OmniAccess RN™

User Guide

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, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 60/61, Alcatel 70, and Alcatel 52 are trademarks of Alcatel Internetworking, Inc. in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of 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.

Contents

	Preface xi
	Document Organization
Chapter 1	Deploying Access Points 1
	Overview
Chapter 2	Secure Remote Access
	Deploying a Branch Office/Home Office Solution11Securing Communications12How the Secure Remote Access Point Service Works12Configuring the Secure Remote Access Point Service14Double Encryption22
	Managing Software Feature Licenses 1
	Alcatel Software Licenses 1 Software License Types 1 Obtaining a Software License 2 The Software Licensing Process 2 Software License Certificates 2 The System Serial Number 3 The Alcatel License Management 4 Applying The License Key 4

	Additional Software License Information5Permanent Licenses5Evaluation Licenses5Deleting a License Key7Moving Licenses7Switch Resetting7License Fraud Management8Getting Help with Licenses8
Chapter 3	Configuring Network Parameters
	Conceptual Overview
Chapter 4	Configuring Redundancy 17 Conceptual Overview
Chapter 5	Adding a Local Switch31Configuring Local Switches32Configuring the Local Switch32Configuring the L2 / L3 Settings35Configuring Trusted Ports35Configure the APs35Reboot the APs36
Chapter 6	Configuring Wireless LANs 39 Conceptual Overview
	Configuring Wireless LAN—802.11 Networks 40 Pre-requisites 40 Configuring Wireless LANs—Radio
	Configuration 47 Configuring Wireless LANs—Advanced . 49 Example

	Adaptive Radio Management.53Deciding the Channel Setting54Deciding Power Settings54Advantages of Using ARM54Configuring ARM55
Chapter 7	The External ServicesInterface57Understanding ESI57Load Balancing59Configuring the Alcatel ESI59Configuring the ESI servers60Configuring the User Policy62
Chapter 8	Configuring Firewall Roles and Policies
Chapter 9	Configuring AAA Servers81Authentication Timers81Accessing the Configuration page81Authentication Servers83RADIUS Server Configuration83Editing an Existing Entry85Deleting an Existing Entry85Advanced AAA Settings86Selecting the Right Server87Configurations87Example Deployment89Editing an Existing Entry91Deleting an Existing Entry92Internal Database92Editing an Existing Entry95Deleting an Existing Entry95Configuring Server Rules95Example95Example95Example95Example95Example95Example95Example95Example97
Chapter 10	Configuring the Captive Portal



	Guest Logon	. 99 103
	User Logon	104
	Captive Portal	108
	Personalizing the Captive Portal Page .	111
Chapter 11	Configuring 802.1x Security	117
	Default Open Ports	118
	Authentication Only	118
	Sorvers	101
	Example	124
		126
		130
	Configuring MAC-based	
	Authentication	133
	Configuring the Switch	133
	Configuring Users	135
	Configuring 802.1x for Wired Users	137
	Modifying the 802.1x Settings	138
	Resetting the 802.1x Settings	138
	of 802.1x	139
Chapter 12	Configuring Virtual Private	
	Networks	143
	VPN Configuration	1/3
	Enabling VPN Authentication	143
	Configuring VPN with I 2TP IPSec	145
	Enabling Src NAT.	147
	IKE Shared Secrets	147
	IKE Policies	148
	Configuring Alcatel Dialer Example.	150
	Examples	152
Chapter 13	Intrusion Detection	163

Rogue/Interfering AP Detection	163
Denial of Service Detection	164
Man-In-The-Middle Detection	164
Signature Detection	165
Wireless LAN Policies	165
Configuring Rogue AP Detection	166
Configuring Denial of Service	
Attack Detection	168
Configuring Man-In-The-Middle	
Attack Detection	171
Configuring Signature Detection	173
Adding a New Signature Pattern	175
Configuring Wireless LAN Policies .	178
Configuring Wireless Bridge	
Detection	179

Chapter 14 System and Network Management 185

	Configuring SNMP for the Alcatel Mobility Controller
	Points 189 SNMP Traps from the Switch 196 SNMP traps from Access Point/Air
	Monitor
Chapter 15	Configuring Quality of Service for Voice Applications
Chapter 16	Topology Example One 219
Chapter 17	Topology Example Two 227
Chapter 18	Topology Example Three 239
Chapter 19	Topology Example Four 253 Topology Diagram

Topology Description 255



OmniAccess RN: User Guide

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

Document Organization

This user guide includes instructions and examples for commonly used, basic wireless LAN (Wireless LAN) switch configurations such as Virtual Private Networks (VPNs), firewalls, and redundancy. This guide shows you how to configure your environment with the most commonly needed features and services.

To use this guide effectively, apply the configuration or configurations required and skip the rest. Unless otherwise indicated, chapters are not dependent on each other. That is, you do not need to configure a feature in an earlier chapter before you can configure a feature in a subsequent chapter. Chapter order is not significant.

For information on parameters and settings on the WebUI, refer to the *Alcatel AOS-W Reference Guide*.

Related Documents

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

- Alcatel Mobility Controller Installation Guides
- Alcatel AP Installation Guides
- Alcatel AOS-W Reference Guide

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:				
	 Sample screen output System prompts Filenames, software devices, and certain commands when mentioned in the text. 				
Commands	In the command examples, this bold font depicts text that the user must type exactly as shown.				
<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.				

TABLE P-1 Text Conventions

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 RN: User Guide

CHAPTER 1 Deploying Access Points

This chapter outlines the recommended methods used to deploy and provision Alcatel Access Points (APs) in an enterprise network environment, detailing the various provisioning options and steps required.

Overview

Alcatel wireless APs (also applicable to APs deployed as Air Monitors (AMs) are designed to be low-touch configuration devices that require only minimal provisioning to make them fully operational on an Alcatel-enabled Wireless LAN network. Once the AP has established Layer-3 communication with its host Alcatel Mobility Controller, advanced configuration and provisioning may be applied either to individual APs or globally across the entire wireless network centrally using the WebUI of the Master Alcatel Switch.

Getting Started

1. Planning

Decide where you wish to locate the APs in advance of physical installation. Alcatel RF Plan can be utilized to provide an AP placement map relative to a building floor plan to ensure optimal RF coverage. (For more information on RF Plan, see the *Alcatel RF Plan for Windows User Guide*.)

When deploying APs, note the AP MAC address and serial number against the physical location. This will be useful in assigning location code identifiers to APs (see "Assigning AP Location Codes" below), which will greatly enhance location-based services and wireless network calibration. 2 Provisioning the Network for AP-Switch Communications

There are deployment prerequisites that must be met before deploying APs in a live network environment. These prerequisites ensure that the APs are able to discover and attach to a host Alcatel Mobility Controller (defined as the master). This also relieves the administrator from the need to manually configure each AP.

Note—Alcatel APs can only obtain their software image and configuration from a master Alcatel Mobility Controller.

The deployment prerequisites for Alcatel APs are:

• A Valid IP Address

Alcatel APs require a unique IP address on a subnet that has routable Layer-3 connectivity to a master Alcatel Mobility Controller. Alcatel recommends assigning the AP an IP address via DHCP (either from an existing network server or directly from an Alcatel Mobility Controller configured with a DHCP server).

To configure the AP IP address, go to "Assigning the IP Address to the AP".

Master Alcatel Mobility Controller/loopback IP Address

This is the IP address from which the AP will attach to and obtain its software image and configuration. The master Alcatel Mobility Controller/loopback IP address can be provided to an Alcatel AP using one of the following methods:

DNS Server Configuration	Alcatel APs are factory configured with Alcatel-master as the DNS host name. A DNS server on the network can be configured with an entry for Alcatel-master with the master Alcatel Mobility Controller/loopback IP address as the resolution. To configure this option see "DNS Server-derived AP
	Provisioning ".
DHCP Server Configuration	A DHCP server on the same subnet as the AP can be configured to not only provide the AP its own IP address, but also provide the IP address of a master Alcatel Mobility Controller to which the AP should attach. This is achieved by configuring the DHCP standard vendor specific option (attribute 43) in the DHCP server, with the desired master Alcatel Mobility Controller/loopback IP address. When the DHCP server returns its offer to the AP, this attribute will be returned with it. To configure this option see "DHCP Server-derived AP Provisioning ".

Alcatel Discovery Protocol (ADP) - Plug and Play	Alcatel APs are factory configured with ADP, a feature that allows plug and play provisioning for APs connected via Layer 2/3 to a master Alcatel Mobility Controller on an ADP-enabled network. ADP equipped APs send out periodic multicast and broadcast queries to locate a master Alcatel Mobility Controller. If an Alcatel switch is present in the same broadcast domain as the APs, it will respond with the switch/loopback IP address of the master switch. If the APs and Alcatel switch reside in different broadcast domains, the APs can discover the Alcatel master switch using IP multicast (IP multicast must be enabled in the network for this to function). The ADP multicast queries are sent to the IP multicast group address 224.0.82.11. Alternatively, you can configure a master Alcatel Mobility Controller address as the IP Helper/relay address on any Layer-3 switch on the same broadcast domain as the APs, thus mitigating the need to enable multicast in the network. ADP also functions for APs connected directly to Ethernet ports on a master Alcatel Mobility Controller. To configure this option see "Alcatel
	Ethernet ports on a master Alcatel Mobility Controller. To configure this option see "Alcatel Discovery Protocol (ADP)".



Step 2a. Assigning the IP Address to the AP

Either configure a DHCP server in the same subnet where the APs will be connected to the network, or configure a device in the same subnet to act as a relay agent for a DHCP server on a different subnet that can provide the AP with its IP information.

If you are planning on using a network-based DHCP server, skip to "AP-Master Switch Provisioning".

If the APs are on the same subnet as the master Alcatel Mobility Controller, the Alcatel switch can be used as a DHCP server to manage IP address assignment to APs. (The Alcatel Mobility Controller must be the only DHCP server for this subnet.)

To enable DHCP server capability on an Alcatel switch:

- Navigate to the **Configuration > DHCP Server** page.
- Create a DHCP server pool configuration.
- Create an excluded address range.
- Click **Apply** to apply the configuration to the switch.
- Click **Start** to start the on-switch DHCP server.

Step 2b.AP-Master Switch Provisioning

It is imperative that the administrator chooses one of the aforementioned options to provide the Access Points with the master Alcatel Mobility Controller/loop-back IP address. To configure each of these options see below:

DNS Server-derived AP Provisioning

When DNS server-derived provisioning is the chosen option to provide the AP with the master Alcatel Mobility Controller/loopback IP address, verify that the DNS server used by the AP (usually supplied by DHCP) has an entry configured for the standard name Alcatel-master.

Note—The APs request for DNS resolution is for the Fully Qualified Domain Name Alcatel-master so make sure that this name is configured. After initial provisioning, if the default domain name values are changed, make sure the AP and switch domain name settings match.

Alcatel recommends DNS server-derived AP configuration because it involves minimal changes to the network and offers the greatest flexibility in placement of APs.

If you select this option, skip the remainder of this section and proceed to "Deploying APs in the Network".

DHCP Server-derived AP Provisioning

When DHCP server-derived provisioning is the chosen option to provide the AP with the master Alcatel Mobility Controller/loopback IP address, make sure the DHCP server is configured to return the Alcatel vendor-specific attribute information in its DHCP offer to the AP.

Configure the DHCP server to send the Alcatel master switch IP address within the DHCP vendor-specific attribute option 43. The vendor class identifier used to identify DHCP requests from Alcatel APs is AlcatelAP.

NOTE—DHCP requires the format and contents of the vendor class identifier to be correct (AlcatelAP).

If you select this option, skip the remainder of this section and proceed to "Deploying APs in the Network".

Alcatel Discovery Protocol (ADP)

Note—When APs are NOT on the same broadcast domain as the master Alcatel Mobility Controller, you must enable multicast or employ IP Helper to relay broadcast messages across the network for ADP to function correctly.

If ADP is the preferred option to provide the AP with the master Alcatel Mobility Controller/loopback IP address, and the APs are on the same broadcast domain as any master Alcatel Mobility Controller, no additional network configuration is required. APs will send broadcast queries to which a master Alcatel Mobility Controller will respond, along with its switch/loopback IP address, and the APs will boot to this switch.

ADP is enabled on all Alcatel Mobility Controllers by factory default. However, to ensure that ADP discovery is enabled on your switch use the following command:

```
(Alcatel4324) #show adp config
```

```
ADP Configuration
key value
discoveryenable
igmp-joinenable
```

If ADP discovery is not enabled, use the following command to enable it:

```
(Alcatel4324) (config) #adp discovery enable
```

When APs are connected to Alcatel switches indirectly (via an IP-routed network), the administrator needs to make sure that multicast routing is enabled in the network, and that all routers are configured to listen for IGMP joins from the master Alcatel Mobility Controller and to route these multicast packets.

Make sure both ADP discovery and IGMP-join options are enabled. Verify using the **show adp config** command as shown above.

Should ADP discovery or IGMP-join options not be enabled:



• Enable ADP discovery by entering:

(Alcatel4324) (config) #adp discovery enable

• Enable IGMP join by entering:

(Alcatel4324) (config) #adp igmp-join enable

Proceed to "Deploying APs in the Network" below.

3 Deploying APs in the Network

You are now ready to physically install the APs and attach them to the network. (For information on mounting and powering options please refer to the AP hardware installation guide that shipped with the AP.)

When deploying APs, note the AP MAC address and serial number against the physical location. This will be useful in assigning location code identifiers to APs (see "Assigning AP Location Codes" below), which will greatly enhance location-based services and wireless network calibration.

- Physically install the Access Point in the desired location.
- Connect the Access Point to the network port.
- Make sure power is available to the AP using 802.3af-compliant Power over Ethernet (PoE) or via the optionally available AC power adapter kits. (The **POWER** and **ENET** LEDs on the AP will respectively indicate power/network link states.)
- APs will now attempt to locate their master Alcatel Mobility Controller in the network.
- 4 Assigning AP Location Codes

Now the APs are provisioned on the network, the final step in Access Point deployment is to configure (re-provision) each AP with a unique location code, which is used for location service capability. This location code is numerical and in the format 1.2.3 (where 1=building, 2=floor, 3=location). This can be configured for each AP in the network using the WebUI of the master Alcatel Mobility Controller.

To configure an AP with a unique location code:

Navigate to the Maintenance > Program AP > Re-provision page.

This page displays a list of APs that have registered with the Master switch with either their default location code (-1.-1.-1) or their currently configured location code (if the AP has been provisioned already).

	Provision	Re-Provision				
Sea	arch					
	Location	AP IP *	AP Type 🔺	AP MAC Address *	AP Serial Number 🔶	
С	Not set	192.168.0.151	AP-70	00:0b:86:c4:01:ea	A50000345	
С	Not set	192.168.0.152	AP-70	00:0b:86:c4:01:74	A50000286	
С	Not set	192.168.0.153	AP-70	00:0b:86:c4:01:7c	A50000290	
С	Not set	192.168.0.155	AP-70	00:0b:86:c4:00:d2	A50000205	
С	Not set	192.168.0.156	AP-70	00:0b:86:c4:01:ba	A50000321	
С	Not set	192.168.0.162	AP-70	00:0b:86:c4:01:ec	A50000346	
С	Not set	192.168.0.172	AP-70	00:0b:86:c4:01:3e	A50000259	
С	Not set	192.168.0.173	AP-70	00:0b:86:c4:00:d6	A50000207	
С	Not set	192.168.0.174	AP-70	00:0b:86:c4:01:44	A50000262	
С	Not set	192.168.0.175	AP-70	00:0b:86:c4:01:32	A50000253	
		1	2 3 <u>Next</u> 1	-10 of 22 10 💌		
						1 Jan 1

• Select the AP that is to be configured from the list. This can be selected by using the MAC address of the AP or the serial number of the AP. Click **Enable** to start provisioning the AP.



AP Parameters										
Location]								
AP-70 Model-specific Parameters	-	-			Í.					
Antenna Selection © Internal Antenna © External	Antenna									
AP-6x/70 IPSEC Parameters										
IKE PSK	Confirm IKE PSK									
User Name										
Password	Confirm Password									
Master Discovery										
C Use Aruba Discovery Protocol										
C Host Switch IP Address ③		Master Switch IP Add	Iress 🧿]					
Host Switch Name	master									
IP Settings										
Obtain IP Address Using DHCP										
C Use the following IP Address										
IP Address	192.168.0.151	Subnet Ma	sk 🗌							
DNS IP Address		Domain Na	ne							
Gateway IP Address										
4D15.4										
AP LIST Index Slot/Port AP MAC/IP	Location Maste	r IP Host IP/Name	IP	GW IP/DNS IP/Domain	5 GHz/2 GHz Gain	5 GHz Ant	2 GHz Ant	Ext Antenna	St	
1 N/A 192.168.0.151	N/A N/A	N/A/aruba-master	N/A/N/A	N/A/N/A/N/A	N/A/N/A	N/A	N/A	N/A	P	4P-7

- Enter the location code in the format explained above.
- If the AP being provisioned is a model with detachable antenna capability (such as an Alcatel AP-60) enter the antenna gain in dBi, for example 4.0. This is mandatory for all detachable antenna models as the AP will not will bring up its radio interface or function as an AP without it.
- Click Apply to apply the configuration to the AP.

NOTE—The configuration does not take effect until the AP is rebooted.

- Navigate to the Maintenance > Reboot AP page.
- Select the AP from the list of the APs and click **Reboot** to reboot the AP.
- Navigate to the Maintenance > Program AP > Re-provision page to confirm that the new settings have taken effect.

Chapter 1



OmniAccess RN: User Guide

CHAPTER 2 Secure Remote Access Points

The Secure Remote Access Point Service allows users to connect APs on remote sites over the Internet to an Alcatel Mobility Controller. This capability allows remote locations equipped with Remote Access Points to connect to a corporate office, for example, over the Internet.

The Remote AP uses L2TP/IPSEC to connect to the Alcatel Mobility Controller with NAT-T (UDP port 4500 only) support. All of the AP control traffic and 802.11 data are carried through this tunnel to the Switch.

Since the Internet is involved, securing data between the AP and switch becomes key. Also most branch/home office deployments sit behind a firewall or a NAT device. In case of Remote AP, all traffic between the switch and the Remote AP is VPN encapsulated, and all control traffic between the switch and AP is encrypted. Administrators have a choice of encrypting the data in addition to the control traffic as additional security.

The advantage of using the Secure Remote Access Point Service as a Remote Access Point is the corporate office is now extended to the Remote Site. The users can enjoy similar feature sets as the corporate office users, VoIP application can be extended to remote sites while the servers and the PBX sit securely in the corporate office. The corporate network is virtually extended to the remote user.

Deploying a Branch Office/Home Office Solution

To deploy the Remote AP in a branch office or home office as shown in the illustration below, the following requirements need to be met: The Wireless LAN environment should be a single switch environment. Future releases of the code are planned to enable multi-switch support and redundancy.



Securing Communications

The Remote Access Point configurations can also be used to secure control traffic between the AP and the switch in a corporate environment. In this case, the AP and switch are in the company's private address space. The Remote AP will be similar to the Alcatel AP while tunneling and encrypting all data and control traffic to the switch.

How the Secure Remote Access Point Service Works

The Secure Remote Access Point Service APs can be deployed in one of the following ways:

1. The Remote Access Point and switch in a private network which is used to secure AP-to-switch communication. (Alcatel recommends this deployment when AP-to-switch communications need to be secured.)



2 The Remote Access Point is on the public network or behind a NAT device and the switch is on the public network



3 The Remote Access Point is on the public network or behind a NAT device and the switch is also behind a NAT device. (Alcatel recommends this deployment for remote access.)





The basic operation for each of these deployments is the same, differing only slightly in configuration details. The difference in configuration for each of these deployments will be highlighted in the steps below.

The Secure Remote Access Point Service APs have to be configured with the tunnel termination address, and address IP1 in the above figures. This address would be the switch's IP address, or the NAT device's public address, depending on the deployment scenario.

In the case where the switch is behind a NAT device (as in deployment scenario 3), NAT-T (UDP 4500 port only) needs to be enabled, and all packets from the NAT device on UDP port 4500 should be forwarded to the Alcatel Mobility Controller.

The AP uses IP1 to establish a VPN/ IPSec tunnel with the switch. Once the VPN tunnel is established, the AP bootstraps and becomes operational.

Configuring the Secure Remote Access Point Service

To configure the Secure Remote Gird Point Service (refer to the three deployment illustrations above):

- Configure the AP as a Remote AP with the master address, the LMP IP, IKE PSK, and the username and password for authentication.
- Configure IPSec VPN tunnels on the switch the AP will use before it bootstraps.
- Configure the Secure Remote Access Point Service user role and permissions.

• Add the entry for the username/password used for authentication by Secure Remote Access Point Service to the authentication server.

Configure the NAT device to which the switch connects (deployment scenario 3 only).

These steps are explained below:

1. Configure the AP with the master address, username and password authentication.

All AP60/61 and AP70 Alcatel Access Points can be provisioned to offer Secure Remote Access Point Services. The easiest way is to use the Program AP Web configuration page to configure the AP settings.

Once the AP boots up, it will appear as an un-provisioned AP if it is a new AP. If the AP is an already provisioned AP which has to be re-configured to provide Secure Access Point Services, continue with the next step. Otherwise, navigate to the Wireless LAN > Program AP > Provision AP page and provision the AP as you would a regular AP with its location and master IP. Apply the changes and reload the AP. This step ensures that the AP now boots with the 2.4 code (or higher) that supports this feature.

.....

Deployment Scenario	Master IP Address Value while Provisioning the AP			
Deployment 1	Alcatel Mobility Controller IP address			
Deployment 2	Alcatel Mobility Controller public IP address			
Deployment 3	Public address of the NAT device to which the Alcatel Mobility Controller is connected.			



WEAN > Program AP > Re-Provisio	IF 192.10	0.0.131					
AP Parameters							
Location							
AP-70 Model-specific Parameters Antenna Selection Timernal Antenna C External Antenna							
AP-6x/70 IPSEC Parameters							
IKE PSK Confirm IKE PSK]					
User Name							
Password Confirm Password							
Master Discovery							
C Use Aruba Discovery Protocol							
C Host Switch IP Address 💿	Master Switch IP Addre	ess 🕐					
Host Switch Name master							
IP Settings							
Obtain IP Address Using DHCP							
C Use the following IP Address							
IP Address 192.168.0.151	Subnet Mask						
DNS IP Address	Domain Name	•					
Gateway IP Address							
AP List	D Hest ID /Name		ain E CHa/2 CHa Cain	E CHa Ant	2 CHa Ant	Eut Antonna	51
1 N/A 192.168.0.151 N/A N/A	N/A/aruba-master N	N/A/N/A N/A/N/A/N/A	N/A/N/A	N/A	N/A	N/A	P AP-70

- Select the AP that needs to be configured to provide Secure Access Point Services on the **Program AP > Reprovision** page. Configure the AP username and password, and the IKE PSK for the IPSec settings. Set the master IP to the public IP address if the AP is connected to the switch over the Internet.
- Regardless of the deployment type, Alcatel recommends that the LMS-IP of the AP be set to the switch IP address, (either the loopback address of the switch or the VLAN 1 IP address).
- Navigate to the Configuration > Wireless LAN > Advanced page. Select the AP to be configured as a Remote Access Point. Configure the LMS-IP to the Alcatel Wireless LAN switch IP address.
- 2 Configure the IPSec VPN settings on the switch by navigating to the Configuration > Security > VPN Settings > IPSec page.

IPSEC	PPTP	Dialers	Emulate	e VPN Servers	Advanced	
L2TP and	XAUTH Para	ameters				
Enable L2T	Р	V				
Authentica	tion Protocols	PAP		ISCHAP 🗖 MSC	THAPv2	
Primary DN	S Server	0.0.0.0				
Secondary	DNS Server	0.0.0.0				
Primary WI	NS Server	0.0.0.0				
Secondary	WINS Server	0.0.0.0				
Address I	Pools					
Pool Nam	e Start Ad	dress	End Address	Actions		
Add						
Source N	AT					
Enable Sou	rce NAT	Г				
NAT Pool		~				
IKE Aggres	sive Group Nan	ne chan	geme (Only	needed for XAL	ITH)	
IKE Share	ed Secrets					
Subnet	Subnet Mas	k Length	Key Act	tions		
Add)					
IKE Polici	es					
Priority	Encryption	Hash	Authentica	tion Group	Lifetime	Action
Default	3DES	SHA	RSA	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete
odd						

To configure PAP authentication for L2TP:

Make sure that PAP Authentication Protocol is selected. Click **Apply**, to apply the configuration changes made.

From the CLI enter:

```
(Alcatel4324) # config t
(Alcatel4324) (config) # vpdn group l2tp
(Alcatel4324) (config-vpdn-l2tp) # ppp authentication PAP
(Alcatel4324) (config-vpdn-l2tp) # exit
(Alcatel4324) (config) #
```

To configure the L2TP IP pool:



Click **Add** in the **Address Pools** panel. Configure the L2TP pool from which the APs will be assigned addresses.

Pool Name		
Start Address		
End Address		

From the CLI enter:

(Alcatel4324) # config t (Alcatel4324) (config) # ip local pool l2tppool1 192.168.69.1 192.168.69.254 (Alcatel4324) (config) #

To configure an ISAKMP encrypted subnet and pre-share key:

Click **Add** in the **IKE Shared Secrets** panel and configure the pre-shared key and the address pool. For more details, refer to "Configuring Virtual Private Networks" on page 143.

Subnet	0.0.0.0	
Subnet Mask	0.0.0.0	
(Please use the defaults 0.0.0.0 for the S	iubnet and Subnet mask if you do not intend to have	multiple pre-shared keys)
IKE Shared Secret	•••••	
Verify IKE Shared Secret		

From the CLI enter:

```
(Alcatel4324) # configure t
(Alcatel4324) (config) # crypto isakmp key testkey address 0.0.0.0 netmask 0.0.0.0
(Alcatel4324) (config) #
```

To create an ISAKMP policy:

Click Add in the IKE Policies panel.

Priority	1	
Encryption	3DES 💌	
Hash Algorithm	SHA 💌	
Authentication	PRE-SHARE 💌	
Diffie Hellman Group	GROUP 2 🔽	
Life Time(secs)		

Set the priority to 1 and authentication to pre-share on the **Add Policy** page. Click **Apply** to apply the changes made.

From the CLI enter:

```
(Alcatel4324) # configure t
(Alcatel4324) (config) # crypto isakmp policy 1
(Alcatel4324) (config-isakmp) # authentication pre-share
(Alcatel4324) (config-isakmp) # exit
(Alcatel4324) (config)
```

3 Create a user-role for the Remote AP.

Once the remote AP is VPN authenticated successfully, the remote AP is assigned a role. This role is a temporary role assigned to AP until it completes the bootstrap process after which it inherits the ap-role. The appropriate ACLs need to be enabled to permit traffic from the switch to the AP and back to facilitate the bootstrap process.

From the CLI enter:

```
(Alcatel6000) #configure terminal
(Alcatel6000) (config) #user-role remote-ap
(Alcatel6000) (config-role) #session-acl allowall
(Alcatel6000) (config-role) #exit
(Alcatel6000) (config) #
```

The ACLs in this step contain the following rules:



```
(6000) # configure t
(6000) (config) # ip access-list session control
(6000) (config-sess-control)#
                               any any svc-icmp permit
(6000) (config-sess-control) # any any svc-dns permit
(6000) (config-sess-control)#
                              any any svc-papi permit
(6000) (config-sess-control)#
                               any any svc-adp permit
(6000) (config-sess-control) #
                               any any svc-tftp permit
(6000) (config-sess-control) #
                               any any svc-dhcp permit
(6000) (config-sess-control) # any any svc-natt permit
(6000) (config-sess-control) # exit
(6000) (config) # ip access-list session ap-acl
(6000) (config-sess-ap-acl) # any any svc-gre permit
(6000) (config-sess-ap-acl) # any any svc-syslog permit
(6000) (config-sess-ap-acl) # any user svc-snmp permit
(6000) (config-sess-ap-acl) # user any svc-snmp-trap permit
(6000) (config-sess-ap-acl) # user any svc-ntp permit
(6000) (config-sess-ap-acl) # exit
(6000) (config) # ip access-list session ftp-allow
(6000) (config-sess-ftp-allow) # user any svc-ftp permit
(6000) (config-sess-ftp-allow) # exit
```

4 Add Secure Remote Access Point Service user to the authentication server.

Enable the Alcatel VPN Authentication service. Configure the authentication server and add the Secure Remote Access Point Service user/password into the database to allow the Secure Remote Access Point Service user to authenticate successfully.

If you use the switch local database, navigate to the **AAA Servers > Internal DB** page and click **Add User**.

Jser Name	remoteap1		
assword	•••••		
erify Password			
tole	~		
-mail]	
inabled	N		
Entry does not expire			
C Set Expiry time (mins)			
C Set Expiry Date (mm/dd/yyyy)		Expiry Time(hh:mm)	_:_
C Set Expiry Date (mm/dd/yyyy)		Expiry Time(hh:mm)	-

Add the username and password. If the default VPN role is not the role remote ap role, then set the role on this page to the remote ap role. Click **Apply** to apply the changes made.

CAUTION—For security purposes, Alcatel recommends that you use a unique username/password for each remote AP. You should assign a unique username and password to each AP.

From the CLI enter:

To specify the role explicitly:

(Alcatel6000) **#local-userdb add username remoteap1 password remote role remote-ap** (Alcatel6000)

By default, no authentication server is defined under VPN authentication. When using VPN authentication, make sure an authentication server is configured. For example, after adding the username/password in the appropriate user database, if the user is to use the Internal Server for VPN authentication, enable this configuration using the following commands:

```
(Alcatel6000) #configure terminal
(Alcatel6000) (config) #aaa vpn-authentication auth-server Internal
(Alcatel6000) (config) #
```



Also the role created for the Secure Remote Access Point Service in Step 3 needs to be added into aaa vpn-authentication as well by entering:

(Alcatel6000) #configure terminal (Alcatel6000) (config) #aaa vpn-authentication default-role remote-ap (Alcatel6000) (config) #

For more information on configuring IPSec and VPNs, see "Configuring Virtual Private Networks" on page 143 and see "Configuring AAA Servers" on page 81 for more information on configuring the AAA server.

5 Configuring the NAT device that is connected to the Alcatel Mobility Controller.

The AP and secure switch communication uses the UDP 4500 port. When both the switch and the AP are behind NAT devices, the AP is configured to use the NAT device's public address as its master address. On the NAT device, it is necessary to enable NAT-T (UDP port 4500 only) and forward all packets to the public address of the NAT device on UDP port 4500 to the Alcatel Mobility Controller to ensure that the Remote AP bootstraps successfully.

Double Encryption

The Remote AP control traffic sent to the switch is over an IPSec tunnel. The user traffic will be encrypted as per the AP/user authentication/encryption configured. If the administrator wants the user traffic to be further encrypted using IPSec, then enable double encryption.

```
(Alcatel4324) (config) # ap location 10.0.0
(Alcatel4324) (sap-config location 10.0.0) # double-encrypt enable
(Alcatel4324) (sap-config location 10.0.0) # exit
(Alcatel4324) (config) #
```

NOTE—Alcatel recommends that double-encryption not be turned on for inter-device communication over untrusted networks in AOS-W 2.4 or higher, as doing so is redundant and adds significant processing overhead for APs.

Managing Software Feature Licenses

This chapter includes the following information:

- Understanding Alcatel software feature licenses
- Installing software feature licenses
- Maintenance of software feature licenses

Alcatel Software Licenses

Alcatel product licenses enable the following software modules:

- Policy Enforcement Firewall (PEF)
- VPN Server (VPN)
- Wireless Intrusion Protection (WIP)
- Advanced AAA (AAA)
- External Services Interface (ESI)
- Client Integrity (CIM)
- xSEC (XSC)
- Remote Access Point (RAP)

Software License Types

For all licensed software modules, two categories of licenses are available:

- 1. **Permanent license** This type of license permanently "enables" the desired software module on a specific wireless LAN switch. Permanent licenses can be obtained through the sales order process only. Permanent software license certificates are printed documents, physically mailed to the user and also accompanied by an email confirmation.
- 2. **Evaluation license** This type of license allows the user to evaluate the unrestricted functionality of a software module on a specific wireless LAN switch for 90 days (in 3 x 30 day increments) without the requirement to purchase a permanent software license.

At the end of the 90 day period, a permanent license must be applied to re-enable this software module on the wireless LAN switch. Evaluation software license certificates are electronic only and are emailed to the user.

Obtaining a Software License

To obtain either a permanent or evaluation software license, please contact your sales account manager or authorized reseller. They will process your order for a permanent license certificate or email an evaluation license certificate to you as desired.

The Software Licensing Process

Software licenses (permanent or evaluation) are unlocked individually by module type and are applied to each Alcatel wireless LAN switch as a Software License Key. Software License Keys are unique alpha-numerical strings created for individual Alcatel wireless LAN switches and are only valid for the designated wireless LAN switch.

Certain steps must be taken and criteria met in order to facilitate successfully enabling software license features on your OmniAccess Wireless LAN switch:

- 1. Obtain a valid Alcatel Software License Certificate.
- Locate the Alcatel wireless LAN switch system Serial Number (or Supervisor Card Serial Number) of the switching platform to which you wish to apply the software license.
- Visit the Alcatel Software License Management Web site at <u>http://eservice.ind.alcatel.com/oaw/</u> login and use the Software License Certificate ID and the System Serial Number to activate a Software License Key.
- Log in using the WebUI to the wireless LAN switch on which you wish to apply the license. Navigate to Maintenance > License Management, and enter the Software License Key and click Apply.

Software License Certificates

The software license certificate is a software-module and switch-class specific document (printed or emailed) that states:

- The orderable part number for the license
- A description of the software module type and wireless LAN switch platform for which it is valid
A unique, 32-character alpha/numerical string that can be used to access the license management Web site and which, in conjunction with a wireless LAN switch system / supervisor card serial number, will generate a unique software license key



FIGURE 2-1 License Certificate

The System Serial Number

The serial number of the unique wireless LAN switch platform for which the license will be valid for:

- System Serial Number that is specified on the rear of an Alcatel wireless LAN switch chassis
- System Serial Number of the Supervisor Card (not the chassis) for an Alcatel modular 6000 series wireless LAN switch platform
- System serial numbers may obtained by physically inspecting the chassis or card or from the wireless LAN switch WebUI (by navigating to the Switch > Inventory page.



Note that removal of a Supervisor Card is required on a modular platform for visual inspection and this can result in network down time.

The Alcatel License Management Web Site

In order to activate a Software License Key, you must log in to the Alcatel License Management Web site at <u>http://eservice.ind.alcatel.com/oaw/.</u>

- If you are a first time user of the licensing site, the Software License Certificate ID number can be used to log in initially and request a user account. If you already have a user account, log into the site.
- Once logged in, you will be presented with three options:
- 1. Activate a Certificate to activate a new certificate and create the Software License Key that will be applied to your wireless LAN switch platform
- 2. Transfer a Certificate to transfer a Software Certificate ID from one wireless LAN switch to another (in the event of transferring licenses to a spares system for example)
- 3. List Your Certificates to view all currently available and active Software License Certificates for your account

To activate a software license certificate, select **Activate a Certificate**, enter the certificate ID number, then the System Serial Number of the wireless LAN switch that you wish to apply the license to. Then click **Activate**. A copy of the transaction and the Software License Key will be emailed to you at the email address you enter at time of license activation.

This Software License Key is *only* valid for the System Serial Number you activated it against.

Applying The License Key

To "Enable" the software module and functionality, you must now apply the Software License Key to your Alcatel OmniAccess wireless LAN switch.

- 1. Using the WebUI, log into your Alcatel OmniAccess wireless LAN switch with Administrative access rights.
- 2. Navigate to: **Maintenance > License Management** where system License Information and the License Table can be found.
- 3. Copy the Software License Key that was emailed to you, and paste it into the **Add New License Key** field. Click **Add** and **Apply** to apply the License Key.

				and the second second		-	Internet and internet.	
LCATEL Mainten	ance				Omn	Access 6	000	
ntoring Configuration D	sgnostics Maintenance Marter Switch	tenses will expire in 22 days			the second		10	
etch Inage Minagement	Maintenance > License Manag	ement				- Notifie	cation of Expiring Licens	
Reboot Switch	License Information				6			
Clear Config Ignotraces Database Jacob Parameter Sock Parameters Tage Plane Capy Lang Tage Caulty Files Tachao Files Tachao Files Caultor Files	Service Status and Current Limits AccessParks 128 Literative AccessParks 128 Weekes Intrusion Proteom DIALED Protock Aris Diale Diale Company Protock Protocol Diale Diale Company Protock Protocol Diale Diale Diale Company Client Monghy Wolde Diale Dial	Econse keys via the web web Ster: and the following: http:// instal.number of the webch or informed conflicate number of th	so keys via the web: In: In: Inflooms: http://eservice.ind.alcatel.com/oaw autor of the webcher agein-story mobile conflicate number of the service you web to activate			License Service St		
LAN Nogran (IP	License Table						License Table	
Reboot AP	Cardo, DE 1999 AL NORMAN T, Starting & 200 March	Installed	Expires	Flags Service	Type	Actions		
sitve Portal	will +PML GROWTT, PT-Ghotte JacOdd M. West Sal- C	2005-04-27 00:42:04	Never E	Clerit Ista	erito Merida	Delete		
pload Certificate	ROWSC-ROVEY20+-OEV58+M-RPS++19-528+Itop	Uko 2005-04-21 08:30/22111	2005-05-21 D0 20-22 F	Reporte Ac	rescPoints 16	Delete		
Iouil Sygate-On-Demand Agent	hof 94%3p-XXXC57pb-thradiarM3-xAXXCFwU-vPg/SxN	-the0 2005-04-27 00:42:03	Never E	Palicy Enfo	canent Pineval	Delete	/	
Abasel Clustone Lorgin Pages	w38nRup2-45U0g:Tr-igGR1104HUAR-tx075-UP7-CPF-8	+0 2005-04-27 00 42:03	Never E	Weless In	trusion Protection	Delete		
	tGerdWaph-LovaBall-JDaIns7th-Milgzr+ff-fUaTDeLT-ris	2005-04-21 06:30:43[1]	2005-05-21 00:30:43 E	Renote Ac	caren Pointos: 48	Delete		
	FOGTen/T-GWQ0680T-SLCXT86U-Onvnp/M6-rr43duP/	Mate 2005-04-27 00:42:08	Nover E	VPN Server		Delete		
	2/Chedj3-JMR/nugli-racsRv0R-en5HtrlbP-+c3Q.hq3-1	2005-04-27 00:42:03	Never E	Advenced	AAA	Delete		
	870dyCgh+HO%Ed+s-V8h9N69-vacirV6R-Lv8kQMIP-M	4 2005-04-27 00:42:09	Never E	External Se	evices Interface	Delete		
	Ghigalityg-Californi-Divolog/8-Febrari/F-Y0rWa36p-c	GA. 2005-04-27 00:42:04	Never t	Remote Ac	caas Pointac 64	Delete		
	Plage: A - auto-generated; E - enabled			_			Adding License Keys	
	Add New License Key		Add				_ naung License Keys	

FIGURE 2-2 License Management Screen

4. You must now reboot your wireless LAN switch in order for the new feature to become available.

Additional Software License Information

Permanent Licenses

Permanent Software Licenses report the software module as **Enabled** on the on-switch WebUI. These license types will never expire, even in the event of the Operating System software being upgraded to a newer version. (Licenses will carry over one for one).

Evaluation Licenses

Evaluation licenses support the following behavior:

 Evaluation licenses are limited to 3 x 30-day periods. Evaluation licenses time individually, supporting multiple evaluation licenses for various software modules each expiring at different times



- During evaluation, full functionality relating to that software module will be made available to the user
- During a software evaluation the wireless LAN switch WEB UI will report in the summary page at initial login that software licenses are expiring

The time remaining on the licensing term displays on the CLI upon login, as shown below:

```
(Alcatel6000)
User: admin
Password: *****
NOTICE
NOTICE -- This switch has active licenses that will expire in 29 days
NOTICE
NOTICE -- See 'show license' for details.
NOTICE
(Alcatel6000) >
```

The WebUI will also display the same information. To view the license information, click the **Licensing** tab on the main screen, or navigate to the **Monitoring > Licensing** page. The expiration date of trial licenses displays on this page.

Monitoring - Microsoft I	internet Explorer	8					٦ċ
Ele Edit View Favorites	⊥ools <u>H</u> elp						
ALCATEL Mon	itoring				\mathcal{G}	OmniAccess 6000	
Monitoring Configuration	Diagnostics	Maintenance Master Sv	ritch Licenses will expire in 22 d	ays			Logout
Switch Switch Summary	Switch Sur	mmary					
Access Points Wired Access Points	WLAN Switch I	nformation					
Wined Musser	Switch Name	A2-0					
Air Monitors	Switch Model	OAW-5000					
Clients	AOS-W Version	2.4.0.0					
Cherics	IP Address	192.168.102.1					
blackist Clients	MAC Address	00:08:86:00:CA:00					
Hirewall Hits	Master IP Address	192.168.101.1					
External Services Interface							
Ports	WLAN Switch S	tatus					
Inventory	Current System Tir	me Thu Apr 28 11:05:14 PST 2	005				
Local Events	Switch Up Time	17 minutes 45 seconds					
WLAN	Switch Utilization	3 %					

NOTE—In the event of multiple evaluation licenses running concurrently on the same switch, the reported expiration time is the for the licensed feature with the least amount of duration remaining.

The time remaining on an evaluation license is also logged every day.

When each evaluation period expires the following behavior occurs:

- The wireless LAN switch will automatically backup the startup configuration and reboot itself at midnight (time in accordance with the system clock)
- All permanently enabled licenses will be unaffected. The expired evaluation licensed feature will no longer be available, shown as **Expired** in the WebUI.
- The Software License Key may be reapplied to the switch, provided the 90 day evaluation time for that feature has not been reached. If the maximum evaluation time for the evaluation license has been reached, the startup configuration will still be backed up. However, the feature can now only be re-enabled with a permanent license key.

Deleting a License Key

To remove a license from a system:

- 1. Navigate to the Maintenance > License Management page.
- 2 Select the feature / Service Type to be removed and click **Delete** (permanent license keys) or **Disable** (evaluation license keys) to the right of the feature entry in the License Table.
- 3 If the feature to be deleted is under the trial period of an evaluation license, no key will be generated. If the feature is a fully licensed feature, deleting the feature will result in the feature key being displayed.
- **NOTE**—If you are unable to delete a license key on a disabled or damaged system that is subsequently returned, you can reinstall this license on another machine. The factory will take the necessary steps to remove the license key.

Moving Licenses

It may become necessary to move licenses from one chassis to the other or simply delete the license for future use. To move licenses, delete the license from the chassis as described above in "Deleting a License Key". Then install the license on the new switch using that switch's serial number to generate the license key.

Switch Resetting

System Reboot

Rebooting or resetting a wireless LAN switch will have no effect on licensing, whether permanent or evaluation.



Resetting Switch Configuration

Issuing the write erase command to a switch running software licenses will **not** affect the license key management database on the switch, only the configuration.

Issuing the write erase all command will reset the switch to the factory default, deleting all on-switch databases including the license key management database, requiring the system administrator to reinstall all previously installed license keys.

License Fraud Management

The act of self-moving a license from one switch to another is provided as a courtesy to allow customers maximum flexibility to manage their organizations network and sparing at their convenience and with minimal interaction with Alcatel customer support. License fraud detection is monitored and enforced by Alcatel. When abnormally high volumes of license transfers for the same license certificate to multiple switches is experienced, this can indicate breach of the Alcatel end user software license agreement and will be investigated.

WARNING

When license keys are enabled on an Alcatel OmniAccess wireless LAN switch, abnormal tampering of the switch's system clock (setting the system clock back by 2 hours or more) will result in the "Disabling" of software licensed modules and their supported features. This can be network service effecting.

Getting Help with Licenses

For information or support with licensing issues, contact your Alcatel sales representative or log onto the Alcatel license support website at: http://www.alcatel.com/enterprise/.

CHAPTER 3 Configuring Network Parameters

This section outlines the steps involved to configure the various network parameters required to set up an Alcatel Mobility Controller. This includes configuring VLANs, IP interfaces, static routes, and loopback IP addresses.

Conceptual Overview

The concept of VLAN is used in the Alcatel Mobility Controller as a layer 2 broadcast domain as well as a layer 3 IP interface, similar to most layer 2/3 switches. The administrator can configure a set of ports to be members of a VLAN and define an IP address/netmask for the VLAN interface. A single physical port can be a member of multiple VLANs by use of 802.1q trunking/tagging.

The loopback IP address is a logical IP interface that is used by the Alcatel Mobility Controllers and APs to communicate amongst each other. To make use of this interface, ensure that the IP address is reachable through one of the VLAN interfaces. The examples and configuration guidelines below will illustrate the same.

Network Configuration

Create/Edit a VLAN

1. Navigate to the **Configuration > Switch > VLAN** page on the WebUI.

Monitoring	Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Lo	gout .
Switch General		Switch > VLAN	
Managemen WLAN	t	General Port VLAN Tunnels IP Routing VRRP DHCP Server	
Network	<	VLAN ID IP Address Net Mask Associated Ports Actions	_
Radio		1 10.200.14.6 255.255.255.0 Fa1/0-5,Fa1/7-23,Gig1/24-25 Edit Delete	
Advanc	ed	2 10.210.14.1 255.255.0 Fa1/6 Edit Delete	
RF Managen Calibrat	ion	Add	
Optimiza	ation	Use the Add button to Edit and Delete	
Protecti	on	create additional VLANs specific VLAN	
Monitori	ing		

2 Click **Add** to create a new VLAN. To edit an existing VLAN click **Edit** for this VLAN. On the next screen (as shown below), enter the VLAN ID, the IP address and network mask of the VLAN interface. If required, the address of the DHCP server for that VLAN can also be configured by clicking **Add**.

The VLAN can be assigned to the required ports by selecting the appropriate boxes in the **Assign this VLAN to Ports** fields. However, the recommended procedure for assigning VLANs to ports is explained in the following section.

Monitoring Configuration	Diagnostics	Maintenance Plan	Events Repo	orts	Save Configuratio	n Logout
Switch	Switch	> VLAN > Add N	ew VLAN			< Back
General						
Management WLAN	Configura	tion	DHCP	Helper Addresses		
Network	VLAN ID	3	No He	elper Addresses C		
Radio	IP Address	10.200.15.10	Add			
Advanced	Net Mask	255.255.255.0				
RF Management			Required fiel	ds for VLAN cr	eation	
Calibration	_				Culton	
Optimization		1				- 11
Monitorion	Port s	election uptions of the selection criteria to ch	ose ports for configu	ration		
Advanced	or many	ally select one or more ports b	y clicking on the ports	l.		
Security	Cast	raso seeu ar the ports using	C construction		Over March 1	
Roles	• Ad	ninistrative State	 Operational St 	ate	Port Mode	<u> </u>
Policies	CVL	N Association	C Trusted	~		
AAA Servers						
Authentication Methods	Assig	this VLAN to Ports				
VPN Settings		0		22		
Firewall Settings		•				
Secure Access		1		23	24	25
Secure Service Interfaces			Select All	Clear All		
Advanced WI AN Television Restaction	0				. developed	
Rogue AP	Cum	nt configuration of the	port under the r	nouse cursor will b	e displayed	
Denial of Service	Adm	nistrative State	N/A	Operational State	NJA	
Man-In-the-Middle	Powe	r Over Ethernet	N/A	Is Port Trusted	N/A	
Signatures	Is Po	rt an Access or a Trunk Po	rt N/A	Port Policy	N/A	
Policies	Span	ning Tree	N/A			
	VLAN	(s)	N/A			
						- 11
	la serie					

- 3 Click **Apply** to apply this configuration.
- 4 Verify that the VLAN has been created on the VLAN page.

Monitoring Configuration	Diagnostics	Maintenano	te Plan	Events Report		1	Save Configuration	Log
Switch General	Switch	> VLAN						
Management WLAN	General	Port	VLAN Tu	noels IP Routi	ng VRF	RP C	HCP Server	
Network.	VLAN ID	IP Address	Net Mask	Associated Port	5 A(ctions	- 52	
Radio	1	10.200.14.6	255.255.255.0	Fa1/0-23,Gig1/24-2	5 Edit		23	
Advanced	2	10.210.14.1	255.255.255.0	,	Edit	Delete		
RF Management Calibration	3	10.200.15.10	255.255.255.0		Edit	Delete		
Optimization	bbA							
Protection								
Monitoring								
Advanced								

Configuring a Port to Be an Access Port

The in-band Ethernet ports can be configured as access ports and members of a single VLAN using the following steps:

1. Navigate to the **Configuration > Switch > Port** page on the WebUI.

Monitoring Configuration	Diagnostics Maintenance Plan Events	Reports	Save Configuration
Switch	Switch > Dort		
Management	Switch > Port		
WIAN	General Port VLAN Tunnels	IP Routing VRRP DHCP Se	rver
Network.			
Radio	Port Selection Options		
Advanced	Use any of the selection criteria to choose ports for c or manually select one or more ports by dicking on the	nfiguration	
RF Management	You can also select all the ports using the 'Select All' of	edbox.	
Calibration	C Administrative State	State C Port Mode	>
Optimization			
Protection	C VLAN Association	~	
Monitoring			
Advanced	Port Selection		
Security Roles	0	22	
Policies			
AAA Servers		23 24	25
Authentication Methods	Select A	Clear All	
VPN Settings	Port FE 1/6 Configuration Details		
Firewall Settings	Administrative State Enable	Operational State Up	
Secure Access	Power Over Ethernet Enable	Is Port Trusted Yes	Moving the mouse cursor
Secure Service Interfaces	Is Port an Access or a Trunk Port	Part Policy N/A	over a port box will show
Advanced	is Forcen Access of a frunk Porce Access	Force oncy IQA	for that part
WLAN Intrusion Protection	Spanning Tree Forwa	ding; cost: 19; prio: 128 (portfast off)	for that port
Rogue AP	VLAN(s) 1		
Denial of Service	<u></u>		
Man-In-the-Middle			

2 Select the port to be configured by clicking on the appropriate box in the Port Selection section of the page. After selecting the port, choose the VLAN from the drop down list in the Configure Selected Ports, Enter VLAN(s) section and click Apply to complete the choice.



