APs**. The following type of report displays.

AP Reports Active Rogue APs	Reports > Active Valid APs													
All Rogue APs	Search Result									Search				
Active Valid APs	Course Due Mana													
Inactive Valid APs	Group by None	•												
All Valid APs	AP Type	Location *	Manufacturer	IP Address 🕈	Radio 🕈	Channel 🕈	SSID *	BSSID ^	Clients	Status 🕈				
Active Interfering APs	VALID	1.73.38	a Networks	192.168.64.176	802.11g	1	aruba-ap	00:0b:86:a0:54:40	0	up				
All Interfering APs	VALID	1.73.222	a Networks	192.168.64.164	802.11g	1	aruba-ap	00:0b:86:a0:69:e0	0	up				
Active Known Interfering APs	VALID	1.73.311	a Networks	192.168.64.175	802.11g	1	aruba-ap	00:0b:86:a0:50:80	0	up				
All Known Interfering APs	VALID	1.73.39	a Networks	192.168.64.177	802.11g	1	aruba-ap	00:0b:86:a0:4f:e0	0	up				
Top Congested APs	VALID	1.73.35	a Networks	192.168.64.172	- 802.11a	1	aruba-ap	00:0b:86:a0:6b:70	0	un				
Active Interfering Clients		1 79 999	n Notworks	102 169 64 159	902.11a	-		00.05.96.50.60.40	-					
All Interfering Clients		1.73.223	anecworks	192,100.04,150	002.11g	1	aruba-ap		0	up				
Active Valid Clients	VALID	1.73.34	a Networks	192.168.64.155	802.11g	1	aruba-ap	00:0b:86:a0:6c:a0	0	up				
All Valid Clients	VALID	1.73.31	a Networks	192.168.64.167	802.11g	1	aruba-ap	00:0b:86:a0:71:60	0	up				
Top Talker Clients	VALID	1.73.312	a Networks	192.168.64.173	802.11g	1	aruba-ap	00:0b:86:a0:45:90	0	up				
Custom Reports	VALID	1.73.316	a Networks	192.168.64.101	802.11g	1	aruba-ap	00:0b:86:a0:50:90	0	up				
Create AP Report				1.2 Next	1-10 of 18	10 🗸								
Create Client Report	_						_							
<no custom="" report=""></no>	Status :	Set as Valid	Set as Interf	ering S	Set as Know	n Interfering	S	et as Rogue	Disable	Clear				

FIGURE 25-19 Report on all Active Valid APs

### Status

To get details on a specific device on a report, click the checkbox to the left of the device and click **Status**. Detailed information for this device displays as shown in Figure 25-20.



No listening AM's four	nd.							
RSSI Name	Location	IP Address	АР Туре	Туре	Radio			
Listening Air Mo	nitors / A	4Ps			11			
Set as valid	Seta	is internering		et as k	nown Interfering		Set as Rogue	Disable
Last Seen	C - 1 -	14:12:19 1/13/	12005			1		Disable
Status	Status up			Clients			0	
Туре	VALID		4	AP Type		Aruba AP		
Radio	802.11g		C	hannel		1		
SSID	SID 101_qa_Gui_Vap-1			E	SSID		00:0b:86:a0:59:e	i
Location	tation 127.255.65535		I	P Address		10.4.21.23		
Manufacturer		a Networks		P	lame			

FIGURE 25-20 Selected AP Status

Using the Command Line Interface

You may use the CLI to detect and disable rogue APs. However, it is significantly more complex and difficult than using the Web-based Management Interface.

Enable or disable rogue detection using the ap-policy protect-unsecure-ap [enable | disable] command. See "Air Management Commands" on page 804.

## **Custom Reports**

You can customize reports to suit your needs. Go to **Reports > Create AP Report** to create a custom Access Point report. Go to **Reports > Create Client Report** to create a custom wireless client report as shown below.

Monitoring Configuration	Maintenance Plar	Events Reports						Logout
AP Reports Active Rogue APs	Reports > Cr	eate Client Rep	ort					
All Rogue APs	Search		Hi	de Search				
Active Valid APs	Location	MAC Ad	dress					
Inactive Valid APs	SSID	BSSID						
All Valid APs	Liser	IP Addre	***					
Active Interfering APs	Badia Anu	Channel	Anu ar					
All Interneting Ars	Raulo Ally		Any					
All Known Interfering APs	Client Type Any	Status	Any 💌	_				
Top Congested APs	Number of results per	page: 10 💌 Searc	h Reset Save	As				
Client Reports Active Interfering Clients	Search Result							Hide Search
All Interfering Clients	Group By None	<b>~</b>						
Active Valid Clients	Client Type *	Manufacturer	MAC Address	SSID ^	BSSID  Channel	Radio *	Last Seen	Status *
All Valid Clients	INTERFERING	SPECTRALINK CORP.	00:90:7a:01:13:1d	wifiphone	00:06:86:80:99:63 1	802.11a	14:33:16 7/26/2004	t up
Top Talker Clients		Actiontec Electronics Inc	00:20:e0:8e:08:3d	asfa-alpha-	an 00:0b:86:80:60:70.1	802.11a	14-32-32 7/26/2004	t down
Create AP Report		Cieco Sustane	00:0b:fd:52:de:d7	asfa-alpha-	ap 00:0b:86:80:60:70 1	802.110	14:31:18 7/26/2004	tun
Create Client Report		Cisco Systems	00:05:10:02:06:07	-thousehouse	00.05.00.001.00.001	002.119	14:05:10 7/20/200	- op
<no custom="" report=""></no>		Philips Components	00:05:46:43:ac:01	ethersphere	00:00:86:81:07:78 40	002.11a	14:25:19 7/26/200-	down
	INTERFERING	Philips Components	00:05:4e:45:f3:44	ethersphere	00:0b:86:80:9e:c8 56	802.11a	14:23:06 7/26/2004	/ down
	INTERFERING	The Linksys Group, Inc.	00:0c:41:15:15:cf	ethersphere	00:0b:86:81:07:f8 40	802.11a	14:23:01 7/26/2004	r up
	INTERFERING	Cisco Systems	00:0b:be:2c:e5:68	parag-ap	00:0b:86:80:7a:e0 1	802.11g	14:20:14 7/26/2004	ł down
	INTERFERING	Cisco Systems	00:0d:bd:8f:49:dc	aruba-alpha-	ap 00:0b:86:80:60:70 1	802.11g	14:18:40 7/26/2004	ł down
	INTERFERING	Netgear, Inc.	00:09:5b:96:ba:73	BM	00:0b:86:a0:01:b0 52	802.11a	14:18:25 7/26/2004	l up
	INTERFERING	SMC Networks, Inc.	00:04:e2:64:c9:31	ethersphere	00:0b:86:80:9f:68 60	802.11a	14:14:37 7/26/2004	l up
			1 2	Next   1-10	of 13 10 💌			
		Statu	s Set as Valid	Set as	Interfering Disable Cle	ar		



**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 26 Firewall Logging

This chapter discusses firewall logging and explains the events found in those logs. Firewall logging in the AOS-W software (version 2.4 or higher) is International Computer Security Association (ICSA) compliant.

# Log Entries (alphabetical)

access-list <name> {created | edited | deleted }, type = {standard | extended | eth | mac | session }

The possible dispositions are:

- Created
- Edited
- Deleted

## Authentication failed for User <username>: connection type SERIAL

This entry is issued when a user connected through the serial port fails to authenticate.

# Authentication failed for User <username> : src ip <IPaddr>src port <portnum> dst ip <IPaddr>dst port <portnum> connection type TELNET

This entry is issued when a user connected through TELNET fails to authenticate. Information about the source and destination IP addresses and ports is provided.

# Authentication succeeded for User <username> : connection type SERIAL

This entry is issued when a user connected through the serial port successfully authenticates.

# Authentication succeeded for User <username> : src ip <IPaddr> src port <portnum>dst ip<IPaddr> dst port <portnum> connection type TELNET

This entry is issued when a user connected through TELNET successfully authenticates. Information about the source and destination IP addresses and ports is provided.

```
ICMP srcip=<ipaddr>, dstip=<ipaddr>, type=<number1>,
code=<number2>,sequence=<number3>, id=<number4>,
action=<action>, policy=<policy>
```

where:

srcip	indicates the source IP address of the packet.		
dstip	indicates the destination IP address of the packet.		
type	indicates the ICMP type number.		
code	indicates the ICMP code number.		
sequence	indicates the sequence number.		
id	indicates the ID number if the packet is an ICMP echo request or response		
	packet.		
action	indicates the disposition of the packet, which will be one of the followin		
	deny:	The packet was dropped.	
	permit:	The packet was forwarded.	

	<pre>src-nat:</pre>	The packet was forwarded with the source IP address
		modified.
	dst-nat:	The packet was forwarded with the destination IP address
		modified.
	redirect:	The packet was forwarded without modifying the address
		fields, but through an interface other than that indicated in
		the IP routing table.
policy	indicates which firewall policy was matched in order to generate the log message .	

network destination <name> { created | edited | deleted }

The possible dispositions are:

- Created
- Edited
- Deleted

network service <name> { created | edited | deleted }

The possible dispositions are:

- Created
- Edited
- Deleted

nat pool<name> { created | edited | deleted }

The possible dispositions are:

- Created
- Edited
- Deleted



# {TCP | UDP} srcip=<ipaddr>, srcport=<srcport>, dstip=<ipaddr>, dstport=<dstport>, action=<action>, policy=<policy>

where:					
srcip	indicates the source IP address of the packet.				
srcport	indicates the source TCP or UDP port number of the packet.				
dstip	indicates the destination IP address of the packet.				
dstport	indicates the destination TCP or UDP port number of the packet.				
action	indicates the disposition of the packet, which will be one of the following:				
	deny: The packet was dropped.				
	permit: The packet was forwarded.				
	<pre>src-nat: The packet was forwarded with the source IP address modified.</pre>				
	dst-nat: The packet was forwarded with the destination IP address				
	modified.				
	redirect: The packet was forwarded without modifying the address fields,				
	but through an interface other than that indicated in the IP routing table.				
policy	indicates which firewall policy was matched in order to generate the log				
	message.				

# CHAPTER 27 Troubleshooting AOS-W Environments

## **Basic Connectivity**

The troubleshooting information in this chapter covers problems with basic wireless connectivity, such as inability to associate or inability to communicate after association.

Figure 27-1 describes the steps you should take to install and configure your Alcatel wireless network. If you follow these steps in the order they appear, then troubleshooting becomes a more straightforward process of finding where the process flow is broken.



FIGURE 27-1 Normal Process Flow

# General

The Wi-Fi Alliance has made great strides in testing interoperability between 802.11 devices from many different manufacturers. Despite these efforts, however, client incompatibility remains the primary complaint from network managers deploying wireless LANs. A wide range of wireless hardware and software is in use, with a corresponding wide range of quality – a given client adapter card may work fine with one revision of driver software, but experience numerous problems with another. A given operating system may perform poorly on a wireless network until specific vendor patches are applied. For this reason, Alcatel recommends that enterprise network managers develop standard supported configurations for their deployment. This configuration should consist of:

- Device type and model (laptops, PDAs, handheld devices, voice handsets, etc.)
- Operating system (Windows 2000, Windows XP, MacOS X, Linux, etc.)
- Wireless NIC hardware manufacturer and model
- Wireless NIC software driver
- Wireless NIC firmware revision, if required
- Wireless NIC client utility or radio manager, if needed
- Authentication and encryption software (VPN client, 802.1x supplicant, etc.)

Spending the time up front to develop and test such configurations will greatly reduce troubleshooting time and effort after the network is deployed and operational. A table of configurations tested by Alcatel appears in the Design Guide, but this testing cannot take into account all possibilities. Network managers can use these recommendations but should always perform testing in their own environments with their own applications.

# Client cannot find AP

Before a wireless client can associate to a network, it must locate at least one Access Point. Most wireless clients locate available network by broadcasting a series of 802.11 *probe-request* frames on multiple channels. APs hearing these probe-request frames should answer with *probe-response* frames containing the AP's ESSID and various other capability parameters. Two types of probe-request frames are possible:

**Broadcast Probe Request** – In a broadcast probe request, a client looks for any available ESSID. It does so by leaving the ESSID field empty in the probe-request frame. Normally, all AP's receiving the probe-request, regardless of ESSID, will answer. This is how Windows XP, for example, populates the list of available wireless networks.



**Specific Probe Request –** In this type of probe-request, the client is only interested in one particular ESSID. It will include this ESSID in the request, and only APs supporting this ESSID will respond.

It is possible in an Alcatel deployment to disable responses to broadcast probe-requests, and require a specific probe-request with the correct ESSID before an AP will answer. If a client does not find an AP to associate with, there are a number of possible causes.

A packet capture of a normal probe-request/probe-response sequence is shown in the figure below. Detailed packet capture data can be found in Appendix A.

Source	Destination	Protocol	BSSID
SMC Net:64:BE:08	Ethernet Broadcast	802.11 Probe Req	FF:FF:FF:FF:FF:FF
SMC Net:64:BE:08	Ethernet Broadcast	802.11 Probe Req	FF:FF:FF:FF:FF:FF
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Ala Net: 9D:65:E0	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:9D:65:E0
Cisco:4F:75:90	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Ala Net: 80:A6:00	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:80:A6:00
Ala Net: 9D:65:E0	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:9D:65:E0
Netgear:85:DF:38	SMC Net:64:BE:08	802.11 Probe Rsp	00:09:5B:85:DF:38
Linksys Group:0F:6	SMC Net:64:BE:08	802.11 Probe Rsp	00:06:25:0F:6E:1F
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
The Linksys Group:	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:41:8F:9E:D8

#### FIGURE 27-2 Network Discovery

#### Client's list of available networks is empty

Consider the following possible fixes:

- Ensure that the user is physically located in an area with AP coverage. Sometimes wireless LANs are deployed only in certain parts of a building. The user may not be aware of this fact, and may be reporting a problem when there is none.
- Make sure the client's wireless adapter is enabled. Some newer laptops with built-in wireless hardware have a physical switch that enables and disables the radio. NIC client utilities often contain similar software switches. Finally, the adapter may be disabled by the operating system.
- If responses to broadcast probe-requests have been disabled in the Alcatel network, ensure that the client has been configured with the proper ESSID.
   If the ESSID is incorrect, the client will not be able to locate any APs.
- Ensure that the wireless network is operational and that no APs or switches have failed. If part of the network has failed, it is likely that multiple users will report problems. Note that in a standard dense-mode Alcatel deployment, multiple APs will normally be able to provide service to one user, so the failure of one AP is unlikely to cause this symptom.
- Enable client debugging for the client device in question. From the Alcatel CLI, use the command "aaa user debug mac <MAC address of client>".
   Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). Verify that the switch is receiving probe requests from the client.
- Perform a wireless packet capture through the Alcatel system for the appropriate area where the user is located. Filter the capture for the user's MAC address. A packet capture is a sure way to find out if the client is transmitting probe-requests, if the probe-requests contain the correct ESSID, and if an AP is answering probe-requests.
- Reset the client NIC or operating system. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.
- Replace the client NIC. If a packet capture appears normal and client mis-configuration has been ruled out, it is possible that the client NIC has failed.

# Client's list of available networks contains some entries, but not the correct ESSID

Consider the following possible fixes:

- If responses to broadcast probe-requests have been disabled in the Alcatel network, ensure that the client has been configured with the proper ESSID.
   If the ESSID is incorrect, the client will not be able to locate any APs.
- Ensure that the wireless network is operational and that no APs or switches have failed. If part of the network has failed, it is likely that multiple users will report problems. Note that in a standard dense-mode Alcatel deployment, multiple APs will normally be able to provide service to one user, so the failure of one AP is unlikely to cause this symptom.
- Perform a wireless packet capture through the Alcatel system for the appropriate area where the user is located. Filter the capture for the user's MAC address. A packet capture is a sure way to find out if the client is transmitting probe-requests, if the probe-requests contain the correct ESSID, and if an AP is answering probe-requests.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.



## Client finds AP, but cannot associate

After a client has located one or more APs supporting the desired ESSID, it must associate to that AP. Association is a four-step process consisting first of 802.11 authentication (not to be confused with 802.1x or VPN authentication) followed by association. Four frames are exchanged on the wireless network during association, as shown in the figure below.



FIGURE 27-3 Association Process

The figure below shows a packet capture of a normal authenticate/associate sequence. Detailed packet capture data can be found in Appendix A.

Source	Destination	Protocol	BSSID
SMC Net:64:BE:08		802.11 Auth	00:0B:86:80:18:00
Ala Net: 80:18:00	SMC Net:64:BE:08	802.11 Ack	
Ala Net: 80:18:00	SMC Net:64:BE:08	802.11 Auth	00:0B:86:80:18:00
SMC Net:64:BE:08	Ala Net: 80:18:00	802.11 Assoc Req	00:0B:86:80:18:00
Ala Net: 80:18:00	SMC Net:64:BE:08	802.11 Ack	
Ala Net: 80:18:00	SMC Net:64:BE:08	802.11 Assoc Rsp	00:0B:86:80:18:00

#### FIGURE 27-4 Association Process Packet Capture

If the client and AP are configured differently, association will typically fail. Very little information is given to the user when an association fails, so most troubleshooting must be done from the network side. The most likely cause for an authentication or association failure is client misconfiguration.

# 802.11 Authentication Fails

The 802.11 *authenticate* exchange is a primitive form of authentication specified by the original 802.11 standard, and is not related to secure authentication such as 802.1x or VPN. This authentication exchange must still take place before an association exchange, but no useful information is exchanged.

- Enable client debugging for the client device in question. From the Alcatel CLI, use the command "aaa user debug mac <MAC address of client>".
   Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). The log file should indicate the reason for a failed authentication or association. Often the cause is a capability mismatch between the client and AP.
- If the authenticate process fails, it is likely because the client has been configured for *shared-key authentication*. Shared-key authentication opens a security vulnerability and should never be used the Alcatel system does not support shared-key authentication. The client should be configured for either "open system" or "WPA" authentication, but never shared-key.
- Ensure that the user is physically located in an area with AP coverage. If signal strength is too low, radio transmission may be garbled to the point that authentication or association is impossible. The Station Manager log will indicate with which AP the client is attempting to associate ensure that this AP is near the user's physical location.
- Perform a wireless packet capture. If the Station Manager log provides no useful information or is inaccessible, a packet capture will always show the reason for a failed association.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.
- **NOTE**—It is not possible to set authentication to 'fall-through' to another method or server if the first authentication fails. If a user fails authentication to a server, it just "fails". For networks with more than one authentication server for each authentication method, a secondary server will kick-in only if the primary server fails (the whole server, not an authentication fail).

#### **Association Fails**

During the association request/response exchange, a number of capabilities are exchanged. If there is a mismatch between the client and network configuration, the association will often be rejected by the AP. On the client, there is often no indication that an association has failed other than a lack of association. For example, under Windows XP using the built-in "Zero Configuration" service, Windows will continually display "One or more wireless networks are available..."



- Enable client debugging for the client device in question. From the Alcatel CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). The log should indicate the reason for a failed authentication or association. Often the cause is a capability mismatch between the client and AP.
- Verify that the AP has not reached the maximum number of users. If the system has been configured to allow only 20 associations per AP, the 21<sup>st</sup> client will be rejected. A simple way to do this is using the "show ap-leds" command to view the status of AP LEDs on the switch. An AP that is full will indicate such via the AP LEDs.
- If the client fails association, the likely cause is a client misconfiguration. If the network has been configured for WPA and TKIP encryption, and the client has been configured for open system and WEP encryption, association will fail.
- Ensure that the user is physically located in an area with AP coverage. If signal strength is too low, radio transmission may be garbled to the point that authentication or association is impossible. The Station Manager log will indicate with which AP the client is attempting to associate ensure that this AP is near the user's physical location.
- In a dense-mode AP deployment, the AP's minimum rate may have been adjusted to a higher value. If the client cannot support this higher value because of signal impediments or configuration, association will fail.
- Perform a wireless packet capture. If the Station Manager log provides no useful information or is inaccessible, a packet capture will always show the reason for a failed association.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.
- If "Authentication Failure Auto-Blacklisting" has been enabled on the Alcatel switch, multiple authentication failures will cause a client to be denied association. If this feature has been enabled, check the current "Black List" in the management GUI by navigating to Monitoring→Client→Client Blacklist. Ensure that the authentication problem has been fixed before re-attempting association.
- Verify that no denial of service attack is underway. From the client perspective, a successful association followed by an immediate disassociation appears the same as an unsuccessful association. Examine the Wireless Management System (WMS) log files on the Alcatel switch by navigating in the management GUI to the Events tab. A packet capture will also reveal the presence of a denial of service attack.

# Client associates to AP, but higher-layer authentication fails

Problems with higher-layer authentication such as 802.1x are normally not related to basic connectivity, but can disguise themselves as such. If association to an AP is successful, basic connectivity problems are likely ruled out.

- Reset the client NIC. If association is successful a second or third time but authentication continues to fail, it is unlikely that a basic connectivity problem is causing the issue. See the "Authentication" section of this guide for more details on troubleshooting higher-layer authentication problems.
- Perform a wireless packet capture. If authentication problems are being caused by a busy network or a denial of service attack, a packet capture will make this clear.

# Client associates/authenticates, but has no network connectivity

In this scenario, a client has successfully associated to an AP and, if configured, has successfully gone through higher-layer authentication. However, the client has no access to network services.

- Static WEP Key mismatch: If the client and AP are configured for static WEP, it is likely that the WEP keys do not match. This symptom commonly manifests itself when a client configured for DHCP fails to obtain an IP address. Check the client's WEP key and ensure that it matches the WEP key configured in the Alcatel system.
- Dynamic WEP Key Exchange Failure: If the network uses 802.1x with automatically-assigned WEP keys (dynamic WEP), it is possible that the key exchange process failed. Because this key exchange is non-standard and does not involve a verified "handshake", the process sometimes fails without an error message being generated. Resetting the client NIC or rebooting the client operating system often restores connectivity in this situation.
- WPA/802.11i Key Exchange Failure: In a WPA or 802.11i network, the dynamic key exchange process may fail. This is an error condition and indicates either a man-in-the-middle attack or a faulty NIC driver. Examine the "Authentication" log file in the Alcatel switch for details because the WPA/802.11i key exchange is a standard and utilizes a four-way verified handshake, error messages will be generated when part of the process fails. To view the Authentication log file in the Alcatel management GUI, navigate to Monitoring→Process Logs and filter on "Authentication." From the CLI, enter the command "show log authmgr".



- Once association and higher-layer authentication have succeeded, it is analogous to the link light turning on in a wired Ethernet network. Troubleshoot the problem using traditional tools such as "ping" and "traceroute". Problems such as this often indicate faults in the wired network or in client network settings. For example, the client may be configured for a static IP address, the default gateway for the network may be down, or there may be a routing problem.
- If the client is configured for DHCP and does not obtain an IP address, it may indicate a problem with the DHCP server or the uplink network from the Alcatel switch. Enable client debugging for the client device in question. From the Alcatel CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). DHCP activity appears in the log file.
- If multiple users on the same AP are experiencing problems, examine statistics on the AP. It is possible that the network is extremely busy, is experiencing interference, or is experiencing a denial of service attack. Perform a wireless packet capture when in doubt.

# Client initially has network connectivity, then loses connectivity

In this scenario, a client successfully associates to an AP, authenticates, and has network connectivity. At some future time, communication fails.

- Ensure that a higher-layer network failure has not taken place. Use tools such as "ping" and "traceroute" to verify. If an attempt to ping the Alcatel switch from the client fails, the problem can be isolated to the wireless network.
- If the failure took place while the user was moving, it is possible that roaming failed. Examine the client's current signal strength and data rate. If they are low, compare the user's physical location with the location of the currently associated AP. This is sometimes caused by an issue known as "client stickiness" the tendency for a client to maintain an existing association and ignore closer APs even when signal strength has significantly degraded. Ideally, pre-deployment testing will identify client NICs and drivers that exhibit this problem so that they can be excluded from the deployment.
- Dynamic WEP Key Exchange Failure: If the network uses 802.1x with automatically-assigned WEP keys (dynamic WEP), it is possible that the key exchange process failed. Because this key exchange is non-standard and does not involve a verified "handshake", the process sometimes fails without an error message being generated. Resetting the client NIC or rebooting the client operating system often restores connectivity in this situation.

- WPA/802.11i Key Exchange Failure: In a WPA or 802.11i network, the dynamic key exchange process may fail. This is an error condition and indicates either a man-in-the-middle attack or a faulty NIC driver. Examine the "Authentication" log file in the Alcatel switch for details because the WPA/802.11i key exchange is a standard and utilizes a four-way verified handshake, error messages will be generated when part of the process fails. To view the Authentication log file in the Alcatel management GUI, navigate to Monitoring→Process Logs and filter on "Authentication." From the CLI, enter the command "show log authmgr".
- If multiple users on the same AP are experiencing problems, examine statistics on the AP. It is possible that the network is extremely busy, is experiencing interference, or is experiencing a denial of service attack. Perform a wireless packet capture when in doubt.

# Client has network connectivity, then loses wireless association

In this scenario, a client successfully associates to an AP, authenticates, and has network connectivity. At some future time, the association is dropped.

- If the failure took place while the user was moving, it is possible that the user roamed to an area with no radio coverage and cannot re-associate.
- If the problem repeats often, debug may be enabled for the client experiencing the problem. If the Alcatel switch is dropping the association, this will be indicated in the log file. To enable client debug in the Alcatel CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file).
- In a network configured to ignore broadcast probe requests, Windows devices may spend an excessive amount of time transmitting broadcast probe requests before finally transmitting probe requests for a specific ESSID. Under these circumstances, roaming performance between APs may be extremely slow, and may cause the wireless association to be dropped for a long period of time. If this is the cause of the problem, the association will eventually be restored. A wireless packet capture will verify this situation. To resolve, make sure the latest Windows OS patches have been applied. Also consider enabling responses to broadcast probe requests this feature should be used only as a convenience factor to hide special-purpose ESSIDs from clients and should not be considered a security feature.
- The cause for the dropped association may have been a denial of service attack – specifically a "deauth" or "disconnect station" attack. View the Alcatel Wireless Management System log file by navigating in the management GUI to the Events tab to see if this is the case. A wireless packet capture will also verify this situation.



 Reset the client NIC. If an internal error has caused the dropped association, a reset of the NIC may restore connectivity.

#### **Client experiences poor performance**

This scenario covers many different situations. In general, the complaint will be slow performance – download speeds may be low, application timeouts may occur, or general sluggishness may be reported.

- If the performance problems began while the user was moving, it is possible that roaming failed. Examine the client's current signal strength and data rate. If they are low, compare the user's physical location with the location of the currently associated AP. This is sometimes caused by an issue known as "client stickiness" the tendency for a client to maintain an existing association and ignore closer APs even when signal strength has significantly degraded. Ideally, pre-deployment testing will identify client NICs and drivers that exhibit this problem so that they can be excluded from the deployment.
- Examine client statistics from the Alcatel management GUI. Navigate to Monitoring > Clients > Enterprise Clients, select the affected client, and click on "Client Activity".
  - If RSSI also known as signal strength is low (below 20), the client has poor signal strength to the nearest AP. This may indicate a roaming failure, described above.
  - If "transmit retries" is high, the client is sending frames that are not being acknowledged by the AP. The client is then forced to re-transmit these frames, reducing performance. The cause may be interference or low signal strength.
  - If "receive retries" is high, the AP is sending frames that are not being acknowledged by the client. The AP is then forced to re-transmit these frames, reducing performance. The cause may be interference or low signal strength.
  - If the transmit or receive data rate is low, it indicates that the client or AP's rate adaptation algorithm has detected errors at higher data rates and is forcing a lower rate. This could indicate interference or low signal strength.
  - If signal strength is high, retry rate is high, and data rate is low, the cause may be localized interference. These symptoms indicate a client that is close to the AP with good signal strength, but with poor communication between the AP and client. Examine the Events tab in the GUI and look for any indications of detected interference.

- If the above parameters are within acceptable ranges, but throughput is still low, it may indicate a congested AP. Perform activity monitoring on the entire AP rather than on the individual client to examine how much bandwidth is being consumed on the AP. If there are too many clients connected to a given AP, performance may be increased by reducing the maximum number of clients allowed on the AP. (The theoretical maximum number of clients allowed per AP is 255. A real world maximum may well be closer to 10.)
- There may be congestion on the wired portion of the network. Examine the wired network using traditional tools such as "ping" and "traceroute" or using sniffer software.
- Perform a wireless packet capture to view any anomalous conditions in the area covered by the AP.

# **Troubleshooting Access/Grid Points**

The Alcatel Access Points support auto duplex and auto speed. When one side of the link is hard coded for 100/full and the Access or Grid Point is set to auto speed/duplex, the resulting connection will be half duplex. This configuration causes the Access/Grid Point to fail.

Refer to the following chart for information on duplex setting/speed combinations.



NIC Speed/Duplex Configuration	Switch Speed/Duplex Configuration	Resultant NIC Speed/Duplex Configuration	Resultant Switch Speed/Duplex Configuration	Observations
Auto	Auto	1000Mbps/F ull-duplex	1000Mbps/F ull-duplex	Proper configuration. If this configuration causes problem, verify that the NIC is operating as configured.
1000Mbps/Full-d uplex	Auto	1000Mbps/F ull-duplex	1000Mbps/F ull-duplex	Link is good but the switch will not see any autonegotiatio n information from the NIC. So the Wireless LAN switches (which only support full-duplex operation with 1000 Mbps), will default to full-duplex.
1000Mbps/Full-d uplex	1000Mbps/Full- duplex	1000Mbps/F ull-duplex	1000Mbps/F ull-duplex	Proper configuration. If this configuration causes problem, verify that the NIC is operating as configured.

# TABLE 27-1 Access Point Duplex/Speed Matrix

NIC Speed/Duplex Configuration	Switch Speed/Duplex Configuration	Resultant NIC Speed/Duplex Configuration	Resultant Switch Speed/Duplex Configuration	Observations
100Mbps/Full-du plex	1000Mbps/Full- duplex	No link	No link	Because the speeds do not match, no link is established.
100Mbps/Full-du plex	Auto	100Mbps/Fu II-duplex	100Mbps/H alf-duplex	There is a duplex mismatch (half and full) which may provide connectivity, but there will likely be performance problems and poor quality, intermittent connectivity.
Auto	100Mbps/Full-d uplex	100Mbps/H alf-duplex	100Mbps/Fu II-duplex	There is a duplex mismatch (half and full) which may provide connectivity, but there will likely be performance problems and poor quality, intermittent connectivity.

 TABLE 27-1
 Access Point Duplex/Speed Matrix



NIC Speed/Duplex Configuration	Switch Speed/Duplex Configuration	Resultant NIC Speed/Duplex Configuration	Resultant Switch Speed/Duplex Configuration	Observations
100Mbps/Full-du plex	100Mbps/Full-d uplex	100Mbps/Fu II-duplex	100Mbps/Fu II-duplex	Proper configuration. If this configuration causes problem, verify that the NIC is operating as configured.
100Mbps/Half-d uplex	Auto	100Mbps/H alf-duplex	100Mbps/H alf-duplex	The switch, which is configured for Auto, will default to half duplex for 10/100Mbps settings.
10Mbps/Half-du plex	Auto	10Mbps/Hal f-duplex	10Mbps/Hal f-duplex	The switch, which is configured for Auto, will default to half duplex for 10Mbps settings.

#### TABLE 27-1 Access Point Duplex/Speed Matrix

NIC Speed/Duplex Configuration	Switch Speed/Duplex Configuration	Resultant NIC Speed/Duplex Configuration	Resultant Switch Speed/Duplex Configuration	Observations
10Mbps/Half-du plex	100Mbps/Half- duplex	No Link	No Link	Because the speeds do not match, no link is established.
Auto	100Mbps/Half- duplex	100Mbps/H alf-duplex	100Mbps/H alf-duplex	The switch, which is configured for Auto, will default to half duplex for 100Mbps settings.
Auto	10Mbps/Half-d uplex	10Mbps/Hal f-duplex	10Mbps/Hal f-duplex	The switch, which is configured for Auto, will default to half duplex for 10Mbps settings.

#### TABLE 27-1 Access Point Duplex/Speed Matrix

# **Authentication**

Most enterprise wireless networks make use of some form of secure authentication. This typically means 802.1x or VPN, although other choices are possible. The troubleshooting process is different depending on which authentication scheme is in use.

# 802.1x

Authentication using 802.1x may be accomplished in combination with dynamic WEP key exchange, WPA with TKIP, or 802.11i with AES. The troubleshooting process for the authentication portion is identical in all cases.



#### Incorrect Username/password (TTLS or PEAP)

A typical cause of authentication failure is an incorrect username, password, or one-time token. In most cases, this is a simple problem to troubleshoot, because the client will generate an error message indicating the cause of the failure. However, depending on the 802.1x supplicant in use, this error may not be obvious.

- Check the RADIUS server. The first line of troubleshooting for authentication problems should always involve the authentication server. Because the actual authentication exchange in 802.1x happens between the client and the authentication server, the server is the most accurate entity for examining logging information. Server log messages will often indicate what triggered the failure.
- If the RADIUS server is inaccessible, check authentication log messages on the Alcatel switch. From the management GUI, navigate to Monitoring→Process Logs and filter on Authentication. From the CLI, issue the command "show log authmgr". As an 802.1x authenticator, the Alcatel switch can only see an 802.1x success or failure, but has no information about why a failure occurred. Checking this log will indicate that a failure was signaled by the authentication server, which can then lead to further troubleshooting.

#### Server certificate is not validated

802.1x operation in wireless networks (PEAP, EAP-TLS, and TTLS) relies on a valid certificate being transmitted from the authentication server to the client. The certificate must not be expired, must be valid for the server name, and must be trusted by the client (if the certificate is signed by a certificate authority, the certificate authority must be trusted by the client.)

Certificate errors may or may not be indicated by the client. For example, the Funk Odyssey client will turn an icon red and indicate an explicit error when a certificate problem occurs. The Microsoft supplicant built into Windows XP will not.

- If a certificate problem is suspected, most 802.1x supplicants provide an option to disable server certificate validation. As a troubleshooting mechanism, temporarily disable this option if available. If authentication is successful after this option is disabled, a certificate problem has been confirmed. Note: Do not leave the "validate server certificate" option turned off in the 802.1x supplicant. This opens a security vulnerability making a man-in-the-middle attack possible.
- Verify that the client configuration matches the standard enterprise client configuration. Most 802.1x problems are caused by a misconfigured client. For example, the wrong certificate authority or wrong server domain name may have been selected, or password authentication may be selected when one-time token use is required by the authentication server.

 Perform a wireless packet capture. If 802.1x authentication is observed to begin, and then abruptly stops, a certificate error may be the cause. The 802.1x supplicant should not proceed with authentication if it detects an invalid server certificate.

## Client Certificate is not accepted (EAP-TLS only)

When using EAP-TLS as an 802.1x authentication method, a client certificate must be validated by the RADIUS server in order for authentication to succeed. If the client certificate cannot be validated, authentication will fail.

- Examine the RADIUS server log files. In most cases, the RADIUS server will provide necessary clues to troubleshoot the problem.
- A common problem for client certificates is an incorrect Common Name (CN). If the CN is not recognized by the RADIUS server, the RADIUS server cannot locate the user in the database. Check the RADIUS server documentation for the correct format. For example, Microsoft IAS expects the certificate CN to be in the form "user@domain" in order to locate the user correctly in Active Directory.
- Verify that the client certificate has not expired by examining the certificate "Valid to" date.
- Verify that the client certificate has not been revoked. The certification authority Certificate Revocation List (CRL) contains all revoked certificates.

#### Client is using the wrong form of PEAP

PEAP (Protected Extensible Authentication Protocol) is a widely-deployed authentication method for 802.1x. There are two different forms of PEAP in use – Microsoft PEAP and Cisco PEAP. Both client and server must be using the same form of PEAP. If the RADIUS server is Microsoft IAS and the client is Microsoft Windows using the built-in Wireless Zero Configuration utility, for example, it is likely that both sides are using Microsoft PEAP. However, in a mixed environment, mismatches may occur.

- The client may not provide useful information on which type of PEAP is in use. However, a clue may be to examine the PEAP "inner" authentication protocol. Microsoft PEAP allows MS-CHAP v2 and a smart card/certificate as the inner authentication protocol. Cisco PEAP also supports one-time passwords or token cards as the inner authentication protocol. If a one-time password or secure token is available in the client's PEAP configuration, Cisco PEAP is most likely being used.
- Current versions of Cisco's ACS RADIUS server support both MS-PEAP and Cisco PEAP. However, older versions of ACS do not support MS-PEAP. Ensure that an updated version of ACS is being run if MS-PEAP is used by clients.



#### RADIUS Server reports "Authentication Method Not Supported"

This error message is caused by the client and server using different 802.1x authentication methods.

 Verify that the RADIUS server and client are configured for the same 802.1x authentication method. For example, if the RADIUS server is configured to use PEAP, the client must also be configured this way. Microsoft clients default to EAP-TLS (Smart card or other certificate).

Client stops communicating after roaming (WPA)

In a network running WPA/TKIP, the NIC card may fail to re-negotiate encryption keys after roaming to a new AP. This behavior will manifest itself as the client continuing to hold an active association, but unable to communicate to the network. Resetting the NIC card will clear the problem.

- This problem has been seen with Proxim Orinoco A/B/G cards with driver version 2.4.2.17. After roaming to a new AP, the client will generate MIC (Message Integrity Check) failures during phase 2 of the 4-way WPA key exchange handshake.
- Verify the problem by enabling 802.1x debugging on the Alcatel switch:

(config) # logging console debug # debug authmgr dot1x dot1xtrace

# VPN

#### VPN Dialer displays "Interface is down or no route"

This message indicates that the client does not have an IP address or a route to reach the Alcatel switch. To view the IP address and default gateway for the client, click the "Network Info" button in the VPN dialer.

- If there is no IP address on the interface, verify that the interface is configured to obtain an address via DHCP.
- Verify that association to the wireless network succeeded. Examine the output of "show user" on the Alcatel switch to view the client's association state.
- Verify that the DHCP server is active. If the Alcatel internal DHCP server is in use, the command "show log dhcp" will provide information on DHCP server activity.

# VPN Dialer displays "No Alcatel switches detected"

When this error message is displayed, it indicates that the VPN dialer could not verify that the client was associated to an Alcatel switch. The mechanism used to determine if an Alcatel switch is present is a DNS lookup. If the client is associated to an Alcatel switch, the DNS request will be intercepted by the Alcatel switch and a response sent back to the client.

The likely cause of this error message is that the client has no DNS server configured or learned through DHCP. If the client has no DNS server to use for lookups, the client will not generate DNS requests, and the Alcatel switch will not be able to intercept the request and respond to it. There are three possible solutions:

- Configure the DHCP server so that it supplies clients with a DNS server address.
- Statically configure the client with the address of a DNS server.
- In the Alcatel VPN dialer, turn off the option labeled "Wait for wireless". Note that with this option disabled, the VPN dialer will try to establish a connection any time the wireless NIC is connected to a network and has an IP address.

VPN Dialer displays "There was no answer"

This is a generic message indicating that the VPN client was unable to connect. Common causes are a mismatch between the dialer configuration on the client and the VPN configuration on the switch, or an internal Windows error.

- Examine log files on the Alcatel switch. First, examine the output of "show log crypto". The following error messages are common:
  - NO\_PROPOSAL\_CHOSEN: Indicates the client and switch are not configured in a like manner. If using the Alcatel dialer, verify that the lifetime, encryption, and hash for both IKE and IPSec match.
  - INVALID\_HASH\_INFORMATION: Indicates that the client and switch's IKE pre-shared keys do not match. If using a 3<sup>rd</sup>-party VPN client, the IKE pre-shared key is sometimes called the "group key" or "group password".
  - INVALID\_PAYLOAD\_TYPE, INVALID\_COOKIE, and PAYLOAD\_MALFORMED: May indicate that the IKE pre-shared key does not match between the client and switch.
- Examine the output of "show crypto isakmp sa". This command will list all IKE security associations (SAs) currently active in the switch. If no SA appears for the client in question, it is likely that the IKE pre-shared keys do not match between the client and switch.



Examine the output of "show crypto ipsec sa". Once IKE negotiation has succeeded (an IKE SA appears for the client), this command will list all IPSec security associations (SAs) currently active in the switch. If no SA appears for the client in question, it is likely that the client and switch have mismatching lifetimes, encryption types, or hash configuration.

#### VPN Dialer hangs while showing "Connecting"

Consider the following:

- One possible cause of this problem is a lack of IP connectivity to the Alcatel switch. It is unlikely that this is the cause when the client is attempting a VPN connection to the switch with which it is associated. However, the VPN client is sometimes used across multi-hop IP networks. If this problem appears, it may mean that the client has an IP address and a default route, but an upstream router does not have a path to the VPN termination point.
- Another possible cause of this problem is that the Windows IPSec service is not running. Bring up the Windows "Services" control panel by navigating to Start→Settings→Control Panel→Administrative Tools→Services. Look for the IPSec service, and verify it is configured as the following figure shows. Note that the IPSec service in turn depends on the Remote Procedure Call (RPC) service – verify that both are enabled.

I	PSEC Services Pro	perties (Local Computer)	? X
	General Log On	Recovery Dependencies	
	Service name:	PolicyAgent	
	Display name:	IPSEC Services	
	Description:	Manages IP security policy and starts the ISAKMP/ Oakley (IKE) and the IP security driver.	<u>▲</u>
	Path to executabl C:\WINDOWS\S	e: ystem32\lsass.exe	
	Startup type:	Automatic	•
	Service status:	Started	
	Start	Stop Pause Resume	
	You can specify t from here.	he start parameters that apply when you start the servic	e
	Start parameters:		
		OK Cancel Ap	ply

FIGURE 27-5 Windows IPSec Service

IPSec is up, but dialer does not display "Logging on" message

This message indicates that IPSec was successful, but L2TP was not.

- Verify the diagnosis by examining the output of show crypto ipsec sa. If a security association exists for the client, IPSec was successful. Examine the output of show vpdn tunnel 12tp. If L2TP has failed, no tunnel will exist for the client in question.
- This is an error condition. Contact Alcatel Technical Support for assistance.

Dialer displays "Logging on", but never displays "Connected"

This condition normally indicates that there is no IP address pool configured for the VPN, or that the address pool has been exhausted.

- Examine the output of show vpdn 12tp configuration. Verify that an IP address pool has been assigned.
- Examine the output of show vpdn 12tp local pool. Verify that there are IP addresses free. If there are not, it will be necessary to configure an additional IP address pool.



# Sample Packet Captures

# Broadcast Probe Request Frame

### Packet Information

Flags:	0x00
Status:	0x01
Packet Length:	54
Timestamp:	17:04:36.126816600 04/09/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	68%
Signal dBm:	-42
Noise Level:	0%

# 802.11 MAC Header

Version:	0
Туре:	%00 Management
Subtype:	%0100 Probe Request
Frame Control Flags:	80000000
	0 Non-strict order
	.0 WEP Not Enabled
	0 No More Data
	0 Power Management - active mode
	0 This is not a Re-Transmission
	0 Last or Unfragmented Frame
	0. Not an Exit from the Distribution
System	
	0 Not to the Distribution System
Duration:	0 Microseconds
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Source:	00:04:E2:64:C1:C0 SMC Net:64:C1:C0
BSSID:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Seq. Number:	349
Frag. Number:	0

# 802.11 Management - Probe Request

SSID			
Element	ID:	0	SSID
Length:		0	

```
Supported Rates
 Element ID:
                     1 Supported Rates
 Length:
                      8
  Supported Rate:
                    1.0 (Not BSS Basic Rate)
  Supported Rate:
                     2.0 (Not BSS Basic Rate)
  Supported Rate:
                     5.5 (Not BSS Basic Rate)
  Supported Rate:
                     11.0 (Not BSS Basic Rate)
  Supported Rate:
                     6.0 (Not BSS Basic Rate)
                     12.0 (Not BSS Basic Rate)
  Supported Rate:
  Supported Rate:
                     24.0 (Not BSS Basic Rate)
  Supported Rate:
                     36.0 (Not BSS Basic Rate)
Extended Supported Rates
 Element ID:
                 50 Extended Supported Rates
                      4
 Length:
                     9.0 (Not BSS Basic Rate)
  Supported Rate:
  Supported Rate:
                     18.0 (Not BSS Basic Rate)
  Supported Rate:
                     48.0 (Not BSS Basic Rate)
                      54.0 (Not BSS Basic Rate)
  Supported Rate:
```

# FCS - Frame Check Sequence

FCS	(Calculated):	0xCF771F24
-----	---------------	------------

# Specific Network Probe Request Frame

#### Packet Information

Flags:	0x00
Status:	0x01
Packet Length:	54
Timestamp:	17:04:36.126816600 04/09/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	68%
Signal dBm:	-42
Noise Level:	0%

# 802.11 MAC Header

Version:	0
Type:	%00 Management
Subtype:	%0100 Probe Request
Frame Control Flags:	80000000
	0 Non-strict order



	.0 WEP Not Enabled
	0 No More Data
	0 Power Management - active mode
	0 This is not a Re-Transmission
	0 Last or Unfragmented Frame
	O. Not an Exit from the Distribution
System	
	Not to the Distribution System
Duration:	0 Microseconds
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Source:	00:04:E2:64:C1:C0 SMC Net:64:C1:C0
BSSID:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Seq. Number:	349
Frag. Number:	0

# 802.11 Management - Probe Request

SSID	
Element ID:	0 SSID
Length:	16
SSID:	wireless-network
Supported Rates	
Element ID:	1 Supported Rates
Length:	8
Supported Rate:	1.0 (Not BSS Basic Rate)
Supported Rate:	2.0 (Not BSS Basic Rate)
Supported Rate:	5.5 (Not BSS Basic Rate)
Supported Rate:	11.0 (Not BSS Basic Rate)
Supported Rate:	6.0 (Not BSS Basic Rate)
Supported Rate:	12.0 (Not BSS Basic Rate)
Supported Rate:	24.0 (Not BSS Basic Rate)
Supported Rate:	36.0 (Not BSS Basic Rate)
Futended Currented Deter	_
Extended Supported Rates	
Element ID:	50 Extended Supported Rates
Length:	4
Supported Rate:	9.0 (Not BSS Basic Rate)
Supported Rate:	18.0 (Not BSS Basic Rate)
Supported Rate:	48.0 (Not BSS Basic Rate)
Supported Rate:	54.0 (Not BSS Basic Rate)

# FCS - Frame Check Sequence

FCS (Calculated): 0xCF771F24

# **Beacon Frame**

# Packet Information

Flags:	0x00
Status:	0x00
Packet Length:	97
Timestamp:	17:04:36.139436600 04/09/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	38%
Signal dBm:	-73
Noise Level:	0%

# 802.11 MAC Header

Version:	0
Type:	%00 Management
Subtype:	%1000 Beacon
Frame Control Flags:	%0000000
	0 Non-strict order
	.0 WEP Not Enabled
	0 No More Data
	0 Power Management - active mode
	0 This is not a Re-Transmission
	0 Last or Unfragmented Frame
	O. Not an Exit from the Distribution
System	
	0 Not to the Distribution System
Duration:	0 Microseconds
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Source:	00:0B:86:80:48:80 Alcatel Net:80:48:80
BSSID:	00:0B:86:80:48:80 Alcatel Net:80:48:80
Seq. Number:	3635
Frag. Number:	0

## 802.11 Management - Beacon

Timestamp:	82013696522	Microseconds
Beacon Interval:	100	
Capability Info:	%00000000011	0001



Disabled microseconds]	<pre>x Reserved .x Reserved 0 DSSS-OFDM is Not Allowed x Reserved 0 Robust Security Network 0 G Mode Short Slot Time [20 x. Reserved x. Reserved  0 Channel Agility Not Used  0 PBCC Not Allowed 1 Short Preamble 1 Privacy Enabled 0 CF Poll Not Requested  0 CF Not Pollable  0 CF Not Pollable</pre>
	1 ESS Type Network
SSID Element ID: Length: SSID:	0 SSID 16 wireless-network
Supported Rates	
Element ID: Length: Supported Rate: Supported Rate: Supported Rate: Supported Rate:	<pre>1 Supported Rates 4 1.0 (BSS Basic Rate) 2.0 (BSS Basic Rate) 5.5 (Not BSS Basic Rate) 11.0 (Not BSS Basic Rate)</pre>
Direct Sequence Para	ameter Set
Element ID: Length: Channel:	<pre>3 Direct Sequence Parameter Set 1 1</pre>

# Extended Supported Rates

Element ID:	50	Extended Supported Rates
Length:	8	
Supported Rate:	6.0	(Not BSS Basic Rate)
Supported Rate:	9.0	(Not BSS Basic Rate)
Supported Rate:	12.0	) (Not BSS Basic Rate)

Rate:	18.0	(Not	BSS	Basic	Rate)
Rate:	24.0	(Not	BSS	Basic	Rate)
Rate:	36.0	(Not	BSS	Basic	Rate)
Rate:	48.0	(Not	BSS	Basic	Rate)
Rate:	54.0	(Not	BSS	Basic	Rate)
	Rate: Rate: Rate: Rate: Rate:	Rate:       18.0         Rate:       24.0         Rate:       36.0         Rate:       48.0         Rate:       54.0	Rate:       18.0       (Not         Rate:       24.0       (Not         Rate:       36.0       (Not         Rate:       48.0       (Not         Rate:       54.0       (Not	Rate:       18.0       (Not BSS         Rate:       24.0       (Not BSS         Rate:       36.0       (Not BSS         Rate:       48.0       (Not BSS         Rate:       54.0       (Not BSS	Rate:18.0(Not BSS BasicRate:24.0(Not BSS BasicRate:36.0(Not BSS BasicRate:48.0(Not BSS BasicRate:54.0(Not BSS Basic

# **ERP** Information

42 ERP Information
1
80000010
x Reserved
.x Reserved
x Reserved
x Reserved
x Reserved
0 Not Barker Preamble Mode
1. Use Protection
0 Non-ERP Not Present

# Reserved 171

Element ID:	171 Reserved 171
Length:	11
Value:	0x000B86080400010A040026

# Traffic Indication Map

Element ID:	5	Traffic	Indication	Мар
Length:	4			
DTIM Count:	0			
DTIM Period:	1			
Traffic Ind.:	0			
Bitmap Offset:	0			
Part Virt Bmap:	0x0	C		

# FCS - Frame Check Sequence

FCS	(Calculated):	0xDCE7628D
FCS	(Calculated):	0xDCE7628D

# **Probe Response Frame**

Flags:	0x00
Status:	0x00
Packet Length:	82



Timestamp:	14:33:18.161865000 02/10/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	45%
Signal dBm:	0
Noise Level:	0%
Noise dBm:	0

Version:	0
Туре:	%00 Management
Subtype:	%0101 Probe Response
Frame Control Flags:	80000000
	0 Non-strict order
	.0 WEP Not Enabled
	0 No More Data
	0 Power Management - active mode
	0 This is not a Re-Transmission
	0 Last or Unfragmented Frame
	O. Not an Exit from the Distribution
System	
	0 Not to the Distribution System
Duration:	11547 Microseconds
Destination:	00:04:E2:64:BE:08 SMC Net:64:BE:08
Source:	00:0B:86:80:18:00 Alcatel Net:80:18:00
BSSID:	00:0B:86:80:18:00 Alcatel Net:80:18:00
Seq. Number:	2948
Frag. Number:	0

# 802.11 Management - Probe Response

Timestamp:	16683297454 Microseconds
Beacon Interval:	100
Capability Info:	%00000000110001
	x Reserved
	.x Reserved
	0 DSSS-OFDM is Not Allowed
	x Reserved
	0 Robust Security Network
Disabled	
	0 G Mode Short Slot Time [20
microseconds]	
	x Reserved

.....xReserved.....0Channel Agility Not Used.....0PBCC Not Allowed.....1Short Preamble....0Privacy Enabled....0CF Poll Not Requested....0CF Not Pollable....0Not an IBSS Type Network....1ESS Type Network

# SSID

Element	ID:	0	SSID
Length:		4	
SSID:		air	c1

# Supported Rates

Element ID:	1 Supported Rates
Length:	4
Supported Rate:	1.0 (BSS Basic Rate)
Supported Rate:	2.0 (BSS Basic Rate)
Supported Rate:	5.5 (Not BSS Basic Rate)
Supported Rate:	11.0 (Not BSS Basic Rate)

# Direct Sequence Parameter Set

Element ID:	3	Direct	Sequence	Parameter	Set
Length:	1				
Channel:	1				

# FCS - Frame Check Sequence

FCS (Calculated): 0x2C987D53

# 802.11 Authenticate Frame

Flags:	0x00
Status:	0x00
Packet Length:	34
Timestamp:	14:33:23.619951000 02/10/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	48%
Signal dBm:	0



Noise	Level:	0%
Noise	dBm:	0

Version:	0		
Туре:	%00 Management		
Subtype:	%1011 Authentication		
Frame Control Flags:	%0000000		
	0 Non-strict order		
	.0 WEP Not Enabled		
	0 No More Data		
	0 Power Management - active mode		
	0 This is not a Re-Transmission		
	0 Last or Unfragmented Frame		
	O. Not an Exit from the Distribution		
System			
	0 Not to the Distribution System		
Duration:	12315 Microseconds		
Destination:	00:0B:86:80:18:00 Alcatel Net:80:18:00		
Source:	00:04:E2:64:BE:08 SMC Net:64:BE:08		
BSSID:	00:0B:86:80:18:00 Alcatel Net:80:18:00		
Seq. Number:	0		
Frag. Number:	0		

# 802.11 Management - Authentication

Auth. Algorithm:	0 Open System
Auth. Seq. Num.:	1
Status Code:	0 Reserved

# FCS - Frame Check Sequence

FCS (Calculated):	0x31C54ADD
-------------------	------------

# 802.11 Authenticate Response (Success)

Flags:	0x00
Status:	0x00
Packet Length:	34
Timestamp:	14:33:23.622964000 02/10/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz

Signal Level:	37%
Signal dBm:	0
Noise Level:	0%
Noise dBm:	0

Version:	0			
Type:	%00 Management			
Subtype:	%1011 Authentication			
Frame Control Flags:	%0000000			
	0 Non-strict order			
	.0 WEP Not Enabled			
	0 No More Data			
	0 Power Management - active mode			
	0 This is not a Re-Transmission			
	0 Last or Unfragmented Frame			
	0. Not an Exit from the Distribution			
System				
	0 Not to the Distribution System			
Duration:	9499 Microseconds			
Destination:	00:04:E2:64:BE:08 SMC Net:64:BE:08			
Source:	00:0B:86:80:18:00 Alcatel Net:80:18:00			
BSSID:	00:0B:86:80:18:00 Alcatel Net:80:18:00			
Seq. Number:	3009			
Frag. Number:	0			

# 802.11 Management - Authentication

Auth.	Algorithm:	0	Open	System
Auth.	Seq. Num.:	2		
Stati	us Code:	0	Suc	ccessful

# FCS - Frame Check Sequence

FCS (Calculated): 0x045/AE
----------------------------

# Association Request Frame (includes WPA)

Flags:	0x00	
Status:	0x00	
Packet Length:	80	
Timestamp:	14:33:23.624195000	02/10/2004



Data Rate:	2	1.0	Mbps
Channel:	1	2412	MHz
Signal Level:	379	010	
Signal dBm:	0		
Noise Level:	08		
Noise dBm:	0		

Version:	0			
Type:	%00 Management			
Subtype:	%0000 Association Request			
Frame Control Flags:	%0000000			
	0 Non-strict order			
	.0 WEP Not Enabled			
	0 No More Data			
	0 Power Management - active mode			
	0 This is not a Re-Transmission			
	0 Last or Unfragmented Frame			
	O. Not an Exit from the Distribution			
System				
	Not to the Distribution System			
Duration:	9499 Microseconds			
Destination:	00:0B:86:80:18:00 Alcatel Net:80:18:00			
Source:	00:04:E2:64:BE:08 SMC Net:64:BE:08			
BSSID:	00:0B:86:80:18:00 Alcatel Net:80:18:00			
Seq. Number:	1			
Frag. Number:	0			
Frag. Number:	0			

# 802.11 Management—Association Request

Capability Info:	80000010000110001
	x Reserved
	.x Reserved
	0 DSSS-OFDM is Not Allowed
	x Reserved
	0 Robust Security Network
Disabled	
	1 G Mode Short Slot Time [9
microseconds]	
	x Reserved
	x Reserved
	0 Channel Agility Not Used

..... .1.... Short Preamble
..... Privacy Enabled
..... CF Poll Not Requested
..... CF Not Pollable
..... Not an IBSS Type Network
..... 1 ESS Type Network

Listen Interval:

# SSID

Element	ID:	0	SSID
Length:		4	
SSID:		air	1

#### **Supported Rates**

Element ID:	1 Supported Rates
Length:	8
Supported Rate:	1.0 (Not BSS Basic Rate)
Supported Rate:	2.0 (Not BSS Basic Rate)
Supported Rate:	5.5 (Not BSS Basic Rate)
Supported Rate:	11.0 (Not BSS Basic Rate)
Supported Rate:	6.0 (Not BSS Basic Rate)
Supported Rate:	9.0 (Not BSS Basic Rate)
Supported Rate:	12.0 (Not BSS Basic Rate)
Supported Rate:	24.0 (Not BSS Basic Rate)

1

# **Extended Supported Rates**

Element ID:	50 Ex	tended Supported Rates
Length:	4	
Supported Rate:	18.0	(Not BSS Basic Rate)
Supported Rate:	36.0	(Not BSS Basic Rate)
Supported Rate:	48.0	(Not BSS Basic Rate)
Supported Rate:	54.0	(Not BSS Basic Rate)

# WPA

```
Element ID:221 WPALength:24OUI:0x00-0x50-0xF2-0x01Version:1Multicast cipher OUI:0x00-0x50-0xF2-02 TKIPNumber of Unicast1Unicast cipher OUI:0x00-0x50-0xF2-02 TKIPNumber of Auths1
```



Auth OUI: 0x00-0x50-0xF2-01 SSN Extra bytes (Padding): .. 00 00

# FCS - Frame Check Sequence

FCS (Calculated): 0x0499A2D5

# **Association Response**

#### Packet Info

Flags:	0x00
Status:	0x00
Packet Length:	40
Timestamp:	14:33:23.627186000 02/10/2004
Data Rate:	2 1.0 Mbps
Channel:	1 2412 MHz
Signal Level:	47%
Signal dBm:	0
Noise Level:	0%
Noise dBm:	0

## 802.11 MAC Header

Version:	0
Type:	%00 Management
Subtype:	%0001 Association Response
Frame Control Flags:	80000000
	0 Non-strict order
	.0 WEP Not Enabled
	0 No More Data
	0 Power Management - active mode
	0 This is not a Re-Transmission
	0 Last or Unfragmented Frame
	O. Not an Exit from the Distribution
System	
	$\ldots$ 0 Not to the Distribution System
Duration:	12059 Microseconds
Destination:	00:04:E2:64:BE:08 SMC Net:64:BE:08
Source:	00:0B:86:80:18:00 Alcatel Net:80:18:00
BSSID:	00:0B:86:80:18:00 Alcatel Net:80:18:00
Seq. Number:	3010
Frag. Number:	0

## 802.11 Management—Association Response

Capability Info:	80000010000110001
	x Reserved
	.x Reserved
	x Reserved
	0 Robust Security Network
Disabled	-
	1 G Mode Short Slot Time [9
microseconds]	
	x Reserved
	x Reserved
	0 Channel Agility Not Used
	1 Short Preamble
	Privacy Enabled
	CF Poll Not Requested
	O CF Not Pollable
	1 ESS Type Network
Status Code:	0 Successful
Association ID:	
	0.0001
Supported Rates	
Element ID:	1 Supported Rates
Length:	4
Supported Rate:	1.0 (BSS Basic Rate)
Supported Rate:	2.0 (BSS Basic Rate)
Supported Rate:	5.5 (Not BSS Basic Rate)
Supported Rate:	11.0 (Not BSS Basic Rate)

# FCS - Frame Check Sequence

FCS (Calculated): 0xA470AA64

# **Packet Sniffing**

As of AOS-W 2.3 and later, two types of packet sniffing have been added to existing remote sniffing from APs and IKE (VPN) sniffing:



- Session mirror sniffing and
- Packet-capture for control path packets

# Packet Capture

This CLI utility allows sniffing of all control path packets. This is useful for sniffing RADIUS, 802.1x, VPN control path (IKE is encrypted, L2TP is not), station up/down opcodes, mobility, DHCP, and virtually any other packets that traverse the control path CPU.

To invoke the command as an action (not saved), enter:

# packet-capture tcp <all|disable|ports> udp <all|disable|ports>
Alcatelmsg <all|disable|ports> other <enable|disable>

To invoke the command as a config option which can be saved across switches in the running configuration, enter:

(config)# packet-capture-defaults tcp <all|disable|ports> udp <all|disable|ports> Alcatelmsg <all|disable|opcodes> other <enable|disable>

These commands create a file named filter.pcap in the logs directory that can then be extracted using tar logs. The file is also copied into the crash directory in the event of a crash. The file is limited to 1.5MB and will be backed up to filter.1.pcap if filled. So up to 3MB of captured packets can be retained for future inspection. These commands allow a complete playback of what happened.

**NOTE**—Be careful when using these commands as use passwords and keys may be stored inside filter.pcap.

To see the results of these commands, enter:

# show packet-capture

or

#### # show packet-capture-defaults

You can enable/disable sniffing on TCP, UDP, Alcatel messages, or any other types of packets. Note that "ports" and "opcodes" are comma separated values and you can sniff up to 10 of them. Whenever they're present, only those ports or opcodes are captured.

The following types of packets are always skipped:

• Alcatel message hellos

- Alcatel message BPDUs
- TCP cli ports (default ones)

### Examples

Debugging a wireless WEP station doing VPN would typically require:

- station up/down: Alcatel msg opcode 30
- wep key plumbing: Alcatel msg opcode 29
- DHCP: Alcatel msg opcode 90 (not udp 67 as that won't catch mobility packets)
- ike: udp port 500 & 4500
- 12tp: udp port 1701

#### Enter:

#### packet-capture Alcatelmsg 30,29,90 udp 500,4500,1701,1812,1645

#### Debugging 802.1x with TKIP would typically require:

- station up/down: Alcatel msg opcode 30
- 802.1x opcode: Alcatel msg opcode 13
- forward dot1x: Alcatel msg opcode 71
- tkip key plumbing: Alcatel msg opcode 70
- DHCP: Alcatel msg opcode 90
- radius: 1812 typically or 1645

#### Enter:

#### packet-capture Alcatelmsg 30,13,71,70,90 udp 1812,1645

**NOTE**—These examples give you all the messaging plus timestamps associated to them. This is useful for seeing whyfor example, users got associated but took 2 minutes to get an IP.

# SESSION MIRRORING

As of AOS-W 2.3.0.0 and later code you can mirror Ethernet packets on a per session basis. This feature is only accessible from the CLI.

For each ACL you want to be able to mirror, add the mirror flag and destination IP. For example, to see L2TP control packets unencrypted, enter:

```
firewall session-mirror-destination 1.2.3.4
ip access-list session vpnlogon
any any svc-l2tp permit mirror
```



Use ethereal on the target machine, in the above example, that's 1.2.3.4. It does not require an Alcatel specific ethereal as the packet format is GRE w/ Ethernet bridging. The target does *not* need to be trusted, the packet will be sent to the target regardless of being trusted or untrusted.
# CHAPTER 28 Diagnostic Tools

The Web UI Diagnostic tab contains information on tools to help you coordinate your troubleshooting of your Alcatel Wireless LAN environment with Alcatel Technical Support.

# **Network Utilities**

# Ping

To launch a ping from the WebUI, navigate to **Diagnostics > Ping.** 

Enter the target IP address and click **Ping**.





# Traceroute

To see the path traffic is taking by using the WebUI, navigate to **Diagnostics > Traceroute**. Enter the destination IP address and click **Trace**.

IP Address	10.100.101.30		
		Trace	Stop Tracing
10.4.21.25	4 0.62 msec 0.564 msec 0.562 msec		
2*** 2***			
, 1***			
5***			
5***			
7***			
B***			

FIGURE 28-2 Traceroute Test

# **General Information**

# **Contacting Technical Support**

To create a report on your configuration navigate to the **Diagnostics > Technical Support** page.

General > Technical Support			
Output File (stored in /flash/config)	]		
	Create Report File	View Report	Copy Report

FIGURE 28-3 Technical Support

# **Access Point Diagnostics**

The Access Point section of the Diagnostics tab provides support information on your Access Point devices.

# **Received Configuration**

To capture AP configurations, navigate to **Diagnostics > Received Configuration**. Enter the AP IP address and ESSID and click **Show Configuration**.

IP Address	
ESSID (optional)	
	Show Configuration

FIGURE 28-4 AP Recieved Configuration

# Software Status

To display software status information for specified APs, navigate to **Diagnositcs > Software Status**, enter the IP address of the target AP and click **Show Status**.

ccess Point > Software Status	
P Address	
	Show Status

FIGURE 28-5 AP Software Status



# Debug Log

To display the debug log when you have run debug tests, navigate to **Diagnostics > Debug Log**, enter the IP address of the logging device, and click **Show Debug Log**.

ccess Point > Deb	ug Log	
IP Address		
		Show Debug Log

FIGURE 28-6 Debug Log

# **Detailed Statistics**

To examine statistics for APs, navigate to **Diagnostics > Detailed Statistics**, enter the IP address of the target AP, then click **Show Statistics**.

Access Point > Detailed Statistics	
IP Address	
	Show Statistics

FIGURE 28-7 Detailed Statistics

# Web Diagnostic

To see diagnostics information from an AP's Web Server, navigate to **Diagnostics > Web Diagnostics**, enter the IP address of the target AP, and click **Link to AP Web Server**.

**NOTE**—The AP's Web server can only be accessed while the AP is booting.

Access Point > Web Diagnostics			
IP Address (web server available only during AP bootstrap)			
	Link to AP Web Server		

FIGURE 28-8 Diagnostic Tab



**OmniAccess Reference: AOS-W System Reference** 





**OmniAccess Reference: AOS-W System Reference** 

# CHAPTER 29 AOS-W Commands

# **Understanding the Command Line Interface**

The AOS-W command line interface is designed to conform with networking industry standard CLIs. Commands are grouped into modes so commands that perform similar functions are accessed at the same level. The system prompt identifies the current mode level.

When you enter a command and press **Enter**, the command executes. Use caution when testing a command as executing it will affect the switch.

**NOTE—** In the event that a command has undesirable consequences, you can always reset the switch to factory defaults by entering: (switch)# write erase all

(switch)# reload

# Navigating the CLI

To access a specific command, you must navigate to the mode containing that command. To reach a specific mode, you must access each lower-level mode starting from the Execute mode. For example, to configure air monitoring, you must log onto the switch (Exec mode), access Privileged mode commands, then access the AM mode commands.

To return to the previous mode, use the Exit command or specific termination command listed for that mode (for example, Ctrl-Z exits Config Terminal mode). Exit will always work for any mode.

# **Getting Help**

Online help is available for all commands by pressing ?. There are two levels of help.

To see what other command strings match what you have entered, type ? at the end of the string (no space) for which you want information. For example:

(switch) #reload?							
reload	Coldstart	the	swito	ch			
reload-peer-SC	Coldstart	the	peer	Supervisor	Card	(OmniAccess	6000)

shows you what commands start with the string reload.

To see help text for a command, enter the command for which you want help, enter a space, then type **?**. For example:

```
(switch) #ping ?
<ipaddr> Send ICMP echo packets to a specified IP address.
```

# Tips

To save time in entering commands, you only need to enter the first unique characters, then press Tab. The CLI will complete the rest of the command string.

The following sections explain the commands that are available at each mode. Notice that AOS-W Wireless LAN Switch commands are not listed alphabetically as one might expect in a reference manual. Because commands only apply in the mode, or context, in which they are executed, this chapter lists commands alphabetically by mode. This is intended to help you understand the difference, for example, of a aaa command in Privileged mode versus a aaa command in Configuration Terminal mode. Commands that function the same across all modes, (exit or traceroute, for example) are defined once and cross referenced.

# **Execute Mode Commands**

Exec mode commands allow very basic administrative access to the switch. Users who know the username and password for this level, but not the Privileged mode password, can only confirm basic Layer-3 connectivity.

Prompt	Commands	Description
(switch) >	enable	Turn on Privileged commands (switch)#
	exit	End this session. Any unsaved changes are lost. Same as the logout command.
	logout	End this session. Any unsaved changes are lost. Same as the exit command.
	ping	Send ICMP echo packets to a specified IP address.
	traceroute	Map the path the packets took to get to the specified address.

TABLE 29-1 Exec Mode Commands
-------------------------------

#### enable

Changes the CLI mode from the current Exec mode to Privileged mode. Privileged mode commands allow users to perform basic file management and system management functions.

## Example

(switch)> enable
(switch) #

## exit

Typically leaves the current mode and returns the previous mode. In the case, since the Exec mode is the entry-level mode, entering this command terminates the connection to the switch.

## Example

(switch) > exit



See logout.

#### logout

Terminates the session.

## Example

(switch) > logout

\_

See exit.

#### ping

Equivalent to the Unix ping command (with default options). This command issues a query to the specified device such that if the specified device is active and online, that device will respond back to the device issuing the ping. Useful for determining network connectivity between devices.

## Syntax

ping <ipaddr>

where ipaddr is the IP address of the device to send ping (or ICMP echo) packets.

## Example

```
(switch)> ping 10.1.1.1
Press 'q' to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
56.73/61.485/75.943 ms
```

(switch)>

#### traceroute

Equivalent to the Unix traceroute command (with default options). This command traces the path packets take to go from the switch to the specified device.

## Syntax

```
traceroute <ipaddr>
```

where ipaddr is the IP address of the destination device. The path to be traced is that between the switch and the specified device.

Example (switch) #traceroute 10.1.2.3 Press 'q' to abort. Tracing the route to 10.1.2.3 10.4.21.254 0.788 msec 0.564 msec 0.56 msec 1 2 \* \* 3 \* \* \* 4 \* \* \* . . . \* \* \* 20 21 \* (switch) #

# **Privileged Mode Commands**

Users who know the Privileged mode password have access to the commands that control the switch's file operating system, and such modes as the AAA and Air Monitor modes. This mode also allows access to the Configuration Terminal mode which is the mode that controls the switch configuration.

Prompt	Commands	Description
(switch) #	aaa	Accesses Triple-A (authentication, authorization, accounting) commands.
	am	Accesses Air Monitor commands.
	ap-upgrade-config	Updates existing 802.11b configurations to use 802.11g.
	apboot	Reboots all the specified Access Points.
	apflash	Reflashes the specified AP.
	audit-trail	Enables Audit Trail.
	backup	Backs up files in flash.

TABLE 29-2 Privileged Mode Commands



Prompt	Commands	Description
	boot	Restarts the switch.
	clear	Accesses clear commands.
	clock	Sets the system clock.
	configure	Accesses the configuration commands. (Alcatel) (config) #
	сору	Copies the specified files.
	database	Manages the database.
	debug	Access the debug commands.
	delete	Removes files.
	dir	Displays directories in flash.
	local-userdb	Manages the local user database.
	no	Specifies the 'no' form of commands that support this syntax.
	page	Access the Page command.
	paging	Specifies output paging.
	panic	Accesses the system panic information commands.
	рсар	Accesses the packet capture commands.
	ping	The ICMP command.
	reload	Executes a cold boot of the switch. Contrasts with the boot command which warm starts the switch.
	rename	Changes the specified file name.

 TABLE 29-2
 Privileged Mode Commands (Continued)

	_	
Prompt	Commands	Description
	restore	Restores the directories on flash.
	secret	Commands reserved for Alcatel engineering. Do not access these commands with Alcatel tech support assistance.
	show	Access the show commands.
	site-survey	Accesses the site survey commands.
	stm	Accesses the Station Management commands.
	swkey	Accesses licensing controls.
	tar	Creates a tar file of the specified directory.
	traceroute	Traces the route a packet has taken to the specified IP address.
	whoami	Displays the name of the user who is logged on.
	wms	Accesses the Wireless LAN Management System commands.
	write	Saves the running configuration file to the specified location.

 TABLE 29-2
 Privileged Mode Commands (Continued)

# aaa Commands

The Privileged mode aaa commands include:

(switch) #aaa ?
inservice Bring authentication server into service
stateful-authentication
test-server Test authentication server



user

User commands

See also the aaa commands in Configure mode.

#### (switch) #aaa inservice

Enables the specified authentication server.

#### Syntax

aaa inservice <string> where string is the name of the authentication server to be enabled.

#### Example

(switch) # aaa inservice Alcatel.com

See also:

aaa test-server

#### (switch) #aaa inservice stateful-authentication

Enables stateful authentication on authentication servers.

#### Syntax

[no] aaa inservice stateful-authentication

#### Example

(switch) # aaa inservice stateful-authentication To disable stateful-authentication, enter:

(switch) # no aaa inservice stateful-authentication

## (switch) #aaa stateful-authentication dot1x delete-all

#### Syntax

aaa stateful-authentication dot1x delete-all

## Example

## (switch) #aaa test-server

#### Syntax

aaa test-server <string>

## Example

The following example verifies that the authentication server Alcatel is enabled and working.

(switch) # aaa test-server Alcatel

#### (switch) #aaa user

Manages users for authentication purposes. You can add, delete, logoff, and debug users. You can also clear sessions for an individual user.

# Syntax

add <ipaddr></ipaddr>	Adds the IP address of a user
clear-sessions <ipaddr></ipaddr>	Clears the specified user session.
debug <ipaddr mac name <string="">&gt;</ipaddr mac name>	Debugs user by user's IP address, MAC address, or name.
delete <ipaddr all mac name <string> role<string>&gt;</string></string></ipaddr all mac name 	Deletes specified user. Use all to delete all connected users.
logout <ipaddr></ipaddr>	Logs the specified user out

## Examples

The following examples show a user being added, their sessions being cleared, a user being debugged, a user being deleted, and a user being logged out.

(switch) #aaa user add 192.10.10.1
(switch) #aaa user clear-sessions 192.10.10.1
(switch) #aaa user debug name vipin
(switch) #aaa user delete 192.10.10.1
1 user deleted

(switch) #aaa user logout 192.10.10.1

#### ads netad learn

Learn the system on which an anomaly has been flagged by NETAD.

## Syntax

ads netad learn <anomaly-id>

where anomaly-id is the ID of the anomaly reported by the show command .



#### Example

(switch) #ads netad learn

#### am

Configures scanning on the specified channel for the specified Air Monitor.

## Syntax

am scan <am-ip> <channel> <bssid>

where:

<am-ip)> is the IP address of the Air Monitor to be scanned.

<channel> is the channel to tune to. Set this to 0 to start scanning.

<bssid> is the MAC Address of the Air Monitor

## Example

(switch) **#am scan 10.4.4.4 11** Module AM is busy. Please try later

## ap-upgrade-config

Allows you to convert your existing 802.11b configurations to support 802.11g as well.

## Example

(switch) #ap-upgrade-config
(switch) #

## apflash

Reflashes the specified Access Point.

Syntax (switch) #apflash <ipaddr>

## Example

(switch) **#apflash 192.10.10.1** 

## audit-trail

Example (switch) #audit-trail

#### backup

Backs up and compresses critical files to flashbackup.tar.gz.

## Example

(switch) #backup flash

See also restore.

#### boot

Specifies the configuration file and the partition the switch uses to boot.

## Syntax

boot <config-file> <filename> | <system> <0|1>

## Example

The following example directs the switch to boot from config file 9147.

(switch) #boot config-file 9147
The following example directs the switch to boot from partition 0.

(switch) #boot system partition 0

# clear Commands

The clear command resets counters to zero for:

Parameter	Description
ads	Anomaly Detection System Commands
arp	Clear arp table
counters	Clear counters on one or all interfaces
crypto	Clear crypto state
ip	
loginsession	Login Session
mobile	mobility manager
rap-wml	Rogue AP Wired MAC Lookup Commands
site-survey	Site Survey Clear Commands
stm	Station Management commands
vpdn	Clear vpdn state



Parameter	Description					
wms	Wireless	LAN	Management	system	commands	

#### clear ads netad anomaly

Sets the network anomaly detection counters to zero.

Parameter	Description
all	Resets all NETAD anomaly counters to zero.
id	Resets the specified NETAD anomaly counter to zero.

## Example

(switch) #clear ads netad anomaly all

#### clear arp

Clears the Address Resolution Protocol statistics.

#### Example

#### clear counters fastethernet

Resets the fastethernet port counters to zero.

#### Syntax

```
clear counters fastethernet <slot/port>
    where the <slot/<port> specifies which card and which port is to be reset.
```

#### Example

```
(switch) #clear counters fastethernet 1/1
```

#### clear counters gigabitethernet

Resets the gigabitethernet port counters to zero.

#### Syntax

clear counters fastethernet <slot/port>
 where the <slot/<port> specifies which card and which port is to be reset.

## Example

(switch) #clear counters gigabitethernet 1/1

#### clear counters vrrp

Clears the Virtual Router Redundancy Protocol statistics.

## Syntax

clear counters vrrp <id> where <id> is the Virtual Router ID. Valid ID range is 1-255.

## Example

(switch) #clear counters vrrp 1
(switch) #clear arp

## clear crypto

Turns off cryptographic state.

## Syntax

dp	Clear crypto latest DP pack- ets		
<pre>ipsec {sa   <peer> <ipaddr>}</ipaddr></peer></pre>	Clear crypto isakmp state		
isakmp	Clear crypto isakmp state		

## Example

To clear dp packets, enter:

(switch) #clear crypto dp

To clear the IPSec crypto state for the security association peer at 192.10.10.1, enter:

(switch) #clear crypto ipsec sa peer 192.10.10.1

## clear ip dhcp binding

Clears DHCP server bindings.

## clear loginsession

Clears the specified logging session.

## Syntax

```
clear loginsession <id>
    where:
```

<id>

Session id 2-6

## Example

To clear login session 2, enter:



(switch) #clear loginsession 2

#### (switch) #clear mobile

packet-counters Clears mobility packet counters

registration-statisti.. Clears mobile ip message counts for a mobile node

(switch) #clear mobile packet-counters ?

<cr>

(switch) #clear mobile registration-statistics ?

<ip> IP address of mobile node

(switch) #clear mobile registration-statistics ip ?

(switch) #clear mobile registration-statistics 192.10.10.1?

<cr>

#### (switch) #clear rap-wml

cache Clear Wired MAC Lookup Cache for a DB Server

(switch) #clear rap-wml cache ?

<server-name> DB Server Name

(switch) #clear rap-wml cache paul ?

<cr>

#### (switch) #clear site-survey

calibration Clear Site Survey Calibration In Progress

channel-plan

(switch) #clear site-survey calibration ?

<br/>suilding-id> Building ID to start site survey on

(switch) #clear site-survey calibration 1.2.3?

(switch) #clear site-survey calibration 1.1.1?

(switch) #clear site-survey channel-plan ?

<br/>suilding-id> Building ID to start site survey on

(switch) #clear site-survey channel-plan 1.1.1 ?

#### (switch) #clear stm

hole Clear a coverage hole state

(switch) #clear stm hole ?

all Clear all flagged coverage holes



bssid BSSID for the flagged AP to clear hole

(switch) #clear stm hole all ?

<cr>

(switch) #clear stm hole testap ?

(switch) #clear stm hole 00:00:00:01:01:01 ?

#### (switch) #clear vpdn

tunnel Clear vpdn tunnel

(switch) #clear vpdn tunnel ?

I2tp Clear vpdn all L2TP tunnel

pptp Clear vpdn all PPTP tunnel, not supported

(switch) #clear vpdn tunnel l2tp ?

id Tunnel ID to clear

<cr>

(switch) #clear vpdn tunnel pptp?

id Tunnel ID to clear, not supported

<cr>

## (switch) #clear wms

ap Clear AP information

probe

sta Clear STA information

(switch) #clear wms probe ?

<bssid>

(switch) #clear wms ap ?

<bssid> BSSID of AP

(switch) #clear wms sta?

<mac> MAC Address of STA

(switch) #clear wms 00:00:01:01:0a ?

(switch) #

## clock

See also the clock commands in Configuration mode.

## Syntax

clock set <year> <month> <day> <hour> <min> <sec>



where <year> is the four-digit year, <month> is the name of the month, <day> is the number of the day (1-31), hour is the time in hours (0-24), <min> is the number of minutes in the hour (0-60), and <sec> is the number of seconds in the minute (0-60).

## Example

To set the time to be 5 January 2005 at 11:23:00 PM, enter:

(switch) #clock set 2005 January 5 11 23 00
(switch) #

**NOTE**—In AOS-W 2.3 or higher, specify the month by its name (for example, December) rather than by its number (for example, 12). Also note that dates are set in the format of year, month, and date rather than day, month, and year, or month, day, and year.

#### configure terminal

Accesses the switch configuration mode.

#### Example

```
(switch) #configure terminal
(switch) (config) #
```

#### сору

Duplicates files.

## Syntax

flash:	
ftp:	ftp file system
log	Logging
running-config	Running Configuration
startup-config	Startup Configuration
system:	System Partition
tftp:	Tftp file system

#### copy flash

Copies the flash file to a backup file on the switch or to an external host using TFTP.

## Syntax

```
copy flash <srcfilename> <flash:destfilename> |<tftp:tftphost>
```

# Examples

(switch) #copy flash: 9147 tftp:10.1.1.55

(switch) #copy flash: 9147 flash: copy9147

#### copy system

Copies the system from one partition to the other.

## Syntax

copy system: <source partition 0l1> <destination partition 0l1>

## Example

(switch) #copy system: partition 1 0

## copy log

Copies the specified log file to the specified location.

## Syntax

```
copy <module> <destination>
    where modules are:
```

aaa	Logging for	administrator authentication	
ads	Logging for Anomaly Detection		
all	Copy All the	e log files	
authmgr	Logging for	user authentication	
cfgm	Logging for	Configuration Manager	
crypto	Logging for	VPN (IKE/IPSEC)	
dhcpd	Logging for	DHCP packets	
errorlog	Errors logge	ed in the system	
fpapps	Logging for	Layer 2,3 control	
intuser	Logging for	User Information (Internal)	
12tp	Logging for	L2TP	
localdb	Logging for	local database	
master	Logging for	Mobility Master Database (Master	
switch only)			
mmgr	Logging for	Mobility Manager	
mobagent	Logging for	Mobility Agent	
packetfilter	Logging for	packet filtering of Alcatel	
messaging and control f	rames		
pim	Logging for	Protocol Independent Multicast	
pptp	Logging for	PPTP	
processes	Logging for	run-time processes	
publisher	Logging for	publish subscribe service	



sapm	Logging	for	AP Manager (Master switch only)
snmp	Logging	for	SNMP agent
ssi	Logging	for	Secure Service Interface
stm	Logging	for	Station Management
suser	Logging	for	User Information
traffic	Logging	for	traffic
wms	Logging	for	Wireless Management (Master switch
only)			

#### copy running-config

Copies the running-config file to the specified location.