NOTE—Make sure that the Port Mode is **Access** in the Configure Selected Ports section.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration Logout
Switch		
General	Switch > Port	
Management		
WLAN	General Port VLAN Tunnels IP Routing VRRP DHCP Server	
Network.	Deut Calastian Onlines	
Radio	Use any of the selection criteria to choose ports for configuration	
Advanced	or manually select one or more ports by clicking on the ports.	
Calbration	Tou can also select all the ports using the Select All checkbox.	
Ontimination	C Administrative State 🔄 C Operational State 🔄 C Port Mode	
Protection	C must and C Trusted	
Maniharing	VLAN Association	
Advanced	Deut Oxfordien	
Security	Port Selection	
Roles	0 22	
Policies		lar.
AAA Servers] 29
Authentication Methods	Select All	
VPN Settings		
Firewall Settings	Configure Selected Ports	
Secure Access	Enable Port	V
Secure Service Interfaces	Enable 802.3af Power Over Ethernet	v
Advanced	Enable Cisco Power Over Ethernet(Enabling this option will disable 802.3af Power Over Ethernet)	
WLAN Intrusion Protection Roque AP	Make Port Trusted	
Denial of Service	Port Mode Ensure that Access is selected for port mode.	@ Access C Trunk
Man-In-the-Middle		
Signatures	Enter VLAN(S) Select VLAN from pull down menu then click	2 5 2 2
Policies	Firewal Polcy On < to add it to the port configuration.	stateful-dot1x V Delete
Policies	Firewal Polcy On < to add it to the port configuration.	stateful-dot1x V Delete
Policies	Frewal Poky On < to add it to the port configuration.	statelui-dot1x C Delete
Policies	Frewal Poky On < to add it to the port configuration.	Ersbled
Potoes	Frewal Polcy On < to add it to the port configuration.	statetui-dottx V Delete Enabled 19 Port Cost 128 Priority
Poices	Frewal Poky On < to add it to the port configuration.	elatelui-dotta V Delete Enabled 19 Port Cost 128 Port Fast

3 Click **Apply** to make this configuration active.

Note—This will apply the entire configuration shown in the Configure Selected Ports section, including changes that were not explicitly made. Make sure that the configuration for all items on the list is as desired before clicking **Apply**.

Verify that the Configuration was applied by navigating to the Configuration
 Switch > VLAN screen. The port configured should be shown as a member of the configured VLAN.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logo
Switch General	Switch > VLAN
Management	General Port VLAN Tunnels IP Routing VRRP DHCP Server
Network	ULAN TO Address Net Mark Associated Darks Actions
Radio	1 10.200.14.6 255.255.255.0 Fa1/0-5, Fa1/7-23, Gg1/24-25 Edit Ociote
Advanced	2 10.210.14.1 255.255.25.0 Fa1/6 Edit Delete
RF Management Calibration	3 10.200.15.10 255.255.255.0 Edit Delete
Optimization	Add to VLAN 2
Protection	0 10 10 10
Monitoring	

Configuring a Trunk Port

An in-band Ethernet port can be configured to be a trunk port and a member of multiple VLANs using the following steps:

1. Navigate to the **Configuration > Switch > Port** page on the WebUI. Select the port(s) to be configured by selecting the appropriate checkbox in the **Port Selection** section.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration	Logout
Switch General Management	Switch > Port		
WLAN Network	General Port VLAN Tunnels IP Routing VRRP DHCP Server		
Radio Advanced RF Management Calibration Optimization Protection Monitoring	Port Selection Options Use any of the selection orber to to choose ports for configuration or manually select one or more ports by cloing on the ports. You can also select all the ports using the Select Af chectbox. C Administrative State C Operational State C VLAN Association C C VLAN Association C		
Advanced	Port Selection		
Security Roles Policies AAA Servers Authentication Methods	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		
VPN Settings	Configure Selected Ports		
Firewall Settings	Enable Port	F	7
Secure Access	Enable 802 3af Power Over Ethernet	- -	-
Advanced	Enable Gran Remark Core Educated (Enables this relies will deable 202 2nd Remark Core Etherent)		-
WLAN Intrusion Protection	Enable Cisco Power Over Edvernet(Enabling dis option will disable 302.331 Power Over Edvernet) Make Powt Trusted	r	
Rogue AP Denial of Service	Port Mode Select Trunk to enable trunk configurations for VL	ANS CAccess Tru	nk
Mon-In-the-Middle Signatures Policies	Enter YLAN(s) To allow or disallow multiple VLANs select a VLAN from the puil down list, click <, then select another VLAN from the puil down menu	+VLAN 1 « 1 « All VLANs nd VLANs 1,3 « 3 « VLANs 2 « 2 «	
	Firewal Policy	V Dele	te
	Enable MUK	Г	
	Spanning Tree	I Enable I Port Co I 20 Priori Port Fa Apply	ed ist ty ist

- 2 Select the Trunk option to the Port Mode section.
- 3 Select **Allow all VLANs** to assign all configured VLANs to this port. If the desired list of VLANs is different from all configured VLANs, choose the Allowed VLAN list option and add to the list of allowed VLANs and disallowed VLANs as required.
- 4 Click **Apply** to apply this configuration.
- 5 Verify VLAN membership is as configured by navigating to the **Configuration > Switch > VLAN** page.

Monitoring Configuration	Diagnostics	Maintenano	e Plan	Events	Reports	Save Cont	iguration	Logou
Switch General	Switch :	> VLAN						
Management	General	Port	/LAN Tu	nnels	IP Routing	/RRP	DHCP Serve	r
Network.	VLAN ID	IP Address	Net Mask	Ass	ociated Ports	A	tions	
Radio	1	10.200.14.6	255.255.255.	0 Fa1/0-5,	Fa1/7 23, 3ig1/24-25	Edit	Delete	
Advanced	2	10.210.14.1	255.255.255.	0 Fa1/6	Ă	Edit	Delete	
Calibration	3	10.200.15.10	255.255.255.	Fa1/23	←	Edit	Delete	
Optimization	Add			\smile	Port 23 Tru	nk con	firmed in	
Protection					both \	LAN 1	& 3	
Monitoring					1000	10.000		



Configuring Static Routes

1. Navigate to the **Configuration > Switch > IP Routing** page.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Switch > IP
Management	General Port VLAN Tunnels JP Routing VRRP DHCP Server
WLAN Network	Default Gateway
Radio	Destination IP Address Destination mask Next Hop (Forwarding Router Address) Cost Action
Advanced	10.200.18.1 255.255.255.0 10.200.17.1 1 Delete
RF Management	Add
Calibration	Apply
Optimization	Commands Hide Commands
Protection	ip route 10.200.18.1 255.255.255.0 10.200.17.1 1
Monitoring	
Advanced	The Commands feature allows the equivilent CLI commands to be
Security Roles	shown below the GUI settings. Click "Show Commands" to enable this feature or "Hide Commands" to hide this feature.
Policies	and the second sec

2 Click **Add** to add a static route to a destination network or host. Enter the destination IP and network mask (255.255.255.255 for a host route) and the next hop IP address.

Monitoring Configuration	Diagnostics Maintena	ance Plan	Events	Reports	Save Configuration	Logout
Switch General	Switch > IP >	Add Stati	c Route	•	l	« Back
Management	Destination IP Address	10.200.19.19				
Network	Destination Network Mask	255.255.255	.0			
Radio	Next Hop IP Address	10.200.18.1				
Advanced	Cost	3				
Calibration	Add Cancel					

3 Click **Add** to confirm the entry.

NOTE— The route has not yet been added to the routing table.

Click **Apply** to add this route to the routing table. The message Configuration Updated Successfully will confirm that the route has been added.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Log	out
Switch General	Switch > IP	
Management	General Port VLAN Tunnels JP Routing VRRP DHCP Server	
Network	Default Gateway	
Radio	Destination IP Address Destination mask Next Hop (Forwarding Router Address) Cost Activ	on
Advanced	10.200.10.1 255.255.255.0 10.200.17.1 1 Dele	te
RF Management	10.200.19.19 255.255.255.0 10.200.18.1 3 Dele	ete.
Calibration	Add	
Optimization	Route addition confirmed - also shown in Commands below	ply
Protection	Commands Hide Commands	
Monitoring	ip route 10.200.18.1 255.255.255.0 10.200.17.1 1	
Advanced	ip route 10.200.19.19 255.255.255.0 10.200.18.1 3	

Modifying the Loopback IP Address

NOTE—This procedure requires a switch reboot.

To change the switch loopback IP address:

1. Navigate to the **Configuration > Switch > General** page on the WebUI.



2 Modify the loopback IP address in the **Loopback Interface** section on this page as required. Click **Apply** to apply this configuration.



CAUTION—If you are using the loopback IP address to access the WebUI, this will result in loss of connectivity. Alcatel recommends that you use one of the VLAN interface IP address to access the WebUI to make this change.

3 Navigate to the **Maintenance > Switch > Reboot** page to reboot the switch to apply the change of loopback IP address



4 Click **Continue** to save the configuration.



5 When prompted that the changes were written successfully to flash, click **OK**.



6 The switch will boot up with the changed loopback IP address.

CHAPTER 4 Configuring Redundancy

This chapter outlines the steps required to configure the various redundancy options available in an Alcatel network. The redundancy can include backing up an Alcatel Mobility Controller for the Access Points being controlled (and through them the clients accessing the wireless network), backing up an Alcatel Master switch.

Conceptual Overview

The underlying mechanism for the redundancy solutions in the Alcatel solution is the standard redundancy protocol, Virtual Router Redundancy Protocol (VRRP). This mechanism can be used to create various redundancy solutions, including pairs of local switches acting in an active-active mode or a hot-standby mode, master backing up a set of local switches, a pair of switches acting as a redundant pair of master switches in a hot standby mode. Each of these modes is explained in greater detail with the required configuration.

VRRP is a protocol that is designed to eliminate the single point of failure by providing an election mechanism amongst *n* switches to elect a "*master*" switch. This *master* switch is the owner of the configured Virtual IP address for this VRRP instance. When the *master* becomes unavailable, one of the backup switches takes the place of the *master*, thereby getting ownership of the Virtual IP address. All the network elements (such as the Access Points and other switches in this case) can be configured to access the Virtual IP, thereby providing a transparent redundant solution to the rest of the network.

Redundancy Configuration

In an Alcatel network, the Access Points are controlled by an Alcatel Mobility Controller. The APs tunnel all data to the switch that does all the processing of the data, including encryption/decryption, bridging/forwarding etc.

Local switch redundancy refers to providing redundancy for this switch such that the APs *"failover"* to a *backup* switch if a switch becomes unavailable. Local switch redundancy is provided by running VRRP between a pair of Alcatel Mobility Controllers.

NOTE—The two switches need to be connected on the same broadcast domain (or layer-2 connected) for VRRP operation. The two switches should be of the same class (4308 to 4308 or higher), and both switches should be running the same version of AOS-W.

The Access Points are now configured to connect to the *"virtual-IP"* configured on the VRRP instance.

Configuring Local Switch Redundancy

To configure redundancy for a local switch:

1. Collect the following information needed to configure local switch redundancy:

- VLAN ID on the two local switches that are on the same layer 2 network and will be used to configure VRRP.
- **Virtual IP address** that has been reserved to be used for the VRRP instance.
- 2 Navigate to the Configuration > Switch > VRRP page on the WebUI for each of the local switches. Click Add to start creating a VRRP instance.

Monitoring Configuration	Diagnostics Maintenance Plan	Events Reports	Save Configuration Logout
Switch General	Switch > Virtual Router		
Management	General Port VLAN TU	unnels IP Routing V	RRP DHCP Server
WLAN	Virtual Router Table		
Radio	Router Name IP Address VLAN	Admin State Operational	State Action
Advanced	Add		
RF Management			
Calibration	Database Synchronization Paramete	ers	
Optimization	Enable periodic database synchronization		
Protection	Database synchronization period in minutes	0	
Monitoring	Include RE Plan data		
Advanced		1.	
Security			Apply
Roles	Commands		View Compands
Policies	Commanus		Mew Commanus

3 Enter the various VRRP parameters for the VRRP instance. The table below explains what each of the parameters means and the recommended/expected values for this configuration.

Parameter	Explanation	Expected/Recommended Values
Virtual Router ID	This is the Virtual Router ID that uniquely identifies this VRRP instance.	Recommended to configure this with the same value as the VLAN ID for easy administration.
Advertisement Interval	This is the interval between successive VRRP advertisements sent by the current <i>master</i>	Recommended to leave as default (1000ms = 1s).
Authentication Password	This is an optional password that can be used to authenticate VRRP peers in their advertisements	A password of up to 8 characters length can be configured in this field or it can be left empty to take the default of no authentication password.
Description	This is an optional textual description to describe the VRRP instance	
IP Address	This is the Virtual IP address that will be owned by the elected VRRP <i>master</i> .	Configure this with the Virtual IP address reserved in step i.



Enable Router Pre-emption	Selecting this option means that a switch can take over the role of <i>master</i> if it detects a lower priority switch currently acting as <i>master</i>	For this topology it is recommended NOT to select this option.
Priority	Priority level of the VRRP instance for the switch. This value is used in the election mechanism for the <i>master</i>	It is recommended to leave this as the default for this topology.(default = 100).
Admin State	Administrative state of the VRRP instance	To start the VRRP instance, change the admin state to UP.
VLAN	VLAN on which the VRRP protocol will run.	Configure this to be the VLAN ID from step i.

4 Configure the values in the respective fields as shown in the table above and click **Add** to enter the values.

Monitoring	Configuration	Diagnostics Maintenance	Plan Events	Reports	Save Configuration	Logout
Switch General		Switch > VRRP >	Add Virtual F	Router	l	« Back
Managemen	t	Virtual Router Id	11			
Network	ς	Advertisement Interval (msecs)				
Radio		Authentication Password	password			
Advance DE Managan	ed	Description	VRRP-11			
Calibrati	on	IP Address	10.200.11.254			
Optimiza	ation	Enable Router Pre-emption				
Protecti	on	Priority				
Monitori	ng	Admin State	DOWN 🐱			
Advance Security	ed	VLAN	1 🗸			
Roles		Add Cancel				
Policies						

5 Click **Apply** to apply the configuration and add the VRRP instance.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Switch > Virtual Router
Management	General Port VLAN Tunnels IP Routing VRRP DHCP Server
WLAN Network	Virtual Router Table
Radio	Router Name IP Address VLAN Admin State Operational State Action
Advanced	II IU.200.11.254 I DOWN Edit Delete
RF Management	Add Confirm that the VRRP
Calibration	instance has been added
Optimization	Database Synchronization Parameters
Protection	Enable periodic database synchronization
Monitoring	Database synchronization period in minutes
Advanced	
Security	
Roles	Analy
Policies	Apply
AAA Servers	LUIIIIIarius Hide Commands
Authentication Methods	authentication password
VPN Settings	description "WRP-11" Clicking on "View Commands" can
Firewall Settings	vlan 1 also confirm the commands used to
Secure Access	create the VRRP entry

6 Configure the Access Points to terminate their tunnels on the Virtual-IP address. This can be done with greater flexibility and ease from the CLI. The APs can be identified by their location code (building.floor.location) with 0 being used as a wild card for any of the values. Thus a location code of 10.0.0 would refer to all the APs in building 10. Refer to the AP provisioning guide for directions on how to provision the APs with their location codes.

Note—This command needs to be executed on the Master switch as only the Master switch controls all APs in the network.

Use the steps in the table below to configure the "Ims-ip" for a set of AP(s).

	Command	Purpose
Step 1	configure terminal	Enter the global configuration mode.
Step 2	ap location <i>b.f.l</i>	Use the location code value to select set of AP(s) to configure.
Step 3	lms-ip ip-address	Configure the <i>Ims-ip</i> for the selected set of APs.

The example below shows how the steps shown above can be used to configure the *Ims-ip* for all APs in building 10:



(Alcatel4324) (config) #ap location 10.0.0 (Alcatel4324) (sap-config location 10.0.0) #lms-ip 10.200.11.254 (Alcatel4324) (sap-config location 10.0.0) #

Master Switch Redundancy

The Master switch in the Alcatel solution acts as a single point of configuration for global policies such as firewall policies, authentication parameters, RF configuration to ease the configuration and maintenance of a wireless network. It also maintains a database related to the wireless network that is used to make any adjustments (automated as well as manual) in reaction to events that cause a change in the environment (such as an AP becoming unavailable). The Master switch is also responsible for providing the configuration for any AP to complete its boot process. If the Master becomes unavailable, the network continues to run without any interruption. However any change in the network topology or configuration will require the availability of the Master switch.

To maintain a highly redundant network, the administrator can use a switch to act as a hot standby for the Master switch. The underlying protocol used is the same as in local redundancy, that is VRRP.

To configure master switch redundancy:

- 1. Collect the following data before configuring master switch redundancy.
 - VLAN ID on the two switches that are on the same layer 2 network and will be used to configure VRRP.
 - Virtual IP address that has been reserved to be used for the VRRP instance
- 2 Connect to the switch CLI using Telnet or SSH. After logging into the switch, enter the global configuration mode.

To configure VRRP on the VLAN ID.

	Command	Explanation	Expected/Recommen ded Values
Step 1	vrrp vrrp-id	Creates the VRRP instance.	It is recommended to configure the VRRP ID to be the same as VLAN ID on which the instance runs for easier administration and maintenance.
Step 2	vlan vlan-id	Associates the VRRP instance with a VLAN.	VLAN ID from step i.
Step 3	ip address ip-address	Virtual IP address for the VRRP instance	Virtual IP address from step i.
Step 4	priority priority-value	Priority of the VRRP instance that is used in the election of the <i>master</i> . By default, the value is 100.	The following are the recommended values for the priority on the <i>"initially preferred"</i> master and <i>"initially preferred"</i> backup switches:
			Master: 110
			Backup: 100
			Note : these values are closely related to the value of the <i>value</i> to be added to the priority by tracking in step 7.
Step 5	preempt	Enable preemption	



Step 5	authentication <i>password</i> (Optional)	Optional authentication password that is used to authenticate packets between VRRP peers	Any password of up to 8 characters can be configured on both the peer switches. This is an optional configuration.
Step 6	description <i>description</i> (Optional)	Optional description to the VRRP instance.	Any text description can be configured in this field. This is an optional configuration.
Step 7	tracking master-up-time duration add value	Configures a tracking mechanism that adds value to the priority after a switch has been the master for the VRRP instance for a duration longer than the configured value duration. This is used to avoid failing over to a backup Master for transient	The value of <i>duration</i> is the length of time that the administrator expects will be long enough that the database gathered in the time is too important to be lost. This will obviously vary from instance to instance. The recommended value of <i>value</i> in conjunction to the values for priority
		failures.	in step 4 is 20.
Step 8	no shutdown	Administratively enables the VRRP instance.	N/A.

The following shows an example of the configuration on the *"initially-preferred master"*.

```
(Alcatel4324) (config) #vrrp 22
(Alcatel4324) (config-vrrp) #vlan 22
(Alcatel4324) (config-vrrp) #ip address 10.200.22.254
(Alcatel4324) (config-vrrp) #priority 110
(Alcatel4324) (config-vrrp) #preempt
(Alcatel4324) (config-vrrp) #authentication password
(Alcatel4324) (config-vrrp) #description Preferred-Master
```

Chapter 4

```
(Alcatel4324) (config-vrrp) #tracking master-up-time 30 add 20
(Alcatel4324) (config-vrrp) #no shutdown
```

The following shows the corresponding VRRP configuration for the peer switch.

```
(Alcatel4324) (config) #vrrp 22
(Alcatel4324) (config-vrrp) #vlan 22
(Alcatel4324) (config-vrrp) #ip address 10.200.22.254
(Alcatel4324) (config-vrrp) #priority 100
(Alcatel4324) (config-vrrp) #preempt
(Alcatel4324) (config-vrrp) #authentication password
(Alcatel4324) (config-vrrp) #description Backup-Master
(Alcatel4324) (config-vrrp) #tracking master-up-time 30 add 20
(Alcatel4324) (config-vrrp) #no shutdown
```

Use the following steps to associate the VRRP instance with master switch redundancy.

	Command	Explanation	Expected/recommen ded Values
Step 1	master-redundancy	Enter the master-redundancy context	N/A
Step 2	master-vrrp vr-id	Associates a VRRP instance with master redundancy	VR-ID of the VRRP instance configured in step iii.
Step 3	peer-ip-address ip-address	Loopback IP address of the peer for master redundancy	Loopback IP address of the peer switch.



NOTE—Note: All the APs and local switches in the network should be configured with the Virtual IP address as Master IP. The Master IP address can be configured for local switches during the Initial Setup Dialog (refer Quick Start Guide for more details). The administrator can also use the following commands to change the Master IP of the local switch. The switch will require a reboot after changing the Master IP of the switch.

	Command	Explanation	Expected/recomm ended values
Step 1	masterip ip-address	Configures the Master IP address of a local switch	Configure this to be the virtual IP address of the VRRP instance used for master redundancy.

If DNS resolution is the chosen mechanism for the APs to discover their Master switch, ensure that the name *"Alcatel-master"* resolves to the same Virtual IP address configured as a part of the master redundancy.

Master-Local Switch Redundancy

This section outlines the concepts behind a redundancy solution where a master can act as a backup for one or more local switches and shows how to configure the Alcatel Mobility Controllers for such a redundant solution. In this solution, the local switches act as the controller for the APs. When any one of the local switches becomes unavailable, the master takes over the APs controlled by that local switch for the time that the local switch remains unavailable. It is configured such that when the local switch comes back again, it can take control over the APs once more.

This type of redundant solution is illustrated by the following topology diagram.

NOTE—This solution requires that the master switch has a layer-2 connectivity to all the local switches.



In the network shown above, the master switch is layer 2 connected to the local switches on VLANs 1, 2... n respectively. To configure redundancy as described in the conceptual overview for master-local redundancy, configure VRRP instances on each of the VLANs between the master and the respective local switch. The VRRP instance on the local switch is configured with a higher priority to ensure that when available, the APs always choose the local switch to terminate their tunnels.

To configure the master and local switches for such a topology:

1. Configure the interface on the master switch to be a trunk port with 1, 2... n being member VLANs. Refer to the "Configuring Network Parameters" for more details on how to configure this.

- 2 Collect the following data before configuring master switch redundancy.
 - VLAN IDs on the switches corresponding to the VLANs 1, 2...n shown in the topology above.
 - Virtual IP addresses that has been reserved to be used for the VRRP instances.
- 3 Connect to the switch CLI using Telnet or SSH. After logging into the switch, enter the global configuration mode.



4 Use the following steps to configure VRRP on the master and local switches respectively. Note: the master switch will be configured for a number of VRRP instances (equal to the number of local switches the master is backing up).

	Command	Explanation	Expected/Recommen ded Values
Step 1	vrrp vrrp-id	Creates the VRRP instance.	It is recommended to configure the VRRP ID to be the same as VLAN ID on which the instance runs for easier administration and maintenance.
Step 2	vlan vlan-id	Associates the VRRP instance with a VLAN.	VLAN ID from step 2 above.
Step 3	ip address ip-address	Virtual IP address for the VRRP instance	Virtual IP address from step 2 above.
Step 4	Priority priority-value	Priority of the VRRP instance that is used in the election of the <i>master</i> . By default, the value is 100.	The following are the recommended values for the priority on the master and local switches:
			Master: 100
			<i>Local:</i> 110.
Step 5	Preempt	Enable preemption	

Step 5	authentication password (Optional)	Optional authentication password that is used to authenticate packets between VRRP peers	Any password of up to 8 characters can be configured on both the peer switches. This is an optional configuration.
Step 6	description <i>description</i> (Optional)	Optional description to the VRRP instance.	Any text description can be configured in this field. This is an optional configuration.
Step 7	no shutdown	Administratively enables the VRRP instance.	N/A.

The following shows an example configuration of the Master switch in such a topology for one of the VLANs (in this case VLAN 22).

```
(Alcatel4324) (config) #vrrp 22
(Alcatel4324) (config-vrrp) #vlan 22
(Alcatel4324) (config-vrrp) #ip address 10.200.22.254
(Alcatel4324) (config-vrrp) #priority 100
(Alcatel4324) (config-vrrp) #preempt
(Alcatel4324) (config-vrrp) #authentication password
(Alcatel4324) (config-vrrp) #description
Master-acting-as-backup-to-local
(Alcatel4324) (config-vrrp) #tracking master-up-time 30 add 20
(Alcatel4324) (config-vrrp) #no shutdown
```

The following shows the configuration on the corresponding local switch.

```
(Alcatel4324) (config) #vrrp 22
(Alcatel4324) (config-vrrp) #vlan 22
(Alcatel4324) (config-vrrp) #ip address 10.200.22.254
(Alcatel4324) (config-vrrp) #priority 110
(Alcatel4324) (config-vrrp) #preempt
(Alcatel4324) (config-vrrp) #authentication password
(Alcatel4324) (config-vrrp) #description local-backed-by-master
(Alcatel4324) (config-vrrp) #no shutdown
```



Configure the APs with the appropriate Virtual-IP address depending on which switch is expected to control the AP. As an example, the administrator can configure such that all APs on floor 1 are controlled by local switch 1, all APs on floor 2 are controlled by local switch 2 and so on. All the local switches are backed up by the master switch as shown above. In such a case, configure all APs on floor 1 to be controlled by the Virtual IP address of the VRRP between local switch 1 and master and so on. This can be done by following these steps:

	Command	Explanation	Expected/recommend ed values
Step 1	ap location <i>b.f.l</i>	Choose the APs to configure by using the location code in the building.floor.location format.	Depending on the set of APs to be configured, enter the location code using 0 as a wild card value. As an example all APs on building 1 and floor 1 can be represented by the location code 1.1.0.
Step 2	lms-ip <i>ip-address</i>	Configure the IP address of the switch controlling the APs chosen	Configure this IP address to be the same as the Virtual IP address for the VRRP instance between the appropriate local switch and master switch.

The following example shows how these steps are used to configure the APs on floor 1 of building 1 to use the pair of switches configured in the above example.

NOTE—This command is executed on the Master switch.

```
(Alcatel4324) (config) #ap location 1.1.0
(Alcatel4324) (sap-config location 1.1.0) #lms-ip 10.200.11.254
(Alcatel4324) (sap-config location 1.1.0) #
```

CHAPTER 5 Adding a Local Switch

This chapter explains how to expand your network by adding a local switch to a master switch configuration. Typically, this is the first expansion of the network beyond a network with just one switch (which is a master switch by default). This chapter is a basic-level discussion of creating master-local switch configurations. More complicated multi-switch configurations are discussed in other chapters. For example, for information on configuring redundant switches, see "Configuring Redundancy" on page 17.

A single Wireless LAN configuration, the master switch is the switch which controls the RF and security settings of the Wireless LAN network. Additional switches to the same Alcatel Wireless LAN will serve as local switches to the master switch. The local switch operates independently of the master switch and depends on the master switch only for its security and RF settings (the global settings across the network like RF, user policies, and authentication settings). The Layer-2 and Layer-3 configurations are configured on the local switch and are independent of the master switch. The local switch needs to have connectivity to the master are propagated to the local switch.

Some of the common reasons to move from a single to a multi switch-environment include:

- Scaling to include a larger coverage area
- Setting up a branch office switch
- Network requirements to re-distribute APs from a single switch to multiple switches

The addition of a local switch could also become necessary depending on the network setup and connectivity specific to the network topology at hand.

Configuring Local Switches

A single master configuration can be one with one switch, the master switch or a master redundant configuration with one master switch and the VRRP redundant backup switch. This section will highlight the difference in configuration for both of these scenarios.

The steps involved in migrating from a single to a multi-switch environment are:

- 1. Configure the local switch to point to the master switch IP.
- 2 Configure the Layer-2 / Layer-3 settings on the local switch (VLANs, IP subnets, IP routes).
- 3 Configure the ports the master and local switch will use to communicate with each other to be trusted ports.
- 4 Configure the LMS-IP to point to the new local switch for those APs that need to boot off the local switch.
- 5 Reboot the APs if they are already on the network, so that they now connect to the local switch.

These steps are explained below.

Configuring the Local Switch

There are multiple ways of doing this, using the startup dialog or the web interface.

Using the Setup Dialog

When you power up an unconfigured Alcatel Mobility Controller, or reboot a configured Alcatel Mobility Controller after executing a **write erase**, **reload** sequence, you see the following setup dialog (using an Alcatel 4324 as an example):

Enter system name [Alcatel4324]: Enter VLAN 1 interface IP address [172.16.0.254]: 10.200.14.6 Enter VLAN 1 interface subnet mask [255.255.0]: Enter IP Default gateway [none]: 10.200.14.1 Enter Switch Role, (master|local) [master]: local <-----Enter Master switch IP address: 10.4.21.10 <-----Enter password for admin login (up to 32 chars): ***** Re-type Password for admin login: ***** Enter password for enable mode (up to 15 chars): ***** Re-type password for enable mode: ****** Re-type password for enable mode: ****** Do you wish to shutdown all the ports (yes|no)? [no]: Current choices are:

System name: Alcatel4324 VLAN 1 interface IP address: 10.100.2.30 VLAN 1 interface subnet mask: 255.255.255.0 IP Default gateway: 10.100.2.1 Switch Role: local Master switch IP address: 10.200.14.6 Ports shutdown: no

If you accept the changes the switch will restart! Type <ctrl-P> to go back and change answer for any question Do you wish to accept the changes (yes|no) \mathbf{y} Creating configuration... Done.

System will now restart!

When prompted to enter the operational mode in the setup dialog, enter **local** to set the switch operational mode to be a local switch.

You are then prompted for the master switch IP address. Enter the IP address of the master switch of the Wireless LAN network.

Using the Web UI

Once the switch is up and operation with Layer-3 connectivity, the following needs to be configured to set the switch up as a local switch:

• The mode of the switch has to be set to local.



The master IP address is the IP address of the master switch. If master redundancy is enabled on the master, this address should be the VRRP address for the VLAN instance corresponding to the switch IP.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports			
Switch		Switch >	General						
General									
Managemei	nt	General	Port VLAN	I Tur	nnels	IP Routing			
WLAN	de								
	r.	Switch Role	Local 🗸						
Radio		Master IP Add	iress 10.4.21.2	1					
Advano DE Masaaa	ced								
Calibra	tion	Loophack I	nterface						
Ontimia	ation	MAC Address	00:0B:86:00:0C:	00					
Opumiz		ID Address	10 4 21 21		1				
Protect		IF Address	10.4.21.21						
Monito	ring	Quitch ID D	ataile (Loonha	ala		19			
Advano	ced	MAC address		00.					
Security		TRACADDRESS 00:00:00:00:00:00							
Delision		Subpet Mack	255 255 255 255	-					
Policies		Dubliet Mask	200,200,200,200	,					
AAA Se	ervers	Mobility Co	nfiguration						
Auther	itication Methods	Enable Mability							
VPN Se	ttings	Enable Mobilic	y Iv						
Firewal	ll Settings	MUX Config	uration						
Secure	Access	Enable MUX	L.						
Advanc	ted	MUX Server IF	Address						
WLAN Intru	sion Protection	110/12011012	1100/055						
Rogue	AP	Enable MUX S	erver 🥅						
Denial	of Service								
Man-In	i-the-Middle	MUX VLANS							
Signatu	ures	HUA YEARS	Dala	<					
Policies			Dele	(e					

Configuring the L2 / L3 Settings

The VLANs, subnets, and IP address on the local switch need to be configured on the local switch for IP connectivity. (Refer to "Configuring Network Parameters" on page 9.)

Verify connectivity to the master switch by pinging the master switch from the local switch.

On the master switch ensure that the master switch recognizes the new switch as its local switch.

Monitoring	Configuration	Diagnostic	s Mair	itenance	Plan	Events	Reports
Network Network Su	immary	Networl	k > Al	WLAN	Switc	hes	
All WLAN S	witches	Network Sv	witches				
All Access F	Points	Switch IP	Name	Location	Туре	Version	Status
All Air Monit	tors	10.4.21.21	5000	Building1.floo	or1 master	2.4.0.0	up
All WLAN C	lients	10.4.21.11	800	Building1.floo	or1 local	2.4.0.0	up
Global Ever	nts						

The local switch will be listed with type local in the All Alcatel Mobility Controllers page on the master. It will take about 4 – 5 minutes for the master and local switches to sync up configurations.

Configuring Trusted Ports

Navigate to the **Configuration > Switch > Port** page and make sure that the port on the local switch connecting the master is trusted. Repeat for the port on the master switch connecting to the local switch.

Configure the APs

For APs that will boot off of the local switch, you must configure the LMS-IP address. This configuration has to be done on the master switch. When the changes are applied, the master switch will push out these configurations to the local switch.

1. Navigate to the **Wireless LAN > Advanced > General** page. Select the AP that has to bootstrap from the local switch.

- 2 Configure the LMS-IP for the APs under the AP's location ID on the master.
- 3 Apply the configuration on the master.



NOTE—To verify that the local switch has obtained a copy of the global settings, check the local switch for the global config changes made on the master like authentication changes, WMS settings.

Hentorng Configuration	Diagnostics Pt	in Events F	leports	A REAL PROPERTY AND		
Switch General	WLAN > Adv	vanced > G	ener	ral (1.1.20)		
Management	SSID 802.1	1b/g 902.11	1 (General		
Network.	UMS IP	10.3.18.1		Backup LMG IP	-	
Radio	Tunnel MTU			If no value is specified, the MTU will be negotiated		
Advanced	Power Management	P		Double Encrypt (IPSEC AP)	F	
RF Management Calibration	Radio Off Threshold	3		Bootstrap Threshold	35	
Optinization Protection	Rf Band a 🛩					
Monitoring	Disable Radio For Tir	ne Range				
Advanced	Restore configuratio	n to factory default	F			
Security Roles	AP Debugging a	nd Logging				
Policies	Dump Server		1			
AAA Servers Authoritization Matheds	AP Module Log	ging Level				
VDN Settings	SAP Info	national 🐱				
Firesual Settings	AM Wa	nings 💌				
Advanced	SNMP Info	national 💌				
WLAN Intrusion Protection	SNMP System In	formation				and March

Reboot the APs

The configuration changes take effect only after rebooting the affected APs which allows them to reassociate with the local switch. In the example above, AP 1.1.20 will be rebooted. After rebooting, these APs appear to the new switch as local APs.

Location *	AP IP -	AP Type *	.bg Clients/Channel/Power Level *	a Clients/Channel/Power L
1.1.14	10.3.10.03	52	0/13/2	0(44)1
1.1.1B	10.3,18.85	52	1/11/4	0/64/4
1.1.20	10.3.18.56	52	0/0/4	0/161/0
1.1.33	10.3.18.88	61		0/161/0
			1 1-101-1 🛛 🖌	
	L.1.14 1.1.18 1.1.20 1.1.33	1.1.14 10.3.10.03 1.1.18 10.3.18.85 1.1.20 10.3.10.06 1.1.33 10.3.18.88	L.1.14 10.3.10.03 52 1.1.18 10.3.18.85 52 1.1.20 10.3.10.66 52 1.1.33 10.3.18.88 61	1.1.14 10.3.10.03 52 0/13/2 1.1.18 10.3.18.85 52 1/13/4 1.1.20 10.3.10.66 52 0/0/4 1.1.33 10.3.18.88 61 1 1.4.0f 4 ♥

Chapter 5



OmniAccess RN: User Guide
CHAPTER 6 Configuring Wireless LANs

This document details the Wireless LAN configuration using the GUI or the web interface.

Conceptual Overview

The Wireless LAN configuration page is primarily used to set the 802.11 related parameters such the SSID, encryption methods, transmit powers, to name a few. The following section walks the user through the basic 802.11 configurations.

The web interface classifies the Wireless LAN configurations into 3 major categories

- Network—The global Wireless LAN configurations can be done under this section
- Radio—The radio configurations for the .11a and g radio can be done under this section.
- Advanced—This section is primarily used for Access Points having unique configurations that are different from the global settings.

The first few sections deal with the configurations procedures. The last section consists of examples.

Configuring Wireless LAN—802.11 Networks

Pre-requisites

Before configuring a new SSID or editing an SSID setting, you should have the following information regarding the SSID. (This is not mandatory and you can return to these pages to modify the configuration at any time.)

Multiple SSIDs can be configured per AP. When doing so each of the following fields needs to be configured for each SSID separately.

Parameter	Definition	Explanation
SSID	The SSID of the network	
Radio type	Choose the radio types to apply the configurations. a, b/g, a/b/g.	a, b/g, a/b/g.
SSID Default Vlan	The VLAN that would be assigned to the user associating to this SSID. The VLAN should exist at the time of Wireless LAN configuration.	
Encryption type	WEP or TKIP or None.	
WEP	Static WEP or Dynamic WEP.	If Static WEP, the hex key (10 / 24 character size).
ТКІР	PSK or WPA.	If PSK, hex or passphrase
		Hex key should 64 characters in length.
		Passphrase should be 3-63 ascii characters in length.

AES-CCM	Advanced Encryption Standard (AES) in Counter with CBC-MAC (CCM) Mode
Mixed TKIP/AES-CCM	Combined TKIP and AES-CCM
Reply to Broadcast probe requests	Whether the AP should respond to broadcast probe request with this SSID.

1. Navigate to the **Configuration > Wireless LAN > Network** page.

WLAN > Network > SSID												
SSID	General											
SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Period	Actions							
AP-10.3.17.75	802.11a/b/g	Default	No Encryption	1	Edit							
Add												

- 2 To add a new SSID, click **Add**. To edit an existing SSID click **Edit**. The SSID configuration page appears.
- **NOTE**—The default SSID present is Alcatel-ap. This will be broadcast as a valid SSID if the value is not changed This is the only SSID that permits the change of the SSID name.



Monitoring Configuration	Diagnostics Mainte	enance Plan Event	s Reports	Save Configuration Logout
Switch General	WLAN > Netw	vork > Edit SSIE)	« Back
Management	Edit SSID			
Network	SSID	AP-10.4.17.75		
Radio	Radio Type	802.11 a/b/g ⊻		
Advanced	Hide SSID		Encryption	● NULL ○ WEP ○ TKIP ○ AES-CCM
RF Management Calibration	SSID Default VLAN	0 < None 💙	Туре	C Mixed TKIP/AES-CCM
Optimization	Ignore Broadcast Probe Request	v		
Protection Monitoring	DTIM Period	1		
Advanced				
Security Roles	Commands			<u>View Commands</u>
Policies			Apply	
AAA Servers				

SSID	Enter the SSID name used by the wireless clients to associate. The SSID is case sensitive.
Radio Type	Specify the radio type that this SSID will be applied to. This can be applied to the a network only, the b/g network only or to a nd b/g by making the appropriate selection from the pull down menu.
Encryption type	This can be:
	NULL - without any encryption, open system
	WEP
	ТКІР
	AES-CCM
	Mixed TKIP/AES-CCM
SSID Default VLAN	The VLAN that will be assigned to the wireless users after they associate to the SSID. The value for the VLAN can be selected from the pull down menu and the "< " should be clicked on for the changes to the VLAN selection to be applied.
Ignore Broadcast Probe Request	Select this checkbox to prevent the AP from responding back with this SSID to broadcast requests. If this is checked the clients will have to configure the SSID on their client utility to associate with this SSID.
DTIM Period	Delivery Traffic Indication Message.

Once the selection is made, the corresponding dialog windows will open to allow the user to configure as per the selection.

Configuring NULL Encryption

If the encryption type selected is null or the open system then there will be no encryption. The packets between the AP and the client would be in clear text. Click the *Apply* tab to apply the configuration changes made and to prevent loss of work before navigating to other pages.

Monitoring	Configuration	Diagnostics	Maintenano	e Plan	Events	Rep	orts		Save Config	uration	Logout
Switch General		WLAN >	Networ	k > Edi	t SSID						« Back
Manageme	nt	Edit SSID									
WLAN	d.	SSID	AF	P-10.4.17.7	5				~		
Padio	ĸ	Radio Type	8	12.11 a/b/o	~			O NULL (O	WEP C TKIP	O AES-	-CCM
Aduo		indie Type				Francisk	inn	C Mixed TKI	P/AES-CCM		
DE Manago	.eu	Hide SSID	V			Туре	.1011	WEP	•		
Calibra	tion	SSID Default V	LAN 0	< 1	None 🔽			Static WE		WED	
Optimi:	ation	Ignore Broadca Request	ast Probe	1				Selectio	ng Static W	FD En	cryption
Protec		DTIM Period	1]		opens L	WEP Key	confi	duration
Monito	ring							-perior	panel be	low	garanon
Advan	ted								- frances - a		
Security		WEP Keys									
Rules		🔽 Apply Globa	lly (Always app	lied globally)							
Policies		S. No			Use as T	x Key	WEP	Key		S	iize
AAA St	ervers	1								1	0 Hex 🔽
Auther	itication Methods	2			0					1	
VPN Se	ttings	2			· ·						
Firewa	ll Settings	3			0					1	0 Hex 🚩
Secure	Access	4			0					1	0 Hex 🔽
Secure	Service Interfaces				Enter 40-bi	t WEP key	/s as 10) hexadecimal d	igits(0-9.a-f, or	A-F)	
Advan	ted				Enter 128-b	oit WEP ke	eys as 2	26 hexadecimal	digits(0-9.a-f, o	A-F)	
WLAN Intru	sion Protection										
Rogue	AP	Commands						Vie	w Commands		
Denial	of Service										
Man-Ir	-the-Middle					Apply	(
Signati	ures										

Configuring WEP Encryption

- Select the radio button to enable WEP encryption. This opens the WEP encryption dialog
- Select Static WEP or dynamic WEP.
- If Static WEP is selected, the user will have to enter a hex key that would have to configured on the client.
- Click the Use as Tx Key radio button corresponding to the S. No of the key to be used.



- From the pull down menu select the key size 10 hex characters or 26 Hex Characters.
- Type in the key as per the selection made. The characters should belong to the set [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f]. The keys are case insensitive.
- Click **Apply** to apply the configuration changes made and to prevent loss of work before navigating to other pages.

Configuring TKIP Encryption

Monitoring	Configuration	Diagnostics Mainter	nance Plan Event	s Reports	Save Configura	ation Logout
Switch General		WLAN > Netw	ork > Edit SSII	0		« Back
Management		Edit SSID				
Network		SSID	AP-10.4.17.75			
Radio		Radio Type	802.11 a/b/g 💙		ONULL OWEP € TKIP	C AES-CCM
Advanced	ł	Hide SSID	V	Encryption	C Mixed TKIP/AES-CCM	
RF Manageme Calibration	ent N	SSID Default VLAN	0 < None 💌	Туре	C PSK TKIP . WPA TKIP	
Optimizati	ion	Ignore Broadcast Probe Request				
Protection	n	DTIM Period	1			
Monitoring Advanced	J					
Roles		Commands			View Commands	
Policies						
AAA Serv	ers			Apply		

- Select the radio button to enable TKIP encryption. This opens the TKIP dialog.
- Select PSK TKIP for static TKIP key configuration and WPA TKIP for dynamic TKIP.
- If PSK TKIP is selected, the key can be hex or ASCII. Enter a 64 character hex key or a 8 63 character ASCII key.
- From the pull down menu select the key size 10 hex characters or 26 Hex Characters.
- Type in the key as per the selection made. The characters should belong to the set [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f]. The keys are case insensitive.
- Click **Apply** to apply the configuration changes made and to prevent loss of work before navigating to other pages.

Configuring AES-CCM Encryption

NOTE—AES-CCM was formerly referred to as AES-CCMP.

Monitoring Configuration	Diagnostics Mainten	ance Plan Events	Reports	Save Configuration Logout
Switch General	WLAN > Netwo	ork > Edit SSID		« Back
Management	Edit SSID			
WLAN Network	SSID	AP-10.4.17.75		
Radio	Radio Type	802.11 a/b/g 🔽		
Advanced	Hide SSID		Encryption	WPA2
RF Management Calibration	SSID Default VLAN	0 < None 💙	Type	PSK AES-CCM WPA2 AES-CCM
Optimization	Ignore Broadcast Probe Request			Enable Pre-authentication
Protection	DTIM Period	1	Selec	ting PSK AES-CCM will
Monitoring			open	up the key panel below
Advanced Socurity	🔽 Apply Globally (Alway	s applied globally)	1	
Roles	PSK AES Key/Passphrase		Format	Hex 💙
Policies	The PSK AES	Hex Key should be a 64 char	acter hexadecim	al string
AAA Servers	The PSK AES Pass	phrase should be an ASCII st	ring 8-63 charac	ters in length
Authentication Methods				
VPN Settings	Commands			View Commands
Firewall Settings				<u></u>
Secure Access			Apply	
Secure Service Interfaces				

- Select the radio button to enable AES-CCM encryption. This opens the WPA2 dialog.
- Select PSK AES-CCM for static PSK AES key configuration and WPA2 AES-CCM for dynamic AES.
- If PSK AES-CCM is selected, the key can be hex or ASCII. Enter a 64 character hex key or a 8 – 63 character ASCII key.Valid characters are letters and numbers but not spaces, dashes, commas, colons are other punctuation characters.
- Click **Apply** to apply the configuration changes made and to prevent loss of work before navigating to other pages.



Configuring Mixed TKIP and AES Encryption

Monitoring Configuration	Diagnostics Mainter	nance Plan Events	Reports	Save Configuration Logout
Switch General	WLAN > Netw	ork > Edit SSID)	« Back
Management	Edit SSID			
Network	SSID	AP-10.4.17.75		O NULL O WEP O TKIP O AES-CCM
Radio	Radio Type	802.11 a/b/g 🔽		Mixed TKIP/AES-CCM
Advanced	Hide SSID	v	Encryption	Mixed TKIP/AES-CCM
RF Management Calibration	SSID Default VLAN	0 < None 💙	Туре	PSK TKIP/AES-CCM O WPA/2 TKIP/AES- CCM
Optimization	Ignore Broadcast Probe Request			Enable Pre-authentication
Protection Monitoring	DTIM Period	1]	
Advanced Security	Apply Globally (Alway	rs applied globally)	6	Select PSK
Roles	PSK AES Key/Passphrase	•••••	Format	PSK Passphrase V Passphrase for
Policies	The PSK AES	Hex Key should be a 64 cha	racter hexadecim	al string ASCII text keys
AAA Servers	The PSK AES Pass	phrase should be an ASCII s	tring 8-63 charac	ters in length
Authentication Methods				
VPN Settings	Commands			View Commands
Firewall Settings				
Secure Access			Apply	
Secure Service Interfaces				

- Select the radio button to enable TKIP/AES-CCM encryption. This opens the Mixed TKIP/AES-CCM dialog.
- Select PSK TKIP/AES-CCM for static TKIP and AES key configuration or WPA/2 TKIP/AES-CCM for dynamic TKIP and AES.
- If PSK TKIP/AES-CCM is selected, the key can be hex or ASCII. Enter a 64 character hex key or a 8 – 63 character ASCII key.
- Click **Apply** to apply the configuration changes made and to prevent loss of work before navigating to other pages.
- 3 To configure multiple SSID, click **Add** and repeat the steps mentioned above.
- 4 To modify the SSID name The default SSID is the only SSID that permits the changing of the SSID name. To change the SSID but retain the configurations:
 - Create a new SSID with the desired name and settings.
 - Delete the existing SSID entry.
- 5 To configure the general parameters like the SNMP System, Trap receivers, SNMP users navigate to the **Wireless LAN > Network > General** page.

6 Configure the LMS address

The AP can bootstrap with any switch on the Wireless LAN network (in a setup with master and local switches), if all of the switches are on the same VLAN, and if load balancing is enabled on the switches. To force the AP to bootstrap with a particular switch the Imsip is configured with the IP address of the desired switch. The AP is then forced to bootstrap with that switch.

- Navigate to the Wireless LAN > Network > General page.
- Configure the LMS IP address
- Click **Apply** for the change to take effect.

Configuring Wireless LANs—Radio Configuration

The radio settings can be fine tuned using the Web interface. (Selecting these options may affect roaming performance.)

- 1. Navigate to the **Configuration > Wireless LAN > Radio > 802.11b/g** page.
- 2 In case of AP, set the Max Clients to the maximum number of clients that the AP can support. Ideal setting is 20.
- 3 Check the Initial Radio State Up button to ensure that the AP radio is up on reboot.
- 4 Check the Deny Broadcast Enable checkbox to disable probe replies. Otherwise, check **Disable**.
- 5 Check Hide SSID to exclude including the SSID in periodic beacons.
- 6 Set the Mode to Access Point to use the AP as an Access Point. If the AP needs to operate as an Air monitor, check the Air Monitor checkbox under Mode.



Monitoring Configuration	Diagnostics Maintenand	te Plan Events	Reports	Save Configuration Logou
Switch General	WLAN > Radio >	802.11b/g		
Management WLAN	802.11b/g 802.11	a		
Network	RTS Threshold (bytes)	2333	Ageout (secs)	1000
Advanced	Hide SSID		Deny Broadcast	€ Enable ○ Disable
RF Management	Max Retries	4	DTIM Period	1
Calibration	Max Clients	20	Beacon Period (ms)	100
Protection	Initial Radio State	€ Up C Down	Mode	Access Point C Air Monitor
Monitoring	Default Channel	1 💌	Initial Transmit Power	14 dBm(25.119 mW) 💌
Advanced	Short Preamble			
Security Roles	Basic Rates (Mbps)		9 🗆 11 🗖 12 🗖 1	18 🗆 24 🗖 36 🗖 48 🗖 54
Policies	Supported Rates (Mbps)		🗸 9 🔽 11 🔽 12 🔽 1	18 🔽 24 🔽 36 🔽 48 🔽 54
AAA Servers	Commands			View Commands
Authentication Methods VPN Settings	Commanus			View Commands
Firewall Settings	Apply Clear			
Secure Access	inppr) oldar			
Secure Service Interfaces				

- 7 Check **Apply** to apply the changes before navigating to other pages to prevent loss of configuration.
- 8 The above configuration can be created for 802.11a by navigating to the **Configuration > Wireless LAN > Radio > 802.11a** page.