#### Syntax

```
copy running-config <flash:destfilename> |<tftp:tftphost>
```

#### copy startup-config

Copies the startup-config file to the specified location.

#### Syntax

copy startup-config <flash:destfilename> |<tftp:tftphost>

#### copy tftp

Copies the specified file to the specified location using TFTP.

#### Syntax

copy tftp: <tftphost> <filename> <flash | system partition>

where:

<tftphost> Is the TFTP server host name or IP address.

<filename> Is the name of the file to be copied.

flash Specifies that the file be copied to the flash file system.

system Specifies the System Partition number, 0 or 1.

#### Example

The following example specifies that the file main be copied to system partition 1 using TFTP.

(switch) #copy tftp: main 9147 system: partition 1

#### copy ftp

Copies the specified file to the specified location using FTP.

## Syntax

copy ftp: <filename> <flash | system partition> where:

<filename> Is the name of the file to be copied.

flash Specifies that the file be copied to the flash file system.

system Specifies the System Partition number, 0 or 1.

## Example

The following example specifies that the file main be copied to system partition 1 using FTP.

(switch) #copy ftp:

## crypto

Configures IKE.

## Syntax

cyrpto isakmp

## Example

(switch) #crypto isakmp

## database

Syncs the database.

## Example

(switch) #database synchronize

## debug

Enables debugging for the following switch features:

ааа	Debugging for administrator authentication
ads	Debugging for Anomaly Detection
all	Enable all debug
authmgr	Debugging for user authentication
cfgm	Debugging for Configuration Manager
-	



crypto	Debugging for VPN (IKE/IPSEC)
dhcpd	Debugging for DHCP packets
fpapps	Debugging for Layer 2,3 control
intuser	Debugging for User Information (Internal)
l2tp	Debugging for L2TP
localdb	Debugging for local database
master	Debugging for Mobility Master Database (Master switch only)
mmgr	Debugging for Mobility Manager
mobagent	Debugging for Mobility Agent
packetfilter	Debugging for packet filtering of Alcatel messaging and control frames
pim	Debugging for Protocol Independent Multicast
pptp	Debugging for PPTP
processes	Debugging for run-time processes
publisher	Debugging for publish subscribe service
sapm	Debugging for AP Manager (Master switch only)
snmp	Debugging for SNMP agent
ssi	Debugging for Secure Service Interface
stm	Debugging for Station Management
suser	Debugging for User Information
traffic	Debugging for traffic
wms only)	Debugging for Wireless Management (Master switch

# Example

The following examples turns on debugging for all aaa module functions.

(switch) #debug aaa all
(switch) #

#### delete

Removes the specified file name from flash. The file must exist in flash and be correctly specified before the delete command can remove it.

## Syntax

delete <filename>

where <filename> is the name of the file in flash that is to be erased.

## Example

The following example removes the file named test from flash.

```
(switch) #delete test
```

#### dir

Displays a listing of all the files in flash. This command is the same as the DOS dir command (similar to the Unix ls command).

## Example

The following example lists all the files in the root directory of flash.

(switch) #dir

-rw-rr	1 roo	ot root	50	Dec	3	18:55	db_dump.sql
-rw-rr	1 roo	ot root	18383	Dec	13	09:42	default.cfg
-rw-rr	1 roo	ot root	252928	Dec	13	10:49	logs.tar
-rw-rr	1 roo	ot root	294896	Dec	1	14:47	rfplan.js
xr	1 roo	ot root	25431	Nov	17	17:33	run2.0.8
-rw-rr	1 roo	ot root	27515	Nov	18	18:11	run2.2.4
-rw-rr	1 roo	ot root	28221	Nov	16	16:00	<pre>runconfig2.2.3</pre>
-rw	1 roo	ot root	136	Nov	17	18:04	webtrace

#### (switch) #

#### halt

Gracefully stops all processes on the switch. Uses should halt the switch before rebooting or shutting down to avoid interrupting processes underway.



```
Example
 (switch) #halt
 (switch) #
```

#### local-userdb

Manages the user database.

#### Syntax

local-userdb {add <username> | del | del-all | export | fix-database | import | modify}

#### where

add	Add a user
del	Delete a user
del-all	Delete all users
export	Export the Local User Database to a file
fix-database	Use this command with CAUTION, it will wipe out
the whole database. To s	save existing data use the export command.
import	Use this command with CAUTION, it will Replace
the existing users with	the user entries from the imported file.
modify	Modify the User Attributes.

## Example

The following example illustrates adding the user Vipin to the local user database.

(switch) #local-userdb add Vipin

#### no

Disables the feature specified.

#### Syntax

```
(switch) #no ?
aaa Authentication commands
audit-trail Enable Audit Trail
crypto Configure IPSec, IKE, and CA
debug Debugging Functions
paging Output paging
```

#### Example

To disable IKE, enter:

(switch) **#no crypto isakmp** To disable debugging the L2TP module, enter:

(switch) #no debug 12tp

#### packet-capture

Configures monitoring the specified types of traffic. This is useful for diagnostic purposes.

#### Syntax

```
packet-capture {Alcatelmsg <opcodes> | other <enable | disable> | tcp
<ports> | udp <ports>}
```

where:

Alcatelmsg Enables or disables Alcatel internal messaging packet cap turing. For debugging only.

opcodesSpecifies opcodes to capture. You can specify up ten opcodes, separated by commas.

otherEnables or disables all other types of packets.

tcp Enables or disables TCP packet capturing.

udpEnables or disables TCP packet capturing.

portsSpecifies the ports to which packets are addressed. Specify up to ten ports, separated by commas. To specify all ports, enter all.

#### Example

(switch) **#packet-capture Alcatelmsg all tcp all** 

#### page

TBD

## Syntax

page <length>

where <length> specifies the size of the page. Valid range is 24 - 100.

## Example

The following example sets the page size to 80

(switch) #**page 80** (switch) #

paging TBD



## Example

```
TBD
(switch) #paging
(switch) #
```

#### panic

Manages files created during a system crash.

## Syntax

```
panic {clear | info <file filename | nvram symbolfile> | list <file |
nvram> | save filename}
```

#### where:

clear removes the panic files from flash.

info prints out the specified panic file information from either NVRAM or flash.

list displays all the flash or NVRAM panic files.

save saves the panic file with the specified file name.

## Example

The following example shows how to display any panic files in NVRAM. (There are no panic files.)

```
(switch) #panic list nvram
# Date PN PANIC/EX ver built by Process
0 IS EMPTY
1 IS EMPTY
```

#### рсар

Starts or stops packet capture sessions. Info

## Syntax

```
pcap {<start | stop | resume> | clear | interactive ipaddr | raw-start
<ipaddr> <target-ipaddr> <target-port> <format> [bssid | channel]}
where:
```

```
startStart New Packet Capture session
stopStop a Packet Capture session
clear
interactive
raw-start
```

bssid BSSID of AM interface to start PCAP on channel Channel to tune into to capture packets

## Example

The following example starts a raw packet capture session for the AM at 10.100.100.1 and sends the frames to the target IP address 192.168.22.44 on port 604 with pcap format .

(switch) **#pcap raw-start 10.100.100.1 192.168.22.44 604 0** Explanation

## ping

#### Syntax

ping <ipaddr>

where ipaddr is the IP address of the device to send ping (or ICMP echo) packets.

## Example

```
(switch)> ping 10.1.1.1
Press 'q' to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
56.73/61.485/75.943 ms
```

(switch)>

## reload

Resets the system to boot to the configuration file.

## Example

```
(switch) #reload
Do you really want to reset the system(y/n) : y
System will now restart!
...
Restarting system.
```

## reload-peer-sc

Example



(switch) #reload-peer-SC

#### rename

Changes the specified file name to a new file name.

#### Syntax

(switch) #rename <filename> <newfilename>

#### Example

The following example changes the file named bud to pub.

#### (switch) **#rename bud pub**

#### restore

Reinstates the backed up flash directories in flashbackup.tar.gz. The tar backup file is untarred and uncompressed.

#### Syntax

restore flash

#### Example

(switch) **#restore flash** 

See also backup.

#### secret

These commands are intended for use by authorized support personnel. Do not use these command unless directed to do so by Alcatel Support.

#### show

The show commands display information on the following modules:

(switch) # <b>show ?</b>	
aaa	Show AAA configuration
access-list	Show access-lists
acl	Show internal ACL tables
adp	ADP related commands
ads	Show Anomaly Detection System state
am	Air Monitor commands
ap	Access Point commands
ap-leds	Show AP LED array state for a slot
ap-params	AP environment variables to be programmed
arp	ARP information
audit-trail	Show Audit Trail Log
banner boot. clock configuration country cpuload crypto database datapath debugging destination dot 1xfirewall hostname image interface inventory ip keys local-switches local-userdb location loq logging loginsessions mac-address-table master-redundancy memory mgmt-modules mgmt-role mgmt-user mobile mux netdestination netservice netstat ntp packet-capture config

User's in the Local User DataBase Show the switch location Show the contents of the logging buffers Show Logging Levels for applications Show administrator login sessions MAC Forwarding Table Master Switch Redundancy Configuration Display the memory information Show the predefined Management Modules Management Role Definition Show Management User Information Displays mobility information Show MUX Information Show network destinations Show network services Show current active network connections NTP Server Info Show packet-capture settings. packet-capture-defaul.. Show packet-capture default settings (saved in file). Packet Capture commands Show switch port configuration Show system processes

Display boot parameters

Show saved configuration

Show crypto configuration

Show 802.1X Information

Show hardware inventory

IP information

Display the host name

Display CPU Load

Database management Datapath statistics

Displays the country code setting

State of each debugging option

Show network destination information

Show System image version information

Show global firewall configuration

Interface Status and Configuration

Show optional keys/features enabled

Local switches connected to the master



processes

pcap port

provisioning-ap-list rap-wml Rogue AP Wired MAC Lookup Commands rfsm Show RF Spectrum Management Information rights Show access rights for user roles roleinfo Show the switch role routerid Router Id of the Switch running-config Show running configuration sapm Show session access-list session-access-list site-survev Show Site Survey information slots Slots which have line cards in them. Display the SNMP Configured snmp Spanning tree topology spanning-tree Global spanning tree topology spantree ssi Show Security Service Interface information startup-config Show saved configuration station-table Show internal station table stm Show 802.11 station management information storage Display the switch storage information switch Switch Configuration M-switches connected to the master and the master switches included switchinfo Display the switch system information Display the system contact syscontact syslocation Display the system location Display the general switch information tech-support Show time-range time-range Vlan Trunk Port Information trunk un-provisioned user user-table Show internal user table Show administrative users users version Show System version virt-ap Show virtual APs configured at a location vlan VLAN IP Interface Show vpdn state vpdn Show VPN dialers vpn-dialer vrrp VRRP configuration information Wireless LAN Show Wireless LAN Information Commands for viewing Wireless IDS configuration wms

(switch) #

These commands are explained in detail in "Show Commands" on page 833.

## site-survey

See also the site-survey commands in Configuration mode.

# Syntax

# Example

## (switch) #site-survey ?

- calibrate Start site survey calibration and channel assignment
- channel-plan Start channel assignment
- update-channel-plan Update channel plan for specific AP

(switch) #site-survey channel-plan ?

<br/>suilding-id> Building ID to start site survey on

(switch) #site-survey channel-plan 1.1.9?

(switch) #site-survey channel-plan 1.1.2 ?

(switch) #site-survey channel-plan 1.1.1 ?

(switch) #site-survey calibrate ?

<br/>suilding-id> Building ID to start site survey on



AOS-W Commands | 665

(switch) #site-survey calibrate 1.1.1?

(switch) #site-survey update-channel-plan ?

<bssid> AP bssid

(switch) #site-survey update-channel-plan bud ?

(switch) #site-survey update-channel-plan bud

#### stm

Manages the station manager commands.

See also the stm commands in Configuration mode.

# Syntax

# Example

(switch)	#stm	?
----------	------	---

- add-dos-sta Add a STA to DoS list
- kick-off-sta Kick off an STA
- remove-dos-sta Remove a STA from DoS list
- start-trace Start tracing probe request/probe response from mac
- stop-trace Stop tracing probe request/probe response from mac

(switch) #stm add-dos-sta?

<mac> STA to add to DoS list

(switch) #stm add-dos-sta 00:00:00:01:01:ab ?

<cr>

(switch) #stm add-dos-sta 00:00:00:01:01:ab

(switch) #stm kick-off-sta ?

<mac> STA to kick off

(switch) #stm kick-off-sta 00:00:00:01:01:ab ?

<bssid> AP to to kick off STA from

(switch) #stm kick-off-sta 00:00:00:01:01:ab bud ?

(switch) #stm kick-off-sta?

<mac> STA to kick off

(switch) #stm kick-off-sta paul ?

(switch) #stm remove-dos-sta?



<mac> STA to remove from DoS list

(switch) #stm remove-dos-sta 00:00:00:01:01:ab ?

<cr>

(switch) #stm remove-dos-sta 00:00:00:01:01:ab

(switch) #stm start-trace ?

<mac>

(switch) #stm start-trace 00:00:00:01:01;ab ?

(switch) #stm stop-trace ?

<mac> STA/BSSID to stop tracing

(switch) #stm stop-trace 00:00:00:01:01:ab

(switch) #

#### swkey

The software licenses key. Enables the specified feature.

# Syntax

```
swkey <softwareKey>
where <softwareKey> is the Software activation Key.
```

# Example

TBD

# tar

Creates a file in Unix tar file format.

# Syntax

tar {clean | crash | flash | logs}

## where:

clean Removes a tar file
crash tar the crash directory to crash.tar
flash tar and compress the /flash directory to flash.tar.gz
logs tar the logs directory to logs.tar

# Example

To create a tar file for the directories in flash, enter:

(switch) #tar flash

## traceroute

Equivalent to the Unix traceroute command (with default options). This command traces the path packets take to go from the switch to the specified device.

# Syntax

```
traceroute <ipaddr>
```

where ipaddr is the IP address of the destination device. The path to be traced is that between the switch and the specified device.

# Example

(switch)#traceroute 10.1.2.3 Press 'q' to abort. Tracing the route to 10.1.2.3

```
1 10.4.21.254 0.788 msec 0.564 msec 0.56 msec

2 * * *

3 * * *

4 * * *

20 * * *

21 *
```



(switch) #

See also the traceroute command in Configuration mode and Exec mode.

#### whoami

This command returns the name of the user who is logged in to this session. It is the same as the Unix command of the same name.

## Example

```
(switch) #whoami
user admin - role root
```

#### wms

See also the wms commands in Configuration mode.

# Syntax

# Example

#### (switch) #wms ?

ар	configure AP mode
clean-db	Clean Database
export-db	Export DB to a file
import-db	Import DB from a file
reinit-db	Reinitialize Database
station	configure station mode

(switch) #wms ap ?

<bssid> bssid of AP

Chapter 29

(switch) #wms ap pub ?

(switch) #wms ap pub

۸

% Invalid input detected at '^' marker.

(switch) #wms clean-db?

<cr>

(switch) #wms export-db?

<filename> Name of file to export db to

(switch) #wms export-db main ?

<cr>

(switch) #wms import-db?

<filename> Name of file from which to import db

(switch) #wms import-db secondary ?

<cr>

(switch) #wms reinit-db?

<cr>



(switch) #wms station ?

<mac> MAC Address of station

(switch) #wms station test ?

(switch) #

#### write

Saves the running configuration to memory or to the terminal computer. Can also be used to erase the running configuration and return the switch to factory defaults.

#### Syntax

write {erase all | memory | terminal}

#### Example

To delete the running configuration and databases and return the switch to factory default settings, enter:

(switch) **#write erase all** 

To save the running configuration and databases to memory, enter:

(switch) #write memory

# **Configure Terminal Commands**

**NOTE**—This section was under construction at print time. This section includes incomplete information. For a more up-to-date discussion, refer to the online version of this document.

The following command allow you to configure your Wireless LAN Switch and APs.

Prompt	Commands	Description
(switch) (config) #	ааа	Configure Authentication
	adp	Alcatel Discovery Protocol Com- mands
	ads	Configure Anomaly Detection Sys- tem
	ар	Specify configuration of an AP by location or by BSSID
	arm	Adaptive Radio Management
	arp	Add arp entry
	auto-rra	Auto Radio Resource Allocation Configuration
	banner	Define a banner
	clock	Configure time-of-day clock
	crypto	Configure IPSec, IKE, and CA
	database	Database management
	destination	Configure network destination (dep- recated; use netdestination)
	dot1x	Configure IEEE 802.1X Authentica- tor
	enable	Modify the enable password
	encrypt	Enable Encryption
	firewall	Configure global Firewall policies
	foreign-agent	Accesses local commands for for- eign agent
	home-agent	Accesses local commands for home agent
	hostname	Change the Hostname
	interface	Select an interface to configure
	ip	interface Internet Protocol config commands
	location	Configure the switch location
	logging	Modify Message Logging Facilities

 TABLE 29-3
 Terminal Configuration Mode Commands



Prompt	Commands	Description
	loginsession	Login Session
	mac-address-table	Configure the MAC address table
	master-redun- dancy	Accesses Master Switch Redun- dancy Configuration commands
	masterip	Configure the master ip address for the switch
	mgmt-role	Management Role Definition
	mgmt-user	Configure a management user.
	mobagent	Accesses configuration global parameters for mobility agent
	mobility	Accesses configuration mobility manager commands
	mobility-local	Accesses configuration commands for local mobility manager
	mux-address	Set MUX Server IP Address. 0.0.0.0 to disable
	mux-vlan	Enable MUX functionality on a VLAN
	netdestination	Configure network destination
	netservice	Configure a network service
	newbury	Specify Newbury Locate Server Information
	no	Delete Command
	ntp	Configure NTP
	ping	Send ICMP echo packets to a speci- fied IP address.
	pptp	Configure IP information for PPTP
	program-ap	Provision APs by plugging them into the switch
	program-ap	Provision APs by plugging them into the switch
	rap-wml	Wired MAC Lookup for AP Classification commands
	router	Router Mobile
_	sapm	Help not defined

 TABLE 29-3
 Terminal Configuration Mode Commands

Prompt	Commands	Description
	service	Configure services
	shutdown	Shut down interface
	site-survey	Site Survey configuration com- mands
	snmp-server	Enable SNMP; Modify SNMP parameters
	spanning-tree	Spanning Tree Subsystem
	ssi	Configure Security Service Interface
	stm	802.11 station management config- uration
	syscontact	Change the system contact
	syslocation	Change the system location
	telnet	Enable telnet port
	time-range	Configure a time range
	traceroute	Trace route to specified IP address.
	trusted	Make this a trusted port
	user-role	Configure user role
	vlan	Create Switch VLAN Virtual Inter- face
	vpdn	Configure Virtual Private Dial-In Net- working
	vpn-dialer	Configure the VPN dialer
	vrrp	Virtual Router Redundancy Protocol Configuration
	wms	Accesses Wireless LAN Manage- ment System Commands

 TABLE 29-3
 Terminal Configuration Mode Commands

# aaa Commands

This command controls user authorization and authentication for the switch. Use the no form of this command to disable AAA functions.



# Syntax

aaa {bandwidth-contract | captive-portal | derivation-rules | dot1x | kerberos | ldap-server | mac-authentication | mgmt-authentication | pubcookie-authentication | radius-accounting | radius-attributes | radius-server | stateful-authentication | timers | trusted-ap | vpn-authentication | web}

#### aaa bandwidth-contract

Configures the bandwith contract.

## Syntax

aaa bandwidth-contract <STRING> <kbits | mbits> <bandwidth>
 Where: STRING is the name of the bandwidth contract

kbits specifies the bandwith in kbits/second

mbits specifies the bandwith in mbits/second

<bandwidth> is the amount of bandwidth. Valid range is either 0-64 mbits/second or 0-65536 kbits/second

## Example

The following example sets the amount of bandwidth for the bandwidth contract named test to 48 mbits per second.

(AlcatelWireless LAN) (config) #aaa bandwidth-contract test mbits 48

## aaa captive-portal

Configures the Captive Portal.

# Syntax

aaa captive-portal {auth-server <string> <position> <range> | default-role <string> | guest-logon | login-page <string> | logon-wait <cpu-utilization> <%> | <range> <value> | logout-popup-window | max-authentication-failures <value> | protocol-http | redirect-pause <time> | show-fqdn | lsygate-on-demand <enable> <remediation-failure {role <name> | url <name>} | theme <name> | user-logon | welcome-page <string>}

where:

auth-serverAssigns the specified authentication server the order in which it is used. To assign highest order (position) enter 1.

default-roleSpecifies the default role.

guest-logonAllows guest log ins

login-page Specifies the name of the alternate login page HTML file.

logon-wait Configures a logon wait when the CPU is overloaded. Specify either the percentage of CPU utilization when a logon wait is to be enforced, or specify a number of seconds (range) to wait for captive portal logons. The minimum wait is one second.

logout-popup-windowOpens a popup window for logout after authentication.

max-authentication-failuresConfigures the maximum number of authentication failures before the user is blacklisted.

protocol-httpSpecifies the use of HTTP for authentication. The default is HTTPS.

redirect-pause Specifies the pause time in seconds for automatic redirect.

show-fqdnAllows the user to see and select the fully qualified domain name (FQDN).

sygate-on-demandConfigures the Sygate-on-demand agent.

themeSelected the theme for the captive portal page. Specify default1, default2, default3, or custom.

user-logonAllows registered users to log in.

welcome-pageSpecifies the complete URL to an alternate welcome page to show after authentication.

## Example

The following example shows how to blacklist any user unsuccessfully attempting more than three times to log onto the captive portal.

(Alcatel2400) (config) #aaa captive-portal max-authentication-failures 3



#### aaa derivation-rules server

Configures rules to derive user role or VLAN after successful authentication.

#### Syntax

aaa derivation-rules server <STRING>

where *STRING* is the name of the authentication server. (The server must have already been configured.)

## Example

(Alcatel6000) (config) #aaa derivation-rules server Alcatel

#### aaa derivation-rules user

Configures rules to derive user role or VLAN based on user attributes.

#### Syntax

aaa derivation-rules user

## Example

(Alcatel6000) (config) #aaa derivation-rules server user

#### aaa dot1x auth-server

Sets the Backend Authentication Server for 802.1X Authentication.

## Syntax

aaa dot1x auth-server <name>
where name is the name of the authentication server.

## Example

(Alcatel6000) (config) #aaa dot1x auth-server Alcatel

## aaa dot1x default-role

Assigns the default role.

## Syntax

aaa dot1x default-role STRING where *STRING* is the name of the default role.

## Example

(Alcatel6000) (config) #aaa dot1x default-role guest

## aaa dot1x enforce-machine-authentication

Configures machine authentication.

# Syntax

none

# Example

(Alcatel6000) (config) **#aaa dot1x enforce-machine-authentication** 

# aaa dot1x max-authentication-failure

Configures the maximum number of authentication failures before user is blacklisted.

# Syntax

aaa dot1x max-authentication-failures NUMBER

where *NUMBER* is the number of times a user can attempt to authenticate before being blacklisted. Valid range is .

# Example

(Alcatel6000) (config) #aaa dot1x max-authentication-failures 4

## aaa dot1x mode

Enables or disable 802.1X-based Authentication. Enable this mode to support WPA Key management using 802.1x.

# Syntax

aaa dot1x mode *<disable> <enable>* where *disable* turns of 802.1x authentication and *enable* turns it on.

# Example

(Alcatel6000) (config) #aaa dot1x mode enable

(Alcatel6000) (config) #aaa dot1x mode disable

## aaa kerberos <name>

Configures the name Kerberos Domain Controller (KDC) for Kerberos Authentication.

# Syntax

aaa kerberos <name> <domain-name> <host> <mode> <timeout>

where *name* is the name of the KDC., *domain-name* is the fully qualified domain name, *host* is the address of the KDC, *mode* enables or disables Kerberos authentication, *timeout* configures the time period allowed between Kerberos requests and responses. The valid range is 0-60 seconds.

# Example

(Alcatel6000) (config) #aaa kerberos Alcatel.com domain-name Alcatel.com host paul mode enable timeout 30



## aaa Idap-server

Configures an LDAP server.

## Syntax

aaa ldap-server *STRING* where *STRING* is the name of the LDAP server

## Example

(Alcatel6000) (config) #aaa ldap-server paul (Alcatel6000) (config-ldapserver-paul)#

#### aaa Idap-server admin-dn

Configures the administrator's Distinguished Name.

#### Syntax

admin-dn STRING

where STRING is the Distinguished Name.

## Example

(Alcatel6000) (config-ldapserver-paul)#admin-dn pauldn

(Alcatel6000) (config-ldapserver-paul)#

#### aaa ldap-server admin-passwd

Configures the password the for administrator.

## Syntax

admin-passwd [STRING] <cr >

where STRING is the password for the Admin user who can search for the LDAP user.

and <cr>

## Example

(Alcatel6000) (config-Idapserver-paul)#admin-passwd paul

(Alcatel6000) (config-ldapserver-paul)#

## aaa Idap-server allow-noencrypt

Syntax [no] allow-noencrypt Example

(Alcatel6000) (config-Idapserver-paul)#allow-noencrypt

(Alcatel6000) (config-Idapserver-paul)#

(Alcatel6000) (config-Idapserver-paul)#allow-noencrypt

## aaa Idap-server authport

Specifies the port number used for LDAP authentication. The default for LDAP over SSL is port 636. The default for SSL over LDAP is port 389.

#### Syntax

[no] authport INTEGER

where INTEGER is the port number to be used for authentication.

## Example

(Alcatel6000) (config-ldapserver-paul)#authport 65000

(Alcatel6000) (config-Idapserver-paul)#

#### aaa Idap-server base-dn

Configures the Base Distinguished Name used to search for the LDAP server.

## Syntax

base-dn STRING

where STRING is the Base Distinguished Name for searching the LDAP server.

limits, length, etc TBD.

## Example

(Alcatel6000) (config-ldapserver-paul)#base-dn paulbase

(Alcatel6000) (config-ldapserver-paul)#

#### aaa Idap-server filter

Defines the filter to be used as the key when searching for the LDAP server.

## Syntax

[no] filter STRING

where STRING is the filter that is used as a key when searching the LDAP server.

See also aaa Idap-server key-attribute



Example

(Alcatel6000) (config-ldapserver-paul)#filter filter

(Alcatel6000) (config-ldapserver-paul)#

## aaa Idap-server host

Specifies the IP address of the LDAP server.

#### Syntax

host STRING

where STRING is the IP address of the LDAP server.

## Example

(Alcatel6000) (config-Idapserver-paul)#host 192.11.2.0

(Alcatel6000) (config-ldapserver-paul)#

#### aaa Idap-server inservice

Enables the LDAP server as being in service.

#### Syntax

[no] inservice

#### Example

(Alcatel6000) (config-Idapserver-paul)#inservice

(Alcatel6000) (config-ldapserver-paul)#

#### aaa Idap-server key-attribute

Defines the attribute to be used as the key when searching for the LDAP server. Active Directory uses the key-attribute sAMAccountName.

#### Syntax

key-attribute keyattribute STRING

where STRING is the name of the attribute to be used as the key when searching the LDAP server.

#### Example

(Alcatel6000) (config-Idapserver-paul)#key-attribute keyattribute

(Alcatel6000) (config-ldapserver-paul)#

See also aaa Idap-server filter

#### aaa ldap-server mode

Enables or disables the LDAP server.

## Syntax

inservice

# Example

(Alcatel6000) (config-Idapserver-paul)#inservice

(Alcatel6000) (config-Idapserver-paul)#

#### aaa Idap-server no

Disables the following commands:

allow-noencrypt

authport

filter

inservice

timeout

See individual commands for more information.

#### aaa Idap-server timeout

Configures the LDAP request timeout. The default is 20 seconds.

## Syntax

[no] timeout <seconds>

where seconds is the timeout value in seconds. Valid range is 1-30 seconds.

# Example

(Alcatel6000) (config-Idapserver-paul)#timeout 25

(Alcatel6000) (config-ldapserver-paul)#

#### aaa mac-authentication auth-server

Configures the authentication server for MAC-based authentication.



#### syntax

aaa mac-authentication auth-server STRING position

where *STRING* is the name of the authentication server and *position* is the server priority. Valid range is . Specify 1 for the highest position. The default is lowest position.

#### Example

(Alcatel6000) (config) #aaa mac-authentication auth-server internal-db 5

#### aaa mac-authentication default-role

Configure the MAC-based authentication server default role.

#### syntax

aaa mac-authentication default-role STRING where *STRING* is the name of the default role.

## Example

(Alcatel6000) (config) #aaa mac-authentication default-role guest

#### aaa mac-authentication max-authentication-failures

Configures the number of times a user can attempt MAC-based authentication before being blacklisted.

#### syntax

(Alcatel6000) (config) #aaa mac-authentication max-authentication-failures NUMBER

where *NUMBER* is the number of times a user can attempt unsuccessfully to login before the system blocks them out by blacklisting them.

## Example

(Alcatel6000) (config) #aaa mac-authentication max-authentication-failures 4

#### aaa mac-authentication mode

Turns MAC-based authentication on or off.

#### syntax

(Alcatel6000) (config) #aaa mac-authentication mode <disable | enable> where enable turns MAC-based authentication on, and disable turns it off.

#### Example

To turn MAC-based authentication on, enter:

(Alcatel6000) (config) #aaa mac-authentication mode enable

## aaa mgmt-authentication auth-server

Configures administrator user authentication

## syntax

aaa mgmt-authentication auth-server STRING position

where *STRING* is the name of the authentication server and *position* is the server priority . Valid range is . Specify 1 for the highest position. The default is lowest position.

# Example

```
(Alcatel6000) (config) #aaa mgmt-authentication auth-server internal-db 5
```

## aaa mgmt-authentication default-role

Configures the default management role.

## syntax

aaa mgmt-authentication default-role STRING where *STRING* is the name of the default role.

# Example

(Alcatel6000) (config) #aaa mgmt-authentication default-role guest

## aaa mgmt-authentication mode

Turns the administrative authentication on or off.

## syntax

(Alcatel6000) (config) #aaa mgmt-authentication mode <disable | enable> where enable turns MAC-based authentication on, and disable turns it off.

# Example

To turn MAC-based authentication on, enter:

(Alcatel6000) (config) #aaa mgmt-authentication mode enable

# aaa pubcookie-authentication

Configures pubcookie authentication.

# Syntax

aaa pubcookie-authentication

# Example

(Alcatel6000) (config) #aaa pubcookie-authentication



#### aaa radius-accounting

Configures RADIUS accounting.

## Syntax

aaa radius-accounting

## Example

(Alcatel6000) (config) #aaa radius-accounting

#### aaa radius-attributes

Configure RADIUS attribute

#### Syntax

aaa radius-attributes add *STRING* INT <date | integer | ipaddr | string> [vendor <STRING > <INTEGER>]

where *STRING* is the name of the attribute to be added, *INT* is the attribute type of:

date Attribute type is Date

integer Attribute type is Integer

ipaddr Attribute type is IP address

string Attribute type is String

vendor STRING is the name of the vendor specific attribute, and INTEGER is the vendor Identifier.

## Example

The following example adds the RADIUS name-value pair: employee-type-admin.

(Alcatel6000) (config) #aaa radius-attributes add employee-type INT admin

#### aaa radius-server

Configures a RADIUS server.

## Syntax

(Alcatel6000) (config) #aaa radius-server STRING [acctport <port\_num> | authport
<port\_num> | host <hostname> | inservice | key <key\_name> | match-essid <essid> |
match-fqdn <fqdn> | mode <disable|enable> | nas-identifier <nas\_ID> | retransmit
<retransmit num> | timeout <timeout value> | trim-fqdn]

Chapter 29

where the options to this command are:

STRING specifies the name of RADIUS server.

acctport specifies the port number used for accounting

authport specifies the port number used for authentication (default is port 1812)

host specifies the IP address of the RADIUS server

inservice enables the server into service immediately

key specifies the shared secret text string

match-essid requires a match the specified ESSID

match-fqdn requires a match to the specified FQDN

mode enables or disables the use of the RADIUS server

nas-identifier configures the NAS-Identifier attribute in RADIUS packets

retransmit specifies the maximum number of times a RADIUS request is retried

timeout specifies the timeout period for RADIUS request. The default is 10 seconds.

trim-fqdn trims the FQDN from the user name before sending to server

<cr>

# Example

(Alcatel6000) (config) #aaa radius-server bigboy acctport 2550 authport 88 host 10.200.200.20 inservice key blue match-essid COFFEE match-fqdn Alcatel.COM mode enable nas-identifier 254 retransmit 3 timeout 30 trim-fqdn

#### aaa stateful-authentication dot1x ap-config

Configures the AP and Radius Server parameters for stateful inspection.



AOS-W Commands | 687

## Syntax

aaa stateful-authentication dot1x ap-config <name> ap-ipaddr radius-server-name <name> [key <keyvalue>]

Where

<name> is the configuration name

ap-ipaddr is the IP Address of AP (NAS) configured for 802.1X stateful authentication

radius-server-name is the name of the RADIUS Server used for stateful  $802.1 \ensuremath{\mathsf{X}}$  Authentication

key is the optional secret shared between AP and RADIUS Server

## Example

(Alcatel6000) (config) #aaa stateful-authentication dot1x ap-config paulconfig ap-ipaddr 1.1.2.3 radius-server-name paulserver key boo

#### aaa stateful-authentication dot1x auth-server

Configures the Backend Authentication Server for Stateful 80 2.1X authentication.

## Syntax

```
aaa stateful-authentication dot1x auth-server <auth-server-name>
    Where
```

<auth-server-name> is the name of the Backend Authentication server for stateful 802.1x authentication.

## Example

(Alcatel6000) (config) #aaa stateful-authentication dot1x auth-server paulauthser

(Alcatel6000) (config) #

## aaa stateful-authentication default-role

Assigns the default role for 802.1x stateful authentication.

## Syntax

aaa stateful-authentication dot1x default-role STRING

Where STRING is the label for the default role.

# Example

(Alcatel6000) (config) #aaa stateful-authentication dot1x default-role
pauldefrole
(Alcatel6000) (config) #

## aaa stateful-authentication mode

Enables or disables 802.1x stateful authentication.

# Syntax

aaa stateful-authentication dot1x mode <disable | enable >

Where:

disable turns this feature off

enable turns this feature on

<cr>

# Example

```
(Alcatel6000) (config) #aaa stateful-authentication dot1x mode enable
(Alcatel6000) (config) #
```

# aaa stateful-authentication dot1x timeout

Configures the allowed length of time allowed to elapse between receiving a RADIUS Request from a AP (NAS) and the response from the Authentication Server.

## Syntax

aaa stateful-authentication dot1x timeout <0-20>

Where

<0-20> is the valid range of time that can elapse in the reply

# Example

```
(Alcatel6000) (config) #aaa stateful-authentication dot1x timeout 10
(Alcatel6000) (config) #
```

## aaa stateful-authentication kerberos

Specifies Kerberos as the stateful authentication method.

**Syntax** aaa stateful-authentication kerberos enable



Example
(Alcatel6000) (config) #aaa stateful-authentication kerberos enable
(Alcatel6000) (config) #

Chapter 29

# aaa timers dead-time

Configure authenti	cation timers
(Alcatel6000) (conf	ig) #aaa timers ?
dead-time	Help not defined
idle-timeout	Set user idle timeout (in minutes)
logon-lifetime	Set maximum lifetime of unauthenticated users
(Alcatel6000) (conf	ig) #aaa timers dead-time ?
<1-60> [	Dead time in Minutes
(Alcatel6000) (conf <cr></cr>	ig) #aaa timers dead-time 30 ?
(Alcatel6000) (conf	ig) #aaa timers idle-timeout ?
<0-255>	Minutes. Value of 0 disables idle timeout.
(Alcatel6000) (conf <cr></cr>	ig) #aaa timers idle-timeout 50 ?
(Alcatel6000) (conf	ig) #aaa timers logon-lifetime ?
<1-255>	Minutes. Default is 5 minutes. 0 disables the timeout

(Alcatel6000) (config) #aaa timers logon-lifetime 20 ? <cr>

(Alcatel6000) (config) #aaa timers logon-lifetime 20



# aaa timers idle-timeout

(Alcatel6000) (config) #aaa timers ?		
dead-time	Help not defined	
idle-timeout	Set user idle timeout (in minutes)	
logon-lifetime	Set maximum lifetime of unauthenticated users	
(Alcatel6000) (con	fig) #aaa timers dead-time ?	
<1-60>	Dead time in Minutes	
(Alcatel6000) (con	fig) #aaa timers dead-time 30 ?	
<cr></cr>		
(Alcatel6000) (con	fig) #aaa timers idle-timeout ?	
<0-255>	Minutes. Value of 0 disables idle timeout.	
(Alcatel6000) (con	fig) #aaa timers idle-timeout 50 ?	
<cr></cr>		
(Alcatel6000) (con	fig) #aaa timers logon-lifetime ?	
<1-255>	Minutes. Default is 5 minutes. 0 disables the timeout	

(Alcatel6000) (config) #aaa timers logon-lifetime 20 ? <cr>

.

(Alcatel6000) (config) #aaa timers logon-lifetime 20

# aaa timers logon-lifetime

(Alcatel6000) (cont	fig) #aaa timers ?
dead-time	Help not defined
idle-timeout	Set user idle timeout (in minutes)
logon-lifetime	Set maximum lifetime of unauthenticated users
(Alcatel6000) (cont	fig) #aaa timers dead-time ?
<1-60>	Dead time in Minutes
(Alcatel6000) (cont	fig) #aaa timers dead-time 30 ?
<cr></cr>	
(Alcatel6000) (con	fig) #aaa timers idle-timeout ?
<0-255>	Minutes. Value of 0 disables idle timeout.
(Alcatel6000) (con	fig) #aaa timers idle-timeout 50 ?
<cr></cr>	
(Alcatel6000) (cont	fig) #aaa timers logon-lifetime ?
<1-255>	Minutes. Default is 5 minutes. 0 disables the timeout

(Alcatel6000) (config) #aaa timers logon-lifetime 20 ? <<r>

(Alcatel6000) (config) #aaa timers logon-lifetime 20



#### aaa trusted-ap

Configure trusted third party APs.

Syntax

aaa trusted-ap <mac-addr>

where <mac-addr> is the MAC address of the AP in A:B:C:D:E:F notation.

Example

(Alcatel6000) (config) #aaa trusted-ap 43:a:4:1:a:0

(Alcatel6000) (config) #

## aaa user fast-age

Configures fast aging with multiple instances of the same user (same MAC address).

Syntax

aaa user fast-age

Example

(Alcatel6000) (config) #aaa user fast-age

(Alcatel6000) (config) #

#### aaa vpn-authentication auth-server

Assigns an authentication server.

Syntax

(Alcatel6000) (config) #aaa vpn-authentication auth-server ?

STRING Name of authentication server

(Alcatel6000) (config) #aaa vpn-authentication auth-server paul ?

position Server Position. Default is lowest. 1 is highest.

<cr>

(Alcatel6000) (config) #aaa vpn-authentication auth-server paul position 4 ?

<cr>

(Alcatel6000) (config) #aaa vpn-authentication auth-server paul position 4

Example

## aaa vpn-authentication default-role

Assigns a default role.

## aaa vpn-authentication max-authentication-failures

Configures the maximum number of times a user can attempt to login unsuccessfully before being blacklisted.

## aaa vpn-authentication mode

Enables or disables VPN authentication.

#### aaa web

Web server configuration



Syntax

(Alcatel6000) (config) #aaa web admin-port https port number

where :

admin-port configures a port for Web administration

https specifies HTTPS protocol for the port

Port Number is the number of the HTTPS port. Valid range is 0-65535.

# Example

(Alcatel6000) (config) #aaa web admin-port https 6500

(Alcatel6000) (config) #

# aaa xml-api client

Configures the exernal XML API.

Syntax

aaa xml-api client IPaddress

where:

client Configure external XML API client

A.B.C.D IP address of external client

(Alcatel6000) (config) #aaa xml-api client 1.2.3.4

(Alcatel6000) (config) #

Example

(Alcatel6000) (config) #aaa xml-api client 1.2.3.4

(Alcatel6000) (config) #

# adp Commands

These commands control Access Point configuration and management using the Alcatel Discovery Protocol.

## adp

Enables the Automatic Discovery Protocol commands.

## adp discovery

Enables or disables ADP.

Syntax

(Alcatel6000) (config) # adp [discovery <disable | enable> | igmp-join <disable | enable> | igmp-vlan <vlanid>]

Where:

discovery enables or disables ADP

igmp-joine enables or disables IGMP Join for ADP IP Multicast addresses

igmp-vlan specifies which VLAN to send IGMP Reports to. Default 0. Uses default route VLAN.

# Example

(Alcatel6000) (config) # adp discovery enable igmp-join enable igmp-vlan
565
(Alcatel6000) (config) #

# ads Commands

## (Alcatel6000) (config) #ads ?

## netad

Configure Network Traffic Anomaly Detection (NETAD)

(Alcatel6000) (config) #ads netad ?

mode Specify NETAD mode

## (Alcatel6000) (config) #ads netad mode ?

- detect Run NETAD in anomaly detection mode
- disable Disable NETAD algorithms
- learn Run NETAD in learning mode



# (Alcatel6000) (config) #ads netad mode learn ?

<cr>

(Alcatel6000) (config) #ads netad mode detect ?

<cr>

(Alcatel6000) (config) #ads netad mode detect

(Alcatel6000) (config) #ads netad mode disable ?