Monitoring	Configuration	Diagnostics	Maintenanc	e Plan	Even	ts	Report	ts		Save Configurat	ion Logout
Switch General		WLAN >	Radio >	802.1	1a						
Managemer WLAN	nt	802.11b/g	802.11	a							
Networ	k	RTS Thresh	iold (bytes)	2333			Ageout	: (secs)		1000	
Advance	ed	Hide SSID		v			Deny B	roadcas	t	€ Enable ○ Disable	
RF Manager	nent	Max Retrie:	5	4			DTIM P	eriod		1	
Calibrat	tion	Max Clients		20			Beacor	n Period	(ms)	100	
Optimiz Protect	ation ion	Initial Radio) State	⊙ _{Up} O	Down		Mode			Access Point C Air	r Monitor
Monitor	ing	Default Cha	annel	52 💌			Initial 1	ransmit	Power	12 dBm(15.849 mW)	¥
Advanc	ed	Basic Rates	(Mbps)	₩6 □9	▼ 12	18	▼ 24	1 36	4 8	54	
Security Roles		Supported	Rates (Mbps)	▼ 6 ▼ 9	№ 12	✓ 18	▼ 24	▼ 36	▼ 48	▼ 54	
Policies AAA Se	rvers	Command	ls							View Commands	
Authen	tication Methods										
VPN Set	ttings	Apply	Clear								
Firewall	Settings										
Secure	Access										

Configuring Wireless LANs—Advanced

While the above two sections deal with global AP configurations, individual AP can be configured with specific settings using the Advanced tab under Wireless LAN. Each of the APs are identified by unique locations and these locations are used to configure the AP uniquely.

The global configurations will be overridden by the location specific configurations.

1. Navigate to the Configuration > Wireless LAN > Radio > Advanced page..

Monitoring	Configuration	Diagnostics	Maintenance	Plan Events	Reports Save (Configuration	Logout
Switch General		WLAN :	> Advance	d			
Managemen	t	Location	Default ESSID	802.11 a Channel	802.11 b/g Channel	Actions	
WLAN							
Network	< Contract of the second se	Add					
Radio							
Advance	ed						
RF Managen Calibrati	ion						

2 Click Add to add a new location.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	WLAN > Advanced
Management	Location Default ESSID 802.11 a Channel 802.11 b/g Channel Actions
WLAN	
Network	Add New Location
Radio	Location 4.2.6 Ex: 1.2.3 (Bldg.Floor.Plan where Bldg=1, Floor=2, Plan=3)
Advanced	Add Cancel Click Add to create a new AP location and go to the advanced
RF Management Calibration	settings for that AP. These will over-ride the global settings

- 3 Enter a location ID of the format

 sldg.floor.plan> where each of these is an integer.
- 4 Click **Add** to add the location. Once the location ID is entered and applied, the global configuration if any will get inherited to the location



Monitoring Cor	nfiguration	Diagnostics	Maintenano	e Plan	Events	Reports	Save Conf	iguration	Logout
Switch General		WLAN >	Advance	ed > SS	ID (4.2	2.6)			« Back
Management WLAN		SSID	802.11b/g	802.11a	Gener	ral			
Radio		SSID	Radio Type	SSID Defa	ult VLAN	Encryption T	ype DTIM	Period	Actions
Advanced		AP- 10.4.17.75	802.11a/b/g	Default		No Encryption	1	i	Edit
Calibration									
Optimization		Add	The glo	bal settin	gs will b	e adopted	to this new	w locatio	on.
Protection			Advanc	ea eaits v	/iii over-	ride the gi	obal settin	gs.	
Monitoring									

The configuration of the specific location can be customized by adding SSIDs and configuring the radios as required by selecting the tabs on the page. To add a new SSID:

1. Click **Add** and configure the SSID similar to configuring the 802.11 Networks.

- 2 All radio configurations for the location can also be made by selecting the 802.11b/g or the 802.11a tab
- 3 Apply the configurations for the configurations to take effect.

Example

The following example includes:

- A a/b/g SSID called Alcatel with dynamic WEP
- A b/g SSID called voice with static WEP
- The AP in location 4.2.6 is set to have guest SSID in addition to the other two SSID. The guest SSID is open

1. Configure the a/b/g SSID Alcatel in the global location 0.0.0 with dynamic WEP.

Monitoring	Configuration	Diagnostics	Maintenance	Plan Ever	nts Reports	Save Configuration Logout
Switch General		WLAN >	Advanced	> Add SS	ID (4.2.6	« Back
Managemer	nt	Add SSID				
WLAN Networ	k	SSID	Alcate	əl]	
Radio		Radio Type	802.11	a/b/g 🔽		ONULL OWEP OTKIP OAES-CCM
Advanc	ed.	Hide SSID			Encryption	C Mixed TKIP/AES-CCM
RF Manager Calibral	ment tion	SSID Default V	LAN 0	< None 💌	Туре	Static WEP
Optimiz	ation	Ignore Broadca Probe Request	ast 🗖			To use dynamic WER ha
Protect	ion	DTIM Period	1]	sure to uncheck Static and
Advanc	ed					check Dynamic WEP
Security		Commanda				Utana Casara da
Roles		commanus				view Commands
Policies						
AAA Se	ervers				Apply	
Authen	tication Methods				прріу	

2 Configure the b/g voice SSID in the global location 0.0.0



Monitoring Configuration	Diagnostics Mainte	nance Plan	Events	Reports		Save Confi	guration Logout
Switch General	WLAN > Adva	nced > A	dd SSII	D (4.2.6)			« Back
Management	Add SSID						
WLAN	SSID	Voice					
Radio	Radio Type (802.11 b/g	V		O NULL O	WEP O TKI	P C AES-CCM
Advanced	Hide SSID	-		Encryption	C Mixed TKI	P/AES-CCM	
RF Management				Туре	WEP		
Calibration	SSID Default VLAN	0 <	None 🚩		🛛 🗹 Static WEI	P) Dynami	c WEP
Optimization	Ignore Broadcast Probe Request						
Protection	DTIM Period	1		Be sure to	o select b/g	and stati	c WEP for
Monitoring				this type of	of AP. Com	plete the	SSID by
Advanced				entering t	he WEP ke	y and Tx	Key below
Security	WEP Keys						
Roles	Apply to Location						
Policies	5. No U	se as Tx Key	WEP Key			Size	
AAA Servers	1 (@			•••		10 Hex 🔽	
Authentication Methods	2	-				10 Hou 👽	
VPN Settings	<u>د</u> ۱۰					TO HEX 💌	
Firewall Settings	3 C					10 Hex 🚩	
Secure Access	4 C					10 Hex 💌	
Secure Service Interfaces	Ent	er 40-bit WEP ke	ys as 10 hex	adecimal digits(0	-9.a-f, or A-F)		
Advanced	Ent	er 128-bit WEP k	eys as 26 he	xadecimal digits(0-9.a-f, or A-F)		
WLAN Intrusion Protection							
Rogue AP	Commands				<u>Vie</u>	w Commands	
Denial of Service							
Man-In-the-Middle							
Signatures				Apply			

- 3 Configure the guest SSID for location 1.10.2
 - Add the location 1.10.2.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save	Configuration	Logout
Switch General		WLAN :	> Advance	d					
Managemer	nt	Location	Default ESSID	802.11 a	Channel	802.11 b/g Ch	nannel	Actions	
WLAN		4.2.6	AP-10.4.17.75	52		1		Edit Delete	
Networ Radio	к			1	1-1 of 3	1			
Advanc	ed	Add New L	ocation						
RF Manager Calibrat	nent ion	Location	1.10.2		Ex: 1.2.	3 (Bldg.Floor.Plar	n where B	3ldg=1, Floor=2, P	lan=3)
Optimiz	ation	Add Can	cel						
Protect	ion								

• Once the location is added, the location page is opened up with the inherited SSID. Click **Add** to add a new SSID guest.

Monitoring Configuration	Diagnostics Maintenance	Plan Events	Reports	Save Config	uration L
Switch General	WLAN > Advanced	SSID (1.10	.2) Once th	e location is :	»
Management WLAN Network	SSID 802.11b/g	802.11a General	SSID ca	n be added to	o it.
Radio	SSID Radio Type	SSID Default VLAN	Encryption Type	DTIM Period	Actions
Advanced	AP-10.4.17.75 802.11a/b/g	Default	No Encryption	1	Edit
RF Management Calibration					
Optimization	Add				
Protection					
Monitoring					

• Configure the SSID with open system and native VLAN for the guest users to be the required VLAN.

Monitoring	Configuration	Diagnostics N	1aintenance	Plan	Events	Reports		Save Configura	ation	Logout
Switch General		WLAN > A	dvanced	> Ad	d SSIE) (1.10.2)			« Back
Managemer	nt	Add SSID								
WLAN Networ	k	SSID	guest							
Radio		Radio Type	802.11	a/b/g 💊	٠					
Advanc	red	Hide SSID				Encryption	⊙ NULL (O WEP O TKIP	C AES	-CCM
RF Manager Calibra	n ent :ion	SSID Default VLAN	J 0	< N	one 🔽	Туре	C Mixed T	KIP/AES-CCM		
Optimiz	ation	Ignore Broadcast Request	Probe							
Protect	ion	DTIM Period	1							
Advanc	ing ed									
Security		Commands					<u>v</u>	/iew Commands		
Roles							_			
Policies										
AAA Se	rvers					Apply				

Adaptive Radio Management

Adaptive Radio Management (ARM) is the next generation RF resource allocation algorithm in AOS-W. ARM is an enhancement to Auto-RRA functionality and performance.

ARM is the state of the art RF management technology for a stable, self healing RF design. ARM takes the distributed algorithm approach allowing APs to decide their transmit power and channel settings based on what they hear in the air. The APs make their channel/power setting decisions based on



the RF environment as they hear it, independent of the switch. This results in a highly scalable and reliable RF environment while also significantly reducing the time the AP takes to adapt to the changing RF environment.

The APs scan all valid channels (channels in the regulatory domain) at regular intervals and compute the following metrics per channel:

- Coverage index: Signal to noise ratio for all valid APs
- Interference index: Signal to noise ratio for all APs

These metric are used by the APs to decide the best channel and transmit power settings for optimal coverage.

Deciding the Channel Setting

In addition to the interference index, the APs use the free-channel index for deciding the optimal channel setting. The free-channel-index is configurable parameter on the switch used by an AP to qualify a channel before moving to it. An AP will choose to move to a new channel only if its current channel interference index is greater than the interference index on the new channel by a value greater than or equal to the free-channel index. If the criteria are not met, the AP will remain on the current channel.

Deciding Power Settings

The power assignment decisions are based on the APs coverage index. The benchmark used here is the ideal coverage index. The ideal-coverage index is the ideal power setting that an AP should have for good coverage. It is a configurable parameter on the switch. The AP will increase or decrease its power settings based on the difference between the value of its current channel coverage index and the ideal-coverage-index value. The power settings increment/decrement by a single unit at any given time.

Advantages of Using ARM

Using ARM provides the following benefits:

- With ARM, the switch does not have a downtime for initial calibration. Though this process is still optional, it is no more a necessity.
- The AP response time to noise is quick and reliable, even to the non-802.11 noise, especially when the client traffic starts generating errors due to the noise.

NOTE—Non-801.11 noise detection is disabled by default and needs to be explicitly enabled.

- ARM algorithm is based on what the AP hears which means that the system can compensate for scenarios like broken antenna and blocked signal coverage on neighboring APs.
- Since channel decisions are based on the information the AP receives from the RF environment, interference due to third-party APs are accounted for.
- ARM compliments Alcatel's next generation AOS-W architecture.

Configuring ARM

1. ARM configuration has to be enabled on the radio PHY- type under **Radio** or under **Advanced**. ARM can be enabled per AP or under the global setting. Navigate to the **Wireless LAN > Radio > 802.11b/g** page to enable ARM on the b/g radio.

witch General	WLAN > Radio >	802.11b/g		
Management /LAN Network	802.11b/g 802.11	a	-	
Radio	RTS Threshold (bytes)	2333	Ageout (secs)	1000
Advanced	Hide SSID	v	Deny Broadcast	C Enable 🙃 Disable
F Management	Max Retries	4	DTIM Period	1
Calibration	Max Clients	4	Beacon Period (ms)	100
Optimization Protection	Initial Radio State	G Up C Down	Mode	• Access Point C Air Monitor
Monitoring	Default Channel	1 💌	Initial Transmit Power	14 dBm(25.119 mW) 🔽
Advanced	Short Preamble	v		
ecurity Roles	Basic Rates (Mbps)	▼ 1 ▼ 2 □ 5 □ 6	□9 □11 □12 □1	8 🗆 24 🗂 36 🗂 48 🗂 54
Policies	Supported Rates (Mbps)	▼ 1 ▼ 2 ▼ 5 ▼ 6	▼ 9 ▼ 11 ▼ 12 ▼ 1	8 🔽 24 🖾 36 🔽 48 🔽 54
AAA Servers	ARM Assignment	Single Band 💌	ARM Client Aware	v
Authentication Methods	ARM Scanning		ARM Scan Time (msecs)	110
VPN Settings	ARM Scan Interval (secs)	10]	
Advanced	Apply Clear	Annual Control of Cont	1	
YLAN Intrusion Protection	(ippi) ereal			
Rogue AP	Commands			View Commands
Denial of Service				
Man-In-the-Middle				
Signatures				
Policies				

- 2 Set **ARM Assignment** to **Single Band** from the pull down menu to enable ARM.
 - **NOTE**—The **Multi Band** option is currently unavailable and is planned to be made available in future releases. Until then, selecting the **Multi Band** option sets the selection to **Single Band** automatically.
- 3 Select ARM Scanning to enable scanning on the AP.



- 4 The **ARM Scan Interval** and **ARM Scan Time** can be set on a per AP basis. These values can be left to the default setting unless they need to be modified for a specific environment.
- 5 The AP will scan the network and hop to the best available channel based on the algorithm. Sometimes the clients may not be able to adapt to this kind of dynamic AP channel change. To disable an AP from changing channel when an active client is connected to it, check **ARM Client Aware**.
- 6 Once these changes are made along with the Radio changes, click **Apply** to apply the configurations.

CHAPTER 7 The External Services Interface

The Alcatel External Services Interface (ESI) provides an open interface to integrate security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance. ESI permits configuration of different server groups— each with group potentially performing a different action on the traffic. The Alcatel ESI can be configured to do one or more of the following for each group:

- Perform health checks on each of the servers in the group
- Redirect specified types of traffic to the server
- Perform per-session load balancing between the servers in each group
- Provide an interface for the server to return information about the client that can place the client in special roles such as "quarantine"

Understanding ESI

In the example shown in this section, the Alcatel ESI is used to provide an interface to the AntiVirusFirewall (AVF)¹ server device for providing virus inspection services. AVF is one of many different types of services supported in the ESI.

^{1.}In AOS -W 2.4, the only AVF server supported is Fortinet.



In the topology shown above the client connect to the Alcatel Access Points (both wireless and wired). The wired access points tunnel all traffic back to the Alcatel switch over the existing network.

The Alcatel switch receives the traffic and redirects relevant traffic (including but not limited to all HTTP/HTTPS, Email protocols such as SMTP, POP3) to the AntiVirusFirewall (AVF) server device to provide services such as Anti-virus scanning, email scanning, web content inspection etc. This traffic is redirected on the "un-trusted" interface between the Alcatel switch and the AntiVirusFirewall (AVF) server device. The Alcatel switch also redirects the traffic intended for the clients – coming from either the Internet or the internal network. This traffic is redirected on the "trusted" interface between the Alcatel switch and the AntiVirusFirewall (AVF) server device. The Alcatel switch forwards all other traffic (for which AntiVirusFirewall (AVF) server does not perform any of the required operations such as AV scanning). An example of such traffic would be database traffic running from a client to an internal server.

The Alcatel switch can also be configured to redirect traffic only from clients in a particular role such as "guest" or "non-remediated client" to the AntiVirusFirewall (AVF) server device. This might be done to reduce the load on the AntiVirusFirewall (AVF) server device if there is a different mechanism such as the Alcatel-Sygate integrated solution to enforce client policies on the clients that are under the control of the IT department. These policies can be used to ensure that a anti-virus agent runs on the clients and the client can only get access to the network if this agent reports a "healthy" status for the client. Refer to the paper on Alcatel-Sygate integrated solution for more details on this solution.

Load Balancing

The Alcatel switch is also capable of load balancing between multiple AntiVirusFirewall (AVF) server appliances. This provides more scalability as well as redundancy by using multiple AntiVirusFirewall (AVF) server appliances. Also the Alcatel switch can be configured to have multiple groups of AntiVirusFirewall (AVF) server devices and different kinds of traffic can be redirected to different groups of devices – with load balancing occurring within each group. This is depicted in the following sample topology.



Configuring the Alcatel ESI

This section describes the relevant configuration required on the Alcatel switch to integrate with a AntiVirusFirewall (AVF) server appliance. Refer to the User Guide for more details on configuring the Alcatel switch.



There are two sections to configure on the Alcatel switch as a part of the solution. The first part configures the "servers" and "server groups". The term "server" here refers to the AntiVirusFirewall (AVF) server device. In the second part the user roles are configured with the policies instructing the Alcatel switch to redirect the different types of traffic to different "server groups"

Configuring the ESI servers

1. To configure the ESI servers on the Alcatel switch, navigate to the **Configuration > Security > External Service Interface** page on the GUI.

Monitoring Co	nfiguration	Diagnostics	Maintena	ance Plan	Events	Reports			
Switch General		Security >	> Grid	Service In	terface	Security	/ Servers		
Management		Security Ser	rvers						
WLAN		Health-Check	Configur	ation					
Network		Profile Name	Frequen	cy Timeout	Retry G	roup Count Act	ions		
Radio		Add							
PE Management									
Calibration		Server Groups	5						
Optimization		Group Name	Health-C	heck Profile	Server Cour	nt Actions			
Protection		Add							
Monitoring									
Advanced		Security Serve	ers						
Security Roles		Server Name	Group	Server Mode	Trusted II	P Untrusted IP	Trusted Port	Untrusted Port	Actions
Policies		Add							
AAA Servers									Apply
Authenticatio	n Methods	Owner and a					10 0		
VPN Settings		commands					view Comman	nas	
Firewall Settin	ngs								
Secure Acces	~								

- 2 Click **Add** in the **Health Check Configuration** section to configure a health check profile. If a profile exists and needs to be edited, click **Edit** for the profile. Provide a name to the profile. Also provide the following details:
 - Frequency (secs): This indicates how frequently the Alcatel switch will attempt to monitor the server(s)'s status (to verify if the server is up and running).
 - Timeout (secs): This indicates the number of seconds the Alcatel switch will wait for a response to its health check query before marking it as a failed health check.
 - Retry count: This is the number of failed health checks after which the Alcatel switch will mark the server as down.
- 3 Click **Done** after this configuration has been entered.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports						Save Configurati
Switch General		Security >	Grid Serv	vice Ir	terfac	e > Secu	rity Server	rs > Add	Profile			
Management		Profile Name	profile1									
WLAN Network		Frequency (secs)			j							
Radio		Timeout (secs)										
Advance	ed	Retry Count										
RF Manager	ent			Done	1							
Calibrati	on											
Optimiza	ition											
Ducksch												

4 Click **Add** button in the **Server groups** section to configure a server group. If a group exists and needs to be edited, click **Edit** for the group. Provide a name to the group and map the required health check profile to this server group.

Monitoring Configura	ation Diagnostics Maintenance Plan Events Reports Save	e Configuratio
Switch General	Security > Grid Service Interface > Security Servers > Add Server Group	
Management WLAN Network	Group Name grp1 Health-Check Profile default 💌	
Radio	Done	
Advanced RE Management		

- 5 Click **Done** to accept this configuration.
- 6 Click **Add** in the **Security Servers** section to add a AntiVirusFirewall (AVF) server device/server.
 - Provide a name to the device/server.
 - Assign this server to a group from the existing configured groups.
 - Choose the mode as bridge/route as the topology may require. Refer to the description above to understand the differences between the two modes.
 - If the bridge mode is chosen, enter the trusted port and un-trusted port as defined above in the description above.
 - If the route mode is chosen, enter the IP addresses of the trusted and un-trusted interfaces on the AntiVirusFirewall (AVF) server device as defined above.
- 7 Click **Done** to accept this configuration.



8 Click **Apply** to apply the configuration (changes). Note that the configuration will not take effect till this step is completed.



Monitoring Configuration	Diagnostics	Maintena	nce Plan	Events	Repo	orts					Save Conf
Switch General	Security :	> Grid S	Service I	nterfa	ce >	Security S	ervers				
Management	Security Se	rvers									
WLAN	Health-Check	Configura	tion								
NELWORK	Profile Name	Frequenc	y Timeout	Retry	Group	Count Act	ions				
Radio	default	5	2	2	1	Edit	Delete				
Advanced	Add										
RF Management											
Optimization	Server Group	s									
Protection	Group Name	Health-Cl	heck Profile	Server C	ount	Actions					
Monitoring	gro 1	default		1		Edit Delete					
Advanced	gipi	der date				Eait Delete					
Security	Add										
Roles	Security Serv	ers									
Policies	Server Name	Group	Server Mode	Trus	ted TD	Untrusted ID	Trusted D	ort I	Intrusted Port	Actions	
AAA Servers	Serverhame	aroup	Server Ploue	Trus	ccu IP	onci asteu ir	nasteuri	one e	Sinci ascell Port	Actions	
Authentication Methods	f1	grp1 r	oute	10.168.1	151.3 (HC)) 10.168.150.3 (HC	.)			Edit Delete	
VPN Settings	Add										

Configuring the User Policy

1. To configure the user roles to redirect the required traffic to the server(s), navigate to the **Configuration > Security > Policies** page.

Monitoring	Configuration	Diagnostics	Maintenance	Plan Events Reports		- 10
Switch General		Security >	Firewall P	olicies		
Management		Name	Rule Count	Policy Usage	A	ction
WLAN		control	5	stateful logon	Edit	Delete
Network		validuser	1	Not Assigned	Edit	Delete
Aduo	d	captiveportal	3	logon	Edit	Delete
RF Managem	ent	allowall	1	trusted-ap default-vpn-role authenticated	Edit	Delete
Calibratio	m	srcnat	1	Not Assigned	Edit	Delete
Optimizal	tion	vpnlogon	5	logon	Edit	Delete
Protectio	n	remediation-only-p	olicy 1	remediation-only	Edit	Delete
Monitorin	ig J	cplogout	1	Not Assigned	Edit	Delete
Security	u	guest	12	guest	Edit	Delete
Roles		stateful-dot1×	0	Not Assigned	Edit	Delete
Policies)	ap-acl	5	Not Assigned	Edit	Delete
AAA Sen	vers	stateful-kerberos	1	Not Assigned	Edit	Delete
VPN Sett	cation Methods ings	Add				

2 Click **Add** to add a new policy. If an existing policy needs to be modified, click **Edit** for the policy.

Monitoring Configuration	Diagnost	ics Mainter	nance P	lan E	vents	Reports						
Switch General	Securi	ty > Fire	wall Po	licies	> Ec	lit Poli	cy(gu	est)				
Management												
Network	Rules											
Radio	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action
Advanced	Add											
RF Management												Apply
Calibration	0											
Optimization	Comman	as						View Comm	ands			
Protection												

- 3 After entering the name for the policy (for new policies), click on Add to add a rule to the policy.
- 4 Choose parameters such as source, destination, service in the same way as other firewall policy rules.

- Select the "redirect to ESI group" from the drop down list as the "Action".
- Select the appropriate ESI-group (configured as described in the "Configuring the ESI servers" section).
- The direction indicates the traffic direction on which this rule is applied. The "forward" direction refers to the direction of traffic from the (untrusted) client or user to the (trusted) server (such as the HTTP server or Email server).

Monitoring Configuration	Diagnostics	: Maintenai	nce Plan	Events	Report:	s								Save	Configurat
Switch General	Security	/ > Firew	all Polic	cies > Ec	lit Poli	icy(gu	est)								
Management															
WLAN															
Network	Rules														
Radio	Source D	estination	Service A	iction Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Prio	rity Action				
Advanced	Add														
RF Management	Source	Destination		Son	dee			Action	1.04	Mirror	Ουρμο	Time Pange	Black Liet	TOS	802 1n B
Calibration	Joarce	Deschadon		561	nce		Conditional In	CCI meren i M	1	, 111101	Queue	nine kange	DIGCK LISC	105	002.101
Optimization			service	~			reulectic	dol gloup			o o .		-		
Protection	any ⊻	any 🚩	Service sv	c-http (tcp 80)		💌 Ne	w GSI Group	grp1 💌	_ □	og 🔲 Mirror	🕑 Low 🔾 High			×	~
Mapitoring							Traffic Dire	ction both	*						
Advanced													Cancel	Add	
Auvaliceu Commitui															
Belor															
Roles	Commands						View Comr	hands							
Policies															
AAA Servers															

- 5 Click **Add** to add this rule to the policy.
- 6 Repeat the steps to configure the redirection policy for all required services/protocols. This would generally include HTTP, HTTPS, SMTP, POP3 at a minimum.

witch	Citignos	uus Mainter	iance i	Plan Events Reports										Save
General	Securi	ity > Fire	wall Po	licies > Edit Policy(g	uest)								
Management														
LAN														
Network	Rules													
Radio	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Ac	tion	
Advanced	any	any	svc-http	redirect gsi-group grp1 direction both			low					Delete		•
F Management	any	any	svc-https	redirect gsi-group grp1 direction both			low					Delete	۸	Ŧ
Calibration	any	any	svc-pop3	redirect gsi-group grp1 direction both			low					Delete	۸	Ŧ
Protection	any	any	svc-smtp	redirect gsi-group grp1 direction both			low					Delete	۸	v
Monitoring	any	any	svc-dns	permit			low					Delete	٨	Ŧ
Advanced	any	any	svc-icmp	permit			low					Delete	٨	T
ecurity	any	any	svc-l2tp	permit			low					Delete		T
Roles	any	any	svc-ike	permit			low					Delete	٨	T
AAA Servers	any	any	svc-dhcp	permit			low					Delete	٨	T
Authentication Methods	any	any	svc-esp	permit			low					Delete	۸	Ŧ
VPN Settings	any	any	svc-pptp	permit			low					Delete	۸	Ŧ
Firewall Settings	any	any	tcp 5900	permit			low					Delete	۸	Ŧ
Secure Access	Add													

- 7 Click **Apply** to apply this configuration. Note that the configuration will not take effect till this step is completed.
- 8 Add this policy to the required. Refer to "Configuring Firewall Roles and Policies" on page 65 for directions on how to apply a policy to a user role.



OmniAccess RN: User Guide

CHAPTER 8 Configuring Firewall Roles and Policies

This chapter discusses configuring firewall roles and policies in an Alcatel network. The firewall roles and policies form the cornerstone of all functionality in an Alcatel Mobility Controller. Every *"user"* in the system is associated with a *"role"* and this role determines the privileges associated with the *"user"*.

Every user in an Alcatel network is associated with a user role. The user role is defined as a set of network privileges permitted to a user associated with the user role. This concept of users and user-roles is central to the entire functioning of the Alcatel network.

In a practical scenario, the administrator can configure firewall policies by creating a new firewall policy and adding rules to the policy or by editing existing pre-defined firewall policies. The administrator can then associate a set of these firewall policies with a user role to define the network privileges associated with a user role.

Every user that associates to the Alcatel network is placed in an initial pre-defined role called *"logon"* role having enough privileges to use one of the authentication methods to authenticate the user and be placed in a user role accordingly. The role of an authenticated user can be derived from the following mechanisms:

1. Server derivation rules: The administrator can configure these rules to match attributes returned by the authentication server (such as the RADIUS attributes) in different ways to values to derive a role for the authenticated user.

As an example, consider a user *abc* authenticated using a RADIUS server. The administrator can create a rule that says if attribute *x* contains the string *"xyz"*, the user shall derive a role called *"Authenticated-user-role1"*. Refer to "Configuring AAA Servers" on page 81 for more explanation on how to configure these rules.

- 2 User derivation rules: The administrator can configure these rules to match a user characteristic in different ways to values to derive a role for the user. The various user characteristics that can be used to derive a user role are:
 - **BSSID** of the Access Point that client is associated to.
 - Encryption type used by the client.
 - **ESSID** that the client is associated to.
 - **Location** of the Access Point that the client is associated to.
 - MAC address of the client.

As an example, the administrator can configure a rule to assign the role *"VoIP-Phone"* to any client that has a MAC address that starts with bytes *xx:yy:zz.*

3 Default role for an authentication method: Every authentication method can be derived with a default role for users that are successfully authenticated using that method. Refer to the guides to configure each of the authentication method (802.1x, VPN, Captive Portal) for more details on how to configure the default role for each authentication method.

As an example, the administrator can configure the default role of all users authenticated using 802.1x as *"employee"*.

Configuring Policies

This section describes the steps to configure the rules that constitute a policy. This policy can then be applied to a user role (until the policy is applied to a user role, it does not have any effect).

Creating a New Policy

To create a new policy:

1. Navigate to the Configuration > Security > Policies page on the WebUI.

Monitoring Configuration	Diagnostics	Maintenance	Plan Events Re	eports		Save Co
Switch General	Security	> Firewa	ll Policies			
Management	Name	Rule Count	Policy Usage	A	ction	
WLAN	control	7	ap-role guest stateful logon	Edit	Delete	
Radio	validuser	1	Not Assigned	Edit	Delete	
Advanced	captiveportal	3	logon	Edit	Delete	
RF Management	allowall	1	trusted-ap default-vpn-role	Edit	Delete	
Calibration	vpnlogon	5	logon	Edit	Delete	
Optimization	srcnat	1	Not Assigned	Edit	Delete	
Monitoring	cplogout	1	guest	Edit	Delete	
Advanced	guest	0	Not Assigned	Edit	Delete	
Security	stateful-dot1x	0	Not Assigned	Edit	Delete	1
Roles	ap-acl	5	ap-role	Edit	Delete	i.
Policies	stateful-kerberos	1	Not Assigned	Edit	Delete	ī .
AAA Servers	Add		-			
VDN Settings						
Firewall Settings						
Secure Access						
Secure Service Interfaces						

2 Click Add to create a new policy.

Monitoring Configuration	Diagnostics Maintenance Pl	an Events Reports	Save Configuration Logout
Switch General	Security > Firewall Po	licies > Add New Policy	
Management WLAN			« Back
Network Radio	Policy Name		
Advanced	Rules		
RF Management Calibration	Source Destination Service Add Clicking Add will ope	Action Log Mirror Queue Time Range BlackList TOS en the rule configuration panel below.	6 802.1p Priority Action
Optimization	Source Destination Serv	ice Action Log Mirror Queue Time R	ange Black List TOS 802.1p Priority
Protection	any 🔽 any 🔽 any	permit 🔽 🗆 Log 🗆 Mirror 📀 Low O High 💌	
Monitoring			Cancel Add
Advanced			
Security			Apply
Roles	Commands	View Commands	

3 Click **Add** to add a rule to the policy being created. The following table summarizes the various fields that are required for a rule to be created and the various options that may be used in the rule.



Field	Required /Optiona I	Explanation	Expected/Recomme nded values
1. Source	Required	Source of the traffic	The source can be configured to be one of the following:
			 any: It acts as a wildcard and applies to any source address. user: This refers to traffic from the wireless client/user. host: This refers to traffic from a specific host. When this option is chosen, it is required to configure the IP address of the host. network: This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, it is required to configure the IP addresses. When this option is chosen, it is required to configure the P addresses. When this option is chosen, it is required to configure the IP address and network mask of the subnet. alias: This refers to using a alias for a host or network. The alias can be configured by navigating to the Configuration > Advanced > Destinations page.
2. Destination	Required	Destination of the traffic	The destination can be configured exactly as the source. Refer above for explanations of each of the options.

3.	Service	Required	Type of traffic. This field can indicate the Layer 4 protocol (TCP/UDP) along with the port numbers of the same or an application such as HTTP/HTTPS	 This can be configured as one of the following: <i>TCP</i>: Using this option, the administrator can configure a range of TCP port(s) to match for the rule to be applied. <i>UDP</i>; Using this option, the administrator.
			etc.	 trator can configure a range of UDP port(s) to match for the rule to be applied. <i>Pre-defined Service</i>: Using this option, the administrator can use one of the pre-defined services (common protocols such as HTTPS/HTTP and many others) as the protocol to match this rule to. <i>Protocol</i>: Using this option the administrator can configure a different layer 4 protocol (other than TCP/UDP) by configuring the IP protocol value.



4.	Action	Required	The action that the administrator wants the switch to perform on a packet that matches the criteria provided above.	 This field can take one of the following fields: <i>permit:</i> Permits the traffic matching this rule. <i>drop:</i> Drops the packets matching this rule without any notification <i>reject:</i> Drops the packet and sends an ICMP notification to the source of traffic. <i>src-nat:</i> Does a NAT translation on the packets matching the rule. When this option is selected, the administrator also needs to select a NAT pool. If this pool is not configured, the administrator pool by navigating to the Configuration > Security > Advanced > NAT pools. <i>dst-nat:</i> Selecting this option redirects the traffic to the configured IP address and destination port. An example of this option is to redirect all HTTP packets to the captive portal port on the Alcatel Mobility Controller as used in the pre-defined policy called "captiveportal". <i>redirect:</i> This option is used to redirect traffic into a GRE tunnel. This option is used to redirect all guest traffic into a GRE tunnel. This option is used primarily to redirect all guest traffic into a GRE tunnel. This option is used primarily to redirect all guest traffic into a GRE tunnel. This option is used primarily to redirect all guest traffic into a GRE tunnel.

5.	Log	Optional	This field indicates if any match of this rule should be logged.	Select this option if it is required to log a match to this rule. It is recommended to use this option when a rule indicates a security breach such as a data packet on a policy that is meant only to be used for voice calls.
	Mirror	Optional		
6.	Queue	Optional	This field indicates the queue in which a packet matching this rule should be placed.	Select the high priority queue for higher priority data such as voice and low priority queue for the type of traffic that may be lower in priority.
7.	Time Range	Optional		



8.	Black List	Optional	This field indicates that a client that is the source or destination of traffic that matches the rule should be automatically blacklisted.	Select this option if it is required to auto-blacklist a client that is involved in a traffic session matching this rule. This option is recommended for rules that indicate a security breach and the blacklisting option can be used to prevent access to clients that are attempting to breach the security.
9.	ToS	Optional	This field indicates the ToS bits in the IP header that should be marked for packets matching the rule.	Value of ToS bits to be marked in the packet when it leaves the switch if it matches the rule.
10.	802.1p Priority	Optional	This field indicates the 802.1p priority bits that should be marked for frames matching this rule.	Value of 802.1p priority to be marked in the frame when it leaves the switch if it matches the rule.

Monitoring	Configuration	Diagnostics	Maintenano	e Plan Events	Reports						Sar	re Config	uration Logout
Switch General		Security	/ > Firewa	all Policies >	Add Nev	v Policy							
Managemen	x.												< Back
WLAN													
Network	k	Policy Name									Block serv	rice polic	y
Radio		Rules											
RF Managen Calbrat	red ment Son	Source I Add	Destination	iervice Action L	og Mirror	Queue Time Ra	nge Blad	kList TO	6 802.1p Pri	ority Action			
Optimizi	ation	Source	Destination	Service	•	Action	Log	Mirror	Queue	Time Range	Black List	105	802.1p Priority
Protecti	ion			service 💌									
Monitori	ing			Service		and and		—	e		-	_	
Advano	ed	ary 💌	any 💌	svc-telnet (tcp 23)	~	refect	V Log	g Mirror	Cow C High	Y			
Security				New									
Roles											Cancel	Add	
Policies													A state
AAA Set	rvers												Apply
Authors	binabian Mable da	Commands				View Co	mands						

4 Click **Add** to add this rule to the policy being created. If more rules are needed, follow the same process to create and add more rules to the policy

Monitoring Configuration	Diagnosti	s Maintena	nce Plar	n Events Report	5							Save Co	nfiguration	Logout
Switch General	Secur	ity > Fire	wall Po	licies > Add Ne	w P	olicy								
Management WLAN														< Back
Network														
Dadia	Policy Nam	Policy Name Block service policy												
Radio	Rules													
Advanced	Source	Destination	Service	Action	Log	Mirror	Oueue	Time	Range	BlackList	TOS	802.1p Priority	Acti	
RF Management	1000	2011	Second?	dem cend-dem-remonse	Ver		hish			No			Delete	
Calibration	any	any	stepops	ueity senu-ueity-response	165		ingri			140			Diere.	
Optimization	any	any	"svc-teinet"	deny send-deny-response	Yes		low			No			Delete	A Y /
Protection	Add												~	
Monitoring									Once	multiple	rules	are created.		terration of
Advanced								_	they	can be pri	oritize	d using the	-	Apply
Security	Comman	nds					lew Commar	vds	up an	d down b	uttons	on the		
Roles									right.					
Policies														

NOTE—If required, the rules can be re-ordered by the using the up and down buttons provided with each rule.

5 Once all the required rules are created (and ordered as required), click the Apply button to apply this configuration.

NOTE—The policy is not created until the configuration is applied.

Editing an Existing Policy

1. Navigate to the **Configuration > Security > Policies** page on the WebUI. This page shows the list of the currently existing policies.

Monitoring	Configuration	Diagnostics N	4aintenance	Plan Events Rep	orts	Save	Configuration Logout
Switch General		Security >	Firewall	Policies			
Management		Name	Rule Count	Policy Usage	A	ction	
WLAN		control	7	ap-role guest stateful logon	Edit	Delete	
Network		validuser	1	Not Assigned	Edit	Delete	
Advancer	4	captiveportal	3	logon	Edit	Delete	
RF Manageme	ent	allowall	1	trusted-ap default-vpn-role	Edit	Delete	Confirm policies
Calibratio	n 🤇	Block service policy	2	Not Assigned	Edit	Delete	are created
Optimizat	ION	vpnlogon	5	logon	Edit	Delete	and constant
Protection	r	even ak	1	Not Accine ad	E dit.	Delete	
Monitorin	g	sruiau	1	NUC ASSIGNED	CUIC	Delete	
Advanced	ł	cplogout	1	guest Ed		Delete	Edit or delete
Security		guest	0	Not Assigned	Edit	elete	policies by
Roles		stateful-dot1×	0	Not Assigned	Edit	Delete	clicking on the
Policies		an-acl	5	an-role	Edit	Delete	appropriate
AAA Serv	ers				- In	Delete	action button
Authentic	ation Methods	stateful-kerberos	1	Not Assigned	Edit	Delete	
VPN Setti	ngs	Add					
Firewall S	ettings						

2 Click **Edit** for the policy that is to be edited. In the example shown below the "guest" policy is being edited.



3 On the Edit policy page, the administrator can delete existing rules, add new rules (following the same procedure in Step 3 of "Creating a New Policy" on page 66), or reorder the policies.

Monitoring	Configuration	Diagnostics	Maintenand	e Plan:	Events	Reports					Sav	re Configur	ration Logout
Switch General		Securi	:y > Firew	all Polic	cies > E	lit Poli	icy(gu	est)					
Managemer	it												« Back
WLAN													
Networ	k	Rules											
Radio		Source	Dectination	Service A	ction Log	Mirror	Ουριο	Time D	ange Blackli	et TOS	802 1p Priority	Action	
Advanc	ed	Add	Descination		iccion Log	1 11 101	Queue	TIME K	inge blacker	50 105	002.1101101103	Accion	
RF Manager	nent	Muu											
Calibrat	ion	Source	Destination	Service	Ac	tion	Log	Mirror	Queue	Time Rang	ge Black List	T05 8	302.1p Priority
Optimiz	ation	any 💊	any 🔽	any 🔽	permit	1	🖌 🗖 Log	Mirror		~		~	*
Protect	ion										Cancel	Add	
Monitor	ing												á poly
Advanc	ed												whhia
Security		Command	ls					View Cr	ommands				
Roles													

- 4 When all rules have been edited as required, click **Apply** button to apply the configuration.
- **NOTE**—The changes will not take effect until the configuration is applied by using this step.

Applying the Policy to a User Role

This section outlines the steps required to apply the policy to a user role. A policy can be applied to one or more user roles. Similarly, each user role can constitute one or more policies.

1. Navigate to the **Configuration > Security > Roles** page on the WebUI. This page shows the list of currently configured user roles and the policies that constitute each user role.

Monitoring Con	figuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Co	onfiguration
Switch General		Security	> User Ro	les				
Management		Name	Firewall Pe	olicies	Bandw	idth Contrac	: Actio	ns
WLAN		ap-role	control, ap-acl		Not Enfo	rced	Edit D	elete
Network		trusted-ap	allowall		Not Enfo	rced	Edit D	elete
Radio		default-vpn-role	allowall		Not Enfo	rced	Edit D	elete
RF Management		guest	control, cplogout		Not Enfo	rced	Edit D	elete
Calibration		stateful-dot1×	Not Configured		Not Enfo	rced	Edit D	elete
Optimization		stateful	control		Not Enfo	rced	Edit D	elete
Protection Monitoring		logon	control, captive po	rtal, vpnlogo	n Not Enfo	rced	Edit D	elete
Advanced		Add						
Security								
Roles								
Policies								

2 If creating a new user role, click **Add** to start creating and configuring a new user role.


- 3 Enter the desired name for the role. In the example used below, the name given to the role is *"employee"*.
- 4 To apply a set of policies to this user role, click the Add button in the Firewall Policies section.



Monitoring Con	iguration Diagnos	tics Mainten	ance Plar	Events	Reports	Save Configuration	Logout
Switch General	Secu	rity > Use	r Roles	> Add Ro	le		
Management WLAN							« Back
Radio	Role N	ame employee]			
Advanced RF Management Calibration Optimization Protection Monitoring Advanced Econution	Firewa Name controln Add	II Policies Rule Count W 7	Location 0.0.0 ed Policies CO	Action Edit Delete	Location 0.0	.0	-
Roles Policies AAA Servers Authentication VPN Settings	Methods	ate New Policy C	m Existing Polie	y control	Crea	Done Cancel	
Firewall Setting Secure Access	IS Re-aut	hentication In Change	i terval e (O disables	re-authenticatio	n. A positive value	enables authentication)	

The following table summarizes the different fields visible and the expected/recommended values for each field.

	Field	Explanation	Expected/recommended values			
1.	Firewall Policies	This will consist of the policies that will define the	There are three options to add a firewall policy to a user role:			
		privileges of a user in this role. The field called Location is used when a policy is meant to be used only in a particular location. As an example, the administrator can configure access to the HTTP protocol only in conference rooms and lobbies. The location code is in the <i>building.floor.location</i> format. The location code can be a specific AP or a	 Choose from configured policies: Select a policy from the list of configured policies and click the "Done" button to add the policy to the list of policies in the user role. If this policy is to be applied to this user role only for specific locations, the applicable location codes can be entered in the field called "Location" Create a new policy from configured policy: This option can be used to create a new policy that is derived from an existing policy. 			
		wildcard value of 0.	option is useful in creating a new policy. The rules for the policy can be added as explained in step 1.a.iii above.			
2.	Re-authenticatio n interval					
3.	Role Vlan-ID	By default, a user is assigned a VLAN on the basis of the ingress VLAN for the user to the switch. This feature can be used to over ride this assignment and provide role-based VLANs.	If this option is required, configure the VLAN ID that is to be assigned to the user role. Note: This VLAN ID needs to be configured with the IP configuration for this to take effect.			



4.	Bandwidth contract	A bandwidth contract can be assigned to a user role to provide an upper limit to the bandwidth utilized by users in this user role. As an example, the administrator may want to cap the total bandwidth used by the guest users in a network to 2Mbps.	To create a new bandwidth contract, select the "Add New" option. Enter the name of the bandwidth contract and the bandwidth to be allowed (in kbps or mbps). Click Done to add the new contract and assign it to the role.
		If the per-user option is selected, the bandwidth contracts are applied on a per-user basis as compared to all users in the role.	
5.	VPN Dialer	This assigns a VPN dialer to a user role. For details about VPN dialer, refer to the "Configuring VPNs" section.	Select a dialer from the drop-down list and assign it to the user role. This dialer will be available for download when a user logs in using Captive Portal and is assigned this role.
6.	L2TP Pool	This assigns a L2TP pool to the user role. For more details about L2TP pools, refer to the "Configuring VPNs" section.	Select the required L2TP pool from the list to assign to the user role. The inner IP addresses of VPN tunnels using L2TP will be assigned from this pool of IP addresses for users in this user role.
7.	PPTP Pool	This assigns a PPTP pool to the user role. For more details about PPTP pools, refer to the "Configuring VPNs" section.	Select the required PPTP pool from the list to assign to the user role. The inner IP addresses of VPN tunnels using PPTP will be assigned from this pool of IP addresses for users in this user role.

5 After entering the values as explained above, click **Apply** to apply this configuration.

NOTE—The role will not be created until the configuration is applied.

6 To edit an existing role, click **Edit** for the required user role to start editing a user role. The fields are the same as shown above. The screen shot below shows the screen when the **Edit** option is chosen for the *"guest"* user role.

Monitoring	Configuration	Diagnostics	Maintenance P	lan Events	Reports	Save Configuration	Logout
Switch		Security	> User Role	s > Edit Ro	le(quest)	`	
General		occurrey .	00011010		ic(guese)		
Managemer	nt						« Back
WLAN	ŀ						
Padio	ĸ	Firewall Polici	ies				
Aduppa	-od	Name Rule	Count Location	Action			
REManager	nent	control 7	0.0.0	Edit Delete	A V		
Calibrat	tion	cologout 1	0.0.0	Edit Delete			
Optimiz	ation	cpiogode 1	0.0.0	Ealt Doloto			
Protect	ion	Add					
Monitor	ring						
Advanc	ed	Re-authentic	ation Interval				
Security		Disabled	Change (0 disab	les re-authenticatio	n. A positive val	ue enables authentication)	
Roles							
Policies		Role VLAN IF	1				
AAA Se	ervers	Not Assigned	r Iot Assigned 🔽 — Ch	20.00			
Authen	tication Methods			lange			
VPN Set	ttings						
Firewal	l Settings	Bandwidth C	ontract				
Secure	Access	Not Enforced	oice (384kbps) 🔽	Change 🗌 🗖 Pe	r User		
Secure	Service Interfaces						
Advanc	ed	VPN Dialer					
WLAN Intru: Rogue	sion Protection AP	Not Assigned N	ot Assigned 👻 🛛 Ch	lange			
Denial o	of Service	L 2TD Dool					
Man-In-	-the-Middle	default-l2to-pool	Not Assigned	Chapter			
Signatu	ires	uerauic-iztp-poor	Not Assigned	Change			
Policies							
		PPTP POOL		- •			
		default-pptp-poo	ol Not Assigned 🚩	Change			
		Commands				View Commands	
		Apply					



OmniAccess RN: User Guide

CHAPTER 9 Configuring AAA Servers

The software allows users to use an external server or create an internal user database for authentication purposes. This document briefly describes the configuration procedure involved on the switch to interface with an external authentication server (RADIUS and LDAP), or to create an internal database of users and set the authentication timers for authentication purposes.

To try and authenticate users, external authentication servers are often used. The switch needs to be configured with information about the servers to enable it to interface with these servers. On the server side, the switch needs to be recognized for the server to process requests from the switch. This document talks only about the configuration on the switch. The configuration on the server side, specific to the server, should be done as per the vendor specification.

Authentication Timers

Currently two authentication timers are available for configuration by the administrator - the User Idle Timeout and the Authentication Server Dead Time. These timers are common to all users and RADIUS servers and apply to all servers and users. These timers can be left at the default values for most implementations.

Accessing the Configuration page

- 1. Login to the web interface.
- 2 Navigate to Configuration > Security > AAA Servers. The AAA server configuration page displays.
 - c. Configure the timers on the General tab.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > AAA Servers > General
Management	General Radius LDAP Internal DB Accounting
WLAN Network	Authentication Timers
Radio	
Advanced	User Idle Timeout (minutes) 5
RF Management Calibration	Authentication Server Dead Time (minutes) 10
Optimization	Apply
Protection	
Monitoring	
Advanced	Commands <u>View Commands</u>
Security	
Roles	
Policies	
AAA Servers	

4 Set the user idle timeout value. The value of this field is in minutes. To prevent the user from timing out set the value of this field to 0.

The user idle timeout is the time in minutes for which the switch maintains state of an unresponsive client. If the client does not respond back to the switch within this time, the switch deletes the state of the user. The user will have to re-authenticate to gain access once the user state has been deleted. Set the value of the user idle timeout. The value of this field is in minutes

5 Set the Authentication Server Dead Time value in minutes.

The Authentication Server Dead Time is applied only when there are two or more authentication servers configured. The authentication Server Dead Timeout is the maximum period for which an authentication server is proclaimed dead before being activated again.

Scenario 1: If the authentication server is the only server. In this case the server is never marked down and all requests are sent to this server irrespective of the timer setting.

Scenario 2: If one or more backup servers are configured.

In this case, once the server (server A) is found to be un-responsive it is marked as down and the subsequent requests are sent to the next server on the priority list. The server A is marked down for the dead time after which it is brought back into the list. If the priority of this server is higher than the server currently servicing the requests, this server (server A) takes over. If it is still non-accessible, it will be marked down for the Authentication Server Dead Time Period.

- 6 Once the values are set click **Apply** before moving onto another page or closing the browser. Failure to do this will result in the loss of configuration and the user will have to reconfigure the settings.
- 7 To save the configuration, click the Save Configuration tab on the upper right hand corner of the screen.

RADIUS Server Configuration

To add a new RADIUS server entry:

1. The values to the following parameters are required. A good habit would be to collect this information for every RADIUS server that needs to be configured prior to configuration. Individual values can be re-configured and applied in case of errors and changes at any time.

Parameter	Description	Value in the Example
Server Name	< The name of the Authentication Server >	Radius_Server_1
IP Address	< The address of the authentication server>	192.168.100.1
Shared Secret	<the and="" auth="" between="" secret="" server="" shared="" switch="" the=""></the>	Alcatel
Authentication Port	<the 1812="" authentication="" default="" on="" port="" server.="" the=""></the>	1812 (default maintained)
Accounting Port	<the 1813="" accounting="" default="" on="" port="" server.="" the=""></the>	1813 (default maintained)
Num of Retries	<maximum number="" of="" retries="" sent<br="">to the server by the switch before the server is marked as down. Default 3></maximum>	3 (default maintained)
Timeout	<the in="" maximum="" seconds,<br="" time="">the switch waits before timing out the request and re-sending it. Default 5 seconds ></the>	5 (default maintained)

- 2 Navigate to Configuration > AAA Servers > RADIUS page.
- 3 Configure the RADIUS settings.



Monitoring	Configuration	Diagnosti	cs Mainten	iance Plan	Events	Reports	Save	e Configuration	Logout
Switch General		Secur	ity > AAA	Servers	s > Rad	ius Server	s		
Managemen	t	Gener	al Radius	LDAP	Internal	DB Account	ting		
WLAN		Name	IP Address	Authenticati	on Port 🖌	ccounting Port	Status	In Service	Action
Network	C	Add							
Radio			Any existin	ng servers	will be lis	sted in this ta	able. Cli	ck	
Advance	ed		Add to cre	ate a new l	Radius se	rver.			
RF Managen	nent								
Calibrati	ion								
Optimiza	ation								
Protecti	on								

4 Click **Add** to add a new RADIUS server entry. Enter the values gathered from the previous step.

Monitoring	Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration	Logout
Switch General		Security > AAA Servers > Radius Servers > Add	Radius Server	
Managem	ent			« Back
WLAN	ork	Server Name		
Radio		IP Address		
Adva	nced	Shared Secret		
RF Manage	ement	Verify Shared Secret		
Optim	nization	Authentication Port	1812	
Prote	ction	Accounting Port	1813	
Monit	oring	Num Retries	3	
Adva	nced	Timeout	5	
Security				
Policie	5	Match ESSID		
AAA :	Servers		Add Delete	
Authe	entication Methods			
VPN S	Settings	Match FQDN		
Firew	all Settings		Add Delete	
Secur	e Access	Trim FQDN		
Secur	e Service Interfaces	Mode	Enable V	
Adva WLAN Tobe	nced	Corrior Dulas		
WLAN INC	e AP	Rule Action Attribute Condition Matching Value Value Action		
Denia	l of Service	Add Click add to open cerver rules window to create a		
Man-J	(n-the-Middle	new raidus server rule	Apply	
Signa	tures			
Policie	es	Commands View	v Commands	

- 5 Set the Mode to **Enable** to activate the authentication server.
- 6 Click **Apply** to apply the configuration.

NOTE—The configuration will not take effect until this step is performed.

7 For additional RADIUS servers, repeat steps 1 through 6.

Monitoring Configuration	Diagnostics Mainte	enance Plan Eve	ents Reports		Save C	onfiguration	Logou
Switch General	Security > AA	A Servers > R	adius Servei	s			
Management	General Radi	us LDAP Inte	rnal DB Accoun	iting			
WLAN	Name IP Address	Authentication Port	Accounting Port	Status	In Service	Action	
Network	Radius 1 192.1.1.1	1812	1813	Enabled Y	es	Edit Del	lete
Radio	Radius 2 192.1.2.1	1812	1813	Enabled Y	es	Edit Del	lete
Advanced	0.d.d						
RF Management	AUG						

Editing an Existing Entry

- 1. Navigate to the Configuration > AAA Servers > RADIUS page.
- 2 Click Edit on the right side of the desired RADIUS Server entry.
- 3 The configuration page displays. Make the required modifications on the page and click **Apply** to save the configurations.

Deleting an Existing Entry

- 1. Navigate to the Configuration > AAA Servers > RADIUS page.
- 2 Click **Delete** on the right side of the desired RADIUS Server entry. A pop-up window displays with the message "Are you sure you want to delete the RADIUS server <RADIUS server name>?"

Monitoring Configuration	Diagnostics Mainte	enance Plan Ever	nts Reports		Save Configuration	Logout		
Switch General	Security > AA	A Servers > Ra	adius Server	s				
Management	General Radi	us LDAP Inter	hal DB 🛛 Accoun	ting				
WLAN	Name IP Address	Authentication Port	Ac Qunting Port	Status In Service	Action			
Network	Radius 1 192.1.1.1	1812	1813	Enabled Yes	Edit Delete			
Radio	Radius 2 192.1.2.1	1812	1813	Enabled Yes	Edit Delete			
Advanced PF Mapagement	Add							
Calibration								
Optimization								
Protection		Microsoft Internet F	kolorer					
Monitoring								
Advanced		Are you sure	vou want to delete the	e radius server Radius 2?				
Security		V						
Roles								
Policies		OK Cancel						
AAA Servers								
Authentication Methods								

3 To continue with the deletion click **OK**. The entry is deleted.



Advanced AAA Settings

Alcatel's AAA Advanced feature is a licensed feature that configures a Alcatel Mobility Controller to allow users using one authentication method (like Captive Portal or 802.1x) to be authenticated against different authentication servers based on the domain and realm (FQDN) used by the client or the client associated ESSID.



In the topology shown above, all clients authenticate using the same method (for example, Captive Portal). Alcatel allows all users using sales.com to authenticate against auth server *Server1* and the engineering users using the engineering.com in their user name to authenticate against *Server2*.

Additionally, Alcatel supports users associating with the guest ESSID to authenticate against *Server2*.

This feature adds flexibility to AAA configuration by allowing IT managers to maintain servers by departments or ESSIDs in different campuses, or in cases where two different companies merge

Captive Portal configurations permit users to see the FQDN configured during user logon.

Selecting the Right Server

The server is selected if the user name contains any configured Fully Qualified Domain Name (FQDN) or the user ESSID matches any of the ESSIDs configured for the server.

The selection of the server happens as follows, in the order of server prioritization:

- Server is skipped if disabled or out of service.
- Server is selected if there is no FQDN and ESSID filters configured.
- Server is selected if the user ESSID matches any ESSID attached with the server.
- Server is selected if the user name has a FQDN component and it matches any FQDN attached with the server.
- **NOTE**—The FQDN match is attempted if, and only if, the username has a FQDN component and the server has at least one FQDN configured for matching. If server has a FQDN list configured, but the user name does not have a FQDN component, the server will not be selected.

Configurations

- 1. Navigate to the Configuration > AAA Servers > RADIUS page.
- 2 To add a new server, follow the steps described in "RADIUS Server Configuration" on page 83.
- 3 To modify the server settings, click **Edit** to the right of the server entry.
- 4 To add a new ESSID that will be used by this server, click on **ADD ESSID**.
- 5 In the resulting dialog box, add the ESSID (case sensitive) as configured and press **ADD**. Repeat this step to add more ESSIDs that will be used by this server.



Configuration	The information of the second s	ophy at 2005-03-14 00:00	1:00
Gerenal Gerenal Management	Security > AAA Servers > Radius Servers > Edi	t Radius Server((best3)
MLAN Materic	Barror Nama	turt?]
Radio	JF Addross	10.105.8.7]
Advanced	Sharod Source]
UP Managemeent	Yorly Shared Docret]
Colimination	Authoritication Fort	1812]
Probaction	Accounting Part	1817]
monsoring	Num Robitos	3]
Advanced	Timoset	8	1
Recurrey	Match CEOP	omployoo Add	Daloto
Policies	add ere	momenth quest	
AAA Service		Add	Cannel
Puthentication methods		Ideall com	
WPTV Settinge	Match PQDN	dept2.com Add	Delete
Rrewell Eattings	THIM FOOM		
Gold Service Interface	Mode	Enable 😁	
Advenced	Carver Rules		
MLAH Indexation Protection	Rule Action Attribute Condition Matching Value Talue Action		
Decisi of Castles	Add		
the second se			Apply

- 6 To add the domains that this server will use, click **ADD FQDN**.
- 7 In the resulting dialog box, add the entry and click **ADD**. To add more entries, repeat this step.
- 8 To trim the FQDN portion of the username before sending the credentials to the auth server, check the TRIM FQDN option. If this option is not selected, the username along with the FQDN component is sent to the server and the server should be configured for the same for a match to be successful.

For example : Client3@sales.com is the username the user uses to authenticate. If TRIM FQDN is enabled, only Client3 is sent to the server. If unchecked, Client3@sales.com is sent to the server for authentication.

9 Click **APPLY** to apply the changes before navigating to another page.

Example Deployment

All departments use the same authentication method (such as 802.1x) and the same ESSID for all users and departments to ensure smooth mobility but users of each department are authenticated against the RADIUS server maintained by the department for control.



Users can move across the departments but the users belonging to *department1* will always use the RADIUS server in *department1* regardless of whether they are trying to authenticate from *department1* or *department2* as long as they use the right FQDN.

LDAP Server Settings

NOTE—As of AOS-W 2.4 and higher LDAP support has been expanded to include Secure LDAP.

To add a new LDAP server entry:

 Navigate to the Configuration > AAA Servers > Security > LDAP page. To configure the switch, the following information is required.

Parameters	Description	Values
Server Name	<the ldap<br="" name="" of="" the="">server></the>	LDAP_Server1
IP Address	<the address="" ip="" ldap="" of="" server="" the=""></the>	192.168.200.1
Authentication Port	<the ldap<br="" on="" port="" the="" which="">server is configured. The default value is 389.></the>	600



Base DN	<the distinguished="" name="" of<br="">the node which contains the entire user database that we want to use.></the>	cn=Users,dc=Im,dc=AlcateIn etworks, dc=com
Admin DN	<a has="" read="" search<br="" user="" who="">privileges across all the entries in the LDAP database. The user need not have write privileges ñ the user should be able to search the database, and read attributes of other users in the database.>	cn=Alcatel Admin,cn=Users,dc=Im, dc=AlcateInetworks,dc=com
Admin Password		Alcatel
Key Attribute	<the attribute="" contains<br="" that="">the unique key for the LDAP object. This is the name of the attribute that contains the login ID of the users.></the>	sAMAccountName
Filter	<the be<br="" filter="" should="" that="">applied to search of the user in the LDAP database. The default filter string is: ì(objectclass=*)î.></the>	(objectclass=*)
Timeout	< The timeout period of a LDAP request in seconds. Default is 10 seconds>	10

2 Click ADD to add a new entry.



- Monitoring Configuration Diagnostics Maintenance Plan Events Reports Switch Security > AAA Servers > LDAP Servers > Add LDAP Server General Management « Back WLAN Server Name LDAP 1 Network Is Server Active Directory Radio Advanced IP Address 192.1.1.1 RF Management Authentication Port Calibration Base DN Optimization Protection Admin DN Monitoring Admin Password Advanced Verify Admin Password Security Key Attribute Roles Policies Filter AAA Servers Timeout Server rules can be created and prioritized Authentication Methods Mode using the add, up and down buttons Enable 🔽 VPN Settings Server Rules Firewall Settings Rule Type Attribute Condition Matching Value Value Action Secure Access Role Assignment test ends-with 1 ap-role Delete 🔺 🔻 Secure Service Interfaces Add Advanced WLAN Intrusion Protection Apply Rogue AP Commands View Commands Denial of Service
- 3 Fill in the information collected from step 1.

- 4 Set the mode to **Enable** to enable the LDAP server when it is online.
- 5 Click **Apply** to apply the changes made to the configuration.
 NOTE—The configuration does not take effect until this step is performed.

6 To add multiple servers, repeat steps 1 through 5 for each server.

Monitoring	Configuration	Diagnostics	Mainter	nance Plai	n Ever	its Re	ports	Save Configuration	Logout
Switch General		Securit	y > AA	A Server	s > LD	AP Se	ervers		
Managemen	it	General	Radiu	s LDAP	Intern	nal DB	Accounting		
WLAN		Name I	^o Address	Authentica	tion Port	Status	In Service	Action	
Networi	ĸ	LDAP 1 193	2.1.1.1	389		Enabled	yes	Edit Delete	
Radio		Add							
Advano	ed								

Editing an Existing Entry

- 1. Navigate to the Configuration > AAA Servers > Security > LDAP page.
- 2 Click **Edit** for the entry to be modified and modify the desired parameters.
- 3 Click **Apply** to have the changes take effect.



Deleting an Existing Entry

- 1. Navigate to the Configuration > AAA Servers > Security > LDAP page.
- 2 Click **Delete** for the entry to be deleted. A pop-up box displays with the message "Are you sure you want to delete the LDAP server <server name>?"

Monitoring Configuration	Diagnostics	Maintenance	Plan Events	Reports	Save Configuration	Logout
Switch General	Security	> AAA Serv	/ers > LDAP	Servers		
Management	General	Radius LD	AP Internal DB	Accounting		
WLAN	Name IP A	ddress Auther	tication Port Stal	us In Service	Action	
Network	LDAP 1 192.1	1.1 389	Enable	ed yes	Edit Delete	
Radio	Add					
Advanced						
RF Management						
Calibration		Microsoft Inte	rnet Explorer			
Optimization						
Protection		🕐 Arey	ou sure you want to de	lete the LDAP server	LDAP 1?	
Monitoring						
Advanced						
Security				Lancei		
Roles						

3 Click **OK**. The entry is deleted.

Internal Database

The internal database can also be used to authenticate users. The internal database can store a list of users along with the user password and their default role. When the switch is configured as the primary server, user information in the incoming authentication requests will be checked against the internal database.

The internal database is used to store user name and passwords. One entry needs to be created for each user.

To add a new user entry to the Internal Database:

1. Navigate to the **Configuration > AAA Servers > Internal Database** page.

The parameters, a description of the parameters and the values used in this example are listed below.

Parameter s	Description	Values used in the example
User Name	<the be="" name="" that="" used<br="" user="" will="">by the user. Mandatory field></the>	User1
Password	<the of="" password="" the="" user.<br="">Mandatory field></the>	User123
Role	<the get="" is="" not<br="" role="" the="" user="" will="">configured. Optional field. Default is guest></the>	-None-
mail	<the address="" email="" of="" the="" user=""></the>	User1@example.com

2 Click Add User under Users. The user configuration page displays.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General Management	Security > AAA Servers > Internal Database General Radius LDAP Internal DB Accounting
WLAN	Server Rules
Network	
Radio	Rule Action Attribute Condition Matching Yalue Value Action
Advanced	Role Assignment Role value-of Delete 🔺 🔻
RF Management	Add
Calibration	Maintenance
Optimization	Expert Import Delete All Users Benair Database
Protection	Export Import Delete All Osers Repail Database
Monitoring	Users
Advanced	
Security	User Name Password Role E-mail Enabled Expiry Action
Roles	Test 1 ****** guest test1@example.com Yes Disable Delete Modify
Policies	Add User
AAA Servers	1 1-1 of 1
Authentication Methods	- 1- 1011

- 3 Add the user information.
- 4 Check the **Enable** box if this entry needs to be activated on creation. If this box is unchecked, this user entry will not be considered during authentication.
- 5 Configure the role of the user.



Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports		Save Configuration	Logout
Switch General		Security	> AAA Sei	vers >	Inter	nal Dat	abase > A	dd User	
Managemer	nt								« Back
WLAN	k	User Name		User1					
Radio		Password		•••••					
Advanc	ed	Verify Password	ł	•••••					
RF Manager Calibrat	nent ion	Role			~				
Optimiz	ation	E-mail		r1@exan	nple.com				
Protect	ion	Enabled		v					
Monitor	ing	• Entry does	not expire						
Advanc Security	ed	C Set Expiry t	time (mins)						
Roles		O Set Expiry (Date (mm/dd/yyyy)) E	xpiry Time(hh	:mm) 🔡 :		
Policies						Арр	ly		
AAA Se	rvers								

6 Apply the configuration by clicking **Apply** after creating each user.

NOTE—The changes will not take effect until this step is performed.

7 Click **Back** and verify that all the users created are visible.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Log	gout
Switch General Management	Security > AAA Servers > Internal Database General Radius LDAP Internal DB Accounting	
WLAN	Server Rules	
Network		
Radio	Rule Action Attribute Londition Matching Value Value Action	
Advanced	Role Assignment Role value-of Delete	
RF Management	Add	
Calibration	Maintenance	
Optimization	Export Import Delete All licers Repair Database	_
Protection		
Monitoring	Users	
Advanced		
Security	User Name Password Role E-mail Enabled Expiry Action	
Roles	Test 1 ******* guest test1@example.com Yes Disable Delete Modify	
Policies	User1 ******* guest User1@example.com Yes Disable Delete Modify	
AAA Servers	Add licer	-
Authentication Methods	Verify all the users you create are in this table	
VPN Settings		
Firewall Settings		
Secure Access		
Secure Service Interfaces		

Editing an Existing Entry

- 1. Navigate to the **Configuration > AAA Servers > Internal Database** page.
- 2 To edit an existing entry, delete the entry and re-create the entry with the necessary modifications.

All entries must be individually created and modified.

Deleting an Entry

- 1. Navigate to the **Configuration > AAA Servers > Internal Database** page.
- 2 Clicking **Delete** to the right of the entry on the page. A pop up window displays which says "Are you sure you want to delete the user <user name>?"

Monitoring	Configuration	Diagnostics	Maintenan	ce P	lan Events	Reports		Save	e Configuration	Logout
Switch General Manageme	int	Security General Server Rules	> AAA S Radius	LDAF	Internal DB	Accounting	ise			
Netwo	rk									
Radio		Rule Action	Attribu	ite Co	ndition Matchi	ng Value 🛛 Valu	e Actio	n		
Advan	ced	Role Assignm	ent Role	val	ue-of		Dele	te 🔺 🔻		
RF Manage	ment	Add								
Calibra	ation	Maintenanc	9							
Optimia	zation	Export	Import	Delet	e All Licerc	Repair Data	hace			
Protect	tion	Export	Import	Delet	te Air Osers	Kepair Data	5430			
Monito	ring	Users								
Advan	ced									
Security		User Name	Password	Role	E-mail	Enabled	Expiry	Action		
Roles		Test 1	alelelelelek	guest	test1@example.	com Yes		Disable	Delete M	odify
Policies	5	User1	****	guest	User1@example	.com Yes		Disable	Delete M	lodify
AAA Se	ervers	Add User								
Auther	ntication Methods								1	
VPN Se	ettings				Microsoft	Internet Explo	rer	<u> </u>		
Firewa	II Settings									
Secure	e Access				\mathbf{Q}	Are you sure you (want to del	ete user Test 1?		
Secure	e Service Interfaces									
Advan	ced					ОК	Cancel			
WLAN Intru	ision Protection									
Rogue	AP									

3 Click **OK** to delete the entry.

Configuring Server Rules

Once a server is configured, it is possible to set the VLAN and role for some users based on the attributes returned for the user during authentication. These values would take precedence over the default role and VLAN configuration for the authenticated user.



To add a server rule:

- 1. Navigate to the **Configuration > Security > AAA Servers** page.
- 2 Select the authentication Server type from the tabs.
- 3 Click **Add** under Server rules. The server rule page displays.

Monitoring Configuration	Diagnostics	: Maintenance Plan Events Reports Save Confi	guration Logout
Switch General	Securit	y > AAA Servers > Radius > Add Server Rule	« Back
Management WLAN	Rule Type	Role Assignment 💙	
Network		a-Admin-Role	
Radio	Attribute	a-User-Vlan	
Advanced		a-User-Role	
RF Management	Add Attr	ribute Delete Attribute	
Calibration	Condition	contains 🗸	
Optimization	11-h-s		
Protection	Value		
Monitoring	Role/Vlan	ap-role 🗸	
Advanced		Done	
Security			
Roles			
Policies			
AAA Servers			

The parameters are:

Paramet er	Description
Rule type	This can be one of Role Assignment or Vlan Assignment. With Role assignment, a user can be assigned a specific role based on the RADIUS attributes returned. In case of VLAN assignment, the user can be placed in a specific VLAN based on the RADIUS attributes returned.
Attribute	This is the attribute that is returned by the RADIUS server based on whose value the user is assigned a role or a VLAN

	in <i>Value</i> is matched with the attribute value returned by the AAA server.						
	 contains - the rule is applied if and only if the attribute value contains the string in parameter <i>Value</i>. Starts-with - the rule is applied if and only if the attribute value returned starts with the string in parameter <i>Value</i> Ends-with - the rule is applied if and only if the attribute value returned ends with the string in parameter <i>Value</i> Equals - rule is applied if and only if the attribute value returned equals with the string in parameter <i>Value</i> Not-equals - rule is applied if and only if the attribute value returned is not equal to the string in parameter <i>Value</i> Value-of - This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned as the value of the attribute selected must be already configured on the switch when the rule gets applied. 						
Value	This specifies the value that the attribute must match along with the condition for the rule to be applied.						
Role / VLAN	The role or the VLAN applied to the user when the rule is matched.						

Condition The condition specifies the match method using which the string

The server rules are applied based on the first match principle. The first rule that is applicable for the server and the attribute returned will be applied to the user and would be the only rule applied from the server rules.

These rule will also be applied uniformly across all the authentication types that use the server as the primary authentication server.

Example

Based on the filter-ID returned, users will be classified as admin, employee and guest.

Parameter	Value	Role
MS-Filter	EMP	employee
MS-Filter	ADMIN	Admin

If none of the rules match, the role is set to the default role of the authentication type.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration Logout
Switch	Security > AAA Servers > Radius Servers > Add Radius Ser	ver
Management		« Paole
WLAN	Course Manage	« DdCk
Network	Server Name	Radius I
Radio	IP Address	192.1.1.1
Advanced	Shared Secret	•••••
Calibration	Verify Shared Secret	•••••
Optimization	Authentication Port	1812
Protection	Accounting Port	1813
Monitoring	Num Retries	3
Advanced	Timeout	5
Security		
Policies	Match ESSID	
AAA Servers		Add Delete
Authentication Methods		
VPN Settings	Match FODN	
Firewall Settings		Add Delete
Secure Access	Trim FODN	
Secure Service Interfaces	Mode	Enable V
Advanced	Prode	
Reque AP	Server Rules Rule Action Attribute Condition Matching Value Value Action	
Denial of Service	Role Assignment M5-CHAP2-CPW equals EMP ap-role Delete A	
Man-In-the-Middle	Role Assignment a-Admin-Role equals ADMIN default-von-role Delete	i)
Signatures	Add	
Policies	Confirm rules are created and in the correct order	Analy
		Abbiy

The first rule that matches the condition gets applied. Also the rules are applied in the order shown. To change the order use the \blacktriangle or \triangledown arrows to the right of the entry.

CHAPTER 10 Configuring the Captive Portal

This document deals with the configuration of captive portal to support guest logon and for user authentication.

One of the methods of authentication supported by the Alcatel Mobility Controller is captive portal. This document outlines the steps required to configure the captive portal authentication parameters for both guest logon as well as standard user authentication. Captive portal can be configured to authenticate users against an external / internal database or skip the authentication and allow users gain limited access into the network by allowing them to logon as guests. Captive portal can also be configured to allow users to download the Alcatel VPN dialer for the Microsoft VPN client if the VPN is going to be terminated on the Alcatel Mobility Controller.

Alcatel Mobility Controller also allows the customization of the logon page. **Captive Portal customization** will talk about customizing the captive portal page.

Configuring Captive Portals for Guest Logon

Configuring captive portal for guest logon does not require an authentication server. A user trying to access the network will be assigned a logon role. The user will then have to pull up a browser. The user will be re-directed to a logon page, where the user will need to enter the credentials (an email ID in this case). The user is then granted a default role with limited access to browse the internet.

1. Navigate to the **Configuration > Security > Authentication Methods > Captive Portal Authentication** page.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > Authentication Methods > Captive Portal Authentication
Management WLAN	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption Advanced
Network	Address and a state of the stat
Radio	Authencication Enabled
Advanced	Default Role guest
Calibration	Enable Guest Logon
Optimization	Enable User Logon 🔽
Protection	Enable Logout Popup Window
Monitoring	Protocol Type (Chttps:) firewall captive portal policy for HTTP
Advanced	Redirect Pause Time(secs) or HTTPS under Security > Policies
Roles	Welcome Page Location /auth/welcome.html
Policies	Logon Wait Interval
AAA Servers	
Authentication Methods	CPU Utilization Infeshold
VPN Settings	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Firewall Settings	Show FQDN List
Secure Access	Sygate On-Demand Agent
Secure Service Interfaces	Enable Agent Support
Advanced	Remediation failure role
WLAN Intrusion Protection Roque AP	Remediation failure LIRI. N/A
Depial of Service	
Man-In-the-Middle	
Signatures	Authentication Corvers
Policies	Name Type II Address Authentication Port Status Actions
	Add Apply
	Commands <u>View Commands</u>

- 2 Configure the role that the guest logon users will take. (See *"Configuring Firewall Roles and Policies"* for information on configuring a role).
- 3 Determine the protocol captive portal will use. Modify the *captiveportal* policy to support the selected protocol.
 - **HTTP:** If the protocol selected is http, ensure that the following rules are included in the *captiveportal* policy:

Monitoring Configuration		Diagnosti	es Maintena	ince Pl	an Events	5 R	eports					Save Co	nfiguration	L	.ogou
Switch General		Secur	ity > Fire	wall Po	olicies >	Edi	: Polic	:y(cap	tiveportal))					
Management WLAN														« E	3ack
Network		Rules													
Radio		Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Acti	n	
Advanced	1	user	mswitch	svc-http	permit			low					Delete	۸	¥
Calibration	ſ	user	any	svc-http	dst-nat 8080			low F	Be sure these	policies	are ex	ist to allow	Delete	۸	¥
Optimization	1	user	any	svc-https	dst-nat 8081			low	ior captive r	ortarior	guesti	ittp logon.	Delete	۸	¥
Protection		Add If	the policies	do not	exist, then										
Advanced		cre	ate them us	ing the	add buttor	۱.								(ppl)	f
Security		Commar	nds						View Commands						
Roles															
Policies															

user alias mswitch svc-http permit user any svc-http dst-nat 8080 user any svc-https dst-nat 8081

• **HTTPs:** If the protocol is https, ensure that the *captiveportal* policy has the following rules:

Monitoring Configuration	Diagnostic	s Maintena	nce Pla	n Events	; Re	eports					Save Cont	figuration	Log	gout .
Switch General	Secur	ity > Fire	wall Po	licies >	Edit	Polic	y(cap	tiveportal))					
Management WLAN													« Ba	ck
network Darka	Rules													
Radio	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Actio	n	
Advanced	user	mswitch	svc-https	permit			low					Delete	۰ ا	,
Calibration	user	any	svc-http	dst-nat 8080			low	Be sure to	have http	s for		Delete	•	•
Optimization	user	any	svc-https	dst-nat 8081			low	the mswitch	permit al	nd the		Delete		7
Protection	Add							enable a	n https lo	ain				-
Monitoring	_						1		to service of			0	noly	
Advanced									_			~	pp17	-
Security	Commar	nds						View Commands						
Roles														
Policies														

user alias mswitch svc-https permit user any svc-http dst-nat 8080 user any svc-https dst-nat 8081

4 In the default user role of un-authenticated users (*logon* role by default), ensure that the *captiveportal* policy has been added. The user traffic needs to hit the rules in this policy for captive portal to work.



Monitoring Configuration	Mainte	nance Plan	Events	Reports		1000000	an Calabati Cara	SPRAISES AS	20	10 10	Save Configuration	1 Logout
Switch	Secur	ity > Fire	wall Po	licles >	Edi	t Polic	y(captive)	portal)				
Management WLAN Network												« Back
Radio	Rules										1	
Advanced	Source	Destination	Service	Action	Log	Queue	Time Range	BlackList	TDS	802.1p Priority	Action	
RF Management	user	mswitch	syc-https	permit		low					Delete * *	
Calbretion	user	any	svc-http	dst-nat 0000		low					Delete * *	
Protection	user	any	svc-https	dst-nat 8081		low					Delete * *	
Monitoring	Add											
General											Apply	

5 Configure the captive portal parameters.

Parameter	Description
Default role	The role assigned to the guest user on logon.
	Default: guest
Enable Guest Logon	This field need to be checked to enable guest logon as explained above.
	Default: Unchecked
Enable User Logon	This field needs to be checked to enable user logon authentication using an authentication server. In case of guest logon this field needs to be unchecked if captive portal is used for guest logon only.
	Default: Checked
Enable Logout Popup Window	When this is enabled, a pop up window will appear with the Logout link for the user to logout after the user logs in.
	If this is disabled, the user remains logged in till the user timeout period or till station reloads as the user does not have a logout mechanism.
	Default: Checked
Protocol type	The protocol used on re-direction to captive portal page. http / https – If http is selected, the captive portal policy will have to be modified to allow http traffic.
	Default: https

Redirect Pause Timeout	This is the time seconds, the system remains in the initial welcome page before re-directing the user to the final web URL. If set to 0, the welcome page is skipped.
	Default: 10 seconds
Welcome Page Location	The welcome page is the page that appears soon after logon and before re-direction to the web URL. This can be set to any URL.
	Default: /auth/welcome.html
Logon wait Interval	Time range in seconds, the user will have to wait for the logon page to pop up in case the CPU load is high. This works in conjunction with the CPU Utilization Threshold.
	Default: 5 - 10 seconds
CPU Utilization Threshold	The CPU utilization percentage above which the Logon wait interval gets applied while presenting the user with the logon page.
	Default value: 60 %

- 6 From the pop-down menu select the desired role the user will be placed in after logon.
- 7 Uncheck the **Enable User Logon** checkbox if the intended use of captive portal is for guest logon alone. If Captive Portal will be also used to authenticate users against a AAA server, leave this option selected.
- 8 Check **Show FQDN** to enable advanced AAA. (Requires that FQDNs be configured for the RADIUS servers.)
- 9 Set the protocol type http or https as per the requirement.
- 10 Set the welcome page location to the required URL.
- 11 Click **Apply** to apply the configuration.

NOTE—The configuration does not take effect till this step is completed.

Example

This example sets up the captive portal for guest only logon:

 The user gets cap_guest role which allows user to access the internet only.



- If CPU utilization is above 50% wait for 10 -15 seconds before popping up logon page.
- In this example, there is no "*pause time*" before redirecting to the captive portal page.

Monitoring Configuration	Maintenar	nce Plan	Events	Repor	ts	1		 	 Save Config	ration Lo	gout
Switch	Security	/ > User	Roles >	Edit	Role	(lo	gon)				
Management						1					
WLAN Network										« Ba	sck
Radio	Firewall Po	licies									
Advanced	Name	Rule Count	Location		Action						
RF Management Calibration	control	s	0.0.0	Edit	Delete	*	•				
Optimization	captiveportal	3	0.0.0	Edit	Delete	*	•				
Protection	vpnlogon	5	0.0.0	Edit	Delete						
Monitoring	Add					-					
General											

Parameter	Values for this example
Default role	cap_guest
Enable Guest Logon	Checked
Enable User Logon	Unchecked
Enable Logout Popup Window	Checked
Protocol type	https
Redirect Pause Timeout	0
Welcome Page Location	Leave as default
Logon wait Interval	10 – 15
CPU Utilization Threshold	50

Configuring Captive Portal for User Logon

Captive Portal can also be used to authenticate users using an authentication server. It can interface will all servers that the switch can support.

1. Navigate to the **Configuration> Security > Authentication Methods > Captive Portal Authentication** page.

Monitoring Configuration	Diagnostics Maintenance Plan Events	Reports Save Configuration Logout
Switch General	Security > Authentication Meth	ods > Captive Portal Authentication
Management WLAN	802.1x VPN Captive Portal MAC	Address Stateful 802.1x SSID L2 Encryption Advanced
Radio	Authentication Enabled	
Advanced	Default Role guest 💉	
RF Management Calibration	Enable Guest Logon	
Optimization	Enable User Logon	
Protection	Enable Logout Popup Window	V
Monitoring	Protocol Type	C http thtps
Advanced Security	Redirect Pause Time(secs)	0
Roles	Welcome Page Location	/auth/welcome.html
Policies	Logon Wait Interval	10 - 15 seconds
AAA Servers	CPU Utilization Threshold	50 %
VPN Settings	Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)
Firewall Settings	Show FQDN List	

- 2 Configure the role that a user authenticated using captive portal will take. ("Configuring Firewall Roles and Policies" on page 65 for information on configuring a role).
- 3 Determine the protocol captive portal will use. Modify the *captiveportal* policy to support the selected protocol.
 - **HTTP:** If the protocol selected is http, ensure that the following rules are included in the captive portal policy

Configuration	n in the	69972 J. HEL	ARRAND R	120018						11111	10000000000000000000000000000000000000	C 191218
Sultch	Secur	tty > Fire	wall Po	dicles >	Edi	Polic	v(captive)	portal)				
Management:		- A - 11 - 11 - 11 - 11 - 11 - 11 - 11 -			9999	10 2312						
Nation National												K Badk
Radio	Rates										1	
Advanced	Source	Destination	Service	Action	Log	Quese	Time Range	Backint	TOS	BO2.1p Priority	Action	
RF Management	LEPET	nswitch	sychttps	permit		low -					Daleta	
Calibration	11997	54	sychttp	dst-nat 8080		loe:					Delate 3 Y	
Optimisation				11 1		1					mentioned (2) (2)	
Protection	TRea.	a.4	sychtigs	B8-N8080		10M					Delete	
Maniforming	bba											
General											Apple	

user alias mswitch svc-https permit user any svc-http dst-nat 8080 user any svc-https dst-nat 8081



• **HTTPs:** If the protocol is https, ensure that the *captiveportal* policy has the following rules

Configura	ation	1917 - HU	A STATE	1. (11)(11)							STREET, LANS	2 . M228.
Sultch	Secur	tty > Fine	wall Po	dicles >	Edi	Polic	(captive)	portal)				
WLAN Babwark												« Badk
Radio	Rule:											
Advenced	Source	Destination	Service	Action	Log	Quese	Time Range	Backlat	TOS	BO2.1p Priority	Action	
RF Management	UP9T	nsetch	sve-https	permit		loe .					Dalata	
Calibration	mea.	511	syc-http	dst-nat 6060		low					Balata 2 ¥	
Optimisation				AN BOARD		11					succession and the state	
Protection	Rea.	any.	syc-https	dst-nat/6061		loe .					Daleta * *	
Maritoring	bba											
General											Apple	

user alias mswitch svc-https permit user any svc-http dst-nat 8080 user any svc-https dst-nat 8081

4 In the default role for unauthenticated users (*logon* role by default), ensure that the *captiveportal* policy has been added. The user traffic needs to hit the rules in this policy for captive portal to work.

Switch Security > User Roles							
Management Name Firewall Policies Bandwidth Contract	Actions						
WLAN ap-role control, ap-acl Not Enforced Ed	it Delete						
natio trusted-ap allowall Not Enforced Ed	it Delete						
Advanced default-vpn-role allowall Not Enforced Ed	Edit Delete						
RF Management guest control, cplogout Not Enforced Ed	it Delete						
Calibration stateful-dot1x Not Configured Not Enforced Ed	it Delete						
Optimization stateful control Not Enforced Ed	it Delete						
Protection I control I was a state of a stat	it Delete						
Monitoring logon control, captiveportal, vpnlogon Not Enrorced	C Delete						
Advanced Add							
Security							
Roles							
Manifestra Conferentias Diservatias Distributions Director	0						
Monitoring Configuration Diagnostics Maintenance Han Events Reports	Save Configuration Log						
Switch Security > User Roles > Edit Role(logo	n)						
Management							
WLAN	« Ba						
Network							
Radio Firewall Policies	Firewall Policies						
Advanced Name Rule Count Location Action							
RF Management control 7 0.0.0 Edit Delete A V	Confirms the three						
Calibration Captiveportal 3 0.0.0 Edit Delete A V	rules that have						
vpnlogon 5 0.0.0 Edit Delete A V	been configured						
Protection Add							
monitoring							

5 Configure the captive portal parameters.

Parameter	Description
Default role	The role assigned to the guest user on logon.
	Default: guest
Enable Guest Logon	This field needs to be checked to only if guest logon needs to be enabled in addition to user logon.
	Default: Unchecked
Enable User Logon	This field needs to be checked to enable user logon authentication using an authentication server.
	Default: Checked
Enable Logout Popup Window	When this is enabled, a pop up window will appear with the Logout link for the user to logout after the user logs in.
	If this is disabled, the user remains logged in till the user timeout period or till station reloads as the user does not have a logout mechanism.
	Default: Checked
Protocol type	The protocol used on re-direction to captive portal page. http / https – If http is selected, the captive portal policy will have to be modified to allow http traffic.
	Default: https
Redirect Pause Timeout	This is the time (in seconds) that the system remains in the initial welcome page before re-directing the user to the final web URL. If set to 0, the welcome page is skipped.
	Default: 10s



Welcome Page Location	The welcome page is the page that appears soon after logon and before re-direction to the web URL. This can be set to any URL.
	Default: /auth/welcome.html
Logon wait Interval	Time range in seconds, the user will have to wait for the logon page to pop up in case the CPU load is high. This works in conjunction with the CPU Utilization Threshold.
	Default: 5 – 10s
CPU Utilization Threshold	The CPU utilization percentage above which the Logon wait interval gets applied while presenting the user with the logon page.
	Default value: 60 %

- 6 From the pull-down menu select the desired role the user will be placed in after logon. Note that this role would be applied only if there are no other derivation rules that supersede it.
- 7 Ensure that the Enable User Logon checkbox is selected
- 8 Set the protocol type http or https as per the requirement.
- 9 Set the welcome page location to the required URL.

Configuring the AAA Server for Captive Portal

To configure the AAA server that captive portal will use for authentication:

1. Click Add under the Authentication Servers heading.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout						
Switch	Security > Authentication Methods > Cantive Portal Authentication						
General	Security > Authentication Methods > Captive Fortan Authentication						
Management	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption Advanced						
Network							
Radio	Authentication Enabled 🔽						
Advanced	Default Role employee 🗸						
RF Management Calibration	Enable Guest Logon						
Optimization	Enable User Logon 🔽						
Protection	Enable Logout Popup Window 🔽						
Monitoring	Protocol Type C http: C https						
Advanced	Redirect Pause Time(secs) 0						
Roles	Welcome Page Location /auth/welcome.html						
Policies	Logon Wait Interval 10 - 15 seconds						
AAA Servers	CPULIBilization Threshold 50 %						
Authentication Methods	A skewisting Taking Threshold (an Chaine Diaditation D						
VPN Settings							
Firewall Settings	Show FQDN List						
Secure Access	Sygate On-Demand Agent						
Secure Service Interraces	Enable Agent Support						
WLAN Intrusion Protection	Remediation failure role						
Rogue AP	Remediation failure URL N/A						
Denial of Service							
Man-In-the-Middle							
Signatures	Authentication Servers						
Policies	Name Type IP Address Authentication Port Status Actions						
	Apply						
Choose an Authentication Server							
	Internal/Server Tunel ocal IP Address 10 200 14 2111 V Add Cancel						
	Internal/Server Type:Local IP Address:10.200.14.211)						

- 2 Under **Choose an Authentication Server** is a pull down menu. From this menu select the authentication server that will be the primary server.
- 3 Click **Add** for the selection to be applied.
- 4 To add more authentication servers as backup servers, repeat the steps above.
- 5 The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the or to the right on the entry to move it higher up or lower down in the list.
- 6 Click the **Apply**, for the configuration changes made to take effect.

Example

This example sets up the captive portal for user logon:

• The user gets *employee* role.



- If CPU utilization is above 50% wait for 10 -15 seconds before popping up logon page. No redirect pause time at the welcome page.
- Select the RADIUS Server as the primary server. If this server fails use the internal server for authentication.

Monitoring	Configuration	Diagnostics	Mainte	enance Pl	an Events	Repo	rts	Save	e Config	guration Logout
Switch		Security > Authentication Methods > Cantive Portal								
General		Authent	icatio	n						
WLAN	ic.									
Networl	<	802.1x	VPN	Captive F	Portal MAC	: Addres	ss Sta	iteful 802.1)	(S	SID L2 Encryption
Radio		Advanced								Encryption
Advanc	ed									
RF Managen	nent	Authentication	Enabled	R						
Ontimiz.	ation	Defeult Dele	rendbiod							
Protecti	00	Derault Role		employee	*	-				
Monitor	ina	Enable Guest I	.ogon							
Advanc	ed	Enable User Lo	ogon			~				
Security		Enable Logout Popup Window			V					
Roles		Protocol Type C http			O http	O http: https://www.communications.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/organizations.com/orga				
Policies		Pedirect Pauce Time(cecc)			0					
AAA Se	rvers					ter l				
Authen	cication Methods	Welcome Page Location			/auth/weicome.html					
VPN Set	contract	Logon Wait Interval 10 - 1			- 15	seconds				
Firewall	Settings	CPU Utilization Threshold 50 %								
Secure	Aucess Somico Interfaces	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)								
Advanc	ad	Show FQDN List				Ensure the				
WLAN Intrus	ion Protection	Servers are in the correct								
Rogue /	AP	Enable Agent	Support							priority order.
Denial o	f Service	o tra								use the arrow
Man-In-	the-Middle	Remediation failure role llogon keys to adjust								
Signatu	res	Remediation h	ailure URL	. N/A						1
Policies		Authenticat	tion Ser	vers						
		Name	Туре	IP Address	Authenticatio	on Port	Status	Action	5	
		Radius Server F	Radius 1	0.1.15.1	1812		Enabled	Delete	• •	
		Internal L	ocal 1	0.200.14.211	n/a		Enabled	Delete	▲ ▼	
		Add						A	pply	
									_	

Parameter	Values for this example
Default role	employee
Enable Guest Logon	Unchecked
Enable User Logon	Checked
Enable Logout Popup Window	Checked
Protocol type	https
Redirect Pause Timeout	0
---------------------------	------------------
Welcome Page Location	Leave as default
Logon wait Interval	10 – 15
CPU Utilization Threshold	50
Authentication Server	Radius_Server_1
	Internal_Server

Personalizing the Captive Portal Page

The following can be personalized on the captive portal page:

- Captive portal background
- Page text
- Acceptance Use Policy
- 1. Navigate to the Maintenance > Captive Portal > Customize Login page.

When both the user and guest logins are enabled, the default role applies to the user login. A user logging in using the guest interface gets the guest role.





You can choose one of three page designs. To select an existing design, click the first or the second page design present.

To customize the page design,

- 1. Select the YOUR CUSTOM DESIGN page.
- 2 Under **Additional Information**, enter the location of the JPEG image in the space provided beside **Upload your own custom background**.
- 3 You can also set the background color in the **Custom page background color**. The color code has to a hex value of the format #hhhhhh.

4 The background setting can be viewed by first clicking **Submit** on the bottom on the page, then clicking the **View CaptivePortal** link that will actually open up the captive portal page as seen by the users.



To customize the captive portal background text:

Enter the text that will needs to be displayed in the Page Text (in HTML format) message box. To view the changes, click Submit at the bottom on the page and then click the View CaptivePortal link. This will bring up the captive portal page as seen by the users

To customize the text under the Acceptable Use Policy:

• Enter the policy information in the **Policy Text** text box. This appears only in case of guest logon. To view the changes, click **Submit** at the bottom on the page and then click the **View CaptivePortal** link. This will bring up the captive portal page as seen by the users







The text keyed in will appear in a text box when the **Acceptable Use Policy** is clicked on the captive portal web page.



OmniAccess RN: User Guide

CHAPTER 11 Configuring 802.1x Security

The main aim of this document is to help the user configure 802.1x through web interface. This document includes a description of the steps, examples and any common problems the user needs to watch out for while configuring 802.1x on the Alcatel Mobility Controllers.

802.1x is an IEEE standard designed to provide authentication before L2 access to the network is permitted. The authentication protocols that operate inside the 802.1x framework suitable for wireless networks include EAP-TLS, PEAP and TTLS. These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. These authentication protocols are all based on EAP (Extensible Authentication Protocol) and are also referred to as EAP types.

The 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 and permits or denies access to the supplicants. Finally, the *authentication server* provides a database of information required for authentication and informs the authenticator with information to deny or permit access to the supplicant.

The Alcatel Mobility Controller acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type or authentication protocols are transparent to the switch and have to be consistent between the authentication server and supplication or client.

Default Open Ports

You need to be aware that when you are configuring security for your wireless network, some (trusted) ports on Alcatel Mobility Controllers are open by default. For details on these ports, refer to the *AOS-W Reference*.

Configuring Wireless User Authentication Only

802.1x can be used to authenticate users. The procedure for configuring wireless user authentication is described in this section.

1. Prior to configuring 802.1x on the switch, the following need to be configured:

- **Role** The role that will be assigned as the default role for the 802.1x users. (*Refer to "Configuring Firewall Roles and Policies" on page 65*).
- Authentication Server The authentication server the switch will use to validate the users. Verify that the authentication server supports 802.1x. Most LDAP servers do not. The Internal Server does not support 802.1x either. (*Refer to "Configuring AAA Servers" on page 81*)
- **AP encryption** Identify the SSID that the 802.1x user will use and set the opmode to dynamic WEP or dynamic TKIP. (*Refer to "Deploying Access Points" on page 1*).
- 2 Navigate to the Configuration > Security > Authentication Methods > 802.1x Authentication page.
- 3 Configure 802.1x for wireless user authentication.

Monitoring Configuration	Diagnostics Maintenance Plan Events	Reports Save Configuration Logout
Switch General Management	Security > Authentication Met Authentication	hods > 802.1 x
WLAN Network Radio	802.1x VPN Captive Portal MAC L2 Encryption Advanced	Address Stateful 802.1x SSID
Advanced RE Management		
Calibration		E
Optimization		<u> </u>
Protection	Enable Reauthentication	
Monitoring	Enable Opportunistic Key Caching (WPA2)	
Advanced	Enforce Machine Authentication	
Boles	Enable Wired Clients	
Policies	Machine Authentication Default Role	guest 🗸
AAA Servers	User Authentication Default Role	auest 🗸
Authentication Methods	Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)
VPN Settings	Advanced Configuration	Consumer and a state of the sta
Firewall Settings	Auvanceu configuration	<u>2004</u>
Secure Access		
Secure Service Interfaces	Authentication Servers	
Advanced	Name Type IP Address Authentication P	ort Status Actions
WLAN Intrusion Protection	Add	Apply
Depial of Service		
Man-In-the-Middle		
Signatures	Commands	<u>View Commands</u>
Policies		

The following fields need to be modified for wireless user authentication:



Parameters	Description	Type of Value	Operation
Default Role	Enter the default role to be assigned to the user when the user signs in using 802.1x authentication. The default value is guest. If derivation rules are present, the roles assigned to the user through these rules will take precedence over the default role. Default role: guest .	Pull down menu of roles configured	Select the role from the menu that will be the 802.1x default role

Enable Authentication	To select 802.1x as an authentication method this field needs to be checked. Default: Unchecked	Checkbox	Select this box
Enable Re-authenticat ion	When set this will force the client to do a 802.1x re-authentication after the expiry of the default timer for re-authentication. The default value of the timer is 24 hours. If the user fails to re-authenticate will valid credentials, the state of the user is cleared. If derivation rules are used to classify dot1x users then the Re-authentication timer per role will over-ride this setting.	Checkbox	Select this box only if re-authentication needs to be enabled. The re-authentication timer can also be modified if required as explained in Advanced Configuration options of 802.1x.
	Default: Unchecked		
Authentication Failure Threshold for Station	This is a security feature. This specifies the number of times a user can try to login	Integer	Set value to 0 to disable blacklisting.
Blacklisting	with wrong credentials after which the user will be blacklisted as a security threat. Default: 3		Set to a non zero integer value to blacklist after the specified number of failures.

Configuring the Authentication Servers

The Authentication server to which the switch will send authentication requests needs to be configured in addition to the 802.1x settings.

1. Click **Add** under the **Authentication Server** to add a radius server to the 801.x setting.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch	Security > Authentication Methods > 802.1x Authentication
General	
WLAN	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID
Network	L2 Encryption Advanced
Radio	Choose a role from the pull down menu, the roles
Advanced	Derault Role guest Should be created prior to setting up 602. Ix
RF Management	Enable Authentication
Optimization	Enable Reauthentication
Protection	Enable Opportunistic Key Caching (WPA2)
Monitoring	Enforce Machine Authentication
Advanced	Enable Wired Clients
Security	Machine Authentication Default Role
Policies	
AAA Servers	
Authentication Methods	
VPN Settings	Advanced Configuration Choose a server from previously
Firewall Settings	Created Authentication Servers
Secure Access	Authentication Servers
Secure Service Interfaces	Name Type IP Address Authentication Port Status Actions
Advanced	
WLAN Intrusion Protection	Choose an Authentication Server
Rogue AP	Radius Server(Server Type:Radius IP Address:10.1.15.1) VAdd Cancel
Denial of Service	Radius Server/Server Type:Radius IP Address:10.1.15.1)
Man-In-che-midule	
After adding the A	Authentication Servers
Servers they wil	be Name Type IP Address Authentication Port Status Actions
listed as show	n in Radius Server Radius 10.1.15.1 1812 Enabled Delete 🔺 🔻
priority order,	use Radius Server 2 Radius 10.14.1.9 1812 Enabled Delete 🛦 🔻
the arrow button	s to
adjust prio	

- 2 From the pull down menu under **Choose an Authentication Server**, select the RADIUS server that will be the primary authentication server. Click **Add** after making the choice.
- 3 To add multiple auth servers repeat steps above for each server.