<cr>

(Alcatel6000) (config) #ads netad mode disable

# ap Commands

Configures Access Points either by BSSID or by location.

## ap bssid

Configures APs by their MAC address (BSSID).

## Syntax

```
ap bssid <bssid>
Where:
<bssid> specifies the BSSID in typical MAC address format:
AA:BB:CC:DD:EE:FF
```

# Example

(Alcatel6000) (config) #ap bssid 00:00:00:01:02:ff

(Alcatel6000) (config) #ap bssid 00:00:00:01:02:ff
## ap location

Accesses the AP location mode.

# arm Commands

Configures the Adaptive Radio Management commands.

# Syntax

arm [acceptable-coverage-index <index> | backoff-time <backoff time> | error-rate-threshold <threshold value> | error-rate-wait-time <wait time> | free-channel-index <free channel index value> | ideal-coverage-index <coverage index value> | min-scan-time <scan time> | wait-time <wait time value> ] <cr>]



Where:

Option acceptable-coverag e-index <index></index>	<b>Description</b> This specifies to the AP how good the coverage in on this channel should be. The range is .
backoff-time <backoff time=""></backoff>	The default is 2. In general, the more APs there are in a given area, the lower this number should be. Specifies how long (in seconds) the AP should wait after asking for a new channel or power setting. The default is 230 seconds. Range . Specifies the minimim percentage of errors in traffic on a
error-rate-threshold <threshold value=""></threshold>	channel the AP experiences before it should change channels. The default is 0% but Alcatel recommends a setting of 50%. Range is 0-100%.
error-rate-wait-time	Speifies how long the AP experiences high error rates.
free-channel-index <free channel="" index<br="">value&gt;</free>	Specifies how much better the new channel must be (in terms of interference) before the AP will switch to the new channel.
ideal-coverage-inde	The higher the value, the lower the likehood that an AP will move to the new channel. The default is 25. Specifies what the ideal coverage (as opposed to the
x <coverage index<br="">value&gt; min-scan-time <scan time=""></scan></coverage>	denser the AP deployment, lower this value should be. The default is 5. In general, the more APs there are in a given area, the lower this number should be. Specifies the least amount of time an AP must scan a channel before determining if it is suitable to switch to
x <coverage index<br="">value&gt; min-scan-time <scan time=""> noise-threshold</scan></coverage>	denser the AP deployment, lower this value should be. The default is 5. In general, the more APs there are in a given area, the lower this number should be. Specifies the least amount of time an AP must scan a channel before determining if it is suitable to switch to Specifies how much noise can exist on a channel before the AP must switch to another channel. The default is 0 but Alcatel recommends 80

# Example

(Alcatel6000) (config) #arm acceptable-coverage-index 2 arm backoff-time 230 arm error-rate-threshold 3 arm error-rate-wait-time 50 arm free-channel-index 30 arm ideal-coverage-index 2 arm min-scan-time 30 arm wait-time 40

# arp

Adds a static Address Resolution Protocol entry to the routing table.

# Syntax

arp <ipaddr> <mac>

where:

<ipaddr> is the IP address of the device to be added to the ARP table.

<mac> is the 48-bit hardware address of the device, entered in the following format:

xx:xx:xx:xx:xx:xx

# Example

(Alcatel6000) (config) #arp 64.121.71.218 00:00:01:01:02:ae

**NOTE**— If the IP address does not belong to a valid IP subnet, the ARP entry will not be added. If the IP interface that defines the subnet for the static ARP entry is deleted, you will be unable to use the arp command to overwrite the entry's current values. Do a **no arp** *a.b.c.d*, and then issue the new arp command.

# banner motd

Creates a message (the Message Of The Day, or motd) that allusers see when logging into the CLI.

# Synatx

banner motd <delimiter> <message body>

where:

delimiter is a character that ends the message creation session and returns to the prompt.

# Example

In the following exmaple, the letter E (capital E) terminates the entering of the message text and returns to the CLI prompt.

(Alcatel6000) (config) **#banner motd E** Enter TEXT message. End with the character 'E'.

Hello TuesdayE



```
(Alcatel6000) (config) #
```

## clock Commands

Configures the Wireless LAN Switch's clock to show the Switch's timezone and to toggle to Daylight Saving Time as appropriate for the timezone setting.

#### clock summer-time

Configures the start of summer (daylight saving) time.

#### Syntax

```
clock summer-time <WORD> recurring [<1-4>|first|last>] [day] [month]
{hh:mm] [<1-4>|first|last>] [day] [month] {hh:mm] [<-23-23] [<0-59>] <cr>
    where:
```

<WORD> is the label of the timezone. This label should be no less than three and no more than five characters long and should not start with a colon (:).'

recurring specifies that the Switch should start daylight saving time everytime the starting specifications are met.

 $[<1-4>| \mbox{first}| \mbox{last}>] [day] [month] {hh:mm} specifies the week, day of the week, month, and exact hour that the switch to daylight saving time should start.$ 

 $[<1-4>| \mbox{first}| \mbox{last}>] [day] [month] {hh:mm} specifies the week, day of the week, month, and exact hour that the switch to daylight saving time should end.$ 

<-23 - 23> is the number of hours offset from UTC.

<0-59> is the number of minutes of offset from UTC.

#### Example

The following example specifies that daylight saving time should start the first Sunday in April at 2 AM and end the last Sunday in October also at 2 AM. The timezone is Pacific Standard Time and the offset from Grenwhich time is -8 hours.

(Alcatel6000) (config) # clock summer-time PST recurring 1 Sunday April
02:00 4 Sunday )October 02:00 -8 0
(Alcatel6000) (config) #

**NOTE**—Be sure to configure clock timezone when configuring summer-time.

#### clock timezone

Configures the time zone in which the Switch is located.

## Syntax

```
clock summer-time <WORD> [<-23-23] [<0-59>] <cr>
where:
```

<WORD> is the label of the timezone. This label should be no less than three and no more than five characters long and should not start with a colon (:).'

<-23 - 23> is the number of hours offset from UTC.

<0-59> is the number of minutes of offset from UTC.

#### Example

The following example configures the timezone label to show PST and sets this timezone to be 8 hours behind Grenwhich time.

```
(Alcatel6000) (config) # clock timezone PST -8 0
(Alcatel6000) (config) #
```

# crypto Commands

Configures the cryptographic settings including IPSec tunnels, ISAKMP keys, and dynamic maps.

#### crypto dynamic-map

Configure Dynamic Maps commands in crypto dynamic-map mode.



#### syntax

dynamic-map <dynamic-map-name> <dynamic-map-number> <nolset<pfs> <group>lsecrity-association <lifetime> <seconds> ltransform-set >>

where:

<dynamic-map-name> is the name of the dynamic-map to create or modify

<dynamic-map-number> is the priority of the map. Valid range is 1 - 10000

no disables the specified command

set enables one of:

pfs enables Perfect Forward Secrecy mode for group 1 (768-bit Diffie Hellman prime modulus group) or group2 (1024-bit Diffie Hellman prime modulus group). security-association configures the Security Association by specifying the life-time with a valid range of 300 to 86400 seconds.

transform-set configures a Transform Set for this dynamic map. Specify up to four transform sets.

#### Example

(Alcatel6000) (config) #crypto dynamic-map PAULMAP 6655

(Alcatel6000) (config-crypto-map)#

(Alcatel6000) (config-crypto-map)# set pfs group2

(Alcatel6000) (config-crypto-map)# set security-association lifetime seconds 300

(Alcatel6000) (config-crypto-map)# set transform-set PAULTransform PaulTransform2 trans3 tras4 ?

The following command disable dynamic-map configurations:

(Alcatel6000) (config-crypto-map)# no set pfs

(Alcatel6000) (config-crypto-map)# no set transform-set

(Alcatel6000) (config-crypto-map)# no set security-association lifetime

#### crypto ipsec

Configure IPSec paramters.

## Syntax

crypto ipsec <mtu> <size> l < transform-set> <transform-set-name> <encryption> <auth>

Where:

mtu configures the IPSec MTU

transform-set configures a transform set to support:

ESP with 168-bit Triple DES encryption, or

ESP with 128-bit AES encryption, or

ESP with 192-bit AES encryption, or

ESP with 256-bit AES encryption, or

ESP with 56-bit DES encryption

and

ESP with the MD5 (HMAC variant) authentication algorithm, or

ESP with the SHA (HMAC variant) authentication algorithm

(Alcatel6000) (config) #crypto ipsec transform-set PaulTrans esp-3des esp-sha-hmac

(Alcatel6000) (config) #

#### isakmp

Configures the IETF's Internet Security Association and Key Management Protocol.

#### Syntax

crypto isakmp <address> <disable> <enable> <groupname> <key> <policy>

Where:

address	Configure the IP for the group key
disable	Disable the IKE processing
enable	Enable the IKE processing
groupname	Configure IKE Aggressive group name
key	Configure the IKE PRE-SHARED key
policy	Configure an IKE policy mode commands.



(Alcatel6000)	(config)	#crypto	isakmp	?
---------------	----------	---------	--------	---

address	Configure the IP for the group key
disable	Disable the IKE processing
enable	Enable the IKE processing
groupname	Configure IKE Aggressive group name
key	Configure the IKE PRE-SHARED key
policy	Configure an IKE policy

(Alcatel6000) (config) #crypto isakmp address ?

<peer-address> Configure the IP for the group key

(Alcatel6000) (config) #crypto isakmp address 10.25.5.34 ?

netmask Configure the IP netmask for the group key

(Alcatel6000) (config) #crypto isakmp address 10.25.5.34 netmask 255.255.255.0 ?

<cr>

(Alcatel6000) (config) #crypto isakmp address 10.25.5.34 netmask 255.255.255.0

Key:\*

Mismatch between mask and network address

(Alcatel6000) (config) #

(Alcatel6000) (config) #crypto isakmp address 10.25.5.34 netmask 255.255.255.255

Key:\*\*\*\*\*\*\*\*\*

Re-Type Key:\*\*\*\*\*\*\*\*\*

Not Supported

(Alcatel6000) (config) #(Alcatel6000) (config) #crypto isakmp ?addressConfigure the IP for the group keydisableDisable the IKE processingenableEnable the IKE processinggroupnameConfigure IKE Aggressive group namekeyConfigure the IKE PRE-SHARED keypolicyConfigure an IKE policy

(Alcatel6000) (config) #crypto isakmp disable ?

<cr>

(Alcatel6000) (config) #crypto isakmp disable

(Alcatel6000) (config) #crypto isakmp?

address	Configure the IP for the group key
disable	Disable the IKE processing
enable	Enable the IKE processing
groupname	Configure IKE Aggressive group name
key	Configure the IKE PRE-SHARED key
policy	Configure an IKE policy

(Alcatel6000) (config) #crypto isakmp enable

(Alcatel6000) (config) #crypto isakmp enable ? <cr>

(Alcatel6000) (config) #crypto isakmp enable



(Alcatel6000) (config) #crypto isakmp groupname ?
<name> Configure IKE Aggressive group name

(Alcatel6000) (config) #crypto isakmp groupname paul ? <cr>

(Alcatel6000) (config) #crypto isakmp groupname paul

(Alcatel6000) (config) #crypto isakmp key ?

<keystring> Configure the value of the IKE PRE-SHARED key, must b e between 6-64 characters

(Alcatel6000) (config) #crypto isakmp key 111111111 % Incomplete command.

(Alcatel6000) (config) #crypto isakmp key 1111111111?

address Configure the IP for the group key

(Alcatel6000) (config) #crypto isakmp key 1111111111 10.100.101.102 ?

(Alcatel6000) (config) #crypto isakmp key 1111111111 10.100.101.102

^

% Invalid input detected at '^' marker.

(Alcatel6000) (config) #crypto isakmp key 1111111111?

address Configure the IP for the group key

(Alcatel6000) (config) #crypto isakmp key 1111111111 address ?

<peer-address> Configure the IP for the group key

(Alcatel6000) (config) #crypto isakmp key 1111111111 address 100.100.100.1 % Incomplete command.

(Alcatel6000) (config) #crypto isakmp key 1111111111 address 100.100.100.1 ?

netmask Configure the IP netmask for the group key

(Alcatel6000) (config) #crypto isakmp key 1111111111 address 100.100.100.1 netmask ?

<mask> Configure the IP netmask for the group key

(Alcatel6000) (config) #crypto isakmp key 1111111111 address 100.100.100.1 netmask 255.255.255.255 ?

<cr>

(Alcatel6000) (config) #crypto isakmp key 1111111111 address 100.100.100.1 netmask 255.255.255.255

(Alcatel6000) (config) #

(Alcatel6000) (config) #crypto isakmp policy 6655

(Alcatel6000) (config-isakmp)# ?

authentication Configure the IKE authentication method

encryption Configure the IKE encryption algorithm

- group Configure the IKE Diffie Hellman group
- hash Configure the IKE hash algorithm
- lifetime Configure the IKE lifetime in seconds

(Alcatel6000) (config-isakmp)# authentication ?



pre-share	Use Pre Shared Keys for IKE authentication
rsa-sig	Use RSA Signatures for IKE authentication

(Alcatel6000) (config-isakmp)# authentication pre-share ? <<r>

(Alcatel6000) (config-isakmp)# authentication rsa-sig ? << r>

(Alcatel6000) (co	nfig-isakmp)# encryption ?
3DES	Use 168-bit 3DES-CBC encryption algorithm
AES128	Use 128-bit AES-CBC encryption algorithm
AES192	Use 192-bit AES-CBC encryption algorithm
AES256	Use 256-bit AES-CBC encryption algorithm
DES	Use 56-bit DES-CBC encryption algorithm

(Alcatel6000) (config-isakmp)# encryption 3deS ?

<cr>

(Alcatel6000) (config-isakmp)# group ?

- 1 Use the 768-bit Diffie Hellman prime modulus group
- 2 Use the 1024-bit Diffie Hellman prime modulus group

(Alcatel6000) (config-isakmp)# group 1 ?

<cr>

(Alcatel6000) (config-isakmp)# hash ?

md5	Use MD5 (HMAC variant) as the hash algorithm
sha	Use SHA-1 (HMAC variant) as the hash algorithm

(Alcatel6000) (config-isakmp)# hash md5 ? <cr>

(Alcatel6000) (config-isakmp)# lifetime ?

<seconds> [300 - 86400] seconds

(Alcatel6000) (config-isakmp)# lifetime 301 ? <<r>

(Alcatel6000) (config-isakmp)# lifetime 301

(Alcatel6000) (config-isakmp)# ?

authentication	Configure the IKE authentication method
encryption	Configure the IKE encryption algorithm
group	Configure the IKE Diffie Hellman group
hash	Configure the IKE hash algorithm
lifetime	Configure the IKE lifetime in seconds

(Alcatel6000) (config-isakmp)#

#### map

Configures the crypto map.

#### syntax

crypto map <global-map > <map-number> <ipsec-isakmp> <dynamic> <dynamic-map-name>



Where:

<global map> configures the default global map <map-number> defines the priority of the map ipsec-isakmp specifies the IPSec map dynamic specifies the use of a dynamic map <dynamic-map-name> specifies the name of the dynamic map

## Example

(Alcatel6000) (config) # crypto map global-map 5 ipsec-isakmp dynamic Paulmap (Alcatel6000) (config) #

# database synchronize

Synchronizes the internal database or RF Plan data on redundant master switches.

(Alcatel6000) (config) #database ?

#### Syntax

database synchronize <period> <interval> | rf-plan-data

Where:

<period> Specifes that the syncrhonization with standby (Master-Master Communication) should happen every <time> seconds. Valid interval range is 1-25200 minutes.

rf-plan-data Include RF Plan data when synchronising with standby

#### Example

(Alcatel6000) (config) #database synchronize period 60

(Alcatel6000) (config) #

(Alcatel6000) (config) #database synchronize rf-plan-data

(Alcatel6000) (config) #

# destination

## Syntax

destination STRING <IP address><subnet mask> [invert | <cr>]

Where:

STRING is the name of destination host or subnet

IP address is the IP Address of destination host or subnet

<subnet mask> is the subnet mask of the destination host

invert Specifies to use all destinations EXCEPT this destination

# Example

(Alcatel6000) (config) #destination farleytech 67.121.71.218

(Alcatel6000) (config) #destination farleytech 67.121.71.218 invert

(Alcatel6000) (config) #

# dot1x Commands

Controls the 802.1x configuration which includes the following commands:

default	Set global 802.1X parameters to default values
framed-mtu	Set the Framed-MTU attribute sent to the
authentication server	
key-retries	Set the number of retries for the unicast and
multica	
	st key rotation message
key-size	Set the Dynamic WEP Key Size, Default Key Size
is 128	
	-Bit
max-req	Set maximum number of identity requests
multicast-keyrotation	Enable Multicast WEP Key Rotation
opp-key-caching	Enable Opportunistic Key Caching
re-authentication	Enable periodic 802.1X authentication
reauth-max	Maximum number of reauthentication attempts
server	Set authentication server parameters



timeout	Set 802.1X timeout values
unicast-keyrotation	Enable Unicast key Rotation
use-session-key	Use Radius Session Key as the Unicast WEP key
use-static-key	Use static key
wired-clients	Enable 802.1x for wired supplicants
wpa-key-retries	Set the number of retries for the wpa key
handshake	
xSec-MTU	xSec MTU

#### dot1x default

Sets global 802.1X parameters to their default values.

Syntax dot1x default

### Example

```
(Alcatel6000) (config) # dot1x default
(Alcatel6000) (config) #
```

#### dot1x framed-mtu

Sets the Framed-MTU attribute that is sent to the authentication server,

#### Syntax

```
dot1x framed-mtu <mtu-size>
    where
```

<mtu-size> is the size of the Frame MTU. Valid range is 400 to 1500 bytes.

#### Example

```
(Alcatel6000) (config) # dot1x framed-mtu 555
(Alcatel6000) (config) #
```

#### dot1x key-retries

Sets the number of retries for the unicast and multicast key rotation message

#### Syntax

```
dot1x key-retries <number>
```

where

<number> is the number of times the system will . Valid range is 1-3.

### Example

```
(Alcatel6000) (config) # dot1x key-retries 3
(Alcatel6000) (config) #
```

## dot1x key-size

Set the Dynamic WEP Key Size.

# Syntax

dot1x key-size <128> |<40>

where

128 specifies the 128-bit key (the default)

40 specifies the 40-bit key

# Example

(Alcatel6000) (config) # dot1x key-size 40

(Alcatel6000) (config) # dot1x key-size 128
(Alcatel6000) (config) #

### dot1x max-req

Sets the maximum number of identity requests.

## Syntax

dot1x max-req <retry>

where

<retry> is the number of retries. Valid range is 1-10.

# Example

(Alcatel6000) (config) # dot1x max-req 5
(Alcatel6000) (config) #

## dot1x multicast-keyrotation

Enable Multicast WEP Key Rotation

Syntax dot1x multicast-keyrotation

# Example

(Alcatel6000) (config) # dot1x multicast-keyrotation
(Alcatel6000) (config) #

## dot1x opp-key-caching

Enable Opportunistic Key Caching



Syntax dot1x opp-key-caching ?

### Example

(Alcatel6000) (config) # dot1x opp-key-caching
(Alcatel6000) (config) #

#### dot1x re-authentication

Enables periodic 802.1X authentication.

#### Syntax

```
dot1x opp-key-caching
```

### Example

```
(Alcatel6000) (config) # dot1x opp-key-caching
(Alcatel6000) (config) #
```

#### dot1x reauth-max

Maximum number of reauthentication attempts

#### Syntax

ot1x reauth-max <auth-count>

where

<auth-count> specifies the value of maximium authentication count.

### Example

```
(Alcatel6000) (config) # dot1x reauth-max 3
(Alcatel6000) (config) #
```

#### dot1x server

Sets authentication server parameters.

#### Syntax

dot1x server <server-retry><number> l<server-timeout> <timeout>

where:

<server-retry> Set the maximum number of authentication requests

<number> is the number of retries. Valid rage is 0-3.

server-timeout Set the authentication server timeout

timeout specifies the timeout in seconds. Valid range is 1-65535 seconds.

```
(Alcatel6000) (config) # dot1x server server-retry 3
(Alcatel6000) (config) #
(Alcatel6000) (config) # dot1x server server-timeout 244
(Alcatel6000) (config) #
```

## dot1x timeout idrequest-period

Sets 802.1X timeout period between identification requests.

# Syntax

dot1x timeout idrequest-period <1-65535>

where

<1-65535> is the number of seconds between requests.

# Example

```
(Alcatel6000) (config) # dot1x timeout idrequest-period 2
(Alcatel6000) (config) #
```

## dot1x timeout mcastkey-rotation-period

Set 802.1X time period betweeen multicast key rotations.

## Syntax

dot1x timeout mcastkey-rotation-period <period>

where:

<period> is the rotation period in seconds. Valid range is 60-2147483647
seconds.

# Example

```
(Alcatel6000) (config) # dot1x timeout mcastkey-rotation-period 333
(Alcatel6000) (config) #
```

## dot1x timeout quiet-period

Sets the 802.1X quiet period following failed authentication.

## Syntax

#dot1x timeout quiet-period <period>

where:

<period> is the number of seconds the quiet period lasts. Valid range is
1-65535 seconds.



(Alcatel6000) (config) # dot1x timeout quiet-period 22
(Alcatel6000) (config) #

#### dot1x timeout reauth-period

Sets the 802.1X time period between reauthentication attempts.

#### Syntax

dot1x timeout reauthperiod <period | server>

where:

<period> is the length of the reauthentiation period in seconds. Valid range is 60-2147483647 seconds.

server specifies the use of the server provided reauthentication interval

#### Example

(Alcatel6000) (config) # dot1x timeout reauthperiod server

(Alcatel6000) (config) # dot1x timeout reauthperiod 500
(Alcatel6000) (config) #

#### dot1x timeout ucastkey-rotation-period

Sets the 802.1X time period between unicast key rotations.

#### Syntax

dot1x timeout ucastkey-rotation-period <period>

where:

<period> is the number of seconds between unicast key rotations. Valid range is 60-2147483647 seconds.

#### Example

```
(Alcatel6000) (config) # dot1x timeout ucastkey-rotation-period 232
(Alcatel6000) (config) #
```

#### dot1x timeout wpa-key-timeout

Sets the 802.1X timeout values for each WPA key exchange.

# Syntax

dot1x timeout wpa-key-timeout <period>

where:

<period> is the timeout in seconds for each WPA key exchange. Valid range is
1-5 seconds.

# Example

```
(Alcatel6000) (config) # dot1x timeout wpa-key-timeout 4
(Alcatel6000) (config) #
```

## dot1x unicast-keyrotation

Enables Unicast Key Rotation.

Syntax

dot1x unicast-keyrotation

# Example

(Alcatel6000) (config) # dot1x unicast-keyrotation
(Alcatel6000) (config) #

### dot1x use-session-key

Use Radius Session Key as the Unicast WEP key.

## Syntax

dot1x use-session-key

# Example

```
(Alcatel6000) (config) # dot1x use-session-key
(Alcatel6000) (config) #
```

### dot1x use-static-key

Uses a static key.

## Syntax

dot1x use-static-key

# Example

(Alcatel6000) (config) # dotlx use-static-key
(Alcatel6000) (config) #

## dot1x wired-clients

Enable 802.1x for wired supplicants



Syntax dot1x wired-clients

## Example

(Alcatel6000) (config) # dot1x wired-clients
(Alcatel6000) (config) #

#### dot1x wpa-key-retries

Set the number of retries for the WPA key handshake.

#### Syntax

dot1x wpa-key-retries <number>

where:

<number> is the WPA Key Retry Count. Valid range is 1-5.

### Example

(Alcatel6000) (config) # dot1x wired-clients 5
(Alcatel6000) (config) #

#### xSec-MTU

Specifies the xSec MTU.

#### Syntax

dot1x xSec-MTU <number>

where:

<number> is the size of the xSEC MTU. Valid MTU sizes are from 1024-1500 bytes.

### Example

```
(Alcatel6000) (config) # dot1x xSec-MTU 1200
(Alcatel6000) (config) #
```

### enable

Configures the enable-level password.

#### Syntax

enable <password:> <re-typed password>

where <password> and <re-typed password> is the new enable-level password.

```
(Alcatel6000) (config) # enable
Password:*****
Re-Type password:*****
(Alcatel6000) (config) #
```

# encrypt

Enables encryption on the switch.

# Syntax

encrypt <disable | enable>

# Example

To turn on encryption, enter:

```
(Alcatel6000) (config) # encrypt enable
(Alcatel6000) (config) #
```

# firewall Commands

Use these commands to configure the firewall.

## firewall allow-tri-session

Allow three way session when performing destination NAT.

## Syntax

firewall allow-tri-session

# Example

(Alcatel2400) (config) #firewall allow-tri-session

(Alcatel2400) (config) #

## firewall attack-rate ping

Configures the firewall to monitor ping attacks.

# Syntax

firewall attack-rate ping <number>
where
<number>



is the number of pings per second allowed. Higher number of pings per second are deemed to be an attack. Valid range is 1-255 pings per second.

### Example

#### firewall attack-rate session

Configures the firewall to monitor the number of IP sessions.

#### Syntax

firewall attack-rate session <number>
where
<number> is the limit of the number of IP sessions that can occur. Higher
numbers of IP sessions than this limit are considered an attack. Valid
range is 1-255 IP sessions per second.

## Example

(Alcatel2400) (config) #firewall attack-rate session 33

(Alcatel2400) (config) #

#### firewall attack-rate tcp-syn

Configures the firewall to monitor SYN attacks.

### Syntax

firewall attack-rate tcp-syn <number> where <number> is the threshold above which incoming TCP SYN traffic will be considered an attack. Valid range is 1-255 SYN messages per second.

## Example

(Alcatel2400) (config) #firewall attack-rate tcp-syn 44

(Alcatel2400) (config) #

#### firewall deny-inter-user-bridging

Disallow forwarding non-IP frames between untrusted users .

### Syntax

firewall deny-inter-user-bridging

(Alcatel2400) (config) #firewall deny-inter-user-bridging

(Alcatel2400) (config) #

# firewall disable-ftp-server

Disables the FTP server.

Syntax (firewall disable-ftp-server

# Example

(Alcatel2400) (config) # firewall disable-ftp-server

(Alcatel2400) (config) #

## firewall disable-stateful-sip-processing

Disable stateful SIP processing. Default is enabled.

**Syntax** firewall disable-stateful-sip-processing

# Example

(Alcatel2400) (config) # firewall disable-stateful-sip-processing

(Alcatel2400) (config) #

# firewall drop-ip-fragments

Drops all IP fragments.

Syntax firewall drop-ip-fragments

# Example

(Alcatel2400) (config) # firewall drop-ip-fragments

(Alcatel2400) (config) #



#### firewall enable-per-packet-logging

Enable per-packet logging. Default is per-session logging.

#### Syntax

firewall enable-per-packet-logging

## Example

(Alcatel2400) (config) #firewall enable-per-packet-logging (Alcatel2400) (config) #f

#### firewall enforce-tcp-handshake

Enfroce TCP handshake before allowing data

#### Syntax

firewall enforce-tcp-handshake

## Example

(Alcatel2400) (config) #firewall enforce-tcp-handshake

(Alcatel2400) (config) #

### firewall log-icmp-error

Log all received ICMP errors.

#### Syntax

firewall log-icmp-error

## Example

(Alcatel2400) (config) #firewall log-icmp-error

(Alcatel2400) (config) #

### firewall prohibit-ip-spoofing

Prohibits IP spoofing.

#### Syntax

firewall prohibit-ip-spoofing

(Alcatel2400) (config) #firewall prohibit-ip-spoofing

(Alcatel2400) (config) #

# firewall prohibit-rst-replay

Prohibits TCP RST replay attack.

# Syntax

firewall prohibit-rst-replay

# Example

(Alcatel2400) (config) #firewall prohibit-rst-replay

(Alcatel2400) (config) #

# firewall session-mirror-destination

Configures a destination for a mirrored session.

# Syntax

```
firewall session-mirror-destination ip-address <ipaddr>
where
<ipaddr> is the IP address of the device acting as the mirror
destination
```

# Example

```
(Alcatel2400) (config) # firewall session-mirror-destination ip-address
1.1.1.1
(Alcatel2400) (config) #
```

# foreign-agent

Accesses the foreign-agent mode commands ((Alcatel6000) (config-fa) #).

# secure delete

Removes the specified Foreign-agent Home-agent security association.



Syntax

secure delete <spi\_value>

where

<spi\_value> is the Security Parameter Index greater than 256.

## Example

(Alcatel2400) (config-fa) #secure delete 400

(Alcatel2400) (config-fa) #exit

(Alcatel2400) (config) #

#### secure host

Configures the security association parameters between the foreign agent and the home agent

#### Syntax

secure host <ip> spi <spi\_value> shared-secret <shared\_secret>

where:

<ip> is the IP address of the home agent

<spi\_value> Is the SPI number - an integer greater than 256.

<shared\_secret> Is the shared serect, a string no more than 32 characters
long

### Example

```
(Alcatel6000) (config-fa) # secure host 192.168.1.10 spi 5500 shared-secret paul
(Alcatel6000) (config-fa) # exit
(Alcatel6000) (config) #
```

## home-agent

Accesses the home-agent command mode ((Alcatel6000) (config-ha)).

#### secure-foreign delete

Deletes the home-agent-foreign-agent security association.

## Syntax

home-agent delete <spi\_value>

where:

<spi\_value> is the number of the Security Parameter Index. This is an integer greater than 256.

## Example

(OAW-Wireless LAN) (config-ha) #secure-foreign delete 400

#### secure-foreign spi

Configures the security association parameters between the home agent and the foreign agent.

## Syntax

secure-foreign spi <spi\_value> host <ipaddr> shared\_secret <secret>

where:

<spi\_value> is the number of the Security Parameter Index. This is an integer greater than 256.

host <ipaddr> specifies thelP address of foreign agent

shared-secret is the shared secret between the HA and FA and is a string no longer than 32 characters.

# Example

```
(Alcatel6000) (config-ha) #secure-foreign spi 5500 host 192.168.2.2
shared-secret paul
(Alcatel6000) (config-ha) #exit
(Alcatel6000) (config)#
```

# hostname

Configures the name string that appears in the system prompt.



Syntax

hostname <hostname>

where:

<hostname> Specifies the hostname

## Example

(Alcatel6000) (config-ha) #hostname labtest

(labtest) >

**NOTE**— When you change the hostname you are returned to Exec mode and must log back in.

# Interface Commands

Allows access to the interface type commands. This release supports the following interfaces:

- FastEthernet IEEE 802.3
- GigabitEthernet
- Loopback
- Management (Ethernet)
- Tunnel
- VLAN

#### interface fastethernet <slot/port>

Accesses the FastEthernet mode which allows you to configure the Fastethernet interface for the specified port on the specified slot.

#### Syntax

```
interface fastethernet <slot/port>
    where:
```

slot is the chassis slot of the module to be configured Range is

port is the specific port on the module to be configured. Range is:

#### Example

```
(switch) (config) # interface fastethernet 1/1
(switch) (config-if) #
```

## description

# Syntax

description <text>

where

line> is a text lable. Lables can be up to

# Example

```
(Alcatel6000) (config-if)# description this_is_a test
(Alcatel6000) (config-if)#
```

# duplex

Configures the interface to support duplex and half duplex traffic.

# Syntax

```
duplex <auto | full | half>
    where
```

auto configures the interface to automatically adjust to full or half duplex transmissions based on the traffic requirements.

full configues the interface to support full duplex traffic.

half configures the interface to support half-duplex traffic.

# Example

(Alcatel6000) (config-if)# duplex auto

(Alcatel6000) (config-if)#

### ip

Configures the IP parameters for this FastEthernet port.

# Syntax

```
ip access-group <name> <in | out | session>
    where
```

<name> is the name of this access control list (ACL). .

 $\verb"in|out|session"$  applies the ACL to incoming, outgoing, or this session only traffic.

# Example

```
(Alcatel6000) (config-if)# ip access-group test session
(Alcatel6000) (config-if)#
```



## muxport

Configures Mux functionality on the port.

## Syntax

where

# Example

(Alcatel6000) (config-if)#

## interface fastethernet <slot/port>

no Delete Command

Syntax

where

# Example

(Alcatel6000) (config-if)#

# interface fastethe

## Syntax

where

### (Alcatel6000) (config-if)#

rnet <slot/port>

poe Power Over Ethernet

### interface fastethernet <slot/port>

port Perform switch port configuration

Syntax

where

# Example

(Alcatel6000) (config-if)#

## interface fastethernet <slot/port>

shutdown Shut down the selected interface

Syntax

where

# Example

(Alcatel6000) (config-if)#



#### interface fastethernet <slot/port>

snmp Modify SNMP interface parameters

Syntax

where

Example

(Alcatel6000) (config-if)#

### interface fastethernet <slot/port>

spanning-tree Spanning Tree subsystem

Syntax

where

Example

(Alcatel6000) (config-if)#

## interface fastethernet <slot/port>

speed Configure Speed Operation

# Syntax

where

# Example

(Alcatel6000) (config-if)#

# interface fastethernet <slot/port>

switchport Set the switching mode characteristics

Syntax

where

# Example

(Alcatel6000) (config-if)#

## interface fastethernet <slot/port> trusted

trusted Make this a trusted port

Syntax

where



(Alcatel6000) (config-if)#

### interface fastethernet <slot/port> trusted

xsec Xtreme Security enabled on the port

Syntax

where

## Example

(Alcatel6000) (config-if)#

### interface gigabitethernet

GigabitEthernet Interface

Syntax

## Example

interface loopback Loopback Interface

### interface mgmt

Management Ethernet Interface

## Syntax
# Example

### interface port-channel

Ethernet channel of interfaces

Syntax

Example

interface range

interface tunnel

Syntax

Example

## interface vlan Switch VLAN Virtual Interface

(switch) (config-if)#

(Alcatel6000) (config) #interface gigabitethernet ?

<slot/port> GigabitEthernet Interface is <slot>/<port> format

(Alcatel6000) (config) #interface gigabitethernet 1/0

(Alcatel6000) (config-if)#

(Alcatel6000) (config) #interface loopback ?



<cr>

(Alcatel6000) (config) #interface loopback

(Alcatel6000) (config-loop)#?

ip Interface Internet Protocol config commands

(Alcatel6000) (config-loop)#ip ?

address Set the IP address of loopback interface, to be used as switch ip.

(Alcatel6000) (config-loop)#ip address ?

A.B.C.D A.B.C.D IP address

(Alcatel6000) (config-loop)#ip address 127.4.4.4

(switch) (config) # interface loopback ?

<cr>

(switch) (config) # interface loopback

(switch) (config) # interface loopback

(switch) (config-loop)#?

ip Interface Internet Protocol config commands

(switch) (config-loop)# ip ?

address Set the IP address of loopback interface, to be used

as switch ip.

(switch) (config-loop)# ip address ?

A.B.C.D A.B.C.D IP address

(switch) (config-loop)# ip address 10.4.21.29 ?

A.B.C.D A.B.C.D IP subnet mask

<cr>

(switch) (config-loop)# ip address 10.4.21.29 255.255.255.0?

<cr>

(switch) (config-loop)# ip address 10.4.21.29 255.255.255.0

Switch IP Address is Modified. Switch should be rebooted now

(switch) (config-loop)#

# **IP Commands**

These commands configure the Internet Protocol attributes of the Wireless LAN switch, including:

Access-list which configures access-lists.

Default-gateway which specifies the default gateway (if not routing IP).

DHCP which configures the DHCP Server.

Local which configures local IP information for L2TP.



NAT which configures Network Address Translation.

RADIUS which configures RADIUS authentication.

Route which specifies static routes.

Router which enables a routing process.

Each command is described below.

#### ip access-list eth

Configures an Ethernet type access list.

#### Syntax

```
ip access-list eth <accname>
    where
```

<accname> is the access list name or number. If you specify a number it must be between 200 and 299.

#### Example

```
(hostswitch) (config) #ip access-list eth 209
(hostswitch) (config) #
```

#### ip access-list extended

Configures an extended access list.

### Syntax

```
ip access-list extended STRING
```

where STRING is a name or number. If you specify a number, the valid ranges are betwen 100 and 199 and between 2000 and 2699.

#### Example

```
(hostswitch) (config) #ip access-list extended 109
(hostswitch) (config) #
```

#### ip access-list mac

Configures a MAC type access list.

#### Syntax

ip access-list mac STRING
 Where:

STRING is the access-list name or number. If you specify a number, valid ranges are between 700 and 799 and between 1200 and 1299.

# Example

(hostswitch) (config) #ip access-list mac 709
(hostswitch) (config) #

### ip access-list session

Configures a session access list.

## Syntax

ip access-list session <accname>
 Where:

<accname> is the Access-list name.

# Example

```
(hostswitch) (config) #ip access-list session corporate
(hostswitch) (config) #
```

### ip access-list standard

Configures a standard access list.

## Syntax

ip access-list standard STRING
 Where:

STRING is the access list name or number. If you specify a number is must be between 1 and 99, or between 1300 and 1399.

# Example

```
(hostswitch) (config) #ip access-list standard 9
  (hostswitch) (config) #
```

### ip default-gateway

Specifies the default gateway. Specify the default gateway if you are not routing IP.

## Syntax

```
ip default-gateway <nexthop> [mgmt]
Where:
<nexthop> is the IP address of the default gateway
mgmt identifies this as the default gateway for the Management port.
```



## Example

```
(hostswitch) (config) #ip default-gateway 1.1.1.1 mgmt
(hostswitch) (config) #
```

#### ip dhcp excluded-address

Configures the DHCP server's excluded address range.

#### Syntax

```
ip dhcp excluded-address <low-address> [var2]
Where:
```

<low-address> specifies the low range of the DHCP excluded addresses

<var2> specifes the optional high range of DHCP excluded addresses.

#### Example

```
(hostswitch) (config) #ip dhcp excluded-address 1.1.1.1 20.2.2.2
(hostswitch) (config) #
```

#### ip dhcp pool

Configures the name of the DHCP address pool.

#### Syntax

```
ip dhcp pool <pool_name>
    Where:
```

<pool\_name> is the label of the DHCP pool.

### Example

```
(hostswitch) (config) #ip dhcp pool Lab_pool
(hostswitch) (config) #
```

```
(hostswitch) (config-dhcp)#?
                        DHCP server will NAK for DHCP discovers and
authoritative
requests
                        not valid on the configured subnet
default-router
                        Configure DHCP default router
dns-server
                        Configure DHCP DNS server
domain-name
                        Configure DHCP Domain Name
lease
                        Configure DHCP lease time
netbios-name-server
                        Configure DHCP NETBIOS server
network
                        Configure DHCP network number
```

no	Delete Command			
option	Configure	client	specific	options

#### ip igmp

Configure Internet Group Management Protocol

### Syntax

### Example

### ip local

Configures the local address pool for L2TP.

## Syntax

[no] ip local pool <pool\_name> <pool\_start\_address> <pool\_end\_address>
Where:
pool configures a local IP pool for L2TP
<pool\_name> is the local IP pool's name
<pool\_start\_address> specifies the starting address of the local pool
<pool end address> specifies the ending address of the local pool

## Example

(hostswitch) (config) #ip local pool lab\_Pool\_Tunnel 1.1.1.1 2.2.2.2 ?
(hostswitch) (config) #

### ip nat

Configure the NAT address pool and specifies the name of the pool.

### Syntax

ip nat pool STRING A.B.C.D A.B.C.D
Where:
[no] STRING is the pool name
A.B.C.D specifies the starting IP address in the pool
A.B.C.D specifies the ending IP address in the pool.

# Example

(hostswitch) (config) #ip nat pool natpool\_lab 1.2.3.4 6.6.6.6
(hostswitch) (config) #



#### ip radius dynamic-authorization

Configures a RFC-3576 compliant RADIUS client.

### Syntax

```
ip radius dynamic-authorization client A.B.C.D
Where:
A.B.C.D is the IP address of the RADIUS client.
```

### Example

```
(hostswitch) (config) #ip radius dynamic-authorization client 3.3.3.3
(hostswitch) (config) #
```

#### ip radius nas-ip

Configures the NAS IP address sent in RADIUS packets.

#### Syntax

```
ip radius nas-ip A.B.C.D Where:
```

A.B.C.D is the NAS IP address.

### Example

```
(hostswitch) (config) # ip radius nas-ip 30.30.30.0
(hostswitch) (config)
```

#### ip radius source-interface

Selects the source address of outgoing RADIUS requests.

### Syntax

```
ip radius source-interface <loopback | <vlan><vlanid>
    Where:
```

loopback specifies the use of the IP address of the loopback interface

vlan specifies the use of the IP address of the specified VLAN

vlanid is the VLAN number (a number between 1 and 4096).

### Example

```
(hostswitch) (config) #ip radius source-interface loopback
(hostswitch) (config) #
```

```
(hostswitch) (config) #ip radius source-interface vlan 3030
(hostswitch) (config) #
```

### ip route

Establishes static routes.

# Syntax

ip route <destip> <destmask> <nexthop> [cost]
Where:
<destip> is the IP address of the destination host
<destmask> is the subnet mask of the destination host
<nexthop> is the IP address of the forwarding router
<cost> is the dstance metric for this route info-

# Example

The following example establishes a static route to the host at 1.1.1.1 and specifies that the route has a cost of 4.

(hostswitch) (config) #ip route 1.1.1.1 255.255.255.255 2.2.2.2 4 (hostswitch) (config) #

## ip router

Enables RIP (Routing Information Protocol).routing protocol.

# Synatx

ip router rip

# Example

```
(hostswitch) (config) #ip router rip
(hostswitch) (config) #
```

# key

(switch) (config) # key ?