Monitoring Configuration	Diagnostics N	/laintenar	nce Plar	n Events	Report	s	Save Co Logout	nfiguration
Switch General Management	Security > 802.1x Aut	Auth	entication	tion Metl	nods >	>		
WLAN Network Radio	802.1x \ SSID L2	/PN Encrypt	Captive Po ion Ad	rtal MAC vanced	Address	State	eful 802.1>	(
Advanced RF Management Calibration	Default Role gu	est	*					
Optimization Protection	Enable Authentica Enable Reauthent	ition ication						
Monitoring Advanced	Enable Opportunis Enforce Machine A	stic Key Ca Authentica	aching (WPA2 Ition	2)				
Roles Policies	Enable Wired Clier Machine Authentic	nts :ation Def	ault Role		D guest	*		
AAA Servers Authentication Methods	User Authentication	on Default ilure Thres	Role shold for Stat	ion Blacklisting	guest	V disables b	olacklisting)	
Firewall Settings Secure Access	Advanced Cont	figuratio	on					<u>Show</u>
Secure Service Interfaces	Authentication	n Server	'S					
Advanced	Name 1	Type I	P Address	Authentical	ion Port	Status	Actio	ns
Rogue AP	Radius Server Ra	10 IUS 10	.1.15.1	1012		Enabled	Delete	
Denial of Service	Radius Server 2 Ra	adius IU	.14.1.9	1812		Enabled	Delete	
Man-In-the-Middle	Add Th	e serv	ers will b	e listed in t	he prio	rity orde	er,	Apply
Signatures Policies		use th	e arrow l	eys to adju	ist the j	priority		
	Commands						<u>View C</u>	ommands

- 4 The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the ▲ or ▼ to the right on the entry to move it higher up or lower down in the list.
- 5 Click the **Apply** to apply the changes made. Ensure that the changes made have taken effect on the resultant page.



Example

The following example uses the following settings:

Default role	dot1x_user
Vlan the users are in	100 (configured by role)
Authentication Server	Radius_Server_1 (RADIUS server that supports 802.1x)
SSID	dot1x with dynamic TKIP
Authentication Failure Threshold for Station Blacklisting	3

NOTE—If necessary, create dot1x_user and VLAN 100.

1. Configure the access policies and the VLAN for the 802.1x users.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Edit Role(dot1x_user)
Management WLAN Network Radio	« Back
Advanced RF Management Calibration Optimization Protection Monitoring Advanced Security	Name Rule Count Location allowallnew 1 0.0.0 Edit Delete Image: Create a policy to apply to the 802.1x users Add Create a policy to apply to the 802.1x users Re-authentication Interval Disabled Change (0 disables re-authentication. A positive value enables authentication)
Ades Policies AAA Servers Authentication Methods VPN Settings Firewall Settings Secure Access Secure Service Interfaces Advanced	Role VLAN ID 100 Image Select VLAN 100, create using Switch > VLAN if necessary Bandwidth Contract Not Enforced Image Per User VPN Dialer Not Assigned Image Change

2 Configure the authentication server setting for Radius_server_1.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports		Save Configuration	Logout
Switch General		Security	> AAA Ser	vers	> Radiu	us Serve	ers > Ado	d Radius	
Managemer	nt	Server							
WLAN	k								« Back
Radio	K.	Server Name						Radius_Server_1	
Advanc	ed	IP Address					10.11.1.18		
RF Manager	nent	Shared Secret	Shared Secret					•••••	
Optimiz	ation	Verify Shared	Shared Secret				•••••		
Protect	ion	Authentication	thentication Port				1812		
Monitor	ing	Accounting Po	rt					1813	
Advanc	ed	Num Retries						3	
Roles		Timeout						5	
Policies									
AAA Se	rvers	Match ESSID							
Autheni	tication Methods							Add Del	ete

3 Create the SSID dot1x with dynamic TKIP.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	5 Reports		Save Configuration	Logout
Switch General		WLAN >	Network >	> Add :	SSID)		l	« Back
Managemer	ıt	Add SSID							
WLAN Networl	k	SSID	dot1×						
Radio		Radio Type	802.11 a	/b/g 🔽			C NULL	. О WEP 🖲 ТКІР С	AES-CCM
Advanc	ed	Hide SSID				Encryption	C Mixe	ed TKIP/AES-CCM	_
RF Managen	nent	SSID Default V	1AN 100	100	~	Туре	TKIP		
Calibrat	ion	Ignore Broadc	ast _				O PSK	TKIP 💿 WPA TKIP	
Optimiz	ation	Probe Request							
Protecti	on 	DTIM Period	1						
Monicor	ng -d								
Security	eu								
Roles		Commands						View Commands	
Policies									
AAA Se	rvers					unely.			
Authen	tication Methods				-	4ppiy			

4 Click **Apply** to apply the configuration.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > Authentication Methods > 802.1x Authentication
Management	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption
WLAN	Advanced
Network	
Radio	
Advanced	
RF Management	Enable Authentication
Calibration	Enable Reauthentication
Optimization	Eashle Opportunistic Key Cashing (WDM2)
Protection	Enable Opportunistic Key Cathing (WPA2)
Monitoring	Enforce Machine Authentication
Advanced	Enable Wired Clients
Security	Machine Authentication Default Pole
Roles	
Policies	User Authentication Default Role
AAA Servers	Authentication Failure Threshold for Station Blacklisting 3 (0 disables blacklisting)
Authentication Methods	Advanced Configuration Show
VPN Settings	
Firewall Settings	
Secure Access	Authentication Servers
Secure Service Interfaces	Name Type IP Address Authentication Port Status Actions
Advanced	Radius_Server_1 Radius 10.11.1.18 1812 Enabled Delete 🔺 🔻
WLAN Intrusion Protection	Add
Rogue AP	
Denial of Service	

Configuring User and Machine Authentication

802.1x can be used to perform user and machine authentication. This tightens the authentication process further since both machine and user need to be authenticated.

Enabling machine authentication gives rise to the following scenarios.

Machin e Auth Status	User Auth Status	Description	Role	Typical Access Policy	
Failed	Failed	Both machine authentication and user authentication failed. User remain in the logon role	Logon	No access to network	
Failed	Passed	If the machine authentication fails, due to reasons like information not present on server and user authentication succeeds, the user will get the User Authentication Default Role . The derivation roles if present will not apply.	User Authenticatio n Default Role	Limited access depending on users like guest.	
Passed	Failed	If machine authentication succeeds and user authentication has not been initiated, the role assigned would be the Machine Authentication Default Role. The derivation rules if present will not apply	Machine Authenticatio n Default Role	Access depending on how secure the machine is as far as who access is concerned.	
Passed	Passed	In case both machine and user are successfully authenticated, the resultant role is the 802.1x Default role . In case of derivation rules, the rules assigned to the user via derivation rules will take precedence over the default role. This is the only case where derivation rules would get applied.	Default role or role assigned by derivation rules.	Most secure since both authentication succeeded. Permissions could not depend purely on the user classification like guest, employee, admin etc.	

Before configuring 802.1x on the switch for machine authentication, you need to configure:



- Role There are three different roles when machine authentication is enabled as described above – the User Authentication Default Role, the Machine Authentication Default Role and the Default role. The three can be the same but would be preferable to define the roles as per the polices that need to be enforced as explained above. (*Refer to document on firewall policies to configure roles*)
- Authentication Server The authentication server the switch would use to validate the users. Verify that the authentication server supports 802.1x. Most LDAP servers do not. The Internal Server does not support 802.1x either. (*Refer to document on Configuring AAA servers to configure the authentication server*)
- **AP encryption** Identify the SSID that the 802.1x user will use and set the opmode to dynamic WEP or dynamic TKIP. (*Refer Wireless LAN setting document to configure the AP encryption mode*).

1. Navigate to the **Configuration > Security > Authentication Methods > 802.1x Authentication** page.

2 Configure 802.1x for wireless users and machine authentication.

Monitoring Configuration	Diagnostics Mainte	enance Plar	n Events	Reports	Save	e Configuratio	n Logout
Switch General Management	Security > Au Authenticatio	hods >	802.1	Lx			
WLAN Network Radio	802.1x VPN L2 Encryption	Captive Po Advanced	ntal MAC	CAddress	State	ful 802.1x	SSID
RF Management	Default Role dot1x_u	ser 🔽					
Calibration	Enable Authentication			V	-		
Optimization	Enable Reauthentication	1		V	alle	icking show	v will inced
Protection	Enable Opportunistic Ke	v Caching (WDð:	2)		setti	ngs, not re	quired
Monicoring	Enable Opportunistic Ke	y caching (wrm	-/		1	for typical u	Ise
Security	Enforce Machine Auther	ntication		~			
Roles	Enable Wired Clients						
Policies	Machine Authentication	Default Role		guest	~		
AAA Servers	User Authentication Def	ault Role		guest	~		
Authentication Methods	Authentication Failure T	hreshold for Stal	ion Blacklisting	0 (() disables b	lacklisting)	
VPN Settings	Advanced Configur	ation	-				Show
Firewall Settings	2						
Secure Access	Authentication Con						
Secure Service Interfaces	Name Tune	TD Address	Authoptical	tion Bork	Chabur	Actions	
WI AN Intrusion Protection	Radius Server Radius	10.1.15.1	1812		Fnabled	Delete	T
Rogue AP	Radius Server 2 Dadius	10.14.1.0	1012		Enabled	Delete A	
Denial of Service	Raulus Server 2 Raulus	10.14.1.9	1012		chableu	Delete -	·
Man-In-the-Middle	Add					App	лу
Signatures							
Policies	- I						
	commands					View Comm	iands

The following fields need to be modified for machine and user 802.1x authentication

The machine credentials can be cached and reused between re-auths so the Switch does not have to authenticate every time it reloads. The variable that controls this is the Machine Authentication Cache Timeout.

To set the value of the Machine Authentication Cache Timeout :

- 1. Click Show on the right of the Advanced Configuration section.
- 2 Set the value of the **Machine Authentication Cache Timeout** to the desired value. The default value is 24 hours.

Note—The Advanced Configuration settings should not be modified unless there is a need to customize at a more detailed level.

The Authentication server to which the switch will send authentication requests needs to be configured in addition to the 802.1x settings. To configure the authentication servers:



- 1. Click **Add** under the **Choose an Authentication Server** to add a RAIDIUS server to the 801.x setting.
- 2 From the pull down menu, select the RADIUS server that will be the primary authentication server.
- 3 Click Add after making the choice.
- 4 To add multiple auth servers repeat above steps for each server.

Monitoring Configuration	Diagnostics Mainten	ance Plan Eve	nts Reports		Save Configuration	Logou
Switch General	Security > Aut	hentication M	lethods > 802.1	x Authentication		
Management	802.1x VPN	Captive Portal	MAC Address Statef	ul 802.1x SSID L2 F	Encryption Ad	lvanced
WLAN						
Network	Default Role dot1x_use	*				
Advanced	Enable Authentication		V			
RF Management Calibration	Enable Reauthentication					
Optimization	Enable Opportunistic Key	Caching (WPA2)				
Protection	Enforce Machine Authenti	ation	V			
Monitoring	Enable Wired Clients		Г	And all Another		
Advanced Security	Machine Authentication De	efault Role	guest 🗸	from the p	oull down menu	u and
Roles	User Authentication Defau	ılt Role	guest 🔽	prioritiz	e them as need	bed
Policies	Authentication Failure Thr	eshold for Station Blackli	sting 0 (0 disables bla	acklisting)		
AAA Servers	Advanced Configurat	ion				Shov
Authentication Methods						
VPN Settings						
Firewall Settings	Authentication Serve	ers				
Secure Access	Name	Туре	IP Address	Authentication Port	Status Ad	tions
Secure Service Interfaces	Radius Server	Radius	10.1.15.1	1812	Enabled Delet	ie 🔺 🔻
Advanced	Radius Server 2	Radius	10.14.1.9	1812	Enabled Delet	te 🔺 🔻
WLAN Intrusion Protection						
Depial of Service	Choose an Authenti	cation Server				Apply
Man-In-the-Middle	Radius_Server_1(Server	Type:Radius IP Address:	10.11.1.18) 👽 🛛 Add 🛛 Ca	incel		
Signatures	Radius Server 1(Server	[ype:Radius IP Address:]	0.11.1.18)			
Policies						

- 5 The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the ▲ or ▼ to the right on the entry to move it higher up or lower down in the list.
- 6 Click **Apply** to apply the changes made. Ensure that the changes made have taken effect on the resultant page.

Example

This example uses the following configuration:

Default roledot1x_user

Machine Authentication Default Role dot1x_mc

User Authentication Default Roleguest

Vlan the users are in100 (configured by role)

Authentication Server Radius_Server_1 (RADIUS server that supports 802.1x)

SSID dot1x with dynamic TKIP

Authentication Failure Threshold for Station Blacklisting3

In this example,

- If machine authentication succeeds, the role assigned would be the dot1x_mc role.
- If only user authentication succeeds, the role assigned would be the *guest role* and
- If both machine and user get authenticated the role assigned would be dot1x_user.
- On failure of any type of authentication, the user remains in the logon role.
- 1. Configure the roles used for 802.1x:

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save	e Configura	ition	Logout
Switch General		Security	> User Ro	les						
Managemer	nt	Name	Firewall Pe	olicies	Bandw	idth Contract	A	tions		
WLAN		ap-role	control, ap-acl		Not Enfo	rced	Edit	Delete		
Networ	k	trusted-ap	allowall		Not Enfo	rced	Edit	Delete		
Advanc	ed:	default-vpn-role	e allowall		Not Enfo	rced	Edit	Delete		
RF Manager	nent	guest	internet_access_	only	Not Enfo	rced	Edit	Delete		
Calibrat	tion	stateful-dot1×	Not Configured		Not Enfo	rced	Edit	Delete	-	
Optimiz	ation	ctatoful	control		Not Enfor	read	Edit	Delete		
Protect	ion	staterui	Control		NOCENIO	ceu	Luit	Delete		
Monitor	ring	logon	control,captivepo	rtal,vpnlogo	on Not Enfo	rced	Edit	Delete		
Advanc	:ed	dot1x_mc	access_subnet_A	_only	Not Enfo	rced	Edit	Delete		
Security		dot1x_user	allowall		Not Enfor	rced	Edit	Delete		
Roles		bbA							and the	
Policies										

2 Configure the authentication server setting for Radius_server_1:



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration Logout
Switch General	Security > AAA Servers > Radius Servers > Add	Radius
Management WIAN	Server	
Network		« Back
Radio	Server Name	Radius_Server_1
Advanced	IP Address	10.11.1.18
RF Management	Shared Secret	•••••
Optimization	Verify Shared Secret	•••••
Protection	Authentication Port	1812
Monitoring	Accounting Port	1813
Advanced	Num Retries	3
Security Roles	Timeout	5
Policies		
AAA Servers	Match ESSID	
Authentication Methods		Add Delete

- 3 Enter the values as per the example.
- 4 Click **Apply** for the configuration to take effect.

Monitoring	Configuration	Diagnostics	Maintena	ance Plan	Events	Report	s		Save C	onfiguration	Logout
Switch General		Security	> Auti	henticat	ion Metl	10ds >	> 802.1	x Authe	nticat	ion	
Managemen WLAN Network	t	802.1x Advanced	VPN	Captive Por	tal MAC	Address	Statef	ūl 802.1x	SSID	L2 Encryp	tion
Radio											
Advance	ed	Default Role	dot1x_user	~							
RF Managen	nent	Enable Authent	ication			\checkmark					
Calibrati	ion	Enable Reauthe	entication			V					
Protecti		Enable Opportu	inistic Key C	aching (WPA2)	I.						
Monitori	ng	Enforce Machin	e Authentic	ation							
Advance	ed	Enable Wired C	lients			П					
Security		Machine Author	ptication De	fault Dole		quest	~				
Policies		Machine Mache				guest					
	wers	User Authentic	ation Deraul	IC ROIE		guest	×				
Authent	ication Methods	Authentication	Failure Thre	eshold for Stati	on Blacklisting	3	(0 disables bla	acklisting)			
VPN Set	tings	Advanced Co	onfigurati	ion							<u>Show</u>
Firewall	Settings										
Secure /	Access	Authenticat	ion Serve	ers							
Secure 3	Service Interfaces	Name	Туре	IP Address	Authentica	ation Porl	t Status	Actions	۶.		
Advance	ed	Radius_Server_	1 Radius - 1	10.11.1.18	1812		Enabled	Delete 4	¥ 🔻		
WLAN Intrus Rogue A	ion Protection	Add						Ap	oply		
Denial o	f Service										

Configuring MAC-based Authentication

This section of the document shows how to configure MAC-based authentication on the Alcatel switch using the WebUI.

Use MAC-based authentication to authenticate devices based on their physical MAC address. While not the most secure and scalable method, MAC-based authentication still implicitly provides an addition layer of security authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if users are allowed access to the network via station A, then one method of authenticating station A is MAC-based. Users may be required to authenticate themselves using other methods depending on the network privileges required.

MAC-based authentication can also be used to authenticate WiFi phones as an additional layer of security to avoid other devices from accessing the voice network using what is normally an insecure SSID.

Configuring the Switch

To enable MAC-based authentication on the Alcatel Mobility Controller:

1. Before configuring MAC-based authentication on the switch, you must first configure:

- **The role** that will be assigned as the default role for the MAC-based authenticated users. (*See Chapter xi, Configuring Firewall Roles and Policies. for information on firewall policies to configure roles). If derivation rules exist or if the user configuration in the internal database has a role assignment, these values are prioritized over this value.*
- The Authentication Server that the switch uses to validate the users. The internal database can be used to configure the users for MAC-based authentication. See "Configuring Users" on page 135 for information on configuring the users on the local database. For information on configuring AAA servers, *Refer to* "Authentication Servers" on page 83.
- 2 Select the Configuration tab. Navigate to the Security > Authentication Methods > MAC Authentication page.
 - Check the Authentication Enabled checkbox to enable authentication.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Log
Switch General	Security > Authentication Methods > MAC
Management	Authentication
WLAN Network Radio	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption Advanced SSID
Advanced	
RF Management	Authentication Enabled
Calibration	Default Role guest 🗸
Optimization Protection	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Monitoring	
Advanced	Authentication Servers
Security	Name Type IP Address Authentication Port Status Actions
Delicios	Radius_Server_1 Radius 10.11.1.18 1812 Enabled Delete 🔺 🔻
AAA Servers	Add
Authentication Methods	

- From the pull down list for Default Role select the default role that will be assigned to the MAC-authenticated users.
- Set the Authentication Failure Threshold for station Blacklisting to a non-zero value if you want the station to be blacklisted upon failure to authenticate within the specified number of tries. If not, set the value to 0.

Parameter s	Description	Type of value	Operation
Authentication Enabled	To enable MAC-based authentication this field must be checked. Default : Unchecked	Checkbox	Select this box
Default Role	Enter the role to be assigned to the user when the user is MAC-authenticated. The default value is guest . If derivation rules are present, the roles assigned to the user through these rules will take precedence over the default role. Default role : guest .	Pull down menu of roles configured.	Select the role from the menu that will be the MAC-authenticati on default role.

of failures. This is a security feature.

Authentication Failure Threshold for Station	This specifies the number of times a user can try to login with wrong credentials after	Integer	Set value to 0 to disable blacklisting.
Blacklisting	which the user will be blacklisted as a security threat. Default : 3		Set to a non zero integer value to blacklist after the specified number

- 3 Configure the authentication servers.
 - This is the authentication server to which the switch will send authentication requests. To add an authentication server, click Add under
 Choose an Authentication Server. Select the internal database option to use the local database on the switch for MAC-based authentication.
 - From the pull down menu select the RADIUS server that will be the primary authentication server. Click **Add** after making the choice.
 - To add multiple auth servers repeat these steps for each server.

The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the \blacktriangle or \triangledown arrows to the right of the entry to move it higher up or lower down in the list.

4 Click **Apply** to apply the changes made. Verify that the changes made have taken effect on the resultant page.

Configuring Users

This section explains how to configure users in the local database for MAC-based authentication:

To authenticate users using MAC-authentication by adding a user to the local database:

1. Under the **Configuration** tab, navigate to the **Security > AAA Servers > Internal Database** page.

Under the Users section click Add User. This opens the Add User page.



Monitoring Configuration	Diagnostics Maintenance	Plan Events Report	ts Save Configuration Logout
Switch General	Security > AAA Se	rvers > Internal D	atabase >
Management	Add User		
WLAN			« Back
Network	Lines Name	12. ft. a. 24.09. da	Enter the MAC address for
Radio	User Name	12:01:00:00	Enter the WAC address for
Advanced	Password	•••••	the user name to enable
RF Management	Verify Password	•••••	WAC authentication
Optimization	Role	employee 🛛 🔽	
Protection	E-mail	employee@compa	
Monitoring	Enabled	V	
Advanced	Entry does not expire		
Security	 Entry does not expire 		
Roles	C Set Expiry time (mins)		
Policies	C Set Expiry Date (mm/dd/yyyy) / / Expiry Tim	e(hh:mm)
AAA Servers			Apply
Authentication Methods			

- In the User Name field, enter the MAC-address of the device to be used, (this is the MAC-address of the physical interface that will be used to access the network). The entry should be in xx:xx:xx:xx:xx format. (If you are using an external RADIUS server, the username/password format is: xxxxxxx.)
- Enter the same address in the above mentioned format in the **Password** and **Verify Password** fields.
- If you want to assign a special role to the user that is different from the MAC-based authentication default role, in the **Role** field enter the role for the user.
- Select the **Enabled** checkbox to activate the user.
- Click **Apply** to apply the settings.
- 2 Deleting/ Disabling user from the database
 - To delete a user from the database, navigate to the **Security > AAA Serv**ers > Internal Database page.
 - Click **Delete** to the right of the user you wish delete. The user is deleted.
 - You can also disabled the user such that the entry will exist in the database but will not be used for authentication purposes. This can be achieved by clicking **Disable** on the right of the user entry.

Monitoring Configuration	Diagnostics	Maintenance	Plan I	Events Reports		Save	Configuration	Logout
Switch General Management	Security > General	AAA Sei Radius I	DAP Ir	Internal Databa	ase g			
WLAN	Server Rules							
Network	Rule Action	Attribute	Condition	Matching Value Valu	le Action	User c	an be impo	orted
Radio	Role Assignme	nt Role	value-of		Delete 🔺 🔻	or exp m	orted to re anual entry	auce /
RF Management	Add							8
Calibration	Maintenance	-						
Optimization	Turnet I		S-1-4- All 11	nu Duniu Dutu		l la a di	a antian la	
Protection	Export	nport L	Jelete All Us	ers Repair Data	abase	Use tr disz	ble delete	eys to
Monitoring	Users					m	odify a use	r
Advanced								-
Security	User Name	Password	Role	E-mail	Enabled Expiry	Action		
Roles	Test 1		guest	test1@example.com	Yes	Disable	Delete	Modify
Policies	User1		guest	User1@example.com	Yes	Disable	Delete	Modify
AAA Servers	12:af:ea:34:98:	c ******	employee	employee@company.cor	n Yes	Disable	Delete	Modify
Authentication Methods	Add User		-					
VPN Settings				1 1 1 2 4	.f.a			
Firewall Settings				1 1-3 (11.3			

Configuring 802.1x for Wired Users

The switch can also be configured to support dot1x authentication for wired users in addition to the wireless users. To create this configuration:

1. Configure the 802.1x for user or user and machine authentication as explained in the previous sections.

2 Check the **Enable Wired Clients** check box in addition to the above setting to enable wired 802.1x authentication. The principles of role derivation that apply to the wireless users will also apply to the wired users.



Monitoring Configuration	Diagnostics Maintenance Plan Events	Reports Save Configuration Logout
Switch General Management	Security > Authentication Met Authentication	hods > 802.1 x
WLAN Network Radio	802.1x VPN Captive Portal MAC L2 Encryption Advanced	Address Stateful 802.1x SSID
Advanced RF Management	Default Role quest	
Calibration	Enable Authentication	V
Protection	Enable Reauthentication	
Monitoring	Enable Opportunistic Key Caching (WPA2)	
Advanced	Enforce Machine Authentication	
Roles	Enable Wired Clients	
Policies	Machine Authentication Default Role	stateful-dot1x
AAA Servers	User Authentication Default Role	guest 💌
Authentication Methods	Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)
VPN Settings	Advanced Configuration	Show
Secure Access		
Secure Service Interfaces	Authentication Servers	
Advanced	Name Type IP Address Authentical	tion Port Status Actions
WLAN Intrusion Protection	Radius Server Radius 10.1.15.1 1812	Enabled Delete 🔺 🔻
Depial of Service	Radius Server 2 Radius 10.14.1.9 1812	Enabled Delete 🔺 🔻
Man-In-the-Middle	Add	Apply

3 Continue configuration as explained above.

Modifying the 802.1x Settings

The 802.1x settings can be modified at any time by simply accessing the page, making the required changes and applying these changes. Care should be taken to clear all logged on users and forcing them to re-authenticate.

Remember to apply the changes made by clicking **Apply** for the changes to take effect.

Resetting the 802.1x Settings

The 802.1x setting can be reset to factory defaults as follows:

1. Navigate to the **Configuration > Security > Authentication Methods > 802.1x Authentication** page.

2 Click **Show**_on the right side of **Advanced Configuration**. The advanced configuration menu displays.

Diagnostics Mainter	nance Plan Events	Reports	Save Con	figuration Logout
Security > Aut	thentication Met	nods >	302.1x	
Authentication	1			
802.1xVPNL2 Encryption	Captive Portal MAC Advanced	Address	Stateful 80	2.1x SSID
Default Role guest	~			
Enable Authentication		v	Oliakin	
Enable Reauthentication		V	display t	g snow will he Advanced
Enable Opportunistic Kou	Caching (WD02)		configu	rations, click
	Cauling (WPA2)		hide to	not display
Enforce Machine Authent	ication	~	these	e settings
Enable Wired Clients				
Machine Authentication E	efault Role	stateful-dot1:	× ×	
User Authentication Defa	ult Role	guest	*	
Authentication Failure Th	reshold for Station Blacklisting	0 (0 d	lisables blacklisti	ing)
Advanced Configura	tion			Show
	A designed Day Company attack			
	Advanced Configuration		Hide	
Authentication Serv	Authentication Server Timeout(secs)		30	
Authentication Serv Name Type	Authentication Server Timeout(secs) Client Response Timeout(secs)		30 30	ctions
Authentication Serv Name Type Radius Server Radius	Advanced configuration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs)		Hide 30 30 30	tions te ▲ ▼
Authentication Serv Name Type Radius Server Radius Radius Server 2 Radius	Advanced Computation Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count		Hide 30 30 30 30 30 30 30 30 30 30 30 30 30	ttions te ▲ ▼ te ▲ ▼
Authentication Serv Name Type Radius Server Radius Radius Server 2 Radius	Advanced Comiguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count		Hide 30 30 30 30 2	tions te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Configuration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count		Hide 30 30 30 30 3 1 1 1	ttions te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Corniguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count Reauthentication Time Interval(secs)		Hide 30 30 30 3 2 1 86400 -	te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Configuration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count Reauthentication Time Interval(secs) Enable Multicast Key Rotation		Hide 30 30 30 30 3 2 1 86400	ttions te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Corniguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Resultentication Time Interval(secs) Enable Multicast Key Rotation Multicast Key Rotation Time Interval(secs)	Hide 30 30 30 30 3 2 1 866400 1 1 1000 1	te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Corniguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count Reauthentication Time Interval(secs) Enable Multicast Key Rotation Multicast Key Rotation Multicast Key Rotation Enable Unicast Key Rotation	secs)	Hide 30 30 30 30 3 2 1 5 66400 1 1 800 5 900	tions te ▲ ▼ te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Corriguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count Reauthentication Time Interval(secs) Enable Multicast Key Rotation Multicast Key Rotation Multicast Key Rotation Multicast Key Rotation Unicast Key Rotation Time Interval(secs) Enable Unicast Key Rotation Unicast Key Rotation Time Interval(secs)	secs) tory Defaulte	Hide 30 30 30 30 30 30 30 30 30 30	te ▲ ▼ Apply
Authentication Server Name Type Radius Server Radius Radius Server 2 Radius Add Add	Advanced Computation Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Key Retry Count Reauthentication Time Interval(secs) Enable Multicast Key Rotation Multicast Key Rotation Time Interval(Enable Unicast Key Rotation Unicast Key Rotation Time Interval(secs) Reset 802.1sr Parameters to Fail	secs) scs) ctory Defaults	Hide 30 30 30 30 3 2 1 86400	te ▲ ▼ Apply
Authentication Serv Name Type Radius Server 2 Radius Radius Server 2 Radius Add	Auvanced Comiguration Authentication Server Timeout(secs) Client Response Timeout(secs) Authentication Failure Timeout(secs) Client Retry Count Server Retry Count Resulthentication Time Interval(secs) Enable Multicast Key Rotation Multicast Key Rotation Time Interval(se Result Retry Rotation Time Interval(se Reset 802.11x Parameters to Fai Machine Authentication Cache Timeo WPA Key Retry Count	secs) scs) ctory Defaults ut(Hours)	Hide 30 30 30 30 30 3 2 1 86400 1800 2 4 3	ttions te ▲ ▼ Apply

- 3 Check the Reset 802.1x Parameters to Factory Defaults.
- 4 Click **Apply**. This will reset the settings to factory default.

Advanced Configuration Options of 802.1x

This section talks about the Advanced Configuration on the 802.1x page.

NOTE— The Advanced Configuration settings should not be modified unless there is a need to customize at a more detailed level.

1. Accessing the Advanced options can be done by clicking the *Show* tab on the right of the Advanced Configuration option on the 802.1x configuration page.



Advanced Configuration	Hide
Authentication Server Timeout(secs)	30
Client Response Timeout(secs)	30
Authentication Failure Timeout(secs)	30
Client Retry Count	3
Server Retry Count	2
Key Retry Count	1
Reauthentication Time Interval(secs)	86400
Enable Multicast Key Rotation	
Multicast Key Rotation Time Interval(secs)	1800
Enable Unicast Key Rotation	
Unicast Key Rotation Time Interval(secs)	900
Reset 802.1x Parameters to Factory Defaults	
Machine Authentication Cache Timeout(Hours)	24
WPA Key Retry Count	3
WPA Key Timeout (secs)	1

The various fields, a brief description and the default values in this section is:

Fields	Description
Authentication Server Timeout	Time in seconds. Time after which the authentication server is timed out as the 802.1x server after it fails to respond.
Client Response Timeout	Time in seconds. Time after which the client is timed out as after it fails to respond.
Authentication Failure Timeout	The time is seconds after which is the authentication packet is not received the transaction is marked as failed.
Client Retry Count	This is the number of attempts the switch makes to obtain an authentication from a client.
Server Retry Count	This is the number of attempts the switch makes to obtain an authentication from a server.
Key Retry Count	This is the number of attempts the switch makes to obtain the key.

Reauthentication Time Interval	This is the time period after the elapse of which the re-authentication of supplicants takes place. Unicast keys are updated after each re-authorization.
Enable Multicast Key Rotation	This option enables the rotation of multicast keys. Multicast keys are used to encrypt multicast packets generated for each AP. Multicast keys are associated with each SSID
Multicast Key Rotation Time Interval	The time period between each multicast key rotation.
Enable Unicast Key Rotation	This option enables the rotation of unicast keys.
Unicast Key Rotation Time Interval	The time period between each unicast key rotation
Reset 802.1x Parameter to Factory Defaults	Resets the dot.1x settings to the factory defaults.
Machine Authentication Cache Timeout	Time in hours
WPA Key Retry Count	This is the number of attempts the switch makes to obtain the WPA key.
WPA Key Timeout	Time in seconds. Time after which the authentication server is timed out after WPA key fails to respond.

- 2 To access the **Advanced Configuration** section, click **Show** tab on the right of this option.
- 3 Change the value of the required parameter described above.



OmniAccess RN: User Guide

CHAPTER 12 Configuring Virtual Private Networks

The aim of this document is to help users configure VPN using the web-interface.

The combination of L2TP and IPSec, known as L2TP/IPSec, is a highly secure technology for making remote access virtual private network (VPN) connections across public networks such as the Internet. In case of wireless, VPN can also be used to further secure the wireless data from attackers. The Alcatel Mobility Controllers can be used as a VPN concentrator terminating all VPN connections from wire and wireless users. For Windows, a dialer can be downloaded from the switch to auto configure the tunnel settings on the dialer. This document primarily deals with the configuration of VPN tunnels – L2TP and PPTP.

VPN Configuration

To configure VPN on the switch, the VPN Authentication method needs to be enabled first.

Enabling VPN Authentication

The following pre-requisites must be configured:

- **Role** The role that will be assigned as the default role for the 802.1x users. (*Refer to document on firewall policies to configure roles*).
- Derivation rules if present will take precedence over this setting.
- Authentication Server The authentication server the switch would use to validate the users. (*Refer to document on authentication servers for configuration details*)

To enable VPN authentication:

1. Navigate to the **Configuration > Security > Authentication Methods > VPN Authentication** page.

Monitoring Configuration	Diagnostics Maintenance Plan Event	s Reports Save Configuration Logout						
Switch General	Security > Authentication Methods > VPN							
Management	Authentication							
WLAN Network	802.1x VPN Captive Portal M	AC Address Stateful 802.1x SSID						
Radio	L2 Encryption Advanced							
Advanced								
RF Management	Authentication Enabled							
Calibration	Default Role	default-vpn-role 🗸						
Optimization	Authoptication Enilyza Throshold for Chation Placklistic	2 (O display blacklisting)						
Protection	Addiencication Pallure Threshold for Station blackisti	ig 5 (O disables blacklisting)						
Monitoring								
Advanced	Authentication Servers							
Security	Name Type IP Address Authen	tication Port Status Actions						
Roles	Radius_Server_1 Radius 10.11.1.18 1812	Enabled Delete 🔺 🔻						
Policies	bbA	Apply						
AAA bervers		- 18 B V						
Authentication Methods								

- 2 Select the Authentication Enabled checkbox to enable VPN authentication.
- 3 Choose the default role for the users from the pull down menu for **Default Role**.
- 4 Set **Authentication Failure Threshold for Station Blacklisting** to an integer value. This number indicates the number of contiguous authentication failures before the station is blacklisted.
- 5 Click **Apply** to apply the settings and to avoid loss of work. To save the configuration between reloads, click the *Save* tab on the left hand top corner.

The Authentication server which the switch will use to authenticate the VPN users needs to be configured. To configure the authentication server:

1. Navigate to the **Configuration > Security > Authentication Methods > VPN Authentication** page.

- 2 Click Add under Authentication Server to add a RADIUS server.
- 3 From the pull down menu select the radius server that will be the primary authentication server. Click **Add** after making the choice.
- 4 To add multiple auth servers repeat steps above for each server.

Monitoring Config	uration Diagnostic	s Maintenance	Plan Events	s Reports		Sav	e Configura	tion Logout	
Switch General	Securi	ty > Authen	tication Me	thods > VPI	N Auther	itication			
Management WLAN Network	802.1)	VPN Capt	ive Portal M	AC Address St	tateful 802.1x	SSID L2	Encryption	Advanced	
Radio	Authentica	ition Enabled		V					
Advanced	Default Ro	Default Role default-vpn-role 🗸							
RF Management Calibration	Authentica	ation Failure Threshold I	or Station Blacklistin	g 3 (0 disable	es blacklisting)				
Optimization									
Protection	Authent	ication Servers							
Monitoring		Name	Туре	IP Address	s Aul	thentication Port	Status	Actions	
Advanced	Radius_Ser	ver_1	Radius	10.11.1.18	1812		Enabled	Delete 🔺 🔻	
Security Roles Policies	Choose	an Authentication	i Server tress:10.200.14.211) V Add	Cancel			Apply	
AAA Servers Authentication M VPN Settings	ethods Internal(S Radius Se Radius Se	Internal/Server Type:Local IP Address: 10:200 14:211) Radius Server(Server Type:Radius IP Address:10:1.15:1) Radius Server Zype:Radius IP Address:10:1.14:1.9)							
Firewall Settings	Comman	ds			View Co	mmands			
Secure Access									

- 5 The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the ▲ or ▼ to the right on the entry to move it higher up or lower down in the list.
- 6 Click **Apply** to apply the configuration changes made before navigating to other pages to avoid losing the changes made.
- 7 Click **Save Configuration** to save the configuration between reboots.

Configuring VPN with L2TP IPSec

The following pre-requisites must be configured:

1. The steps in the "Enabling VPN Authentication" must be completed along with the L2TP IPSec configuration to enable VPN.

- 2 Enable VPN Authentication as mentioned in the previous section.
- 3 Navigate to the **Configuration > Security > VPN Settings > IPSEC** page.



Monitoring	Configuration	Diagnostic	s Mainten	ance	Plan Eve	ents	Reports	Save Configur	ation Logout
Switch		Securi	tv > VPN	l Sett	inas > 1	IPSE	С		
General									
WIAN	c	IPSEC	PPTP	Dialer	s Emula	ate VPI	N Servers	Advanced	
Network	<	L2TP and XAUTH Parameters							
Radio		Enable L21	P	\checkmark					
Advance	ed	Authentica	ation Protocols	PAP	🗹 снар 🗖	MSCH	AP 🗖 MSC	HAPv2	
RF Managem	hent	Primary Di	IS Server	10.11.1	.231				
Calibrati	lon	Secondary	DNS Server	11.10.1	.123				
Drotocti	adon	Duine and LU		10.11.1					
Monitori		Primary W	IND Derver	10.11.1					
Advance	ng ed	Secondary	WINS Server	11.10.1	.124				
Security	50	Address	Pools						
Roles		Pool Nan	ne Start Ad	dress	End Addres	s	Actions		
Policies		Contenentin e	10.11.1.1		0.44.4.45		al 5.1.4	-	
AAA Ser	vers	Swimming 10.11.1.1 10.11.1.45 Edit Delete							
Authent	ication Methods	Add							
VPN Set	tings	Source N	AT						
Firewall	Settings	Enable Sou	urce NAT						
Secure 4	Access	NAT Pool		~					
Secure S	Service Interfaces	IKE Aggre	sive Group Nar	ne char	, neme (On	lv neer	led for XAL	ITH)	
Advance WLAN Johnson	ed	ine nggro.			igonio (on	.,			
Roque A	AP	IKE Shar	ed Secrets						
Denial ol	f Service	Subnet	Subnet Mas	k Lengt	h Key	Ac	tions		
Man-In-	the-Middle	10.11.1.1	255.255.0.0		****	Edit	Delete		
Signatur	res	Add							
Policies	Policies								
		Priority	Encryption	Hash	Authentic	ation	Group	Lifetime	Action
		ritority	Cherypelon				aroap	[300 - 86400]	Edit
		Default	3DES	SHA	RSA		GROUP 2	seconds, no volume limit	Delete
		Add						mm.	
		1100							

- 4 To enable L2TP, check Enable L2TP.
- 5 Select the authentication method. Currently supported methods are PAP, CHAP, MSCHAP and MSCHAPv2.
- 6 Configure the Primary, Secondary DNS servers and Primary and Secondary WINS Server that will be pushed to the VPN Client.
- 7 Configure the VPN Address Pool.

This is the pool from which the clients are assigned addresses.
Monitoring Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General	Security	> VPN Set	tings	> IPSE	EC > Ad	1	« Back
Management	Address	2001					
WLAN Network	Pool Name	Swimming					
Radio	Start Address	10.11.1.1					
Advanced	End Address	10.11.1.45					
Calibration			Done				

- 8 Click Add. The Add Address Pool page appears.
- 9 Specify the start address, the end address and the pool name.
- 10 Click **Done** on the completion to apply the configuration.

Enabling Src NAT

In case the users need to be nated to access the network the use this option. The pre-requisite for using this option is to have a NAT pool which can be created by navigating to the **Security > Advanced > NAT Pools** page.

IKE Shared Secrets

Set the value of the IKE key. The key can be configured by subnet. This can be done by specifying the subnet and subnet mask. Care should be taken to ensure that this key matches the key on the client.

To make the key a global key:

1. Specify the address as 0.0.0.0 and netmask as 0.0.0.0.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports		Save Configuration	Logout
Switch General		Security	> VPN Set	tings	> IPSE	EC> Add	IKE Sec	ret	« Back
Managemen WLAN	t	Subnet				0.0.0.0		Use 0.0.0.0 to	enable
Network	<	Subnet Mask				0.0.0.0		a global key	
Radio		(Please use th	e defaults 0.0.0.0 f	or the Sub	onet and Sub	net mask if you	i do not intend t	o have multiple pre-sha	red keys)
Advance	ed	IKE Shared Se	cret			•••••	•		
RF Managen Calibrati	nent ion	Verify IKE Sha	red Secret			•••••	•		
Optimiza	ation								Done

- 2 Under IKE Shared Secrets click Add. This will open the Add IKE Secret page.
- 3 Configure the Subnet and Subnet mask. To make the IKE key global specify 0.0.0.0 and 0.0.0.0 for both the values.



- 4 Configure the IKE Shared Secret and Verify IKE Shared Secret.
- 5 Click **Done** to apply the configurations.
- 6 Click **Back** to return to the main VPN L2TP configuration page.

IKE Policies

- 1. Click Add under IKE Policies opens the IPSEC Policy configuration page.
- 2 Set the **Priority** to 1 for this configuration to take priority over the Default setting
- 3 Set the Encryption type to DES or 3DES.
- 4 Set the HASH Algorithm to SHA or MD5.
- 5 Set the Authentication to Pre-Share or RSA.
- 6 Set the **Diffie Helman Group** to **1** or **2**.
- 7 The configurations from 1 through 5 along with the pre-share key need to be reflected in the VPN client configuration. When using a 3rd party VPN client, set the VPN configuration on clients to match the choices made above. In case the Alcatel dialer is used, these configuration need to be made on the dialer prior to downloading the dialer onto the local client.
- 8 Click **Apply** to activate the changes.
- 9 Click **Back** to return to the main VPN L2TP configuration page.
- 10 Click **Apply** to apply the changes made before navigating to other pages.

Configuring VPN with PPTP Example

The following pre-requisites must be configured:

1. The steps in "Enabling VPN Authentication" must be completed along with the PPTP configuration to use PPTP.

- 2 Enable VPN Authentication as described in the previous section "Enabling VPN Authentication".
- 3 Navigate to the **Configuration > Security > VPN Settings > PPTP** page

Monitoring Configuration	Diagnostics	Mainten	ance	Plan Even	ts Reports	Save Config	uration Log		
Switch General	Security	Security > VPN Settings > PPTP							
Management	IPSEC	PPTP	Diale	rs Emulate	VPN Servers	Advanced			
Network	PPTP Param	neters							
Radio	Enable PPTP		~						
Advanced	PPTP Echo Tim	neout(secs)	60						
RF Management Calibration	Authentication	n Protocols	MS MS	CHAPv2					
Optimization	Primary DNS S	Primary DNS Server		.1.231					
Protection	Secondary DN	Secondary DNS Server		.1.123					
Monitoring	Primary WINS	Server	10.11	.1.232					
Advanced Security	Secondary WI	INS Server	11.10	.1.124					
Roles	Address Po	ols							
Policies AAA Servers	Pool Name	Start Ad	dress	End Address	Actions				
Authentication Methods	Swimming	10.1.1.1		10.1.1.45	Edit Delete				
VPN Settings	Add								
Firewall Settings							Apply		
Secure Access	I								
Secure Service Interfaces	Commands					View	<u>v Commands</u>		

- 4 To enable PPTP, check the *Enable PPTP* radio button.
- 5 Select the authentication method. Currently supported method is MSCHAPv2. Check the radio button to select it.
- 6 Configure the Primary, Secondary DNS servers and Primary and Secondary WINS Server that will be pushed to the VPN Dialer.
- 7 Configure the VPN Address Pool.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General		Security	> VPN Set	tings	> PPT	⊃ > Edit		« Back
Managemeni	t	Address	Pool(Swim	ming)			
Network	;	Pool Name	Swimming					
Radio		Start Address	10.1.1.1					
Advance	ed	End Address	10.1.1.45					
RF Managen Calibrati	on			Done				

This the pool from which the clients are assigned addresses.

- 1. Click Add. The Add Address Pool page displays.
- 2 Specify the start address, the end address and the pool name.



- 3 Click *Done* on the completion to apply the configuration.
- 4 Click **Back** to access the main PPTP config page.
- 5 Click **Apply** to apply the changes made before navigating to other pages.

Configuring Alcatel Dialer Example

1. Navigate to the **Security > VPN Settings > Dialers** page. Click **Add** to add a new dialer or *Edit* tab to edit an existing dialer.

- 2 Configure the dialer
- 3 Enter the **Dialer name** that will be used to identify this setting.
- 4 Configure the dialer to work with PPTP or L2TP by checking the **Enable PPTP** or the **Enable L2TP** checkbox.

Monitoring	Configuration	Diagnostics Maintenance F	lan Events Reports Save Configuration Logout					
Switch General Management		Security > VPN Settings > Dialers > Add Dialer						
WLAN Networ	k	Dialer Name	Dialer_1					
Radio		Enable PPTP						
Advanc	ed	Enable I 2TD						
RF Manager	nent	Enable L21P						
Calibrat	ion	Send Direct Network Traffic In Clear (Split Tunneling)						
Optimiz	ation	Disable Wireless Devices When Client	is 🗖					
Protecti	ion	Wired						
Monitor	ing	Enable SecurID New and Next Pin Mode						
Advanc Security Roles	ed	Authentication						
Policies		IKE Lifetime (secs)	28800					
AAA Se	rvers	IKE Encryption	In Book C DES					
Authen	tication Methods	IKE Diffie Hellman Group	© 2 C 1					
VPN Set	ttings	IKE Hash Algorithm	© SHA ⊂ MDS					
Firewall	Settings	IKE Authentication	C RSA Signatures Preshared Key Password					
Secure	Service Interfaces	IPSEC Lifetime (secs)						
A duran	- 4	In SEC Enrolante (Secs)	7200					
Advanc	eu	IPSEC Mode Group						
Rogue /	AP	IPSEC Encryption						
Denial c	of Service	IPSEC Hash Algorithm						
Man-In-	-the-Middle		Apply					
Signatu	res							

5 Select the *authentication* protocol. This should match the L2TP protocol list selected if **Enable L2TP** is checked or the PPTP list configured if **Enable PPTP** is checked.

For L2TP :

- 1. Set the type of **IKE Hash Algorithm**, SHA or MD5 in the IKE Policies page.
- 2 In case Pre-shared was selected as the IKE *Authentication* in the IKE Policies page (*as described in the L2TP IPSec configuration*), key in the pre-share key used in the L2TP configuration. **NOTE: The two keys should match.**
- 3 Select the Group configuration as per the IKE Policy configuration setting for **Diffie Helman Group**.
- 4 Select the IPSEC Encryption as per the IKE Policy configuration setting for **Encryption**.
- 5 Select the IPSEC Hash Algorithm as per the **Algorithm** selected on the IKE Policy page of IPSEC.
- 6 Click **Apply** to apply the changes made prior to navigating to another page.
- 7 The VPN dialer can be downloaded using Captive Portal. To enable this, in the role the user gets assigned after captive portal, configure the dialer by the name used to identify the dialer.

Example if my captive portal user gets the *guest* role after logging on through captive portal and my dialer is called *mydialer*, configure mydialer as the dialer to be used in the guest role.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Edit Role(guest)
Management	« Back
WLAN	
Dadia	Firewall Policies
Radio	Name Rule Count Location Action
RE Management	control 7 0.0.0 Edit Delete 🔺 🔻
Calibration	cologout 1 0.0.0 Edit Delete A V
Optimization	
Protection	A00
Monitoring	
Advanced	Re-authentication Interval
Security	Disabled Change (0 disables re-authentication. A positive value enables authentication)
Roles	
Policies	Role VLAN ID
AAA Servers	Not Assigned Not Assigned V Change
Authentication Methods	
VPN Settings	Bandwidth Contract
Firewall Settings	
Secure Access	
Secure Service Interfaces	
Advanced	VPN Dialer
WLAN Intrusion Protection	Not Assigned Dialer_1 Change After a VPN Dialer is created use the
Rogue AP	Not Assigned pull down menu to assign it to a User
Denial or Service	L2TP Pool Dialer_1
Man-In-the-Middle	default-l2tp-pool Not Assigned 🗸 Change
Signatures	
Policies	PPTP Pool
	default-potn-pool Not Assigned V Change
	bb 4 been 1999 and 19

Examples

In this example, the following settings apply.

VPN Settings

Authentication Server	radon
Default VPN role	vpn_user
Authentication method	MSCHAPv2
Primary DNS	10.10.1.1

Secondary DNS	10.10.1.2
Primary WINS	10.1.1.2

L2TP Setting

L2TP Pool	192.168.100.1 - 192.168.100.100
Pre-shared key	test123
Primary DNS	10.10.1.1
Secondary DNS	10.10.1.2
Primary WINS	10.1.1.2
IKE encryption	3DES
IKE Authentication	Pre-shared
IKE Hash	SHA
IKE Group	2

PPTP Setting

PPTP Pool

192.168.200.1 - 192.168.200.100

Configuration

1. Enable VPN Authentication.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > Authentication Methods > VPN
Management	Authentication
WLAN Network Radio	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption Advanced SSID
Advanced	
RF Management	Authentication Enabled
Calibration	Default Role
Optimization	
Protection	Authentication Failure Threshold for Station Blacklisting U (U disables blacklisting)
Monitoring	
Advanced	Authentication Servers
Security	Name Type IP Address Authentication Port Status Actions
Roles	Add
Policies	
AAA Servers	

Configure L2TP IPSec

1. Configure the DNS and WINS server.

Monitoring Configuration	iagnostics Maintenance Plan Events Repo	irts Save Configuration Logout
Switch General	ecurity > VPN Settings > IPSEC	
Management	IPCEC DDTD Dialore Emulate VDN Serv	are Advapced
WLAN	2TD and YAUTH Daramators	Sio Auvanceu
Network		
Radio		
Advanced	Authentication Protocols 🗌 PAP 🗌 CHAP 🗌 MSCHAP 🗹 r	4SCHAPv2
Calibration	Primary DNS Server 10.10.1.1	these four fields to
Optimization	Secondary DNS Server 10.10.1.2	create a new
Protection	Primary WINS Server 10.1.1.2	IPSEC policy
Monitoring	Secondary WINS Server 0.0.0.0	
Advanced	uddrass Dools	
Security	autress Pools	
Roles	Pool Name Start Address End Address Action	15
Policies	ool 192.168.200.1 192.168.200.100 Edit De	lete
Authentication Methods	Add	
VPN Settings		
Firewall Settings		
Secure Access		
Secure Service Interfaces	NAT Pool	
Advanced	IKE Aggressive Group Name changeme (Only needed for)	(AUTH)
WLAN Intrusion Protection	KE Shared Secrets	
Rogue AP Depial of Service	Subnet Subnet Mask Length Key Actions	
Man-In-the-Middle	.0.0.0 0.0.0.0 ******** Edit Delet	e
Signatures	Add	
Policies		
	KE POlicies Priority Ensuration Hash Authoptication Crow	n Lifetime Action
	rnoncy Encryption hash Authentication arou	
	efault 3DES SHA RSA GROU	no volume limit Delete
		Edit
	3DES SHA PRE-SHARE GROUI	2 300 Delete
	Add	

- 2 Configure the L2TP pool.
- 3 Click Add below Address Pools. Once completed, click Done.



Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General Managemen	t	Security Address	> VPN Set Pool	tings	> IPSE	EC > Add	1	« Back
WLAN Network	< Contract of the second se	Pool Name	COC_POOL					
Radio		Start Address	192.168.200.1					
Advance RE Managen	ed	End Address	192.168.200.10	0				
Calibrat	ion			Done				
Optimiza	ation							

4 Configure the IKE shared secret test123

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports		Save Configuration	Logout	
Switch General		Security	> VPN Set	ttings	> IPSE	EC> Add IKE Secret				
Managemen WLAN	t	Subnet				0.0.0.0]		
Network	<	Subnet Mask			0.0.0.0					
Radio		(Please use th	e defaults 0.0.0.0 f	or the Sub	onet and Subr	bnet mask if you do not intend to have multiple pre-shared keys)				
Advanc	ed	IKE Shared Se	cret			•••••]		
RF Managen Calibrat	n ent ion	Verify IKE Sha	red Secret			•••••]		
Optimiza	ation								Done	

5 Configure the IKE policies.

Monitoring	Configuration	Diagnostics I	Maintenance	Plan	Events	Reports	Save Configuration	Logout	
Switch General		Security >	> VPN Set	tings	> IPSE	EC > Ad	d Policy	« Back	
Managemen WIAN	ıt	Priority	1						
Network	k	Encryption	3DES 💊	•					
Radio		Hash Algorithm	Hash Algorithm SHA 💌						
Advance	ed .	Authentication	ation 🛛 PRE-SHARE 💌 💦 Life Tim				Time field can be from		
Calibrati	ion	Diffie Hellman Gro	GROUP 2	*		300 to 86	400 seconds		
Optimization		Life Time(secs)	Time(secs) 300						
Protecti	on		Ap	ply					
Monitori	ina								

6 The final config page should look like the page below. Once this done click **Apply** to apply the configurations.

Monitoring Conf	figuration	Diagnostics	Mainten	ance	Plan Ev	ents	Reports		Save Co	nfiguration	Logout
Switch		Securi	v > VPN	l Sett	inas > l	IPSEC	2				
General											
Management		IPSEC	PPTP	Dialer	s Emula	ate VPN :	Servers	Advanced			
Network		L2TP and	XAUTH Par	ameters	6						
Radio		Enable L2T	Р								
Advanced		Authentica	tion Protocols			MSCHAP	🗹 MSCH	APv2			
RF Management		Primary DN	S Server	10.10.1	1.1						
Optimization		Secondary	DNS Server	10.10.1	L.2						
Protection		Primary WI	NS Server	10.1.1.	2						
Monitoring		Secondary	WINS Server	0.0.0.0							
Advanced		Decondary	WIND DOING	0.0.0.0							_
Security		Address I	Pools								
Roles		Pool Nam	e Start Ad	ldress	End Addres	is A	ctions				
Policies		COC_POOL	192.168.2	00.1	192.168.200.1	LOO Edit	Delete				
AAA Servers	Mahhada	Add				_		-			
VPN Settings	metrious										
Eirewall Setting	15	Source N	41	-							
Secure Access		Enable Sou	rce NAT		1						
Secure Service	Interfaces	NAT Pool		~							
Advanced		IKE Aggres	sive Group Nar	ne char	ngerne (Or	nly needed	d for XAUTH	H)			
WLAN Intrusion Pr	otection	IKE Share	d Secrets								
Rogue AP		Subnet	Subnet Ma	k Lenat	h Kev	Actio	nns				
Denial of Servic	18 141-	Jublict	Jubilet i la	ik Lenge							
Signatures	JOIE	0.0.0.0	0.0.0.0		******	Edit)elete				
Policies		Add									
1 Olicies		IKE Polici	es								
		Priority	Encryption	Hash	Authentio	ation	Group	Lifetir	ne	Act	ion
		2	3DES	MD5	PRE-SHARE	G	ROUP 2 3	800 seconds, no volu	me limit	Edit	Delete
		Default	3DES	SHA	RSA	G	ROUP 2 [300 - 86400] second	s, no volume limit	Edit	Delete
		Add									

7 Configure the dialer by configuring the key to match the IKE shared secret key in "Configure the IKE policies." Click **Apply** when done to apply the changes.



WLAN D Network E Radio	Naler Name	coc_dialer	
Network El Radio El			
Radio E	nable PPTP	Г	
	nable L2TP	v	
RF Management S	end Direct Network Traffic In Clear(Split Tunneling)	E.	
Calibration	isable Wireless Devices When Client is Wired	E Contraction of the second se	
Protection	nable SecurID New and Next Pin Mode	E	
Monitoring A	uthentication	□ PAP □ CHAP □ MSCHAP ▼ MSCHAPv2 □ Cache SecureID Token	
General D	KE Lifetime (secs)	28800	
Security Roles D	KE Encryption	€ 3DES C DES	
Policies D	KE Diffie Hellman Group	€ 2 C 1	
AAA Servers D	KE Hash Algorithm	€ SHA C MDS	
Authentication Methods D	KE Authentication	C RSA Signatures Preshared Key Password	
Global Firewall Settings	PSEC Lifetime (secs)	7200	
Advanced IF	PSEC Mode Group	@ 2 C 1	
WLAN Intrusion Detection	PSEC Encryption	€ ESP-3DES C ESP-DES	
Rogue AP Depial of Service	PSEC Hash Algorithm	€ ESP-SHA-HMAC C ESP-MD5-HMAC	

8 Configure the dialer in the captive portal user role that will be used to download the dialer.

Configuring PPTP

1. Navigate to the PPTP configuration page as explained in the previous sections

Monitoring Configuration	Diagnostics	Maintena	ance	Plan Event:	s Reports	Save Configu	Iration Logo
Switch General	Security	> VPN	Set	tings > PP	PTP		
Management	IPSEC	PPTP	Dialer	rs Emulate	VPN Servers	Advanced	
WLAN Network	PPTP Param	eters					
Radio	Enable PPTP		•				
Advanced	PPTP Echo Tim	eout(secs)	60				
RF Management Calibration	Authentication	n Protocols	MS MS	ichapv2			
Optimization	Primary DNS S	erver	10.1.1	L.2			
Protection	Secondary DN	S Server	10.1.1	L.3			
Monitoring	Primary WINS	Server	10.1.1.3				
Advanced Security	Secondary WI	NS Server	0.0.0				
Roles	Address Po	ols					
Policies AAA Servers	Pool Name	Start Ad	dress	End Address	Actions		
Authentication Methods	PPTP_pool	192.168.20	0.1	192.168.200.100	Edit Delete		
VPN Settings	Add						
Firewall Settings							Apply
Secure Access	On second se					18	
Secure Service Interfaces	commands					Viev	/ Commands

- 2 Configure the DNS and WINS server. Check the Enable PPTP and MSCHAPv2 checkbox.
- 3 Configure the PPTP pool

Monitoring Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General Management	Security Address	> VPN Set Pool	tings	> PPTI	P > Add		« Back
WLAN Network	Pool Name	PPTP_pool					
Radio	Start Address	192.168.200.1					
Advanced	End Address	192.168.200.10)0				
Calibration			Done				

4 Click **Apply** for the configurations to take effect.



Monitoring Configuratio	n Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > VPN Settings > PPTP
Management	IPSEC PPTP Dialers Emulate VPN Servers Advanced
WLAN Network	PPTP Parameters
Radio	Enable PPTP 🗸
Advanced	PPTP Echo Timeout(secs) 60
RF Management Calibration	Authentication Protocols V MSCHAPv2
Optimization	Primary DNS Server 10.1.1.2 and the pool is correct then
Protection	Secondary DNS Server 10.1.1.3 click apply to save settings
Monitoring	Primary WINS Server 10.1.1.3
Advanced Security	Secondary WINS Server 0.0.0.0
Roles	Address Pools
Policies AAA Servers	Pool Name Start Address End Address Actions
Authentication Methods	5 PPTP_pool 192.168.200.1 192.168.200.100 Edit Delete
VPN Settings	Add
Firewall Settings	Apply

5 Configure the dialer. Check the Enable L2TP and MSCHAPv2 checkbox. Ensure that all the Authentication types are unchecked. Apply the changes.

Monitoring Configuration	Diagnostics Maintenance Plar	n Events Reports Save Configuration Logout				
Switch General	Security > VPN Setting	gs > Dialers> Add Dialer «Back				
Management WLAN	Dialer Name	pptp_dialer				
Network	Enable PPTP					
Radio	Enable L2TP					
Advanced RF Management	Send Direct Network Traffic In Clear (Split Tunneling)					
Calibration Optimization	Disable Wireless Devices When Client is Wired					
Protection	Enable SecurID New and Next Pin Mode					
Monitoring Advanced	Authentication	Token				
Security	IKE Lifetime (secs)	28800 Ensure that only the				
Roles Policies	IKE Encryption	G 3DES ○ DES desired Authentication method(s) is checked				
AAA Servers	IKE Diffie Hellman Group	© 2 C 1				
Authentication Methods	IKE Hash Algorithm					
VPN Settings	IKE Authentication	C RSA Signatures • Preshared Key Password				
Firewall Settings	IPSEC Lifetime (sers)	7200				
Secure Access	IDSEC Mode Group	A key is required to create the dialer				
Secure Service Interfaces		0201				
WLAN Intrusion Protection	IPSEC Encryption	ESP-3DES C ESP-DES				
Rogue AP	IPSEC Hash Algorithm					
Denial of Service		Apply				

6 Configure the dialer in the captive portal user role that will be used to download the dialer by navigating to the **Configuration > Security > Authentica-***tion > Methods > Captive Portal Authentication* page.



OmniAccess RN: User Guide

CHAPTER 13 Intrusion Detection

This document outlines the steps needed to configure the various IDS capabilities present in an Alcatel network. Like most other security related configuration on the Alcatel system, the IDS configuration is completely done on the Master switch in the network.

The Alcatel solution offers a variety of IDS/IPS features that can be configured and deployed as required. The following are the important IDS/IPS features provided in the Alcatel solution:

Rogue/Interfering AP Detection

The most important IDS functionality offered in the Alcatel solution is the ability to detect an interfering/rogue AP and classify it as an interfering or a rogue AP. An interfering AP is an Access Point that the Alcatel Access points/Air Monitors detected in the air. A rogue AP is an Access Point that is detected as interfering AND is connected to the network on the wired side. An Access Point that is connected to the network is the one that presents a security threat while an AP that is not part of the network only contributes to the interference in the air. The administrator can enable rogue AP containment. If this feature is enabled, the APs that are detected as rogue

NOTE—Interfering APs are contained by disallowing clients from associating to this AP. Refer to the *"Configuring Rogue AP Detection" on page 166* section for more details on how to configure Rogue AP detection/classification/containment.

Denial of Service Detection

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. 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. The Alcatel Mobility Controller can be configured with the thresholds that indicate a DoS attack and can detect the same. Refer to the *Configuring Denial of Service attack detection* section for more details.

• Fake AP: FakeAP is a tool that was 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. Refer to the *Configuring Denial of Service attack detection* section for more details.

Man-In-The-Middle Detection

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.

- Station disconnection: 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. 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.
- 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.

- 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.
- AP Impersonation: 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.

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. For more details on how to configure and create new signatures refer to the *Configuring Signature detection* section.

Wireless LAN Policies

- Adhoc network detection/containment: 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.
- 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.



- Misconfigured AP detection: 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 Alcatel Mobility Controller cannot configure the 3rd-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 3rd-party AP and changes the configuration, this policy is useful in blocking access to that AP until the configuration can be fixed.
- 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. The Alcatel system will monitor for devices using weak WEP implementations and generate reports for the administrator of which devices require upgrades.
- Multi Tenancy: The Alcatel system 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.
- MAC OUI: The Alcatel system 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.

Configuring Rogue AP Detection

Follow the steps below to configure the Alcatel network to detect insecure APs and classify them as rogue and interfering respectively as defined in the section above.

1. Navigate to the **Configuration > Wireless LAN Intrusion Detection > Rogue AP** page on the WebUI of the Master switch.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General		Intrusio	n Protectio	n > F	logue	AP		
Management WIAN		Disable Users f	rom Connecting to	Rogue Ac	ess Points	V		
Network		Mark All New A	Mark All New Access Points as Valid Access Points					
Radio		Mark Unknown Access Points as Rogue Access Points						
Advanced RE Manageme	nt			CI	ear App	ly		
Calibration								

2 The following table explains the fields for this configuration and what it means to select each of them.

	Field	Description
1.	Disable Users from Connecting to Rogue Access Points	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.
2.	Mark All New Access Points as Valid Access Points	When installing an Alcatel Mobility Controller in an environment with an existing 3 rd -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.



3. Mark Unknown Access Points as Rogue Access Points 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:** 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.

Configuring Denial of Service Attack Detection

Follow the steps below to configure Denial of Service attack detection:

1. Navigate to the **Configuration > Wireless LAN Intrusion Detection > Denial of Service** page on the WebUI. To configure Rate Analysis, select **Rate Analysis**.

Monitoring Configuration	Diagnostics	Maintenance Plar	n Events R	eports	Save Configuration	Logout
Switch General	Intrusion	Prevention >	> Denial of	Service > Rate	Analysis	
Management	Rate Analys	is Fake AP				
Network	Rate Analysis					
Radio	Enable Rate And	maly Checking				
Advanced	Detection Pa	rameters				
RF Management	Frame Type	Channel Threshold	Channel Time	(sec) Channel Quiet Ti	me(sec)	
Calibration	Association	30	3	900		
Optimization	Probe Request	200	3	900		
Protection	Probe Response	200	3	900		
Monitoring	Disassociation	30	3	900		
Advanced	Authentication	30	3	900		
Security	Deauthentication	30	3	900		
Roles			Edit Cancel			
Policies						
AAA Servers	Frame Type	Node Threshold	Node Time(sec)	Node Quiet Time(sec)		
Authentication Methods	Association	30 6	0	900		
VPN Settings	Probe Request	200 1	5	900		
Firewall Settings	Probe Response	150 1	5	900		
Firewaii Sectings	Disassociation	30 6	0	900		
Secure Access	Authentication	30 6	0	900		
Secure Service Interfaces	Deauthentication	20 6	0	900		
Advanced		Edit	Cancel			
WLAN Intrusion Protection						
Rogue AP					Apply	
Denial of Service						

2 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. The following table explains what each field implies. To edit any of the values from the default values for a channel, click the Edit button in the appropriate section (channel/node).

	Field	Description
1.	Channel/Node threshold	Specifies the number of a specific type of frame that must be exceeded within a specific interval to trigger an alarm.
2.	Channel/Node time	Specifies the time interval in which the threshold must be exceeded in order to trigger an alarm.



3. 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 log file.

To configure the Fake AP detection, select the Fake AP tab on the **Configuration** > Wireless LAN Intrusion Detection > Denial of Service page.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports		Save Configuration	Logout
Switch General		Intrusio	n Preventi	on >	Denial	of Servi	ice >	Fake AP	
Management WLAN Network Badin		Rate Anal	ysis 🛛 Fake Al	2					
		Fake AP							
		Enable Fake Al	P Flood Detection						
Advanc	ed	Flood Inc Time	(secs)	3					
RF Management Calibration		Flood Threshol	d	50					
		Quiet Time (se	cs)	900					
Protecti	ion	Apply							
Monitor	ing	Commands						View Commands	
Aduppe	od	communicas						Mow Commands	

The table below summarizes the meaning of each of the fields in this section.

	Field	Description
1.	Enable Fake AP Flood Detection	Enables or disables the feature
2.	Flood Inc Time (secs)	The time period in which a configured number of FakeAP beacons must be received.
3.	Flood Threshold	The number of FakeAP beacons that must be received within the Flood Inc Time in order to trigger an alarm.
4.	Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

Configuring Man-In-The-Middle Attack Detection

Navigate to the Configuration > Wireless LAN Intrusion Detection >

Man-In-The-Middle page on the WebUI of the Master switch. Select the required tab to configure each of the following:

1. To configure station disconnection detection, click **Disconnect Station**.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	$\label{eq:intrusion} Intrusion\ {\sf Prevention} > {\sf Man-In-the-Middle} > {\sf Disconnect\ Station}$
Management	Disconnect Station EAP HandShake Sequence Number AP Impersonation
Network	Disconnect Station Analysis
Radio	Enable Disconnect Station Analysis
Advanced	Disconnect Station Detection Quiet Time (secs) 900
RF Management Calibration	Apply
Optimization	Commands View Commands
Protection	

The following table gives a brief description of the fields in this section.

	Field	Description
1.	Enable Disconnect Station Analysis	Enables/disables this feature.
2.	Disconnect Station Detection Quiet Time (secs)	After a station disconnection is detected, the amount of time that must pass before another identical alarm can be generated.

1. To configure EAP Handshake analysis, click the EAP Handshake.





The following table describes each of the fields in this section.

	Field	Description
1.	Enable EAP Handshake Analysis	Enables or disables this feature.
2.	EAP Handshake Threshold	The number of EAP handshakes that must be received within the EAP Time Interval in order to trigger an alarm.
3.	EAP Time Interval (secs)	The time period in which a configured number of EAP handshakes must be received.
4.	EAP Rate Detection Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered

1. To configure Sequence number analysis, click the **Sequence Number**.

Monitoring	Configuration	Diagnostics	Maintenance	Plan Ev	vents F	Reports		Save Configuration	Logout
Switch General		Intrusio	n Preventi	on > Ma	n-In-t	the-Middle	Sequence	Number	
Managemen	t	Disconnec	t Station EA	P HandShak	e Sec	quence Number	AP Impersonation	1	
WLAN Network		Sequence N	umber Analysis						
Radio		Enable Sequence Number Discrepancy Checking							
Advanced		Sequence Number Difference Threshold			100]			
RF Management Calibration Ontimization		Sequence Number Checking Time Tolerance (msec)			c) 500	500			
		Sequence Num	ber Checking Quiel	Time (secs)	900]			
Protecti	n	Apply							
Monitori	ng	Commande					View Commands		
Advanced		Commanus					view Commands		

The following table gives a brief description of the fields in this section.

	Field	Description
1.	Enable Sequence Number Discrepancy Checking	Enables or disables this feature.
2.	Sequence Number Difference Threshold	The maximum allowable tolerance between sequence numbers within a specific time interval.
3.	Sequence Number Checking Time Tolerance (msec)	The time interval in which sequence numbers must exceed the sequence number difference threshold in order for an alarm to be triggered.

4. Sequence Number Checking Quiet Time (secs) After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

1. To configure AP impersonation detection, click the **AP Impersonation**.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Intrusion Prevention > Man-In-the-Middle > AP Impersonation
Management	Disconnect Station EAP HandShake Sequence Number AP Impersonation
WLAN Network	Enable AP Impersonation Detection
Radio	Enable AP Impersonation Protection
Advanced	Beacon Rate Increment Threshold 50
RF Management Calibration	Apply
Optimization	Commands View Commands
Protection	

The following table gives a brief description of the fields in this section.

	Field	Description
1.	Enable AP Impersonation Detection	Enables detection of AP impersonation.
2.	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.
3.	Beacon Rate Increment Threshold	The percentage increase in beacon rate that will trigger an AP impersonation event.

Configuring Signature Detection

Navigate to the **Configuration > Wireless LAN Intrusion Detection > Signatures** page on the WebUI on the Master switch.



Monitoring Configuratio	<mark>n</mark> Diagnostics Maint	enance Plan Eve	nts Reports	Save Configuration Lo	igout
Switch General	Intrusion Pre	evention > Sign	atures		
Management	Signature Analysis	•			
Network	Enable Signature Analy	ysis 🗌			
Radio	Signature Analysis Qui	et Time (secs) 900			
Advanced	Name	Category Active	Action		
RF Management Calibration	ASLEAP	Pre-Defined Yes	Edit Delete		
Optimization	Null-Probe-Response	Pre-Defined Yes	Edit Delete		
Protection	AirJack	Pre-Defined Yes	Edit Delete		
Monitoring	NetStumbler Generic	Pre-Defined Yes	Edit Delete		
Advanced	NetStumbler Version 3.3	3.0x Pre-Defined Yes	Edit Delete		
Security	Deauth-Broadcast	Pre-Defined Yes	Edit Delete		
Policies	Add				
AAA Servers				Ap	oply
Authentication Methods	; Commands			View Commands	

The table below explains the configuration parameters in this section:

	Field	Description
1.	Enable Signature Analysis	Enables or disables this feature.
2.	Signature Analysis Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.
	The table below summarizes t AOS-W ver. 2.4 or higher.	he pre-defined signatures that are supported by
	Signature	Description
1.	ASLEAP	A tool created for Linux systems that has been used to attack Cisco LEAP authentication protocol.
2.	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.

3.	AirJack	Originally a suite of device drivers for 802.11(a/b/g) raw frame injection and reception. It was intended to be used as a development tool for all 802.11 applications that need to access the raw protocol Alas, one of the tools included allowed users to force off all users on an Access Point.
4.	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.
5.	NetStumbler Version 3.3.0x	Version 3.3.0 of NetStumbler changed the characteristic frame slightly. This signature detects the updated frame.
6.	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.

Adding a New Signature Pattern

To add new signatures in addition to the pre-defined signatures described above, follow the steps below:

1. On the **Configuration > Wireless LAN Intrusion Detection > Signatures** page, click **Add** to start adding a new signature pattern.

Monitoring	Configuration	Diagnostics	Mainte	nance f	Plan	Events	Reports	Save Configuration	Logout
Switch General		Intrusio	n Pre	ventior	1 > A	dd IDS	Signatı	ire	« Back
Managemer WIAN	ıt	Signature Nar	ne						
Networl	k	Signature Mo	ie 🗖						
Radio		Signature F	tules						
Advanc	ed	Attribute	Value	Action					
RF Managen	nent	Add							
Calibrat	ion			Apply					
Optimiz	ation								
Protecti	on	Commands						<u>View Comman</u>	<u>ds</u>
Monitor	ing								



- 2 Enter a name for the newly added signature pattern in the Signature Name field and select the Signature Mode option to enable detection for this signature (leave this field disabled if only creating a signature but enabling detection at this point).
- 3 Click **Add** to add a signature rule.

Monitoring Configura	a <mark>tion</mark> Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Intrusion Prevention >Add IDS Signature « Back
Management WLAN	Signature Name Test
Network	Signature Mode 🔽
Radio	Signature Rules
Advanced	Attribute Value Action
RF Management Calibration	Add
Optimization	
Protection	Add Condition
Monitoring	Attribute bssid Value 00:00:00:00:00:0a
Advanced	Add Cabssid
Security	dst-mac
Roles	payload
Policies	Commander View Commander
AAA Servers	wew Commands
Authentication Meth	nods

- 4 In the **Add Condition** section, add a rule that matches an attribute to a value. The attribute can be one of the following:
- BSSID: This refers to the BSSID field in the 802.11 header of frames.
- Destination MAC address: This refers to the Destination MAC address in 802.11 header of frames.
- Frame Type: This refers to the type of 802.11 frame. For each type of frame further details can be specified to filter and detect only the required frames. It can be one of the following:
 - Association
 - Auth
 - Control
 - Data
 - Deauth
 - Deassoc
 - Management
 - Probe-request
 - Probe-response
 - Beacon.

- Payload: This looks for a pattern at a fixed offset in the payload of a 802.11 frame. The administrator can configure the pattern and the offset where the pattern is expected to be found in the frame.
- Sequence Number: This refers to the sequence number of the frame.
- Source MAC address: This refers to the source MAC address of the 802.11 frame.
- 5 After completing configuring the rule to be added, click Add to add the rule to the list of rule. In the example shown, a rule that matches the BSSID to the value 00:00:00:00:00:00 has been added.

Monitoring	Configuration	Diagnostics	Maintenanc	e Plan	Events	Reports	Save Configuration	Logout
Switch General		Intrusio	n Prever	tion >	Add IDS	6 Signatu	re	« Back
Managemer WLAN	it	Signature Nan	e Test					
Networ	k	Signature Mod	e 🗸					
Radio		Signature R	ules					
Advanc	ed	Attribute	Value Acti	on				
RF Manager	nent	Add						
Calibrat	ion		ADD	dv				
Optimiz	ation							
Protect	ion	Add Conditi	on					
Monitor	ing	Attribute bs	sid 🔽 V	alue 00:0	0:00:00:00:	0a		
Advanc	ed		-1					
Security		Add Canc	31					
Roles								
Policies		o						
AAA Se	rvers	commands					View Command	<u>s</u>

6 If required, add another rule to the list of the rules as shown above. When the required number of rules has been added, click Apply to apply the configuration.

NOTE—The configuration will not take effect if it is not applied.



Configuring Wireless LAN Policies

Navigate to the **Configuration > Wireless LAN Intrusion Detection > Policies** page on the WebUI.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Intrusion Prevention > Policies > Adhoc Network
Management	Adhoc Network Wireless Bridge Misconfigured AP Weak WEP Multi Tenancy MAC OUI
WLAN Network	Adhoc Network
Radio	Enable Adhoc Networks Activity Detection
Advanced	Enable Adhoc Network Protection
RF Management Calibration	Adhoc Detection Quiet Time (secs) 900
Optimization	Apply
Protection	
Monitoring	Commands <u>View Commands</u>

Configuring Ad-hoc Network Protection

The table below describes the parameters in this section.

	Field	Description
1.	Enable Adhoc Networks Activity Detection	Enable detection of Ad-hoc networks.
2.	Enable Adhoc Network Protection	When Ad-hoc networks are detected, they will be disabled using a denial of service attack.
3.	Adhoc Detection Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

Configuring Wireless Bridge Detection

To configure detection of wireless bridges, navigate to **Configuration > Wireless** LAN Intrusion Detection > Policies > Wireless Bridge, as shown in the figure below.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Intrusion Prevention > Policies > Wireless Bridge
Management	Adhoc Network Wireless Bridge Misconfigured AP Weak WEP Multi Tenancy MAC OUI
WLAN Network	Wireless Bridge
Radio	Enable Wireless Bridge Detection
Advanced	Wireless Bridge Detection Quiet Time (secs) 900
RF Management Calibration	Apply
Optimization	Commands View Commands
Protection	

The table below describes the fields in this section.

	Field	Description
1.	Enable Wireless Bridge Detection	Enable detection of Ad-hoc networks.
2.	Wireless Bridge Detection Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before

Misconfigured AP Protection: To configure protection of misconfigured APs, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Misconfigured AP**, as shown in the figure below

another identical alarm may be triggered.



Monitoring Configuration	Diagnostics Maintenance Plan Even	ts Reports	Save Configuration	Logout
Switch General	Intrusion Prevention > Polic	ies > Misconfigured AP		
Management	Adhoc Network Wireless Bridge	Misconfigured AP Weak WEP Multi Tenancy	MAC OUI	
Network	Misconfigured Access Points			
Radio	Detect Misconfigured Access Points			
Advanced	Disable Detected Misconfigured Access Points			
RF Management Calibration	Valid Enterprise 802.11b/g Channels	✓ 1 □ 2 □ 3 □ 4 □ 5 ♥ 6 □ 7 □ 8 □ 9 □ 10 ♥ 11		
Optimization	Valid Enterprise 802.11a Channels	▼ 36 ▼ 40 ▼ 44 ▼ 48 ▼ 52 ▼ 56 ▼ 60 ▼ 64 ▼ 149 ▼ 15	53 🔽 157 🔽 161 🔽 165	
Protection	Enforce Short Preamble as invalid AP configuration			
Monitoring	Prevent Clients from roaming to interfering APs			
Advanced Security	Enforce WEP Encryption for all Traffic	<u>v</u>		
Roles	Enforce WPA Encryption for all Traffic			
Policies				
AAA Servers Authorities Methods	Valid Access Point Manufacturers OUI List			
VPN Settings	the format xxxxxxxxxxxx where x			
Firewall Settings	is a nexadecimal number, i being the wildcard)	Add Delete (Adding/Deleting to/from the OUI list will immedia	ately update the switch config	uration)
Secure Access			4	Apply
Secure Service Interfaces				

The table below describes the fields shown in this section.

	Field	Description
1.	Detect Misconfigured Access Points	Enable/disable the misconfigured AP detection feature.
2.	Disable Detected 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.
3.	Valid Enterprise 802.11b/g Channels	Defines the list of valid 802.11b/g channels that 3 rd -party APs are allowed to use.
4.	Valid Enterprise 802.11a Channels	Defines the list of valid 802.11a channels that 3 rd -party APs are allowed to use.
5.	Prevent 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.
6.	Enforce WEP Encryption for all Traffic	Any valid AP not using WEP will be flagged as misconfigured.
7.	Enforce WPA Encryption for all Traffic	Any valid AP not using WPA will be flagged as misconfigured.

 8. Valid Access Point Manufacturers OUI List (OUIs must be entered in the format xx:xx:xx:xx:xx:xx:xx where x is a hexadecimal number, f being the wildcard)
 A list of MAC address OUIs that define valid AP manufacturers. Any valid AP with a differing OUI will be flagged as misconfigured.

Configuring Weak WEP Detection

1. To configure detection of weak WEP implementations, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Weak WEP**, as shown in the figure below.

Monitoring 🛛	Ionfiguration	Diagnostics Mainte	enance Plan Ev	rents Reports		Save Config	guration Logout
Switch General		Intrusion Pre	vention > Pol	icies > Weak	NEP		
Management		Adhoc Network	Wireless Bridge	Misconfigured AP	Weak WEP	Multi Tenancy	MAC OUI
WLAN Network		Weak WEP					
Radio		Detect APs and Clients	Using Weak WEP IV				
Advanced					A	pply	
RF Managemer	nt						
Calibration		Commands			<u>View Comma</u>	ands	
Optimizatio	In						

2 Select the option to "Detect APs and Clients Using Weak WEP IV" to enable this feature.

Configuring Multi-Tenancy Detection

To configure multi-tenancy policies, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > Multi Tenancy**, as shown in the figure below.



Monitoring Configuration	Diagnostics Maintenance Plar	n Events Reports	Save Configuration	Logout
Switch General	Intrusion Prevention >	> Policies > Multi Tenancy		
Management	Adhoc Network Wireless Br	idae Misconfigured AP Weak WEP	Multi Tenancy MAC OUI	
WLAN	Multi-Topopsu		,	
Network	multi-renancy			
Radio	Disable Access Points Violating Enterprise SSID List			
Advanced RF Management Calibration Optimization Protection Monitoring	Valid Enterprise SSID List	Add Delete (Adding/Deleting to/from the SSID configuration)) list will immediately update the switch	1
Advanced Security	Disable Access Points Violating Channel Allocation Agreements			
Roles	Reserved Enterprise 802.11b/g Channels	□1□2□3□4□5□6□7□8□9□	10 🗖 11	
Policies AAA Servers	Reserved Enterprise 802.11a Channels	36 - 40 - 44 - 48 - 52 - 56 - 60 - 64	□ 149 □ 153 □ 157 □ 161 □ 1	65

The table below describes the fields in this section.

Field

Description

1.	Disable Access Points 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.
2.	Valid Enterprise SSID List	A list of reserved SSIDs.
3.	Disable Access Points 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.
4.	Reserved Enterprise 802.11b/g Channels	A list of reserved channel numbers for b/g mode.
5.	Reserved Enterprise 802.11a Channels	A list of reserved channel numbers for a mode.

Configuring MAC OUI Checking

To enable MAC OUI checking, navigate to **Configuration > Wireless LAN Intrusion Detection > Policies > MAC OUI**, as shown in the figure below.
Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports			Save Config	guration	Logout
Switch General		Intrusion	Preventi	on > P	olicies	> MAC	OUI				
Management		Adhoc Net	work Wirel	ess Bridge	Miso	onfigured AF	Weak W	VEP	Multi Tenancy	MAC O	UI
WLAN Network		Enable MAC OU	II Check 🛛 🕅								
Radio		MAC OUI Quiet	Time (secs) 900								
Advance RF Managem Calibrati	ed ient	Apply									
Optimiza	tion	Commands					View	/ Comman	<u>nds</u>		

The table below describes the fields in this section.

	Field	Description
1.	Enable MAC OUI Check	Enables or disables the feature.
2.	MAC OUI Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.



OmniAccess RN: User Guide

CHAPTER 14 System and Network Management

This document outlines the steps to configure SNMP and syslog for an Alcatel wireless network.

Configuring SNMP for the Alcatel Mobility Controller

Alcatel Mobility Controllers and APs support versions 1, 2c, and 3 of SNMP for reporting purposes only. In other words, SNMP cannot be used for setting values in an Alcatel system in the current version.

Follow the steps below to configure a switch's basic SNMP parameters:

1. Configure the host name by navigating to the **Configuration > Management > SNMP** page on the WebUI.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configurat	ion Logout
Switch General	Management > SNMP	
Management	SNMP Access Control Logging	
WLAN	System Group	
Radio		
Advanced	Host Name Aruba2400	
RF Management	System Contact	
Calibration	System Location	
Optimization		
Protection	Add	
Monitoring	Read Community Strings Delete	
Advanced		
Roles	Enable Trap Generation	
Policies	Trap Receivers	
AAA Servers	IP Address SNMP Version Community String UDP Port Action	
Authentication Methods	Add	
VPN Settings		
Firewall Settings	SNMPV3 Users	
Secure Access	User Authentication Protocol Privacy Protocol Action	
Secure Service Interfaces	Add	
Advanced		
WLAN Intrusion Protection	Apply	
Rogue AP		
Denial of Service	Commands View Cor	<u>nmands</u>

	Field	Description	Expected/recommend ed Value
1.	Host Name	Host name of the switch.	String to act as the host name for the switch being configured.
2.	System Contact	Name of the person who acts as the System Contact or administrator for the switch.	System contacts name/ contact information.
3.	System Location	String to describe the location of the switch.	Description of the location of the switch.

4.	Read Community Strings	Community strings used to authenticate requests for SNMP versions before version 3. Note: This is needed only if using SNMP v2c and is not needed if using version 3.	These are the community strings that are allowed to access the SNMP data from the switch.
5.	Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers. Refer to the list of traps in the "SNMP traps" section below for a list of traps that are generated by the Alcatel Mobility Controller.	Select this option and configure the details of the trap receivers to enable generation of traps for various events by the Alcatel Mobility Controller.
6.	Trap receivers	Host information about a trap receiver. This host needs to be running a trap receiver to receive and interpret the traps sent by the Alcatel Mobility Controller	Configure the following for each host/trap receiver: IP address SNMP version: can be 1 or 2c. Community string UDP port on which the trap receiver is listening for traps. The default is the UDP port number 162. This is OPTIONAL, and will

If the administrator is using SNMPv3 for getting the values from the Alcatel Mobility Controller, follow the steps below to configure valid users for SNMPv3:

1. Click Add in the SNMPv3 users section to add a new SNMPv3 user.



use the default port number if not modified by the user.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch	Management > SNMP
General	
Management	SNMP Access Control Logging
Network	System Group
Radio	
Advanced	Host Name
RF Management	System Contact
Calibration	System Location
Optimization	
Protection	Add
Monitoring	Read Community Strings
Advanced	Delete
Security	
Roles	
Policies	Trap Receivers
AAA Servers	IP Address SNMP Version Community String UDP Port Action
Authentication Methods	Add
VPN Settings	
Firewall Settings	SNMPV3 Users
Secure Access	User Authentication Protocol Privacy Protocol Action
Secure Service Interfaces	Add
Advanced	
WLAN Intrusion Protection	User Name
Rogue AP	Authentication
Denial of Service	Protocol SNPV3 support requires
Man-In-the-Middle	Authentication these additional security
Signatures	Privacu Protocol
Policies	SNMPv3 communcations
	Password
	Add Cancel
	Apply

2 Enter the details for the SNMPv3 user as explained in the table below.

Field	Description	Expected/recommend ed Values
User name	A string representing the name of the user.	A string value for the user name.

1.

2.	Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol which is used.	 This can take one of the two values: MD5: HMAC-MD5-96 Digest Authentica- tion Protocol SHA: HMAC-SHA-96 Digest Authentica- tion Protocol
3.	Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol.	String password for MD5/SHA depending on the choice above.
4.	Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used.	This takes the value DES (CBC-DES Symmetric Encryption Protocol).
5.	Privacy protocol password	If messages sent on behalf of this user can be en/decrypted, the (private) privacy key for use with the privacy protocol.	String password for DES.

Configuring SNMP for the Access Points

The Alcatel Access Points also support SNMP and the administrator can configure all or some of the Access Points to access data using SNMP as well as receive traps from the Access Points. The Access Points can be acting as Air Monitors when they are used to access information about the wireless



network using SNMP. The SNMP configuration for the Access Points can be done at a global level (thereby being applicable for all the Alcatel Access Points in the network) as well as for a particular set of Access Point(s) by using the AP location codes. The steps required for each type of configuration is explained below. **Note:** The configuration for Access Points is always done on the Master switch only.

Follow the steps below to configure SNMP parameters for Access Points in the network at a global level:

1. Navigate to the **Configuration > Wireless LAN > Network > General** page on the WebUI of the Master switch. This page includes fields for configuring the SNMP parameters on all Access Points in the network.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	WLAN > Network > General
Management	SSID General
WLAN Network	LMS IP Backup LMS IP
Radio	Tunnel MTU If no value is specified, the MTU will be negotiated
RF Management	Power Management 🔽 Double Encrypt (IPSEC AP)
Optimization	Radio Off Threshold 3 Bootstrap Threshold 7
Protection	RF Band g 💌
Monitoring Advanced	Disable Radio For Time Range
Security Poles	Restore configuration to factory default
Policies	AP Debugging and Logging
AAA Servers	Dump Server
VPN Settings	AP Module Logging Level
Firewall Settings	SAP Informational
Secure Access	AM Warnings V
Secure Service Interfaces	SNMP Informational 💙
Advanced WLAN Intrusion Protection	SNMP System Information
Rogue AP	Host Name
Denial of Service	System Location
Man-In-the-Middle	System Contact
Policies	Enable SNMP Traps 🛛 🗖
	Communities Add Delete
	Trap Receivers
	Server IP Version Community Strings UDP Port Actions
	SNMDV3 Heare
	User Name Authentication Protocol Privacy Protocol Actions
	Add
	Commands View Commands
	Apply Clear

2 Configure the basic SNMP parameters in the section "SNMP System Information". The fields are similar to the ones explained for the switch and are explained in the table below.



	Field	Description	Expected/recommended Values
1.	Host Name	Host name for all Access Points in the network.	Any name to identify the devices as Alcatel APs.
2.	System Location	Location for Access Points in the network	String to identify the location of the APs.
3.	System Contact	Contact name or information for administrative contact.	String to identify administrative contact for all APs.
4.	Enable SNMP Traps	Enables generation of SNMP traps from all Access Points. Refer to the list of traps in "SNMP traps" section for a complete list of traps that may be generated by Alcatel Access Points in the network.	Select this option to enable generation of traps. Note: Ensure that at least one trap receiver is configured to complete the traps configuration.
5.	Communities	Community strings used to authenticate requests for SNMP versions before version 3. Note: This is needed only if using SNMP v2c and is not needed if using version 3.	These are the community strings that are allowed to access the SNMP data from the APs.
6.	Trap receivers	Host information about a trap receiver. This host needs to be running a trap receiver to receive and interpret the traps sent by the Alcatel Access Points	 Configure the following for each host/trap receiver: IP address SNMP version: can be 1 or 2c. Community string
			UDP port on which the trap receiver is listening for traps. The default is the UDP port number 162. This is OPTIONAL, and will use

3 If the administrator is using SNMPv3 for getting the values from the Alcatel Mobility Controller, follow the steps below to configure valid users for SNMPv3.

the default port number if not modified by the user.

	Field	Description	Expected/recommend ed Values
1.	User name	A string representing the name of the user.	A string value for the user name.
2.	Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol which is used.	 This can take one of the two values: MD5: HMAC-MD5-96 Digest Authentication Protocol. SHA: HMAC-SHA-96 Digest Authentication Protocol.
3.	Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol.	String password for MD5/SHA depending on the choice above.
4.	Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used.	This takes the value DES (CBC-DES Symmetric Encryption Protocol).
5.	Privacy protocol password	If messages sent on behalf of this user can be en/decrypted, the (private) privacy key for use with the privacy protocol.	String password for DES.



All the above parameters can also be configured for a subset of all the Access Points in the Alcatel network by using the location code of the Access Points in the *building.floor.location* format. The administrator can use 0 as the wild card value for any of the fields in this format. As an example, all APs in building 10 can be represented by the location code *10.0.0*. To configure the SNMP parameters for a set of APs, follow these steps:

1. Navigate to **Configuration > Wireless LAN > Advanced** page on the WebUI of the Master switch

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logou
Switch General		WLAN >	Advance	d				
Managemen	t	Location	Default ESSID	802.11 a C	hannel	802.11 b/g Channe	el Actions	
WLAN		1.2.4	а-ар	52	1	L	Edit Delete	
Network Radio	ς			1	1-1 of 1	L		
Advance RF Managen Calibrati	ed nent	Add						

2 If the required set does not exist, click **Add** to add the set of APs represented by a location code (using 0 as the wild card value when required as explained above). If the set already exists, click **Edit** for the chosen set and proceed to step 4 to configure the SNMP parameters for the chosen set.

Monitoring Co	onfiguration	Diagnostics	Maintenance	Plan Events	Reports Sa	ve Configuration	Logout
Switch General		WLAN >	> Advance	d			
Management		Location	Default ESSID	802.11 a Channel	802.11 b/g Channel	Actions	
WLAN		1.2.4	а-ар	52	1	Edit Delete	
Network				1 1-1 0	f1		
Radio							
Advanced		Add New L	ocation				
RF Management Calibration	t	Location	3.6.5	Ex: 1.3	2.3 (Bldg.Floor.Plan where	Bldg=1, Floor=2, Pl	an=3)
Optimization		Add Can	ncel				

3 Click **Add** to complete adding the location.

Monitoring	Configuration	Diagnostics	Maintenance	e Plan Eve	nts Reports	Save Config	guration	Log
Switch General		WLAN >	Advance	ad > SSID	(3.6.5)		*	Ba
Managemer WLAN Networl	nt k	SSID	802.11b/g	802.11a (General			
Radio		SSID	Radio Type	SSID Default VLA	N Encryption Type	DTIM Period	Actions	
Advanc	ed	a-ap 8	802.11a/b/g D	efault	No Encryption	1	Edit	
RF Managen Calibrat	n ent tion							
Optimiz	ation	Add						
Protecti	ion							
Monitor	ing							

4 Click the **General** to configure the SNMP parameters for the set of APs.

Monitoring Configuration	Diagnostics Ma	intenance Plan Ev	vents Reports	Save Configuration Logout
Switch	WLAN > Ad	vanced > Gene	ral (1.2.4)	« Back
General				
Management WIAN	SSID 802	.11b/g 802.11a	General	
Network	LMS IP		Backup LMS IP	
Radio	Tunnel MTU		If no value is specified, the MTU will be perotiated	
Advanced RF Management	Power Management	v	Double Encrypt (IPSEC AP)	
Calibration Optimization	Radio Off Threshold	3	Bootstrap Threshold	7
Protection	DE Pand			
Monitoring	Kribandi g 💌			
Advanced	Disable Radio For 1	ïme Range 🛛 💌		
Security Roles	Restore configurat	ion to factory default 🛛 🥅		
Policies	AP Debugging	and Logging		
AAA Servers	Dump Server			
Authentication Methods	AD Madula 1 a			
VPN Settings	SAP MODULE LO	gging Level		
Firewall Settings				
Secure Access	AM W	arnings 💌		
Secure Service Interfaces	SNMP Inf	ormational 💌		
Advanced WLAN Intrusion Protection	SNMP System I	nformation		
Rogue AP	Host Name			
Denial of Service	System Location			
Man-In-the-Middle	System Contact		7	
Signatures	Epable SMMP Trans			
Policies	Communities	Add Delete		

- 5 Refer to the tables above for the fields to be configured for the set of APs.
- 6 Click **Apply** to apply the configuration.



SNMP Traps from the Switch

The following is a list of key traps generated by the Alcatel Mobility Controller.¹

1. Switch IP changed.

Description: This indicates the switch IP has been changed. The Switch IP is either the Loopback IP address or the IP address of the VLAN 1 interface (if no loopback IP address is configured).

Priority Level: Critical

2 Switch role changed

Description: This indicates that the switch has transitioned from being a Master switch to a Local switch or vice versa.

Priority Level: Critical

3 User entry created/deleted/authenticated/de-authenticated/authentication failed.

Description: Each of these traps are triggered by an event related to a user event. The event can be a new user entry being created in the user table, deletion of a user entry, a user getting authenticated successfully, a user getting de-authenticated, or a failed authentication attempt. Each of these traps will be generated by the switch on which the user event occurs. In other words this is a local event to the switch where the user is visible.

Priority Level: Medium.

4 Authentication server request timed out.

Description: This trap indicates that a request to a authentication server did not receive a response from the server within a specified amount of time and therefore the request timed out. This usually indicates a connectivity problem from the Alcatel Mobility Controller to the authentication server or some other problem related to the authentication server.

Priority Level: High.

5 Authentication server timed out

^{1.} For a complete list of traps, refer to the *Alcatel MIB Reference* (0600059).

Description: This trap indicates that an authentication server has been taken out of service. This is almost always same as AuthServerReqTimedOut except when there is only one authentication server in which case the server will never be taken out of service. In that case the AuthServerReqTimedOut will continue to be raised but not then AuthServerTimedOut.

Priority level: High

6 Authentication server up.

Description: This trap indicates that an authentication server that was previously not responding has started responding to authentication requests. This will be triggered by a user event that causes the switch to send an authentication request to the authentication server.

Priority Level: Low.

7 Authentication user table full.

Description: This trap indicates that the authentication user table has reached its limit with the number of user entries it can hold. This event is local to the switch that generates the traps. The maximum number of user entries that can be present at the same time in the user table is 4096.

Priority Level: Critical.

8 Authentication Bandwidth contracts table full

Description: This trap indicates that the maximum number of configured bandwidth contracts on the switch has been exceeded. The threshold for this is 4096

Priority Level: High

9 Authentication ACL table full.

Description: This trap indicates that the maximum number of ACL entries in the ACL table has been exceeded. The limit for this is 2048 entries on a switch.

Priority Level: High

10 Power supply failure

Description: As the name indicates, this trap indicates the failure of one of the two possible power supplies in the switch.

Priority Level: Critical

11 Fan failure



Description: As the name indicates, this trap indicates a failure of the fan in the switch.

Priority Level: Critical

12 Out of Range Voltage

Description: This trap indicates an out of range voltage being supplied to the switch.

Priority Level: Critical

13 Out of Range temperature.

Description: This trap indicates an out of range operating temperature being supplied to the switch.

Priority Level: Critical

14 Line card inserted/removed.

Description: These traps indicate that a Line Card has been inserted or removed from the switch.

Priority Level: Critical.

15 Supervisor card inserted/removed.

Description: These traps indicate that a Supervisor card has been inserted or removed from the switch

Priority Level: Critical

16 Power supply missing

Description: This trap indicates that one of the power supplies is missing.

Priority Level: Critical.

SNMP traps from Access Point/Air Monitor

The following are the key traps that can be generated by the Access point or an Air Monitor:¹

1. Unsecure AP detected.

^{1.}For a complete list of traps, refer to the *Alcatel MIB Reference* (0600059).

Description: This trap indicates that an Air Monitor has detected and classified an Access Point as unsecure. It will indicate the location of the Air Monitor that has detected the unsecure AP, the channel on which the AP was detected as well as the BSSID and SSID of the detected AP.

Priority Level: Critical.

2 Station impersonation.

Description: This trap indicates an Air Monitor has detected a Station impersonation event. The trap will provide the location of the Air Monitor that has detected the event and the MAC address of the Station.

Priority level: Critical

3 Reserved channel impersonation.

Description: This trap indicates an Access Point is being detected is violating the Reserved Channels. The location of the AP/AM that detects the event is provided in the trap. In addition to this, the BSSID and SSID of the detected AP is also included.

Priority Level: High

4 Valid SSID violation

Description: This indicates a configuration in the configuration of the SSID of the AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap.

Priority Level: High

5 Channel misconfiguration

Description: This trap indicates an error in channel configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap

Priority Level: High

6 OUI misconfiguration.

Description: This trap indicates an error in the OUI configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap

Priority: High

7 SSID misconfiguration.



Description: This trap indicates an error in the SSID configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap

Priority level: High

8 Short Preamble misconfiguration.

Description: This trap indicates an error in the Short Preamble configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap. This check will be done only if the short-preamble option is selected for the AP from the CLI or the WebUI.

Priority level: High

9 AM misconfiguration.

Description: This trap indicates an error in the Short Preamble configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap

Priority Level: High

10 Repeat WEP-IV violation.

Description: This trap indicates that the Air Monitor has detected a valid station or a valid AP sending consecutive frames that has the same IV (Initialization vector). This usually means that entity has a "flawed" WEP implementation and is therefore a potential security risk.

Priority Level: High

11 Weak WEP-IV violation.

Description: This trap indicates that the Air Monitor has detected a valid station or a valid AP sending frames with an IV that is in the range of IV that are known to be cryptographically weak and therefore are a potential security risk.

Priority Level: High.

12 Adhoc networks detected.

Description: This trap indicates that the Air Monitor has detected Adhoc networks.

Priority Level: High.

13 Valid station policy violation.

Description: This trap indicates that a valid Station policy is being violated.

Priority Level: High.

14 AP interference.

Description: This trap indicates that the indicated Air Monitor (identified by the BSSID/ SSID) is detecting AP interference on the indicated channel.

Priority Level: Medium

15 Frame Retry rate exceeded.

Description: This trap refers to the event when the percentage of received and transmitted frames with the retry bit crosses the High watermark. This event can be triggered for an AP, a station or a channel. The two values that should be configured related to this event are Frame Retry Rate – High Watermark and Frame Retry Rate –Low watermark. The High Watermark refers to the percentage threshold which if surpassed triggers the event that causes the trap to be sent. The Low Watermark refers to the percentage threshold such that if the retry rate reaches a value lower than this value the event is reset. What this means is that the trap will be triggered the first time the Frame Retry rate goes under the Low Watermark and then crosses the High Watermark again. This holds true for all the thresholds explained below as well.

Priority level: Medium.

16 Frame Bandwidth rate exceeded.

Description: This trap refers to the event of the bandwidth rate for a station exceeding a configured threshold (High watermark). The terms High Watermark and Low Watermark hold the same meaning as explained above.

Priority Level: Medium

17 Frame low speed rate exceeded.

Description: This trap refers to the event when the percentage of received and transmitted frames at low speed (less that 5.5Mbps for 802.11b and less that 24 Mbps for 802.11a) exceeds the configured High Watermark. The terms High Watermark and Low Watermark hold the same meaning as explained above.

Priority level: Medium



Configuring Logging

This section outlines the steps required to configure logging on an Alcatel Mobility Controller. The logging level can be set for each of the modules in the software system. The table below summarizes these modules:

	Module	Description
1.	Management AAA	The module responsible for authentication of management users (telnet/ssh/WebUI).
2.	Authentication	The module responsible for authentication of wireless clients.
3.	Configuration Manager	The module responsible for configuration changes in the Alcatel network and configuration synchronization amongst all Alcatel Mobility Controllers.
4.	VPN server	The module responsible for all VPN connections.
5.	DHCP server	The in-switch DHCP server.
6.	Switching	The module responsible for all layer 2/3 switching functionality.
7.	Mobility	The module responsible for inter- and intra-switch mobility for wireless clients.
8.	User	The module responsible for user state maintenance.
9.	Access Point Manager	The module responsible for managing the Access Points in the network.
10.	Station Manager	The module responsible for all wireless stations at a 802.11 level.
11.	Traffic	A logical module to track traffic patterns to help troubleshooting.
12.	RF Director	The monitor responsible for monitoring the wireless network for any rogues/intrusions etc.

The administrator can configure the logging levels for each of these modules as well as the IP address of a syslog server that the switch can direct these logs to. Follow the steps below to configure the same:;

1. Navigate to the Configuration > Management > Logging page on the WebUI

Monitoring Configuration	Diagnostic	s Maintenance	Plan Ever	its Reports	Save Configuration	Logout
Switch General	Manag	ement > Lo	gging			
Management	SNMP	Access Contro				
WLAN	Logging	Servers	or Logging			
Network	No Comp	n Addresse d				
Radio	No Serve	r Addresses y				
Advanced	Add					
RF Management	Logging	Levels				
Calibration		Module	Logging Level			
Protection	🗖 Man	agement AAA	informational			
Monitoring	Auth	hentication	informational			
Advanced	Con	figuration Manager	informational			
Security			in formation of			
Roles		berver	Informational			
Policies	DHC	P Server	informational			
AAA Servers	🔲 Swit	ching	informational			
Authentication Methods	🗖 Mob	ility	informational			
Firewall Settings	Acce	ess Point Manager	informational			
Secure Access	🗌 Stat	ion Manager	warnings			
Secure Service Interfaces	🗖 Traf	fic	informational			
Advanced WLAN Intrusion Protection	E RF 0	Director	informational			
Rogue AP	🗖 Secu	ure Service Interface	informational			
Denial of Service	- Man	agement SNMP	informational			
Man-In-the-Middle	L Man	agomone prani	an ormacion dr			
Signatures	Apply					
Policies	Comman	ds			View Commands	

- 2 To add a logging server, click **Add** in the Logging Server section.
- 3 Click **Add** to add the logging server to the list of logging servers. Ensure that the syslog server is enabled and configured on this host.
- 4 If the logging levels of all the modules are as required, proceed to step 6. To modify the logging level of any of the modules, select the required module from the list of the modules shown. From the drop down list that appears on the screen, choose the appropriate logging level. In the example shown below, the logging level of the Authentication and VPN server module is being modified to debugging.



Monitoring Configuration	Diagnostics Maintenance	e Plan Events Reports	Save Configuration Logout
Switch	Management >L	oaaina	
General			
Management	SNMP Access Cont	trol Logging	
WLAN	Logging Servers		
Network	10.4.1.11	Delete	
Radio	10.41.11		
Advanced	Add		
RF Management	Logging Levels		
Calibration	Module	Logging Level	
Optimization	Management 0.0.0	informational	
Protection			
Monitoring	 Authentication 	informational	
Advanced Security	Configuration Manager	informational	
Roles	VPN Server	informational	
Policies	DHCP Server	informational	
AAA Servers	Switching	informational	
Authentication Methods			
VPN Settings		Informational	
Firewall Settings	Access Point Manager	informational	
Secure Access	Station Manager	warnings	
Secure Service Interfaces	Traffic	informational	
Advanced	D DE Director	informational	
WLAN Intrusion Protection			
Rogue AP	Secure Service Interfac	e informational	
Denial or Service	Management SNMP	informational	
Man-In-the-Middle			
Signatures	Logging Level Informational	V Done Cancel	
Policies	Informational		
	Apply Debugging		
	Commands Warnings		View Commands
	Alerts		
	Errors		
	Critical	003-2004 Aruba Wireless Networks, I	nc., All Rights Reserved. Email Support

5 Click **Done** to make the modification.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save	e Configuration Logout
Switch	Management >Logging	
Management		
WLAN	SNMP Access Control Logging	
Network	Logging Servers	
Radio	10.4.1.11 Delete	
Advanced	Add	
RF Management	Logging Levels	
Calibration	Module Logging Level	
Optimization Protection	Management AAA informational	
Monitorina	Authentication informational	
Advanced		
Security		
Roles	J VPN Server informational	
Policies	DHCP Server informational	
AAA Servers	Switching informational	
Authentication Methods	Mobility informational	
Firewall Settings	Access Point Manager informational	
Secure Access	Station Manager warnings	
Secure Service Interfaces	Traffic informational	
Advanced	BE Director informational	
Roque AP		
Denial of Service		
Man-In-the-Middle	in ornacional	
Signatures	Apply Confirmation that logging	
Policies	Operation Performed Successfully) configurations are accepted	
	Commands	View Commands
	© Copyright 2003-2004 Aruba Wireless Networks, Inc., All R	lights Reserved. Email Support

6 Click **Apply** to apply the configuration.

NOTE—Until this step is completed, none of the configuration changes will take effect.

For more information on logging, refer to the *Alcatel Mobility Controller Software System Messages*.



OmniAccess RN: User Guide

CHAPTER 15 Configuring Quality of Service for Voice Applications

This document outlines the steps required to configure QoS on an Alcatel Mobility Controller for voice devices, including SIP phones and SVP phones. Since voice applications are more vulnerable to delay and jitter, the network infrastructure should be able to prioritize the voice traffic over the data traffic.

The central concept of an Alcatel Mobility Controller is of a role. The role of any wireless client determines its privileges including the priority that every type of traffic to/from the client gets in the wireless network. Thus the QoS configuration for voice applications is mostly done as part of the firewall roles and policies configuration (refer to the Configuring Firewall roles and policies document for more details).

Thus in an Alcatel system, the administrator can configure two roles – one for clients that do mostly data traffic such as laptops, and the other for clients that do mostly voice traffic such as VoIP phones. There are different means for the client to derive a role (refer to Configuring Firewall roles and policies for more details). In most cases, the users on the data traffic will be assigned a role after they get authenticated by using an authentication mechanism such as 802.1x or VPN or captive portal. The role for the VoIP phones can be derived from the OUI of their MAC addresses or the SSID they associate to. This role will typically be configured to have access allowed only for the voice protocol being used (for instance: SIP, SVP etc.).

The section below shows the steps to configure an Alcatel network for the two roles with the required privileges (the allowed protocols etc.) and the priorities assigned to different types of traffic.

Configuring QoS for SVP

Follow the steps below to configure a role for phones using SVP and provide QoS for the same.

1. Create a policy called "svp-policy" that allows only SVP traffic.

(Refer to the Configuring Firewall roles and policies for more details on how to add a policy). If providing higher quality of service to the voice traffic, ensure that the *"high"* priority option is selected for the rule allowing SVP traffic as shown in the screen shot below. (**Note**: This is highly recommended when deploying voice over Wireless LAN networks). If this option is not selected, no QoS will be provided to the voice traffic.

2 Create a rule to allow SVP traffic with the high priority as show below.



3 Create a rule to allow TFTP traffic with low priority to allow for software/firmware upgrades of the SVP phones/devices.

Monitoring Configuration	Diagnostic	s Maintena	nce Pla	n Ever	nts	Reports							Sav	re Configurat	ion Logout
Switch General	Securi	ty > Fire	wall Po	licies	> Ad	d Nev	v Polic	ÿ							
Management WLAN															« Back
Network	Policy Name	•											SVP-pe	olicy	
Advanced	Rules														
RF Management	Source	Destination	Service	Action	Log	Mirror	Queue	Time	Range	BlackList	T05	802.1p Prie	ority	Action	
Calibration	any	any	"svc-svp"	permit	Yes		high			No			D	elete 🔺	•
Optimization	Add														
Protection	Course	Deskinskis	-	Consis	-			1	Minner	0		ina Danas	Dia als I	TOC	902 1 p Deinviku
Monitoring	Source	Destinatio		Servic	e	~	LUUII	LUY	MILLOL	Queue		ine kange	DIGUKL	ISC 105	ouz.1p Prioricy
Advanced	_		Service	•				_	_ /		_		_		
Security	any	🗙 any 🔽	svc-tftp	(udp 69)	~	permit	*	🔽 Log	🗆 Mirró	r 🔍 Low 🕤	High 📘	~		*	*
Roles			New												
Policies													Cance	bhA I	
AAA Servers													2 11/00		
Authentication Methods															Apply

Create a rule to allow DHCP traffic with low priority to allow the phones to use DHCP.

Monitoring Configuration	Diagnost	cs Maintena	ance Pl	an Eve	ents	Reports					Save Co	nfiguration	Lo
Switch General	Secur	ity > Fire	wall Po	olicies	> Ad	d Nev	v Polic	;y					
Management VLAN													« Ba
Network	Policy Nam	e									SVP-policy]
Advanced	Rules												
F Management	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Actio	ı I
Calibration	any	any	"svc-svp"	permit	Yes		high		No			Delete	•
Optimization	any	any	"svc-tftp"	permit	Yes		low		No			Delete	•
Protection	any	any	"svc-dhcp"	permit			low		No			Delete	• •
Monitoring	Add												
Advanced	1100											_	
iecurity												A	oply
Roles	Comma	nds						View Comman	ids				
Policies													

4 Create a role for SVP phones called *"svp-phones"* and assign the policy *"svp-policy"* to it. (Refer to Configuring Firewall Roles and Policies for more details on adding and configuring a firewall role).

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General		Security	> User Ro	les >	Add Ro	le		
Managemer WLAN Networ Radio	nt k	Role Name [svp-phones					« Back
Advanc RF Manager Calibral Optimiz	ed ment tion ration	Firewall Poli Name Ru Add	cies le Count Locat Select S	ion Ac	tion cy from tl	ne pull do	wn menu	
Protect Monitor Advanc	ion 'ing :ed	Choose fro	om Configured Polic w Policy From Exist	ies SVP-p	olicy	Location 0.	0.0	5
Security Roles Policies		C Create Ne	w Policy Create				Done Cancel	
AAA Se Authen VPN Se Firewal	ervers Itication Methods Itings I Settings	Re-authent Disabled	ication Interva	l lisables re-	authenticatic	on. A positive v	value enables authentication	1)

- 5 Configure the devices to be placed in the role *"svp-phones"* on the basis of the SSID used or OUI of their MAC address. Each of the two are explained in the following two steps:
 - i. SSID based role derivation:
 - ii. Navigate to Configuration > Security > Authentication Methods > SSID.



Monitoring	Configuration	Diagnostics	Maintenance	Plan Ev	vents Repor	rts 📃 Save Configura	ition Logout
Switch General		Security	> Authen	ication	Methods	> SSID	
Managemen	it	Authent	ication				
WLAN Networl	k	802.1x	VPN Capt	ive Portal	MAC Addres	s Stateful 802.1x	SSID
Radio		L2 Encryp	otion Advanc	ed			
Advanc	ed	Condition	Matching Value	Role Name	e Actions		
RE Managen	nent	Add					
Calibrat	ion						
Optimiz	ation						

iii.Add a condition *"equals"* with the SSID value being *"voice-SSID"* (i.e the SSID being used for voice devices) and role name being *"svp-phones"* (i.e. the role name configured in the step above).

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout		
Switch General Managemer	nt	Security > Authentication Methods > SSID Authentication > Add Condition								
WLAN Networ	k	Condition	equals 🔽							
Radio		Value	voice-SSID							
Advanc RF Manager Calibrat	ied nent tion	Role Name Apply	svp-phones 💌 ap-role trusted-ap default-vpn-role							
Protect Monitor Advanc	ion ing red	Commands	guest stateful-dot1x svp-phones stateful logon	•	、 、		<u>View Commands</u>	Ē		
Security Roles Policies AAA Se Authen	rvers tication Methods				Select from th	the role c ie pull dov	reated for svp phor vn menu	ies		

iv.Click Apply to apply the configuration.

NOTE— The changes will not take effect until this step is completed.

Monitoring Configuration	Diagnostics	Maintenance	Plan E	Events	Reports		Save Configur	ation	Logout
Switch General	Security	> Authen	tication	Meth	nods >	SSI	D		
Management	Authent	ication							
WLAN Network	802.1x	VPN Capt	ive Portal	MAC	Address	Sta	ateful 802.1x	SSID	
Radio	L2 Encryp	otion Advanc	ed	_		1			
Advanced	Condition	Matching Value	Role Nam	ie i	Actions	. 1			
RF Management	SSID equals	voice-SSID	svp-phones	Del	ete 🔺 🔻)			
Calibration	Add	Confin			itian and		riting if page		
Optimization		Comm	m the nev	w cona	nion and	prio	nuze il nece	ssary	
Protection									

- v. OUI based role derivation:
- vi.Navigate to Configuration > Security > Authentication Methods > Advanced.

Monitoring	Configuration	Diagnostics	Maintenan	ce Pla	an Ev	ents	Reports	Save Co	nfiguration	Logout
Switch General		Security Authent	> Authorication	entica	tion I	/leth	nods > .	Advanced		
Managemen WLAN Network	τ	802.1x	VPN	Captive P	ortal	MAC	Address	Stateful 802.	1x SSID	
Radio		L2 Encryp	tion Adv	anced	Pole Na	me	Actions			
Advance RF Managen Calibrati	ed n ent on	Add	Condición	Tuluc	KOIC Hu					
Optimiza	ation									

vii.Add a condition with rule type *"Mac Address"*, condition *"contains"*, value being the first three octets or the OUI of the devices being used (for instance, we are using the Spectralink OUI 00:09:7a), and role name being *"svp-phones"* i.e. the role configured in the steps above.



Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General Managemen	t	Security Authent	<pre>/ > Authent tication > A</pre>	icatio dd Co	on Meth Indition	nods > /	Advanced	« Back
WLAN Network	<	Rule Type	Mac Address 💌					
Radio		Condition	contains 💌					
Advanc	ed .	Value	00:09:7a					
Calibrat	ion	Role Name	svp-phones 🛛 💌					
Optimiza	ation	Apply						
Protecti	on	Commanda					Utaw Carrieda	
Monitori	ng	Commanus					view commands	
Advanc	ed							

viii.Click Apply to apply this configuration. **Note:** The changes will not take effect until this step is completed.

Monitoring	Configuration	Di	agnostics	Mainten	ance P	lan Ev	ents	Reports		Save Config	guration	Logout
Switch General		S	ecurity	> Aut	hentic	ation	Met	hods >	Adva	nced		
Managemen	t	Α	uthent	ication	l							
WLAN Network	(802.1x	VPN	Captive	Portal	MAG	C Address	State	eful 802.1x	SSID	
Radio			L2 Encryp	otion A	dvanced							
Advance	ed	F	Rule Type	Condition	n Value	Role Na	me	Actions				
RF Managen	nent	ma	acaddr	contains	00:09:7a	svp-phon	es	Delete 🔺	V			
Calibrati	ion	A	dd									
Optimiza	ation	_										

Note—For deployments where there is expected to be considerable delay between the switch and the Access Points, for example in a remote location where an AP is not in range of another Alcatel AP, Alcatel recommends that you enable the "local probe response" feature. (Generating probe responses on the Alcatel Mobility Controller is an optimization that allows AOS-W to take better decisions.)

To do this, access the CLI of the switch (using the console connection or by performing a Telnet/SSH into the switch) and using the following commands:

```
(Alcatel4324) (config) #ap location 0.0.0
(Alcatel4324) (sap-config location 0.0.0) #local-probe-response enable
(Alcatel4324) (sap-config location 0.0.0) #
```

```
You can also increase the value for bootstrap-threshold and radio-off-threshold to minimize the chance of AP re-booting due to tempo-
rary lost of connectivity with the Alcatel Mobility Controller.
```

Follow the steps below to configure a role for phones using SIP and provide QoS for the same.

1. Create a service for SIP traffic called *"svc-sip"* that corresponds to the UDP protocol 5060.

i. Navigate to **Configuration > Security > Advanced**.

Monitoring	Configuration	Diagnostics	Maintena	ance	Plan Eve	ents	Reports	Save Con	figuration	Logout
Switch General		Security	/ > Adv	ance	d > Serv	vices				
Management	:	Services	Destin	ations	Bandwid	th Cont	racts N	AT Pools	Time Ra	nae
WLAN		Name	Protocol	Port	End Port	4 Oone	Action	ATT 0010	TITIO I Ka	igo
Network		svc-dhcp	udp	67	68	Edit	Delete			
Radio		svc-smb-tcp	tcp	445	N/A	Edit	Delete			
Advance RE Managore	ed and	svc-https	tep	443	N/A	Edit	Delete			
Calibrati	on	svc-ike	udp	500	N/A	Edit	Delete			
Optimiza	ition	svc-l2tp	udp	1701	N/A	Edit	Delete			
Protectio	on	svc-svslon	udo	514	NA	Edit	Delete			
Monitorir	ng	syc-pptp	ten	1723	N/A	Edit	Delete			
Advance	ed .	svc-telpet	ten	23	N/A	Edit	Delete			
Security		sue lifte	ude	40	N/A	Edit	Delete			
Roles		sve-urp	uup	5969	NVA	Eule Calie	Delete			
POlicies	Verr	sve-sip-cep	up	5060	NVA NVA	Eulit Eulit	Delete			
Authenti	ication Methods	svc-kerberos	uap	88	мин	Edit	Delete			
VPN Sett	tinns	svc-pop3	tcp	110	N/A	Edit	Delete			
Firewall	Settinas	svc-adp	udp	8200	N/A	Edit	Delete			
Secure A	Access	svc-dns	udp	53	N/A	Edit	Delete			
Secure S	Service Interfaces	svc-msrpc-tcp	tcp	135	139	Edit	Delete			
Advance	ed be	svc-http	tcp	80	N/A	Edit	Delete			
WLAN Intrus	ion Protection	svc-nterm	tcp	1026	1028	Edit	Delete			
Rogue A	P	svc-sip-udp	udp	5060	N/A	Edit	Delete			
Denial of	f Service	svc-papi	udp	8211	N/A	Edit	Delete			
Man-In-t	the-Middle	svc-ftp	tcp	21	N/A	Edit	Delete			
Signatur	es	svc-natt	udp	4500	N/A	Edit	Delete			
Policies		svc-svp	119	0	N/A	Edit	Delete			
		svc-gre	gre	0	N/A	Edit	Delete			
		svc-smtp	tep	25	N/A	Edit	Delete			
		svc-smb-udp	udp	445	N/A	Edit	Delete			
		svc-esp	esp	0	N/A	Edit	Delete			
		svc-bootp	udp	67	69	Edit	Delete			
		svc-snmp	udp	161	N/A	Edit	Delete			
		svc-icmp	icmp	0	N/A	Edit	Delete			
		svc-ntp	udp	123	N/A	Edit	Delete			
		syc-msrpc-udr	udp	135	139	Edit	Delete			
		svr-ssh	ten	22	N/A	Edit	Delete			
		any	anv	0	N/A	Edit	Delete			
		Add		-		2010	Doloto			
		Huu								

ii. Click Add to add a new service alias for SIP traffic. Enter the details for SIP traffic i.e Service name = "svc-sip", Protocol = "UDP", Starting port = "5060".



Monitoring	Configuration	Diagnostics 1	Maintenance	Plan	Events	Reports	Save Configuratio	on Logout
Switch General		Security >	Advance	ed > S	ervice	s > Add		« Back
Managemer	ıt	Service						
WLAN Networ	k	Service Name	svc-sip					
Radio		Protocol	O TCP (O UDP O	Protocol			
Advance DE Managara	ed	Starting Port	5060					
Calibrat	ion	End Port						
Optimiz	ation							Apply
Protect	ion	Commands					View Co	mmands
Monitor	ing							

iii.Click Apply to apply the configuration.

NOTE—The changes will not take effect until this step is completed.

2 Create a policy called *"sip-policy"* that allows only SIP traffic (refer to Configuring Firewall rules and policies for more details on creating a new policy). If providing higher quality of service to the voice traffic, ensure that the *"high"* priority option is selected for the rule allowing SIP traffic as shown in the screen shot below. If this option is not selected, no QoS will be provided to the voice traffic.

Monitoring Configuration	Diagnostics Maintena	nce Plan Events F	Reports				Save Config	juration Logout
Switch General	Security > Fire	vall Policies > Ad	d New Polic	Y				
Management WLAN								« Back
Radio	Policy Name						sip-policy	
Advanced RF Management Calibration	Rules Source Destination Add	Service Action Log	Mirror Queue	Time Range I	BlackList TOS	802.1p Priority	Action	
Optimization	Source Destinatio	n Service	Action	Log Mirror	r Queue	Time Range	Black List TOS	i 802.1p Priority
Protection Monitoring Advanced Security	any 💙 any 💙	service V Service svc-sip-udp (udp 5060) V New	permit 🗸	🗌 🗆 Log 🗖 Mirro	or ⊂ Low ® High	v [v
Roles Policies							Cancel Add	Apply

3 Create a role for SIP phones called "*sip-phones*" and assign the policy "*sip-policy*" to it.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Add Role
Management WLAN Network	« Back Role Name sip-phones
Advanced RF Management Calibration Optimization	Firewall Policies Name Rule Count Location Action Add Add
Protection Monitoring Advanced	Choose from Configured Policies sip-policy V Location 0.0.0 Create New Policy From Existing Policy sip-policy V Create
Security Roles Policies AAA Servers	C Create New Policy Create Done Cancel
Authentication Methods VPN Settings Firewall Settings	Re-authentication Interval Disabled Change (0 disables re-authentication. A positive value enables authentication)

- 4 Configure the devices to be placed in the role "*sip-phones*" on the basis of the SSID used or the OUI of their MAC address. Each of the two are explained in the following two steps respectively:
 - i. SSID based role derivation:
 - ii. Navigate to Configuration > Security > Authentication Methods > SSID.

Monitoring	Configuration	Diagnostics	Maintenance	Plan Ev	ents Reports	Save Configuratio	on Logout
Switch General		Security	> Authen	tication I	Methods >	SSID	
Managemen	ıt	Authent	ication				
WLAN Network	<	802.1x	VPN Cap	tive Portal	MAC Address	Stateful 802.1x	SSID
Radio		L2 Encryp	otion Advanc	ed 🛛			
Advanci	ed	Condition	Matching ¥alue	Role Name	Actions		
RF Managen	nent	Add					
Calibrat	ion						
Optimiza	ation						

iii.Add a condition "equals" with the SSID value being "voice-SSID" (i.e the SSID being used for voice devices) and role name being "sip-phones" (i.e. the role name configured in the step above).



Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Co	nfiguration	Logout
Switch General Managemer	ıt	Security Authen	y > Authen tication > A	ticatio dd Co	on Meth ondition	nods > S I	SID	1	« Back
WLAN Networl	k	Condition	equals 💌						
Radio		Value	voice-SSID						
Advanc	ed	Role Name	sip-phones 🛛 🗸						
RF Managen Calibrat	n ent :ion	Apply							
Optimiz	ation	Commands	;					View Command	ls
Protecti	ion								
Monitor	ing								

iv.Click **Apply** to apply this configuration.

NOTE—The changes will not take effect until this step is completed

Monitoring	Configuration	Diagnostics	Maintenance	Plan Ev	ents Reports	Save Configuration Logout					
Switch General		Security	Security > Authentication Methods > SSID								
Managemer	ıt	Authen	Authentication								
WLAN Networl	k	802.1x	VPN Capt	ive Portal	MAC Address	Stateful 802.1x SSID					
Radio		L2 Encry	otion Advanc	ed							
Advanc	ed	Condition	Matching Value	Role Name	Actions						
RF Managen	nent	SSID equals	voice-SSID	sip-phones	Delete 🔺 🔻						
Calibrat	ion	Add									
Optimiz	ation										
Protecti	on										

v. OUI based role derivation:

vi.Navigate to Configuration > Security > Authentication Methods > Advanced.

Monitoring	Configuration	Diagnosti	cs Mainte	enance P	lan Ever	nts Reports	Save Configuration	Logout
Switch General Managemen	t	Secur Authe	ity > Au nticatio	ithentic n	ation M	ethods >	Advanced	
WLAN Network	¢	802.1 L2 En	x VPN cryption	Captive Advanced	Portal	MAC Address	Stateful 802.1x	SSID
Advanci	ed	Rule Ty	pe Conditi	ion Value	Role Nam	e Actions	v	
RF Managen Calibrat	ion	Add	Click to		ule fer cir	nhanas		
Optimiza Protecti	ation on	\smile	CHER to a	auu new n	ule for sig	p-phones		

vii.Add a condition with rule type "Mac Address", condition "contains", value being the first three octets or the OUI of the devices being used (for instance, we are using an example OUI 00:0a:0b), and role name being "sip-phones" i.e. the role configured in the steps above.

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout	
Switch General Management		Security > Authentication Methods > Advanced Authentication > Add Condition							
WLAN Network		Rule Type	Mac Address 💌						
Radio Advanced		Condition Value	contains 💌 00:0a:0b						
RF Management Calibration Optimization Protection Monitoring		Role Name Apply	sip-phones 💌 👻						
		Commands	;				View Comman	<u>ds</u>	

viii.Click **Apply** to apply this configuration.

NOTE—The changes will not take effect until this step is completed.



Monitoring	Configuration	Diagnostics	Maintenan	ice Plan	Events	Reports	Save Configuration	Logout		
Switch General		Security > Authentication Methods > Advanced								
Management		Authentication								
WLAN Network		802.1x	VPN	Captive Portal MA		C Address	Stateful 802.1x	SSID		
Radio		L2 Encry	otion Ad	vanced						
Advanced RF Management Calibration Optimization		Rule Type	Condition	Value Ro	le Name	Actions				
		macaddr	contains	00:09:7a svp-phones		Delete 🔺 🔻				
		macaddr	contains	s 00:0a:0b sip-phones		Delet <mark>e</mark> 🔺	v			
		Add								
Protection		Be sure to put the rules in priority								
Monitoring		order using the arrow buttons								
CHAPTER 16 Topology Example One

The example included in this chapter require that the Alcatel Mobility Controller has been set up according to the instructions in the *Quick Start Guide*. These examples use specific Alcatel Mobility Controllers and Access Points. However, these configurations are valid for all Alcatel Mobility Controllers (6000, 4324, and 4308) and for all Alcatel Access Points (APs) (AP52/60/61/70), unless explicitly mentioned otherwise.

This example is based on a topology which has the following characteristics:

- Single SSID
- Directly Connected APs.
- Static WEP encryption.
- Captive portal authentication
- Single user role : Authenticated/un-authenticated.
- Rogue AP detection.



FIGURE 16-1 Example One Topology

The following steps configure the topology shown in Figure 16-1.

1. Configure the DHCP server on the switch to serve the subnet that includes the AP.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Switch > DHCP Server
Management	General Port VLAN Tunnels IP Routing VRRP DHCP Server
WLAN Network	DHCP Server Start Stop
Radio	Pool Configuration
Advanced RF Management Calibration	Name Default Router Network Range Action Add
Optimization	Excluded Address Range
Protection Monitoring Advanced	Excluded Address Add
Security	
Roles	
Policies	Арріу
AAA Servers	Commands View Commands

FIGURE 16-2 Configuring the DHCP Server

2 Click Add (Pool Configuration) and enter the details for the pool:

Monitoring Configuratio	n Diagnostics	Maintenance Plan	Events	Reports	Save Configuration	Logout
Switch General	Switch >	DHCP > Add D	HCP Poo	bl		
Management						« Back
WLAN Network	Pool Name	vlan 14				
Radio	Default Router	10.200.14.1				
Advanced	DNS Servers	10.4.0.12	(Multiple DNS	Servers sho	uld be separated by space	ces)
RF Management Calibration	Domain Name	14.ALCATEL.COM				
Optimization	WINS Servers		(Multiple WIN	IS Servers sh	ould be separated by sp	aces)
Protection	Lease	Days Hrs	s Mir	ns		
Monitoring	Network	IP Address 10.200.14.0	Netmask	255.255.25	55.0	
Advanced	Authoritative	(This should be left off	in most cases)		
Security Roles						
Policies		4	Add Car	ncel		

FIGURE 16-3 Adding the DHCP Pool

- 3 Apply this configuration and then start the DHCP server.
- 4 Add all the ports on the Alcatel Mobility Controller to the subnet 14.
- 5 On the **Configuration > Switch > Port** page, click **Select All** to select all ports on the switch and configure:
 - Add VLAN 14 in the Enter VLAN(s) field.



- Select **Make Port Trusted** to make all ports trusted.
- Select Enable 802.3af Power Over Ethernet to enable PoE on all ports.

Switch General Switch > Port Management WLAN General Port Network General Port Radio Advanced Port Selection Options Advanced Use any of the selection orker is to choose ports for configuration or more ports by icking on the ports. RF Management Use any of the selection orker is to choose ports for configuration or more ports by icking on the ports. Port Selection Contraction Optimization Cultation Optimization VLAN Association Advanced Advanced Security Advanced Roles Immediation for the port under the mouse cursor will be displayed Advanced Operational State Port Selection Immediation of the port under the mouse cursor will be displayed Advanced NA Secure Access Secure Social State N/A Secure Access Secure Social State N/A Secure Scrutes Spanning Tree N/A Manistrative State N/A Operational State N/A Power Over Ethernet N/A Spanning Tree N/A Spanning Tree N	Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
General Switch > Port Management General Port VLAN Network: Radio Advanced Des any of the selection offerious Advanced Use any of the selection offerious Optimization Optimization Prot Selection Operational State Advanced Image: Construction of the ports under the onts use the data the orts use the data the orts use the data the orts use the data the orts. Advanced Image: Construction of the port select all checkbox. Advanced Image: Construction of the port under the mouse cursor will be displayed Advanced Image: Construction of the port under the mouse cursor will be displayed Advanced Secure Service Interfaces Advanced Secure Service Interfaces Advanced Image: Construction of the port under the mouse cursor will be displayed Advanced Spanning Tree WIAN Intrusion Protection N/A Rogue AP Denial of Service Denial of Service Enable 800: 38 Prower Over Ethernet Signatures Enable 800: 38 Prower Over Ethernet Policies Enable 80: 38 Prower Over Ethernet	Switch	
Management General Port VLAN Tunnels IP Routing VRP DHCP Server Metwork Radio Advanced Port Selection criteria to choose ports for configuration or manually select one or more ports by clicking on the ports. Yue and the ports using the ports using on the ports. Ref Management Calibration Optimization Port Selection Yue and so select all the ports using the Select Aff neekbox. Optimization Optimization Image: Select Aff neekbox. Port Selection Image: Select Aff neekbox. Advanced Port Selection Image: Select Aff neekbox. Image: Select Aff neekbox. Image: Select Aff neekbox. Security Roles Image: Select Aff neekbox. Image: Select Aff neekbox. Image: Select Aff neekbox. Advanced Port Selection Image: Select Aff neekbox. Image: Select Aff neekbox. Image: Select Aff neekbox. Advanced Port Selection Image: Select Aff neekbox. Image: Select Aff neekbox. Image: Select Aff neekbox. Advanced Power Over Ethernet Image: Select Aff neekbox. Image: Select Aff neekbox. Image: Select Aff neekbox. Secure Service Interfaces Advanced N/A Image: Select Aff neekbox. Ima	General	Switch > Port
WLAN General Port VLAN Tunnels IP Routing VRP DHCP Server Network Radio Use any of the selection Options Use any of the selection core more ports by cleding on the ports. RF Management You can also select all the ports using the Select All checkbox. Image: Contract on the port of the ports. Port Mode Image: Contract on the port of the ports. Calibration Optimization Image: Contract on the port of the ports. Image: Contract on the port of the ports. Image: Contract on the ports. Monitoring Advanced Image: Contract on the port of the port. Image: Contract on the port of the port. Image: Contract on the port. Advanced Image: Contract on the port. Image: Contract on the port. Image: Contract on the port. Security Roles Image: Contract on the port. Image: Contract on the port. Image: Contract on the port. Advanced Image: Contract on the port on the port under the mouse cursor will be displayed. Administrative State N/A Secure Service Interfaces Administrative State N/A Operational State N/A Advanced Spanning Tree N/A Is Port Trusted N/A Spanning Tree N/A <td>Management</td> <td></td>	Management	
Network Port Selection Options Advanced Use any of the selection or there is to choose ports for configuration or manually select on or or more ports by cleding on the ports. RF Management You can also select all the ports using the Select All Checkbox. Calbration	WLAN	General Port VLAN Tunnels IP Routing VRRP DHCP Server
Radio Put Selection Optimization or manually select one or more ports by cloing on the ports. Ref Management You can also selection or remore ports by cloing on the ports. Calibration Optimization Optimization VLAN Association Protection VLAN Association Roles Image: Constraint of the port under the mouse cursor will be displayed Advanced Image: Current configuration of the port under the mouse cursor will be displayed Advanced Current configuration of the port under the mouse cursor will be displayed Administrative State N/A VPN Settings Administrative State Power Over Ethernet N/A VPN Settings Secure Access Secure Access Is Port an Access or a Trunk Port N/A Secure Service Interfaces Is Port an Access or a Trunk Port N/A Man-In-the-Middle Enable Port Image: Configure Selected Ports Signatures Policies Is Port Over Ethernet Image: Configure Selected Ports Policies Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Benalio of Service Enable Port Image: Configure Selected Ports Image: Configur	Network	Deut Celestian Ontinue
Advanced or manually select one or more ports by ticking on the ports. RF Management You can also select all the ports using the Select All Checkbox. Calibration	Radio	Use any of the selection criteria to choose ports for configuration
RF Management Fold Can also Select all the ports using the Select All Chebook. Galibration Optimization Protection Image: Constraint of the port subing the Select All Chebook. Monitoring Port Selection Advanced Image: Constraint of the port subing the Select All Chebook. Security Image: Constraint of the port subing the Select All Chebook. Policies Image: Constraint of the port subing the Select All Chebook. Advanced Image: Constraint of the port subing the Select All Chebook. Policies Image: Constraint of the port under the mouse cursor will be displayed. Advanced Image: Current configuration of the port under the mouse cursor will be displayed. Advanced Image: Current configuration of the port under the mouse cursor will be displayed. Advanced Power Over Ethernet N/A Secure Access Power Over Ethernet N/A Secure Service Interfaces Is Port an Access or a Trunk Port N/A Advanced Spanning Tree N/A WLAN Intrusion Protection Image: Configure Selected Ports Image: Configure Selected Ports Signatures Policies Enable Port Image: Configure Selected Ports Image: Configure Select Select Se	Advanced	or manually select one or more ports by clicking on the ports.
Optimization C Administrative State C Operational State C Port Mode Protection C VLAN Association C Trusted Image: Contract of the port Mode Advanced Port Selection Image: Contract of the port Select of the port Mode Image: Contract of the port Mode Image: Contract of the port Mode Security Image: Contract of the port Select of the port Mode Image: Contract of the port Mode Image: Contract of the port Mode Advanced Image: Contract of the port Under the mouse cursor will be displayed Administrative State N/A Advanced Image: Contract of the port Under the mouse cursor will be displayed Administrative State N/A Secure Access Power Over Ethernet N/A Is Port Trusted N/A Secure Service Interfaces Is Port an Access or a Trunk Port N/A Port Policy N/A Man-In-the-Middle Spanning Tree N/A N/A Image: Configure Selected Ports Image: Configure Selected Ports Signatures Enable Port Image: Configure Selected Ports Image: Configure Select Service Image: Configure Select Service Policies Enable Port Image: Configure Select Service	Calibration	You can also select all the ports using the Select All checkbox.
Protection Monitoring Advanced Security Roles Policies AAA Servers Authentication Methods VPN Settings Firewall Settings Secure Access Secure Service Interfaces Advanced WLAN Intrusion Protection Nan-In-the-Middle Signatures Policies Man-In-the-Middle Signatures Policies Policies Advanced VLAN Escure Coeffiguration of the port under the mouse cursor will be displayed Administrative State N/A Operational State N/A Power Over Ethernet N/A Pointie of Service Man-In-the-Middle Signatures Policies Enable Port Enable Port Enable Port Enable Port Enable Port Enable Rot Enable Rot Enable Rot	Ontimization	C Administrative State Operational State OPort Mode
Monthoring Advanced Security	Protection	Current L C Trusted
Advanced Port Selection Security	Monitoring	VLAN Association
Security 0 × × × × × × × × × × × × × × × × × × ×	Advanced	Port Selection
Roles 1 X X X X X X X X X X X Z 23 24 X X 25 AAA Servers 1 X X X X X X X X X X X Z 23 24 X X 25 AAA Servers Select All Clear All Authentication Methods VN Settings Firewall Settings Administrative State N/A Derival of Service Power Over Ethernet N/A Advanced Spanning Tree N/A VLAN Intrusion Protection Rogue AP VLAN(s) N/A Denial of Service Enable Port Image: Configure Selected Ports Enable Port Image: Configure Science Over Ethernet Image: Configure Selected Ports Policies Enable Port Image: Configure Selected Ports Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Enable Sci. 3af Power Over Ethernet Image: Configure Selected Ports Image: Configure Selected Ports Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Enable Sci. 3af Power Over Ethernet Image: Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Enable Sci. Sci. Sci. Sci. Sci. Sci. Sci. Sci.	Security	0 X X X X X X X X X X X X 22
Policies 1 X X X X X X X X X X 2 2 2 4 X X 25 AAA Servers Secure Service All Authentication Methods Current configuration of the port under the mouse cursor will be displayed Administrative State N/A Power Over Ethernet N/A Secure Service Interfaces Is Port an Access or a Trunk Port N/A Advanced Spanning Tree N/A WLAN Intrusion Protection Rogue AP VLAN(s) Man-In-the-Middle Enable Port I Signatures Enable Port I Policies Enable Port I	Roles	
AAA Servers Image: Class All	Policies	1 <u>X X X X X X X X X X X 23</u> 24 <u>X X 25</u>
Authentication Methods Current configuration of the port under the mouse cursor will be displayed Firewall Settings Administrative State N/A Operational State N/A Secure Access Power Over Ethernet N/A Is Port Trusted N/A Secure Service Interfaces Advanced Spanning Tree N/A Power Over Ethernet N/A Mutant Intrusion Protection Rogue AP VLAN(s) N/A Power Over Ethernet VIA Denial of Service Configure Selected Ports Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Signatures Enable Port Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Finale Signatures Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Secure Science Over Ethernet Image: Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Secure Science Over Ethernet Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Finable Science Power Over Ethernet Finable Science Power Over Ethern	AAA Servers	Select All Clear All
VPN Settings Current configuration of the port under the mouse cursor will be displayed Firewall Settings Administrative State N/A Operational State N/A Secure Access Power Over Ethernet N/A Is Port Policy N/A Secure Service Interfaces Advanced N/A Port Policy N/A Man-In-the-Middle Sequere Service N/A Power Over Ethernet Image: Current Configure Selected Ports Signatures Enable Port Enable Port Image: Current Configure Selected Ports Image: Current Configure Selected Ports Policies Enable Port Image: Current Configure Selected Ports Image: Current Configure Selected Ports Image: Current Cu	Authentication Methods	
Firewall Settings Administrative State N/A Operational State N/A Secure Access Power Over Ethernet N/A Is Port Trusted N/A Secure Service Is Port an Access or a Trunk Port N/A Port Policy N/A WLAN Intrusion Protection Rogue AP VIAN(s) N/A Port Policy N/A Denial of Service Configure Selected Ports VIAN(s) VIAN(s) VIAN(s) Policies Enable Port Image: Second Power Over Ethernet Image: Second Power Over Ethernet	VPN Settings	Current configuration of the port under the mouse cursor will be displayed
Secure Access Power Over Ethernet N/A Is Port Trusted N/A Secure Service Interfaces Is Port an Access or a Trunk Port N/A Port Policy N/A Advanced Spanning Tree N/A Port Policy N/A VLAN Intrusion Protection Rogue AP VLAN(s) N/A Port Policy N/A Denial of Service Configure Selected Ports Image: Configure Selected Ports Image: Configure Selected Ports Signatures Enable Port Image: Configure Selected Ports Image: Configure Selected Ports Policies Enable Row Over Ethernet Image: Configure Selected Ports Image: Configure Selected Ports	Firewall Settings	Administrative State N/A Operational State N/A
Secure Service Interfaces Is Port an Access or a Trunk Port N/A Port Policy N/A Advanced Spanning Tree N/A N/A Port Policy N/A WLAN Intrusion Protection R/A VLAN(s) N/A VLAN(s) VLAN(s) Denial of Service Configure Selected Ports VLAN(s) VLAN(s) VLAN(s) VLAN(s) Signatures Enable Port VLAN(s) VLAN(s) VLAN(s) VLAN(s) Policies Enable 802.3af Power Over Ethernet VLAN(s) VLAN(s) VLAN(s)	Secure Access	Power Over Ethernet N/A Is Port Trusted N/A
Advanced Spanning Tree N/A WLAN Intrusion Protection Spanning Tree N/A Rogue AP N/A N/A Denial of Service N/A VEX.05 N/A Man-In-the-Middle Configure Selected Ports Image: Configure Selected	Secure Service Interfaces	Is Port an Access or a Trunk Port N/A Port Policy N/A
WLAN Intrusion Protection VLAN(s) N/A Denial of Service Man-In-the-Middle Configure Selected Ports Signatures Enable Port Image: Configure Selected Ports Policies Enable 802.3af Power Over Ethernet Image: Configure Selected Ports Policies Enable 802.3af Power Over Ethernet Image: Configure Selected Ports	Advanced	Spanning Tree N/A
Denial of Service Configure Selected Ports Man-In-the-Middle Configure Selected Ports Signatures Enable Port Policies Enable 802.3af Power Over Ethernet Enable Cicro Power Over Ethernet Image: Cicro Power Over Ethernet	WLAN Intrusion Protection	VLAN(s) N/A
Denkal of 35 who Configure Selected Ports Man-In-the-Middle Enable Port Signatures Enable Port Policies Enable 802.3af Power Over Ethernet Finable Circo Power Over Ethernet/Enabling this option will disable 802.3af Power Over Ethernet/Enabling this opti	Depial of Service	
Signatures Enable Port Folicies Enable 802.3af Power Over Ethernet Fonable 802.3af Power Over Ethernet Fonable Cisco Power Over Ethernet/Fonabling this option will disable 802.3af Power Over Ethernet)	Man-In-the-Middle	Configure Selected Ports
Policies Enable 802.3af Power Over Ethernet Fnable Cisco Power Over Ethernet/Enabling this option will disable 802.3af Power Over Ethernet)	Signatures	Enable Port
Enable Cisco Power Over Ethernet/Enabling this ontion will disable 802.3af Power Over Ethernet)	Policies	Enable 802.3af Power Over Ethernet
Endor Credit of the official and the part of the space from the state of the state		Enable Cisco Power Over Ethernet(Enabling this option will disable 802.3af Power Over Ethernet)
Make Port Trusted		Make Port Trusted
Port Mode C Access C Trunk		Port Mode C Access C Trunk
Enter VLAN(s) 14 < 14 🗸		Enter VLAN(s) 14 < 14 🗸
Firewall Policy 🔽 🔽 Delete		Firewall Policy 🔽 🔽 Delete
Enable MUX		Enable MUX
Spanning Tree Enabled 19 Port Cost 128 Priority Fort Fast		Spanning Tree Spanning Tree
Apply		Apply

FIGURE 16-4 Configuring the Ports

- 6 Apply this configuration.
- 7 Plug the Alcatel AP into one of the fast Ethernet ports. The Alcatel AP will be powered by PoE from the Alcatel Mobility Controller.
- 8 AP-provisioning steps: as per the WebUI.

9 Configure the Wireless LAN network parameters on the Configuration > Wireless LAN > Network > SSID page.

Monitoring Configuration	Diagnostics Mainte	nance Plan Event:	Reports	Save Configuration	on Logout
Switch General	WLAN > Netw	ork > Edit SSID)		« Back
Management WLAN Network Radio Advanced RF Management Calibration Optimization Protection Monitoring	Edit SSID SSID Radio Type Hide SSID SSID Default VLAN Ignore Broadcast Probe Request DTIM Period	demo-a 802.11 a/b/g ♥ □ 0 < None ♥ 1	Encryption Type	C NULL ⓒ WEP C TKIP C C Mixed TKIP/AES-CCM WEP I♥ Static WEP □ Dynamic WEP	AES-CCM
Advanced Security Roles Policies	WEP Keys	s applied globally)	a global key not ha	r is applied, then WEP ke ve to be entered below	eys do
AAA Servers Authentication Methods VPN Settings Firewall Settings Secure Access Secure Service Interfaces Advanced WLAN Intrusion Protection Rogue AP Denial of Service	5. No 1 2 3 4 Commands	Use as Ta C C C Enter 40-bit Enter 128-b	KEY WEP	Key	Size 10 Hex ▼ 10 Hex ▼ 10 Hex ▼ 10 Hex ▼ 10 Hex ▼
Man-In-the-Middle Signatures			Apply		

FIGURE 16-5 Configuring the SSID

- 10 Click Edit to change the parameters of the default Wireless LAN network. Specify the following basic configuration:
 - SSID (demo-Alcatel)
 - Encryption type (Static WEP).
 - WEP key.
- 11 Apply this configuration.
- 12 Enable the AP to accept association requests from clients by configuring the maximum number of clients permitted on each Access Point. Configure this parameter on the **Configuration > Wireless LAN > Radio** page by increasing the value of Max Clients from 0 to the required value (20 in this example).



Monitoring Configuration	Diagnostics Maintenan	ce Plan Events	Reports	Save Configuration Log
Switch General	WLAN > Radio >	> 802.11b/g		
Management WLAN	802.11b/g 802.11	la		
Network	RTS Threshold (bytes)	2333	Ageout (secs)	1000
Advanced	Hide SSID		Deny Broadcast	C Enable 🖲 Disable
RF Management	Max Retries	4	DTIM Period	1
Calibration	Max Clients	20	Beacon Period (ms)	100
Optimization Protection	Initial Radio State	€ Up C Down	Mode	Access Point C Air Monitor
Monitoring	Default Channel	1 🗸	Initial Transmit Power	14 dBm(25.119 mW) 🔽
Advanced	Short Preamble	V		
Security Roles	Basic Rates (Mbps)		9 🗆 11 🗆 12 🗆 1	8 🗆 24 🗖 36 🗖 48 🗖 54
Policies	Supported Rates (Mbps)	▼ 1 ▼ 2 ▼ 5 ▼ 6 ▼	9 🗹 11 🔽 12 🔽 1	8 🔽 24 🔽 36 🔽 48 🔽 54
AAA Servers Authentication Methods	Commands			<u>View Commands</u>
VPN Settings Firewall Settings	Apply Clear			

FIGURE 16-6 Configuring the Radio Parameters

- 13 Apply this configuration.
- 14 Configure the role for an authenticated user (called authenticated-user in this example) on the **Configuration > Security > Roles** page.

Monitoring	Configuration	Diagnostics	Maintenance	Plan Events	Reports	Save Configu	Iration	Logout
Switch General		Security	> User Rol	es				
Management		Name	Firewall Po	licies Bandw	idth Contract	Actions		
WLAN		ap-role	control, ap-acl	Not Enfo	rced	Edit Dele	te	
Network Radio		trusted-ap	allowall	Not Enfo	rced	Edit Dele	te	
Advance	d	default-vpn-role	e allowall	Not Enfo	rced	Edit Dele	te	
RF Managem	ent	guest	control,cplogout	Not Enfo	rced	Edit Dele	te	
Calibratio	n	stateful-dot1×	Not Configured	Not Enfo	rced	Edit Dele	te	
Optimizal	tion	svp-phones	SVP-policy	Not Enfo	rced	Edit Dele	te	
Protectio Monitorin	n	stateful	control	Not Enfo	rced	Edit Dele	te	
Advance	d	logon	control,captiveport	al,vpnlogon Not Enfo	rced	Edit Dele	te	
Security		sip-phones	sip-policy	Not Enfo	rced	Edit Dele	te	
Roles		Add					_	
Policies								

FIGURE 16-7 Configuring the User Roles

- 15 Click **Add** to add a new user-defined role called authenticated-user. Configure the following:
 - Name of the user-role : authenticated-user.
 - Privileges for a user in this role : In this case, choose allowall to give all privileges to an authenticated user. Click **Done** after choosing the policy called allowall from the list to add the policy to this user-role.
- 16 Click **Apply** to apply this configuration.