<client\_key> Shared secret (text string)

(switch) (config) # key paul ?

<cr>



(switch) (config) # key paul

Syntax Error processing command

(switch) (config) #

## location

Specifies the switch location.

Syntax

location <switchlocation>

Where:

switchlocation> is he location of the switch.

### Example

(switch) (config) # location 10.4.21.1 ?

(switch) (config) #

# **logging Commands**

(switch) (config) # logging ?

### logging <A.B.C.D>

Set Remote logging Server

Syntax

### Example

logging console Set Console Logging level

Syntax

# Example

# logging level

Set Facility Logging level

### logging monitor

Set Terminal Line (monitor) logging level

(switch) (config) #logging monitor alerts

# loginsession timeout

Specifies how long a session will stay active without activity.

### Syntax

loginsession timeout <val>

Where:

<val> is the time out value in minutes. Specify from 5 to 60 minutes. The default is 15 minutes.

### Example:

(hostswitch) (config) # loginsession timeout 30

(hostswitch) (config) #

## mac-address-table static

Configures the MAC address table for Fastethernet and Gigabitethnet.

### Syntax

mac-address-table static <macaddr> <fastethernet | gigabitethent> <slot/port> <vlan><vlanid>

Where:

<macaddr> is the MAC address

fastethernet specifies FastEthernet per the IEEE 802.3 specification



gigabitethernet specifies Gigabit Ethernet per the IEEE 802.3 specification

<slot/port> specifes the module slot and port number on that module

vlan <vlanid> specifies the VLAN name.

#### Example

(hostswitch) (config) # mac-address-table static 00:00:00:1:2:3 fastethernet 3/4 vlan

(hostswitch) (config) #

### master-redundancy

Accesses the commands that configure redundancy (VRRP) on the Master Switch.

#### master-vrrp

Configures the VRRP router ID.

#### Syntax

```
master-vrrp <id>
Where:
<id> specifies the Master Switch virtual router ID. Valid range is
1-255.
```

### Example

(hostswitch) (config-master-redundancy)#master-vrrp 24 (hostswitch) (config-master-redundancy)#

#### no

Disables VRRP configurations.

#### Syntax

no <master-vrrp | peer-ip-address >

Where:

selecting master-vrrp disables the master switch virtual router ID, and

selecting peer-ip-address disables the redundant host.

Chapter 29

## Example

(hostswitch) (config-master-redundancy)# no master-vrrp (hostswitch) (config-master-redundancy)# (hostswitch) (config-master-redundancy)# no peer-ip-address (hostswitch) (config-master-redundancy)#

### peer-ip-address

Configures the redundant host.

## Syntax

peer-ip-address A.B.C.D

Where:

A.B.C.D is the IP address of the redundant host.

## Example

(hostswitch) (config-master-redundancy)#peer-ip-address 10.1.1.1

(Alcatel6000) (config-master-redundancy)#

## masterip

Specifies the IP address of the Wireless LAN Switch configured as the Master Switch.

### Syntax

masterip <masterip>

#### Where:

<masterip> is the IP address of the switch configured as the master switch.

### Example

(Alcatel6000) (config) #masterip 10.10.10.1

(Alcatel6000) (config) #



## mgmt-role

Access the commands that define the Management Role.

### Syntax

mgmt-role <rolename>

Where:

<rolename> is the name of the Management Role. Valid name length is 1-32 characters.

### Example

(hostswitch) (config) #mgmt-role bigboss

(Alcatel6000) (mgmt-role)#

#### Description

Describes the Management Role.

# Syntax

description

## Example

#### no

Disables the Management Role definition.

#### Syntax

no

### Example

Tbd

### permit

Defines which modules the Management Role can control.

### Syntax

permit

Chapter 29

# Example

TBD

## mgmt-user

(Alcatel6000) (config) #mgmt-user ?

<username> Name of the user.

(Alcatel6000) (config) #mgmt-user pauluser ?

<rolename> Role of the user.

(Alcatel6000) (config) #mgmt-user pauluser paulrole ?

PASSWD User password.

<cr>

(Alcatel6000) (config) #mgmt-user pauluser paulrole

ERROR: Configuring the Password.

(Alcatel6000) (config) #mgmt-user pauluser paulrole paul

(Alcatel6000) (config) #no mgmt-user ?

<username> Name of the user.

(Alcatel6000) (config) #no mgmt-user pauluser

Error Deleting the User Entry

(Alcatel6000) (config) #no mgmt-user ?

<username> Name of the user.



(Alcatel6000) (config) #no mgmt-user pauluser ?

<cr>

(Alcatel6000) (config) #no mgmt-user pauluser

Error Deleting the User Entry

(Alcatel6000) (config) #

### mobagent

Accesses mobilty agent mode commands.

(Alcatel6000) (config) #mobagent
(Alcatel6000) (config-mobagent) #?

#### foreign-agent

Foreign Agent Global Configuration

#### home-agent

Home Agent Global Configuration

#### secure-mobile

Configure the security association parameters between

the homeagent and the mobile node

(Alcatel6000) (config-mobagent) #

## mobility

#### Accesses the mobility mode commands.

```
(Alcatel6000) (config-mobagent) #mobility ?
<cr>
```

```
(Alcatel6000) (config-mobagent) #mobility
(Alcatel6000) (config-mob) #?
```

Chapter 29

### event-threshold

## Syntax

Example

### ignore-I2-broadcast

Ignore layer 2 broadcasts for making mobility decisions. Default disabled.

Syntax

## Example

### inter-essid

Enable/disable mobility across different essids

Syntax

## Example

ip-release Quit proxy dhcp for client

Syntax

Example

### manager

Enables/disables mobility management for the mswitch

Syntax



## Example

### max-dhcp-requests

Maximum number of DHCP DISCOVERS/REQUESTS after which Proxy DHCP should quit

Syntax

### Example

#### no

Delete Command

### Syntax

## Example

#### on-association

Enable/disable mobility to trigger on station association

### Syntax

### Example

#### parameters

Set the global parameters for the mobility manager

#### Syntax

### Example

### proxy-dhcp

Enables/disables proxy dhcp support for the mswitch

#### secure

Configure the global security association parameters for the mobility manager.

### Syntax

### Example

#### station-masquerade

Enable/disable station masquerading. Enable this if uplink routers do not accept Gratuitous ARPs

Syntax

Example

#### trusted-roaming

Mobility handles roam from untrusted to trusted. Default disabled.

```
(Alcatel6000) (config-mob) #
```

Syntax

Example

# mobility-local

Accesses the mobility manager mode commands for the local switch.

```
(Alcatel6000) (config-mob) #mobility-local ?
<cr>
```

(Alcatel6000) (config-mob) #mobility-local (Alcatel6000) (config-mob-local) #?

#### exclude-vlan

Quit mobility management for users moving to/from this VLAN



Syntax

## Example

### ha-priority

Set Home Agent priority for this VLAN

Syntax

Example

### local-ha

If enabled, sets mswitch as HA for all subnet it owns else accepts HA designated by master

### Syntax

### Example

#### no

**Delete Command** 

(Alcatel6000) (config-mob-local) #

## mobmaster primary-subnet

Syntax

Example

## mux-address

(Alcatel6000) (config) #mux-address ?
<mux-ip-address> A.B.C.D IP address
(Alcatel6000) (config) #mux-address 10.100.101.30 ?
<cr>
(Alcatel6000) (config) #mux-address 10.100.101.30
(Alcatel6000) (config) #no mux-address

## mux-vlan

(Alcatel6000) (config) #mux-vlan ?

<mux-vlan-id> VLAN ID to enable MUX termination on

(Alcatel6000) (config) #mux-vlan 24

(Alcatel6000) (config) #show mux vlan

MUX VLANs

-----

VLAN ID

\_\_\_\_\_

24

(Alcatel6000) (config) #no mux-vlan



% Incomplete command.

(Alcatel6000) (config) #no mux-vlan 24

(Alcatel6000) (config) #show mux vlan

MUX VLANs

-----

VLAN ID

\_\_\_\_\_

(Alcatel6000) (config) #

# netdestination

(Alcatel6000) (config) #netdestination ?

STRING Name of destination host or subnet

(Alcatel6000) (config) #netdestination myplace ?

<cr>

(Alcatel6000) (config) #netdestination myplace

# newbury

(Alcatel6000) (config) # newbury ?

<ip-addr> Specify IP Address of Locate Server A.B.C.D

(Alcatel6000) (config) #

## no

Disables the following actions:

(Alcatel6000) (config) #no ?

#### no aaa

**Configure Authentication** 

Syntax

## Example

### no ap

Specify configuration of an AP by location or by BSSID

### Syntax

Example

### no arp

Configure ARP parameters.

### Syntax

# Example

no cap Cisco Access point



no clock

Configure time-of-day clock

### Syntax

Example

#### no crypto

Configure IPSec, IKE, and CA

Syntax

### Example

#### no database

Database management

#### no destination

Configure network destination (deprecated; use netdestination)

Syntax

### Example

#### no dot1x

Configure IEEE 802.1X Authenticator

### Syntax

## Example

#### no enable

Modify the enable password

Chapter 29

Syntax

# Example

## no firewall

Configure global firwall policies

Syntax

Example

## no interface

Select an interface to configure

Syntax

# Example

### no ip

Interface Internet Protocol config commands

# Syntax

Example

# no logging Modify Message Logging Facilities

# Syntax

Example



no loginsession Login Session

Syntax

Example

#### no mac-address-table

Configure the MAC address table

Syntax

### Example

#### no masterip

Configure the master ip address for the switch

Syntax

### Example

no mgmt-role Management Role Definition

#### no mgmt-user

Configure a management user.

### Syntax

### Example

#### no mux-vlan

Enable MUX functionality on a VLAN

Chapter 29

Syntax

## Example

no netdestination Configure network destination

#### no netservice

Configure a network service

Syntax

## Example

#### no newbury

Specify Newbury Locate Server Information

## Syntax

## Example

### no ntp

Configure NTP

### no pptp

Configure IP information for PPTP

## Syntax

## Example

**no rap-wml** Wired MAC Lookup for AP Classification commands



## Syntax

# Example

### no router

Router Mobile

Syntax

Example

### no service

Configure services

Syntax

Example

### no shutdown

Shut down interface

Syntax

Example

#### no snmp-server

Enable SNMP; Modify SNMP parameters

Syntax

### Example

### no spanning-tree

Spanning Tree Subsystem

Syntax

Example

no telnet

Enable telnet port

Syntax

Example

no time-range Configure a time range

Syntax

Example

**no trusted** Make this a trusted port

Syntax

Example

no udp-port

Configure the UDP port to receive Discennect-Requests. Default is 3999.

#### no user-role

Configure user role



Syntax

## Example

#### no vlan

Create Switch VLAN Virtual Interface

Syntax

Example

#### no vpn-dialer

Configure the VPN dialer

#### no vrrp

Virtual Router Redundancy Protocol Configuration

(Alcatel6000) (config) #no

### ntp server

(Alcatel6000) (config) #ntp ?

server Configure NTP Server

(Alcatel6000) (config) #ntp 10.100.101.30 ?

(Alcatel6000) (config) #ntp 10.100.101.30

۸

% Invalid input detected at '^' marker.

(Alcatel6000) (config) #ntp 10.100.101.30 ?

(Alcatel6000) (config) #ntp 10.100.101.30

# packet-capture-defaults

(Alcatel6000) (config) #packet-capture-defaults
(Alcatel6000) (config) #
(Alcatel6000) (config) #packet-capture-defaults ?

### packet-capture-defaults Alcatelmsg

Enable or disable Alcatel internal messaging packet capturing. For debugging only.

Syntax

Example

#### packet-capture-defaults other

Enable or disable all other types of packets.

#### packet-capture-defaults tcp

Enable or disable TCP packet capturing.

#### packet-capture-defaults udp

Enable or disable TCP packet capturing.

(Alcatel6000)	(config)	<pre>#packet-capture-defaults Alcatelmsg ?</pre>		
<opcodes></opcodes>		Up to 10 comma separated opcodes to capture.		
Use [al				
		<pre>l] to sniff all opcodes or [disable] to bypass</pre>		
all.				
(Alcate16000)	(coniig)	#packet-capture-defaults other ?		
disable		Disable all other types of packets.		
enable		Enable all other types of packets.		



(Alcatel6000) (config) #packet-capture-defaults tcp ? Up to 10 comma separated ports to capture. Use ports [all] to sniff all tcp ports or [disable] to bypass all. All CLI ports are always skipped. (Alcatel6000) (config) #packet-capture-defaults udp ? ports Up to 10 comma separated ports to capture. Use [all] to sniff all udp ports or [disable] to bypass all. (Alcatel6000) (config) #packet-capture-defaults udp % Incomplete command. (Alcatel6000) (config) #packet-capture-defaults (Alcatel6000) (config) #show packet-capture-defaults ? <cr> (Alcatel6000) (config) #show packet-capture-defaults Current Active Packet Capture Actions (current switch) \_\_\_\_\_ Packet filtering for TCP ports disabled. Packet filtering for UDP ports disabled. Packet filtering for Alcatel messaging opcodes disabled. Packet filtering for all other packets disabled. Packet Capture Defaults (across switches and reboots if saved) \_\_\_\_\_ Packet filtering for TCP ports disabled. Packet filtering for UDP ports disabled. Packet filtering for Alcatel messaging opcodes disabled. Packet filtering for all other packets disabled. (Alcatel6000) (config) #no packet-capture-defaults ? (Alcatel6000) (config) #no packet-capture-defaults % Invalid input detected at '^' marker.

(Alcatel6000) (config) #

## ping

(Alcatel6000) (config) #ping ? <ipaddr> Send ICMP echo packets to a specified IP address. (Alcatel6000) (config) #ping 10.100.101.30 Press 'q' to abort. Sending 5, 100-byte ICMP Echos to 10.100.101.30, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1.032/1.1152/1.432 ms

(Alcatel6000) (config) #

## pptp

(Alcatel6000) (config) #pptp ? Configure IP information for PPTP ip (Alcatel6000) (config) #pptp ip ? local Configure local IP information for PPTP (Alcatel6000) (config) #pptp ip local ? Configure a local IP pool for PPTP pool (Alcatel6000) (config) #pptp ip local pool ? <pool name> Configure local IP pool's name (Alcatel6000) (config) #pptp ip local pool paulpool ? <pool start address> Configure the start address of the local pool (Alcatel6000) (config) #pptp ip local pool paulpool 192.168.1.1 192.168.1.255 (Alcatel6000) (config) #show pptp % Invalid input detected at '^' marker. (Alcatel6000) (config) #no pptp ? Configure IP information for PPTP ip



```
(Alcatel6000) (config) #no pptp ip ?
local Configure local IP information for PPTP
(Alcatel6000) (config) #no pptp ip local ?
pool Configure a local IP pool for PPTP
(Alcatel6000) (config) #no pptp ip local pool ?
<pool_name> Configure local IP pool's name
(Alcatel6000) (config) #no pptp ip local pool paulpool ?
<cr>
(Alcatel6000) (config) #no pptp ip local pool paulpool
(Alcatel6000) (config) #no pptp ip local pool paulpool
(Alcatel6000) (config) #
```

pptp provision mode

tbd

Syntax

#### Example

#### program-ap

(Alcatel6000) (config) # program-ap ?
<cr>

(Alcatel6000) (config) # program-ap

(Alcatel6000) (config) #>

### prompt

(Alcate16000) (config) #prompt ?
<prompt> Enter the new prompt

(Alcatel6000) (config) #prompt Alcatel5050 ?
<cr>

(Alcatel6000) (config) #prompt Alcatel5050

(Alcate15050) >
(Alcate15050) >enable
Password:\*\*\*\*\*\*
(Alcate15050) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Alcate15050) (config) #show prompt ?
(Alcate15050) (config) #show prompt ^
% Invalid input detected at '^' marker.
(Alcate15050) (config) #no prompt ^
% Invalid input detected at '^' marker.
(Alcate15050) (config) #no prompt ^
% Invalid input detected at '^' marker.
(Alcate15050) (config) #prompt Alcate16000

```
(Alcatel6000) >enable
Password:******
(Alcatel6000) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

(Alcatel6000) (config) #

**NOTE**—resetting prompt dumps you back to Exec mode.

### rap-wml

(Alcatel6000) (config) # show rap-wml?

cache	Show Cache of all lookups for a DB Server
servers	Show DB Server State
wired-mac	Show Wired MAC Discovered on traffic through AP

(Alcatel6000) (config) # show rap-wml



% Incomplete command.

(Alcatel6000) (cor	nfig) # show rap-wml ?				
cache	Show Cache of all lookups for a DB Server				
servers	Show DB Server State				
wired-mac	Show Wired MAC Disco	overed on traffic th	rough AP		
(Alcatel6000) (cor <cr></cr>	nfig) # show rap-wml serve	ərs ?			
(Alcatel6000) (cor	nfig) # show rap-wml serve	ers			
WML DB Servers					
name ip typ	e user password db-na	ıme cache ageou	ut(sec) in-service		
paulsql 0.0.0.0 u	inknown	disable 32768	disable		
WML DB Tables					
server db table o query-count	column timestamp-colum	n lookup-time(sec	) delimiter 		

(Alcatel6000) (config) #no rap-wml ?
<server-name> Specify Name of MSSQL Server

table Specify Table Name for Lookup

(Alcatel6000) (config) #no rap-wml paulsql

(Alcatel6000) (config) #show rap-wml

% Incomplete command.

(Alcatel6000) (config) #show rap-wml servers

WML DB Servers

-----

name ip type user password db-name cache ageout(sec) in-service

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

WML DB Tables

-----

server db table column timestamp-column lookup-time(sec) delimiter query-count

(Alcatel6000) (config) #

# router

(Alcatel6000) (config) #router ?
mobile Enable Mobile IP



```
(Alcatel6000) (config) #router mobile ?
                       IP Address to be used for Mobile IP Service
<A.B.C.D>
<cr>
(Alcatel6000) (config) #router mobile
Module Mobile IP is busy. Please try later
(Alcatel6000) (config) #
(Alcatel6000) (config) #
sapm
(Alcatel6000) (config) #
(Alcatel6000) (config) #sapm ?
general
(Alcatel6000) (config) #sapm general ?
update-batchsize
                      Number of APs to update in a single batch
(Alcatel6000) (config) #sapm general update-batchsize ?
<batch>
                        Number of APs to update in a single batch
(Alcatel6000) (config) #sapm general update-batchsize 10 ?
<cr>
(Alcatel6000) (config) #sapm general update-batchsize 10
(Alcatel6000) (config) #show sapm ?
ap-search
                       Complex AP Listing
config-sync
counters
                      SAPM counters for debugging
gw-list
                       show TTL hops for each LMS to known AP gateways
lms-list
                       Shows the list of LMSs that sapm knows about
(Alcatel6000) (config) #show sapm counters ?
bssid
                      BSSID of wireless interface
location
                       Location in B.F.L notation
(Alcatel6000) (config) #show sapm counters location 0.0.0 ?
<cr>
(Alcatel6000) (config) #show sapm counters location 0.0.0
```

Chapter 29

# SAPM\_COUNTERS\_RESULT

LOC SAP\_IP Updates Sent ACKs Rcvd APBoots Sent APBoots Rcvd Bootstraps Reboots Calibration .g Calibration .a

Num APs:0

(Alcatel6000) (config) #no sapm ?

(Alcatel6000) (config) #

# service

#### Enable disable DHCP.

(Alcatel6000) (config) # service ? dhcp Enable DHCP service (Alcatel6000) (config) # service dhcp ? <cr> (Alcatel6000) (config) # service dhcp (Alcatel6000) (config) #show service ? (Alcatel6000) (config) #show service ? % Invalid input detected at '^' marker. (Alcatel6000) (config) #no service ? dhcp Enable DHCP service (Alcatel6000) (config) #no service dhcp ? <cr>

(Alcatel6000) (config) #no service dhcp



# shutdown

(switch) (config) # shutdown ?
all All the physical interfaces in the switch
(switch) (config) # shutdown all ?
<cr>
(switch) (config) # shutdown all

# site-survey

(switch) (config) #site-survey

#### site-survey calibration-max-packets

(switch) (config) #site-survey calibration-max-packets ?
<calibration-max-pack.. max packets to send per tx power and rate</pre>

(switch) (config) #site-survey calibration-max-packets 10 ?
calibration-transmit-rate transmit rate of Alcatel ap
ha-compute-time time in milliseconds when HA reconvergence
algorithms are kicked off
max-ha-neighbors max neighbor to increase to increase tx power for
HA recovery
neighbor-tx-power-bump amount of increase in tx power for a neighbor for
HA recovery
rra-max-compute-time max time in seconds for RRA computation
<cr>

#### site-survey calibration-trasmit time

Chapter 29

neighbor-tx-power-bump amount of increase in tx power for a neighbor for HA recovery rra-max-compute-time max time in seconds for RRA computation <cr>

#### site-survey ha compute-time

(switch) (config) #site-survey ha-compute-time ? <ha-compute-time> time in milliseconds when HA reconvergence algorithms are kicked off (switch) (config) #site-survey ha-compute-time 15 ? calibration-max-packe.. max packets to send per tx power and rate calibration-transmit-.. transmit rate of Alcatel ap max-ha-neighbors max neighbor to increase to increase tx power for HA recovery neighbor-tx-power-bump amount of increase in tx power for a neighbor for HA recovery rra-max-compute-time max time in seconds for RRA computation <cr>

### site-survey max-ha-neighbors

(switch) (config) #site-survey max-ha-neighbors ? <max-ha-neighbors> max neighbor to increase to increase tx power for HA recovery (switch) (config) #site-survey max-ha-neighbors 25 ? calibration-max-packe.. max packets to send per tx power and rate calibration-transmit-.. transmit rate of Alcatel ap time in milliseconds when HA reconvergence ha-compute-time algorithms are kicked off neighbor-tx-power-bump amount of increase in tx power for a neighbor for HA recovery rra-max-compute-time max time in seconds for RRA computation <cr>



(switch) (config) #site-survey neighbor-tx-power-bump ?
<neighbor-tx-power-bu.. amount of increase in tx power for a neighbor for
HA</pre>

recovery

#### site-survey neighbor-tx-power-bump

#### site-survey rra-max-compute-time

```
(switch) (config) #site-survey rra-max-compute-time ?
<rra-max-compute-time> max time in seconds for RRA computation
(switch) (config) #site-survey rra-max-compute-time ?
<rra-max-compute-time> max time in seconds for RRA computation
(switch) (config) #site-survey rra-max-compute-time 40 ?
calibration-max-packe.. max packets to send per tx power and rate
calibration-transmit-.. transmit rate of Alcatel ap
ha-compute-time
                       time in milliseconds when HA reconvergence
algorithms
                        are kicked off
                       max neighbor to increase to increase tx power for
max-ha-neighbors
ΗA
                        recovery
neighbor-tx-power-bump amount of increase in tx power for a neighbor for
ΗA
                        recovery
<cr>
(switch) (config) #
```

### snmp-server

(switch) (config) #snmp-server ? community set read-only community string enable host Specify host address to receive SNMP notifications. Traps defined in the new MIB's supported. new User Name configuration for the USM security user model <cr> (switch) (config) #snmp-server (switch) (config) #no snmp-server (switch) (config) #show snmp ? Display the configured snmp communities community trap-hosts Display the configured trap hosts Display the Trap Queue trap-queue user-table

### snmp-server community

(switch) (config) #snmp-server community ? WORD SNMP community string

# Syntax

# Example

### snmp-server enable

(switch) (config) #snmp-server enable ? trap Enable SNMP Traps

(switch) (config) #snmp-server enable trap ?
<cr>



#### snmp-server host

```
(switch) (config) #snmp-server host ?
A.B.C.D IP address of SNMP notofication host.
??
(switch) (config) #snmp-server new ?
traps The system will generate new versions of the
trap.
(switch) (config) #snmp-server new traps ?
```

#### snmp-server user

<cr>

```
(switch) (config) #snmp-server user ?
WORD USM Security Model User Name
```

(switch) (config) #snmp-server user

# spanning-tree

(switch)	(config)	#show	span?
spanning-	tree		Spanning tree topology
spantree			Global spanning tree topology

(switch) (config) #show spanning-tree

Spanning Tree is executing the IEEE compatible Spanning Tree protocol Bridge Identifier has priority 32768, address 00:0b:86:40:01:00 Configured hello time 2, max age 20, forward delay 15 We are the root of the spanning tree Topology change flag is set, detected flag set, changes 1 Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15 Timers: hello 0, notification 0 Last topology change: 0 days, 0 hours, 0 mins, 24 secs

(switch) (config) #no spanning-tree

(switch)	(config)	#spanning	-tı	ree ?			
forward-t	ime	Set	а	Spanning	Tree	FORWARD	Interval
hello-tim	ne	Set	а	Spanning	Tree	HELLO Ir	nterval
max-age		Set	а	Spanning	Tree	MAX AGE	Interval
priority		Set	а	Spanning	Tree	Priority	7
<cr></cr>							

### spanning-tree forward-time

(switch) (config) #spanning-tree forward-time ?
<value> Set a Spanning Tree FORWARD Interval <4-30>
(switch) (config) #spanning-tree forward-time 15 ?
<cr>
(switch) (config) #spanning-tree forward-time 15

# spanning-tree hello-time

(switch)	(config)	<pre>#spanning-tree hello-time ?</pre>	
<value></value>		Set a Spanning Tree HELLO Interval <1-10	>
(switch)	(config)	<pre>#spanning-tree hello-time 2</pre>	
(switch) <value></value>	(config)	<pre>#spanning-tree max-age ?     Set a Spanning Tree MAX AGE Interval &lt;6-</pre>	40>

# spanning-tree max-age

(switch) (config) #spanning-tree max-age 20

# spanning-tree priority

```
(switch) (config) #spanning-tree priority ?
<value>
                        Set a Spanning Tree Priority <0 - 65535>
(switch) (config) #spanning-tree priority ?
<value>
                        Set a Spanning Tree Priority <0 - 65535>
(switch) (config) #spanning-tree priority 32768
(switch) (config) #show spann
Spanning Tree is not currently active
The following parameters have been configured
Stp Status : Disabled
Protocol
                       : IEEE
Max Age (sec)
                       : 20
Hello Time (sec)
                       : 2
Forward Delay (sec) : 15
Bridge Priority : 32
                       : 32768
```



(switch) (config) #show spanning-tree

Spanning Tree is not currently active The following parameters have been configured : Disabled Stp Status Protocol : IEEE Max Age (sec) : 20 Hello Time (sec) : 2 Forward Delay (sec) : 15 Bridge Priority : 32768 (switch) (config) #spanning-tree enable ^ % Invalid input detected at '^' marker.

(switch) (config) #spanning-tree

Connection to host lost.

 $H: \setminus >$ 

### stm

(switch) (config) #stm	?
ap-inactivity-timeout	Amount of time after which AP is aged out. in seconds
auth-failure-block-ti	Amount of time to block a STA if it fails repeated au thentications. In seconds. 0 blocks indefinitely
coverage-hole-detecti	Enable/Disable STM coverage hole capabilities
dos-prevention	Enable/Disable STM DoS prevention capabilities
fast-roaming	Enable/Disable Fast Roaming
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than

	this value
sta-dos-block-time	Amount of time to block a STA on with DoS is detected
	. In seconds. 0 blocks indefinitely
sta-dos-prevention	Enable/Disable STA DoS prevention.
strict-compliance	Enable/Disable strict WECA compliance
<cr></cr>	

# stm ap-inactivity-timeout

(switch) (config) #stm ap-inactivity-timeout ?
<ap-inactivity-timeou.. Amount of time after which AP is aged out. in seconds</pre>

(switch) (config) #stm	ap-inactivity-timeout 10 ?
auth-failure-block-ti	Amount of time to block a STA if it fails repeated au
	thentications. In seconds. 0 blocks indefinitely
coverage-hole-detecti	Enable/Disable STM coverage hole capabilities
dos-prevention	Enable/Disable STM DoS prevention capabilities
fast-roaming	Enable/Disable Fast Roaming
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than this value
sta-dos-block-time	Amount of time to block a STA on with DoS is detected . In seconds. O blocks indefinitely
sta-dos-prevention	Enable/Disable STA DoS prevention.
strict-compliance <cr></cr>	Enable/Disable strict WECA compliance
(switch) (config) #stm disable enable	ap-inactivity-timeout 10 coverage-hole-detection ? Disable Enable
(switch) (config) #stm	ap-inactivity-timeout 10 coverage-hole-detection enable ?
auth-failure-block-ti	Amount of time to block a STA if it fails repeated au thentications. In seconds. 0 blocks indefinitely
dos-prevention	Enable/Disable STM DoS prevention capabilities
fast-roaming	Enable/Disable Fast Roaming
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value



#### **OmniAccess Reference: AOS-W System Reference**

good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen
	erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in
	fo with bad RSSI to one of the APs is aged out. in se
	conds
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than this value
sta-dos-block-time	Amount of time to block a STA on with DoS is detected
	. In seconds. U blocks indefinitely
sta-dos-prevention	Enable/Disable STA Dos prevention.
<cr></cr>	Enable/Disable Strict WECA compliance
(switch) (config) #stm a auth-failure-block-time	ap-inactivity-timeout 10 coverage-hole-detection enable ?
<auth-failure-block-t< td=""><td>Amount of time to block a STA if it fails repeated au</td></auth-failure-block-t<>	Amount of time to block a STA if it fails repeated au
	thentications. In seconds. 0 blocks indefinitely
(switch) (config) #stm a	ap-inactivity-timeout 10 coverage-hole-detection enable
auth-failure-block-time	20 ?
dos-prevention	Enable/Disable STM DoS prevention capabilities
fast-roaming	Enable/Disable Fast Roaming
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than this value
sta-dos-block-time	Amount of time to block a STA on with DoS is detected . In seconds. 0 blocks indefinitely
sta-dos-prevention	Enable/Disable STA DoS prevention.
strict-compliance <cr></cr>	Enable/Disable strict WECA compliance

# stm auth-failure-block-time

Syntax

# Example

# stm coverage-hole-dectection

# Syntax

# Example

# stm dos-prevention

(switch) (config) # (switch) (config) #stm dos-prevention ? Disable disable enable Enable (switch) (config) #stm dos-prevention enable ? ap-inactivity-timeout Amount of time after which AP is aged out. in seconds auth-failure-block-ti.. Amount of time to block a STA if it fails repeated au thentications. In seconds. 0 blocks indefinitely coverage-hole-detecti.. Enable/Disable STM coverage hole capabilities fast-roaming Enable/Disable Fast Roaming good-rssi-threshold stop hole detection if RSSI from STA is more than thi s value Amount of time after with STA with good RSSID to one good-sta-ageout of the APs is aged out. in seconds hole-detection-interv.. Amount of time after with hole detection event is gen erated. in seconds idle-sta-ageout Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds poor-rssi-threshold kick off hole detection if RSSI from STA is less than this value sta-dos-block-time Amount of time to block a STA on with DoS is detected . In seconds. O blocks indefinitely sta-dos-prevention Enable/Disable STA DoS prevention. strict-compliance Enable/Disable strict WECA compliance <cr>

# stm fast-roaming

(switch) (config) #stm dos-prevention enable fast-roaming ? disable Disable



#### **OmniAccess Reference: AOS-W System Reference**

enable	Enable
(switch) (config) #stm ( ap-inactivity-timeout	dos-prevention enable fast-roaming enable ? Amount of time after which AP is aged out. in seconds
auth-failure-block-ti	Amount of time to block a STA if it fails repeated au thentications. In seconds. 0 blocks indefinitely
coverage-hole-detecti	Enable/Disable STM coverage hole capabilities
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than this value
sta-dos-block-time	Amount of time to block a STA on with DoS is detected . In seconds. O blocks indefinitely
sta-dos-prevention	Enable/Disable STA DoS prevention.
strict-compliance <cr></cr>	Enable/Disable strict WECA compliance

# stm good-rssi-threshold

<pre>(switch) (config) #stm o good-rssi-threshold ?</pre>	dos-prevention enable fast-roaming enable
<good-rssi-threshold></good-rssi-threshold>	stop hole detection if RSSI from STA is more than thi s value
(switch) (config) #stm o good-rssi-threshold 30 (	dos-prevention enable fast-roaming enable ?
ap-inactivity-timeout	Amount of time after which AP is aged out. in seconds
auth-failure-block-ti	Amount of time to block a STA if it fails repeated au thentications. In seconds. 0 blocks indefinitely
coverage-hole-detecti	Enable/Disable STM coverage hole capabilities
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen erated. in seconds
idle-sta-ageout	Amount of time after which STA with potential hole in fo with bad RSSI to one of the APs is aged out. in se conds $% \left( {\left[ {{{\rm{STA}}} \right]_{\rm{STA}}} \right)$
poor-rssi-threshold	kick off hole detection if RSSI from STA is less than

```
this value
sta-dos-block-time
sta-dos-prevention
strict-compliance
<cr>
this value
Amount of time to block a STA on with DoS is detected
In seconds. 0 blocks indefinitely
Enable/Disable STA DoS prevention.
Enable/Disable strict WECA compliance
<cr>
```

### stm idle-sta-ageout

```
(switch) (config) #
(switch) (config) #
(switch) (config) #stm idle-sta-ageout ?
<idle-sta-ageout>
                        Amount of time after which STA with potential hole in
                        fo with bad RSSI to one of the APs is aged out. in se
                        conds
(switch) (config) #stm idle-sta-ageout 35 ?
ap-inactivity-timeout Amount of time after which AP is aged out. in seconds
auth-failure-block-ti.. Amount of time to block a STA if it fails repeated au
                        thentications. In seconds. 0 blocks indefinitely
coverage-hole-detecti.. Enable/Disable STM coverage hole capabilities
dos-prevention
                        Enable/Disable STM DoS prevention capabilities
fast-roaming
                        Enable/Disable Fast Roaming
good-rssi-threshold
                       stop hole detection if RSSI from STA is more than thi
                        s value
good-sta-ageout
                        Amount of time after with STA with good RSSID to one
                        of the APs is aged out. in seconds
hole-detection-interv.. Amount of time after with hole detection event is gen
                        erated, in seconds
                        kick off hole detection if RSSI from STA is less than
poor-rssi-threshold
                        this value
sta-dos-block-time
                        Amount of time to block a STA on with DoS is detected
                        . In seconds. 0 blocks indefinitely
sta-dos-prevention
                        Enable/Disable STA DoS prevention.
strict-compliance
                        Enable/Disable strict WECA compliance
<cr>
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold ?
                       kick off hole detection if RSSI from STA is less than
<poor-rssi-threshold>
                         this value
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold 45 ?
ap-inactivity-timeout Amount of time after which AP is aged out. in seconds
auth-failure-block-ti.. Amount of time to block a STA if it fails repeated au
                        thentications. In seconds. 0 blocks indefinitely
```



```
coverage-hole-detecti.. Enable/Disable STM coverage hole capabilities
dos-prevention
                        Enable/Disable STM DoS prevention capabilities
fast-roaming
                       Enable/Disable Fast Roaming
good-rssi-threshold
                       stop hole detection if RSSI from STA is more than thi
                        s value
good-sta-ageout
                       Amount of time after with STA with good RSSID to one
                        of the APs is aged out. in seconds
hole-detection-interv.. Amount of time after with hole detection event is gen
                        erated. in seconds
                       Amount of time to block a STA on with DoS is detected
sta-dos-block-time
                        . In seconds. 0 blocks indefinitely
sta-dos-prevention
                       Enable/Disable STA DoS prevention.
strict-compliance
                       Enable/Disable strict WECA compliance
<cr>
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold 45 sta-dos-block-time
?
<sta-dos-block-time>
                       Amount of time to block a STA on with DoS is detected
                        . In seconds. O blocks indefinitely
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold 45 sta-dos-block-time
50 ?
ap-inactivity-timeout Amount of time after which AP is aged out. in seconds
auth-failure-block-ti.. Amount of time to block a STA if it fails repeated au
                        thentications. In seconds. O blocks indefinitely
coverage-hole-detecti.. Enable/Disable STM coverage hole capabilities
dos-prevention
                       Enable/Disable STM DoS prevention capabilities
fast-roaming
                       Enable/Disable Fast Roaming
good-rssi-threshold
                      stop hole detection if RSSI from STA is more than thi
                        s value
good-sta-ageout
                        Amount of time after with STA with good RSSID to one
                        of the APs is aged out. in seconds
hole-detection-interv.. Amount of time after with hole detection event is gen
                        erated. in seconds
sta-dos-prevention
                       Enable/Disable STA DoS prevention.
strict-compliance
                       Enable/Disable strict WECA compliance
<cr>
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold 45 sta-dos-block-time
50 strict-compliance ?
disable
                        Disable
enable
                        Enable
(switch) (config) #stm idle-sta-ageout 35 poor-rssi-threshold 45 sta-dos-block-time
50 strict-compliance enable ?
ap-inactivity-timeout Amount of time after which AP is aged out. in seconds
```

auth-failure-block-ti	Amount of time to block a STA if it fails repeated au
	thentications. In seconds. O blocks indefinitely
coverage-hole-detecti	Enable/Disable STM coverage hole capabilities
dos-prevention	Enable/Disable STM DoS prevention capabilities
fast-roaming	Enable/Disable Fast Roaming
good-rssi-threshold	stop hole detection if RSSI from STA is more than thi s value
good-sta-ageout	Amount of time after with STA with good RSSID to one of the APs is aged out. in seconds
hole-detection-interv	Amount of time after with hole detection event is gen $% \left( {{{\left( {{{{c}_{{\rm{m}}}}} \right)}_{{\rm{m}}}}} \right)$ and ${{{c}_{{{\rm{m}}}}}} \right)$
sta-dos-prevention	Enable/Disable STA DoS prevention.
<cr></cr>	

# stm hole-detection-interval

# stm idle-sta-ageout

Syntax

Example

stm poor-rssi-threshold

Syntax

Example

stm sta-dos-block-time

Syntax

Example



stm sta-dos-prevention

stm strict-compliance

Syntax

Example

# syscontact

(switch) (config) # syscontact ?
<syscontact> Change the system contact
(switch) (config) # syscontact rama ?
<cr>
(switch) (config) # show syscontact ?
<cr>
(switch) (config) # show syscontact
Contact is not configured
(switch) (config) #syscontact Rama
(switch) (config) #show syscontact
Rama

# syslocation

(switch) (config) #syslocation ?
<syslocation> Change the system location
(switch) (config) #syslocation Crossman main lab ?

# telnet cli

```
(switch) (config) # telnet ?
             Enable telnet to Command Line Interface (CLI) port
cli
             Enable telnet to Serial Over Ethernet (soe) port
soe
(switch) (config) # telnet cli ?
<cr>
telnet soe
(switch) (config) # telnet soe ?
<cr>
(switch) (config) # show telnet?
(switch) (config) # show telnet
% Invalid input detected at '^' marker.
(switch) (config) #no telnet ?
cli
                        Enable telnet to Command Line Interface (CLI)
port
                        Enable telnet to Serial Over Ethernet (soe) port
soe
(switch) (config) #no telnet soe ?
<cr>
(switch) (config) #no telnet cli ?
<cr>
```

(switch) (config) #



# time-range

Informs the Switch when a time-restricted feature, like an access list, is to be used.

(switch) (config) #time-range ? STRING Name of time range (switch) (config) #time-range Side ? Configure an absolute time-range absolute periodic Configure a PERIODIC time-range (switch) (config) #time-range Side periodic ? <cr> (switch) (config) #time-range Side absolute ? Specify end date of time-range end start Specify start date of time-range <cr> (switch) (config) #time-range Side absolute start ? mm/dd/yyyy Starting day of time-range (switch) (config) #time-range Side absolute start 12/20/2004 ? hh:mm Starting time in 24-hour clock (switch) (config) #time-range Side absolute start 12/20/2004 00:00 ? end Specify end date of time-range <cr> (switch) (config) #time-range Side absolute start 12/20/2004 00:00 end ? mm/dd/yyyy Day when time-range ends (switch) (config) #time-range Side absolute start 12/20/2004 00:00 end 12/30/2004 ? hh:mm Ending time in 24-hour clock (switch) (config) #time-range Side absolute start 12/20/2004 00:00 end 12/30/2004 24:00 ? <cr> (switch) (config) #show time-range ? STRING Name of time-range <cr>

Chapter 29

```
(switch) (config) #show time-range
(switch) (config) #
traceroute
(switch) (config) #traceroute ?
<ipaddr>
                      Trace route to specified IP address.
(switch) (config) #traceroute 64.121.71.217
Press 'q' to abort.
Tracing the route to 64.121.71.217
 1 10.4.21.254 0.783 msec 0.559 msec 0.565 msec
 2 * * *
 3 *
(switch) (config) #traceroute 64.121.71.217 ?
<cr>
(switch) (config) #traceroute 64.121.71.217
Press 'q' to abort.
Tracing the route to 64.121.71.217
 1 10.4.21.254 0.599 msec 0.556 msec 0.554 msec
 2 * * *
 3 * * *
 4
   * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
```



```
20 * * *
21 * * *
21 * * *
21 * * *
22 * * *
23 * * *
23 * * *
24 * * *
25 * * *
26 * * *
26 * * *
27 * * *
28 * * *
28 * * *
29 * * *
30 * * *
(switch) (config) #show traceroute ?
(switch) (config) #show traceroute ^
% Invalid input detected at '^' marker.
(switch) (config) #
```

# trusted

# udp-port

#### user

```
(switch) (config) # user ?
<username> Enter a user name
(switch) (config) # user paul ?
<passwd> Enter the password for the user
(switch) (config) # user paul paul ?
```

<cr>

```
(switch) (config) #show user ?
authentication-method Match authentication method
bssid
                  Match BSSID
debug
                  Show users that are currently being debugged
essid
                  Match ESSID
                  Displays summary of all users currently in the system
global-user-map
                  Show internal user entries
internal
                  Match IP address
ip
location
                  Match location
                  Match MAC address
mac
                  Show mobile users
mobile
name
                  Match name
                  Match PHY type
phy-type
                  Match role
role
                   Show certain rows
rows
<cr>
(switch) (config) #show user name ?
STRING
                   Name
(switch) (config) #show user name paul
Users
____
      MAC Name Role Age(d:h:m) Auth VPN link location
   ΙP
Roaming Essid/Bssid/Phy
_____
User Entries: 0/2
(switch) (config) #show user name rama ?
<cr>
(switch) (config) #show user name rama
Users
____
                         Name Role Age(d:h:m) Auth VPN link
  ΙP
             MAC
location Roaming E
_____
                                ____
                          _____
                                          _____ ____
----- ----- -
```



AOS-W Commands | 793

#### **OmniAccess Reference: AOS-W System Reference**

10.4.21.102 00:00:00:00:00 rama ap-role 00:00:25 VPN 10.4.21.229 1/0 Wired 10.4.21.104 00:00:00:00:00 rama ap-role 00:23:28 VPN 10.4.21.193 1/0 Wired User Entries: 2/2

(switch) (config) #

# user-role

```
(switch) (config) #user-role
% Incomplete command.
(switch) (config) #user-role ?
                    Name of user role
STRING
(switch) (config) #user-role rama ?
<cr>
(switch) (config) #show user role
% Incomplete command.
(switch) (config) #show user role ?
STRING
                    Role name
(switch) (config) #show user role ap-role ?
                   Show certain rows
rows
<cr>
(switch) (config) #show user role ap-role
Users
____
   ΤP
       MAC Name Role Age(d:h:m) Auth VPN link
location Roaming E
_____
                         _____ ____
                                           ----- -----
_____ _
10.4.21.102 00:00:00:00:00 rama ap-role 00:00:26 VPN 10.4.21.229
1/0
      Wired
10.4.21.104 00:00:00:00:00:00 rama ap-role 00:23:29 VPN 10.4.21.193
1/0 Wired
User Entries: 2/2
```

(switch) (config) #show user role guest ? rows Show certain rows <cr> (switch) (config) #show user role guest Users \_\_\_\_ ΙP MAC Name Role Age(d:h:m) Auth VPN link location Roaming Essid/Bssid/Phy \_\_\_\_\_ User Entries: 0/0 (switch) (config) #user-role ? STRING Name of user role (switch) (config) #user-role visitor ? <cr> (switch) (config) #user-role visitor (switch) (config-role) #show user ? authentication-method Match authentication method bssid Match BSSID debug Show users that are currently being debugged essid Match ESSID global-user-map Displays summary of all users currently in the system Show internal user entries internal Match IP address ip location Match location mac Match MAC address mobile Show mobile users Match name name Match PHY type phy-type Match role role Show certain rows rows <cr> (switch) (config-role) #show user role

% Incomplete command.



#### **OmniAccess Reference: AOS-W System Reference**

# version

(switch) (config-role) #version ?

<versionnum>

(switch) (config-role) #version

Λ

% Invalid input detected at '^' marker.

(switch) (config-role) #version ?

<versionnum>

(switch) (config-role) #version 2.4 ?

<cr>

(switch) (config-role) #version 2.4

(switch) (config) #show version ?

<cr>

(switch) (config) #show version

Alcatel Wireless Operating System Software.

AOS-W (MODEL: switch), Version 2.4.0.0

Website: http://www.alcatel.com

Copyright (c) 2003-2005 by Alcatel, Inc.

Compiled on 2004-12-22 at 19:08:49 PST (build 9270) by p4build

ROM: System Bootstrap, Version CPBoot 1.1.5 (Aug 30 2004 - 01:52:13)

Switch uptime is 23 hours 40 minutes 48 seconds

Reboot Cause: User reboot.

Alcatel Supervisor Card

Alcatel Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of memory.

32K bytes of non-volatile configuration memory.

256M bytes of Supervisor Card System flash (model=256MB CHH).



(switch) (config) #

# vlan

```
(switch) (config) # vlan <id>
(switch) (config) #show vlan
VLAN CONFIGURATION
_____
VLAN Name Ports
____ ___
            ____
1 Default Fa1/0-23 Gig1/24-25 Pc0-7
(switch) (config) #vlan 2
(switch) (config) #show vlan 2
VLAN CONFIGURATION
_____
VLAN Name Ports
____ ___
             ____
2 VLAN0002
(switch) (config) #show vlan
VLAN CONFIGURATION
_____
VLAN Name Ports
             ____
____ ___
1 Default Fa1/0-23 Gig1/24-25 Pc0-7
   VLAN0002
2
(switch) (config) #no vlan 2
(switch) (config) #
vpdn
```

```
(switch) (config) #vpdn ?
group Configure vpdn groups
(switch) (config) #vpdn group ?
l2tp Configure the L2TP group
```

Configure the PPTP group pptp (switch) (config) #vpdn group 12tp ? <cr> (switch) (config) #vpdn group pptp ? <cr> (switch) (config) #show vpdn ? 12tp Show vpdn L2TP state Show pptp state pptp tunnel Show vpdn tunnel state (switch) (config) #show vpdn 12tp % Incomplete command. (switch) (config) #show vpdn 12tp ? configuration Show L2TP configuration local Show 12tp local IP pool (switch) (config) #show vpdn 12tp configuration ? <cr> (switch) (config) #show vpdn l2tp configuration Enabled Hello timeout: 60 seconds DNS primary server: 0.0.0.0 DNS secondary server: 0.0.0.0 WINS primary server: 0.0.0.0 WINS secondary server: 0.0.0.0 PPP client authentication methods: PAP CHAP MSCHAP MSCHAPv2 IP LOCAL POOLS: remoteappool: 10.4.21.101 - 10.4.21.110 (switch) (config) #show vpdn ? Show vpdn L2TP state 12tp Show pptp state pptp Show vpdn tunnel state tunnel



(switch) (config) #show vpdn pptp ? configuration Show PPTP configuration local Show PPTP local IP pool (switch) (config) #show vpdn pptp configuration Enabled Hello timeout: 60 seconds DNS primary server: 0.0.0.0 DNS secondary server: 0.0.0.0 WINS primary server: 0.0.0.0 WINS secondary server: 0.0.0.0 PPP client authentication methods: MSCHAPv2 MPPE Configuration 128 bit encryption enabled IP LOCAL POOLS: (switch) (config) #show vpdn ? Show vpdn L2TP state 12tp Show pptp state pptp tunnel Show vpdn tunnel state (switch) (config) #show vpdn tunnel ? 12tp Show 12tp state Show pptp state pptp (switch) (config) #show vpdn tunnel 12tp ? id Show tunnel state <cr> (switch) (config) #show vpdn tunnel 12tp L2TP Tunnel Information (Total tunnels = 2) Tunnel ID = 199 is up, remote id is 30821 Tunnel state is SCCCN: Connection Connected Remote Internet Address 10.4.21.229, port 1701 Tunnel ID = 4 is up, remote id is 61927Tunnel state is SCCCN: Connection Connected Remote Internet Address 10.4.21.193, port 1701

(switch) (config) #show vpdn tunnel pptp ?

<cr> (switch) (config) #show vpdn tunnel pptp Command obsolete. Please use show user-table to get a list of users. All PPTP

(switch) (config) #

# vpn-dialer

(switch) (config) STRING	<pre>#vpn-dialer ?     Configuration Name of the VPN dialer</pre>
(switch) (config)	#show vpn-dialer
default-dialer	
Attribute	Value
PPTP L2TP DNETCLEAR WIREDNOWIFI PAP CHAP MSCHAP MSCHAPV2 CACHE-SECURID IKESECS IKEENC IKEGROUP IKEHASH IKEAUTH IKEPASSWD IPSECSECS IPSECGROUP IPSECENC IPSECAUTH SECURID NEWPINMODE	disabled enabled disabled disabled enabled enabled enabled disabled 28800 3DES TWO SHA PRE-SHARE ******* 7200 GROUP2 ESP-3DES ESP-SHA-HMAC E disabled

(switch) (config) #vpn-dialer ?



STRING Configuration Name of the VPN dialer (switch) (config) #vpn-dialer test ? <cr> (switch) (config) #vpn-dialer test (switch) (config-vpn-dialer) #show vpn-dialer default-dialer \_\_\_\_\_ Attribute Value \_\_\_\_\_ \_\_\_\_ PPTP disabled L2TP enabled disabled DNETCLEAR WIREDNOWIFI disabled PAP enabled CHAP enabled MSCHAP enabled MSCHAPV2 enabled CACHE-SECURID disabled IKESECS 28800 IKEENC 3DES TWO IKEGROUP IKEHASH SHA IKEAUTH PRE-SHARE \*\*\*\*\*\*\* IKEPASSWD IPSECSECS 7200 IPSECGROUP GROUP2 IPSECENC ESP-3DES IPSECAUTH ESP-SHA-HMAC SECURID NEWPINMODE disabled test \_\_\_\_ Attribute Value \_\_\_\_\_ \_\_\_\_ disabled PPTP l2tp enabled disabled DNETCLEAR disabled WIREDNOWIFI enabled PAP CHAP enabled MSCHAP enabled MSCHAPV2 enabled

```
CACHE-SECURID
                    disabled
IKESECS
                    28800
IKEENC
                    3DES
                    TWO
IKEGROUP
IKEHASH
                    SHA
IKEAUTH
                   PRE-SHARE
IKEPASSWD
                    *******
IPSECSECS
                    7200
IPSECGROUP
                    GROUP2
IPSECENC
                    ESP-3DES
IPSECAUTH
                    ESP-SHA-HMAC
SECURID NEWPINMODE disabled
(switch) (config-vpn-dialer) #no vpn-dialer test
% Invalid input detected at '^' marker.
(switch) (config-vpn-dialer) #no vpn-dialer ?
(switch) (config-vpn-dialer) #no vpn-dialer test
% Invalid input detected at '^' marker.
(switch) (config-vpn-dialer) #
(switch) (config-vpn-dialer)#?
                        Bind the VPN dialer to the wireless link
auto-dial-wpn
dialup
                        Configure dialup information for the Dialer.
enable
                        Enable PPTP, L2TP, dnetclear, wirednowifi, or
securid
                        newpinmode for the dialer
                        Configure the IKE
ike
                        Configure the IPSEC lifetime in seconds
ipsec
no
                        Delete Command
                        Configure PPP
ppp
                        Configure the VPN gateway
vpngateway
(switch) (config-vpn-dialer)#
```

### vrrp

```
(switch) (config) #vrrp ?
<id> <1-255> Virtual Router ID
```



intra-switch Intra-switch Virtual Router Redundancy Protocol Confi guration (switch) (config) #vrrp 25 ? <cr> (switch) (config) #show vrrp (switch) (config) #show vrrp ? <vrid> <1-255> Virtual Router ID statistics <cr> (switch) (config) #show vrrp statistics ? <vrid> <1-255> Virtual Router ID (switch) (config) #show vrrp statistics % Incomplete command. (switch) (config) #show vrrp statistics 1 (switch) (config) #vrrp ? <id> <1-255> Virtual Router ID intra-switch Intra-switch Virtual Router Redundancy Protocol Confi guration (switch) (config) #vrrp intra-switch ? <cr> (switch) (config) #vrrp intra-switch (switch) (config-vrrp) #show vrrp (switch) (config-vrrp) #no vrrp % Invalid input detected at '^' marker. (switch) (config-vrrp) #no ?

shutdown Disable VRRP intra-switch

```
(switch) (config-vrrp)#no shutdown ?
<cr>
```

(switch) (config-vrrp)#no shutdown Can't start router: VR ID is not configured

(switch) (config-vrrp)#?
no Delete Command
shutdown Disable VRRP intra-switch

(switch) (config-vrrp)#

### web-server

```
(switch) (config) #web-server ?
<cr>
(switch) (config) #web-server
(switch) (config-webserver) #show web-server
% Incomplete command.
(switch) (config-webserver) #show web-server ?
configuration
                        Show web server configuration
(switch) (config-webserver) #show web-server configuration ?
<cr>
(switch) (config-webserver) #show web-server configuration
Web Server Settings:
Security Protocol ..... sslv2 sslv3 tlsv1
Cipher Suite Strength .. high
Admin HTTPS port ..... 4343
(switch) (config-webserver) #?
admin-port
                        Configure port for WEB administration
ciphers
                        Configure cipher suite strength. Default is high
                        Delete Command
no
ssl-protocol
                        Configure SSL/TLS protocol. Default is to use
SSLv2,
```



SSLv3 and TLSv1

#### admin-port

```
(switch) (config-webserver)#admin-port ?
https Specify https port
```

```
(switch) (config-webserver)#admin-port https ?
<0-65535> Port Number
```

```
(switch) (config-webserver)#admin-port https 22 ?
<cr>
```

# ciphers

```
(switch) (config-webserver)#ciphers ?
high Cipher suite with encryption keys larger than 128
bit
s
low Cipher suite with 56 or 64 bit encryption keys
medium Cipher suite with 128 bit encryption keys
(switch) (config-webserver)#ciphers medium ?
<cr>
```

```
(switch) (config-webserver)#ciphers no ?
```

### no

```
(switch) (config-webserver)#no ?
admin-port Configure port for WEB administration
ciphers Configure cipher suite strength. Default is high
ssl-protocol Configure SSL/TLS protocol. Default is to use
SSLv2,
SSLv3 and TLSv1
```

```
(switch) (config-webserver)#ssl-protocol ?
sslv2 Use SSLv2
sslv3 Use SSLv3
tlsv1 Use TLSv1
```

<cr>

### ssl-protocol

```
(switch) (config-webserver)#ssl-protocol tlsv1 ?
sslv2 Use SSLv2
sslv3 Use SSLv3
```
```
<cr>
(switch) (config-webserver)#ssl-protocol tlsv1 sslv2 ?
sslv3 Use SSLv3
<cr>
(switch) (config-webserver)#ssl-protocol tlsv1 sslv2 sslv3 ?
<cr>
(switch) (config-webserver)#
```

#### web-ui

```
(switch) (config) # webui ?
user Configure the web ui administrator password
(switch) (config) # webui user ?
administrator Configure the web ui administrator password
(switch) (config) # webui user administrator ?
<passwd> Enter web ui administrator password
(switch) (config) # webui user administrator admin ?
<cr>
(switch) (config) # show webui ?
(switch) (config) # show webui ?
% Invalid input detected at '^' marker.
(switch) (config) #
```

#### wms

```
(switch) (config) #wms
(switch) (wms) #?
ap-config
                        Setup Valid AP Configuration
                        Configure ap policies
ap-policy
event-threshold
                        Configure Statistics event thresholds
general
                        Configure general attributes
global-policy
                        Configure global policy applied for AP and STA
ids-policy
                        configure IDS Policy for AP and AM
ids-signature
                        configure a signature for the IDS check
                        Delete Command
no
```



reserved-11a-channel	enable/disable 80211a channel as multi tenancy protec
	ted channel
reserved-11b-channel	enable/disable 80211b channel as multi tenancy protec
	ted channel
station-policy	Configure Station Policy
valid-11a-channel	enable/disable 80211a channel as valid
valid-11b-channel	enable/disable 80211b channel as valid
valid-oui	configure valid OUI for AP
valid-ssid	configure valid SSID for AP
wired-mac	configure Wired MAC of router or server

#### ap-config

```
(switch) (wms) #ap-config ?
privacy
                        enable/disable Encryption as valid ap configuration
short-preamble
                        enable/disable short preamble as valid ap configurati
                        on
                        enable/disable WPA support as valid ap configuration
wpa
<cr>
(switch) (wms) #ap-config privacy ?
disable
enable
(switch) (wms) #ap-config privacy enable ?
                        enable/disable short preamble as valid ap configurati
short-preamble
                        on
                        enable/disable WPA support as valid ap configuration
wpa
<cr>
(switch) (wms) #ap-config privacy enable short-preamble ?
disable
enable
(switch) (wms) #ap-config privacy enable short-preamble enable ?
                        enable/disable WPA support as valid ap configuration
wpa
<cr>
(switch) (wms) #ap-config privacy enable short-preamble enable wpa ?
disable
enable
(switch) (wms) #ap-config privacy enable short-preamble enable wpa enable ?
<cr>
```

#### ap-policy

(switch) (wms) #ap-policy ?

ap-lb-max-retries	max tries to encourage STA to move to a unloaded AP		
ap-lb-user-high-wm	High WM on max users that triggers enabling ap load b alancing		
ap-lb-user-low-wm	Low WM on max users that triggers disabling ap load b alancing		
ap-lb-util-high-wm	High WM on utilization that triggers enabling ap load balancing		
ap-lb-util-low-wm	Low WM on utilization that triggers disabling ap load balancing		
ap-lb-util-wait-time	Time in seconds to wait before enabling or disabling load balancing once threshold is hit		
ap-load-balancing	enable/disable AP load balancing		
beacon-diff-threshold	percent increase in beacon rate that should trigger a n ap impersonation event. Default 50		
beacon-inc-wait-time	Amount of time to wait in seconds before generating a n ap impersonation event when AP impersonation is sus pected. Default 3		
classification	enable/disable AP Classification.		
detect-ap-impersonati	enable/disable AP Impersonation Detection		
detect-misconfigured	enable/disable detect misconfigured ap policy		
learn-ap	enable/disable learn AP.		
min-pot-ap-beacon-rate	Min beacon rate acceptable from a potential AP. In % of configured beacon interval		
<pre>min-pot-ap-monitor-ti</pre>	Min time a potential AP has to be up before it is cla ssified as a real AP. In seconds		
protect-ap-impersonat	enable/disable AP Impersonation Protection		
protect-ibss	enable/disable protect Adhoc Network Policy		
protect-misconfigured	enable/disable protect misconfigured ap policy		
protect-mt-channel-sp	enable/disable protect multi tenancy channel split po licy		
protect-mt-ssid	enable/disable multi tenancy ssid protection policy		
protect-unsecure-ap <cr></cr>	enable/disable protect unsecure ap policy		
(switch) (wms) #			
(switch) (wms) #ap-po	plicy ?		
ap-lb-max-retries AP	max tries to encourage STA to move to a unloaded		
ap-lb-user-high-wm load b	High WM on max users that triggers enabling ap		
	alancing		
ap-lb-user-low-wm load b	Low WM on max users that triggers disabling ap		
	alancing		
ap-lb-util-high-wm load	High WM on utilization that triggers enabling ap		



balancing ap-lb-util-low-wm Low WM on utilization that triggers disabling ap load balancing ap-lb-util-wait-time Time in seconds to wait before enabling or disabling load balancing once threshold is hit ap-load-balancing enable/disable AP load balancing beacon-diff-threshold percent increase in beacon rate that should trigger a n ap impersonation event. Default 50 Amount of time to wait in seconds before beacon-inc-wait-time generating a n ap impersonation event when AP impersonation is SUS pected. Default 3 classification enable/disable AP Classification. detect-ap-impersonati.. enable/disable AP Impersonation Detection detect-misconfigured-.. enable/disable detect misconfigured ap policy enable/disable learn AP. learn-ap min-pot-ap-beacon-rate Min beacon rate acceptable from a potential AP. Tn 😤 of configured beacon interval min-pot-ap-monitor-ti.. Min time a potential AP has to be up before it is cla ssified as a real AP. In seconds protect-ap-impersonat.. enable/disable AP Impersonation Protection protect-ibss enable/disable protect Adhoc Network Policy protect-misconfigured.. enable/disable protect misconfigured ap policy protect-mt-channel-sp.. enable/disable protect multi tenancy channel split po licv protect-mt-ssid enable/disable multi tenancy ssid protection policy protect-unsecure-ap enable/disable protect unsecure ap policy <cr> (switch) (wms) #? ap-config Setup Valid AP Configuration ap-policy Configure ap policies Configure Statistics event thresholds event-threshold general Configure general attributes global-policy Configure global policy applied for AP and STA ids-policy configure IDS Policy for AP and AM

ids-signature	configure a signature for the IDS check
no	Delete Command
reserved-11a-channel protec	enable/disable 80211a channel as multi tenancy
	ted channel
reserved-11b-channel protec	enable/disable 80211b channel as multi tenancy
	ted channel
station-policy	Configure Station Policy
valid-11a-channel	enable/disable 80211a channel as valid
valid-11b-channel	enable/disable 80211b channel as valid
valid-oui	configure valid OUI for AP
valid-ssid	configure valid SSID for AP
wired-mac	configure Wired MAC of router or server

#### event-threshold

(switch) (wms)	#event-threshold ?		
bwr-high-wm	Bandwidth Rate High Watermark in %		
owr-low-wm Bandwidth Rate Low Watermark in %			
fer-high-wm	Frame Error Rate High Watermark in %		
fer-low-wm	Frame Error Rate Low Watermark in %		
ffr-high-wm	Frame Fragmentation Rate High Watermark in 🗞		
ffr-low-wm	Frame Fragmentation Rate Low Watermark in $\%$		
flsr-high-wm	Frame Low Speed Rate High Watermark in %		
flsr-low-wm	Frame Low Speed Rate Low Watermark in $\%$		
fnur-high-wm	Frame Non Unicast Rate High Watermark in %		
fnur-low-wm	Frame Non Unicast Rate Low Watermark in %		
frer-high-wm	Frame Receive Error Rate High Watermark in 🗞		
frer-low-wm	Frame Receive Error Rate Low Watermark in %		
frr-high-wm	Frame Retry Rate High Watermark in %		
frr-low-wm	Frame Retry Rate Low Watermark in %		
<cr></cr>			

#### general

(switch) (wms) #general	?		
ap-ageout-interval	AP ageout interval in minutes. O to disable		
ap-inactivity-timeout	AP inactivity timeout in scan seconds.		
grace-time	am & wms comm. latency grace time in		
milliseconds			
laser-beam	enable or disable force station deauthentication		
for policy enforcement			
laser-beam-debug	enable or disable laser beam debug mode		
poll-interval	am poll interval in milliseconds		



```
poll-retries# of retries before it is declared downsta-ageout-intervalSTA ageout interval in minutes. 0 to disablesta-inactivity-timeoutSTA inactivity timeout in scan seconds.stat-updateenable or disable Stat update in DBwired-laser-beamenable or disable wired side protection
```

#### global-policy

baselines

<cr>

#### ids-policy

(switch) (wms) #ids-pol	icy ?
adhoc-check	IDS Adhoc Network Detection
adhoc-quiet-time activit	Time to wait in seconds after detecting Adhoc
	y after which the check can be resumed
ap-flood-check	IDS Fake AP Flood Detection
ap-flood-inc-time count	Number of consecutive seconds over which the AP
	is more than the threshold
ap-flood-quiet-time flood b	Time to wait in seconds after detecting an AP
	efore continuing the check
ap-flood-threshold dsta-check	The number of spurious APs in the system IDS Disconnect Station Analysis
dsta-quiet-time	Time to wait in seconds after detecting
disconnect st	
	ation attack after which the check can be resumed
eap-check	IDS EAP Handshake Anomaly Detection
eap-rate-quiet-time	Time to wait in seconds after detecting an EAP
handsh	

Chapter 29

ake anomlay after which the check can be resumed eap-rate-threshold Number of EAP handshake packets over the time interva 1 that constitutes an anomaly eap-rate-time-interval Time interval in seconds over which the packet count. should be checked. Maximum is 120 seconds. mac-oui-check IDS MAC OUI Validation mac-oui-quiet-time Time to wait in seconds after detecting an invalid MA C OUI after which the check can be resumed IDS Rate Analysis rate-check rate-frame-type-param Type of frame for rate check IDS Sequence Analysis sequence-check sequence-diff Difference between sequence numbers that will be cons idered an anomaly Time to wait in seconds after detecting a sequence-quiet-time sequence nu mber anomaly after which the check can be resumed sequence-time-toleran.. Difference in the time between two packets that is co nsidered to be non-consecutive (in ms). signature-check IDS Signature Analysis signature-quiet-time Time to wait in seconds after detecting a signature m atch after which the check can be resumed wbridge-check IDS Wireless Bridge Detection wbridge-quiet-time Time to wait in seconds after detecting a wireless br idge after which the check can be resumed <cr> (switch) (wms) #ids-(switch) (wms) #ids-? ids-policy configure IDS Policy for AP and AM ids-signature configure a signature for the IDS check (switch) (wms) #ids-policy ? adhoc-check IDS Adhoc Network Detection adhoc-quiet-time Time to wait in seconds after detecting Adhoc activit y after which the check can be resumed



ap-flood-check IDS Fake AP Flood Detection ap-flood-inc-time Number of consecutive seconds over which the AP count. is more than the threshold ap-flood-quiet-time Time to wait in seconds after detecting an AP flood b efore continuing the check ap-flood-threshold The number of spurious APs in the system IDS Disconnect Station Analysis dsta-check dsta-quiet-time Time to wait in seconds after detecting disconnect st ation attack after which the check can be resumed eap-check IDS EAP Handshake Anomaly Detection eap-rate-quiet-time Time to wait in seconds after detecting an EAP handsh ake anomlay after which the check can be resumed Number of EAP handshake packets over the time eap-rate-threshold interva 1 that constitutes an anomaly eap-rate-time-interval Time interval in seconds over which the packet count should be checked. Maximum is 120 seconds. mac-oui-check IDS MAC OUI Validation mac-oui-quiet-time Time to wait in seconds after detecting an invalid MA C OUI after which the check can be resumed rate-check IDS Rate Analysis rate-frame-type-param Type of frame for rate check sequence-check IDS Sequence Analysis sequence-diff Difference between sequence numbers that will be cons idered an anomaly sequence-quiet-time Time to wait in seconds after detecting a sequence nu mber anomaly after which the check can be resumed sequence-time-toleran.. Difference in the time between two packets that is co nsidered to be non-consecutive (in ms). signature-check IDS Signature Analysis signature-quiet-time Time to wait in seconds after detecting a signature m atch after which the check can be resumed IDS Wireless Bridge Detection wbridge-check

Chapter 29

```
ids-policyconfigure IDS Policy for AP and AMids-signatureconfigure a signature for the IDS check
```

#### ids-signature

```
(switch) (wms) #ids-signature ?
<name>
                        name of signature
(switch) (wms) #ids-signature paul ?
<cr>
(switch) (wms) #
(switch) (wms) #?
ap-config
                        Setup Valid AP Configuration
                        Configure ap policies
ap-policy
event-threshold
                        Configure Statistics event thresholds
general
                        Configure general attributes
global-policy
                        Configure global policy applied for AP and STA
                        configure IDS Policy for AP and AM
ids-policy
                        configure a signature for the IDS check
ids-signature
                        Delete Command
no
reserved-11a-channel
                        enable/disable 80211a channel as multi tenancy
protec
                        ted channel
reserved-11b-channel
                        enable/disable 80211b channel as multi tenancy
protec
                        ted channel
station-policy
                        Configure Station Policy
valid-11a-channel
                        enable/disable 80211a channel as valid
valid-11b-channel
                        enable/disable 80211b channel as valid
valid-oui
                        configure valid OUI for AP
valid-ssid
                        configure valid SSID for AP
wired-mac
                        configure Wired MAC of router or server
```

no

reserved-11a-channel



#### reserved-11b-channel

```
(switch) (wms) #reserved-11b-channel 11 ?
mode enable/disable
```

```
(switch) (wms) #reserved-11b-channel 11 mode enable ?
<cr>
```

#### station-policy

```
(switch) (wms) #station-policy ?
detect-association-fa.. enable/disable STA association failure detection
detect-sta-impersonat.. enable/disable station impersonation detection
handoff-assist
                       enable/disable AP assisted handoff
ista-detection-interv.. Impersonating station detection interval in
milliseco
                        nds
ista-max-retries
                        max retries to detect station impersonation
low-rssi-threshold
                       Min RSSI above with deauth should never be sent
protect-valid-sta
                       enable/disable protect valid station policy
rssi-check-frequency How often in seconds to sample RSSI value
rssi-falloff-wait-time Seconds (max 8) to wait with decreasing RSSI
before de
                       auth is sent to the client
<cr>
```

**NOTE**—The handoff-assist option allows the switch to force a sticky client off of an AP when the RSSI drops below the defined minimum threshold. This is useful when a client will not let go of an AP as long as it was getting any Acks (even at 1 Mbps) and will only look for new AP after about 10 seconds of not getting Ack responses from the old AP.

#### valid-11a-channel

(switch) (wms) #valid-11a? valid-11a-channel enable/disable 80211a channel as valid (switch) (wms) #valid-11a-channel ? <valid-11a-channel> enable/disable 80211a channel as valid (switch) (wms) #valid-11a-channel 2 ? enable/disable mode (switch) (wms) #valid-11a-channel 2 mode enable ? <cr> (switch) (wms) #? ap-config Setup Valid AP Configuration ap-policy Configure ap policies event-threshold Configure Statistics event thresholds Configure general attributes general global-policy Configure global policy applied for AP and STA configure IDS Policy for AP and AM ids-policy ids-signature configure a signature for the IDS check Delete Command no reserved-11a-channel enable/disable 80211a channel as multi tenancy protec ted channel reserved-11b-channel enable/disable 80211b channel as multi tenancy protec ted channel station-policy Configure Station Policy valid-11a-channel enable/disable 80211a channel as valid valid-11b-channel enable/disable 80211b channel as valid valid-oui configure valid OUI for AP valid-ssid configure valid SSID for AP wired-mac configure Wired MAC of router or server

## valid-11b-channel

(switch) (wms) #valid-11b-channel ?
<valid-11b-channel> enable/disable 80211b channel as valid



#### **OmniAccess Reference: AOS-W System Reference**

(switch) (wms) #valid-11b-channel 14 ? mode enable/disable

(switch) (wms) #valid-11b-channel 14 mode enable ?
<cr>

#### valid-oui

(switch) (wms) #valid-oui ?
<valid-oui> configure valid OUI for AP

(switch) (wms) #valid-oui 4 ?

#### valid-ssid

```
(switch) (wms) #valid-ssid ?
<valid-ssid> configure valid SSID for AP
(switch) (wms) #valid-ssid 3434 ?
mode enable or disable a SSID
(switch) (wms) #valid-ssid 3434 mode enable ?
<cr>
```

#### wired-mac

(switch) (wms) #wired-mac ?
<wired-mac> configure Wired MAC of router or server
(switch) (wms) #wired-mac 00:00:01:00:00:11 ?
mode enable disable a wired MAC
(switch) (wms) #wired-mac 00:00:01:00:00:11 mode enable ?
<cr>
(switch) (wms) #wired-mac 00:00:01:00:00:11 mode enable

# CHAPTER 30 Action Commands

Action Commands are available from the main Command-Line Interface (CLI) prompts in user mode and privileged mode. These commands take effect as soon as they are entered and, if appropriate, any resulting configuration changes are automatically saved. Different Action commands are available in each mode.

This chapter provides a summary of the action commands available on the Alcatel Wireless LAN Switch in your network. The command summary is organized by command function. Each command entry depicts the syntax. Many provide usage details.

For more information on the commands, use the CLI help feature described on page 18.

## **User Mode Commands**

User mode is entered when you first log in to the Alcatel Wireless LAN Switch. This mode is indicated by the host> prompt, where host is the host name of the switch, if defined. From any other mode or sub-mode, you can return to the user mode using the global exit command.

Parameters are entered immediately after the command, and are entered as name-value pairs with a single space separating each item on the line. There are no delimiters or operators used when entering parameters. End the line and execute the command by typing a Carriage Return <Enter> after the command.

An Example of a command would be:

> command name parameter1 value1 parameter2 value2 <Enter>

## **Switch Management Commands**

#### enable

Type this command to enter the privileged mode. You will be prompted for the password.

## logout

Close this CLI session. Any configuration changes which have not yet been saved are lost.

## swkey <software key>

Use this privileged command to enable extra features in the Alcatel switch software. Contact Alcatel sales for more information about additional features and obtaining keys.

## Layer 2/Layer 3 Commands

## ping <IP Address>

This command sends ICMP packets to a host specified by the *IP Address* argument.

## traceroute <IP Address>

This command traces the route, displaying each hop, to a host specified by the *IP Address* argument.

## **Privileged Mode Commands**

Privileged mode is entered from the user mode through the enable command (see page 820). This mode provides access to configuration and information collection commands. Privileged mode is indicated by the host# prompt, where host is the host name of the switch, if defined. From any privileged mode or sub-mode, you can exit to the user mode using the global exit command.

## Switch Management Commands

#### boot...

Set the configuration file or software image to be used the next time the system boots.

Variations:

boot config-file <filename>

Set the name of the file used for the switch configuration data. The named file will be used when saving the configuration (see the write command on page 824) and will be loaded the next time the switch is booted. This command requires a valid file.

boot system {partition0|partition1}

Set the location of the switch software image to be used the next time the system is booted.

clock set <year> <month> <day> <hour> <minute> <second>

Set the switch's clock to the current date and time.

Parameters:

year	The current year, specified in YYYY format (2003, for example).
month	The current month of the year (1-12).
day	The current day of the month (1-31).
hour	The current hour of the day, specified in 24 hour format (0-23).
minute	The current minute of the hour (0-59).
second	The current second of the minute (0-59).



#### configure terminal

Enter the configuration mode. This mode provides access to system configuration commands. The commands available depends on the switch mode. Local configuration commands (see page 445) are available on any switch. Master configuration commands (page 797) are only available on the master switch.

#### copy...

Copy file or image items from one location to another.

Variations:

- copy flash <source filename> flash <dest filename>
   Copy a system file.
- copy flash <source filename> tftp <host> <dest filename>
   Copy a system file to a TFTP destination.
- copy running-config flash <dest filename>
   Copy the current configuration to a system file.
- copy running-config tftp <host> <dest filename>
   Copy the current configuration to a TFTP destination.
- copy running-config startup-config

Copy the current configuration settings to the switch configuration file used the next time the system starts. This is the equivalent of the write memory command (see page 824).

- copy startup-config flash <dest filename>
   Copy the saved configuration to a system file.
- copy startup-config tftp <host> <dest filename>
   Copy the saved configuration to a TFTP destination.
- copy tftp <host> <source filename> flash <best filename> Download a file into the system via TFTP.
- copy tftp <host> <source filename> system {partition0|partition1}
   Download a switch software image file into one of the switch image banks.

## **copy log** <*type> <destination IP address>* [*<user name> <password>*]

Copy a specified log file to the destination address via FTP. The transferred file is named type.log.

#### Parameters:

type

A variety of logs are available for transfer:



destination IP address	The IP address of the FTP destination for the <i>type</i> .log file.
user name	If required, the name of a valid user account at the destination.
password	If required, the password for the user account at the destination.

## delete <filename>

Delete the specified file from the system. To view a list of files, use the  ${\tt dir}$  command.

## dir

List the system files.

## exit

Exit the current mode or sub-mode and return to one above it. When entered from the privileged mode main prompt (#), this commend returns you to the user mode.

## masterip <master IP address>

This command is used to configure the master IP address of the switch. It is entered in the standard IP address format (*AA.BB.CC.DD.EE*).

Use this command to change the role of the switch from Master to Local or back to Master. Setting the switch's IP address to the IP address of another switch configures the switch as a local switch, returning it to its own IP address makes the switch a Master Switch. In either case, you will have to reboot the switch to make the changes effective and you will be prompted to reboot after you enter the new IP address.



## reload

Reboot the system after prompting the user to verify the command. If there are any unsaved configuration changes, you will be prompted whether you wish to save them first.

## halt

Shuts down the switch (the switch will not reboot automatically).

## **rename** <*filename*> <*new filename*>

Change the name of a system file. To view a list of files, use the dir command.

#### show

Enter the Show mode (see page 833). The Show mode is used to display a variety of system information and statistics.

#### write...

Variations:

write erase

Erase the system configuration file. The next time the system boots, the configuration will be reset to factory defaults.

write file <filename>

Save the current configuration to the specified system file.

write memory

Save the current configuration to the system configuration file. Any configuration changes made during this session will be made permanent.

#### write terminal

Display the current configuration.

## Layer 2/Layer 3 Commands

## ping <IP Address>

This command sends ICMP packets to a host specified by the *IP Address* argument.

## traceroute <IP Address>

This command traces the route, displaying each hop, to a host specified by the *IP Address* argument.

## **Air Management Commands**

Air Monitor Commands

am scan <IP address> <channel> [bssid <MAC address>]

#### pcap...

Variations:

- pcap clear <air monitor IP address> <pcap ID> [bssid <MAC address>]
- pcap interactive <air monitor IP address> <filter> <target IP address> <target UDP port> [bssid <MAC address>] [channel <channel>]
- pcap pause <air monitor IP address> <pcap ID> [bssid <MAC address>]
- raw-start <target IP address>
- raw-start <air monitor IP address>
- pcap resume <air monitor IP address> <pcap ID> [bssid <MAC address>]
- pcap start <air monitor IP address> <filter> [bssid <MAC address>] [channel <channel>] [max-packet-size <size>] [max-packets <number>]
- pcap stop <air monitor IP address> <pcap ID> [bssid <MAC address>]



#### WMS Commands

## wms ap <MAC address> [mode <type (dos | interfering | valid)>]

This command defines the access point specified by the MAC address argument as either an interfering, valid, or denial of service type access point.

## wms station <MAC address> [mode <type (dos | interfering | valid)>]

This command defines the station specified by the MAC address argument as either an interfering, valid, or denial of service type station.

## wms export-db <filename>

This command is used to export the WMS database to an external file. The file is exported as an ASCII text file. The filename plus any extensions may be no longer than 32 characters in length and may contain only keyboard characters.

#### wms import-db <filename>

This command is used to import the specified file into the WMS database. The imported file replaces the existing WMS database. The imported file must be a valid WMS database file previously exported using the wms export-db command.

**CAUTION**—Attempting to import a file not exported with the wms export-db or importing a modified file, may result in a serious malfunction of the switch.

#### wms reinit-db

This command re-initializes the WMS database to the factory defaults. No automatic backup of the current database is made.

## Site Survey Commands

#### site-survey ...

Variations:

- site-survey calibrate <building ID> <type (alb | G)> [channel <channel>] [max-per
  <number>] [overlap-factor <percent>]
  [post-process {0|1}]
- site-survey channel-plan <building ID> <type (ab)>
  [max-per <number>] [overlap-factor <percent>] [post-process {0|1}]
- site-survey update-channel-plan <BSSID> <channel> <transmit power level>
- site-survey walkabout-start <building ID> <type (alb)>
- site-survey walkabout-stop <building ID> <type (alb)>



## **Authentication Commands**

#### AAA Commands

The following immediate commands are used for Accounting, Authentication, & Authorization (AAA). Other AAA commands can be found starting on page 823.

#### aaa debug {save-config}

#### **aaa inservice** <server name>

Place the named AAA server into service.

#### aaa test-server <server name> <user name> <password>

Test the response of a configured AAA server. The command checks whether the user and password combination is recognized by the specified AAA server and returns a pass/fail response. The server must be able to accept PAP.

Parameters:

server name	The name of the AAA server to test.
user name	The name of the user account to test.
password	The password for the tested user account.

#### aaa user...

Variations:

- aaa user add <IP address> [name <user name>] [role <role>] [mac <MAC address>]
- aaa user delete {<*IP* address>|all}
- aaa user logout <IP address>

## Local Database Commands

The local user database is an internal Wireless LAN switch database for authenticating users. If using an external RADIUS server for authentication, the internal database is not required.

## local-userdb...

Variations:

local-userdb add username <user name> password <password> [disable]
[email <address>] [role <role name>]

Add a user to the local user database. The user is initially enabled unless the disable option is used.

local-userdb del username <user name>

Delete the named user from the local user database.

local-userdb del-all

Delete all users from the local user database.

local-userdb export <file name>

Save the local user database to the specified file. Once saved, the copy command can be used to transfer the file. to another location (see page 822).

local-userdb fix-database

This command deletes and re-initializes the local database. Use with caution, save the database using the *local-userdb export* command, see above.

local-userdb import <file name>

Import the named file for use as the new local user database. This requires a valid database file downloaded into the Wireless LAN switch (see the copy command on page 822).

local-userdb modify username <user name> [disable|enable] [email <address>] [password <password>] [role <role name>]

Modify the properties of an existing user entry in the local user database. Use this to enable or disable the user, or to update the user's e-mail address, password, or role.

Parameters:

user name	Specify the login name for the user.
password	Specify the login password for the user.
address	Optional. Specify the e-mail address for the user.
role name	Specify the role applied to the user upon successful authentication. The role can be associated with various Access Control Lists (ACLs) to determine the privilege level of the user.
file name	The name of the database file to export or import.



## **Clear Commands**

#### clear arp

This command clears the ARP table.

## clear counters [fastethernet <slot>/<port> | gigabitethernet <slot>|<port>]

This command clears the counters on the specified port.

## clear crypto dp

This command displays the last few commands in the debug buffer that were sent from the control path to the data path, adding or deleting IPSec SAs and routes.

The buffer is cleared after the stored commands have been displayed.

## clear crypto <ipsec|isakmp> sa [peer <IP address>]

This command clears the IPSec or ISAKMP security association for the specified peer *IP Address*.

## clear loginsessions <id>

# clear mobile [registration-statistics <IP Address>| messages|packet-counters]

## clear vpdn [l2tp|pptp] [id <tunnel ID>]

## clear wms [ap <bssid>|probe <bsid>|sta <MAC addr>]

This command removes the specified AP, Probe, or STA from the WMS database.

## clear site-survey <building ID>

This command clears the site survey channel plan for the building specified in the *building ID* argument

## clear stm hole <BSSID>

This command clears the coverage hole information for the specified BSSID.

## **Debug Commands**

## debug...

Variations:

• debug <type> [<sub-type>...]

Turn debugging on for the specified feature type and sub-type.

• undebug {all|<*type*> [<*sub-type*>...]}

Turn debugging off for the specified feature type and sub-type.

#### Parameters:

Туре	Sub-type			
authmgr	[all] [acl] [config] [dot1xcfg] [dot1xeapol] [dot1xkeymgt] [dot1xsapmmsg] [dot1xsm] [messages] [mobility] [user]			
Alcatelcert	[all]			
crypto	[ipsec] [isakmp]			
fp	[cli] [emweb] [nim]			
ha	[api] [datapath] [dhcp] [flag] [info] [messages] [states] [timers]			
l2tp	[packets]			
localdb	[all]			
master	[api] [datapath] [dhcp] [flag] [info] [messages] [states] [timers]			
mmgr	[api] [datapath] [dhcp] [flag] [info] [messages] [states] [timers]			
mobagent	[api] [datapath] [dhcp] [flag] [info] [messages] [states] [timers]			
ppp	[packets]			
pptp	[packets]			
sapm	[all]			
stm	[all]			
wms	[all]			



## Panic Commands

#### panic clear

This command Clears all panic information from NVRAM.

# panic info [file <panicfilename> <symbolfilename>|nvram <symbolfilename>]

This command prints the contents of the specified panic file(s).

## panic list [file <panicfilename>|nvram]

This command lists all the panics in the specified *panicfilename* or in nvram.

#### panic save <panicfilename>

This command saves all the panic information stored in nvram to the specified *panicfilename*.

## **Screen Display Commands**

## encrypt <enable | disable>

This command enables and disables the on-screen encryption of keys and passwords. It must be executed from the configuration mode.