Monitoring Configuration	Diagnostics	Maintenance Plan	Events Reports	Save Configuration
Switch General	Security	> User Roles		
Management	Name	Firewall Policies	Bandwidth Contract	Actions
WLAN	ap-role	control, ap-acl	Not Enforced	Edit Delete
Network	trusted-ap	allowall	Not Enforced	Edit Delete
Advanced	default-vpn-role	e allowall	Not Enforced	Edit Delete
RF Management	guest	control, cplogout	Not Enforced	Edit Delete
Calibration	stateful-dot1×	Not Configured	Not Enforced	Edit Delete
Optimization	svp-phones	SVP-policy	Not Enforced	Edit Delete
Monitorina	stateful	control	Not Enforced	Edit Delete
Advanced	logon	control, captive portal, vpnlogo	n Not Enforced	Edit Delete
Security	sip-phones	sip-policy	Not Enforced	Edit Delete
Roles	Add			

FIGURE 16-8 Adding User Roles

- 17 Configure the authentication parameters for Captive Portal Authentication on the Configuration > Security >Authentication Methods page. Select the Captive Portal tab to configure the parameters. Configure the following parameters:
 - Ensure that the Authentication Enabled option is selected.
 - Change the default-role to authenticated-user from the list of roles.
 - Add an authentication server that will be used to authenticate the user. In this case, we will use the Internal authentication server that is provided in the switch.

18 Apply this configuration.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch	Security > Authentication Methods > Captive
General	Portal Authentication
Management WIAN	
Network	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID
Radio	L2 Encryption Advanced
Advanced	
RF Management	Authentication Enabled 🔽
Calibration	Default Role authenticated-user 💌
Protection	Enable Guest Logon
Monitorina	Enable User Logon
Advanced	Enable Logout Popun Window
Security	
Roles	
Policies	Redirect Pause Time(secs)
AAA Servers	Welcome Page Location /auth/welcome.html
Authentication Methods	Logon Wait Interval 5 - 10 seconds
Firewall Settings	CPU Utilization Threshold 60 %
Secure Access	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Secure Service Interfaces	Show FQDN List
Advanced	Sygate On-Demand Agent
WLAN Intrusion Protection	
Rogue AP	
Man-In-the-Middle	Remediation railure role Togon
Signatures	Remediation nature or L N/A
Policies	
10100	A disc the first for the
	Authentication Servers
	Internal Local 10.200.14.211 p/a Epabled Delete A
	nyy)
	Configuration has been changed successfully

FIGURE 16-9 Configuring Captive Port Authentication

19 This step is not needed if you are using an external authentication server. If you are using the internal server, use the following CLI commands to add the required users to the database:

(Wireless LAN-switch) #local-userdb add username <username> password <password> role authenticated-user

CHAPTER 17 Topology Example Two

The example included in this chapter require that the Alcatel Mobility Controller has been set up according to the instructions in the *Quick Start Guide*. These examples use specific Alcatel Mobility Controllers and Access Points. However, these configurations are valid for all Alcatel Mobility Controllers (6000, 4324, and 4308) and for all Alcatel Access Points (APs) (AP52/60/61), unless explicitly mentioned otherwise.

This example is based on a topology which has the following characteristics:

- Indirectly connected APs (Layer 3 connected to the Alcatel Mobility Controller).
- No location specific configuration for Access Points.
- ADP enabled and configured in the network.
- Employee/guest roles.
 - Employees authenticating using 802.1x, and
 - Guests using guest logon using captive portal and using static WEP encryption.



FIGURE 17-1 Example Two Topology

This section covers some basic network configuration required to allow the Access Points to use the Alcatel Discovery Protocol to discover the Alcatel Mobility Controller.

1. In this example, configure an IP helper address on the Layer-3 switch on the same subnet as the Access Points with the IP address of the Alcatel Mobility Controller. Additionally, configure an IP helper address on the Layer-3 switch for the DHCP server that serves the subnet of the APs.

Layer-3 Switch Configuration

```
layer3(config) #interface vlan 15
layer3(config-if) #ip helper-address 10.4.0.12
; DHCP Relay
```

layer3(config-if) #ip helper-address 10.200.14.14

; ADP relay

2 Configure the Wireless LAN parameters for the Wireless LAN network on the Configuration > Network > SSID page. Click Edit to modify the parameters of the default Wireless LAN network.

Monitoring Configuration	Diagnostic:	5 Maintenan	ce Plan Event	s Reports	Save Configu	Iration Logout
Switch General	WLAN	> Networ	k > SSID			
Management	SSID	General				
WLAN						
Network	SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Period	Actions
Radio	demo-a	802.11a/b/g	Default	Static WEP	1	Edit
Advanced	company-ss	id 802.11a/b/g	Default	Static WEP	1	Edit Delete
RF Management						
Calibration		Add a SSI) called company	-ssid, if it exists	, click	
Optimization	Add	ec	lit to confirm the	confirmation		
Protection						

FIGURE 17-2 Configuring SSIDs

3 Configure the SSID of the network as desired (company-ssid in the example). Select WEP as the encryption type and select both Static WEP and Dynamic WEP. Also enter the static WEP key to be used, as shown below.



Monitoring Configuration	Diagnostics M	laintenance P	lan Event:	s Reports		Save Configu	ration Logout
Switch General	WLAN > N	etwork >	Add SSIC)			« Back
Management	Add SSID						
WLAN	SSID	company-	ssid				
Network	Radio Tuno	902.11 s/b	la 🐱			• WEP O TK	IP C AES-CCM
Radio	Kaulo Type		y v		O Mixed 1	KIP/AES-CCM	
Advanced RE Management	Hide SSID			Encryption Type	WEP	ital yineb ceri	
Calibration	SSID Default VLAN	0 <	None 🔽		Chable U		a wen
Optimization	Ignore Broadcast Probe Request				It State v	исе портап	
Protection	DTIM Period	1					
Monitoring							
Advanced							
Security	WEP Keys						
Roles	🗹 Apply Globally						
Policies	S. No	Use as Tx Key	WEP Key			Size	
AAA Servers	1	C	•••••	•		10 Hex 🔽	
Authentication Methods	2	0				26 Hex 🗸	
VPN Settings		~					
Firewall Settings	3	0				26 Hex 💌	
Secure Access	4	0				26 Hex 🔽	
Secure Service Interfaces	E	Enter 40-bit WEP ke	ys as 10 hexad	ecimal digits(0-9.	a-f, or A-F)		
Advanced	E	Enter 128-bit WEP k	eys as 26 hexa	decimal digits(0-	9.a-f, or A-F)		
WLAN Intrusion Protection							
Rogue AP	Commands					View Comman	<u>ds</u>
Denial of Service							
Man-In-the-Middle				Apply			
Signatures				мрріу			

FIGURE 17-3 Editing the SSID

4 Apply the configuration to complete the Wireless LAN network configuration. 5 To enable the APs to accept associations from clients, configure the Max Clients value on the Wireless LAN > Radio > 802.11b/g page. (Configure the same on the 802.11a page if you are also using 802.11a clients).

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configurati	ion Logo
Switch General	WLAN > Radio > 802.11b/g If using 802.11a also configurate	Max
Management WLAN	802.11b/g 802.11a	
Network	RTS Threshold (bytes) 2333 Ageout (secs) 1000	
Radio	Hide SSID Deny Broadcast C Enable Disable	
RE Management	Max Retries 4 DTIM Period 1	
Calibration	Max Cliente 20 Percent Paried /max	
Optimization	Max cliencs 20 Beacon Period (ms) 100	
Protection	Initial Radio State C Up C Down Mode C Access Point C Air	r Monitor
Monitoring	Default Channel 1 💌 Initial Transmit Power 14 dBm(25.119 mW)	¥
Advanced	Short Preamble	
Security Roles	Basic Rates (Mbps) 🔽 1 🔽 2 🗆 5 🗆 6 🗔 9 🗔 11 🗔 12 🗔 18 🗔 24 🗔 36 🗔 46	3 🗖 54
Policies	Supported Rates (Mbps) 🔽 1 🔽 2 🔽 5 🔽 6 🔽 9 🔽 11 🔽 12 🔽 18 🔽 24 🔽 36 🔽 48	3 🔽 54
AAA Servers		
Authentication Methods	Commands <u>View Commands</u>	
VPN Settings		
Firewall Settings	Apply Clear	
Secure Access	(PPP)) acar	

FIGURE 17-4 Configuring the Radios

6 Apply this configuration to enable Access Points to accept associations.

For the RADIUS server configuration, the client IP address is the IP address of the interface that connects the Alcatel Mobility Controller to the RADIUS server. In this example, VLAN 14 is the interface. Therefore, the client IP address for the RADIUS server configuration is the IP address of the VLAN 14 interface (10.200.14.6).

The NAS-IP-Address¹ is the loopback IP address or the switch IP of the Alcatel Mobility Controller. In this case, the value of this IP address if 10.200.14.14.

7 Configure the roles and their associated privileges for the users authenticated using 802.1x and the guest users (authenticated by using guest logon on captive portal). To do this, create a role called "authenticated-user" on the **Configuration > Security > Role** page and configure it to have all privileges by adding the pre-defined policy called allowall to the list of policies for this role.

^{1.}Effective with AOS-W 2.4 and higher, you can configure the NAS-IP-Address attribute per RA-DIUS server (as opposed to one NAS IP address per system). This means you can configure a Wireless LAN environment with multiple RADIUS servers, each owned by a different ISP.



Monitoring Configuration	Diagnostics N	1aintenance Plan	Events Reports S	ave Configuration	Logout
Switch General	Security >	User Roles			
Management	Name	Firewall Policies	Bandwidth Contract	Actions	
WLAN	ap-role	control, ap-acl	Not Enforced	Edit Delete	
Network	and an end		No. C. Constant	E IN Delate	
Radio	authenticated-user	allowall	Not Enforced	Edit Delete	
Advanced	trusted-ap	allowall	Not Enforced	Edit Delete	
RF Management	default-vpn-role	allowall	Not Enforced	Edit Delete	
Calibration	guest	control, cplogout	Not Enforced	Edit Delete	
Optimization	stateful-dot1×	Not Configured	Not Enforced	Edit Delete	
Monitoring	svp-phones	SVP-policy	Not Enforced	Edit Delete	
Advanced	stateful	control	Not Enforced	Edit Delete	
Security	logon	control, captiveportal, vpnlo	gon Not Enforced	Edit Delete	
Roles	sip-phones	sip-policy	Not Enforced	Edit Delete	
Policies	Add Do	An entry of the second second	tine for		
AAA Servers		termine if an role e	XISTS TOP		
Authentication Methods	au	thenticated-user: If	it exists click		
VPN Settings	au	a, in not call to com	in consulation		

FIGURE 17-5 Configuring User Roles

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Edit Role
Management	(authenticated-user)
WLAN	" Back
Network	~ D00K
Radio	
Advanced	Firewall Policies
RF Management	Name Rule Count Location Action
Calibration	allowall 1 0.0.0 Edit Delete 🔺 🔻
Optimization	Add
Protection	
Monitoring	
Advanced	Re-authentication Interval
Security	Disabled Change (0 disables re-authentication. A positive value enables authentication)
Roles	

FIGURE 17-6 Adding User Roles

- 8 Configure the pre-defined guest role to have privileges to only use HTTP protocol. To do this, configure the pre-defined policy called guest on the **Configuration > Security > Policies** page to add a rule to allow HTTP traffic.
- 9 Apply this configuration to complete configuring the guest policy.

Diagnostic	s Maintena	nce 🛛 Pla	n Ever	nts Rep	orts						Save	Configura	tion Logout
Securi	ity > Firev	wall Po	licies	> Edit I	Policy(gu								
													« Back
Rules													
Source	Destination	Service	Action	Log Mi	rror Queue	Time	e Range	BlackList	TOS	802.1p Pr	iority	Action	
any	any	"svc-http"	permit		low			No			De	lete 🔺	•
Add													
Source	Destinatio	n	Service	e	Action	Log	Mirror	Queue	Ti	me Range	Black List	TOS	802.1p Priority
any	🗙 any 💌	service Service svc-http New	▶ os (tep 443)	perm	it 💌	🗆 Log	Mirror	●Low C ⊢	ligh 🚺			~	V
											Cancel	Add	
													Apply
Commar	nds					Viev	w Comman	<u>ds</u>					

FIGURE 17-7 Applying the User Role Configuration

Diagnos	tics Maintena	nce Pla	n Ever	nts	Reports								Save	e Configuration	Logout
Secu	rity > Fire	wall Po	licies	> Ed	it Poli	cy(gue	est)								
															« Back
															- Duble
Rules															
Source	e Destination	Service	Action	Log	Mirror	Queue	Time Ra	inge 🛛	BlackList	TOS	802.1p Priori	ty Ac	tion		
any	any	"svc-http"	permit			low		N	0			Delete	• 🔺 🔻		
any	any	"svc-https"	permit			low		N	0			Delete	• 🔺 🔻		
Add															
_	Source	Destina	tion Se	rvice		Action	Log	Mirror	Que	ue	Time Range	Black List	TOS	802.1p Priority	Y
network	. •)														
Host 1 IP	0.0.0.0	any	✓ any	*	reject	~	🗹 Log	🗆 Mirro	or • Low	C High	*		~	~	
Mask 2	55.255.255.0	Sele	cting "n	etwo	rk" fron	the pul	Idown	menu	will one	n un					
_		the ri	le confi	aurat	ion for	a notwo	rk rulo	Tore	ioct an	ontiro					
		are ru	euk	gui al		0 and a	255.0.0	10 cub	not	enare		Cancel	Add		
			346	mer u	3e x.o.	.o and a	200.0.0		mer		Be	sure to c	lick Ad	d Apply	
Comma	ands						View Co	mmands				then Ap	ply		

FIGURE 17-8 Editing Policies

10 Add this policy to the list of applied policies to the pre-defined role guest to complete configuration guest privileges on the network.



Monitoring	Configuration	Diagnosti	cs Maintei	nance Pl	an Events	Repor	ts 📕 Save Configuration	Logout
Switch General		Secur	ity > Use	er Roles	s > Edit F	Role(gu	iest)	
Managemen	it							« Back
WLAN								
Network	k							_
Radio		Firewall	Policies					
Advanc	ed	Name	Rule Count	Location	Acti	DN		
RF Managen	nent	control	7	0.0.0	Edit Delet	:e 🔺 🔻		
Calibrat	ion	cplogout	1	0.0.0	Edit Delet	e 🔺 🔻		
Optimiza	ation	Add						
Protecti	ion	Add						

FIGURE 17-9 Adding Policies to Roles

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Edit Role(guest)
Management WLAN Network	« Back
Radio	Firewall Policies
Advanced	Name Rule Count Location Action
RF Management	control 7 0.0.0 Edit Delete 🔺 🔻
Calibration	cplogout 1 0.0.0 Edit Delete 🔺 🔻
Optimization	Add
Protection	
Monitoring	
Advanced	
Security	Create New Policy From Existing control
Roles	C Create New Policy Create validuser
Policies	captiveportal Done Cancel
AAA Servers	allowall
Authentication Methods	vpniogon srcnat
VPN Settings	Cologout
Firewall Settings	
Secure Access	Disabled Unange (U disat ap-acl A positive value enables authentication)
C	staterul-kerberos

FIGURE 17-10 Editing Roles

- 11 Apply this configuration to complete the configuration of the guest privileges.
- 12 Complete the 802.1x configuration for the deployment model by adding the RADIUS server and its characteristics to the list of servers on the **Configura-***tion* > Security > AAA Servers > Radius page.

Monitoring	Configuration	Mainte	enance	Plan	Events	Reports				Save Configuration	Logout
Switch		Secur	itv >	AAA	Servers	s > Radiu	s Server	5			
Managemen	ıt										
WLAN		Gene	ral	Radius	LDAP	Internal DI	B Account	ing			
Network		Name	IP Add	ress	Authenticati	ion Port Acc	counting Port	Status	Action		
Radio		Add									
Advanced											

FIGURE 17-11 Configuring RADIUS Servers

Monitoring Confi	guration	Diagnostics	Maintenand	e Plan Eve	nts Reports	Save Co	onfiguration	Logout
Switch General		Security	> AAA S	ervers > Ra	adius Server	s		
Management		General	Radius	LDAP Inter	hal DB Account	ing		
WLAN		Name IP	Address Au	thentication Port	Accounting Port	Status	In Service	Action
Network		Add			_			
Radio								
Advanced								
RF Management								
Calibration								
Optimization								
Protection								
Monitoring								
Advanced								
Security								
Roles								
Policies								
AAA Servers								

FIGURE 17-12 Adding a RADIUS Server

13 Apply this configuration.

The following screen should indicate that the RADIUS server configuration is successfully applied.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration Logout
Switch General	Security > AAA Servers > Radius Servers > Add	Radius Server
Management		« Back
WLAN	Server Name	radon
Network Dadie	TP Address	10.4.0.21
Radio		
RE Management	Shared Secret	
Calibration	Verify Shared Secret	•••••
Optimization	Authentication Port	1812
Protection	Accounting Port	1813
Monitoring	Num Retries	3
Advanced	The set	
Security	Imeout	5
Roles		
Policies	Match ESSID	
AAA Servers		Add Delete
Authentication Methods		
VPN Settings	Match FQDN	
Firewall Settings		Add Delete
Secure Access	Trim FQDN	
Secure Service Interfaces	Mada	Enable 1
Advanced	Mode	
WLAN Intrusion Protection	Server Rules	
Rogue AP	Rule Action Attribute Londition Matching Value Value Action	1
Man Ta bha Middla	Add	-
Man-in-the-Middle		Apply

FIGURE 17-13 RADIUS Server Configuration Successful

- 14 Enable 802.1x authentication and configure the 802.1x parameter on the **Configuration > Security > Authentication Methods > 802.1x** page.
- 15 Choose the newly created role called authenticated-user as the default-role and User authentication as the default role.
- 16 Select Enable Authentication to enable 802.1x authentication and add the RADIUS server to the list of authentication servers.

The following screen shot shows this configuration.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > Authentication Methods > 802.1x Authentication
Management WLAN Network	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID L2 Encryption Advanced
Radio Advanced RE Management	
Calibration Optimization	Enable Reauthentication
Protection	Enable Opportunistic Key Caching (WPA2)
Monitoring	Enforce Machine Authentication
Advanced Encomitor	Enable Wired Clients
Roles	Machine Authentication Default Role guest
Policies	User Authentication Default Role authenticated-user
AAA Servers	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Authentication Methods	Advanced Configuration Show
VPN Settings	Click Add to not to "Choose an Authentication Server" nanol holew
Firewall Settings	Authentication Converse
Secure Access	Authentication Servers
Secure Service Interfaces	Name Type IP Address Authentication Port Status Actions
Advanced	Add
Roque AP	Choose an Authentication Server Apply
Denial of Service	Tradon(Server Type:Radius IP Address: 10.4.0.21) ▼ Add Cancel Be sure to apply to
Man-In-the-Middle	Tadon/Server Type:Radius IP'Address:10.4.0.21

17 Apply this configuration to complete 802.1x configuration.

FIGURE 17-14 Completing 802.1x Authentication Configuration

- 18 Select the Captive Portal tab on Authentication Methods to enable guest logon using Captive Portal.
- 19 Select Enable Guest Logon to allow for guest logon using the Captive Portal.



Monitoring Configuration	Diagnostics Maintenance Plan Events	Reports Save Configuration Logo
Switch General Management	Security > Authentication Met Portal Authentication	hods > Captive
WLAN Network Radio	802.1x VPN Captive Portal MAC L2 Encryption Advanced Instant Sector Instant Sector	C Address Stateful 802.1x SSID
Advanced RF Management Calibration	Authentication Enabled V Default Role	_
Protection Monitoring	Enable Guest Logon	
Advanced Security Roles	Enable Logout Popup Window Protocol Type	Chttp Chttps
Policies AAA Servers Authentication Methods	Redirect Pause Time(secs) Welcome Page Location	10 /auth/welcome.html
VPN Settings Firewall Settings	Logon Wait Interval CPU Utilization Threshold Authentication Failure Threshold for Station Blacklisting	5 - 10 seconds 60 % 0 (0 disables blacklisting)
Secure Access Secure Service Interfaces Advanced	Show FQDN List	
WLAN Intrusion Protection Rogue AP	Enable Agent Support	
Denial of Service Man-In-the-Middle	Remediation failure URL N/A	

FIGURE 17-15 Configuring Captive Portal Authentication

CHAPTER 18 Topology Example Three

The example included in this chapter require that the Alcatel Mobility Controller has been set up according to the instructions in the *Quick Start Guide*. These examples use specific Alcatel Mobility Controllers and Access Points. However, these configurations are valid for all Alcatel Mobility Controllers (6000, 4324, and 4308) and for all Alcatel Access Points (APs) (AP52/60/61), unless explicitly mentioned otherwise.

This example is based on a topology which has the following characteristics:

- Redundant switch.
- Indirectly connected APs.
- WEP encryption:
 - 802.1x/Dynamic WEP for employees, and
 - Static WEP using Captive Portal (Guest Logon) for guests.
- Different privileges for employees and guest on single SSID.
- Rogue AP detection.



FIGURE 18-1 Example Three Topology

Use the following steps to configure the topology shown in Figure 18-1 above:

This section applies only to Access Points in a different subnet from any Alcatel Mobility Controller. If the Access Points are in the same subnet as the Alcatel Mobility Controllers, skip this section. This section covers some basic network configuration required to allow the Access Points to use the Alcatel Discovery Protocol to discover the Alcatel Mobility Controller over a layer-3 network. There are various methods that can be used by this protocol (including IP multicast/broadcast, DHCP Vendor Specific Options and DNS resolution).

1. In this example, configure an IP helper address on the gateway for the IP addresses of the Access Points with the IP address of the Alcatel Mobility Controller.

2 Also configure an IP helper address on the Layer-3 switch for the DHCP server that serves the subnet of the APs.

Layer-3 switch configuration:

```
layer3(config) #interface vlan 15
layer3(config-if) #ip helper-address 10.4.0.12
; DHCP Relay
layer3(config-if) #ip helper-address 10.200.14.14
; ADP relay
```

3 Configure the Virtual Router Redundancy Protocol (VRRP) on both the switches on the subnet that connects the two Alcatel Mobility Controllers as shown below:

Monitoring Configuration	Diagnostics Maintenance	Plan Events Re	ports Save C	onfiguration Logout
Switch General	Switch > Virtual Ro	uter		
Management	General Port VLAN	I Tunnels IP R	louting VRRP	DHCP Server
Network	Virtual Router Table			
Radio	Router Name IP Address	VLAN Admin State	Operational State	Action
Advanced	Add			
RF Management				
Calibration	Database Synchronization P	arameters		
Optimization	Enable periodic database synchroni	ization 🔽		
Protection	Database synchronization period in	minutes 0		
Monitoring	Include RE Plan data			
Advanced	Include for Fight data	1.		
Security				Apply
Roles	Community		18-	Apply
Policies	Commanus		Vie	w Commands

FIGURE 18-2 Configuring VRRP

4 Click Add to create a new VRRP instance on the switch and configure various VRRP related parameters:



Monitorina	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Save Configuration	Logout
Switch General	comgaradori	Switch >	> VRRP >	Add Vi	rtual R	outer		« Back
Managemer WLAN	it	Virtual Router	Id	20				
Network	k	Advertisement	: Interval (msecs)					
Radio		Authentication	Password					
Advanc DE Managan	ed	Description						
Calibrat	ion	IP Address		10.200.2	00.254			
Optimiz	ation	Enable Router	Pre-emption					
Protecti	ion	Priority						
Monitor	ing	Admin State		UP	~			
Security	eu	VLAN		1 💌				
Roles		Add Cance	el					
Policies								

FIGURE 18-3 Adding Virtual Routers

- 5 Click Add configuring the various parameters and configuring the Admin state to Up.
- 6 The VRRP instance should be added to the list of VRRP instances as shown below:

Monitoring Configuration	Diagnostics Mainten	ance Plan	Events Re	ports Save	Configuration	Logout
Switch General	Switch > Virtu	al Router				
Management	General Port	VLAN TU	unnels IP R	touting VRRP	DHCP Server	
WLAN	Virtual Router Table					
Radio	Router Name IP Ad	dress VLAN	Admin State	Operational State	Action	
Advanced	20 10.200.	200.254 1	UP		Edit Delete	
RF Management	Add					
Calibration						
Optimization	Database Synchroniz	ation Paramet	ers			
Protection	Enable periodic database :	synchronization				
Monitoring	Database synchronization	period in minutes	0			
Advanced	Toclude DE Plan data					
Poles	Include for Fight data		l.			
Policies						Apply
AAA Servers	Commands			Vi	ew Commands	
Authentication Methods						
VPN Settings						

FIGURE 18-4 Completing VRRP Configuration

7 Configure the Wireless LAN parameters for the Wireless LAN network on the **Configuration > Network > SSID** page. Click **Edit** to modify the parameters of the default Wireless LAN network

Monitoring	Configuration	Diagnostics	Maintenan	ce Plan Event	s Reports	Save Configu	uration Logout
Switch General		WLAN >	> Networ	k > SSID			
Management		SSID	General				
Network		CCTD	D - 4 - T	companya di su su	F	DTM D	
Necmon		5510	кадю туре	SSID Default VLAN	Encryption Type	DTIM Period	Actions
Radio		demo-a	802.11a/b/g	Default	Static WEP	1	Edit
Advanced		company-ssid	802.11a/b/g	Default	Static WEP	1	Edit Delete
RF Manageme	nt						
Calibration	ı						
Optimizatio	on	Add					
Protection							

FIGURE 18-5 Configuring SSIDs



8 Configure the SSID of the network as desired (company-ssid) in the example). Select WEP as the encryption type and select both Static WEP and Dynamic WEP. Also enter the static WEP key to be used, as shown below.

Monitoring	Configuration	Diagnostics	Maintenand	e Plan	Events	Rep	orts		Save Configu	uration	Logout
Switch General		WLAN >	Networ	k > Edi	t SSID						« Back
Manageme	nt	Edit SSID									
WLAN	rk	SSID	co	mpany-ssi	d						
Radio		Radio Type	8	12.11 a/b/g	*			O NULL @	WEP C TKIP	C AES	-CCM
Advan	ced	Hide SSID				Encrypt	tion	C Mixed TK	IP/AES-CCM		_
RF Manage	ment	SSID Default V	AN 1		1 🗸	Туре		WEP			
Calibra	ition	Japore Broads	st Brobo					🗹 Static WB	EP 🗹 Dynamic '	WEP	
Optimi	zation	Request									
Protec	tion	DTIM Period	1								
Monico	ring										
Security	ceu	WED Your									
Roles			II. / Al	RED LIEURA							
Policie	;	M Apply Globa	iliy (Always app	ileo giobaliy)	lise as T	vKev	WEP	Kev		6	ize
AAA S	ervers	1								1	0 Hex 🗸
Auther	ntication Methods	-			~						
VPN Se	ettings	2			U.						ь нех 🔽
Firewa	ll Settings	3			0					2	6 Hex 💌
Secure	Access	4			0					2	6 Hex 🔽
Secure	Service Interfaces				Enter 40-bi	t WEP key	ys as 10	hexadecimal c	ligits(0-9.a-f, or	A-F)	
Advan	ced				Enter 128-b	oit WEP k	eys as 2	6 hexadecimal	digits(0-9.a-f, o	r A-F)	
WLAN Intru Boque	sion Protection	Commanda									
Depial	of Service	cominands						<u>Vie</u>	ew Commands		
Map-II	or bervice https://www.com/					Annh	(
FIGH-1	n cho miladio					- Abbi)					

FIGURE 18-6 Editing SSIDs

9 Apply the configuration to complete the Wireless LAN network configuration. 10 To enable the APs to accept associations from clients, configure the Max Clients value on the **Wireless LAN > Radio > 802.11b/g** page. (Configure the same on 802.11a page if you are also using 802.11a clients).

Monitoring Configuration	Diagnostics Maintenan	ce Plan Events	Reports	Save Configuration Logou
Switch General	WLAN > Radio >	> 802.11b/g		
Management WLAN	802.11b/g 802.11	la		
Network	RTS Threshold (bytes)	2333	Ageout (secs)	1000
Advanced	Hide SSID		Deny Broadcast	C Enable 💿 Disable
RF Management	Max Retries	4	DTIM Period	1
Calibration	Max Clients	20	Beacon Period (ms)	100
Optimization Protection	Initial Radio State	© Up ○ Down	Mode	• Access Point C Air Monitor
Monitoring	Default Channel	1 💌	Initial Transmit Power	14 dBm(25.119 mW) 💌
Advanced	Short Preamble	v		
Security Roles	Basic Rates (Mbps)		9 🗆 11 🗆 12 🗖 1	18 🗆 24 🗖 36 🗖 48 🗖 54
Policies	Supported Rates (Mbps)	▼ 1 ▼ 2 ▼ 5 ▼ 6 ■	🔽 9 🔽 11 🔽 12 🔽 1	18 🔽 24 🔽 36 🔽 48 🔽 54
AAA Servers				
Authentication Methods	Commands			<u>View Commands</u>
VPN Settings	Apply Clear			
Firewall Settings				

FIGURE 18-7 Configuring Radios

- 11 Apply this configuration to enable Access Points to accept associations.
- 12 For the RADIUS server configuration, the client IP address is the interface IP address of the interface that connects the Alcatel Mobility Controller to the RADIUS server.

In this example, VLAN 14 is that interface. Therefore, the client IP address for the RADIUS server configuration is the IP address of the VLAN 14 interface (10.200.14.6).

The NAS-IP-Address¹ is the loopback IP address or the IP of the Alcatel Mobility Controller. In this case the value of this IP address is 10.200.14.14.

- 13 Configure the roles and their associated privileges for the users authenticated using 802.1x and the guest users (authenticated by using guest logon on captive portal).
- 14 Create a role called authenticated-user on the **Configuration > Security > Role** page and configure it to have all privileges by adding the pre-defined policy called allowall to the list of policies for this role.

^{1.}Effective with AOS-W 2.4 and higher, you can configure the NAS-IP-Address attribute per RA-DIUS server (as opposed to one NAS IP address per system). This means you can configure a Wireless LAN environment with multiple RADIUS servers, each owned by a different ISP.



Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout
Switch General	Security > User Roles > Edit Role(authenticated-user)
Management WLAN Network	« Back
Radio Advanced	Firewall Policies Name Rule Count Location Action
RF Management Calibration	Add
Optimization Protection	Choose from Configured Policies allowall Control Create New Policy From Existing Control Create Cre
Monitoring Advanced	C Create New Policy Create sip-policy create cartive control c
Security Roles	allowali Done Cancer ypnlogon srcnat
AAA Servers	Re-authentication Interval guest
Authentication Methods VPN Settings	Disabled Change (0 disal ap-acl ap-acl stateful-kerberos

FIGURE 18-8 Adding Roles

- 15 Additionally configure the pre-defined guest role to have privileges to only use HTTP protocol. To do this, configure the pre-defined policy called guest on the **Configuration > Security > Policies** page to add a rule to allow HTTP traffic.
- 16 Apply this configuration to complete configuring the guest policy.

Monitoring	Configuration	Diagnostics I	Maintenance	Plan Ev	ents	Reports	Save Cor	nfiguration	Logout
Switch General		Security >	User Ro	es					
Managemen	it	Name	Firewall	Policies	Bandw	vidth Contra	nct A	ctions	
WLAN		ap-role	control,ap-acl		Not Enfa	orced	Edit	Delete	
Networl	ĸ	authenticated-use	r Not Configured		Not Enfo	rced	Edit	Delete	
Radio Advanc	ed	trusted-ap	allowall		Not Enfo	rced	Edit	Delete	
RF Managen	nent	default-vpn-role	allowall		Not Enfo	rced	Edit	Delete	
Calibrat	ion	guest	control,cplogou	t,guest	Not Enfo	orced	Edit	Delete	
Optimiza	ation	stateful-dot1×	Not Configured		Not Enfo	rced	Edit	Delete	
Protecti Monitori	ion ina	svp-phones	SVP-policy		Not Enfo	orced	Edit	Delete	
Advanc	ed	stateful	control		Not Enfo	orced	Edit	Delete	
Security		logon	control, captive	portal, vpnlogoi	n Not Enfa	rced	Edit	Delete	
Roles		sin-nhones	sin-policy		Not Enfo	rced	Edit	Delete	
Policies		Add	or bouch				Loit	20.000	
AAA Se	rvers	Add							

FIGURE 18-9 Configuring User Roles

Diagnostics	Maintenance Pla	an Even	ts Reports						Save	Configura	ation Logout
Security	> User Roles	> Edit	Role(guest) > Edit	Policy	(gues	st)			« Back	
Location		0.0.0									
Rules											
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p	Action
any	any	svc-http	permit			low					Delete 🔺 🔻
any	any	svc-https	permit			low					Delete 🔺 🔻
10.0.0.0 255.25	5.255.0 any	any	deny send-deny-res	ponse Yes		low					Delete 🔺 🔻
Add											
											Apply

FIGURE 18-10 Editing Policies

17 Add this policy to the list of applied policies to the pre-defined role guest to complete configuration guest privileges on the network.

Monitoring	Configuration	Diagnostic:	s Mainter	nance Pl	lan E	Events	Reports	Save Configuration	Logout
Switch General		Securi	ty > Use	er Roles	s > E	dit Ro	le(gue	est)	
Managem WLAN	ent							l	« Back
Netwo	ork								
Radio		Firewall F	Policies						
Advar	nced	Name	Rule Count	Location		Action			
RF Manage	ement	control 7		0.0.0	Edit	Delete	▲ ▼		
Calibr	ation	cplogout 1		0.0.0	Edit	Delete	A V		
Optim	ization	add							
Prote	tion								
Monit	oring	6		1 m 1 m 1					-
Advar	nced	Choose	e from Configu	red Policies	guest	¥	Location	0.0.0	
Security		C Create	New Policy Fr	om Existing	control	y	 C 	reate	
Roles		O Create	New Policy (Create	validuser				
Policie	s	Crodic	Nom Folicy_		sip-policy cantivend	ortal		Dere Orecel	
AAA S	iervers				allowall			Done Cancer	
Authe	ntication Methods			1	vpnlogon srenat				
VPN S	ettings				cplogout				
Firew	all Settings	Re-authe	entication I	nterval	quest tatoful d	otlu			
Secur	e Access	Disabled	Chan	ge (Odisat	ap-acl	DUIA	A positiv	e value enables authenticatio	n)
Decu	C HCC033			5	stateful-ki	erberos			

FIGURE 18-11 Completing User Role Configuration



Monitoring	Configuration	Diagnosti	cs Maintei	nance Pl	an Event	s Reports	Save Configuration	Logout
Switch General		Secur	ity > Use	er Roles	s > Edit	Role(gue	est)	
Managemer WLAN Networ	nt							« Back
Radio		Firewall	Policies					
Advanc	ed	Name	Rule Count	Location	Act	ion		
RF Manager	nent	control	7	0.0.0	Edit Dele	te 🔺 🔻		
Calibrat	tion	cplogout	1	0.0.0	Edit Dele	te 🔺 🔻		
Optimiz	ation	quest	3	0.0.0	Edit Dele	to 1		
Protect	ion	guese	J	0.0.0	Luic Doie			
Monitor	ing	Add						
Advanc	ed							

FIGURE 18-12 Editing Roles

- 18 Apply this configuration to complete the configuration of the guest privileges.
- 19 To complete the 802.1x configuration for the deployment model add the RADIUS server and its characteristics to the list of servers on **Configuration > Security > AAA Servers > Radius** page.

Monitoring	Configuration	Diagnosti	cs Mainter	nance l	Plan Eve	nts R	leports	Save C	onfiguration	Logout
Switch General		Secur	ity > AA/	A Serve	ers > Ra	adius	Serve	rs		
Managemen	t	Gener	ral Radiu	s LDA	P Inter	nal DB	Accour	nting		
WLAN		Name	IP Address	Authenti	ication Port	Accou	inting Port	Status	In Service	Action
Network	<	Add								
Radio										

FIGURE 18-13 Configuring RADIUS Servers

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports	Save Configuration Logout
Switch General	Security > AAA Servers > Radius Servers > Add	Radius Server
Management		« Back
WLAN	Server Name	radon
Network	TP Address	10.4.0.21
Aduanced	Chanad Count	
REManagement	Shared Secret	
Calibration	Verify Shared Secret	••••••
Optimization	Authentication Port	1812
Protection	Accounting Port	1813
Monitoring	Num Retries	3
Advanced	Timeout	5
Security	Thirdeac	
Roles		
Policies	Match ESSID	
AAA Servers		Add Delete
Authentication Methods		
VPN Settings	Match FQDN	
Firewall Settings		Add Delete
Secure Access	Trim FQDN	
Secure Service Interfaces	Mode	Enable 🗸
Advanced	Comune Bullon	
Roque AP	Rule Action Attribute Condition Matching Value Value Action	
Denial of Service	Add	
Man-In-the-Middle		Apply
Signatures		mpb()

FIGURE 18-14 Adding a RADIUS Server

20 Apply this configuration.

The following screen should indicate that the RADIUS server configuration was successfully applied.

Monitoring	Configuration	Diagnost	ics Mainte	nance	Plan	Event	:s Re	eports		Save Cor	nfiguration	Logout
Switch General		Secu	ity > AA	A Ser	vers	> Ra	dius	Server	s			
Managemen	t	Gene	ral Radiu	IS L	.DAP	Interna	al DB	Account	ting			
WLAN		Name	IP Address	Authe	entication	n Port	Accour	nting Port	Status	In Service	Actio	n
Network	<	radon	10.4.0.21	1812			1813		Enabled	Yes	Edit [Delete
Radio		Add										
Advance	ed	1133										

FIGURE 18-15 Completing RADIUS Server Configuration

21 Enable 802.1x authentication and configure the 802.1x parameter on the **Configuration > Security > Authentication Methods > 802.1x** page.



22 Choose the newly created role called authenticated-user as the default-role and User authentication default role. Select Enable Authentication to enable 802.1x authentication and add the RADIUS server to the list of authentication servers.

The following screen shows this configuration.

23 Apply this configuration to complete 802.1x configuration.

Monitoring Configuration Switch General	Diagnostics Maintenance Plan Events Reports Save Configuration Logout Security > Authentication Methods > 802.1x
Management	Authentication
WLAN	
Network	802.1X VPN Captive Portal MAC Address Stateful 802.1X SSID L2 Encryption
Radio	Advanced
Advanced	
RF Management Calibration	Default Role authenticated-user
Optimization	Enable Authentication
Protection	Enable Reauthentication
Monitoring	Eachle Oppertunistic Kay Cachine (WDA2)
Advanced	Enable opportunistic key Caching (wPA2)
Security	Enforce Machine Authentication
Rules	Enable Wired Clients
POlicies	Machine Authentication Default Role guest
Authentication Methods	User Authentication Default Role
VPN Settings	Authentication Failure Threshold for Station Blacklisting 0 (0 disables blacklisting)
Firewall Settings	Advanced Configuration Show
Secure Access	····· - ····· - ····· - ···· · · · · ·
Secure Service Interfaces	
Advanced	Authentication Servers
WLAN Intrusion Protection	Name Type IP Address Authentication Port Status Actions
Rogue AP	Choose an Authentication Server
Denial of Service	Apply
Man-In-the-Middle	radon(Server Type:Radius IP Address:10.4.0.21)
Signatures	
Policies	
	Commands View Commands
<	

FIGURE 18-16 Configuring 802.1x Authentication

- 24 Select the Captive Portal tab on Authentication Methods to enable guest logon using Captive Portal.
- 25 Select Enable Guest Logon to allow guest logon using the Captive Portal.

Monitoring Configuration	Diagnostics Maintenance Plan Events Reports Save Configuration Logout		
Switch	Security > Authentication Methods > Captive		
General	Portal Authentication		
Network	802.1x VPN Captive Portal MAC Address Stateful 802.1x SSID		
Radio	L2 Encryption Advanced		
Advanced			
RF Management	Authentication Enabled 📈		
Calibration	Default Role guest		
Optimization	Enable Guest Logon		
Monitoring	Enable User Logon		
Advanced	Enable Loggit Ropus Window		
Security			
Roles	Protocol Type C http		
Policies	Redirect Pause Time(secs) 10		
AAA Servers	Welcome Page Location /auth/welcome.html		
Authentication Methods	Logon Wait Interval 5 - 10 seconds		
VPN Settings	CPU Utilization Threshold 60 %		
Firewall Settings	0 thentication Eailure Threshold for Station Blacklisting 0 (0 disables blacklisting)		
Secure Access			
Secure Service Interfaces	Show FQDN List		
WI AN Intrusion Protection	Sygate On-Demand Agent		
Rogue AP	Enable Agent Support		
Denial of Service	Remediation failure role		
Man-In-the-Middle	Remediation failure URL N/A		
Signatures			
Policies			
	Authentication Servers		
	Name Type IP Address Authentication Port Status Actions		
	Internal Local 10.200.14.211 n/a Enabled Delete 🔺 🔻		
	radon Radius 10.4.0.21 1812 Enabled Delete 🔺 🔻		
	Add Apply		

FIGURE 18-17 Configuring Captive Portal Authentication



26 Rogue AP detection and classification is enabled by default. To enable the feature that disables users from connecting to Access Points that have been identified as Rogue Access Points, go to Configuration > Wireless LAN Intrusion Detection > Rogue AP and select Disable Users from Connecting to Rogue Access Points as shown in Figure 18-18 below.

Switch General Intrusion Protection > Rogue AP Management WLAN Disable Users from Connecting to Rogue Access Points	ionitoring Configuration	
Management Disable Users from Connecting to Rogue Access Points 🔽	iwitch General	
	Management Disable Users from Connecting to Rogue Access Points	
Network Mark All New Access Points as Valid Access Points	Network	
Radio Mark Unknown Access Points as Rogue Access Points	Radio	
Advanced Clear Apply RF Management Calibration	Advanced \F Management Calibration	
Optimization Commands View Commands	Optimization	

FIGURE 18-18 Configuring Rogue APs

27 Click **Apply** to apply this configuration.



CAUTION—Be careful 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.

CHAPTER 19 Topology Example Four

Consider a building with three floors looking to deploy a switch on each floor. The APs on each floor would be connected via a L2/L3 network to local switch on that floor and would bootstrap with the same switch.

Each of these Local switches is on a different VLAN and subnet. The clients associating with each of these would also belong to the same VLAN and subnet. The switches can act as the DHCP server for the subnet or can use an external DHCP server.

To enable seamless mobility between the subnets as the clients move, mobility needs to be enabled

A brief description of the requirements that this topology satisfies is discussed below.

Redundancy

This topology consists of N local switches and 1 master switch. The master switch serves as a backup for each of the local switches.

SSID / User Firewall Policies

1.	User	Guest
	SSID	guest
	Encryption	None
	Firewall Policies	NAT users. Permission to access
	internet only	
	Authentication method	Captive portal
	VLAN	Local VLAN on the switch and the
	user is nated out.	

The guest users will be allowed to access the network using the guest SSID. This will be an open system without encryption. All the guest users will be allowed to access the internet alone. The user IP addresses will be nated. The users are authenticated using captive portal to connect to the internet.

Alternative:

In this case the guest user traffic is unencrypted. If the guest access also needs to be controlled, static WEP can be used to access to only those with the WEP key.

2.	User	Employee
	SSID	employee1
	Encryption	WPA-TKIP
	Firewall Policies	Access to the entire network
	Authentication method	MSFT PEAP using IAS RADIUS
	VLAN	Native VLAN of the local switch

The employee user will have to associate with the employee SSID and authenticate using MSFT PEAP to access the intranet. The traffic, if employee SSID used, will be encrypted.

3. User

SSID Encryption Firewall Policies Authentication method VLAN

Employee

employee2 Static WEP Access to the entire network VPN (PPTP and IPSEC) Native VLAN of the local switch

This in itself is a valid and secure access. In this case however it is used during the transitional phase before converting all system to WPA-TKIP with PEAP authentication.
Topology Diagram



Topology Description

Redundancy

This topology uses the N+1 redundancy. The master switch acts as a backup for all local switches. The master is not redundant which means that if the master goes down, the network will be affected as there is no redundant master to take its place.

However if a local switch goes down, the master will take over the operations of the local switch till the local switch recovers.



During failover, the operation state of the client is not maintained and the client will have to re-authenticate to gain access.

VRRP instance	Switches	Master and Local_101		
VLAN 101	involved			
	VRRP address	10.1.101.12		
	VRRP instance	Priority = 150		
	on local_101			
		Pre-empt = enable		
	VRRP instance	Priority = 100		
	on master			
		Pre-empt = disable		
VRRP instance	Switches	Master and Local_102		
VLAN 102	involved			
	VRRP address	10.1.102.12		
	VRRP instance	Priority = 150		
	on local_102			
		Pre-empt = enable		
	VRRP instance	Priority = 100		
	on master			
		Pre-empt = disable		
VRRP instance	Switches	Master and Local_101		
VLAN 103	involved			
	VRRP address	10.1.103.2		
	VRRP instance	Priority = 150		
	on local_103			
		Pre-empt = enable		
	VRRP instance	Priority = 100		
	on master			
		Pre-empt = disable		

Requirements on the Master Switch

- The master switch should have an interface on each of the vlans the local switches belong to.
- The master switch also has a separate VRRP instance for each of the local switches corresponding to the local switch's VLAN and subnet.
- The VRRP instances on the master have a lower priority since the master is a backup and needs to take over the Home agent functionality only if the local switch goes down.
- The preemption on all the master switch's VRRP instances is disabled.

Requirements on the Local Switch

The local switch shares a VRRP instance with the master. The address of the VRRP instance, VLAN ID on the local switch and the corresponding instance on the master must be the same. Ex. The VRRP instance between the switch local1 and master would have the VRRP address 10.1.101.10 and VLAN ID 101 configured on both switches.

- The priority of the VRRP instance on the local switch should be higher than that of the master
- The pre-emption on the local switch must be enabled to allow the local switch to take over as master when it is functional.

AP and RF Settings

AP Settings

This topology has all the APs bootstrapping to the local switch on the corresponding floor. This would mean that each of these APs need to know the Local switch address that they need to bootstrap with (the Imsip).

In addition to this, a good practice is to configure the VLAN ID the clients associating to the APs would be placed in to ensure uniformity among the clients associating to the L2 connected APs and L3 connected APs. All RF settings are configured on the master switch.

Requirements

- The configuration on the APs is the same for APs on the same floor but the vlan-id and Ims-ip differ for APs on the different floors. One approach is to number the APs such that APs connected to local switch have the same building and floor ID, but the APs on a different switch will have a different floor ID, ex. APs connected to Local1 have location ids 1.101.X, APs connected to Local2 have location ids 1.102.X and so on. The global configuration are then applied to location 1.101.0, 1.102.0 etc. where 0 is a wildcard.
- For each wildcard location (ex 1.101.0), the Imsip needs to be configured to ensure that the APs bootstrap to the right local switch. Since redundancy is used, this address **would not** the switch address of the local but the VRRP instance address, ex. 10.1.101.1.10 for VLAN 101 on local 1

RF Settings

On the RF side three SSIDs are required under location 1.101.0, 1.102.0 etc. The SSIDs, encryption, VLAN IDs and Ims-ip settings as per the topology are listed below.

Parameters		1.101.0	1.102.0	1.103.0
Lms-ip (VRRP addresses)		10.1.1	10 10.1.1	10.1.10
		1.10	02.10	3.10



SSID	guest	Vlan-ID	50	50	50
		encryption	Open system	Open system	Open system
	employee1	Vlan-ID	101	102	103
		Encryption	WPA-TKIP	WPA-TKI P	WPA-TKIP
	employee2	Vlan-ID	101	102	103
		Encryption	Static WEP	Static WEP	Static WEP
		WEP key	12345678 90	12345678 90	12345678 90

User Authentication and Access Policies

Guest Access

Guest users will use the SSID guest. Authentication method is captive portal with guest logon enabled.

- A local VLAN and subnet needs to be created on all the local switches for the guest users associating with them. Since these VLANs are not going to be visible outside the switch, we use the same VLAN ID on all switches. Create a local VLAN on the switch, ex. on switch_101 create a local VLAN 50 and a subnet 192.168.50.0/16 for that VLAN.
- **NOTE**—If guest users are placed on different vlans on the local switches, these vlans ids must be created on the master switch to allow failover.
- Create a small NAT pool of 1 5 address belonging to the switches IP address subnet and nat the guest users using that pool. For example, on local users could be nated using a pool of two address 10.1.101.15-10.1.101.16.
- Appropriate ACLs will be applied to the guest role. For example, Internet_access with nat, ensure that the user has access to the gateway, DNS after nating and deny access to all internal subnets. All traffic from the guest will be nated using the nat pool.

Employee Access with Static WEP and VPN

- The PPTP and L2TP VPN configurations need to be made as described in the user guides. The default roles for the VPN users would be employee.
- IAS server would be the authentication server of choice.
- Captive portal for employee users needs to be configured to facilitate downloading of the VPN dialers.

Employee Access with WPA TKIP and PEAP

- 802.1x authentication must be enabled for MSFT PEAP
- Set the employee role as the default role for 802.1x authentication.
- Configure the IAS RADIUS server as the authentication server.



OmniAccess RN: User Guide