```
(Alcatel) (config) #encrypt enable
(Alcatel) (config) #
```

# page <length>

This commands sets the number of lines of text the terminal will display when paging is turned on. Valid lengths are from 24 to 100 lines.

## paging

This command turns paging on. Use the no form of this command to turn paging off.

# CHAPTER 31 Show Commands

This chapter provides a summary of the show commands available on the Alcatel Wireless LAN Switch in your network. The command summary is organized by command function. Each command entry depicts the syntax. Many provide output examples.

Show commands may only be executed from the Privileged mode. For more information on the commands, use the CLI help feature described on page 18.

## General Switch Management Commands

## **Switch Management Commands**

These commands display information about the physical and logical contents of the switch.

#### show country

This command displays the configured country code for the switch.

## show cpu load

This command displays percent of usage of the switch CPU.

#### show image version

This command displays version information about the software image.

#### show keys

This command displays the status of features on the Alcatel switch.

#### show users

This command displays administrative users and their access modes.

```
(Alcatel) # show users
User Name Access Mode
______
admin Read/Write
```

Information returned by this command is:

- User Name: The user's login name
- Access Mode: The user's privileges

## show loginsessions

This command displays information about current sessions.

(Alcatel) # show loginsessions				
ID	User Name	Connection From	Idle Time	Session Time
00	admin	10.1.1.70	00:00:00	00:06:33

Information returned by this command is:

- ID: Session ID
- User Name: The login name of the connected user
- Connection From: IP Address of the connected user
- Idle Time: The time the session has been idle
- Session Time: The total time the session has been running

#### show memory

This command shows the status of memory on the Alcatel switch.

#### show mgmt-user

This command displays the management user table.

```
(Alcatel) (config) #show mgmt-user
Management User Table
-----
USER PASSWD ROLE
---- -----
admin ***** root
administrator ***** root
```

## show startup-config

This command displays a table with all the information about the startup configuration for the switch.



#### show station-table

This command displays information about the stations connected to the switch. Executing this command with no options will display all the stations on the switch.

Options:

mac <MACaddr> Show the station with the specified MAC address.

#### show trunk

This command displays the Trunk Port table.

#### show version

This command shows the current versions of the boot code, processor, and assembly. It also displays the switch uptime, processor memory, and non-volatile configuration memory.

#### show ip radius source-interface

This command shows the currently configured address for outgoing RADIUS packets. An IP address of 0.0.0.0 means that the switch will use the interface with the best route to the RADIUS server.

(Alcatel) (config) #show ip radius source-interface

```
RADIUS client source IP address = 0.0.0.0
```

#### show firewall

This command displays the current status of the firewall.

```
(Alcatel) (config) #show firewall
Global firewall policies
------
Policy Action
------
Enforce TCP handshake before allowing data Disabled
Prohibit RST replay attack Disabled
Deny all IP fragments Disabled
Send RST on denied TCP connection Disabled
```

## show inventory

This commands shows the physical contents of the switch. It also shows the status of each power supply and fan.

```
(Alcatel) # show inventory
Supervisor Card slot
                    : 0
Supervisor FPGA Rev : 0x6 ID 0x0
Assembly#
                    : 00004A00 (Rev:02.08)
Serial#
                    : P00000016 (Date:03/14/03)
Crypto Assembly : 00005A00 (Rev:02.00) Serial#: P00000041
Mgmt Port HW MAC Addr : 00:0B:86:FF:FF:D4
Line Card HW MAC Addr : 00:0B:86:00:15:80 to 00:0B:86:00:15:FF
PEER Supervisor Card : Absent
Line Card 2
            : Present
       Line Card 2 FPGA
                                   : Rev 0x5 ID 0x1
      Line Card 2 Mez Card
                                  : Present
      Line Card 2 SPOE
                                : Present
      Line Card 2 Supervisor Card 0 : Present ( Active )
      Line Card 2 Supervisor Card 1 : Absent
Line Card 3
                    : Absent
Line Card 1
                    : Absent
Fan Tray
                    : Present
Fan O
                    : OK
Fan 1
                    : OK
Fan 2
                    : OK
Fan Speed
                    : High
Power Supply 0
                    : Absent
Power Supply 1
                    : Absent
Power Supply 2
                    : Absent
Internal Temp
                    : 30.00 degrees Celsius
                    : Current reading 5.00 Volts
SYSTEM 5.00V
                   : Current reading 3.28 Volts
SYSTEM 3.30V
SYSTEM 2.50V
                    : Current reading 2.51 Volts
                     : Current reading 2.00 Volts
CPU 2.00V
```

## show ntp servers

This command displays the currently configured time servers.

```
(Alcatel) (config) #show ntp servers server 216.244.192.3
```



#### show processes

This command shows which processes are currently running and their command paths.

PID	TTY	Uid	Size	State	Command
	1	root	548	S	init
	2	root	0	S	[keventd]
	3	root	0	R	[ksoftirqd_CPU0]
	4	root	0	S	[kswapd]
	5	root	0	S	[bdflush]
	6	root	0	S	[kupdated]
8	32	root	628	S	/sbin/cardmgr
11	11	root	0	S	[kjournald]
11	19	root	504	S	<pre>/mswitch/bin/syslogd -x -r -f /mswitch/conf</pre>
13	39	root	568	S	/bin/sh /mswitch/mysql/bin/safe mysqld
15	56	root	11252	S	/mswitch/mysql/libexec/mysqldbasedir=/ms
15	57	root	11252	S	/mswitch/mysql/libexec/mysqldbasedir=/ms
15	59	root	11252	S	/mswitch/mysql/libexec/mysqldbasedir=/ms
17	71	root	584	S	/mswitch/bin/nanny /mswitch/bin/sbcon 1 0
17	73	root	704	S	/mswitch/bin/sbConsoled
17	77	root	592	S	/mswitch/bin/nanny /mswitch/bin/nanny_list

## show clock

This command displays the current date and time.

#### show boot

This command displays the current configuration file name and the boot partition.

#### show hostname

This command displays the name of the switch, if one has been specified in the configuration file.

#### show switch ip

This command displays the switch's IP address.

## show syslocation

This command displays the physical location of the switch, if it has been specified in the configuration file.

## **Configuration Manager Commands**

## show roleinfo

This command displays the role of the switch.

## show local-switches

This command displays the IP Address and location of each local switch.

## show location

This command displays the physical location of the switch.

## show switches

This command displays the IP addresses and physical location of all the switches on the network segment.

```
(Alcatel) # show switches
All Switches
------
Ip Address Location
------
10.3.25.1 Building1.floor1
```

Information returned by this command is:

- Ip Address: The IP address of the switch
- Location: The physical location of the switch



## Layer 2/Layer 3 Commands

#### Layer 2 Commands

#### show mac-address-table

Displays the MAC addresses that have either been learned or that have been manually configured for each device.

```
(Alcatel) # show mac-address-table
Dynamic Address Count:
                             0
Static Address (User-defined) Count:
                                            0
System Self Address Count:
                                     0
Total MAC Addresses :
                             5
Maximum MAC addresses :
                                     5
MAC Address Table
_____
Destination Address Address Type VLAN Destination Port
   _____
                  _____ ____
                                     _____
00:0b:86:00:15:80
                                    vlan 1
                  Mqmt
                               1
                               7
00:0b:86:00:15:80
                                     vlan 7
                  Mgmt
00:0b:86:00:15:80
                  Mamt
                              99
                                     vlan 99
```

Information returned by this command is:

- Dynamic Address Count: The number of MAC addresses discovered dynamically by the switch.
- Static Address Count: The number of MAC addresses manually configured in the switch
- System Self Address Count
- Total MAC Addresses: The total number of addressed in the database.
- Maximum MAC addresses: The maximum number of MAC addresses allowed in the table.
- Destination Address: A specific MAC address that has been discovered or statically configured.
- Address Type: The method of creation of the MAC address, the options are; Mgmt for vlan entries, Static for manually created addresses, and Dynamic for address that the switch discovers automatically.
- VLAN: The numeric designation of a vlan created on the switch
- Destination Port: the destination port for packets containing the destination MAC address.

#### show spantree

This command display information about the status of spanning-tree ports. Execute this command with no options to view the spanning tree configuration for all the ports on the switch.

Options:

•	blocking	Displays	the	ports	in a	a blocking	state.

• forwarding Displays the ports in a forwarding state.

#### show spanning-tree

This command displays information about the spanning tree topology.

## show spanning-tree interface <interface> <slot>/<port>

#### interface = fastethernet|gigabitethernet

This command displays spanning information about the specified slot-port pair for the interface specified in the command.

```
(Alcatel) # show spanning-tree interface fastethernet 2/0
```

Interface Fa 2/0 (port 1) in Spanning tree is FORWARDING
Port path cost 19, Port priority 128
Designated root has priority 32768 address 00:0b:86:00:15:80
Designated bridge has priority 32768 address 00:0b:86:00:15:80
Designated port is 1, path cost 0
Timers: message age 0, forward delay 0, hold 0



## show vlan [<ID>]

This command displays the name and ports for the specified vlan. If the  $\langle ID \rangle$  parameter is not specified, then the command displays information for all the vlans on the switch.

Information returned by this command is:

- VLAN: The VLAN number
- Name: The name of the VLAN name
- Ports: The physical port type and port number on which the VLAN exists. Physical port types may include the following:
  - Fa Fast Ethernet
  - Pc Port channel
  - Gig Gigabit Ethernet

#### show vlan status <id>

This command displays the operational status of the specified VLAN.

#### show vlan summary

This command displays the number of existing VLANs.
## Layer 3 Commands

## show ip route [static]

```
(Alcatel) # show ip route
Codes: C - connected, O - OSPF, R - RIP, S - static
U - route usable, * - candidate default
Gateway of last resort is 10.3.25.254 to network 0.0.0.0
S* 0.0.0.0/0 [0/0] via 10.3.25.254*
C 10.3.25.0 is directly connected, VLAN1
C 10.2.12.0 is directly connected, VLAN212
C 10.2.13.0 is directly connected, VLAN213
C 10.1.5.0 is directly connected, VLAN7
```

## show routerid

This command displays the IP Address of the switch.

```
(Alcatel) # show routerid
Router Id : 10.3.25.1
```



show a	arp
--------	-----

(Alcatel) #	show arp		
Protocol	Address	Hardware Address	Interface
Internet	10.3.25.170	00:80:C8:1F:9F:D3	vlan1
Internet	10.1.5.254	00:04:E2:38:3F:E8	vlan7
Internet	10.1.5.1	00:09:5B:06:3E:E1	vlan7
Internet	10.3.25.237	00:30:F1:71:D5:BD	vlan1
Internet	10.1.5.11	00:0B:86:FF:FF:B6	vlan7
Internet	10.2.12.253	00:30:F1:71:D5:BF	vlan212
Internet	10.2.13.174	00:30:F1:71:D5:CE	vlan213
Internet	10.3.25.242	00:05:5D:79:85:FE	vlan1
Internet	10.3.25.253	00:30:F1:71:D5:E2	vlan1
Internet	10.3.25.219	00:20:E0:8E:08:29	vlan1
Internet	10.3.25.182	00:30:F1:71:D6:26	vlan1
Internet	10.3.25.254	00:0B:86:00:0B:00	vlan1
Internet	10.3.25.149	00:0B:CD:15:11:29	vlanl

# **DHCP Commands**

# show ip dhcp database

This command displays information about DHCP pools created using the *ip dhcp pool* command.

```
(Alcatel) # show ip dhcp database
# 212
subnet 10.2.12.0 netmask 255.255.255.0 {
    option domain-name "Alcatelnetworks.com";
    option domain-name-servers 10.1.1.2;
    option netbios-name-servers 10.1.1.2;
    option routers 10.2.12.254;
    range 10.2.12.21 10.2.12.253;
}
# 213
subnet 10.2.13.0 netmask 255.255.255.0 {
    option domain-name "Alcatelnetworks.com";
    option domain-name-servers 10.1.1.2;
    option netbios-name-servers 10.1.1.2;
    option netbios-name-servers 10.1.1.2;
    option routers 10.2.13.254;
    range 10.2.13.21 10.2.13.253;
```

Information returned by this command is:

- The name of the pool
- Subnet and subnet mask
- Domain names
- Domain name servers
- Netbios name servers
- Default gateways
- Range of IP addresses in the pool.

# show ip dhcp binding

This command displays a list of all the IP addresses that have been assigned by the server. It shows what IP Addresses have been assigned to each MAC Address and the date on which the assignment was made. There will be a new entry every time the MAC Address renews its lease or receives a new IP Address.



## **Interface Commands**

#### show port link-event

This command displays a count of up/down links on each of the switch's ports.

#### show port monitor

This command displays the current configuration of the port monitor.

#### show port stats

This command displays statistics about the amount of packet and byte traffic on each port.

#### show port status

This command displays the status of each port on the switch.

(Alcatel)	# show po	ort status					
Port Stati	us						
Slot-Port	PortType	adminstate	operstate	poe	Trusted	SpanningTree	PortMode
2/0	FE	Enabled	Up	Enabled	Yes	Forwarding	Access
2/1	FE	Enabled	Down	Disable	d Yes	Disabled	Access
2/2	FE	Enabled	Down	Disable	d Yes	Disabled	Access
2/3	FE	Enabled	Down	Disable	d No	Disabled	Access
2/4	FE	Enabled	Up	Enabled	No	Forwarding	Access
2/5	FE	Enabled	Down	Disable	d No	Disabled	Access
2/6	FE	Enabled	Up	Enabled	No	Forwarding	Access
2/7	FE	Enabled	Down	Disable	d No	Disabled	Access
2/8	FE	Enabled	Down	Disable	d No	Disabled	Access
2/9	FE	Enabled	Down	Disable	d No	Disabled	Access
2/10	FE	Enabled	Down	Disable	d No	Disabled	Access
2/11	FE	Enabled	Down	Disable	d No	Disabled	Access

Information returned by this command is:

- slot-port
- Port Type
- Administrate
- Operstate

- POE
- Trusted
- SpanningTree
- PortMode

# show port trusted

This commands displays a list of trusted ports.

(Alcatel) # show port trusted
Fa 2/0
Fa 2/1
Fa 2/2
Fa 2/23

Information returned by this command includes:

- The port type
- The slot and port pair



# show interface counters

This command displays the various inbound and outbound packet counters on each port.

(Alcatel)	# show inte	erface counters		
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Fa2/0	236999510	2672298	0	48
Fa2/4	305181819	3510613	0	47
Fa2/6	72455908	685872	0	47
Fa2/12	307104269	3694953	0	46
Fa2/13	273342450	3473747	0	46
Fa2/18	3707856	17188	34	1106
Fa2/22	1044473	3295	4	4451
Fa2/23	49960830	95117	281	3861
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Fa2/0	149481842	576986	583	5710
Fa2/4	168576835	677455	583	5719
Fa2/6	80821297	380311	583	5718
Fa2/12	123359080	561104	306	1036
Fa2/13	35375874	157434	306	34
Fa2/18	4662501	7591	292	3216
Fa2/22	618243	4034	306	52
Fa2/23	30056800	91694	305	1867

# show interface {fastethernet|gigabitethernet} <slot>/<port> [switchport] [allowed-vlan|native-vlan]

This command displays information about the interface. The parameters must be specified in the order shown above. The show interface command may be invoked as it with no arguments. If so, it will display verbose information about all the interface ports. Specifying parameters will provide increasing levels of granularity.

The following screen is an example of invoking the show interface command with no arguments.

#### (Alcatel) # show interface

```
Fa 2/0 is up, line protocol is up
Hardware is FastEthernet, address is 00:0B:86:00:15:81 (bia
00:0B:86:00:15:81)
Description: 10/100 Copper-Level
Encapsulation ARPA, loopback not set
Duplex ( AUTO ), speed ( AUTO )
MTU 1500 bytes, BW is 200 Mbit
Last clear of "show interface" counters 5 day 11 hr 17 min 39 sec
link status last changed 5 day 11 hr 16 min 58 sec
   10749889 packets input, 946118065 bytes
   Received 48 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 10749841 unicast
   1373076 packets output, 302155390 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
This port is TRUSTED
POE Status of the port is ON
```

Variants of the show interface command envoked with arguments are shown below.



#### show interface fastethernet <slot>/<port>

```
(Alcatel) # show interface fastethernet 2/1
Fa 2/1 is up, line protocol is down
Hardware is FastEthernet, address is 00:0B:86:00:15:82 (bia
00:0B:86:00:15:82)
Description: 10/100 Copper-Level
Encapsulation ARPA, loopback not set
Duplex ( AUTO ), speed ( AUTO )
MTU 1500 bytes, BW is 200 Mbit
Last clear of "show interface" counters 1 day 12 hr 16 min 48 sec
link status last changed 1 day 12 hr 16 min 48 sec
    0 packets input, 0 bytes
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input error bytes, 0 CRC, 0 frame
    0 multicast, 0 unicast
   0 packets output, 0 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
This port is TRUSTED
POE Status of the port is OFF
```

#### show interface fastethernet <*slot*>/<*port*> switchport

```
(Alcatel) # show interface fastethernet 2/1 switchport
Name: Fa2/1
Switchport: Enabled
Administrative mode: static access
Operational mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Access Mode VLAN: 1 (Default)
Trunking Native Mode VLAN: 1 (Default)
Trunking Vlans Enabled: NONE
Trunking Vlans Active: NONE
```

# show interface fastethernet <slot>/<port> switchport native-vlan

(Alcatel) # show interface fastethernet 2/1 switchport native-vlan
1 (Default)

## show interface gigabitethernet <slot> <port>

```
(Alcatel) # show interface gigabitethernet 2/24
Gig 2/24 is up, line protocol is down
Hardware is Gigabit Ethernet, address is 00:0B:86:00:17:99 (bia
00:0B:86:00:17:99)
Description: Gigabit-Level
Encapsulation ARPA, loopback not set
Duplex ( AUTO ), speed ( AUTO )
MTU 1500 bytes, BW is 2000 Mbit
Last clear of "show interface" counters 1 day 22 hr 28 min 34 sec
link status last changed 1 day 22 hr 28 min 34 sec
   0 packets input, 0 bytes
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 0 unicast
    0 packets output, 0 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
This port is NOT TRUSTED
```

## show interface loopback

This command displays the current configuration of the interface loopback.

#### show interface mgmt

```
(Alcatel) # show interface mgmt
mgmt is up line protocol is up
Hardware is Ethernet, address is 00:0B:86:FF:FF:D4
```



show interface port-channel <0-7>

```
(Alcatel) # show interface port-channel 0
Port-Channel id 0 is administratively up
Hardware is Port-Channel, address is 00:0B:86:00:15:81 (bia
00:0B:86:00:15:81)
Description: Unit: 0, Slot: 4, Port: 0, Link Aggregate, cardID:
0xff010001
Spanning Tree is disabled
VLAN membership:
                     1
Member port:
Last clear of "show interface" counters 1 day 12 hr 29 min 14 sec
link status last changed 1 day 12 hr 29 min 14 sec
    0 packets input, 0 bytes
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
   0 multicast, 0 unicast
   0 packets output, 0 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
Port-Channel id 0 is NOT TRUSTED
```

#### show interface vlan <1-4094>

```
(Alcatel) # show interface vlan 1
VLAN1 is up line protocol is up
Hardware is CPU Interface, Interface address is 00:0B:86:00:15:80
(bia 00:0B:86:00:15:80)
Description: 802.1Q VLAN
Internet address is 10.3.25.1 255.255.255.0
Routing interface is enable, Forwarding mode is enabled
Directed broadcast is disabled
Encapsulation ARPA, loopback not set
MTU 1500 bytes, BW is 10 Mbit
Last clear of "show interface" counters 1 day 12 hr 30 min 49 sec
link status last changed 1 day 12 hr 30 min 49 sec
Tunnels Configured on this Interface: 4212 , 4202 , 4216
```

## show local-userdb [<username>]

This command displays information about local users.

(Alcatel) # show local-userdb							
User Detai	ls						
 Name	 Password	Role	E-Mail	Enabled			
mprashant	*******	employee		Yes			
aagarwal	*******	employee		Yes			
rchou	*******	employee		Yes			
kmelkote	*******	employee		Yes			
kent	*******	employee		Yes			
pmanglik	*******	employee		Yes			
jtaylor	*******	employee		Yes			
tfroess	******	employee		Yes			
ysato	*******	employee		Yes			
dcallisch	******	employee		Yes			
test1	******	test1		Yes			
khuey	******	employee		Yes			
kester	******	employee		Yes			
rbalay	******	employee		Yes			
partha	******	employee		Yes			
sdekate	******	employee		Yes			
ghuber	******	employee		Yes			
kperedia	*******	employee		Yes			

Information returned by this command is:

- Name: The user's login user name
- Password: Password is displayed as a string of stars only
- Role: The role assigned to the user name
- Enabled



# **VPN Commands**

## **IPSec Commands**

#### show crypto dp

This command displays the last few add and delete commands sent from the control path to the data path.

## show crypto isakmp {policy | sa | key}

This command displays information about the Internet Key Exchange (IKE) policies, keys, and security associations. It displays the data encryption and authentication method(s), and how often the encryption keys are changed.

Policy option

```
(Alcatel) # show crypto isakmp policy
ISAKMP ENABLED
Protection suite priority 10
        encryption algorithm: 3DES - Triple Data Encryption
Standard (168 bit keys)
        hash algorithm: Secure Hash Algorithm
        authentication method: Pre-Shared Key
        Diffie-Hellman Group: #2 (1024 bit)
        lifetime: [300 - 86400] seconds, no volume limit
```

Key option

## show crypto ipsec transform-set [tag <transform-set-name>]

This command displays the encryption and data authentication type associations used in the *transform-set-name* specified in the tag parameter of the command. If no tag parameter is envoked, then the command will return the default transform-set.

```
(Alcatel) # show crypto ipsec transform-set
Transform set default-transform: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, },
```

## show crypto ipsec sa

This command displays the actual key(s) used for data encryption.

# show crypto dynamic-map [tag <dynamic-map-name>]

This command will display the mapping between IPSec and ISAKMP used in the *dynamic-map-name* specified in the tag parameter. If no tag parameter is envoked, then the command will return the default dynamic map.

```
(Alcatel) # show crypto dynamic-map
Crypto Map Template"default-dynamicmap" 10000
    lifetime: [300 - 86400] seconds, no volume limit
    PFS (Y/N): N
    Transform sets={ default-transform }
```

#### show crypto map

This command displays the global IPSec/ISAKMP mapping in a manner similar to the show crypto dynamic-map command.

```
(Alcatel) # show crypto Map
Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
lifetime: [300 - 86400] seconds, no volume limit
PFS (Y/N): N
Transform sets={ default-transform }
```



# **L2TP Commands**

## show vpdn tunnel {l2tp|pptp|tunnel} [id <tunnelID>]

This command displays information about the tunnel specified by tunnellD in the id parameter.

Information returned when the tunnel *id* is not specified.

```
(Alcatel) # show vpdn tunnel l2tp
L2TP Tunnel Information (Total tunnels = 1)
Tunnel ID = 17767 is up, remote id is 67
Tunnel state is SCCCN: Connection Connected
Remote Internet Address 10.3.14.199, port 1701
Control Ns 38, Nr 7
Local RWS 4, Remote RWS 8
```

Information returned when the tunnel *id* is specified.

**Note**—The tunnel *id* used in the command below is the *remote id* reported in the display above.



# show vpdn {12tp|pptp} configuration

This command displays information about the VPN tunnel settings.

#### L2TP option

PPTP option



# show vpdn {12tp|pptp} local pool [pool name>]

This command displays information about local pools.

# **VPN Dialer Commands**

# show vpn-dialer [<dialername>]

This command displays all the attributes of the specified dialername. If no dialername parameter is specified, the command will display information about all the dialers.

(Alcatel) # <b>shc</b>	w vpn-dialer
default-dialer	
Attribute	Value
PPTP	disabled
L2TP	enabled
DNETCLEAR	disabled
WIREDNOWIFI	disabled
PAP	enabled
CHAP	enabled
MSCHAP	enabled
MSCHAPV2	enabled
CACHE-SECURID	enabled
IKESECS	28800
IKEENC	3des
IKEGROUP	TWO
IKEHASH	SHA
IKEAUTH	PRE-SHARE
IKEPASSWD	w3lc0m3
IPSecSECS	7200
IPSecGROUP	GROUP2
IPSecENC	ESP-3DES
IPSecAUTH	ESP-SHA-HMAC



# **PPTP Commands**

# show vpdn pptp configuration

This command displays the VPN configuration for PPTP. This command is exactly analogous to the show vpn {l2pp|pptp} command.

# show vpdn pptp local pool [<pool\_name>]

This command displays information about local pools. This command is exactly analogous to the show vpdn {l2tp|pptp} command.

```
(Alcatel) # show vpdn pptp local pool
0 IPs used - 0 IPs free
```

## show mobile active-user-table

This command displays information about all currently active users.

# show foreign-agent [configuration|pending| security|status]

This command displays information about foreign agents associated with the switch. This information includes configuration, pending registration requests, security associations between the foreign agent and the home agent, and the current status of the foreign agent.

```
(Alcatel) # show foreign-agent configuration
SwitchIp: 10.3.25.1
                               UDP: 434
Interfaces: Device: lo IP: 127.0.0.2
Interfaces: Device: IP: 10.3.25.1
Tunnel Lifetime (secs): 500 Mode: Reverse Registration Required:
TRUE
Max Bindings: 300 Max Pending Allowed: 5 Max Pending Lifetime:
120
(Alcatel) #show foreign-agent security
Authentication Algorithm: HMac MD5
(Alcatel) #show foreign-agent status
Total Tunnels:0
                       Bindings: 0 Pending: 0
Registration Requests Status: Accepted: 0 Rejected: 0
Registration Replies Status: Accepted: 0
                                             Rejected: 0
Rejection Statistics:
Unknown Extension: 0 Malformed Packet: 0 Unknown Vendor Extension:
```



# show home-agent [configuration|{security [foreign|mobile]}|status]

This command displays information about the home agent.

```
(Alcatel) # show home-agent security mobile
Authentication Algorithm: HMac MD5 Replay Method: Nonce
SPI: 1000 Binding Life: 400 Shared Secret: Alcatel
```

show home-agent options:

configurati on	This configuration returns information related to the configuration of the home agent. There are no optional parameters or variables associated with this option.
security	The security option displays the security associations between the home agent and either foreign or mobile agents. The security option must be invoked for either foreign or mobile as shown here:
	show home-agent security foreign
	show home-agent security mobile
status	The status option returns information regarding tunnels, bindings, registration requests, and rejection statistics.

## show mobile bindings

This command displays all the users with current bindings to the home agent.

# show mobile client [verbose < IP>]

This command will display information about mobile clients currently registered with the home agent. If the command is issued without the IP argument it will simply show what clients are registered. If the command is issued with the verbose parameter and the client IP address it will return detailed information about the client.

```
(Alcatel) # show mobile client
Mobile Nodes
-----
Id Mac
                     Ιp
                                  HomeAgent Vlan Location
   ___
                                  _____ ___
                                                 _____
___
                     ___
1
   00:30:f1:71:d5:bd 10.3.25.237 10.3.25.1 1
                                                  2/4
2
   00:30:f1:71:d5:bf 10.2.12.253 10.3.25.1 212
                                                  2/12
3
   00:30:f1:71:d6:26 10.3.25.182 10.3.25.1 1
                                                  2/6
4
   00:80:c8:1f:9f:d3 10.3.25.170 10.3.25.1 1
                                                 1.2.2
5
6
   00:30:f1:71:d5:ce 10.2.13.174 10.3.25.1 213 2/13
   00:09:5b:06:3e:e1 10.1.5.1
                                  10.3.25.1 7
                                                  2/22
7
   00:0b:86:ff:ff:b6 10.1.5.11
                                  10.3.25.1 7
                                                 2/22
8
   00:04:e2:38:3f:e8 10.1.5.254
                                  10.3.25.1 7
                                                  2/22
g
   00:30:48:51:05:d5 10.1.5.10
                                  10.3.25.1 7
                                                 2/22
(Alcatel) # show mobile client verbose 10.3.25.237
Mac: 00:30:f1:71:d5:bd IP: 10.3.25.237 Roaming State: Home
Switch/Home Vlan
Home Agent: 10.3.25.1 Home Network: 10.3.25.0/24 Home Vlan: 1
Current Location (Mswitch/Vlan/Slot/Port): 10.3.25.1/1/2/4
DHCP Server: 0.0.0.0 DNS Server: 0.0.0.0 Default Gateway: 0.0.0.0
Tunnel Id: No Tunnel Mode: Auto Reverse
                                             Lifetime: 300
Authentication: HMac MD5
                        Replay Method: Nonce
                                                  Spi: 1000
Shared Secret:Alcatel
Last Req Request Sent: Never Last Req Reply Recvd: Never
Last Registration Reply Code: 0 (registration accepted) Total Error
Count: 0
```



#### show mobile configuration

This command displays information bout the mobility manager configuration.

```
(Alcatel) # show mobile configuration
Switch IP: 10.3.25.1 Master: 10.3.25.1
Mobility: Enabled Proxy Dhcp: Enabled
Local Mobility Agent: 127.0.0.2 Mobility Port: 434
Tunnel Mode: Auto Reverse Lifetime(secs): 300
Reregistration(secs): 275
Spi: 1000 Shared Secret: Alcatel Length: 32
Authentication: HMac MD5 Replay Method: Nonce Buffer Size:32
```

#### show mobile dhcp proxy-stopped

This command displays the MAC addresses that the module manager quit proxy-DHCP.

(Ald	catel	) #	shc	w mobile	dhcp	proxy-stopped		
Id	Time	÷				Mac	IP	Reason
1	Wed	Aug	6	00:17:23	2003	00:05:5d:79:85:fe	0.0.0.0	Changed Essids
2	Wed	Aug	6	00:28:18	2003	00:0b:be:8d:44:1a	10.3.25.233	Released
3	Wed	Aug	6	08:52:26	2003	00:05:5d:79:85:fe	0.0.0.0	Changed Essids
4	Wed	Aug	6	10:01:14	2003	00:05:5d:79:85:fe	0.0.0.0	Count Exceeded
5	Thu	Aug	7	19:00:41	2003	00:0b:be:8d:44:1a	10.3.25.233	Released
6	Thu	Aug	7	19:11:06	2003	00:0b:be:8d:44:1a	10.3.25.233	Released

Information returned by this command is:

- ID
- Time: The time the m-manager dropped the proxy
- Mac: The MAC address for which the proxy was dropped
- IP: The IP address of the MAC for which the proxy was dropped
- Reason: The reason the proxy was dropped

# show mobile dhcp-history [num <num\_packets>| wildcard <mc>]

This command displays a history of packets received by the mobility manager.

## show mobile home-agents {global|local}

This command displays the home agent tables.

```
(Alcatel) # show mobile home-agents global
Home Agent Table
_____
Id Subnet Netmask HomeAgent Type
__ ____
           _____
                        _____ ____
1
 10.3.25.0 255.255.255.0 10.3.25.1 Alcatel
2
  10.1.5.0 255.255.255.0 10.3.25.1 Alcatel
3
  10.2.12.0 255.255.255.0 10.3.25.1 Alcatel
 10.2.13.0 255.255.255.0 10.3.25.1 Alcatel
(Alcatel) # show mobile home-agents local
Home Agent Table
_____
Id Subnet Netmask
                        HomeAgent Type
___
  _____
           _____
                         _____ ___
1
  10.3.25.0 255.255.255.0 10.3.25.1 Alcatel
2
  10.1.5.0 255.255.255.0 10.3.25.1 Alcatel
3
  10.2.12.0 255.255.255.0 10.3.25.1 Alcatel
4
   10.2.13.0 255.255.255.0 10.3.25.1 Alcatel
```

The following information is contained in each Home Agent Table:

- ID: serial numbering of agents
- Subnet: the subnet which the agent manages
- Netmask: the subnet mask for the subnet which the agent manages
- HomeAgent: the IP address of the Home Agent
- Type: the type of switch used as the agent.



#### show mobile messages

(Alcate)	l) # <b>show</b>	mobile	messages
Datapath	n Messages	3	
Opcode	Туре	Sent	Recvd
0x4	Session	0	N/A
0x5	Forward	84	N/A
0x2	Bridge	515	N/A
0x15	Mac	12239	10972
0x17	Tunnel	0	0
0x8	Arp	262	8

The messages shown by the mobile messages command are listed below, each message table contains the opcode, type of message, number sent, and number received.

- Datapath Messages
- Master Messages
- Authentication Messages
- Station Management Messages
- Control Messages

#### show mobile packet-counters

This command displays statistics about all the packets received from the datapath by the Mobility Manager.

(Alcat	el) #	show	mobi	le pac	ket-co	unters					
Packet	Coun	t									
Туре	ARP	TCP	UDP	DHCP	ICMP	IGMP	IPIP	GRE	OTHERIP	MISC	TOTAL
Recvd Sent	295 301	20 20	183 134	348 347	1 1	3 3	0 0	296 296	4 4	47 47 47	 1197 1144

#### show mobile received-packets <num (0-50)>

(Alcatel) # show mobile :	received-pack	ets 5					
Packet History							
No. Time DestIp Type Action	Opcode	Vlan	Slot	Port	SrcMac	DestMac	SrcIp
1 Fri Aug 8 07:26:47 10.3.25.237 10.3.25.1 (	2003 0x2f GRE HANDLEI	1	2	4	00:30:f1:71:d5:b	d 00:0b:86:00:15:	80
2 Fri Aug 8 07:26:47 10.3.25.237 10.3.25.1	2003 0x2f GRE HANDLED	1	2	4	00:30:f1:71:d5:b	d 00:0b:86:00:15:	80
3 Fri Aug 8 07:26:47 10.3.25.237 10.3.25.1	2003 0x2f GRE HANDLED	1	2	4	00:30:f1:71:d5:b	d 00:0b:86:00:15:	80
4 Fri Aug 8 07:26:47	2003 0x2f GRE HANDLED	1	2	4	00:30:f1:71:d5:b	d 00:0b:86:00:15:	80
5 Fri Aug 8 07:26:47 10.3.25.237 10.3.25.1	2003 0x2f GRE HANDLEI	1	2	4	00:30:f1:71:d5:b	d 00:0b:86:00:15:	80

Information returned in the table includes:

- No
- Time
- Opcode: manufacturing information.
- Vlan: VLAN on which the packet arrived.
- Slot: Slot on which the packet arrived.
- Port: Port on which the packet arrived.
- SrcMac: Source MAC extracted from the ethernet frame.
- DestMac: Destination MAC extracted from the ethernet frame.
- SrcIP: Source IP address extracted from the ethernet frame.
- DestIP: Destination IP address extracted from the ethernet frame
- Type: Type of packet.
- Action: What action the Mobility Manager took on the packet. The possible actions are:
  - Handled The Mobility Manager buffered the packet and completed the necessary mobility management.
  - Forward The Mobility Manager returned the packet to the datapath. ed
  - Dropped The packet was silently discarded and no further action was taken.



#### show mobile registration-statistics

This command displays mobile IP packet registration statistics for a user with the IP address specified in the *IP* variable.S

```
(Alcatel) # show mobile registration-statistics 10.3.25.237
Requests: Registration: 0 Deregistration: 0 Reregistrations: 0
Replies: Registration: 0 Deregistration: 0 Accepted: 0 Denied: 0
```

## show mobile trail-archive <IPaddr>

This command displays a history of the locations, switches, and times where the specified mobile client has associated. Find a client IP address using the (alpha) **#show user command**.

#### show mobile tunnel-users <tunnel ID>

This command displays all the users using the IPIP tunnel with the tunnel-id specified in the *tunnel ID* variable.

## show mobile tunnels [ mobile-ip | sap ]

This command displays all the IPIP tunnels existing between M-switches.

```
(alpha) (config) # show mobile tunnels sap
Sap Tunnels
_____
                       Essid IP
No. TunnelId Bssid
                                            Vlan Location
                                             ----
  0x1069 00:0b:86:9d:5e:28 Alcatel-alpha-ap 10.3.25.249 1
1
                                                  1.2.3
 2
                                                1.2.3
3
 0x106b 00:0b:86:9d:5e:20 Alcatel-alpha-ap 10.3.25.249 1 1.2.3
4
 0x106c 00:0b:86:9d:5e:20 alpha-guest 10.3.25.249 7 1.2.3
5
   0x106d 00:0b:86:9d:5b:f0 alpha-guest
                                  10.2.12.252 7
                                                1.1.2
(alpha) (config) # show mobile tunnels mobile-ip
Mobile IP Tunnels
_____
No. TunnelId Local Remote
   _____ ____
                 _____
   4217 10.3.25.1 10.3.18.1
1
```

# show mobile user {address <IPaddr>|mac-address <MACaddr>}

This command displays information about a specific mobile user. The options in this command allow you to see authentication, location history, and VPN information about the user.

Options:

•	all	This option displays all mobility information about the user.
•	auth	This option displays authentication information about the user.
•	location	This option displays the last 10 locations of the user.
•	vpn	This option displays VPN information about the user.



# show mobile user-status [address <IP Address>] [mac-address <Address>]

```
(Alcatel) # show mobile user-status address 10.3.25.237
RoamingState:User is currently associated with this Mswitch which is the Home
Mswitch for the user.
The user is on the Home Vlan
Mobility State
_____
Home Agent Home Network Home Vlan DHCP State
----- ------ -------
10.3.25.1 10.3.25.0/24 1
                           Complete
DHCP Information
_____
         Ingress Vlan Source IP Dest IP Requested IP DHCP Server
Type
Relay Agent Egress Vlan Last Seen
     ______ _____ _____
____
----- -----
DHCP_REQUEST 110.3.25.23710.3.25.10.0.0.00.0.0.00.0.0.00Wed Dec 3116:00:001969
```

#### show mobile user-summary

(Alcatel) # show mobile user-summary										
Summary										
Id	Mac	Ip	User	HomeAgent	Role					
32	00:30:f1:71:d6:26	10.3.25.182		10.3.25.1	logon					
31	00:30:f1:71:d5:bd	10.3.25.237		10.3.25.1	logon					
33	00:30:f1:71:d5:bf	10.2.12.253		10.3.25.1	logon					
25	00:0b:86:00:0b:00	10.2.15.1	jtaylor		employee					
44	00:30:f1:71:d5:ce	10.2.13.174		10.3.25.1	logon					
45	00:30:48:51:05:d5	10.1.5.10		10.3.25.1	logon					

#### show mobile visitors <vlan>

This command will display all the visiting hosts currently on the specified VLAN.

## show mobile vlan-configuration

This command displays all the current VLANs on the switch.



# Air Management Commands

## **Air Monitor Commands**

```
show pcap free-space <AM IP address>
```

(Alcatel) # show pcap free-space 10.1.1.162

free-memory:1027072 bytes

This command displays the amount of memory available for pcap batch files.

## show pcap status <AM IP address>

This command displays the state of all active PCAP sessions

#### show am air-mac <am-ip> <bssid>

This command displays information about all the MACs on the wireless side of the specified air monitor.

#### show am ap-search <am-ip>

This command returns information about the access points associated with the air monitor specified in the *am-ip* argument.

## show am bssid-scan <am-ip> <channel>

This command lists the ....

Г

(Alcatel) (config) #show am bssid-scan 10.3.25.248 1									
BSSID Scanned									
bssid	beacon	rssi	active-time	inactive-time					
00:06:25:0f:6e:1f	n	19	0	0					
00:0b:86:20:27:19	n	14	0	0					
00:00:00:00:00:00	n	50	0	0					
00:0b:86:80:04:30	У	3	0	0					
00:0b:86:80:20:f0	У	23	0	0					
00:0b:86:80:13:60	У	13	0	0					
00:0b:86:20:37:30	У	23	0	0					
00:0b:86:20:27:1b	n	16	0	0					
00:0b:86:20:27:a5	У	40	0	0					
00:0b:86:20:27:8e	У	3	0	0					
00:0b:86:80:08:10	У	6	0	0					
00:0c:41:13:f9:cd	n	49	0	0					
00:30:bd:62:4b:48	У	12	0	0					
00:0b:86:b0:01:cb	У	0	0	0					
00:0b:86:b0:02:55	У	17	0	0					
00:0b:86:20:27:8f	У	6	0	0					
00:06:25:b5:6f:0a	n	1	0	0					
00:80:c8:b0:55:66	n	57	0	0					
00:0b:86:20:27:1d	У	27	0	0					

## show am channel <am-ip> <channel>

This command displays the statistics for a specific channel on the specified air monitor.

# show am ids-state <IPaddress>

This command and its options return information about the IDS state of a specified air monitor.

Options:



#### show am pot-ap-list <am-ip>

This command displays the BSSIDs seen on the specified air monitor which it cannot classify as access points.

```
(Alcatel) (config) #show am pot-ap-list 10.3.25.248
Potential AP Table
_____
              channel phy num-beacons tot-beacons mt at
bssid
____
               _____ ___
                             ----- --- ---
                                                       ___
00:0b:86:a0:01:fc 36
                      80211a O
                                         9
                                                    27 0
00:0b:86:20:27:8e 1
                      80211b 0
                                       9
                                                   12 0
00:00:0
00:0b:86:a0:04:15
00:0b:86:b0:01:47 1
06:20:27:7f 1
                     80211a 0
                                        9
                                                    13 0
                      80211b 0
                                        9
                                                   5 0
                                        9
                      80211b 0
                                                   18 0
00:0b:86:20:27:24 6
                      80211b 0
                                        9
                                                    19 0
                                       9
00:0b:86:20:27:af 1
                      80211b 0
                                                    28 0
Num Potential APs:7
```

#### show am pot-sta-list <am-ip>

This command displays the BSSIDs seen on the specified air monitor which it cannot classify as stations.

#### show am rf-summary <am-ip>

This command displays the RF statistics for all the channels being monitored by the specified air monitor.

#### show am sta-search <am-ip>

This command displays information about stations being monitored by the specified air monitor.

#### **show am state** <*am-ip*> <*bssid* | *mac*>

This command displays the internal state for an access point or station associated with the specified air monitor.

# show am stats <AM IP address> <MAC address> [verbose]

TIP: You can find an AP or AM IP address and MAC by using the show stm connectivity command.

```
show ap stats <ap-ip> <MAC address> [verbose]
```

```
      (Alcatel) # show ap stats 10.2.12.212 00:30:f1:70:49:65

      Frame rates

      ------

      retry low-speed non-unicast recv-error frag bwidth

      -----

      0
      33

      100
      0
      0

      8

      RSSI

      -----

      100
      100

      165
      13
      9

      39
```



(Alcatel) # show ap stats 10.2.12.212 00:30:f1:70:49:65 verbose Frame rates \_\_\_\_\_ retry low-speed non-unicast recv-error frag bwidth \_\_\_\_\_ \_\_\_\_\_ 0 9 100 0 7 RSSI \_\_\_\_ cur-signal low-signal high-signal cur-noise low-noise high-noise 100 100 165 12 9 39 Raw Stats \_\_\_\_\_ tx-pkt tx-byte rx-pkt rx-byte tx-retry-pkt rx-retry-pkt tx-frag-pkt rx+ 247960 19878186 27075 4577596 18 3559 0 0 + Tx Frame Type Stats \_\_\_\_\_ mqmt-pkt mqmt-byte ctrl-pkt ctrl-byte data-pkt data-byte \_\_\_\_\_ \_\_\_\_\_ 247568 19804838 0 0 392 73348 Rx Frame Type Stats \_\_\_\_\_ mgmt-pkt mgmt-byte ctrl-pkt ctrl-byte data-pkt data-byte ----- ------ ------548 25264 0 0 26527 4552332 Dest Addr Type Stats \_\_\_\_\_ bcast-pkt bcast-byte mcast-pkt mcast-byte ucast-pkt ucast-byte \_\_\_\_\_ \_\_\_\_\_ 247684 19833378 7 975 269 43833 Frame Size Packet Stats \_\_\_\_\_ type 0-63 64-127 128-255 256-511 512-1023 1024+ ---- ---- ------ ------ -----tx 96 134 114 42 3 3 rx 10397 9292 4241 1982 66 549 Tx Frame Rate Stats \_\_\_\_\_ pkt-1m byte-1m pkt-2m byte-2m pkt-5.5m byte-5.5m pkt-11m byte-11m 14 518 0 0 0 0 34 2949 Rx Frame Rate Stats \_\_\_\_\_ pkt-1m byte-1m pkt-2m byte-2m pkt-5.5m byte-5.5m pkt-11m byte-11m 1568 135551 5699 768444 5736 924896 14072 2748705

### show am association <AM IP address> <ap-bssid>

This command displays information about a specific station associated with an air monitor.

```
(Alcatel) # show am association 10.1.1.162 00:0b:86:80:24:10
Association Table
mac rsta-type auth phy-type
--- 00:0b:fd:52:dc:f6 valid yes 80211b
```

# show am ap-list <AM IP address>

This command displays basic information about access points .



show am sta-list <AM IP address>

```
(Alcatel) # show am sta-list 10.1.1.162
STA Table
_____
             bssid essid
                                             sta-type auth
mac
phy-type mt it
___
              ____
                             ____
                                             _____ ____
____ __
            ___
00:e0:00:d3:47:15 00:0b:86:16:b7:9c ethersphere valid
                                                        yes
80211b 205 2
00:80:c8:17:14:3e 00:09:5b:2f:37:a8 qa netgear wab102b valid
                                                        no
80211b 295 0
00:0b:fd:52:dc:d4 00:30:f1:70:49:5e smoketest ap b interfering no
80211b 1412 5
00:80:c8:18:93:95 00:30:f1:71:93:da ethersphere valid
                                                        yes
80211a 591 1
00:0c:41:15:1d:be 00:0b:86:16:a7:7b ethersphere valid
                                                        yes
80211b 96 1
Num STAs:5
```

#### show am config <AM IP address>

```
(Alcatel) # show am config 10.1.1.56
Wireless LAN Configuration
_____
bssid
                       tx-pwr chan lms
              essid
                                           encr mode rat+
                        _____ ___
____
              ____
                                            ----
                                                   ____
                                                          ---+
00:30:f1:70:49:6f Alcatel-alpha-ap 4 6 10.3.25.1 s-wep/ master f
00:30:f1:71:93:d5 Alcatel-alpha-ap 4 52 10.3.25.1 s-wep/ master
ff0+
```

## show am status <AM IP address>

This command displays the current status of each interface on the specified air monitor.

#### show am wired-mac <AM IP address> <BSSID>
show am version <AM IP address>

```
(Alcatel) # show am version 10.1.1.162
$Id: //depot/margot/FCS1.1/soft-ap/asap_module/release.h#51 $
$Revision: #51 $
$Author: p4build $
$DateTime: 2003/08/05 23:30:29 $
$DateTime: 2005/08/05 23:30:29 $
```

# show am scan-times <AM IP address>

This command displays the scan times for the specified Air Monitor.

```
(alpha) (config) #show am scan-times 10.3.25.248
Channel Scan Time
_____
channel scan-time RRA-scan-time mask
_____ _____
       306
             0
                            5
1
2
3
4
5
6
      35
               0
                           1
      312
              0
                            5
      35
               0
                            1
                0
       35
                            1
       314
                0
                            5
```



(Alcatel) # show am cou	nters 10.1.1.162
Counters	
Name	Value
Remove Event	4
Probe Register	4
Set Mode	3
AP Message	258
Set RAP Type	158
STA Message	278
Set RSTA Type	44
Configuration Update	4
Poll Request	777
Poll Response	387
Probe AP Type	101
Probe Get Mode	3
Probe Wired MAC Update	4
Add Event	39

# WMS Commands

WMS commands are privileged commands entered from the WMS sub-mode.

1 Enter the privileged mode.

Type configure terminal <Enter>

2 Enter the WMS mode.

Type wms <Enter>

#### show wms

This command displays information about the wireless management system and its components.

Options:

- ap *<bssid>* Displays information about a specified access point.
- ap-config Displays information about valid access point configurations.
- ap-policy Displays the ap-policy attributes.
- buildings Use this command to discover how many of each phy-type devices are in each building.
- counters This command displays all the WMS counters.
- event-threshold
   This command displays the currently configured WMS event threshold values.
- general This command displays the WMS general attributes
- global-policy This command displays the global policy attribute
- ids-policy
   This command displays the WMS general attribute
- ids-signature This command displays information about which IDS policies are enabled and the currently configured IDS parameters.
- site-survey This command displays the site survey attributes.
- sta<*MacAddr*> This command displays information about the access point.
- station-policy This command displays the station policy attributes.



#### show wms ap <BSSID>

This command displays the monitors that are listening to the access point specified in the *BSSID* argument. The soft-ap entry in the displayed data is the station itself.

(Alcatel) (config) #show wms ap 00:0b:86:20:28:13 AP Info \_\_\_\_\_ Channel Type BSSID SSID RAP Type Status \_\_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_ 00:0b:86:20:28:13 alpha-guest 1 soft-ap valid up Probe Info \_\_\_\_\_ MAC IP Loc Type Status \_\_\_ \_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_\_ 00:0b:86:20:27:a0 10.3.25.249 1.2.3 air-monitor up 00:0b:86:20:28:13 10.2.13.252 1.1.1 soft-ap up 00:0b:86:20:27:ac 10.2.12.252 1.1.2 air-monitor up 00:0b:86:20:27:a1 10.1.1.150 1.1.3 sap-monitor up 00:0b:86:20:27:a6 10.3.25.248 1.1.4 air-monitor up

# show wms sta <MAC address>

This command displays the monitors that are listening to the station specified in the *MAC Address* argument. The soft-ap entry in the displayed data is the station itself.

(Alcatel) (config) #show wms sta 00:30:f1:71:93:d5 AP Info \_\_\_\_\_ BSSID SSID Channel Type RAP Type Status \_\_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ 00:30:f1:71:93:d5 alpha-guest 48 soft-ap valid up Probe Info \_\_\_\_\_ MAC ΙP Loc Type Status \_\_\_ \_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_\_ 00:30:f1:71:94:08 10.3.25.249 1.2.3 air-monitor up 00:0b:86:a0:00:5a 10.2.12.252 1.1.2 air-monitor up 00:30:f1:71:93:54 10.3.25.248 1.1.4 air-monitor up 00:30:f1:71:93:d5 10.1.1.150 1.1.3 soft-ap up



show wms counters

(Alcatel) # show wms c	counters
Counters	
Name	Value
DB Reads	2266
DB Writes	382945
Remove Event	206
Probe Register	105
AP Message	10196
Set RAP Type	5221
STA Message	14332
Set RSTA Type	2480
Configuration Update	110
Poll Request	19091
Poll Response	19080
Probe AP Type	76
Probe Unsecure AP	1
SAP Down	13
Probe Wired MAC Update	e 107
Add Event	371

#### Site Survey Commands

```
show site survey calibration [dst<bssid> |
max-per<number> | src<bssid> ]
```

Options:

•	dst	The bssid of the destination calibration data
•	max-per	The maximum packet error rate to filter on
•	src	The bssid of the source calibration data

# show site survey channel-plan <Building> <PhyType>

This command displays information about the configured and actual channel and power settings of the AP that match the Building and PhyType arguments.

# show site survey in-progress

This commands displays information about any site survey currently in progress.

# **Station Management Commands**

This family of command displays information about station management functions.

# show stm ap-list [<essid>]

This command displays ID and location information about access points associated with the switch. You may filter on an essid to narrow the amount of information returned by the command.

#### show stm association <bssid>

This command displays information about wireless devices seen by a specified AM/AP.

## show stm config

This command displays information about the configuration of the Station Manager.

#### show stm connectivity

This command displays information about all the AMs/APs connected to the switch. You may see information about all the stations connected to the switch by using the command without specifying any options.

Options:

- bssid
   Show only information for the station with the specified bssid.
- essid
   Show only information for stations with the specified essid
- port Show only information for station on the specified port.



#### show stm dos-sta

This command displays information about stations that are currently subject to DoS (Denial of Service).

#### show stm essid

This command displays all the active essid's on the switch.

#### show stm holes

This command displays all the detected coverage holes.

#### show stm packets

This command display the last specified number of packets received by the switch. Options allow you to specify the number of packets to display up to a maximum of 128, and you may display packets for a specific AP or station by specifying the station MAC Address.

Options:

•	count	Specify the number of packets to display. Max count = 128
•	mac	The MAC address of a station or AP from which to display packets.

#### show stm state <MacAddr>

This command displays state information about a station with the specified MAC address.

#### show stm trace-addr

This command displays the information contained in the Trace Address Buffer.

#### show stm virtual-ap <bssid>

This command displays information about VLANs on a specific access point identified by its bssid.

# Alcatel Soft AP Commands

```
show ap config location <location>
```

This command displays the configuration of a specified access point. Location and BSSID information about access points may be obtained using the show stm connectivity command.

<pre>(Alcatel) (config) #show ap config location 1.1.2 CONFIG_AP_RESULT</pre>						
Location (Bldg.Flr.Loc)	1.1.2	1.1.2				
BSSID	N/A	N/A				
Channel	1	36				
ESSID	alpha-guest	alpha-guest				
Encryption	staticWep	staticWep				
Device Type	am_mode	am_mode				
Authentication	opensystem	opensystem				
Short Preamble	Enabled	N/A				
RTS Threshold (Bytes)	2333	2333				
Transmit Power (Level)	2	2				
Hidden SSID	Disabled	Disabled				
Deny_Broadcast Probes	Disabled	Disabled				
b/g Mode	mixed	N/A				
Country Code	US	US				
WPA Hexkey	N/A	N/A				
WPA Passphrase	N/A	N/A				
LMS IP	N/A	N/A				
Backup LMS	0.0.0.0	0.0.0.0				

# show ap config bssid <BSSID>

This command displays the configuration of a specified access point. Location and BSSID information about access points may be obtained using the show stm connectivity command.



#### show ap configs

This command displays the configuration information for all APs.

#### show ap effective-config bssid <BSSID>

This command displays the actual configuration that will be applied to a BSSID. The command traverses the configuration tree and site survey database to compile the configuration.

The BSSID of the access point may be obtained using the **show stm connectivity** command.

```
(Alcatel) (config) #show ap effective-config bssid 00:0b:86:9d:63:e0
CONFIG AP RESULT
_____
PARAMETER
                             802.11b/q
                             _____
_____
                            1.1.3
Location (Bldg.Flr.Loc)
BSSID
                            00:0b:86:9d:63:e0
Channel
                            1
ESSID
                           alpha-guest
Encryption
                           staticWep
Device Type
                           ap mode
Authentication
                           opensystem
Short Preamble
                           Enabled
                           2333
RTS Threshold (Bytes)
Transmit Power (Level)
                           2
                           8
Retry Limit
DTIM Interval (beacon periods) 1
                           64
Max Associations
                           100
Beacon Period (millisecs)
Basic Rates
                            1,2
                           1,2,5,11
Transmit Rates
AP Radio
                           Enabled
                           Enabled
Power Management
Station Ageout Time (secs) 1000
VLAN TD
                            7
Hidden SSID
                           Disabled
Deny Broadcast Probes
                           Disabled
b/g Mode
                           mixed
Country Code
                            US
WPA Hexkey
                           N/A
WPA Passphrase
                           N/A
LMS IP
                            10.3.25.1
Backup LMS
                            0.0.0.0
```

# show ap keys <location>

This command displays the keys for the AP in the specified location. If the encrypt feature has been enabled the keys will display as a string of asterisks (\*\*\*\*).

Use the (Alcatel) (config) # encrypt disable command to see the keys.

# show ap-leds <slot>

This command displays the AP LED state for all access points on a specified slot. The condition numbers are explained below.

Number	Condition
0	AP radio down
1	Unsecure AP found
2	Wireless LAN IDS event
3	Interference detected
4	AP overload
5	ОК
6	No AP connected

TABLE 31-1 AP LED Conditions

#### show ap locations

This command displays a simple table of AP locations. Use this command to get location information to use in other **show** ap commands.

# show ap node-config location <location>

This command displays the configuration information for all the nodes in the specified location.

# show ap node-keys location <location>

This command displays the keys for all the nodes at the specified location.See show ap keys on page 889.



#### show ap registered location <location>

Different values for STATE are as follows:

- O: SAPCP\_STATE\_INIT
  1: SAPCP\_STATE\_GOT\_TUN\_REQ
  2: SAPCP\_STATE\_SNT\_TUN\_RSP
  3: SAPCP\_STATE\_GOT\_REGISTER
  4: SAPCP\_STATE\_SNT\_REG\_RESP
  5: SAPCP\_STATE\_GOT\_CONF\_REQ
  6: SAPCP\_STATE\_SNT\_CONF\_RSP
  7: SAPCP\_STATE\_STEADY
  8: SAPCP\_STATE\_SNT\_CONF\_UPDATE
- 9: SAPCP\_STATE\_GOT\_UPDATE\_RSP
- 10: SAPCP\_STATE\_SNT\_IMG\_PULL
- 11: SAPCP\_STATE\_SNT\_APBOOT

Steady state (7) is the expected value.

#### show ap stats <IPaddr><MACaddr>

This command displays statistics about the access point specified by IP address and MAC address (bssid). The information includes aggregate statistics and RSSI stats.

# **General Authentication Commands**

```
show netservice [<name>]
(Alcatel) # show netservice Alcatel1645
Services
-----
Name Protocol Ports
---- Alcatel1645 udp 1645
```

# show destination [<name>]

```
(Alcatel) # show destination
Services
_____
Name Destination
                              Inverted
_____
                               _____
Alcatel
        10.1.1.2
                                No
user 255.255.255.255 0.0.0.0 No
RSA 10.1.1.58 No
mswitch 10.3.25.1
                               No
Alcatel2 10.1.1.3
                                No
any 0.0.0.0 0.0.0.0
                               No
```

# show user-table (Deprecated)

Options:

•	authentica- tion-method	Show users logged in with a specific authentication method.
•	ip	Show information about a specific user by IP Address.
•	location	Show information about users in a specific location.



•	mac	Show information about a specific user by MAC address.
•	mobile	Show information about mobile users.
•	name	Show information about a specific user by user name.
•	role	Show information about users with a specific role.
•	verbose	Show all the information in the user table.

#### show user

This command displays information about users, including: roles, IP addresses, MAC addresses, user names, location, associations, and authentication methods. Executing this command without options displays all users.

Options:

authentication method [method]

This option displays IP address, MAC address, user name, location, and role information for users authenticated by a specified authentication method.

The choices for authentication methods are:

- dot1x
- mac
- stateful-dot1x
- vpn
- web 🔰
- ip <IPaddr>
   This option displays VLAN, switch, and access point for a user identified by a specific IP address.
- location <*hf.l>* This option displays VLAN, switch, and access point for a user identified by a specific location.
  - mac This option displays VLAN, switch, access point, the association table, and mobility state for a user identified by a specific MAC address

•	mobile	This option displays IP address, name, role, authentication, and location information for users that have moved away or are visiting the switch.
•	name	This option displays VLAN, switch, and access point for a user identified by user name.
•	role < <i>RoleName</i> >	This option displays IP address, MAC address, name, and authentication information for all users with the specified role.
•	rows <start row=""> <range></range></start>	This option displays the information from a specified range of rows in the user table.

# show rights

(Alcatel) (conf	ig) #	show rights				
RoleTable						
Name	ACL	Bandwidth	ACL List	Туре		
ap-role trusted-ap employee vpnemployee marketing guest stateful-dot1x stateful	3 5 18 19 20 2 4 21	No Limit No Limit No Limit No Limit No Limit No Limit No Limit	control ap-acl allowall vpnlogon employee vpnemployee marketing control cplogout	System System User User User System User		
logon	1	No Limit	control captiveportal vpnlogon	User		

# show rights <role name>

This commands shows the rights assigned to a specific role name.



# IEEE 802.1x Commands

#### show dot1x config

The show dot1x config command displays the current values the 802.1x authenticator's parameters.

When the command is executed the system will display a screen similar to the one below.

```
(Alcatel) # show dot1x config
Authentication Server Timeout :30
Client Response Timeout:30
Fail Timeout :30
Client Retry Count :3
Server Retry Count :2
Reauthentication :Disabled
Reauthentication Time Interval :2147483647
Multicast Key Rotation :Disabled
Multicast Key Rotation Time Interval :1200
Unicast Key Rotation :Disabled
Unicast Key Rotation Time Interval :240
Statefull Authentication :Enabled
Statefull Authentication Response Timeout :30
```

#### show dot1x ap-table

The show dot1x ap-table command and its variants display information about access points connected to the switch.

Options:

	dynamic-wep	Displays access	points	using	Dynamic	WEP
--	-------------	-----------------	--------	-------	---------	-----

- static-wep Displays access points using Static WEP
- tkip Displays access points using TKIP

#### show dot1x supplicant-info list-all

The show dot1x supplicant-info list all command displays details about the supplicants associated with the switch.

When this command is executed the system returns a screen containing a table the includes the following information about each of the supplicants.

- MAC Address of the supplicant
- User Name
- Authentication Status (yes/no)
- AP MAC
- Encryption Key
- Authorization Mode
- EAP type

# show dot1x supplicant-info statistics

The show dot1x supplicant-info statistics command displays statistical information about each supplicant.

When this command is executed the system returns a screen containing a table that includes the following statistical information about each of the supplicants.

- MAC The supplicant's MAC Address
- Name
   User name
- Auth-Succs The number of times the supplicant has been successfully authenticated.
- Auth-Fails The total number of times the supplicant sent invalid user credentials and/or entered an incorrect password.
- Auth-Timeout The number of times authorization requests timed out.
- Reauths The number of times the supplicant has successfully reauthenticated.
- Supp-Naks The number of times a Supplicant NAK occurred. This may be due to an EAP mismatch between the supplicant and authentication server, or if the server has been configured for multiple EAP types.
- UkeyRotations
   The number of times the Unicast key associated with the supplicant has been rotated.
- MKeyRotations
   The number of times the Multicast key associated with the supplicant has been rotated.



#### Accounting, Authentication, Authorization

#### show aaa derivation-rules

This command displays derivation rules configured for an authentication server or for deriving roles based on user information.

Options:

•	server [ <name>]</name>	Display all the derivation rules configured for the specified server. Use this option without specifying a name to show rules for all servers.
•	user	Display the rules for deriving user roles based on user information.

#### show aaa kerberos server

This command displays configuration and status information for kerberos servers.

Options:

server-name Display information for a specific server.
 [<name>]

```
show aaa radius-server [server-name <name>]
```

```
(Alcatel) # show aaa radius-server
Auth Server List
_____
Pri Host IP addr Port Acct Retries Timeout Secret Status Inservice
---- -----
                  ____ ____
2
  Alcatel 10.1.1.2 1645 1646 3
                                 5
                                       Alcatel Enabled Yes
 Alcatel2 10.1.1.3 1645 1646 3 5
RSA 10.1.1.58 1645 1813 3 5
3
                                       Alcatel Enabled Yes
                                5 Alcatel Enabled Yes
4
(Alcatel) #show aaa radius-server server-name Alcatel
Auth Server List
_____
Pri Host IP addr Port Acct Retries Timeout Secret Status Inservice
    ____
                 ---- ---- ------ -----
   Alcatel 10.1.1.2 1645 1646 3 5 Alcatel Enabled Yes
```

#### show aaa server-rules <server name>

This command displays the User Rule Table for the named authentication server. You may discover the names of the current hallucination servers by using the show aaa radius-server command.

#### show aaa captive-portal

```
(Alcatel) # show aaa captive-portal
Default Role = 'employee'
Guest logon = enabled
Auto Redirect delay = 5 seconds
Auth Server List
------
Pri Name Type Status Inservice Applied
--- ---- ------
1 Alcatel RADIUS Enabled Yes 1
```

#### show aaa mac-authentication

This command displays the current configuration of MAC based authentication and a table of servers that may be used for MAC authentication.

#### show aaa vpn-authentication



#### show aaa timers

```
(Alcatel) # show aaa timers
User idle timeout = 1 minutes
Auth Server dead time = 10 minutes
```

#### show aaa bandwidth-contracts

This command displays the name of each configured bandwidth contract and its associated rate.

show aaa state messages

```
(Alcatel) # show aaa state messages
PAPI Messages
_____
Msg ID Name Since last Read Total
----- ---- -----
13 mm inter move 13
                              13
5004set master ip 17005Set switch ip 1
                              1
                               1
16 mm move user 11
                               11
RAW socket Messages
_____
            Since last Read Total
Msg ID Name
----- ---- -----
1
   raw PAP req 1
                             1
Sibyte Messages
_____
Opcode Name Since last Read Total
_____ ___
              _____
    route 24
acl 19
3
                             24
15
                             19
     ace
16
              77
                             77
  user 80
wkey 78
station 10
nat 1
17
                             80
29
                             78
30
                             10
42
                             1
    user tmout 117
ace log 62
43
                             117
53
                             62
56
     forw unenc 50
                             50
     auth 24
64
                             24
```



# show aaa state user <IP address>

```
(Alcatel) #show aaa state user 10.3.25.237
Name: Alcatel-alpha-ap, IP: 10.3.25.237, MAC: 00:30:f1:71:93:5c,
Role:ap-role, Age: 03:17:48
Authentication: No, status: not started, method: , protocol: ,
server:
Role Derivation:
ACL Hits:
```

#### show aaa state configuration

```
(Alcatel) #show aaa state configuration
SAPI state: cfgm1, fpapps1, mob1, cert0
switch IP is 10.3.25.1
Master IP is 10.3.25.1
Switch Role is master
USER: cur 11, max 12 total 29
STATION: cur 2, max 3 total 3
ACL: curr 20, tunnel 0
```

#### show aaa radius-attributes

This command displays a list of RADIUS attributes that the server will recognize. For an attribute not on the list to be recognized by the Alcatel switch it must be configured using the aaa radius-attributes add command.

#### show aaa stateful-authentication dot1x <name>

This command displays configuration information about RADIUS server/access point pairs used for stateful 802.1x authentication.

show aaa localdb-server [server-name <name>]

#### show aaa dot1x

The show aaa dot1x commands displays which servers are configured for 802.1x authentication, the priority of each server, and the default role assigned to all users authenticated under 802.1x.

When the command is executed the system will display a screen similar to the one below.

```
(Alcatel) # show aaa dot1x
Mode = 'Enabled'
Default Role = 'guest'
Auth Server List
-----
Pri Name Type Status Inservice Applied
--- ---- -----
1 Alcatel RADIUS Enabled Yes 1
2 IAS RADIUS Enabled Yes 1
```

- Pri The order in which the server will be queried for authentication
- Name The name of the authentication server
- Type The server type
- Status Enabled or Disabled
- Inservice This field indicates the status of connectivity between the switch and the server.



```
show aaa auth-server [server-name <name>]
[server-type {radius|ldap|local}] [auth-method
{cp|mac|vpn|dot1x}]
```

This command displays configuration information about authentication servers. The available options allow you to see all servers (no arguments), or you may view the servers by server type or authentication method.

#### show aaa web admin-port

This command displays the configured admin port numbers.

```
(Alcatel) (config) #show aaa web admin-port
https port = 4343
http port = 80
```

#### Local Database Commands

```
show local-userdb [username <user name>]
```

Show the local user database used for authentication.

#### **Dialer Commands**

# show vpn-dialer [<dialer name>]

This command displays the configuration information for the named VPN dialer. If execute the command without specifying a dialer name the command will return the configuration of all VPN dialers on the switch.

# **Access Lists Commands**

# show access-list [<name>|<number>]

Display a list of the configured ACLs, or a specific ACL by name or number. See show ip access-list.

```
(Alcatel) # ip access-list session employee
employee
_____
Priority Source Destination Service Action Opcode TimeRange
Log Expired Queue
                        ----- -----
        _____
              _____
                                             _____
   _____
          ____
      any any tcp 80 permit
High
2
                   any permit
      any any
Low
```

# show acl]

This command displays information from the acl and ace tables.

Options:

- ace-table This option does a screen dump of the ace table entries.
- acl-table
   This option displays the ACL table
- hits This option displays a table of ACL hits by user role.



# show ip access-list [<name>|<number>]

Preferred from of the show access-list command. Display a list of the configured ACLs, or a specific ACL by name or number.

```
(Alcatel) # show ip access-list control
ip access-list session control
control
_____
Priority Source Destination Service
                                   Action Opcode Log Queue
----- ----- ------
                                    ----- ----- ----
1
        any
               any
                          svc-dhcp
                                   permit
                                                      Low
2
        user
                          svc-nbns permit
                                                      Low
               any
3
                          svc-dns
                                   permit
                                                      Low
       user anv
4
                          svc-tftp permit
        user
               any
                                                      Low
5
        user
               any
                           svc-gre
                                    permit
                                                      Low
6
                          svc-bootp permit
                                                      Low
        any
               any
7
                           svc-icmp
                                    permit
                                                      Low
        user
               any
```

#### show session-access-list

This command displays a list of access control lists.

```
(Alcatel) # show session-access-list
control
dew
airmon
employee
captiveportal
allowall
vpnlogon
guest
stateful-dot1x
stateful-kerberos
89
```

#### show time-range

This command displays currently configured time ranges.

# **MUX Commands**

#### show mux

This command displays information about the MUX configured on the switch. Options:

•	config	This option displays the current configuration of the MUX.
•	state	This option displays the current operational state of the MUX.
•	vlan	This option displays the VLANs assigned to the MUX



# **Enhanced Show Commands**

Depending on the target of the show command, the output is more clearly formatted in summary or detail tables:

Summary Tables

The show commands that display information for a general feature or a large set of items output columns of information in a summary table. For example:

(Alcatel) # show datapath user table									
User Table Entries									
IP	 MAC	ACL	Contract	Location	Flags				
10.5.10.2	00:00:00:00:00:00	36	0	0.0.0					
10.5.168.101	00:90:7A:01:1C:72	34	0	1.1.8					
10.5.168.103	00:90:7A:01:35:01	34	0	1.1.8					
10.5.168.102	00:90:7A:01:2D:B7	34	0	1.1.8					
10.5.168.105	00:90:7A:01:2C:36	34	0	1.1.8					
10.5.168.104	00:90:7A:01:2C:D9	34	0	1.1.8					
10.5.168.107	00:90:7A:01:2E:30	34	0	1.1.8					
10.5.168.106	00:90:7A:01:13:1D	34	0	1.1.8					
10.5.2.16	00:00:00:00:00:00	3	0	1.1.6					
10.5.2.18	00:00:00:00:00:00	3	0	1.1.8					
10.5.2.93	00:04:E2:64:C1:C0	36	0	1.1.8					
10.5.2.228	00:05:4E:41:EB:D0	36	0	1.1.1	A				
10.5.2.236	00:03:93:EC:C2:37	1	0	1.1.6					
10.5.2.245	00:90:7A:01:1B:8E	34	0	1.1.8					
10.5.2.247	00:90:7A:01:1D:47	34	0	1.1.1					
10.5.2.246	00:90:7A:01:3F:6B	34	0	1.1.4					
10.5.2.240	00:0B:BE:8D:44:1A	1	0	1.1.6					
10.5.2.242	00:04:23:4A:F5:FF	36	0	1.1.8					
10.5.2.252	00:90:7A:01:48:EF	34	0	1.1.1					

**NOTE**—You can also force most general show commands to present information in the detail list format by adding the verbose option to the end of the command (such as show Wireless LAN verbose)

#### Detail Lists

The show commands that display information for a specific device, protocol, or event present detailed information in a list format. For example.

(Alcatel) # show ap config location 0.0.0							
CONFIG AP RESULT							
PARAMETER	802.11b/g	802.11a					
Location (Bldg.Flr.Loc)	0.0.0	0.0.0					
BSSID	N/A	N/A					
Channel	1	36					
ESSID	ether	sphere					
Encryption	staticWep,dynamicWep	TKIP					
Device Type	ap_mode	ap_mode					
Authentication	opensystem	opensystem					
Short Preamble	Disabled	N/A					
RTS Threshold (Bytes)	2333	2333					
Transmit Power (Level)	2	2					
Retry Limit	8	3					
DTIM Interval (beacon periods)	1	1					
Max Associations	50	50					
Beacon Period (millisecs)	100	100					
Basic Rates	1,2,5,11	48.54					
Transmit Rates	1,2,5,11	48,54					
AP Radio	Enabled	Enabled					
Power Management	Enabled	Enabled					
Station Ageout Time (secs)	1000	1000					
VLAN ID	0	0					
Hidden SSID	Disabled	Enabled					
Deny Broadcast Probes	Disabled	Enabled					
b/g Mode	mixed	N/A					
Country Code	US	US					
WPA Hexkey	N/A	N/A					
WPA Passphrase	N/A	N/A					
LMS IP	N/A	N/A					
Backup LMS	0.0.0	0.0.0.0					



**OmniAccess Reference: AOS-W System Reference** 

# Part 6

# Appendices





**OmniAccess Reference: AOS-W System Reference** 

# Glossary

#### 10BaseT\*

An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) with twisted pair cabling and a wiring hub.

#### 802.11 standard\*

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (Wireless LANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), http://standards.ieee.org. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi, 802.11, is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for Wireless LANS operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

#### 802.11a\*

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

#### 802.11b\*

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

#### 802.11g\*

Similar to 802.11b, but this standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

#### Access point\*

A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

There are various types of access points and base stations used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

#### Air Monitor

A wireless access point used to detect wireless devices within range of itself for the purpose of determining the existence near the network and to monitor their activity.

#### Application software\*

A computer program that is designed to do a general task. For example, word processing, payroll, Internet browsers and graphic design programs would all be considered applications.

#### Authentication server

An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. Example: Microsoft IAS is an Authentication Server.

#### Authenticator

An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. Example: OmniAccess-6000 is an 802.1x Authenticator.

#### Backbone\*

The central part of a large network that links two or more subnetworks and is the primary path for data transmission for a large business or corporation. A network can have a wired backbone or a wireless backbone.

#### Bandwidth\*

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

#### Bits per second (bps)\*

A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second—bps— is often confused with bytes per second—Bps. While "bits" is a measure of transmission speed, "bytes" is a measure of storage capability. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps or 11 Mbits/sec), it is sending data at 1.375 megabytes per second (1.375 MBps).

#### Bridge\*

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.



#### Bus adapter\*

A special adapter card that installs in a PC's PCI or ISA slot and enables the use of PC Card radios in desktop computers. Some companies offer one-piece PCI or ISA Card radios that install directly into an open PC or ISA slot.

#### Captive Portal

A secure, dedicated, web connection between a client station and a server.

#### Certificates

Certificates are digital documents which are commonly used for authenticating users, computers and for securing information on open networks. Certificates bind public keys to the entity that possesses the private key and are digitally signed by the issuing certification authority (CA).

#### Certification authority (CA)

A certification authority is an entity which is responsible for establishing and vouching for the authenticity of public keys belonging to subjects (usually users or computers) or other certification authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and certificate revocation.

#### CLI

Command Line Interface

#### Client\*

Any computer connected to a network that requests services (files, print capability) from another member of the network.

#### Client devices\*

Clients are end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

#### Collision avoidance\*

A network node characteristic for proactively detecting that it can transmit a signal without risking a collision.
# Crossover cable\*

A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.

# CSMA-CA\*

CSMA/CA is the principle medium access method employed by IEEE 802.11 Wireless LANs. It is a "listen before talk" method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a Wireless LAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

# CSMA/CD\*

A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

# DC power module\*

Modules that convert AC power to DC. Depending on manufacturer and product, these modules can range from typical "wall wart" transformers that plug into a wall socket and provide DC power via a tiny plug to larger, enterprise-level Power Over Ethernet systems that inject DC power into the Ethernet cables connecting access points.



# DHCP\*

A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

#### Diversity antenna\*

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference.

#### DNS\*

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

#### DoS

Denial of Service.

### EAP

(Extensible Authentication Protocol) is a general protocol for PPP authentication which supports multiple authentication mechanisms.

### EAP-TLS

(EAP-Transport Level Security) is used in certificate-based security environments. It provides the strongest authentication and key determination method. EAP-TLS provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the client and the authenticator.

# EAP-TTLS

(EAP- Tunnelled TLS Authentication Protocol) is an EAP protocol that extends EAP-TLS. In EAP-TLS, a TLS handshake is used to mutually authenticate a client and server. EAP-TTLS extends this authentication negotiation by using the secure connection established by the TLS handshake to exchange additional information between client and server. In EAP-TTLS, the TLS handshake may be mutual; or it may be one-way, in which only the server is authenticated to the client.

# Encryption key\*

An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

## Enterprise\*

A term that is often applied to large corporations and businesses. The enterprise market can incorporate office buildings, manufacturing plants, warehouses and R&D facilities, as well as large colleges and universities.

### ESSID\*

The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

### Ethernet\*

International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

# Firevvall\*

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

### Gateway\*

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

### Hub\*

A multiport device used to connect PCs to a network via Ethernet cabling or via WiFi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub



transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

# HZ\*

The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.

### I/O\*

The term used to describe any operation, program or device that transfers data to or from a computer.

### ICSA

International Computer Security Association.

### IEEE\*

Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

### IEEE802.11\*

A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. WECA's focus is on 802.11b, an 11 Mbps high-rate DSSS standard for wireless networks.

#### IP\*

A set of rules used to send and receive messages at the Internet address level.

# IP address\*

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

## ISA\*

A type of internal computer bus that allows the addition of card-based components like modems and network adapters. ISA has been replaced by PCI and is not very common anymore.

### ISDN\*

A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.

### ISO Network Model\*

A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- 1, Physical\*
- 2, Data Link\*
- 3, Network\*
- 🧧 4, Transport\*
- 5, Session\*
- 6, Presentation\*
- 7, Application\*

 The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sub-layer.

### IKE

Internet Key Exchange. The Internet Key Exchange (IKE) protocol is a key management protocol standard which is used in conjunction with the IPSec standard.

# IPSec

IPSec is an IP security feature that provides robust authentication and encryption of IP packets.



# L2TP

Layer 2 Tunnelling Protocol. L2TP is an extension of Point-to-Point Protocol (PPP).

### LAN\*

A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or Wireless LAN.

#### Laser-beam

A stream of de-authorization packets sent from an Air Monitor (AM) to an Access Point (AP), enforcing security policies. Typically when a Rogue AP has been detected.

#### MAC\*

Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

# Mapping\*

Assigning a PC to a shared drive or printer port on a network.

#### Mobile professional\*

A salesperson or a "road warrior" who travels frequently and requires the ability to regularly access his or her corporate networks, via the Internet, to post and retrieve files and data and to send and receive e-mail.

### NAT\*

A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

# Network name\*

Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

## NIC\*

A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

### PC card\*

A removable, credit-card-sized memory or I/O device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

# PCI\*

A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

# PEAP

(Protected EAP) is an authentication protocol that uses TLS to enhance the security of other EAP authentication methods. PEAP for Microsoft 802.1X Authentication Client provides support for EAP-TLS, which uses certificates for both server authentication and client authentication, and Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MS-CHAP v2), which uses certificates for server authentication and password-based credentials for client authentication.

# PHY\*

The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The PHY defines parameters such as data rates, modulation method, signalling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.



# Plug and Play\*

A computer system feature that provides for automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

#### PPTP

Point-to-Point Tunnelling Protocol. A secure method of transmitting data on a virtual private network (VPN).

#### Proxy server\*

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.

### RADIUS

(Remote Authentication Dial-In User Service) is a distributed client/server system that secures networks against unauthorized access. OmniAccess-6000 can be configured as a RADIUS Client and send authentication requests to the configured RADIUS servers that contains all user authentication and network service access information.

#### Range\*

How far will your wireless network stretch? Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile.

#### RJ-45\*

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

#### Roaming\*

Moving seamlessly from one AP coverage area to another with no loss in connectivity.

### Rogue AP

A Rogue AP is an unauthorized access point attached to a network, and providing unauthorized access to that network.

# Router\*

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

#### Server\*

A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

#### Site survey\*

The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

### SSH

Secure SHell, also known as secure socket shell. A UNIX-based command interface used to gain secure access to a computer or computer network. Alcatel implements OpenSSH.

**Note**—It is Alcatel's policy in supporting OpenSSH to continuously apply security patches and bug fixes. However, Alcatel does not update the OpenSSH version string when security patches do not update the version. Changing the version introduces possible incompatibilities with SSH client v3.2.0b267 and 4.1.3.2.

### SSID\*

A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one Wireless LAN from another, so all access points and all devices attempting to connect to a specific Wireless LAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.



# SSL\*

Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session

#### Subnetwork or Subnet\*

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

### Supplicant

An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link. Example: Win-XP/2K Wireless station is a supplicant.

#### Switch\*

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

### TCP\*

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

# TCP/IP\*

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

# TLS

(Transport Layer Security) provide privacy and data integrity between two communicating applications.

# Virtual AP

An instance of a unique virtual access point.

### VPN\*

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

# WAN\*

A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (Wireless LANs).

# War Driver

A program or utility used to discover and gain unauthorized access to wireless access points in order to corrupt or collect information stored on the network.

### WEP\*

Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.



#### Wi-Fi\*

An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

Wireless LAN\*

Also referred to as LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

WMS

Wireless LAN Management System

#### WPA WPA/2

Wireless Protected Access and the update to this standard.

<sup>\*</sup>Wi-Fi Alliance terms and definitions used by permission.



**OmniAccess Reference: AOS-W System Reference**